International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Prevention of DDos Attacks in Cloud Using Honeypot

Kumar Shridhar[1], Nikhil Gautam[2]

[1, 2]Department of Computer Science and Engineering, Bhagwan Parshuram Institute of Technology
Rohini, Delhi, India

Abstract: ***Cloud computing is a type of internet based computing where different services – such as server, storage and applications are shared on the internet. This makes cloud computing one of the most promising and rapidly growing technology. As it relies on sharing computer resources, it is prone to various security risks. One such security issue is Distributed Denial of Services attack on cloud. A DDos attack can originate from anywhere in the network and typically overwhelms the victim server by sending a huge number of packets. This paper deals with the prevention of DDos attacks and how honeypot approach can be used in cloud computing to counter DDos attacks.***

Keywords: Cloud Computing, Honeypot, cloud attacks, DDos, cloud models

1. Introduction

Cloud computing is a computing paradigm where a large pool of system are connected in private or public network to provide dynamically scalable infrastructure for application data & file storage. [1] According to Gartner Inc. cloud computing is a disruptive phenomenon with the potential to make IT organization more responsive than ever, cloud computing promise economic advantage speed, agility, flexibility, infinite elasticity and innovation.

2. Types of cloud computing models

2.1 SAAS (software as a service)

In this model a complete application is offered to the customer as per the demand of the customer on cloud only single instance of service runs. Now a days software as a service is offered by Google, Salesforce, and Microsoft [1]. In this cloud provider manages the infrastructure and platform that run the application, sometimes it is referred as "on demand service" and is usually priced on pay per usage.

2.2 PAAS (platform as a service)

In platform as a service an operating system ,hardware and network are provided by the provider and the customer only install or develop its own software and models[2].

2.3 IAAS (infrastructure as a service)
It is a provision model in which organization outsources the equipment for support in some operations. They outsource storage, hardware, servers and networking components. In IAAS cloud provider is the owner of all equipment which are outsourced by the organization and service provider is responsible for running and maintaining its equipment.[3]

3. Deployment Models of Cloud

3.1 Public Cloud

Public cloud are owned and operated by cloud provider. In public cloud user pay only for the time duration they use the service i.e. pay per usage.[2]

3.2 Private Cloud

Private cloud are those cloud which are operated only for specific organisation and these cloud are maintained and managed by the third party.[4]

3.3 Hybrid Cloud

Hybrid cloud is the combination of multiple cloud. In this we have public cloud as well as private cloud and community cloud also.[2]

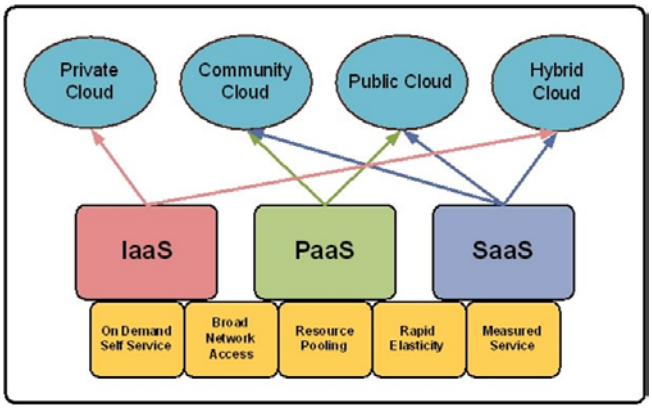


Figure 1: Cloud deployment and computing model

4. List of Attacks

Here is the list of top threats to the cloud computing which is pointed out by the CSA (cloud security alliance) [5]

1. Data breaches
2. Data loss
3. Account or service traffic hijacking

4. Insecure interfaces and API
5. Dos (denial of services)
6. Malicious insider
7. Cloud abuse
8. Insufficient due diligence

Here are some other attack on cloud computing: [6]

1. SQL injection attacks
2. Captcha breaking
3. Cross site scripting
4. Reused IP address
5. DDos (distributed denial of services)

Now we will discuss some of the attacks:-

4.1 Data breaches

For our data to be safe we encrypt our data but once we lose the encryption key, we will lose our data. So how hackers breaches a cloud infrastructure? [7] Answer of that question lies in the following steps:

- **Incursion**- hackers gain access to network using side channel timing information to extract private cryptographic keys.
- **Discovery** – hackers map out the company's system and search the confidential data.
- **Capture** – attacker take control of keysytem and collect the data as it flows through these system.
- **Exfiltration** – the stolen data is sent out the front door to external services under control of the attacker. [7]

