SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I7P109

Volume 10 Issue 7, 87-96, July 2023

Review Article

A Comparative Study of DDoS Attack in Cloud Computing Environment

Animesh Kumar[1], Sandip Dutta[2], Prashant Pranav[3]

[1,2,3]*Department of Computer Science & Engineering, Birla Institute of Technology, Mesra, Jharkhand, India.*

[3]*Corresponding Author : prashantpranav19@gmail.com*

Received: 02 May 2023 Revised: 28 June 2023 Accepted: 18 July 2023 Published: 31 July 2023

Abstract - *DDoS Attack refers to the flooding of the server through various mechanisms by the attackers to devoid the user of having access to the resources or to deplete the user's available resources. DDoS attack in the cloud has been one of the most frequent attacks in the service, eventually hampering the provider's and users' economic and resource availability. This paper categorized the DDoS research papers based on Network Management, Deep Learning Methods, Machine Learning, Software-Defined Networks, Resource Management, Load Distribution, Fuzzy Approach, etc. Accuracy, Precision, Recall, and F1 Score are compared with forty-one different proposed methods, and comparative graphs are also shown. SaDE-ELM performs best in all datasets, and SVM performs worst.*

Keywords - *Cloud attack, Cloud computing, Deep learning, Machine learning, Security issues.*

1. Introduction

A DDoS (Distributed Denial of Service) attack in cloud computing refers to an attacker trying to flood a cloud-based server or network with massive requests, thus rendering the server unavailable for regular users. The attacker seeks to exploit system vulnerabilities and use botnets or other means to direct a high volume of traffic from multiple sources toward the target cloud server. This can cause the server to overload, resulting in slow response times or even complete server downtime. The impact of a DDoS attack can be severe, causing loss of revenue, damage to reputation, and disruption of critical services.

DDoS attack targets and exploits the facilities provided by cloud computing, such as resource pooling, elasticity, broad network coverage, and other on-demand services. DDoS attack in cloud computing floods the large volume of malicious traffic in the victim's cloud system creating service unavailability issues. Attackers also use a low rate of malicious traffic to target cloud resources. It infects many clouds connected systems and servers in a relatively very short period.

In cloud computing DDoS multiple distributed infected machines, also known as bots [1], target the cloud servers. These attacks cause financial losses and long-term and short-term effects on cloud service providers (CSPs). The attacker tries to hamper the service level agreement (SLA) [2] between the client and CSPs.

The rapid elasticity facility of cloud computing used by the attacker for DDoS attacks causes unnecessary scaling up of cloud resources, which increases the financial burden of CSPs over a long period because of unpaid malicious usage.

1.1. Motivation

Motivations to write this review paper are as follows:

1) Detail Classifications of the defence mechanism of DDoS attacks need to be addressed appropriately in existing papers.
2) Proper categorization needs to be included in papers based on the technique employed by the authors.

Thus, there is a need to rewrite the DDoS attack paper over the cloud to minimize the attack effects.

1.2. Contribution

We have categorized the DDoS research papers based on network management, deep learning method, machine learning software-defined network, resource management, load distribution, Fuzzy Approach, etc.

Forty-one techniques are compared and analyzed in terms of accuracy, precision-recall value, and F1 Score.

Comparison of CICIDS, KDD, UNB-ISCX, and CS_Dataset are compared to determine the best and worst techniques for DDoS Attacks in the cloud.

1.3. Types of DDoS Attacks

DDoS attacks are generally divided into two groups based on their malicious traffic flow, Brute force attack (High -rate) and Semantic attack (Low-rate). Brute Force attacks involve massive requests with a network bandwidth of more than 500Gpbs [3].

Network and Transport Layer attacks and Application-Level attacks are of two types—network and transport layer attack target TCP-SYN, ICMP, UDP Floods, etc. Application-Level Flood Attack targets DNS, HTTP, SMTP, HTTPS, etc. Semantic attacks consume less network bandwidth (in Mbps) [4]. They are generally of four different types. Shrew, Reduction of Quality (RoQ) attack, Low-Rate DDoS attack (LoRDAS), and Economic Denial of Service (EDoS). DDoS attack generally disrupts legitimate users by limiting their bandwidth and router processing capacity and may initiate transport and network layer attacks (Flooding attacks).

2. Defense Mechanism for DDoS Attacks

This section shows some prevailing defence mechanisms against DDoS attacks.

2.1. Based on Network Management

Kautish et al. [5] (2022) proposed a novel Tree Architecture and called it scattered Denial of Service Mitigation (SDTMA) to mitigate DDoS attacks in a hybrid cloud. The greedy stepwise algorithm is used to improve the network security of the cloud. In terms of accuracy, 99.7%, specificity 98.32%, and sensitivity 99.92%, results were achieved compared to other techniques. Future work suggests it is possible to use a fuzzy-based approach, adopting artificial intelligence (federated learning) in the real-time scenario to counter DDoS attacks. Nadeem et al. [6] (2021) proposed an efficient intrusion detection and prevention system for DDoS and Brute force attacks. The alert message, signature system, encryption method, and two-step authentication techniques were implemented.

