Journal of Engineering and Applied Sciences 14 (21): 8114-8120, 2019
ISSN: 1816-949X

A Conceptual Framework for Denial-of-Service Attack Mitigation and Prevention in Cloud Computing

Nancy Awadallah Awad
Department of Computer and Information Systems, Sadat Academy for Management Sciences, Cairo, Egypt rarecore2002@yahoo.com

Abstract: While cloud computing provides various benefits to users, there are also underlying security and privacy risks such as multi-tenancy, resource pooling and shareability features can be exploited by cybercriminals and anyone with a malicious intent. Distributed Denial of Service (DDoS) attacks are considered the main methods to destroy the availability of critical online services they overwhelm the victim with huge volume of traffic and render it incapable of performing normal communication or crashes it completely. This flooding attacks due to that all network resources and operations are blocked all at once. This study discuss some related approaches for mitigating or preventing DDoS attacks for cloud environment. It also presents a conceptual cloud DDoS defense framework based on classifier and change point detection components to compare the traffic and resource usage in normal and attack situations and take a countermeasure action to drop threated packet and alarm administrator.

Key words: DDoS, flooding attack, cloud computing, change point detection, anomaly detection, online services

INTRODUCTION

Cloud computing is a target for many attacks as any other platform. These attacks have various aims such as eavesdropping, destruction, reconnaissance and any action to complete system failure. Denial of Service (DoS) attacks try to render the service unavailable to its authorized users. The attack consumes large amounts of system resources such as processing power, memory and bandwidth. This consumption will leave the service inaccessible to the users or intolerably slow (Alani, 2016).

DDoS attack is considered one of the main threats that the internet and one of the security threats that challenge the availability. It makes use of many different resources to send a lot of useless packets to the target in a short time which will consume the target's resource and make the target's service unavailable. The idea behind launching the attack from multiple location is to make detection much harder.

The flooding DDoS attacks such as (SYN, UDP, DNS, ICMP) flooding can be identified and alleviated by some mechanisms easily cause of the characteristics as flow rate, size of attack packets but still it is difficult to detect and identifies the low-rate DoS attack because the attacker periodically send short burst packets which behave as legitimate traffic to the server (Kumawat and Meena, 2014; Osanaiye *et al*., 2016). Researchers presents several tools that used to facilitate detection DDoS attacks and due to mitigate DDoS in cloud computing environment (Grobauer *et al*., 2011; Deshmukh and Devadkar , 2015). Two contrasts are found in DDoS mitigation technique identified by Wang *et al*. (2015):

- The computational resources and Cloud Provider (CP)
- The resources are shared by users in cloud and network infrastructure

Literature review: Several cases of such DDoS attacks mitigation and prevention in cloud environment have been reported recently. Kumawat and Meena (2014), presented a framework for characterization, identification and mitigation of low-rate DoS attacks which effectively characterize the flows as attack or legitimate, detects the low-rate DoS attack on the basis of characteristics of low rate and mitigate the effect of this by stopping the attack flow near the source.

Osanaiye *et al*. (2016), presented a framework for detecting cloud DDoS change-point to identify statistical anomaly. They trusted that DDoS attack is effective where it expends generous transfer speed and resources which overpowers the objective.

Wang *et al*. (2015) discussed a DaMask which is DDoS attack of cloud guard. It has three layers which are network of switches, controllers and application and two modules (an attack mitigation module-DaMask-M)

and (anomaly based network attack detection module-DaMask-D). An alert is issued once DaMask-D detected an attack. DaMask-M performs two capacities, to be specific: countermeasure determination (drop the packet) and log generation. Measurable techniques utilized in identifying anomaly include the utilization of consecutive change point algorithm that mentions objective fact and saves the perception as an input (De Oca *et al*., 2010).

Data mining approach presened by Choi *et al*. (2014) who utilized map reduce model to alleviate HTTP GET DDoS attacks of application layer. The packet and log module investigations packet transmission and web server logs and the pattern examination module makes the attack pattern for DDoS identification. The detection module utilizes a typical standard of conduct to recognize DDoS attacks.

