Asia-Pacific Journal of Information Technology and Multimedia 15(1) 2026: 43 – 59
https://doi.org/10.17576/apjitm-2026-1501-03

# Applying Machine Learning for Detecting DDoS Attacks in Software-Defined IoT Networks

# Menggunakan Pembelajaran Mesin untuk Mengesan Serangan DDoS dalam Rangkaian IoT Ditakrifkan Perisian

*Noor Afiza Mohd Ariffin*[*]*, Yang Lei*

*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia*

[*]*Corresponding author: noorafiza@upm.edu.my*

*Received 31 July 2025*
*Accepted 22 April 2026, Available online 30 June 2026*

## ABSTRACT

In Software-Defined Internet of Things (SD-IoT) networks, Distributed Denial of Service (DDoS) attacks remain a major threat due to the large number of heterogeneous and resource-constrained devices. This study proposes an SDN-integrated machine learning framework for real-time DDoS detection using three supervised classifiers: Naïve Bayes (NB), Decision Tree (DT), and Support Vector Machine (SVM). The framework leverages centralized SDN control for dynamic flow management and attack mitigation. The BoT-IoT dataset was used with proper preprocessing and stratified train–test splitting (70–30). Performance was evaluated using accuracy, precision, recall, F1-score, false positive rate, detection time (milliseconds), CPU usage, and memory overhead. Experimental results show that the Decision Tree classifier achieved the best accuracy of 98.9%, with an average detection time of 480–500 ms, while incurring only a 3% increase in controller CPU and memory usage. These findings demonstrate that lightweight supervised ML models integrated into SDN controllers can provide efficient and scalable DDoS detection for SD-IoT environments.

Keywords**:** Software-Defined Networking (SDN); Internet of Things (IoT); DDoS Attacks; Machine Learning; Network Security

## ABSTRAK

Dalam rangkaian Software-Defined Internet of Things (SD-IoT), serangan Distributed Denial of Service (DDoS) kekal sebagai ancaman utama berikutan jumlah peranti yang heterogen dan mempunyai kekangan sumber. Kajian ini mencadangkan satu rangka kerja pembelajaran mesin bersepadu SDN untuk pengesanan DDoS secara masa nyata dengan menggunakan tiga pengelas terselia, iaitu Naïve Bayes (NB), Decision Tree (DT), dan Support Vector Machine (SVM). Rangka kerja ini memanfaatkan kawalan berpusat SDN bagi pengurusan aliran trafik secara dinamik serta mitigasi serangan. Set data BoT-IoT telah digunakan dengan proses prapemprosesan yang sesuai serta pembahagian data latihan dan ujian secara berstrata (70–30). Prestasi model dinilai berdasarkan ketepatan (accuracy), kejituan (precision), kepekaan

(recall), skor F1, kadar positif palsu, masa pengesanan (milisaat), penggunaan CPU, dan lebihan penggunaan memori. Keputusan eksperimen menunjukkan bahawa pengelas Decision Tree mencapai ketepatan tertinggi iaitu 98.9%, dengan purata masa pengesanan antara 480–500 ms serta hanya meningkatkan penggunaan CPU dan memori pengawal sebanyak 3%. Dapatan ini membuktikan bahawa model pembelajaran mesin terselia yang ringan dan diintegrasikan dalam pengawal SDN mampu menyediakan pengesanan DDoS yang cekap dan berskala untuk persekitaran SD-IoT.

Kata kunci**:** Rangkaian Ditakrifkan Perisian (SDN); Internet Perkara (IoT); Serangan DDoS; Pembelajaran Mesin; Keselamatan Rangkaian

## INTRODUCTION

The Internet of Things (IoT) has revolutionized digital connectivity, with its integration across healthcare, transportation, industrial, and residential sectors. It is expected that over 100 billion IoT devices will be connected by 2025 (Almaraz-Rivera et al., 2022). This expansion enables unprecedented data collection and automation but also creates serious cybersecurity vulnerabilities (Aljuhani, 2021). Due to limited computational capabilities and weak security protocols, IoT devices are increasingly targeted by attackers. These vulnerabilities are often exploited to hijack sensitive data or form botnets used in large-scale Distributed Denial of Service (DDoS) attacks (Singh & Jain, 2024).

DDoS attacks are among the most disruptive threats to IoT networks, overwhelming services by flooding them with malicious traffic from compromised devices. Reports indicated that 85 million IoT-targeted attacks were detected in 2022 alone (Tripathy et al., 2024), with malware such as Mirai and Nyadrop infecting millions of devices worldwide. A notable example is the 2016 attack on Dyn's DNS servers, which caused widespread outages affecting major platforms, including Facebook and Twitter. These incidents highlight the increasing sophistication, scale, and real-world impact of IoT-driven DDoS attacks.
Software-Defined Networking (SDN) offers a dynamic, programmable, and centralized approach to managing IoT networks. It enables real-time monitoring, intelligent routing, and fine-grained traffic control (Aggarwal et al., 2025). The SDN controller functions as the centralized control plane, providing adaptive traffic flow management and security policy enforcement (Belachew et al., 2025). The core characteristics of SDN—abstraction, programmability, and centralized intelligence—make it particularly suitable for handling the heterogeneity and scalability challenges of IoT environments.

The synergy between SDN and machine learning (ML) presents a powerful paradigm for strengthening IoT security. Supervised ML classifiers, including Support Vector Machine (SVM), Decision Trees (DT), and Naive Bayes, can learn discriminative patterns from network traffic features to accurately differentiate legitimate and malicious flows (Haddad et al., 2024; Infantia et al., 2025). However, many existing ML-based intrusion detection systems (IDS) operate as external modules or offline analytical tools, limiting their responsiveness and real-time deployment capability within dynamic SD-IoT architectures.

