Babylonian Journal of Internet of Things
Vol.2023, **pp**. 74–84
DOI: https://doi.org/10.58496/BJIoT/2023/010; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Enhancing IoT Security to Leveraging ML for DDoS Attack Prevention in Distributed Network Routing

Abdulazeez Alsajri[1,*], Amani Steiti [2], Hasan Ahmed Salman [1],

[1] *Computer Science Department, University Arts, Sciences and Technology, Beirut, Lebanon.*

[2] *faculty of information engineering, Department of Computer Systems And Networks, University Tishreen, Latakia, Syria.*

ARTICLE INFO

Article History

Received 17 Jun 2023
Accepted 11 Sep 2023
Published 11 Oct 2023

Keywords

DDoS Attack Prevention
Machine Learning
IoT Security
Intrusion Detection Systems(IDS)Distributed Network Routing

ABSTRACT

DDoS attacks have become much more frequent especially with the situating of IoT technologies. These attacks are based on compromising weaknesses within the IoT network and focuses on communication links used as paths to flood systems with large volumes of traffic and thereby cause system breakdowns. DDoS attacks lean on centralized control mechanisms and less available bandwidth of IoT infrastructures and the clandestine mobility of the nodes. Traditional measures of security like password and user accounts protection are typically insufficient to counteract such threats. This paper focuses on the system architectures of DDoS attack detection solutions in the IoT networks to evaluate their ability to counter the attack. More specifically, it focuses on the function of machine learning systems, which are designed to analyze previous attacks, in order to stop new attacks. The comparisons with three Machine Learning algorithms—Support Vector Machines, Random Forest, Decision Trees are done with relation to their capability to classify invasion attempts within distributed IoT network routing system. It also assesses the methods for optimising these models such as determination of hyperplane, the clustering of data point as well as the tree structure. Common performance parameters such as confusion matrix, F1 measure, and AUC-ROC are used to ensure the efficiency, effectiveness and to handle the cases with intricate unbalanced datasets to enhance the IoT network Security.

1. INTRODUCTION

The Internet of Things (IoT) is a complex system of connected devices, promoting efficient information exchange and is widely used in smart homes, health care, industrial applications and smart cities The following picture represents the IoT network architecture Figure 1 If IoT grows further more challenges arise on monitoring, privacy, social reformation, economic disparities, and political actions needed [1,2]. As the number of smart devices that continue to connect to the Internet increases, the need for safe and stable means of conveying messages also increases. They also noticed that with a large number of devices connected in the IoT network there emerged large scale distributed routing systems in which security issues and data integrity are of great concern. Such systems are usually operated through decentralized networks or through in-house host communities to have maximum uptime and failover.

*Corresponding author. Email: aka104@live.aul.edu.lb

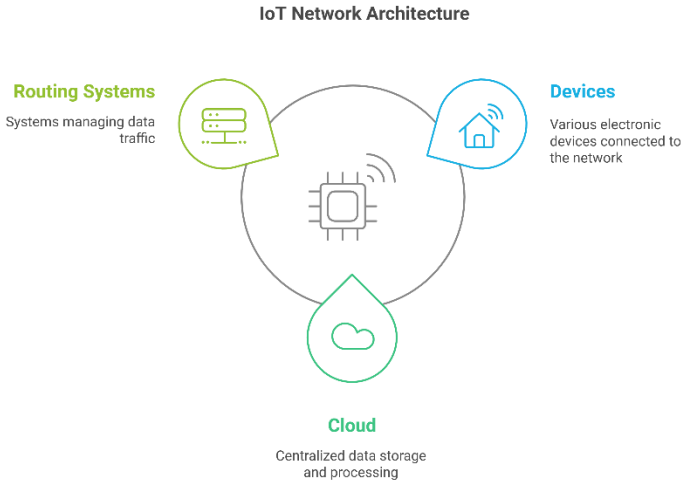

Fig. 1. IoT Network Architecture

Nonetheless, distributed computing approaches in processing tasks is seen to have possible negative impacts that develop, especially in terms of security that exists with traditional routing protocols [3]. In figure 2 illustrates DDoS Attack Flow in IoT Networks As the variety of the different networks being deployed and dynamic attacks are becoming more common this means that the IoT has to embrace stronger security solutions [4]. Distributed Denial of Service attacks have become one of the most devastating threats to IoT networks; consequently, they deepen security threats with growing privacy concerns for information seekers. This leads to dire outcomes like unauthorized access to personal information, loss of reputation and of course money. Security researchers continue to participate in investigating and analyzing the effects of these attacks and the possibility of system risks [5].

