Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 13, Issue 1, July 2022: 2079-2088

Detection of DDos Attack Using Machine Learning Algorithms In Cloud Computing

Kanimozhi S[1], Radhika D[2]

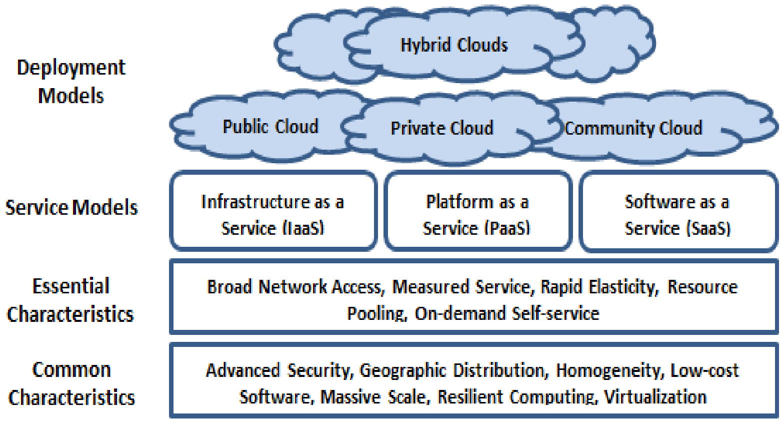
[1 2] Department Of Computer Science And Engineering, Vivekananda College of Engineering For Women (Autonomous), Elayamapalayam, Tiruchengode- 637205

Abstract: Cloud computing is a major research point for researchers to its widespread application and benefits. Cloud computing reliance on the internet service provision and its distributed nature propose. DDoS attack is to disturb to their services. Established detection methods, such as firewalls, are unable to detect insider attacks. Our work proposes an DDoS detection technique in the hypervisor layer to reduce DDoS activities. The proposed detection approach is developed by the radial basis function (RBF) with particle swarm optimization (PSO) for DDoS attack detection and classification of the traffic that is exchanged between virtual machines. The analysis of our proposed approach is to detect and classify the DDoS attack with high detection accuracy.

Keywords: distributed denial of service, DDoS, radial basis function, artificial neural network, back propagation neural network.

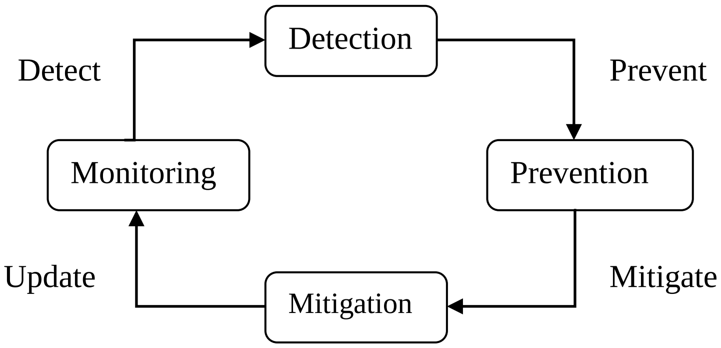
I. introduction

Cloud computing is the platform to deliver services through the internet. Many companies moving to cloud computing technologies due to its ease of use. It is the easiest way to minimise infrastructure cost. Cloud services are used anywhere at any time, users can able to pay per use. Cloud computing technology is very easy technology to use in wide range. Cloud computing provides better service with effective cost and infrastructure. Cloud Services can be used in all electronic devices like computer, phone and tablet. The figure shows the architecture of cloud computing environment[1]


Deployment Models
Hybrid Clouds
Public Cloud
Private Cloud
Community Cloud
Service Models
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Essential Characteristics
Broad Network Access, Measured Service, Rapid Elasticity, Resource Pooling, On-demand Self-service
Common Characteristics
Advanced Security, Geographic Distribution, Homogeneity, Low-cost Software, Massive Scale, Resilient Computing, Virtualization

1.1 Architecture of cloud computing environment

Cloud computing security it was a biggest challenge to the service contributors. Distributed denial of service (DDoS) attack it was one of the biggest challenge in cloud computing security. DDoS attack happend when the attacker trying to disturb the normal transformation process, attacker will turn normal data as botnet or zombies and create a flood to disturb the normal traffic; this kind of process is called as DDoS attack.DDoS attack has four phases such as monitoring, detection, prevention, and mitigation. The detection phase identifies the DDoS attack.



