Using SDN Approach to Secure Cloud Servers Against Flooding Based DDoS Attacks

Houda Guesmi, Leïla Azouz Saïdane
CRISTAL LAB, National School of Computer Science (ENSI), Tunisia
Email:{ houda.guesmi@ensi-uma.tn, leila.saidane@ensi-uma.tn }

***Abstract*—Distributed Denial of Service (DDoS) attacks represent major risks for the current cloud computing architecture. The rate of DDoS attacks in cloud is growing because of the essential characteristics of cloud computing. In this paper, we propose to use Software Defined Network (SDN) architecture and Fast Entropy approach in order to secure cloud computing environment from DDoS attacks in real time. Thus, we exploited the centralized control and programmable characteristics of SDN architecture to supervise cloud traffics. The provided architecture collects and analyzes flow tables from switches. It also detects DDoS attacks by the controller using Fast Entropy algorithms. Through the performed experimental tests, we evaluated the performance of our solution in defending Cloud computing infrastructure against Distributed Denial of Service attacks.**

Keywords—Cloud Computing, Software Defined Network, Fast Entropy, DDoS attacks.

I. INTRODUCTION

The rapid evolution of using of cloud computing [1] services makes this technology a target for attacks [2]. In cloud computing environments, one of the most dangerous threats is Distributed Denial of Service (DDoS) attacks [2]. Thus, in recent years, several DDoS attacks have temporarily blocked cloud services [3], which decreased the confidence of cloud customers. In fact, protecting cloud traffic from these attacks has become a major challenge in the cloud security domain. Indeed, when the DDoS attackers increase the rate of packets in order to consume all the cloud resources, it will be difficult to distinguish DDoS attacks from legitimate packets.

The main utility of cloud computing is to provide on-demand services of different levels, which makes the availability crucial in the security requirements of cloud computing. Indeed DDoS attacks are the main risks that threaten the availability in cloud. In this context, the recent Software Defined Network (SDN) architecture [4], [5] carries a promising features and new opportunities to abort attacks in cloud computing environments [4], [6]. This architecture provides logical centralized control, software based traffic analysis, dynamic updating of forwarding rules and global view of the network. These capabilities make it easy to defeat DDoS attackers.

In this paper, we exploit Software Defined Network (SDN) capabilities and Fast Entropy method [7] to secure the cloud system from DDoS attacks in real time. Indeed, Fast Entropy is a method that uses modified information entropy in order to detect attacks. It has more reduced computational time compared to that of conventional entropy.

The remainder of this paper is organized as follows: Section II provides an overview of DDoS attacks in Cloud computing environments. Section III presents the Software-Defined Networking concept and its capabilities to defeat DDoS attacks. Section IV illustrates related works defending cloud computing against DDoS attacks. In section V, we describe our architecture. The obtained results of our simulation experiments are shown in section VI. Finally, Section VII concludes the paper and presents future work.

II. DDOS ATTACKS IN CLOUD COMPUTING ENVIRONMENTS

The rate of DDoS attacks occurrence in cloud computing environments has increased due to the main characteristics of cloud computing, such as on-demand self-service, resource pooling, rapid elasticity, broad network access and measured service. In this section, we describe the classification of DDoS attacks. Then, we explain their growth in cloud computing environments.

A. Classification of DDoS Attacks

Although a DDoS attack can be launched easily, it can be hardly avoided. Indeed, cyber-attackers often establish a network of computers to launch a DDoS attack. This network is known as a botnet. In [8], the classification of DDoS attacks is based on the target protocol level. According to this classification, we can distinguish two types of attacks:

- Network/transport-level DDoS flooding attacks: They exhaust victim network bandwidth to disrupt legitimate user's connectivity. Attackers mainly use UDP, ICMP, TCP and DNS protocol packets to be launched.
- Application-level DDoS flooding attacks: In order to disrupt legitimate users' services, these attacks exhaust the server resources, such as memory, sockets, bandwidth and CPU.