Tools based on host-based intrusion detection systems (HIDS), signature-based intrusion detection systems (SIDS), and Network-based intrusion-based detection (NIDS) to save the routers and cloud servers. In the future, there is scope for secured algorithms for cloud systems (RAM, CPU, cache memory). Better algorithms tools can be prepared using tools like Snort, OSSEC, and Suricata to secure the cloud.

Table 1. Some low-level DDoS attacks

Name of LDoS Attack	Layers	Protocol	Target
CXPST	Application layer	BGP & TCP	Border Router
LoRDAS	Application layer	HTTP	Terminal Layer
ZMW	Application layer	BGP & TCP	Border Router
RoQ	Network layer	AQM	Network Node
Shrew attack	Transmission layer	TCP	Network Node & Link
Full-buffer shrew	Transmission layer	TCP	Network Node & Link
Link-saturation shrew	Transmission layer	TCP	Network Node & Link
AIMD-based PDoS	Transmission layer	TCP	Network Node & Link
RTO-based PDoS	Transmission layer	TCP	Network Node & Link

2.2. Based on Deep Learning (DL) Approach

Divyasree et al. [7] (2022) proposed a Domain Adversarial Defense (DAD) technique to overcome domain mismatch in real-time attacks in the cloud. Fog and Deep-Learning approach was implemented in DAD. An adversarial training algorithm was used to counter real-time attacks using unsupervised learning[8]. The result proves that the DAD model has better improvement in minimum overhead and latency and has better efficiency as compared to another state of art previous work.

Bhardwaj [9] (2020) proposed Deep Neural Network (DNN) architecture and AutoEncoder (AE) in network traffic for DDoS classification. The proposed architecture is compared with ten other machine-learning classifiers. The experiment uses the CICIDS2017 [10] and NSL-KDD [11] datasets. Algorithm for Train_AE for training for optimized AE used for selecting the best model—Train_DNN for optimized DNN for optimized DNN. The result shows 98.43% accuracy in the NSL-KDD dataset and 98.92% in the CICIDS2017 dataset. The proposed technique can be upgraded for real-time traffic analysis using less time and complexity.

Mean Square Error (MSR) /Cross-Entropy:

$$d(X,R) = \frac{1}{n}\sum_{i=1}^{n}(X-R)^2 \quad (1)$$

Where, X= input vector, R=output, "n" =length Binary cross entropy

$$d(X,R) = -(X.\log(R) + (1-X).\log(1-R)) \quad (2)$$

"." = element-wise product and all other operators only computed element-wise.

2.3. Based on the Machine Learning (ML) Approach

Kushwah [12] (2022) proposed a hybrid ML model using extreme learning machine (ELM) [13, 14] and modified self-adaptive differential evolution (SaDE) [15] and called (SaDE-ELM) for the detection of DDoS attacks in cloud computing. ELM is part of an artificial neural network (ANN), used mainly for high accuracy and quick learning feature. Modified SaDE is best suitable for crossover operators, the crossover rate during evolution, and the best mutation strategy. SaDE-ELM works on both the network and hypervisor levels.

At the network level, it is deployed between the firewall and switch, and all outward and inward cloud traffic is monitored. At the hypervisor level, traffic monitoring between the virtual machine and hypervisor and in the virtual network so that an inside attacker is detected. Database, pre-processor, and classifiers are three components of the proposed model. Pseudocode for SaDE is specified. Time Complexity is O ($g \times N \times n^2 \times P$), where P is the population of target vectors. The result proves an accuracy rate of 97.23% on NSS-KDD, 98.28 % with CIDDS-001, and 91.46% with the ISCX IDS 2012 dataset.

Alqarni [16] (2022) proposed a technique to merge different ML classifiers to detect DDoS attacks in the cloud more accurately and with low-performance overheads. Naive Bayes, Decision Tree, SVM, Majority Voting, and K-NN were base classifiers. The Majority vote ensemble method used for DDoS is explained using a training set, classification model, prediction, and voting specified. Base classifiers, data collection, feature selection, and ensemble are four sections of this proposed method. The architecture of the proposed method is shown using a proper flow diagram. The result proves 98.02%accuracy, 97.45% sensitivity, and 98.65% specificity using CICDDOS2019 datasets. Performance comparison of the ensemble with execution time per instance is also shown.

Liu et al. [17] (2020) proposed the search algorithm, Bayesian Q-learning game scheme against DDoS attacks in sensor edge cloud. The optimal resource allocation technique is allocated in the game's first stage. The next step is to analyze resource distribution among defenders and DDoS attackers under the edgeVM. Algorithms for Greedy Q-Learning are shown in the paper. A comparative graph of Defender's average utilities concerning Bayesian Q-learning, SARSA, Q-learning, and DQN methods is appropriately displayed. The simulated result shows that the proposed algorithm is advanced compared to other dependable resource allocation mechanisms.

Li et al. [18] (2019) proposed a novel dynamic Low-Rate DDoS attack mitigation technique over a container-based cloud environment. This technique coordinates user resource allocation and increases the Quality of Service (QoS). The model is purely based on queueing theory. DDoS attack mitigation technique is explained. The result shows it can effectively solve low-rate DDoS problems using minimum resources. The graph shows a comparative analysis of the average staying time between attack and non-attack scenarios. MATLAB is used to conduct simulated experiments. Future work is possible to solve the pricing issues in container-based cloud environments that counter DDoS attacks and provide solutions for Low-rate DDoS attacks in microservices with unlimited resources.

Zekri et al. [19] (2017) proposed a novel C.4.5 algorithm to counter the DDoS attack. The signature detection method uses a decision tree approach to solve high-rate DDoS attacks automatically. The Network and Transport layer is mainly focused. C4.5 algorithm is compared with Naive Bayesian and K-Means methods. The result proves that the rate of detection is more than 98%. There is future scope in developing a better prototype model for detecting and mitigating DDoS attacks in real-time traffic Scenarios.

Sahi et al. [20] (2017) proposed novel classifier systems for DDoS attacks in the public cloud named "CS_DDoS." This system is designed to ensure the security and availability of e-Health records. This system works in the detection and prevention phase. CS_DDoS system architecture is shown using the data flow diagram, how incoming packets from the attacker are blocked. Algorithms for pre-processing of data are explained for data analysis. Malicious source IP addresses will be blocked from accessing the cloud.

The performance of this classifier is tested using K-fold validation [21]. The proposed system is compared with least square SVM (LS-SVM), naïve Bayes, and K-nearest methods. The result proves 97% accuracy in terms of DDoS attack detection. In the future, the extension of CS_DDoS attacks is possible by overcoming the challenges of the spoofed IP addresses.

CS_DDoS accuracy, sensitivity, and specificity are shown using mathematical equations (1) (2) (3). Figure 1 and 2 below shows the graphical representation of the DDoS prevention mechanism through different ML algorithm. As it can be observed from both the figures, the Neural Network-based method to prevent DDoS attacks performs the worst among all the algorithms, followed by Ensemble Learning and TEHO – DBN, while SaDE- ELM performs the best.

$$CS\_DdoS_{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \times 100\% \quad (3)$$

$$CS\_DDoS_{Sensitivity} = \frac{TP}{TP+TN} \times 100\% \quad (4)$$

$$CS\_DDoS_{specificity} = \frac{FP}{FP+TN} \times 100\% \quad (5)$$

Where True Negative (TN) = Normal packets correctly identified. False Negative (FN) = Normal packets incorrectly identified. True Positive (TP) = Abnormal packets correctly identified. False Positive (FP) = Abnormal packets incorrectly identified.

2.4. Software-Defined Network (SDN) in the Cloud

Harikrishna [22] (2021) proposed a rival model penalized self-organizing map in an SDN environment named (RMPSOM-SDNDM). The model differentiates between normal and malicious data traffic by using Euclidean distance[23]. The result shows data accuracy rate improves by 18 %. Precision increased by 10 %, Recall by 8 %, and optimality rate by 9 %. In the future, fuzzy logic can be implemented to upgrade the proposed model.

Debroy et al. [24] (2020) proposed an SDN-based resource adaptation to defend cloud-based applications from DDoS attacks by applying the concept of "moving target defence" (MTD). This technique focuses on the VM migration method. The utility maximization algorithm is used for resource allocation and increasing net utility. DDoS attacks were reduced by 40% compared to the traditional cloud resource method.

Performance testing is done on GENI Cloud Environment [25]. There is a 30% increase in CSP resource utilization. Detection of dummy traffic used by an attacker is shown in graphical form. In the future, cost-cutting from CSP's end is possible using MTD based approach. This technique can be implemented on the source side to block DDoS attacks.

Phan [26] (2019) proposed a novel scheme for DDoS attacks, enhanced history based on filtering of Internet Protocol called "eHIPF" based on cloud SDN. SVM and self-organizing map [27] algorithms are used in this approach. DDoS defence scheme, Boundary calculation for the following observation, and eHIPF abnormal source detection algorithms are given.

Experiment results show that eHIPF increases the detection rate of DDoS attacks compared to traditional networks. A comparison of detection, accuracy, and false alarm rate is displayed using the graphical form. In the Future, Deep Learning will be applied to this scheme. Designing new modules is possible for a more protected communication channel.

2.5. Based on Resource Management

DDoS attacks drain the maximum resources from the cloud system. Yuan et al. [28] (2020) proposed a resource management mechanism based on the birth-death process to solve this issue. The model reduces the financial burden of CSPs. Memory consumption and processing time are calculated using the birth and death process model. Cost-cutting in cloud systems is done through fine-grained resource management.

The model provides the facility of scaling in/out and down/up. Integer linear programming is used for selecting the proper leasing mode for cloud service customers (CSC). Algorithm for picking the optimal leasing mode based on the number of VMs and their types. It can save around 53.58% to 93.75% on financial costs for the DDoS attack defence. There is a future scope of work in the other resources like the network and storage domain. The different pricing models can be suggested in the On-demand, Spot, and reserved requests.

Somani et al. [29] (2017) proposed the "Scale Inside-out" technique. During DDoS attacks, the resource utilization factor is reduced to the minimum value to ensure resource availability. Attack detection and service report timing, and co-related services downtime improved significantly. The author shows all three stages of the DDoS attack mitigation method. Scale Inside Out Algorithms used for attack mitigation. Function ScaleInsideOut () algorithm is used for updating in resource utilization factor.