1.2 Life Cycle of Ddos Attack

Machine learning it is a Sub-division of artificial intelligence. Machine learning provides a way to train algorithms itself. Using simple mathematical calculations the algorithms learn itself and as well as grow itself. Artificial neural network (ANN) it was a subfield of machine learning.

ANN algorithms are inspired by the process of human brain, in which they contains the interconnection of millions of neurons, the neurons having three layers such as input layer, output layer and hidden layer. Many algorithms are proposed by the behaviour of neurons.

II.Literature Review

Idhammad M et al. (2018) presents a new detection method of HTTP DDoS attacks in a cloud environment. The proposed detection method performs based on two ensemble learning algorithms such as Information Theoretic Entropy (ITE) and RF. A time-based sliding window technique is used to calculate the entropy of the feature of network header of the incoming traffic signals. in a Cloud environment based on Open Stack platform. The classification tasks are produce when the expected entropy exceeds its usual range the pre-processing[2].

Rawashdeh A et al. (2018) proposes an anomaly intrusion detection technique in the hypervisor layer to depress DDoS performance between virtual machines. The proposed detection method is developed by the evolutionary neural network. The evolutionary neural network is incorporates the particle swarm optimisation (PSO) with neural network for DDoS attack detection and classification of the traffic data [3]. Here most previous research used KDD CUP 99 and NSL-KDD datasets to evaluate their approaches. On the other hand, the dataset only handles the traffic that exchanges between VMs, so the traffic that comes from an outside host machine could be studied in future work.

Kushwah, G.S. et al. (2020) proposed a new method for detecting DDoS attacks in cloud computing environment. The new detection method is developed based on voting ELM (VELM) [4].

Here NSL-KDD dataset and ISCX intrusion detection dataset are used. It has been shown that proposed system gives better accuracy than other systems built based on backpropagation ANN, ANN trained with black hole optimization, ELM, random forest and, Adaboost.

Kushwah, G.S et al. (2019) presents new DDoS attack detection model by using ELM. Here the NSL-KDD dataset used for experimentation. The proposed detection model produces high detection rate and takes less computation time.

Hezavehi S.M et al. A TPA along with DDoS attack detection capabilities called third party auditor notification generator (TPANG). The proposed detection frameworks combined a third party auditor notification generator along with notification of detection is called TPANGNDn n. Sahi A et al. (2017) developed a new classification based detecting system and preventing DDoS TCP flood attacks in public clouds environment. A new developed DDoS detection method presents a solution to protectthe stored records by classifying the incoming packets and building a decision according to the classification outcome.Wireshark network analyzer used to capture the flood attack. The proposed detection methods identify and establish whether a packet is regular or created from an attacker during the prevention phase.

Wani A.R et al. (2019) presents a new detection algorithm based on SVM. Out of the three algorithms used SVM shows the better results in terms of accuracy, recall .precision, specificity and f measure closely followed by Random Forest. The datasets are carried out on the own cloud environment using Tor Hammer attacking tool [5].

He z et al. (2017) presents a new DDoS attack detection model on the source side in the cloud environment based on machine learning approaches. This detection scheme statistical information from both the virtual machine and the hypervisor to avoid network packages from being sent out to the exterior system [6].

