2016 International Conference on Computing, Analytics and Security Trends (CAST)
College of Engineering Pune, India. Dec 19-21, 2016

A Study on the Impacts of DoS and DDoS Attacks on Cloud and Mitigation Techniques

Awatef Balobaid, Wedad Alawad and Hanan Aljasim
Department of Computer Science and Engineering
Oakland University
Rochester, MI 48309, USA
asbalobaid, wmalawad, hkaljasi@oakland.edu

***Abstract* — The use of cloud computing has increased significantly in recent years; therefore, many cloud platforms have become in demand such as OpenStack, AWS etc. One of the challenges in cloud computing is providing secure and reliable services. For the last few years, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are the biggest threats in cloud security. DoS and DDoS attacks are initiated by the hacker to make an online service occupied by compromising it with massive traffic from multiple sources. The aim of this paper is to study the impacts of several types DoS/DDoS attacks in the cloud, and the procedures that they use to affect the services' availability. Furthermore, several mitigation techniques are discussed as well. To achieve this study, research and simulation work has been done.**

***Index Terms*— Denial of Service (DoS), Distributed Denial of Service (DDoS), OpenStack, cloud computing**

I. Introduction

Cloud computing has become popular in recent years as it offers a powerfully built framework which also supports the end users to access it through Internet. Some of the significant advantages of the cloud are the speed and reliability. A cloud computing can clone a virtual server rapidly; however, with the increase of the potential use of it, the risk of cyber-attacks to the cloud is increasing day by day. Most of the businesses are now shifting to the cloud from traditional physical servers, but the security of the cloud is under the threat of DoS and DDoS attacks. In order to overcome the cloud attack issues, the need for security measures must be well established as to ensure efficient and operative Internet security controls are provided. It focuses on three major aspects, which are confidentiality, integrity and availability; these three are commonly known as CIA. Confidentiality focuses on the effort to protect any resources, information and assets to be possessed without legal permission, whereas integrity is merely about maintaining original data [1]. Meanwhile, availability implies the act of making the resources obtainable whenever possible and without any barriers. This vulnerable condition needs three actions to be in place in ensuring security measures are established namely prevention, detection and reaction. These are the control measures that are established simply to avoid any attempt of Internet exploitation [1][2].

Discussing DoS and DDoS attacks, it involves both data and services [3]. According to the researchers, it was found that the DoS attack acts as the major threat of the availability aspect. However, it was initially seen as non-significant issues for security experts and researchers until it became aggressively intimidating at some point to attack e-commerce and high-profile web servers or organizations [4]. As such, it became one of the successful attacks that led to harmful consequences on the Internet service application. The aim of the DoS and DDoS attack is making any service unavailable by overwhelming it with traffic from multiple sources.

To investigate the impacts of DoS/DDoS attacks on the cloud and the efficiency of mitigation techniques, we divide our work into two parts in order to present a reliable and effective study. The research part mainly focuses on related work on DoS and DDoS attacks in the cloud environment. In the simulation part, a DoS attack (Syn flood and UDP flood) is simulated in 2 virtual machines. This study primarily focuses on the DoS and DDoS attacks on the cloud, and how it affects the cloud security. We have answered in this paper the following questions:

- Are software-based firewalls capable of mitigating DDoS attacks in the cloud?
- Are hardware-based firewalls and IDS/IPS capable of mitigating attacks in the cloud?
- What other strategies can mitigate the DDoS attacks in the cloud?

II. DoS and DDoS Attacks

DoS attacks are a process in which a user or organization is bereft of the services they usually expect to possess. This is a general term used when a single system attacks the target. But there are cases in which the number of attackers is greater than one, which is known as DDoS. In DDoS, giant numbers of compromised systems (sometimes known as a botnet) attack one target.

