Detection And Countermeasures of DDoS Attacks in Cloud Computing

Mahmoud Said Elsayed

Nile University, Cairo, Egypt

Email:Eng.mahmoud101@gmail.com

Marianne A. Azer

National Telecommunication Institute, Cairo, Egypt

Nile University, Cairo, Egypt

mazer@nu.edu.eg

Abstract - ***Greater portions of the world are moving to cloud computing because of its advantages However, due to its distributed nature, it can be easily exploited by Distributed Denial of Service (DDoS) attacks. In distributed DDoS attacks, legitimate users are prevented from using cloud resources. In this paper, the various DDoS detection and defenses mechanisms cloud computing are reviewed. We propose a new technique based on Remote Triggered Black Hole (RTBH) to prevent DDoS attacks before it target to cloud resources.***

Keywords: BGP, Cloud Computing, DDoS, EDDoS, Eucalyptus, RTBH, Snort, vIDS, vFirewall, Virtual Machines

I. Introduction

Computing resources can be delivered via internet through cloud technology. One of the several benefits of cloud computers is solving the scalability problems. A recent survey [1] revealed the following statistics.

1- In three years, 55% of business applications permit direct API access for its major applications.

2- By 2018, the cloud will be the best preference Delivery Mechanism for Analytics, 150% increasing in Public Data Consumption and Preparing the way for many new industry applications.

3- By 2018, 85% of Enterprise IT Organizations will commit to Multi-Cloud Architectures.

4- By 2018, the expected number of Cloud Industries will Triple compared to 2016.

5- By 2020, at least 50% of IT Spending will based on cloud. Although cloud computing has become ahead of world communications today, there many security concerns. One of the most critical issues on cloud is availability problem which represents 83.3% from security concerns [2]. The availability issue can be affected by DDoS attacks especially the cloud payment that depends on the pay as use concept. Research labs of Kaspersky and Symantec have concluded that the majority of threats to internet security were by DDoS. The average attack size increased to 800 Gbps in the year 2016 and the attack size has been growing year over year. The DDoS growth from year 2007 to 2016 is shown in Fig. 1 [3].

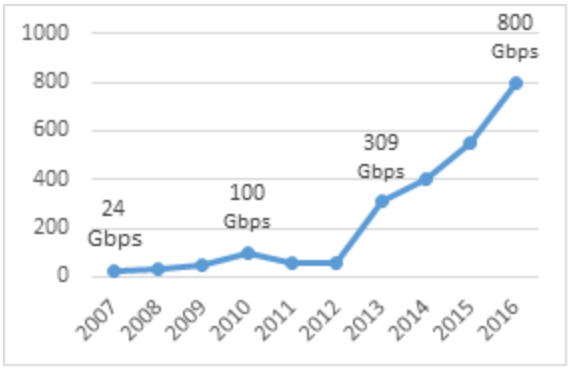

Fig. 1. Average attack size [3].

There are two main categories of DDoS attacks [4]:

1- *Bandwith Attacks:* This type of attacks exhausts resources like network bandwidth or equipment's by overflowing it with a high volume of packets [5]. The most common type of bandwidth attacks is flooding attack. In the flooding attacka large number of TCP, UDP and ICMP packet flood the network when directed to a specific target which can fail under the load by consuming all CPU by 99.99% and put it in a hanged state [6].

2- *Application Attacks* [7]: Where attackers target the layers 7 which is the end user layer of the OSI model. There are various types of applications attacks such as DNS, HTTP and HTTPS. During these of attacks, the attacking machine

generates a low traffic rate, which makes these attacks very difficult to detected or mitigated [8].

In this paper, we focus on DDoS attacks and their countermeasures Some of the various related works that have been researched and discussed to give the state of art and the future possible work in this field. We also propose a new solution to detect and mitigate DDoS based on Remote Triggered Black Hole (RTBH) technique. The remainder of this paper is organized as follows. Section II, and III present an overview of the related work, and a proposed scheme respectively. Finally, conclusions and our future work will be presented in section IV.

II. Related Work

In this section, we present the different techniques that were proposed to test the performance of networks under DDoS attacks. We also present the techniques used for attack mitigation.

The authors in [9] proposed a new system to test the performance of cloud computing applications and the quality of the network services under DDoS attack. In this test-bed, the authors tested the throughput value using open cloud applications running on Ubuntu Linux operating system with apache web server, PH5, MySQL. They used two scenarios to represent the attacks to the server. In the first scenario, three computers run DDoS on the cloud server and in the last one, the attacks were launched using 6 PCs. From analysis, the average throughput measured from experiment decreased by 11.19% from normal state in first DDoS attack scenario and decreased by 26.15% in second scenario.

Experimental tests were performed in [10] to evaluate the effects of DDoS for both network and applications attacks in cloud. Authors represented a cloud private model using the open source Eucalyptus [11]. In this test-bed the attacks were executed from two Ubuntu virtual machine act as botnets Hping3 DDoS tools to perform network attack and slowhttptest to flood http packets acting as application attacks. The experimental shows that the System is overloaded during DDoS attack and CPU utilization increased to 99.2 %.

Experimental tests to detect and analyze DDoS were presented in [12]. The authors used data mining to classify intrusion attacks by predicting correct and incorrect number of instances to get three metrics.

1. *Sensitivity:* True positives proportion in the testing dataset.

2. *Specificity:* True negatives proportion in the testing dataset.

3. *Accuracy:* Overall proportion of the testing dataset.

In these test bed, 7-types of DDoS were executed to test the attacks at network, presentation and application layers Fig. 2 [12]. Different scenarios were simulated to test and measure the performance of target VMs under different types of DOS attack. The attacks were done using one VM, two VMs and three VMs scenarios.

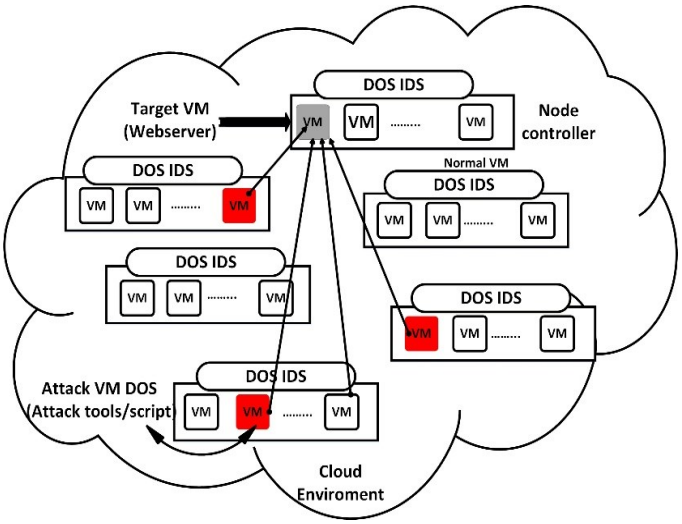

Fig. 2. Testbed setup in the cloud [12].

In most DDoS detection modules in the cloud, the amount of traffic should exceed the threshold metric to avoid false positive rate [13]. However, it very difficult to determine attack pattern because the normal traffic flow in the cloud is dynamic. The authors in [4] introduced a detection scheme based on the analysis of time series. The purpose was to reduce detection latency as well as minimize false positives and false negatives by dividing the original time series into random and trend components. A double auto correlation technique was applied; this is shown in Fig. 3 [4]. After applying anomaly detection methods for each component alone, comprehensive decisions were taken depending on the collected results at decision module. The drawback is that the authors did not present simulation results to prove they claim.