4.2 Data Loss

According to CSA data get lost due to some disaster such as fire, flood or any earthquake. Data lost may also take place because of some malicious hacker. Sometime malicious hacker deletes the data. [5]

4.3 Malicious Insider

In this threat some current or former employee, contractor who has or had authorized access to an organisation network, system or data and intentionally exceeded or misused that access in a manner that negatively affect the confidentiality of information system.[8]

4.4 Dos (denial of services)

According to CSA Dos attack is ranked as fifth top threat to cloud computing. As cloud services becoming increasingly popular these days denial of services attack are attacks are getting more frequent. A dos attack make the network or machine unavailable to user by flooding them with connection request.[5][10]

4.5 DDos (Distributed denial of services)

Distributed Denial of Service (DDoS) attack, which means many nodes systems attacking one node all at the same time with a flood of messages.

5. Distributed Denial of Services

Denial of service (DoS) attacks are among the oldest types of attacks against Web sites. The variant forms of DDoS attack tools like Agobot (F-Secure, 2003; Sophos, 2009), Mstream (Dittrich, 2000) and Trinoo (Dittrich, 1999) are still used by attacker today. But most attackers are more inclined to use the less complicated web based attack tools like Extensible Markup Language (XML)-based Denial of Service (X-DoS) and Hypertext Transfer Protocol (HTTP) - based Denial of Service (H-DoS) attack due to their simple implementation and lack of any real defenses against them.

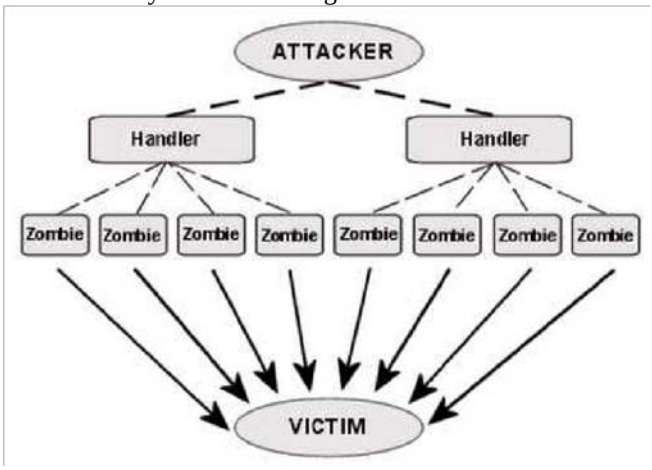


Figure 2: Architecture of a DDos attack

5.1 XML Based DDos attack

An XML denial-of-service attack (XDoS attack) is a content-borne denial-of-service attack whose purpose is to shut down a web service or system running that service. XML DoS attacks are extremely asymmetric: to deliver the attack payload, an attacker needs to spend only a fraction of the processing power or bandwidth that the victim needs to spend to handle the payload. Use of XML-based Web services removes the network safety net because messages will transit ports that are open for internet access (ports 80 and 443).[11]

5.2 HTTP Based DDos attack

This kind of attack is particularly troublesome to deal with. While simplistic packet-based attacks can be more easily mitigated upstream, with an HTTP-based attack it is often difficult to distinguish attack traffic from legitimate HTTP requests. When an HTTP client talks to an HTTP server (a Web server), it sends requests which can be of several types, the two main being GET and POST. A GET request is what is used for "normal links", including images; such requests are meant to retrieve a static piece of data, the URL pointing to that piece of data.

When you enter a URL in the URL bar, a GET is also done. POST requests are used with forms. A POST request includes parameters, which are usually taken from the input fields on the same page. [11]

