ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 7, July 2016

Anomaly Based DDoS Attack Detection Mechanism using SDN in Cloud computing

Nishtha Goel
Mtech. Student
Dept. of Computer Science and Engg.
DCRUST, Murthal
Sonepat, India

Dinesh Singh
Assistant Professor
Dept. of Computer Science and Engg.
DCRUST ,Murthal
Sonepat, India

Abstract-: Cloud computing has recently came into view as a new paradigm for hosting and delivering services over the Internet. Cloud computing is captivating to business owners as it eliminates the requirement for users to plan ahead for providing, and allows enterprises to start from the small and increase resources only when there is a rise in service demand. Meanwhile, Software Defined Networking (SDN) is a network framework that provides the central control over the network . Central control is provided by using a Controller, which acts as an operating system. This operating system can send instructions and apply changes through its interface. The main objective of this paper is to study the impact on DDoS attack defense mechanisms, in an enterprise network where both technologies are adopted.

Keywords: Cloud Computing, Software Defined Networking , DDoS attack , Openflow.

1. INTRODUCTION

With the swift development of processing and storage technologies and the success of the Internet, computing resources have become economic, more powerful and more pervasively available than ever before. This technological trend has enabled the apprehension of a new computing model called **cloud computing**, in which resources (e.g., CPU and storage) are provided as general utilities that can be leased and liberated by users through the Internet in an on-demand fashion. In a cloud computing environment, the traditional responsibility of service provider is divided into two: the **infrastructure providers** who manage cloud platforms and charter resources according to a usage-based pricing model, and **service providers** , who lease resources from one or many infrastructure providers to serve the end users[1]

Some characteristics of Cloud Computing that make it attractive to business owners, as shown below :

1) **No up-front investment**: Cloud computing uses a pay-as you-go pricing model. A service provider does not need to expend in the infrastructure to start attaining advantage from cloud computing. It simply lease resources from the cloud according to its own needs and pay for the usage.

2) **Lowering operating cost**: Resources in a cloud environment can be rapidly allocated and de-allocated on demand. Hence, a service provider no longer needs to provide capacities according to the peak load. This provides huge savings since resources can be released to economize on operating costs when service demand is low.

3) **Highly scalable**: Infrastructure providers pool large number of resources from data centers and make them easily accessible. A service provider can easily expand its service to large scales in order to handle rapid increase in service demands [2].

1.2 Software Defined Networking

SDN is a network framework that separates the data plane and the control plane of network switches and moves the control plane to a centralized application known as network controller. The network controller maintains the entire network through a vendor-independent interface called as OpenFlow [3] , which defines the low-level packet forwarding behaviours in the data plane. Figure 2 shows different layers of SDN structure. The application layer will have a single view of the network through the control layer and the whole system looks like one logical switch. The control layer is where the controller abstracts the network infrastructure from the application layer. By using the control layer, any configurations and modifications can be done in real-time. In the infrastructure layer, there is no need for each device to learn different protocols and the only task left is forwarding [4].

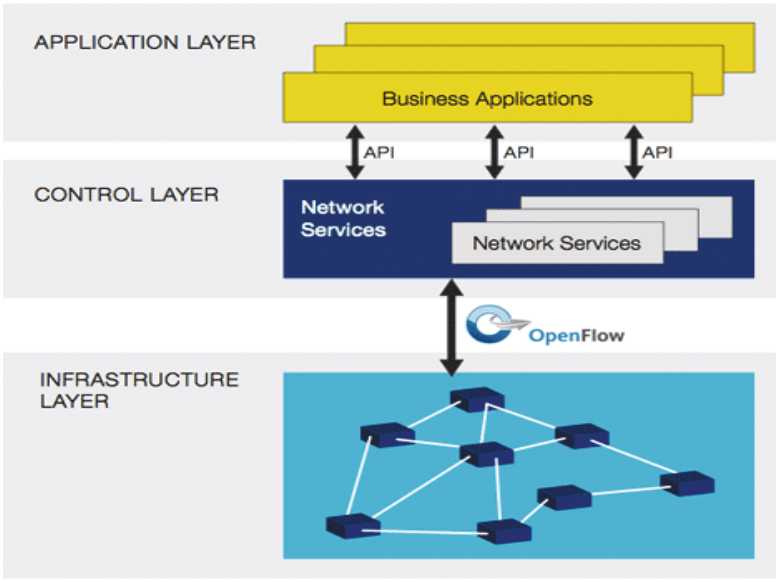

Fig 2. SDN Structure [4].

.

