Enhancing IoT Security through Advanced Machine Learning Models for Anomaly Detection

Rahat Bhatia
Computer Science and Electrical Engineering
Eastern Washington University
Cheney, USA
rbhatia@ewu.edu

Breeanna Lang
Computer Science and Electrical Engineering
Eastern Washington University
Cheney, USA
bjohnson32@ewu.edu

Dr. Sanmeet Kaur
Computer Science and Electrical Engineering
Eastern Washington University
Cheney, USA
skaur20@ewu.edu

***Abstract*— The rapid proliferation of the Internet of Things (IoT) has brought unprecedented connectivity, transforming industries and daily life. However, this integration comes with critical cybersecurity challenges, exposing IoT networks to sophisticated threats like Distributed Denial-of-Service (DDoS) attacks and other malicious activities. This paper investigates IoT vulnerabilities by analyzing the CICIoT2023 dataset and employing advanced machine learning techniques, specifically Random Forest and XGBoost, to detect and mitigate anomalies in network traffic. Through rigorous preprocessing, feature selection, and model tuning, both algorithms demonstrated exceptional performance, achieving accuracy and F1 scores exceeding 99%. XGBoost outperformed Random Forest in key metrics, showcasing its scalability and precision for complex datasets, while Random Forest proved advantageous for resource-constrained environments due to its simplicity and interpretability. This research not only highlights the strengths of machine learning in IoT security but also provides actionable insights for real-time anomaly detection and adaptive defenses. Future work aims to enhance these models for real-world deployment, adaptive learning, and broader applicability across diverse IoT ecosystems, ensuring a secure and resilient interconnected landscape.**

Keywords*— *IoT Security, Anomaly Detection, Artificial Intelligence (AI) for Cybersecurity

I. Introduction

The Internet of Things (IoT) has revolutionized the way we live and work, seamlessly integrating devices into our daily lives. From smart homes and wearable technology to industrial automation and healthcare systems, IoT devices have become indispensable. However, this connectivity has also introduced significant cybersecurity challenges, as these devices are often deployed with minimal security measures, making them attractive targets for cybercriminals.

Cyber threats to IoT systems can lead to devastating consequences, including unauthorized access, data breaches, and operational disruptions. Sensitive information such as authentication credentials, biometric data, and personal details are at constant risk of exposure. These vulnerabilities are compounded by the heterogeneous nature of IoT devices and their reliance on interconnected networks, creating a complex attack surface.

The significance of IoT security extends beyond individual devices; it impacts critical infrastructure, industries, and economies. As IoT adoption continues to grow, so does the need for robust cybersecurity frameworks. Research into IoT security not only mitigates current risks but also helps anticipate and address emerging threats.

This paper investigates existing vulnerabilities in IoT systems by analyzing widely used datasets and applying advanced machine learning techniques. By evaluating and enhancing models such as Random Forest and XGBoost, we aim to bridge gaps in existing research and propose scalable solutions for securing IoT networks. Our findings contribute to a deeper understanding of IoT cyber threats and offer actionable insights for strengthening defense mechanisms.

II. Related Work

The rapid expansion of the Internet of Things (IoT) has introduced significant security challenges, necessitating innovative research to detect and mitigate cyber threats. Machine learning has emerged as a powerful tool in IoT security, enabling adaptive and automated approaches to anomaly detection and threat mitigation. Multiple studies have explored IoT anomaly detection, including one focused on ultra-low-powered wireless networks [1] and intrusion detection using a convolutional neural network [2]. Also, secure IoT node provisioning showcases how important lightweight security mechanisms are [3]. This section reviews key contributions in the field and analyzes important datasets used in IoT security research, concluding with the rationale for selecting the CICIoT2023 dataset for this study.

