iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Integration of Virtual Machine with Cloud

Nimish Aggarwal[1], Deepanshu Garg[2], Diksha Nagpal[3]
[1, 2, 3]*Chandigarh University*

I. INTRODUCTION

Cloud computing has recently emerged as a technology to allow users to access infrastructure, storage, software and deployment environment based on a pay-for-what-they-use model. Criminal use of cloud computing is an impending possibility as cloud becomes omnipresent. Likewise, the need for digital forensic analysis of cloud computing environment and applications has become customary. So for this it is necessary, digital forensics in the cloud environment comprises of stages: Identification, Collection, Examination/ Analysis and Reporting/ Presentation.VMM or a Virtual Machine running under the VMM analyzes the attacked VM when attack is identified. This technique is called VMI Malicious events can be identified by performing VMI which is the technique of examining a running VM from either another VM not under examination or from the hypervisor. Poisel et al proposed hypervisor forensics and presents the possibility of acquiring evidence from hypervisors to perform digital forensics. Virtual Machine Introspection is suggested as the most practical approach to identify the malicious VM. If the intrusion detection system resides on the host, it may be susceptible to attack and if intrusion detection system resides in the network it is more resistant to attack. A virtual machine introspection based approach to intrusion detection is proposed where the Intrusion Detection System is outside the host for good attack resistance.

II. TERMS AND TERMONOLOGIES

A. *What is virtual machine?*

In computing, a virtual machine (VM[1]) is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination. They provide functionality needed to execute entire operating systems. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine.

B. *Virtual Machine Introspection*

Virtual Machine Monitor (VMM) is running under the VMM analyzes the attacked VM when attack is identified. This technique is called Virtual Machine Introspection(VMI).A virtual machine introspection based approach to intrusion detection is proposed where the intrusion detection system is outside the host for good attack resistance.

C. *What are Virtual Machine Snapshots?*

Virtual machine snapshots are file-based snapshots of the state, disk data, and configuration of a virtual machine at a specific point in time. You can take multiple snapshots of a virtual machine, even while it is running. You can then revert the virtual machine to any of the previous states by applying a snapshot to the virtual machine. To take a snapshot, you can use either Hyper-V Manager or Virtual Machine Connection. All of the other tasks you can perform with snapshots, such as applying or deleting a snapshot, or viewing a list of all snapshots for a specific virtual machine, are available through Hyper-V Manager. You also can inspect or edit the .avhd files, as well as determine which snapshot an. avhd file is associated with.

III. VM IN CLOUD COMPUTING

Cloud computing has recently emerged as a technology to allow users to assess infrastructure, storage, software and deployment environment based on for what they use models. As criminal use of cloud computing is an impending possibility as cloud become omnipresent. Likewise there are more cases regarding the security, for this need is to protect them which can be done by the process of VM Snapshots.

A. *Features of snapshots*

The snapshot feature is most useful when you want to preserve the state of the virtual machine so you can return to the same state repeatedly. To simply save the current state of your virtual machine, then pick up work later with the virtual machine in the same state it was when you stopped, suspend the virtual machine. For details, see Using Suspend and Resume. You can take a snapshot of a virtual machine at any time and revert to that snapshot at any time. You can take a snapshot while a virtual machine is powered on, powered off or suspended. A snapshot preserves the virtual machine just as it was when you took the snapshot - the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended.

IV. PROPOSED MODEL

CSP[2] provide various types of services to users, few users from specific organization frequently use the same kind of service based on pay-per-what-they-use and some providers provide free trial period with unlimited bandwidth and storage capacity which gives users an opportunity to perform malicious activities. Malicious users can steal the sensitive and confidential information from cloud users which in turn affect the trust of the CSP. Cloud necessitates protection from these malicious activities and CSP should have a provision to use either introspection to monitor customer VMs and detect malicious activity.Users can create VM of their choice from the available physical machines. In spite of users request, any cloud software like eucalyptus, Open Stack generates snapshots of a running VM continuously and stores it till the VM terminates. Maximum number of snapshots can be saved for a specific VM allotted; if maximum is reached older once are deleted. Snapshots can decrease the performance of a virtual machine based on how long the snapshot is stored and how much it changed from the time previous snapshot is taken.

