SECURITY ISSUES IN CLOUD COMPUTING: A REVIEW

Toseef Akher Bhutta[1] ,Umar Shoaib and Muhammad Shahzad Sarfraz

[1]tos_bhutta@hotmail.com

[1]Department of Computer Science, University of Gujrat, Pakistan.

[2]umar.shoaib@uog.edu.pk, [3]shahzad.sarfraz@uog.edu.pk

***ABSTRACT*:** *With the urging need of an ever increasing amount of memory and very large number of software and hardware resources to meet the computing needs of customers of enterprises the technique of cloud computing has emerged to provide a platform that promises to meet all such computing needs in a virtual and distributed manner. It provides resources and services as a utility. In this paper we present an overview of this new technology and also discuss some security threats that exist with cloud computing. And finally it gives the solutions to these threats and security issues.*

Key Words: Cloud Computing, Security, Cloud service, cloud utilities, security threads.

I. INTRODUCTION

In the past when technology was newly introduced, the need of memory and storage was very little. In fact, the users of early computers thought that only a few kilobytes of memory was enough for any computer user. But, as the advancements in IT field progressed and the size of Internet users rapidly began to grow, the enterprises had to offer to their online customers more storage capacities and software and hardware resources.

The earlier approach for an organization to satisfy the massive growing amount of customers in order to provide them with their online services was simply by increasing the amount of hardware like servers to boost the storage capacity. But this is very inefficient and an error prone approach. Moreover, the software, the entire team of technical persons, the upgrades needed to run and maintain the huge amount of hardware results in increased costs.

A newly emerged technology is called cloud computing. It is new way of computing in which resources that are dynamically scalable, virtualized are provided via Internet as services. It tends to resolve the problems with traditional approaches.

National Institute of Standards and Technology has defined this technology (cloud computing) as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. applications, networks and storage, etc) that can be quickly provided and released with minimal management effort or service provider interaction [1].

The basic concept is that it is a utility or a service which is provided as per its use just like electricity and gas, etc [2]. So in the same way others utilities are used, cloud computing is used by organizations to provide services to their customers and therefore paying for this utility.

Another important concept in cloud computing is the scalability. An organization can control the size and number of customers to be given the services easily. Cloud computing can be thought of as an infinite number of virtual, distributed and sharable resources [4] to be used from pool in order to satisfy customer needs [3].

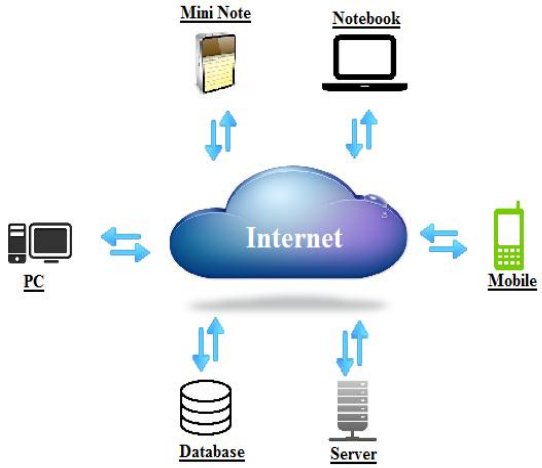

Fig. 1 A scenario of Cloud Computing

This idea of distributed computing saves costs and staff for maintaining a large size of hardware resources. In this manner, there is absolutely no need to worry about any hardware failure and the organization can pay more attention to customers rather than hardware resources.

II. TYPES OF CLOUD COMPUTING

There are four cloud deployment models:

A. Public Cloud:

A public cloud also known as an external cloud is available to the cloud customers in general or general public. It is the leading implementation model. Customers can be individuals or companies accessing cloud services on Internet through a third party service provider who owns a public cloud. Main concern in this type is about the safety of consumers. Examples of providers are public cloud services, Google App Engine, Amazon AWS and Microsoft.

B. Private Cloud:

Private cloud also known as an internal cloud is actually used in one organization; it goes behind the firewall and is managed by the organization or some third party service provider. Organizations primarily use private cloud for their data privacy and maximize their existing resources. It

is also used for research and teaching. Private clouds are mostly used by large organizations or government agencies.

C. Hybrid Cloud:

It is combination of both public and private clouds that remain separate, linked by standards [5]. Using this, a company can keep their critical data behind their firewall and less critical data available to the public. Standardization and interoperability are the main problems in hybrid clouds.

