Indian Journal of Science and Technology, *Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/93175, September 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment

B. S. Kiruthika Devi* and T. Subbulakshmi

School of Computing Science and Engineering, VIT University Chennai - 600127, Tamil Nadu, India; kiruthikadevi.bs2015@vit.ac.in, research.subbulakshmi@gmail.com

Abstract

Cloud security is of the major concern in the deployment and protection of cloud deployment models. In this paper, detailed investigations on the recent DDoS attacks and comparative analysis of the various DDoS security solutions in the cloud computing environment are carried out. The comprehensive study of the cloud DDoS solutions clearly exemplifies the techniques, deployment layer, benchmark datasets, tools and performance metrics. The Cloud DDoS Detection and defense model using learning algorithms is designed to protect the cloud infrastructure considering the pitfalls in the existing procedures for real world problems. The model is based on anomaly detection and thus it is capable of protecting the public/private cloud from zero-day attacks. The availability of the cloud applications is improved significantly by defending cloud DDoS attacks and offers high quality of services to the legitimate users.

Keywords: Cloud Computing, DDoS, Detection, Defense, Security

1. Introduction

Cloud computing provides resource provisioning on demand through computer network. Users can use the cloud services and process their task without acquiring the software and hardware. With the introduction of the cloud deployment models users can choose any kind of services/applications. The cloud deployment models are categorized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS provides the computing facilities, PaaS provides the cloud platform and SaaS provides the software for the cloud applications.

The basic idea of the cloud is that any computer in the cloud is connected to set of computing resources to aid in storing the files, operating with remote servers and processing any cloud application. Since cloud environment is a multi-user and distributed architecture the security implications are raising along with the cloud deployment. The major security issues of cloud computing are availability, integrity and confidentiality. The security in the cloud is achieved by providing authentication and access control using digital certificates[1].

Inspite of the security, Distributed Denial of Service (DDoS) attacks are a kind of powerful attack that affects the availability of cloud applications and services. Large amount of illegitimate traffic targeted at the cloud server tampers the cloud resources such as bandwidth and connectivity.

2. DDoS Attacks

Distributed Denial of Service (DDoS) attacks still remains challenging problem in the area of cloud security. DDoS attack is highly complicated because of its complex and aggressive kind where a botmaster owns insecure nodes to target cloud services as shown in Figure 1. This attack devastates cloud servers by deliberately injecting malicious packets on the cloud to rapidly devour critical resources. DDoS attackers are using

Author for correspondence

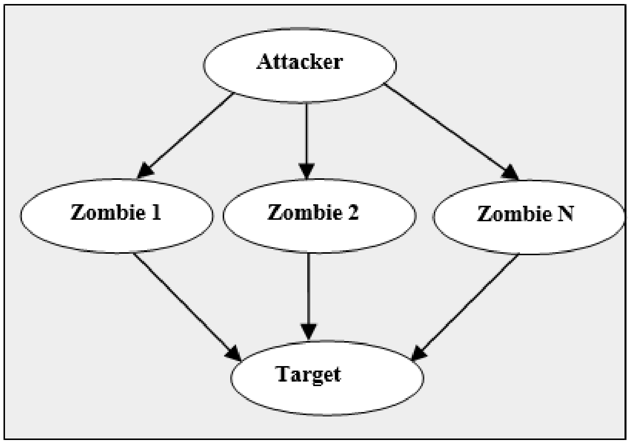

Figure 1. DDoS attack scenario.

much sophisticated tools to easily collapse and interrupt the normal functioning of cloud services. The DDoS targets are shockingly government organizations, financial companies, defense and military departments. Major sites like facebook and ebay etc., suffered from DDoS attacks denying access to legitimate users, service disruption and financial loss[2].

