



NITTE
EDUCATION TRUST

N.M.A.M. INSTITUTE OF TECHNOLOGY

(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)

Nitte – 574 110, Karnataka, India

(ISO 9001:2015 Certified), Accredited with 'A' Grade by NAAC

☎: 08258 - 281039 - 281263, Fax: 08258 - 281265

Department of Computer Science and Engineering

B.E. CSE Program Accredited by NBA, New Delhi from 1-7-2018 to 30-6-2021

Report on Mini Project

Analysis of Simulation of DDoS Attacks in Cloud

Course Code : 20CSE33

Course Name : Cloud Computing

Semester: VI SEM

Section: A

Submitted To:

Dr. Sandeep Hegde
Associate Professor
Department of Computer Science and
Engineering

Submitted By:

Harshitha J
4NM20CS077

Jyotsna N Shenoy
4NM20CS081

Date of submission:

02-05-2023

ABSTRACT

Distributed denial-of-service (DDoS) attack is a try to disrupt the conventional traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. A DDoS attack can easily exhaust the computing and communication resources of its victim within a brief period. Cloud computing is susceptible to security threat attacks.

Cybercriminals can use DDoS attacks to stop corporates and end-users from accessing internet services. During this experiment, we are going to be defining Infrastructure as a service (IAAS) in cloudsim and simulation of attacks are administered on the few VM instances defined in cloudsim and computational parameters of VM are observed for VM with normal operation and VM when DDoS attack is made.

TABLE OF CONTENTS

| | |
|-------------------------------------|-----|
| TitlePage | i |
| Abstract | ii |
| TableofContents | iii |
| Introduction | 1 |
| ProblemStatement | 2 |
| Objectives | 3 |
| Hardware/Software Requirement | 4 |
| Literature Survey | 5 |
| Methodology | 12 |
| ImplementationDetails | 14 |
| Results | 18 |
| Conclusion andFutureScope | 20 |
| References | 21 |

INTRODUCTION

Cloud computing is the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the web to supply faster innovation, flexible resources, and economies of scale. It's been credited with increasing competitiveness through cost reduction, greater flexibility, elasticity and optimal resource utilization. One will pay just for the services they use thus lowering their operating costs. It also can help in running their infrastructure efficiently and scaling the business. Although cloud environments employ security measures, they still face security threats. This is often one amongst the possible reasons why most companies lack confidence in making use of cloud computing services.

Distributed Denial of Service (DDoS) is one among the various security threats. Denial of service attacks are methods to forestall genuine users from accessing online web applications, SaaS, PaaS or IaaS Cloud services and computing resources. together with the expansion in cloud computing, these attacks saw major changes in scale, methods, aims, and targets. the benefits provided by cloud computing are available to both victims and attackers. This has made the DDoS race interesting and quite complex. With the assistance of DDoS attacks, attackers make the target server or any resource so flooded that it's not in a very position to produce proper service to its consumers. It may also result in loss of knowledge in a corporation and loss of giant computational costs because the cloud relies on pay per use utility.

PROBLEM STATEMENT

Cloud computing is one of the leading development technology of this era. The cruel reality about cloud computing is that they're susceptible to security threat attacks and DDoS is one of them. These attacks can cause disruptions in operations on a very large scale. Major problems caused by DDoS attacks include loss of data, consumers being denied service, unavailability of resources, loss of time and money in repairing the damage caused by it and loss of consumers to Cloud Service providers. Some

damages caused by DDoS attacks can also be permanent and irrecoverable. During this project, we attempt to simulate DDoS attacks allotted on some VM instances defined in cloudsim by flooding a targetted VM with multiple cloudlets. We also make comparisons on the computation time taken by VM under attack and without attack.

OBJECTIVES

- We start by defining Infrastructure as a Service (IaaS) in CloudSim.
- Run the program without enabling an attack on VMs.
- Carry out simulation of attacks on VM instances.
- Compare the computational parameters for VM under attack and VM in normal operation.

HARDWARE / SOFTWARE Requirements

HARDWARE:

- Ram: 8GB or Higher • CPU: Intel i3 or Apple M1

SOFTWARE:

- Eclipse: <https://www.eclipse.org/downloads/>
- Cloudsim for modelling and simulation of cloud computing

LITERATURE SURVEY

[1] Simulation and Analysis of DDoS Attacks

It provides a basic understanding of various DDoS attack methods such as Smurf, ICMP, TCP SYN, UDP, TCP floods and their combinations. It doesn't provide any way to enforce the global deployment of a particular security mechanism or security policy.

[2] Combating DDoS Attacks in the Cloud

It provides an appraisal of the requirements of DDoS mitigation solutions and the factors governing them. The methods followed are DDOS detection using traffic filtering, mitigation, prevention and recovery as traffic filtering alone may not be sufficient to combat DDoS attacks in the cloud environment.

[3] Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud

This paper uses Enhanced DDoS- Mitigation System to encounter DDoS attacks. It proves that the firewall mitigates the DDoS impacts successfully. Enhanced DDoS-MS depends on firewall security measures.

[4] Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment

This paper reviews various DDoS attack schemes and discusses the advantages and disadvantages of each one of them and proposes a statistical model. It also discusses Covariance Matrix, Kendall's Tau and Entropic approach.

[5] Solutions for DDoS Attacks in Cloud

It introduces denial of service and provides trends on top DDoS attack locations/targets/Vectors. It provides insight into different types of DDoS attacks. Most solutions are unable to provide a proper and adequate protection against varied levels of network or application attacks.

[6] Analysis of Simulation of DDOS Attack in Cloud

This paper defines Infrastructure as a Service in Cloudsim and gives analysis of the impact of DDoS attack on VM and provides a graph showing time taken by VM in normal operation and time taken by VM under attack. The computation parameters and methodology are not mentioned properly.

[7] Detecting TCP-based DDoS Attacks in Baidu Cloud Computing Data Centers

This paper identifies two attack modes: fixed source IP attacks (FSIA) and random source IP attacks (RSIA). It uses a real-time TCP-based DDoS detection approach, which extracts effective features of TCP traffic and distinguishes malicious traffic from normal traffic.

[8] Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks

This paper gives us ways to prevent DDoS attacks without human intervention. It provides different methods of defence such as DDoS Attack Identification, Defense Footprint, Traditional Defense Implementation, Automated Defense Against DDoS and Automatic Detection in the SDN.

[9] DDoS attack defence framework for cloud using fog computing

It proposes a framework to generate DDoS attack traffic using the concept of fog computing, which is a distributed decentralized computing infrastructure. In this, traffic passes through fog defender and DDoS attack traffic gets filtered allowing the legitimate requests only.

