A Forensics Approach for Hypervisor

Lokendra Pratap Singh
M.Tech Scholar
Dept. of Computer Science Engineering
The Glocal University
Sharanpur, UP, India

Mukesh Kumar
Asst. Professor
Dept. of computer Science Engineering
The Glocal University
Sharanpur, UP, India

ABSTRACT
Cloud Forensics defines as a post investigation and discussion of the survey results generated by the cyber attacks over Cloud. The exponential growth of the Cloud in private and public Sectors has also increased the Cyber Crimes in the Cloud. Virtualization is the Techniques running at the back of Cloud computing in which virtual machines simultaneously operates and application that controls and managed them is hypervisor. Many models for security of virtualization have been proposed for the protection of resources but still virtualization is being vulnerable to many attacks. Hypervisor forensics is a post approach to investigate and analyze security threats at hypervisor level. In this paper we have proposed an algorithm and implement this framework which will work for maintaining the data log file in terms of attacks graphs.

Keywords
Hypervisor, Virtual Machine , rootkit , Cloud Computing

1. INTRODUCTION
The National Institute of Standards and Technology (NIST) [1] characterizes cloud computing as "...a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Carlton et. al [10] defines that cloud computing is, a combination of existing technologies from technical point of view." Cloud Computing is a collection of virtualized computing resources or virtual machines and the environment is called virtualization. Application layer which acts as an interface between the host physical machine and guest operating system is the hypervisor. A hypervisor or Virtual machine monitor (VMM) or Virtual Machine Manager is defined as the piece of computer software which runs and manages virtual machines. Hypervisor is used to a controls the resource and host processor, allocating what is needed to each operating system in turn and making sure that the guest operating systems(called virtual machines) cannot disrupt each other. Responsibilities of hypervisor is to allocate resources to the guest OS and is done by the set of virtual hardware devices (memory, CPU) whose jobs are then scheduled on the physical hardware. Virtualization can be categorized into many forms based according to the computing architecture layer like Java virtual machine[1] or Dalvik virtual machine[2] come under application virtualization. Another category is operating system virtualization like Virtual Box [2] , Vmware , Xen [4] , Kernel virtual machine[5]. And Full virtualization which Cloud computing strictly follows. Recent survey [3] depicts that number of well known hypervisor brands deployed in data centers are expanding with a multi-Hypervisor strategy becoming the norm. Under this Vmware has a total presence of 81% and 52% of data centre use it as a primary Hypervisor followed by Xen (81% presence, 18% as primary), Kvm (58 % presence, 9% as primary [6,7]). With the rising popularity of virtualization technology, the issue about security and acceptance are also growing [8]. However hypervisor has also unfortunately introduced unfamiliar security threats like kernel level rootkit[7],malware spreading during migration of virtual machines or aid future detection[9]. Cloud Forensics is a derived branch of digital forensics . Cloud forensics involves gathering information from cloud environment for the purpose of investigation. According to National Institute of Standards and Technology (NIST), "Challenges with data replication, location visibility, are somewhat unique to cloud computing forensics" [2]. Ruan et al. [8] defines that cloud forensics is a technical layer between cloud computing and digital forensics which further sub classified as a branch of network forensics. Hypervisor Forensics is a post investigation of attacks at hypervisor level. This paper is divided in two two sections . Section- A specifies the related work in Hypervisor Forensics . Section – B specifies the proposed algorithm and its framework for finding the log evidences of attacks at hypervisor level.

2. RELATED WORK
Cloud Computing has change the method we manage, stores or process the data.[9] . With the migration of servers, Networks over a single platform i.e Cloud performing digital investigation is a vital challenge at this level. As the report by National Institute of Standards and Technology challenges in investigating attacks are classified into 9 parts which are related to [7], architecture, training, data collection, analysis, anti-forensics, incident first responders, role management, legal issues and standards.

Many researchers and research project are in progress who aims to overcome the challenges of Cloud Forensics .An investigator has proposed a Pull model for Hypervisor which traces and investigates the network periodically in a hadoop distributed system and can be used for Forensics analysis. A thread monitoring framework [10] has been proposed for forensic analysis which aims to provide a Virtual Machine Introspection at Hypervisor level. This model works between virtual machines resources and hardware. An effective reference model has been proposed [11] which can perform Forensics Analysis at Cloud Service Provider (CSP) level. Apart from the earlier method an online solution has been proposed which utilizes the Cloud Forensics tool .

