INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH VOLUME 7, ISSUE 11, NOVEMBER-2016
ISSN 2229-5518

DDoS Attack in "Cloud of Things" Environment, Software Defined Networking (SDN) and A Research on Defense Mechanisms against DDoS using SDN

Tasnim Tamanna

System Engineer, Data Network, NovoCom Limited, Dhaka-1212, Bangladesh.
E-mail: aisharjaw.tasnim@gmail.com

Abstract- The Internet of Things presents the user with a novel means of communicating with the Web world through ubiquitous object-enabled networks. While IoT is exciting on its own, the real innovation will come from combining it with cloud computing. In the new era of Internet of Things integrated with cloud computing, Distributed Denial Service of Attacks (DDoS) is growing substantially. With the advancement of Software Defined Networking (SDN), defense mechanisms against DDoS attack has opened a new door to *Cloud of Things* environment. This paper discusses on how to make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments as well as cloud based IoT environment. The research results in this paper can be expanded to prepare a new architecture of SDN enabled secured *Cloud of Things* environment.

Index terms- cloud computing, Internet of Things, Software Defined Networking, cloud security, security threats, DDoS, control plane centralization

1. INTRODUCTION

The Internet of Things (IoT) involves the internet-connected devices we use to perform the processes and services that support our way of life. Another component set to help IoT succeed is cloud computing, which acts as a sort of front end. Cloud computing is an increasingly popular service that offers several advantages to IOT, and its based on the concept of allowing users to perform normal computing tasks using services delivered entirely over the internet[1][2][3]. The growth of IoT and the rapid development of associated technologies create a widespread connection of "things." This has lead to the production of large amounts of data, which needs to be stored, processed and accessed. Cloud computing as a paradigm for big data storage and analytics. While IoT is exciting on its own, the real innovation will come from combining it with cloud computing [6]. The combination of cloud computing and IoT will enable new monitoring services and powerful processing of sensory data streams. However, when IoT meets cloud, new challenges arise. The critical concerns during integration are quality of service (QoS) and quality of experience (QoE), as well as data security, privacy and reliability. Among the security requirements, availability is crucial since the core function of cloud computing is to provide on-demand services of different levels [13]. *Denial of Service* (DoS) attacks and *Distributed Denial of Service* (DDoS) flooding attacks are the main methods to destroy availability of cloud computing and IoT based devices.

With recent advances in software-defined networking (SDN), SDN-based cloud brings us new chances to defeat DDoS attacks in cloud computing environments. Good features of SDN offer new opportunities to defeat attacks in cloud computing environments. This paper discusses the new trends and characteristics of DDoS attacks in cloud computing, and provide a comprehensive survey of defense mechanisms against DDoS attacks using SDN.

2. WHAT IS SDN?

ONF has provided the most explicit and well received definition of SDN as follows: "In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications" [11]. In the simplest possible terms, SDN entails the decoupling of the control plane from the forwarding plane and offloads its functions to a centralized controller. Rather than each node in the network making its own forwarding decisions, a centralized software-based controller (likely running on commodity server hardware) is responsible for instructing subordinate hardware nodes on how to forward traffic.

3. BASIC SDN ARCHITECTURE

The basis of SDN is virtualization, which in its most simplistic form allows software to run separately from the underlying hardware. Virtualization has made cloud computing possible and now allows datacenters to dynamically provision IT resources exactly where they are needed, on the fly. To keep

INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH VOLUME 7, ISSUE 11, NOVEMBER-2016
ISSN 2229-5518

up with the speed and complexity of all this split-second processing, the network must also adapt, becoming more flexible and automatically responsive. We can apply the idea of virtualization to the network as well, separating the function of traffic control from the network hardware, resulting in SDN.

An SDN architecture consists of three layers. The lowest layer is the infrastructure layer, also called the data plane. It comprises the forwarding network elements. The responsibilities of the forwarding plane are mainly data forwarding, as well as monitoring local information and gathering statistics. One layer above, we find the control layer, also called the control plane. It is responsible for programming and managing the forwarding plane. To that end, it makes use of the information provided by the forwarding plane and defines network operation and routing. It comprises one or more software controllers that communicate with the forwarding network elements through standardized interfaces, which are referred to as southbound interfaces.