B. Cloud computing characteristics leading to DDoS attacks.

The rate of DDoS attacks is growing considerably in cloud computing environments. However, the traditional defense

978-1-5386-0610-0/17 $31.00 © 2017 IEEE
DOI 10.1109/ICSEng.2017.31

mechanisms of DDoS attacks face many challenges in these environments. According to the recent Cloud Security Alliance (CSA) survey, DDoS attacks are critical threats to cloud security [9]. The quarterly State of the Internet Report (SOTI) from Akamai Technologies [10] shows that DDoS attacks in the fourth quarter of 2012 increased by 200% over 2011. We present, in this sub-section, the essential characteristics of cloud computing and we show how they influence the rate growth of DDoS attacks in cloud computing environments.

1) On-Demand Self-Service

The development and emergence of botnets is one of the major reasons of DDoS attacks growth. Botnet networks are composed of machines or bots compromised by malware. Large-scale botnets, such as Rustock, Bobax and Srizbi, gained bad reputation for their malicious activities such as realizing DDoS attacks [11]. On demand, self-service characteristic of cloud allows legitimating users to rapidly add or subtract computing power. These capabilities could be used to immediately evoke a powerful botnet [12].

2) Broad Network Access and Rapid Elasticity

Broad network access and rapid elasticity in cloud could be used by attackers to produce immense DDoS attacks. In addition, they use heterogeneous client platforms to launch more sophisticated and flexible DDoS attacks. Attackers profit from botnets and other high-speed Internet access technologies to increase the size and frequency of DDoS attacks and disturb their victim's network infrastructure. These attacks become more sophisticated because they threaten specific applications, such as DNS, VoIP and HTTP with smaller and more furtive attacks [13].

3) Resource Pooling

In cloud computing, physical and virtual computing resources are pooled to serve multiple users using a multi-tenant model [14]. Therefore, launching DDoS attacks is more easier and the victims are more vulnerable with multi-tenant infrastructure and virtualization technology. Indeed, in each cloud, attackers can employ a virtual machine configured to connect instantly upon startup to one or more meeting points to receive marching orders [12]. In [15], on a DDoS attack, the performance of a virtualized web server can degrade by up to 23%, while that of a server non-hosted in a VM on the same hardware degrades by only 8%.

4) Rapid Elasticity and Measured Service

With cloud computing capabilities of rapid elasticity and measured service, adopters of the cloud service model are charged based on a pay-per-use basis of the network resources and cloud server. In this case, a DDoS attack on network resources and server is transformed into a new breed of attack, namely Economic Denial of Sustainability attack (EDoS) targeting the cloud adopter's economic resource [16].

III. SOFTWARE DEFINED NETWORKING (SDN)

In this section, we present the SDN architecture. Then, we describe its important defense capabilities against DDoS attacks.

A. Software-Defined- Networking (SDN) architecture

Recently, Software Defined Networking (SDN) [4] [5] has become extensively applied in the industrial field and academia. In this context, the Open Networking Foundation (ONF) [17] was established as a non-profitable association whose main objectives are to develop, standardize and commercialize SDN. Indeed, ONF is high-level design for SDN. It is made up of three major layers as shown in Figure 1.

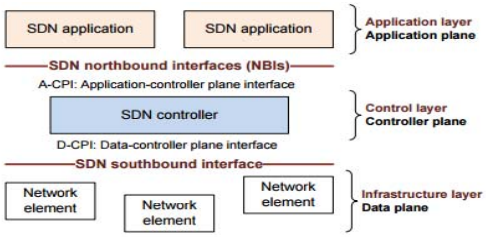

Fig. 1. SDN architecture [17]

- **Infrastructure Layer**: It is also called data plane containing Forwarding Elements (FEs): i) virtual switches (Open vSwich), ii) physical switches (Juniper Junos MX-series). The two types of switches can be accessed through an open interface in order to forward packets.
- **Control Layer:** It is also named control plane. This layer is made up of software-based SDN controllers. The latter use open APIs in order to control the forwarding behavior of the network via an open interface. They communicate using three interfaces: southbound, northbound and east/westbound interfaces [6].
- **Application Layer**: It contains the end-user business applications, like security application, network virtualization and mobility management. These applications performed the network services and SDN communications [6].

In fact, Open-Flow protocol [19] represents a part of SDN architecture. It assists the afore-mentioned switches in their flows-level control. It was first introduced at Stanford University in order to: i) make the communication among the software-based controller and the switches within an SDN architecture standard, ii) and allow researchers perform their experimental processes [6]. With clouds computing, the network storage and computation, nowadays, becomes possible without employing local resources.

B. *Features of SDN*

SDN brings new opportunities that we can profit from to defend cloud computing services against DDoS attacks. The important characteristics of SDN are described below:

- **Decoupling control plane and data plane**: SDN architecture separates the data plane from the control plan. This separation makes it easy to establish experiments of attacks and defense in large scale. This functionality of SDN brings new ideas and methods to mitigate attacks [4]. Thus, the separation of virtual networks allows experimenting new ideas using a programmable network platform.
- **Logical centralized control of the network**: The SDN Controller has a global knowledge and view of the network system. It enables to create a coherent security police for analyzing and monitoring traffic against security threats [4].
- **Network programmability by external applications**: The programmability of SDN supports intelligent algorithms extracted from Intrusion Detection Systems (IDSs) [20]. These algorithms are flexible to be used in attack detection.
- **Software-based traffic analysis**: In SDN architecture, the capabilities of switches can be improved using any technique based on software. The use of software tools and machine learning algorithms performs the traffic analysis in real time [21].
- **Dynamic updating of forwarding rules**: In case of attack traffic detection, we can add forwarding rules to switches in order to block the attack from disseminating in the network [4].

IV. RELATED WORK

In this section, we present popular defense methods to defeat DDoS attacks in cloud environment.

Chapade et al. proposed an approach in order to secure cloud servers against Distributed Denial of Service (DDoS) attacks [22] based on a distance estimation method to estimate traffic rates. First, the distance was calculated using the Time-To-Live of a packet. Then, the exponential smoothing was used to calculate the real-time measurement of the IP traffic round trip. Finally, absolute deviation was applied to decide if the behavior is abnormal. The major weakness of this solution is that it cannot identify the attackers in order to block the DDoS attack source.

Shweta Tripathi et al. presented a Hadoop-based defense method to handle DDoS Attacks [23]. As the first step, Hadoop used the Map Reduce framework to manipulate large volumes of data. This method replaced the First In First Out (FIFO) scheduling mechanism with a Self-Adaptive Map Reduce (SAMR) calendar. Afterwards, SAMR split the tasks into a set of sub-tasks assigned to the card nodes. Despite its advantages, this solution is not able to identify the DDoS attack source and it is time consuming.

Lanjuan Yang et al. developed DDoS attack detection system [24] for cloud computing based on the use of traffic filtering system and the Service Oriented Architecture (SOA) trace-back approach. The latter was employed by adding a tag to SOA packets to record the tracked route. However, this system is not able to determine the attack source.

Bansidhar Joshi et al. introduced an approach of trace-back DDoS attacks in cloud computing environments [25]. It is based on using Data Protection Manager (DPM) and network of neurons. Although this solution has a success rate of correctly identifying about 75% of attack traffic, it is not able to identify their sources. Moreover, the use of DPM may be limited with the introduction of IPv6 protocol.

V. PROPOSED METHOD

Unfortunately, current cloud architectures do not have a clear and effective security policy against distributed denial of service attacks, which reduces the consumers' confidence in such architecture. Thus, in this research work, we propose a solution based on using the SDN architecture to secure cloud environment against DDoS attacks (SecCloudDD). Indeed, the centralized control and programmability characteristics of SDN make the supervision of cloud traffics more effective and more secure (Figure 2). Therefore, SecCloudDD is able to identify DDoS attackers among legitimate users and block them in order to stabilize the system in real time.