Performance evaluation of DDoS mitigation service, with and without "Scale Inside-Out," shown using both graphical and tabular format. The result demonstrates a reduction of up to 95% in total attack downtime of the victim service. Future work suggests a scope of new work in "in-resources" scaling, ultimately leading to early detection of DDoS attacks.

2.6. Based on Load Distribution

Wahab et al. [30] (2017) applied the load distribution approach to solving the DDoS menace problem. They proposed a trust model that combines objective and subjective sources with Bayesian inference to build a confident relationship between hypervisor and guest VMs. Virtual Machine Monitoring algorithm for calculating resource consumption and monitoring of hypervisor. For experimental analysis, CloudSim [31] simulator is used. The model increases the detection rate to 26-reduction up to 20% in false positive and negative values. The Cloud system's CPU consumption is minimized by up to 15 percent, memory utilization approx. 11 percent, and network bandwidth consumption reduced to 5 percent. This technique performs better in large-scale data centres, where roughly 4.4 seconds are required to run in cloud environments with 50 co-hosted VMs [32-34].

2.7. Fuzzy-Based Approach

The problem of Allocation and De-allocation of time resources with compromising SLAs in the cloud environment was solved through a fuzzy approach. Rizvi [35] (2019) proposed a resource provisioning technique based on fuzzy Q-Learning [36] and Chebyshev's inequality principle [37]. Algorithms for autonomic computing are used for the monitoring, analysis, planning, and execution phase. Separate algorithms for the planning and execution phase are used for updating q valves. Nine fuzzy rules are implemented. CloudSim 3.0 and MATLAB software is used for experimental analysis. The result proves that the proposed model performs better in VM provisioning, and cost minimization and response time are significantly reduced. In the future, improvement in the monitoring, analysis, planning, and execution phases is possible through dynamic Q-learning.

2.8. Scheduling Methods

To solvethe problem of traffic scheduling and improvement in the QoS from DDoS attacks in edge computing. Li et al. [38] (2021) proposed a Time-Wavelength division multiplexing method for the passive optical network called "TWDN-PON." The adaptive traffic scheduling (ATS) algorithm is used to update the network status and usage of the edge network. The time complexity of ATS is O (N ×m ×2). N is the number of arrival computing tasks, and m is the number of edge nodes.

The investigational result shows proposed technique can successfully mitigate DDoS attacks. Future work suggests there is scope for improvement in traffic scheduling methods and passive optical networks.

2.9. Bandwidth

The DDoS attack consumes most of the server's resources and network link bandwidth; Ravi [39] (2020) proposed a learning-based detection mitigation technique called (LEDEM) that detects and mitigate DDoS attack using supervised ML in Cloud IoT[40]. LEDEM algorithms are used to detect and remove malicious packets.

ML classifiers like SVM, Adaboost, and J48 are used for comparison. The result shows an accuracy rate of 96.23% in detecting DDoS attacks. A 21% increase in throughput is achieved compared to other techniques. Other ML techniques are also applied in the future to improve DDoS attack detection.

Network Accuracy and F-Measure is determined through Equation 6 and 7.

$$NA = \left(\frac{DD'+BB'}{DD'+BB'+BD'+DB'}\right) \times 100\% \quad (6)$$

For correct prediction of model accuracy (F -Measure)

$$F = \left(\frac{2*DD'}{(2*DD')+BD'+DB'}\right) \times 100\% \quad (7)$$

Here, DD' is True Positive.BD'= False Negative, DB'= False Positive, BB'=True Negative.

Table 2. Comparison table based on CICIDS dataset

S. No	Approach	Dataset	Accuracy	Precision	Recall	F1 Score
1	VSI-RTN [41]	CIC-DDOS2019	98.74	-	98.73	-
2	AE+DNN [9]	CICIDS	98.92	97.45	98.97	98.35
3	Naive AE+DNN [9]	CICIDS	93.00	94.70	92.70	93.70
4	AE+SVM [9]	CICIDS	99.41	99.67	99.66	99.66
5	DT [9]	CICIDS	-	99.8	99.91	99.95
6	ANN [9]	CICIDS	-	99.6	99.98	99.97
7	SVM [9]	CICIDS	-	88.18	45.43	59.97
8	LSTM [9]	CICIDS	-	99.98	-	99.99
9	SAVAER + DNN [9]	CICIDS	89.36	95.98	84.86	90.08
10	SaDE-ELM [12]	CIDDS-001	99.98	-	99.96	-
11	SaE-ELM [12]	CIDDS-001	99.91	99.99	99.95	-
12	E-ELM [12]	CIDDS-001	99.87	99.81	99.95	-
13	ELM [12]	CIDDS-001	98.22	98.98	97.47	-
14	BP-ANN [12]	CIDDS-001	97.34	96.37	98.34	-