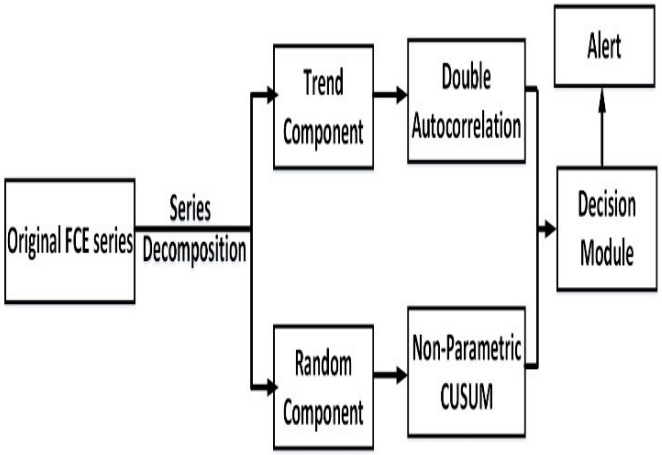

Fig. 3. Illustration of time series detection scheme [4].

A new type of DoS attacks called migrant attacks was presented by the authors in [14]. The Visualization technology allows the running machines (VMs) to be migrate between Physical Machines (PMs) on demand. The objective was to improve the quality of service, increase resource utilization and reduce power consumption through shutting down unloaded PMs and move its VMs to another server. However, the frequent migrations of VMs between PMs pulls down cloud performance [15]. More power consumption and instability of services during frequent

downtime to complete the migration process. In Migrant attack, attacker can use some batch tasks to exploit the weak isolation by test the physical machine load from various allocators. Attackers after that can use the observed threshold to deceive the allocator to falsely determine that PMs require load balance or consolidation. Authors used a test-bed to emulate the network's CPU performance using mathematical computation and compare quality load balancing performance during migrant attack.

A detection system based on anomaly detection technology to distinguish both known and unknown DoS traffic was presented in [16]. This system is divided into three stages as shown in Fig. 4 [16].

- *Stage one*: Called basic feature generation, where internal traffics are analyzed and monitored before passing through stage two.

- *Stage two:* which is divided into two sections: The first section is called Triangle Area Map Generation (TAM) to extract relevance between two distinctive characteristics within traffic from an earlier stage or from a second normalization unit section.

- *Stage three*: Is called decision making, where legitimate traffic profiles are developed. No simulations were done to support their arguments.

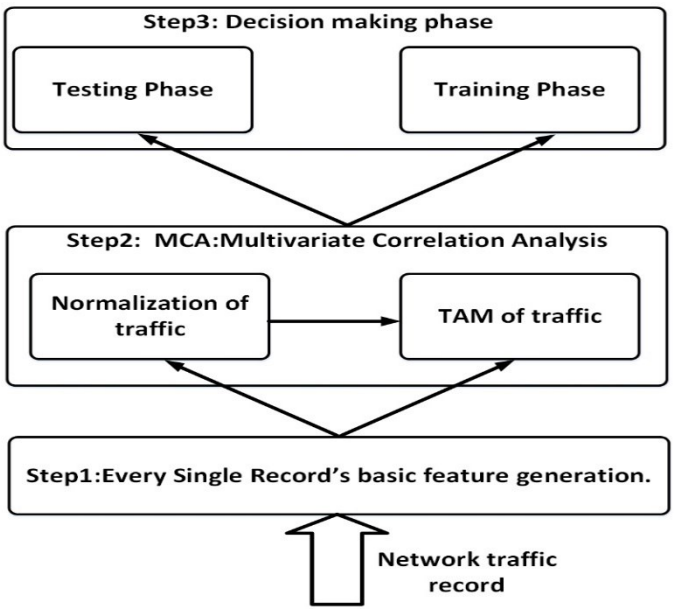

Fig. 4. DOS detection system framework [16].

An approach depending on Adaptive Pattern Attack Recognition Technique (APART) against EDoS was suggested in [17]. In cloud, payment depends on pay as you use. DDoS flood network resources to impact the cloud availability service. This leads to a new type of DDoS called Economical DoS (EDoS) as shown in Fig. 5 [17]. It is like DDoS but with different objectives. Customers who do not pay do not enjoy services. The nature of cloud to scale up automatically helps the attackers to exploit its services by sending a huge number of requests. The fake requests appear as legitimate on the surface causing the costs to rise with the up scaling. As result you will a point can be reached, where the bill is higher than the ability to pay.