Various ML-based frameworks and IDS mechanisms have been proposed for DDoS detection in IoT. For example, HADEC, a Hadoop-based real-time detection framework, achieves fast detection but incurs significant computational overhead (Janardhana et al., 2023). Similarly, cosine similarity-based vector matching techniques rely primarily on packet-level analysis and lack adaptability to evolving SD-IoT traffic patterns (Bhayo et al., 2023). Most existing

solutions either depend on legacy network infrastructures or fail to provide comprehensive evaluation beyond accuracy metrics, neglecting resource utilization and statistical robustness. To overcome these limitations, this work integrates supervised ML classifiers directly into the SDN controller, enabling intelligent, real-time DDoS detection within SD-IoT environments. Unlike conventional architectures, the proposed approach embeds the detection logic within the control plane, allowing immediate mitigation actions and enhanced traffic visibility. Furthermore, the SDN controller is enhanced with a logging mechanism for detailed traffic monitoring and feature extraction, supporting adaptive and data-driven security enforcement.
The main contributions of this work are summarized as follows:

1. SDN-Controller Integrated ML Detection Architecture – A tightly coupled framework where supervised ML classifiers are embedded within the SDN controller for real-time DDoS detection and mitigation.
2. Logging-Enhanced SDN Modification – Extension of the SDN controller with advanced logging capabilities to enable efficient traffic monitoring and structured dataset generation.
3. Comprehensive Multi-Metric Evaluation – Performance assessment using precision, recall, F1-score, detection rate, false positive rate, and other relevant metrics beyond conventional accuracy.
4. Resource-Aware Performance Analysis – Evaluation of computational overhead, controller response time, and memory utilization to ensure suitability for resource-constrained IoT environments.
5. Formal Metric Formulation and Statistical Validation – Inclusion of mathematical performance metric equations and statistical validation to ensure the reliability and robustness of experimental results.

The proposed architecture consists of three main components: (1) an IoT Control Module built upon SDN to orchestrate network operations, (2) a Data Plane comprising IoT devices and software-defined switches for real-time traffic collection, and (3) an ML-Based Detection Module that leverages supervised classifiers trained on labeled traffic datasets. This modular yet tightly integrated design ensures rapid detection, adaptability to dynamic IoT behavior, and resilience against large-scale DDoS attacks in SD-IoT ecosystems.

## RELATED WORK

Numerous studies have explored the detection and mitigation of Distributed Denial of Service (DDoS) attacks in both traditional and software-defined IoT (SD-IoT) environments. Common defense strategies include attack detection and mitigation, traffic isolation, and source traceback mechanisms (Singh & Jain, 2024). These approaches attempt to distinguish malicious from legitimate traffic flows, isolate abnormal packet patterns, and trace the origin of attacks. However, their real-world effectiveness remains limited due to two primary challenges: (a) many DDoS attacks are launched using seemingly legitimate requests, making early detection difficult; and (b) the sheer volume of network data in modern IoT infrastructures hinders real-time identification and response (Kumar et al., 2024).
Statistical and machine learning (ML)-based methods have gained attention for their potential to address these challenges. For example, covariance analysis of TCP header flags has been used to detect SYN flood attacks (Qaiser et al., 2023). However, reliance on limited flag fields often results in low generalization capability. Similarly, statistical-based models typically fail to detect slow-rate or stealthy attack traffic due to their dependency on threshold settings. Clustering-based methods can provide resilience by constructing standard samples from benign traffic (R et al., 2024), yet these are sensitive to initialization and parameter tuning. Meanwhile,

machine learning approaches such as Spark-based parallel detection frameworks (e.g., SAD-F) improve efficiency but face high computational overhead during model training and execution (Ravi & Shalinie, 2020).

Other emerging techniques include multi-class SVMs with newly defined features to capture relative patterns, probabilistic packet marking (PPM) for source traceback (Sangodoyin et al., 2021), and k-nearest neighbor (k-NN) classifiers for traffic state classification. While these methods have shown high accuracy, they are often limited by processing delays and scalability concerns, especially as the volume of concurrent flows increases. Deep learning models such as breakdown-point-based classifiers further improve feature extraction and reduce detection time compared to conventional methods (Sebbar & Zkik, 2023). Nonetheless, many of these models were developed using outdated datasets or legacy network environments, making them less suitable for dynamic SD-IoT deployments.

To enhance network security, recent research has focused on integrating SDN with advanced detection techniques. SDN-based honeypot architectures and pseudo-honeypot game (PHG) strategies have been introduced to dynamically lure and isolate attackers, with support from software-defined components (Sharma & Babbar, 2024). Other detection methods based on entropy scoring, matrix co-segmentation, and relevance filtering have been proposed to classify abnormal flows more accurately. Supervised algorithms are used to reduce false positives, while unsupervised models help discover unknown attack patterns. Despite these advances, false alarm rates remain a significant issue, and many existing works do not effectively address IPv6-capable or low-power IoT devices (Wang et al., 2022).

Recent efforts have demonstrated improvements in detection accuracy. For instance, random forest (RF) classifiers trained with the WEKA tool on NSL-KDD datasets achieved an accuracy of 97.76% in identifying DDoS traffic (Wang et al., 2022). Similarly, a CORR-SVM model reported 100% malicious traffic detection and 88.58% overall accuracy under IPv6-enabled SDN conditions (Yungaicela-Naula et al., 2021). A deep neural network combined with feature selection via Whale Optimization Algorithm (FS-WOA) achieved 95.35% detection accuracy by pre-processing data with min-max normalization and homomorphic encryption for secure cloud uploading (Djuitcheu et al., 2022).

Despite these innovations, most existing models are not specifically tailored for SD-IoT environments, where programmability, centralization, and real-time adaptation are critical. SDN provides a flexible and dynamic architecture that simplifies the deployment of intelligent detection mechanisms. By decoupling the control and data planes, SDN reduces network management overhead and facilitates fine-grained flow control. Existing research reveals two dominant trends: (i) traditional algorithm-based DDoS detection, and (ii) machine learning-driven DDoS identification. Evaluation metrics such as CPU utilization, RAM consumption, response time, and packet throughput have been used to compare methods across studies (Bhayo et al., 2023).

In this context, our work proposes a machine learning-based supervised detection architecture specifically designed for SD-IoT networks. It leverages the capabilities of SDN to manage traffic flow while utilizing trained ML classifiers to identify malicious traffic patterns in real-time. This integrated framework aims to address existing shortcomings, such as false positives, slow detection times, and scalability, thereby improving the security and reliability of IoT applications in critical sectors like healthcare, transportation, and smart cities.

## METHODOLOGY

The current framework provides a machine learning-based DDoS detection process, as shown in Figure 1 (Bhayo et al., 2023). The architecture is composed of four layers: at the bottom layer, IoT nodes generate either normal or attack traffic, which is uploaded via Sensor

OpenFlow Switches (SOFS). The Sink serves as the intermediate node responsible for processing traffic and forwarding unknown packets to the SDN-WISE controller in the middle layer. The controller manages the network and issues rules to the topmost Security Application layer, which contains a security detection module. This module includes a machine learning classifier to analyze and verify attack traffic, forwarding detection results to the SDN-WISE controller for dynamic flow table updates. This closed-loop system ensures effective detection and defense against DDoS attacks in real time, performing data acquisition, intelligent analysis, and active response within the IoT network.

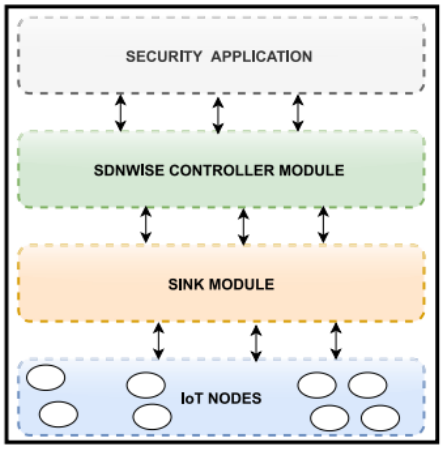


FIGURE 1. Current DDoS detection framework for IoT network (Bhayo et al., 2023)

*A. Threat Model*

In this study, compromised IoT nodes generate flooding-based DDoS traffic targeting victim nodes. The attacker aims to exhaust SDN controller resources, simulating real-world attack scenarios to evaluate the framework's resilience.

*B. Dataset and Preprocessing*

The BoT-IoT dataset is employed for training and testing the machine learning models. Preprocessing steps include duplicate removal, Min-Max scaling, stratified 70–30 train-test split, and imbalance handling to ensure unbiased and robust model evaluation.

*C. Machine Learning Formulations*

Three machine learning classifiers are implemented for DDoS detection:

1. Naïve Bayes

P(C|X)=P(X|C)P(C)P(X)P(C|X) = \frac{P(X|C) P(C)}{P(X)}P(C|X)=P(X)P(X|C)P(C)

2. Decision Tree (Gini Index)

Gini=1−∑(pi2)Gini = 1 - \sum (p_i^2)Gini=1−∑(pi2)

3. Support Vector Machine (SVM)

w·x+b=0w \cdot x + b = 0w·x+b=0

*D. Performance Metrics*

Model performance is evaluated using standard metrics:

- Accuracy: (TP+TN)/(TP+TN+FP+FN)(TP + TN) / (TP + TN + FP + FN)(TP+TN)/(TP+TN+FP+FN)
- Precision: TP/(TP+FP)TP / (TP + FP)TP/(TP+FP)
- Recall: TP/(TP+FN)TP / (TP + FN)TP/(TP+FN)
- F1-score: 2×(Precision×Recall)/(Precision+Recall)2 \times (Precision \times Recall) / (Precision + Recall)2×(Precision×Recall)/(Precision+Recall)
- False Positive Rate (FPR): FP/(FP+TN)FP / (FP + TN)FP/(FP+TN)

*E. Test-bed SD-IoT Framework*

This study proposes a security analytics-driven framework targeting machine communication threats in IoT environments, with a focus on early DDoS attack detection. While IoT security threats span across the device, network, and application layers, this work emphasizes detecting flooding-based DDoS attacks generated by compromised nodes. An SD-IoT test-bed network is implemented, comprising three key components: the SDN controller, IoT controller, and clustered IoT nodes connected via Sensor OpenFlow Switches (SOFS). Malicious nodes are embedded within each cluster to simulate real-world DDoS scenarios by generating flood traffic toward target nodes. The network design allows for the analysis of various attack parameters, such as the number of attacker nodes, packet flooding frequency, and simulation time, enabling dynamic evaluation of the detection framework's performance in identifying abnormal traffic patterns.

There are more extensive evaluations with respect to performance: CPU/Memory usage, network thruput and attack detection time, amongst others. The ML-based framework consists of three core modules: (1) Module of Data plane: It contains Sensor OpenFlow Switches (SOFS), a network of SD-IoT and IoT devices. It controls the incoming traffic in IoT network and also serves as a gateway between the controller and the source IOT nodes. (2) IoT Controller Module: This module controls network traffic by directing SOFS switches to where packets should be forwarded by using a modified SDN controller. (3) DDoS Detection Module- Based on machine learning, this module performs traffic analysis on IoT nodes and also identifies and classifies DDoS attack packets (Figure 2).

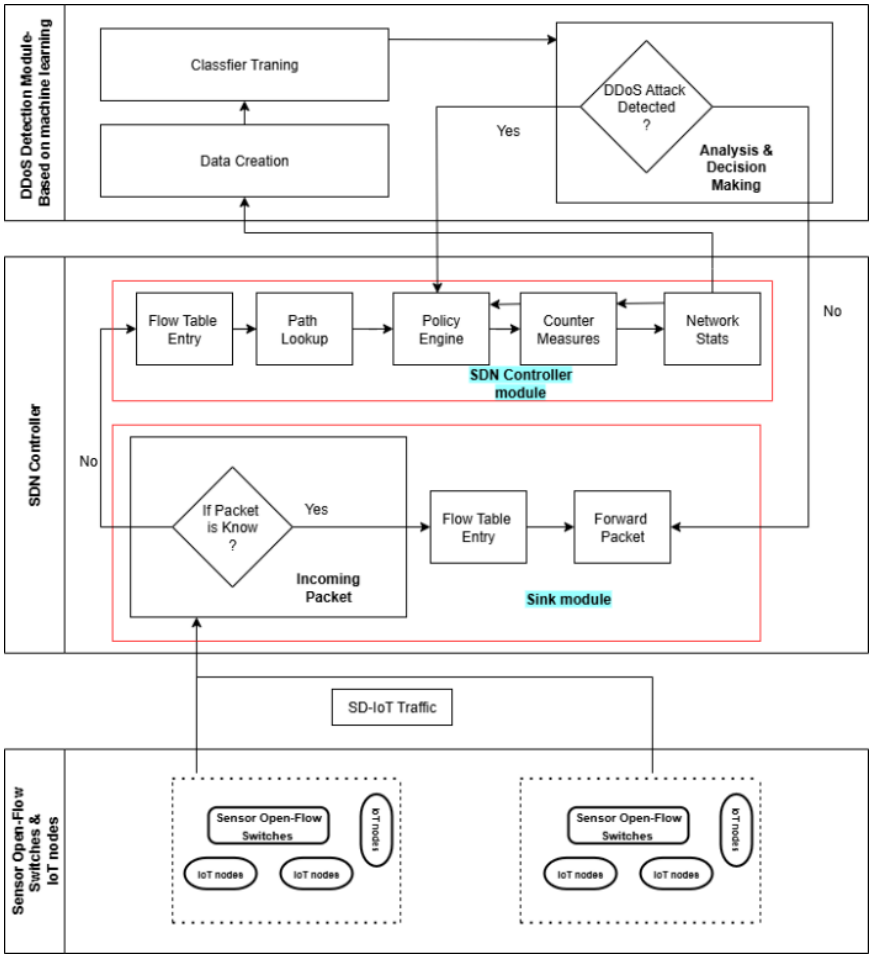


FIGURE 2. ML-based DDoS attack detection framework for SD-IoT networks

*F. SDN Controller*

The SDN controller integrates a logging module at the forwarding layer, recording every packet for DDoS detection and policy analysis. Topology discovery uses a decentralized beacon-based mechanism to identify optimal paths for nodes. Flow rules are stored in SOFS, dictating packet handling. Each IoT node maintains an Accepted IDs Array to filter incoming packets. The SDN controller orchestrates traffic flow, integrates ML-based security analytics, and responds to anomalies in real time.

*G. Machine Learning Integration*

Within the SDN controller, ML functions as a black-box interface for detecting DDoS attacks. Incoming packets from SOFS are first inspected by the IoT controller. Unknown packets are sent to the ML detection module for classification. The BoT-IoT dataset is loaded into WEKA, converted into a Java JAR to work with the SDN controller, and executed as a command-line argument specifying the classifier (Naïve Bayes, DT, or SVM). The classification output enables network operators to dynamically insert rules into the controller's flow table, forwarding or discarding packets based on detection results. Training features include simulation time, IoT node identifiers, detection timestamps (in milliseconds), packet frequency, and packet size.

# RESULTS AND ANALYSIS

This section will describe in detail the testbed which has been implemented and compare the results of various groups of simulations. Specifically, efficiency and functionality of DDoS detection section based on ML embedded within the Software-Defined Networking controller has been thoroughly examined.

The testbed specifications used for the experiments are Ubuntu v16. 0. 2, Intel® Core™ i5-9300H CPU 2.40 GHz processor, and 4.0 GB RAM. The SDN controller is employed with the testbed to simulate SDN-IoT network flow. The efficiency of the algorithms was quantified using the data correctly classified into posed or genuine on our dataset with a 20% training set and 80% testing set being obtained and used. For this this research prefer working with Cooja simulator which is a very good tool because both cooja are concerned with low-power reasons. In this study, Software-Defined IoT network model can be divided into four core parts: Machine Learning DDoS attack detection module on SDN controller, Software-Defined IoT network and controller. This Software-Defined IoT network element consists of IoT devices such as smart devices, sensors and other devices communicating using SOFS. This study constructed a network composed of malicious nodes and benign nodes. The Software-Defined IoT network is getting malicious/normal traffic by these IoT devices. Source of flooding set (SOFS) is a forwarding element that is used to forward Software-Defined IoT network flow based on the flow table. The IoT controller is a bridge between the SD-IoT network and machine learning (ML)-based security enriched deployments which are operated on the higher level SDN controller. The network controller enables the network management of network and provides northbound APIs for safe implementations. The Machine Learning based attack detection module is an overlay on the SDN that employ machine learning algorithms for the DDoS attacks detection. The experiments has shown the variations of these features: Simulation time, Number of attacking nodes and Packet-rate limit (normal and burst mode) (packets per minute).

These parameters was size dependent in experiments applied to test the model. This research performed a great deal of experiments to find out how much resources (like CPU, memory, detection time, etc.) of tuning size of each parameter to get the best results.

*A. Average Performance of Accuracy and Detection Rate*

In this machine learning framework, accuracy is defined as the average result of correctly classified packets, whereas detection rate is defined as the ratio of successfully detected attack packets to the total number of packets processed. These results are shown in Table 4.1, which is the average accuracy and detection rate of every finding in this research. Our Naive Bayes classifier has an accuracy of 97.9%, the Decision Tree classifier has an accuracy of 98.9% and the SVM classifier has an accuracy of 97.2%. It can be concluded from Table 4.1 to Table 4.11 that the DT model performs well in experiments A and experiments B, while the NB performs more efficient in experiment C. The overall average score of the proposed framework is 98.0%.

TABLE 4.1 Average performance of accuracy and detection rate

| Classifier name | Detection rate | Accuracy % |
|---|---|---|
| Naive Bayes | 557 | 97.9% |
| Decision Tree | 435 | 98.9% |
| SVM | 631 | 97.2% |
| Overall Average | 541 | 98.0% |

*B. IoT Node*

To present attack detection time of algorithms and methods in SD-IoT networks This research performed four experiments (Table 4.2 to Table 4.5). The configurations of Experiments A1 to A4 involve a fixed simulation time, a variable number of IoT nodes and a fixed packet transmission frequency.

There were four different conditions in experiment A. The Naive Bayesian Classifier, Support Vector Machine (SVM) classifier and Decision Tree (DT) Classifier are employed for the experiment. Results indicate that the detection times of three classifiers are also similar. Furthermore, the experiment also found that the Software-Defined IoT network of 5-45 nodes can make good use of the ML detection module, and achieve very good results, as shown in Figure 3. DT classifier has a good comparison result on detection time in average compared with the Naive Bayesian and the Support Vector Machine.

TABLE 4.2 EXP-A1 IoT node variations (5 IoT nodes)

| Algorithm name | Simulation time(min) | (Vary) IoT nodes | Packetfrequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 5 | 20 | 588 |
| DT | 15 | 5 | 20 | 491 |
| SVM | 15 | 5 | 20 | 610 |

TABLE 4.3 EXP-A2 IoT node variations (15 IoT nodes)

| Algorithm | Simulation time(min) | IoT nodes (Vary) | Packet frequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 15 | 20 | 585 |
| DT | 15 | 15 | 20 | 489 |
| SVM | 15 | 15 | 20 | 605 |

TABLE 4.4 EXP-A3 IoT node variations (30 IoT nodes)

| Algorithm | Simulation Time(min) | IoT nodes (Vary) | Packet frequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 30 | 20 | 583 |
| DT | 15 | 30 | 20 | 485 |
| SVM | 15 | 30 | 20 | 612 |

TABLE 4.5 EXP-A4 IoT node variations (45 IoT nodes)

| Algorithm | Simulation time(min) | IoT nodes (Vary) | Packet frequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 45 | 20 | 579 |
| DT | 15 | 45 | 20 | 485 |
| SVM | 15 | 45 | 20 | 608 |

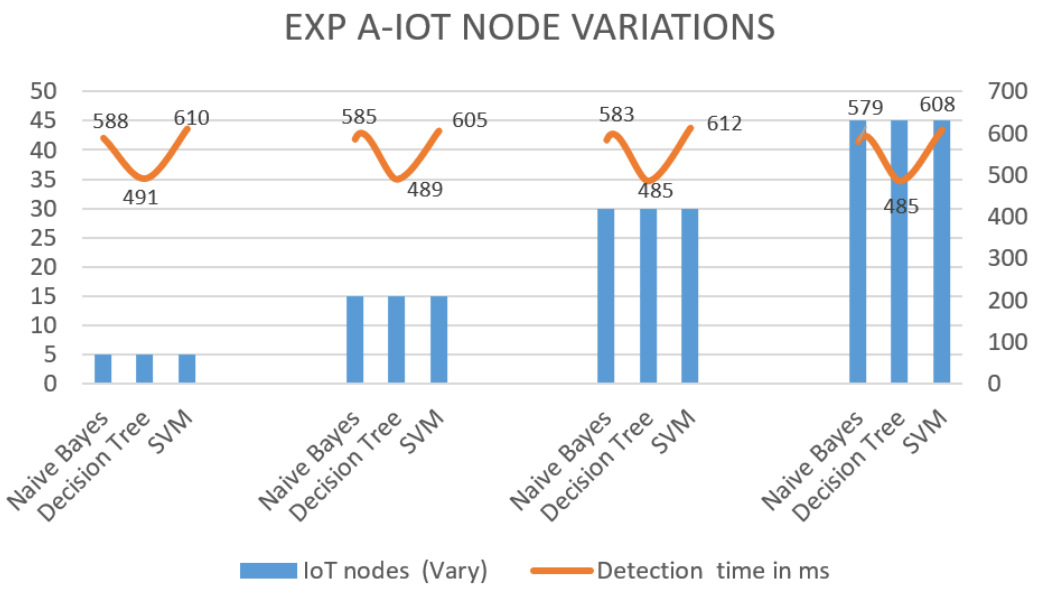


FIGURE 3. EXP A-IoT Node Variations

*C. IoT Packet*

In experiment B1 to B4, packet frequency is selected as the variable parameter, while the other four parameters are held constant, as shown in Table 4.6 to Table 4.9. Similar to experiment A, experiment B1 to B4 also was performed with five parameters and was observed that all selected ML classifiers spent similar detection time. The results illustrated that the ML based detection module requires up to 50 packets that can be generated per minute and doesn't affect detection time. However, the decision tree (DT) has a shorter average classification time compared with both NB and SVM, as shown in Figure 3.

TABLE 4.6 EXP-B1 IoT packet variations (10 pac/min)

| Algorithm | Simulation time (min) | IoT nodes | Packet frequency (Vary)( pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 15 | 10 | 570 |
| DT | 15 | 15 | 10 | 355 |
| SVM | 15 | 15 | 10 | 601 |

TABLE 4.7 EXP-B2 IoT packet variations (20 pac/min)

| Algorithm | Simulation time (min) | IoT nodes | Packet frequency (Vary)( pac/min) | Detection latency (ms) |
|---|---|---|---|---|
| NB | 15 | 15 | 20 | 575 |
| DT | 15 | 15 | 20 | 362 |
| SVM | 15 | 15 | 20 | 609 |

TABLE 4.8 EXP-B3 IoT packet variations (30 pac/min)

| Algorithm | Simulation time (min) | IoT nodes | Packet frequency (Vary)( pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 15 | 30 | 580 |
| DT | 15 | 15 | 30 | 358 |
| SVM | 15 | 15 | 30 | 608 |

TABLE 4.9 EXP-B4 IoT packet variations (50 pac/min)

| Algorithm | Simulation time (min) | IoT nodes | Packet frequency (Vary)( pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 15 | 50 | 577 |
| DT | 15 | 15 | 50 | 354 |
| SVM | 15 | 15 | 50 | 607 |

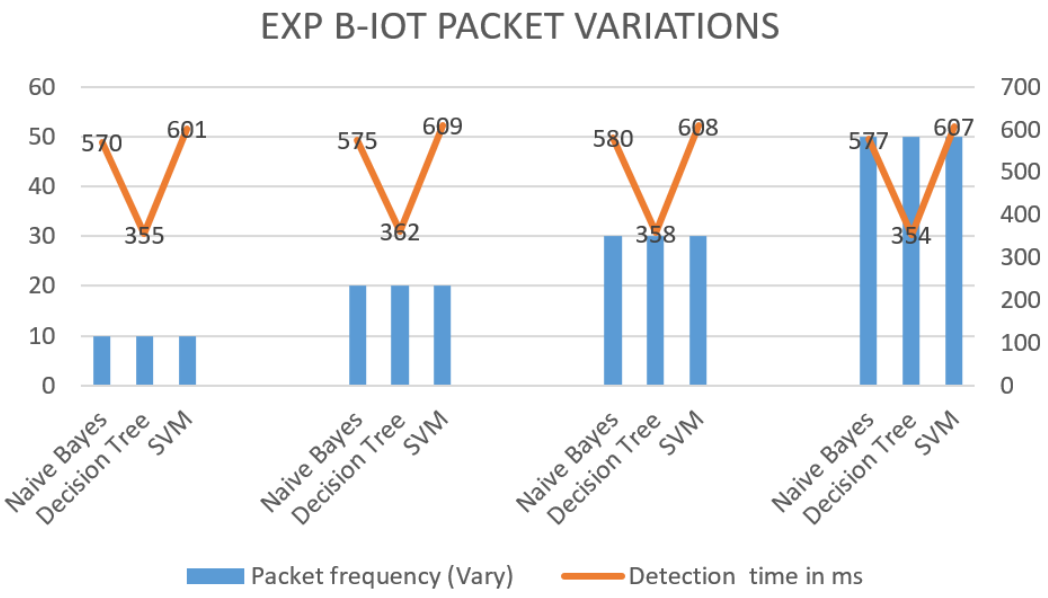


FIGURE 4. EXP B IoT packet variations

*D. Simulation Time*

In experiment C, this study chooses the interval of simulation time as the variable parameter from 45 to 15 min and another four parameters as constant values (Table 4.10 to Table 4.12). The results illustrated that it can't affect the detection time of ML module (Figure 5). But in terms of classification time on average, the Decision Tree (DT) classifier outperformed the other two classifiers.

TABLE 4.10. EXP-C1 simulation time variations (45 min)

| Algorithm | Simulation Time (Vary)(min) | IoT nodes | Packet frequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 45 | 15 | 20 | 411 |
| DT | 45 | 15 | 20 | 507 |
| SVM | 45 | 15 | 20 | 601 |

TABLE 4.11 EXP-C2 simulation time variations (30 min)

| Algorithm | Simulation Time (Vary) | IoT nodes | Packet frequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 30 | 15 | 20 | 459 |
| DT | 30 | 15 | 20 | 502 |
| SVM | 30 | 15 | 20 | 611 |

TABLE 4.12 EXP-C3 simulation time variations (15min)

| Algorithm | Simulation Time (Vary) | IoT nodes | Packet frequency (pac/min) | Detection time (ms) |
|---|---|---|---|---|
| NB | 15 | 15 | 20 | 571 |
| DT | 15 | 15 | 20 | 486 |
| SVM | 15 | 15 | 20 | 611 |

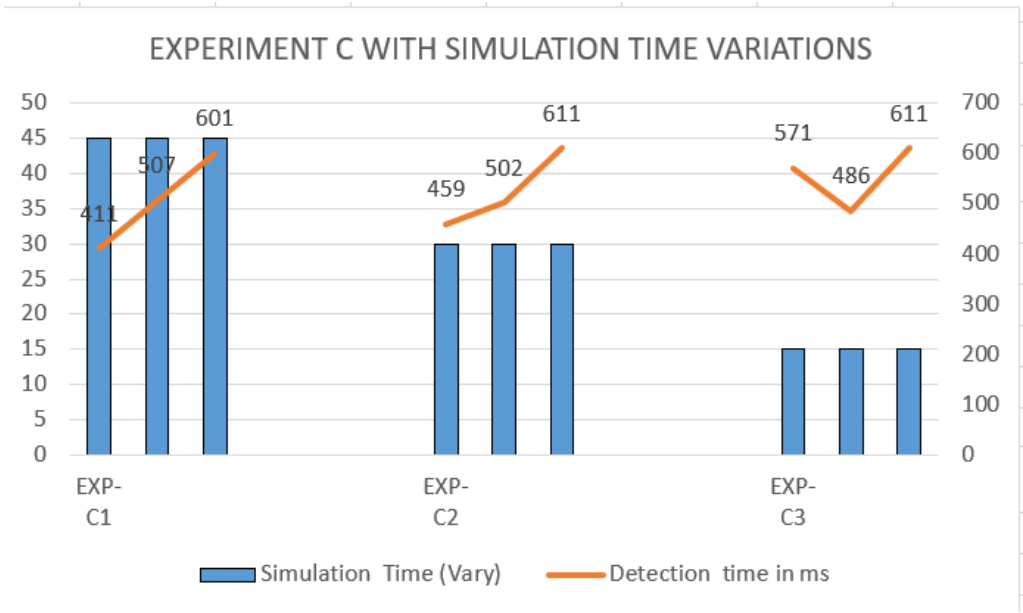


FIGURE 5. EXP C simulation time variations

*E. Usage of CPU and Memory Comparison*

This experiment aimed to compare CPU usage and memory utilization across these machine learning classifiers. These results demonstrated that machine learning module imposed minimal load on the system, consuming an incremental 3% of CPU used resources. Similarly,

memory usage increased by just 3% due to the module's operation, as illustrated in Figure 6. The findings revealed that the Support Vector Machine (SVM) classifiers and Decision Tree (DT) classifiers consumed nearly the same amount of CPU. However, the DT classifier required more memory than both SVM and Naive Bayes, as also shown in Figure 6.

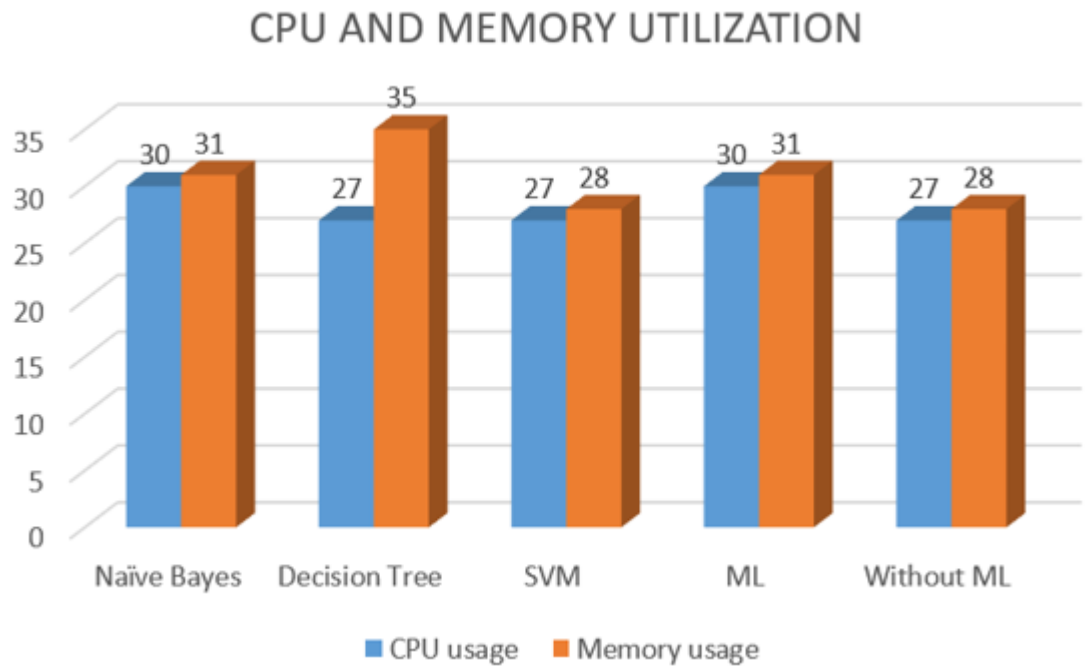


FIGURE 6. CPU and memory usage

## DISCUSSION

We observe that the CPU or memory usage is not affected if we increase the number of IoT nodes (at default node parameters) as shown in the experiments. However, certain factors, such as controller workload parameters, network throughput, and IoT nodes of SD-IoT, do influence CPU and memory consumption with the growth of packet payload, attack nodes, and burst mode of IoT. In this way, changes to these parameters have no impact on the algorithm, as it uses counters for storing integer and floating-point data. The set of IoT nodes in the study is up to 10, with a message rate ranging from 1 message per second up to 1000 messages per second in burst mode. The storage of counters can scale massively, so the counter variables themselves are unaffected. Moreover, the counter-based algorithm relies on reprogramming the counter value by a threshold, generating a DDoS attack alert message when the counter reaches the threshold. Results confirm that lightweight supervised ML integrated within SDN can provide high detection accuracy with minimal overhead.

Study results showed that the DT classifier can efficiently categorize harmful network packets in 480–500 ms for NB and SVM under other static parameters, with the number of IoT nodes ranging from a minimum of 5 to a maximum of 45. Attack detection times of the DT classifier decrease as packet frequency slows, although increasing packet frequency does not produce marked changes. Using different sizes for the two simulation parameters, NB performs better over shorter simulation durations of 30 and 45 minutes. The detection time difference is substantial, with the SVM classifier taking 597, 611, and 611 ms at simulation times of 45, 30, and 15 minutes, respectively. Overall, the DT classifier shows the best performance, while

SVM has the longest detection time, and changes in the number of IoT nodes have negligible effect, though packet frequency causes fluctuations in detection time.

From the CPU and memory utilization experiments, it was observed that the SVM classifier exhibits lower memory and CPU usage than Naive Bayes and DT classifiers. DT consumes the most memory at 35%, whereas the lowest CPU utilization observed among the classifiers is 27%. The SVM classifier shows the lowest CPU and memory usage during periodic inspections and the highest when inspecting all packets. In contrast, DT consistently incurs higher memory costs under both inspection modes.

While our results demonstrate that lightweight supervised ML integrated within SDN can achieve high detection accuracy with minimal overhead, several limitations should be noted. First, the study focuses on binary classification only, which may not fully capture more complex attack scenarios. Second, experiments were conducted on a small-scale testbed (5–45 IoT nodes), limiting generalization to large-scale networks. Third, validation was dataset-specific, so performance may vary with different traffic patterns or attack datasets. Finally, comparisons with deep learning-based approaches were discussed conceptually rather than experimentally, leaving room for future empirical evaluation.

## CONCLUSION

As key components of the modern digital ecosystem, IoT devices contribute to service availability and support mobile connectivity. Since IoT devices have limited energy and are often deployed in open environments, they are exposed to various attacks. This work focuses on security vulnerabilities related to IoT devices, particularly the detection and defense of DDoS attacks, both against and through IoT devices, which is indispensable for any IoT system. This research presents a new method using machine learning to detect DDoS attacks. The attack detection service leverages Software-Defined Networking (SDN) and operates on a centralized SDN controller, offering robust security defense for IoT networks. The network topology includes both innocent and malicious nodes to simulate large volumes of traffic. The DDoS attack detection program runs on the high-level SDN controller and applies machine learning classifiers such as Naive Bayes, Decision Tree, and SVM to classify the traffic. Timely detection of attacks is critical, allowing IoT devices interacting with malicious nodes to be isolated and preventing higher-level attacks from forming.

This study experimented with the proposed framework by simulating different types of attacks. The research can be further expanded to develop attack mitigation strategies and performance optimization solutions through the combination of supervised and unsupervised classifiers. Furthermore, the proposed solution can be applied to multiple DDoS attack forms and trained on different IoT-based datasets collected by sensors, improving model robustness and providing deeper insights. This work can also be generalized using supervised machine learning algorithms such as XGBoost, Random Forest, and other statistically driven techniques, and potentially extended to semi-supervised, unsupervised, or reinforcement learning. Additionally, it can include a DDoS defense module to discard attack traffic and shut down compromised nodes.

The proposed SDN-integrated ML framework achieves strong DDoS detection performance while maintaining low resource overhead. Future work will extend to multi-class attacks and deep learning-based comparative evaluation.

# REFERENCES


Abid, Yawar Abbas, Jinsong Wu, Guangquan Xu, Shihui Fu, and Muhammad Waqas. 2024. "Multilevel Deep Neural Network Approach for Enhanced Distributed Denial-of-Service Attack Detection and Classification in Software-Defined Internet of Things Networks." IEEE Internet of Things Journal 11 (14): 24715–25. https://doi.org/10.1109/jiot.2024.3376578.

Aggarwal, Saransh, Bhagrajyoti Behera, Murari Kumar Singh, and Ajeet Kumar Sharma. 2025. "Optimizing DDoS Attack Detection Using Machine Learning." 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), February 6, 245–50. https://doi.org/10.1109/cictn64563.2025.10932452.

Aljuhani, Ahamed. 2021. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments." IEEE Access 9: 42236–64. https://doi.org/10.1109/access.2021.3062909.

Almaraz-Rivera, Josue Genaro, Jesus Arturo Perez-Diaz, Jose Antonio Cantoral-Ceballos, Juan Felipe Botero, and Luis A. Trejo. 2022. "Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset." IEEE Access 10: 106909–20. https://doi.org/10.1109/access.2022.3211513.

Belachew, Habtamu Molla, Mulatu Yirga Beyene, Abinet Bizuayehu Desta, Behaylu Tadele Alemu, Salahadin Seid Musa, and Alemu Jorgi Muhammed. 2025. "Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning." IEEE Access 13: 10194–214. https://doi.org/10.1109/access.2025.3526692.

Bhayo, Jalal, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, and Dirk Draheim. 2023. "Towards a Machine Learning-Based Framework for DDOS Attack Detection in Software-Defined IoT (SD-IoT) Networks." Engineering Applications of Artificial Intelligence 123 (August): 106432. https://doi.org/10.1016/j.engappai.2023.106432.

Djuitcheu, Hubert, Maik Debes, Matthias Aumuller, and Jochen Seitz. 2022. "Recent Review of Distributed Denial of Service Attacks in the Internet of Things." 2022 5th Conference on Cloud and Internet of Things (CIoT), March 28, 32–39. https://doi.org/10.1109/ciot53061.2022.9766655.

Haddad, Nabeel Mahdy, Aqeel Sahi, Mohammed Diykh, et al. 2024. "Layered Model Stacking: Enhancing DDoS Detection Through Advanced Ensemble Machine Learning Techniques." TENCON 2024 - 2024 IEEE Region 10 Conference (TENCON), December 1, 1909–12. https://doi.org/10.1109/tencon61640.2024.10902823.

Infantia, H Niroshini, Kaviya K, and Harini M. 2025. "Empowering IoT Cyber Network Attacks Using Machine Learning." 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI), April 24, 90–96. https://doi.org/10.1109/icoei65986.2025.11013580.

Janardhana, D R, A P Manu, and V Pavan Kumar. 2023. "Detecting Privacy Attacks in IoT Network Using Deep Learning Models." 2023 IEEE 3rd Mysore Sub Section International Conference (MysuruCon), December 1, 1–6. https://doi.org/10.1109/mysurucon59703.2023.10397002.

Kumar, Abhishek, Pratyush Kushaniya, Vicky Kumar, and Avneesh Kumar. 2023. "A Review on Machine Learning Techniques for Secure IOT Networks." 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), December 15, 88–91. https://doi.org/10.1109/icac3n60023.2023.10541477.

Kumar, Gotte Ranjith, Anagha Deepak Kulkarni, B Santhosh Kumar, Navdeep Singh, V Revathi, and T.Ch.Anil Kumar. 2024. “Machine Learning Approaches for Anomaly Detection in IoT Networks.” 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), May 9, 1–5. https://doi.org/10.1109/accai61061.2024.10601954.

Mahdi, Zaed, Nada Abdalhussien, Naba Mahmood, and Rana Zaki. 2024. “Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms.” Computers, Materials & Continua 80 (2): 2139–59. https://doi.org/10.32604/cmc.2024.053542.

Qaiser, Ghazia, Siva Chandrasekaran, Rifai Chai, and Jinchuan Zheng. 2023. “Classifying DDoS Attack in Industrial Internet of Services Using Machine Learning.” 2023 15th International Conference on Computer and Automation Engineering (ICCAE), March 3, 546–50. https://doi.org/10.1109/iccae56788.2023.10111178.

R, Varaprasad, Prabhu Chakkaravarthy A, and Veeresha M. 2024. “A Comprehensive Analysis of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms.” 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), August 23, 1–5. https://doi.org/10.1109/iacis61494.2024.10721636.

Raj, Ritu, and Sandeep Singh Kang. 2022. “Mitigating DDoS Attack Using Machine Learning Approach in SDN.” 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), December 16, 462–67. https://doi.org/10.1109/icac3n56670.2022.10074307.

Ravi, Nagarathna, and S. Mercy Shalinie. 2020. “Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture.” IEEE Internet of Things Journal 7 (4): 3559–70. https://doi.org/10.1109/jiot.2020.2973176.

Sakr, Hesham A., Mostafa M. Fouda, Ahmed F. Ashour, Ahmed Abdelhafeez, Magda I. El-Afifi, and Mohamed Refaat Abdellah. 2024. “Machine Learning-Based Detection of DDoS Attacks on IoT Devices in Multi-Energy Systems.” Egyptian Informatics Journal 28 (December): 100540. https://doi.org/10.1016/j.eij.2024.100540.

Sangodoyin, Abimbola O., Mobayode O. Akinsolu, Prashant Pillai, and Vic Grout. 2021. “Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning.” IEEE Access 9: 122495–508. https://doi.org/10.1109/access.2021.3109490.

Sebbar, Anass, and Karim Zkik. 2023. “Enhancing Resilience against DDoS Attacks in SDN - Based Supply Chain Networks Using Machine Learning.” 2023 9th International Conference on Control, Decision and Information Technologies (CoDIT), July 3, 230–34. https://doi.org/10.1109/codit58514.2023.10284387.

Sharma, Anshika, and Himanshi Babbar. 2024. “Enhancing DDoS Attack Detection Deploying Machine Learning in Software Defined Networking Environment.” 2023 4th International Conference on Intelligent Technologies (CONIT), June 21, 1–6. https://doi.org/10.1109/conit61985.2024.10626979.

Singh, Chandrapal, and Ankit Kumar Jain. 2024. “A Comprehensive Survey on DDoS Attacks Detection & Mitigation in SDN-IoT Network.” E-Prime - Advances in Electrical Engineering, Electronics and Energy 8 (June): 100543. https://doi.org/10.1016/j.prime.2024.100543.

Tripathy, Asis Kumar, Alekha Kumar Mishra, and Rashmi Panda. 2024. “Performance Comparison and Analysis of Machine Learning and Deep Learning Models for Network Intrusion Detection In IoT-Edge Frameworks.” 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), February 22, 1–6. https://doi.org/10.1109/ic-etite58242.2024.10493276.

Wang, Song, Juan Fernando Balarezo, Karina Gomez Chavez, et al. 2022. “Detecting Flooding DDoS Attacks in Software Defined Networks Using Supervised Learning Techniques.” Engineering Science and Technology, an International Journal 35 (November): 101176. https://doi.org/10.1016/j.jestch.2022.101176.

Yungaicela-Naula, Noe Marcelo, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. 2021. “SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning.” IEEE Access 9: 108495–512. https://doi.org/10.1109/access.2021.3101650.