Volume 4, Issue 1, January 2017 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Improved Spoofing Attacks Detection and Prevention Mechanism in Cloud Computing Environment

Mukta Bhatele
Associate Professor
Department of Computer Science & Engineering
Gyan Ganga Institute of Technology & Sciences
Jabalpur (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

Abhiruchi Pillai
M.Tech. Research Scholar
Gyan Ganga Institute of Technology and Science
Jabalpur (M.P.), [INDIA]
Email: abhiruchip@gmail.com

Abstract

Over the internet, the cloud computing reveals a remarkable potential to provide on-demand services to consumers with greater flexibility in a cost effective manner. While moving towards the concept of on-demand service, resource pooling, shifting everything on the distributive environment, security is the major obstacle for this new dreamed vision of computing. Especially some spoofing attacks can break existing security mechanisms. In the research, an advanced detection and prevention mechanism is proposed for spoofing attacks over the virtualization and cloud computing model. The proposed method uses Wireshark, DSNIFF, ETTERCAP and other web service tools for implementation and simulation. Also for preventing the spoofing attacks, improved script is implemented. After implementing and analyzing the proposed concept, results shows better detection and real time prevention of spoofing attacks in virtualization.

Keywords:— *Cloud computing, Virtualization, Attacks, Network Security*

I. Introduction

Using internet and remote server for keeping data and applications is new technology known as cloud computing. Furthermore, users can use applications or services on the clouds through web browsers or web services by utilizing the internet [1]. It offers enormous potential to enhance productivity, decrease costs, dynamic virtualized resources, and distribution of many economic advantages among its adapters [2]. It is remarkable that cloud computing and improves the validity of an organization and maintains competent management support with minimum resources [6]. The latest technology, known as cloud, altered peoples' lives and fortified their employable years via several cloud services. Individual lives are affected by this technology via operations and storage abilities. Currently, many organizations have recognized the emphasis of the cloud for its compliance, operational benefits, and substantial cost savings.

Owing to the nature of a centralized network, susceptible and personal information has become an objective for attack by malicious worm which is one of the most precarious roads for attacking a cloud host. Regarding an attack, the intruder attempts to corrupt a barbed service, application or virtual machine in cloud formation and exhibits itself as a genuine user and hatches its personal barbed service, application or virtual machine, and utilizes the malicious code into the cloud structure [8]. Moreover, depending on signature based antivirus it has ability to detect high accuracy when the signature has been known.

The shortcoming of this type of detection is when the malware morphs its signature completely. Generally, this type of antivirus would fail to detect a novel attack. Cloud computing experiences numerous traditional attacks such as MitM attack, denial of service (DoS) attack, authentication attack, cloud malware injection attack, IP spoofing and distributed denial of service (DDoS). Efficient intrusion detection systems (IDS) must be embedded in cloud framework to alleviate such intrusions.

II. Spoofing Attack

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypasses access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.

1.2.1 IP Address Spoofing Attacks

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false (or "spoofed") source address in order to disguise it. Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses. There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target's IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target's IP address, all responses to the spoofed packets will be sent to (and flood) the target's IP address.

IP spoofing attacks can also be used to bypass IP address-based authentication.

1.2.2 ARP Spoofing Attacks

ARP is short for Address Resolution Protocol, a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker's MAC address with the IP address of a legitimate member of the network. This type of spoofing attack results in data that is intended for the host's IP address getting sent to the attacker instead. Malicious parties commonly use ARP spoofing to steal information, modify data in-transit or stop traffic on a LAN. ARP spoofing attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and man-in-the-middle attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

1.2.3 DNS Server Spoofing Attacks

The Domain Name System (DNS) is a system that associates domain names with IP addresses. Devices that connect to the internet or other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses. In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address. In many cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware. DNS server spoofing attacks are often used to spread computer worms and viruses.

III. Spoofing Attack Prevention and Mitigation

There are many tools and practices that organizations can employ to reduce the threat of spoofing attacks. Common measures that organizations can take for spoofing attack prevention include:

(i) ***Packet filtering:*** Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).

(ii) ***Avoid trust relationships***: Organizations should develop protocols that rely on trust relationships as little as possible. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.

