DDoS Detection in Software-Defined Network (SDN) Using Machine Learning

Conference Paper · August 2023

DOI: 10.5121/ijci.2023.120408

4 authors, including:

Haya Alubaidan
Imam Abdul Rahman bin Faisal University
6 PUBLICATIONS **21** CITATIONS

SEE PROFILE

DDOS DETECTION IN SOFTWARE-DEFINED NETWORK (SDN) USING MACHINE LEARNING

Haya Alubaidan, Reem Alzaher, Maryam AlQhatani, Rami Mohammed

College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Saudi Arabia

ABSTRACT

In recent years, the concept of cloud computing and the software-defined network (SDN) have spread widely. The services provided by many sectors such as medicine, education, banking, and transportation are being replaced gradually with cloud-based applications. Consequently, the availability of these services is critical. However, the cloud infrastructure and services are vulnerable to attackers who aim to breach its availability. One of the major threats to any system availability is a Denial-of-Service (DoS) attack, which is intended to deny the legitimate user from accessing cloud resources. The Distributed Denial-of-Service attack (DDoS) is a type of DoS attack which is considerably more effective and dangerous. A lot of efforts have been made by the research community to detect DDoS attacks, however, there is still a need for further efforts in this germane field. In this paper, machine learning techniques are utilized to build a model that can detect DDoS attacks in Software-Defined Networks (SDN). The used ML algorithms have shown high performance in the earliest studies; hence they have been used in this study along with feature selection technique. Therefore, our model utilized these algorithms to detect DDoS attacks in network traffic. The outcome of this experiment shows the impact of feature selection in improving the model performance. Eventually, The Random Forest classifier has achieved the highest accuracy of 0.99 in detecting DDoS attack.

KEYWORDS

Cloud Computing; Distributed Denial of Service (DDoS); Software-Defined Network (SDN); Machine Learning.

1. INTRODUCTION

In the age of the Internet - the age of information technology - the amount of data and information available on the Internet increases dramatically, and files accumulate inside public and private computers. Therefore, a large segment of society needs to have this information in a system that allows to be accessed and viewed at any time. Cloud computing has been a popular topic for many years. It is one of the most interesting and fastest-growing areas in the field of computer science. The reason that it is so popular is because provides a broad network access and it offers an easy way to do computing without having to buy and maintain expensive hardware. One application of the cloud computing is the Software-Defined Network (SDN). It is a programmable network architecture that enables both dynamic and programmatic control of the network; It is centrally controlled by the so-called Network Controller (SDN Controller). So, it is mainly based on the separation of the two main pillars of the network: control and command execution [1].

As more people use cloud computing and SDN technologies, security becomes a more pressing issue. The current challenges and issues associated with cloud computing security. These issues are divided into four categories: architectural issues, service delivery model issues, cloud

Dhinaharan Nagamalai (Eds): EDU, SCMC, COMSCI -2023
pp. 93-104, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120408

characteristic issues, and cloud stakeholder issues. Security costs a lot of money (security solution licensing), takes a lot of resources (security is a resource-intensive operation), and is a difficult problem to conquer, according to cloud providers. But skipping security from the cloud computing model roadmap will violate the expected revenues [2].

Despite the widespread use of cloud computing and SDN technologies, its security is threatened by attackers. Nowadays, distributed denial of service (DDoS) is one of the most dangerous attacks aimed at breaching network availability. As stated by Penttinen [3], "A distributed denial of service attack is a DoS attack, in which multiple hosts perform DoS attacks in a coordinated fashion to one or more targets". The definition emphasizes three main characteristics that distinguish a DDoS attack from other types of attack. First, a DDoS attack is basically a DoS attack. In other words, it is a subset of DoS attacks. Second, the attack comes from multiple sources. Third, the attacking hosts must have coordination among themselves, which is the essential feature of a DDoS attack.

