IJCTA, 9(40), 2016, pp. 519-526 ISSN: 0974-5572
© International Science Press

Prevention of EDoS Attack using Hybrid Filtering Technique (EDoS Guard)

Shruti Wadhwa*, Rama Krishna Challa* and Poonam Saini**

ABSTRACT

Cloud computing is latest IT delivery model which would be the rebellion in the IT Company signifies various development trends which are from distributed service to centralized service, hardware to software and software to services. However, security is one of major challenge in cloud. EDoS is the latest kind of DDoS attack on the cloud infrastructure. The purpose is to consume cloud resources although the price of services is pay off by the valid customer. The key intention of DDoS attack bring down the specific service by draining server's resources whereas EDoS's objective is to create an economical unsustainability in the cloud resources for the object and causes financial consequences by exhausting resources and leading to a heavy bill. This paper proposes a novel proactive method for the mitigation of the EDoS attack which consist VF (virtual Firewall) as key component which discards the attack traffic before billing is triggered and helps to lessen the negative impact of EDoS attack which taking place on cloud services using hybrid filtering technique.

Keywords: Cloud Computing, Economic denial of Sustainability (EDoS), Distributed denial of Service (DDoS), Ingress and Egress filtering

1. INTRODUCTION

The design behind cloud computing is reducing the workload from user's computer to cloud making use of simple internet connection. It gives user the facility of pay-per-user which provides measured services like servers, networks, applications, storage, as per their demand. For various business operations such as computing capability, hardware requirement over the internet companies require services which is provided by cloud computing. By means of any latest technology trends, cloud computing is not secured from risk and susceptibilities of security. As cloud computing confronts different attacks and threats from the hackers community [1] and this has turn out to be the main obstacle in advancing of Cloud computing services. Farzad Sabahi [2] provide the various issues of security and availability in cloud computing and suggest some obtainable solution for them. Dimitrios Lekkas [3] has defined the requirements of threats and security is present at the different stages of the cloud execution. Cloud is vulnerable to various attacks being Malware injection, Metadata spoofing, DNS and DDoS attacks, Cross-site scripting, SQL injection, and Wrapping Attack. And, DDoS is the familiar kind of attack among these attacks that has been performed against cloud environment. According to our study, the key findings of Incapsula Survey are:

- 49% of DDoS attacks likely to end amid 6-24 hours. It means that with a projected budget of $40,000 per hour, the usual cost of DDoS can be evaluated at about approximately $500,000.
- Budget is not only constrained to the IT group nonetheless they similarly have a huge impact on risk and security management, sales, and customer service.
- Companies having 500 or more employees are major victim of DDoS attack; experience complex attack costs and involve additional personnel to combat the attack.

* Department of Computer Science and Engineering, NITTTR, Chandigarh, Punjab, India, *Emails: shrutiwadhwa99@gmail.com, rkc_97@yahoo.com*

** Department of Computer Science and Engineering, PEC, Chandigarh, Punjab, India, *Email- nit.sainipoonam@gmail.com*

A special kind of DDoS attack which is particular to only cloud infrastructure called Economic Denial of Sustainability (EDoS). The main aim of EDoS is to make resources of cloud carefully untenable for the victim, whereas DDoS attack is focus on worsen or block cloud services. The time period of DDoS attacks is short while EDoS attacks are extra indefinable and performed over a longer time period. The pay-per-use model has converted problem of Cloud's Distributed Denial of Service attack to an economic one identified as EDoS attack (figure 1).

EDoS attack harms the cloud's auto scaling feature through which an attacker creates malicious requests of HTTP for web application and Cloud Service Provider measures the design mechanically to deal with those requests for which the cost is incurred by a cloud consumer. Its outcome is maintainable drop in the client's budget. Moreover, the spiteful HTTP traffic imitates to be real and thus go undetected [5].