(iii) ***Use spoofing detection software***: There are many programs available that help organizations detect spoofing attacks, particularly ARP spoofing. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.

(iv) ***Use cryptographic network protocols:*** Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.

IV Virtualization Methods

In a traditional environment consisting of physical servers connected by a physical switch, IT organizations can get detailed management information about the traffic that goes between the servers from that switch. Unfortunately, that level of information management does not provide from a virtual switch which has some links from the physical switch that attaches to virtual machines. In addition, the lack of oversight of the traffic flows among the virtual machines on the same physical level affects security abilities and overall performance. Generally, there are several common approaches to virtualization with differences between how each controls the virtual machines. The architecture of these approaches is illustrated in Figure.

A. Operating System-Based Virtualization

In this approach, virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server with the characteristic that all are on the same operating system kernel with exclusive control over the hardware infrastructure. The host operating system can view and has control over the Virtual Machines. This approach is simple, but it has vulnerabilities, such as when an attacker injects controlling scripts into the host operating system that causes all guest OS's to gain control over the host OS on this kernel. The result is that the attacker will have control over all VMs that exist or will be established in the future.

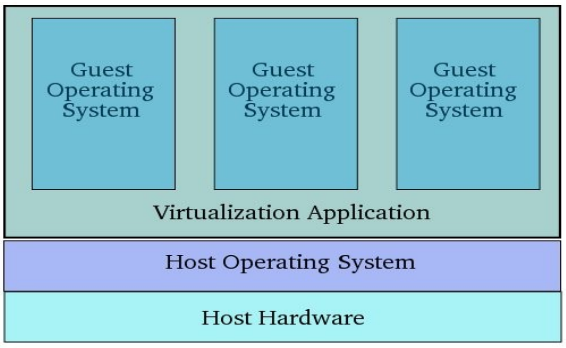


Figure 1: Operating system-based virtualization

B. Application-Based Virtualization

An application-based virtualization is hosted on top of the hosting operating system. This virtualization application then emulates each VM containing its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to Operating system-based.

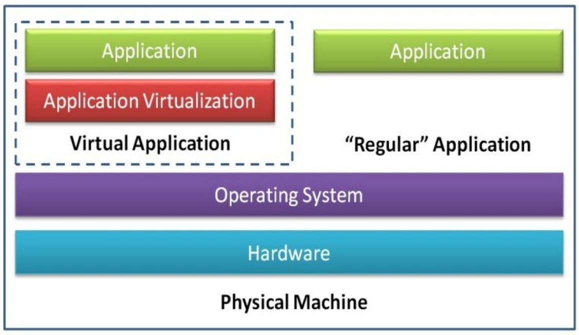


Figure 2: Application-based virtualization

C. Hypervisor-Based Virtualization

The hypervisor is available at the boot time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions that manage the virtualization platform and hosted Virtual Machines. In this architecture, the privileged partitions view and control the Virtual Machines. This approach establishes the most controllable environment and can utilize additional security tools such as intrusion detection systems. However, it is vulnerable because the hypervisor has a single point of failure. If the hypervisor crashes or the attacker gains control over it, then all VMs are under the attacker's control. However, taking control over the hypervisor from the virtual machine level is difficult, though not impossible.

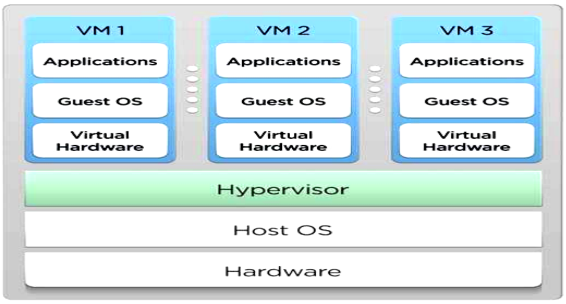


Figure 3: Hypervisor-based virtualization

V. INTRUSION DETECTION AND PREVENTION SYSTEM

An Intrusion Detection System (IDS) is an equipment/programming mix or a mix of both equipment and programming that recognizes the interruptions into a framework or system. IDS supplements a firewall by giving a careful review of both the bundles' header and its substance in this manner ensuring against assaults, which are generally seen by a firewall as apparently kind-hearted system movement. Firewalls take a gander at the control manages; a parcel is either permitted or denied. Types of IDS:

There are two types of IDS:

(i) *Host-based IDS:* Protects the end system or the network resources.