IoT Security and Machine Learning

Anomaly detection plays a pivotal role in IoT security, allowing systems to identify deviations from normal behavior that could indicate malicious activity. Traditional approaches, such as rule-based and signature-based detection, are insufficient for dynamic and evolving IoT networks. Recent studies have focused on supervised learning models like Random Forest and XGBoost, as well as unsupervised methods such as clustering and autoencoders, to detect attacks [4]. These models are particularly effective in identifying patterns within high-dimensional data, making them suitable for IoT applications. Recent research in 5G networks and Software-Defined Networking has demonstrated its effectiveness in mitigated DDoS attacks [5]. The use of deep learning based methods have also been researched, with results that detect enemies in encrypted traffic [6]. Additionally, federated learning and edge computing frameworks have been explored to improve scalability and real-time response in IoT environments.

Analysis of Key Datasets

High-quality datasets are essential for training and evaluating machine learning models for IoT security. Below is an analysis of four widely used datasets in this domain:

Table 1: Dataset Comparison and Analysis

Dataset	Key Features	Attack Types	Strengths	Limitations
CICIoT 2023 [4]	218,805 entries, 47 features; attributes like flow duration, protocol type, flag counts	DDoS-SYN, DDoS-TCP, DDoS-UDP, Normal	Comprehensive, real-world scenarios, labeled data for training supervised models	Limited focus on real-time implementation
Edge-IIoT [5[	Seven-layer architecture, includes cloud, edge, and blockchain frameworks	DoS, MitM, and others	Realistic simulation of IoT environments, supports federated learning	Complex architecture may not be applicable to all IoT use cases
N-BaIoT [6]	Focuses on botnet detection (Mirai, BASHLITE); uses deep autoencoders to detect anomalies	Botnet attacks	High true positive rate, adaptable to diverse IoT devices	Limited to botnet attacks
Kitsune [7]	Lightweight solutions; uses autoencoders and tree-based algorithms	Mirai botnets	High prediction speed and accuracy, ideal for resource-constrained devices	Limited scalability for large-scale datasets

Rationale for Selecting CICIoT2023

The CICIoT2023 dataset was selected for this study due to its comprehensive nature and alignment with the objectives of the research. It provides a large, diverse dataset with labeled traffic for both normal and attack scenarios, enabling robust training and evaluation of supervised machine learning models. Its focus on large-scale attacks such as DDoS-SYN, DDoS-TCP, and DDoS-UDP reflects real-world challenges in IoT security. Furthermore, the dataset's detailed features, such as flow duration and protocol type, allow for fine-grained analysis and optimization of detection models like Random Forest and XGBoost.

III. METHODOLOGY

To enhance IoT security, this study employs advanced machine learning techniques to classify and detect malicious network traffic. The methodology focuses on leveraging widely used datasets and refining existing models to address gaps in anomaly detection. The primary objective is to develop scalable and robust machine learning models to enhance the detection and prevention of IoT cyber threats.

Data Overview

The CICIoT2023 dataset [4] is a robust benchmark for developing and evaluating machine learning models in IoT network security. It comprises 712,312 entries and 47 features that capture essential attributes of network traffic, such as flow duration, protocol types, and flag counts. These features are instrumental in distinguishing normal and anomalous behaviors. The dataset is labelled into 34 distinct traffic classes, encompassing a wide variety of threats and benign behaviors. Table 1 highlights the top 10 most common classes in the dataset, along with a brief description of each attack type.

Table 2: Most common Traffic Attacks in Dataset

Class	Instance Count	Description
DDoS-ICMP Flood	108,662	Overwhelms a target using excessive ICMP packets.
DDoS-UDP Flood	82,011	Generates excessive UDP traffic to disrupt network operations.
DDoS-TCP Flood	68,289	Utilizes TCP traffic to overload network functionality.
DDoS-PSHACK Flood	62,171	Exploits PSH and ACK flags to flood and disrupt target systems.
DDoS-RSTFIN Flood	61,652	Uses RST and FIN flags in malicious traffic to overwhelm a target.
DDoS-SYN Flood	61,460	Launches SYN packets to exhaust system resources.
DDoS-Synonymous IP Flood	54,749	Utilizes multiple identical source IPs to target a system.
DoS-UDP Flood	50,371	Overloads the target using excessive UDP traffic in a denial-of-service attack.
DoS-TCP Flood	40,391	Overwhelms the target by exploiting TCP traffic for denial-of-service attacks.
Benign Traffic	16,577	Regular, non-malicious network behavior.