The application layer contains network applications that can introduce new network features, such as security and

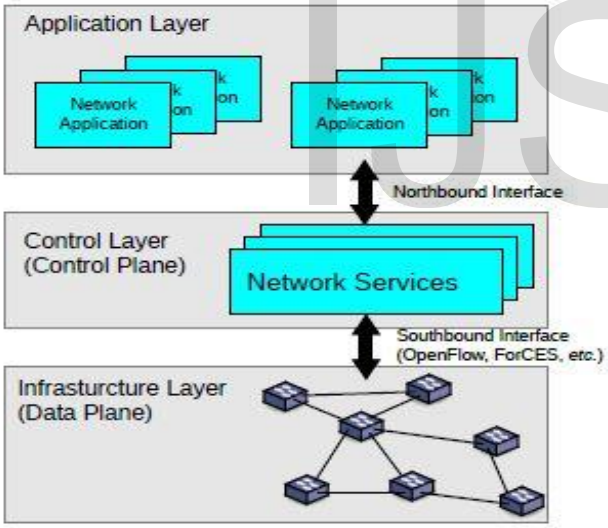


Image source [Future Internet 2014, 6, 302-336;]

manageability, forwarding schemes or assist the control layer in the network configuration. The application layer can receive an abstracted and global view of the network from the controllers and use that information to provide appropriate guidance to the control layer. The interface between the application layer and the control layer is referred to as the northbound interface.

The most common southbound interface is OpenFlow, which is standardized by the Open Networking Foundation (ONF). OpenFlow is a protocol that describes the interaction of one or more control servers with OpenFlow-compliant switches.

An OpenFlow controller installs flow table entries in switches, so that these switches can forward traffic according to these entries. Thus, OpenFlow switches depend on configuration by controllers. A flow is classified by match fields that are

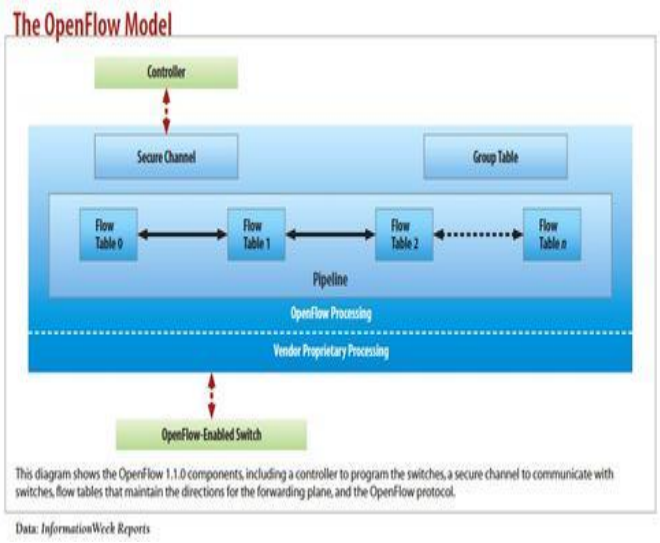


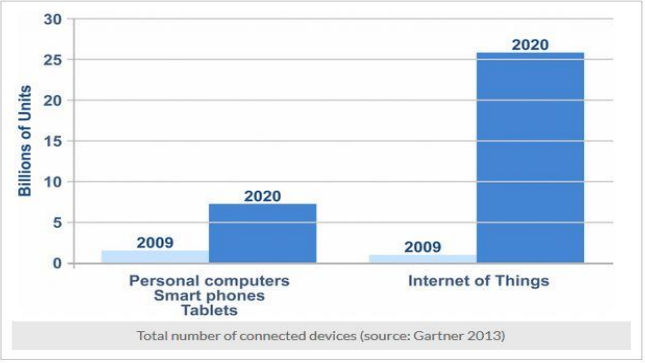
Image Source [Information Week Reports]

similar to access control lists (ACLs) and may contain wildcards.