(ii) ***Network-based IDS:*** Monitors network traffic for attacks. A Network IDS is deployed on the network near a firewall, on the DMZ or even inside the trusted internal network.

An Intrusion Prevention System (IPS) is utilized to keep the interruption. It is an expansion of IDS. IDS just identifies though

IPS shields the system from interruption by dropping the parcel, denying passage to the bundle or hindering the association.

Cloud computing is a technology which not only gained advantages from ascendant technologies, but also suffered from its security breaches, of which availability is the most serious security issue. Cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existent in these protocols as well as threats introduced by newer architectures raise many security and privacy concerns. Security of the virtual network is the most significant concern in the cloud platform. So, there is need of security improvement and enhancement of security methods for preventing attacks.

VI. Proposed System

The proposed system is based on intrusion detection and prevention model. This system is based on user's events monitoring process on server system. To implement the system, we are using virtualization software. The client system consists of Windows operating system with Apache Tomcat server with database server and authentication application for IPspoofing. On other side for server system, Ubuntu operating system is used with Hypervisor. Over Ubuntu, Wireshark and Apache server is configured. An application service which is based on php is created. Script.sh is created for Wireshark analysing system. The proposed architecture of system is shown here.

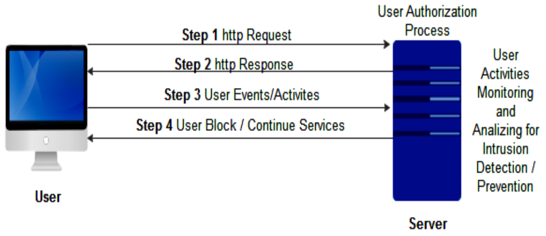

User Authorization Process
Step 1 http Request
Step 2 http Response
Step 3 User Events/Activites
Step 4 User Block / Continue Services
User Activities Monitoring and Analizing for Intrusion Detection / Prevention
User
Server

Figure 4: Proposed Architecture

The working methodology of the system is based on host based analysis, monitoring, detection and prevention mechanism. The server system is based upon Ubuntu system, which includes WireShark and Apache as two main frameworks.

WireShark uses Etercap, Dsniff and attack prevention script in script.sh. Client's activities and events are stored with the help of MySQL database. The Authentication services are used, which is based on PHP. User/Client's activities are recorded, Monitored and analyzed by server system with help of WireShark.

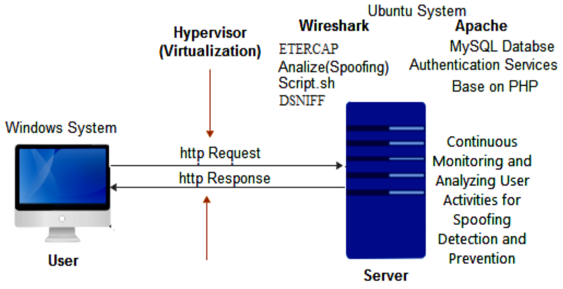


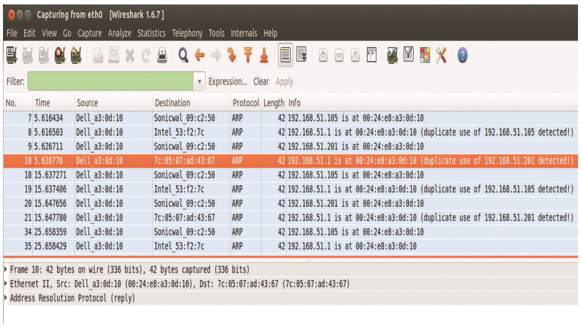
Figure 5: Working Methodology ofProposed Architecture

Analysis of user activities includes the authentication credentials of client system. Real time monitoring of client activities performed by system, activities matched with previous events performed by client system. If there is any mismatch is found, user services are blocked from server at the same time. The mismatch of client's activities shows that the client is not authentic user and tries to attacks on server and makes unauthorized access of data.This system is efficient for detecting and preventing spoofing attacks.

VII. Implementation And Results

The security tools and the techniques described in previous section have been implemented to design and develop secure ARP Spoofing system. In this paper, we assume that the attacker PC captures traffic using Wireshark to check unsolicited IP replies. Once the attack is successful, the traffic between two targets will also be captured. If traffic from the victims PC contains clear text authentication packets, the credentials could be revealed. Wireshark gives information such as 'Duplicate use of IP is detected' under the 'Info' column once the attack is successful. The actual packet travels and is captured after a successful IP poisoning attack.

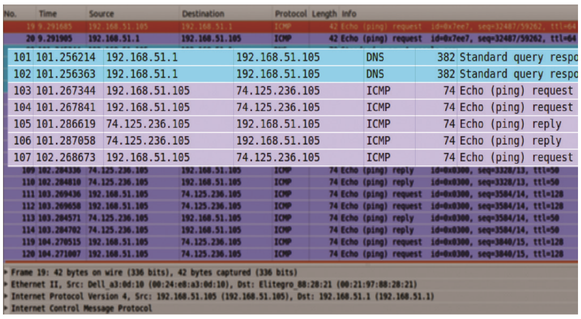
When the packet from the victim PC starts for the router, at Layer 2, the poisoned MAC address of the attacker (instead of the original router MAC) is inserted as the target MAC; thus the packet reaches the attackers PC. The attacker sees this packet and forwards the same to the router with the correct MAC address. The reply from the router is logically sent towards the spoofed destination MAC address of the attackers system (rather than the victims PC). It is captured and forwarded by the attacker to the victims PC. In between, the sniffer software, Wireshark, which is running on the attackers PC, reads this traffic.


Capturing from eth0 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time       Source        Destination        Protocol Length Info
   7 5.616434   Dell_a3:0d:10 Sonicwal_09:c2:50  ARP      42 192.168.51.105 is at 00:24:e8:a3:0d:10
   8 5.616503   Dell_a3:0d:10 Intel_53:f2:7c     ARP      42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!)
   9 5.626711   Dell_a3:0d:10 Sonicwal_09:c2:50  ARP      42 192.168.51.201 is at 00:24:e8:a3:0d:10
  10 5.626776   Dell_a3:0d:10 7c:05:07:ad:43:67  ARP      42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!)
  18 15.637271  Dell_a3:0d:10 Sonicwal_09:c2:50  ARP      42 192.168.51.105 is at 00:24:e8:a3:0d:10
  19 15.637406  Dell_a3:0d:10 Intel_53:f2:7c     ARP      42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!)
  20 15.647656  Dell_a3:0d:10 Sonicwal_09:c2:50  ARP      42 192.168.51.201 is at 00:24:e8:a3:0d:10
  21 15.647780  Dell_a3:0d:10 7c:05:07:ad:43:67  ARP      42 192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!)
  34 25.658359  Dell_a3:0d:10 Sonicwal_09:c2:50  ARP      42 192.168.51.105 is at 00:24:e8:a3:0d:10
  35 25.658429  Dell_a3:0d:10 Intel_53:f2:7c     ARP      42 192.168.51.1 is at 00:24:e8:a3:0d:10

▸ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▸ Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: 7c:05:07:ad:43:67 (7c:05:07:ad:43:67)
▸ Address Resolution Protocol (reply)
```

Figure 6: Wireshark capture on attackers PC ARP Packet



```
No.  Time        Source          Destination     Protocol Length Info
  19 9.291685    192.168.51.105  192.168.51.1    ICMP     42 Echo (ping) request  id=0x7ee7, seq=32487/59262, ttl=64
  20 9.291905    192.168.51.1    192.168.51.105  ICMP     42 Echo (ping) request  id=0x7ee7, seq=32487/59262, ttl=64
 101 101.256214  192.168.51.1    192.168.51.105  DNS     382 Standard query respo
 102 101.256363  192.168.51.1    192.168.51.105  DNS     382 Standard query respo
 103 101.267344  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request
 104 101.267841  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request
 105 101.286619  74.125.236.105  192.168.51.105  ICMP     74 Echo (ping) reply
 106 101.287058  74.125.236.105  192.168.51.105  ICMP     74 Echo (ping) reply
 107 102.268673  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request
 109 102.284336  74.125.236.105  192.168.51.105  ICMP     74 Echo (ping) reply    id=0x0300, seq=3328/13, ttl=50
 110 102.284810  74.125.236.105  192.168.51.105  ICMP     74 Echo (ping) reply    id=0x0300, seq=3328/13, ttl=50
 111 103.269436  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request  id=0x0300, seq=3584/14, ttl=128
 112 103.269658  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request  id=0x0300, seq=3584/14, ttl=128
 113 103.284571  74.125.236.105  192.168.51.105  ICMP     74 Echo (ping) reply    id=0x0300, seq=3584/14, ttl=50
 114 103.284702  74.125.236.105  192.168.51.105  ICMP     74 Echo (ping) reply    id=0x0300, seq=3584/14, ttl=50
 119 104.270515  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request  id=0x0300, seq=3840/15, ttl=128
 120 104.271007  192.168.51.105  74.125.236.105  ICMP     74 Echo (ping) request  id=0x0300, seq=3840/15, ttl=128