DDoS can target both the cloud and the SDN by affecting specific components of its architecture. SDN is a combination of application, control, and information levels. Based on this, DDoS in SDNs is categorized into three categories in each of them targeting a specific level of SDN. On the other hand, DDoS in the cloud has a significant impact on realizing the basic characteristics of the cloud, such as resource pooling, wide network access and on-demand self-service, because it aims to penetrate the availability of the cloud [4].

In this paper, an intrusion detection technique is build using machine learning to detect the DDoS attack in the SDN environment. The model is trained and tested using a SDN dataset which has been used previously for research purposes. However, we have utilized different supervised classifiers to identify the traffic packets that indicate potential DDoS attack. These classifiers are SVM, Logistic Regression, KNN, Random Forest and LSTM. Moreover, we have shown the effect that feature selection has on improving the model performance. In conclusion, an outstanding result have been achieved with an accuracy of 99% for random forest classifier.

This work is organized as follows. Section 2 contains a review of earlier literatures. Section 3 contains the proposed machine learning methods, which are Logistic Regression, SVM, KNN, Random Forest and LSTM. Section 4 contains empirical studies that include dataset description and experimental setup. Section 5 presents results and discussion while section 6 contains the conclusion and recommendation emanating from this work.

2. REVIEW OF RELATED LITERATURES

There has been extensive research on Distributed Denial of (service DDoS) and Software defined Networking (SDN) attacks in cloud computing. In this section, we show some of pervious work in literature that are directly related to our work.

Authors in [5] used Software Defined networking (SDN) -base cloud concept to defence of DDoS attacks on the cloud computing environment. Also, they showed many feathers and discussed many challenges in SDN-based cloud to increase the chances on protection from DDoS attacks. Because the SDN-cloud base still new and attention for both academia and industry they tried to address the gap by showed comprehensive survey on previous work by others and they considered the existing methods in three different class by introduced a detailed comparison.

In addition, Authors in [6] discussed and analyzing the merits and vulnerabilities for SDN in the cloud environment. in their study they proposed the new method can detect DDoS attacks in SDN-based Cloud by using one of the features of SDN. They utilized Mininet tool (an open-

source network emulator tool) to create virtual network switches and hosts. They implement their proposed method using POX. POX is an open-source development environment for OpenFlow SDN controllers based on Python. they used OpenFlow 1.0 to build their recommended technique as an application on a controller. As an outcome of their study, they were able to identify DDoS attacks with little communication and processing overhead.

On other hand, Authors in [7] have shown the correlation between different feature selection filters and classification algorithms during DDoS attacks, thus, achieving a high detection accuracy in minimal time. Four filters have been utilized to find the 14 optimum features among 41 features. After that, the dataset is classified using different machine learning algorithms. As result, J48 algorithm with a chi-squared filter have obtained the highest correlation.

Moreover, Authors in [8] proposed a machine learning model to accurately detect whether the network traffic is normal, or it indicates a potential DDoS attack. The system has utilized decision tree (C.4.5) algorithm along with signature detection techniques to build a robust and high accurate system. Decision tree (C.4.5) algorithm was compared with other machine learning algorithms such as Naïve Bayesian and k-means. however, Decision tree (C.4.5) outperformed other algorithms and it was able to detect DDoS attacks with an accuracy of 98.8% in less time.

Also, Authors in [9] proposed a method to detect a DDoS attack using machine learning based on Artificial Neural Networks (ANN) with black hole optimization algorithms. Their method analysis network traffic across the router both the cloud server and detection solution connected to this router. The detection solution is consisted of three components: training database, Pre-processor, and classifier. This experiment was performed in MATLAB. Moreover, the dataset used for training and testing it performed ten times to measure the accuracy of detection the top accuracy detection achieved was 96.30%.