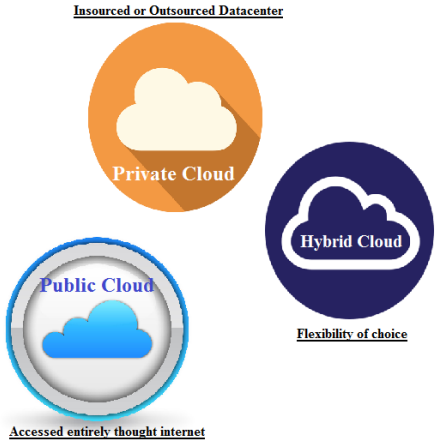

Fig. 2 Types of Cloud Computing

D. Community Cloud:

In this type of cloud several organizations with similar needs share their cloud infrastructure thus sharing the cost. A hybrid cloud can be hosted by one of the common organizations or a third party.

III. LAYERS OF CLOUD COMPUTING

In layered model the entire environment of cloud computing is divided in four layers:

A. Hardware Layer:

Layer material consists of material resources of cloud, including switches, servers, cooling systems, etc. This layer is implemented in the data center service provider cloud, where servers reside. Some of these issues are in the hardware layer, traffic management, hardware configuration, power and cooling management, etc.

B. Infrastructure Layer:

Infrastructure for the virtualization layer uses virtualization techniques such as VMware to create a resource pool of storage or computation.

C. Platform Layer:

It consists of application frameworks and operating systems. Layer platform effectively reduces the load of applications in VM containers.

D. Application Layer:

It is the highest peak in this layer of cloud. The application layer consists of concrete applications in order to run in the cloud. The cloud applications to improve performance and reduce costs.

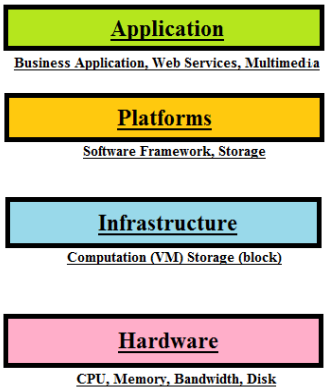

Fig. 3 Layers of Cloud Computing

The cloud layers are similar to the concept of layers in the OSI model. Modularity in layers of cloud computing reduces maintenance [6].

IV. TYPES OF CLOUD SERVICES

There are three main types of cloud services. These services allow users to run applications and store data online. But each service provides a level of flexibility and control of another user:

A. Software as a Service (SaaS):

It allows users to run applications existing online. In this service, a platform of common applications such as databases and resources, etc. is provided to multiple users [7]. Users can easily access services though the Internet from any device. It facilitates collaborative work. It is also called in the software application. Some examples are SalesForce.com, IBM, Google Docs, etc.

B. Platform as a Service (PaaS):

It allows users to create their own cloud applications using specific tools suppliers and programming languages such as API. Users can create and run their own applications on the cloud without the cost of purchasing and managing software and hardware. Some examples are, Microsoft Azure, Google App Engine, etc.

C. Infrastructure as a Service (IaaS):

It allows the users to run applications they want on hardware of their choice of cloud infrastructure. Virtualization technology is mainly used in IaaS to bring the physical resources in an ad hoc environment [5]. It comes in four categories according to the types of servers involved, the private cloud, dedicated, and hybrid cloud hosting. Some examples are, Amazon EC2, Rockspace Hosting, etc.

V. VIRTUALIZATION

Virtualization is the abstraction of lower-level functions and covering materials [8]. This useful technique is mainly used in cloud computing. Without virtualization can be no cloud. It balances the load between data centers. Nowadays, this concept is being applied to all aspects of computing such as networking, storage, software, memory, etc. The idea of

virtualization in cloud computing, it is easy for an organization to satisfy their customers without the need managing material resources. They can simply use virtual resources through a service by a service provider. The concept of migration of a virtual machine migration process evolved. This is the period of unavailability of a few tens of milliseconds to approximately one second. Migrating a complete operating with all its applications as a single unit system clears most of the problems encountered in the technical process migration [11].

This virtualization technique, it is possible for consumers to use these resources without knowing or feeling be virtual or remotely located.