Ref. No.	**Algorithms**	**Performance**	**Approaches**	**Types**	**Tools**
[7]	ITE+RF	Low processing time and high accuracy	-	HTTP DDoS attack	OpenStock
[3]	BPNN+PSO	High detection accuracy	Anomaly	UDP Flood and TCP SYN	MATLAB
[4]	Voting ELM	minimum false alarms and high detection accuracy	-	-	MATLAB
[8]	TPA	low overhead of computations less rate of false negative	Anomaly	Application layer	Cloudsim + TPANGND Detector

[9]	-	High detection accuracy	-	TCP flood attack	WiresharkNetwork Analyzer
[10]	XGBoostclassificer +SDN	Higher accuracy, lower false positive rate, fast-speed and scalability.	-	TCP flood attack	Hyenae
[5]	SVM	High accuracy	-		SNORT
[6]	SVM +Linear Kernel	High detection accuracy	-	SSH brute-force, DNS reflection, ICMP flooding and TCP SYN attacks	OpenStock
[11]	MAS+PSO	High detection accuracy	-	-	JAVA+Cloudsim
[12]	FT-EHO+DBN	Higher detection accuracy	-	-	MATLAB
[13]	AIS+Feature selection	high detection accuracy and low false alarm rate	Anomaly	-	Cloudsim
[14]	PSO-PNN	Capable of extracting meaningful information and high detection accuracy	-	-	IXIA PerfectStorm tool
[15]	VFDT	high detection accuracy, low false positive and false negative ratio	-	WBAN	JAVA netbeans and WEKA
[16]	Hope-count algorithm	very small storage and has the ability of fast detection	Anomaly		Netwag Tool + JPCap
[17]	K-FKNN	high precision	-	-	Ryu controller
[18]	Feature selection + TEHO-DBN	Enhancing the detection accuracy	-	-	
[19]	C4.5 algorithm	Low computational	Signature	-	Wireshark

		cost and Faster detection rate			

III.Existing system

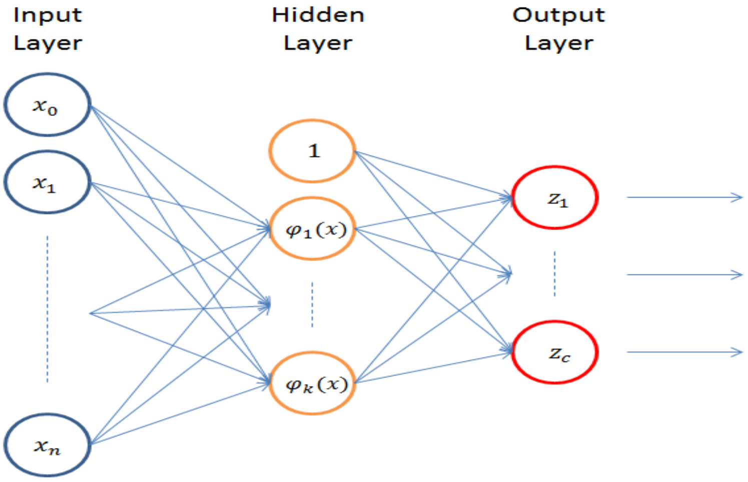
To detect DDoS attack more number of algorithms is proposed. The proposed algorithms are used some classification and detection techniques to achieve high detection accuracy and efficiency. But in some of the parameters they are failed to achieve high detection accuracy. The proposed techniques are

- Back Propagation Neural Network
- Back Propagation Neural Network Particle Swarm Optimization

This above two algorithms is proposed to detect DDoS attack, and they are failed to achieve some parameters.

A.Radial basis function:

Radial Basis Function (RBF) is a feed forward neural networks model with good performance and global approximation. In RBF it has three layers, such as input layer, hidden layer, output layer. In hidden layer, it contains the node is called as RBF units that is Gaussian function node. An RBF neural network has two key parameters that describe location function center and width of the RBF unit. The data points may not be evenly distributed to the input space when the center and width of the RBF neuron selected by random. By using clustering techniques for selecting center and width of hidden neurons in RBF, that reflects more accurately in distribution in the data points.



