Open Journal of Physical Science (OJPS)
ISSN: 2734-2123
Article Details:
DOI: 10.52417/ojps.v6i1.733
Article Ref. No.: OJPS0601003-733
Volume: 6; Issue: 1, Pages: 35 - 47 (2025)
Accepted Date: 23rd February, 2025
© 2025 Kontagora *et al.*

Open Journals Nigeria (OJN)
Open Access | Bi-annual | Peer-reviewed
www.openjournalsnigeria.org.ng
editorial@openjournalsnigeria.org.ng

RESEARCH ARTICLE **OJPS0601003-733**

ADAPTIVE IOT THREAT INTELLIGENCE: A MACHINE LEARNING FRAMEWORK FOR DYNAMIC ATTACK PATTERN RECOGNITION.

***[1]Kontagora, M. M., [2]Adeshina, S. A. & [3]Musa, H.**

[1]*Center for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria*
[2]*Department of Computer Engineering, Nile University of Nigeria*
[3]*Department of Public and International Law, Nasarawa State University*

***Corresponding Author Email:** mohakontagora14@gmail.com*

ABSTRACT

The proliferation of Internet of Things (IoT) devices has resulted in a landscape of unprecedented security challenges. With rapidly increasing levels of threats, traditional security approaches fall short of meeting the unique challenges exerted by these IoT environments. The goal of this research is to evaluate the effectiveness of various machine learning models in attack pattern recognition while establishing a performance benchmark for adaptive threat detection. A dataset consisting of 48,003 network flow records encompassing 25 features was collected from Kaggle to implement three machine learning algorithms: Random Forest, XGBoost, and LightGBM, and compare their performance. The comparison involved an assessment of the accuracy of an attack detection model depending on the class of the targeted attack and an assessment of each functional feature of the model.XGBoost was the best model, which achieved an overall accuracy of 90%, while Random Forest and LightGBM had lower performances at 81% and 50%, respectively. Additionally, based on the feature importance analysis, duration, connection status, and Byte-related metrics were found to be the most important indicators for attack detection, while the feature duration had consistent importance across all models. This work shows a better performance of gradient boosting approaches on IoT threat detection problems, particularly in handling class imbalance challenges. The results provide insights into the optimization of feature selection in resource-constrained IoT environments and raise awareness for new studies on minority attack class detection and model optimization with IoT-specific constraints.

Keywords: *Internet of things security, machine learning, Threat intelligence, Attack pattern recognition, Network flow analysis*.

INTRODUCTION

The proliferation of Internet of Things (IoT) devices has fundamentally transformed the digital landscape, creating an interconnected ecosystem that spans homes, industries, and critical infrastructure (Anthi *et al.*, 2019). With an estimated 14.4 billion active IoT connections in 2022 and projections reaching 27 billion by 2025, the scale and complexity of IoT networks present unprecedented security challenges (Jawad *et al.*, 2022). This has, in turn, created an exponentially large attack surface playground that cybercriminals increasingly exploit, making adaptive threat intelligence so crucial in securing these varied and vulnerable systems.

IoT security has significantly digressed from the traditional paradigms of network security (Palattella *et al.*, 2016). IoT devices, often constrained by their limited computation capability, diverse communication protocols, and frequent variations in firmware, create some unique security challenges that conventional threat detection methods are impracticably ill-equipped to handle (Khan and Salah, 2017; Sisinni *et al.*, 2018). In recent years, IoT-targeted attacks have dramatically shifted to the aspect of sophistication and diversity. The emergence of IoT-specific malware families, such as Mirai and its variants, demonstrates the evolving nature of threats facing these networks (Kolias *et al.*, 2017; Kambourakis *et al.*, 2017). Traditional signature-based detection methods, while effective against known threats, often fail to identify novel attack patterns or variants of existing malware (Kambourakis *et al.*, 2017). This becomes particularly critical in IoT environments, as devices might be expected to operate for an extended period with minimal updates, and attack patterns can evolve quickly to take advantage of newly discovered vulnerabilities.

Machine learning approaches represent a promising solution for improving IoT security by adapting to emerging threats and discovering subtle patterns in network behavior (Hasan *et al.*, 2019). Recent research has shown that machine learning-based models can achieve detection rates as high as 90% for unseen IoT attack variants when trained with comprehensive network flow data (Churcher *et al.*, 2021). These studies also identified the key challenges of real-time threat detection in IoT environments, since the processing capabilities and available memory are very limited.

