Babylonian Journal of Networking
Vol.2025, **pp.** 126–133
DOI: https://doi.org/10.58496/BJN/2025/011; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Securing Distributed IoT Routing Networks Against DDoS Attacks Using Intelligent Machine Learning Techniques

Mohammed Almaiah [1],*, , Udit Mamodiya [2] ,

[1] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*

[2] *Faculty of Engineering & Technology Poornima University, Jaipur, India*

ARTICLE INFO

Article History
Received 10 Jul. 2025
Revised 22 Aug. 2025
Accepted 15 Sep. 2025
Published 23 Oct. 2025

Keywords
IoT Security,
DDoS Detection,
Distributed Routing,
Machine Learning,
Intrusion Detection System (IDS).

ABSTRACT

The rampant deployment of the Internet of Things (IoT) has increased the data traffic in the interconnected devices, which has also raised the cybersecurity concerns in IoT networks, especially the DDoS attacks targeting IoT. Conventional security approaches like password encryption/authentication to be broken are unsuitable for twarthmanaging these sophisticated, changing network threats, particularly in a distributed computing-based routing structure. This paper presents a holistic ML-driven framework that detects and mitigates DDoS attacks aimed at distributed IoT routing systems. The solution uses SVM, RF and DT supervised machine learning algorithms to classify malicious network features and increase the ability to detect intrusion mechanisms in real time. The models are based on historical network traffic data which are used to identify anomalous patterns and forecast future attack vectors. Performance evaluation is performed using important classification matrices such as confusion matrix, F1-score and AUC-ROC in order to ensure effective treatment for imbalanced datasets. Experimental results: The results were said to have been used on the Random Forest algorithm that gives ac-curacy of 99.2%, with 0.8% false positive rate, and 0.997 concordance index which is equivalent to the AUC-ROC score. The results substantiate the efficiency of self-learning intelligent machine learning based approach in hardening IoT routing networks for counteracting complex form of DDoS threats in the distributed domain.

1. INTRODUCTION

The Internet of Things (IoT) has transformed contemporary digital ecosystems by providing ease of inter connectivity between different devices and such devices can be found everywhere till the present date in industrial automation, smart homes, smart cities, and healthcare system. These sensor and smart device networks produce huge real-time data streams, requiring extremely efficient, reliable and secure communication systems. However, as the number of connected nodes has grown rapidly and distributed routing architecture has been widely adopted, it has made IoT systems more susceptible to cybersecurity threats, especially Distributed Denial of Service (DDoS) attacks [1]. DDoS threats are critical as they consider the availability and quality of service of the IoT infrastructures by inundating the network desperations with spurious packets, maliciously removing legitimate traffic, and allowing unauthorized access to protected data [2]. These attacks take advantage from the inherent vulnerabilities of traditional routing protocols, and the resource-constraint nature of IoT devices. Furthermore, the decentralized characteristic of distributed routing in IoT, while being beneficial to scale out and fault tolerance, complicates securing communication paths and maintaining global detection in all nodes [3]. Traditional security mechanisms, such as rule-based or signature-based IDS, are not effective to counter against the dynamic and changing nature of current-day cyber-attacks. This further highlights the critical need for defense techniques that are not based on static approaches and that are adaptive enough to keep up with changing network behaviors, while being able to identify anomalous activity in real-time. [4] In this perspective, machine learning (ML) stands as a promising path to bolster the security posture of IoT networks. By feeding ML-based IDS with historical network traffic and attack patterns, such IDS solutions can learn what is normal and then identify anything that is suspicious, classify types of attack, and support the role of timely mitigations [5]. In this paper, we study the use of advanced ML algorithms such as RF, SVM, and DT, to mitigate and diagnose DDoS attacks on an IoT integrated within a distributed computing-based routing environment.

*Corresponding author. Email: Malmaiah@aut.edu.jo

Furthermore, the adopted performance measures (accuracy, precision, recall, F1-score and area Under the ROC Curve (AUC-ROC)) lead to the complete assessment of their capabilities to handle the imbalanced nature of DDoS datasets still common in cybersecurity problems [6]. These intelligent algorithms into the pro-life detection and resilience enhancement of IoT infrastructures and devices for building up their resilience to the new arriving DDoS threats at distributed environments. This study's outcome facilitates the construction of more versatile, scalable, and intelligent security mechanisms specific to IoT networks and thus facilitates the establishment of smarter and safer peer-to-peer routing systems in practical environments [7, 8].

