Analysis of Simulation of DDOS Attack in Cloud

Mr S.Karthik
Dept of Computer Science & Engg
GHRCE, Nagpur
skarthik_16@yahoo.com

Prof J.J.Shah
Dept of Information Technology
GHRCE, Nagpur

Abstract—**Cloud computing is one of the leading development technology of current era. It has got so much of importance because of the high optimization of IT resources as a service to the consumers on demand with high availability, flexibility, reliability and scalability. Cloud computing basically converts the desktop computing into service level computing using remote servers or huge datacenter. The cloud computing has lended many user friendly features in terms of various services available through internet but the harsh reality about cloud computing is that they are prone to security threat attacks. One of the major concerning security threats is called Distributed Denial of service attack (DDOS). DDOS attack destroys the ability of the system to provide service by overwhelming the bandwidth of network device and saturating the computation resources of service provider. This paper describes experimental analysis of impact of flooding DDOS attack in cloud environment through simulation in cloudsim. In this experiment we will be defining Infrastructure as service (IaaS) in cloudsim and this IaaS will be deployed in Eucalyptus cloud suite. Simulation of attacks will be carried out on the few VM instances defined in cloudsim and computational parameters of VM are observed for VM with normal operation and VM under attack.**

Keywords—**Cloudcomputing, DDOS, Cloudsim, Eucalyptus, IaaS**

I. Introduction

Cloud computing is group of computers networked together in same or different geographical locations, operating together to serve many consumers with different need and workload on demand basis with help of virtualization. Cloud computing is the most user friendly way for the consumers to deal with their needs uniquely through internet. User just needs a browser with internet connectivity to avail the many cloud services. Most widely used now a day's popular cloud services are Gmail, Facebook, Dropbox etc are all can be accessed through browser having internet connectivity anywhere through laptop , cell phones or tablet etc with any modes of mobility [1].

The cloud infrastructure is fully virtualized to utilize hardware through remote serves and huge database as datacenter. One of the major advantage of cloud computing is that cloud infrastructure and its maintenance will be taken care by the third party or cloud service provider on their own cost. This point is basically allured many big IT industries and other industries to adopt cloud computing for their organization to reduce their IT cost. But still most of the industries have lack of confidence on cloud computing because they are prone to security threats and they cannot take chance with their loss of data.

As cloud computing provide so many benefits to the user at the same time it provides facility to attackers. With the help of DDOS attacks attacker make the target server or any resource so saturated that it is not in a position to provide stable service to its consumers. Sometimes DDOS proves so threatening that it can cause loss of data in organization and loss of huge computational cost as cloud rely on pay per use utility.

II. related work

In [2] author has proposed XML and HTTP DDOS attack in cloud environment. Here author has proposed cloud SaaS environment in Windows Azure or Amazon EC2 and suggested application layer attack using XML and HTTP DDOS attacks. Here users make request using XML and then send this request using HTTP protocol which will make interface with SaaS using REST protocol. Attacker implements the attack from REST protocol which will be difficult to detect by IDS.

In [3] author in their paper has described various DDOS attacks which they have broadly classified under two class one which caused bandwidth depletion and second cause resource depletion. Under bandwidth depletion they have mentioned attacks mainly due to flooding like UDP, ICMP. While resource depletion causes mainly due to protocol exploitation attack like TCP-SYN, PUSH & ACK. On the other hand they have enlisted classic tools available for DDOS attacks with their impact and type. Tools enlisted namely Trinoo, TFN, Stacheldraht, mstream, Knight, Trinity etc.

In [4] author has proposed web based Economic denial of service (EDOS) based attacks using XML and HTTP protocols at application layer. Author hosted cloud environment in Amazon EC2 and the service provided by CSP were attacked from multiple source nodes sending XML and HTTP request which will result in the saturation of Amazon EC2 resources causing denial of service. Due to attack

ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE

computation time increases for the service to be processed which ultimately cause huge financial loss as cloud services are provided under pay per utility. Remaining paper will describe Related work in II, Methodology in III, Experiment modules in IV, Results in V and conclusion in VI

.

III. Methodolgy

In this paper we are performing an experimental analysis of simulation of DDOS attack on the few VM instances pooled under Eucalyptus IaaS to check the impact on the computational time of VM working under attack and VM working normally.

As we know cloud services are provided to consumers on pay per utility. Cloud service provided they have huge infrastructure in terms of huge datacenter with physical and many VM.Services which are provided to consumers are responded by VM pooled in cloud infrastructure. If any DDOS attack occurs at this VM then it will increase the computational time to process the request and cause the denial of service it overwhelming request sent to VM. As cloud services are available to consumer on pay per utility so such attacks cause consumer to pay heavily and CSP will lose their customers

In this experiment we are using some tools which are broadly classified below:

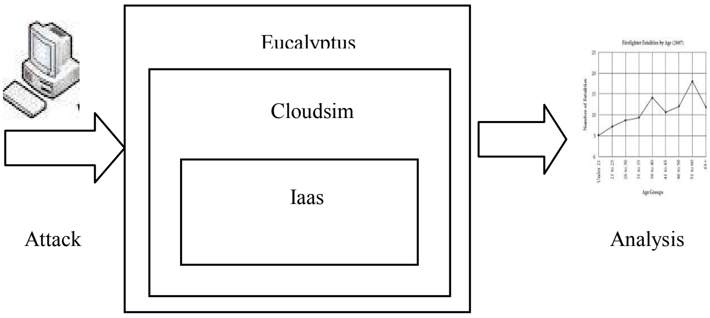


Fig. 1. Experiment model

A. Cloudsim

Cloudsim is software developed by “The cloud computing and distributed systems (CLOUDS) laboratory, University of Melbourne”. We will be using version 3.03.This software provided cloud framework for modeling and simulation of cloud services and infrastructures. So under cloudsim we will be simulating our virtualized datacenter and will be creating our virtual machines under datacenter. Under cloudsim we will create and schedule the simulated jobs

B. Eucalyptus

In this experiment we are using Eucalyptus an open source cloud software framework developed by Eucalyptus system which will implement Infrastructure as service (IaaS) and give user the control and run virtual machine instances deployed across physical layers when they are used in real time environment. Our experimental machine containing windows integrated with Eucalyptus which can be used integrate our with any private cloud deployed in real environment for future real time analysis.

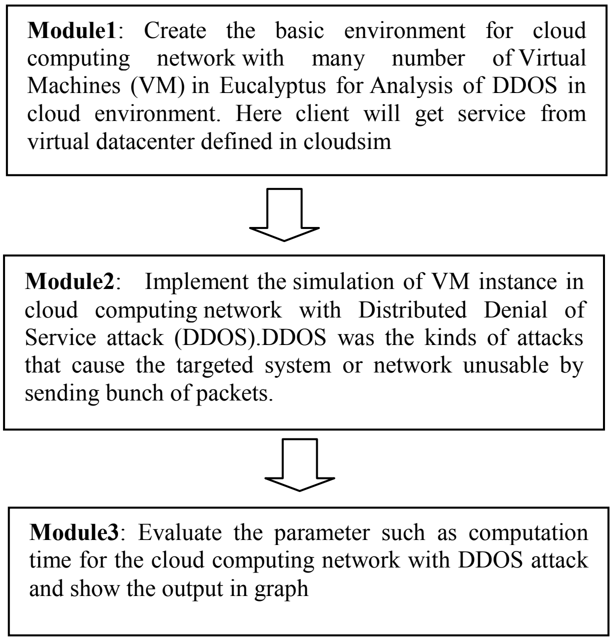
C. Programming Tools

The main language used for programming is Java. We will be using Netbean 7.4 for writing Java program. All the predefined libraries for modeling and simulation are called from cloudsim libraries through Java program. There will be JDK used for Java development program in Netbean 7.4 Also we will be using Mysql server 5.6.14 for database management.

In this experiment the nature of attack is mainly flooding typing. In the simulation we will show the attacker from one virtual machine will send multiple requests for the predefined time slot. We are targeting network layer DDOS attack through flooding attack.

IV. Experiment modules

Experimental module will define the phase wise the progress of this experimental set up. This project is broadly divided into broadly 3 modules which are briefly explained below;

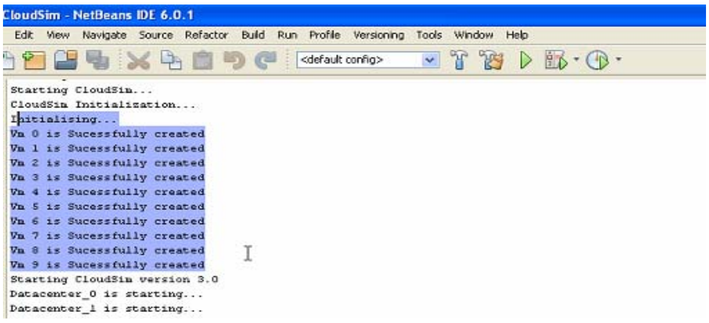


Module1: Create the basic environment for cloud computing network with many number of Virtual Machines (VM) in Eucalyptus for Analysis of DDOS in cloud environment. Here client will get service from virtual datacenter defined in cloudsim

Module2: Implement the simulation of VM instance in cloud computing network with Distributed Denial of Service attack (DDOS).DDOS was the kinds of attacks that cause the targeted system or network unusable by sending bunch of packets.

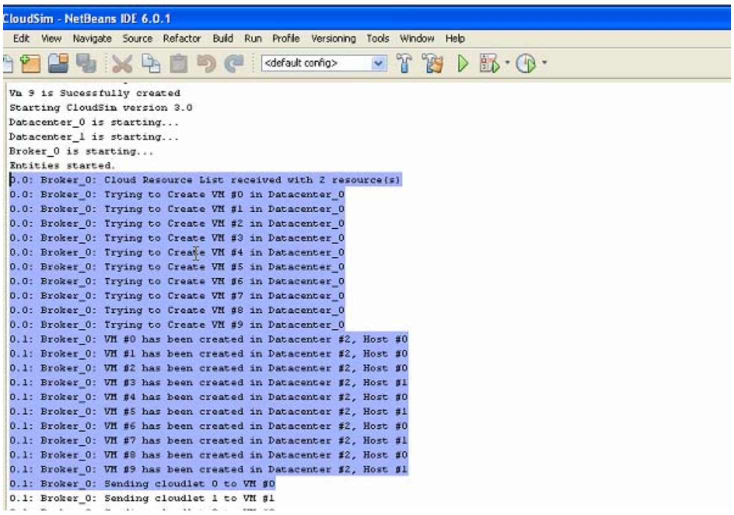
Module3: Evaluate the parameter such as computation time for the cloud computing network with DDOS attack and show the output in graph

Under this section we show the various simulation results:


CloudSim - NetBeans IDE 6.0.1
Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help
<default config>

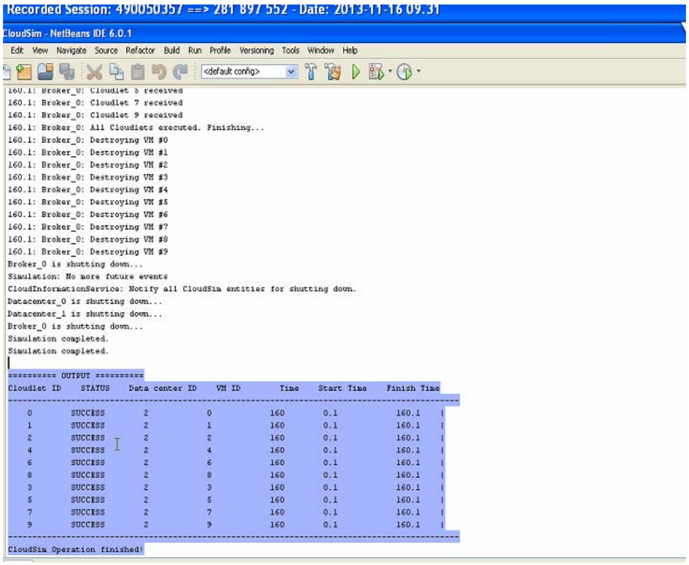
```
Starting CloudSim...
CloudSim Initialization...
Initialising...
Vm 0 is Sucessfully created
Vm 1 is Sucessfully created
Vm 2 is Sucessfully created
Vm 3 is Sucessfully created
Vm 4 is Sucessfully created
Vm 5 is Sucessfully created
Vm 6 is Sucessfully created
Vm 7 is Sucessfully created
Vm 8 is Sucessfully created
Vm 9 is Sucessfully created
Starting CloudSim version 3.0
Datacenter_0 is starting...
Datacenter_1 is starting...
```

Fig. 2. Snapshot of VM creation in cloud sim


CloudSim - NetBeans IDE 6.0.1
Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help
<default config>

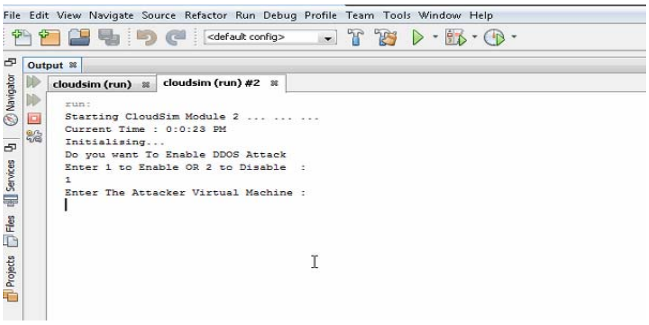
```
Vm 9 is Sucessfully created
Starting CloudSim version 3.0
Datacenter_0 is starting...
Datacenter_1 is starting...
Broker_0 is starting...
Entities started.
0.0: Broker_0: Cloud Resource List received with 2 resource(s)
0.0: Broker_0: Trying to Create VM #0 in Datacenter_0
0.0: Broker_0: Trying to Create VM #1 in Datacenter_0
0.0: Broker_0: Trying to Create VM #2 in Datacenter_0
0.0: Broker_0: Trying to Create VM #3 in Datacenter_0
0.0: Broker_0: Trying to Create VM #4 in Datacenter_0
0.0: Broker_0: Trying to Create VM #5 in Datacenter_0
0.0: Broker_0: Trying to Create VM #6 in Datacenter_0
0.0: Broker_0: Trying to Create VM #7 in Datacenter_0
0.0: Broker_0: Trying to Create VM #8 in Datacenter_0
0.0: Broker_0: Trying to Create VM #9 in Datacenter_0
0.1: Broker_0: VM #0 has been created in Datacenter #2, Host #0
0.1: Broker_0: VM #1 has been created in Datacenter #2, Host #0
0.1: Broker_0: VM #2 has been created in Datacenter #2, Host #0
0.1: Broker_0: VM #3 has been created in Datacenter #2, Host #1
0.1: Broker_0: VM #4 has been created in Datacenter #2, Host #0
0.1: Broker_0: VM #5 has been created in Datacenter #2, Host #1
0.1: Broker_0: VM #6 has been created in Datacenter #2, Host #0
0.1: Broker_0: VM #7 has been created in Datacenter #2, Host #1
0.1: Broker_0: VM #8 has been created in Datacenter #2, Host #0
0.1: Broker_0: VM #9 has been created in Datacenter #2, Host #1
0.1: Broker_0: Sending cloudlet 0 to VM #0
0.1: Broker_0: Sending cloudlet 1 to VM #1
```

Fig. 3. Snapshot of Virtual Datacenter creation in cloudsim


Recorded Session: 490050357 ==> 281 897 552 - Date: 2013-11-16 09.31
CloudSim - NetBeans IDE 6.0.1
Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help
<default config>

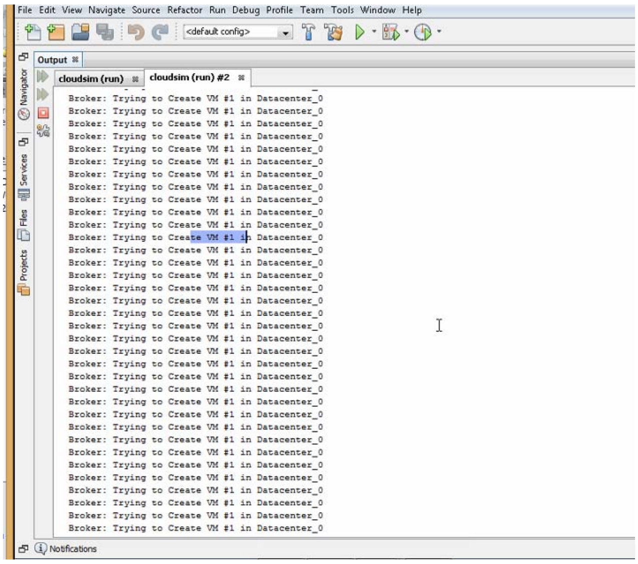
```
160.1: Broker_0: Cloudlet 5 received
160.1: Broker_0: Cloudlet 7 received
160.1: Broker_0: Cloudlet 9 received
160.1: Broker_0: All Cloudlets executed. Finishing...
160.1: Broker_0: Destroying VM #0
160.1: Broker_0: Destroying VM #1
160.1: Broker_0: Destroying VM #2
160.1: Broker_0: Destroying VM #3
160.1: Broker_0: Destroying VM #4
160.1: Broker_0: Destroying VM #5
160.1: Broker_0: Destroying VM #6
160.1: Broker_0: Destroying VM #7
160.1: Broker_0: Destroying VM #8
160.1: Broker_0: Destroying VM #9
Broker_0 is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Datacenter_1 is shutting down...
Broker_0 is shutting down...
Simulation completed.
Simulation completed.

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID       Time     Start Time     Finish Time
------------------------------------------------------------------------------------------
    0        SUCCESS          2              0          160        0.1           160.1
    1        SUCCESS          2              1          160        0.1           160.1
    2        SUCCESS          2              2          160        0.1           160.1
    4        SUCCESS          2              4          160        0.1           160.1
    6        SUCCESS          2              6          160        0.1           160.1
    8        SUCCESS          2              8          160        0.1           160.1
    3        SUCCESS          2              3          160        0.1           160.1
    5        SUCCESS          2              5          160        0.1           160.1
    7        SUCCESS          2              7          160        0.1           160.1
    9        SUCCESS          2              9          160        0.1           160.1
------------------------------------------------------------------------------------------
CloudSim Operation finished!
```

Fig. 4. snapshot of cloudlet creation



```
run:
Starting CloudSim Module 2 ... ... ...
Current Time : 0:0:23 PM
Initialising...
Do you want To Enable DDOS Attack
Enter 1 to Enable OR 2 to Disable  :
1
Enter The Attacker Virtual Machine :
```

Fig. 5. Client window enabling attack



```
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
Broker: Trying to Create VM #1 in Datacenter_0
```

Fig. 6. Flooding Attack on VM1 sending multiple requests to datacenter

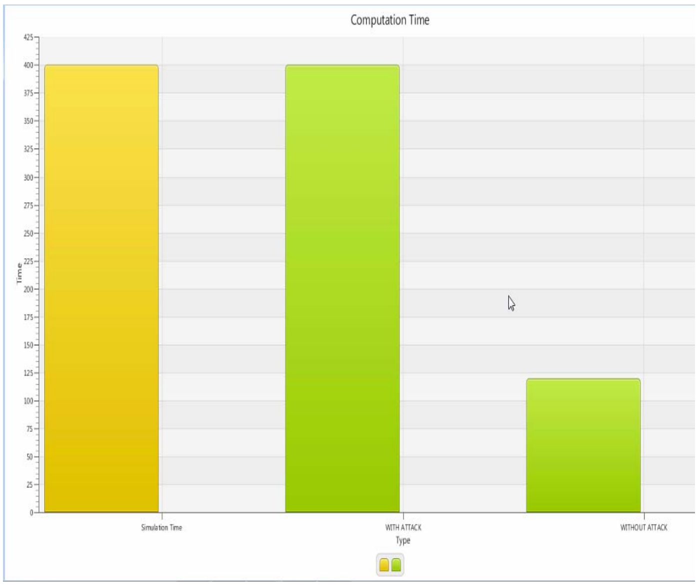


Fig. 7. Overall Computation time VM normal V/s VM under attacK

TABLEI: Computational evaluation

Parameter	With Attack	W/O Attack
Computational time (msec)	400	125

The very first step in this experiment is creation of IaaS in cloudsim. Under IaaS we are focusing on virtual machines and one datacenter. So Fig 2 shows the creation of virtual machine in cloudsim. In cloudsim we can configure any configuration of virtual machine depending upon our needs. Here we can configure like the RAM, Memory storage, VMware etc used for the virtual machine. Fig 3 demonstrates the creation of corresponding creation of datacenter which will be configured in the cloud sim. Similarly for datacenter we will define the storage requirement for the host to be created for the corresponding virtual machine request to be responded and the total simulation time. Fig 4 describes the creation of cloudlet with the successful creation of virtual machine with simulated time for the creation of the same. Fig 2-4 shows the results for Module1. Fig 5-6 talks about Module 2. Fig 5 is the attacker window from where attacker will enable the DDOS flood attack. Fig 6 shows the simulated window describing DDOS flood attack triggered by VM 1 sending continuous flood request to the datacenter and making an attempt to saturate datacenter and creating the situation of denial of service for the other genuine virtual machine sending genuine request to the datacenter. Finally Fig 7 describes our last module i.e. the graphical analysis of computational time. From the metrics derived in Table 1 shows the difference in the computation time when VM operating under normal scenarios and VM operating under DDOS attack.

VI. CONCLUSION

Simulation results in Fig 7 clearly demonstrate that the computation time required by VM under attack is very high as compared to normal VM under operation. Under high overwhelming attack the VM operation may be disrupted and legitimate user will be denied from service. As cloud services are pay per utility genuine user will have to pay hefty amount to get the service paid which result in high consumer dissatisfaction and from CSP point of view they missing their SLA.

No doubt the recent advancement in the field of cloud computing technology proved to be very helpful to many industries and individual consumers in terms of availing various services through internet across globe but security threats pose a great challenge to leading industries that are totally willing to migrate their IT resources in cloud environment. DDOS attack proves extremely threatening by looking at the consequences which causes huge data leakage

and financial loss to industries. Also time and cost involved to fix these issues are very high which is quite enough reasons to moral down the confidence of many industries whom are totally intended to rely on cloud infrastructure. To avoid any theft or data leakage CSP should implement effective anti DDOS strategies so that they can keep their customers happy and never miss on their SLA and financial loss to industries.

VII. REFERENCES

[1] Vincent Shi-Ming Huang , Robert Huang and Ming Chiang, “A DDoS Mitigation System with Multi-Stage Detection and Text-Based TuringTesting in Cloud Computing,” 27th International Conference on Advanced Information Networking and Applications Workshops,IEEE 2013

[2] Tarun Karnwal,T.Sivakumar,G.Aghila, on ” A Comber Approach to protect cloud computing against XML DDOS and HTTP DDOS attack”,IEEE student conference on Electrical,Electronics and computer science,2012.

[3] Arun raj kumar,S.Selvakumar “Distributed Denial of service threat in collaborative environment- A survey on DDOS tools and Traceback mechanism,” IEEE International Advance Computing Conference,2009

[4] S Vinvindar, sudhir shenai, “Economic Denial of Sustainability in cloud services using HTTP and XML based DDOS attacks”, International Journal of computer application,volume 41-No.20,March,2012

[5] A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi, “ Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud”, International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013

[6] Qi Chen, Wenmin Lin, Wanchun Dou ,Shui Yu, “CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment”, Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing,2011 pp.427-434.

[7] Chu-Hsing Lin, Chen-Yu Lee, Shin-Pin Lai1 and Wei-Shen Lai,“A Semantic Rule-based Detection Scheme against Flooding Attacks on Cloud Environment”, International Journal of Security and Its ApplicationsVol. 6, No. 2, April, 2012.

[8] A.M. Lonea, D.E. Popescu, H. Tianfield, “Detecting DDoS Attacks in Cloud Computing Environment, International Journal of Computing and communication , ISSN 1841-9836 8(1):70-78, February, 2013

[9] Siaterlis, C. And Maglaris, B., One step ahead to Multisensor Data Fusion for DDoS Detection. *Journal of Computer Security*, 13(5):779-806, 2005

[10] Dissanayake, A., *Intrusion Detection Using the Dempster-Shafer Theory*. 60-510 Literature Review and Survey, School of Computer Science, University of Windsor, 2008.

[11] Lo, C-C. , Huang, C-C. And Ku, J., A Cooperative Intrusion Detection System Framework *for Cloud Computing Networks*. In 39th International Conference on Parallel Processing Workshops, pp.280-284, 2010.

[12] Zhen chen, Fuye Han, Junwei Cao, Xin Jian and Shuo Chen Published a paper titled “ cloud computing – Based Forensic analysis for collaborative Network security Management system” 2013

[13] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing”, Technical Report No. UCB/EECS-2009-28

[14] Kashan Samad, Ejaz Ahmed, Riaz A. Shaikh, Ahmad Ali Iqbal, “ANALYSIS OF DDOS ATTACKS AND DEFENSE MECHANISMS”, 2005

[15] Hang Chau, Network Security – Mydoom, Doomjuice, Win32/Doomjuice Worms and DoS/DDoS Attacks”, USA

[16] Puneet Zaroo, “A Survey of DDoS attacks and some DDoS defence mechanisms”, Advanced Information Assurance (CS 626).

[17] Stephen M. Specht, Ruby B. Lee, “Distributed Denial of Service : Taxonomies of Attacks, Tools and Countermeasures”, September 2004

[18] Yu Chen, Kai Hwang, Wei-Shinn Ku, Distributed Change point Detection of DDoS Attacks: Experimental Results on DETER Testbed”, 2007

[19] Preeti, Yogesh Chaba, Yudhvir Singh, “Review of Detection and Prevention Policies for Distributed Denial of Service Attack in MANET”, March 2008

[20] S.Meenakshi, Dr.S.K.Srivatsa, “A Comprehensive Mechanism to reduce the detection time of SYN Flooding Attack”, 2009

[21] Bryan Parno, Zongwei Zhou, Adrian Perrig, “Don’t Talk to Zombies: Mitigating DDoS Attacks via Attestation”, June 2009

[22] Konstantinos Meintanis, Brian Bedingfield, Hyoseon Kim, “The Detection & Defense of DDoS Attack”,University of Texas