B.Particle swarm optimization

It was the most popular metaheuristic algorithm. usually, a group of animals that has no clear leader will discover the location of food by random, following one of the individuals (particles) of the swarm which has the nearest positionto the food source (potential solution) .the PSO algorithm poses multi-agent parallel search technique. It was working with the pbest and gbest values according to the position change those values are changing. According to particle position changing the values is updated for every movement.

IV.Proposed work

In this work we undertake the detection process of DDoS attack that was affect the normal data traffic in cloud. The proposed RBF with PSO (RBF-PSO) algorithm monitor and detect the flood attack in network.

An RBF neural network has two key parameters that describe location function center and width of the RBF unit. RBF network performs a nonlinear mapping from input space R^n to the output space R^m . R^n is an input vector space that is denoted by x_i (for i=1, 2, 3….n) and R^m is output vector space that is denoted by y (for i=1, 2….m). The j^{th} neuron of the Radial Basis Function, it is computes a Gaussian function as below

$$Z_i(x) = \exp(-\frac{\left\| x - c_j \right\|}{2\sigma_i^2}) \quad j = 1, 2, ...m \quad (1)$$

Where x is input feature vector with n dimension. c_j is the center of Gaussian vector of i and σ_i is width of the hidden layer. The width of the hidden layer σ_i is calculated by $\sigma_j = \sqrt{\frac{1}{m_j} \sum_{i=1}^{m_j} d^2(c_j - x_i)}$

(2)

The PSO algorithm mainly used for the weight adjustment process, the weights are based on the random inputs.

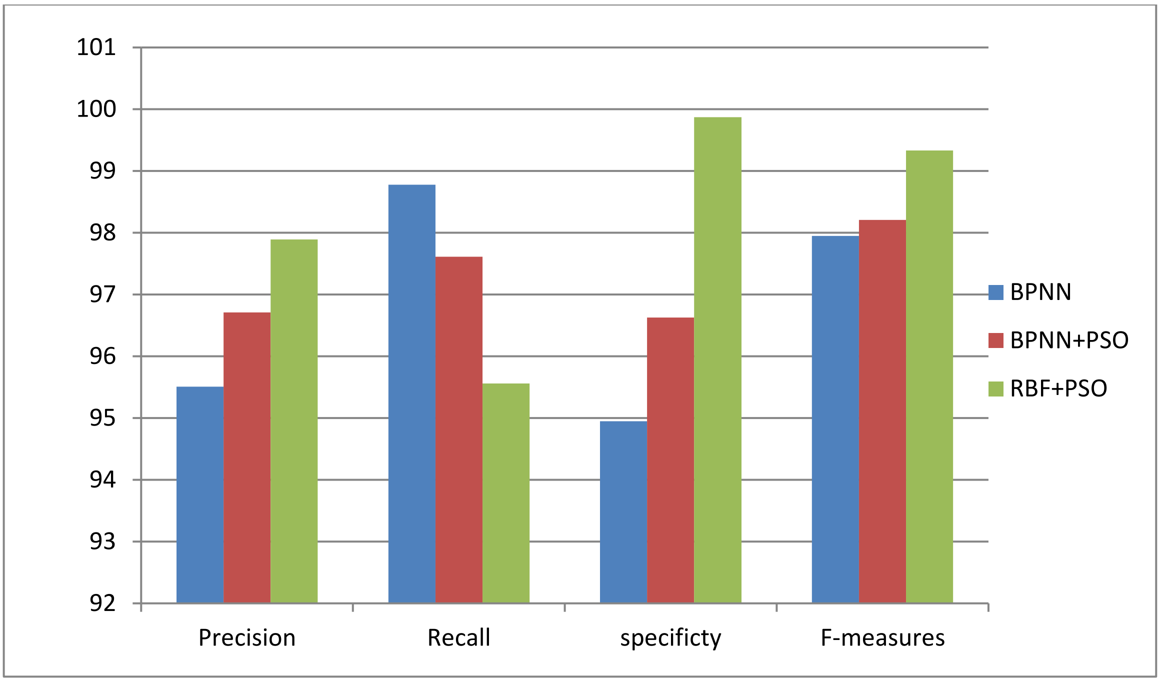
V.Experiments and Results

A.Datasets:

Our proposed algorithm trained with two datasets as NSL-KDD, KDD CUP99. There is no proper dataset is available to detect the flood attack in cloud computing. In cloud computing, behavioural-based approaches suffer from the unavailability of datasets, where most previous research used KDD CUP 99 and NSL-KDD datasets to evaluate their approaches.