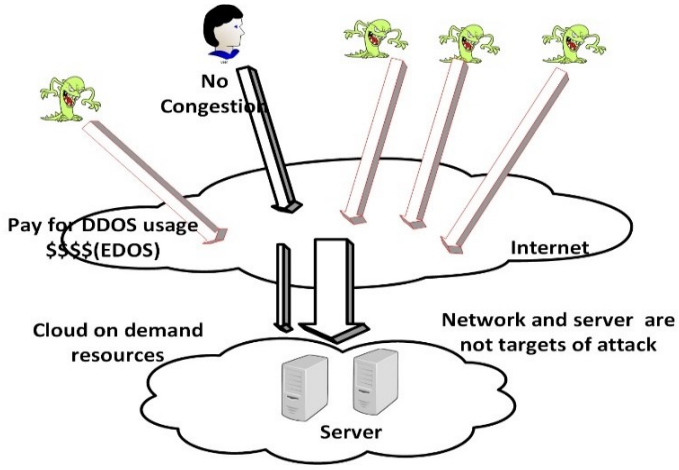

Fig. 5. EDDoS attack [17].

The authors used different attacks scenarios to test delay and performance of cloud services. The positive point in this scheme is that it used some existing security detection enhanced EDOS shilled model. Also, it worked on enhancing the existing detection techniques to detect pattern attacks, where the attackers act similar to legitimate users and send the limited traffic from many sources to exhaust the cloud processing.

A model to determine attacks location by tracing the attack path was suggested in [18]. Initially, the source router creates and inserts a Path Identification (PID) for each destination router in the routing table during routing topology creation. For example, if the packet is sourced from host connected to router A and is targeted to a host connected to router B. A new PID entry is inserted in router A packet path and this PID parameter are attached to the packet delivered. When an attack is detected, the router looks up on its path table depending on the PID value to determine the source of packets and the suitable drop policy is activated. This scheme has the advantages of consuming low bandwidth and being faster compared to others. However, amongst the drawbacks is that the insertion of new entries in the routing table may consume more processing, in addition attackers can compromise the router itself.

A system that detects the source of the packet even with spoofed packets was suggested in [19]. Fig.6 [19] illustrates the proposed detector TCP/IP header values are different from an Operating System (OS) to another. Some knowledge can be collected from received packet analysis like TTL value, total length, don't fragment and windows size. These parameters may help to detect the source of attack and determine its locations. Authors used some tools to identify remote hosts based on its OS. Active and passive fingerprints can be executed to know the OS and compare it with the known OS database. Passive test tools are used to analyze incoming packet header and match the result with known OS database to specify OS of incoming packet. In active tests, tools like NMAP are used to send probe packets to source IP and identify it OS. The last step after the OS of incoming packet is categorized, TCP/IP headers

from passive and active stage are compared for TTL value matching to avoid any chance of common OS by real source and spoofed source. If the TTL value matching is satisfied, then a true source IP address is identified, otherwise it is a spoofed IP address and dropped. The problem with this technique is that it fails to identify source of packet if it traverses on different path to destination. Also, attackers may use fingerprint concealing tools in to change and modify the source packets sent towards remote hosts.

