International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Mitigation of Cyber Attacks in SDN-Based IoT Systems Using Machine Learning Techniques

[1]Kamal Singh, [2]Prof. (Dr.) Brijesh Kumar, [3]Sunil Kumar, [4]Veer Pratap Singh, [5]Ashanendra Singh

Submitted: 01/10/2023 **Revised**: 29/11/2023 **Accepted**: 09/12/2023

Abstract: Complex Distributed Denial-of-Service (DDoS) security assaults threaten the expansion of intelligent network infrastructure for the Internet of Things (IoT). The IoT cannot be protected by the enterprise network security solutions currently in use because they are too expensive. Integrating newly developed software-defined networking (SDN) technology effectively mitigates a computational load on an IoT network device, enabling the implementation of supplementary security measures. Because it is utilized in the precursor stage of the design for SDN-enabled IoT networks. However, sampling-based security offers poor DDoS attack detection accuracy. This study aims to investigate cognitive techniques for detecting and mitigating cyber risks in software-defined and contemporary network applications. SDN is a modern technology network that allows for centralized control and cyber threat detection with built-in machine learning techniques for increasing the adoption of (IoT) devices. SDN applications have become vulnerable to cyber threats. To ensure the security of these applications, detection and mitigation of cyber threats are crucial. Adopting SDN can result in benefits, including increased manageability, scalability, and overall performance. However, SDN poses issues, primarily if it is controlled and open to DDoS attacks. Machine learning-based models were employed in this specific research project to identify DDoS attacks in SDN. Based on the research results, the KNN classifier, in combination with the wrapper feature, leads to the most fantastic accuracy rate of about 98.3% in detecting attacks.
The results of this study indicate that in addition to the anticipated reduction in processing burdens, feature selection and machine learnin g techniques can enhance DDoS attack detection in SDN.

Keywords: *Cyber Threats; SDN; DDOS; IOT, Network Security*

1. Introduction:

Due to advancements in cloud computing, big data, and mobile networks, there has been a consistent rise in the number of IoT use cases and connected devices. Use cases for the IoT that significantly improve the quality of our lives include, amongst many others, autonomous vehicles, smart cities, smart homes, security systems, and remote medical treatment. Improvements are needed to the current wireless networks to meet the quality of service (QoS) requirements of these many use cases, given the massive amounts of data generated by the Internet of Things. Networks that go beyond 5G and depend on network function virtualization (NFV) and SDN for resource management will be significant enablers for the ubiquitous IoT of the future [1]. A wide variety of security risks, such as "malware, ransomware, phishing attacks, and DDoS attacks," can affect IoT networks. Malicious software assaults could use IoT device vulnerabilities to obtain unauthorized access to the device or other network components. These attacks can substantially harm IoT networks by encrypting data stored on IoT devices. Phishing attacks have the potential to gain unauthorized access to IoT devices, in addition to facilitating the initiation of several other types of attacks, including DDoS attacks [2]. While SDN offers flexibility and centralized control over network resources, IoT devices bring connectivity and data exchange capabilities to various applications. However, this convergence also introduces new attack vectors and vulnerabilities. Here are some common SDN-based IoT system-related attacks:

1. *DoS attacks:* Attackers can flood the SDN controller with a high volume of requests or flood IoT devices with excessive traffic, leading to a denial of service. This can interfere with the accessibility and functionality of the IoT system.

2. Man-in-the-middle (MitM) attacks: Data can be intercepted and altered by attackers when exchanged between IoT devices and the SDN controller or other components in the network. This allows them to eavesdrop on sensitive information or inject malicious commands.

3. Unauthorized access: Weak authentication and authorization mechanisms in SDN and IoT devices can

[1]*IT Architect, IPGSL, UK, Manav Rachna International Institute of Research and Studies, India*
Email ID: kamallohiaji@gmail.com
[2]*Dean Academics, Manav Rachna International Institute of Research and Studies, India*
Email ID: brijesh.fet@mriu.edu.in
[3]*Executive Director, KPMG, Malaysia*
Email ID: sunildayal366@gmail.com
[4]*IT Architect, IPGSL, UK*
Email ID: veerupra@gmail.com
[5]*Principal Consultant, Wipro, Australia*
Email ID: ashanendra@hotmail.com

permit unauthorized access to the network by attackers. Once inside, they can compromise devices, steal data, or launch further attacks.

4. Data breaches: IoT devices often gather and send information. Attackers who gain access to the SDN controller or IoT devices can intercept or manipulate this data, leading to data breaches and privacy violations.

5. Firmware or software vulnerabilities: IoT devices may have vulnerabilities in their firmware or software, which threat vectors can exploit to gain control over the device or inject malicious code into the network.

6. IoT botnets: Attackers can compromise many IoT devices and turn them into botnets. This botnet can then launch DDoS attacks or perform other malicious activities.

The most significant potential consequences of DDoS assaults on IoT devices are outlined in Table 1.