4. FROM *"THE THING"* TOWARDS *"THE CLOUD OF THINGS"*

In truth, cloud computing and IoT are tightly coupled. Cloud computing, the recent trend in IT, takes computing from desktop to the whole World Wide Web and yet, the user doesn't need to worry about maintenance and managing all the resources. User has to bear only the cost of usage of service(s), which is called, pay-as-you-use, in cloud computing terms. With this cloud computing, a smart phone can become a large data center. Back in the early 1990s, engineers began using clouds as a metaphor for the Internet in textbooks and diagrams. The structure of the Internet – as seen from a distance – is amorphous like a cloud. Later, *the cloud* was used as a way to represent Internet-based services.

In practical terms, cloud computing is an array of networked computers that allow you to offload processing tasks or storage from your embedded system. It is a simple idea, but one that hides a lot of underlying complexity. Many companies have launched services that try their best to simplify this complexity; these include Apple's iCloud, Google Cloud Platform, Microsoft OneDrive, and others. But these cloud computing systems are intended for use with personal computers, and embedded developers need something similar for IoT devices. Industry analysts forecast



the creation of *billions* of IoT devices by 2020, and these devices will produce huge amounts of data. Storing that data locally and temporarily will not be possible any more. There is going to be a need of rental storage space. Also, this huge amount of data must also be utilized in the way it deserved. Data must not only be processed to form information and further, to form knowledge, but it should be made a mean of wisdom for the user. This asks for more processing, which is not possible at the IoT end, where devices are low cost and light-weight. Again, processing and computation must also be available there on rental basis. All this is possible with cloud computing. IoT and cloud computing working in integration makes a new paradigm.

In Cloud computing, most of the computing resources exist on the Internet on servers, as opposed to client machines such as laptops or personal computers. Cloud computing is commonly associated with Information Technology (IT) services, but can theoretically be extended to embedded software programming [10]. Integrating Cloud computing with Wireless Sensor Networks (WSNs) brings the concept of Cloud-based embedded system programming. Not surprisingly, people and embedded devices use the Internet very differently. People make use of the Internet largely through the World Wide Web — a set of applications that run on the Internet. Of course, the Web is not the entirety of the human interface for the Internet. We also use e-mail, text messages, mobile apps, and bevy of social media tools.

In the Internet of Things, by comparison, autonomous electronic devices exchange information with each other over the Internet. But these devices do not yet have the machine equivalent of Web browsers and social media. We are at the beginning of the development of these new tools and services.

5. CURRENT SCENARIO AND TYPES OF DDOS ATTACK IN CLOUD ENVIRONMENT

According to Cloud Security Alliance, DDoS is one of the top nine threats to cloud computing environment. Out of many attacks in cloud environment 14% are DoS attacks. Many popular websites like yahoo were affected by DDoS in early 2000. Website of grc.com was hit by huge DDoS in May, 2001. The company was dependent on internet for their production work and business was greatly impacted. Forrester Consulting was contracted by VeriSign in March 2009 to perform a study on DDoS threats and protection. The survey was performed among 400 respondents from the US and Europe 74% had experienced one or more DDoS attacks in their organizations. Out of this 74%, according 31% the attacks caused service disruption, according 43% attacks does not result into services disruption as shown in Fig.1 [4]

Distributed Denial of Service (DDoS) attacks typically focus on large number of IP packets at specific network entry elements. In cloud computing where infrastructure is distributed between large number of clients, DDoS attacks make have the potential of having much greater impact than against single inhabitated architectures [9]. The two main goals of the attacker are:

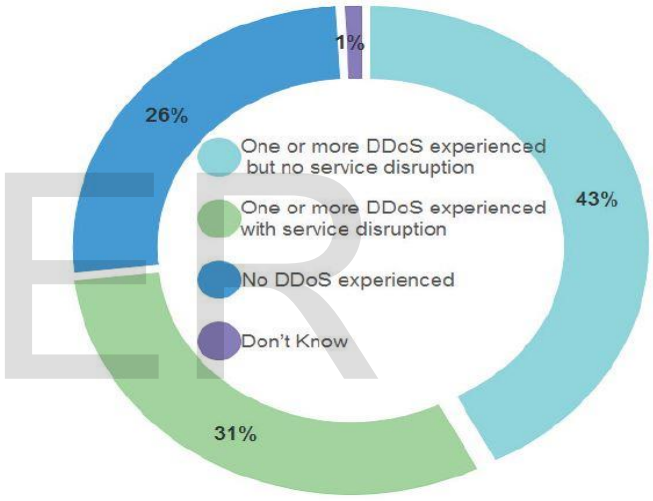


Image Source [International Journal of Computer Engineering and Applications, Volume VII, Issue II, August 14.][4]

- Bandwidth Depletion Attacks: This type of attack consumes the bandwidth of the victim or target system by flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim network.
- Resource Depletion Attacks: The DDoS Resource depletion attack is targeted to exhaust the victim system's resources, so that the legitimate users are not serviced.

