

Detection of DDoS Attack Using Machine Learning Algorithm in Cloud Computing

D.Radhika¹, S.Kanimozhi²

¹ Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, Namakkal, Tamilnadu, India, radhika@vcew.ac.in

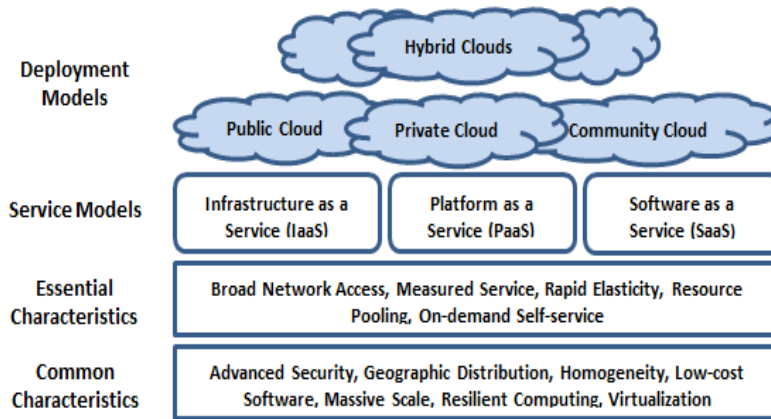
² P.G.Scholar, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, Namakkal, Tamilnadu, India, m.s.kanimozhi98@gmail.com

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 disturb to their services. Traditional defence mechanisms, such as firewalls, are unable to detect insider attacks. This work proposes an DDoS detection approach in the hypervisor layer to discourage DDoS activities between virtual machines. 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 performance analysis and results of our proposed approach detect and classify the DDoS attacks in the cloud environment with minimum false alarms and high detection accuracy.

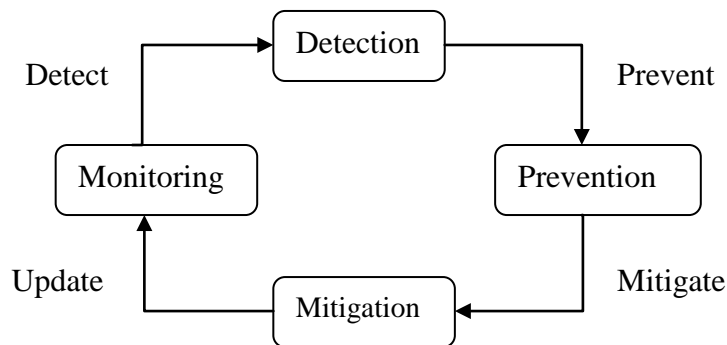
Keywords: distributed denial of service, DDoS, radial basis function, artificial neural network, back propagation neural network.

1 introduction

Cloud computing is the delivery of different services through the internet. Many industries moving to cloud computing technologies due to its ease of use. It is the effective way to minimise infrastructure cost. Cloud services are used anywhere at any time, users can able to pay per use. Cloud computing technology is easy to scale up. 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]



Cloud computing security it was a challenge to the service providers. Distributed denial of service (DDoS) attack it was one of the biggest challenge in cloud computing security. DDoS attack occurs when the attacker trying to disturb the normal transformation process, attacker will turn normal data packets 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.



Machine learning it is a field of artificial intelligence. Machine learning gives a way to train algorithms itself. Using simple mathematical calculations the algorithms learn and grow it. Artificial neural network (ANN) it was a subfield of machine learning.

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

Related works

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. CIDDS-001 (Coburg Intrusion Detection Dataset) is an up-to-date labelled flow-based dataset.] 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. proposed an anomaly-based detection of DDoS attack methods in cloud environment using a third party auditor (TPA). 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 protect the 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. Extract statistical features of four DDoS attacks and launch real attacks in lab settings for evaluation. 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 low rate of false negative	Anomaly	Application layer	Cloudsim + TPANGND Detector
[9]	-	High detection accuracy	-	TCP flood attack	Wireshark Network Analyzer
[10]	XGBoost classifier +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	OpenStock

				attacks	
[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 cost and Faster detection rate	Signature	-	Wireshark

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. 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 with Particle Swarm Optimization

Proposed work

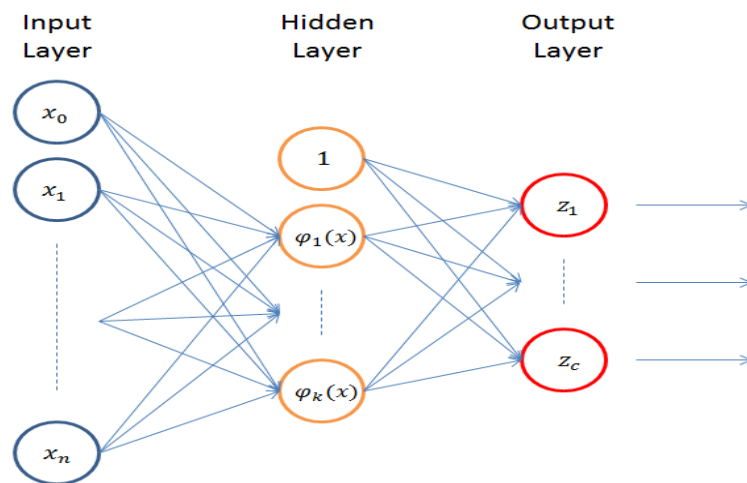
In this work we undertake the detection process of DDoS attack that was affect the normal data traffic in cloud. The proposed RBF with PSO (RBF-PSO) algorithm monitor and detect the flood attack in network.

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.

Radial basis function:

Radial Basis Function (RBF) is a feed forward neural networks model with good performance and global approximation. In RBF have three layers, such as input layer, hidden layer, output layer. In hidden layer, it contains node is called 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.



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 position to 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.

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