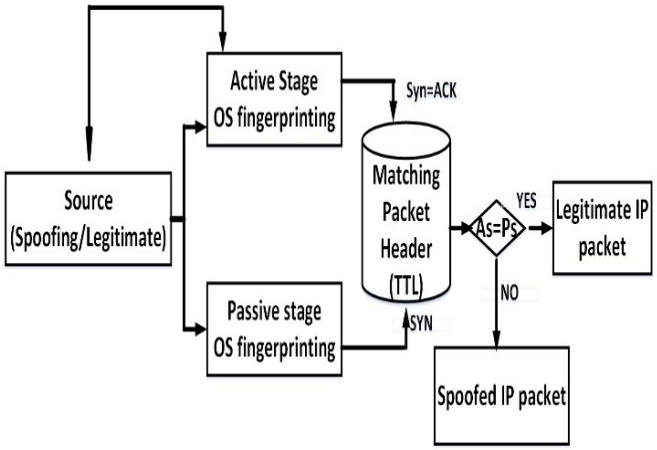

Fig. 6. Spoofed DDoS Detector [19].

III. Proposed Scheme

As it was discussed in the previous section, DDoS attacks can cause harm to the cloud infrastructures. Traditional firewalls and IDSs are unable to satisfy the large computing requirements of cloud by themselves. Firewalls do not provide proper detection against large attacks and are easy to penetrate. IDSs can't report that the attacker changes of IP address when it is spoofed. And if using IDs succeeds to detect the spoofed IP it can't identify the attackers. In addition, most of the techniques deal with a DDoS attack after detection and fall short of them in terms of mitigation and ensuring business continuity. A system that detects and mitigates the attacks before the traffic is routed to the cloud is needed.

In this section, we propose a technique that provides defense against DDoS attacks based on Remote Triggered Black Hole (RTBH) [20]. Blackhole Routing (PHR) is one of the common mitigation techniques used recently against DDoS attack [21]. In RTBH, the victim is protected from DDoS by dropping malicious traffic before it enters a protected network. Preconfigured policy on the router is configured to send the abuser packets to the null0 interface where nobody can reach it. However, the main problem with PHR is that it drops all traffic, both legitimate and malicious. In this scheme, we modify PHR solution as follows. If a DDoS attack occurs, all traffic forwarding to victim server will be redirected to the cleaning center instead of dropping it. In the cleaning center, the legitimate traffic will be filtered and redirected back to the destination server and malicious traffic will be dropped Fig. 7.

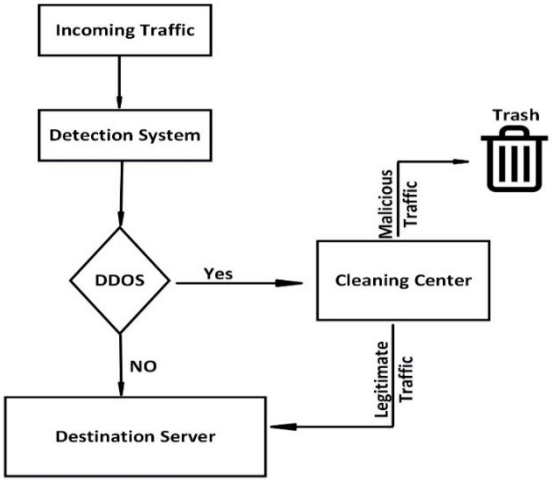

Fig. 7. Proposed scheme based on RTBH.

The Border Gateway Protocol (BGP) is the most powerful routing protocol used for connection between different Autonomous Systems (AS). The applied policy in BGP depends on a set of attributes that allow the network administrator to select the best path based on many options. BGP when used inside the same AS is called Inter BGP (IBGP). The most proper place to discard DDoS is early as possible before it enters the system to avoid any harm to cloud servers. The border routers are the suitable place to block malicious traffic. The basic setup of BGP-BHR is required preconfigured the trigger router with a static entry route to redirect all traffic to the cleaning center instead of dropping it. The trigger router will propagate the configured route to all border routers using IBGP. After BGP updates are received from trigger router, border routers will update their routing table with the new route. All traffic destined to cloud will be redirected to cleaning center to filter desired traffic and routed it again to destination victim Fig. 8.