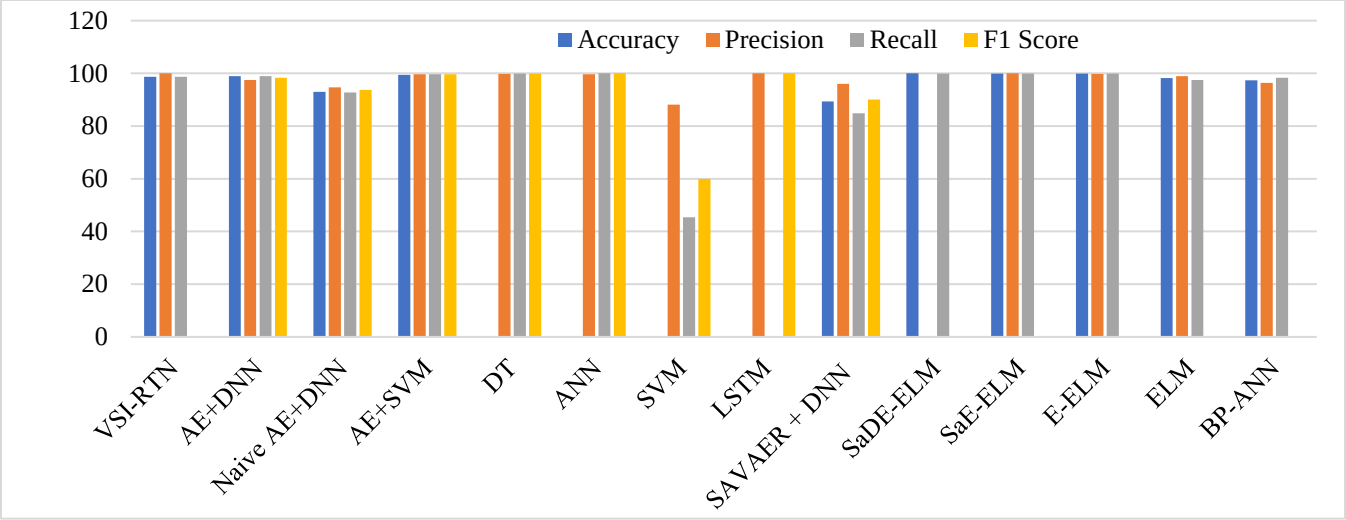

Fig. 1 Graphical comparison of approach based on CICIDS dataset

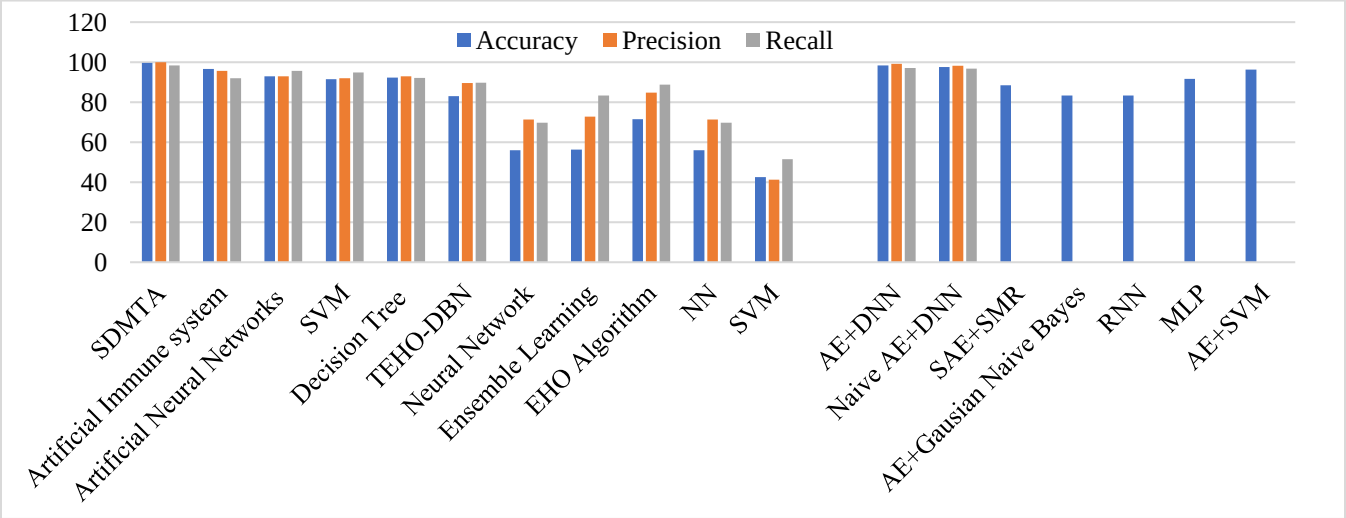

Fig. 2 Graphical comparison of approach based on NSS-KDD dataset

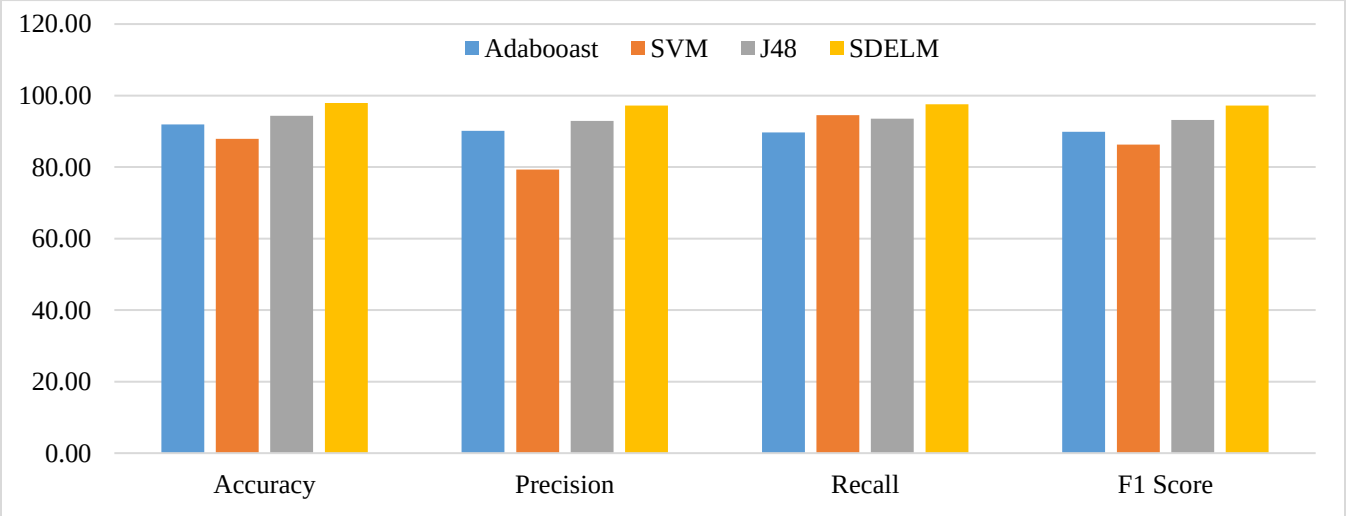

Fig. 3 Graphical comparison of approach based on UNI-ISCX dataset

Table 3. Comparison table based on KDD dataset

S. No	Approach	Dataset	Accuracy	Precision	Recall
1	SDMTA [5]	KDD999	99.7	99.92	98.32
2	Artificial Immune system [43]	KDD'99	96.56	95.60	91.90
3	Artificial Neural Networks [43]	KDD'99	92.87	93.00	95.60
4	SVM [43]	KDD'99	91.54	92.00	94.80
5	Decision Tree [43]	KDD'99	92.33	93.00	92.20
6	TEHO-DBN [42]	KDD	83.00	89.60	89.80
7	Neural Network [42]	KDD	55.95	71.40	69.80
8	Ensemble Learning [42]	KDD	56.25	72.70	83.33
9	EHO Algorithm [42]	KDD	71.42	84.80	88.80
10	NN [42]	KDD	55.95	71.40	69.80
11	SVM [42]	KDD	42.57	41.30	51.50