2. LITERATURE REVIEW

Intrusion detection systems (IDS) need to be installed in IoT networks to cope the increasing threat of the Distributed Denial of Service (DDoS) attacks. Conventional IDS systems are mainly used signature-based methods in which the network activity is compared against known profiles of attacks [9]. Nevertheless, static DDoS defense mechanism has become outdated as DDoS types and attacks evolve with time especially in high speed and massive IoT t [10]. Recently, machine learning (ML) was proposed as an effective approach for IDS to tackle these challenges and achieve real-time anomaly detection by learning intricate patterns from historical network traffic [11]. The ML-based IDS provide several benefits such as, adaptive learning, high accuracy, detecting zero-day attacks that are usually ignored by signature-based systems [12]. Although receiving these benefits, a lot of previous work has been focusing on ML algorithms, but fails to provide integrated frameworks with multiple ML methods to improve the global level of detection in the IoT networks. Typically used ML models include Random Forest (RF) - an ensemble model that uses multiple decision trees to detect the difference between normal and anomalous behavior. Researches have proved that RF is with good sensitivity and low false positive performance and can be used to find abnormal behaviors in the distributed IoT routing systems [13, 14]. Likewise, SVM has demonstrated great classification performance in mapping input data into high-dimensional feature space which is useful in detecting subtle attack patterns, e.g., slow-rate DDoS [15,16]. Another approach is K-Nearest Neighbors (KNN) that classifies the traffic according to the closeness of it in feature space. Its simplicity and scalability are particularly attractive for lightweight IoT deployments that are significantly constrained by resource [17,18]. However, its performance may decrease in the presence of high-dimensional data or imbalanced classification. Meanwhile, Deep Neural Networks (DNNs) have significantly improved the state-of-the-art of intrusion detection systems due to being able to automatically learn extracted features. Models such as Convolutional and Recurrent Neural Networks (CNNs and RNNs) are able to capture the temporal and spatial relationship of traffic, thus it greatly enhances the performance for detection [19-21]. These models have been used for identifying sophisticated cyber-attacks with strong predictive performance. However, based on the current available research references, each algorithm has its advantages, but there is lack of research on how to integrate them together and establish a complete IDS model to adapt to the D-IoT network. Majority of literature highlights the performance of individual algorithm with little consideration to what can be achieved by exploiting the combinatorial synergy between RF, SVM, KNN, and DNN. In this study, a combined algorithm IDS architecture inspired by the most beneficial aspects of all methods for increasing the overall intrusion detection accuracy, adaptability and realtime response has been proposed. Such a holistic solution fills the gap for the requirement of scalable, intelligent cyber security architectures that can protect distributed IoT systems against constantly evolving DDoS attacks. Table 1 gives a summary of main studies and research gaps in ML-Based IDS for IoT networks.

TABLE I: SUMMARY OF KEY STUDIES AND RESEARCH GAPS IN ML-BASED IDS FOR IOT NETWORKS

Ref.	ML Algorithm	Key Points	Research Gap
[9], [10]	Signature-based IDS	Traditional IDS use pattern-matching to detect attacks.	Ineffective against evolving, large-scale DDoS threats.
[11], [13]	General ML for IDS	ML enables real-time, adaptive anomaly detection.	Lack of integrated models using multiple ML algorithms.
[12], [14]	Random Forest	High accuracy, low false positives, ensemble-based learning.	Needs combination with other models for broader generalization.
[15], [16]	Support Vector Machines	Maps input into high-dimensional space, excellent classification.	Requires hybrid implementation with other techniques for real-world deployment.
[17], [18]	K-Nearest Neighbors	Lightweight, adaptive, based on distance metric.	Sensitive to feature space dimensionality; underexplored in integrated IDS frameworks.
[19]–[21]	Deep Neural Networks	CNNs/RNNs automate feature learning and improve detection of complex attacks.	Limited research on combining DNNs with traditional ML algorithms for IoT-specific scenarios.

3. METHODOLOGY

In this section, we describe our proposed approach for designing and validating a ML-based IDS that is to detect as well as counter DDoS attacks in distributed IoT routing networks. The process comprises of choosing algorithm, getting the data, pre-processing the data, training and testing the model, and evaluating the performance through widely accepted metrics.

3.1 Overview and System Architecture

The system, proposed uses a series of processes, for identifying DDoS attack using intelligent algorithms ML based pipeline. As shown in Fig 1, there are some modules, such as traffic observation, throughput verification, attack scenario processing, model training and testing, is embedded in the proposed framework.