6. DDos defense mechanism

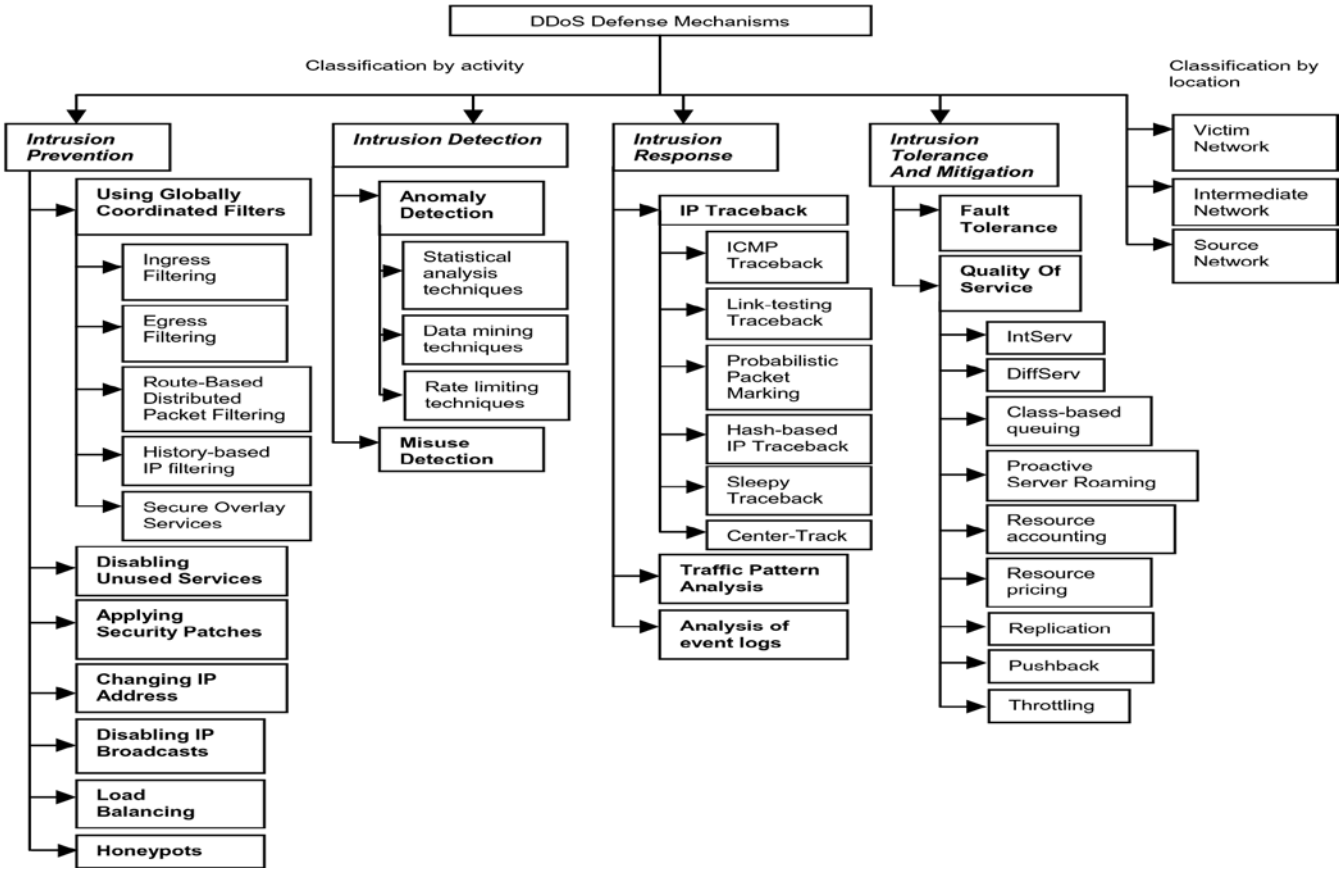
There is no fixed way to detect and prevent DDos attacks as the nature of attack varies. Also the attacker can hide his identity and use IP spoofing.

We may classify DDoS defense mechanisms using two different criteria. [22] The first classification categorizes the DDoS defense mechanisms according to the activity deployed. Thus we have the following four categories:

- Intrusion Prevention,
- Intrusion Detection,
- Intrusion Tolerance and Mitigation
- Intrusion Response.

The second classification divides the DDoS defenses according to the location deployment resulting into the following three categories of defense mechanisms:

- Victim Network,
- Intermediate Network, and
- Source Network.



7. Related Work

In [12], the author used Egress Filtering to filter the network outbound traffic. It briefly gives example for what DDos attacks it can block and provide details on how to execute filtering to the site.

In [13], the author used port hopping technique in which application parties communicate via port that changes over time. But no pre calculated formula can be used as it becomes easier to trace and random number generator should be preferred.

In [14], the author used covariance matrix calculation modelling which occurred in three phases: In first phase the network is monitored and if found abnormal, detection phase starts. Then finally when the attack has been known, legitimate traffic to victim's virtual machine is shifted to same virtual machine but in another physical machine.

In [15], the author uses queuing theory model to detect Dos attacks. It first detects the abrupt change in the model and signal generation module is used for processing it.

In [16], the author tells the performance of time based queue management practices in context of flood Dos attack on connection oriented protocols where service resources are depleted by uncompleted illegitimate requests generated by the attacker. It included both crippling Dos attack and Quality of Service (QoS) degradation attack.

In [17], the author uses a simple, effective, and straight forward method for using ingress traffic filtering to prohibit Dos attack which uses forged IP addresses to be propagated from behind and Internet Service Provider (ISP) aggregation point.

In [18], the author applied a cloud intrusion detection system known as Entropy based Anomaly Detection System. Used defense mechanism helps user to detect and block the attack after reaching the victim with high detection rate. If threshold

of entropy is carefully set, it can completely detect the DDos attacks.

In [19], the author uses Virtual Machine Monitor (VMM) to monitor virtual machine resource availability and aims to monitor and compute the available amount of current system resources and compares it with a given threshold to find the existence of an attack. This method makes the system to escape from attack without stopping the operating system.

8. Proposed Framework

Several proposals have been proposed to deal with DDos attacks but as the way of attack change every time, no proposal can completely prevent attack DDos attacks.

One such approach is Honeypot approach. Honeypots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. [26]

The mechanism works in two steps: First we can defend our operational network with a high probability against known DDoS and against new, future variants. Second, we trap the attacker so that recording of the compromise can help in a legal action against the attacker.

Figure 4 illustrates the implementation of honeypot in the cloud. In this security infrastructure, we introduce a new system: a honeypot that should attract distributed denial- of-service attackers. [23] Web server, mail server, client etc. are forwarded to the legitimate destination and honeypot fulfil the task of luring the attacker. Standard mechanisms are used for protection of web and mail servers. Services such as web, mail, ftp services and DNS that should be accessible form the out- side are situated in a demilitarized zone (DMZ).

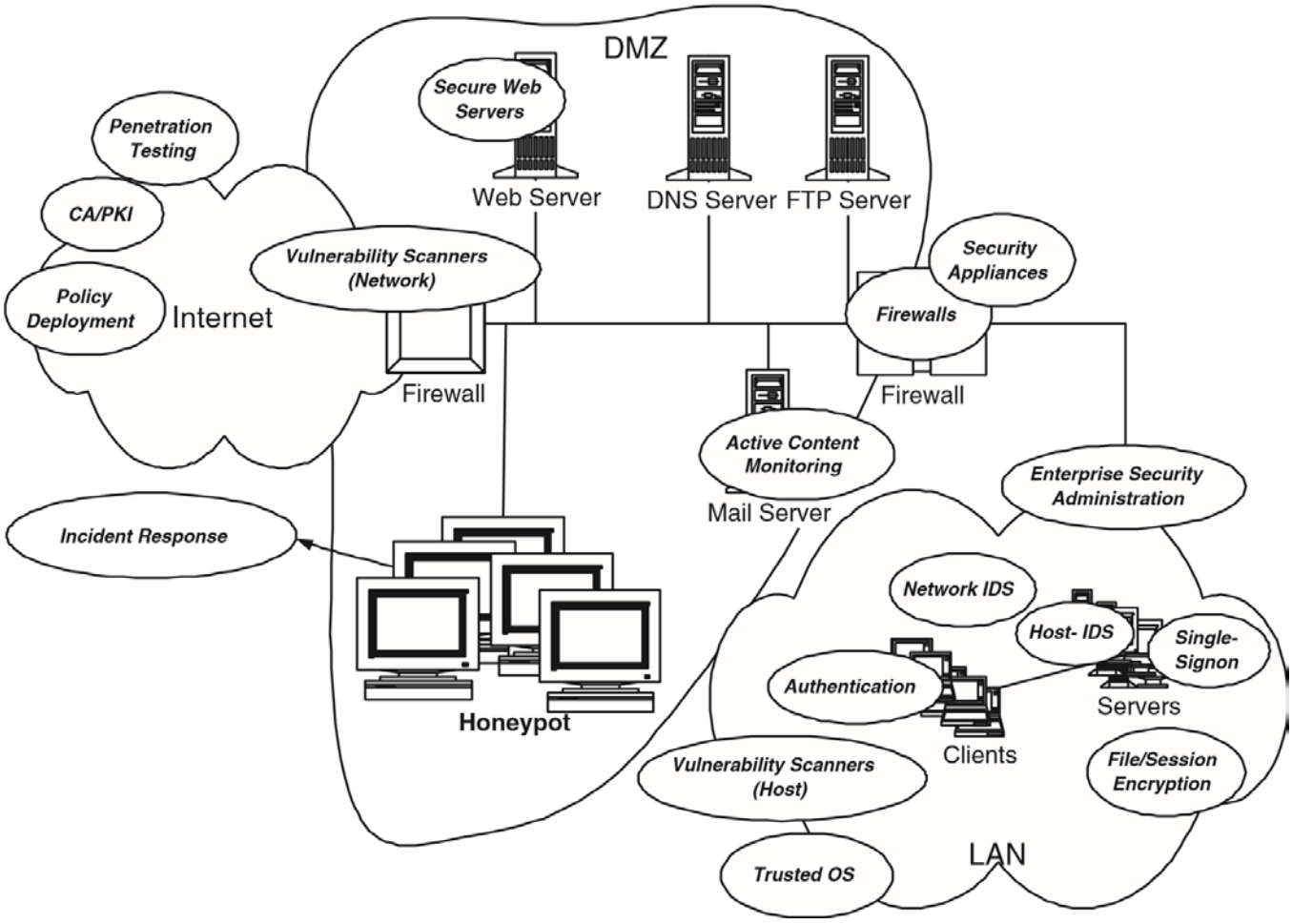


Figure 4: Implementation of Honeypot in cloud

Three major problems must be solved to successfully project this illusion to the attacker:

1. The attack must be detectable.
2. The attack packets must be actively directed to the honeypot.
3. The honeypot must be able to simulate the organization's network infrastructure, at least the parts known to the attacker.

The first issue is linked to the solution of the second problem: both should ideally be implemented by a transparent packet forwarder at the border of the corporation's DMZ. Finally, the third problem can be solved by employing a variant of the Honeynet approach.

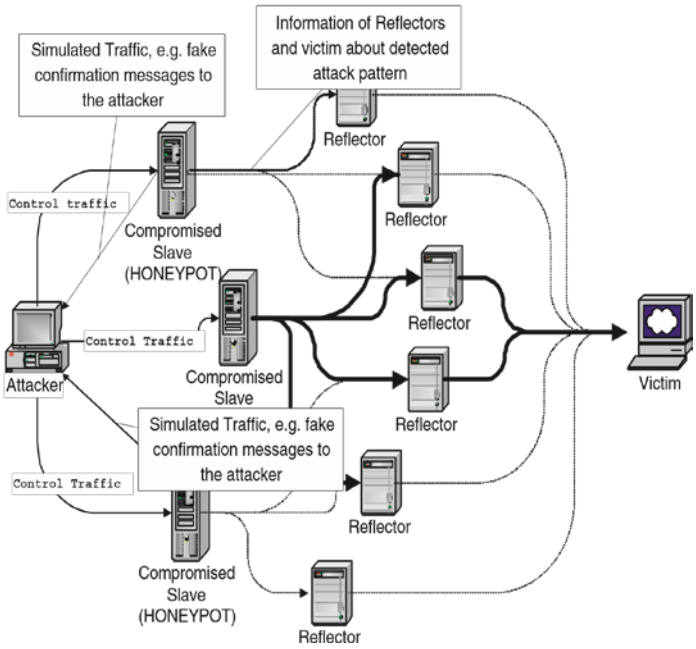


Figure 5: Tracing of the attacker

This method is very much effective but has a drawback. New attacks may not be detected unless our system knows the signature.

9. Conclusion and Future Outlook

Cloud computing is one of the most rapidly growing technology and is constantly under threat of attacks. This paper deals with one such attack – DDos attack and its prevention strategies. Honeypot approach is used to deal with such attack as it not only lures the attacker to attack the network but also alert the network administrators of a possible intrusion by trailing the attacker. Honeypots can be used together with some other form of security such as an IDS to increase its efficiency. Both the cloud computing and honeypot approach are new topics and further refinement can be done in each field.