Alqahtani and Gamble (2015) recognized DDoS attacks utilizing anomaly detection to perform at the service level and cloud level using a hash map to outline the data stream. Their flow rate is estimated utilizing a dynamic data separate measurement to contrast and a pre-decided limit. On the off chance that the deliberate ranges are higher than the previous characterized edge at that point the movement is named an attack.

Choi *et al*. (2013) utilized mapreduce to identify attacks of application layer HTTP GET flooding which classify parameters belong to packet preceding utilizing entropy insights to gauge unwavering quality of the parameters.

MATERIALS AND METHODS

DDoS attacks classification in cloud: Researchers divided resource starvation attacks into two general categories: vulnerability attacks and flooding attacks (Ozcelik, 2015). Vulnerability attacks leverage software or protocol bugs to exhaust system resources such as memory, CPU time, disk space or data structures.

Flooding attacks send more packets or requests than the system can handle. There are several denials of service attacks such as (SYN flooding, UDP Flooding, ICMP flooding, Reflection or Amplification Attack, Application-level DdoS Attack, Ping of Death) (Fig. 1).

In the DDoS attack, an attacker performs attack via. a single machine but in distributed denial of service attack, attacker creates zombies to launch a DDoS attack, zombies send to the victim sham traffic/requests (Kumawat and Meena, 2014).

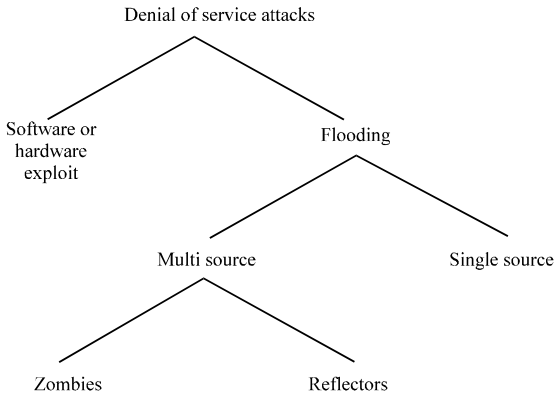

Fig. 1: Classificatin of denial of service attacks (Alani, 2016)

DDoS can be used vulnerable nodes known as zombie computers (Deshmukh and Devadkar, 2015). The targeted system when receiving malformed packets may not know how to deal with packets. If this event occurs, the access to the resources and cloud services will be denied by cloud user.

In classification of DDoS attacks, researchers by Deshmukh and Devadkar (2015) focused in resource depletion while researchers by Cha and Kim (2011) focused in flooding attacks in cloud web services and researchers Wong and Tan (2014) focused in infrastructural level attacks and application level attacks. Also, researchers by Ali-Eldin *et al*. (2012) classified it into application-bug and infrastructural attacks (Fig. 2) illustrated cloud DDoS attack classification.

Application-bug level: In this level of attack, attackers abuse system shortcomings to render cloud resources to be unavailable for cloud users. Also this level include several attacks such as misconfiguration, system weakness, outdated patches and protocol vulnerability.

Infrastructural level: This level known as flooding attacks which can be done in a reflector attack and direct attack. It also target cloud components to be inaccessible to genuine cloud. The attackers in this level just need the IP address of the objective without misuse any helplessness.

Direct attack: It ordered to application and network layer DDoS attacks and aims to overpower the objective system by devouring every accessible resources, bringing about the system being inaccessible to authentic users. It includes the utilization of traded off zombie PCs to send huge pernicious bundles.

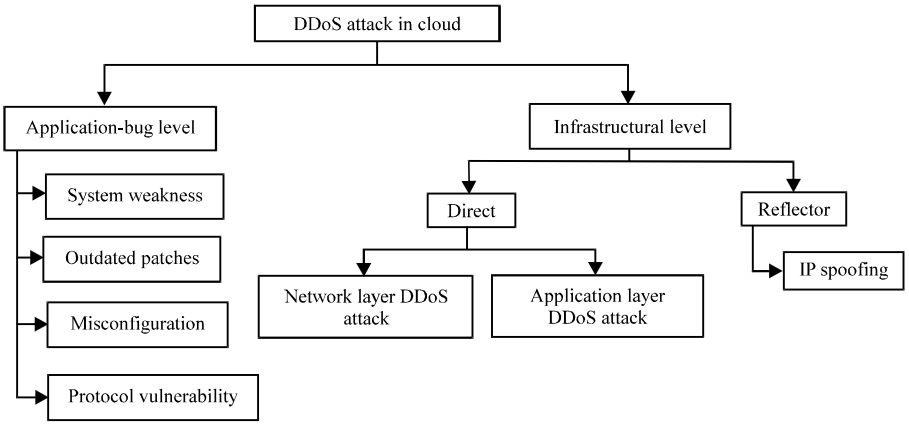

Fig. 2: Distributed denial of service attack classification in cloud (Osanaiye *et al*., 2016)

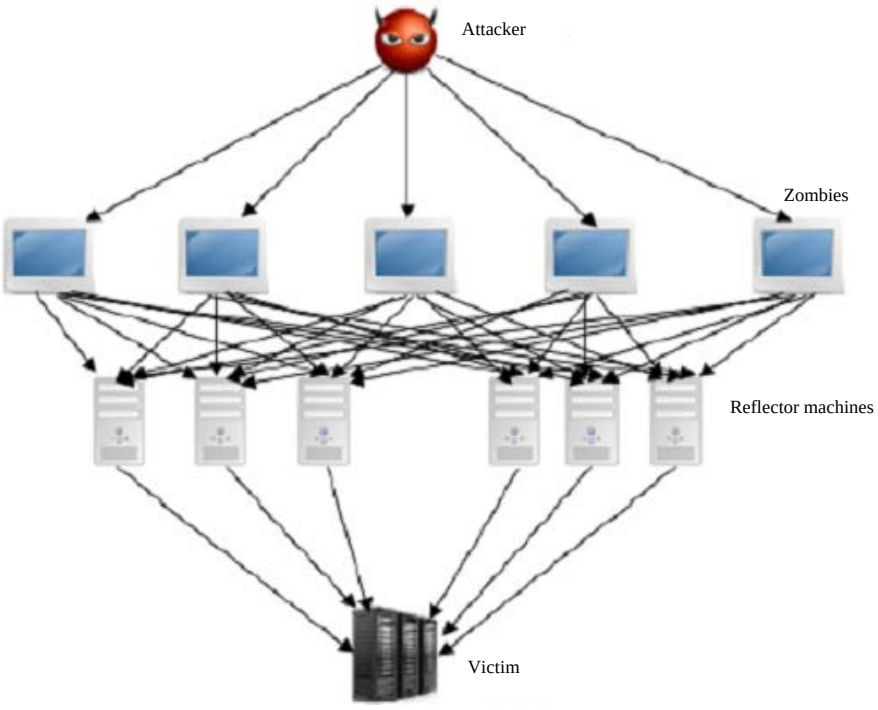

Fig. 3: Ddos reflector attack (Beitollahi and Deconinck, 2012)

Network layer DDoS attack: It consists of instances of attacks such as ICMP, UDP and TCP SYN flood. Flooding the objective host occurred, if there are any protocols found in the network and transport (Zargar *et al*.,2013).

Application layer DDoS: Attacks on the application layer utilizing flood packets to the objective cloud services and use HTTP flood to overpower an objective webserver hosted in the cloud. It additionally has effect in the efficiency, service quality, CP income, experience quality and reputation (Wong and Tan, 2014).

Reflector attack: As illustrated in Fig. 3 in this kind, the attacker parodies an IP address and sends their request to an extensive number of host's reflector. During the requests are gotten, the objective received the reaction via. host's reflector which also bring flooding to this the objective. The hosts enhance the attack by guiding their ping reaction to the objective.

DDoS defences classification in cloud: Yan *et al.* (2015) explored the capability of utilizing software defined network SDN to vanquish cloud computing DDoS. While

