IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Security Algorithm for Distributed Denial of Service Attack in Cloud

Geetanjali Nenvani[1], Huma Gupta[1]

Department of CSE, TIEIT, Bhopal, India[1]

Abstract: Cloud consists of distributed data centres located at various geographical locations. Distributed denial of service (DDOS) attack is a major trouble to its availability. DDOS is performed in order to disrupt the services provided by the data centres. The attacker can greatly degrade the quality or fully breakdown victim's network connectivity. The attacker first compromises many agents or hosts and then uses these depletes the target network by using these agents. The main aim of a DDoS attack is to make the victim unable to use the resources. In this paper,a flooding based defence algorithm for DDOS attack is proposed which yields better performance.

Keywords: DDOS, flooding attack, cloud VMM.

1. INTRODUCTION

Cloud computing is a model for providing service as Platform, Software, Hardware over internet enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and launched with minimal management effort or service provider interaction [1].
Cloud computing is the latest effort in delivering computing resources as a service. User can hire computing resources online as a product.These computing resources will be used by user online [1], this helps in reducing costs and providers will take charge of it and provide on demand service that is delivered to consumers over the internet from large-scale data centres or "clouds". Cloud computing is gaining rapid popularity in the IT industry.
Cloud Computing consist of collection of scattered servers known as masters who provide the demanded services and resources to the clients known as central controller or cloud manager in a network with scalability and reliability.On-demand service will be provided by distributed servers. Services may be software resources (e.g. Software as a Service, SaaS) or physical resources (e.g. Platform as a Service, PaaS) or hardware/ infrastructure (e.g. Hardware as a Service, HaaS or Infrastructure as a Service, IaaS). Amazon EC2 (Amazon Elastic Compute Cloud) is an example of cloud computing services.

Cloud services are provisioned to use by service providers, for example, Amazon, Google on the Internet. Usually, the resources available to the user of the cloud are virtualized that is (Paas, Iaas, and Saas) services are virtual service. User gets the required service without any dependencies or constraints and in return, companies take some charge for which is nominal as compared to the actual cost of that particular service. Because of this, cloud is becoming popular. Cloud computing technology uses internet and central remote servers to maintain data and applications [2]. Cloud computing allows any user from anywhere to use the updated version of services and application. We do not need to purchase software with the license because updating and maintaining software are the server's responsibility, only we need to have internet connection, with that we can use applications without installing it on our system. Gmail, yahoo mail or Hotmail, etc. are the common and largely used cloud examples.For using any kind of cloud service, you must have an internet connection.

Scientific applications need a large amount of calculation and storage for which you need large computation, storage and power. Previously, all the scientific applications were deployed on Grid [3]. However, Grid computing is costly and not available all over the word. Therefore, the scientific applications are moving towards the cloud. Cloud provides an alternative to grid and supercomputers for a scientist in a lower cost. Cloud is an evolving area and perfect for such applications. For the improvement of deploying an application over cloud, many strategies have been developed, for example load balancing, scheduling algorithm for VM allocation in cloud.

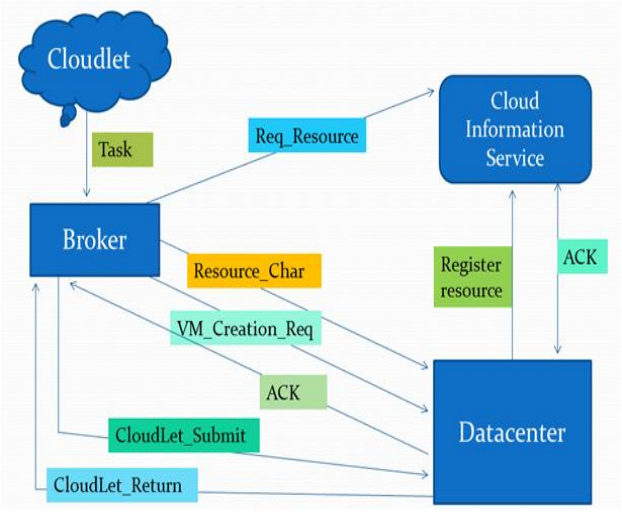


Fig 1: Figure showing cloud architecture

DOI 10.17148/IJARCCE.2016.5610

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

2. LITERATURE REVIEW

Virtualization is one of the major factors contributing to the popularity of Cloud Computing.

