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

Major Requirements and Demands for Building Smart Homes in metropolitan Cities by using Internet of Things Technologies

Ranganathan B. A[1]
[1]*New Horizon College of Engineering*

I. INTRODUCTION

Most of the people think that computer is just using in a company and office. It is a most misleading concept as we have a SMART HOUSE. The complete SMARTHOUSE System has been available since early 1993. In a SMART HOUSE, Engineers have build a relationship between computer and home. The SMART HOUSE is a home management Most of the people are thinking that it is difficult or only illusion to find a relationship between home and system that makes home owners or working group to easily manage their daily livings by providing for a lifestyle that brings together security, energy management, water management, parents management ,children take care ,entertainment, communications, and lighting features. So, the SMART HOUSE technology can installed in both existing structure ,new structure and upcoming. Now, the system can be installed in a home undergoing reconstruction where walls have been completely exposed. The SMART HOUSE Consortium is investigating a number of different option to more easily install the SMART HOUSE system in an existing home. Moreover, the SMART HOUSE system has been packaged to satisfy any home buyer's needs and budget. Now, more on all types of saving can be done in the SMART HOUSE System .Many management options that have the potential to reduce a home as per owner's utility and nearly50% or more per year depending on the options installed. In smart house one can control power systems, it will help save on our power bill. Studies have shown that the room heating and air conditioning can be more efficiently controlled and utilized by a computer. This saving tremendously on the cost of maintaining a consistent temperature within in a house. The exact level of savings will pay vary by house due to local utility rate structures, size of home, insulation, lifestyle, etc.

Secondly, it is an easily operating system. Home users can control their SMART HOME by using control panel, Smartphone, laptops, remote control or programmable wall switch. All SMART HOUSE controls are designed to be simple and easy to use. Because smart houses are independence, they can help people with disabilities maintain an active life.

resent development in the communities many of Things will turn Smart Homes from model to prototype . Smart Homes have become one of the important in the building Now a days, for Smart Cities waiting for dream from many years since late 1980 has made Automation Home which was not possible In the begging of the personal computers entered into home area. Now Smart Homes can divert most of the technologies. Present there are many characteristics that makes a Smart Homes. This paper has given importance to some of the essential requirements for homes Smart Homes The 7 unique requirement are classified according as per special quality of the Smart Homes building.

II. SMART HOME AND SMART CITIES

Smart Home or smart living may be the essential for the present buildings in the Cities, and the Establishment of rapid global urbanization. By 2050, nearly 65% of the global population may be living in urban areas of ‘‘mega-cities’’ with more than 100 lakhs inhabitants or more may be adding in the same area to share all resources and comfort effectively, but, provision of services to individual inhabitants is very difficult without collecting and learning habits . smart Labs, smart front offices, smart industries, and smart transport. Smart homes plays important role in measuring Smart Cities to gain data to protection privacy and properly details .property used interchange by in this method paper and they refer to the applications technologies in the good home environment. Any forgery made will be easily dictates .Making any forgery is difficult due to many interfacing technologies available in the market to trace easily Power or Energy harvesting source, Devises are fitted for temperature sensors which will wake up after every 15 minutes, Computers systems running full day . Repetitiveness of control system shall vary from nearly 100 times to a day once or yearThe idea of smart homes started in some ware 1961 s when computer started coming to homes .In the begins it was used for bookkeeping, temperature recording and controlling etc. Then person computers started in large only in mid 1970s.Then break through started in automatic control; of home appliances.

A breakthrough was discover of remote control was succeeded by decoding. But real research was started for smart homes. The real breakthrough started only after 1992 as emergency to the market. after lot of research by many companies now also we have not seen much significant in the smart homes due to high coast, difficulties in adaptation, complicated in operations, not eco-friendly, there is lack of knowledge by architects and civil engineers and need of skill labor, services need after installation and many more.

A. Sensor/probes networks for Smart Homes

The probes or networking as such of sensors things are connected By using wires or by using wireless technologies in homes depending on the weather or environment. Fo working of wireless systems, radio waves of short range and long range Links are to be provide for 2 different communication programs to fit in it was very different system for architectures and engineers. Wires system is having better efficiency than wireless system but while upgrading the system wire system is not feasible. Due to high cost in wireless system as not gain moment in the purchase. Introduction of LAN network communication for computers is gaining in smart homes. This may requires high bandwidth Video & audio streaming at homes.