12	AE+DNN [9]	NSL-KDD	98.43	99.22	97.12
13	Naive AE+DNN [9]	NSL-KDD	97.54	98.15	96.73
14	SAE+SMR [9]	NSL-KDD	88.39	-	-
15	AE+Gausian Naive Bayes [9]	NSL-KDD	83.34	-	-
16	RNN [9]	NSL-KDD	83.28	-	-
17	MLP [9]	NSL-KDD	91.70	-	-
18	AE+SVM [9]	NSL-KDD	96.36	-	-

Table 4. Comparison table based on UNB-ISCX dataset

S. No	Approach	Dataset	Accuracy	Precision	Recall	F1 Score
1	Adabooast [39]	UNB-ISCX	91.90	90.10	89.70	89.90
2	SVM [39]	UNB-ISCX	87.90	79.30	94.50	86.3
3	J48[39]	UNB-ISCX	94.30	92.90	93.50	93.2
4	SDELM [39]	UNB-ISCX	97.90	97.20	97.60	97.2

Table 5. Comparison of own dataset and VSI-TN dataset

S. No	Approach	Dataset	Accuracy	Precision	Recall
1	LS-SVM [20]	CS_DDoS Dataset	94.00	95.00	94.00
2	Naïve Bayes [20]	CS_DDoS Dataset	88.00	92.00	94.00
3	K-nearest [20]	CS_DDoS Dataset	84.00	92.00	93.00
4	Multilayer Perceptron [20]	CS_DDoS Dataset	88.00	95.00	95.00
5	VSI-TN [41]	UNSW-NB15	98.26	97.99	98.87

