e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

Detecting DDoS Attacks in Software-Defined Network Controllers using Machine Learning.

Aishwarya M S [1], Suraj M Tariwal [2], Vidyashree N T [3], Vidyasree N M [4]

Prof. Vishwanath V K [5], Prof. Shryavani K [6]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[1]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[2]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[3]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[4]

Assistant Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering andTechnology, Davangere, Karnataka, India[5]

Assistant Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[6]

ABSTRACT: The term Software-Defined Network (SDN) is a network model that enables the detection of fraudulent traffic and the detection of unique potential failures. It is also the land of various security threats that lead to complete disruption of this network. To mitigate such attacks, this article relies on machine learning techniques to facilitate rapid detection of these attacks and reviews methods of detecting DDoS attacks and selects the most accurate for classification of this type in SDN, and shows results. It has been determined that the proposed system gives better results in detecting DDOS attacks in SDN networks and the accuracy of the decision tree (DT) algorithm is 99.90%.

KEYWORDS: DDOS attacks, Feature selection, Logistic regression, Machine learning, Software, defined networking.

I. INTRODUCTION

Software Defined Networking (SDN) defines software by separating the control level from the data level SDN networking is a model [1] that helps to solve traditional network design's limitations. It has three main levels: private level, data plane device, control level, and application level. The data plane carries traffic on the network according to the controller's preferences. To determine the flow, it calculates the control plane routing table [2]. SDN networks, along with other application processes such as load balancing, firewalls, and quality services [3], help improve the performance of the control room and their effectiveness in the network from the separation of the message generator [4]. A management application running with a management policy will manage multiple routers in the network [5]. Applications can only access processed network data over SDN. Load balancing and intrusion detection are easier when multiple applications are integrated [6]. When an error is detected, the application tells the controller to re-enter flight data [7]. These network devices have special open interfaces controlled by software to control and control the data flow between routers scattered in the network [8].

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

Multiple devices can be reconfigured simultaneously in an SDN architecture. Configuration of network devices is done in this layer using the application process [9].

II. RELATED WORK

The control plane of the DDoS-SDN architecture. DDoS attacks have a significant impact on SDN uptime. DDoS attacks have the greatest impact on SDN controllers as they are the most vulnerable. When it comes to SDN, there is only one thing that doesn't work: central control. Flight data and flight control use a secure southbound connection to exchange messages. Even a small amount of channel congestion can cause significant network delays. Mel et al. [11] In a tree-network architecture, they use a mini-network emulator to perform a DDoS attack on the controller. Using Support Vector Machines (SVM), a machine learning technique, they identified DDoS attacks by running the flow on switches and evaluated the physical attack patterns of DDoS attacks when detected. Using our detection tools, we were able to reduce the impact of DDoS attacks on Ryu controllers by 36%.Rahman et al. [12] detected and blocked DDoS attacks on SDN networks using various machine learning algorithms, including J48, RF, SVM, and K-NN. The models learned and selected during the evaluation are planned to be the best for the network, relying on all scripts that help reduce, prevent, and mitigate attacks and their impact on SDN networks. The findings show that J48 outperforms other algorithms, especially in terms of the time required for training and test cases. Sun et al. [13] proposed a method for SDN controllers to detect DDoS attacks in real-time. Entropy is first used after suspicious notifications are given, and DDoS attack features in the SDN environment are learned and important features related to attacks are extracted. Retrieves the stream input for the open stream switch. Distribute traffic in real-time to detect DDoS attacks using the ANN method called BILSTM-RNN. Compared to other methods, this method can better detect DDoS attacks and reduce controller load in the SDN environment. Dehkordi et al. [14] proposed a unique method to detect DDoS attacks on SDN. The three-person summation system is entropy-based and distribution-based. The outputs of UNB-ISCX and ISOT data show that the proposed method is competitive in detecting DDoS threats.

Chen et al. [15] presented machine learning-based multi-layer IoT DDoS attack detection, including IoT devices, gateways, SDN switches, and cloud servers. As a first step, they installed eight smart cameras at the school that collects data from every frame via a wired or wireless network. Then they delete the signature as a kind of DDoS attack. In our tests, the system can be used to detect DDoS attacks. Additionally, the SDN checker can block malicious devices by using the blacklist of IoT DDoS attacks to detect the system. Sen et al. [16] Ada Boosting is used as a base classifier with decision logs of a private network dataset in an SDN environment. The model offers an accuracy of 93% and a low negative value. They share their findings after evaluating the performance of the model and comparing it to several machine learnings. path. Tan et al [17] SDN DDoS environments use this technique for detection and attack. First, they use data plane detection of DDoS events to monitor the network for unexpected traffic. They identify traffic anomalies based on detection using machine learning based on K-Means and K-Nearest Neighbor (KNN) algorithms and rely on the rate-asymmetric nature of traffic. Finally, the controller will respond to the attack using appropriate countermeasures. The new control plane and data plane collaboration detection technology systems successfully increase detection accuracy and efficiency while protecting against SDN threats. Ahmed et al. [18] SDN DoS and DDoS attacks can be mitigated using machine learning. Relying on security detection based on machine learning algorithms has a significant impact on the future of communications, and this process is judged by the extent to which controllers and DDOS are affected. The accuracy of DVM was determined as 97.5%. The presentation is as follows: 1. Introduction, 2. Plan, 3. Methods, 4. Results and discussion, 5.In conclusion

III. METHODOLOGY

The model used is based on LR, NB, and DT machine learning algorithms and the main steps are shown in Figure 1. The matching strategy is based on competing requests from nodes in real time compared to data collected from training behavior. (SDN custom data created using a mini network simulator and used in car classification for machine learning). It compares the location, IP address, and MAC address and if the incoming request has the corresponding authorization, it waits for the transaction and is classified as
usual. In addition, the training model can be classified as a competitor if the information data is already inconsistent with the behavior set in the first step.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

.

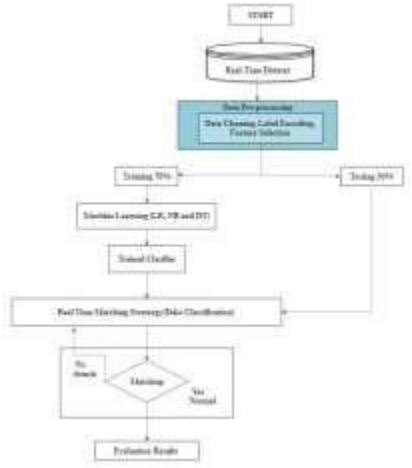


Figure 1: the proposed machine learning system model

The proposed system is used online to directly test and evaluate incoming requests after different comparisons as DDOS traffic or normal data. The results are calculated by three machine learning algorithms namelylogistic regression (LR) algorithm, pure Bayes (NB) algorithm, and decision tree (DT) algorithm. The proposed algorithm generates implicit or explicit patterns from given data to create machines that can learn from data without programming, helping to find and better understand hidden patterns. Figure 2

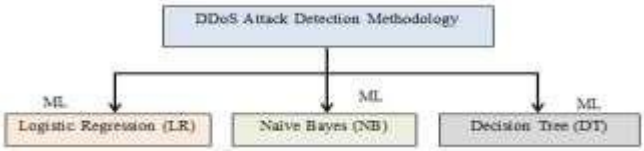


Figure 2. The used machine learning algorithms

Initial work is to develop a logistic regression (LR) based model for detecting DDoS attacks from a training and test SDN environment, by providing a distribution model to prove the outcome of transaction X with Y feature vectors. It is done using methods to find the relationship between classes and vectors. He assumed that the distribution P(YX), where Y is the class and X is the symbol vector, is borderline, and he proved this from the data. Table 3 shows the accuracy and time details of DDoS attack detection on the LR-based SDN controller, and the confusion matrix evaluation is negative cost and not negative cost. In addition, there are other test results in Table 4, Figure 1. 3 the proposed method based on the LR classifier

Table 2. The results of LR algorithm for DDoS attack detection case study

Method Name	Accuracy	False Positive Rate	False Negative Rate	Time
Logistic Regression (LR)	72.65%	0	71511	7.844 sec

Table 3. Evaluation Details of the DDoS attack detection with LR

Evaluation Parameters	*Machine Learning Algorithms Logistic Regression (LR)*
Precision	1.0
Recall	0.35
F-Measure	0.52
Accuracy	0.5288