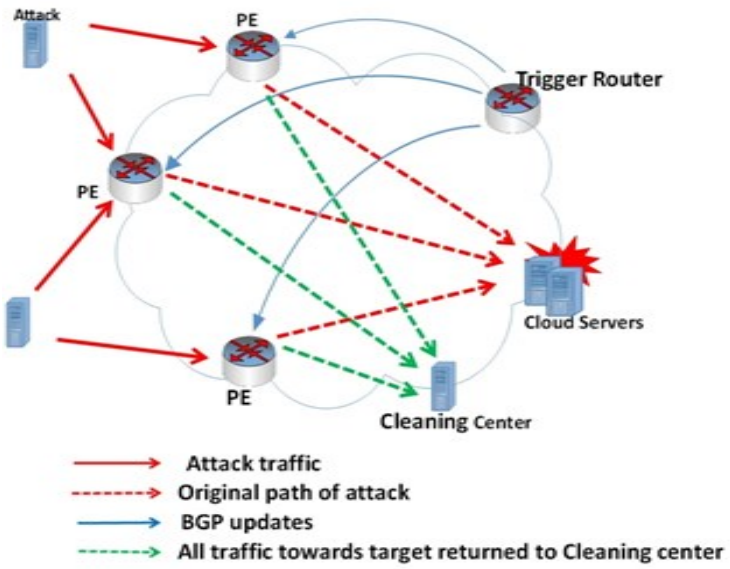

Fig. 8 Destination-Based cleaning center Filtering.

In this scheme, open source detection system SNORT with a plugin program SnortSam is added to satisfy automated detection and react with attack [22]. After the

attack is detected, SNORT detection system takes the suitable actions and sends a preconfigured route command to the trigger router, which broadcasts this update to other border routers via IBGP update. The configured route, as mentioned earlier, redirects all traffic which toward to destination victim to cleaning center.

IV. Conclusions and Future work

With propagating techniques and tools accessible to the attackers, DDoS attacks represent a great challenge to the cloud computing. In this paper, we presented DDoS attacks in cloud computing and compared different mechanisms that were used recently to detect and defense DDoS.

We proposed a new technique based on RTBH to mitigate the DDoS effect before it reaches the victim destination. In future, we plan to have a real time implementation of this system and the performance of cloud will be tested before and after applying this solution.

REFERENCES

[1] IDC FutureScape: Worldwide Cloud 2017 Predictions" https://www.idc.com/"

[2] O Yevsieieva , S Mild "Analyis of the Impact of the Slow HTTP DoS and DDoS Attack on the Cloud Environment "2017 IEEE 4th International Scientific Partial Conference Problem in Communications. Science and Technology

[3] Arbor Networks' 12th Annual Worldwide Infrastructure Security Report 2016 Available: https://www.arbornetworks.com

[4] A Khadke; M Madankar "Review on Mitigation of Distributed Denial of Service (DDoS) Attacks in Cloud Computing" 2016 IEEE, 10th International Conference on Intelligent Systems and Control (ISCO), Pages: 1-5, IEEE, 2016.

[5] Patil and Madhubala R. "Survey on security concerns in Cloud computing" 2015 IEEE, International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE,2015.

[6] Rakesh Kumar Sahu; Narendra S. Chaudhari "A Performance Analysis of Network under SYN-Flooding Attack" 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), Pages: 1 – 3, IEEE,2012.

[7] H.ABDULQADDER, D ZOU "SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks"IEEE .2018 National Science Foundation of China, ACCESS

[8] W Alosaimi; M Alshamrani; K Al-Begain " Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud" 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Pages: 60-65, IEEE,2015

[9] R Bahaweres; J Sharif; M Alaydrus "Building a private Cloud Computing and The Analysis against DOS (Denial of service) attacks" 2016 4th International Conference on Cyber and IT Service Management, Pages:1-6.IEEE, 2016.

[10] A Dar; B Habib; F Khurshid; M Banday "Experimental Analysis of DDoS Attack and it's Detection in Eucalyptus Private Cloud Platform" 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Pages: 1718 – 1724, IEEE, 2016.

[11] -Eucalyptus [Online] Available https://docs.hpcloud.com/eucalyptus/4.2.1/.