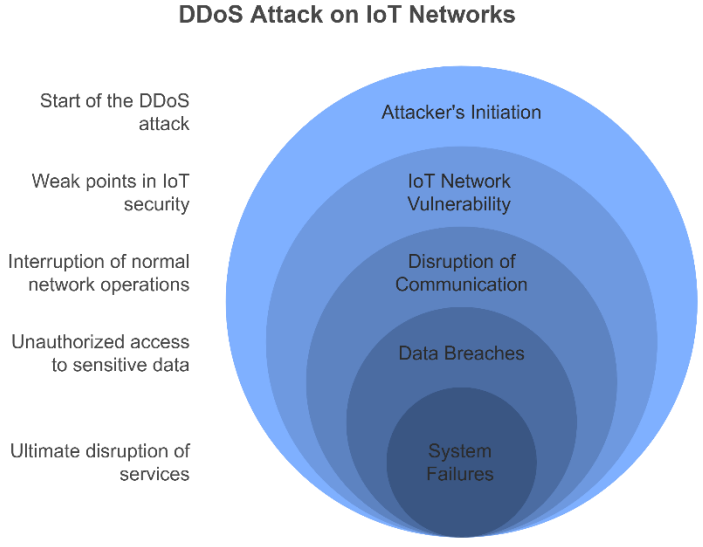

Fig. 2. DDoS Attack Flow in IoT Networks

Information transfer through distributed models is advantageous in computing models, while using the distributed system creates a security threat from routinary protocols and the system architecture. Due to the inherent dynamism witnessed in technologies such as blockchain and other distributed networks, cyber security architecture is fast emerging as a complex problem that calls for creative solution [6][7]. DDoS attacks stand to hurt IoT networks, most evidently through denying access and/or leading to leakage of information, loss of credit worthiness and financial losses. There are cooperation

between the security specialists and hackers, which played an important role in the revealing and ending of the sources of these attacks [8].
Machine learning (ML) [9], can provide a good addition to the IoT networks making it more reliable and secure. In this context, this study's objective is therefore to enhance the reliability and privacy of the IoT devices through embracing ML technology. Figure 3 on the integration of ML in IoT Networks for mitigating DDoS attacks Machine learning ML techniques are now being triggered to perform a pattern check to identify fake and misconstrued communications or flow and ensure it does not require changes to counteract the, more advanced DDoS attack methods. The goal is to implement machine learning in the IoT networks in order to capture and analyze the network traffic and therefore combat DDoS attacks..

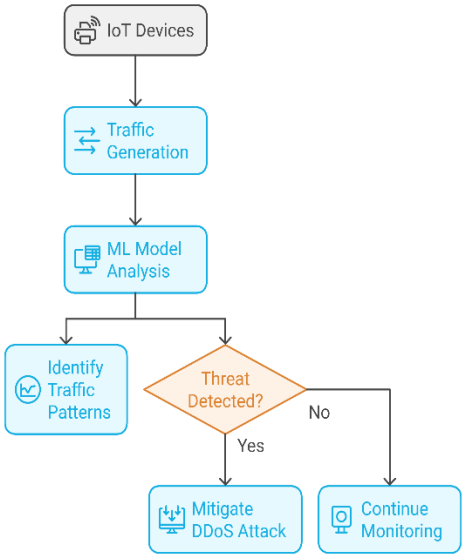

Fig. 3. ML Integration with IoT Networks for DDoS Attack Prevention

The given solution to the problem resorts to machine learning to detect threats as they use duration and previous attacks to create future threats. A good example is to use anti-malware solutions, to increase the capacity of the network, and maximize performance. The project also envisages improving IDS based on the application of new Machine Learning algorithms. Other techniques like Random Forest, Support Vector Machines and k nearest neighbor will also be used to improve alerts passing through the efficiency of layers of the supervised IDS.
The assessments for this research will be criterion referenced as shall be evidenced by the precision values, false-positive rate, false-negative rate, F1 scores, and AUC-ROC. These make IoT networks susceptible to DDoS attacks due to centralized control and a limited bandwidth to support security measures for cloud control. While IDS are widely used in IoT networks, many of them cannot offer constant protection against all kinds of threats.
To mitigate these weaknesses, this study recommends the use of advanced artificial intelligence technique namely, Deep Neural Networks (DNNs) to enhance the performance of IDS in the detection and mitigation of DDoS attacks. This attempt will use ML algorithms in conjunction with statistical and logical methods to strengthens networks and protect from black hole attacks.

2. LITERATURE REVIEW

IDS is essential for defending IoT systems and networks against increasingly common and capable DDoS attacks, which substantially degrade system and data integrity as well as posing a security concern. Conventional IDS as you are aware depend on techniques such as signature based detection, whereby traffic patterns are compared with established attacks. Still, new and more advanced DDoS attacks must be countered by specialized tools capable of responding to new and changing threats on the fly. Modern advances in the area of ML has contribute greatly to IDS in that it has allowed IDS to learn from data patterns in order to enhance its capability in detecting anomalies and new threats like zero-day attack, which would not be easily detected with other traditional means [10-12].

IDS that employs machine learning have some benefits over other detection systems. They are better accuracy, constant analysis of emerging threats and the opportunity to identify new types of threats which remain unnoticed. The most utilized ML algorithms in IDS are Random Forest or RF of SVM, or KNN and DNNs; however, each has its advantages in detecting DDoS attacks in IoT networks.