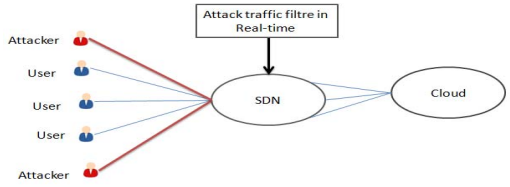

Fig. 2. Attack traffic filtre in cloud

A. *Proposed architecture*

Our architecture is composed of (Figure 3):

- SDN Switches: They are responsible for updating and storing the properties of user's requests and routing this information to the controller. This entity communicates with the controller using open-flow protocol [19].
- SDN controller: This element integrated in the classic cloud architecture is responsible for detecting and blocking DDos attacks by collecting and analyzing data packets. These data packets are received from SDN Switches.

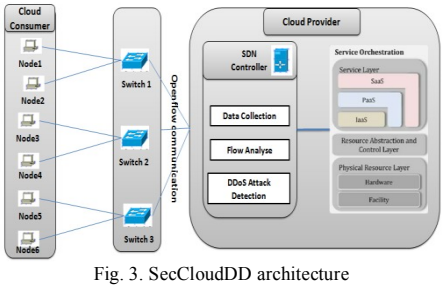

Fig. 3. SecCloudDD architecture

- Cloud provider: This entity offers a set of services and resources to legitimate users.
- Cloud users: The user exploits cloud services by sending one or more request to the switch. Then, the latter sends the request properties to the controller to check if the owner of that request is a malware.

1) SDN Switches

A switch is composed of a set of tables named "Flow tables". Upon client request receipt, the switch updates the set of request parameters in a Flow table. Afterward, these parameters are sent to the controller.

Flow table contains the IP addresses of each client. It saves, for each query, the source IP address, the cloud IP address and a counter that designates the number of requests sent by the same source to the same cloud server. This table also contains a parameter indicating whether the proper source is blocked or allowed. This parameter is the result of SDN Controller computations (Figure 4).

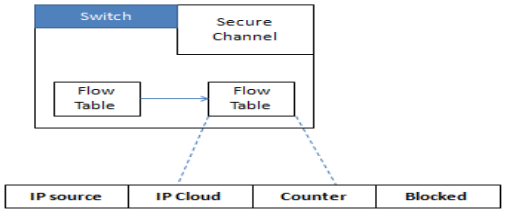

Fig. 4. SecCloudDD SDN Switch components

2) SDN Controller

The main element of our solution is the controller. It is responsible for protecting our cloud against DDoS attacks. In order to achieve this task, the controller launches several operations (data collection, data analysis and attack detection). If SDN Controller receives flow packets from SDN Switches element, it launches a set of algorithms for DDoS attack detection (Figure 5).

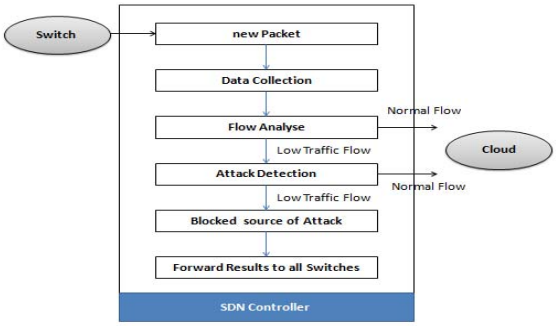

Fig. 5. SDN Controller functioning

B. SecCloudDD approach

In this section, we detail the steps of our approach:

1) Data Collection

For each new client request, the SDN Switches update the request properties (source IP address, cloud IP address and the counter) in the flow tables. Then, it sends these properties to the controller. The latter collects statistics from all switches connected with it in order to store them in a global flow table. This table contains these columns:

Connection Number	Source Address	Destination Address	Flow Count

2) Data Analysis:

After data collection operation, the controller supervises the traffic evolution using the flow count column of its global flow table. Cloud administrator sets a threshold for the sum of flow counts. If this sum exceeds the threshold in a time slot, our system launches attack detection algorithm. Otherwise, the controller sends user's request to cloud provider.

3) Attack Detection:

Our attack detection algorithm is based on Fast Entropy Approach [7]. Window size and a threshold are two essential components to entropy to detect DDoS attacks. The window size is based on a time interval. In fact, we compute entropy within a time slot to measure uncertainty in the coming traffics. If entropy value exceeds a threshold, cloud system is under an attack DDoS.