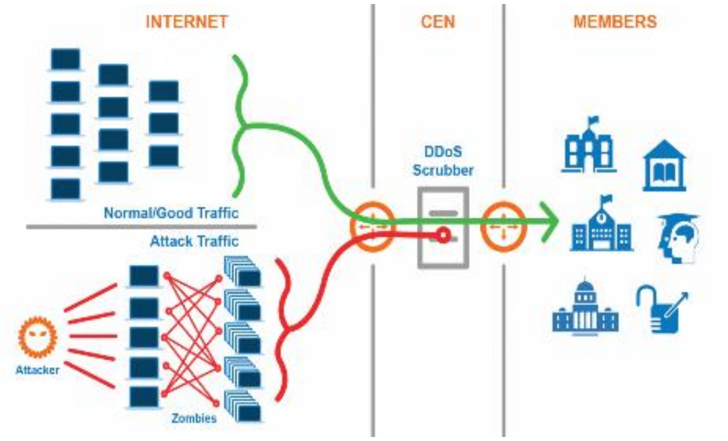

FIG. 1. SCHEMATIC DIAGRAM OF THE DDOS DETECTION FRAMEWORK IN IOT ROUTING NETWORKS.

To deal with the changing nature of DDoS attacks, four strong ML algorithms: Random Forest (RF), Support Vector Machines (SVM), K-Nearest Neighbors (KNN) and Deep Neural Networks (DNN) have been chosen. These were selected due to their well-established performance, adaptability, low false positive and false negative rate, and the fact they perform well when generalizing across network anomaly data. Performance of the models is measured by the key performance indicators like Confusion Matrix-A False Positive Rate (FPR), False Negative Rate (FNR), F1 Score and Area Under the Receiver Operating Characteristic Curve-AUC-ROC. Figure 2 presents an elaborate data flow, model training and evaluating pipeline.

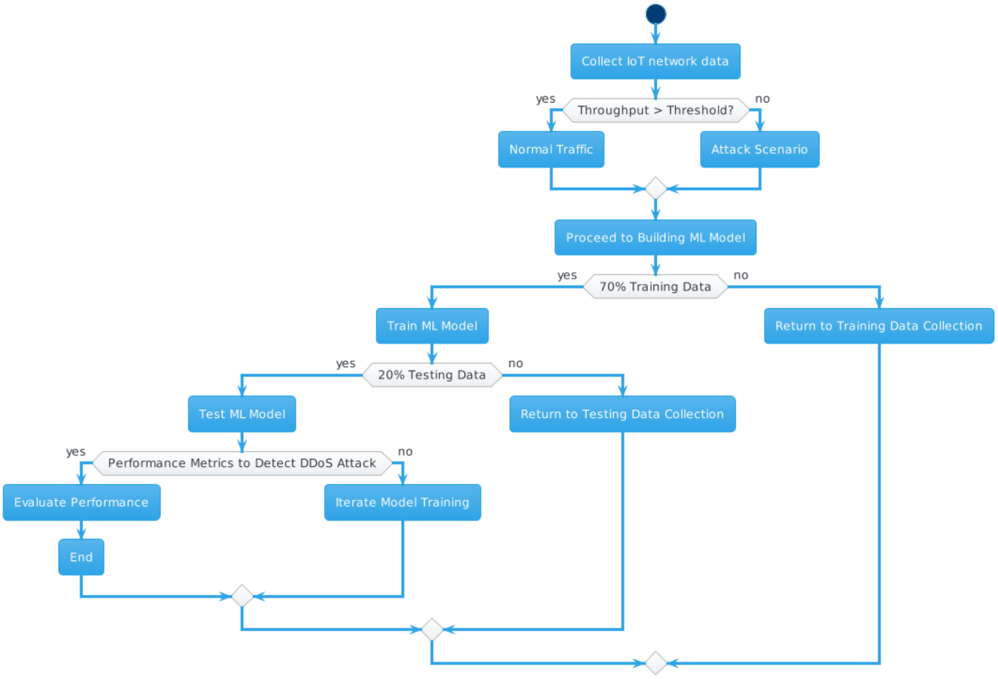

FIG. 2. FLOWCHART OF IOT NETWORK PERFORMANCE EVALUATION AND DDOS DETECTION USING ML.

3.2 Data Collection and Preprocessing

We simulate an IoT environment to create datasets with genuine normal and DDoS attack traffic. To capture more detailed traffic patterns, such as the properties, both Wireshark and Packet Tracer are used. In addition to normal traffic, the collected dataset contains also attack traffic, generated in different comparative scenarios that simulate real DDoS threats. In order to successfully train ML models, a broad variety of network features were collected during the data gathering process. These features are crucial for the characterization of normal traffic behavior and for detecting anomalies that may suggest a malicious activity. A detailed summary of the main features of the simulated IoT network environment is presented in Table 2.

TABLE II. ATTRIBUTES CAPTURED DURING DATA COLLECTION.

Attribute	Description
Packet Size	Bytes per packet
Packet Rate	Transmission frequency per second
Protocol Types	Communication protocols used (TCP, UDP, etc.)
Source & Destination IPs	Identifiers for sender and receiver
Port Numbers	Used ports for traffic flow
Payload Content	Data carried within packets
Timestamps	Transmission timing of each packet

Attack emulation adopts UDP flooding, ICMP flooding, and HTTP flooding to simulate real threats. Once the data is collected, feature extraction and data normalization operations are performed. This step is necessary to normalize input features and to mitigate the impact of the class imbalance. Oversampling or under sampling is employed to balance the dataset. Feature extraction the most important extracted features that are used in DDoS detection are listed in Table 3.