Hypervisor Forensics is memory forensics of virtualization environments. The terminology which will be used is virtual machine introspection. Hypervisor forensics is the methodology of post investigation of attack to find the evidence and source of the attack. It comes under Cloud forensics.

Data acquisition and log evidence in Cloud computing environment is differ from the traditional digital forensics methodologies [12] due to its elasticity and scalability of resources. This Paper is design to provide better awareness of hypervisor security and its forensics methodologies with the research gap and challenges. We surveyed the various proposed models of hypervisor security and its forensics

Removes hardware dependency and provides solution to Forensics Experts.[13]. In the field of Log evidences of Cloud Forensics a secure Logging service framework has been proposed [14] in which Cloud Forensics investigator uses an application programming in a secure way to capture crucial log files for the investigation. Irfan M, Abbas H et al [15] proposed a framework in their paper for analyzing challenges of Hypervisor Forenics. A snapshot based approach has been proposed by Rani DR et al[19] which is a Intrusion detection system . This framework identifies the suspicious activity in network over Cloud , it identifies the problem at Hypervisor level and report it to CSP . CSP takes sudden steps by taking snapshot of that virtual machines and isolate it from the Cloud Network. B.Martini et al[16] in their paper proposed a framework for investigation consisting of identification , preservation , collection , examination , analysis ,reporting and presentation. J.Pfoh et al [17] has given some suggestion in his paper to potimize the working of some tools such as Encase, LIBVmi and proposed the method of semantic gap. Lengyel et al[18] perform information analysis in his work so that malware can be identified. He has contributed in a project having automated malware collection and analysis of honeypot system. The CloudSec project [19] focussed on real time monitoring of threats of VM's security at IaaS level. In this physical memory diagnosis in done by Virtual machine Introspection tools. Dollan-Gavitt et al[20] interlinked the hypervisor forensics as Live memory Forensics to improve data acquisition. Dykstra et al[21] suggested to hypothetical concepts examining the evidence collection from a cloud crime. Thorpe et al [22] has mede various efforts of a log auditing tool that address data collection from hypervisor. He has applied this method in his UTECH project for investigation. [4] Penny Pritzker, Willie E. May proposed a NIST Forensic Science Challenges for Cloud Computing. This paper conclude the research done by Group members of NIST Cloud Computing Forensic Science Working then aggregate, categorize and discuss the forensics challenges and difficulties faced by experts on the time to respond to the clients that have been occurred in a ecosystem of cloud-computing.

The challenges are shown with the referenced associated literature. The main goal of the document is to begin an forensic science concerns with dialogue in ecosystem of cloud computing.

The last and long-term aim of this effort is to gain a broad and deep knowledge of those challenges and difficulties to identify technologies as well as standards that can make them less. [3] Rainer Poisel, Erich Malzer, and Simon Tjoa proposed an idea in inspection in Virtual Machine. The digital forensics investigations which can be performed in cloud computing environments is offered by Cloud Computing.

Today digital investigators have many of the Scientific, technical, legal, and business issues, challenges and problems those arose with recent developments in the field of cloud computing. Because of the nature which is dynamic and relevant, to make correct the digital forensic investigations in cloud environments, Cloud computing also appoint several chances.

[24] **Mariano Graziano, Andrea Lanzi, and Davide Balzarotti** proposed a integrated in the Volatility framework to apply all the previous analysis tools on the virtual machine address space which allows forensics analysts. Memory forensics is the branch of computer forensics that aims to extract artifacts from memory snapshots which has been taken from a system which is in a running medium.

3. TYPES OF HYPERVISORS IN CLOUD COMPUTING

There are different types of hypervisors those support different aspects of the cloud. Types of Hypervisors are following as:-

3.1 Native Hypervisors

Native hypervisor [27] defines as the hypervisor, which sit directly on the hardware platform those are most likely used to gain better performance for particular users. Native hypervisors run directly on the host's hardware to control the hardware as well as to manage guest operating systems. For this reason, they are sometimes called BARE METAL hypervisors.