B. Major requirements for building Smart Home

High degree of Safety ,Health & user friendly to use or operate by common person, demands of security and privacy protection, are all typical and critical local requirements of smart homes. Humans are the ultimate owners or users of all the things in the home space. The complexity will become more complex when there are multiple owners in a single home space. When there are multiple users or operators then different rules shall be applied at the same time, in the same single place, The minimum requirements are

1) Heterogeneity
2) Self configurable
3) Extensibility
4) Context Awareness
5) Usability
6) Security and Privacy Protection
7) Intelligence.

III. CHALLENGES

Research Organizations around the global have been promoting Smart homes technology by forecasting the huge potential of businesses
in almost in every market. Many organization and institutions are investing huge resource and money to place the technologies in place for development of smart homes to serve the general public. Many miles are there are still to meet challenges that need to be addressed for full utilization and development of smart homes.

A. Standardization

A smart system has to be developed for domestic with the most are connecting the devices in such way their probes or sensors, locally installed and available. In case of smart phones, tablets, laptops and travel from home to office to home , state to state , within country and countries to countries. There is a need for common standards throughout the world as International standards
The industries are taking sometime to adopt the local and international standards and produce for consumer products.
The new threats will become obvious when heterogeneous technologies are combined together.

B. Internet of people

As the internet is expanding at an exponational scale connecting people all over the world and even outside the globe The Internet connectivity will become an integral part of our day to day life, especially the Millennial eneration

IV. CONCLUSIONS AND FUTURE WORK

The major requirements will be based on architectures and technologies Included in the research. By adopting these requirements will not equate to a system that all will use, but it may helps to a common platform for a god smart home applications. The smart home utilization is still in a tortoise speed as there are no large Customers for users to upgrade from ordinary or common homes to smart home and then from remote controlling of house hold systems from remote places or from work place is a additional

investment rather than a necessity at present senior .With regard to real benefits from saving energy through automation, from remote monitoring for the elderly through tele-care
services, and from controlling appliances for disabled persons are gesture inter face. Tailor-made smart homes are needed with single computers with large number of invisible computers at home
The present trend in the Internet of Things will be changing and making an changes to Smart Homes and Smart Cities from illusion hype to reality. Smart Homes are the major constructing block for Smart Cities and having long dreams from decades, since from 1970s onwards. Home Automation came into picture and thinking of possible when personal computers started entering in the home spaces. The smart homes started sharing most of the internet technologies; there are some unique characteristics that started making smart home special. From the result of a recent survey and research survey on smart home this paper making to define the important requirements for building smart home

A. Keywords
Smart Cities Smart Home requirements ambient intelligence Internet of Things Home Automation

REFRENCES

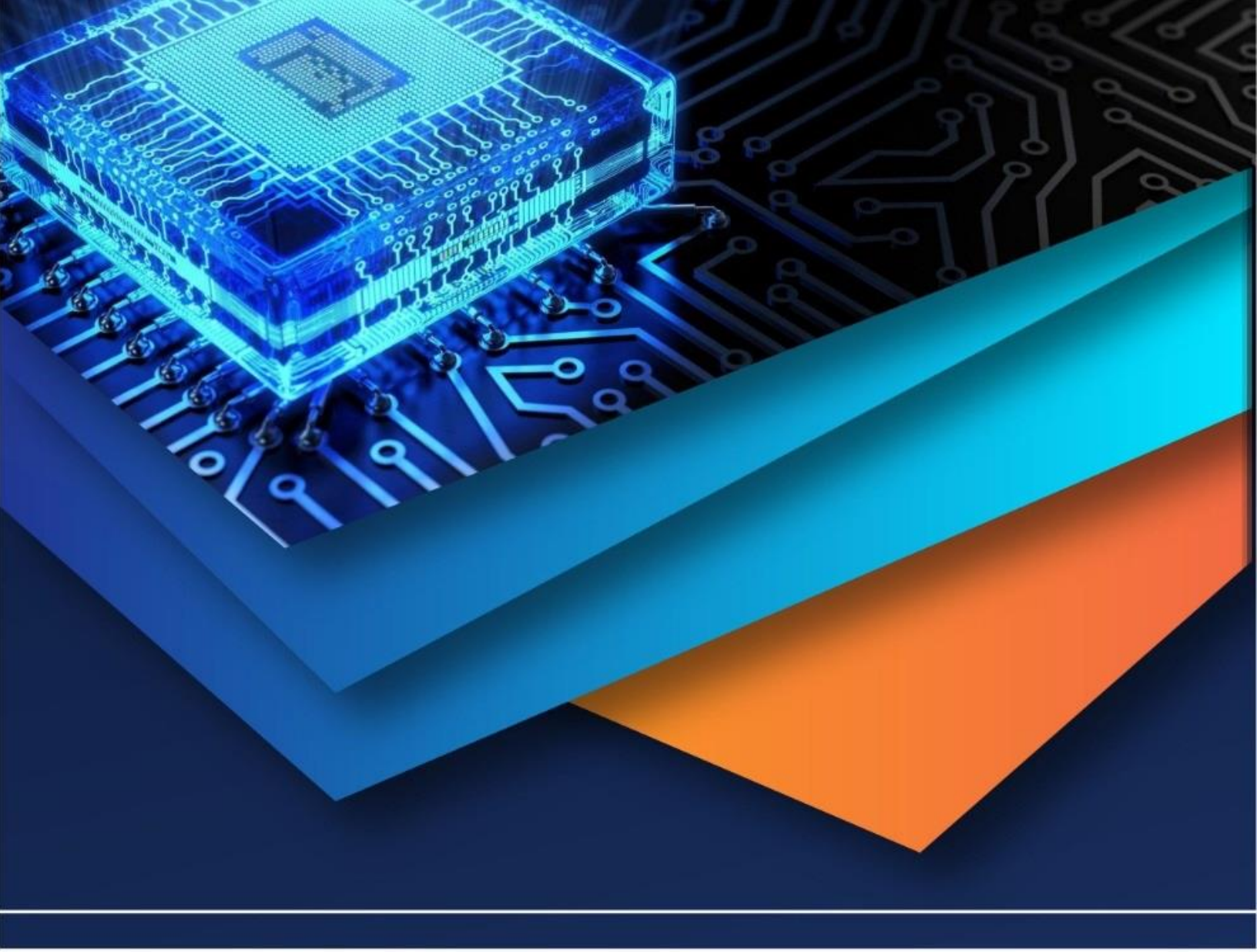
[1] V.D.K. Mai, Y. Kim, Using DLNA cloud for sharing multimedia contentsbeyond home networks, in: 16th International Conference on AdvancedCommunication Technology, ICACT, 2014, pp. 54–57. http://dx.doi.org/10.1109/ICACT.2014.677892
[2] K. Ashton, That 'Internet of Things' thing, RFID J. 22 (7) (2009) 97–114.
[3] D. Evans, The Internet of Things: How the Next Evolution of the Internet isChanging Everything, Tech. Rep., 2011, CISCO white paper. URL https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[4] C. Withanage, R. Ashok, C. Yuen, K. Otto, A comparison of the popularhome automation technologies, in: Innovative Smart Grid Technologies -Asia, (ISGT Asia), IEEE, 2014, pp. 600–605. http://dx.doi.org/10.1109/ISGTAsia.2014.6873860
[5] J. Sachs, Capillary networks - a smart way to get things connected, Tech.Rep., Ericsson Review, 2014, URL http://www.ericsson.com/news/140908-capillary-networks_244099436_c
[6] W. Webb, Standard's net gains [Communications Emerging Standards], Eng.Technol. 8 (5) (2013) 76–78. http://dx.doi.org/10.1049/et.2013.0512
[7] T. Yamazaki, Beyond the smart home, in: International Conference onHybrid Information Technology, ICHIT'06, Vol. 2, 2006, pp. 350–355.http://dx.doi.org/10.1109/ICHIT.2006.253633
[8] L. Xuemei, X. Gang, Service oriented framework for modern home appliances, in: ISECS International Colloquium on Computing, Communication, Control, and Management, CCCM'08, Vol. 1, 2008, pp. 700–703.http://dx.doi.org/10.1109/CCCM.2008.386

Integration of Virtual Machine with Cloud Nimish Aggarwal1 , Deepanshu Garg2 , Diksha Nagpal3 1, 2, 3Chandigarh 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 (VM1) 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 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 ©IJRASET (UGC Approved Journal): All Rights are Reserved 2 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 CSP2 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 IDS3 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. 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 ©IJRASET (UGC Approved Journal): All Rights are Reserved 3 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. 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 ©IJRASET (UGC Approved Journal): All Rights are Reserved 4 VI. REVIEW LITERATURE SURVEY A. VmwareVSphere 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. VmwareVcenter 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-onwrite (CoW) mechanism, where the root VM handles faults (using a fault handler), copies the content of the page (using copy-onfault)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 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 ©IJRASET (UGC Approved Journal): All Rights are Reserved 5 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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY