ijergs
Open Access
International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in
ISSN: 2455 - 1597
Volume -2, Issue-4, July – August 2016, Page No. 20 - 29

DDOS Attack using Cloud Trace Back Methodology

Binita Gaurav[1], Sumit Kumar Bola[2], Mrs. Anuradha[3]
[1]M.Tech.Scholar, JVWU, Jaipur, India
[2,3]Research Supervisor, JVWU, Jaipur, India

Abstract
In the term Cloud computing, cloud means "everywhere". Cloud computing, is also on demand computing, which is Internet based computing system .Cloud computing is a technology in which we can store and collect the data through the internet .There are three services which is used in cloud computing i.e. SAAS, PASS&IAAS. Beside the advantages cloud computing has disadvantages too. In cloud architecture, Data security and privacy protection Issues are related to both hardware and software. When the Issues of cloud security come up, security threats such as maintenance of data integrity, data safety and data hiding dominate clients concerns. The data communicates on the internet is at risk to the attackers attack. Several techniques and methods are being used to secure Cloud environment from these attackers. Cloud Computing uses the virtualization concept. Virtualization is a methodology of resource divide of a computer into multiple execution environments, by applying technologies such as software and hardware partitioning In the traditional technology we download the software in to the internet or install own computer but in the new technology we don't need the download the software in the internet all works are completed without download any software. Cloud computing works as PAY-PER-USE..In this research paper i would like to highlight some core issues like what is the cloud computing system ,advantage and disadvantage of cloud computing service models of cloud computing system, and virtualization or cloud trace back model that are used in this research paper to prevent or detect for DDOS attack. The environment can be setup using Desktop PC's running ubuntu with Open Stack by using Open Stack Cloud Manager
Keywords: Cloud computing, SAAS, PAAS, IAAS, Virtualization, DDOS, Open Stack, Cloud Trace, Back Model.

1. Introduction

Cloud computing is a technology in which we can store and collect the data through internet. With the help of it users store the local data in remote data server. Service provider is a cloud service provider system through which we find stored data in remote data centre. So that we have to be much careful while we are searching our stored data in remote data centre. Now a day's cloud computing system is become more sensual subject. Shared computing resource collection is called cloud. Cloud computing system is used for virtualization. Virtualization is a methodology which divided computer resources in many execution environments and it works with many technologies. It provides development environment, allocation and reallocation of resources when needed, storage and networking facility virtually. Garter defines Cloud Computing as "a style of computing where massively scalable IT enabled capabilities are delivered 'as a service' to external customers using Internet technologies" [1] cloud computing is a type of next generation computing system which is based on internet. It provides services easily to the users so that they will easily work on different type of computing system. It gives a new technique so that with the help of internet we are able to access and store cloud data.

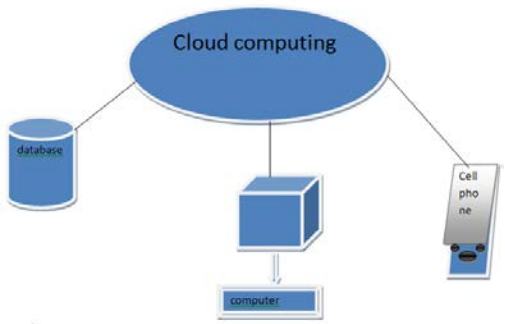

Figure 1: Cloud Computing Architecture

2. Cloud computing Classification based on services provided

Cloud Computing Service Models: There are three services which are based in cloud computing system. The cloud computing services are also known as SPIMODEL which are defined by the NIST{National Institute Of Standards And Technology}.

These three services models are:-

- SAAS:-Software as a service
- PAAS:-Platform as a service
- IAAS:-Infrastructure as a service

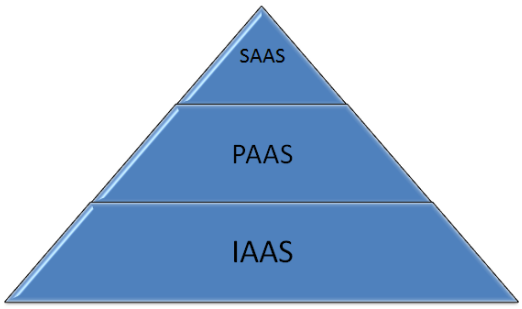

Figure 2: Service Model

Software as a service (SAAS): SAAS is internet based software. It is a delivery model where the software and the associated data are hosted in a cloud environment by a third party such as Cloud Service Provider (CSP)[2][3]. It provides the computing platform to user for use. Some example of SAAS Face book, Twitter, Google apps.