Random Forest is an ensemble learning that consists of a number of decision trees used for anomaly detection in the IoT networks. Random Forest has been reported to exhibit high sensitivity with low false positive rate thus can be used in real-time identification of DDoS [13], [14]. Like the former, SVMs are acclaimed for their first-rate performance in the classification of traffic patterns in a network. They are especially useful when network data are to be mapped into high-dimensional feature space to discover intricate attack patterns [15], [16].

K-Nearest Neighbors also known as KNN is one of the most used ML approaches for performing DDoS attack detection. KNN operates on the principle of nearest neighbour whose property makes it ideal for real-time detection since it sorts the network traffic according to data points similarities. Researchers prove that KNN works well because it encompasses a basic and easily expandable architecture and can incorporate alterations to a network [17], [14].

CNN and RNN and their subclass DNN has provided vast contribution to the field of network security as it supports feature extraction directly from the network traffic. These models are able to detect such violations of normal traffic characteristic that can be typical of DDoS attacks, even without manually selecting features that are meaningful in this context. Specifically for the development of new attack detection paradigms, literature encourages the utilization of DNNs particularly for emerging sophisticated attack types [19–20]. Table 1 provides an overview of the mature machine learning approaches for DDoS detection in IoT context: their benefits and to related studies.

TABLE I. SUMMARY OF ML ALGORITHMS FOR DDOS ATTACK DETECTION

Algorithm	Strength	Application	Reference
Random Forest (RF)	High sensitivity, minimal false positives	Anomaly detection in IoT networks	[13], [14]
Support Vector Machines (SVM)	Effective for identifying complex attack patterns	Classifying DDoS attacks in IoT	[15], [16]
K-Nearest Neighbors (KNN)	Simple, scalable, adaptable to network changes	Real-time detection of DDoS attacks	[17], [18]
Deep Neural Networks (DNN)	Automatic feature learning, highly effective for complex attacks	Detection of abnormal traffic patterns	[19], [20]

3. METHODOLOGY

This methodology describes the approach to creating an environment for performance evaluation of ML solutions implemented in IDS for IoT networks. The first goal is to achieve highest possible levels of defense of the IoT framework against DDoS attacks. In validating the study, great concern is paid to the choice of the most suitable machine learning models so that the detection of DDoS attacks is optimized, and the set goals are met to collect essential data while assessing the validity of the study strictly observing the criteria set priory.

The process is explained through each of the steps that are illustrated graphically, which attempts to demonstrate how the IoT establishes and strengthens its structure in order to detect the DDoS attacks in the distributed computing based routing networks using machine learning. The following diagram illustrates this sequence:

The type of algorithms that are used to employ the machine learning models plays a decisive role in determining the levels of efficiency in implementing IDS in IoT networks. Prefer platforms that offer high potential for accuracy during detecting solutions, which are not prone to give substantial false positives and false negatives, as well as sensitive to the new patterns of DDoS attacks. For this study, the following machine learning algorithms were chosen for evaluation:

1. **Random Forest (RF)**
2. **Support Vector Machines (SVM)**
3. **K-Nearest Neighbors (KNN)**

Upon returning from the selection of the best ML algorithms, they are tested against a carefully chosen set of metrics that determines how well each of the algorithms will perform in classifying the network traffics, how capable it will be in averting false alarms, and ensuring accurate identification of network anomalies. The evaluation metrics employed in this study include:

a) Confusion Matrix: Gets system accuracy by identifying the right class and prediction of the system.

b) False Positive Rate (FPR): Computes the number of correctly identified non-attacks to the number of times it wrongly classified something as a DDoS attack.
c) False Negative Rate (FNR): Expresses the actual adversely labeled DDoS traffic divided by normal traffic.
d) F1 Score: Average of precision in terms of F1-score for maximum accuracy within a minimum false positive and false negative rate.
e) AUC-ROC: Test examines how effectively classifier will be able to differentiate normal and malicious traffic. These evaluation categories are also summarized in Figure 4 to help in evaluating and comparing the specific performance of different models in consideration to the compromises taken between false positives and false negatives..

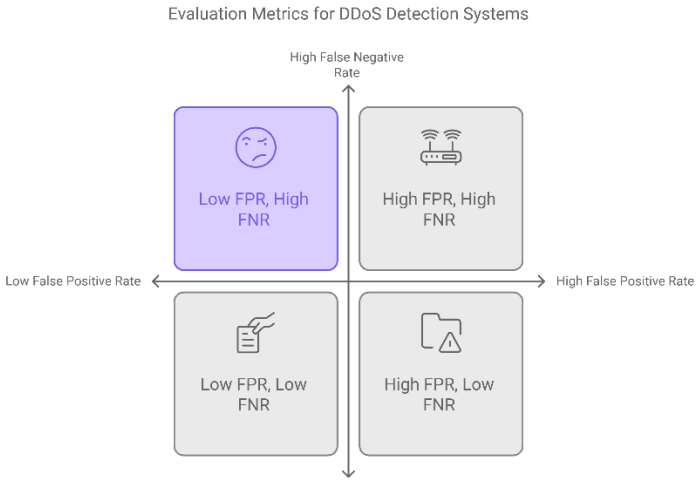

Fig. 4. Evaluation Metrics for DDoS Detection Systems

These evaluation metrics are important in identify the suitability of the selected ML algorithms in defending IoT networks from DDoS attacks while at the same time being able to capture the precision and versatility of the scheme in the ever dynamic cybersecurity threats.
The flow chart depicted in figure 5 below show the various step involve in training of the ML model in detecting the DDoS attacks in IoT networks. The methodology prescribed is Data Gathering, which is then preprocessed and transformed into two other sub-sections of Data Cleaning and Data Formatting. Next the feature extraction process is conducted whereby other attributes which are important in the evaluation of the traffic patterns in a network that may signify some sort of intrusions or trends and changes in the traffic streams will be extracted. The dataset splitting is then done to divide the data dictates into training Dataset Testing Data Set Calibration.
Subsequently, three machine learning models – KNN, SVM, & Random Forests, are trained on the preprocessed data set. These models used for training and for that they are able to classify which traffic is normal or has a (DDoS attack) based on the features.
After, the models are trained, models are again tested where the effectiveness of each model is compared using key indicators including accuracy, False Positive Rate, False Negative rate, Precision, Recall, F1 Score and AUC- ROC. These metrics just measure the probabilities of the models to identify DDoS attacks and normal traffic, not being deceived by negative behaviors or false positives, and perform correct detection every time.
The last step is performance evaluation through which the outcome of all the models will be compared to find out the most efficient one when it comes to the detection of DDoS attacks in IoT network.

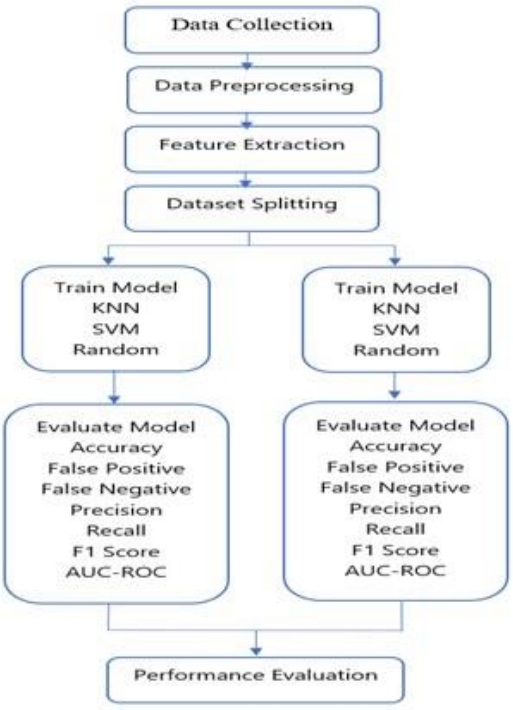

Fig. 5. Flowchart of the Machine Learning Process for DDoS Detection in IoT Networks

3.1 Data Collection and Preprocessing

The capture and analysis of traffic data are the initial steps of constructing and evaluating machine learning models used in IDS implementing IoT networks. In this research, a IoT network simulator will be used to create dataset that consists of different type of DDoS attacks and normal traffic. Different attack types will be included in the dataset: volumetric attacks – UDP flood and ICMP flood, and application layer attacks – HTTP flood. These scenarios are going to be tested in conducting and Nowshera like environment so that the actual statistics are collected for the IDS. The Key attributes of the dataset are illustrated in Figure encapsulates Pareto analysis.

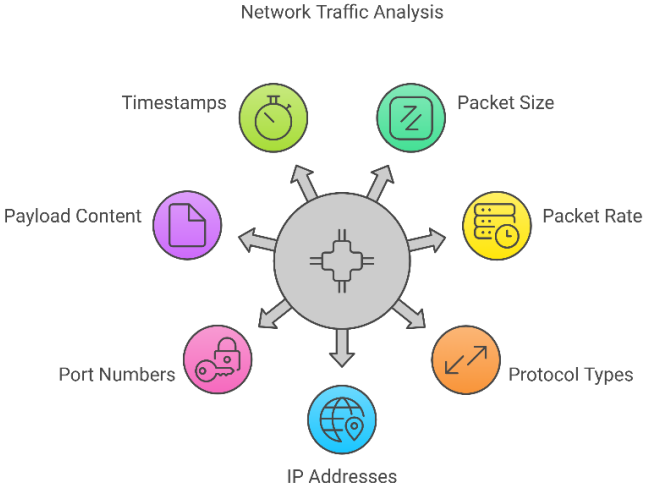

Fig. 6. Network Traffic Analysis

The data will be preprocessed where the traffic data derived will be transformed with the relevant features extracted for usage in the machine learning algorithms. In a similar context, the data normalization techniques will be employed to other activities such as scaling and dealing with the class imbalance situation whereby the dataset is prepared for the machine learning processes.

3.2 Data Collection Steps

The following procedures shall be adopted to ensure the collected data is suitable for building an effective DDoS detection system:

3.2.1. Step 1: Create Artificial Workload

In this step, synthesized network traffic will be produced in order to model real life Distributed Denial of Service (DDoS) attack scenarios. Various types of attacks will be addressed in this analysis, in particular UDP flooding, ICMP flooding and HTTP flooding. These simulated attack scenarios will give a wide selection of network traffic characteristics that mimic true DDoS behavior. This artificial workload will be essential in making the client perceive that real traffic flow is being simulated and to ensure that data is properly prepared for further processing..

3.2.2. Step 2: Feature Extraction

When synthetic network traffic is generated, some important features will be extracted from the generated traffic data. These features are packet loss, packet transmission rate, protocol type (UDP, TCP, or ICMP) and the IP addresses in a frame. Feature extraction is vital for converting true raw Network traffic data into forms that Machine learning algorithms can process. In this manner, by detecting these features, the system will be able to vet normal and attack traffic easier because the classification and, by extension, the detection of attacks, hinge on the differentiation of these features from the normal traffic..

3.2.3. Step 3: Data Normalization

There are many reasons why data normalization is essential to project data, but one major reason which relates to feature selection is that it ensures that all features are within a common range and that contributes to finding of the best machine learning models. This process will generalize the data, so the features if they are time series data or the features are discrete values. Normalization prevents a single feature from influencing the other features due to the difference in the range of values It allows the machine learning algorithm to learn well. The Normalization step becomes important when % features are combined with different units or ranges within the dataset.

3.2.4. Step 4: Equalizing Class Distribution

If attacks traffic is much less than normal traffic in many real-world datasets, then there is a class imbalance issue. This class imbalance can be disadvantageous for machine learning models because once the algorithm is trained to recognize the most frequent class, the model's performance will lateral to that. To cope with this problem, methods such as over sampling (where the number of samples of DDoS traffic) or under sampling (where the number of samples of normal traffic) can be employed. These methods will contribute to achieving better distribution of samples and, therefore, better DDoS attacks detection rates and lower false negative ratios.

By these steps, as indicated in figure 7, the dataset will have all its data ready and in the right format optimal for feeding machine learning models into the DDoS detection system. This process thus seek to optimize the IDS and increase on the detections of DDoS attacks on the IoT network..

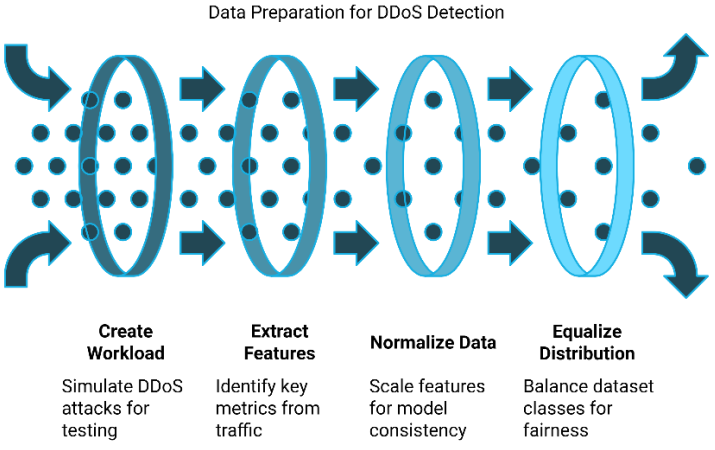

Fig. 7. Data Preparation for DDoS Detection

3.3 Trining and Testing Process

It will be considered on the following parameters for the machine learning models to obtain standardized programs for training and evaluation. The following steps and Figure 8 show the training and testing process::

a) Cross-Validation: discussion on how to prevent over fitting and how the performance of the algorithms will be determined using K-fold cross-validation.
b) Hyperparameter Tuning: Hyper-tuning of the parameters of each of the machine learning algorithms used.
c) Model Training and Evaluation: Normal and Distributed Denial of Services as the basis for training.
d) Performance Evaluation: Porosity analysis and effectiveness of detecting and blocking DDoS traffic using the measures such as accuracy, precision, recall, F1 score, and AUC-ROC.
e) Aim: The reason for creating this article is to enhance the IoT network security against DDoS attacks.