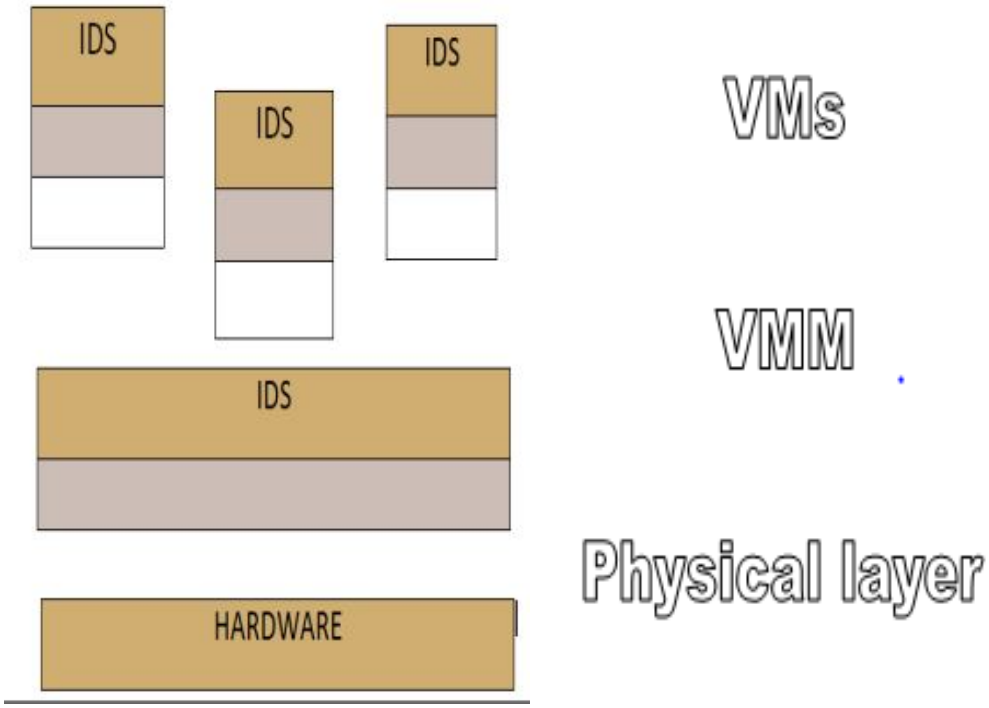


Fig.1 Incorporating IDS at VMs and VMM

Malicious activities are identified when users of that VM perform any activity like excessive access from location, upload malware to a number of systems in the cloud infrastructure, intense number of downloads and uploads in a short period of time, launch dynamic attack points, cracking passwords, decoding / building web tables or rainbow tables, corruption or deletion of sensitive data, malicious data hosing, altering data, executing botnet commands. Our proposed model incorporates IDS[3] on VMs which allows it to monitor itself and on VMM to detect malicious activity between VMs. It shows that IDS are incorporated in all the VMs and VMM for monitoring malicious activities. Deploying, managing and monitoring the Intrusion Detection Systemis done by cloud service provider.

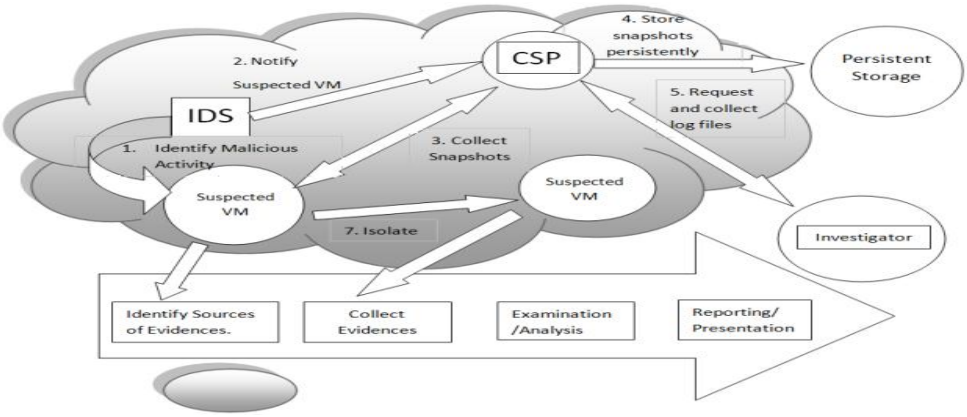


Fig.2 Proposed approach to perform digital forensics using VM snapshots

The idea of the proposed model is that the CSP stores snapshots of a VM whose activities are identified as malicious by an intrusion detection system. Simultaneously the CSP should be requested for log files of the suspected VM and the investigator collects and processes the log files to obtain the evidence. To collect proper and correct evidence, the suspected VM should be monitored for some more time after it is identified to be performing malicious activities. The more time the suspected VM is monitored the more it can be sure of the possibility of malicious behavior.