Moving from Decision tree algorithms and Artificial Neural Networks (ANN) to Support Vector Machine (SVM) authors in [10] performed SVM based DDoS detection in SDN. Here the controller collects the flow status information of network traffic on the switch. Then used the support vector machine method to evaluate the traffic and detect DDoS attacks after extracting the six-tuple characteristic values associated to DDoS attacks. It focused on the analysis of changes in traffic characteristic values and used the SDN experimental environment to validate the method's practicality. The experiment's detection accuracy rate is high, while the false alarm rate is low, generating the expected results.

More Authors in [11] worked on experiment to detection of DDoS attacks on cloud computing using three different machine learning algorithms: Support Vector Machine (SVM), Naïve Bayes (NB) and Random Forest (RF). This experiment was held on open-source platform called own cloud. Moreover, they used secure tool to simulate DDoS attack as result for their experiment SVM was achieved very high accuracy 99.7% also better in recall, precision, specificity. On another hand RF and NB had closely result.

As part of test more different algorithms authors in [12] used a voting mechanism based on a fast KNN binary classifier (K-FKNN) and pre-processing using "K-means++." and the modular detection system is shown in the controller. Several tests are carried out to evaluate the system's performance. The findings indicate that K-FKNN increases KNN detection accuracy and efficiency and has great precision and stability in DDoS detection in SDN.

Moreover, authors in [13] worked to improved KNN by follow a novel concept called the degree of attack is created to detect DDoS. After that, a detection algorithm called DDADA is built based on this concept, as well as a machine learning algorithm called DDAML to effectively

identify DDoS. The performance of DDADA and DDAML were compared with existing solutions, and they achieved a higher detection rate with an accuracy of 0.89 for DDADA and 0.91 for DDAML.

In addition, authors in [14] have created a framework based on machine learning algorithms to detect and defend against DDoS attacks in a software-defined network (SDN). Two modules have been created, the first one uses K-means for selecting the features and the second module uses KNN algorithms for detecting DDoS attacks. The proposed framework has shown an accuracy of 98.85% compared to existing methods.

More and more authors in [15] used a Support Vector Machine (SVM) in concert with a kernel principal component analysis (KPCA) and a genetic approach to improve detection accuracy (GA). KPCA is used to reduce the dimension of feature vectors in the proposed SVM model, while GA is utilized to optimize different SVM parameters. An improved kernel function (N-RBF) is presented to decrease the noise generated by feature variations. The experimental findings suggest that the proposed model achieves more accurate classification and better generalization than single-SVM. Furthermore, the proposed model can be implemented within the controller to build security rules that will restrict attackers from launching assaults.

Also, Authors in [16] analysed features that were extracted from the SDN traffics dataset, with the goal of reducing bias data from the dataset. The 10-fold cross-validation approach was used to test the SDNTraffficsDS traffic features dataset. It splitted each group in this validation and calculated the evaluation score, precision, recall, and F1-score for each. By comparing this dataset to other datasets, such as the KDDCUP 99 dataset, this study was able to verify its efficacy. So, this suggested dataset can be utilized to train SVM on SDN successfully. Other authors in [17] applied common machine learning (ML) methods to explore machine learning-based detection and classification of Distributed Denial of Service (DDoS) flooding attacks on (Software Defined Networks) SDNs. Quadratic discriminant analysis (QDA), Gaussian Nave Bayes (GNB), K-Nearest Neighbour (k-NN), and classification and regression tree are the ML algorithms, classifiers, and methodologies researched (CART). Experimental data (i.e. jitter, throughput, and reaction time metrics) from a sample SDN architecture suited for typical mid-sized enterprise-wide networks is utilized to create classification models that properly identify and categorize DDoS flooding attacks, as shown in a case study. The DDoS flooding attacks (i.e. hypertext transfer protocol (HTTP), transmission control protocol (TCP), and user datagram protocol (UDP) assaults) were launched on Mininet using the SDN paradigm.