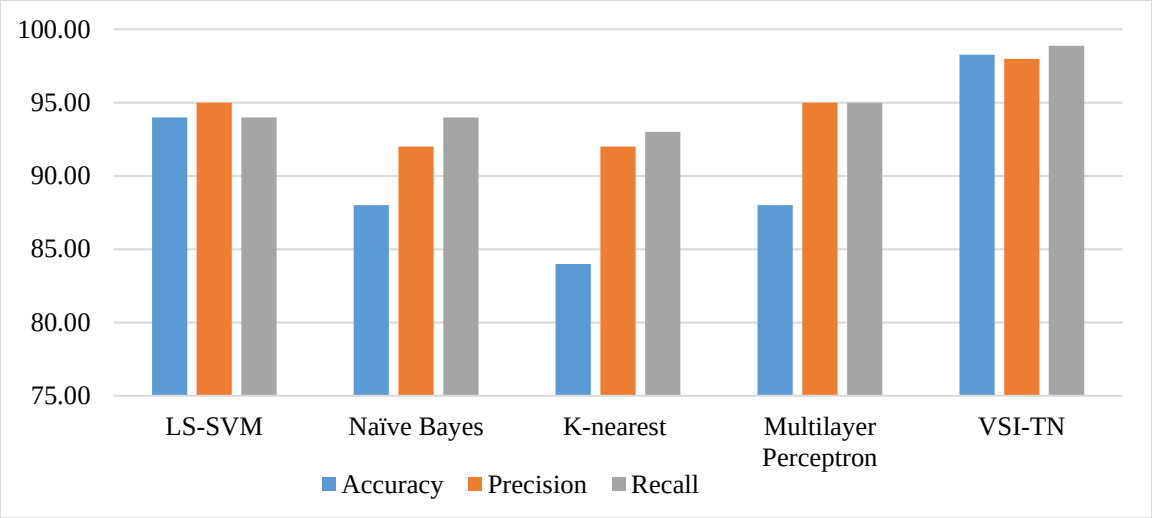

Fig. 4 Graphical comparison of approach based on own dataset

Table 6. Comparison table on different datasets

Dataset	Best Accuracy	Worst Accuracy
CICIDS	SaDE-ELM[12]	SAVAER+DNN[9]
KDD	SDTMA[5]	SVM[42]
UNB-ISCX	SDELM[39]	SVM[39]
CS_DDoS	LS-SVM[20]	K-nearest[20]

3. Result and Discussion

SaDE-ELM [11] performance is best in CICIDS, KDD, UNB-ISCX, and CS_DDoS Dataset, as shown in Table 6. Its primary disadvantage is that it takes more training time. Multiple operators guide the search process for the optimal solution from different directions [11]. SAVAER+ DNN performs worst in CICIDS Dataset in terms of accuracy. SDTMA serves best, and SVM performs worst in KDD Dataset. SDELM performs best and SVM worst in UNB-ISCX dataset. LS-SVM is best, and K-nearest is worst for CS_DDoS Dataset.

4. Conclusion

We analyzed four important attack datasets viz. KDD99, CICIDS, UNB – ISCX, NSL - KDD, and CS_DDoS for their application in different machine learning models. The ML models are mainly supposed to classify the incoming data as usual or attack. Based on our findings, it can be said that SVM has the worst performance for all the considered datasets for DDoS attack detection in a cloud computing environment. SaDE ELM is the best for accuracy metrics for all the datasets. However, these techniques need to be analyzed for more datasets.

References

[1] Anshuman Singh, and Brij B Gupta, "Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, no. 1, pp. 1-43, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Taher Labidi et al., "On the OLS Regression Algorithm and Pearson Correlation Algorithm for Improving the SLA Establishment Process in Cloud Computing," *Innovations in Systems and Software Engineering*, vol. 18, pp. 215–229, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Gaurav Somani et al., "Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 22-32, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Zhaomin Chen et al., "Power Spectrum Entropy-Based Detection and Mitigation of Low-Rate DoS Attacks," *Computer Networks*, vol. 136, pp. 80-94, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] Sandeep Kautish, Reyana A, and Ankit Vidyarthi, "SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6455-6463, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Muhammad Nadeem et al., "Intercept the Cloud Network from Brute Force and DDoS Attacks via Intrusion Detection and Prevention System," *IEEE Access*, vol. 9, pp. 152300-152309, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Divyasree I R, and Selvamani K, "DAD: Domain Adversarial Defense System against DDoS Attacks in Cloud," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 554-568, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Komal Purba, and Nitin Bhagat, "A Review on Load Balancing Algorithm in Cloud Computing," *SSRG International Journal of Computer Science and Engineering*, vol. 1, no. 10, pp. 1-5, 2014. [Google Scholar] [Publisher Link]

[9] Aanshi Bhardwaj, Veenu Mangat, and Renu Vig, "Hyperband Tuned Deep Neural Network with Well Posed Stacked Sparse Auto Encoder for Detection of DDoS Attacks in Cloud," *IEEE Access*, vol. 8, pp. 181916-181929, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ilhan Firat Kilincer, Fatih Ertam, and Abdulkadir Sengur, "Machine Learning Methods for Cyber Security Intrusion Detection: Datasets and Comparative Study," *Computer Networks*, vol. 188, p.107840, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Gerry Saporito, A Deeper Dive into the NSL-KDD Data Set, 2020. [Online]. Available: https://towardsdatascience.com/a-deeper-dive-intothe-nsl-kdd-data-set-15c753364657