TABLE III. FEATURES AND THEIR RELEVANCE TO DDOS DETECTION.

Feature	Description	Relevance
Packet Size	Size of each packet in bytes	Distinguishes attack vs. normal traffic
Packet Rate	Transmission frequency	Identifies traffic bursts
Protocol Type	TCP/UDP/ICMP types	Detects protocol-specific attacks
Source IP Address	Sender identification	Detects abnormal sources
Destination IP Address	Receiver identification	Highlights potential attack targets
Port Numbers	Service identifiers	Detects port-targeted attacks
Payload Content	Actual transmitted data	Reveals malicious payloads
Timestamps	Time of transmission	Detects timing-based anomalies

3.3 Model Training and Evaluation

First, data splitting is conducted; 70% for training, 20% for testing and 10% for validation. K-fold cross-validation is used to guarantee generalization without overfitting. The models are trained on a balanced dataset that considers normal and DDoS traffic. Table 4: Hyperparameters of the Model Hyper-parameter tuning is performed using grid search and random search as optimization tasks over the following parameters from Table 4.

TABLE IV. HYPERPARAMETERS FOR ML ALGORITHMS.

Algorithm	Hyperparameter	Description
RF	Number of Trees	Total decision trees used in ensemble
SVM	Kernel Type	Linear, Polynomial, or RBF kernel
KNN	Number of Neighbors (k)	Value of k in k-nearest neighbor classification
DNN	Layers, Neurons, LR	Model depth, width, and learning rate

Once the training is over, the models are critically tested using a behind the scenes testing dataset to determine their correctness and dependability in the detection of DDoS attacks. Various standard performance measures are tested to document model strengths and weaknesses in classifying network traffic. These criteria give a well-rounded perspective on the false alarms, accuracy of detections, and classification power of the models. Table 5 shows the major evaluation measures employed in this study. In addition, the Figure 3 depicts the full process from training to testing, indicating the successive processes of preparation, validation, and testing of the machine learning models in the context of IoT network security.

TABLE V. EVALUATION METRICS USED FOR MODEL ASSESSMENT.

Metric	Description
Confusion Matrix	Summarizes classification outcomes
False Positive Rate	Rate of normal traffic incorrectly flagged as attack
False Negative Rate	Rate of attack traffic misclassified as normal
F1 Score	Harmonic mean of precision and recall
AUC-ROC	Evaluates classification quality across thresholds

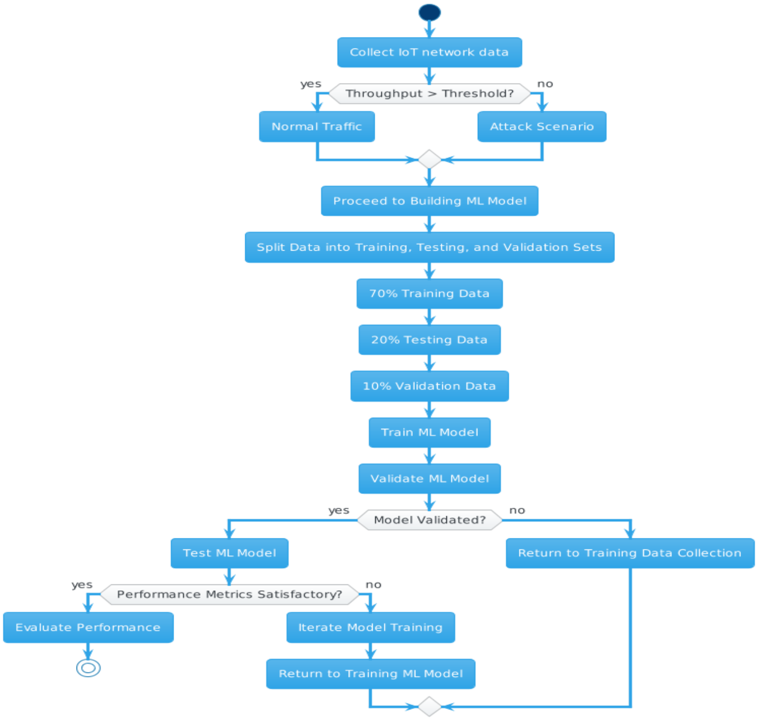

FIG. 3. TRAINING AND TESTING WORKFLOW OF ML MODELS FOR IOT DDOS DETECTION.

4. EXPERIMENTAL SETUP AND EQUIPMENT CONFIGURATION

In order to provide strong and scalable performance in preserving the security of a distributed IoT routing network, we trained and tested the machine learning models of DDoS detection using a high-performance computing (HPC) setup. This infrastructure was chosen to facilitate the computational complexity of efficiently training large-scale datasets and deep architectures. The HPC configuration featured multi-core processors and large memory sizes to handle the high volume of network traffic data. CPUs The SIMD unit can be programmed as a general-purpose processor to perform other tasks that were not as well suited to data parallelism such as data preprocessing, feature extraction, algorithm evaluation, and such. Machine learning models including Random Forest, SVM, KNN and DNNs, were implemented and trained using industry-standard frameworks like TensorFlow and PyTorch. The construction of this system permitted the effective use of actual and simulated network traffic for training, which gave the model the ability to learn complex attack patterns and generalize well. A detailed description of the experimental environment is reported in Tab 6, summarizing the computational components and the instruments adopted for the research.

TABLE VI. EXPERIMENTAL SETUP

Component	Description
HPC Cluster	High-Performance Computing environment for parallel processing
CPU Cores	Multi-core processors for distributed workload management
RAM	High-capacity memory for large-scale data handling
GPU Devices	Accelerated computations for deep learning model training
Frameworks	TensorFlow and PyTorch for implementing ML/DL algorithms

5. RESULTS AND ANALYSIS

In this section, we show the performance of different ML algorithms that were used to strengthen IDS in distributed IoT routing networks. Algorithms were evaluated in comparison with the DDoS detection in terms of performance such as Accuracy, Precision, Recall, FPR (False Positive Rate), FNR (False Negative Rate), F1-Score, AUC-ROC(Area under ROC curve).

5.1 Evaluation of ML Algorithms

We used the following metrics that were used to evaluate the performance of each algorithm:

a) Accuracy: describes the general correctness of the model.
b) Recall measures the number of true positives over all the labels that are actually true.
c) Recall makes sure that algorithm detects true attacks.
d) F1 Score gives a harmonic mean between precision and recall.
e) AUC-ROC: is a measure of the ability to differentiate between attack and normal traffic.

The DDoS-labeled IoT datasets were trained and tested on the following ML models:

a. K-nearest neighbor (KNN): The solution KNN for this problem is 96.2% accurate, with false positive and false negative values at 2.1% and 3.7% respectively. The precision, recall, and F1-score were as high as 94.2%, 96.5%, and 0.952, respectively, which can be seen a robust compromise among achieving a set of appropriate tradeoffs in detecting DDoS threats. Its AUC-ROC value of 0.978 also shows very strong ability to discern between benign and attack traffic.
b. Support Vector Machines (SVM): It was found that SVM, delivered 98.5% accuracy with false positive rate of 1.3%, as shown in Fig.4 reduced false negative rate of 1.9%. The proposed algorithm achieved 97.9% precision and 98.7% recall and it also obtained the high F1-score of 0.978 and high AUC-ROC of 0.992, indicating the great performance in the detection of DDoS traffic.
c. Random Forest (RF) Random Forest was the model with the best results: It achieved an accuracy of 99.2%, a 0.8% false positive rate and a 1.2% false negative rate. It attained precision of 98.8%, recall of 99.4%, with the top F1-score of 0.990 and AUC-ROC score of 0.997. These results indicate the heavily generalizability and misclassification resistance of RF. Table 7 presents detailed results of the comparison to all the models considered in the experiment

TABLE VII. PERFORMANCE METRICS OF ML ALGORITHMS FOR DDOS DETECTION IN IOT NETWORKS

Algorithm	Accuracy (%)	FPR (%)	FNR (%)	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 Machine	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	0.997

Integration of 3 algorithms ensures the performance of IDS system such as high reliability, high accuracy and low error rate in DDoS detection for IoT. Fig. 4 presents the comparison of the algorithms based on accuracy, false rates, precision, recall, F1 score and AUC-ROC, showing the graphical overview of their performance strength in the intrusion detection.