[12] R Kumar; S Lal; A Sharma "Detecting Denial of Service Attacks in the Cloud" 2016 IEEE 14th Intl Conference on Dependable, Autonomic and Secure Computing, 14th Intl Conference on Pervasive Intelligence and Computing, Pages: 309 – 316, IEEE, 2016.

[13] Jake D. Brutlag. Aberrant behavior detection in time series for network monitoring. In *Proceedings of LISA XIV*, Dec 2000.

[14] J Yeh;H Hsiao;A Pang "Migrant Attack: A Multi-Resource DOS Attack on Cloud Virtual Machine Migration Schemes" 2016 11th Asia Joint Conference on Information Security (AsiaJCIS),Pages: 92-99, IEEE, 2016.

[15] W Dargie. "Estimation of the cost of vm migration. In Computer Communication and Networks (ICCCN)" IEEE, 2014 23rd International Conference on, pages 1−8. IEEE, 2014.

[16] K. More; B. Gosavi "A SURVEY ON EFFECTIVE WAY OF DETECTING DENIAL OF SERVICE ATTACK USING MULTIVARIATE CORRELATION ANALYSIS." 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Pages: 246-250,IEEE, 2015.

[17] R Thaper; A Verma " Adaptive Pattern Attack Recognition Technique (APART) against EDoS Attacks in Cloud Computing" 2015 Third International Conference on Image Information Processing (ICIIP), IEEE,2015.

[18] J Eun; H Jung "A technique to make a path table for blocking Distributed Denial-of- Service attacks" 2015 9th International Conference on Future Generation Communication and Networking (FGCN), Pages: 13-16, IEEE,2015.

[19] A. Osanaiye; Mqhele Dlodlo " TCP/IP Header Classification for Detecting Spoofed DDoS Attack in Cloud Environment" IEEE EUROCON 2015 - International Conference on Computer as a Tool (EUROCON), Pages: 1-6, IEEE,2015.

[20] Cisco white paper "REMOTELY TRIGGERED BLACK HOLE FILTERING—DESTINATION BASED AND SOURCE BASED" Available: https://www.cisco.com/

[21] A Sadeghian; Zamani "Detecting and Preventing DDoS Attacks in Botnets by the Help of Self Triggered Black Holes"IEEE 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE) 2014

[22] SNORT [ONLINE]. AVAILABLE: HTTPS://WWW.SNORT.ORG/

Table 1: Summary of techniques against DDoS attacks in cloud

Techniques	Outcome	Restrictions
Defense framework based on time series analysis [4].	1. Minimizes false positive and false negative rate. 2. Reduces detection latency.	No simulation results to support the arguments made by the authors.
Data mining to detect DDoS [12].	1. Time-based and one-class SVM algorithm are applied on detection system. 2. Different attacks are executed to measure target performance.	Fails to detect unknown kinds of attacks.
Migrant attack detection system[14].	1. Uses a test bed to account the downtime period and migration time of target VM during migrant attack	No proposed defense scheme.
Detection methodology depending on normalization feature [16].	1. Identifies both known as well as unknown DDoS attacks. 2. Capability to realize and remember the pattern of valid and invalid route traffic.	No real time implementation.
Adaptive Pattern Attack Recognition Technique (APART) [17].	1. Detects and recognizes the Economical Denial- Of-Sustainability (EDoS). 2. Uses simulated environment to estimate the real-time performance.	No attack prevention, just detection.
Attack route diagnosis based on path table [18].	1. Blocks malicious packets near the source of attacker router. 2. Independent on attack duration and volume of attacker. 3. Creates PID for source and destination router and inserts it in packet delivered.	Consumes more processing in addition to attackers can compromised the router itself.
Spoofed DDoS detection system [19].	1. Identify the source of packet depending on its operating system. 2. Use TTL value to define spoofed DDoS. 3. Use simulation test to evaluate the system	Module failed to identify source of packet if it transverses on different path to destination.