[12] Gopal Singh Kushwah, and Virender Ranga, "Detecting DDoS Attacks in Cloud Computing using Extreme Learning Machine and Adaptive Differential Evolution," *Wireless Personal Communications*, vol. 124, pp. 2613-2636, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Guang-Bin Huang, Qin-Yu Zhu, and Chee-Kheong Siew, "Extreme Learning Machine: A New Learning Scheme of Feedforward Neural Networks," *2004 IEEE International Joint Conference on Neural Networks (IEEE Cat. No.04CH37541)*, Budapest, Hungary, pp. 985-990, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[14] Shifei Ding et al., "Extreme Learning Machine: Algorithm, Theory and Applications," *Artificial Intelligence Review*, vol. 44, pp. 103-115, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. K. Qin, and P. N. Suganthan, "Self-Adaptive Differential Evolution Algorithm for Numerical Optimization," *2005 IEEE Congress on Evolutionary Computation*, Edinburgh, UK, pp. 1785-1791, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ahmed Abdullah Alqarni, "Majority Vote-Based Ensemble Approach for Distributed Denial of Service Attack Detection in Cloud Computing," *Journal of Cyber Security and Mobility*, vol. 11, no. 2, pp. 265-278, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jianhua Liu et al., "A Bayesian Q-Learning Game for Dependable Task Offloading Against DDoS Attacks in Sensor Edge Cloud," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7546-7561, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zhi Li et al., "Exploring New Opportunities to Defeat Low-Rate DDoS Attack in Container-Based Cloud Environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 3, pp. 695-706, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Marwane Zekri et al., "DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments," *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, Rabat, Morocco, pp. 1-7, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] Aqeel Sahi et al., "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," *IEEE Access*, vol. 5, pp. 6036-6048, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] Hoang Lan Vu et al., "Analysis of Input Set Characteristics and Variances on K-Fold Cross-Validation for a Recurrent Neural Network Model on Waste Disposal Rate Estimation," *Journal of Environmental Management*, vol. 311, p. 114869, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Pillutla Harikrishna, and A. Amuthan, "Rival-Model Penalized Self-Organizing Map Enforced a DDoS Attack Prevention Mechanism for a Software-Defined Network-Based Cloud Computing Environment," *Journal of Parallel and Distributed Computing*, vol. 154, pp. 142-152, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] N. Priyanka, and V. Vetriselvi, "Penetration Testing for Software Defined Networks against DOS Attack," *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 8, pp. 10-13, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[24] Saptarshi Debroy et al., "Frequency-Minimal Utility-Maximal Moving Target Defense against DDoS in SDN-Based Systems," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 890-903, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Xenia Mountrouidou, and Vic Thomas, "CyberPaths: Cyber Security Labs for Liberal Arts Institutions using the NSF Global Environment for Network Innovations (GENI)," *SIGCSE'19:Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, p. 1241, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Trung V Phan, and Minho Park, "Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud," *IEEE Access*, vol. 7, pp. 18701-18714, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] V. Gholami et al., "Comparison of Self-Organizing Map, Artificial Neural Network, and Co-Active Neuro-Fuzzy Inference System Methods in Simulating Groundwater Quality: Geospatial Artificial Intelligence," *Water Resources Management*, vol. 36, pp. 451-469, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Bin Yuan et al., "Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2541-2554, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Gaurav Somani et al., "Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 959-973, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[30] Omar Abdel Wahab et al., "Optimal Load Distribution for the Detection of VM-Based DDoS Attacks in the Cloud," *IEEE Transactions on Services Computing*, vol. 13, no. 1, pp. 114-129, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[31] Mohamed Hadi Habaebi et al., "Extending CloudSim to Simulate Sensor Networks," *Simulation*, vol. 99, no. 1, pp. 3-22, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[32] Fei Zhang et al., "A Survey on Virtual Machine Migration: Challenges, Techniques, and Open Issues," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1206-1243, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[33] Mahesh M Baradkar, and Bandu B Meshram, "A Survey on Cloud Security: Infrastructure as a Service," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 6, pp. 17-21, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[34] N. Sendhil Kumar, and G. Jyotheeswar Chowdary, "IAAS Based Cloud Security and a Deep View Trust Model," *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 4, pp. 28-33, 2016. [Publisher Link]

[35] Naela Rizvi, and Dharavath Ramesh, "FBQ-LA: Fuzzy Based Q-Learning Approach for Elastic Workloads in Cloud Environment," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 3, pp. 2715-2728, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[36] P. J. Beslin Pajila, E. Golden Julie, and Y. Harold Robinson, "FBDR-Fuzzy Based DDoS Attack Detection and Recovery Mechanism for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 122, pp. 3053-3083, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[37] Miguel Vivas-Cortez et al., "On some Generalized Raina-Type Fractional-Order Integral Operators and Related Chebyshev Inequalities," *AIMS Mathematics*, vol. 7, no. 6, pp. 10256-10275, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[38] Yajie Li et al., "DDoS Attack Mitigation Based on Traffic Scheduling in Edge Computing- Enabled TWDM-PON," *IEEE Access*, vol. 9, pp. 166566-166578, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[39] Nagarathna Ravi, and S. Mercy Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attacks in IoT via SDN-Cloud Architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] I. Lakshmi, "Security Analysis in Internet of Things using DDoS Mechanisms," *SSRG International Journal of Mobile Computing and Application*, vol. 6, no. 1, pp. 19-24, 2019. [CrossRef] [Publisher Link]

[41] Adil Bin Bhutto et al., "Reinforced Transformer Learning for VSI-DDoS Detection in Edge Clouds," *IEEE Access*, vol. 10, pp. 94677-94690, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[42] S. Velliangiri, and Hari Mohan Pandey, "Fuzzy-Taylor-Elephant Herd Optimization Inspired Deep Belief Network for DDoS Attack Detection and Comparison with State-of-the-Art Algorithms," *Future Generation Computer Systems*, vol. 110, pp. 80-90, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[43] Damai Jessica Prathyusha, and Govinda Kannayaram, "A Cognitive Mechanism for Mitigating DDoS Attacks using the Artificial Immune System in a Cloud Environment," *Evolutionary Intelligence*, vol. 14, pp. 607-618, 2021. [CrossRef] [Google Scholar] [Publisher Link]