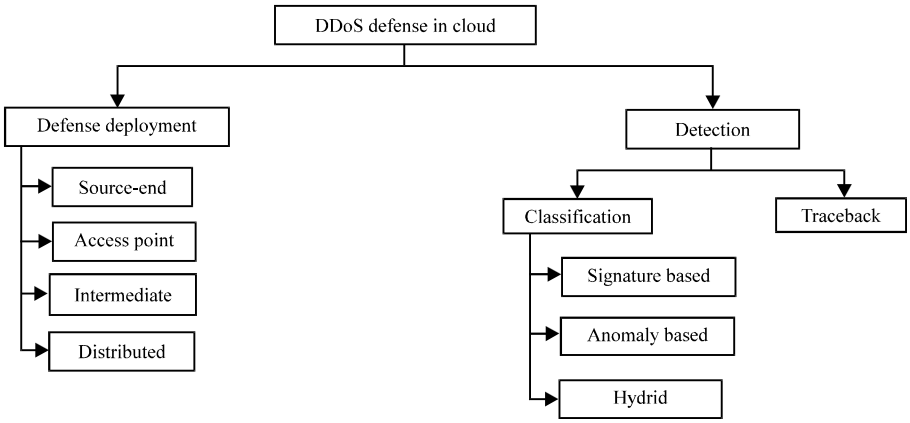

Fig. 4: Cloud DDoS defenses classification (Osanaiye *et al*., 2016)

Wang *et al*. (2014) analyzed the security effect of safeguard methods of DDOS attack where SDN and cloud computing were embraced. Varadharajan and Tupakula (2014) proposed trust improved security model and inspected different attack on cloud hosted services.

DDoS defense deployment: This kind of deployment includes four types which are: distributed, source-end, intermediate network and access point.

Source-end: Safeguards the wellspring of an attack utilize a throttling part to confine the streamed bundles amid packets during DDoS attacks (Bhuyan *et al*., 2013) which will retain the resources of both the target victim and the intermediate network (Fig. 4).

Access point: Each Virtual Machines (VMs) in the front-end, back-end in the cloud computing area is received access point. A key constraint of the access point isn't reasonable for sifting or rate-restricting immersed.

Intermediate-network: This sort restrains the effect of DDoS attacks on the network before the attacks affect the intended target. It forces rate restrains on the traffic in the wake of looking at the traffic against an ordinary profile design (Bakshi and Dujodwala, 2010).

Distributed defense: It is a crossover model consist of source-end, access point as well as middle network deployments. Contingent upon the setup, this model can be accomplished a high identification rate of DDoS attack.

DDoS detection: Techniques of DDoS identification can be sorted into signature based, anomaly based, the packet traffic delegated authentic or malicious.

Signature detection: It utilizes signature attack patterns put away in a database. Bakshi and Dujodwala (2010) proposed for a cloud a signature based DDoS detection, they utilized IDS in VMs to determine DDoS attacks. Lonea *et al*. (2013) utilized the Barnyard tool to capture attacks which produces infrastructural resource exhaustion attack comprising of ICMP flooding, UDP flooding and TCP SYN. Karnwal *et al*. (2012, 2013) proposed the utilization of filter tree approach to deal with application layer flooding. The five modules in the proposed methodology were intended to distinguish and resolve XML and HTTP based DDoS attacks.

Anomaly detection: Its principle objective is to identify consequent patterns that veer off from a normal conduct. Chandola *et al*. (2009) bunch anomalies into three fundamental classifications which are: point, contextual and collective anomalies. Point anomaly happens when data case is viewed as abnormal as for the remainder of the data. Contextual anomaly happens, if data is abnormal in a particular setting, however, not in another unique circumstance. Collective anomaly happens when gathering of data occurrences is irregular as for the entire dataset. DDoS flooding attacks are example when data instance just winds up abnormal and hurtful. Cloud DDoS attacks anomaly detection gathered into classes dependent on the algorithms utilized which are: artificial intelligence, data mining, machine learning, classifiers and statistical (Osanaiye *et al*., 2016).

Hybrid detection: It includes the utilization of both anomaly and signature-based techniques. Krishnan and Chatterjee (2012) discussed a versatile IDS that consolidates abnormality and knowledge based methods to protect toward DDoS attacks cloud which improved the recognition rate by bringing down the false positives. The system likewise actualizes an alarm grouping and analyzer

that encourages all collaborating hubs to separate between malicious nodes and false alarm. Cha and Kim (2011) structure 3-stages anomaly detection, the main stage utilizes a standard system to preprocess known as patterns of DDoS attack. The second stage predicts the normal future burden on every client interface utilizing time-arrangement displaying. The third recognize both obscure and known patterns of DDoS attack. Modi *et al.* (2012) structure a hybrid network intrusion to identify DDoS attacks of cloud. While Teng *et al.* (2014) discussed an intrusion detection modelled with eCargo to safeguard toward cloud DDoS attacks.

