Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 8, 2020

Detection of DDoS Attack in Cloud Computing using an Artificial Intelligence Based Approaches

[1]R.Renuga Devi, [2]*N.Umamaheswari

[1,2,] Department of Computer Science,
Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, Tamilnadu, India,
*Email: [1]nicrdevi@gmail.com, [2]umatag@gmail.com

Received: 23 Feb 2020 *Revised: 22 Mar 2020* *Accepted: 15 Apr 2020*

ABSTRACT

Cloud computing is the services of computer system resources such as data storage and computing power. The security issue of cloud computing is major task in order to make efficient services. Among the various security issues, the distributed denial of service (DDoS) is a very complicated security issue that makes traffic during the resource sharing in a cloud environment. Hence, the detection of DDoS is significant tasks in order to make more efficient resource sharing of the end user. Detection mechanism can manage the computers and networks from unauthorized access of resources in a cloud environment. Building an efficient detection system is challenging tasks. Hence, this paper conducting a comprehensive review related to DDoS attack detection methods.

Keywords: Cloud Computing, Security, Distributed Denial of Services (DDoS), Detection methods, Artificial Intelligence

DOI: http://dx.doi.org/10.31838/jcr.07.08.470

INTRODUCTION

The cloud computing has gained tremendous popularity due to outsourcing computation and providing storage requirements based on the user availability. The cloud computing provides the following salient features including on-demand self service, broad network access, resource pooling, rapid elasticity and measured services [1]. The cloud computing is organized into three categories based on the services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The deployments of cloud computing are private, public and multi or hybrid cloud models. Microsoft, IBM, Google, and Amazon are most leading cloud service provider (CSP) in order to provide an efficient service in the recent years.

The security issues are major issues and challenging task in the cloud computing environment. Among the security issues, distributed denial of service (DDoS) is very important security issues in a cloud environment [2]. It is any event or malicious behavior that diminishes or prevents a cloud's capacity in order to perform its expected functions and services. DDoS attacks caused economic loss, downtime, and short and long time effects on the victim CSP. DDoS attack is more powerful that the attacker creates a defense force in order to attack in the form of zombies or bots. All these bots are trained to attack on the victim and cripple down the functionality of the victim. They use the property offer by the CSP and try to flood them. DDoS can be classified into two categories such as brute-force and semantic.

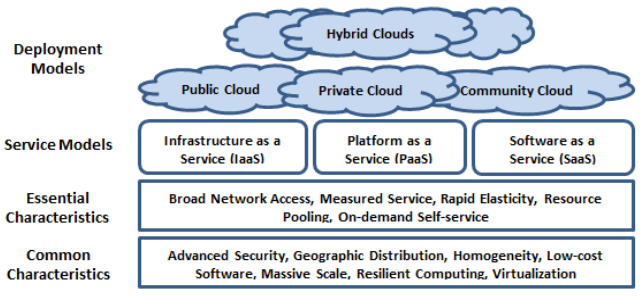

Fig.1. Architecture of cloud computing

A. High rate DDoS attack

The brute force attack also known as high rate or flooding attack. The attackers send an enormous amount of malicious demand to disturb the network bandwidth of the specific cloud server. The disruption of connectivity is caused by killing the router processing ability, network bandwidth ability. The high rate attack is called a transport level flooding attack or network. Transmission Control Protocol (TCP) [3], User Datagram Protocol (UDP) flood, and the Internet Control Message Protocol (ICMP) flood are the example of high rate attacks. The cloud service unavailability to the legitimate users is achieved by killing the server resources like memory, disk, and CPU. These attacks are called as the application level attack, including Hypertext Transfer Protocol (HTTP) flood attack [4], Domain Name System (DNS) flood attack, and the Simple Mail Transfer Protocol (SMTP) flood.

The attackers begin such attacks by developing the vulnerability of an enormous amount of computers in order to generate attack armies called a botnet. The attacker can create the control, then passed by the attacker to the cloud server, which is forwarded to the numerous cooperate hosts. The cooperate hosts forward the flood of needs to target one or more cloud servers. The botnet computer system may use IP spoofing scheme in order to initiate DDoS attacks to hide the true source. Hence, an identifying the authentic location of the attacker is a demanding and essential task.