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

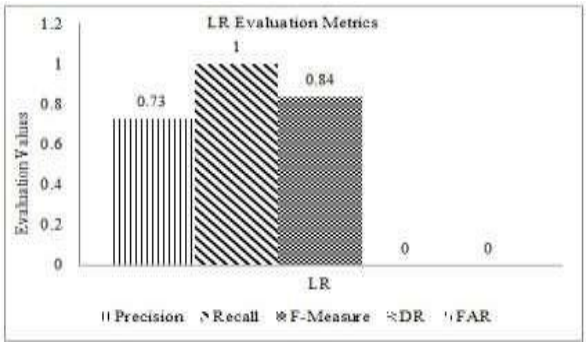


Figure 3. Precision, recall, and F-measure of LR case study

The second study is based on the Naive Bayes (NB) algorithm as a method for the Naive Bayes classifier basedon So. – so-called Bayesian classification of traffic according to normal and abnormal DDoS attacks in SDN. Despite its simplicity, it can give output more complex classification methods. A valid classifier model can be defined as a machine learning model to distinguish various objects based on certain properties. In machine learning, the probabilistic Naive Bayes model is used for task classification. Table 5 shows the NB metricsused in DDoS attack detection. In addition, there are other criteria shown in Table 6. NB classifier-based system is proposed in Figure 4.

Table 4. The results of NB algorithm for DDoS attack detection case study

Method Name	Accuracy	False Positive Rate	False Negative Rate	Time
Naïve Bayes(NB)	52.88%	123371	0	1.910 sec

Table 5. Evaluation details of the DDoS attack detection with NB

Evaluation Parameters	Machine Learning Algorithms Naive Bayes (NB)
Precision	0.73
Recall	1.0
F-Measure	0.84
Accuracy	0.7265

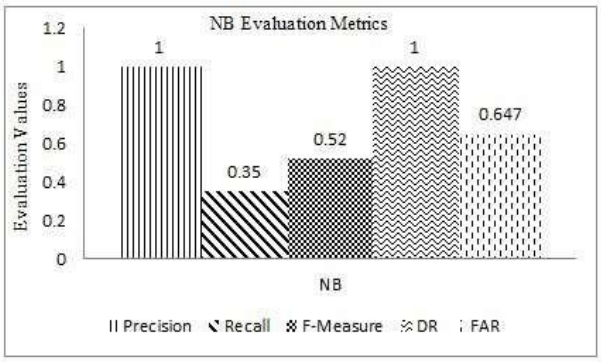


Figure 4. Precision, recall, and F-measure of NB case study

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

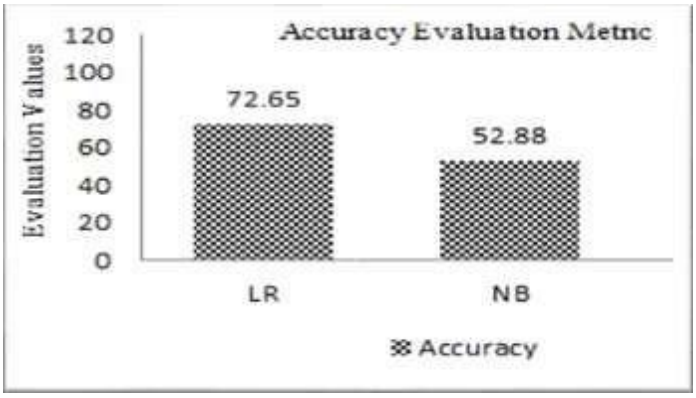


Figure 6. The proposed system accuracy comparison

Figure 9 and Figure 6 show a comparison of suggested machine-learning methods. In addition, the proposedsystem in Table 10 is compared with the related projects. In addition, in Table 10, the system is compared with other related projects. In the case of DT, the correct result of the request for all studies is 99.90%.

Evaluation Parameters	Naive Bayes	Logistic regression	Hybrid model Result
Precision	0.73	1.0	0.999451453647
Recall	1.0	0.35	0.999451453647
F-Measure	0.84	0.52	0.999451453647
Accuracy	0.7265	0.5288	0.999451453647

Table 8. Evaluation details of the used machine learning in DDoS attack detection in SDN e

Table 9. The results of the proposal were compared to SDN's DDoS attacks system

.