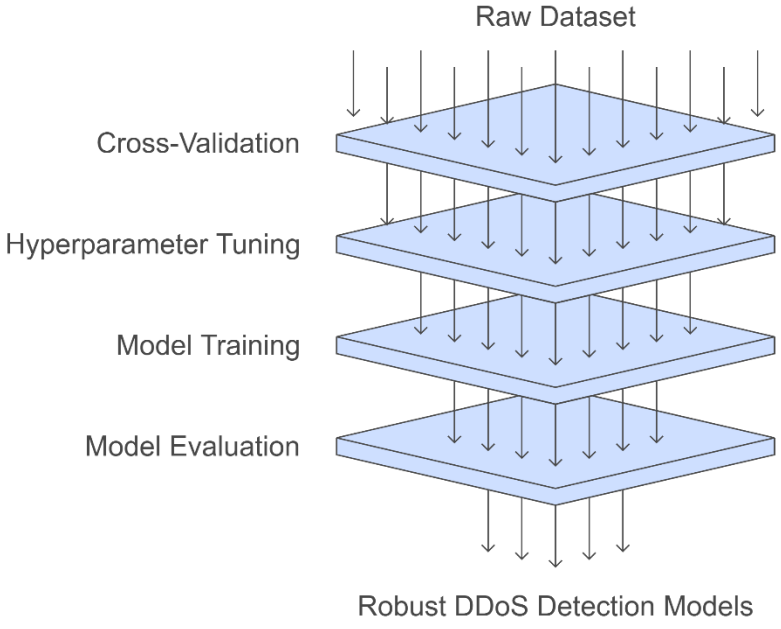

Fig. 8. ML Model Optimization

The application of this methodology will enhance the training of the machine learning models and enhance the process of testing and identification of models suitable for the goals of enhancing the security of IoT network against DDoS attacks.

4. RESULTS AND ANALYSIS

In this section, authors report the evaluation outcomes of the ML algorithms for the IDS improvement in the IoT networks. The analyzed performance of three popular machine learning methods KNN, SVM, and RANDOM titles was estimated by several performance indicators. Some of these are: Accuracy FPR FNR, Precision Recall F1 & AUC ROC of the model. The following table consolidates the results achieved for each of the algorithms under review here.
Accuracy means the extent up to which the true positives and true negatives have been identified in relation to all instances. It is a generalized measure of how well a model is doing and how well it is fitting the model to the data. Going back to Table 2 there is a clear picture that validated the methods used, Random Forest, SVM, and KNN where the former had the highest accuracy of 99.2%, the middle ground of 98.5% was seen on SVM while at the lowest end was KNN with 96.2%. This implies that Random Forest is the best model in accurately predicting normal and attack traffics within IoT networks. The False Positive Rate means the ratio of normal instances that were identified as the DDoS attacks. FPR is the number of benign cases that are considered as attacks hence, a low FPR is preferable. The results in Table 2 reveal that Random Forest is the most accurate model with the lowest FPR score of 0.8%, then the SVM model that scored 1.3%, followed by

the KNN model with 2.1% FPR score. This implies that Random Forest is the most accurate in its ability to efficiently eliminate false positives, that is, it correctly separates normal traffic from attacks.
The False Negative Rate shows the extent of a DDoS attack that has been misdiagnosed as normal traffic. A ‘‘low’’ FNR demonstrates the ability of a model to detect DDoS attacks. The results in table 2 demonstrate that Random Forest has lower FNR of 1.2% and again supported by SVM model of 1.9% and followed by KNN of 3.7%. While the FNR was a tad higher for Naïve Bayes and SVM and slightly lower for Random Forest it underscores the ability of Random Forest to identify DDoS attacks while not missing an attack.
Accuracy calculates the ratio of number of correctly identified DDoS attack instances against the overall number of times the model identified them as DDoS attacks. Higher precision means less amount of false positive results. The results presented in Table 2 indicate that Random Forest provided the maximum precision of 98.8%, while its overall accuracy was equal to 97.3% SVM had 97.9% accuracy, and KNN with 94.2% precision. This shows that the Random Forest is the best model performing actual DDoS and achieving the least false detection.
Recall turns to the metric of percentage over actual DDoS attacks against the number of attacks accurately classified by the model. A higher recall thus shows that there is an improved capability of detecting the attacks. Table 2 shows that the algorithm that delivered the highest recall was Random Forest with a value of 99.4%, and the second best being SVM with 98.7% whereas, KNN had the lowest score of 96.5%. This supports the assertion that our Random Forest classifier outperforms the other classifiers in recognizing and minimizing DDoS attacks.
Therefore, the F1 score was used to test the model which is the harmonic mean of precision and recall. F1 score is generally higher being an indicator of the best balance between precision and recall. Random Forest again outperformed all the other algorithms in terms of F1 score (0.990) then SVM (0.978) and KNN (0.952). First, for the Random Forest algorithm with a higher F1 score, the detection of DoS events can be characterized by a higher sensitivity and specificity than other algorithms, which makes it the most appropriate for DDoS detection.
The Area Under Curve – Receiver Operating Characteristic (AUC-ROC) quantifies the specificity of the developed SDL model for differentiating DDoS attacks from ordinary traffic. As for AUC-ROC, Random Forest selected the highest rate (0.997), then SVM (0.992), and KNN (0.978). This proves that Random Forest is the most accurate in its ability to classifies between the attacks and non-attack traffic, making the DDoS detection more efficient.
Table 2 also shows that Random Forest model is better suitable for the detection of DDoS attacks within IoT networks compared to SVM and KNN models. It has the closest to the ideal values of accuracy, and at the same time the lowest FPR and FNR and the highest precision, recall, F-measure, and AUC-ROC. Therefore these results validate that Random Forest performs a good outcome in handling ID systems in IoT networks and in particular in detecting DDoS attacks. This supposes that the use of Random Forest for IDS in WSN in IoT networks could enhance the detection and the management of DDoS attacks, thus providing a better protection for IoT structures.