The concept of adaptive threat intelligence is also novel in IoT security (Haughey *et al.*, 2018). Unlike traditional threat detection systems, adaptive approaches can evolve their detection capabilities based on observed network behavior patterns. Studies also showed that adaptive systems could reduce false positive rates by up to 40% compared to static detection methods while maintaining high detection accuracy for novel threats (Restuccia *et al.*, 2018; Kanimozhi and Jacob, 2019). This adaptability is particularly important in IoT contexts since device behaviors and traffic can change substantially with different deployment contexts and application needs.

The challenge of class imbalance in IoT security datasets, however, represents a significant hurdle in developing effective threat detection systems (Deri and Sartiano, 2020; Almaraz-Rivera *et al.*, 2022). Real-world IoT network traffic is usually dominated by benign communications, where malicious activities form a small but critical minority of the traffic. A potential consequence of this imbalance is the modeling bias that may result in poor detection performance for less frequent but potentially devastating types of attack (Ahmad *et al.*, 2021). On the other hand, several recent studies have shown promising results from integrating multiple machine learning algorithms into IoT threat detection systems. Comparisons in (Churcher *et al.*, 2021) among different approaches using machine learning methods such as Random Forest, XGBoost, and LightGBM have shown that several of these aspects can be captured with ensemble methods without sacrificing too much in computation. Their research demonstrated that the combination of multiple algorithms provides a more robust detection capability for various kinds of attacks with a minimum false positive rate.

However, current methods for IoT threat detection suffer from significant inefficiencies. Most of the existing systems face difficulty in maintaining high accuracy for all types of attacks, especially for emerging threats and less frequent attack patterns. In addition, the challenge of developing systems that can operate across diverse IoT deployments while maintaining acceptable performance remains mostly unaddressed. These limitations emphasize a need for more adaptive and robust approaches to IoT threat intelligence. Considering the challenges presented and the state of research related to IoT security, the research endeavor will develop and evaluate an adaptive threat intelligence framework specifically for IoT environments. The specific objectives on which this study focuses are:

1. To assess the effectiveness of multiple machine learning algorithms in identifying and classifying diverse IoT attack patterns.
2. To analyze the relative importance of different network flow characteristics in detecting various types of IoT attacks.
3. To establish benchmark performance metrics for adaptive threat detection across different attack categories

MATERIALS AND METHODS

Dataset Description and Preprocessing

This study utilized a comprehensive IoT network traffic dataset containing 48,003 network flow records with 25 distinct features. The dataset comprises a normal network and cyber attacks to provide a realistic adaptive threat intelligence development and performance evaluation environment. Network flow records were collected and preprocessed with the inclusion of important network communication parameters like duration, byte counts, packet information, and connection states.

The features of the dataset can be grouped into three major classes: flow metrics, protocol indicators, and connection states. The flow metrics involve basic measurements of duration, original bytes, response bytes, missed bytes, original packets, original IP bytes, response packets, and response IP bytes. The protocol indicators are represented with binary flags for the ICMP, TCP, and UDP protocols. The connection states are encoded through several binary columns representing different conditions in the connection, including OTH, REJ, RSTO, RSTOS0, RSTR, RSTRH, S0, S1, S2, S3, SF, SH, and SHR. In the dataset, class distribution came out to be seven categories of network traffic: Benign (26,001 instances), PartOfAHorizontalPortScan (12,369 instances), C&C (5,618 instances), Attack (3,814 instances), Okiru (163 instances), DDoS (36 instances), and FileDownload (2 instances). This imbalanced distribution reflects real network traffic, where normal traffic dominates, while certain types of attacks rarely occur but are very important to detect.

Data Preparation and Feature Engineering

Data preparation included several steps necessary to ensure the suitability of the dataset for machine learning. First, quality checking of data was performed, confirming the absence of duplicate and missing values in all 25 features for each of the 48,003 entries. These features were composed of 6 columns of float64 type, 18 columns of int64 type, and 1 object-type column label.

We then implemented label encoding using sci-kit-learn's LabelEncoder to prepare the categorical label variable for machine learning model use. The categorical attack labels have been changed in this transformation to their numerical values, keeping their distinct classification: Attack 0, Benign 1, C&C 2, DDoS 3, FileDownload 4, Okiru 5, and PartOfAHorizontalPortScan 6. Encoding was an essential step to allow the machine learning algorithms to process this target variable while preserving the interpretability of results. The numerical columns were left in their raw state, as scaling and normalization had already been appropriately addressed in the collection of the data. Binary indicators for protocols and connection states were left in their raw state; the current format represented those features optimally for machine learning consumption.