VI. CLOUD SECURITY ISSUES

The success of all new computing technology is based on how it is sure of its use for consumers of this technology [9]. The same question we need in the cloud. Although suppliers of cloud services to ensure and maintain that their services and data stored in the cloud, it's even better and safer than the data in personal computers and secure from theft, etc. But there are examples in the past where cloud services were invaded and down for many hours. So we need to find the real reason behind these security issues such as the invasion, theft, etc.

The public cloud is more vulnerable than the private cloud because, in the case of public cloud, it has a multi-tenant environment. With the rise in the number of users security issues are increased and it becomes more vulnerable. Places that are more prone to threats must be identified.

Due to all these security issues the adoption of private cloud as a solution becomes safer [10].

VII. THREATS IN CLOUD COMPUTING

Some of threats to cloud computing security are discussed here:

A. Denial of Service Attacks:

These attacks are designed for preventing users from a cloud service to be able to access their applications and data. Therefore it forces that cloud service to use too much amount of resources that are limited like CPU power, disk space, network's bandwidth and memory. A denial of service, it's like being caught in the rush hour traffic impasse, there is no way to get to your destination, and you cannot do anything about it, save where sit and wait. Application-level DoS attacks asymmetric because of vulnerabilities in web servers, databases, or other cloud resources, enabling a malicious person to make some application by using extremely very little size of payload of attack commonly, less than 100 bytes long [15].

A Denial of Service attack [10] is an attempt to make it unable for authorized users to use the services. In this attack, the server that proves services is affected by the attack and it becomes busy with a huge number of requests and in this way the service will become unavailable to authorized users. It is experienced that when we sometimes try to access a certain website, then due to overloading the server with requests for access to that website, we become unable to access the website and watch a mistake. This occurs when the number of requests that can be processed by a server are beyond the seating capacity of that server. Incidence of a DoS attack increases the bandwidth consumption as well as causing congestion, resulting in inaccessible to users of some parts of clouds. The use of intrusion detection system or IDS is most popular way to defend against such attacks [12].

A federation of defense is used [13] to guard against the denial of service attacks. Every cloud is loaded with IDS separated. Different IDS systems function on foundation of information exchange. In cases where a particular cloud is under attack, cooperative IDS alert the entire system. A decision on the reliability of cloud is taken by vote, and overall system performance is not hindered. Symptoms of a DoS attack are, the speed of the system is decreased and the applications run very slowly [10].

B. Ping Flood Attacks:

This is a type of attack in which a broadband connection is attacked to flood a network with packets to stop or slow down the authorized traffic through network. The Ping Flood is to send through a network a continuous series of ping or ICMP echo request packets to some target host, that is responded with ICMP echo replies. A continuation of requests, responses can slow network effecting authorized traffic to use the service at a substantially decreased rate, or even, in severe cases, to disconnect. This type of attack can disable the network [21] connectivity.

This attack is mere denial of service in which the one who attacks, overwhelms victim ICMP ping or echo request packets. It's most effective using the option to ping flood that sends these packets as fast as possible, not waiting for the answers. In most cases, the user must be restricted to clarify the option of flooding. This becomes more achievable when attacker has more bandwidth than victim. In this way attacker thinks, victim will respond with ICMP Echo reply packets, consuming both the outgoing and the incoming bandwidth. When the system which is targeted is much slower, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown [22]. The flood ping may also be used as diagnostics for the packet loss also network flow problems [23]. Flooding attack could allow network easily. Flooding attack lose bandwidth and resources leading to additional cost. In this type of attack, attackers can send very large amounts of packets of information resources exploited, and they are known as zombie [24].

The packets may be either one of TCP, UDP, ICMP, or a combination of these protocols. These types of attacks are usually carried out on unauthorized network connections. Due to the nature of cloud computing paradigms, connections to virtual machines are based on the Internet. DDoS attacks affect the availability of serviced land for authorized users.

C. IP Spoofing:

In this type of attack, the attacker spoofs packets of users from reliable sources. Therefore, attacker takes control of system or data itself presenting confidential client. These attacks may be verified by encryption technologies and user authentication on the key exchange. IPSec like techniques help to mitigate risk of identity theft. The filtering incoming and outgoing spoofing attacks can be decreased by enabling encryption sessions and perform ingress [10].

D. Google Hacking:

The Google search engine has become our best choice to find information about something on the network. It's piracy means to use Google for looking up insightful information to use it for his advantage through hacking user account.

Usually, hacker's trying to figure out security gaps check it out on Google for system they want to hack. After collecting required information, they start to hack the desired system. In some cases hacker is in doubt about target. As an alternative he Google out the goal based on security gaps of the desired system. Hacker then looking for all the possible systems with such security gaps that he wants to hack. When Johnny Long initially started collecting attractive queries in Google search, he exposed vulnerabilities, later on those were structured into Google Hacking Database. In a recent case it is found that a group of hackers in China stole login information of several g-mail users. These are few defense bullying that can launch at application level and cause a system downtime, making it inaccessible even to the officials [10].

E. CAPCHA Breaking:

Completely Automated Public Turing test to tell Computers and Humans Apart or just CAPTCHA has been developed to prevent computers or bots from using resources on the Internet. Generally, CAPCHAs are used for preventing overexploitation or spam. By using an automated program, dictionary attacks and registration of multiple websites, etc are prevented by using CAPTCHA.

But even these CAPCHA by Hotmail and G-mail have been broken by hackers recently. These hackers firstly use the audio provided by the services like Hotmail, etc for disabled users and then transform speech to text through converters and therefore break it. In another case, it is found that the Internet users were motivated for solving CAPCHA and thus CAPCHA breaking took place.

F. Sniffer Attacks:

These type of attacks are launched from programs that can capture packets from the network and the data can be read and chances exist that essential information may be traced flowing across network if it is being transferred through those packets isn't encrypted. The sniffer program, through NIC card ensures that traffic or data linked to other systems on network also gets recorded. The NIC by placing on promiscuous mode, it can be achieved. In this mode it can track all data, flowing on same network.

Based on ARP and RTT, a platform of malicious sniffing detection can be used for detecting on a network some sniffing system.

G. Hidden Field Manipulation:

When we are using or browsing a webpage, there are some fields which are not shown and are hidden, they contain information about that page, this is actually used by developers. But, these fields are very vulnerable to any hacker attack because they can be modified easily and posted on the web-page. This can be resulted in severe violations of security [10].

H. Cookie Poisoning:

In cookie poisoning, the cookie contents are changed or modified to make unauthorized access to an webpage or a program. Because cookies have the identity information of user so these cookies can be forged to imitate some authorized user if they can be accessed. This problem can be avoided by implementing encryption for cookies or cleaning regularly these cookies.

I. Debug Options and Backdoor:

Developers commonly enable the debug option when publishing the website. This option makes it possible making developmental changes in code and to implementing these changes in website. Because the debug options assist backend entry to the developers. Often such debug options are left enabled unnoticed, this can provide an easy access for the hacker in website and even make changes inside this website [10].

J. Distributed Denial of Service Attack:

These type of attacks, also superior from the DOS version in terms of the denial of the important services that run on the server by flooding the point of rupture with the countless packets so that the target server is unable to control them. In DOS attack is migrated from different dynamic networks that already at risk DOS reverse. The attackers in this attack can control information flow by allowing some of the information that is available in some cases. So the type and amount of information available to public use is under the control of attacker [14].

The attacker causes a slowing of the intolerable system, leaving all legitimate users of services angry and confused why the service of not responding is. While DDoS attacks tend to generate a lot of fear and media attention (especially when the perpetrators act on the sense of political "hacktivism"), they are not the only form of DoS attack [15].

The Distributed Denial of Service attack is handled by three different units: master, slave and a victim. Master is leading pitcher is at the back all these causing of Distributed Denial of Service attacks; Slave is a network that act as a facilitator for the Master. It provides the stage to control launch the attack on the victims.

That is why it is also called upon to coordinate the attack. Basically, a Distributed Denial of Services attack is prepared in two stages: the first being in stage intrusion where Master is trying to undermine smaller machine hold by flooding the most essential. The next is to install of Distributed Denial of Service tools and attacking the server of the victim or of the machine. Therefore, a DDoS attack results make the service available to authorize similar to how it is done in a DoS attack, but different in how it is run user. A case of this attack has been seen in website of CNN news where the users could not access the website for three plain hours [17]. This method is generally used to fight against this attack is to occupy a significant change in fundamental network. These changes often become expensive for users [16].