Wireshark tool is used for data transformation capturing process.the captured data trained with machine learning algorithms, and they are used for our purpose. Here the three types of attacks are mostly captured they are normal attack,UDP Flood attack,TCP-SYN attack.

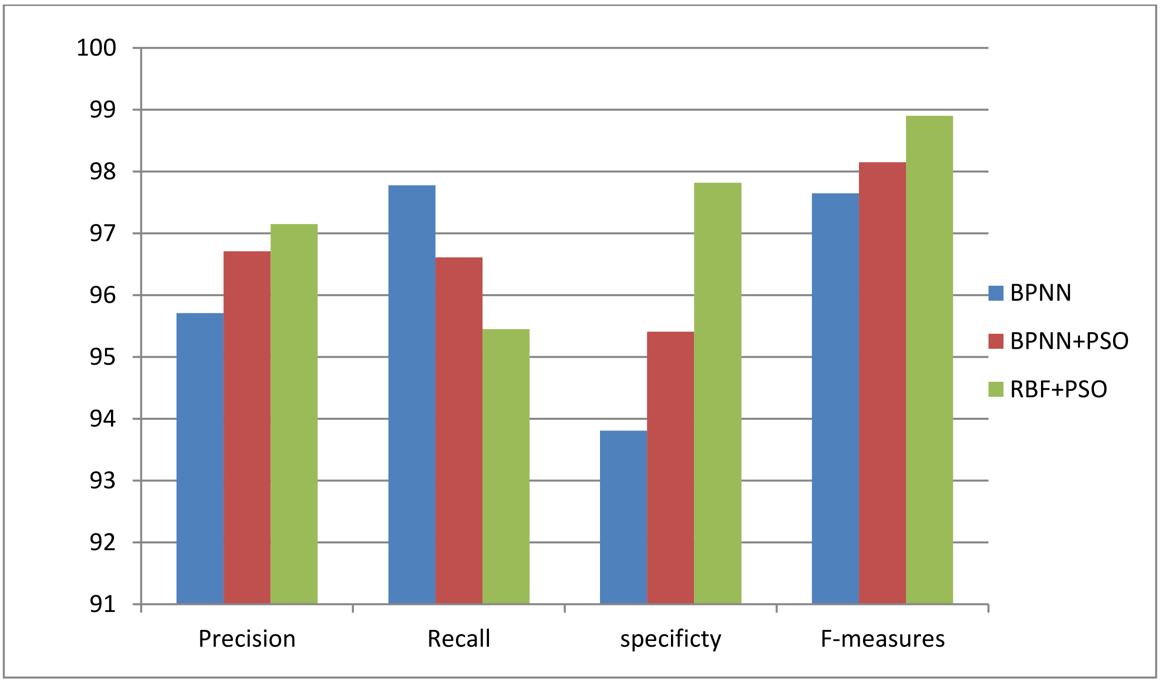
Performance metrics for UDP flood attack



1.3 performance metrices for UDP flood attack

PERFORMANCE METRICES	BPNN	BPNN+PSO	RBF+PSO
Precision	95.51	96.71	97.89
Recall	98.78	97.61	95.56
Specificity	94.95	96.63	99.87
F-Measures	97.95	98.21	99.33