3.2 Embedded Hypervisors

Embedded hypervisor [25] defines as the hypervisor those are integrated into a processor on a separate chip. Use of this type of hypervisor is to gain performance after improvements for a service provider.

3.3 Hosted Hypervisors

Hosted hypervisor [25] defines as the hypervisor run as a distinct software layer above both the hardware and the OS. Use of this type of hypervisor is in private as well as public clouds for gaining performance after improvements. On a conventional operating system Hosted hypervisor can run, like as the other computer programs do.

4. ATTACKS ON HYPERVISOR

The Hypervisor allows users to be isolated from the other ones in a cloud environment even when they are served by same physical resources. Apart from this secure feature there are several attacks which can harm to the hypervisor. As cloud is designed to provide services to all legal users and also it also give services to users that have some malicious purposes. So there are some of the attack at hypervisor level which are as follows.

4.1 Wrapping Attack

This type of attack can be a threat to hypervisor in virtual environment.When a user makes a request to the web browser from his/her virtual machine a message called SOAP(Simple Object Access Protocol) is generated. This attack with the cross site scripting then duplicates the authentic user account and password during login phase so that attacker can affect the SOAP messages that are exchanged during setup time of web browser and web server.

4.2 Data Stealing

Security threats at hypervisor in virtualization system are the data stealing by authorized administrator without leaving the trace of any volume of data. To overcome from this problem login in hypervisor as an administrator create some data replication schemes by applying some policies like RAID and mount the disk image onto the hypervisor and deletes the original copy and lost[26].

4.3 D-Dos Attacks

D-Dos attacks typically works on the flooding of IP packets at specific network for the purpose of damaging the computer system resources. In cloud environment D-Dos attacks has a greater potential to disrupt the cloud infrastructure having the large amount of VM's and its controller called hypervisor. If a hypervisor doesn't provide sufficient resources for its VM's then chances of affecting the system by D-Dos increases. But problem arises when a user inside type D-Dos attack.

5. TYPES OF D DOS ATTACKS

There are following DDOS attacks those can harmful for cloud and detected by Hypervisor Forensic

This attack uses the differences in implementation for resolving overlapping fragment Offsets. The attacker modifies the fragment offset such that when the firewall assembles it, the malicious content gets hidden. However the packet becomes malicious when the victim reassembles it. The attacks are also evaluated in.

5.1 Tear Drop

The attacker exploits the weakness of IP packet reassembly process by purposely sending packets with overlapping fragment offset field.

5.2 Syn Drop

The attacker initiates many half connections with the victim by not completing the three way handshake protocol with ACK packet. The kernel maintains a buffer for such half connections, which eventually overflows causing system crash or D DOS.

5.3 Jolt

The attacker sends very large, fragmented ICMP packets to a target machine. The ICMP packets are fragmented in such a way that the target machine is unable to reassemble them for use.

5.4 Ping of Death

While a single IP packet cannot exceed 65536-bytes, the attacker can make the fragments add up to more than this value. It is usually associated with ICMP, but can contain any protocol.

5.5 Fraggle

The attacker sends a large number of UDP echo (ping) traffic at spoofed source IP address of the victim. UDP echo packets are directed at the Unix UDP services echo (port 7), chargen (port 19), daytime (port13) and qotd (port 17).

5.6 Smurf

The attacker sends many ICMP echo request packets with spoofed source IP address of the victim. All replies to this broadcast are received by the victim, resulting in denial of service.

5.7 Bonk

It is a variant of the teardrop attack and manipulates the fragment offset field in TCP/IP packets. Bonk attack manipulates this number and causes the target machine to reassemble a packet that is much too big to be reassembled and causes the target computer to crash.

5.8 Boink

It is a modified version of the bonk attack, which allows UDP port ranges. It also manipulates the fragment offset field and causes the target computer to crash. NewTear: NewTear attack is simply a modified version of Teardrop which changes padding length and increases the UDP header length field to twice the size of the packet.

6. PROPOSED WORK

6.1 IBM Report 2017 for Cloud Forensics as a big research Challenge up to 2022

The survey highlights the importance of forensic techniques tailored to the Cloud: 81% of respondents agree that forensics in Cloud is hard to implement so various proposed model are invited to make this branch fully establish.

While 76% claim that this area needs more funding and investment than it currently receives. Interestingly, 71% of respondents believe that the general lack of awareness of Cloud security will endure until a major critical incident happens.

This could explain the aforementioned fact that security concerns are not levelled as "critical" by respondents. The results of this question show that the respondents have reached consensus on the significance of Cloud forensics.

We have surveyed the different types of models of services according to the survey report of our Base Paper):-

IAAS: Infrastructure as a Service

PAAS: Platform as a Service

SAAS: Software as a Service.

Our work is to proposed the idea to implement the –

(FAAS)Forensics as a service over cloud

But our proposed work is based on the Network Forensics over Cloud

State of the art Cloud Forensics

In our research, we used a scientific database search engine called Summon a product of Serial Solution (Summon, 2017) which was proposed by Sameera Almulla in her research paper to illustrate the number of attacks(hits) increased in cloud from the year 2006-2017 which was unable to solve in forensics investigation., The Summon solution not only includes a full record of IEEE Explore, Springer, Science Direct and Elsevier but also includes Scopus and Web-of-Science databases.

6.2 Network Forensics

Network Forensic is real-time forensics offered either on basis through software / appliance installation or via the Cloud by capturing the web traffic to the cloud provider. This provides an additional layer of forensic on top of things like IP Traceback to analyze the attacks activities.

6.3 WEB SECURITY

Web Security is real-time protection offered either on basis through software / appliance installation or via the Cloud by proxying or forward web traffic to the cloud provider. This provides an additional layer of protection on top of things like antivirus to prevent malware from entering the enterprise via activities such as web browsing.

- To prevent our cloud environment for security as a service we are using java application tool.
- Benefit of this tool is to save Logfile or Output or Packets for future investigation.

There are of cloud Security as Service that most likely will interest consumers and security professionals are:

- Identity Service and Access Management Service
- Data loss prevention
- Web security
- Email security
- Security Assessments
- Intrusion management, detection and prevention
- Security information and event managements.
- Encryption
- Business continuity and Disaster Recovery
- Network Security.

7. PROPOSED ALGORITHM

7.1 ALGORITHM

The aim of the algorithm is to find the high value of β i.e suspicion value

We require a log file of packet for our algorithm

STEP 1- Start

STEP 2- Input log file

STEP 3- Generating the graph attack

Using Buffer comparison

B1 with tuples-**B1** (**ID1**, **a1**, **E1**, **β1**)

B2 with tuples-**B2** (**ID2**, **a2**, **E2**, **β2**)

if (**B1.ID1**=**B2.ID2**)

B1=**B2**

else

B1=/=**B2**

STEP 4 -Derived Buffer will be $\mathbf{B}_{\beta}(\mathbf{ID}_{\beta}, \mathbf{E}_{\beta}, \boldsymbol{\beta}_{\beta})$

STEP 5- Input $\mathbf{B}_{\beta}$ for the forensics

STEP 6- Input graph attack consisting several network attack

STEP 7-Here we are assuming

B1.ID = **B2.ID**

For a **£** Nodes (**a**) (type of network attack)

Do

if (**B** (**ID, a**))= {**B** £ **B**(**ID**) £ (**a**)}

a **£** node(**a**)

else

a **£** nodes (**a**) = empty

STEP 8-

while true do

For a **£** nodes (**G**) do

if **β**[**a**] = 0

Then

N (**a**) neighbour of a in **G**

$\mathbf{a} = \mathbf{max}_{\mathbf{B}\,£\,\mathbf{N(G)}} * \mathbf{B}_{(\mathbf{ID},\,\mathbf{a},\,\mathbf{E},\,\beta)}$ (occurrence of buffers where it is comaparing the tuples)

B= greater than (Exact match for similarity)
Attacks[**G**]== {where $\mathbf{G}\,£\,\mathbf{B}_{\beta}$ related packets for the Forensics investigation // updated Buffer}