Insecure machines in the cloud can be compromised by DDoS attacks without even knowing the fact that they are in control of botmaster and targets the critical server upon receiving the instruction in order to execute DDoS attack. The widely available DDoS attack can be utilized for the very purpose of launching a powerful attack without the need of technical knowledge nor its consequences. DDoS attacks are classified into two types namely bandwidth and resource depletion attacks. Bandwidth depletion happens when large volume of traffic is witnessed at the victim server consuming the bandwidth and dropping legitimate requests. Resource depletion occurs when the server resources are exhausted by processing malicious requests and blocking genuine requests. UDP attack is one kind of bandwidth depletion attack where the connection does not require acknowledgment and sends flooding traffic at the larger scale to consume the bottleneck link with malicious packets. Similarly, TCP SYN attack is one kind of resource depletion attack where attackers send TCP SYN requests continuously and server allocates resources for the requests. The client never sends the final ACK leaving half open connections at the server. The major resources that are influenced by DDoS attacks are host and network resources such as CPU usage, memory usage, link utilization, throughput and Latency[3]. The degradation of their performance justifies the ongoing attack which can trigger a DDoS defense system to act in such way that the effects are minimized and system can be restored to its normal functionality.

3. Challenges

DDoS attacks are popular in the area of cloud security and the availability of advanced tools is an alarming threat to cloud vendors. Despite the existence of security technologies, arriving at a comprhensive solution to DDoS problem is challenging. Few challenges that the research community faces to provide DDoS solution are briefed[4–7] as below.

- Open Architecture- DDoS tools are deployed at the attacker machines to execute high rate flooding attacks. The openness and collaborative architecture of the internet is exploited to pollute the machines and internetworked devices. The healthy network is maintained if and only if the polluted machines are removed and repaired so that infection to other connecting nodes can be prevented.
- Server Resources- The major resources that are severely attacked when DDoS attack happens are CPU, memory and bandwidth. The server allocates resources to malicious requests and the connections are open till the session expires. Due to the processing of malicious requests the access to legitimate sources are denied.
- High Speed- DDoS attack is distributed where the number of nodes, attack intensity, protocol and other attack parameters are unpredictable. The defense solutions must be highly reactive so as to block the malicious traffic in the high speed networks.
- Classification of legitimate and malicious traffic- The bottleneck link is occupied by attack packets at the buffer queue when the rate of attack intensity is exponentially high compared to legitimate. Without a classification method, it is difficult for the server to decide to whom the resources are to be allocated.
- Datasets- The DDoS solutions require rigorous testing for their standards before real time deployment. Non-availability of standard datasets and the testing platform are the current issues challenged.
- Attack Signatures- Maintaining a comphrensive list of DDoS attack signatures that widely covers all the variants are infeasible in real time. Also, the traffic behavior depends on the target network and may be behave very differently when deployed in some other cloud network.

4. DDoS Tools

The popular DDoS tools that are available in the internet are Trinoo, Tribe flood network, TFN2K, Stacheldraht, Mstream, Shaft, Trinity, Knight, Low orbit canon, High orbit canon and Slowloris. The categorizes of DDoS attack tools[8–17] along with specific protocols and operational layer is shown in Table 1.

5. DDoS Coutermeasures

DDoS countermeasures are classified into three types such as Detection, Mitigation and Defense methods. DDoS detection is highly tedious because of the lookalike pattern of genuine and malicious packets. Unlike, other security attacks, the traffic flows are normal from source and at the intermediate network whereas at the target it becomes high coordinated and intense. An efficient DDoS detection[18] system enables with the classification of genuine and malicious flows. Mitigating techniques throttles the DDoS traffic and reduces the attack effects, whereas defense techniques filters all DDoS flows and provides sufficient bandwidth to legitimate flows. The taxonomy of DDoS countermeasures is shown in Figure 2.

Several detection[19–28], mitigation[29–37] and defense[38–49] strategies for DDoS attack in cloud are compared and tabulated as in Table 2, Table 3 and Table 4. The comparative analysis is categorized based on the techniques, operational layer, dataset, tools used and performance metrics.

Table 1. DDoS tools

DDoS Tools	Protocol	Layer
Trinoo[8]	UDP	Transport
Tribe Flood Network[9], Tribe Flood Network 2000[10], Stacheldraht[11], Shaft[12]	UDP, ICMP, SMURF and TCP SYN	Network and Transport
Mstream[13]	TCP ACK	Transport
Trinity[14]	TCP random flag, TCP RST, TCP established and TCP fragment	Transport
Knight[15]	UDP, SYN and urgent pointer flood	Transport
Low Orbit Ion Cannon[16]	TCP, UDP, HTTP	Application and Transport
High Orbit Ion Cannon[16], Slowloris[17]	HTTP	Application