[10] Securing Cloud Computing Environment Against DDoS Attacks It uses a backpropagation algorithm to find the source of DDoS attacks. 88% result was obtained for testing datasets and 91% result was obtained for training datasets. It tests the efficiency of Cloud Trace Back model

[11] DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments

Here, the DDoS Attack Detection is based on C4.5 Algorithm (decision tree). The results obtained are quite accurate compared to other machine learning algorithms. They have been successful in detecting abnormal traffic flow.

[12] Detecting DDoS attacks in cloud computing using ANN and black hole optimization

It uses ANN with a 99.4% true detection rate. Provides confusion matrix and ROC curve. The model has a detection accuracy of 96.30%. It uses an NSL-KDD dataset with 12500 training samples and 2597 test samples.

[13] Stealthy DDoS detection mechanism for Cloud resilience system

The cloud resilience system, works in making the system function normally even after it has been disrupted. The process of the resilience system involves the method of defending, detecting, restoring and recovering. Attacker uses SIPDAS algorithm to perform the Stealthy DDoS attack.

[14] DDoS Detection and Filtering Technique in Cloud Environment using GARCH model

In this paper, filtering of a variety of DDoS attacks in a cloud is done with the help of a backpropagation artificial neural network (ANN) on the traffic. Non-linear time series model GARCH is used which correctly predicts the traffic state. Chaos theory is used for DDoS attack detection.

[15] A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks

In this paper, a technique is used in which a router marks an incoming packet and filters detected packets on the victim side. It helps in detecting HTTP or XML-Based DoS attacks using a packet-based marking approach. This approach involves complex implementation as it involves marking packets and maintaining a lookup table.

Summary of the Literature

| Author details with year of publication | Paper Title | Methodology | Advantage | Disadvantage |
|---|--|---|--|--|
| Poongothai, M, Department of Information Technology, Institute of Road and Transport Technology, Erode Tamilnadu, India (2012) | Simulation and Analysis of DDoS Attacks | DDoS attack methods commonly deployed are Smurf, ICMP, TCP SYN, UDP, TCP floods and its combinations. | Provides an understanding of the existing attack methods, tools and defense mechanisms, so that a better understanding of DDoS attacks can be achieved. | There is no way to enforce global deployment of a particular security mechanism or security policy, and due to privacy concerns. |
| Gaurav Somani et al., Central University of Rajasthan, India (2017) | Combating DDoS Attacks in the Cloud | DDoS detection using traffic filtering, mitigation, prevention and recovery. | Provides a detailed introduction to the attack methods, consequences, and attack dynamics. | Traffic filtering alone may not be sufficient to combat DDoS attacks in the cloud environment |
| Wael Alosaimi, Mazin et al., Faculty of Computing, Engineering and Science University of South Wales Pontypridd, Wales, United Kingdom (2015) | SimulationBased Study of Distributed Denial of Service Attacks Prevention in the Cloud | Enhanced DDoS-Mitigation System, a new proactive framework is developed to accomplish the objective and to prove the important role that the firewalls can play in this regard. | Proves that the firewall mitigates the DDoS impacts successfully by improving the provided services to the users in terms of the response time and server load under attack. | Enhanced DDoS-MS depends on the firewall security features. |

| | | | | |
|---|--|---|---|--|
| Anteneh Girma et al., Systems and Computer Science Department, Howard University (2015) | Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment | Proposes an effective alternative hybrid scheme against DDoS attacks based on Entropy and Covariance Matrices. | Analyzes different existing DDoS detecting techniques and proposes a hybrid statistical model. | Many of the available DDoS detection schemes performance found to be below the par. |
| Akashdeep Bharadwaj, Computer Science, Dehradun (2016) | Solutions for DDoS Attacks in Cloud | Uses on-premise based DDoS solution, ISP DDoS solutions and Scrubbing defence architecture. | Proposes solutions to mitigate DDoS attacks in cloud. | Most solutions are unable to provide a proper and adequate protection against varied levels of network or application Attacks. |
| Mr S.Karthik, Dept of Computer Science & Engg, GHRCE, Nagpur (2014) | Analysis of Simulation of DDOS Attack in Cloud | Defining IaaS in cloudsim and deploying this IaaS in Eucalyptus cloud suite. Simulation of attacks are carried out on the few VM instances defined in cloudsim. | Demonstrates that the computation time required by VM under attack is very high as compared to normal VM under operation. | Computation parameters are not mentioned clearly. |
| Jiahui Jiao ¹ , et al., Nankai University (2017) | Detecting TCPbased DDoS Attacks in Baidu Cloud Computing Data Centers | Evaluates the proposed approach using a simulated dataset and real datasets. | Provides a different detection strategy for fixed source IP attacks and random source IP attacks. | They are not suited to detecting RSIAmode DDoS attacks. |

| | | | | |
|--|---|---|---|---|
| Jeanette Smithperrone, Tacoma Community College, Tacoma, Washington, USA (2017) | Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks | Uses Intrusion Detection/ Prevention System, volumetric change method and defence footprint. | Provides an overview of the problem of DDoS attack, current mitigation process and proposed automation for identification and precise mitigation. | Adaptation to the changing threat landscape is untenable using IPS/IDS for only known attacks, mitigation by rate limit, and at a high occurrence of false positives. |
| Deepali, National Institute of Technology Kurukshetra, (2017) | DDoS attack defense framework for cloud using fog computing | Fog computing concept is used. | Proposes a framework in which DDoS attack traffic is generated. | This approach only provides defense from TCP and HTTP attack traffic. |
| Bansidhar Joshi et al., NIT Tiruchirappalli, (2012) | Securing Cloud Computing Environment Against DDoS Attacks | Uses backpropagation neural network | 88% result was obtained for testing datasets and 91% result was obtained for training datasets | Misidentification of a small number of ttrack traffic. |
| Marwane Zekri et al., (2017) | DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments | DDoS detection system based on the C.4.5 (decision tree technique) algorithm was designed to mitigate the DDoS threat. | Successful in detecting abnormal traffic flow. | Uses only 3 algorithms for comparison. |
| Gopal Singh Kushwah et al., Department of Computer Engineering NIT Kurukshetra Haryana, India (2017) | Detecting DDoS attacks in cloud computing using ANN and black hole optimization | Neural network is trained with 12500 samples and 2597 samples are used for testing and the output for ith sample is calculated. | Accuracy of 96.30% was obtained. | Complex implementation |

| | | | | |
|--|---|--|--|---|
| G. Aline Sophia et al., Sathyabama University (2017) | Stealthy DDoS detection mechanism for Cloud resilience system | There is a server limit and the server checks all the requests given by each user. Uses Sipdas Attack algorithm. | Attempts to avoid server crash. | User Interface is not clear and objects are not properly aligned. |
| Omkar P. Badve, et al., Department of Computer Engineering, NIT Kurukshetra Kurukshetra, India (2015) | DDoS Detection and Filtering Technique in Cloud Environment using GARCH model | Non-linear time series model called GARCH is used to predict the state of the traffic | Uses ANN with 99.4% true detection rate | Has risk of getting high false positive rate. |
| E.Anitha, PG Student Computer Science and Engineering Kongu Engineering College Perundurai (2013) | A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks | Router marks an incoming packet and filters detected packets on the victim side. | Helps in detecting HTTP or XML-Based DoS attacks using packet based marking approach | This approach involves complex implementation as it involves marking of packets and maintaining a lookup table. |

METHODOLOGY

In this paper, we perform a simulation of a DDoS attack on cloud systems by carrying out an attack on a particular VM instance.

| | |
|-----------------------|--------------|
| <u>Before attack:</u> | |
| Start time: | Finish time: |
| 0.1 | 160.1 |
| <u>After attack:</u> | |
| Start time: | Finish time: |

The cloud has a pay-as-you-go model and the consumer 0.1 4800.1 pays to use the VM services. When a DDoS attack occurs on the VM, it causes the consumer to pay heavily as these services are available on pay per utility. This can also result in Cloud Service Providers losing their customers.

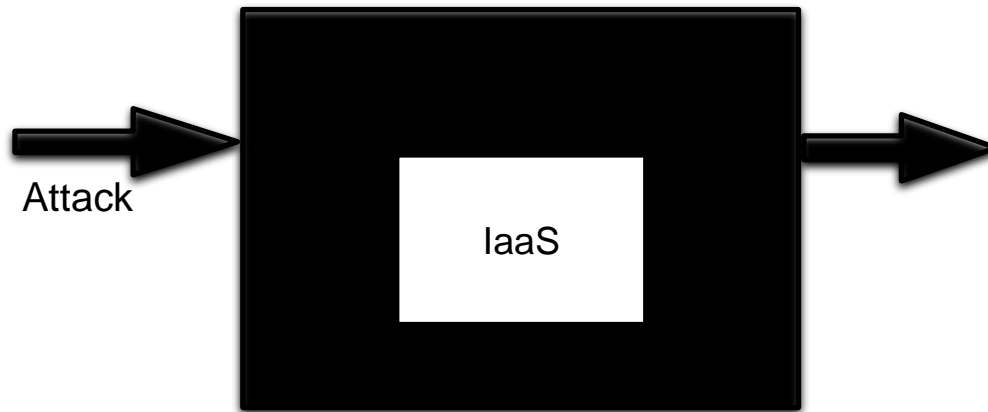


Fig 1.
Experiment
Model

Fig 1. gives the experimental model that we follow. We start by defining Infrastructure as a Service (IaaS) in CloudSim, carry out a DDoS attack on a targeted VM and then compare the time taken by the VM under attack and time taken by VM without attack.

We use the following tools to conduct the experiment: A.

Cloudsim:

Cloudsim is an open-source framework developed by “The cloud computing and distributed systems (CLOUDS) Laboratory, University of Melbourne”. The Cloudsim version that we use is 3.0.3. The benefit of using Cloudsim is that there is no installation or maintenance cost. This software provides predefined allocation policies and utilization models for managing resources and allows the implementation of user-defined algorithms as well. Virtualized data centers can be simulated using Cloudsim. We create virtual machines in Cloudsim.

B. Programming Tools:

We use Java programming language for our experiment. Cloudsim has some predefined libraries for modelling and simulation and it is written in Java.

While attacking, we will be sending multiple requests from one VM for a time slot.

There are 5 steps that we follow to perform the experiment:

Step 1: Create 2 data centers and a broker which coordinates between data centers and cloudlets.

Step 2: Create 10 Virtual Machine instances and host the VMs in data centers.

Step 3: When VM is not under attack, i.e. in a normal scenario, create 15 cloudlets and host them on the available VMs.

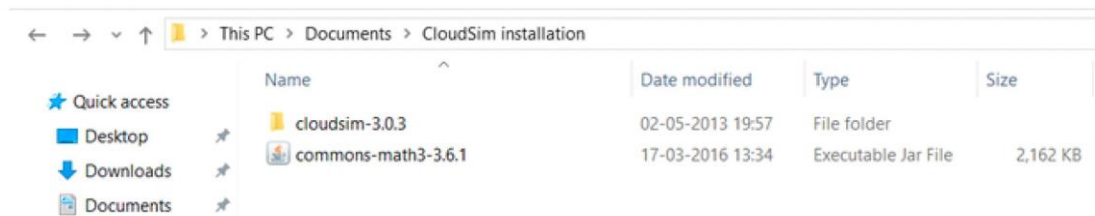
Step 4: Enable the attack by flooding the chosen VM by sending multiple cloudlet requests and then sending 15 legit cloudlet requests.

Step 5: Note the time required by the VM to complete the operation when it is under attack and when it is not under attack.

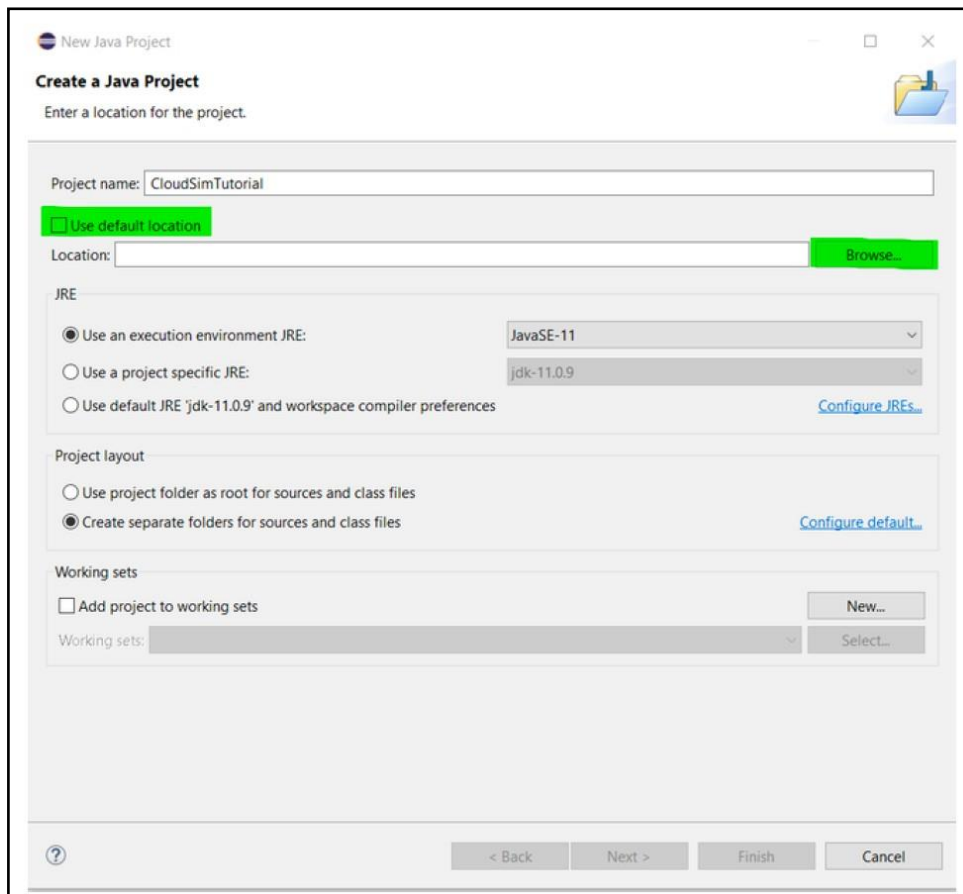
IMPLEMENTATION

1. Installation Steps:

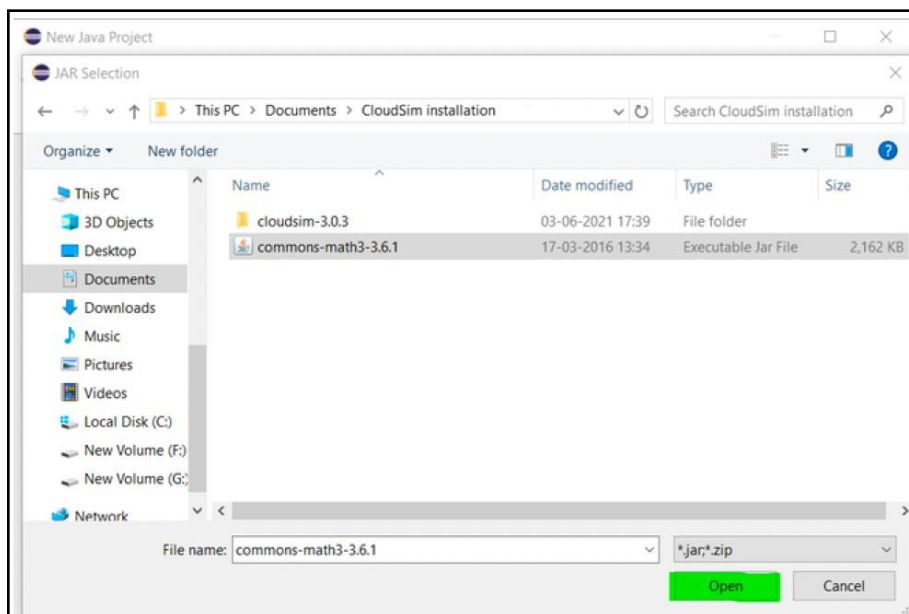
- Download the zip file of CloudSim 3.0.3 from [here](#)
- Download Apache's commons-math3 library zip file from [here](#)
- From the zip folder extracts cloudsim-3.0.3 into a folder. Also, extract the commons-math3-3.6.1 jar into the same folder



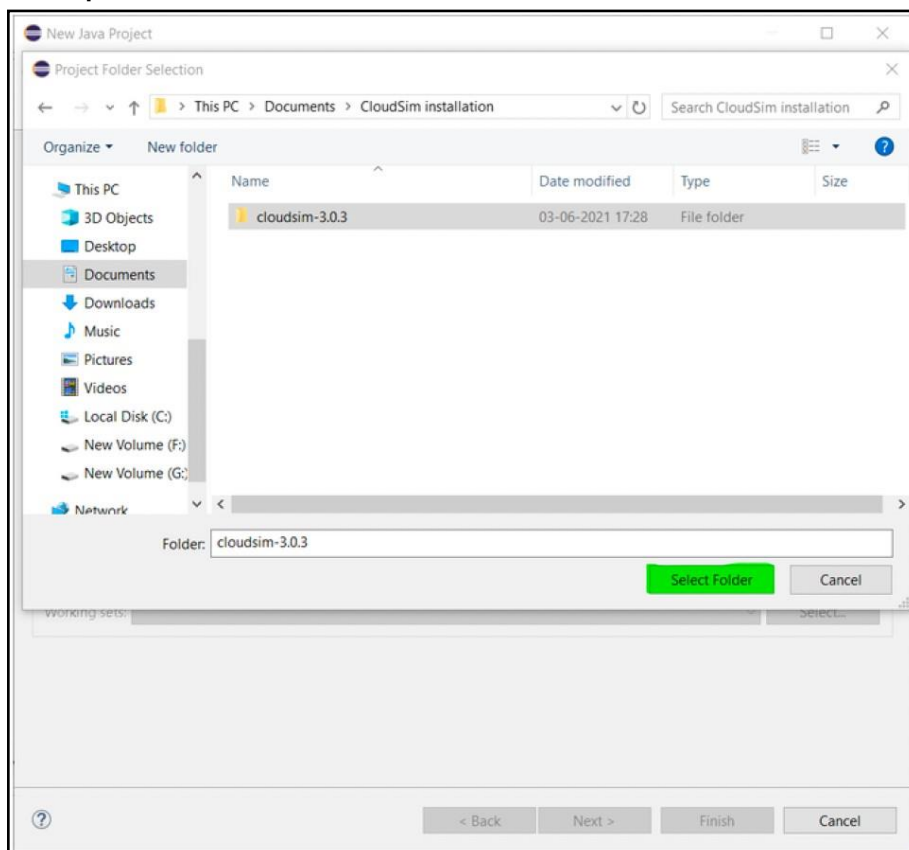
- Open Eclipse IDE and go to File -> New -> Java Project.
- Enter any name for your project and then uncheck the Use default location box just under it and click on Browse



- Browse to the folder where you extracted your files and select the cloudsim-3.0.3 folder

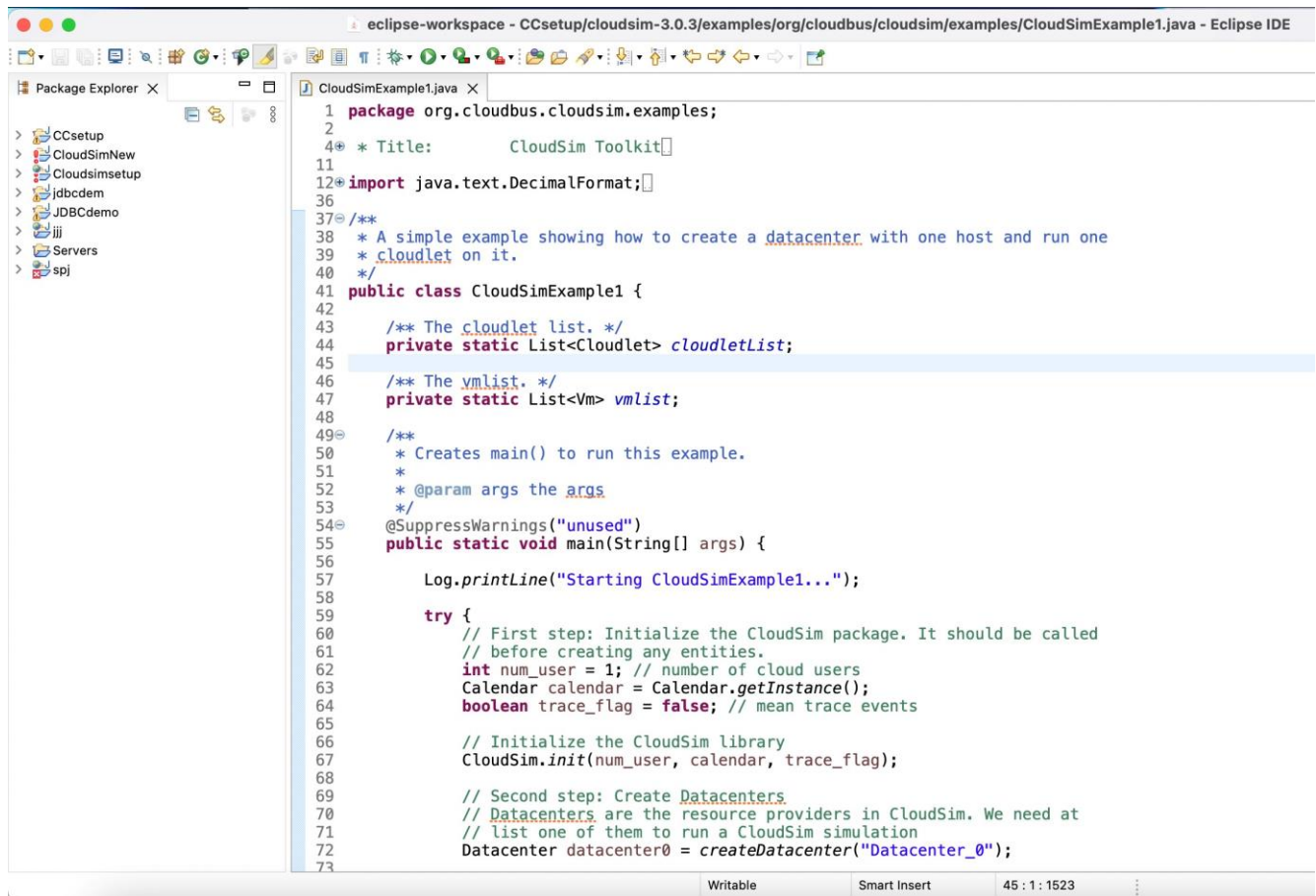


g) Click Next and go to Libraries -> Add External JARs. Now browse to the same folder where you extracted your commons-math3 jar file and Open it



h) Finally click on Finish and wait for the project to build. After the project has been built, from the Project Explorer you can click on your project and from the dropdown go-to examples ->

org.cloudbus.cloudsim.examples where you can find pre-written sample codes and try to run them.



```
1 package org.cloudbus.cloudsim.examples;
2
3
4 * Title:      CloudSim Toolkit
11
12 import java.text.DecimalFormat;
36
37 /**
38  * A simple example showing how to create a datacenter with one host and run one
39  * cloudlet on it.
40  */
41 public class CloudSimExample1 {
42
43     /** The cloudlet list. */
44     private static List<Cloudlet> cloudletList;
45
46     /** The vmlist. */
47     private static List<Vm> vmlist;
48
49     /**
50      * Creates main() to run this example.
51      *
52      * @param args the args
53      */
54     @SuppressWarnings("unused")
55     public static void main(String[] args) {
56
57         Log.println("Starting CloudSimExample1...");
58
59         try {
60             // First step: Initialize the CloudSim package. It should be called
61             // before creating any entities.
62             int num_user = 1; // number of cloud users
63             Calendar calendar = Calendar.getInstance();
64             boolean trace_flag = false; // mean trace events
65
66             // Initialize the CloudSim library
67             CloudSim.init(num_user, calendar, trace_flag);
68
69             // Second step: Create Datacenters
70             // Datacenters are the resource providers in CloudSim. We need at
71             // list one of them to run a CloudSim simulation
72             Datacenter datacenter0 = createDatacenter("Datacenter_0");
73 }
```

2) Simulating DDoS attack:

```

String attack;
int attackVmId;

Scanner s = new Scanner(System.in);

System.out.println("Do you want to enable DDOS Attack (yes/no):");
attack = s.next();

List<Cloudlet> clList;

if(attack.equals("yes")||attack.equals("Yes") ) {
    System.out.println("Enter the virtual machine to be Attacked:");
    attackVmId = s.nextInt();

    broker.attackedVM=attackVmId;

    System.out.println("Enter the no of cloudlets to attack VM "+attackVmId+" :");
    noOfCldlets = s.nextInt();

    //30 cloudlet attack on a particular vm(attackVmId)
    cloudletList = createCloudlet(brokerId, noOfCldlets, 0);

    //Actual Cloudlets
    System.out.println("Actual Cloudlets:");
    clList = createCloudlet(brokerId, 10, noOfCldlets);
    cloudletList.addAll(clList);
}else {
    System.out.println("Actual Cloudlets:");
    cloudletList = createCloudlet(brokerId, 10, 0); // creating 10 cloudlets
}

```

Fig 2. Snapshot of code to enable/disable attack

Here, the code asks whether the user wants to simulate a DDOS Attack. If not, then, legit cloudlets will be created and accommodated in VMs available. If the user wants to simulate an attack, it asks for the VM Id and the number of cloudlets to create for the attack as inputs. It creates those cloudlets first and then creates legit cloudlets, which are then serviced by the targeted VM.

```

protected void submitCloudlets() {
    int vmIndex = 0;
    if(attackedVM==-99) {
        for (Cloudlet cloudlet : getCloudletList()) {
            Vm vm;
            // if user didn't bind this cloudlet and it has not been executed yet
            if (cloudlet.getVmId() == -1) {
                vm = getVmsCreatedList().get(vmIndex);
            } else { // submit to the specific vm
                vm = VmList.getById(getVmsCreatedList(), cloudlet.getVmId());
                if (vm == null) { // vm was not created
                    Log.println(CloudSim.clock() + ": " + getName() + ": Postponing execution of cloudlet "
                        + cloudlet.getCloudletId() + ": bount VM not available");
                    continue;
                }
            }

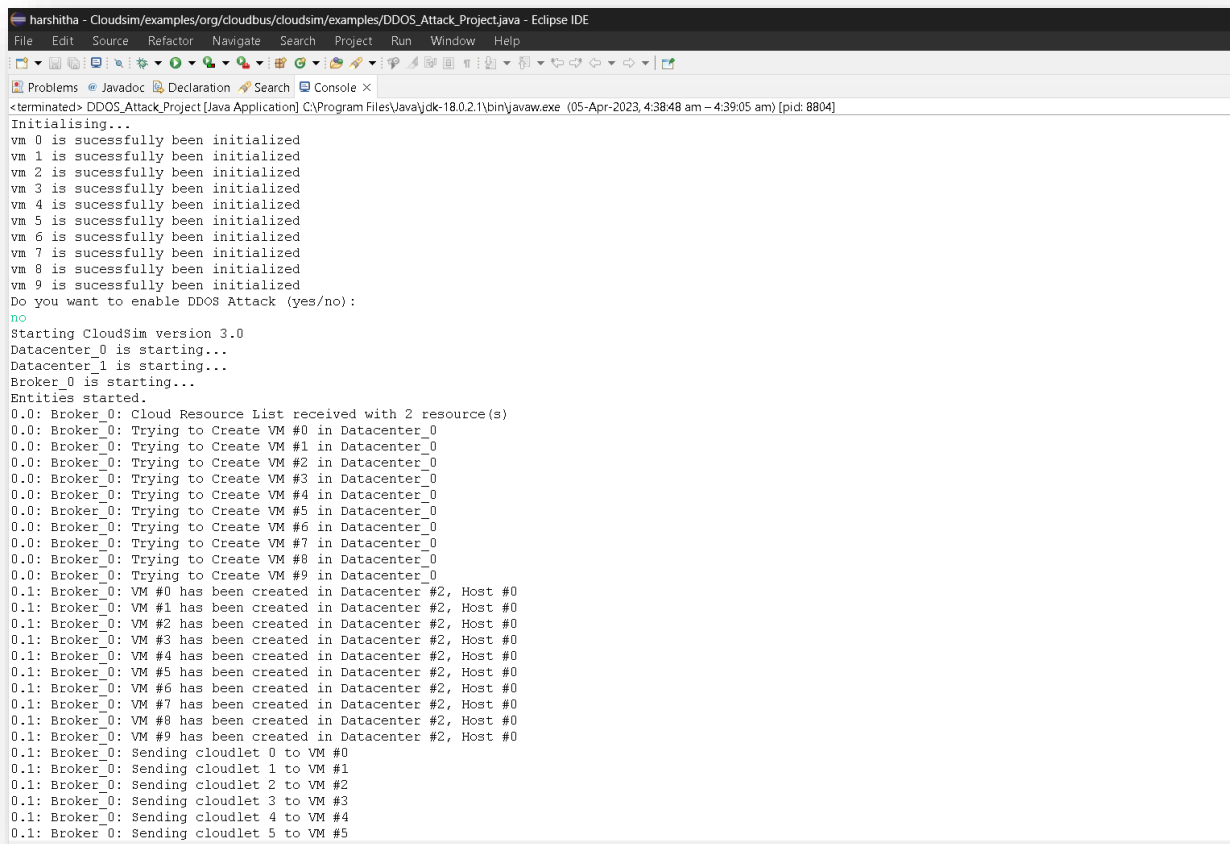
            Log.println(CloudSim.clock() + ": " + getName() + ": Sending cloudlet "
                + cloudlet.getCloudletId() + " to VM #" + vm.getId());
            //cloudlet.setVmId(1);
            cloudlet.setVmId(vm.getId());
            sendNow(getVmsToDatacentersMap().get(vm.getId()), CloudSimTags.CLOUDLET_SUBMIT, cloudlet);
            cloudletsSubmitted++;
            vmIndex = (vmIndex + 1) % getVmsCreatedList().size();
            getCloudletSubmittedList().add(cloudlet);
        }
    } else {
        for (Cloudlet cloudlet : getCloudletList()) {
            Log.println(CloudSim.clock() + ": " + getName() + ": Sending cloudlet "
                + cloudlet.getCloudletId() + " to VM #" + attackedVM);
            cloudlet.setVmId(attackedVM);
            sendNow(getVmsToDatacentersMap().get(attackedVM), CloudSimTags.CLOUDLET_SUBMIT, cloudlet);
            cloudletsSubmitted++;
            vmIndex = (vmIndex + 1) % getVmsCreatedList().size();
            getCloudletSubmittedList().add(cloudlet);
        }
    }
}

```

Fig 3. Snapshot of submitCloudlets() function

If the attack is not enabled, the global variable 'attackedVM' will be at its default value of -99. In that case, the cloudlets will be serviced normally. If the attack is enabled, the global variable 'attackedVM' will be equal to the Id of the VM that needs to be attacked. So now it creates the cloudlets in that particular VM whose Id is 'attackedVM'.

RESULTS AND DISCUSSIONS

The image is a screenshot of the Eclipse IDE's console window. The title bar at the top reads 'harshitha - Cloudsim/examples/org/cloudbus/cloudsim/examples/DDOS_Attack_Project.java - Eclipse IDE'. The console shows the output of a Java application. It starts with a message indicating the application was terminated. Then, it shows the initialization of 10 VMs (vm 0 to vm 9), each successfully initialized. A prompt asks 'Do you want to enable DDOS Attack (yes/no):' and the user has entered 'no'. The simulation then starts CloudSim version 3.0, initializing Datacenter_0, Datacenter_1, and Broker_0. It then shows the creation of 10 VMs in Datacenter_0, with each VM being assigned to Host #0. Finally, it shows the distribution of cloudlets to the VMs, with cloudlets 0 through 5 being sent to VMs #0 through #5 respectively.

```
<terminated> DDOS_Attack_Project [Java Application] C:\Program Files\Java\jdk-18.0.2\bin\javaw.exe (05-Apr-2023, 4:38:48 am - 4:39:05 am) [pid: 8804]
Initialising...
vm 0 is sucessfully been initialized
vm 1 is sucessfully been initialized
vm 2 is sucessfully been initialized
vm 3 is sucessfully been initialized
vm 4 is sucessfully been initialized
vm 5 is sucessfully been initialized
vm 6 is sucessfully been initialized
vm 7 is sucessfully been initialized
vm 8 is sucessfully been initialized
vm 9 is sucessfully been initialized
Do you want to enable DDOS Attack (yes/no):
no
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 #0
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 #0
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 #0
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 #0
0.1: Broker_0: Sending cloudlet 0 to VM #0
0.1: Broker_0: Sending cloudlet 1 to VM #1
0.1: Broker_0: Sending cloudlet 2 to VM #2
0.1: Broker_0: Sending cloudlet 3 to VM #3
0.1: Broker_0: Sending cloudlet 4 to VM #4
0.1: Broker_0: Sending cloudlet 5 to VM #5
```

Fig 4. Snapshot of VM and Virtual Data Center creation in cloudsim Here, 10 VMs having 512MB RAM and 250mips are created and are hosted in 'Datacentre_0' having Id = 2.

```
harshitha - Cloudsim/examples/org/cloudbus/cloudsim/examples/DDOS_Attack_Project.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help

Problems Javadoc Declaration Search Console X

<terminated> DDOS_Attack_Project [Java Application] C:\Program Files\Java\jdk-18.0.2.1\bin\javaw.exe (05-Apr-2023, 4:38:48 am - 4:39:05 am) [pid: 8804]
160.1: Broker_0: Cloudlet 0 received
160.1: Broker_0: Cloudlet 1 received
160.1: Broker_0: Cloudlet 2 received
160.1: Broker_0: Cloudlet 3 received
160.1: Broker_0: Cloudlet 4 received
160.1: Broker_0: Cloudlet 5 received
160.1: Broker_0: Cloudlet 6 received
160.1: Broker_0: Cloudlet 7 received
160.1: Broker_0: Cloudlet 8 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
Actual Cloudlets:
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
3           SUCCESS      2             3       160     0.1         160.1
4           SUCCESS      2             4       160     0.1         160.1
5           SUCCESS      2             5       160     0.1         160.1
6           SUCCESS      2             6       160     0.1         160.1
7           SUCCESS      2             7       160     0.1         160.1
8           SUCCESS      2             8       160     0.1         160.1
9           SUCCESS      2             9       160     0.1         160.1
CloudSim operation finished!
```

Fig 5. Snapshot of legit cloudlet creation without attack

If the attack is not carried out, the cloudlets will be created in available VMs.

```
harshitha - Cloudsim/examples/org/cloudbus/cloudsim/examples/DDOS_Attack_Project.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help
Problems Javadoc Declaration Search Console x
<terminated> DDOS_Attack_Project [Java Application] C:\Program Files\Java\jdk-18.0.2\bin\javaw.exe (05-Apr-2023, 5:19:59 am - 5:20:21 am) [pid: 8580]
Initialising...
vm 0 is successfully been initialized
vm 1 is successfully been initialized
vm 2 is successfully been initialized
vm 3 is successfully been initialized
vm 4 is successfully been initialized
vm 5 is successfully been initialized
vm 6 is successfully been initialized
vm 7 is successfully been initialized
vm 8 is successfully been initialized
vm 9 is successfully been initialized
Do you want to enable DDOS Attack (yes/no):
yes
Enter the virtual machine to be Attacked:
4
Enter the no of cloudlets to attack VM 4 :
20
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 #0
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 #0
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 #0
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 #0
0.1: Broker_0: Sending cloudlet 0 to VM #0
0.1: Broker_0: Sending cloudlet 1 to VM #1
```

Fig 6. Snapshot of enabling the attack on VM ‘4’


```

harshitha - Cloudsim/examples/org/cloudbus/cloudsim/examples/DDOS_Attack_Project.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help
Problems Javadoc Declaration Search Console X
<terminated> DDOS_Attack_Project [Java Application] C:\Program Files\Java\jdk-18.0.2\bin\javaw.exe (05-Apr-2023, 5:19:59 am - 5:20:21 am) [pid: 8580]
480.092: 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       479.99   0.1          480.09
10           SUCCESS   2                0       479.99   0.1          480.09
20           SUCCESS   2                0       479.99   0.1          480.09
1            SUCCESS   2                1       479.99   0.1          480.09
11           SUCCESS   2                1       479.99   0.1          480.09
21           SUCCESS   2                1       479.99   0.1          480.09
2            SUCCESS   2                2       479.99   0.1          480.09
12           SUCCESS   2                2       479.99   0.1          480.09
22           SUCCESS   2                2       479.99   0.1          480.09
3            SUCCESS   2                3       479.99   0.1          480.09
13           SUCCESS   2                3       479.99   0.1          480.09
23           SUCCESS   2                3       479.99   0.1          480.09
4            SUCCESS   2                4       479.99   0.1          480.09
14           SUCCESS   2                4       479.99   0.1          480.09
24           SUCCESS   2                4       479.99   0.1          480.09
5            SUCCESS   2                5       479.99   0.1          480.09
15           SUCCESS   2                5       479.99   0.1          480.09
25           SUCCESS   2                5       479.99   0.1          480.09
6            SUCCESS   2                6       479.99   0.1          480.09
16           SUCCESS   2                6       479.99   0.1          480.09
Actual Cloudlets:
26           SUCCESS   2                6       479.99   0.1          480.09
7            SUCCESS   2                7       479.99   0.1          480.09
17           SUCCESS   2                7       479.99   0.1          480.09
27           SUCCESS   2                7       479.99   0.1          480.09
8            SUCCESS   2                8       479.99   0.1          480.09
18           SUCCESS   2                8       479.99   0.1          480.09
28           SUCCESS   2                8       479.99   0.1          480.09
9            SUCCESS   2                9       479.99   0.1          480.09
19           SUCCESS   2                9       479.99   0.1          480.09
29           SUCCESS   2                9       479.99   0.1          480.09
CloudSim operation finished!

```

Fig 7. Snapshot of false and actual cloudlet creation after the attack
 Fig 6 and Fig 7 shows attack being carried out on VM with Id = 4 . Here, 20 cloudlets are created to attack the VM. Since that particular VM is accomodating the faux cloudlets as well, the time taken to process the actual cloudlet will increase and VM's performance under attack decreases. The decrease in performance of the VM is directly proportional to the number of cloudlets used to attack the VM.

| 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 |
| 3 | SUCCESS | 2 | 3 | 160 | 0.1 | 160.1 |
| 4 | SUCCESS | 2 | 4 | 160 | 0.1 | 160.1 |
| 5 | SUCCESS | 2 | 5 | 160 | 0.1 | 160.1 |

| | | | | | | |
|---|---------|---|---|-----|-----|-------|
| 6 | SUCCESS | 2 | 6 | 160 | 0.1 | 160.1 |
| 7 | SUCCESS | 2 | 7 | 160 | 0.1 | 160.1 |
| 8 | SUCCESS | 2 | 8 | 160 | 0.1 | 160.1 |
| 9 | SUCCESS | 2 | 9 | 160 | 0.1 | 160.1 |

The table given above is the output when the attack is not carried out. Here, the cloudlets are distributed among various VMs in a proper manner.

Given below, is the table that is obtained when an attack is carried out on a VM with Id as 4. Here, 20 faux cloudlets are created to simulate a DDoS attack on the VM. Actual cloudlets are then created. Clearly, the time taken to process the cloudlet increases when the VM is under attack.

| Cloudlet ID | STATUS | Data center ID | VM ID | Time | Start Time | Finish Time |
|-------------|---------|----------------|-------|--------|------------|-------------|
| 0 | SUCCESS | 2 | 0 | 479.99 | 0.1 | 480.09 |
| 1 | SUCCESS | 2 | 1 | 479.99 | 0.1 | 480.09 |
| 2 | SUCCESS | 2 | 2 | 479.99 | 0.1 | 480.09 |
| 3 | SUCCESS | 2 | 3 | 479.99 | 0.1 | 480.09 |
| 4 | SUCCESS | 2 | 4 | 479.99 | 0.1 | 480.09 |
| 5 | SUCCESS | 2 | 5 | 479.99 | 0.1 | 480.09 |
| 6 | SUCCESS | 2 | 6 | 479.99 | 0.1 | 480.09 |
| 7 | SUCCESS | 2 | 7 | 479.99 | 0.1 | 480.09 |
| 8 | SUCCESS | 2 | 8 | 479.99 | 0.1 | 480.09 |
| 9 | SUCCESS | 2 | 9 | 479.99 | 0.1 | 480.09 |
| 10 | SUCCESS | 2 | 0 | 479.99 | 0.1 | 480.09 |
| 11 | SUCCESS | 2 | 1 | 479.99 | 0.1 | 480.09 |
| 12 | SUCCESS | 2 | 2 | 479.99 | 0.1 | 480.09 |
| 13 | SUCCESS | 2 | 3 | 479.99 | 0.1 | 480.09 |
| 14 | SUCCESS | 2 | 4 | 479.99 | 0.1 | 480.09 |
| 15 | SUCCESS | 2 | 5 | 479.99 | 0.1 | 480.09 |
| 16 | SUCCESS | 2 | 6 | 479.99 | 0.1 | 480.09 |

| | | | | | | |
|-------------------|---------|---|---|--------|-----|--------|
| 17 | SUCCESS | 2 | 7 | 479.99 | 0.1 | 480.09 |
| 18 | SUCCESS | 2 | 8 | 479.99 | 0.1 | 480.09 |
| 19 | SUCCESS | 2 | 9 | 479.99 | 0.1 | 480.09 |
| Actual Cloudlets: | | | | | | |
| 20 | SUCCESS | 2 | 0 | 479.99 | 0.1 | 480.09 |
| 21 | SUCCESS | 2 | 1 | 479.99 | 0.1 | 480.09 |
| 22 | SUCCESS | 2 | 2 | 479.99 | 0.1 | 480.09 |
| 23 | SUCCESS | 2 | 3 | 479.99 | 0.1 | 480.09 |
| 24 | SUCCESS | 2 | 4 | 479.99 | 0.1 | 480.09 |
| 25 | SUCCESS | 2 | 5 | 479.99 | 0.1 | 480.09 |
| 26 | SUCCESS | 2 | 6 | 479.99 | 0.1 | 480.09 |
| 27 | SUCCESS | 2 | 7 | 479.99 | 0.1 | 480.09 |
| 28 | SUCCESS | 2 | 8 | 479.99 | 0.1 | 480.09 |
| 29 | SUCCESS | 2 | 9 | 479.99 | 0.1 | 480.09 |

CONCLUSION

The results shown in Fig. 5 and Fig. 7 demonstrate that the computation time taken by VM under attack is very high compared to VM in normal operation. The performance of the VM decreases when it is under attack. This can lead to a genuine user being denied the service, which can ultimately lead to cloud service providers losing their customers. Hence, DDoS is a serious security threat given that it can result in loss of data and financial loss. Cases of DDoS attacks are preventing the IT industries from completely shifting to cloud services. It takes a lot of time and money to fix the damage caused by DDoS attacks and sometimes the damage is permanent.

REFERENCES

- [1] M. Poongothai and M. Sathyakala, "Simulation and analysis of DDoS attacks," 2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSSET), 2012
<https://ieeexplore.ieee.org/abstract/document/6513885/similar#similar>
- [2] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, M. Rajarajan and R. Buyya, "Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions", 2017
<https://ieeexplore.ieee.org/document/7879103>
- [3] W. Alosaimi, M. Alshamrani and K. Al-Begain, "Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud", 2015
<https://ieeexplore.ieee.org/document/7373219>
- [4] A. Girma, M. Garuba, J. Li and C. Liu, "Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment," 2015 12th International Conference on Information Technology - New Generations, 2015
<https://ieeexplore.ieee.org/document/7113475>
- [5] A. Bhardwaj, G. Subrahmanyam, V. Avasthi and H. G. Sastry, "Solutions for DDoS attacks on cloud," 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 2016
<https://ieeexplore.ieee.org/abstract/document/7508107>
- [6] S. Karthik and J. J. Shah, "Analysis of simulation of DDOS attack in cloud," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014
<https://ieeexplore.ieee.org/document/7033841>
- [7] J. Jiao et al., "Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers," 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017
<https://ieeexplore.ieee.org/document/8069091>
- [8] J. Smith-perrone and J. Sims, "Securing cloud, SDN and large data network environments from emerging DDoS attacks," 2017
<https://ieeexplore.ieee.org/document/7943196>

- [9] Deepali and K. Bhushan, "DDoS attack defense framework for cloud using fog computing," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017
<https://ieeexplore.ieee.org/document/8256654>
- [10] B. Joshi, A. S. Vijayan and B. K. Joshi, "Securing cloud computing environment against DDoS attacks," 2012 International Conference on Computer Communication and Informatics, 2012
<https://ieeexplore.ieee.org/document/6158817>
- [11] M. Zekri, S. E. Kafhali, N. Aboutabit and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017
<https://ieeexplore.ieee.org/document/8284731>
- [12] G. S. Kushwah and S. T. Ali, "Detecting DDoS attacks in cloud computing using ANN and black hole optimization," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), 2017
<https://ieeexplore.ieee.org/document/8343555>
- [13] G. A. Sophia and M. Gandhi, "Stealthy DDoS detecting mechanism for cloud resilience system," 2017 International Conference on Information Communication and Embedded Systems (ICICES), 2017
<https://ieeexplore.ieee.org/document/8070740>
- [14] O. P. Badve, B. B. Gupta, S. Yamaguchi and Z. Gou, "DDoS detection and filtering technique in cloud environment using GARCH model," 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), 2015
<https://ieeexplore.ieee.org/abstract/document/7398603>
- [15] E. Anitha and S. Malliga, "A packet marking approach to protect cloud environment against DDoS attacks," 2013 International Conference on Information Communication and Embedded Systems (ICICES), 2013
<https://ieeexplore.ieee.org/document/6508330?arnumber=6508330>