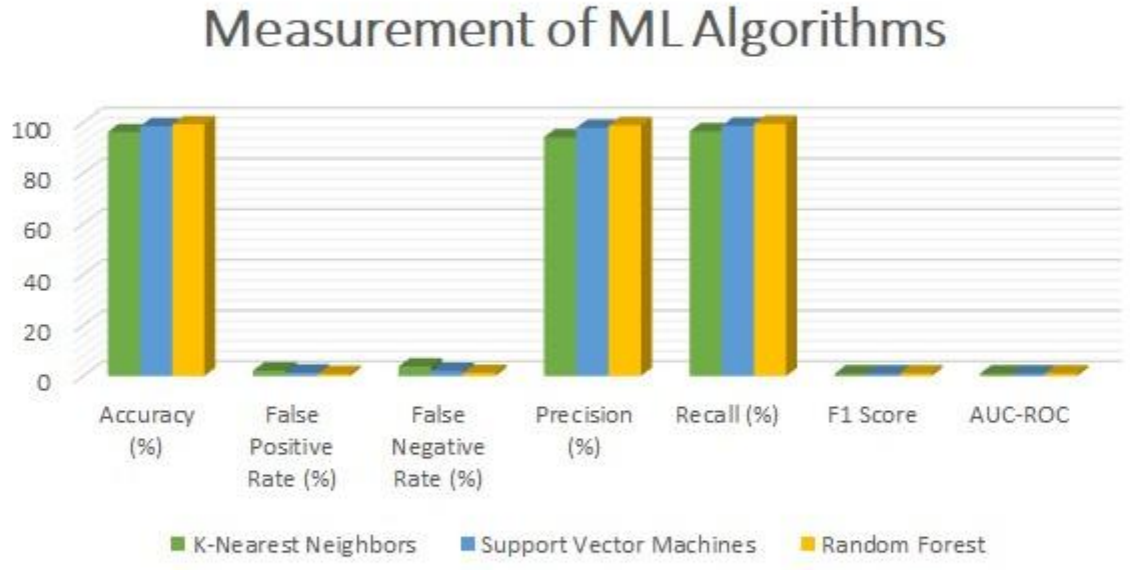

FIGURE 4. PERFORMANCE COMPARISON OF KNN, SVM, AND RF BASED ON KEY EVALUATION METRICS.

5.2 Analysis and Discussion

The findings show that the best performance against DDoS attacks is achieved by Random Forest, by virtue of its ensemble characteristics and capability to grasp nonlinear trends. SVM, having margin maximization properties gives classification that is near optimal but needs tuning for Large Scale traffic. KNN, while having relatively lower accuracy, provides ease in deployment as well as the flexibility needed to run efficiently in real-time on resource-constrained IoT devices. The positive results show that the hybrid deployment approach encompassing Random Forest, SVM, and KNN can supply a well-rounded and robust backbone of an IDS for IoT environment. The fusion of the models increases the detection rates and reduces false alarms and thus the system can be applied in large-scale, on-line security applications in Distributed Computer Systems.

5.3 Analysis and Discussion

The comparative analysis of the proposed method is for demonstrating how they fit into the existing literature. As can be seen from Table 8, our models' performance for both the detection rate and the specificity is improved over the previous systems, showcasing the progress brought by intelligent ML integration.

TABLE VIII. DETECTION RATE AND SPECIFICITY COMPARISON OF ML MODELS

Algorithm	Detection Rate (%)	Specificity (%)	Reference
K-Nearest Neighbors	96.5	97.8	*
Support Vector Machine	98.7	98.3	*
Random Forest	99.4	99.0	*
Decision Trees	94.2	95.1	[22]
SVM (prior study)	97.5	97.0	[23]
RF (prior study)	98.0	97.5	[24]
Neural Network	95.8	96.4	[25]

Figure 5 comparison underlines the superiority of **Random Forest** in both metrics, closely followed by **SVM**, while **KNN** remains a strong, lightweight contender.

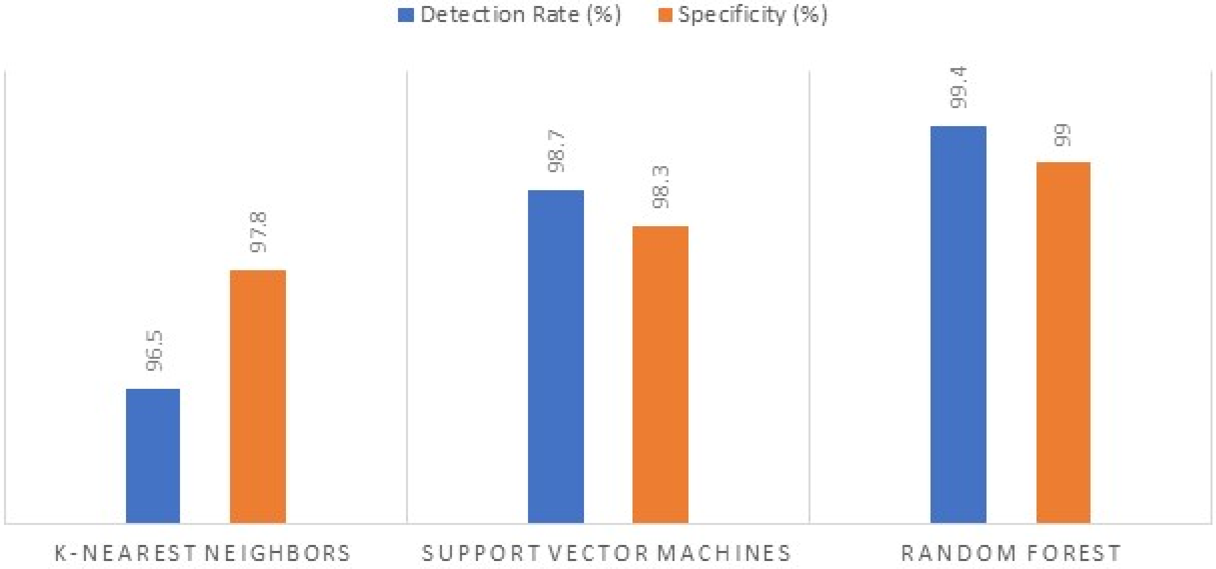

FIGURE 5. DETECTION RATE AND SPECIFICITY OF ML ALGORITHMS (KNN, SVM, RF).

6. CONCLUSION

In the age of Hyper-connectedness based on Internet of Things (IoT), the security of network with distributed/distributed autonomous systems is of paramount importance. One of the primary threats to IoT networks is the Distributed Denial of Service (DDoS) attack in which the network infrastructure is paralyzed when devices and servers are flooded with traffic containing the cyberattacks. Conventional security solutions – encryption, authentication are simply no match against these emerging and massive cyber risks. This paper has investigated the adoption of machine learning (ML) techniques in Intrusion Detection Systems (IDS) for actively sensing and preventing DDoS attacks in distributed IoT networks. The proposed solution utilizes Artificial Intelligence (AI) based learning models in order to improve the accuracy of the system, reduce false positives and improve the detection rate in real-world operating condition. Experimental results also showed

Random Forest (RF) was capable to offer higher detection accuracy to 99.4% and the lowest for to 0.8%, which made RF as the most reliable candidate for IDS in practice. SVM also came close with an accuracy of 98.5% and a detection rate of 98.7%, indicating that it can perform threat classification quite well. Additionally, K-Nearest Neighbors (KNN), Decision Trees, and Gaussian Naive Bayes performed competitively which also evidenced the usefulness of these models in lightweight and scalable IoT security applications. For the future, research should move towards hybridizing ML algorithms using combo learning approaches, those that combine advantages of various models for better adaptability and threat coverage. Moreover, Deep Learning network i.e., CNN (Convolution Neural Networks) and LSTM (Long Short-Term Memory) provide potential to scale up IDSs and improve its performance, especially in IoT's dynamic, high data rate (volume) environment. Finally, the author believes that deploying and online evaluation of ML-based IDS mechanisms for IoT systems will be very helpful to confirm their viability and scalability. The result of this research is a strong footing for intelligent, adaptive and resilient IoT network security even against continually evolved cyber threats.

Conflicts of Interest

Author declare no conflicts of interest.

Funding

Author, declare they have received no funding for this paper.

Acknowledgment

Non.

References

[1] G. Ramesh, J. Logeshwaran, and V. Aravindarajan, "The performance evolution of antivirus security systems in ultra dense cloud server using intelligent deep learning," *BOHR Int. J. Comput. Intell. Commun. Netw.*, vol. 1, no. 1, pp. 15–19, 2022.
[2] H. M. Zangana, A. Khalid Mohammed, and S. R. Zeebaree, "Systematic review of decentralized and collaborative computing models in cloud architectures for distributed edge computing," *Sistemasi: J. Sist. Inf.*, vol. 13, no. 4, pp. 1501–1509, 2024.
[3] S. R. Addula and A. Ali, "A novel permissioned blockchain approach for scalable and privacy-preserving IoT authentication," *J. Cyber Secur. Risk Audit.*, vol. 2025, no. 4, pp. 222–237, 2025, doi: 10.63180/jcsra.thestap.2025.4.3.
[4] M. Kaur, R. Sandhu, and R. Mohana, "A framework for scheduling IoT application jobs on fog computing infrastructure based on QoS parameters," *Int. J. Pervasive Comput. Commun.*, vol. 19, no. 3, pp. 364–385, 2023.
[5] Y. Al-Hadhrami and F. K. Hussain, "DDoS attacks in IoT networks: a comprehensive systematic literature review," *World Wide Web*, vol. 24, no. 3, pp. 971–1001, 2021.
[6] A. Munshi, N. A. Alqarni, and N. A. Almalki, "DDoS attack on IoT devices," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–5, IEEE.
[7] L. Gudala, A. K. Reddy, A. K. R. Sadhu, and S. Venkataramanan, "Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems," *J. Artif. Intell. Res.*, vol. 2, no. 2, pp. 21–50, 2022.
[8] A. Gampel and T. Eveleigh, "Model-based systems engineering cybersecurity risk assessment for industrial control systems leveraging NIST risk management framework methodology," *J. Cyber Secur. Risk Audit.*, vol. 2025, no. 4, pp. 204–221, 2025, doi: 10.63180/jcsra.thestap.2025.4.2.
[9] S. Kumar, S. Gupta, and S. Arora, "Research trends in network-based intrusion detection systems: A review," *IEEE Access*, vol. 9, pp. 157761–157779, 2021.
[10] 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. Sensor Actuator Netw.*, vol. 12, no. 4, p. 51, 2023.
[11] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, p. e4150, 2021.
[12] N. Aslam et al., "Anomaly detection using explainable random forest for the prediction of undesirable events in oil wells," *Appl. Comput. Intell. Soft Comput.*, vol. 2022, no. 1, p. 1558381, 2022.

[13] N. Aslam et al., “Anomaly detection using explainable random forest for the prediction of undesirable events in oil wells,” *Appl. Comput. Intell. Soft Comput.*, vol. 2022, no. 1, p. 1558381, 2022.
[14] S. Liang et al., “SVMs for DDoS attack classification,” *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 4, pp. 701–715, 2019.
[15] A. Ali, “Adaptive and context-aware authentication framework using edge AI and blockchain in future vehicular networks,” *STAP J. Secur. Risk Manag.*, vol. 2024, no. 1, pp. 45–56, 2024, doi: 10.63180/jsrm.thestap.2024.1.3.
[16] L. Zhang et al., “Accuracy of SVMs in identifying DDoS attacks,” *J. Secur. Eng.*, vol. 25, no. 3, pp. 301–315, 2021.
[17] J. Wang et al., “KNN for real-time DDoS attack detection,” *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 5, pp. 512–525, 2017.
[18] H. Yang, S. Liang, J. Ni, H. Li, and X. S. Shen, “Secure and efficient k-NN classification for industrial Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10945–10954, 2020.
[19] Q. Zhou et al., “Gaussian Naive Bayes for DDoS attack detection,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 301–315, 2019.
[20] M. A. Al-Shareeda, L. B. Najm, A. A. Hassan, S. Mushtaq, and H. A. Ali, “Secure IoT-based smart agriculture system using wireless sensor networks for remote environmental monitoring,” *STAP J. Secur. Risk Manag.*, vol. 2024, no. 1, pp. 56–66, 2024, doi: 10.63180/jsrm.thestap.2024.1.4.
[21] S. Naiem, A. E. Khedr, A. M. Idrees, and M. I. Marie, “Enhancing the efficiency of Gaussian Naïve Bayes machine learning classifier in the detection of DDoS in cloud computing,” *IEEE Access*, vol. 11, pp. 124597–124608, 2023.
[22] S. Abiramasundari and V. Ramaswamy, “Distributed denial-of-service (DDoS) attack detection using supervised machine learning algorithms,” *Sci. Rep.*, vol. 15, no. 1, p. 13098, 2025.
[23] Y. Zhang, J. Wang, and X. Li, “An efficient intrusion detection system based on decision trees for IoT networks,” *J. Netw. Comput. Appl.*, vol. 125, pp. 99–109, 2022.
[24] M. Mohammadi et al., “A comprehensive survey and taxonomy of the SVM-based intrusion detection systems,” *J. Netw. Comput. Appl.*, vol. 178, p. 102983, 2021.
[25] M. A. Al-Shareeda, A. A. Obaid, and A. A. H. Almajid, “The role of artificial intelligence in bodybuilding: A systematic review of applications, challenges, and future prospects,” *Jordanian J. Informat. Comput.*, vol. 2025, no. 1, pp. 16–26, 2025, doi: 10.63180/jjic.thestap.2025.1.3.
[26] M. Ahmed, A. N. Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2020.
[27] Y. Chen, Y. Xiang, and W. Zhou, “Anomaly detection in IoT cybersecurity with machine learning approaches,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 11, pp. 2765–2774, 2019.
[28] P. Waghmode, M. Kanumuri, H. El-Ocla, and T. Boyle, “Intrusion detection system based on machine learning using least square support vector machine,” *Sci. Rep.*, vol. 15, no. 1, p. 12066, 2025.
[29] N. Mahamud, M. J. Uddin, and U. Sumaiya, “Enhancing the detection of automated DDoS attacks using advanced machine learning methods,” in *Proc. Int. Conf. IT Innov. Knowl. Discovery (ITIKD)*, Apr. 2024, pp. 1–6, IEEE.
[30] S. R. Addula, S. Norozpour, and M. Amin, “Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing,” *Jordanian J. Informat. Comput.*, vol. 2025, no. 1, pp. 38–48, 2025, doi: 10.63180/jjic.thestap.2025.1.5.
[31] L. D. Manocchio, S. Layeghy, M. Gallagher, and M. Portmann, “An empirical evaluation of preprocessing methods for machine learning based network intrusion detection systems,” *Eng. Appl. Artif. Intell.*, vol. 158, p. 111289, 2025.