Ref. No	Year	Dataset	Method Name	Accuracy
[20]	2021	Real-Time dataset using RYU API-Mininet	Support-Vector-classifier with Random-Forest (SVC-RF) Logistic Regression (LR)	98.8 % 83.69%
[22]	2021	KDD99 dataset	Decision Tree (DT) Support vector machine (SVM)	78 % 85 %
[23]	2021	CICIDS2017 dataset KDD dataset UNSW-NB15 dataset	V-NKDE (Voting -Naive Bayes, K Nearest Neighbours, Decision Tree, and Extra Trees)	99.67 % 99.77 98.09
Proposed system		Real-Time DDoS Attack Classification	Logistic Regression (LR) Naive Bayes (NB)	72.65 % 52.88 %
			Decision Tree (DT)	99.90 %

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

IV. EXPERIMENTAL RESULTS

Logistic Regression Model

```
from sklearn.linear_model import LogisticRegression
Logistic_Regression_model = LogisticRegression(random_state = 0)
Logistic_Regression_model.fit(X,y)
print("Model has been trained.")
```

```
Model has been trained.
```

Naïve Bayes Model

```
NBmodel = GaussianNB()
NB_model = NBmodel.fit(X,y)
print("Model has been trained.")
```

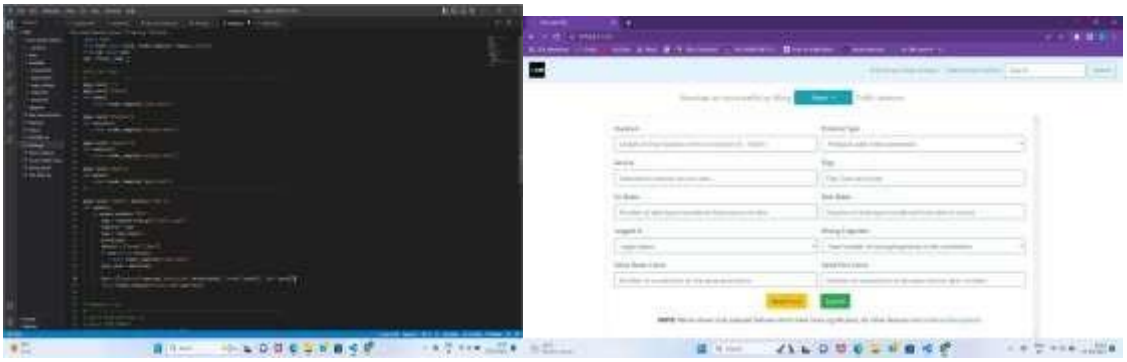
```
Model has been trained.
```

Decision Tree Model

```
dtreemodel = DecisionTreeClassifier()
dtree_model = dtreemodel.fit(X, y)
print("Model has been trained.")
```

```
Model has been trained.
```

Fig. (a) This figure shows Flask Integration using Visual Studio. (b) Prediction Page of UI. (c) Enter the details in Predition Page (e) Preliminary Data Analysis of provided Data. on In SDN Controller Using Machine Learning Techniques