DAMAGE NAME	**DESCRIPTION**
Disruption of Service	AA DDoS attack may lead to a significant influx of network traffic, potentially impeding or rendering impossible the establishment of connections between devices or other systems. Consequently, this disruption of services would ensue.
Malware Infection	Malware can undermine the device's security, giving an attacker access to it to use it against you.
Data Theft	DDoS attacks can facilitate the unauthorized acquisition of sensitive information from IoT devices. A DDoS attack, for example, might be employed by a malicious actor to inundate a targeted device, thereby inducing a system failure and potentially exposing confidential data such as passwords, credit card details, or personally identifiable information.
Network Congestion	DDoS assaults can generate a substantial volume of network traffic, impeding the performance of interconnected devices and causing congestion inside networks. The whole user experience may be negatively impacted due to factors such as latency, packet loss, and various other difficulties.
Reputation Damage	The potential utilization of their devices in DDoS attacks poses a reputational risk for enterprises providing IoT devices and services. Customers may lose faith in the organization and employ alternative alternatives offering greater security.

Table 1: Main potential damage

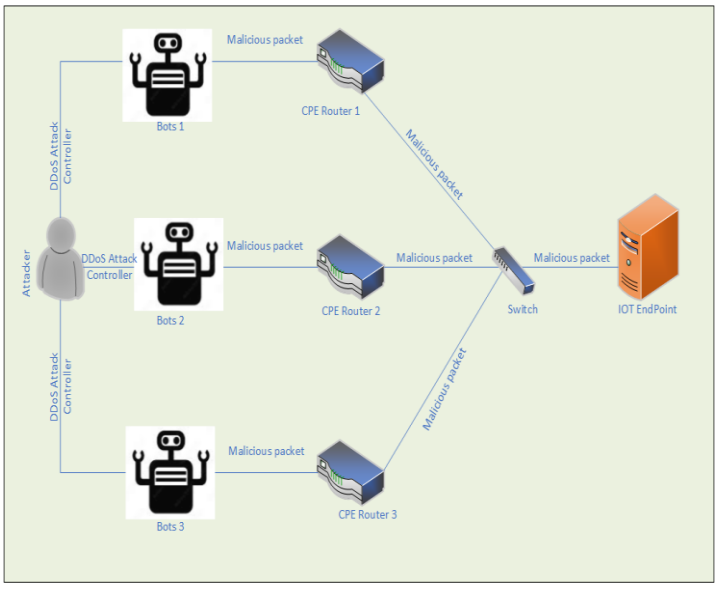


Fig 1: DDoS attacks on the IoT

Using machine learning-based methodologies, SDN administration, security, and optimization concerns can be resolved flexibly, effectively, and intelligently [4]. Timely identification of "DDoS attacks is essential to facilitate fast intervention and uphold network security integrity. Integrating machine learning-based DDoS attack detection systems into the architecture and design of an SDN makes it possible to create a self-governing network with learning and action capabilities. This is achieved through the processing of SDN flow data. Additionally, studies aiming to integrate 5G networks may use SDN with a built-in machine-learning application as a reference model for constructing a secure framework [5,6]. The previous literature relevant to this investigation is elaborated in the following parts.

2. Literature Review:

AUTHORS AND YEARS	METHODOLOGY	FINDINGS
Arevalo Herrera & Camargo (2019) [7]	This article reported investigations using ML in SDN settings for security applications. The reviewed papers are categorized into IDS frameworks for SDN and ML approaches (used to spot broad abnormalities or targeted assaults).	The second group is significant since the first category of examined papers also includes the implementation of data gathering and mitigation measures. The standard datasets, testbeds, and other research resources are also identified in this study.
Vimal et al., (2022) [8]	IoT encryption for information access control is strengthened by designing and integrating the proposed network architecture into Ser IoT approaches. Because of its adaptability, the technique may avoid finite intervals, deterministic energy, target nodes, falling potential cryptographic capacity, and unpredictable system connectivity.	The final antitheft solution that complies with pre-set circuit limits uses appropriate marketing strategies based on genuine statistical data. For the platform to be effective, a study must cooperate by exposing various faults caused by the clusters' visible instability.
Uribe et al., (2022) [9]	A thorough evaluation of the literature was done. This study assessed the risks and assaults that can damage the wireless networks that enable SDR systems and the Internet of Things, as well as the most recent methods for thwarting them. The perception layer of the IoT reference model was determined to be the most exposed. Due to hardware constraints, physical device exposure, and technological heterogeneity, most attacks at this level occur.	However, the complexity of the IoT's cybersecurity concerns makes combining SDR hardware with cognitive and intelligent approaches strongly recommended. Deep learning is one of these strategies that could be used to modify mitigation systems in response to quick technology advancements.
Cai et al., (2023) [10]	To identify and counteract DDoS attacks in software-defined CPSs, the study presented an adaptive DDoS attack mitigation (ADAM) system. Information entropy and unsupervised anomaly detection approaches are combined by ADAM to accurately prevent DDoS attacks after automatically determining the current condition and identifying suspicious aspects.	Under highly intense DDoS attacks, actual data-driven trial findings demonstrate that ADAM has an average mitigation accuracy of 99.13%. Our technique decreases the false-positive rate by 35%-59% compared to previous research.
Khedr et al., (2023) [11]	The study discusses FMDADM, a four-module DDoS attack detection and mitigation framework for IoT networks based on SDN.	The experimental findings showed that FMDADM met the benchmarks for "accuracy,

	The proposed FMDADM framework has a five-tier design and four primary modules. The initial module uses a window size of 32 packets to establish an early detection method that relies on the average drop rate (ADR).	precision, F-measure, recall, specificity, negative predictive value, false positive rate, false detection rate, false negative rate", and average detection time in the following order: 99.79%, 99.43%, 99.77%, 99.79%, 99.95%, 00.21%, 00.91%, 00.23%, and 2.64 s, respectively.

Table 2: Literature Review

The identification of the DDoS assault on the SDN controller and the switches within the data plane is crucial for maintaining network stability and identifying legitimate traffic at the time of the attack, according to previous literature research. Updating new rules to the flow table of switches in the data plane becomes a more straightforward task for the controller when it can identify attack traffic. This will help the controller stop the attack. This offers a significant edge in stopping the attack. So, this study's primary objective is to look into cognitive techniques for detecting and mitigating cyber risks in software-defined and contemporary network applications. This study suggests using feature selection techniques and machine learning models to detect DDoS attacks.

3. Methodology:

SDN Topology

The OpenFlow SDN controller is a critical component of an SDN network that is responsible for managing and controlling data traffic flow between network devices. Some of the critical components of an OpenFlow SDN controller include:

Southbound API is the interface between the OpenFlow controller and the network devices, such as switches and routers. The Southbound API exchanges messages between the controller and the network devices, allowing the controller to instruct the devices on how to forward traffic.

Northbound API: This is the interface between the OpenFlow controller and the network applications. The Northbound API allows applications to communicate with the controller and request network services such as load balancing, security, and QoS.

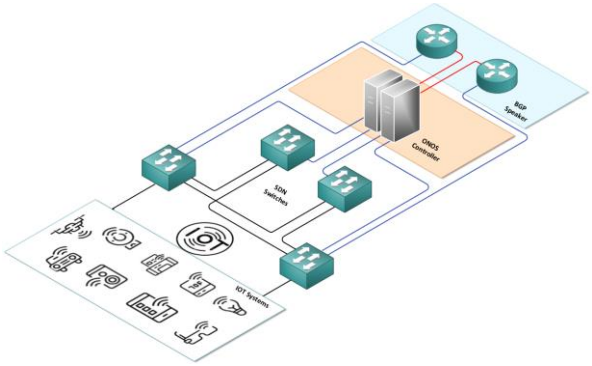
East/Westbound API: East/westbound APIs are the interfaces that allow the SDN controller to communicate to controllers that are distributed out.

Security Module: The security module provides security services such as user authentication, encryption, and access control to ensure that only authorized users can access the network.

Management Module: The management module configures and manages the OpenFlow controller, network devices, and applications.

ONOS (Open et al.) [16]is an open-source SDN controller platform developed by the Open Networking Foundation (formerly ON.Lab) and a community of contributors. It features a modular and distributed architecture, where different functions and services are implemented as microservices that can run on different nodes in a cluster. The core of ONOS is based on the Raft consensus algorithm for cluster coordination and communication. ONOS provides northbound and southbound interfaces for communication with network devices and applications. The southbound interface supports OpenFlow, NETCONF, and other protocols for communication with network switches and routers.

In contrast, the northbound interface provides REST APIs, gRPC, and other interfaces for communication with network applications. ONOS supports various SDN features, including topology discovery, network control and configuration, flow management, load balancing, and network slicing. It also supports virtualization and multi-tenancy, allowing multiple users and applications to share the same network infrastructure. ONOS can be deployed on various platforms, including bare-metal servers, virtual machines, and cloud environments.



Enabled SDN IoT

Mitigating these attacks in SDN-based IoT systems requires a multi-layered approach:

1. Secure authentication and access controls: Implementing robust mechanisms and access control to prevent unauthorized access to both IoT devices and the SDN controller.

2. Encryption and secure communication: Use encryption protocols to secure the communication and data transmission between various IoT devices and the SDN controller. This prevents eavesdropping and tampering of sensitive information.

3. Intrusion detection and prevention systems: Implement intrusion detection and prevention systems to monitor network traffic, spot irregularities, and stop hostile activity in real-time.

4. Regular firmware and software updates: Maintain IoT updated and patched with the most recent software and firmware updates to reduce known risks.

5. Network segmentation: Divide the network into distinct zones or virtual networks to prevent possible assaults and lessen the effects of security breaches.

6. Security monitoring and incident response: Put in place reliable security monitoring systems to quickly identify and stop assaults. This includes logging and analyzing network activities and having an incident response plan.

A Machine Learning-Based DDoS Detection Technique for Software-Defined Networks The dynamic and complicated nature of SDNs makes detecting and mitigating DDoS attacks difficult. To tackle this problem, one way is to use machine learning methods for DDoS detection. An overview of a machine learning-based DDoS detection technique in SDNs is provided below:

1. Data Collection: Gather network traffic data from different points within the SDN infrastructure. This can include flow-level information, packet headers, and other relevant network statistics. The data can be collected using monitoring tools or tapping into network switches.

2. Feature Extraction: Extract meaningful features from the collected data that can help differentiate regular network traffic from DDoS attack traffic. Features include packet rates, flow duration, packet size distribution, protocol distribution, and other statistical characteristics.

3. Training Dataset Preparation: Label the collected network traffic data as usual or DDoS attack traffic. This labelling can use historical attack data, signature-based or anomaly detection techniques. Create a labelled training dataset that contains a representative set of standard and attack traffic samples.

4. Feature Selection: Use feature selection techniques to identify the most relevant features for DDoS detection. Using this step helps reduce the dimensionality of the data and improve the efficiency of the machine learning algorithms.

5. Machine Learning Model Training: Implementing ML technique, SVM or neural networks to train a model using the labelled training dataset. The model learns the patterns and characteristics of ordinary and DDoS attack traffic from the training data.

6. Model Evaluation: The trained machine learning model is evaluated using a separate testing dataset. Measure the model's performance metrics, such as accuracy, precision, recall, and F1-score, to assess its effectiveness in distinguishing between regular and attack traffic.

7. Deployment and Real-Time Detection: Deploy the trained machine learning model in the SDN environment to detect real-time DDoS attacks. The model can continuously analyze incoming network traffic and classify it as usual or malicious based on the learned patterns.

8. Response and Mitigation: Once a DDoS attack is detected, the SDN controller can trigger appropriate mitigation strategies, such as rate limiting, traffic filtering, or redirecting the attack traffic to a dedicated scrubbing centre.

It is worth noting that the success of machine learning-based DDoS detection in SDNs relies on the availability of high-quality training data, continuous monitoring, and regular updates to adapt to evolving attack techniques. Additionally, the detection system should be regularly

evaluated and refined to maintain its effectiveness in the face of new and emerging DDoS attacks.

This study employs machine learning models supported by feature selection approaches to detect DDoS threats. Figure 2 illustrates the procedures that must be taken to implement the feature selection methods and machine learning models successfully. In addition, an explanation of how the data is extracted from the dataset, as well as an analysis of the characteristics and categories of the dataset, are provided in this section. The primary metrics that are indispensable to the upkeep of the SDN architecture were utilized to derive the characteristics included in the dataset that was developed as part of the scope of the investigation. Machine learning methods were used to categorize the attack data gathered due to DDoS assaults. After selecting features from the dataset with the help of feature selection methods, it was determined how well classifiers performed on the generated feature set. An environment called Matlab was used to carry out the study of the application.

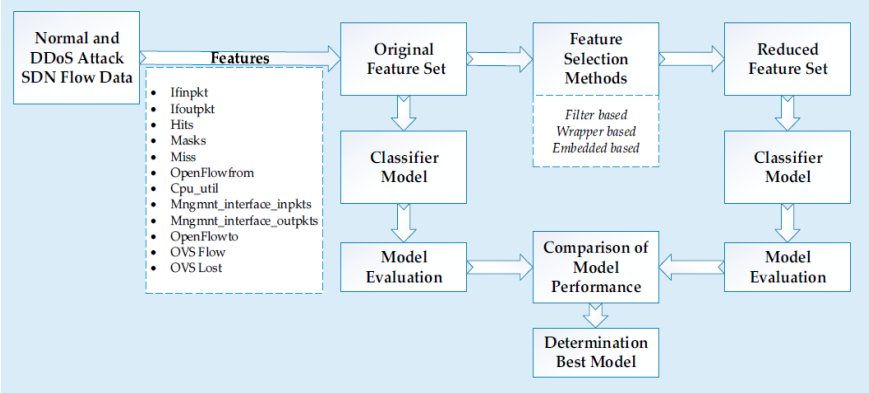


Fig 2: Process steps for applying the feature selection methods and machine learning models [5]

This work employs machine learning models enhanced by feature selection techniques to identify DDoS assaults. Machine learning is a computational approach that generates predictions regarding unknown phenomena by leveraging mathematical and statistical methodologies to draw inferences from existing data. Many diverse machine-learning models have been proposed in the academic literature. The classification of models can be summarised by considering their properties, such as kernel-based, distance-based, neural network-based, and probability-based approaches. The effectiveness of SVM, KNN, ANN, and NB models for identifying DDoS attacks as candidates for their categorization group was examined in this study.

Large numbers of features may be present in the datasets used in the training and testing of machine learning models. Although some of these factors significantly impact the categorization outcome, other features have little to no impact. Utilizing features with minimal bearing on classification might extend processing times and increase expenses. The objective is to provide highly effective features while reducing the use of features with little bearing on classification as feature selection techniques, the filter, embedding, and wrapper approaches were applied. While the wrapper technique mainly focuses on the utility of features depending on the classifier's performance, the filter method primarily focuses on the intrinsic qualities of the features. Among the wrapper-based feature selection techniques, a greedy search-based Sequential Forward Selection (SFS) algorithm was chosen since it has a history of identifying an ideal feature subset. The Lasso or L1 algorithm was chosen as the embedded feature selection method because it introduces a complexity penalty to lessen the degree of overfitting and enhances the mode's optimization efficiency.

ML TECHNIQUES	EXPLANATION	IMPLEMENTATION IN THE PROPOSED STUDY
Support Vector Machine (SVM)	SVM is a supervised learning model used in the learning industry that defines and analyses discovered patterns using regression analysis and classification. The Openflow switch in the SDN architecture	The SDN controller is in charge of gathering switch traffic statistics, making forwarding decisions, and forwarding traffic. Periodically, the OpenFlow switch provides a flow table to the flow state collection, which then replies with the flow table data. The process of creating the six-tuple characteristic values matrix involves extracting the characteristic value from the switch flow table.

	quickly forwards the primary network data.	This is mainly responsible for getting the characteristic values connected with the DDoS assault. Six-tuple characteristic values are classified using an SVM-based method to distinguish between normal and abnormal attack traffic.
Naive Bayes (NB)	NB classification uses a sequence of computations defined by the probabilistic principles to identify the class, or category, of the data entered into the system.	The study illustrates that Naive Bayes classifiers are a group of classification techniques based on the Bayes theorem. It is a collection of algorithms that share a common foundation. This chapter presents the scoreboard dataset's use in DDoS attack detection. The feature vector and the reaction vector are the two components of the dataset. The term "feature vector" refers to a collection of dataset rows, and is made up of a vector that holds the value of a dependent feature, like the number of packets, IP address, port, counter, or flag. The reaction vector contains the value of the class variable (prediction or output) for each row. The outcome demonstrates how well the approach prevents DDoS attacks by categorizing requests.
Artificial Neural Network (ANN)	Based on the artificial neuron concept, ANN is a powerful classification tool. Its fundamental building block is a neuron. The behaviour of artificial neurons is intended to resemble that of organic neurons. This study's single hidden layer of the ANN architecture contains ten neurons and 12 input units.	To teach the ANN DDoS detection system to distinguish between normal and anomalous traffic, the technique looks at the system resources and network data. Legitimate traffic can proceed, whereas suspicious-looking anomalous traffic must pass via a detection and defence mechanism. This ANN-based DDoS detection technique detected DDoS attacks with reasonable accuracy.
K-Nearest Neighbors (KNN)	Both classification and regression issues can be resolved using the KNN technique, a straightforward, broadly applicable, and supervised machine learning approach.	The KNN method is based on the clustering principle. The clustering technique involves grouping the complete data set into units (sometimes called clusters) based on some data similarity. Clustering is a challenge in unsupervised learning. Each time fresh data was met, the Euclidean function was used to calculate how far away it was from the data in the training set. The k dataset with the smallest distance was then chosen to build the classification set. The value of categorization determines the number of nearby KNNs (k). The categorization yielded the value of k as 10.

Table 3: ML techniques used in this study [5]

To examine the effects of the attack traffic, network measurements were collected from the OVS switch using a sFlowDocker image both during the attack and during normal traffic. To do this, an open-source time-series platform called InfluxDB picture with a timestamp was used to record network metrics data using JavaScript.

An attack scenario based on protocols was used in this study. Three different types of flooding attacks—Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Protocol (ICMP)—were used to create a DDoS attack dataset using a "hping3" packet generator. After PC1 was installed on the network, PC6 was chosen as the victim and PC1 as the

attacker thanks to the Hping3 program. PC6 is under assault, and its IP address is 10.0.0.6. The payload size of each protocol-based flooding attack is always 512 bytes, and the packet rates are always 2000 packets per second (pps). As a result, a controller sends out more than 1304 flow modification messages per second, resulting in 6996 entries in the flow table.

Utilizing feature selection techniques, the dataset produced for the study was decreased before the classification was done utilizing these data. As classifiers, SVM, NB, ANN, and KNN were employed. There were two phases to the experimental investigation. All of the features in the dataset were used to train and test classifiers. The dataset was split into training and testing sets using the k-fold cross-validation (k = 10) approach to assess the method's effectiveness [5] in the initial stage. Methods for feature selection were utilized in the second stage. The most efficient feature in the entire dataset was chosen using the Relief, sequential forward floating selection, and Lasso algorithms, respectively, as the filter, wrapper, and embedded feature selection techniques. These feature selection techniques resulted in the creation of three distinct datasets. SVM, NB, ANN, and KNN algorithms independently determined the highest performance ratio for each of the three datasets, between 1 and 12 features.

Figure 3 illustrates an experimental setup designed to gather data encompassing regular network operations and DDoS attacks. The architecture comprises an open-source OpenFlow/SDN controller, specifically ONOS, with a Mininet emulator. The network topology comprises six switches organized in a Spine and Leaf configuration. The topology itself was deployed using VirtualBox-KVM. The Open vSwitch (OVS) switch facilitated the connections between switches. To simulate the DDoS attack, Kali Linux's hping tool was employed.

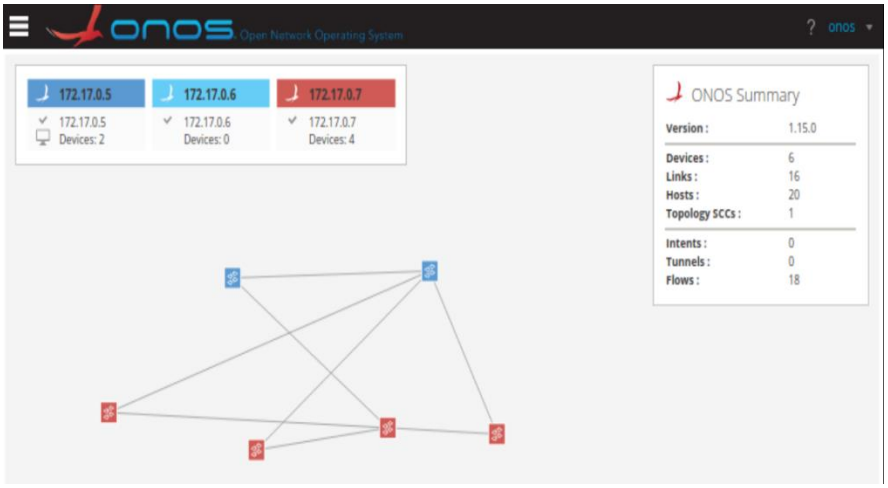
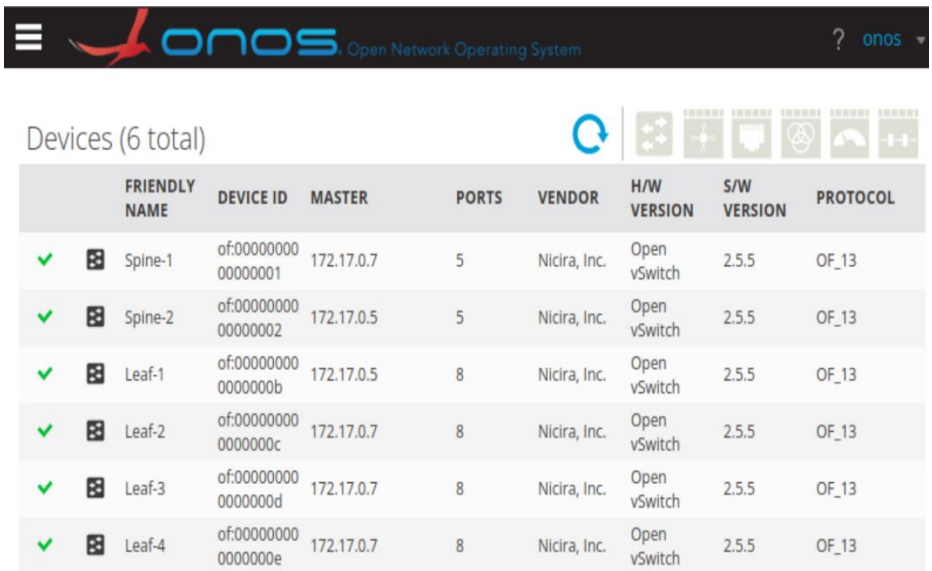
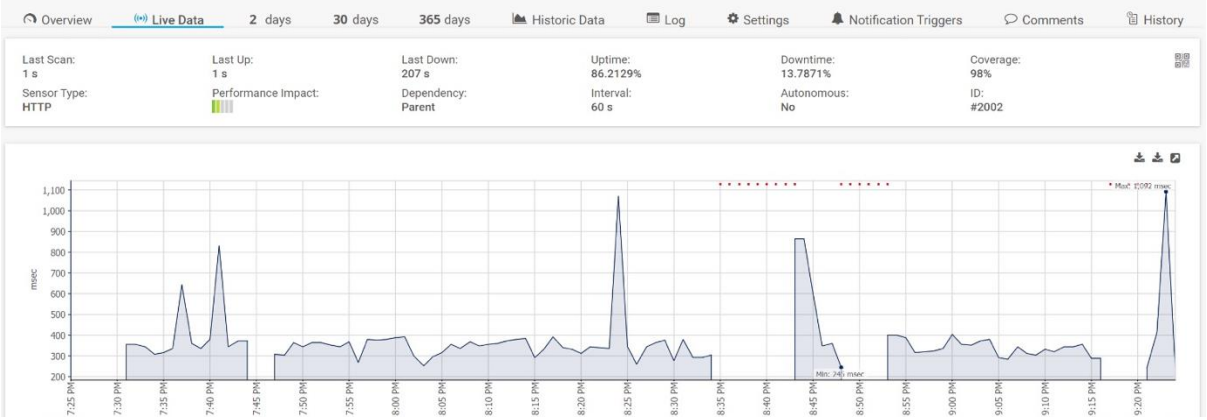


Fig 3: Experimental SDN topology for collecting data.



	FRIENDLY NAME	DEVICE ID	MASTER	PORTS	VENDOR	H/W VERSION	S/W VERSION	PROTOCOL
✓	Spine-1	of:0000000000000001	172.17.0.7	5	Nicira, Inc.	Open vSwitch	2.5.5	OF_13
✓	Spine-2	of:0000000000000002	172.17.0.5	5	Nicira, Inc.	Open vSwitch	2.5.5	OF_13
✓	Leaf-1	of:000000000000000b	172.17.0.5	8	Nicira, Inc.	Open vSwitch	2.5.5	OF_13
✓	Leaf-2	of:000000000000000c	172.17.0.7	8	Nicira, Inc.	Open vSwitch	2.5.5	OF_13
✓	Leaf-3	of:000000000000000d	172.17.0.7	8	Nicira, Inc.	Open vSwitch	2.5.5	OF_13
✓	Leaf-4	of:000000000000000e	172.17.0.7	8	Nicira, Inc.	Open vSwitch	2.5.5	OF_13

SDN Switch Topology



DDOS Attack Traffic Analysis

4. Results and Discussions:

At the beginning of this research project, the dataset analyzes regular traffic moments and DDoS assault traffic moments using SDN architecture. At this point in the investigation, it did not employ any feature selection. Table 4 displays the findings that were acquired from the investigation that was carried out.

Classifier	Accuracy	Sensitivity	Specificity	Precision	F1_Score
SVM	92.11%	88.71%	96.93%	91.42%	89.91%
KNN	95.67%	93.87%	98.01%	97.05%	95.30%
ANN	91.07%	87.27%	96.58%	89.89%	88.45%
NB	94.48%	91.77%	98.29%	92.94%	91.79%

Table 4: Performance of the machine learning models without a feature selection method.

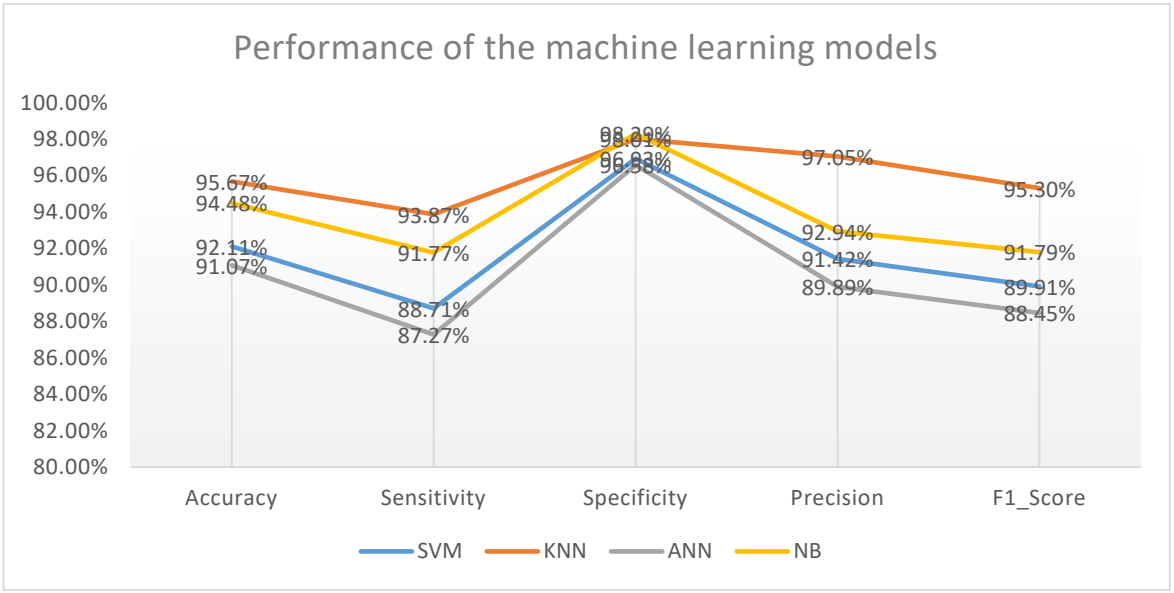


Fig 4: Performance of machine learning models

While processing SDN data, KNN and NB demonstrated superior performance when the success rates were compared after the training that was completed using the KNN algorithm, a curve known as the Receiver Operating Characteristic (ROC) was generated (Figure 5). The ROC curve is a technique for analyzing the test results. It is depicted as a two-dimensional graph with the True Positive (TP) axis on the vertical and the False Positive (FP) axis on the horizontal. The notation TP denotes positive occurrences appropriately classified as positive outputs, whereas the notation FP denotes negative cases incorrectly classified as positive outputs. False Negative

(FN)", which highlights positive cases incorrectly identified as negative output, is another statistic utilized in confusion matrices. In the ROC curve, it was found that the TP value was more significant than 0.9%.