2.1 Virtualization: Virtualization is the foundation of cloud technology. Users can access resources for computing or for storage using virtualization without knowing background detail [2]. Virtualization is a layer between Hardware and operating system. Initially, mainframe is used to support many users using the virtual machine terminal. This terminal shows the simulated behaviour of an operating system for each user. VMware Workstation is a similar product started in 1999 and it facilitates to run multiple operating systems in personal computers

2.2 Virtual Machine Allocation: VM allocation allows proficient sharing of virtual machines to available data centres and these allocation methods help to evaluate and enhance the performance of cloud [4]. Different allocation policies are available and they have their own advantages and limitations. The major objective of every VM allocation method is to minimize time. Throttled Load Balancer (TLB) is also the similar research done before.

Table 2.1: Abbreviations used

VM	Virtual Machine
PDF	Program Descriptor File
Paas	Platform as a Service
Iaas	Infrastructure as a service
Saas	Software as a Service

2.3. Denial of service attack on cloud using VM Flooding
During Dos attack, attacker tries to overload victim's resources, resulting in a reduced or denied service for authorized users who are trying to access the victim's services.

In distributed scenario, the attacker recruits zombies (agents or bots) by infecting numerous machines across the internet. This creates a botnet. These distributed botnets can be used to severely multiply the strength of the attack. In most of the cases, targets could be web servers, CPU, Storage, and other Network resources. In cloud environment, DDoS can reduce the performance of cloud services extremely by damaging the virtual servers.

DDoS attacks are launched by affecting the victim in following forms:

• Attackers scan the network to find the machines having some vulnerability and then these machines are used as agents by the attacker. Attacker can find some weakness or bug in the software implementation and disrupt the service.

• Some attacks deplete all the network bandwidth or resources of the victim's system.

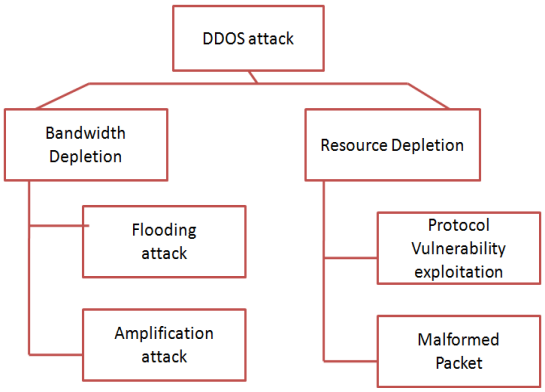


Fig 2: DDos attack classification

2.4.Flood Attacks: This attack is launched by an attacker by sending huge volume of traffic to the victim with the help of zombies.This clogs up the victim's network bandwidth with IP traffic. The victim's system undergoes saturated network bandwidth and slows down rapidly preventing even the authorized traffic to access the network.

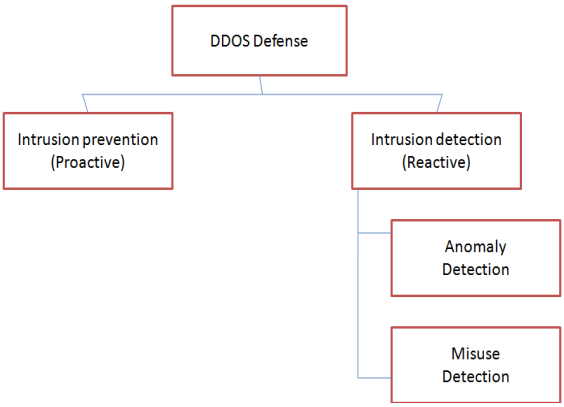


Fig 3: DDOS defense mechanism classification

3. PROPOSED DEFENCE ALGORITHM

In this paper, cloudSim is used to simulate cloud environment. CloudSim is a java based library for simulating cloud.
]

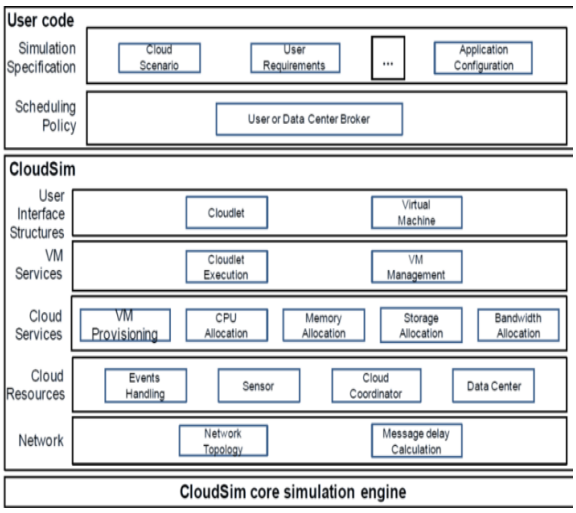


Fig 4: Figure showing CloudSim architecture

DOI 10.17148/IJARCCE.2016.5610

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

CloudSim steps for Simulation:

- Set the no. of user.
- Initialization of common variable.
- CIS will be created by using init method.
- Datacenter will be created by using createDatacenter method. In this,for each datacenter, we create a host with its characteristics.
- Datacenter broker instance will be created.
- Create Instance of virtual machine with PE, RAM and Bandwidth requirement.

Now this virtual machine is submitted to broker.

VMFlooding
{
1. Trace the total capacity of datacenter;
2. Fix capacity of VMs to be used for flooding;
3. N = Capacity of datacenter/ MIPS of each VM;
4. For 1 to N
5. Submit VM on the cloud;
}

AttackProactive approach
{
1. C = Total capacity of datacenter;
2. n = number of cores each PM have;
3. Take a threshold T = C*n;
4.Always calculate summation (S) of capacities of all VMs in the queue;
5. And if (S<T)
6. Assign VMs to datacenter;
7. Else
8. Drop extra VMs without submission so as to avoid failures.
}

4. EXPERIMENTAL SETUP AND RESULTS

Infrastructure has been developed at this point.

- Cloudlet is created with Bandwidth and MIPS requirement.
- Now this Cloudlet will get submitted to Broker.
- Start Simulation process.
- Stop Simulation process.
- Print the status of the Simulation.

Consider a datacenter having 5 hosts having MIPS 1000, 2000, 3000, 1000 and 3000 respectively. So total capacity of all hosts is maximum 10000 so in case of flooding attack if more than this VMs are allocated then the datacenter will not be able to serve all the VMs and some of the VMs will fail.

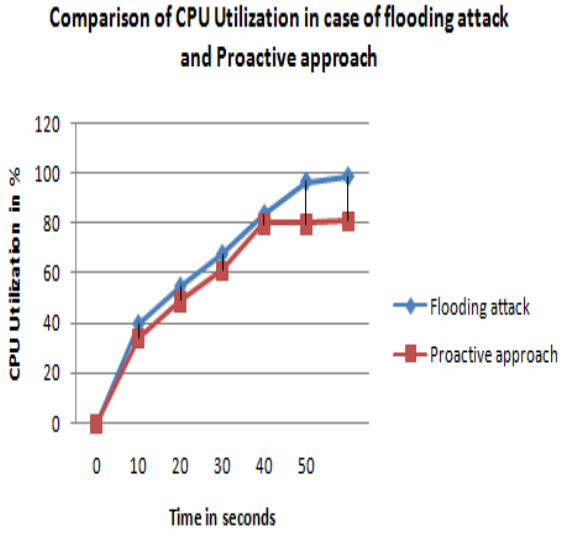
So here in this paper, we have implemented a DDos attack defense algorithm which can make sure availability of datacenter in case of flooding attack.
Here in simulation, we have taken different set of physical machines and virtual machines and for simplicity we have taken all physical machines of same capacity of 2000 MIPS having 2 cores each and VMs of 600 MIPS requires 1 core each.

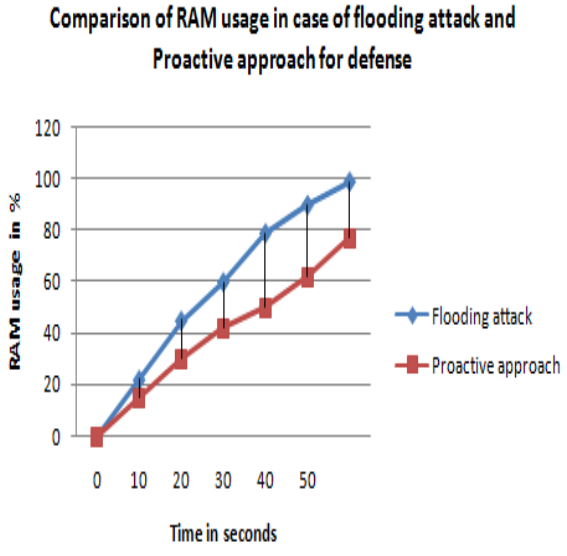
Table 4.1: Success Rate of VMs

No. of PMs	No. of VMs offered	No. of VMs successfully executed	Attack
5	30	30	No
5	60	30	Yes
10	70	60	Yes
20	150	120	Yes

It is clear from the above table that when attached success rate decreases considerably.

In case of flooding attack, for denial of service CPU usage increases drastically and then hosts of cloud become unable to handle more requests. On observation of 50 sec, it is found that in proactive approach CPU utilization doesn't increase after a threshold.





DOI 10.17148/IJARCCE.2016.5610

5. CONCLUSION AND FUTURE WORK

In this paper, a DDOS flooding attack defense algorithm is proposed using CloudSim. The proposed algorithm uses a proactive defense mechanism to avoid DDOS attack on cloud. The given algorithm has considerably worked on different cloud having variable number of datacenters and hosts.

In future, there is a need to design a tool that controls and understands privacy leaks, performs authentication and guarantees availability in the face of cloud denial-of-service attacks.

ACKNOWLEDGEMENTS

I would like to thank the people from TIEIT for making this research possible. Also, I would like to express my sincere gratitude towards **Prof. Huma Gupta** for her guidance and support.

REFERENCES

1. Meiko Jensen, Jorg Schwenk, Nil Gruschka "On technical issues in cloud computing", IEEE International Conference on cloud computing, 2009.
2. N.Weiler, Honeypots for Distributed Denial of Service, in Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109114.
3. P. Ferguson, D. Senie, Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing, in: RFC 2827, 2001.
4. K. Park, H. Lee, On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in power law Internets, in: Proceedings of the ACM SIGCOMM 01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2001, pp. 1526.
5. A. Keromytis, V. Misra, D. Rubenstein, SoS: secure overlay services, in: Proceedings of the ACM SIGCOMM 02 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2002, pp. 6172
6. C. Zou, D. Towsley, and W. Gong, the performance of internet worm scanning strategies, 2003.
7. V. Paxson S. Staniford and N.Weaver, How to own the internet in your spare time, in 11th Usenix Security Symposium, San Francisco, August 2002.
8. V. Paxson S. Staniford and N.Weaver, How to own the internet in your spare time, in 11th Usenix Security Symposium, San Francisco, August 2002.
9. C. Zou, D. Towsley, W. Gong, and S. Cai, Routing worm: A fast, selective attack worm based on ip address information, 2005. Common Vulnerabilities and Exposures, http://cve.mitre.org/cve/
10. J. Mirkovic, G. Prier, P. Reiher, Attacking DDoS at the source, in: Proceedings of ICNP 2002, Paris, France, 2002, pp. 312321.
11. R.R. Talpade, G. Kim, S. Khurana, NOMAD: Traffic based network monitoring framework for anomaly detection, in: Proceedings of the Fourth IEEE Symposium on Computers and Communications, 1998.
12. Y. Huang, J.M. Pullen, Countering Denial of Service attacks using congestion triggered packet sampling and filtering, in: Proceedings of the 10th International Conference on Computer Communications and Networks, 2001.

DOI 10.17148/IJARCCE.2016.5610