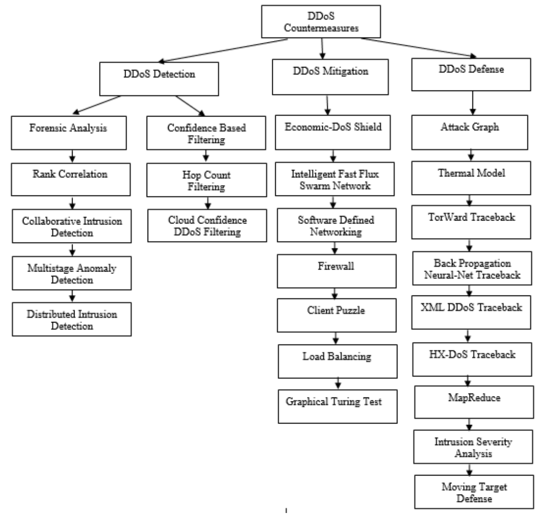

Figure 2. DDoS taxonomy.

6. Proposed Model

The proposed model comprises of two major components namely DDoS Attack Generation System and DDoS System as shown in Figure 3. Attack generation system is used to deploy any cloud DDoS attack scenario by designing the attack scenario, identifying hardware/software requirements, choice of DDoS attack scripts/tools, selection of virtual nodes, defining attack parameters and strength of attack. Designing the attack scenario involves the network topology of the cloud model that is being investigated. Before designing the major task is to decide whether it is public, private or hybrid cloud model. Based on the network model the software/hardware requirements[50] and operating platform are chosen. DDoS tools are abundant and the characteristics of each tool are well enumerated in the literature. The next step is to select the number of virtual nodes that are involved in the attack and define the attack parameters such as time, duration, protocol and rate. Based on the attacking parameters the strength of attack is determined. The researchers propose the attack scenario inorder to monitor, detect and defend cloud DDoS attacks[51] by gathering real time traces.

Hence, the DDoS Attack Response System consists of various modules such as monitoring, data collection, data pre-processing, learning/analyzer model, alert events and filtering. The online monitoring of DDoS performance

Table 2. DDoS detection techniques

Technique used	Layer	Dataset	Tools	Performance Metrics
Forensic Analysis[19]	Network	CNSMS	NA	NA
Confidence-based filtering[20]	Network	MAWI Working Group Traffic Archive	Attack tools, net-filter, C++	False Positive Rate, False Negative Rate and Process Time
Rank Correlation[21]	Network	Simulated	ns2	NA
Collaborative Intrusion Detection[22]	Network	NA	NA	NA
Multistage Anomaly Detection[23]	Network	NA	NA	NA
Distributed Intrusion Detection[24]	Network	NA	NA	NA
Securing Cloud Servers[25]	Network	Simulated	ns2	Detection Rate and False Positive Rate
Intrusion Detection System[26]	Network/ Transport	Simulated	Cloud Simulator and Java	Computation Time and Packets Lost
Detecting Intrusions[27]	Network	Virtual	NA	NA
Statistical-based filtering[28]	Transport	Real Time	Netwag, Jpcap	Accuracy, Detection accuracy, False Alarm Rate and Processing Time

Table 3. DDoS mitigation techniques

Technique used	Layer	Dataset	Tools	Performance Metrics
Cloud-Enabled DDoS Defense[29]	Application	Real Time from Planetlab	Javascript	Effectiveness, Running Time, Maximum Likelihood Estimation, Saved Shuffles
Enhanced EDoS-Shield[30]	Network	Simulated	Discrete Event Simulation Model	Response time Evaluation, Computing Resources Utilization, Cost Evaluation, Legitimate Client Throughput Rate
Mitigating DDoS Attacks[31]	Application	Simulated	Curl loader	Latency
Software-Defined Networking[32]	SDN	Virtual	Floodlight, EC2West, FlowVisor, Snort and iperf	Communication Time
Autonomous Architecture[33]	Network	Virtual	Virtual Firewall	NA
EDoS[34]	Application and Network	Virtual	NA	NA
Hybrid Cloud-Based Firewalling[35]	Network	Virtual	Net filter, virtual firewall and hping3	CPU load, Latency Network and Packet Loss Rate
Enhanced Economical Denial of Sustainability [36]	Network	Virtual	NA	NA
EDoS-Shield[37]	Application	Virtual	Discrete Simulation	Response time Evaluation, Computation Power Utilization, Cost Evaluation and Throughput Rate

Table 4: DDoS defense techniques

Technique used	Layer	Dataset	Tools	Performance Metrics
NICE[38]	Network	Open Source Vulnerability Database (OSVDB),Common Vulnerabilities and Exposures List(CVE) and NIST National Vulnerability Database(NVD)	Open Flow Network Programming API, Snort, Port Scanning, Packet Generator, Network Monitoring Tool	CPU Utilization, Network Capacity, Agent Processing Capacity and Communication Delay
Simulation Study[39]	Network	Simulated	OMNeT++, Zenoss and SNMP	Temperature response and packets dropped/received
TorWard[40]	Network/ Transport	Real time from Planetlab	Open source IDS Suricata, Barnyard2, BASE, ETOpen, ETPro, Deep packet inspection,TShark	Detection Rate and False Positive Rate
HTTP DDoS Detection[41]	Application	Real Time	NetBot,Snort IDS and Wireshark	Detection Rate and Detection Time
Intrusion severity analysis[42]	Network	Computer Programs Cross	Weka	Validation for Dataset, Average Success
Securing cloud[43]	Network	Virtual	Snort, VMwre,honeypot, wireshark	NA
Confidence-Based Filtering [44]	Network	MAWI Working Group Traffic Archive	C++	False Positive Rate, Performance under Different Attack Types and Process
Securing Cloud Computing[45]	Network	DARPA(KDD99) Dataset	NA	Average Legitimate Traffic Detected, Average Attack Traffic
Comber Approach[46]	Application	Virtual	NA	NA
Packet Marking[47]	Application	Virtual	CLASSIE	NA
Moving Target Defense[48]	Application	Virtual	MulVAL	Risk Analysis for Migration Method, Total Attack Cost of deploying OS Diversity, System Risk, Reliability and Probability using Redundancy
Cloud security defence[49]	Application	Virtual	tshark, tcpdump,vmware and VB.Net	Response Time

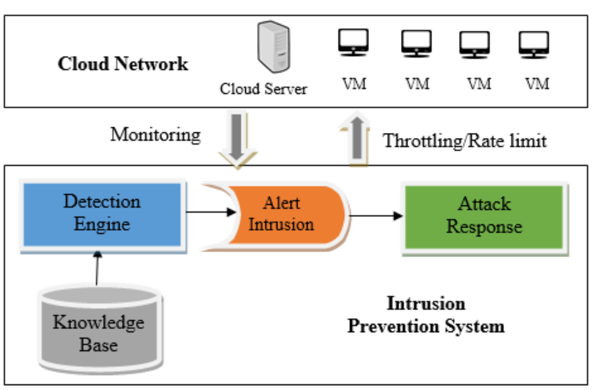

Figure 3. Proposed cloud DDoS detection and defense model.

metrics that combines both host and network performance serve as the indicators for attack diagnosis. The performance metrics considered are CPU usage, Memory usage, Packet loss, Latency, Link utilization and Throughput. The deprivation in DDoS metrics provides first hand report on the cloud network statistics. Data is collected and pre-processed before passing to the learning model. The learning model then discriminates the normal and malicious users with high detection accuracy and low false alarms. The learning model communicates with the knowledge base for detection of any anomalous behavior. The deviations from the matched patterns are alerted to the alerted to the filtering module. Also, new attacks are monitored, analyzed and attack patterns are updated in offline mode to the knowledge base.

6. Conclusion

The article provides a detailed survey on DDoS attack in cloud, challenges, DDoS attack tools, detection, mitigation and defense techniques available in the literature. The comparative analysis of various DDoS countermeasures clearly depicts the recent impact in the cloud environment and motivates the reader to propose effective DDoS solutions for critical infrastructure protection. The proposed work is to be implemented in the private/public cloud and the future research work is to provide DDoS defense solution for cloud computing environment using learning methods.