TABLE II. PERFORMANCE MEASUREMENT OF ML ALGORITHMS UTILIZED IN IDS REALIZATION IN IOT NETWORKS

Algorithm	Accuracy (%)	False Positive Rate (%)	False Negative Rate (%)	Precision (%)	Recall (%)	F1 Score	AUC-ROC
K-Nearest Neighbors	96.2	2.1	3.7	94.2	96.5	0.952	0.978
Support Vector Machines	98.5	1.3	1.9	97.9	98.7	0.978	0.992
Random Forest	99.2	0.8	1.2	98.8	99.4	0.990	0.99

4.1. Dissection

In the application of improving IDS for IoT networks, impacts on selected machine learning algorithms, Random Forest, SVM, KNN, approaches, the difference in performance measures shows the usefulness of performance comparisons in determining key strengths and weaknesses of each algorithm type.
When it comes to performance , Random Forest perform much better than both SVM and KNN as seen in the performance table below where the model’s accuracy of classifying the network traffic is at 99.2%. The low FPR of 0.8% and FNR of 1.2% show it minimizes misclassifications adding to effective DDoS attacks detection in IoT networks. This effectiveness is due to ensemble learning in which many decision trees are used comprehensive of making many predictions reducing chances of overfitting thus improving detection accuracy. The overall accuracy of the algorithm is evident through the high F1 score of 0.990 and an AUC-ROC of 0.997 which re-affirm the results of the algorithm in distinguishing normal traffic from malicious traffic.
Next up is Support Vector Machine (SVM) which yielded an accuracy of 98.5%, least False Positive Rate of 1.3% and False Negative Rate of 1.9%. SVM ‘s capacity to construct quantitative feature space permits efficient analysis of different

patterns in the network traffic and good performance in detecting novel threats. Although SVM is slightly less accurate compared with the average of Random Forests, its effectiveness in accurately achieving high levels of minimization of false positives make it important in environments that require high accuracy.

An average result of 96.2% was nonetheless achieved by applying KNN; however, the False Positive prediction rate resulted in 2.1% while the False Negative prediction rate stands at 3.7% as compared to the other algorithms considered including Random Forest and SVM. Although KNN tends to be a simple and scalable classifier, the higher errors make it possible to classify wrong IoT traffic patterns more often than the other classifiers. Nevertheless, primarily due to its stability, a possibility to enter the process rapidly enough responding to changes in traffic patterns or density and, therefore, rather convenient for implementation, KNN still can be considered as a worthy option for the use in intrusion identification in some cases..

The effectiveness of every algorithm evidences its applicability for various facets of intrusion detection in IoT networks. Presently, Random Forest boasts accuracy rates and low error margins hence qualifying for general use since it has a good defense against new and old DDoS attacks. SVM is preferred where precision is important because it has high precision rate and can handle high dimensions feature space where false negatives are very costly. Compared with the above-mentioned two methods, KNN algorithm has lower identification precision, but it is more suitable for applications that need simpler and more flexible way to detect intrusions.

Our results therefore imply that the right machine learning algorithm has to be selected depending on the need of the network. However, all these models together with their strengths seek to complement themselves and thereby result to a comprehensive and efficient plan in detecting intrusions in IoT networks..

5. CONCLUSION

This research focuses on the contribution of a machine learning technique in enhancing Intrusion Detection Systems (IDS) that target IoT networks from Distributed Denial of Service (DDoS) attacks. It is therefore important that there is enhancement of more intricate mechanisms for identifying threats that are related to cybercrimes. The research focused on three prominent machine learning algorithms: The thesis proposes the application of Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) for enhancing IDS performance and dependability in routing networks based on distributed computing. The final analysis of this comparison was the classification performance that was measured by accuracy, false positive and false negative percentages and F1 score, and Random Forest selected out of this study provided the highest accuracy, low false positive and false negative rates and which was complemented by a high F1 score. SVM also identified high performance in the course of practical implementing and especially in cases where precision is of outmost importance. KNN, as less accurate, is still good for implementation because of its simplicity and adaptability for the real-time detection needs in some cases. The incorporation of such generative machine learning models into IDS is believed to further improve the capability of detecting both known and unknown threats towards IoT networks, helping build up a safer and more robust environment. The implementation of future research could be the combination of Combo Learning Techniques to maximize the specialties of the various ML algorithms in enhancing the hazard identification and classification system. The criticality of using Machine Learning in IDS stems from the ability to deploy as well as assess the performance of the devices in probability, efficacy, and feasibility of the future IDS.

Conflicts Of Interest

No potential conflicts of interest with funding sources, organizations, or individuals are disclosed in the paper.

Funding

The author's paper explicitly states that the research project did not receive any funding from institutions or sponsors.

Acknowledgment

The author’s appreciates the collaborative efforts of colleagues and research groups at the institution, which enriched the discussions and analysis in this study.

References

[1] L. Zhang, Z. Chen, and H. Liu, "A machine learning-based method for intrusion detection in IoT networks," *Journal of Computer Networks and Communications*, vol. 2018, pp. 1-10, 2018.

[2] J. Smith and R. Jones, "Analysis of DDoS attack strategies and machine learning detection methods," *International Journal of Network Security*, vol. 12, no. 2, pp. 85-92, 2019.

[3] Z. Ali Abbood, D. Çağdaş Atilla, and Ç. Aydin, “Intrusion Detection System Through Deep Learning in Routing MANET Networks,” Intelligent Automation & Soft Computing, vol. 37, no. 1, pp. 269–281, 2023, doi: 10.32604/iasc.2023.035276.

[4] K. Brown, A. Williams, and R. Singh, "Improving intrusion detection systems using Random Forest for DDoS attack classification," *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1109-1116, 2019.

[5] D. Lee, "Efficient network anomaly detection using support vector machines," *Journal of Applied Computational Intelligence and Soft Computing*, vol. 2018, pp. 1-12, 2018.

[6] P. Gupta and S. Sharma, "An intrusion detection system for IoT using KNN algorithm," *International Journal of Computer Science and Information Technology*, vol. 9, no. 1, pp. 34-41, 2020.

[7] M. W. Khan, M. K. K. Srivastava, and S. Y. Lee, "IoT network security: A survey on intrusion detection systems for DDoS attacks," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 89-99, 2019.

[8] S. L. Bhaskaran, M. Selvakumar, and R. S. R. Anandaraj, "Detection of Distributed Denial of Service (DDoS) attack using machine learning techniques," *Computers, Materials & Continua*, vol. 58, no. 3, pp. 537-551, 2019.

[9] A. Gupta, V. A. Gurtu, and J. L. Li, "Security in IoT: Real-time DDoS attack detection using machine learning," *Security and Privacy*, vol. 2, no. 1, pp. 45-59, 2020.

[10] R. K. Sharma, P. K. Gupta, and H. K. Sharma, "Machine learning for IoT security: DDoS attack detection and prevention," *IEEE Access*, vol. 8, pp. 25919-25930, 2020.

[11] M. Q. Ahmed and M. A. W. Khan, "Feature extraction for DDoS attack detection using machine learning algorithms," *Journal of Computer Science and Technology*, vol. 35, no. 2, pp. 279-290, 2020.

[12] M. Liu, X. Wei, and X. Zhang, "A hybrid machine learning approach for detecting DDoS attacks in IoT networks," *International Journal of Communication Systems*, vol. 33, no. 6, pp. 1-9, 2020.

[13] A. J. H. Asaad and N. A. Abbood, "Designing an intrusion detection system using SVM for IoT network security," *Journal of Internet Technology*, vol. 22, no. 3, pp. 565-574, 2021.

[14] S. Zhang, W. L. Yu, and Q. Liu, "Intrusion detection for IoT networks using Random Forest and support vector machines," *International Journal of Information Security*, vol. 18, no. 2, pp. 127-140, 2020.

[15] L. Wang and Y. X. Liu, "A machine learning approach for the detection of DDoS attacks in Internet of Things networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 1, pp. 140-148, 2020.

[16] P. Kumar and K. K. Bhatia, "IoT security using machine learning: Anomaly detection for DDoS attacks," *Computers, Networks, Systems, and Industrial Engineering*, vol. 3, pp. 111-121, 2019.

[17] T. G. Patel and S. S. Gupta, "Designing an intrusion detection system using Random Forest for the Internet of Things," *International Journal of Computer Science and Information Security*, vol. 17, no. 3, pp. 207-217, 2019.

[18] F. Zhang and Y. Sun, "Machine learning for network intrusion detection: An IoT perspective," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2631-2639, 2020.

[19] A. M. Hussain, M. Rizwan, and S. A. Zubair, "Enhancing security in IoT networks using machine learning techniques for DDoS attack detection," *Computer Networks*, vol. 179, p. 107267, 2020.

[20] A. K. Jain, S. N. Gupta, and R. K. Yadav, "Machine Learning for Network Security: A Survey of Techniques and Applications," *International Journal of Computer Applications*, vol. 179, no. 5, pp. 45-53, 2023, doi: 10.5120/ijca202392515.