ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Study of Cloud Computing Environment, EDoS attack using CloudSim (Modelling and Simulation/Simulator)

Shikha Vashisht
Student,Computer Science,
Chandigarah Group of Colleges, Landran, Mohali, India

Mandeep Kaur
Astt. Prof, Computer Science
Chandigarah Group of Colleges, Landran, Mohali, India

Abstract: Cloud computing means the using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. It is described as a type of computing that is based on *sharing of resources* rather than having local server or other personal devices to handle applications. Attack is one the emerging problems in cloud computing and in attacks the lime light attack now a days is EDos attack. Edos is basically a malicious code which makes the resources accessibility hard or almost unavailable to the valid users. In this paper the performance is analyzed on the basis of submission time and completion time of the data transmission. And study how the performance is degraded while EDoS attack is made on the cloud environment. The environment of cloud computing made by using simulator called cloud sim.

Keywords*:* Cloud computing, Cloud-Sim, DDoS, EDoS attack.

I. INTRODUCTION

In cloud computing, the word “cloud” is used as a analogy for *"the Internet"* and *cloud computing* means "a type or Internet-based computing," where diverse services such as servers, storage and other internet based applications are delivered to an consumers’ computers and devices through the Internet. Cloud computing aims to power the NGD (next generation data centres) and enables the application service providers to let data centre capabilities for deploying applications depending on users demand (Time and Class of Service). Cloud applications have different composition, configuration, and operational requirements. Cloud computing provide platform, infrastructures, and software that are made available as a “pay-as-you-use”(On the basis of time uses) model to consumers. These services are consults with Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Cloud services provide network of virtual services, Virtual servers, hardware, User interface, Database etc. so that users can be made easily able to access and deploy applications from anywhere in the world on demand at the competitive costs. Due to cloud computing developers do not have any need to develop large size hardware or software infrastructure for their services also it reduces human expenses to operate it. In this way cloud computing are providing liberation to IT companies from the low level task of set up basic hardware as well as software infrastructures and also enables more focus on innovation and creation of business morals [1].

Some traditional and promising Cloud-based application services include social networking, web hosting, content delivery, and real-time instrumented data processing. Each of these application types has variant composition, configuration, and other deployment requirements. Quantify the performance of provision including scheduling and allocation, policies in a real Cloud computing environment (Amazon EC2, Google App Engine, and Microsoft Azure) for different application models.

II. RELATED WORK

In [2] authors discuss the modelling and simulation by using cloud sim simulator. This paper discusses the efforts to design and develop Cloud technologies focus on defining novel methods and mechanisms for resourcefully managing Cloud infrastructures. In [7] proposed an approach to discuss the EDoS attack in a cloud environment by using XML and HTTP. A new type of attack by protocol is discussed in this paper and service is gold through Amazon EC2. In [8] a virtual approach is proposed to mitigate EDoS attack in cloud environment. This mechanism is based on the past behaviour of the user.

III. KEY CONCEPTS AND TERMINOLOGIES

The architectural elements and applications that form the basis for Cloud computing as discuss below.

A. *Cloud computing:*

Cloud computing is a type of parallel and distributed system consists of a collection of interconnected and virtualized computers which are dynamically allocated and presents like one or more fused computing resources based on service-level-agreements(SLA) which is to be established through arbitration between the service provider and customers [4].

Applications of cloud such as social network, game-portals, business applications, and scientific workflows operate at the peak layer of the architecture. These applications have different Quality of Service requirements (QOS).

B. *Layered Design:*

Figure 1 shows the layer design of the service-oriented Cloud architecture. The physical resources alongside with core middleware capabilities form the basis for delivering IaaS. The user-level middleware focuses on providing the PaaS capabilities. The top layer objects on (SaaS) application services by making the appropriate usage of services provided by the lower layer services. PaaS /SaaS services are often developed and provided by the third party service providers, which are different from IaaS providers [5].

a. ***User-Level Middleware****:* This layer covers the software frameworks such as Web 2.0 Interfaces like Ajax, IBM Workplace that help developers in creating rich, affluent, cost effecting user-interfaces for browser-based applications. This layer also gave the programming environments and composition tools which make the creation, deployment, and execution of applications in Cloud comparatively easier.

b. ***Core Middleware****:* This layer implements the platform-level-services that provide runtime environment which further enabling Cloud computing capabilities to application services built using User-Level Middleware. Core services at this layer include Dynamic SLA Management, Accounts, Billing, Execution monitoring and Pricing. The examples of services operating at this layer are: Amazon EC2, Google App Engine, and Aneka.

c. ***System Level****:* The computing power in Cloud computing environments is abounding by a collection of data centres, which are typically installed with hundreds to thousands of servers heaving massive application and storage capacity [3]. These servers are managed by virtual machine toolkit transparently and also these servers are isolated from each other.