B. Low-rate DDoS attack

Semantic attack also called as vulnerability attack or low rate attack that exploits the protocol weakness. The attackers send a low volume of malicious traffic to target application. The finding the lowest rate attack is very challenging and crucial task compared with high rate attacks. Compared with high-rate DDoS attack, the low-rate DDoS attack is a complicated attack and difficult to detect because of its low-rate traffic and silent behavior. Since the attacker sends malicious requests at an extremely low rate and its hidden by the traffic volume based defense mechanisms.The attack influences the Quality-of-Service (QoS) qualified by the legitimate user rather than discontinuing the cloud services. The shrew attack, Reduction of Quality (RoQ) attack, Low-Rate DOS attack, and Economic Denial of Sustainability (EDoS) attack are four kinds of low-rate attacks.

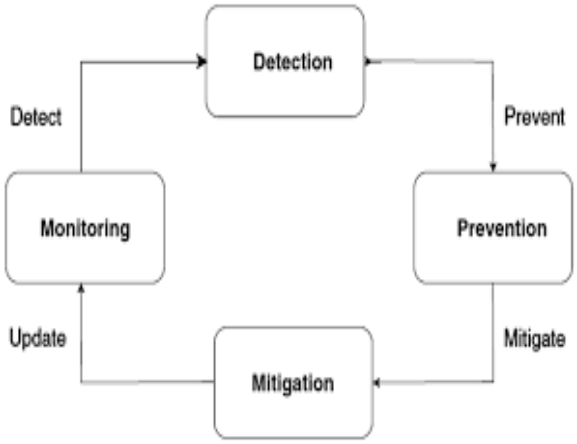

Fig. 2. Life Cycle of DDoS attack.

Life cycle of DDoS attack

DDOS attack has four phases such as monitoring, detection, prevention, and mitigation which is shown in Figure 2 [5]. Monitoring phase is used to capture significant information about the network or host. Detection phase is analyzing the captured network traffic to recognize the malicious attempt. Prevention phase is used to protect the cloud service and resources from developing some applications at different location. Finally, the mitigation phase is the computedseverity of attack and takes precise action in order to manage its impacts. The outcome of the mitigation phase is forwarded to the prevention phase for updating the preventive measures. Among the four phases, this paper conducting a comprehensive review for detection phase only.

Detection of DDoS attack

The DDoS is a very difficult security issue that makes traffic during the resource sharing in a cloud environment. Hence, the detection of DDoS is significant tasks in order to make more efficient resource sharing to the end user [6]. DDoS attacks detection techniques can be broadly categorized into two methods, including signature-based detection methods [6] and anomaly-based detection method [7]. The signature based detection method capture the network traffic that captured network traffic is compared with well-defined attack patterns, including packet sequence or byte. This kind of detection schemes is very easy to understand, develop and provide more significant results compared with anomaly based detection methods. However, the signature-based detection scheme can recognize only known attack that the pattern is pre-defined. The anomaly based detection scheme is used to detect the attack with the help of behavioural patterns. This detection scheme can identify the unknown attack. However, it does not provide low accuracy. The detection mechanism is classified into several categories according to [8].

Virtual machine based, pattern matching and fingerprinting, filtering-based, entropy based, change point detection-based, data mining based, feature section based detection schemes. In this paper, the authors conducting brief survey on detection method using artificial intelligence algorithm. Hence, there are many artificial intelligence approaches are used to detect the DDoS attack in a cloud environment such as support vector machine (SVM) [9], random forest (RF) [4], naive bayes (NB) [6], decision tree (DT), artificial neural network (ANN) [10] , k-nearest neighbors (KNN) classification [11] , convolutional neural network (CNN) [12], particle swarm optimization (PSO).

Related works

Idhammad et al. (2018) [4] present detection system for HTTP DDoS attacks by using Information Theoretic Entropy (ITE) and RF ensemble machine learning method. A time-based sliding window technique is used to calculate the entropy of the network header features of the incoming network traffic. Saied et al. (2016) [10] presented a detect and mitigate known and unknown DDoS attacks in realtime environments using ANN algorithm in order to detect DDoS attacks based on particular distinctive features that split DDoS attack traffic fromlegitimatetraffic.Kumar et al. (2012) adaptive hybrid neuro-fuzzy systems based detection method is proposed for detecting the DDoS attack in a cloud environment [13]. The proposed NFBoost method is obtain by combining ensemble of classifier outputs and Neyman Pearson cost minimization strategy in order to obtain the final classification decision.

Dwivedi et al. (2020) propose a new grasshopper optimization algorithm (GOA) with a machine learning algorithm (GOIDS) [14]. The proposed approach is performed based on creating an intrusion detection system (IDS) in order to accomplish the requirements of the monitored situation and able to distinguish between an attack and normal traffics. Additionally, GOIDS is extracting the most appropriate features from the original IDS dataset that can facilitate to make out typical low-speed DDoS attacks. Then, the selected features are considered as inputs to the classifiers. The SVM, DT, NB, and MLP are used to recognize the attack made in the network.

Latif et al. (2016) [15] propose new a detection method for distributed victim based DDoS attack based on a very fast decision tree (VFDT) learning scheme in cloud-assisted Wireless Body Area Network (WBAN). The proposed scheme achieved higher accuracy for a DDoS attack, reduced false positive and false negative ratio. Velliangiri et al. (2020) [16] proposed a new detection method for detecting the DDoS attack by using an effective fuzzy and the taylor-elephant herd optimization (FT-EHO) inspired by the deep belief network (DBN) classifier uses Taylor series and elephant heard optimization algorithm combined with a fuzzy classifier for rules learning.

Prathyusha et al. (2020) [17] This paper proposes a new DDoS detecting system the use of artificial immune systems by identifying the most significant features of the attack. This proposed detecting method is capable of detecting the threats and responding along with the behaviour of the biological resistance mechanism. Meng Wang et al. (2019) [18] propose a multilayer perceptrons (MLP) combined sequential feature selection in order to choose the best possible features during the training phase. Then, the feedback mechanism is designed to rebuild the attack detector when perceiving significant detection errors dynamically.

Mahdi Rabbani et al. (2019) [19] propose a new attack detector using PSO based probabilistic neural network (PSO-PNN). First, the user behvaiour is converted into meaningfully an understandable format. Then, classified and identified the malicious behaviours by using a multi-layer neural network. Punitha et al. (2020) [20] propose a new centralized cloud information accountability; integrity with imperialist competitive key generation algorithm (CCIAI-ICKGA) is used for hacking by attackers. Also, the proposed method can detect the attack and monitor the practical utilization of the users' information. Cipher text-policy attribute-based encryption (CP-ABE) with key generation utilizes ICKGA and trapdoor generator is used to produce the private and public private keys for every user. Then, the trapdoor generator makes sure data integrity of the user data at both the cloud server and user level. Finally, a dynamically weighted ensemble neural network (DWENN) classifier is used to detect the DDoS attack with more power.

Bhushan et al. (2018) present the flow table-space of a switch by using queuing theory based mathematical model [21]. The flow-table sharing scheme is used to protect the software defined network (SDN) -based cloud from a flow table overloading DDoS attacks. The proposed scheme is an increase the fighting of the cloud system against DDoS attacks with least participation of the SDN controller. YUHUA XU et al. [22] presented a DDoS detection method based on K-MeansCC and Fast K-Nearest Neighbors (K-FKNN).