Break;

else

Nothing to do

End while

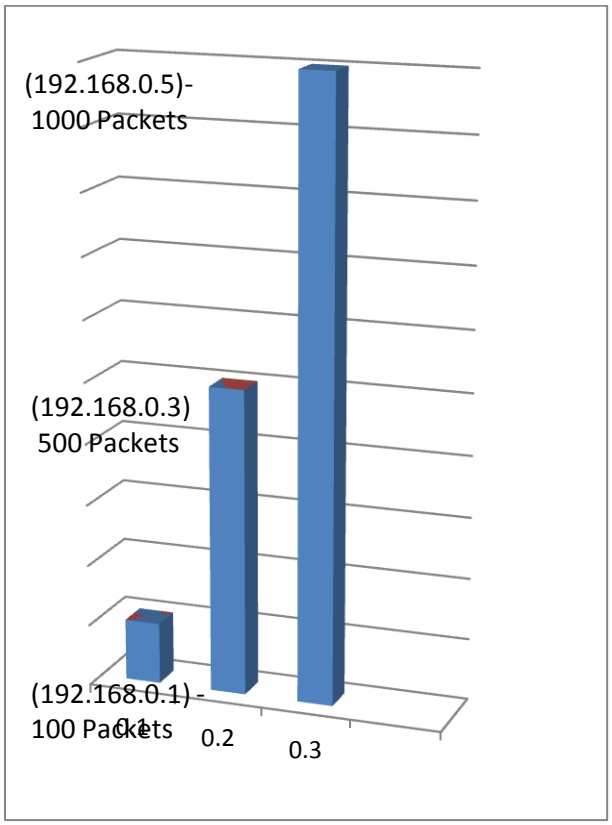
STEP 9- END

Here iteration will follow and algo will compare the network packets from the graph and compare until each of the iteration is not fully compare and we will not achieve the value of B>1. Value of β (suspicion) value will be upgraded then only satisfactory result will be upgraded. Finally Attack [G] graph will be upgraded with co related packets structure.

8. GENERATION OF ATTACKS GRAPH

D. Rane. [21] present an efficient computation engine that generates attack graphs step-by-step and provide an interactive opportunity to trace the attacker's path. He has proposed an idea that Packets Identification ∞ 0.1 times probability of finding the attacker.

So here the Graph generation is



(**Probabilistic graph for finding the attacker)**

9. FEATURES OF GRAPH

1. It is based on the tracing of D-dos attack.
2. In this graph we have shown the Packet sending program
3. Randomly we have send 100, 500, 1000 packets.
4. At last the Probabilistic model graph generate.
5. Number of related packets is directly proportional to 5 times of probability.

10. FUTURE WORK

In Future we should implement all security services which is given by proposed Security model and Security as a Service and make a fully secure service based on need of end user The legal regulation, compliance and investigation domain specifically addressed SLA indistinct responsibilities between providers and customers, the need for incident handling processes, compliance with legal regulations, academic property and privacy, cloud employee monitoring and observation, and the need for cloud experts.

In the future we have main target the security service with Network security and encryption and after that all included security service and make fully combine software of Security as Service as a antivirus means how much you are paying you are getting level of security.

11. REFERENCES

[1] Java virtual machine, (2014), [online]. Available:http://en.wikipedia.org/wiki [Oct,17,2017].Dalvik virtual machine, (2017),[online]. Available: http://en.wikipedia.org/wiki, [Oct, 18, 2014].

[2] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing,"Fröhlich, B. and Plate, J. 2000. Digital Investigation, vol. 9, no. 2, pp. 71–80, November 2016.

[3] Is the Hypervisor Market Expanding or Contracting? http://www.aberdeen.com/Aberdeen-Library/8157/AI-hypervisor-server-virtualization.aspx.National vulnerability database. http://web.nvd.nist.gov/view/vuln/search.

[4] Xen, (2014), [online]. Available: http://www.xenproject.org, [Oct, 21, 2017]

[5] Nexenta Hypervisor Survey. http://www.nexenta.com/corp/nexenta-hypervisor-survey.

[6] J. Levine, J. Grizzard, and H. Owen. Detecting and categorizing kernel-level rootkits to aid future detection. IEEE Security Privacy Magazine, 4(1):24 {32, January{ February 2013}

[7] National Institute of Standards and Technology,(2014), [online] Available: http://en.wikipdeia.org/wiki, [Oct,20,2014]

[8] Ruan ,P. Jain, D. Rane, and S. Patidar, "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment," in Information and Communication Technologies (WICT), 2011 World Congress on, pp. 456-461.

[9] Acquiring forensic evidence from infrastructure-as-a-service cloud, Josiah Dykstra, Alan T. Sherman; Digital Investigation 9 (2015) S90–S98;Elsevier Ltd doi:10.1016/j.diin.2012.05.001

[10] Jackson C, Agrawal R, Walker J, Grosky W Scenariobased design for a cloud forensics portal. IEEE International Symposium Technologies for Homeland Security (HST) 2015; 1-6. DOI 10.1109/THS.2015.7225260.

[11] Meera G, Kumar Raju Alluri BKSP, Powar D, Geethakumari G. A strategy for enabling forensic investigation in cloud IaaS. IEEE International Conference Electrical, Computer and Communication Technologies (ICECCT) 2015; 1-5. DOI 10.1109/ICECCT.2015.7226103

[12] Splunk. Available from: http://www.splunk.com/. Retrieved on Jan 10, 2016.

[13] Abbas H, Mahmoodzadeh QM, Khan FA, Pasha M. Identifying an OpenID anti-phishing scheme for cyberspace. Security and Communication Networks 2016; 9(6):481–491

[14] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, and J. Molina, "Controlling Data in the Cloud:Outsourcing Computation without Outsourcing Control," in Proc. of the 2013 ACM Workshop on Cloud Computing Security (CCSW'09), Chicago, Illinois, USA. ACM, November 2009, pp. 85–90.

[15] Jackson C, Agrawal R, Walker J, Grosky W. Scenariobased design for a cloud forensics portal. IEEE International Symposium Technologies for Homeland Security (HST) 2015; 1-6. DOI 10.1109/THS.2015.7225260.

[16] G. Grispos, T. Storer, and W. B. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics," International Journal of Digital Crime and Forensics (IJDCF), vol. 4, no. 2, pp. 28–48, March 2012.

[17] J. Pfoh, C. Schneider, and C. Eckert, "A formal model for virtual machine introspection," in Proc. of the 1st ACM Workshop on Virtual Machine Security (VMSec'09), Illinois, USA. ACM, November 2009, pp. 1–10.

[18] T. Lengyel, J. Neumann, S. Maresca, B. Payne, and A. Kiayias, "Virtual machine introspection in a hybridhoneypot architecture," in the 5th USENIX conference on Cyber Security Experimentation and Test (CSET'12), Washington, USA, August 2012.

[19] A. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, "CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model," in Proc. of the 5th International Conference on Network and System Security (NSS'11), Milan, Italy. IEEE, September 2011, pp. 113 –120.

[20] B. Dolan-Gavitt, T. Leek, M. Zhivich, J. Giffin, and W. Lee, "Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection," in Proc. of the 2011 IEEE Symposium on Security and Privacy (SP'11), Oakland, California, USA. IEEE, May 2011, pp. 297–312.

[21] D Rane J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," in Proc. of the 12th Annual Digital Forensics Research Conference (DFRWS'12),

Washington, DC, USA, Digital Investigation, vol. 9, August 2012, pp.90–98.

[22] Sun Y, Jara A. An extensible and active semantic model of information organizing for the Internet of things. Personal and Ubiquitous Computing, 2017; 18(8): 1821-1833. DOI:10.1007/s00779-014-0786-z.

[23] Linux,(2014), "KVM 4.2 ", [online]. Available: http://www.linux-kvm.org, [Oct, 15, 2016]

[24] Is the Hypervisor Market Expanding or Contracting? http://www.aberdeen.com/Aberdeen-Library/8157/AI-hypervisor-server-virtualization.aspx.National vulnerabilitydatabase.http://web.nvd.nist.gov/view/vuln/search

[25] Lalit Mohan Joshi and Dr. Rajendra Bharti " A Survey of Hypervisor Forensic in Cloud Computing" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS050822 www.ijert.org Vol. 4 Issue 05, May-2015

[26] Lalit Mohan Joshi, Dr. Rajendra Bharti, Mukesh Kumar" Understanding Threats in Hypervisor, its Forensics Mechanism and its Research Challenges" International Journal of Computer Applications (0975 – 8887) Volume 119 – N