IP spoofing detection: It can find the genuine wellspring source of DDOS attacks as it will in general farce their addresses. Researchers by Jeyanthi *et al.* (2013) proposed an algorithm which is actuated at whatever point there is an abrupt ascent in the packet traffic more noteworthy than a pre-characterized limit. Methodology additionally confirms authenticity of associating cloud client.

DDoS attack defenses forms: Yu *et al.* (2013) considered an Intrusion Prevention System (IPS) was conveyed to screen approaching packets during DDoS attacks at various passageways of the cloud area. The DDoS mitigation algorithm recognizes resources for IPS and accessible resource for the cloud. At the point when diminishing the attack volume, the system will naturally decrease the quantity of IPS and de-arrangement recently distributed back to the pool. Table 1 demonstrated techniques utilized for tracing, identifying the attacker and decrease the attack effect.

RESULTS AND DISCUSSION

In this study, researcher proposed cloud DDoS defense framework. At the point when an assault is distinguished an alert is issued. On the off chance that the packet is identified to be genuine, it will be sent to its destination. Be that as it may, if the packet be attacked by DDoS, it will be countermeasure action to mitigate this attack and drop the packet (Fig. 5).

Packet arrival: Packet has been utilized in network execution checking and distinguishing proof of use over the web. Cheking the packet by deciding the time between the first received and next packets. The assurance, if a DDoS attack is happened in the traffic flow by inter-arrival distribution.

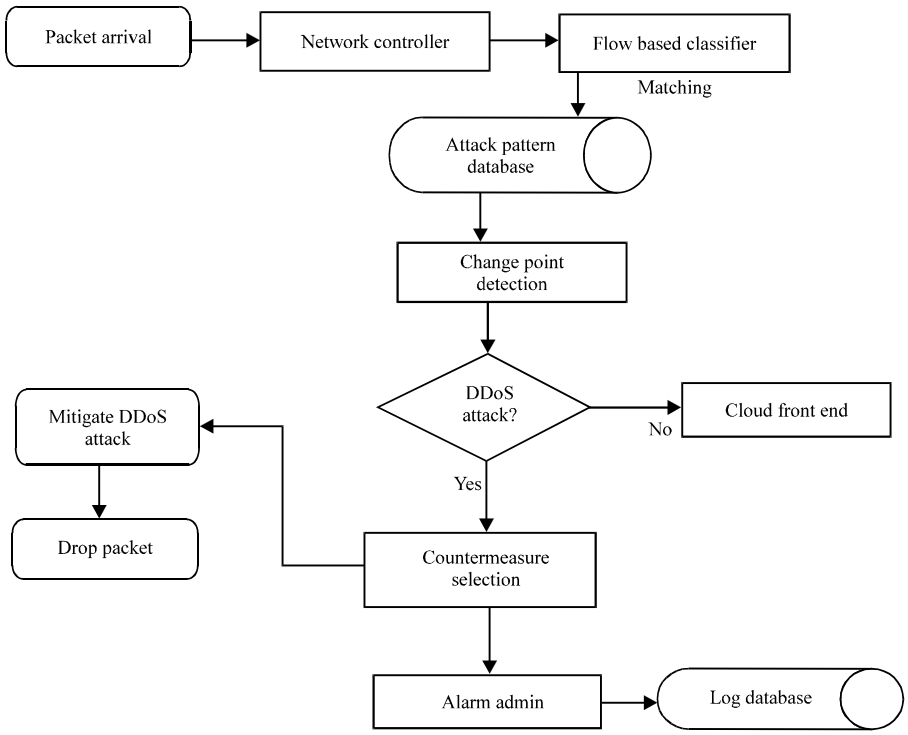

Fig. 5: Conceptual cloud DDoS defense framework

Table 1: Traceback techniques

Traceback method	Description
ICMP	Forwarding low likelihood packets to each router and furthermore sends an ICMP traceback message to destination. The approval of these packets is troublesome and additionally way path detection overhead of information from route map
IP	Traces back the attacker's path to discover the root of attack. In this method, the way of attacker is pursued back to discover its source
Link-testing	Tests each of approaching connects to check its likelihood being an attack
Probabilistic packet making	Conquers disadvantages of connection testing packet marking traceback. It's preference additionally overheads the systems yet there are numerous techniques to stay away from this overhead

Flow based classifier: During DDoS attacks, distinctive types of DDoS attack happened differing between the consistent, throbbing and continuous rate attacks. Flow based classifier is used to inspect the packet's header content to group approaching traffic from various sources. The packet has information about: source IP address: port, destination IP address: port.