Table 1. Performance comparisons of DDoS attack detection algorithms

Ref No.	Year	Detection Methods	Datasets	Merits	Demerits
Idhammad et al. [4]	2018	ITE and RF	CIDDS-001 public dataset	High detection accuracy	Computational complication
Polat et al. [9]	2020	SVM based on feature selections	User extracted data	Reduce detection time	Accuracy is disturbed
Saied et al. [10]	2016	ANN	User extracted data	High detection accuracy	Learning process is low
Amjad et al.[11]	2019	NB and Random Forest	User extracted data	Enhance the detection accuracy	Processing time is high
Ghanbari et al. [12]	2020	CNN	CAIDA	High accuracy	Computational complexity
Kumar et al. [13]	2012	NFBoost	KDD Cup, CAIDA, UCI, SSE Lab and SSENET	High detection accuracy	Processing time is high
Dwivedi et al. [14]	2020	GOIDS	KDD Cup 99 and CIC-IDS 2017	High detection and accuracy with a low false–positive rate	Computational complexity
Latif et al. [15]	2016	VFDT	Synthetic and real datasets	Higher accuracy for DDoS attack, reduced false positive and false negative ratio.	Disturbed accuracy
Velliangiri et al. [16]	2020	FT-EHO+DBN	KDD cup	High accuracy, detection rate, precisionand recall	Computational complexity
Prathyusha, D.J et al. [17]	2020	Artificial Immune Systems	KDD cup	High detection accuracy and low false alarm rate.	More complex to develop for real time use cases
Wang et al. [18]	2020	MLP + Feature selection	ISOT, ISCX collected from author campus network	Reduce detection error with higher detection accuracy	Over fitting / under fitting
Rabbani et al. [19]	2020	Hybrid PSO+PNN	UNSW-NB15	Monitoring and recognition of malicious behaviours	Premature convergence
Punitha et al. [20]	2020	Data integrity + DWENN	User extracted data	Enhance detection accuracy using security	High computation cost
Bhushan et al. [21]	2019	flow table-space	User extracted data	Very low communication overhead	Accuracy is low

Table 2. Performance comparisons of DDoS attack detection algorithms (Continue…)

Ref No.	Year	Detection Methods	Datasets	Merits	Demerits
Yuhua Xu et al. [22]	2019	K-FKNN	User extracted data	Higher detection accuracy with high precision	Local optima
Zereapoor et al. [23]	2018	Hope-count algorithm	syntactic dataset and CAIDA	High accuracyrequires very small storage.	Computational complexity
Kesavamoorthy et al. [24]	2018	Multi-agent PSO	User extracted data	Detection accuracy is high	Premature convergence
Wani et al. [25]	2019	Support Vector Machine	SNORT	High detection rate	Premature convergence
Velliangiri et al. [26]	2020	TEHO-DBN	User extracted data	High detection accuracy	Processing time is high
Zecheng He et al [27]	2017	Machine learning algorithm	User extracted data	High detection accuracy	Computation complexity

The detailed experiments are conducted in order to evaluate the system performance and experimental investigation show that the K-FKNN enhances the detection accuracy with high precision and stability of DDoS. Amjad et al. (2019) [11] presented a detecting and preventing the DDoS attack using machine learning algorithm including NB and RF.Zareapoor et al. (2018) [23] present a method to detect and mitigate DDoS attacks in cloud computing. The proposed detection method requires extremely small storage and has the ability of rapid detection. However, the proposed detection method produced high accuracy with 97%.

Kesavamoorthy et al. (2018) developed a new DDoS detection method using autonomous multi agent system and the agents use the PSO algorithm for strong communication and accurate decision making [24]. The proposed detection method analyzed by the coordinating agent using the entropy and covariance technique to verify for the DDoS attacks.Wani et al. (2019) [25] proposed a new detection method based on SVM in order to detect the DDoS attack in the cloud environment. The proposed scheme is compared with NB and RF. Polat et al. (2020) proposed DDoS attacks in SDN were detected using machine learning-based models [9]. The feature selection algorithm is

used to create optimal features. The selected features are trained and tested with SVM, Naive Bayes (NB), ANN, and KNN classification models.

The experimental results recommended that feature selection based detection algorithm can carry out better results in the detection of DDoS attacks in SDN with capable of processing loads and processing times. Ghanbari et al. (2020) proposed an anomaly detection scheme for enhancing the detection rate of a DDoS attack in a smart grid [12]. The detection rate is enhanced by using classification methods with training and testing phases of the CNN. Velliangiri et al. (2020) propose a new DDoS detecting system in a cloud environment using deep learning-based classifier [26]. The users collected and grouped features that are considered as input to the classifier. The classifier is used a Taylor-Elephant Herd Optimization based Deep Belief Network (TEHO-DBN) for the DDoS attack detection.