As cloud computing provides on-demand, elastic, and unrestricted computing services, more and more enterprises begin to embrace this prototype shift by moving their database and applications into the cloud. At the same time, another epochal concept of the Internet architecture comes to limelight, i.e., Software-Defined Networking (SDN). While cloud computing facilitates the administration of computation and storage resources, SDN is proposed to address another laborious issue hindering the progression of today's Internet, i.e., the complicated network management. Besides the fact that SDN has been proposed as a candidate of the next procreation Internet architecture, companies like Google have already adopted SDN in their internal data centers. Thus, the advent of the era when cloud computing and SDN go hand-in-hand in providing enterprise IT services is looming on the horizon [5].

2. Issues related to Cloud Computing

Using Cloud results applications and data will move under third-party control. The cloud services delivery model will devise clouds of virtual perimeters as well as a security model with responsibilities shared between the customer and the cloud service provider. This shared responsibility model will bring new security management confrontations to the organization's IT operations staff.

Some of the issues related to the cloud are:

i) Data location: When clients use the cloud, they presumably won't know exactly where their data are hosted. Distributed data storage is a typical manner of cloud providers that can cause absence of control and this is not good for customers who have their data in local machine before moving from local to
cloud.

ii) Long-term viability: Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be certain their data will remain available even after such an event.

iii) Data Leakage: Ineptly, when moving to a cloud there is two changes for customer's data. First, the data will store distant from the customer's local machine. Second, the data is moving from a single-tenant to a multi-tenant environment. These changes can raise an important matter that called data leakage. Because of them, Data leakage has become one of the greatest organizational venture from security standpoint [6].

2.1 Cloud Security Issues

Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Identical to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well.

An unauthorized user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can asset which physical servers the victim is using then by implanting a malicious virtual machine at that location to cast an attack [7]. Because all of users who use same virtual machine as infrastructure, if a hacker abduct a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can replicate them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with investigating the data may be find valuable data afterward [8].

1) Attacks in cloud

Nowadays, there are various attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have awful purposes. A hacker can use a cloud to provide a malicious application for achieve his object which may

be a DDoS attacks against cloud itself or arranging another user in the cloud.

a) DDoS attacks against Cloud

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]. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks.

b) Cloud against DDoS attacks

DDoS attacks are one of the powerful threats available in world, especially when casted from a botnet with huge numbers of zombie machines. When a DDoS attack is casted, it sends a heavy flood of packets to a Web server from multiple sources. In this situation, the cloud may be part of the solution. it's interesting to consider that websites experiencing DDoS attacks which have limitation in server resources, can take benifits of using cloud that provides more resource to tolerate such attacks. In the other hand, cloud technology offers the advantage of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown.

3. DDoS Attack and Its Mitigation

The Distributed Denial of Service (DDoS) attack is a well-known malicious attempt to exhaust the resources of a computer or a network of computers by sending heavy traffic to them [10]. The two main goals of the attacker are:

i) Bandwidth depletion.
ii) Resource exhaustion [11].

DDoS attack starts from an attacker planting a code in compromised PCs which are referred to as Botnet. At the time of the attack, these codes are run and a stream of traffic is directed towards the victim. A more sophisticated attack uses a thin layer of compromised PCs called handler to control a larger number of PCs called zombie hosts. The zombie hosts are responsible for generating the attack traffic [11]. Using botnets makes the attack more concentrated and keeps the perpetrator hidden behind the scene.

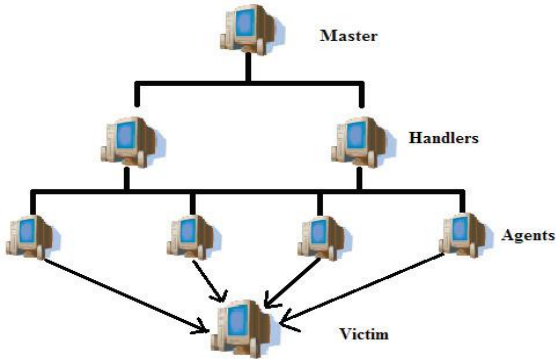

Fig.3 DDoS Attack Components [12]

3.1 Anomaly Detection for DDoS Mitigation

The common factor in different types of DDoS attack is the abnormal traffic sent to the victim. In normal circumstances, there is a pattern in the network activity and an accepted rate of bandwidth consumption. If

there is a sudden increase in traffic, delay, CPU utilization, or sudden drop in performance of any of the network assets, this, often, will be considered abnormal. Any DDoS detection will be looking for such abnormalities in the network. In general, anomalies are related to the nature of data in the network [10]. Understanding the type of data and its characteristics in the network is the first step to detecting anomalies. These characteristics can be packet header information, delay, packet size, protocol, etc. If a network is susceptible to a certain type of threat, then detection and mitigation of the threat has to be matched to it.

3.2 Types of Anomaly Detection Techniques

In IP networks, there is a certain bandwidth and certain processing power for carrying traffic. When some attributes of the network are subjected to statistical analysis, for each attribute a pattern will appear. The longer the time, the more reliable is the pattern. However, this is only true if the network has a steady traffic all the time. If there are variations that are accepted as normal traffic, in the long run, the statistics will stabilize and cannot be considered completely reliable.

Statistical analyses and machine learning are two of the common methods of anomaly detection.

1. Statistical analyses, like Entropy and Chi-Square techniques, have been suggested for detecting change in network traffic [14].

Entropy represents packet headers as independent information symbols with unique probability of occurrence. It is a common method for DDoS detection [15] [16] [17]. By selecting a window of some number, 10,000 for instance, and moving the window forward, a pattern will emerge with probabilities for each type of packet header. Drastic changes in the bins of each header that deviates from the average bin limits will alert the system of anomalies.
If a certain type of intrusion is expected and the type of packet header is known, then Chi-Square is a better model. For instance, if TCP SYN flood is the expected type of attack, then sampling bin of data and measuring the number of TCP SYN headers will show a pattern of the average number of such headers. Any deviation beyond the recognized limits is assumed abnormal.

Equation 3.2.1 shows Chi-Square equation. Ni is the number of packets for one sample and ni is the expected number of packets in normal circumstance. The value of targeted packets per bin is updated as times passes and more samples are taken.

$$X^2 = \sum_{j=1}^{B} \frac{(Ni - ni)^2}{\text{ni}}$$

Equation 3.2.1.

2. **Machine learning and cognitive detection is another method used for defending networks against intrusion**. Instead of setting up a fixed filter an algorithm is trained to constantly update its

filtering criteria based on the events of the network.

An example of such system is neural networks [15]. Neural networks consist of several nodes working in parallel to process data. They work like human brain. When they are trained or given a large amount of information, the collective knowledge of neurons or nodes develop a pattern for the processing of similar data. Three main layers of neural networks are input, output and hidden layers in the middle to process the input data. As time passes and more data is processed, the nodes are learning more and a clearer pattern emerges.

4. Related Work

Bing Wang et. al. (2015) suggested "DDos Attack Prevention Model for Cloud Computing using Software Defined Networking" [5]. This paper proposes a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to enable attack detection and an adjustable control structure to allow fast and specific attack reaction. To cope with the new architecture, paper proposes a graphic model based attack detection system that can deal with the dataset shift problem. The simulation results show that the architecture can effectively and efficiently address the security challenges brought by the new network prototype and our attack detection system can effectively report various attacks using real-world network traffic.

J.RameshBabu et. al. (2014) worked over "a prevention of DDos Attack in cloud computing using NEIF technique" and proposed a model [18].The presented technique provides a way to protect the data from DDos attack , check the probity and authentication by following the best possible industry mechanism. NEIF installed at the ISPs' edge routers and plays as a dual role in defending DDoS attacks. As a first role, the goal of ingress filtering is to discover and prohibit the DDoS attacks launched from its customers. Actually, the ingress filtering has already been extensively deploying to avoid source IP spoofing by discarding packets which have a source address which is not allocated to that customer. Ingress filtering can ensure an ISP's network do not engage in flooding DDoS attacks. Ingress filtering craves the understanding between Internet Service Providers (ISP's) so it takes large amount of time to implement at all ISP's. Egress filtering is used to protect ISP's customers from being attacked.

Anup Bhange et. al. (2012), worked over **"**DDos attack impact on network traffic and its detection approach**"** and discussed a statistical approach to analysis the distribution of network traffic to recognize the normal network traffic behavior. The EM algorism is deliberated to approximate the distribution parameter of Gaussian mixture distribution model [19].

Poonam Yadav et.al. (2013) described "An Architecture for Security and DDoS Defence using Two-tier CAPTCHA" [20]. CAPTCHA (Completely Automated Public Turing Tests to Tell Computers and Humans Apart) is used for Graphical Turing Test. There are many OCR or Non-OCR based

CAPTCHA's are used widely but they are vulnerable to many attacks like Pixel-Count Attack, Recognition by using OCR, Dictionary Attack, and Vertical Segmentation.

Rashmi V. Deshmukh et. al. (2015) defined "DDoS attack and its effect on the Cloud Computing Security" [21] and provide classification of DDos attack as : Bandwidth depletion attacks and Resource depletion attacks. Various countermeasures had been adopted and still developing for mitigating against the DDoS attacks. Mostly DDoS attacks are influenced by an intruder attempting to make an unlawful access in the victim system/network. The paper describes various prevention techniques and defense mechanisms.

5. Discussion and Conclusion

Cloud computing has recently emerged as a imperative paradigm for managing and delivering services over the Internet. The rise of cloud computing is swiftly changing the landscape of information technology, and ultimately turning the long-held promise of utility computing into a reality.