Therefore, Authors in [18] proposed a model using OMNET++ Simulation tool to detect DDoS on the cloud computing environment. The proposed model discarding and detection of malicious requests by utilizing the clustering and packet score methods. In their proposed model they assig the source of all incoming packet then they calculated and compared this source with pre-defined threshold value at the end the malicious packet's source IP address is blacklisted their proposed model follows reactive approach to start flittering the DDoS attack from the beginning to decrease damage. In order that, Authors in [19] evaluated various features selection techniques and machine learning classifiers that give the most accurate and effective results for detecting DDoS. The experimental result of this study shows that the best accuracy of 99.97% is gained by using Recursive Feature Elimination (RFE) with Random Forest (RM) algorithm.

In [20], The proposed approach is composed of two modules. The first module collects the flow and port statistics to create the dataset and the second module applies a machine-learning algorithm to classify the traffic. Authors have contributed by identification of novel features for DDoS attack detections. Novel features are logged into CSV file to create the dataset and machine learning algorithms are trained on the created SDN dataset. They have used various

machine learning techniques to detect the DDoS attack on the novel dataset. The used machine learning algorithms are ANN, Logistic Regression, K-nearest neighbor, SVM, Ensemble, Random Forest, and hybrid classifier. The hybrid classifier combines a Support-Vector-classifier and a Random-Forest classifier. This classifier has achieved the highest accuracy of 98.8% and outperform other.

After reviewing many papers that discussed different techniques in detecting DDoS attack, the most used algorithms in the early studies are SVM, Random Forest (RF), Logistic Regression and K-Nearest Neighbor (KNN), thus, they have been used in our paper. Moreover, there is a noticeable absence in utilizing the deep learning techniques in detecting DDoS attack, so we have utilized Long-Short Term Memory (LSTM) network. Therefore, in our proposed model, we have applied SVM, RF, LR, KNN and Long-Short Term Memory (LSTM). In our paper, we have used the novel dataset created by [20]in detecting DDoS attack and we have shown the impact of feature selection in the model performance.

Table 1: Literature Review Summary

Reference	**Used ML algorithms**	**Algorithm with highest accuracy**
Osanaiya et. al [3]	- J48 - Random Forest (RF) - One R - Decision Tree (DT) - Bayes Net - Naïve Bayes (NB)	J48
Zekri et. al [4]	- C4.5 - K-Means - Naïve Bayes (NB)	C4.5
Kushwah et. Al [5]	- Artificial Neural Networks (ANN)	-
Ye et. al [6]	- Support Vector Machines (SVM)	-
Wani et. al [7]	- Support Vector Machines (SVM) - Naïve Bayes (NB) - Random Forest (RF)	SVM
Xu et. al [8]	- K-FKNN (based on K-means++and Fast K-Nearest Neighbors)	-
Dong et. al [9]	- Naïve Bayes (NB) - K-Nearest Neighbors (KNN) - Support Vector Machines (SVM) - CIC-SVM - DDADA - DDAML	DDAML
Tan et. al [10]	- K-Nearest Neighbors (KNN)	-
Sahoo et. al [11]	- Support Vector Machines (SVM)	-
Oo et. al [12]	- Support Vector Machines (SVM)	-
Sangodoyin et. al [13]	- Classification and regression Tree (CART) - Quadratic discriminant analysis (QDA) - Gaussian Naive Bayes (GNB) - K-Nearest Neighbors (KNN)	CART
Gaurav et. al [14]	- OMNET++ (Cluster Entropy and Packet Store)	-
Nadeem et. al [15]	- Naïve Bayes (NB) - K-Nearest Neighbors (KNN) - Support Vector Machines (SVM)	RF

	- Random Forest (RF) - Decision Tree (DT)	
Ahuja at el. [20]	- Artiftcal Neural Network (ANN) - Logisitc Regression (LR) - Support Vector Machine (SVM) - Random Forest (RF) - K-Nearest Neighbors (KNN) - Ensemble - Hybrid Classifier (SVC-RF)	Hybrid Classifier (SVC-RF)

3. DESCRIPTION OF THE PROPOSED TECHNIQUES

3.1. Logistic Regression

It is a machine learning algorithm that is utilized when objects need to be split into two categories, such as "negative" and "positive." In this situation, the hypothesis function necessitates the fulfillment of the requirement 0 <= h(x) <= 1, which is done by the work of a sigmoid (logistic) function (1) [21]

$$h_\theta(x) = \frac{1}{1+e^{-\theta^T x}} \qquad (1)$$

where Θ - a vector of parameters can be expressed also as $h_\theta(x) = g(\Theta^T x)$, where g(z) – a sigmoid function.