Change point detection: In this proposed framework, researcher uses the change point detection in detecting anomaly behavior which proposed checking and coordinating the packet arrangement with the typical normal behavioral pattern to identify any critical deviation. On the off chance that an attack traffic is distinguished, it will be countermeasure action as an alert is issued and the packets are dropped during traffic obtain entrance to the environment of cloud.

CONCLUSION

Previous studied in DDoS attacks toward the mitigation strategies and cloud services are discussed in this study. A characterization of the distinctive sorts of cloud DDoS attacks are presented which ordered to application bug and infrastructure level. Also, researcher presents cloud DDoS defenses classification which grouped into defense deployment and detection. A conceptual framework in this study consists of three stages which are packet arrival, flow based classifier, change point detection. The assessment and treatment of this framework utilizing genuine real-world data will be included in the future research.

ACKNOWLEDGEMENT

I would like to thank everyone help me to prepare this study.

REFERENCES

Alani, M.M., 2016. Elements of Cloud Computing: Security a Survey of Key Practicalities. Springer, Berlin, Germany, USA., ISBN:978-3-319-41411-9, Pages: 55.

Ali-Eldin, A., J. Tordsson and E. Elmroth, 2012. An adaptive hybrid elasticity controller for cloud infrastructures. Proceedings of the IEEE Network Operations and Management Symposium, April 16-20, 2012, Maui, HI., pp: 204-212.

Alqahtani, S. and R.F. Gamble, 2015. DDoS attacks in service clouds. Proceedings of the 2015 48th Hawaii International Conference on System Sciences, January 5-8, 2015, IEEE, Kauai, Hawaii, USA., pp: 5331-5340.

Bakshi, A. and Y.B. Dujodwala, 2010. Securing cloud from DDOS attacks using intrusion detection system in virtual machine. Proceedings of the 2nd International Conference on Communication Software and Networks (ICCSN'10), February 26-28, 2010, IEEE, Singapore, ISBN: 978-1-4244-5726-7, pp: 260-264.

Beitollahi, H. and G. Deconinck, 2012. Analyzing well-known countermeasures against distributed denial of service attacks. Comput. Commun., 35: 1312-1332.

Bhuyan, M.H., H.J. Kashyap, D.K. Bhattacharyya and J.K. Kalita, 2013. Detecting distributed denial of service attacks: Methods, tools and future directions. Comput. J., 57: 537-556.

Cha, B. and J. Kim, 2011. Study of multistage anomaly detection for secured cloud computing resources in future internet. Proceedings of the 2011 IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, December 12-14, 2011, IEEE, Sydney, Australia, ISBN:978-1-4673-0006-3, pp: 1046-1050.

Chandola, V., A. Banerjee and V. Kumar, 2009. Anomaly detection: A survey. ACM. Comput. Surv., 41: 1-58.

Choi, J., C. Choi, B. Ko and P. Kim, 2014. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft Comput., 18: 1697-1703.

Choi, J., C. Choi, B. Ko, D. Choi and P. Kim, 2013. Detecting web based DDoS attack using MaPreduce operations in cloud computing environment. J. Internet Serv. Inf. Secur., 3: 28-37.

De Oca, V.M., D.R. Jeske, Q. Zhang, C. Rendon and M. Marvasti, 2010. A cusum change-point detection algorithm for non-stationary sequences with application to data network surveillance. J. Syst. Software, 83: 1288-1297.

Deshmukh, R.V. and K.K. Devadkar, 2015. Understanding DDoS attack and its effect in cloud environment. Procedia Comput. Sci., 49: 202-210.