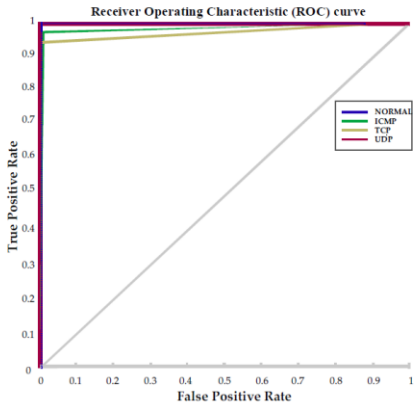


Fig 5: The normal, ICMP, TCP and UDP ROC curves for KNN without future selection

After analyzing the performance results, it was found that the KNN classifier performed better at evaluating the attack data. This was the conclusion reached after examining the performance. The KNN classifier, when used in conjunction with the wrapper feature selection approach, yielded the best accuracy rate (98.3%) when the data complied into the machine learning model. This was the case when the KNN classifier was used. Training and testing six different features achieved this accuracy rate. Based on the results of this study, the implementation of feature selection methods resulted in improved performance metrics when training classifiers on a dataset of 12 features. In comparison to the findings from [4,12,13,14,15, 10], the performance of the machine learning model that was proposed together with the feature selection methods was significantly improved. It is important to remember that various datasets and models were utilized in the comparable investigations published in the academic literature.

5. Conclusion:

Machine learning methods were applied to the investigation of SDN-based detection systems that had been built specifically for DDoS attacks. In the initial strategy offered, algorithms with an accuracy of 98.3% were used to analyze flow data to ensure the identification of attacks without distinguishing between different types of traffic. The second solution that has been presented classifies DDoS attacks as either regular traffic or attack traffic. This is one of the systems that has been offered. KNN algorithms have a sensitivity of 97.7%, allowing them to conduct this control while reducing the controller's workload.

References

[1] Sarica, A. K., & Angin, P. (2020). Explainable security in SDN-based IoT networks. *Sensors*, *20*(24), 7326.

[2] Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., ... & Jilani, S. F. (2022). Adaptive machine learning-based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. *Sensors*, *22*(7), 2697.

[3] Jmal, R., Ghabri, W., Guesmi, R., Alshammari, B. M., Alshammari, A. S., & Alsaif, H. (2023). Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks. *Applied Sciences*, *13*(8), 4953.

[4] Latah, M., & Toker, L. (2018). A novel intelligent approach for detecting DoS flooding attacks in software-defined networks. *International Journal of Advances in Intelligent Informatics*.

[5] Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability*, *12*(3), 1035.

[6] Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, *122*, 149-171.

[7] Arevalo Herrera, J., & Camargo, J. E. (2019). A survey on machine learning applications for software-defined network security. In *Applied Cryptography and Network Security Workshops: ACNS 2019 Satellite Workshops, SiMLA, Cloud S&P, AIBlock, and AIoTS, Bogota, Colombia, June 5–7, 2019, Proceedings 17* (pp. 70-93). Springer International Publishing.

[8] Vimal, V., Muruganantham, R., Prabha, R., Arularasan, A. N., Nandal, P., Chanthirasekaran, K., & Reddy Ranabothu, G. (2022). Enhance Software-Defined Network Security with IoT to Strengthen the Encryption of Information Access Control*: Computational Intelligence and Neuroscience*, *2022*.

[9] Uribe, J. D. J. R., Guillen, E. P., & Cardoso, L. S. (2022). A technical review of wireless security for

the internet of things: Software defined radio perspective. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 4122-4134.

[10] Cai, T., Jia, T., Adepu, S., Li, Y., & Yang, Z. (2023). ADAM: an adaptive DDoS attack mitigation scheme in software-defined cyber-physical system. *IEEE Transactions on Industrial Informatics*.

[11] Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023). FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks. *IEEE Access*, *11*, 28934-28954.

[12] Ye, J., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). A DDoS attack detection method based on SVM in software-defined network. *Security and Communication Networks*, *2018*.

[13] Chakraborty, S., & Banerjee, S. (2018). Proposed approach to detect distributed denial of service attacks in software defined network using machine learning algorithms. *Int. J. Eng. Technol*, *7*, 472-476.

[14] Sahoo, K. S., Tripathy, B. K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An evolutionary SVM model for DDOS attack detection in software-defined networks. *IEEE access*, *8*, 132502-132513.

[15] Swami, R., Dave, M., & Ranga, V. (2019). Software-defined networking-based DDoS defense mechanisms. *ACM Computing Surveys (CSUR)*, *52*(2), 1-36.

[16] ONOS SDN Controller https://opennetworking.org/onos/