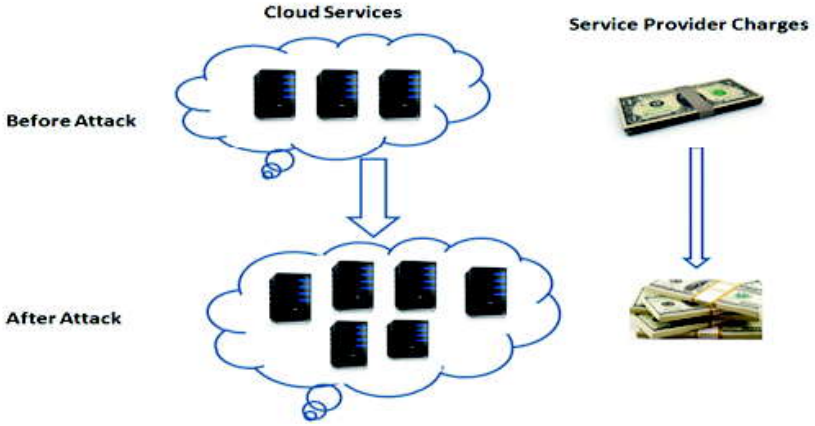


Figure 1: Effect of an EDoS attack in Cloud

2. RELATED WORK

2.1. EDoS Armor [6]

In EDoS Armor mechanism, they detected and mitigated the EDoS attack for E-Commerce based applications. EDoS Armor was dual solution which is admission and congestion control. Firstly they limit the number of users which were continuously sends the requests and allowing only limited users to the server so that they can easily serve within the available resources. In the second phase, they changed the priority of the clients on the basics of their type and thus make sure that most resources were available for good users and limit the access for bad users. The drawback of this mechanism is that it provides defense only for E-Commerce applications not for any other applications.

2.2. EDoS Shield [7]

The main concept used is to authenticate the request whether coming from the legitimate customer or generated by attacker. This is a two step technique which includes two components virtual firewall (VF) and verifier cloud nodes (V-nodes). To identify between the legitimate customer and attacker, first request is forwarded to the verifier node which is responsible for the process of verification using graphic turing test such as CAPTCHA and for the bring up-to-date of the whitelist and blacklist on the basis of outcome of the verification process. And the request coming from the attacker is blocked by virtual firewall as ip address of the attacker is found in the blacklist and thus mitigates the EDoS attack. The disadvantage of this mechanism is that it is not secure from IP Spoofing attack.

2.3. CloudWatch [8]

CloudWatch is a special service from Amazon which lessens the effect of EDoS attack. It monitors Amazon web service resources and applications running on the Amazon infrastructure. The application automatically delivers metrics for CPU utilization, latency and appeal count, customer can also specify more metrics like recall usage, transaction volume or error rates. Every Metric can be made to trigger an alarm, which sends notices to specified end users through AWS's Simple Notifications Service (SNS). One issue was that it cannot process large amounts of custom log data that cloud platforms create, and to react to events in near real time. The restraint of Cloud Watch is it is inefficient for mitigation of EDoS attack as user still be charged for over utilization in case of DDoS attempt.

2.4 In-cloud Scrubber [9]

In this, the authors proposed an on-demand Scrubber Service which is in-cloud eDDoS mitigation web service. In-Cloud Scrubber Service, focused is to produce and authenticate the crypto puzzle i.e. Client puzzle. And the produced crypto puzzle was being resolved by the customer of cloud service by brute force technique in categorize to show its authenticity for locating Service. As a result, puzzle generation and Confirmation was completed by the Scrubber Service. The drawback of the In-Cloud Scrubber mechanism is that legitimate user is unwilling to solve such puzzles and prevents only network level EDoS attack.

2.5 Enhanced EDoS Shield [10]

The author proposed Enhanced EDoS-shield for the mitigation of the EDoS attacks creating from spoofed IP addresses. Hop count filtering is used for protecting the cloud from IP Spoofing attack. They used Time to Live (TTL) parameter for calculating the supreme life time of packet inside the network. The TTL value was decremented each time when packet permitted through any router. When TTL value became zero, the packet was rejected. Thus avoided infinite looping of packets in the network. The drawback of this mechanism is that if an attacker attacks from within the network, the TTL value will be same for attacker or legitimate user.

3. PROPOSED MITIGATION METHODOLGY

In EDoS attack, the parties which involved are [4]:

1) Service Provider of Cloud: This provides its cloud resources and executes the bill
2) User of Cloud: Which use resources of cloud for hosting the web application
3) Authentic Client: Who accesses the services delivered by a user of the cloud
4) Attacker: The one who deliberately creates fake traffic to affect the cloud user's economy

The two elementary approaches of mitigation accessible to guard against EDoS attacks are proactive and reactive [11]. The proactive method helps to reduce or remove the existence of attacks by providing several techniques before the real attacks. Reactive approach is those that respond to some attack event. In this, firstly utilize traffic monitoring to recognize proceeding attacks. After the confirmation of attack, it triggered the system to detect the attack source. At last step, techniques of mitigation are implemented to eradicate or diminish effect of DDoS attacks. The paper is focused on a new proactive method for the mitigation of EDoS attack.

3.1 Attack Model

The EDoS is usually launched in the form of selective jamming attack. The selective jamming attack is the form, which deals with attacking same source with similar attack formations from the single or multiple attackers. The attacker focuses upon making the target available as least as possible to its legitimate users and the resources used by the attacker [12]. The low user count and less hours spent by the users on a particular time span will definitely lower the income of the cloud platform but more resources and more hours spent by the attacker will increase the bill of the legitimate user of the cloud as figure 2 represents the basic EDoS attack. The formation of the proposed attack model is described as following:

1. The attacker (botnet master) gives the command to the managing bots (managers) with attack information which contains the target information, attack physiological parameters or other essential parameters.
2. The manager nodes command and prepare all slave (zombie) nodes to launch the attack on the selected target with the provided information.
3. The zombie nodes launch the attack by flooding the packets towards the selected entry point/s or resource/s in the cloud.
4. The attack data hinders the communication links on the cloud platform and lowers the available bandwidth and resources on the cloud platform.
5. The legitimate users are dropped from the active links due to the lack of bandwidth and resources.

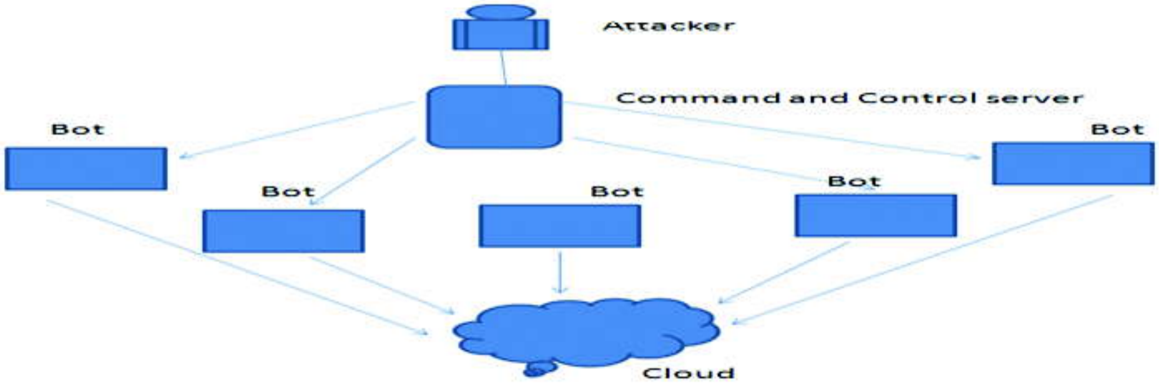


Figure 2: EDoS Attack

3.2 Mitigation

The basic idea for the prevention of EDoS attack is to use Virtual Firewall whose function is to perform real time traffic analysis and also keeps a log file of packet which passes through it. In Virtual firewall, ingress and egress packet pattern matching rules and whitelist/blacklist is used which help to get rid of the attack traffic earlier than billing is triggered as represented by Figure 3. The proposed technique presents a novel method “EDoS-Guard” for the mitigation of the EDoS attack as shown by Figure 4. This hindrance technique is a proactive approach which helps the genuine client to access the resources without being activated by the attacker on billing mechanism.

The key idea is to confirm that request coming from the genuine user not from the attacker. It always checks the packets at the entry point of the cloud. The main component of the mechanism is VF (Virtual Firewall). In VF, the ingress and egress filtering helps to differentiate between the attacker and the legitimate client. Also maintain a Whitelist for the legitimate client and Blacklist for the attacker. Whitelist holds the ip address of the valid client and Blacklist holds ip address of the attacker and the subsequent packets of IP address will access the cloud services if their IP address is present in Whitelist. Ingress filtering is an inbound filtering and a system of confirming that inbound packets received at a network is from the same source of computer that they are claiming to be from earlier to permitting the entry (or ingress).The traffic that has a more possibility of being malevolent is blocked. In short, it implicates forming the mechanism for a list of access control that comprises the IP addresses of allowed source addresses. On the other hand,

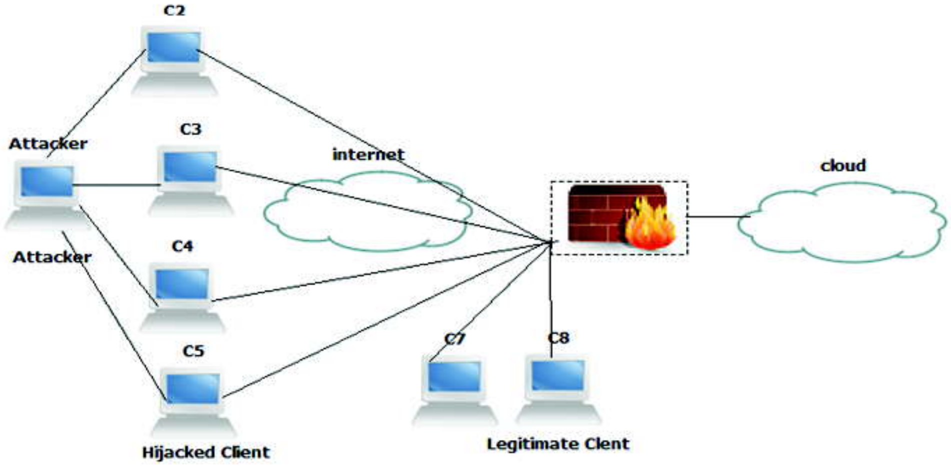


Figure 3. Prevention of EDoS attack

the list of access control may well also be utilized for blocking forbidden source addresses. The IP addresses of the source that are generally blocked with an ingress filter contain ip addresses that are in use at present as an ip address in the internal network, private ip addresses, loopback ip addresses, Multicast ip addresses [13]. This helps in preventing undesired multicast traffic that is probably a spam. Egress filtering is an outbound filtering mechanism which blocks the traffic with an ip address that has an invalid source. This keeps a DoS (denial of service) attack utilizing the spoofing of IP address from initiating on the internal network. The filter must permit traffic to go outside your network only by a source IP address . The key objective of egress filtering is to make sure that traffic that is not wanted or that is destructive does not go outside of a particular network [14]. As RFC 2827[15] Ingress and Egress filtering is used for the protection of IP spoofing. Therefore, it will also protect the cloud environment from the IP spoofing attacks. Instead of using Hop-count filtering we have used, Ingress/Egress filtering because in hop-count filtering, they are not able to recognize the source of request when attacker attacks from with-in the network as TTL value range will be identical for legitimate user as well as for an attacker when attacker attack from within network. And in proposed method, end to end delay is reduced as the packets after successful request by the VF would be promoted directly to protected service of cloud. And for the evaluation of the performance of the proposed mitigation mechanism for EDoS attack parameters included are allocation of resources and response time. Although the EDoS attack is primarily directing the cloud adopter, the cost associated with the computing resources is also evaluated.

3. EXPERIMENT AND RESULT

We perform DDoS flooding attack on the cloud using the slowloris script, we have used three script named goldeneye, slowloris and hulk for performing the attack as because when cloud was tested with single script it doesn’t have major impact on cloud which we needed. As DDoS attack is performed on the cloud resources but when legitimate clients find difficulty to access the cloud services and instead attacker acquires maximum of the services but the bill is paid by legitimate clients for the services of the cloud which actually they have not used. Thus, DDoS attack is converted into EDoS attack. And for the prevention of EDoS attack Virtual Firewall is used for implementing the ingress and egress filtering rules and two access list are also made which contain the valid ip address and invalid i.e attacker ip address. Cloudsim 3.0.3 software platform is use to carry out the simulation. The prevention mechanism can also be done at the edge routers of cloud network when any request is coming for accessing the cloud service first it will go to the VF, in which filtering is performed to check whether the request is coming from legitimate client or from attacker. If the number of packet is greater than the threshold then that ip address is suspected as suspicious ip address and correspondingly it will go to the whitelist and blacklist

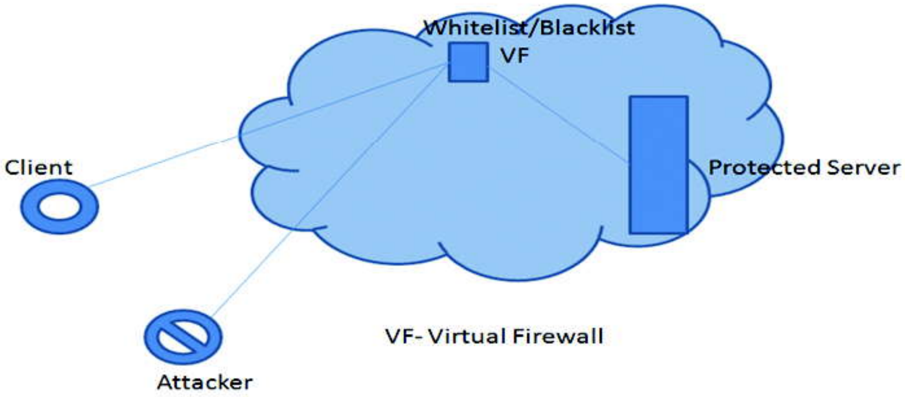
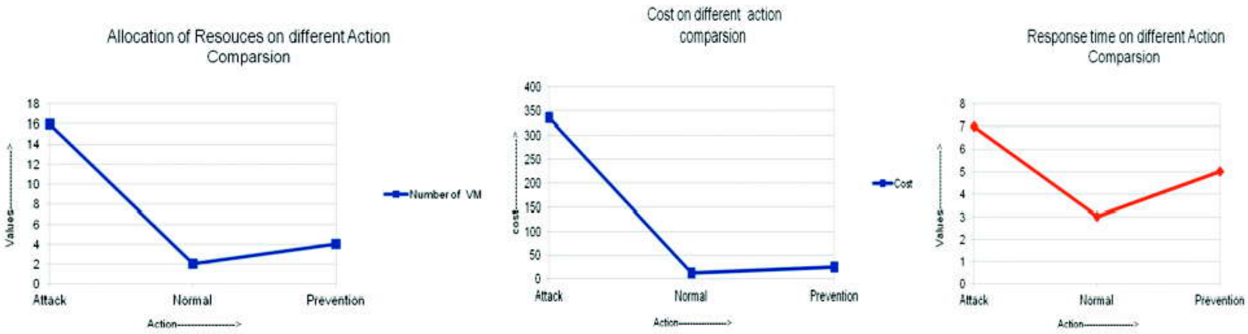


Figure 4: Prevention of EDoS attack



(a) **(b)** **(c)**

Figure 5: (a) Allocation of resources (b) Cost (c) Response time

and then it is allowed to pass to cloud servers. These servers send reply to corresponding cloud client directly without interference.

For the evaluation of the performance of the proposed mechanism parameters used are resources allocation which represents the numeral of resources or virtual machines are assigned to the cloud customer[16] and overall response time which represents the time taken for completing the tasks. We assume that a task can be split into task slices and take the maximum of all task slices execution time as the response time. [17] and cost which is the main parameter for the EDoS which represents the total pricing of the cloud infrastructure which is used by the customer. Figure 5 (a) shows the comparison of allocation of resources in normal scenario, attack scenario and after applying prevention scenario. In Normal case, the legitimate client access the resources as requested but when attacker perform attack the legitimate client is having difficulty to access the resources and also more number of resources is accessed by the attacker. And after applying mitigation mechanism we can see from the figure allocation of resources values is decreased from the attacker case. Figure 5 (b) shows the cost factor in normal scenario, attack scenario and after applying prevention scenario. In the normal case, legitimate client of the cloud pays for the resources which used but when attacker perform attack on cloud resources, the heavy price is paid by the legitimate client in case of attack. And after prevention price is reduced as compared to the attack scenario. Figure 5 (c) shows the comparison of response time in normal scenario, attack scenario and after applying prevention scenario and it is reduced after applying prevention mechanism.

Table 1 show the performance of our proposed in normal, attack and in prevention scenario with various parameters such as number of virtual machines (VM), cost and response time. As seen from the table 1 this method helps to reduce the EDoS effect on cloud and this can be embrace by most of the cloud providers as it proves to be highly effective and saves from permanent denial of service to the network components. The most suitable feature of this method is that the technical administrator is able to decide how much traffic to

Table 1
Experiment Result

Type of response	*Number of VM*	*Cost*	*Response time (millisec)*
Attack	16	336	7
Normal	2	12	3
Prevention	4	25	5

permits inside the network. And such a list gives security to a network as it controls the traffic moving in and out of that point. Any single filtering does not provide fully protection from attack. Therefore, hybrid technique gives a better defense method as both the IP based and the Ingress Egress filters are used jointly which gives the network an enhanced solution.

4. CONCLUSION

Cloud computing enable us to scales our servers up and in order to provision larger amounts of service requests. This unlocks a novel walk of approach for attackers, known as Economic Denial of Sustainability. DDoS is usually easy to spot given vast upsurges in traffic. EDoS attacks are not essentially easy to detect, because the arrangement and business logic is not present in masses of applications and infrastructure for providing the connection between requests and successful transactions. The EDoS idea is to put on mainly to cloud-based services but not to user who acquire their own servers, because if user own his own servers and become target of a DoS attack, they don't directly and robotically scale your process up to a bigger size, as a result the attack doesn't immediately cost client money. It occurs only when the scaling-up is programmed and there's no ceiling that you run the risk of economic damage. We propose a new approach "EDoS Guard" an active mechanism which helps to discards the attack traffic before billing is triggered which helps to lessen the negative impact of EDoS attack which taking place on cloud services. In the future, we show that the same mechanism is used for the mitigation of the DDoS attack as well and the next generation of cloud based capacity planning and scaling may start to focus more on building cost based strategies along with the load and user experience. We found that there is a little work done to minimize the effect of EDoS attack from the cloud platform. The problem of EDoS attack and mitigation of EDoS attack is discussed in order to reduce the effect of EDoS attack. This prevention mechanism works well for small network and it can be implemented with less complexity and it is translucent so that it can be easily accepted by the Cloud Service Provider.

REFERENCES

[1] Mathew Prince (2013) The DDoS That Knoked Spamhaus Offline (And How We Mitigated It). CloudFlare Blog [Online] Available from: http://blog.Cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

[2] Farzad Sabahi. Cloud Computing Security Threats and Responses in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, p. 245-249

[3] Zissis, D. and D. Lekkas, Addressing cloud computing security issues. Future Generation Computer Systems, 2012.28(3): p. 583-592

[4] Incapsula Survey, What DDos Attacks Really Cost Businesses

[5] A. Sukhada Bhingarkar, B. Deven Shah, "A Survey: Securing Cloud Infrastructure against EDoS Attack," in Int'l Conf. Grid & Cloud Computing and Applications (GCA'15), pp. 16-22, 2015.

[6] Masood, M., A Cost Effective Economic Denial of Sustainability (EDoS) Attack Mitigation Framework for E-Commerce Applications in Cloud Environments. 2013

[7] Sqalli, M.H., F. Al-Haidari, and K. Salah. EDoS-shield- a two steps mitigation technique against edos attacks in cloud computing. in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on 2011. IEEE.

[8] CloudWatch, A., monitoring for AWS cloud resources. 2013.

[9] M. Naresh Kumar, et. al.. “Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service”, In Proc. of the Fourth Intl’ Conf. on Computational Intelligence and Communication Networks (CICN), 2012.

[10] Fahd Al-Haidari, Mohammaed H. Sqalli and Khaled Salah, Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses in 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE 2012, p. 1167-1174.

[11] Parminder Singh, Selvakumar Manickam, Shafiq UI Rehman, A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture in Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 IEEE. P. 1-4.

[12] Vashisht, S., & Kaur, M., “Study of Cloud Computing Environment, EDoS attack using CloudSim, “ Int, J. of Advanced Research in Computer Science, Vol.6, No.5, pp. 181-184, May-June 2015

[13] Ingress filtering.[online].Available: www.whatis.techtarget.com/definition/ingress-filtering.

[14] Dan Strom “Global Information Assurance Certification Paper,” As part of GIAC practical repository, December 2015

[15] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing . [online]. Available: www.tools.ietf.org/html/rfc2827

[16] Kamini Bharti, 2Kamaljit Kaur “A Survey of Resource allocation techniques in cloud computing”, journal_ijacect/pdf/vol3_iss2

[17] Kai Li Yong Wang Meilin Liu “A Task Allocation Schema Based on Response Time Optimization in Cloud Computing, arXiv:1404.1124v2 [cs.DC] 18 A pr 2014