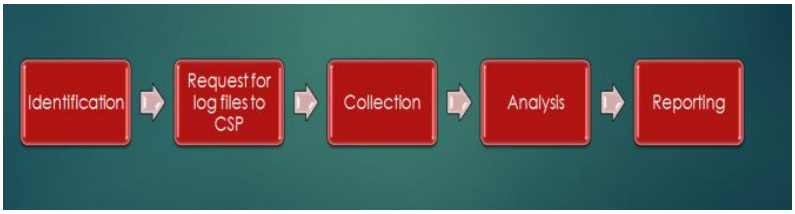


Fig.3 Flowchart for proposed model

Once the investigator identifies the sources of evidence, the suspicious VM is moved to other nodes to preserve confidentiality, integrity and authenticity of other VMs. By moving or isolating, VM evidence can be protected from contamination and tampering. Delport et al introduced new techniques to isolate VM instances on cloud to be investigated. After isolating the suspected VM, the investigators can collect the evidence. Later the evidence can be analyzed using forensic tools and presented it to court of law. So don't worry, you have VM with you to help you. A person can delete everything but not VM- Snapshots.

V. ADVANTAGES &DISADVANTAGES OF SNAPSHOTS

A. Advantages of Snapshots

Taking a snapshot reduces the performance of the virtual machine while the snapshot is created. You should not use these snapshots on virtual machines that provide services in a production environment.

We do not recommend using snapshots on virtual machines that are configured with fixed virtual hard disks because they reduce the performance benefits that are otherwise gained by using fixed virtual hard disks.

Snapshots require adequate storage space. Snapshots are stored asavhd files in the same location at the virtual hard disk. Taking multiple snapshots can quickly consume a large amount of storage space. When you use Hyper-V Manager to delete a snapshot, the snapshot is removed from the snapshot tree but the avhd file is not deleted until you turn off the virtual machine.

B. Disadvantages of VM snapshots

Taking a snapshot reduces the performance of the virtual machine while the snapshot is created. You should not use these snapshots on virtual machines that provide services in a production environment.We do not recommend using snapshots on virtual machines that are configured with fixed virtual hard disks because they reduce the performance benefits that are otherwise gained by using fixed virtual hard disks.

Snapshots require adequate storage space. Snapshots are stored as avhd files in the same location at the virtual hard disk. Taking multiple snapshots can quickly consume a large amount of storage space. When you use Hyper-V Manager to delete a snapshot, the snapshot is removed from the snapshot tree but the .avhd file is not deleted until you turn off the virtual machine.

VI. REVIEW LITERATURE SURVEY

A. Vmware VSphere

The power of virtualization provided by VMware vSphere helps to transform datacenters into simplified cloud computing infrastructures using which flexibility as well as reliability in IT services can be provided by IT organizations. VMware vSphere virtualizes and helps to utilize the underlying physical hardware resources across multiple systems and provides plethora of virtual resources to the datacenter .The vSphere Client is used for the configuration of the host and to manage and operate its virtual machines. The beauty is that it can be downloaded from any host. As a cloud based operating system, a large collections of infrastructure (such as RAM, processor, disk, and networking) as a seamless and dynamic operating environment is managed by VMware vSphere, also it manages the complexity of a datacenter.

B. Vmware Vcenter Server

A centralized management hub to monitor the datacenters is provided by VMware vCenter Server. The aggregated physical resources from multiple ESX/ESXi hosts is presented as central inventory of simple and dynamic resources by the vCenter Server to the system administrator which in turn are allocated to virtual machines in a virtual environment. A central place of management of virtual infrastructure is provided by vCenter Server. Using it, IT administrators are ensure security, reliability, scalability, simplified daily tasks, availability of usually unutilized resources and reduced complexity of managing virtual infrastructure. The various vCenter Server components are user access control, central core services, distributed services, plug-ins, and various interfaces. Using the User Access Control Component, the system administrator can manage and configure different level access permission on vCenter Server to varied classes of users.

C. Esxi hypervisor

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

VMware ESXi provides the foundation for building a reliable, secure and dynamic IT infrastructure. VMware ESXi hypervisors are operating systems using which the resources such as processor, ram, storage, and networking on a server can be allocated to multiple virtual machines that can run unmodified operating systems and applications.