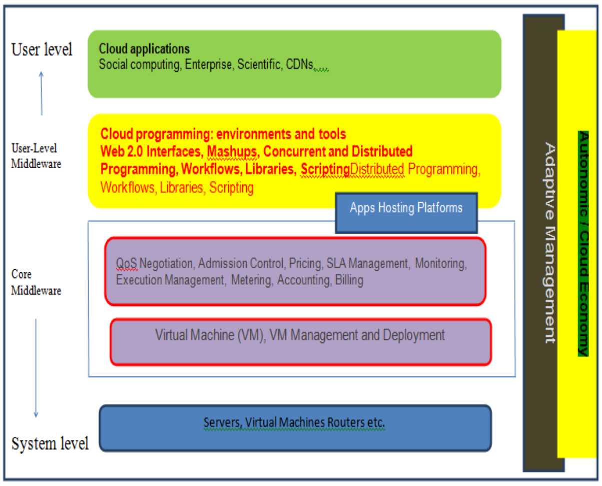
User level
User-Level Middleware
Core Middleware
System level
Cloud applications
Social computing, Enterprise, Scientific, CDNs,….
Cloud programming: environments and tools
Web 2.0 Interfaces, Mashups, Concurrent and Distributed Programming, Workflows, Libraries, ScriptingDistributed Programming, Workflows, Libraries, Scripting
Apps Hosting Platforms
QoS Negotiation, Admission Control, Pricing, SLA Management, Monitoring, Execution Management, Metering, Accounting, Billing
Virtual Machine (VM), VM Management and Deployment
Servers, Virtual Machines Routers etc.
Adaptive Management
Autonomic / Cloud Economy

Figure No 1 layered cloud computing Architecture

C. *Federation (Inter-Networking) of Clouds:*

In order to optimally and most favourable serve costumers needs around than World Current Cloud Computing providers have several data centres at different geographical locations over the Internet. The Cloud service providers are unable to predict geographical division of users consuming their services; therefore the load coordination must happen automatically. The distribution of services must change in response to change in the load behaviour means Cloud service provider should be able to provide non breakable service. Here we have Cloud coordinator, Cloud brokers/users, Cloud Exchange. The Cloud coordinator component is instantiated by every data centre. These cloud coordinators provide application and physical resources to the federation and also they keep track of loads on each application server to provide high-availability. These cloud coordinators undertakes arbitration or negotiation with other Cloud providers for dynamic scaling of services across multiple data centres for handling the services in peak hours. The Cloud brokers stands for users (service consumers) and they find suitable Cloud service provider with the help of Cloud Exchange and negotiate with Cloud coordinator for allocation of their service requirements. The Cloud Exchange is a market maker for collaborating service providers and consumers.

Cloud computing includes social networking like Facebook, Content Delivery Networks (CDNs) and MySpace. Social networking sites serves dynamic contents to billions of customers, whose access and inter-communication patterns are difficult to predict. Generally, Social networking websites are developing using multi-tiered web applications such as WebSphere, and MySQL as a relational database. And each component will run in a different virtual machine, which can be hosted in data centres own by different Cloud computing providers. Each connected developer has freedom to make choose over which Cloud services provider offers the services that are more suitable for him/her.

IV. DDOS AND EDOS ATTACKS

Security has become a big issue in cloud computing as it provide resources, broad network access, and rapid elasticity and on-demand self service. It is the most attractive technology now a days, which not only attract intend user but also to attackers. The security can be administered in a cloud at various levels. This paper deals about the security issues related to the DDoS attack with will further leads to the EDoS attack. The DDoS attack in a cloud network or other can make legitimate request for service to generate an EDoS [9].

A. *DDoS Attack:*

Denial-of-service (DoS) attack is an intentional attempt to make the resources in a network unavailable or inaccessible to their intended users by making the too busy or overload the network. Attacker mostly tends to use large number of system or machine to launch Distributed DDoS attack [7]. The DDos attack is launched by Zombies (infected system) to a particular site, hosted application or any particular network Infrastructure by absorbing available bandwidth or any other resources.

B. *EDoS Attack:*

It is a malicious attack, which allow service providers to dynamic stretch and accommodate number of request for the end users, is exploited to make economical unviable or to make burden upon the service provider to sustain further demand for service from genuine users [8]. The DDoS attack in a cloud highly scalable and services will consume more resources during attack to maintain the SLA (Service Level Agreement), which tend to the loss in revenue. In this attacker targets the service provider economic resources by sending huge number of requests. Thus the DDoS is transformed to Economic Denial of Sustainability (EDoS) [7].

C. *Working of EDoS:*

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. 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, because cloud charge in pay-as-you-use model. The formation of the proposed attack model is described as following:

a. 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.
b. The manager nodes command and prepare all slave (zombie) nodes to launch the attack on the selected target with the provided information.
c. The zombie nodes launch the attack by flooding the packets towards the selected entry point/s or resource/s in the cloud environment.
d. The attack data hinders the communication links on the cloud platform and lowers the available bandwidth and resources on the cloud platform.
e. The legitimate users are dropped from the active links due to the lack of bandwidth and resources.
f. Dropping of legitimate users lowers the active user count, hence the resource usage, which directly affects the earnings during the attack hours.

Algorithm Design for Attack Simulation:

```
1.      Set sourcesEDoS at 100
2.      Set targetCloud at 1
3.      Set packetEDoS at 10000
4.      Set mips at 250;
5.      Set exectime at 100;
6.      Set interval at 10;

7.      Time Overhead = (sourcesEDoS * targetCloud * packetEDoS) / (mips * exectime)

8.      Data Overhead = (sourcesEDoS * targetCloud * packetEDoS) / (exectime / interval)
```

V. CLOUD SIM

The CloudSim is a toolkit to supports modeling and creation of one or more virtual machines (VMs) on a simulated node having Data Centre, jobs, and their mapping to suitable VMs. This simulator also allows simulation of several Data Centres to facilitate a study on grouping and associated policies for migration of VMs for reliability and automatic scaling of applications [2].

The primary objective of this paper is to provide a well-known and extensible simulation/model of framework that enables faultless modeling, simulation, and testing of emerging Cloud computing infrastructures and application services. By using this simulator, researchers and developers can focus on particular system design issues that they want to investigate, without getting worried about the low level details related to infrastructures and services.

Main features of CloudSim are:[6]

a. to support for modeling and simulation of data centres at large scale
b. to support for modeling and simulation of virtualized server hosts, with modified policies • to support for modeling and simulation for energy-aware computational possessions
c. to support modeling and simulation for data centre network topology and message-passing applications
d. to support modeling and simulation of federate clouds
e. to support for dynamic insertion of simulation rudiments, stop and carry on

VI. ANALYSIS OF PERFORMANCE

In this paper, performance is analyzed by comparing the values of the normal case and the case the DDoS attack is launched on the basis of time. The performance will be analysed by using cloud Sim simulator by using the default configuration as shown in the table. The random data is send or accessed by the host. The comparison is shown by plotting the graph for both cases (normal and DDoS attack).Time taken by the processor to complete the task or complete the transmission of data is noted. And same will done in case data when the DDoS attack is launched the unnecessary data is send by the attacker to slow down the processes or to make the resources unavailable to the user. The over head time is noted down and compares the results with the normal case. During the comparison we found that in time over head completion time is much more than that of normal case.

VII. COMPARISON RESULTS

Default configuration

Table 1 Default configuration on cloudsim.

INITIAL SPEED	42
CLOUD LETS	5
CPU(cloudlet)	1
HOST	5
ARCJITECTURE	X86
CPU NO (PE host)	4
MIPS/PE	1000
V.M	5
MIPS(VM)	250
PE(VM)	1

Figure1 clearly shows the time taken by the data to transmit, the x-axis shows the submission time and y-axis shows finish time.

a. ***Submission Time:*** The time taken by the processor to start sending data.

b. ***Finish Time:*** The time taken to start the instance.

The integration of both the submission time or finish time taken is the total time taken at the normal case.

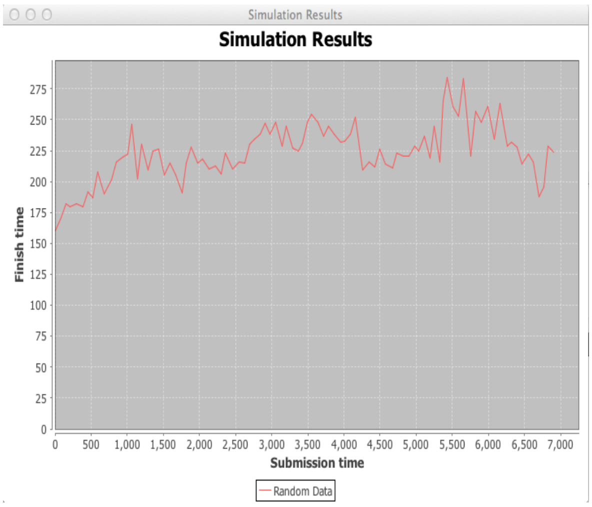

Figure. 2 Time taken for the transmission in normal circumstances

After studying the results of the normal case now we introduced a DDoS attack in the environment. And observe the change in time of submission and finish time. Below the graph in figure3 shows the condition of data transmission during attack. The submission as well as finish time increases as compare to the normal case which finally results time overhead.

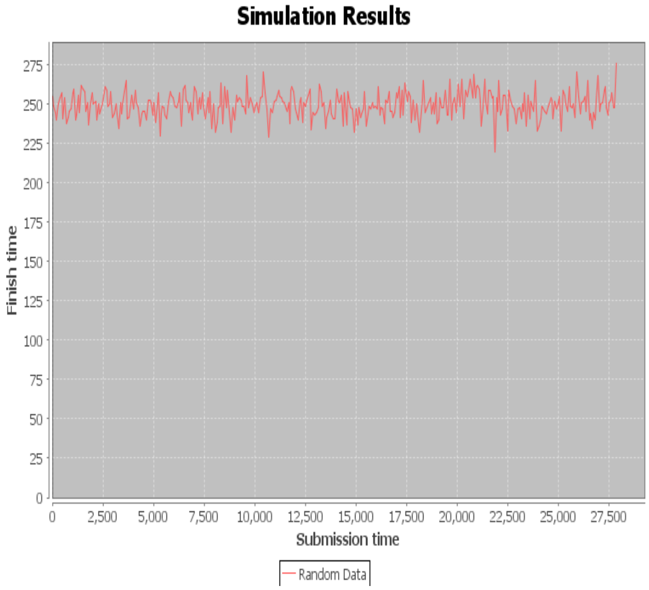

Figure. 3 Time overload shown during DDoS attack.

VIII. CONCLUSION

Cloud Computing provides a wide range of services. Existing Security mechanisms are not up to the mark .New approaches are needed which should be a distributed and scalable approach. New form of attacks is possible in the cloud. One such kind of attack is EDoS attack which is a new breed of DDoS attack. The EDoS attack exists only in the cloud so it can be termed as one of the cloud specific attack. A new security EDoS protection frame work is proposed. Also, an experiment is conducted to demonstrate the EDoS attack. The existing approaches are not capable of completely eliminating the EDoS attack. Research is still needed to provide a better mechanism to protect the cloud from EDoS attack. The attack simulation has shown the maximum effect on the cloud performance. The cloud performance is decreased with the rise in the data volumes launched by the attacker nodes. The results can be clearly seen in the form of the Time Overhead and Data Overhead, where Time overhead signifies the computational cost overhead in the form of time and data overhead signifies the similar parameters in the form of ingress data volume and processing cost overhead produced due to the data floods.

IX. REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica,M. Zaharia “Above the Clouds: A Berkeley View of Cloud computing”, Technical Report No. UCB/EECS-2009-28.

[2]. Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros “Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities”, Grid Computing and Distributed Systems (GRIDS) Laboratory Department of Computer Science and Software Engineering The University of Melbourne, Australia.

[3]. R. Buyya and M. Murshed “GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing”, Concurrency and Computation: Practice and Experience, 14(13-15), Wiley Press, Nov.-Dec., 2002.

[4]. R. Buyya, C. S. Yeo, and S. Venugopal “Market oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities” Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, 2008.

[5]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic “ Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility”, Future Generation Computer Systems, 25(6): 599-616, Elsevier Science, Amsterdam, The Netherlands, June 2009.

[6]. The Cloud Computing and Distributed Systems (CLOUDS) Laboratory, University of Melbourne. http://www.cloudbus.org/cloudsim/

[7]. S. Vivian Sandar, Sudhir Shenai “Economical denial of Sustanibilty in cloud services using http and xml base DDoS attacks”, International journal of computer applications(0975-8887)Vol41-No20,March 2012.

[8]. Zubair A.baig, Farid Binbeshr “controlled virtual resource access to mitigate Economic Denial of Sustainability Attacks Against cloud infra structure”, International conference on cloud computing and big data, 2013.

[9]. Zhang, Jinyu Song, JinShuangWang, Lanjuan Yang,Tao, Ping Chen Institute of Command Automation, PLA University of Science Nanjing, China, “Defense of DDoS Attack for Cloud Computing”, IEEE conference, 2012.