3.2. Support Vector Machine (SVM)

The SVM is a statistical learning theory-based learning method. Without a lot of training data, it can give good classification results. It initializes a nonlinearly separable sample set by mapping it to a high-dimensional or even infinite-dimensional feature space and finding the best classification surface in that space. The SVM kernel function successfully addresses the dimensionality disaster produced by high-dimensional mappings and improves the ability to process high-dimensional small sample data [22]

3.3. K-Nearest Neighbors (KNN)

The KNN is an efficient lazy learning algorithm, and it has been successfully developed in many applications. Suppose all the flows as one Euclidean space R^n[23]. We assume the flowX as vector by $< f_1(x), f_2(x),\ldots,f_n(x) >$. Where $f_m(x)$ represents the m-th feature value of the flow X. Now, let us define the distance of the flow X_i and X_j (i.e., $d(X_i,X_j)$) as the following mathematical formula (2):

$$d(x_i, x_j) = \sqrt{\sum_{m=1}^{n}(a_m(x_i) - a_m(x_j))^2} \qquad (2)$$

Suppose that $f(x_p)$ is the final identification result. Then, we define $f(x_p)$ as follows,

$$f(x_p) \leftarrow \arg_{v\epsilon V} max \sum_{i=1}^{k} D(v, f(x_i)) \qquad (3)$$

Where $f(x_i)$ refers to the result value of the flow x_i and v is in the range [0, 1].

For example, if k =4

, $f(x_1) = 0$, $f(x_2) = 1$, $f(x_3) = 1$ and $f(x_4) = 1$, then $f(x_p) = 1$

3.4. Random Forest (RF)

Leo Breiman [24], [25] invented Random Forest (RF), which is one of the most widely used machine learning approaches for classification. The random forest generates a variety of decision trees. Each tree is constructed using a tree classification algorithm and an alternate bootstrap test from the initial data.

3.5. Long Short-Term Memory (LSTM)

Long Short-Term memory (LSTM) algorithms is one of the deep learning algorithms. It is capable of modeling longer term dependencies by having memory cells and gates that govern information flow, as well as memory cells, can be used to model longer-term dependence [25] As represented in fig 1, The contents of the memory cells C_t are regulated by various gates: Forget gate f_t, Input gate i_t, Reset gate r_t, and Output gate o_t. Each gate is composed of affine transformation with Sigmoid activation function