Planned cloud logic is to guard against the Distributed Denial of Service attack. This logic provides a transparent transport layer, during which common protocols are used such as HTTP, SMTP, etc., can pass without doubt. The user of the Intrusion Detection System in the fundamental machine is proposed in [18] to keep cloud against Distributed Denial of Services attacks. A mechanism of intrusion detection is SNORT; it is loaded on VM to sniff all traffic, either inbound

or outbound. There is another way generally used for guarding against these attacks has systems intrusion detection on all physical machines that contain VMs for user [19]. This diet has been performing well in Eucalyptus [20] cloud.

Symptoms to a DDoS attack are the speed of the system is decreased and the applications run very slowly, from a great number of users, large the connection requests the fewer available resources. Even if at launch DDoS attacks with full power are very harmful because they deplete the resources of the network, yet careful monitoring network may be helpful in keeping these attacks under control [10].

VIII. INTRUSION DETECTION IN CLOUD COMPUTING

Intrusion detection systems (IDS) are one of the practical solutions to withstand attacks. IDS are systems that perform intrusion detection, virus log information, and warning or perform predefined procedures [15, 16]. They can be either hardware or software that includes computer entities whole observed. This does not mean any suspicious event detected an intrusion. Some unexpected events may occur rarely, and it is crucial to decide if they are an intrusion or not. Primarily, three types of IDS systems cloud computing have: distributed, host-based and network based IDS [27].

A. Host based Intrusion Detection Systems:

It analyze suspicious as system, process or thread asset and configuration access by observing the position of the host call activities. It is mainly used to protect valuable and private information on server systems. HIDSs are able to assign NIDS as if they are installed on a single host and configured to detect network activities. HIDS is composed of sensors on servers or workstations that are made to avoid attacks to a host. A HIDS is not only monitor network traffic; it also tracks and adjusts with more local settings of the OS and the log records [27].

B. Network-based Intrusion Detection Systems:

It observation, monitoring and analysis specified and pre-identified network traffic. It can detect different situations based on specific and usually located between endpoint devices, such as routers, firewalls points. It is a system that tries to find out illegal access to a network by analyzing network traffic for signs of malicious activities and access events. The network traffic on different cell layers and each layer provides data from one layer to another layer. OSI Reference Model and TCP / IP model defines how these layers work and manages traffic [27].

C. Distributed Intrusion Detection Systems:

It is the average IDS in a distributed grid as and cloud computing environment. All components of the distributed area provide each other with agent-based approach. There are three basic elements and duties are similar to other types of IDS components. The main topic in DIDSs treats the entire system as a traditional network or host. DIDS components do not have a global standard, but there are network and host-based sensor components, the detection engine and component management [27].

D. Network Behavior Analysis Intrusion Detection:

Behavior Analysis Network Intrusion Detection (NBAD) is a method that provides intrusion detection decide if the network traffic is suspicious or not the statistical data and the formal status of the network traffic. Sensors detect DoS attacks with the help to be aware of network traffic and application services unexpected and rule violations by scanning the network. NIDS systems and traditional NBAD share some common components such as sensors and management consoles, but NBAD systems generally do not have the server database, unlike the traditional NIDS. NBAD systems work to decide, in the case of unexpected traffic data. It is generally effective in detecting DoS attacks and worms [27].

Many other IDS solutions have emerged to cloud computing as, CBIDS, IDS VM-integrated, etc. Each ID has a supportive agent used to compute and find out whether to accept the alerts sent from other IDS or not. So by doing this, the IDS could avoid the same type of attack occurs [29]. Combination of behavioral approaches and scenarios is the best way to get rid of intrusion.

IX. ADVANTAGES OF IDS FRAMEWORK

- CPU usage, memory, and losing packet would be summarized to advance the overall good organization of IDS cloud.
- For a multi-threaded approach, huge size of data could be handled by a single node ID in a cloud environment.
- The skill detecting attack patterns crosswise a whole shared network, with geographical locations that separate the segments by time zones or continents. By using this for a coordinated and well planned organization in question, an early detection against attack can be made, and to let people to safety ensuring that targeted systems are secure and IP in question are prohibited all the access.
- When detection of Internet worm is enabled earlier, it makes it's way through a corporate network. The attained information thus can then be used for identifying, cleaning systems that are infected by worm to avoid it's spread in network, thus lowering the monetary losses that might had been spent [28].

X. SECURING CLOUD

Providers of cloud services use different techniques to ensure safety against several threats to cloud computing. However, some techniques for detecting these threats are: Avoid the use of vigorously generated SQL in code, determine the meta structures in code, the registered users validate parameters, prohibition of production of useless data, etc.

XI. CONCLUSION

The cloud computing technique has provided so much ease for the enterprises and organizations in providing it with a range of hardware, software resources to meet the needs of customers virtually and in distributed manner without feeling any difference. Cloud computing provides different architectures or types to suit the needs of different customers. These types are private, public, hybrid and community clouds. Although, it has provided too much of ease still it poses threats to the security of the users. Cloud service providers assure their customers that their data on clouds is as secure or even more than their personal computers but there

are evidences in the past when the security of a mass number of users was compromised at different sites. So, there are a large variety of threats in cloud computing. Some of them are mentioned in this paper. Therefore, different service providers use different approaches to detect and remove many types of intrusions and threats to cloud computing. CBIDS and VM-Integrated IDS are examples of such techniques. There are also some standard techniques that are used for detecting several threats.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing - v15," 21. Aug 2009.

[2] A Weiss, "Computing in the clouds" - networker, 2007 - di.ufpe.br

[3] A Goyal and Sara Dadizadeh, "A survey on cloud computing", University of British Columbia, Vancouver.

[4] Michael Armbrust, Armando Fox, "Above the Clouds: A Berkley view of Cloud Computing", UC Berkley, California. February 10, 2009.

[5]Tharum Dillon, Chen Wu, "Cloud Computing: Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[6] Qi Zhang, Lu Cheng, "Cloud computing: state-of-the-art and research challenges", The Brazilian Computer Society 2010, J Internet ServAppl (2010) 1: 7–18.

[7]Bhaskar P. Rimal, Ian Lumb, "A Taxonomy and Survey of Cloud Computing", 2009 Fifth International Joint Conference on INC, IMS and IDC.

[8]Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246 doi:10.2498/cit.1001391.

[9] George V. Hulme, "NIST formalizes cloud computing definition, issues security and privacy guidance", 2011 http://www.csoonline.com/article/661620/nist-formalizes-cloud-computing-definition-issues-security-andprivacy-guidance.

[10] RohitBhadauria, "A Survey on Security Issues in Cloud Computing", School of Electronics and Communications Engineering, Vellore Institute of Technology, Vellore, India.

[11] Clark C, Fraser K, Hand S, Hansen JG, Jul E, Limpach C, Pratt I, "Warfield A (2005) Live migration of virtual machines." In: Proc of NSDI.

[12] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society,vol. 12, issue 4, pp. 38-43, 2010.

[13] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.

[14] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.

[15] "The Notorious Nine Cloud Computing Top Threats in 2013", Cloud Security Alliance.

[16]RuipingLua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

[17] Nathan Mcfeters, "Recent CNN Distributed Denial of Service Attack Explained". http://www.zdnet.com/blog/security/recent-cnn-distributed-denial-of-service-ddos-attack explained/1054.

[18]AmanBakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[19] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," Sixth International Conference on Information Assurance and Security, USA, pp. 265-270, Aug. 23-25, 2010. DOI: 10.1109/ISIAS.2010.5604069.

[20] "Eucalyptus web site" http:// www.eucalyptus.com/ [Eucalyptus is the world's most widely deployed software platform for on-premise (private) Infrastructure-as-a-Service (IaaS) clouds. To date, over 25,000 Eucalyptus clouds have been started up all over the globe including more than 2 out of every 5 Fortune 100 companies.]

[21]"Ping flood attack" http://xforce.iss.net/xforce/xfdb/417.

[22]"Wikipedia" http://en.wikipedia.org/wiki/Ping_flood.

[23] http://www.thejoester.com/projects/nettool/doc/documentation.html.

[24] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol.36, no. 1, pp. 42–57, January 2013.

[25] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94 (SP800-94)," Gaithersburg, February 2007.

[26] G. Tyler, "Information Assurance Tools Report Intrusion Detection Systems," Information Assurance Technology Analysis Center (IATAC), September 2009.

[27] U. Oktay, O.K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing".

[28] Mrs. S. Neelima, Mrs. Y. Lakshmi Prasanna "A review on Distributed Cloud Intrusion Detection System".

[29] Chi-Chun Lo, Chun-Chieh Huang, Ku J, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", Parallel Processing Workshops (ICPPW), 2010 39th International Conference on 13-16 Sept, 2010.