Cloud computing is already here to stay and SDN is gaining increased popularity. With both of the technology looming as the future enterprise IT solutions, it is worthwhile to look at the implications of the combination of the two, notably on the enterprise network security. In this paper, we analyze the impact of cloud computing and SDN on DDoS attack defence. Based on our analysis, we identify the challenges and the benefits lifted by these new technologies. We claim that with careful design, SDN could help with DDoS attack protection .Various anomaly based technique discussed above uses statistical analysis method which provides solution to detect DDoS attack by using entropy mechanism. By applying entropy as a detection method, we were able to detect attacks on one host or a subnet of hosts in a network. We believe that this is an effective method in addressing the detection of DDoS in SDN with accuracy and efficiency.

6. Future Work

The entropy based method detects the attacks when the entire network is being targeted by DDoS. When malicious packets are targeting every host, entropy might not change by a large margin. Detecting such attacks will be an addition to this research.

.

REFERENCES

[1] Q. Zhang, L. Cheng , R. Boutaba, "Cloud Computing: State of the art and research Challenges" , Springer, pp. 7- 18, April 2010.

[2]M. Armbrust et al. Above the clouds: a Berkeley view of cloud computing. UC Berkeley Technical Report , 2009.

[3] T. Anderson, H. Balakrishnan, G. Parulkar, J. Rexford, S. Shenker, J. Turner N. McKeown, "OpenFlow: enabling innovation in campus networks," ACM SIGCOMM, vol. 38, no. 2, pp. 69-74, April 2008.

[4] Open Networking Foundation. (2014, Jan.) ONF. [Online]. https://www.opennetworking.org/

[5] B. Wang ,Y. Zheng ,W. Lou and Y.T. Hou . , "DDoS attack prevention in the era of Cloud Computing and Software Defined Networking", Elsevier, 2015.

[6] C. Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009

[7] N. Mead, et al, "Security quality requirements engineering (SQUARE) methodolgy," Carnegie Mellon Software Engineering Institute.

[8] J. W. Rittinghouse and J. F. Ransome, Cloud Computing: Taylor and Francis Group, LLC, 2010

[9] T. Mather, "Data Leakage Prevention and Cloud Computing.", 2011.

[10] M. Masikos, O. Zouraraki C. Patrikakis. (2004, December) CISCO. [Online]. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

[11] A. Mitrocotsa C. Douligeris, "DDoS Attack and Defence Mechanism: A Classification," in Singnal processing and information tecnology in 3rd IEEE International Symposium, pp. 190-193, Apr 2003.

[12] Prolexic. (2013, December) DoS and DDoS attack reports, trends and statistics. [Online]. http://www.prolexic.com/knowledge-center-dos-and-ddos-attackreports.html

[13] Google, Arbor. (2013, Oct) Digital Attack Map. [Online]. http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16003&view=map

[14] D. Schnackenberg, R. Balupari, D, Kindred L. Feinstein, "Statistical Approaches to DDoS Attack Detection and Response," in DARPA Information Survivability Conference and Expedition, vol. 2003, Apr.

[15] Z. Qin, L. Ou, J. Liu, A. X. Liu J. Zhang, "An Advanced Entropy-Based DDoS Detection Scheme," in International Conference on Information, Networking and Automation, pp. 67-71, 2010.

[16] I. Ra G. No, "An efficient and reliable DDoS attack detection using fast entropy computation method," in International Symposium on Communication and Information technology, pp. 1223-1228 , 2009.

[17] Y. Chen , X. Ma, "DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy," IEEE Communications Letters, vol. PP, no. 99, pp. 1-4, 2013.

[18] J. RameshBabu , B. SamBalaji , R.W. Daniel and K. Malathi , "A prevention of DDoS attack in Cloud Computing using NEIF technique ", International Journal of Scientific and Research Publications, Vol. 4, April 2014.

[19] B. Bhange , A. Syad and S. Thakur , " DDoS Attacks Impact on Network Traffic and its Detection Approach", International Journal of Computer Applications, Vol. 40– No.11, February 2012.

[20] P. Yadav and Sujata, " Security Issues in Cloud Computing Solution of DDoS and Introducing Two-Tier CAPTCHA", International Journal on Cloud Computing:

Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013.

[21] R.V. Deshmukh , K.K. Devadkar , "Understanding DDoS Attack & Its Effect In Cloud Environment",Elsevier, 2015, Procedia Computer Science 49 , pp. 202 – 210 , 2015.

[22] A.M. Lonea ,*D.E.* Popescu and H. Tianfield ,"Detecting DDoS Attacks in Cloud Computing Environment" INT J COMPUT COMMUN, pp. 70-78, February, 2013.