VMware ESXi are the most widely deployed hypervisors on servers, which delivers the highest levels of reliable, secure and optimum performance to companies of all sizes. The latest hypervisor architecture from VMware is VMware ESXi. It has an ultra thin architecture with no reliance on a general purpose OS, yet still offers all the same functionality and performance of VMware ESX.It provides a new scale of security and reliability because its coded base is smaller in size that represents a comparatively smaller surface to attack with lesser code to patch. This functionality of small footprint and hardware-like reliability enables VMware ESXi to be built directly into industry standard x86 servers from leading server manufacturers such as Dell, IBM, HP, and Fujitsu-Siemens. The system configurations of VMware makes it the easiest way to get started with VMware virtualization.

D. Virtualization

Virtualization is a core technology in increasing the efficiency of IT investments and has been increasing in various fields such as servers, storage, network, and software throughout the world. The virtualization can be defined as a technology that makes it possible to efficiently use resources by integrating systems in a logical manner or separating a system in a logical manner.

VII. THREATS TO EXISTING HYPER-V SNAPSHOT MECHANISMS

A typical virtualization infrastructure includes a hypervisor, multiple guest VMs, and a privileged management VM, such as the root VM or dom0. The current virtualization architecture supported by Hyper-V, Xen, and VMware ESX server allows the snapshot Service to operate from the privileged management VM. As shown in Figure 1, the rootVM in Hyper-V takes a guest VM's snapshot with only minimal support from the hy-pervisor. More specifically, the root VM only relies on the hypervisor to protect guest memory pages from writes performed by the target guest VM being snap shotted. These writes trigger the root VM's copy-on-write (CoW) mechanism, where the root VM handles faults (using a fault handler), copies the content of the page (using copy-on-fault)before removing the protection, and resumes the guest VM's execution. Concurrently, the snapshot application also copies other guest memory pages. After completion ofthe snapshot, the snapshot file is stored in the root VM and CoW protection on guest memory pages is removed. We evaluated the security of the existing Microsoft Hyper-V snapshot mechanism in a cloud environment under the threat model described above. We developed a concrete tampering attack on a customer's snapshot file by

removing from it evidence of malware infection and other important information that a malicious administrator may want to hide from a customer. To launch the attack, we utilized a forensic analysis utility called Volatility to extract information such as the list of running processes, loaded drivers, opened files, and connections. We first opened the snapshot file in analysis mode and listed all running processes, and we then chose a process from the list to remove—in a real threat scenario, this could be malware. Next, we used Volatility to alter the list of running processes by rewriting the linked list used by Windows to store all running processes. We repeated this experiment to remove a loaded driver from the list of drivers. These malicious modifications will not be detected by the consumers of this snapshot due to the lack of any measurable trust associated with the generated snapshot.