Grobauer, B., T. Walloschek and E. Stocker, 2011. Understanding cloud computing vulnerabilities. IEEE Secur. Privacy, 9: 50-57.

Jeyanthi, N., U. Barde, M. Sravani, V. Tiwaric and N.C.S.N. Iyengar, 2013. Detection of distributed denial of service attacks in cloud computing by identifying spoofed IP. Intl. J. Commun. Networks Distrib. Syst., 11: 262-279.

Karnwal, T., S. Thandapanii and A. Gnanasekaran, 2013. A Filter Tree Approach to Protect Cloud Computing against XML DDOS and HTTP DDOS ATTACK. In: Intelligent Informatics: Advances in Intelligent Systems and Computing, Abraham, A. and S. Thampi (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-32062-0, pp: 459-469.

Karnwal, T., T. Sivakumar and G. Aghila, 2012. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. Proceedings of the 2012 IEEE Student's International Conference on Electrical, Electronics and Computer Science, March 1-2, 2012, IEEE, Bhopal, India, ISBN: 978-1-4673-1516-6, pp: 1-5.

Krishnan, D. and M. Chatterjee, 2012. An adaptive distributed intrusion detection system for cloud computing framework. Proceedings of the International Conference on Security in Computer Networks and Distributed Systems, October 11-12, 2012, Springer, Berlin, Germany, ISBN:978-3-642-34134-2, pp: 466-473.

Kumawat, H. and G. Meena, 2014. Characterization, detection and mitigation of low-rate DoS attack. Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, November 14-16, 2014, Udaipur, Rajasthan, India, ISBN:978-1-4503-3216-3, pp: 1-5.

Lonea, A.M., D.E. Popescu, O. Prostean and H. Tianfield, 2013. Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud. In: Soft Computing Applications: Advances in Intelligent Systems and Computing, Balas, V., J. Fodor, A. Varkonyi-Koczy, J. Dombi and L. Jain (Eds.). Springer, Berlin, Germany, USA., ISBN:978-3-642-33940-0, pp: 367-379.

Modi, C.N., D.R. Patel, A. Patel and R. Muttukrishnan, 2012. Bayesian classifier and snort based network intrusion detection system in cloud computing. Proceedings of the 2012 3rd International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), July 26-28, 2012, IEEE, Coimbatore, India, pp: 1-7.

Osanaiye, O., K.K.R. Choo and M. Dlodlo, 2016. Distributed Denial Of Service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl., 67: 147-165.

Ozcelik, I., 2015. DoS attack detection and mitigation. Ph.D Thesis, Clemson University, Clemson, South Carolina, USA.

Teng, S., C. Zheng, H. Zhu, D. Liu and W. Zhang, 2014. A cooperative intrusion detection model for cloud computing networks. Intl. J. Secur. Appl., 8: 107-118.

Varadharajan, V. and U. Tupakula, 2014. Counteracting security attacks in virtual machines in the cloud using property based attestation. J. Network Comput. Appl., 40: 31-45.

Wang, B., Y. Zheng, W. Lou and Y.T. Hou, 2014. DDoS attack protection in the era of cloud computing and software-defined networking. Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols, October 21-24, 2014, IEEE, Raleigh, North Carolina, USA., pp: 624-629.

Wang, B., Y. Zheng, W. Lou and Y.T. Hou, 2015. DDoS attack protection in the era of cloud computing and software-defined networking. Comput. Netw., 81: 308-319.

Wong, F. and C.X. Tan, 2014. A survey of trends in massive DDoS attacks and cloud-based mitigations. Intl. J. Network Secur. Appl., 6: 57-71.

Yan, Q., F.R. Yu, Q. Gong and J. Li, 2015. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) attacks in cloud computing environments: A survey, some research issues and challenges. IEEE. Commun. Surv. Tutorials, 18: 602-622.

Yu, S., Y. Tian, S. Guo and D.O. Wu, 2013. Can we beat DDoS attacks in clouds?. IEEE. Trans. Parallel Distrib. Syst., 25: 2245-2254.

Zargar, S.T., J. Joshi and D. Tipper, 2013. A survey of defense mechanisms against Distributed Denial of Service (DDoS) flooding attacks. IEEE. Commun. Surv. Tutorials, 15: 2046-2069.