▸ Frame 19: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▸ Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: Elitegro_88:28:21 (00:21:97:88:28:21)
▸ Internet Protocol Version 4, Src: 192.168.51.105 (192.168.51.105), Dst: 192.168.51.1 (192.168.51.1)
▸ Internet Control Message Protocol
```

Figure 7: Wireshark capture on attackers PC sniffed packet from Victim PC and Router

Once Wireshark analyze and detects spoofing attacks in the system, it will generate alert to admin to indicate attacks for initiating necessary control over attacks. The admin take necessary action to prevent attacks. An additional functionality is added for prevention mechanism in our system. It will prevent spoofing attacks when it is initiated by admin command.

VIII. Comparisons

Table: 1 Comparisons of Existing and Proposed System

Parameters	**Existing System**	**Proposed System**
ETTERCAP	Not Used	Efficiently Used
DSNIFF	Not Used	Efficiently Used
Number of IP Trace at Single Unit Time	4	7
Main Detection Tools	OpenStack	WireShark
Tool Vulnerability	More Vulnerable (OpenStack)	Less Vulnerable (WireShark)
Efficiency	Less Efficient (Since OpenStack is used)	More Efficient (Since WireShark is used)
Attacking Tool's Dependency	Cain & Abe (Run only Windows System)	ETTERCAP (Can Run on Windows and Linux Systems)
Attack Prevention Mechanism	OpenStack's in-built functionality	New developed Script for prevention in WireShark

IX. Conclusion

Security of the virtual network is the most significant concern in the cloud platform. The use of the virtualization is to isolate all the co-resident VMs under the hypervisor. But there are various kinds of security breaches in the virtualization which violates the isolation between various VMs. This research focused on the ARP attacks in cloud computing and vulnerabilities associated with virtualization in. The technique we propose in this research uses authentication service provided by Wireshark and its attacks analyzing scripts that is included. During Implementation and testing, the proposed system is accurately detects and prevents attacks. So, our proposed system is more secure and efficient for virtualization attacks and their prevention.

Future research will aim to understand the sensitivity of virtualization in the cloud and measures to secure it from attacks. This research may help to strengthen virtualization and reduce the risks of cloud computing from various attacks. In future, automatic prevention mechanism can be implemented in the system, which can detect and prevent spoofing attacks real time, without manual control or command.

X. Acknowledgement

I would like to thank my supervisor for her support and encouragement. I also want to thank my parents and husband, for all their support.

REFERENCES:

[1] Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Muhammad Nawaz Brohi and Rukshanda Kamran, "Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures", Proceedings of 2012 International of Cloud Computing, Technologies, Applications & Management 978-1-4673-4416-6/12/ $ 31.00 © 20121EEE.

[2] N.Ch. Sriman Narayana Iyengar and Gopinath Ganapathy, "A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment", Int. J. Grid and Utility Computing, Vol. 5, No. 4, 201.

[3] Jung-Sook Chang, Yong-HeeJeon, Sohyun Sim and An Na Kang, "Information Security Modeling for the Operation of a Novel Highly Trusted Network in a Virtualization Environment", International Journal of Distributed Sensor Networks Volume 2015, Article ID 359170.

[4] Hyo Sung Kang, Jae Hyeok Son and ChoongSeon Hong, "Defense Technique against Spoofing Attacks using Reliable ARP Table in Cloud Computing Environment", Copyright 2015 IEICE.

[5] Raghav Vadehra, Nitika Chowdhary and Jyoteesh Malhotra, "Impact Evaluation of Distributed Denial of Service Attacks using NS2", International Journal of Security and Its Applications Vol.9, No.8 (2015), pp.303-316, ISSN: 1738-9976 IJSIA.

[6] Li Lu, Zhen Han, Zhi Chen, "Open Stack vulnerability Detection and Analysis", 6th International Conference, ATIS 2015, Beijing, China, November 4-6, 2015, Proceedings, pp 245-251.

[7] Kanika, Navjot Sidhu, "Analysis of Virtualization: Vulnerabilities and Attacks over the Virtualized Cloud Computing", IJETCAS 14-440; © 2014, IJETCAS All Rights Reserved.

[8] Sarfraz Nawaz Brohi, Muhammad Nawaz Brohi, "Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures", Proceedings of 2012 International of Cloud Computing, Technologies, Applications & Management 978-1-4673-4416-6/12/ $ 31.00 © 20121EEE.

[9] Vaishali Singh & S. K. Pandey, "Research In Cloud Security: Problems and Prospects", International Journal of Computer Science Engineering and Information

Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 3, Aug 2013, 305-314 © TJPRC Pvt. Ltd.

[10] Raghav Vadehra, Nitika Chowdhary and Jyoteesh Malhotra, "Impact Evaluation of Distributed Denial of Service Attacks using NS2", International Journal of Security and Its Applications Vol.9, No.8 (2015), pp.303-316.

[11] Saurabh Singh, Young-Sik Jeong, Jong Hyuk Park, "A Survey on Cloud Computing Security: Issues, Threats, and Solutions", Journal of Network and Computer Applications, 1 September 2016, PII: S1084-8045 (16)30199-0.

[12] David Kolevski, Katina Michael, "Cloud Computing Data Breaches - A socio-technical review of literature", 978-1-4673-7910-6/15/$31.00_c 2015 IEEE.

[13] Abid Shahzad, Alan Litchfield, "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable", Australasian Conference on Information Systems 2015, Adelaide, South Australia.

[14] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Elsevier, Journal of Network and Computer Applications 34 (2011) 1–11.

[15] Modi, C., Patel, D., Borisaniya, B., Patel, A. & Rajarajan, M, "A survey on security issues and solutions at different layers of Cloud Computing", The Journal of Supercomputing, 63(2), pp. 561-592. DOI: 10.1007/s11227-012-0831-5-2013.

[16] Ivan Studnia, Eric Alata, Yves Deswarte, Mohamed Ka^aniche, Vincent Nicomette, "Survey of Security Problems in Cloud Computing Virtual Machines", Applications Rendez-vous (C&ESAR 2012). Cloud and security : threat or opportunity, Nov 2012, Rennes, France. p. 61-74, 2012.

[17] M. Durairaj, A. Manimaran, "Study on Securing Cloud Environment from DDoS Attack to Preserve Data Availability", The International Journal of Science & Technoledge (ISSN 2321 – 919X), Vol 3 Issue 2 February, 2015.

[18] Gabriel Cephas Obasuyi, Arif Sari, "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment", Copyright © 2015 by authors and Scientific Research Publishing Inc., 2015, 8, 260-273.

[19] Tanu Shree, Mukesh Kumar, "Towards a Hypervisor Security-based Service and its Research Challenges", International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 17, April 2015.

[20] Rajesh Bose, Debabrata Sarddar, "A Secure Hypervisor-based Technology Create a Secure Cloud Environment", International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-4, Issue-2) February 2015.

[21] Leonardo Richter Bays, "Virtual network security: threats, countermeasures, and challenges", Bays et al. Journal of Internet Services and Applications (2015) 6:1 DOI 10.1186/s13174-014-0015-z.

[22] Josenilson Dias Araújo, “EICIDS-Elastic and Internal Cloud-based Detection System”, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 7, No. 1, April 2015.

[23] Joe-Uzuegbu C, “Application Virtualization Techniques for Malware Forensics in Social Engineering, 2015 International Conference on Cyberspace Governance – Cyberabuja 2015.

* * * * *