An entropy $E\ (i,w_t)$ for a flow count $C\ (i,\ w_t)$ of a particular connection i within a time window w_t is computed by equation (1).

$$E_{(i,w_t)} = -\log \frac{C_{(i,w_t)}}{\sum_{i=1}^{n} C_{(i,w_t)}} + \varphi_{(i,w_t)} \quad (1)$$

Where

$$\varphi_{(i,w_t)} = \begin{cases} \left| \log \frac{C_{(i,w_{t+1})}}{C_{(i,w_t)}} \right|, C_{(i,w_t)} \geq C_{(i,w_{t+1})} \\ \left| \log \frac{C_{(i,w_t)}}{C_{(i,w_{t+1})}} \right|, C_{(i,w_t)} < C_{(i,w_{t+1})} \end{cases} \quad (2)$$

After calculating the entropy of all flow counts in the time interval w_t, the attack detection algorithm (Figure 6) calculates the following set of variables:

- μ_i = standard deviation of flow count during a particular time t.
- $D(i,w_t)$: absolute value of the difference between μ_i and $E\ (i,\ t)$ (i.e., $D_i = |\ \mu_i - E(i,w_t)\ |$.

- α = mean deviation of flow count during a particular time t.
- β: threshold multiplication factor, positive integer value.
- ω: threshold ($\omega = \beta * \sigma$).

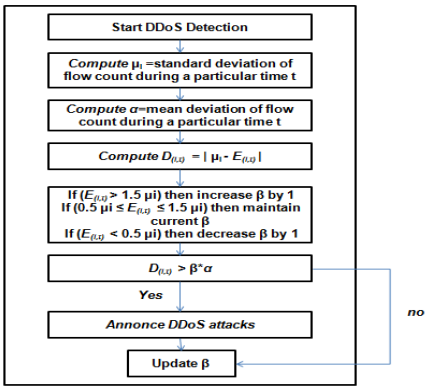

Fig. 6. Adaptive Fast Entropy algorithm

After computing μ_i, we compute D_i which represents the absolute value of the difference between μ_i and E (i, w_t). If $D_i \geq \omega$, we consider that the current Cloud network is under a DDoS attack in the current time window w_t. Otherwise, the traffic condition is always normal (out of attack). The multiplication factor, β, must be modified as a function of the traffic condition.

When the controller detects attack packets, it announces DDoS attack in SDN Switches in order to block the source address of the particular connection i before reaching the cloud server.

VI. Simulation

In order to evaluate SecCloudDD architecture, we realized several simulation scenarios using a set of tools. CloudSim [26] is the simulator applied to design cloud computing architecture, SDN controller, switches and the user nodes. Scapy [27] is employed to generate traffics and DDoS attacks on our cloud server. Table 1 represents the simulation parameters.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Number of nodes	100..300
Number of switches	5% of total number of nodes
Value of β	3
Attack Rate	25%, 50%, 75%
Time Window	1 second
Topology	Hierarchical
Distance between nodes	200 meters
SDN protocol	OpenFlow
Time of simulation	150 Seconds

A. DDoS attack detection

The simulations described in figure 7.a evaluate the reaction of our approach towards two traffic types. The blue line describes a normal traffic behavior, while and the green one represents the behavior of an under attack DDoS traffic. Figure 7 shows that our solution controls cloud traffic and intervenes from the moment that DDoS attacker increases the number of packets to consume all victims' resources. In this case, SecCloudDD stabilizes the traffic to a normal state by blocking the attack source and signaling it in all the switches in real time. The simulations demonstrate (figure 7. a) that anomaly detection and its blocking can be carried out in 15 seconds when the number of packets reaches 25000/second. With the same parameters, figure 7.b shows that the method based on distance estimation [22] reacts in 35 seconds, while the Hadoop-based method [23] reacts in 45 seconds, in the case of DDoS attack traffic (figure 7. c).

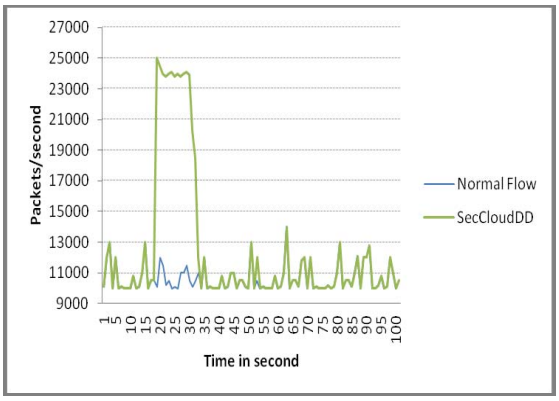

Fig. 7. a. DDoS attack detection using SecCloudDD method

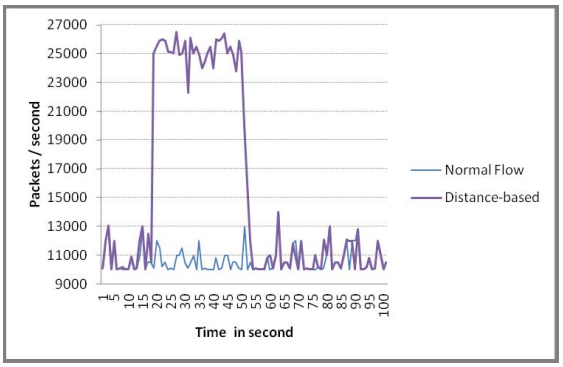

Fig. 7. b. DDoS attack detection using distance estimation method

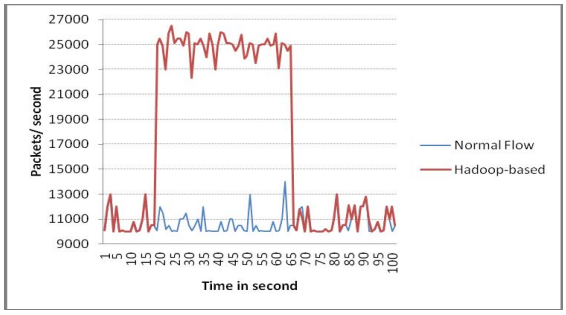

Fig. 7.c. DDoS attack detection using Hadoop-based method

B. *Entropy value variation*

In figure 8, we evaluate our solution in case of an high rate of DDoS attacks. In addition, we show the entropy value variation as a function of the rate of DDoS attacks applied to the cloud system. Thus, we took different percentages of malicious hosts that launch DDoS attacks. When the rate of attacks increases remarkably (superior to 25%), the entropy value decreases in order to signal the anomaly detection. Therefore, the fast entropy algorithm normalizes this value in order to stabilize the system again.

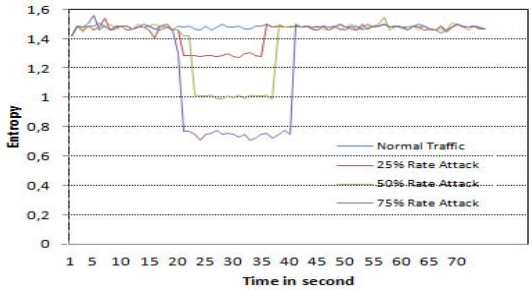

Fig. 8. Entropy value variation

C. *Discussion of simulation results*

All the simulations carried out show the efficiency of SDN controller use and fast entropy algorithm in protecting cloud system from DDoS attacks.

The controller, in our approach, has an important role in analyzing traffics and identifying DDoS attacks from legitimate packets. Thus, it allows cloud traffic supervision by periodically analyzing the variation of cloud traffics and triggers fast entropy algorithm in real time if there is an abnormal increase of traffic packets in order to avoid the DDoS attacks before it reaches the cloud network.

VII. CONCLUSION

Our approach proved its efficiency as it is based on SDN architecture and Fast Entropy method. It allows traffic collection and analysis, attack DDoS detection in real time, blocking attack packets and sending only legitimate flows to the cloud provider. Our experiments showed that it is robust in protecting cloud computing environments against this type of attacks. Thus, our solution helped acquire the trust of cloud computing customers.

In this paper, we only studied DDoS attacks. However, there are several other risks that may threaten the security of cloud environments. In future works, we will propose a secure system based on cryptography for data storage in cloud computing.