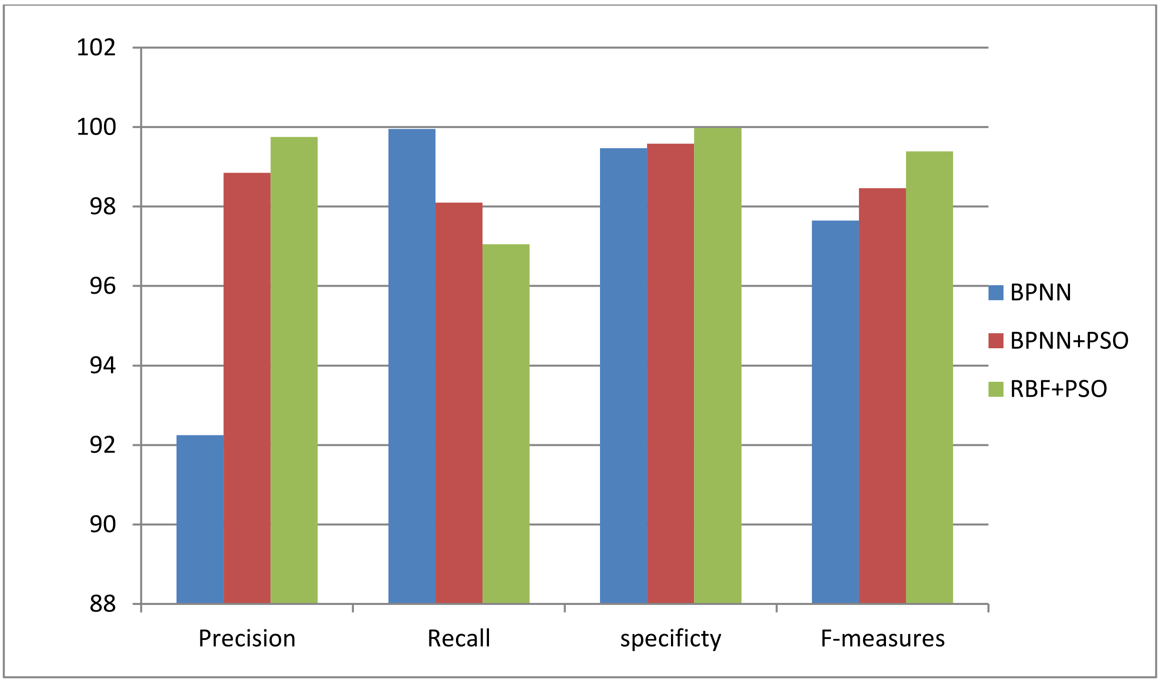
Performance metrics for normal



1.4 performance metrices for normal

PERFORMANCE METRICES	**BPNN**	**BPNN+PSO**	**RBF+PSO**
Precision	95.71	96.71	97.15
Recall	97.78	96.61	95.45
Specificity	93.81	95.41	97.82
F-Measures	97.65	98.15	98.9

Performance metrics for TCP SYN flood attack



1.5 performance metrices for TCP-SYN flood attack

PERFORMANCE METRICES	**BPNN**	**BPNN+PSO**	**RBF+PSO**
Precision	92.25	98.85	99.75
Recall	99.95	98.01	97.05
Specificity	99.47	99.58	99.98
F-Measures	97.65	98.46	99.39

VI.Conclusion

The RBF algorithm is integrates with PSO to choose the optimal weights for the neural network in order to achieve a high level of accuracy in the classification and detection process. Our aim is to achieve low false rate of the proposed model in detecting DDoS attacks in virtual cloud environment. The proposed RBF with PSO detection scheme has been used to monitor, detect and classify the traffic exchange between virtual machines. In addition, our proposed algorithm has been trained and tested with a new generated dataset to identify DDoS attack in cloud environments. Our proposed work it will achieve high detection accuracy and efficiency comparatively.