Figure 1 illustrates the distribution of traffic classes in the dataset, highlighting the number of instances for each of the 34 classes. The visualization showcases the significant diversity within the dataset, with certain classes, such as DDoS-ICMP Flood, DDoS-UDP Flood, and DDoS-TCP Flood, dominating in terms of frequency, while others, including rare attack patterns like SQL Injection and XSS, are less prevalent.

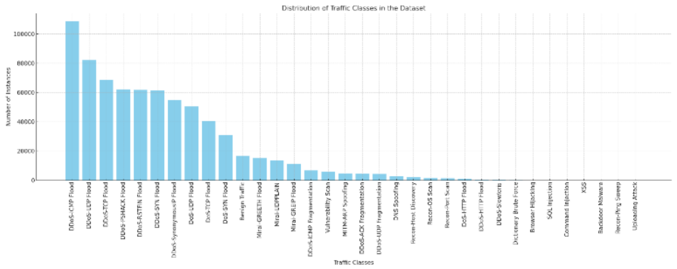

Figure 1: Distribution of Traffic Classes in the Dataset

Data Preprocessing

Data preprocessing is a critical step in ensuring the accuracy and reliability of machine learning models. In this study, several steps were undertaken to prepare the CICIoT2023 dataset for analysis. First, missing and invalid entries, such as NaN and infinite values, were removed, and duplicate rows were eliminated to maintain data integrity. Categorical labels in the target column were encoded using label encoding to convert them into numerical representations suitable for computation. To ensure uniform scaling across all features, numerical attributes were standardized using z-score normalization. Dimensionality reduction was performed using Principal Component Analysis (PCA), which reduced the dataset to 20 principal components while retaining over 95% of the variance. Finally, the dataset was split into training and testing subsets in a 70:30 ratio to facilitate unbiased evaluation of the machine learning models.

Figure 2 provides a comprehensive visual representation of the preprocessing pipeline, showcasing the sequential flow from data cleaning to feature scaling, encoding, dimensionality reduction, and data splitting. This diagram highlights the structured approach taken to optimize the dataset for effective modeling and underscores the importance of preprocessing in achieving reliable results.

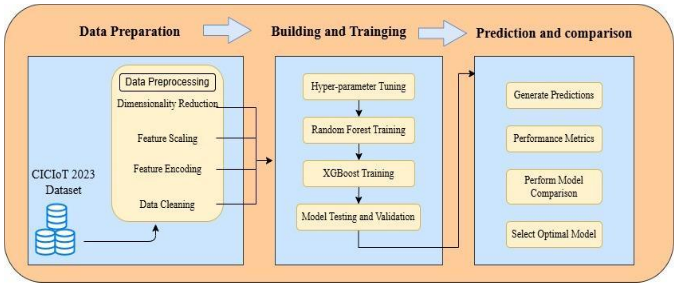

Figure 2: Methodology Workflow

Model Selection

Two machine learning models, Random Forest and XGBoost, were selected for their proven effectiveness in handling large-scale datasets and complex features:

- Random Forest: An ensemble learning method that constructs multiple decision trees and averages their predictions to classify network traffic. It is known for high accuracy, robustness against overfitting, and interpretability through feature importance scores.
- XGBoost: A gradient boosting framework designed for scalability and efficiency, offering regularization to prevent overfitting and parallel computing capabilities for faster processing. Its flexibility in hyperparameter tuning ensures optimal performance across diverse IoT scenarios.

IV. Implementation and Results

This section combines the details of the implementation process and the outcomes of applying machine learning models to the CICIoT2023 dataset. It describes the configurations, tools, and libraries used, as well as the performance of the models in detecting IoT anomalies.

Implementation Details

The implementation focused on leveraging ensemble learning (Random Forest) and gradient boosting (XGBoost) techniques to classify network traffic and identify malicious activity. Each model was fine-tuned using hyperparameters to maximize accuracy and minimize false positives. Python was the primary programming language, with key libraries including Scikit-learn, XGBoost, Pandas, NumPy, and Matplotlib.

- Random Forest Configuration: This model used 100 trees with no maximum depth, ensuring that nodes expanded until all leaves were pure or contained minimal samples. The configuration ensured high accuracy and robust performance.
- XGBoost Configuration: XGBoost utilized 100 boosting rounds with a learning rate of 0.1 and a maximum tree depth of 6. Subsampling and column sampling rates were set to 0.8 to enhance generalization and prevent overfitting.

Model Performance

The performance of both models was evaluated using commonly employed metrics in machine learning: accuracy, precision, recall, and F1 score. These metrics provide a comprehensive understanding of the models' effectiveness in classifying traffic data. The following table summarizes their results, accompanied by the formulas and interpretations of these metrics:

Accuracy:

Accuracy measures the overall correctness of the model by calculating the proportion of correctly classified instances (true positives and true negatives) out of all instances. It indicates how well the model predicts across all classes.

$$Accuracy = \frac{(True\ Positives\ +\ True\ Negatives)}{\begin{pmatrix} True\ Positives\ +\ True\ Negatives\ + \\ False\ Positives\ +\ False\ Negatives \end{pmatrix}}$$

Equation 1: Accuracy Calculation

Precision:

Precision measures the accuracy of positive predictions by calculating the proportion of true positive instances out of all predicted positives. It highlights the model’s ability to minimize false positives.

$$Precision = \frac{True\ Positives}{(True\ Positives + False\ Positives)}$$

Equation 2: Precision Calculation

Recall:

Recall, also known as sensitivity or true positive rate, measures the model’s ability to correctly identify actual positives by calculating the proportion of true positives out of all actual positive instances.

$$Recall\ = \frac{True\ Positives}{(True\ Positives\ +\ False\ Negatives)}$$

Equation 3: Recall Calculation

F1 Score:

The F1 score provides a harmonic mean of precision and recall, offering a balanced metric that is particularly useful when there is a trade-off between these two metrics. It is most valuable in scenarios with imbalanced datasets.

$$F1\,Score\ =\ 2 * \frac{(Precision\ *\ Recall)}{Precision + Recall}$$

Equation 4: F1 Score Calculation

The table below summarizes the performance of the Random Forest and XGBoost models:

Table 3: Performance Metrics

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	99.22%	0.991	0.990	0.990
XGBoost	99.26%	0.993	0.991	0.991

Comparative Insights

The evaluation reveals that both models demonstrated exceptional accuracy and reliability in detecting anomalies within IoT network traffic. XGBoost slightly outperformed Random Forest due to its ability to handle imbalanced datasets and fine-tune hyperparameters effectively. Random Forest, on the other hand, remained a strong candidate for quick deployment in resource-constrained environments due to its simplicity and interpretability.

In comparison with existing studies, the proposed models exhibit competitive performance. The Transformer-based approach introduced by Tseng et al. [7] achieved a multi-class classification accuracy of 99.40% on the CIC-IoT-2023 dataset, marginally outperforming the XGBoost model in this study (99.26%). However, the Transformer model's increased complexity and higher computational cost make tree-based models like Random Forest and XGBoost more suitable for real-time deployment in resource-limited IoT environments. Furthermore, the XGBoost model surpasses the LSTM (98.75%) and DNN (99.11%) models reported in the same study [9]. Compared to the MLP (97.46%) and AutoEncoder (83.81%) models explored by Abbas et al. [8], both Random Forest and XGBoost provide significantly higher accuracy, precision, recall, and F1 scores. These results confirm the robustness and efficiency of the proposed models in intrusion detection for IoT networks.

Table 4: Comparative Performance of IoT Intrusion Detection Models

	Model	Accuracy (%)	Precision	Recall	F1 Score
Two-step Data Clustering [8]	MLP	97.46	0.97	0.97	0.97
	Auto Encoder	83.81	0.83	0.84	0.8
Transformer Based Intrusion Detection [9]	Transformer	99.4	0.94	0.93	-
	RNN	99.11	0.99	0.99	0.99
	CNN	99.21	0.99	0.99	0.99
	LSTM	98.75	0.99	0.99	0.99
	DNN	99.11	0.97	0.97	0.97
Proposed System	**Random Forest**	**99.22**	**0.991**	**0.99**	**0.99**
	XGBoost	**99.26**	**0.993**	**0.991**	**0.991**

V. Conclusion and Future Work

This study explored the application of machine learning techniques, particularly Random Forest and XGBoost, to detect anomalies and improve IoT network security. Using the CICIoT2023 dataset, both models demonstrated exceptional performance, with accuracy and F1 scores exceeding 99%.