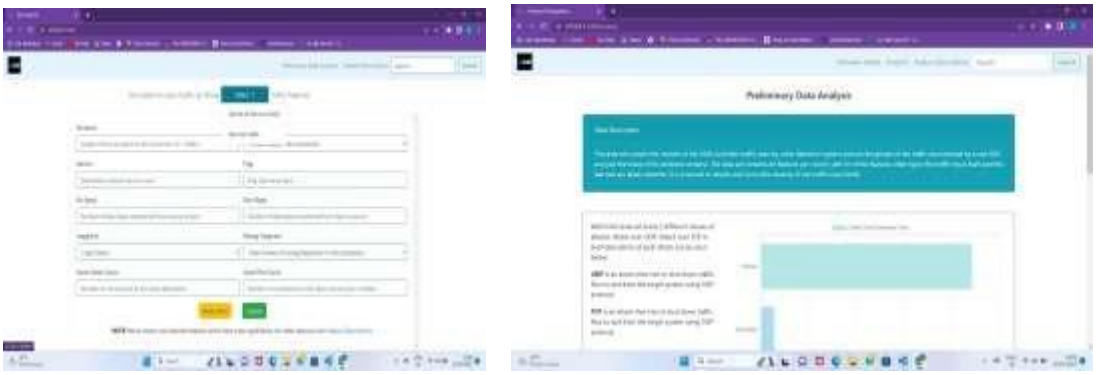


(a) (b)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

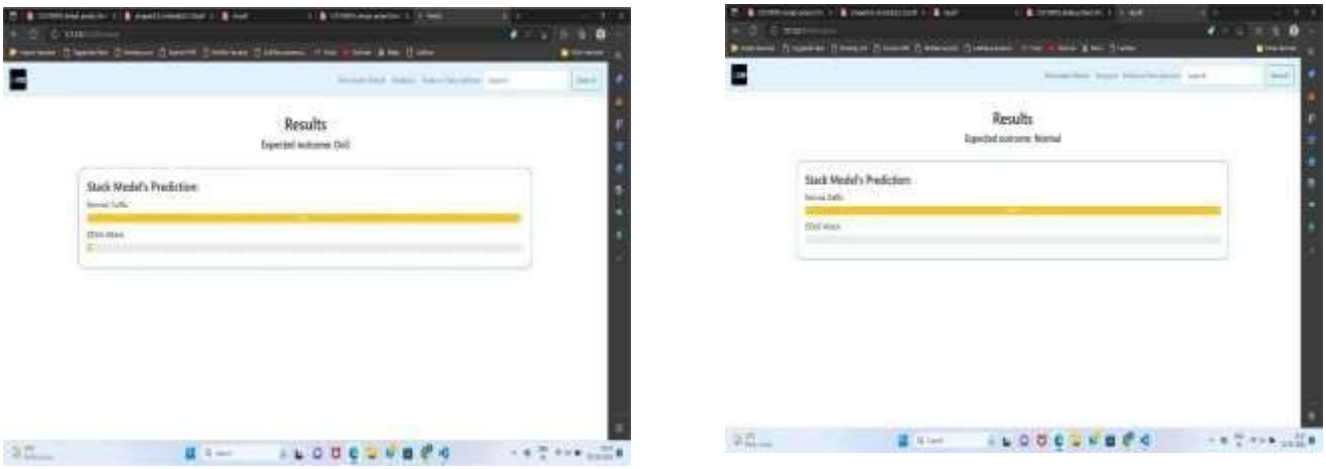
| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |



(a) (d)

Fig. 2 (a) Result Page of UI. (b) Result page of UI.



(a) **(b)**

VI. CONCLUSION

The impact of DDoS is one of the biggest disruptions in the network and if not managed properly it can cause a complete downtime as these attacks become more frequent and can easily bypass many traditional defenses. Machine learning techniques have been applied in SDN to solve cybersecurity issues. DT, NB, and LR algorithms are used to create implicitor explicit patterns from data to create systems that can learn from data without programming, helping to find and better see hidden patterns. Machine learning can also be relied upon to optimize the features of this network, which helps reduce the number of attacks caused by DDoS attacks. Compared to other algorithms, the best machine learning algorithm is DT with 99.90% accuracy. Future work will include developing mitigations for attack detection in this research. Designing a mitigation plan that is both efficient and effective requires addressing many questions, including how to improve the programmability of SDN to shut off all traffic, such as placing special blocks on keyboards. These problems include how to make the best use of management and transfer resources to use mitigation strategies, how to reduce the response time ofthe mitigator, how to reach a solution, etc. includes.

REFERENCES

[1] A. Nayyer, A. K. Sharma, and L. K. Awasthi, "Learning-based hybrid routing for scalability in software-defined networks," *Computer Networks*, vol. 198, p. 108362, Oct. 2021, doi: 10.1016/j.comnet.2021.108362.

[2] A. Hodaei and S. Babaie, "A survey on traffic management in software-defined networks: challenges, effective approaches, and potential measures," *Wireless Personal Communications*, vol. 118, no. 2, pp. 1507–1534, May 2021, doi: 10.1007/s11277-02108100-3.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604027 |

[3] S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber-physical systems," *Computer Communications*, vol. 181, pp. 274–283, Jan. 2022, doi: 10.1016/j.comcom.2021.09.029.

[4] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "An efficient packet parser architecture for software-defined 5G networks," *Physical Communication*, vol. 53, p. 101677, Aug. 2022, doi: 10.1016/j.phycom.2022.101677.