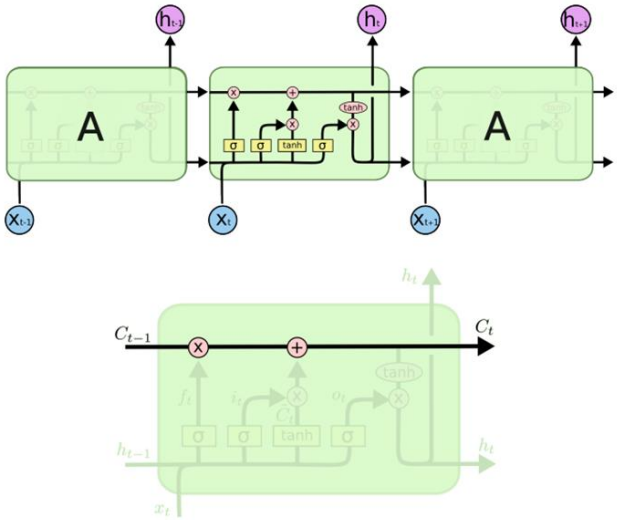

Figure 1. The memory cells

4. EMPIRICAL STUDIES

4.1. Description of Dataset

It is difficult to collect data, especially any data related to attacks and security. This is an SDN-specific dataset created with the Mininet emulator and utilized by machine learning and deep learning algorithms to classify traffic. The dataset contains 1,04,345 rows from Mendeley data [26] The dataset used in this research consists of 23 attributes. Where one of these attributes is called “label” is the target attribute that indicates the status of traffic type either is begin or malicious. Begin traffic labeled as 0 and malicious traffic labeled as 1. We have done some preprocessing techniques, such as deleting null values, encoding, normalizing on the dataset.

4.2. Experimental Setup

The flowchart in Figure 2 shows the steps involved in the experimental procedure. The experiment is carried out using Jupyter Notebook [27] which is an original web application for creating and sharing computational documents. The notebook is build using Python language [28] which offers the necessary libraires and packages for ML applications. First, the essential libraries are imported, such as, panda, numpy, sklearn and keras. Then, data preprocessing techniques have been implemented on the dataset as described in the above section. The dataset is divided into independent variables (input variables) and dependent variable (target). After that, a feature selection technique has been applied into the input to reduce the number of used features, thus, reduce the model complexity and achieve high performance. Moreover, the dataset is portioned using percentage, 80% for the training set, and 20% for the testing set. Finally, the ML models are built and evaluated using the performance metrices.

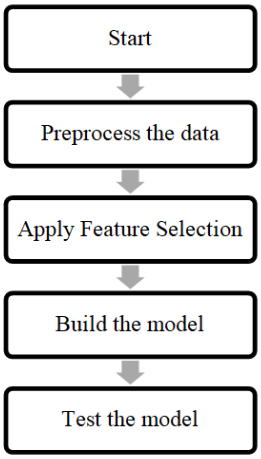

Figure 2. The experimental procedure flowchart

4.3. Performance Measures

The performance of the machine learning model can be evaluated using a variety of feature criteria. The performance measurement utilized in this research are Accuracy, Recall, Precision, and F1. As seen below, we briefly explain these measurements and their mathematical formula.

Accuracy: The measurement of the percentage of true rate value. The performance is better when the percentage of accuracy increases. Accuracy is calculated by formula 4.

$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} \quad (4)$$

"T_P, T_N" stands for True Positive and True Negative, and "F_P, F_N" stands for False Positive and False Negative. T_P rate is calculated using formula 5,

$$T_p\ rate = \frac{T_p}{Actual\ Positive} \quad (5)$$

However, the FR rate can be calculated using formula 6.

$$F_p\ rate = \frac{F_p}{Actual\ Negative} \quad (6)$$

Recall: a different measurement of True Positive rate, is the ratio of T_P rate of relevant results. retrieved relevant when the higher ratio was achieved. It is calculated by using formula 7.

$$Recall = \frac{T_p}{T_p + F_n} \qquad (7)$$

Precision: The ratio of actual positive rate values of pertinent elements to those of irrelevant elements. A higher percentage of precision leads to more relevant results. it can be calculated using formula 8.

$$Precision = \frac{T_p}{T_p + F_p} \qquad (8)$$

F1 score: It is the combination between precision and recall. Also,It uses both false positive and false negatives accounts. moreover, it works perfectly on an imbalanced dataset.it can be calculated using formula 6.

$$F1 = \frac{2 * Recall * Precision}{Recall + Precision} \quad (9)$$

4.4. Feature Selection

Before creating machine learning models, feature selection decreases the number of available features. It seeks to eliminate unnecessary, redundant, and/or noisy features in order to reduce modeling processing time and enhance model accuracy. In this work, we used SelectKBest (Chi^2). SelectKbest method looking for the highest K Score then select them. This method changes the 'score_func' parameter by doing that the method can be applied for both classification and regression data. We selected this method for our work because in selecting phase preparing a large dataset for training is one of the most important steps. As result, from selectKbest, the Best 11 Features are: ['dt', 'switch', 'src', 'pktcount', 'bytecount', 'flows', 'packetins', 'Protocol', 'tx_kbps', 'rx_kbps', 'tot_kbps'].