REFERENCE

1. Masdari, M., and Jalali, M.: ‘A survey and taxonomy of DoS attacks in cloud computing’, Security and Communication Networks, 2016, 9, (16), pp. 3724-3751
2. Kennedy, J., and Eberhart, R.: ‘Particle swarm optimization’, in Editor (Ed.)^(Eds.): ‘Book Particle swarm optimization’ (IEEE, 1995, edn.), pp. 1942-1948
3. Rawashdeh, A., Alkasassbeh, M., and Al-Hawawreh, M.: ‘An anomaly-based approach for DDoS attack detection in cloud environment’, International Journal of Computer Applications in Technology, 2018, 57, (4), pp. 312-324
4. Kushwah, G.S., and Ranga, V.: ‘Voting extreme learning machine based distributed denial of service attack detection in cloud computing’, Journal of Information Security and Applications, 2020, 53, pp. 102532
5. Wani, A.R., Rana, Q., Saxena, U., and Pandey, N.: ‘Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques’, in Editor (Ed.)^(Eds.): ‘Book Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques’ (IEEE, 2019, edn.), pp. 870-875
6. He, Z., Zhang, T., and Lee, R.B.: ‘Machine Learning Based DDoS Attack Detection from Source Side in Cloud’, in Editor (Ed.)^(Eds.): ‘Book Machine Learning Based DDoS Attack Detection from Source Side in Cloud’ (2017, edn.), pp. 114-120
7. Idhammad, M., Afdel, K., and Belouch, M.: ‘Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest’, Security and Communication Networks, 2018, 2018
8. Hezavehi, S.M., and Rahmani, R.: ‘An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments’, Cluster Computing, 2020, pp. 1-19
9. Sahi, A., Lai, D., Li, Y., and Diykh, M.: ‘An efficient DDoS TCP flood attack detection and prevention system in a cloud environment’, IEEE Access, 2017, 5, pp. 6036-6048
10. Chen, Z., Jiang, F., Cheng, Y., Gu, X., Liu, W., and Peng, J.: ‘XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud’, in Editor (Ed.)^(Eds.): ‘Book XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud’ (IEEE, 2018, edn.), pp. 251-256
11. Kesavamoorthy, R., and Soundar, K.R.: ‘Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system’, Cluster Computing, 2019, 22, (4), pp. 9469-9476
12. Velliangiri, S., and Pandey, H.M.: ‘Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms’, Future Generation Computer Systems, 2020

13. Prathyusha, D.J., and Kannayaram, G.: ‘A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment’, Evolutionary Intelligence, 2020, pp. 1-12
14. Rabbani, M., Wang, Y.L., Khoshkangini, R., Jelodar, H., Zhao, R., and Hu, P.: ‘A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing’, Journal of Network and Computer Applications, 2020, 151, pp. 102507
15. Latif, R., Abbas, H., and Latif, S.: ‘Distributed denial of service (DDoS) attack detection using data mining approach in cloud-assisted wireless body area networks’, International Journal of Ad Hoc and Ubiquitous Computing, 2016, 23, (1-2), pp. 24-35
16. Zareapoor, M., Shamsolmoali, P., and Alam, M.A.: ‘Advance DDOS detection and mitigation technique for securing cloud’, International Journal of Computational Science and Engineering, 2018, 16, (3), pp. 303-310
17. Xu, Y., Sun, H., Xiang, F., and Sun, Z.: ‘Efficient DDoS Detection Based on K-FKNN in Software Defined Networks’, IEEE Access, 2019, 7, pp. 160536-160545
18. Velliangiri, S., Karthikeyan, P., and Vinoth Kumar, V.: ‘Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks’, Journal of Experimental & Theoretical Artificial Intelligence, 2020, pp. 1-20
19. Zekri, M., El Kafhali, S., Aboutabit, N., and Saadi, Y.: ‘DDoS attack detection using machine learning techniques in cloud computing environments’, in Editor (Ed.)^(Eds.): ‘Book DDoS attack detection using machine learning techniques in cloud computing environments’ (IEEE, 2017, edn.), pp. 1-7