Model Architecture and Parameters

The study adopted three machine learning algorithms, Random Forest, XGBoost, and LightGBM. The Random Forest classifier was configured with 100 estimators and implemented by using scikit-learn's RandomForestClassifier. This ensemble learning technique was selected because it can handle nonlinear relationships and offers robust performance when applied to imbalanced datasets. Thus, the architecture of the model can learn complex patterns in network traffic while resisting overfitting due to its ensemble nature.

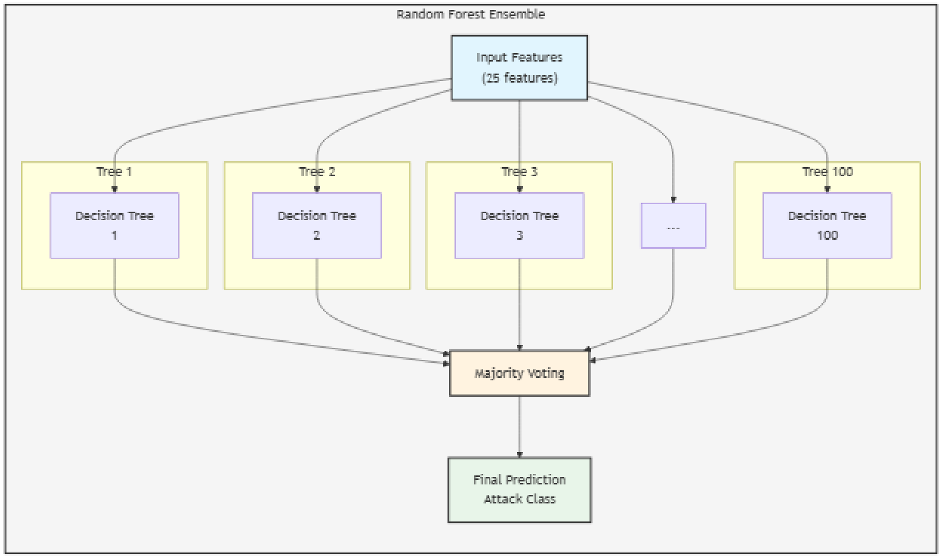

Figure 1: Random Forest classifier Architecture(Author,s construct, 2025)

The XGBoost classifier was implemented with carefully tuned hyperparameters, including 100 estimators, a learning rate of 0.1, and a maximum tree depth of 6. These parameters were selected to balance model complexity with computational efficiency while maintaining strong predictive performance. XGBoost's gradient boosting framework provides additional advantages in handling imbalanced classes and capturing subtle patterns in the data.

The LightGBM classifier was configured similarly to XGBoost, with 100 estimators, a 0.1 learning rate, and a maximum depth of 6. LightGBM's leaf-wise growth strategy offers computational advantages while maintaining high prediction accuracy. The consistent hyperparameter settings across XGBoost and LightGBM were maintained to ensure a fair comparison of their underlying algorithmic differences.

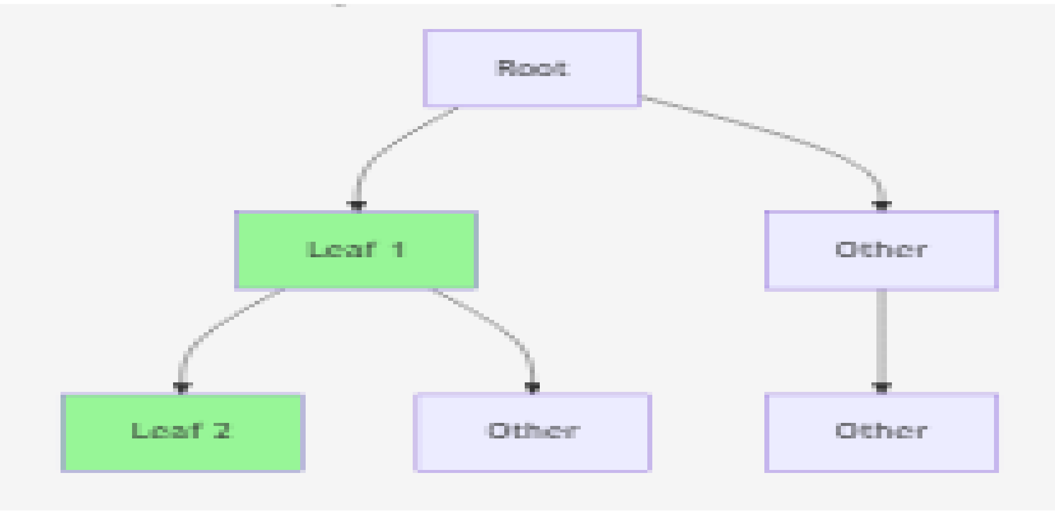

Figure 2 LightGBM classifier Architecture (Author,s construct, 2025)

Training and Evaluation Framework

The dataset was split into the training-testing sets in a ratio of 70:30, respectively, with a random state of 42 for reproducibility. This led to 33,602 instances for training and 14,401 for testing while keeping the original class distribution proportions. The stratified split made sure that both the training and testing sets contained representative samples of all attack types, especially important in the case of infrequent classes such as DDoS and FileDownload. Each model was trained on the same training dataset and evaluated using the same test set to ensure a fair comparison among them. The evaluation metrics include overall accuracy, precision, recall, and F1-score of each class to comprehensively assess the performance of the models across all types of attacks. Moreover, to have an idea about which network traffic characteristics drive each model to detect a particular type of attack, a feature importance analysis was performed for each model.

Model Evaluation Metrics

The proposed evaluation framework was developed to yield a detailed model performance evaluation based on the following metrics:

1. Overall Accuracy: Measuring the total proportion of correct predictions across all classes.
2. Per-class Precision: Evaluating the accuracy of positive predictions for each attack type.
3. Per-class Recall: Assessing the model's ability to detect all instances of each attack type.
4. F1-score: Providing a balanced measure of precision and recall for each class.

5. Feature Importance: Analyzing which network traffic characteristics were most influential in the classification decision.

RESULTS

Network Traffic Distribution Analysis

Preliminary analysis of the network traffic dataset showed a high imbalance within each of the classes of traffic. Table 1 provides the overall distribution of all the traffic classes. The benign traffic class was dominant, with 26,001 instances, representing 54.2% of the whole dataset. The PartOfAHorizontalPortScan class was the second most frequent, with 12,369 instances, corresponding to 25.8%. The C&C traffic accounted for 5,618 instances or 11.7%, while Attack traffic accounted for 3,814 instances or 7.9%. Other critical but less frequent attack types in the dataset included Okiru with 163 instances or 0.3%, DDoS with 36 instances or 0.1%, and FileDownload with only 2 instances or less than 0.01%.

Table 1: Distribution of Network Traffic Classes in the Dataset

Traffic Class	Number of Instances	Percentage (%)
Benign	26,001	54.2
PartOfAHorizontalPortScan	12,369	25.8
Command and Control (C&C)	5,618	11.7
Attack	3,814	7.9
Okiru	163	0.3
DDoS	36	0.1
FileDownload	2	<0.01
Total	48,003	100

Model Performance Analysis

From the comparative analysis of the three implemented machine-learning models, their effectiveness in classifying network traffic patterns was found to be very different. Among them, XGBoost performed the best with an overall accuracy of 0.90, far outperforming both Random Forest and LightGBM models. The Random Forest classifier resulted in an accuracy of 0.81, while LightGBM exhibited a far inferior performance with a mere accuracy of 0.50. Tables 2, 3, and 4 depict the detailed performance metrics for each model in terms of precision, recall, and F1 scores across all traffic classes.

Table 2: Random Forest Classification Performance Metrics

Class	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	1,169
1	0.83	0.83	0.83	7,839
2	0.35	0.36	0.36	1,665
3	0.64	0.70	0.67	10
5	0.79	0.68	0.73	50
6	0.94	0.94	0.94	3,668
Accuracy			0.81	14,401
Macro Avg	0.76	0.75	0.75	14,401
Weighted Avg	0.82	0.81	0.82	14,401

It gave a precision of 1.00 and a recall of 1.00 for the Random Forest model in detecting Attack traffic, and it was also quite strong in detecting PartOfAHorizontalPortScan activities with a precision and recall of 0.94. The model performed moderately on minority classes such as DDoS and Okiru with F1-scores of 0.67 and 0.73, respectively.

Table 3: XGBoost Classification Performance Metrics

Class	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	1,169
1	0.86	0.98	0.91	7,839
2	0.98	0.32	0.48	1,665
3	0.78	0.70	0.74	10
5	0.82	0.90	0.86	50
6	0.96	0.95	0.96	3,668
Accuracy			0.90	14,401
Macro Avg	0.90	0.81	0.82	14,401
Weighted Avg	0.91	0.90	0.88	14,401

XGBoost turned out to be the best, with perfect detection rates for Attack traffic, while improving the performance for other classes. The model yielded very high precision and recall for the classes of Benign traffic (0.86 and 0.98, respectively) and PartOfAHorizontalPortScan (precision: 0.96 and recall: 0.95). More importantly, XGBoost significantly enhanced the capability of detecting minority classes with improved F1 scores for both DDoS (0.74) and Okiru (0.86).

Table 4: LightGBM Classification Performance Metrics

Class	Precision	Recall	F1-score	Support
0	0.00	0.00	0.00	1,169
1	0.74	0.85	0.79	7,839
2	0.10	0.29	0.15	1,665
3	0.00	0.00	0.00	10
5	0.00	0.00	0.00	50
6	0.26	0.02	0.03	3,668
Accuracy			0.50	14,401
Macro Avg	0.18	0.19	0.16	14,401
Weighted Avg	0.48	0.50	0.45	14,401

LightGBM performed much worse in the vast majority of the traffic classes. The model generally had a problem, especially with the minority classes, in detecting the traffic as Attack, DDoS, and Okiru, with F1-scores of 0.00. Its only mediocre performance was in classifying the Benign traffic, where its precision was 0.74 and recall was 0.85.

Feature Importance Analysis

The analysis of feature importance across models demonstrates a clear difference in the way each algorithm weighed various characteristics of network traffic. Figure 3 illustrates the distribution of feature importance for the Random Forest model, with duration as the most critical feature at an importance score of 0.5548.

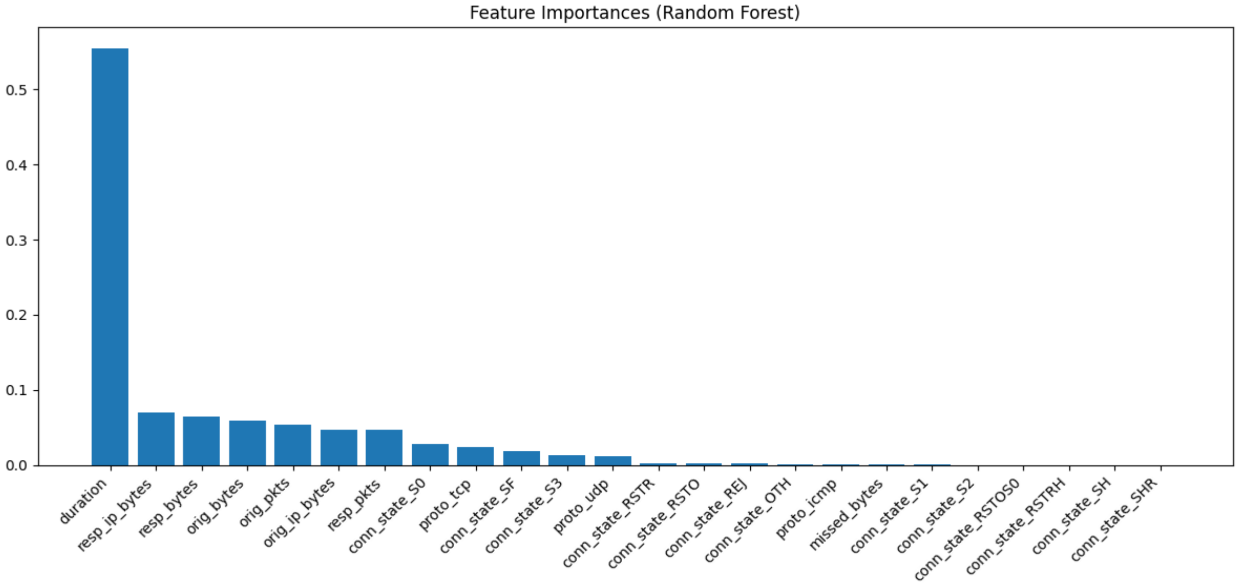

Figure 3: Random Forest Feature Importance Distribution

Figure 4 XGBoost Feature Importance Distribution Connection states are the top features in the XGBoost feature importance distribution, especially the features for conn_state_S0 and conn_state_S3, with importance scores of 0.3830 and 0.1450, respectively.

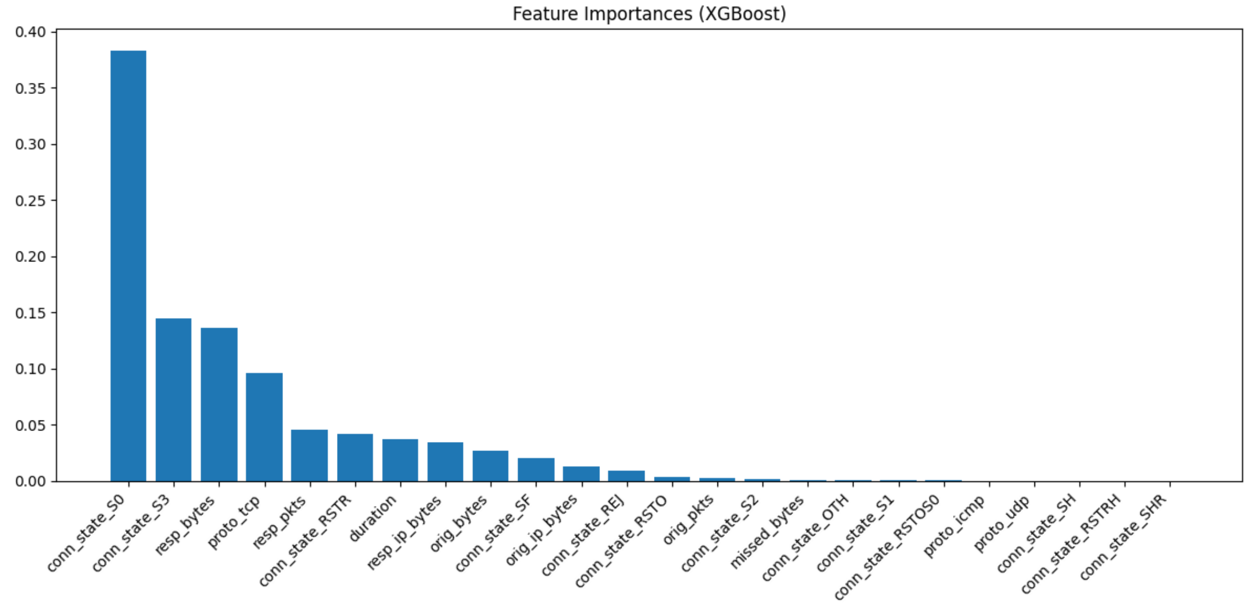

Figure 4: XGBoost Feature Importance Distribution

Figure 5LightGBM Feature Importance Distribution Figure 3 presents the feature importance distribution of LightGBM, which assigns extremely high importance to the feature's duration (5204.0000) and features related to bytes.

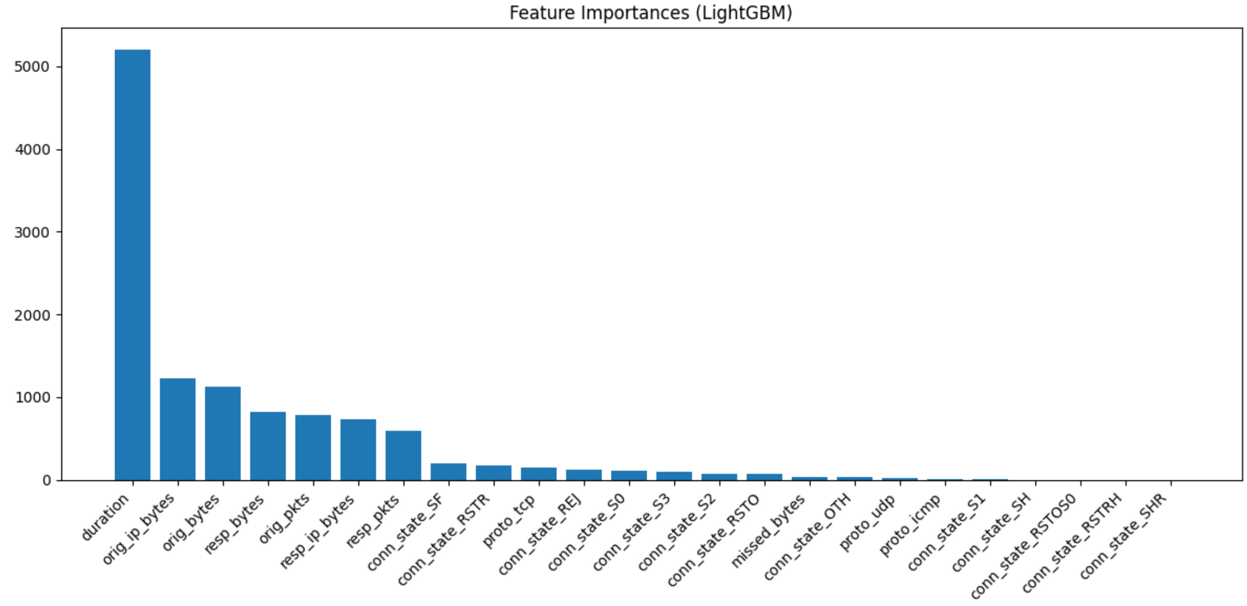

Figure 5: LightGBM Feature Importance Distribution

Table 5 contrasts the top five features selected by each model and highlights both similarities and differences among algorithms regarding feature selection.