7. References

1. Manjusha R, Ramachandran R. Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology. 2015 Apr 1; 8(7):1–8.
2. Arora K, Kumar K, Sachdeva M. Impact analysis of recent DDoS attacks. International Journal on Computer Science and Engineering. 2011 Feb; 3(2):877–83.
3. Devi BSK, Preetha G, Shalinie SM. DDoS detection using host-network based metrics and mitigation in experimental testbed. 2012 International Conference on Recent Trends in Information Technology (ICRTIT); Chennai, Tamil Nadu. 2012 Apr 19. p. 423–7.
4. Bhuyan MH, Kashyap HJ, Bhattacharyya DK, Kalita JK. Detecting distributed denial of service attacks: Methods, tools and future directions. The Computer Journal. 2013 Mar 28.
5. Abliz M. Internet denial of service attacks and defense mechanisms. University of Pittsburgh, Department of Computer Science, Technical Report; 2011 Mar.
6. Zaroo P. A survey of DDoS attacks and some DDoS defense mechanisms. Advanced Information Assurance (CS 626); 2002.
7. Sharifi AM, Amirgholipour SK, Alirezanejad M, Aski BS, Ghiami M. Availability challenge of cloud system under DDOS attack. Indian Journal of Science and Technology. 2012 Jun 1; 5(6):2933–7.
8. Dittrich D. The DoS Projects 'trinoo' distributed denial of service attack tool; 1999.
9. Dittrich D. The tribe flood network distributed denial of service attack tool. University of Washington; 1999 Oct 21. p. 10.
10. Barlow J, Thrower W. TFN2K- An analysis. Axent Security Team; 2014 Sep 05.
11. Dittrich D. The 'stacheldraht' distributed denial of service attack tool; 1999 Dec 31.
12. Dietrich S, Long N, Dittrich D. Analyzing distributed denial of service tools: The shaft case. InLISA; 2000 Dec 3. p. 329–39.
13. Dittrich D, Weaver G, Dietrich S, Long N. The "mstream" distributed denial of service attack tool. Available from: http://staff.washington.edu/dittrich/misc/mstream.analysis.txt
14. Hancock B. Trinity v3, a DDoS tool, hits the streets. Computers and Security. 2000 Nov 1; 19(7):574.
15. Bysin. Knight. Csourcecode; 2001.
16. Kenig R, Manor D, Gadot Z, Trauner D. DDoS Survival Handbook; 2013.
17. Snake R, Lee JK, Slowloris R. HTTP DoS. Available from: http://hackers.org/slowloris/
18. Ahamad T, Aljumah A. Detection and defense mechanism against DDoS in MANET. Indian Journal of Science and Technology. 2015 Dec 1; 8(33):1–4.
19. Chen Z, Han F, Cao J, Jiang X, Chen S. Cloud computing-based forensic analysis for collaborative network security management system. Tsinghua Science and Technology. 2013 Feb; 18(1):40–50.
20. Dou W, Chen Q, Chen J. A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems. 2013 Sep 30; 29(7):1838–50.
21. Wei W, Chen F, Xia Y, Jin G. A rank correlation based detection against distributed reflection DoS attacks. IEEE Communications Letters. 2013 Jan; 17(1):173–5.
22. Tan Z, Nagar UT, He X, Nanda P, Liu RP, Wang S, Hu J. Enhancing big data security with collaborative intrusion detection. IEEE Cloud Computing. 2014 Sep; 1(3):27–33.
23. Cha B, Kim J. Study of multistage anomaly detection for secured cloud computing resources in future internet. IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC); USA. 2011 Dec 12. p. 1046–50.
24. Li H, Wu Q. A distributed intrusion detection model based on cloud theory. IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS); Hangzhou. 2012 Oct 30. p. 435–9.
25. Chapade SS, Pandey KU, Bhade DS. Securing cloud servers against flooding based DDoS attacks. International Conference on Communication Systems and Network Technologies (CSNT); Gwalior. 2013 Apr 6, p. 524–8.
26. Aishwarya R, Malliga S. Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment. International Conference on Recent Trends in Information Technology (ICRTIT); Chennai. 2014 Apr 10. p. 1–6.

27. Maqsood R, Shahabuddin N, Upadhyay D. A scheme for detecting intrusions and minimising data loss in virtual networks. International Conference on Computational Intelligence and Communication Networks (CICN); 2014 Nov 14. p. 738–43.
28. Shamsolmoali P, Zareapoor M. Statistical-based filtering system against DDOS attacks in cloud computing. 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI); New Delhi. 2014 Sep 24. p. 1234–9.
29. Jia Q, Wang H, Fleck D, Li F, Stavrou A, Powell W. Catch me if you can: A cloud-enabled DDoS defense. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); GA. 2014 Jun 23. p. 264–75.
30. Al-Haidari F, Sqalli MH, Salah K. Enhanced edos-shield for mitigating edos attacks originating from spoofed IP addresses. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); USA. 2012 Jun 25. p. 1167–74.
31. Lua R, Yow KC. Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network. IEEE Network. 2011 Jul; 25(4):28–33.
32. Yan Q, Yu F. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine. 2015 Apr; 53(4):52–9.
33. Guenane FA, Jaafar B, Nogucira M, Pujolle G. Autonomous architecture for managing firewalling cloud-based service. International Conference and Workshop on the Network of the Future (NOF); Paris. 2014 Dec 3. p. 1–5.
34. Kumar MN, Sujatha P, Kalva V, Nagori R, Katukojwala AK, Kumar M. Mitigating Economic Denial of Sustainability (EDoS) in cloud computing using in-cloud scrubber service. 4th International Conference on Computational Intelligence and Communication Networks (CICN); Mathura. 2012 Nov 3. p. 535–9.
35. Guenane F, Nogueira M, Pujolle G. Reducing DDoS attacks impact using a hybrid cloud-based firewalling architecture. Global Information Infrastructure and Networking Symposium (GIIS); QC. 2014 Sep 15. p. 1–6.
36. Alosaimi W, Al-Begain K. An enhanced economical denial of sustainability mitigation system for the cloud. 7th International Conference on Next Generation Mobile Apps, Services and Technologies (NGMAST); Prague. 2013 Sep 25. p. 19–25.
37. Sqalli MH, Al-Haidari F, Salah K. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. 4th IEEE International Conference on Utility and Cloud Computing (UCC); NSW. 2011 Dec 5. p. 49–56.
38. Chung CJ, Khatkar P, Xing T, Lee J, Huang D. NICE: Network intrusion detection and countermeasure selection in virtual network systems. IEEE Transactions on Dependable and Secure Computing. 2013 Jul; 10(4):198–211.
39. Anwar Z, Malik AW. Can a DDoS attack meltdown my data center? A simulation study and defense strategies. IEEE Communications Letters. 2014 Jul; 18(7):1175–8.
40. Ling Z, Luo J, Wu K, Yu W, Fu X. TorWard: Discovery, blocking, and traceback of malicious traffic over tor. IEEE Transactions on Information Forensics and Security. 2015 Dec; 10(12):2515–30.
41. Choi J, Choi C, Ko B, Kim P. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft Computing. 2014 Sep 1; 18(9):1697–703.
42. Arshad J, Townend P, Xu J. A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems. 2013 Jan 31; 29(1):416–28.
43. Bakshi A, Yogesh B. Securing cloud from DDoS attacks using intrusion detection system in virtual machine. 2nd International Conference on Communication Software and Networks, ICCSN'10; 2010 Feb 26. p. 260–4.
44. Chen Q, Lin W, Dou W, Yu S. CBF: A packet filtering method for DDoS attack defense in cloud environment. 2011 IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC); NSW. 2011 Dec 12. p. 427–34.
45. Joshi B, Vijayan AS, Joshi BK. Securing cloud computing environment against DDoS attacks. International Conference on Computer Communication and Informatics (ICCCI); Coimbatore. 2012 Jan 10. p. 1–5.
46. Karnwal T, Sivakumar T, Aghila G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS); Bhopal. 2012 Mar 1. p. 1–5.
47. Anitha E, Malliga S. A packet marking approach to protect cloud environment against DDoS attacks. International Conference on Information Communication and Embedded Systems (ICICES); Chennai. 2013 Feb 21. p. 367–70.
48. Hong JB, Kim DS. Assessing the effectiveness of moving target defenses using security models. IEEE Transactions on Dependable and Secure Computing. 2016 Mar-Apr 1; 13(2):163–77.
49. Chonka A, Xiang Y, Zhou W, Bonti A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications. 2011 Jul 31; 34(4):1097–107.
50. Tahmassebpour M. Immediate detection of DDoS attacks with using NetFlow on cisco devices IOS. Indian Journal of Science and Technology. 2016 Jul 18; 9(26).
51. Prasad KM, Reddy AR, Rao KV. Anomaly based real time prevention of under rated app-DDOS attacks on Web: An experiential metrics based machine learning approach. Indian Journal of Science and Technology. 2016 Jul 28; 9(27).