References

[1] Tonny Harris, "*CLOUD COMPUTING AN OVERVIEW*",available at-"http://www.thbs.com/services/cloud-computing" page no-2-3.
[2] http://www.gartner.com/it-glossary/cloud-computing/
[3] Pankaj Arora, Rubal Chaudhary wadhwan, Er. Satinder pal ahuja,"*Cloud computing security issues in Infrastructure as a Service*" ,"*International journal of advance research in computer science and software engineering*"volume-2,issue-1,January 2012.
[4] "*Factsheet*","*office of the privacy commissioner of canada*"available at-www.priv.gc.ca
[5] Top 9 threats to cloud computing discovered by"*cloud security of alliance*"available at-www.infoworld.com/article/2613560/cloud-security/9threats-to-cloud-computing-security.html.
[6] Vahid ashktorab, Seyed Reza Taghizadeh,"*Security threats and countermeasures in cloud computing*"," *International journal of application or innovation in engineering and management*" volume-1,issue-2,October 2012.
[7] "*Industry Brief- Cloud breach* ","*Symantec corporation*"page no-2. Available at-www.symantec.com/cloud.
[8] Minh-Duong Nguyen, Ngoc-Tu Chau, Seungwook Jung, and Souhwan Jung,"A demonstration of malicious insider attacks inside cloud Iaas vendor","*International journal of information and education teachnology*"vol.-4,no.-6,December 2014.
[9] Chimere Barron, Huiming Yu and Justin Zhan,"*Cloud computing security case studies and research*"," *Proceedings of the World Congress on Engineering 2013 Vol II,*",WCE 2013,July 3-5,2013,London U.K.
[10] "cloud computing and denial of service attack:examining the ntp servers",available at-" https://blog.spideroak.com/20140218184853-cloud-computing-and-denial-of-service-attacks-examining-vulnerability-of-ntp-servers"posted on February 2014.
[11] K.Santhi, "A Defense Mechanism to Protect Cloud Comuputing Against Distributed Denial of Service Attacks", "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 5, May 2013
[12] J.Rameshbabu, B.Sam Balaji, R.Wesley, Daneil, K.Malathi, "A prevention of DDos attacks in cloud computing using NEIF attack", "International Journal of Scientific and Research Publications", Volume 4, Issue 4, April 2014
[13] 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)", - Volume4Issue5- May 2013
[14] Mohd Nazri Ismail, Abdulaziz Aborujilah, Shahrulniza Musa, AAmir Shahzad "New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment", "International Journal of Computer Science and Security (IJCSS)", Volume (6) : Issue (4)
[15] Singh, N.S. Ghera, and P. Chaudhari, "Denial of Service Attack : Analysis of Network Traffic Anomaly using Queuing Theory", 2010
[16] Daneil Botneau, Jose M. Fernandez, John McHugh, John Millins, "Queue Management as a Dos Counter Measure", Volume 4779,2007, pp- 263-280
[17] P. Ferguson, D.Senie, "Network Ingress Filtering: Defeating Denial of Services Attacks which employ IP Source Address Spoofing", RFC Editor, 2000
[18] Upma Goyal, Gayatri Bhatti, and Sandeep Mehmi, "A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model", "International Journal of Application or Innovation in Engineering & Management (IJAIEM)", Volume 2, Issue 3, March 2013
[19] Zhao, S.K. Chen, and W.Zheng, "Defend against Denial of Services Attack with VMM", in Grid and Cooperative Computing, 2009, GCC'09, Eight International Conference on.
[20] Nisha H. Bhandari, "Survey on DDoS Attacks and its Detection & Defence Approaches", "International

Journal of Science and Modern Engineering (IJISME)", Volume-1, Issue-3, February 2013
[21] A.M. Lonea, D.E. Popescu, H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment", "INT J COMPUT COMMUN", February, 2013, pp- 70-78
[22] Christos Douligeris , Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Computer Networks 44 (2004) 643–666
[23] Nathalie Weiler, "Honeypots for Distributed Denial of Service Attacks", Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), IEEE 2002
[24] CERT Cordination Center. CA-1999-17: Denial-of-Service Tools. http://www.cert.org/advisories/ CA-1999-1.html
[25] Ashley Chonka, Yang Xiang n, Wanlei Zhou, Alessio Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks", Journal of Network and Computer Applications 34 (2011)
[26] Matthew L. Bringer, Christopher A. Chelmecki, and Hiroshi Fujinoki, "A Survey: Recent Advances and Future Trends in Honeypot Research", "I. J. Computer Network and Information Security", September 2012 in MECS

Author Profile

Kumar Shridhar is currently enrolled in final year of his B.Tech programme (2011-2015) from Bhagwan Parshuram Institute of Technology. He is a certified objective C programmer and a certified ethical hacker. He is currently working on improving the network security issues. Beside these, he loves watching football and listening music

Nikhil Gautam is currently enrolled in final year of his B.Tech programme (2011-2015) from Bhagwan Parshuram Institute of Technology. He is a certified java programmer. He had developed a number of android apps. Beside these, he loves watching movies and listening songs.