[5] N. M. AbdelAzim, S. F. Fahmy, M. A. Sobh, and A. M. Bahaa Eldin, "A hybrid entropy-based DoS attacks detection system for software-defined networks (SDN): A proposed trust mechanism," *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 85–90, Mar. 2021, doi: 10.1016/j.eij.2020.04.005.

[6] S. Bhardwaj and S. N. Panda, "Performance evaluation using RYU SDN controller in software-defined networking environment," *Wireless Personal Communications*, vol. 122, no. 1, pp. 701–723, Jan. 2022, doi: 10.1007/s11277-021-08920-3.

[7] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges, and future directions,"
Computer Science Review, vol. 37, p. 100279, Aug. 2020, doi: 10.1016/j.cosrev.2020.100279.

[8] A. Saritha, B. R. Reddy, and A. S. Babu, "QEMDD: quantum inspired ensemble model to detect and mitigate DDoS attacks at various layers of SDN architecture," *Wireless Personal Communications*, Aug. 2021, doi: 10.1007/s11277-021-08805-5.

[9] S. Mahrach And A. Haqiq, "DDoS flooding attack mitigation in software-defined networks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, 2020, doi: 10.14569/IJACSA.2020.0110185.

[10] M. Abdurohman, D. Prasetiawan, and F. A. Yulianto, "Improving distributed denial of service (DDOS) detection using entropy method in a software-defined network (SDN)," *ComTech: Computer, Mathematics, and Engineering Applications*, vol. 8, no. 4, p. 215, Dec. 2017, doi: 10.21512/com tech.v8i4.3902.

[11] S. Y. Mehr and B. Ramamurthy, "An SVM-based DDoS attack detection method for Ryu SDN controller," in *Proceedings of the 15th International Conference on Emerging Networking EXperiments and Technologies*, Dec. 2019, pp. 72–73. doi 10.1145/3360468.3368183.

[12] O. Rahman, M. A. G. Quraishi, and C.-H. Lung, "DDoS attacks detection and mitigation in SDN using machine learning," in *2019 IEEE World Congress on Services (SERVICES)*, Jul. 2019, pp. 184–189. doi 10.1109/SERVICES.2019.00051.

[13] W. Sun, Y. Li, and S. Guan, "An improved method of DDoS attack detection for the controller of SDN," in *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)*, Aug. 2019, pp. 249–253. doi: 10.1109/CCET48361.2019.8989356.

[14] A. Banitalebi, Soltanaghaei,& Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *The Journal of Supercomputing*, vol. 77, no. 3, pp. 2383–2415, Mar. 2021, doi: 10.1007/s11227-02003323-w.

[15] Y.-W. Chen, J.-P. Sheu, Y.-C. Kuo, and N. Van Cuong, "Design and implementation of IoT DDoS attacks detection system based on machine learning," in *2020 European Conference on Networks and Communications (EuCNC)*, Jun. 2020, pp. 122–127. doi: 10.1109/EuCNC48522.2020.9200909.

[16] S. Sen, K. D. Gupta, and M. Manjurul Ahsan, "Leveraging machine learning approach to setup software-defined network(SDN) controller rules during DDoS attack," 2020, pp. 49–60. doi 10.1007/978-981-13-7564-4_5.

[17] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A new framework for DDoS attack detection and defense in SDN environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020, doi: 10.1109/ACCESS.2020.3021435.

[18] A. Ahmad, E. Harjula, M. Ylianttila, and I. Ahmad, "Evaluation of machine learning techniques for security in SDN," in *2020 IEEE Globecom Workshops (GC Wkshps*, Dec. 2020, pp. 1–6. doi 10.1109/GCWkshps50303.2020.9367477.

[19] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DLSDN: deep learning for DDOS attack detection in software-defined networking," in *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Jan. 2021, pp. 683–688. doi 10.1109/Confluence51648.2021.9376879.

[20] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software-defined networking," *Journal of Network and Computer Applications*, vol. 187, p. 103108, Aug. 2021, doi: 10.1016/j.jnca.2021.103108.

[21] N. M. YungaicelaNaula, C.Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," *IEEE Access*, vol. 9, pp. 108495–108512, 2021, doi:

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com