Rawashdeh A et al. (2018) [7] were developed DDoS detection method using BPNN based PSO. The proposed method can manage the hypervisor layer to discourage DDoS attack and produced high detection accuracy compared with conventional BPNN. But, the discussed research work is using the PSO algorithm for weight adjustment of BPNN. On the other hand, the PSO algorithm has many shortcomings including the problem of premature convergence and need more parameter tuning. Zecheng He et al. (2017) propose a DDoS attack detection scheme based on the source side in the cloud environment using machine learning techniques [27]. The nine machine learning algorithm is discussed and compared in order to detect the DDoS attack in the cloud environments.

Discussion

Merits and demerits of the surveyed papers are discussed in Table-1 and Table-2. From the Tables, it has mentioned brief discussions about the proposed and compared detection method, benefits and drawbacks of the proposed method, and details of the datasets. However, the existingdetection methods are disturbed to the detection accuracy due to its own shortcomingslike computation complexity, communication complexity, and low accuracy. Hence, building an efficient detection method is a very significant task in order to obtain optimal detection accuracy.

For example, Rawashdeh et al. [7] developed DDoS detection method using BPNN based PSO. The BPNN algorithm has the problem of over fitting or under fitting due to selecting the inappropriate number of hidden neurons. The author has not discussed about this issues. The PSO algorithm is used in this paper for adjusting the weights of BPNN. But, the PSO algorithm also has the problem of premature convergence due to more parameters tuning during learning process. Therefore, more computational time has been taken for completing their learning process. Hence, the recommendation of this paper as future enhancement is to introducing alternative method in order to choosing the appropriate hidden neuron in the hidden layer of BPNN.

Performance measures

In the literature, the robustness of every detection algorithm is analyzed by using the set of common performance metrics. In this section, some essential performance metrics are discussed such as True Negative Rate (TNR), True Positive Rate (TPR), and accuracy. Additionally, service response time, attack detection time, victim service downtime, and estimated time are also discussed.

A. Accuracy

Accuracy is the most important performance metric for evaluating the performance of any detection algorithm.

B. Service response time

Service response time is the major performance measuring metric and it defines the period when a request is sent, and the corresponding response is received by the cloud user

C. Attack detection time

Attack detection time is the third critical metric for evaluating the performance of a detection system and it describe the time when the network traffic is classified as legitimate or malicious.

D. Victim service downtime

Service downtime defines the period during which the victim cloud server becomes unavailable and does not succeed to service the legitimate requests. Hence, the low victim service downtime is considered as a better performance.

E. Total estimated cost

Attack detection and mitigation cost define the total calculated cost associated with a detection system. The cost is calculated based on the utilization of computing, bandwidth, storage, and memory resources.

Challenges of DDoS attack Detections

A recent survey on detection of the DDoS attack scheme is show that various detection techniques are presented in this survey paper as a theory. Indeed, developing and perform a perfect and real-time detection scheme is a hard task. The researchers are faced many issue in order to make the efficient detection scheme due to suffice the growing demands for detection and response.

Detection algorithm is required more computations due to which time taken by the scheme is too long to locate the anomalous conditions. Hence, detection time must be given first choice over detection accuracy for the disclosure of attacks in real-time.

Accurate isolation of DDoS attack traffic and usual flash events real-time updating of network statistics and rapid identification of spoofed IPs is the most demanding task in real-time detection environment.

Detecting DDoS attack is difficult to analyze the encrypted packets because detection methods are analyzed the packet contents and traffic flow characteristics for the attack exposures. However, the detection system has failed due to the malicious user modifies the content of packet and traffic flow traits.