Table 2: Features Description

Features Name	**Feature Represent**
dt	Data/Time.
switch	Number of Switches
src	Source IP Address.
pktcount	Packet Count per-flow.
bytecount	Byte Count per-flow.
flows	Total number of flows in a switch
packetins	The count of packet_in messages conveyed to the controller.
Protocol	Protocol name associated with the traffic flow
tx_kbps	The kilobytes transferred per second.
rx_kbps	The kilobytes received per second.
tot_kbps	The bandwidth of a switch port.

5. RESULT AND DISCUSSION

Since DDoS is temporal correlative attack, it should be detected in a timely manner. Therefore, building a machine learning model that can detect a potential attack in a short amount of time is extremely significant. Our machine learning models have shown excellent results in detecting DDoS attack with a smaller number of features, thus, with less computational overhead. As mentioned earlier our experimental findings are evaluated using accuracy, recall, precision and F1.

Table 3 shows the result of each performance metrices obtained from each algorithm. The obtained result shows the robustness of the proposed model on detecting DDoS attack with only 11 features. The Random Forest classifier has successfully achieved the highest result in all measures. In contrast, the Logistic regression has a poor performance, consequently, it does not offer satisfactory results in detecting DDoS.

Table 3: Performance Measures Results

Quality Measures	**Logistic Regression**	**SVM**	**KNN**	**RF**	**LSTM**
Accuracy	0.656	0.967	0.973	0.995	0.966
Recall	0.574	0.964	0.971	0.994	0.968
Precision	0.646	0.965	0.969	0.995	0.959
F1	0.607	0.965	0.970	0.994	0.962

Table 4 represents a comparison with Ahuja at el. [20] work and our proposed models in terms of model accuracy. The result shows the considerable impact of applying the feature selection on the model performance. In our proposed model, the logistic regression does not improve after applying the feature selection. This is due to the binary nature of this algorithm, as it is not affected by the number of features. On the other hand, a noticeable improvement of 11% in the SVM accuracy is achieved. Also, the KNN and RF has slightly improved with smaller number of features. In conclusion, our proposed model was successfully able to detect the DDoS attack with half of the features.

Table 4: Accuracy Comparison

Algorithm	Proposed Model Accuracy	Ahuja at el. [20] Accuracy
Logistic Regression	0.656	0.837
SVM	0.967	0.858
KNN	0.973	0.952
RF	0.995	0.972

6. CONCLUSION AND RECOMMENDATION

DDoS attacks have been a serious and complex problem to Cloud Computing; therefore, we must not underestimate the threat that DDoS imposes. And as time goes by, DDoS attacks will only continue to evolve, for this reason we need to pay attention to prevent these attacks and build a robust mechanism. By using machine learning algorithms, we will be able to detect DDoS, earlier enough to facilitate the proactive provision of proper supports. In this paper, we have utilized various algorithms which are Logistic Regression, SVM, KNN, RF and LSTM. Also, we have shown the importance of feature selection in providing accurate and fast detection and we compared our result with the previous study. In conclusion, The Random Forest classifier has shown a great result in detecting the DDoS with only 11 features, as it has achieved an accuracy of 99%.

REFERENCES

[1] "https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1737," Software - defined networking SDN : a survey, 2016.

[2] **بحث بعنوان** and **الحوسبة السحابية**, "**أياد عماد علي دائرة تقنية المعلومات واالتصاالت البنك المركزي العراقي**."

[3] "Distributed Denial-of-Service Attacks in the Internet," 2005.