XGBoost slightly outperformed Random Forest in key metrics, showcasing its ability to handle complex datasets and optimize performance through gradient boosting.

The results emphasize the potential of machine learning in identifying and mitigating IoT-related threats. Random Forest's simplicity and interpretability make it suitable for resource-constrained environments, while XGBoost's scalability and precision are better suited for larger, more dynamic IoT systems. Together, these models provide complementary solutions for enhancing IoT security.

Future work should address several areas to further advance IoT cybersecurity. First, real-time deployment of these models should be explored to evaluate their robustness and responsiveness under dynamic conditions. This includes integration with live IoT networks to detect and mitigate threats in real-time. Second, adaptive learning mechanisms should be developed to enable continuous updates and adjustments to emerging attack patterns, ensuring long-term effectiveness. Third, future studies should consider testing these models on diverse datasets, such as those reflecting healthcare, industrial IoT, and autonomous vehicles, to evaluate their generalizability across various domains.

Additionally, integrating these models into edge and cloud computing frameworks can enhance scalability and ease of deployment, particularly for large-scale IoT networks. Lastly, optimizing the models for resource-constrained devices through techniques such as pruning or quantization can ensure practical applicability for low-power IoT environments.

In conclusion, this study highlights the transformative potential of machine learning in IoT security. By addressing the outlined challenges and exploring new avenues, these techniques can evolve into indispensable tools for safeguarding the interconnected world of IoT. Continuous innovation and real-world implementation will be essential to ensuring a secure and resilient digital future.

REFERENCES

[1] S. Salgadoe and F. Lu, "An Anomaly Detection Model for Ultra Low Powered Wireless Sensor Networks Utilizing Attributes of IEEE 802.15.4e/TSCH," *Journal of Communications*, vol. 14, no. 4, pp. 205-213, 2019. doi:10.12720/jcm.14.4.205-213.

[2] Z. Wang et al., "Lightweight Convolutional Neural Network Based Intrusion Detection System," *Journal of Communications*, vol. 15, no. 5, pp. 300-310, 2020. doi:10.12720/jcm.15.5.300-310.

[3] I. Yavuz and B. Ors, "End-to-End Secure IoT Node Provisioning," *Journal of Communications*, vol. 17, no. 2, pp. 112-120, 2022. doi:10.12720/jcm.17.2.112-120.

[4] E. C. Neto et al., "CICIOT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Preprints*, May 2023. doi:10.20944/preprints202305.0443.v1.

[5] S. V. Suryanarayana et al., "5G Networks SDN Enabled DDoS Attack Detection and Mitigation," *Journal of Communications*, vol. 16, no. 3, pp. 150-159, 2021. doi:10.12720/jcm.16.3.150-159.

[6] T. Ogino, S. Kitagami, and N. Shiratori, "A Multi-agent Based Flexible IoT Edge Computing Architecture and Application to ITS," *Journal of Communications*, vol. 18, no. 1, pp. 75-85, 2023. doi:10.12720/jcm.18.1.75-85.

[7] V. V. Thieu, N. T. Anh, and T. H. Hai, "A Variational Information Bottleneck Method for Network Intrusion Detection," *Journal of Communications*, vol. 16, no. 6, pp. 380-392, 2022. doi:10.12720/jcm.16.6.380-392.

[8] Gheni, Hadeel Q., and Wathiq L. Al-Yaseen. "Two-step data clustering for improved intrusion detection system using CICIoT2023 dataset." e-Prime-Advances in Electrical Engineering, Electronics and Energy 9 (2024): 100673.

[9] Tseng, Shu-Ming, Yan-Qi Wang, and Yung-Chung Wang. "Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset." Future Internet 16.8 (2024): 284.