ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Distributed Denial of Service (DDOS) Attack Detection in Software Defined Networking with Cloud Computing

Dr.T.Pandikumar[1], Tesfa Belissa[2]
Associate Professor[1], M.Tech Student[2]
Department of Computer & IT
College of Engineering, Defence University, Debre Zeyit, Ethiopia

Abstract:
Cloud computing has almost swept the IT industry replacing the enterprises' traditional computing. With the recent developments in cloud computing has also grown the threats to the security of cloud services and data. Amongst the many security issues, DDoS has its way in threatening the availability of the services provided by the cloud to the intended users. To detect and mitigate these attacks, a classifier algorithm and a forecasting algorithm are used respectively. With these algorithms deployed in SDN architecture, we can greatly reduce the DDoS attacks in the cloud thereby providing the cloud users uninterrupted services.

Keywords: Cloud computing, DDoS attacks, availability, SDN, classifier algorithm, forecasting algorithm

1. INTRODUCTION

Cloud computing is an emerging technology now widely being adapted by companies and organizations which help them to reduce operating costs while increasing efficiency. Even though used by many, still security needs to be focused on to make the renters to use the resources free of threats and attacks to the data stored in the cloud. Cloud computing is fast replacing the traditional way of computing and storage of data. What delay the even faster migration are the security issues in the cloud. Threats to the security of data in cloud have been almost addressed. Yet newer, more efficient solutions are evolved day by day. Low-cost, pay-by-use models can be used to deploy and scale services and benefits in cloud computing. Meanwhile the users who use the services can also enjoy the flexibility provided by the Internet based computing. Users enjoy the on demand provisioning of computing, storage and networking resources according to a pay-per-use business model. Most of the enterprises embrace the paradigm of cloud computing by moving their database and their applications into the cloud. In the recent years, cloud computing has become a widely accepted computing paradigm built around core concepts such as on-demand computing resources, elastic scaling, elimination of up-front investment, reduction of operational expenses and establishing a pay-per use business model for information technology and computing services. Cloud computing makes it possible for content providers to quickly deploy and scale services and benefit from low-cost, pay-by-use models, while service users enjoy the flexibility that Internet-based computing provides. Cloud computing enables users to benefit from on demand provisioning of compute, storage and networking resources according to a pay-per use business model [2]. Resources can be shared from the pool of resources in cloud computing. Cloud computing aims to cut down costs while resources are used as needed. Cloud computing adopts concepts from the service oriented architecture. This helps the user to break the problems into services that can be integrated to provide a solution. The advantages of the cloud computing are: agility, cost reductions, device and location independence, easy maintenance, multi contract, increased productivity, reliability, scalability and elasticity. As per NIST's definition, the five characteristics of the cloud are: on demand self-service, broad network access, resource pooling, rapid elasticity, measured service. Cloud computing provides enormous benefits including on-demand, elastic and pay-as-you-go based accessible computing. Amidst all these benefits presented to the user, there are a lot concerning about security and privacy issues in the cloud. The prevalence of cloud computing is blocked by its security to a great extent. When data is stored in cloud, the risk of data being safe is higher as it is prone to many accesses. DDoS is the acronym for Distributed Denial of Service. It is an attack to make the online services unavailable by overwhelming it with traffic from multiple resources. In this attack, usually Trojan infected multiple systems are used to target a single system which provides service so that the service is denied to the legitimate users. DDoS attack is a major threat since cloud is a resource pool wherein the resources are shared at host level, browser level, network level and server level. It is an attempt to make a service unavailable to its intended user by draining the system or network resources. Many compromised systems are used to send malicious traffic to the target server so that the server would process the malicious traffic instead of servicing the requests from the users. The two main objectives of the DDoS attacks are to overwhelm the server resources and then to hide the identity of the hackers. These attacks affect the organizations costing them more time and money. By exploiting the flaws or vulnerabilities in a computer system, a malicious hacker is able to perform DDoS attack. In such case, a web site or a web server is posed as a master system. Further compromise can be done by the hacker after identifying and communicating with other systems when posed as the master system. Recently, software defined networking (SDN) has attracted much interest as a new paradigm in networking [3]. Although SDN brings numerous benefits by decoupling the control plane from the data plane, there is a contradictory relationship between SDN and DDoS attacks. On one hand, the capabilities of SDN (e.g. software based traffic analysis, logical centralized control, global view of the network, and dynamic updating of forwarding rules) make it easy to detect and to react to DDoS attacks rapidly. On the other hand, the

separation of the control plane from the data plane introduces new attacks. Consequently, SDN itself may be a target of DDoS attacks. Indeed, potential DDoS vulnerabilities exist across the SDN platform [4]. For example, an attacker can take advantage of the characteristics of SDN to launch DDoS attacks against the control layer, infrastructure layer, and application layer of SDN.

1.1 Background

Security issues are becoming the greatest challenge in the era of cloud computing. These issues eventually reduce the growth cloud computing market effecting enterprise business and industries. Internet security is the major concern in Cloud computing. These are several threats to Cloud computing such as worms, spams, phishing attacks etc. Recently, a new severe threat has come to light know as Botnet. Botnets are the main cause of malicious activity in the Cloud computing. Attacker sends malicious content to the computer over the internet. Once those computers become victim of Botnet, they act like a bot for the attacker. These bots form network that being controlled by the attacker. Several malicious activities can be formed using Botnet like leakage of sensitive information etc. but one of the severe attacks is DDoS. In DDoS attack, when a huge number of queries come to the server, the server increases its computational power and starts to entertain every request. The server system has the limited capacity to entertain the number of user request at a time. So, when a huge a number of fake request or queries come to the server, the server gets busy and the actual user request cannot be entertained in that period. Hence the denial of service occurred. Usually, the cloud network is a distributed system, therefore, distributed denial of service happens more often [2]. To the best of our knowledge, the contradictory relationship between SDN and DDoS attacks has not been well addressed in previous works. Essentially, it is the unique dynamics tied with SDN and DDoS attacks that present unique challenges beyond the existing works. We believe that these initial steps we have taken here help understand how to make full use of SDN's advantages to defeat DDoS attacks in cloud environments and how to detect SDN itself from becoming a victim of DDoS attacks, which are important for the smooth evolution of SDN-based cloud without the distraction of DDoS attacks[1].

1.2 Problem Description

At present, network security can be considered a major issue in every networking application. For this reason, Although SDN-based cloud shows many good features, it faces several challenges that must be taken into consideration, including performance, availability, and scalability text band security.

- **Performance**

Performance refers to the processing speed of the network node considering both throughput and latency. The method of SDN to handle new packets brings the programmability. But at the same time it produces performance problems. So how to improve performance and keep programmability need further research.

• Availability

Availability refers to the proportion of time an SDN system is in a functioning condition. The dependence on the controller brings a challenge regarding availability. One advantage of traditional, distributed network architecture is that if a switch fails, the availability of the network can be maintained. But in a pure SDN environment, if a controller fails, the availability of the network may be complete loss.

• Scalability

Scalability is the ability to be enlarged to accommodate network growth. The controller can become a bottleneck of scalability. By introducing distributed or peer-to-peer controller infrastructure may share the communication burden of the controller. But an overall network view is required to direct the communications between the controllers using the east and westbound APIs. Besides controller scalability, there are some other scalability concerns including the flow setup overhead and resilience to failures.

• Security

By decoupling the control plane from the data plane, the attack surface for SDN is augmented, when compared to traditional networks. These days the amount of data which user send and received on internet is becoming very large, such as multimedia and other user data, therefore in order to provide good quality of service with relatively low cost, implementing of Multi-Protocol Label Switching with enhanced security is very important solution. Splitting traffic packets to sub-packets and forward to multipath multi hop wireless local area network and dynamic load balancing in multipath wireless network increase quality of service, and good throughput, ensure end-to-end packet delivery. It is difficult to avoid QoS problems, research works should be done to minimize these problems. Many research works show that Multiprotocol label switching solves QoS problem in data communication and VoIP of wired networks and ordinary wireless networks, but regarding MPLS WLANs, there is a limitation of study to improve the performance of network and security. In this area more researches should be done to improve end to end packet delivery ratio, maximize throughput, minimize packet delay, and load balancing among the same cost links and good security. Our proposal of research work focus on splitting a packet to sub-packets and distribute to multipath multi hop wireless local area network for security purpose and load balancing, our proposed technique provide alternative method of data security.

1.3 Objective of the research

The main contribution of this research is to show how DDoS can bind controller resource into processing malicious packets and add a DDoS detection mechanism to SDN controller. The contributions are as follows:

A. Show how DDoS attack can overwhelm the controller in SDN architecture. Propose a lightweight and simple DDoS detection mechanism based on entropy, in order to protect the controller.

B. Show the effectiveness of the solution through extensive simulations.

1.4 Significance of the research

The main aim of the research is detect/protect applications against DDoS attacks using SDN in cloud computing. Distributed denial-of service (DDoS) attacks pose a serious threat to network security. In this project, we have used a distance-based DDoS technique which uses a simple but effective exponential smoothing technique to predict the flooding attack [4].

1I. RELATED WORKS

2.1 Software Defined Networking (SDN) Based Cloud

Cloud computing offers an effective way to reduce capital expenditure (CapEx) and operational expenditure (OpEx). To reach this target, an agile and programmable network infrastructure is needed. SDN is the key technology that takes

network control into the cloud. In this section, we first introduce the concept of SDN, followed by SDN-based cloud. Then, we present some challenges of SDN-based cloud [1].

2.1.1 Software Defined Network

Software Defined Network is a different way of looking at networks. The main purpose is greater control over network assets. In current production networks, both control and forwarding actions are configured in the hardware by vendors, and they are, mostly, proprietary software. The SDN architecture separates control plane and forwarding plane and allows network admins to take over the control plane. This separation is done by restructuring the network so the switch will receive instructions for forwarding instead of using its resources for processing the incoming packets. The switch will contain tables with flows that instruct forwarding. Open flow is the protocol that orchestrates the SDN architecture. This architecture consists of Open flow enabled switches, a controller and a secure channel between the controllers and switches. Figure 1. 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.

2.1.2 Open flow Protocol

The Open flow protocol can be considered as the workhorse of SDN. It manages the Switches in the network and allows an external entity like the controller to manipulate the flow of packets through the network. Open flow was designed as a tool focused on network research [5]

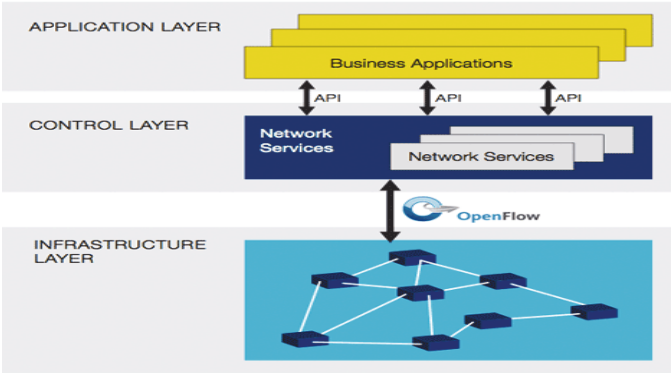

Figure .1. SDN Structure

SDN is currently attracting significant attention from both academia and industry. The Open Networking Foundation (ONF) is a nonprofit consortium dedicated to development, standardization, and commercialization of 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” ONF presents a high-level architecture for SDN that is vertically split into three main functional layers including infrastructure layer, control layer and application layer, as shown in Fig. 1[1]

2.1.3 Open flow Switch

An Open flow switch consists of a flow table or a group of them and a secure channel to the controller. Each table has a match field, counters, and a set of instructions for every entry. The matching process in the switch covers different fields of the packets' header. Table 1 shows the fields that a switch can use to find a match in its tables. In the table, there is a metadata field that is defined (second row in Table .1) as a mask-able register to carry information from one table to the other when there is more than one table. It is a mean to carry header information from one table to the other. Often switches have multiple tables that are pipelined. The packet will move from one table to the other for a match and carry the metadata. If a match is found, the metadata tag will be updated accordingly. Any packets entering the switch will be checked against all existing flows in the tables. If a match is found, the action assigned to that entry is applied and the counter for the entry will be updated.

Table .1. Packet header match fields

Header Field
Ingress Port
Metadata
Ether src
Ether dst
Ether type
VLAN id
VLAN priority
MPLS label
MPLS traffic class
IPv4 src
IPv4 dst
IPv4 proto / ARP opcode
IPv4 ToS bits
TCP / UDP/ SCTP src port
ICMP Type
TCP / UDP / SCTP dst
ICMP code

New packets can be sent as a whole to the controller or the switch can buffer the payload and send only the header. The latter is the default mode. When a packet is sent to the controller, it will be encapsulated and marked as OFPT_PACKET_IN message. We will refer to it as Packet In. Considering the number of switches, time of day, length of packet, priority and other factors, the controller has to process these packets and send a response with an action to deal with that packet and the packets coming after from the same source. This is the point where the processing will be completely handled by the controller and the switch will only cover the forwarding. There is a set of actions that the controller will send to the switch; forward, drop, push in a queue, quality of service and modifying a field, i.e., modifying VLAN tag, MAC address or IP address. The main actions, also called required actions, are forward and drop while queuing and modify fields are optional. The action is set for the packet in

the controller and then sent back to the switch through Packet Out message [5].

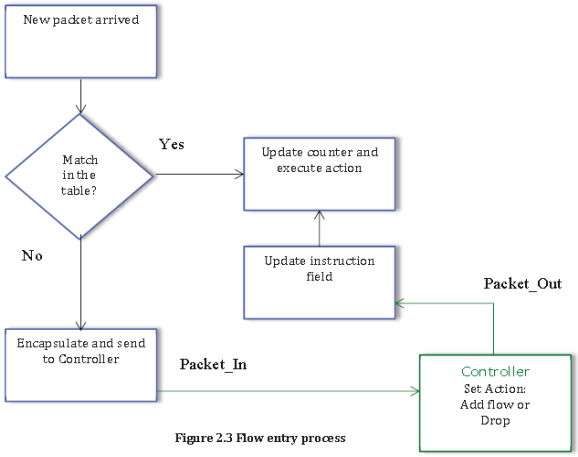

Figure. 2. Flow entry process

2.2 Benefit of SDN

SDN, with its intrinsic separating of control from data planes, brings a greater control of a network using programming. This feature would lead to potential benefits of increased configuration, improved performance of the network, and also works in favor of innovation in network design and operations [3]. These benefits are summarized in Table 2.

Table. 2. Benefit of SDN

	SDN	Conventional Networks
Features	- separated data and control plane - programmability	- a new protocol for every problem - complex network control [14]
Configuration	automated configuration with centralized validation	error manual configuration
Performance	dynamic global control with cross layer information	- limited information -relatively static configuration
Innovation	- easy implementation of the software for innovations - sufficient test environment with isolation - rapid deployment using upgrade of the software	- hard hardware implementation for innovation - limited testing environment - long standardization process

Table 2.1 Benefits of SDN

2.3 SDN Architecture Model

ONF has suggested a reference model for SDN networks [3]. It is illustrated on Figure 3 [3]. The architecture consists of three layers, stacking over each other:

- Infrastructure layer
- Control layer
- Application layer

One of the main differences between SDN and traditional networks is that the physical devices now are just forwarding elements without control functions or any software. The intelligence of the network is removed from the data plane devices to the control plane. Moreover, this networks are built on a top of open standard interfaces (Open flow and e.g), which is a crucial for enabling the communication and configuration between data plane and control plane devices. These open interfaces allow control plane to dynamically configured heterogeneous forwarding devices, which is very difficult in traditional networks. There are two main elements in SDN architecture: the controllers and the forwarding devices. The former is a software stack, while a data plane device is hardware of software element, which are specialized in packet forwarding.

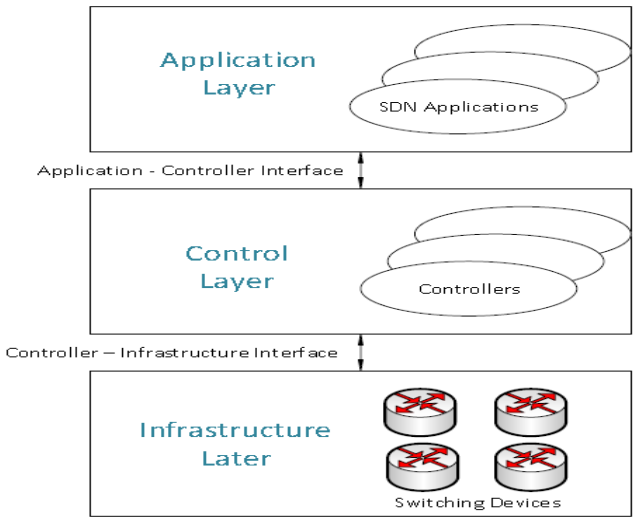

Figure 3. SDN Architecture

I1I.DDOS ATTACKS AND ITS MITIGATION FACTORS

One of the main reasons that make the DDOS attacks widespread and easy in the cloud is the availability of attacking tools and the powerfulness of these tools to generate huge volumes of attacking traffic [6]. The following are the opportunities for the attackers to use attack tools easily to launch attack:

A. Internet security is highly interdependent

The launch of DDoS attack depends upon the global internet security.

B. Limited Internet resources

Each Internet host has limited resources that can be consumed by a sufficient number of users.

C. Control is distributed

Due to privacy concerns of the Internet, sometimes it is nearly impossible to investigate the cross network behavior and to deploy certain global security mechanism.

D. Multipath routing

This causes authentication process difficult and hence it may leads to unauthorized activities. Intermediate router forwards IP packet from source to destination without knowledge about the IP packet whether it is genuine or not.

3.1 DDoS as the Main Threats to Cloud Computing

DDOS attack is a large scale coordinated attack on the availability of service of a target system or network bandwidth. There are various DDoS attacks to disrupt the cloud services. Among these attacks, ICMP (ping) flood where the attackers consumes bandwidth that use ICMP packets, ping of death attack in which the attackers sends multiple malicious pings to a cloud resources (servers), HTTP GET Flood, attackers send huge flood of requests to the cloud servers and consume all the resources and the smurf attack

where the attackers use CMP echo request packet to generate the denial of service attack.[6].

3.2 Anomaly Detection for DDoS Mitigation

The nature of attack, its types and mitigation techniques were briefly covered. A more thorough investigation is beyond the scope of this research as it is more focused on the affect of DDoS on SDN. As a result, the next section will focus on the DDoS in SDN. Being an ever present danger, DDoS attacks are a real threat to any network, especially, SDN. Being a new structure, and in the process of maturing, there is an opportunity for discovering weak points of the SDN for a better defense against such attacks [5].

3.2.1 Good Features of SDN in Defeating DDoS Attacks

SDN brings us new chances to defeat DDoS attacks in cloud computing environments. We summarize the good features of SDN as follows [1].

A. Separation of the control plane from the data plane:

SDN decouples the data plane and control plane and thus enables to establish easily large scale attack and defense experiments. High configurability of SDN offers clear separation among virtual networks permitting experimentation on a real environment. Progressive deployment of new ideas can be performed through a seamless transition from an experimental phase to an operational phase. Moreover it enables innovation and evolution by providing a programmable network platform to implement, experiment, and deploy new ideas, new applications. The feature of SDN brings great convenience in putting forward new thoughts and methods of DDoS attacks mitigation.

B. A logical centralized controller and view of the network:

The controller has network-wide knowledge of the system and global views to build consistent security police and to monitor or analysis traffic patterns for potential security threats. Centralized control of SDN permits dynamically quarantine of compromised hosts and authentication of legitimate hosts based on information obtained through requesting end hosts, requesting a Remote Authentication Dial In User Service (RADIUS) server for users' authentication information and system scanning during registration.

C. Programmability of the network by external applications:

The programmability of SDN supports a process of harvesting intelligence from existing Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems

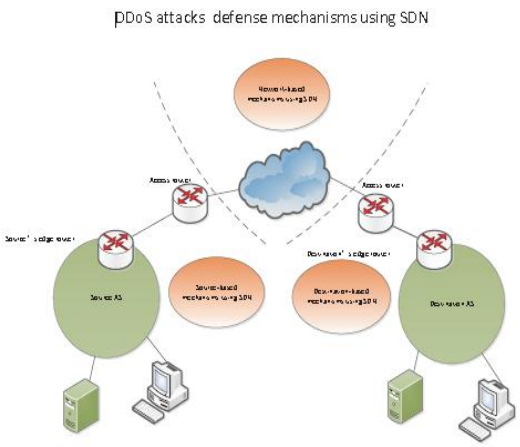

Figure.4. A classification of the defense mechanisms against DDoS attacks using SDN

(IPSs) . More intelligent algorithms can be flexibly used based on different DDoS attacks.

3.3 Software-based traffic analysis

Software-based traffic analysis greatly enables innovation, as it is possible to improve the capabilities of a switch using any software-based technique. 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).

Dynamic updating of forwarding rules and flow abstraction:

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. 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.

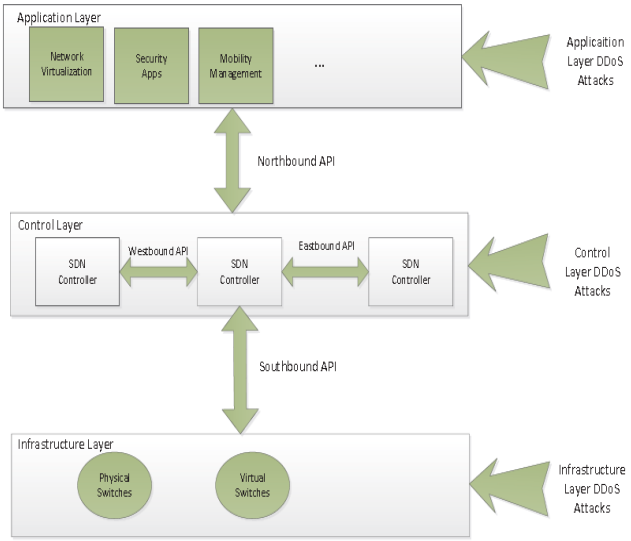

Figure.5. Potential DDoS attacks can be launched on the three layers of the SDN's architecture.

VI. CONCLUSION

In this paper, we first discussed the reasons why DDoS attacks are growing in cloud computing environments. Then we summarized the difficulty in defeating DDoS attacks in cloud computing environments. In addition, we presented some good features of SDN-based cloud in defeating DDoS attacks and discussed some challenges of SDN-based cloud. Since SDN-based cloud is still in its concept phase, we provided a comprehensive survey on some of the works that have already been done to defend DDoS attacks using SDN. We categorized the existing methods in three different class and presented a thorough comparison. Since SDN may be a victim of DDoS attacks, we reviewed the studies about how to launch DDoS attacks on SDN and how to deal with this problem. We also discussed some significant open problems, including how to defeat application-level DDoS attacks using SDN, how to defeat mobile DDoS attacks using SDN, how to implement multiple locations defensive, how to use cross-layer traffic analysis, how to cooperate among the key defensive points, and how to build a DDoS attacks tolerant system using SDN. Finally, we explored some broader perspectives, such as big data analytics, network virtualization and ICN to identify more research opportunities. In summary, SDN brings a fascinating dilemma: a promising tool to defeat DDoS attacks in cloud

computing environments, versus a vulnerable target to DDoS attacks. It is in favor of the community to study how to make full use of SDN's advantages to defeat DDoS attacks and how to prevent SDN itself becoming a victim of DDoS attacks in cloud computing environments. This paper attempts to briefly explore the current technologies related to SDN and DDoS attacks, and we discuss future research that may be beneficial in these issues.

VI. REFERENCES

[1]. Qiao Yan, F. Richard Yu, *Senior Member, IEEE,* Qingxiang Gong, and Jianqiang Li" Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges" DOI 10.1109/ COMST. 2015.2487361, IEEE Communications Surveys & Tutorials

[2]. Iqra Sattar Department of Computer Science University of Lahore (Sargodha), Muhammad Shahid Department of Electrical Engineering PIEAS, Islamabad, Younis Abbas Department of Computer Science University of Lahore (Sargodha) "A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment" 2015

[3]. Martina Stoyanova Todorova and Stamelina Tomova Todorova " DDoS Attack Detection in SDN-based VANET Architectures" June 2016

[4]. "Detecting and Preventing DDoS Attacks in Cloud" International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)*Vol. 3, Issue 3, March 2015.

[5]. Seyed Mohammad Mousavi "Early Detection of DDoS Attacks in Software Defined Networks Controller" Electrical and Computer Engineering, Carleton University Ottawa, Ontario 2014.

[6]. Nagaraju kilari Department of Computer Science, Garden City College, Bangalore, Karnataka, India , Dr. R. Sridaran, Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat, India. "An Overview of DDoS Attacks in Cloud Environment"2015