A. DoS Attack

A DoS is an attack which is used to crash a machine or network, thus making it impossible to access by its clients. DoS attacks make this possible by flooding the source with

978-1-5090-1338-8/16/$31.00 ©2016 IEEE

traffic, or by sending data, which initiates a crash. In each instance, it deprives legal users from the service they wanted. The following are the common ways of DoS attacks [5]:

- The denial of service by saturation is to submerge a terminal request, and to make sure that it's not able to meet the particular demands;
- The denial of service by vulnerability exploitation that is exploiting a flaw of the remote system to render it unusable.

Different DoS assaults only utilize vulnerabilities that cause the objective framework or administration to crash. In these assaults, data is dispatched that exploits bugs inside of the objective that a short time later crash or seriously destabilize the framework, so it can't be accessed or utilized. DoS attacks are a retardant which can affect any server or society significantly those connected to the network. The aim of such attack isn't to retrieve or change data, however damage the name of the corporate on the Internet and probably impairing its operation. From a technical purpose of read, these attacks don't seem to be terribly sophisticated, however they're effective against all terminals with an OS Windows, Linux OS, industrial UNIX or the other systems. Most DoS attacks exploit the vulnerabilities associated with the implementation of a protocol model TCP/IP [5].

B. DDoS Attack

DDoS is fundamentally a pernicious push to make a server or a system asset hindered for the clients, regularly by rapidly intruding on or suspending the administrations of a host associated with the system. Unlike a DoS attack, in which one system and one net alliance is utilized to surge focused on a service with packets, a DDoS attack utilizes many systems and loads of networks, generally dispersed i.e. a botnet. DDoS attacks may be generally divided into 3 categories [6]:

- Volume Attacks: It consists of flood attacks. The primary goal of this type of attack is to decrease bandwidth of the attacked site.
- Protocol Attacks: It includes ACK floods, Ping of Death and additional types. This kind of attack takes up resources of the server being used or the intermediate facilities, like firewalls.
- Application Layer Surge: This includes attacks that concentrate on operating systems' vulnerabilities. Comprised of requests that seem right, the target of those attacks is to breakdown the online server.

C. Sources of DDoS Attacks

DDoS assaults are rapidly turning into the most predominant sorts of assaults, developing quickly in the previous year, as indicated by late statistical surveying. The pattern is shorter length of time, yet greater parcels per-second volume attacks, and the general number of such events reported has developed particularly, too. Amid the 4th quarter of 2011, one review discovered forty five percent more DDoS assaults contrasted with the parallel time of 2010, and about two fold the quantity of attacks saw in 3rd quarter of 2011. The normal assault data transfer capacity saw among this period was 5.2Gbps, which is about 150 percent higher than the past quarter. Another review of DDoS attacking events found that more than forty percent of users experienced assaults that surpassed 1Gbps in data transfer capacity in 2013 and thirteen percent were focused by no less than one attack that surpassed 10Gbps [7].

From an inspirational viewpoint, late research found that DDoS assaults due to morals are on the ascent. The research additionally said budgetary (e.g., aggressive business rivalry) as another regular explanation behind such attacks [8].

III. DOS AND DDOS ATTACK IN CLOUD

In every second large number of data are moving towards cloud because of its versatility, minimal cost, automatic redundancy etc. This massive moving towards cloud is making the attackers interested in exploiting cloud and hack the cloud data. Most smart and sophisticated way in malicious attempt to attack the cloud is using DoS and DDoS attacks. These attacks are aimed to individual as well as high profiled system websites initially and still not to be declared as the serious security issue until it started to attack cloud servers, web servers and e-commerce industry.