6. Defense Mechanisms against DDoS Attack using SDN features

Software Defined Networks provide an ideal platform for distributed detection and mitigation of DDoS attacks, because-

6.1. The whole concept of SDN is flow based.

6.2. There is a logically centralized controller and view of the network.
6.3. Standardized API has been used for control and data plane communication.
6.4. The data plane and control planes are decoupled which enables to establish easily large scale attacks and defense experiments.
6.5. The programmability of SDN supports a process of harvesting intelligence from existing Intrusion Detection Systems (IDSs) [5] and Intrusion Prevention Systems (IPSs) [7].
6.6. Software-based traffic analysis greatly enables innovation, as it is possible to improve the capabilities of a switch using any software-based technique [8]. Traffic analysis can be performed in real time using machine learning algorithms, databases and any other software tool. Traffic of interest can be explicitly directed to IPSs for Deep Packet Inspection (DPI) [12].
6.7. Dynamic updating of forwarding rules helps promptly respond to DDoS attacks. Based on the analysis, new or updated security policy can be propagated across the network in the form of flow rules [8]. If attacks are detected, SDN can install packet forwarding rules to switching devices to block the attack traffic from entering and propagating in a network [12].

Most source based mechanisms using SDN let SDN controllers detect anomaly traffic, filter the malicious packet, or validate the source IP address near the ingress of network. Also, the Flow Collector module is responsible for periodically requesting flow entries from all Flow Tables of OF switches. Apart from these, IP traceback can be used to find the origins and paths of attacking traffic. However, so far, most approaches for IP traceback are hard to be deployed in the Internet because of deployment difficulties.

7. CONCLUSION AND FUTURE WORKS

In this paper, we have discussed on current scenarios of Internet of Things integrated with Cloud Computing environment as well as Software Defined Networking features. Also, we have discussed on present scenario of security threats, i.e. DDoS attack in this environment and various mechanisms to mitigate those attacks using SDN. This work may help to to prepare a new architecture of SDN enabled secured *Cloud of Things* environment.

8. REFERENCES

[1] Strickland, J. (8 April 2008). *"How Cloud Computing Works*". How Stuff Works. InfoSpace, LLC. Retrieved 20 May 2016.
[2] Pinola, M. (30 March 2015). *"What Is Cloud Computing?".* About.com. About, Inc. Retrieved 20 May 2016.
[3] Rouse, M. (September 2015). "*cloud computing*". SearchCloudComputing. TechTarget. Retrieved 20 May 2016.
[4]. Rashmi D. and Kailas D. mitigating ddos attack in cloud environment with packet filtering using iptables in *International Journal of Computer Engineering and Applications*, Volume VII, Issue II, August 14.
[5] 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, Sept. 2011.
[6] Canellos, D. (5 June 2013). "*How the "Internet of Things" Will Feed Cloud Computing's Next Evolution"*. CSA Industry Blog. Cloud Security Alliance. Retrieved 20 May 2016.
[7] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, pp. 1–7.
[8] A. Lara, A. Kolasani, and B. Ramamurthy, "Network innovation using openflow: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, Fourth Quarter 2013.
[10] J. Bungo, "Embedded Systems Programming in the Cloud: A Novel Approach for Academia," Potentials, IEEE, vol. 30, pp. 17-23, 2011.
[11] S. Sezer, S. Scott-Hayward, P.-K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "*Are we ready for SDN? implementation challenges for software-defined networks*," IEEE Commun. Mag., vol. 51, no. 7, July 2013.
[12] W. Xia, Y. Wen, C. Foh, D. Niyato, and H. Xie, "A survey on softwaredefined networking," *IEEE Commun. Surveys & Tutorials*, vol. 17,no. 1, pp. 27–51, First Quarter 2015.
[13] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 2, pp. 843–859, Second Quarter 2013.