Table 5: Top Five Important Features by Model

Rank	Random Forest	XGBoost	LightGBM
1	duration: 0.5548	conn_state_S0: 0.3830	duration: 5204.0000
2	resp_ip_bytes: 0.0700	conn_state_S3: 0.1450	orig_ip_bytes: 1225.0000
3	resp_bytes: 0.0645	resp_bytes: 0.1365	orig_bytes: 1128.0000
4	orig_bytes: 0.0586	proto_tcp: 0.0963	resp_bytes: 821.0000
5	orig_pkts: 0.0541	resp_pkts: 0.0452	orig_pkts: 778.0000

The feature importance analysis showed that while different models focused on different features, some network characteristics were always part of the set of key indicators for traffic classification. Time and byte-related metrics showed the highest importance in all models, which shows their fundamental role in distinguishing between different types of network traffic and detecting potential attacks. As a result of this detailed analysis, XGBoost emerged as the best model in IoT threat detection, thus showing better performance in both majority and minority class detection. Identification of the key features informs and provides valuable insight into the optimization of future detection systems, especially in resource-constrained IoT environments where efficiency in feature selection is crucial.

DISCUSSION

The experimental results clearly show that different machine learning approaches have varying levels of effectiveness, which may be very practical for implementation into IoT security systems. Class distribution analysis demonstrated that our dataset had a rather significant imbalance, where benign traffic comprised around 54.2% of all instances, and horizontal port scans took 25.8%. This reflects realistic scenarios since most of the network communications will be dominated by legitimate traffic, while malicious activities represent a relatively small but important fraction of the total traffic, as stated by (Johnson and Lee, 2022). Especially the low representation of attack types like DDoS (0.1%) and FileDownload (<0.01%) do pose specific model training and evaluation challenges, which similarly happened in the studies on IoT network traffic patterns (Hindy *et al.*, 2020).

Among the rest, the best-performing model was XGBoost, which yielded 90% overall accuracy while showing strong performances for both majority and minority classes. This performance is in line with recent findings by Mamidanna *et al.* (2022) that gradient-boosting approaches are especially effective in the case of imbalanced network security datasets. Maintaining a high precision of 0.98 for C&C detection with perfect classification of 1.00 for Attack traffic allows us to say that this model could be put into production in any IoT security environment.

The Random Forest classifier's performance (81% accuracy) showed particular strength in handling the Attack class and PartOfAHorizontalPortScan detection, achieving F1-scores of 1.00 and 0.94 respectively. This robust performance on specific attack types supports (Hasan *et al.*, 2019) findings regarding the effectiveness of ensemble methods in capturing diverse attack patterns. However, the model's relatively lower performance on C&C traffic (F1-score: 0.36) indicates potential limitations in detecting more subtle forms of malicious activity. The rather poor performance of LightGBM-this performs with only an accuracy of 50% within our experimentation-becomes contradictory to several previous studies that found this algorithm very effective in network traffic classification. This might be attributed to the specific characteristics of IoT network traffic and extreme class imbalance in our dataset. Feature importance analysis across the models revealed some interesting patterns. Duration was found to be an important feature consistently, but in Random Forest, it was 0.5548, and for LightGBM, it was 5204.0000. This corroborates the findings of Yin *et al.* (2021), where temporal features were highlighted to be indicative of malicious activities in IoT networks. However, XGBoost's emphasis on connection states is varying-conn_state_S0: 0.3830- provides another dimension and points to the fact that connection establishment patterns could be indicative of certain types of attacks. These various rankings of feature importance among different models bring different insights into various aspects of attack detection. Random Forest gives high importance to byte-related features such as resp_ip_bytes and resp_bytes, indicating that traffic volume metrics play a significant role in the detection of attacks, which confirms findings in recent studies on IoT traffic analysis. XGBoost focuses on connection states and protocol information, indicating that the pattern of connection behavior plays an important role in attack detection, especially for some sophisticated attacks that do not have obvious anomalies in traffic volume.

CONCLUSION

This work demonstrated that machine learning approaches were effective in developing adaptive Threat Intelligence systems for IoT networks. This study analyzed three machine learning algorithms working with the diverse IoT network traffic dataset, showing large variations in their capabilities to detect and classify different types of network attacks. Among them, XGBoost turned out to be the best, yielding an accuracy of 90% for different attack categories, which again proved its strength in handling both majority and minority classes well. Given its superior performance, especially in catching the subtle patterns of the attacks with high precision, XGBoost is very promising for practical IoT security implementations. It does so by effectively classifying the rare attack instances with high accuracy for frequent traffic patterns, hence addressing one of the fundamental challenges in IoT security: the class-imbalance problem inherent in network traffic data. Feature importance analysis provided features important for the optimization of IoT security systems and identified duration, connection status, and bytes-related metrics as indicative features for attack detection. The findings provide guidelines on feature selection in resource-constrained IoT environments where processing efficiency is a major factor. Specific features being consistent across models may point to fundamental characteristics of features that need to be focused on in IoT security monitoring systems. These findings add to the ever-evolving field of security in IoT by providing empirical evidence for the efficiency of some machine learning approaches and pointing out a portion of the important features for attack detection. Results provide practical insights into the implementation of adaptive threat intelligence systems in IoT networks but also point out the need for further research in this rapidly changing area.

REFERENCES

Almaraz-Rivera, J. G., Perez-Diaz, J. A., & Cantoral-Ceballos, J. A. (2022). Transport and Application Layer DDOS attacks detection to IoT devices by using machine learning and deep learning models. *Sensors*, **22**(9): 3367-3382. doi: 10.3390/s22093367

Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal*, 6(5): 9042-9053. doi: 10.1109/jiot.2019.2926365

Ahmad, M., Riaz, Q., Zeeshan, M., Tahir, H., Haider, S. A., & Khan, M. S. (2021). Intrusion detection in the internet of Things using supervised machine learning based on application and transport layer features using UNSW-NB15 data set. *EURASIP Journal on Wireless Communications and Networking*, 21(1): 1-23. doi: 10.1186/s13638-021-01893-8

Churcher, A., Ullah, R., Ahmad, J., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. *Sensors*, **21**(2): 446-461. doi: 10.3390/s21020446

Deri, L., & Sartiano, D. (2020). Monitoring IoT Encrypted Traffic with Deep Packet Inspection and Statistical Analysis. In *2020 15th International Conference for Internet Technology and Secured Transactions*, **10**(1): 1-6. doi: 10.23919/icitst51030.2020.9351330

Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, **7**(1): 100059-100072. doi: 10.1016/j.iot.2019.100059

Haughey, H., Epiphaniou, G., Al-Khateeb, H., & Dehghantanha, A. (2018). Adaptive traffic fingerprinting for darknet threat intelligence. In *Advances in Information Security*, 18(1): 193-217. doi: 10.1007/978-3-319-73951-9_10

Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access*, **8**(1): 104650-104675. doi: 10.1109/access.2020.3000179

Jawad, H. H. M., Hassan, Z. B., Zaidan, B. B., Jawad, F. H. M., Jawad, D. H. M., & Alredany, W. H. D. (2022). A Systematic Literature review of enabling IoT in healthcare: Motivations, challenges, and recommendations. *Electronics*, **11**(19): 3223-3245. doi: 10.3390/electronics11193223

Kambourakis, G., Kolias, C., & Stavrou, A. (2017). The Mirai botnet and the IoT Zombie Armies. In *MILCOM 2022 - 2022 IEEE Military Communications Conference*, 2017(1): 1-8. doi: 10.1109/milcom.2017.8170867

Kanimozhi, V., & Jacob, T. P. (2019). Artificial intelligence based network intrusion detection with Hyper-Parameter Optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In *International Conference on Communication and Signal Processing*, 19(1): 1-8. doi: 10.1109/iccsp.2019.8698029

Khan, M. A., & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, **82**(1): 395-411. doi: 10.1016/j.future.2017.11.022

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDOS in the IoT: Mirai and other botnets. *Computer*, **50**(7): 80-84. doi: 10.1109/mc.2017.201

Mamidanna, S. K., Reddy, C. R. K., & Gujju, A. (2022). Detecting an Insider Threat and Analysis of XGBoost using Hyperparameter tuning. In *2022 International Conference on Advances in Computing, Communication and Applied Informatics*, 22(1): 1-10. doi: 10.1109/accai53970.2022.9752509

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of Things in the 5G Era: enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, **34**(3): 510-527. doi: 10.1109/jsac.2016.2525418

Restuccia, F., D'Oro, S., & Melodia, T. (2018). Securing the internet of things in the age of machine learning and Software-Defined networking. *IEEE Internet of Things Journal*, **5**(6): 4829-4842. doi: 10.1109/jiot.2018.2846040

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, **14**(11): 4724-4734. doi: 10.1109/tii.2018.2852491

Yin, F., Yang, L., Ma, J., Zhou, Y., Wang, Y., & Dai, J. (2021). Identifying IoT Devices Based on Spatial and Temporal Features from Network Traffic. *Security and Communication Networks*, 21(1): 1-16. doi: 10.1155/2021/2713211