REFERENCES

[1] T. Mahboob, S. Ghaffar, and Z. Batool Akhtar, "A survey — cloud computing a global perspective - IC3e ," 2015.

[2] B.Prabadevi, N.Jeyanthi, “Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey”, IEEE, 17-19 June 2014.

[3] “Arbor special report: Worldwide infrastructure security report volume IX,” Arbor Netw., Inc., Burlington, MA, USA, Tech. Rep.,Dec. 2012.

[4] W. Xia, Y. Wen, C. Foh, D. Niyato, and H. Xie, “A survey on software defined networking,” IEEE Commun. Surveys Tuts., vol. 17, no. 1, pp. 27–51, 1st Quart. 2015.

[5] D. Rawat and S. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey", IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 325-346, 2017.

[6] M. D. Yosr Jarraya and T. Madi, “A survey and a layered taxonomy of software-defined networking,” IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1955–1980, 4th Quart. 2014.

[7] G. No, I. Ra, “An Efficient and Reliable DDoS Attack Detection Algorithm Using a Fast Entropy Computation Method”, Proc. of the 9th International Conference on Communications and Information technologies (ISCIT), Incheon Songdo, South Korea, September, 2009.

[8] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,” IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, 4th Quart. 2013.

[9] “The notorious nine cloud computing top threats in 2013,” Cloud Security Alliance, Seattle, WA, USA, Tech. Rep., Feb. 2013.

[10] “State of the internet report 2012 Q4,” Akamai Technologies, Cambridge, MA, USA, Tech. Rep., Dec. 2012.

[11] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, “Botnets: A survey,” Comput. Netw., vol. 57, no. 2, pp. 378–403, Feb. 2013.

[12] Jean-Francois, Cloud Computing: Weapon of Choice for DDoS?, Dec. 2012.

[13] “Arbor application brief: The growing threat of application-layer DDoS attacks,” Arbor Netw., Inc., Burlington, MA, USA, Tech. Rep., Oct. 2010.

[14] A. Girma, M. Garuba, and R. Goel, “Cloud computing vulnerability: DDoS as its main security threat, and analysis of IDS as a solution model,” in Proc. 11th Int. Conf. ITNG, 2014,

[15] R. Shea and J. Liu, “Performance of virtual machines under networked denial of service attacks: Experiments and analysis,” IEEE Syst. J., vol. 7, no. 2, pp. 335–345, Jun. 2013.

[16] S. VivinSandar and S. Shenai, “Economic denial of sustainability (EDoS) in cloud services using http and xml based DDoS attacks,” Int. J. Comput. Appl., vol. 41, no. 20, pp. 11–16, Mar. 2012.

[17] Open Networking Foundation, Jun. 2014.

[18] S. Sezer et al., “Are we ready for SDN? Implementation challenges for software-defined networks,” IEEE Commun. Mag., vol. 51, no. 7, pp. 36–43, Jul. 2013.

[19] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.

[20] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, “Structural results for combined continuous user authentication and intrusion detection in high security

mobile ad-hoc networks," IEEE Trans. Wireless Commun., vol. 10, no. 9, pp. 3064–3073, Sep. 2011.

[21] A. Lara, A. Kolasani, and B. Ramamurthy, "Network innovation using openflow: A survey," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, 4th Quart. 2013.

[22] S. S. Chapade, et al., "Securing Cloud Servers Against Flooding Based DDOS Attacks," in Communication Systems and Network Technologies (CSNT), 2013 International Conference on, 2013, pp. 524-528.

[23] S. Tripathi, et al., ". Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks," Journal of Information Security, 2013.

[24] Y. Lanjuan, et al., "Defense of DDoS attack for cloud computing," in Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on, 2012, pp. 626-629.

[25] B. Joshi, et al., "Securing cloud computing environment against DDoS attacks," in Computer Communication and Informatics (ICCCI), 2012 International Conference on, 2012, pp. 1-5

[26] RN. Calheiros, R. Ranjan, A Beloglazov, CA De Rose, R. Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms.",2011

[27] Scapy. http://www.secdev.org/projects/scapy/