A. Related Research

A cloud DDoS attack utilizes the cloud resources. The DDoS attack is noticeable through the utilization of cloud and flood based errors. Any DoS/ DDoS attack to any cloud can be software or network based. One of such attack can be Domain Name System (DNS) attacks. After DNS attack the users are routed to any evil cloud. Also some DDoS attack in can sniff cloud flowing packets and reads the unencrypted information [9]. Legitimate users fail to be provided with services by networks and servers when the DoS attacked and considered as malicious attempt. This disturbance can be carried via sending a large quantity of requests which need certain resources to generate replies [10][11]. DoS attack can be achieved by focusing on both network bandwidth and connectivity via draining all available resources leading to interrupt rightful users' requests and affecting network traffic [9][10]. DoS/DDoS attack is not only targeting media or business services but also service providers such DNS or web portals. Since the existence of many hacking tools that available through the internet for free, DoS attack become more complex and sophisticated enough without having advanced technical or programming skills. In addition, when DoS were distributed to become DDoS attack, the complexity will be an increase.

There are some studies and researches about DDoS attacks in the cloud [12][13][14]. Somani at el. presents a comprehensive survey on the nature, prevention, detection and mitigation mechanisms of DDoS attacks. Furthermore, to help the community towards designing effective defense mechanisms, they provided a guideline on powerful solution building and its main requirements [12]. In addition, a novel taxonomy of DDoS mitigation strategies is presented with their features and functionalities in the cloud. The DDoS mitigations methods are compared to analyze their strength and weakness points [13]. Many factors that must be

considered in order to select the suitable DDoS defense solution (e.g. functional, transpicuous, lightweight, precise) are discussed in [14].

DDoS attacks in the cloud attract many researchers and experts to involve deeply in this field [15][16][17]. Osanaiye et al. discussed the efficiency, advantages and limitations of different cloud DDoS defense solutions based on their deployment locations and the techniques that are used to detect the attacks. Furthermore, they proposed a conceptual cloud DDoS change-point detection framework that depends on the packet inter-arrival time (IAT) feature [15]. While an architecture to mitigate DDoS attacks is proposed [16]. It combines a highly programmable network monitoring and a flexible control structure to allow attack detection and to enable fast attack reaction. Also, another paper proposed a Ensemble-based multi-filter feature selection method EMFFS that enhances the performance of anomaly-based DDoS detection mechanisms [17].

IV. Simulating and Analyzing a Cloud Server Attack

Although this study focuses on the related studies on DoS/DDoS attack and mitigation techniques in cloud, a small scale DoS attack was demonstrated to a cloud server on OpenStack cloud platform to observe the impacts of the attack in cloud. It is really difficult to show a large scale DDoS attack in a simulation. No public cloud is used in this simulation for ethical and legal issues. Any DoS/ DDoS attack can create an impact on the public cloud, so it is not possible to show this simulation in large cloud networks. Furthermore, the public cloud (Azure, AWS etc) have their own defense mechanisms. For lack of resources, ethical, and legal issues the simulation was done in a virtual environment with virtual machines and virtual LAN.

A. DoS Attack Simulation in OpenStack Platform

In order to make any attack successful without knowing their enemy, the attacker spoof the source IP addresses via using the intermediate victims' IP [18]. UDP-based and TCP protocols can be use to handle the flood which hit victim and mounted [19]. To perform this simulation, many software and tools are used, see table1. The operating system and OpenStack- Icehouse installed in the virtual box. All the monitoring and mitigation tools installed in Ubuntu OS to monitor and mitigate the attacks. A penetration tool (Hping3) in Kali Linux OS used to generate this attacks.

Table1: simulation requirements

Simulation	Details
Platform / environment	• Oracle Virtual Box – as base environment for all system • OpenStack - Icehouse (single node) as platform for cloud environment • Ubuntu OS - as attacked system • Kali Linux OS – as attacker system
Attacks tool	• Hping tool - Hping3 used to generate attacks.
Monitoring tools	• Bandwidth monitoring tool (bmon) • IP Traffic monitoring (IPTraf) • Ubuntu system monitor • Wireshark
Mitigation tools	• Iptables / Firewall

B. Observation of the Attack in Cloud

Using Hping3 tool, the SYN flood and UDP flood attacks are generated. In this flood attack simulation, a 1000 sized payload is used. The SYN and UDP requests are generating random resources (spoofed IPs). This attack will utilized the cloud server's resources and make it half open. IPTraf, bmon, Ubuntu system monitor and Wireshark are used to observe the attack.