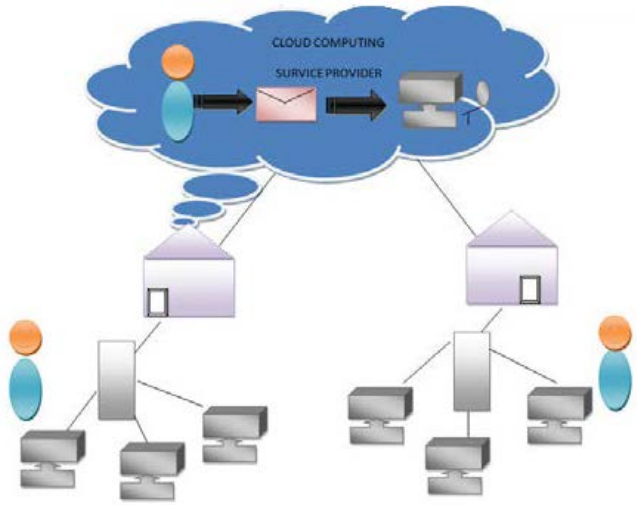

Figure 3: SAAS Architecture

Platform as a service (PAAS): This service models are widely used by the developers who want to develop or run a cloud application for a program. It provide platform as layer resource. It gives the facilities such as: the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers [3].

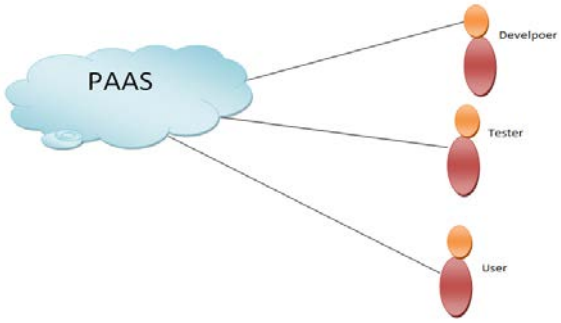

Figure 4: PAAS Architecture

Infrastructure as a service (IAAS): IAAS is the base layer of cloud computing which are based with Virtual machine, server, and storage .This is a complete platform which is used by large scale enterprise customers. IAAS mitigates the need for a data centre, and maintaining hardware at the local level. Sometimes IAAS is otherwise regarded as Hardware as a Service (HAAS). Examples include Amazon Web Service (AWS), Rackspace, and Windows Azure etc. [4]

Cloud computing Deployment model

- Private Cloud
- Public Cloud
- Hybrid Cloud

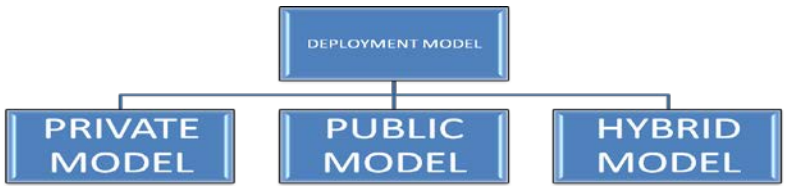

Figure 5: Cloud computing Deployment model

Private Model: In this model recourses are used only for single organization. A private cloud is suitable for organizations that have certain security and performance monitoring tools that the public cloud provider doesn't use. More costly than public cloud.

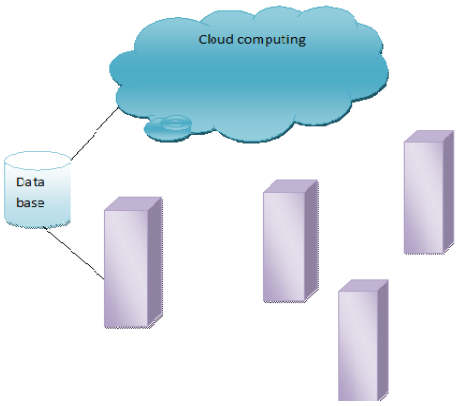

Figure 6: Used by only authenticated organization

Public Cloud: In the public cloud all resources over the internet. Computing resources are measure data granular level, in which the users are pay only for that resources and workloads which they used. [9].Public Cloud works over the PAY-PER-USE model .More resources are available in public cloud.