[4] S. Dong, K. Abbas, and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," IEEE Access, vol. 7, pp. 80813–80828, 2019, doi: 10.1109/ACCESS.2019.2922196.

[5] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Surveys and Tutorials, vol. 18, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 602–622, Jan. 01, 2016. doi: 10.1109/COMST.2015.2487361.

[6] K. Bhushan and B. B. Gupta, "Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing Environment," in 2018 5th International Conference on Signal Processing and Integrated Networks, SPIN 2018, Sep. 2018, pp. 872–877. doi: 10.1109/SPIN.2018.8474062.

[7] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Analysing Feature Selection and Classification Techniques for DDoS Detection in Cloud."

[8] M. Zekri, S. elKafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in Proceedings of 2017 International Conference of Cloud Computing Technologies and Applications, CloudTech 2017, Feb. 2018, vol. 2018-January, pp. 1–7. doi: 10.1109/CloudTech.2017.8284731.

[9] G. Singh Kushwah and S. Taqi Ali, "Detecting DDoS attacks in cloud computing using ANN and black hole optimization," 2017.

[10] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," Security and Communication Networks, vol. 2018, Apr. 2018, doi: 10.1155/2018/9804061.

[11] IEEE Staff, 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE, 2019.

[12] Y. Xu, H. Sun, F. Xiang, and Z. Sun, "Efficient DDoS Detection Based on K-FKNN in Software Defined Networks," IEEE Access, vol. 7, pp. 160536–160545, 2019, doi: 10.1109/ACCESS.2019.2950945.

[13] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," IEEE Access, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[14] 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.

[15] K. S. Sahoo et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," IEEE Access, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/ACCESS.2020.3009733.

[16] M. M. Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Analysis of features dataset for DDoS detection by using ASVM method on software defined networking," International Journal of Networked and Distributed Computing, vol. 8, no. 2, pp. 86–93, Mar. 2020, doi: 10.2991/IJNDC.K.200325.001.

[17] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, and V. Grout, "Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning," IEEE Access, vol. 9, pp. 122495–122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[18] A. Gaurav, B. B. Gupta, C. H. Hsu, D. Perakovic, and F. J. Garcia Penalvo, "Filtering of Distributed Denial of Services (DDoS) Attacks in Cloud Computing Environment," Jun. 2021. doi: 10.1109/ICCWorkshops50388.2021.9473886.

[19] M. W. Nadeem, H. G. Goh, V. Ponnusamy, and Y. Aun, "Ddos detection in sdnusingmachine learning techniques," Computers, Materials and Continua, vol. 71, no. 1, pp. 771–789, 2022, doi: 10.32604/cmc.2022.021669.

[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, Aug. 2021, doi: 10.1016/j.jnca.2021.103108.

[21] R. Muhamedyev, R. I. Muhamedyev, K. Pushkina, and A. Kazakhstan, "Nanostructures for bacteria detection and study (NANOBAC) View project semantic network of ICT domain view project Machine Learning Methods: An overview 1 Introduction 2 Machine learning techniques 2.1 Types of machine learning algorithms 2.2 Setup of machine learning systems 2.3 Formal definition of a machine learning problem 2.4 Regressive algorithms and data classification algorithms 3 Quality assessment of machine learning systems," 2015. [online]. Available: www.cmnt.lv

[22] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," Security and Communication Networks, vol. 2018, Apr. 2018, doi: 10.1155/2018/9804061.

[23] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," IEEE Access, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[24] S. Pande, A. Khamparia, D. Gupta, and D. N. H. Thanh, "DDOS Detection Using Machine Learning Technique," in Studies in Computational Intelligence, 2021, vol. 921, pp. 59–68. doi: 10.1007/978-981-15-8469-5_5.

[25] J. M. Lee, "Recurrent neural networks and Long-short term memory (LSTM)."

[26] "DDOS attack SDN Dataset - Mendeley Data."

[27] "https://jupyter.org."

[28] "https://www.python.org."