While launching the attack the cloud server's system resource usage can be monitor using system monitor tool. The system monitor tool shows that after launching the Hping3 attack a large amount of traffic is coming to the victim machine. For SYN flood attack it is observed that the received packet is between 20.5 MiB/S – 30 MiB/S but the sent packets are only 100-200 KiB/sec. So the SYN flood attack is generating a large amount of traffic to the victim cloud server. Also, the use of system resources is increased significantly. For UDP flood attack it is observed that the received packet is between 19 MiB/S – 25 MiB/S but the sent packets are only 200-250 KiB/sec. So the UDP flood attack is generating a large amount of traffic to the victim cloud server as well. Again the use of system resources is increased significantly. Several payload values are used to observe the impact of the attack in several situations. Using bmon monitor the bandwidth use is monitored. It is observed that the RX bps value varies from 20 to 30 MiB while the attacks are initiated where the TX bps value becomes 1-1.36MiB only. Similar result is observed for UDP flood attack. Other monitoring tools gave similar results.

C. Applied Mitigation Techniques in the Victim Cloud Server

One of the research questions is whether the software based firewalls are capable of mitigating DDoS attack. Another question is to what extent they are capable. In this simulation firewall and iptables are applied and the same SYN flood and UDP floods are generated again to observe the impact.

The primary function of firewall is to protect a system or network from any malicious attack. One of the significance of firewall is the policy; a firewall can be configured based on policy. In this simulation iptables and another software based firewall are used. iptables is actually a default firewall in Linux system [1][3]. Several rules are set in iptables (iptables commands) [20]. It is already proven that firewalls can mitigate any attack to the system but for DDoS attack the firewall can prevent the attack to a certain level. For a high volume attack the firewall cannot mitigate the attack. After applying the iptables and firewall, it is observed that the impact of the SYN flood and UDP flood attacks reduced significantly; the packet receiving becomes 5MiB/s to 6MiB/s.

From the simulation it can be observed that the firewall and iptables cannot fully mitigate the DoS/DDoS attack. But it is observed that the rate of attack decreased significantly. Especially the network resources are less used as some of the attack packets are dropped.

V. DoS and DDoS Attack Mitigation Techniques in Cloud

After analyzing different related studies on DoS/DDoS attacks on cloud, several assumptions are made on the DoS and DDoS mitigation techniques. It is observed that most of the studies focused on strong security architecture in cloud with a specific end goal to completely halting DDOS attacks, one has to comprehend the ideas driving it first. DOS/DDOS attacks are very frequent these days; typically, the attacks are intended to inconclusively or incidentally bring down a server or network whether it is cloud or not. DoS and DDoS attacks make great loss for organizations. The impact can be very expensive for organizations specially using private or hybrid cloud service. DDoS attack insurance assumes a crucial part in keeping organizations on the cloud. A huge number of information focuses in different streams fill a DDoS moderation system continuously amid an attack. There are several other unpublicized DDoS attacks on ecommerce organizations and electronic service suppliers of all sizes.

A. Software-based and Hardware-based Firewall Against the DoS and DDoS Attacks

Hardware based firewalls, router, and different types of intrusion detection systems are basically used to stop DDoS attacks; however, recently they are incapable with regards to very much arranged interruptions. Keeping in mind the end goal to stop the new era of attacks, clients would need to learn the new moderation methods. Firewalls can be very useful to mitigate DoS/DDoS attack. As per some review results (2013), foreswearing of service attacks costed organizations $100,000 every hour in normal, implying that a DDoS attack can cost a web dependent organization $1 million preceding the organization even begins to moderate the attack. Most organizations depend on in-house innovation to protect against attacks: 77% have firewalls, 65% have switches and switches, and 59% have interruption identification. Be that as it may, just 26% use cloud-based moderation services. Most focused on are e-commerce services and monetary services, additionally vast organizations, for example, Amazon, or Yahoo! Not even big was saved [24].

In 2011, WordPress, the webpage that serves 18 million distributers, and is in charge of 10% of all sites on the planet, was down for a few hours and endured genuine loss of income and customers. Another approach to stop the attacks would be to perform an inconsistency mind headers and in addition states and the rates of any gadget [21][24]. A few applications can really sift through the IP addresses and attack bundles henceforth ceasing DDoS attacks. By utilizing basic firewall standards, such attacks would not be conceivable. IPS and IDS are used to detect and prevent DDoS attacks. Both software and hardware based IPS/IDS are available. One of the examples of software based IDS is snort. Snort is an open source IDS that is mostly used in Linux based servers. But in large cloud environment it is crucial to use hardware based IPS and IDS for better security. Any IPS or IDS can use signature-based detection, statistical anomaly-based detection or stateful protocol analysis detection to detect any attack [22].

B. Using DDoS Detection and Reduction Techniques to Defend Against Advanced Threats

DDoS reduction techniques have increased the Network Security Monitoring (NSM) capability to an organization's that have different type of security information. NSM is not the only key component of DDoS detection but it also can be used by network opeFrations groups to analyze performance issues and solve problem that have been detected [14]. By using DDoS detection and mitigation techniques into the network security architecture, every organizations can use the benefit of the extra security intelligence to make it faster in detecting potential attacks and take a few step forward to avoid a compromise and no need to missed by other means. For example, a cloud server is compromised with an attack which is to intrude an internal server that will not notice by the external facing firewall, but it can be detected a DDoS NSM event. If the attack can go to the extraction phase, flow analysis performed by DDoS detection can be effect an alert that based on the other outbound traffic. That is why integrate is very important not just only syslog and alarms but the capability of it to recognize either legitimate-looking traffic is in a location or just at a time that can alert a potential attack [14].

There are many DDoS filtering capabilities of operational devices such as load balancers, firewalls or intrusion prevention systems which can be used as prevention method in small business. However, high volume attacks can prevent these devices and also sophisticated application-level DDoS attacks can usually avoid them. That is the reason why large enterprises or medium-sized businesses with revenue-critical systems is depending on high-availability of Internet connectivity, and also need devoted DDoS mitigation abilities. However, most of enterprises are using multiple ISPs or find the cost of ISP or cloud-provided DDoS mitigation too high for some geographies or websites. Relying solely on external DDoS mitigation can makes it harder to take the benefit of the DDoS monitoring abilities in targeted attacks effectively. For these reasons, most of the large organizations are using hybrid configuration where ISP or cloud-based protection is used and usually known as the first level of protection and local or customer premise-based DDoS prevention is also used on the site.

The DDoS reduction application is applied in synchronization with cloud-based DDoS services at the Internet edge of demilitarized zone (DMZ) for the setting to provide visibility into flows in and out of the organization. This will also prevent the attacks from affecting operational web, application, mail servers and security components such as firewalls. Using this DDoS reduction appliance, DDoS attacks could be traced by network operations or network security staff as the ISP-based services could not sense any attacks below certain bandwidth. Thus, the reduction can be activated at the service provider when the DDoS attack gets larger [9][23]. The minimum investment is required for the setting to bear the detection and avoidance of attacks, but dealing with the attacks delimited due to the inadequacy of visibility into internal network flows. The DoS and DDoS are

normally aiming for the mission-critical business server in the cloud data center. DDoS detection and reduction should be placed between the data center and others appliances. So the analysis and application awareness flow will form a defend wall to the servers.

C. DMZ and Security Appliances Deployment Options

The disadvantage of the additional anti-DDoS appliance is that it is too expensive. To avoid the high costing, a single DDoS appliance can be installed at the data center if the cloud-based DDoS improvement is sufficient to defend the DMZ servers. Most of the organization started to switch their business applications into external cloud service provider from their internal data centers by acquiring applications in Software as a Service (SaaS) or running them on cloud-based Infrastructure as a Service (IaaS). There are two options for the organization; they are able to route the traffic to/from the cloud through DDoS provider or using DDoS reducer provided by SaaS or IaaS. Using a hybrid configuration of their premise-based capabilities and ISP's or external DDoS reduction service, they have strong DDoS scrubbing capabilities as they are dependent on their internet connection available for revenue. Using SaaS/IaaS infrastructure and by giving as the APIs or other mechanisms, customers have authorized to join together their own data center or DMZ-based DDoS monitoring with that [9].

To distinguish between the low-level security (e.g. authorize database content such as support) events and critical security events, most organizations are using Security Information and Event Management (SIEM) products. An alert from DDoS reduction provides information to SIEM products to associate the log events across with the security controls. The integration is not only for alarms, but includes the insights of traffic traversing the network.

D. Deploying Security Policies to Mitigate the DoS/DDoS Attack in Cloud

The latest versions of firewalls and IPS appliances have put some new techniques to make sure it can perceive the urbane attacks by their traffic pattern. However, there are a few numbers of deficiencies which can let the attacks get ahead against these as well. Internal attacks can be handy for organizations. When a user's laptop got problems while out from the area of the network and then the user come back to his or her business network, greatly there is no incoming traffic to inspect because the laptop is safe and in the protected area of networking. The avoid techniques are used by the attackers (such as encryption or fragmented packets) are definitely designed to make sure the pattern can be identified and effectively packet inspection techniques, so that the attacks can avoid the detection. When DDoS techniques are put into the mix, high rates of traffic always can cause inline network defenses to make a choice between failing open traffic can pass by and no need to do the inspection to maintain availability or failing closed (not allow all traffic to pass by to keep safe but causing business disruption). When both of them found the ideal requirement of choking off only offensive traffic during maintaining the legitimate traffic flowing [24]. Operational gaps also can affect the typical perimeter defense, which it cannot function well against the DoS/DDoS attacks. Most of the organizations have subcontracted of email, web and firewall security operations and also monitoring to external managed security service providers or security-as-a-service providers in order to decrease the staffing requirements. Usually, the purposes of ISPs are used for DDoS detection and scrubbing as well. These methods also can reduce the amount of data available to the security staffs to recognize compromised PCs and servers that work on the internal network and at the same time make it tougher to identify incident response. In a few of the organizations, misunderstand about the worker in an organization that should responsible for DDoS detection and reduction can cause unfocused or weak defenses [9].

VI. CONCLUSION

Our paper aims to research several DoS/DDoS attacks and mitigation techniques especially in the cloud environment. These attacks and mitigations are studied based on related researches, current best practices etc. A simulation work has been performed to confirm our research results. For resource limitations, ethical and legal issues, we could not perform a large scale DDoS simulation in this research. Thus, a simulation was performed over a private cloud server to demonstrate some mitigation techniques. However, in the real life, the public and hybrid cloud environments are vast and thousand times larger than that simulation. The discussed DoS/DDoS mitigation techniques will definitely help to protect any cloud from DoS/DDoS attack. Nonetheless, due to the new attack tools, Trojans etc. that are spreading online everyday, these existing techniques might not be enough. It can be stated that both hardware based and software based firewalls are capable to defend known DoS/DDoS attacks. Still, an attack uses several ways to find security holes in any system. In short, a single security device is not capable of mitigating DoS or DDoS attacks, which means other defense techniques are required to protect the full cloud structure including servers, network devices, applications etc. Only then it will be possible to mitigate the DoS/DDoS attack. The future plan of this study will be focused on large cloud environment simulation using different mitigation strategies and security protocols.