Conclusions

This paper is conducting survey on the detection of DDoS attack in a cloud environment using artificial intelligence approaches. At beginning stage of paper, discussion of security issues in cloud computing. Then, the deep discussion is conducted about the DDoS attacks and its types. This survey considers the detection of DDoS attacks in a cloud computing environment using artificial intelligence approaches with its merits and demerits. The essential parameters for evaluating the performance of any detection algorithms also discussed. This survey paper stimulates the security researchers to build up effective detection algorithm against the DDoS attacks in a cloud environment.

REFERENCES

1. Masdari, M. and M. Jalali, A survey and taxonomy of DoS attacks in cloud computing. Security and Communication Networks, 2016. 9(16): p. 3724-3751.
2. Lee, K., et al., DDoS attack detection method using cluster analysis. Expert systems with applications, 2008. 34(3): p. 1659-1665.
3. Osanaiye, O.A. and M. Dlodlo. TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment. in IEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON). 2015. IEEE.
4. Idhammad, M., K. Afdel, and M. Belouch, Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest. Security and Communication Networks, 2018. 2018.
5. Somani, G., et al., DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 2017. 107: p. 30-48.

6. Osanaiye, O., K.-K.R. Choo, and M. Dlodlo, Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications, 2016. 67: p. 147-165.
7. Rawashdeh, A., M. Alkasassbeh, and M. Al-Hawawreh, An anomaly-based approach for DDoS attack detection in cloud environment. International Journal of Computer Applications in Technology, 2018. 57(4): p. 312-324.
8. Agrawal, N. and S. Tapaswi, Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. IEEE Communications Surveys & Tutorials, 2019. 21(4): p. 3769-3795.
9. Polat, H., O. Polat, and A. Cetin, Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. Sustainability, 2020. 12(3): p. 1035.
10. Saied, A., R.E. Overill, and T. Radzik, Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 2016. 172: p. 385-393.
11. Amjad, A., et al., Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm. EAI Endorsed Transactions on Scalable Information Systems, 2019. 6(23).
12. Ghanbari, M. and W. Kinsner, Detecting DDoS Attacks Using Polyscale Analysis and Deep Learning. International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), 2020. 14(1): p. 17-34.
13. Kumar, P.A.R. and S. Selvakumar, Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Computer Communications, 2013. 36(3): p. 303-319.
14. Dwivedi, S., M. Vardhan, and S. Tripathi, Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. International Journal of Computers and Applications, 2020: p. 1-11.
15. Latif, R., H. Abbas, and S. Latif, 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): p. 24-35.
16. Velliangiri, S. and H.M. Pandey, 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.
17. Prathyusha, D.J. and G. Kannayaram, A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment. Evolutionary Intelligence, 2020: p. 1-12.
18. Wang, M., Y. Lu, and J. Qin, A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Computers & Security, 2020. 88: p. 101645.
19. Rabbani, M., et al., A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. Journal of Network and Computer Applications, 2020. 151: p. 102507.
20. Punitha, A.A.A. and G. Indumathi, A novel centralized cloud information accountability integrity with ensemble neural network based attack detection approach for cloud data. Journal of Ambient Intelligence and Humanized Computing, 2020: p. 1-12.
21. Bhushan, K. and B.B. Gupta, Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. Journal of Ambient Intelligence and Humanized Computing, 2019. 10(5): p. 1985-1997.
22. Xu, Y., et al., Efficient DDoS Detection Based on K-FKNN in Software Defined Networks. IEEE Access, 2019. 7: p. 160536-160545.
23. Zareapoor, M., P. Shamsolmoali, and M.A. Alam, Advance DDOS detection and mitigation technique for securing cloud. International Journal of Computational Science and Engineering, 2018. 16(3): p. 303-310.
24. Kesavamoorthy, R. and K.R. Soundar, Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system. Cluster Computing, 2019. 22(4): p. 9469-9476.
25. Wani, A.R., et al. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. in 2019 Amity International Conference on Artificial Intelligence (AICAI). 2019. IEEE.
26. Velliangiri, S., P. Karthikeyan, and V. Vinoth Kumar, Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. Journal of Experimental & Theoretical Artificial Intelligence, 2020: p. 1-20.
27. He, Z., T. Zhang, and R.B. Lee. Machine Learning Based DDoS Attack Detection from Source Side in Cloud. in 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). 2017.