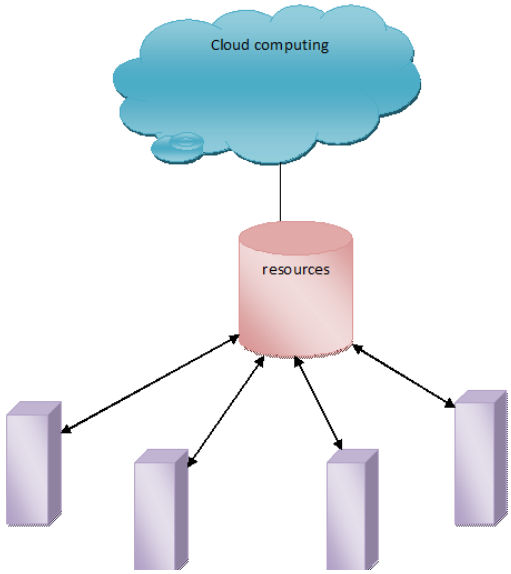

Figure 7: Access the resources when you when you need them. Resources are available for all organization

Hybrid Cloud: The Hybrid cloud deployment is mix-up with Private or Public cloud. One of the disadvantages of these services is that we have to manage different security platforms together.

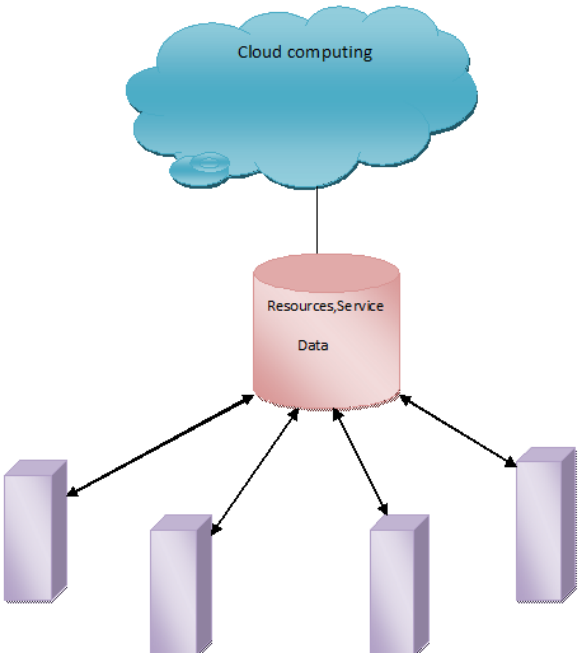

Figure 8: Freedom to Apps & Data Resources

3. Advantages of Cloud Computing

Vast Range: The cloud computing protect from any kind of storage problems. so that the users has not required to install any kind of software.

Flexibility: In cloud computing with the help of internet we are able to access and store cloud data anywhere in the world or any systems. This is the advantage of it.
Effective: Cloud computing is very less expensive so that users need not to expend money on hardware and software systems [5].
Pay–per-use Computing resources are measure data granular level, in which the users are pay only for that resources and workloads which they used. [9].
Synchronization and integrity: Through this function Business people can share their data or documents from one place to another place through the internet. They are free to carry any specific hardware or software with them.[8]

4. Disadvantages of cloud computing

Migration Problems: In this system we can find migration issues when the users have work from other provider. There is difficult to transfer huge data from one provider to the.
Growth of Cloud Computing Vs Smart Computing:- The inflexion point of Smart Computing will happen When analytics, BI and awareness based technologies including RFID can be used to make Customer experiences consistently positive and Drive cultural change throughout a business to centre on customers' expectations. In 2012, financial services, professional services, and manufacturing will be the three industries that dominate software purchases.
Risk in Cloud Company:- Garther says; Cloud computing has "exclusive attributes that require risk measurement in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as discovery, regulatory compliance and auditing," (Compare security product.)Customers demand transparency, avoiding vendors that refuse to provide detailed information on security programs. Ask questions related to the qualifications of policy makers, architects, coders and operators; risk control processes and technical mechanisms; and the level of testing that's been done to verify that service and control processes are functioning as intended, and that vendors can identify unexpected vulnerabilities. According to analyst firm Gartner "Cloud computing is fraught with security risks", Smart customers will consider getting a security assessment from a Impartial third party before committing to a cloud seller, Gartner says in a June report titled "Assessing the Security Risks of Cloud Computing."[7]
Dependency: In cloud computing we find users dependency on the provider.
Risk and Insecurity:- Cloud computing services is a service of mean taking services from remote servers. User are unable to control the software's which they used and also, unable to protect the stored documents. There is less probability to restore all deleted or corrupted stored documents.

Advantages	Disadvantages
Flexibility	Dependency
Effective	Unpredicted cost
Mobility	Migration Problem
Enable IT Innovation	Security and Privacy
Backup and disaster recovery	Control and reliability

Figure 9: Table of advantages or disadvantages in cloud computing

Virtualization: Virtualization is used to improve scalability or resource utilization. Virtualization refers to the act of creating a virtual (rather than actual) version of something, including virtual platforms..etc.

Figure10: Virtualization architecture

Traditionally the operating system and its application were tightly coupled to the hardware they were install in virtualization breaks the link between operating system and physical hardware. This allows the ability to change Hardware without replacing the operating system or application [17].

5. DDOS Attack In Cloud Computing

Distributed Denial of Service is a type of attack that aims to make services or resources unavailable for indefinite amount of time by flooding it with useless traffic. The two main objectives of these attacks are, to disable computer resources (CPU time, Network bandwidth) so that it makes services inaccessible to authorized users. it is also possible that a lot of malevolent hosts correspondent to flood the victim with an great amount of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is called a Distributed DOS, or DDOS attack. DOS attacks attempt to finish the victim's resources.

Types of DDOS Attack There are three types of DDOS attack

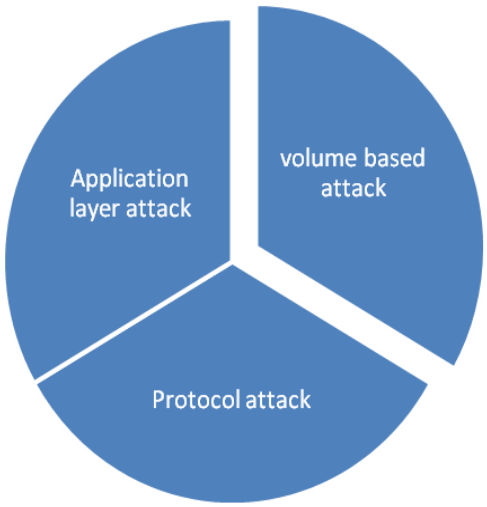

Figure11: Types of DDOS attack

Volume Based Attacks/Bandwidth Based Attacks: This attack makes an attempt to overlay the victim with large amounts of junk data thereby consuming the network bandwidth and resources. Examples include UDP floods, ICMP floods [18] [19].

Protocol attack:-The attack tries to take advantage of the lacuna associated with various network protocols to overload the target's resources. Examples include Ping of Death, Smurf attack, SYN floods, fragmented packet attack etc [18] [19]

Layer attacks: The attack concentrates on specific web applications and sends HTTP requests beyond the limits it can handle. This kind of attack includes HTTP DDOS attack and XML DDOS attacks or REST based attacks [19].

Open Stack: Open Stack is open source cloud computing software that provides Infrastructure as a Service cloud formation for public and private cloud. Open Stack was first proposed in June 2010, born with its original code from NASA's Nebula platform and Rack space's Cloud Files platform. Open stack aims as reported by [23] "To produce the universal open source cloud computing platform that will meet the needs of public and private cloud providers regardless of size, by being simple to implement and massively scalable". Although open Stack is open source software but many Linux Distributions provide it as an operating system also like Ubuntu Canonical [24].

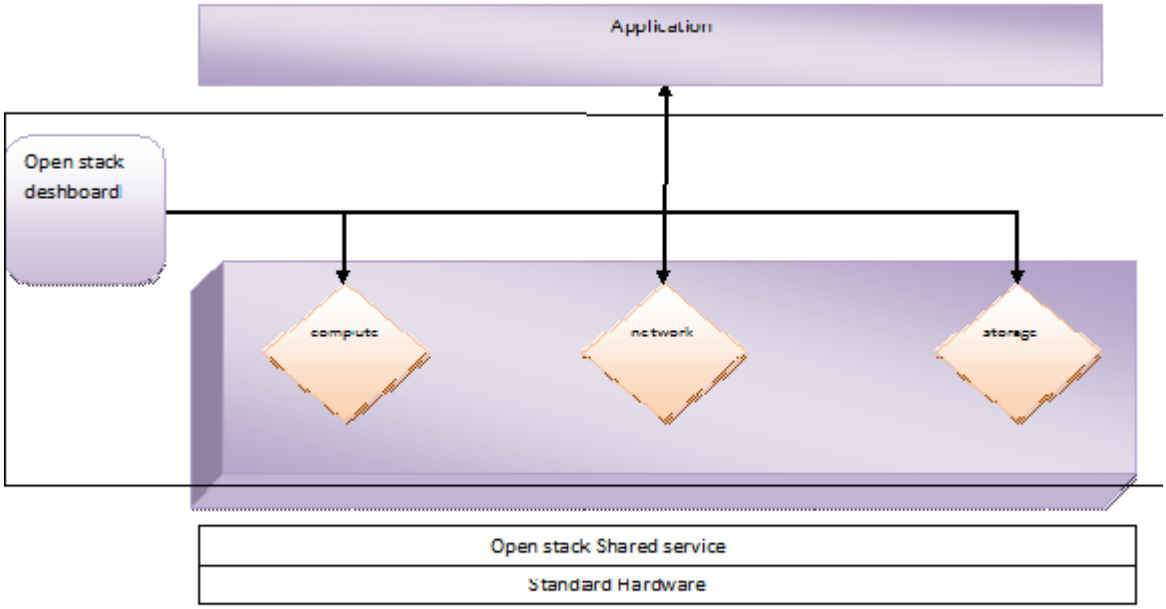

Figure12: Open Stack Architecture

Open stack dash board**:-**open stack dashboard provides a web based user interface to open stack [26].
Compute: The term compute is commonly encountered in server as well as in cloud computing where a big compute as a play off the popular big data item.
Network: A network is a group of two or more computer they combined together.
Storage: A method widely used for storing something for future use.
Open Stack Shared Device: it is the term where all resources are available in the whole system.
Cloud Trace Model (CTM): I developed a technique against DDOS attack in Cloud Computing. Cloud Trace Model (CTB) which is based upon Deterministic Packet Marking (DPM) Algorithm [29] [30]. The verifier node is response for the verification process for updating the white and black lists. On the other hand, the subsequent requests coming from authorized users will be forwarded directly to the target cloud service since their IP addresses will be found in the white list. In an attack scenario, the attack client will request a web service from CTB, which in turn will pass the request to the web server. The attack client will then formulate a SOAP request message based on the service description. Upon receipt of SOAP request message, CTB will place a CTM within the header. Once the CTM has been placed, the SOAP message will be sent to the Web Server. Upon discovery of an attack, the victim will ask for reconstruction to extract the mark and

inform them of the origin of the message. The reconstruction will also begin to filter out the attack traffic. The message is normal, the SOAP message is then forwarded to the request handler for Processing requests or any outgoing message. [30]

Proposed methodology: In this section, a method for DDOS detection and prevention by Cloud Trace Back Model (CTB) is proposed. DDOS attacks can be performed by using command 'hping3', which means that attacker is hiding source IP address i.e. destination machine will see source from random source IP address than actual (IP masquerading), and destination machine will get overloaded within 5 minutes and stop responding. The environment can be setup using Desktop PC's running ubuntu with Open Stack by using Open Stack Cloud Manager

Open stack cloud manager: it is widely used for easy to develop and use cloud management software that is based on open stack.

1. Algorithm : CTM Action

if (CTB places CTM in header)
{
Soap message sent to the server
}
else
{
Wait for place the CTM in headers
}
end if
if (Soap message sent to the web server=TRUE)
{
if (verify the message= no victims)
{
SOAP messages forwarded to the request handler to process the web server (Respond to HTTP Request).
}
else
{
And then repair to extract the mark and educate them of the origin of the message.
}
end
end

2. Algorithm VF Action

Input:
P← Packet
S← IP Address of source packet
D← IP Address of destination packet
BL← Blacklist
WL←Whitelist
begin:
If (S c WL && S∉BL)
Forward P to D
else if (S c BL) **drop** p
else forward p to a V-node
end

3. Algorithm V-NODE Actions

Input:
P ←Packet
S← IP Address of source packet
D← IP address of destination packet
BL← Blacklist
WL←Whitelist

begin:
if (S ∉ BL && S ∉ WL)
{
Send to S a unique Question test
if (Question test passes)
{
WL-WL+S
Forwarded P to d.
}
else
BL-BL+S
end

6. Future Scope

An algorithm can be develop that will extract log information from accessible locations in crime scenes. The development of a guideline that will be used to validate evidence collected using this service. We will be setting up to initial real-time data gathering and testing of Cloud Protector. This will allow us to fine tune CTB to better detect and filter DDOS attacks.

7. Conclusion

Cloud computing is a advance technology of computing system in which we are able to collect data through internet and protect stored data from any kind of viruses. Present work deals with the many core issues such as: introduction of cloud computing system, different types of service models such as SAAS, PAAS, IAAS which is used for specific application and advantages or disadvantages of the cloud system. A virtual machine placed in a cloud environment for used to execute crime. Algorithm 1 and Algorithm 2 shows the actions that is taken by the VF and the V-Node when considering that the architecture is protected against the IP spoofing attacks .this activity is set up by using two Desktop PC's, in which both running Ubuntu 14.04. Here, a open source cloud manager, Open Stack is used, in which one of the hosts is running Open Stack host virtual machines

8. References

[1]. Gartner. Predicts 2014: Cloud Computing Affects All Aspects of IT Technical report. http://www.gartner.com/technology/topics/cloudcomputing.jsp.
[2]. A Survey on Cloud Computing www.ijarcsse.com/docs/papers/Volume_4/7_July2014/V4I7-0216.pdf
[3]. P.Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.
[4]. Layers of cloud – LAAS, PAAS, SAAS . A Survey
www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503394.pdf
[5]. www.ijarcsse.com/docs/papers/volume-3/10-october 2013/V318-0505.pdf
[6]. http://djacademy.ac,in/Tech Freaks/cloud.html.
[7]. Community cloud computing benefits and drawbacks. http://www.computerweekly.com/news/1510117/Community-cloud-computing-benefits-and-drawbacks.
[8]. Cloud computing security, http://en.wikipedia.org/wiki/Cloud_computing_security.
[9]. Survey paper on basics of Cloud Computing and Data Security http://www.ijcstjournal.org/volume-2/issue-3/IJCST-V2I3P4.pdf.
[10]. A survey paper on Cloud Computing ieeexplore.ieee.org/iel5/6167332/6168306/06168399.pdf
[11]. IBM-What is Cloud Computing: https://www.ibm.com/cloud-computing/what-is-cloud-computing
[12].Private Vs Public Vs Hybrid cloud: https://www.glowtouch.com/blog/cloud/private-vs-public-vs-hybrid-cloud-which-is-better/
[13]. Private Vs Public Vs Hybrid cloud: http://www.logicworks.net/blog/2015/03/difference-private-public-hybrid-cloud-comparison/
[14]. Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, and Maik Lindner. A break in the clouds: towards a cloud definition. ACM SIGCOMM Comput. Commun. Rev., 39(1):50–55, 2009.
[15]. Michael Armbrust, Armando Fox, and et al. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB-EECS-2009-28, University of California, Berkeley.
[16]. S.S. Chopade, K.U. Pandey, D.S. Bhade, Securing Cloud Servers against Flooding Based DDOS Attacks, in Proc. International Conference on Communication Systems and Network Technologies,2013.

[17]. DDoS Attack. http:// www.incapsula.com/ddos/ddos-attack
[18]. T.Siva, E.S.Phalguna Krishna, Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, International Journal of Engineering Trends and Technology (IJETT), vol. 4, May 2013.
[19]. B. Prabadevi, N.Jeyanthi, Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey, IEEE Explore, 2014.
[20]. K.Shanti, A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013
[21]. George Sibiya , Hein s. Venter2 and Thomas Fogwill, "Digital Forensic Framework for a Cloud Environment" IIMC International Information Management Corporation, 2012,pp-2-8
[22].Tutorial,OpenStack.CloudCom,IEEE.[Online]2010:http://salsahpc.indiana.edu/CloudCom2010/slides/PDF/tutorials/OpenStackTutorialIEEECloudCom.pdf.
[23]. https://opensource.com/resources/what-is-openstack
[24]. docs.openstack.org/developer/horizon
[25]. Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi,"Securing cloud computing environment against ddos attacks"International Conference on Communication, Volume 5.
[26]. Edos-Shield - A Two-Steps Mitigation Technique against Edos Attacks In Cloud computing," 2011 Fourth IEEE International Conference on Utility and Cloud Computing"

.