REFERENCES

[1] D. Gollmann (2010) Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics,* 2 (5), 544-554.

[2] S. Yu, Y. Tian, S Guo, O Wu (2014) Can We Beat DDoS Attacks in Clouds? IEEE Transactions on Parallel And Distributed Systems, Vol. 25, No. 9, September 2014

[3] C.P. Pfleeger and S.L Pfleeger (2006). *Security in Computing*. 4th ed. Boston: Pearson Education.

[4] G. Loukas and G. Oke (2009). Protection against Denial of Service Attacks: A Survey. *The Computer Journal,* 00 (0), 1-19.

[5] Li, J., Liu, Y., & Gu, L. (2010, November). DDoS attack detection based on neural network. In Aware Computing (ISAC), 2010 2nd International Symposium on (pp. 196199). IEEE.

[6] D. Tipper et al. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attack. *IEEE COMUNICATIONS SURVEY & TUTORIALS,* 15 (4), 2046-2069.

[7] Idziorek, J., Tannian, M., & Jacobson, D. (2012, June). Attribution of fraudulent resource consumption in the cloud. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on (pp. 99-106). IEEE.

[8] L. Constantin (2015) DDOS attacks increased in number and size this year http://www.pcworld.com/article/2035407/ddos-attacks-have-increased-in-number-andsize-this-year-report-says.html

[9] N. Kumar and S. Sharma (2013) Study of Intrusion Detection System for DDoS Attacks in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[10] Z. Chao-Yang (2011). DOS Attack Analysis and Study of New Measures to Prevent. In: Intelligence Science and Information Engineering (ISIE), 2011 International Conference on, pp. 426-429

[11] C. Barna et al. (2012). Model-based adaptive DoS attack mitigation. *In: Software Engineering for Adaptive and Self-Managing Systems (SEAMS), 2012 ICSE Workshop on,* pp. 119-128.

[12] Somani, G., et al. (2015). DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. arXiv preprint arXiv:1512.08187.

[13] A. Shameli-Sendi, et al. (2015). Taxonomy of distributed denial of service mitigation approaches for cloud computing. *Journal of Network and Computer Applications* 58pp. 165-179. 2015. DOI: 10.1016/j.jnca.2015.09.005.

[14] Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science*, 49, 202-210.

[15] O. Osanaiye, K. R. Choo and M. Dlodlo (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications* 67pp. 147-165. DOI: 10.1016/j.jnca.2016.01.001.

[16] B. Wang, et al. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks* 81pp. 308-319. 2015. DOI: 10.1016/j.comnet.2015.02.026.

[17] Osanaiye, O. et al. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, 2016(1), 1.

[18] F. Chen et al (2013). A Rank Correlation Based Detection against Distributed Reflection DoS Attack. *IEEE Communication Letters,* 17 (1), 173-175.

[19] C. Rossow (2014). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. San Diego. Internet Society - http://www.christian-rossow.de/publications/amplification-ndss2014.pdf

[20] R. Russell (2015) iptables Manual - http://ipset.netfilter .org/iptables.man.html

[21] Cyber Defense Magazine (2013) Choosing a DDoS mitigation solution … the cloud based approach http://www.cyberdefense magazine.com/choosing-a-ddos-mitigation-solution-the-cloud-based-approach/

[22] W. Jansen and T. Grance (2015). Guidelines on Security and [Privacy in Public Cloud Computing http://csrc.nist.gov/ publications/nistpubs/800-144/SP800-144.pdf

[23] M. Poongothai and M. Sathyakala (2012). Simulation and analysis of DDoS attacks. *In: Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on,* pp. 78-85.

[24] Akamai Technologies, (2015) Why Cloud-Based Security for DDoS Mitigation? http://www.akamai.com/html/solutions/ cloud-security-ddos-mitigation.html