VIII. UNRECOVERABLE VIRTUAL MACHINE IMAGES

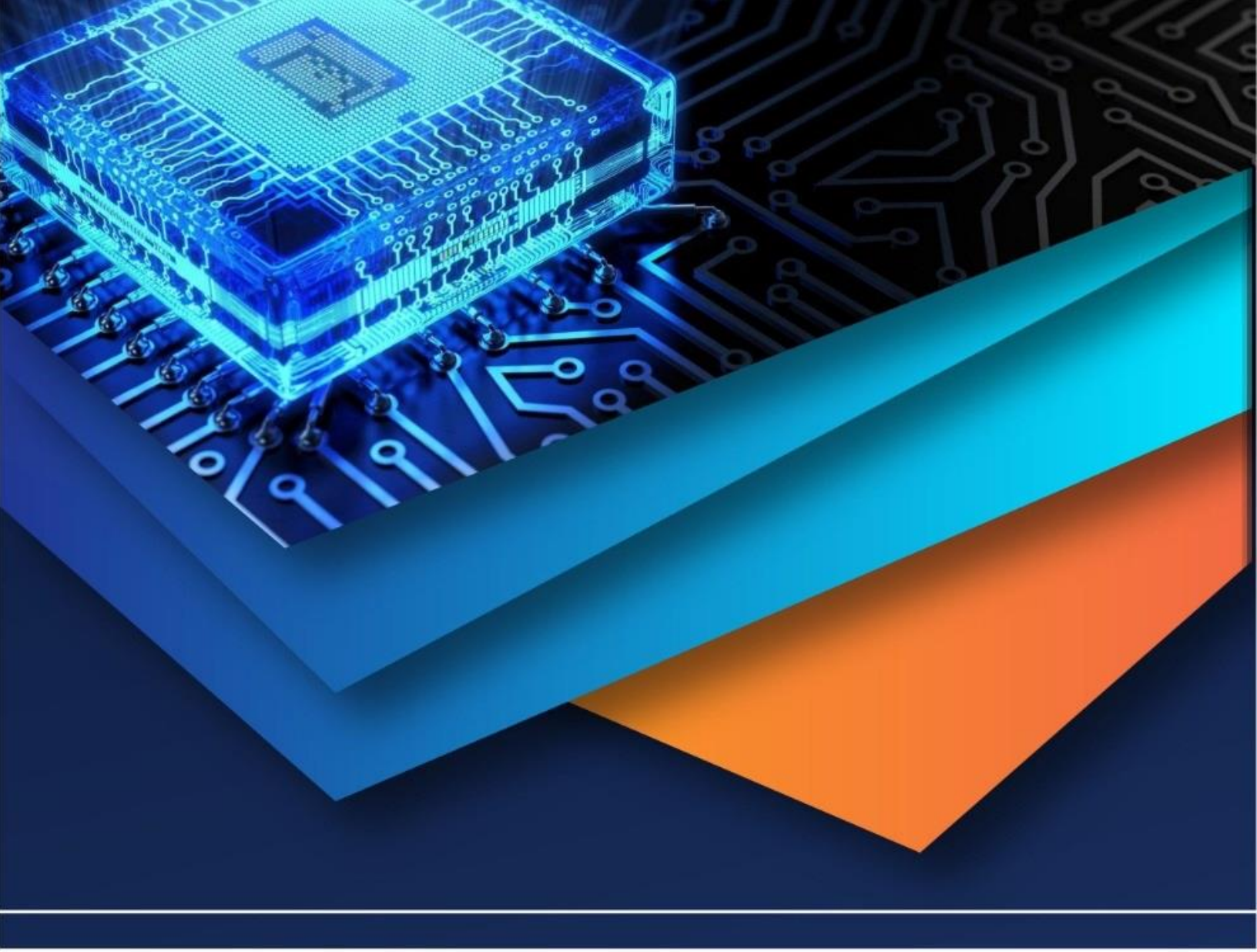
In the case of the virtual machine images determined by the SPARSE Extent, a static analysis using the mount of such virtual machine images is impossible if the grain directory and grain table are damaged. Also, a dynamic analysis is not possible because it cannot be operated. Thus, if the collected virtual machine images are irrecoverable, a direct investigation for such image files is required. The investigation for the images files can be carried out using a recovery method for the remained data and a method for the investigation of the metadata in a file system. Although the virtual machine images store the RAW data by fragmenting it into grains, the meaningful data can be recovered using a file carving method if the data is allocated to a continuous grain. The major subjects to recover are the files, which become evidence of user behavior like document and image files, and the information of the accessed sites is also obtained by recovering the evidence of the use of web pages and web browsers. In particular, as a virtual machine is determined by a Windows system, the information of the user's account and trail can be obtained if a registry file with an signature of 'regf' is obtained using a carving method.

IX. CONCLUSION

This paper presents a new system in virtualization technology. This system will provide additional functionality to administrator for resource optimization and management using which the simplicity to operate the VMware products will increase. Virtual Machine Introspection is suggested as the most practical approach to identify the malicious VM. If the intrusion detection system resides on the host, it may be susceptible to attack and if intrusion detection system resides in the network it is more resistant to attack. A virtual machine introspection based approach to intrusion detection is proposed where the Intrusion Detection System is outside the host for good attack resistance.

REFERENCES

[1] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: A virtual machine-based platform for trusted computing. InProc. of ACM SOSP, NY, Oct. 200
[2] A. M. Azab, P. Ning, Z. Wang, X. Jiang, X. Zhang, and N. C. Skalsky. Hypersentry: Enablingstealthy in-context measurement of hypervisor integrity. InACM CCS, Chicago, Oct. 2010
[3] http://link.springer.com/chapter/10.1007%2F978-3-642-33338-5_1#page-
[4] http://www.cs.ucsb.edu/projects/psc/2012IEEECloud.pdf
[5] http://www.ijarcsms.com/docs/paper/volume2/issue2/V2I2-0111.pdf
[6] http://www.sciencedirect.com/science/article/pii/S0895717711001014
[7] https://pdfs.semanticscholar.org/ee62/4310d44550543fe26fc15bfecc81427869a1.pdf
[8] http://searchvmware.techtarget.com/tip/How-VMware-snapshots-work



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY