Practice on Detecting Malware in Virtualized Environment of Cloud

Himanshu Dhote[a], Prof. Archana Bhavsar [b], Dr. Madhuri Bhavsar [a,b,*]

[a]*16mcei08@nirmauni.ac.in, Nirma University,Ahmedabad, India*
[b]*bhavsar.archana@sscoetjalgaon.ac.in, sscoeit,Jalgaon, India*
[c]*madhuri.bhavsar@nirmauni.ac.in, Nirma University,Ahmedabad, India*

Abstract:
Virtual machines are expanding in notoriety and are being broadly received. The idea of a virtual machine is however not new. As per the cloud hypervisor is one of the major component of security. This paper consist of survey of various research paper in this domain. First we discussed about the functionality of the hypervisor form the research paper. Next, Paper discussed about various malware which has effect on hypervisor and the functionality or feature of that malware which make them to effect the hypervisor in virtualized environment. At long last, late research in the territory of hypervisor security is dissected. Research into the security of hypervisors is constrained. Most security examine is gathered in the cloud stage where hypervisors plays a noticeable part. As an assessment of security, some security bugs announced for the Hypervisor framework and the comparing relief methodologies utilized are likewise talked about.

Keywords:
VM Monitoring, Detection of malware, Integrity, Hypervisor Functionality, Malware analysis, Isolation, Virtualization, Rootkit, Firmware.

1. Introduction

Virtual Machine Manager (VMM) is an administration answer for the virtualized data- center, empowering you to design and deal with your virtualization have, systems administration, and capacity assets to make and send virtual machines and administrations to private mists that you have made.

PC framework analyzing is a basic testbed for looking after frameworks security. Interruption identification, get to control (e.g., DAC, MAC, and RBAC), sandboxing, inclined reference screens, firewalls, and antivirus all include security checking. A perfect checking framework ought to have both an entire perspective of the observed target also, the capacity to (stealthily) secure the observing framework itself. In spite of the fact that there are numerous approaches to do as such, it is not a straightforward errand. In the course of recent decades, an extensive sum of research has been done to look for better and more secure approaches to create such screens. Hypervisors and network node security should be taken into consideration.

The approach taken in this paper depends on the standards, what's more, rules gave by a current flexibility system. The fundamental supposition is that in the close future, cloud frameworks will be progressively subjected to novel assaults and different abnormalities, for which customary signature-based identification frameworks will be inadequately prepared and in this manner ineffectual. In addition, the greater part of current mark based plans utilize resource intensive profound bundle assessment (PBA) that depends intensely on payload data whereas a rule this payload can be encrypted and the cost required for the decryption can be reduced.

The element presented here from the basis in which various malware feature analysis has been done. Which malware till date has done adverse effect on the hypervisor and its solution? Proposed engine to detect and analyze the malware in the cloud for better development of the cloud.

2. Literature Review

This literature survey shows the lists of various cloud security used in hypervisor malware in virtualize environment. Table 1 shows the list of different cloud security which are surveyed that are used in monitoring. Various techniques are used for analysis so that they can be used for prediction. These papers have collected data from various sources like Data from various research paper on cloud, Data from DEFCON, Data from websites like Yahoo, Google and many more[10]

The following papers Apeksha Godiyal, Anhnguyen, Nabilschear (2016) used Lightweight hardware supported virtualization Platform effectiveness of various malware analysis techniques. (Godiyal, 2014)

Keith Harrison, Behzad Bordbar, Syed T.T. Ali, Chris I.Dalton, Andrew Norman(2017) used propose the creation of Forensic Virtual Machines(FVM), which are little Virtual Machines (VM) that can screen diverse VMs to locate the reactions. (Keith Harrison, 2017)

Michael R. Watson, Noor-ul-Hassan Shirazi, Angelosk Marnerides, Andreas Mauthe, David Hutchison (2017) used online cloud anomaly detection approach, comprising dedicated detection components of cloud resilience architecture. (Michael R. Watson, 2017)

Daniele Sgandurra, Emil Lupu (2016) used threat models, security and trust assumptions, and attacks against a virtualized system at the different layers—in particular, hardware, virtualization, OS, and application. (Sgandurra, 2016)

Mohammad M. Masud, Tahseen m. Al-khateeb, Kevin w. Hamlen , Jing Gao, Latifur Khan, Jiawei Han, Bhavani Thuraisingham (2014) used

Electronic copy available at: https://ssrn.com/abstract=3170188

proposes a multipartition, multichunk ensemble classifier in which a collection of v classifiers is trained from the consecutive data chunks using v-fold partitioning of the data, yielding an ensemble of such classifiers. (Masud, 2011)

Asit More and Shashikala Tapaswi focus on the headway of virtual machine keenness mechanical assemblies and their ability to address the semantic gap issue. (More, 2014)

Xuxian Jiang, Xinyuan Wang, Dongyan Xu used usage and assessment of VM watcher new system that defeats in various loophole task setting the malware recognition offices outside of the secured.

Gabor Pek, Levente Buttyan, Boldizsar Bencs Ath (2016) used current threat and existing assaults on different virtualization stages. (Pék, 2013)

Table 1 – Literature Survey.

Author	Paper
Apeksha Godiyal, Anh Nguyen, Nabil schear	A Light Weight Hypervisor For Malware Analysis.
Keith Harrison, Behzad Bordbar, Syed T.T. Ali, Chris I.Dalton, Andrew Norman	A framework for detecting malware in Cloud by identifying symptoms.
Michael R. Watson, Noor-ul-hassan Shirazi, Angelos K. Marnerides, Andreas Mauthe, and David Hutchison	Malware Detection in Cloud Computing Infrastructures.
Daniele Sgandurra, Emil Lupu	Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems.
Mohammad M. Masud, Tahseen m. Al-khateeb, Kevin w. Hamlen , Jing Gao, Latifur Khan, Jiawei Han, Bhavani Thuraisingham	Cloud-Based Malware Detection for Evolving Data Streams.
Asit More and Shashikala Tapaswi	Virtual machine introspection: towards bridging the semantic gap.
Xuxian Jiang, Xinyuan Wang, Dongyan Xu	Stealthy malware detection and monitoring through VMM-based out-of-the-box semantic view reconstruction.
Gabor Pek, Levente Buttyan, Boldizsar Bencs Ath	A Survey of Security Issues in Hardware Virtualization.

2.1. Pros and Cons Of Hypervisor Malware

There are various parameter for measuring pros and cons for the system. Following table describe the parameter which will more discussed about the things which make the security of cloud more desirable and in the same table we are discussing about the parameter which make us concerned about the security of cloud.

Table 2 – Literature Survey.

Paper	Advantage	Disadvantage
A Light Weight Hypervisor For Malware Analysis. (Godiyal, 2014)	Able to dump the physical memory of Invaders and inspect the location of invaders gather information based on key pressed by user for user profiling	General purpose VMMs are as large and complex as modern operating system. More vulnerabilities will get discovered in these system which is impractical for malware analysis
A structure for recognizing malware in Cloud by distinguishing side effects. (Pék, 2013)	changing condition of a VMs memory, forms that take unreasonably long circumstances to instate is disposed of, bits of program code that has been jumbled	Decent variety of Malware, Efficient and versatile administration of computational assets required for Introspection
Malware Detection in Cloud Computing Infrastructures. (ECONOMICS, 2007)	Dedicated monitoring components every VM is especially material to cloud situations and prompts an adaptable discovery framework equipped for recognizing new malware strains with no earlier information of their usefulness or their hidden guidelines	Accuracy is low
Development of Attacks, Threat Models, and Solutions for Virtualized Systems. (Keith Harrison, 2017)	Dangers and assaults against a framework running in a virtualized situation and the examination arrangements went for tending to an arrangement of dangers.	Just a particular danger demon-state and are profoundly touchy to variety to that model.(Threat Model)
Detection of malicious code using data streams. (Masud, 2011)	Multipartition, multipiece group system essentially diminishes order blunder	runtime execution of could be enhanced by misusing extra parallelism
Virtual machine introspection: towards bridging the semantic	Utilization of VMI is prevailing in the security area. Thus, this makes VMI powerless to assaults.	Some execution changes highlights of HVM visitors, for example, go through drivers, put

Electronic copy available at: https://ssrn.com/abstract=3170188

gap. (Jiang, 2010)		impediments on VMI usage. Contemplation utilizing VT bolster can possibly empower VMI yet requires extra work
Domain analysis in hardware virtualization. (Intel Security Tech, 2017)	vulnerabilities and assaults focusing on the visitor, the host OS, the hypervisor layer, the administration interface and the distinctive systems inside a virtual	multitenancy, execute subjective out- of-the-visitor code either locally or remotely ,the capacity work environment

3. Malware analysis

In this section of malware analysis we have describe various malware which have affected the cloud by which it have compromised its data and integrity. Not only we have describe the effect of malware on the cloud but also a various techniques by which we can compromised the security of the cloud. All the vulnerability and security issues on premise have still remain in the cloud beside the malware we have all describe the well know attack which have be performed on the cloud we classify cloud applicable attacks into four groups; provide sample attack incidents from each group, and present comparative analysis of some of the famous security mitigation techniques

Table 3 – Malware Analysis.

Malware	Working Of Malware
BluePill. (invisiblethings, 2016)	Exploit AMD64 SVM Extension to move the operating system into the virtual machine. Provide Thin Hypervisor to control the OS. No reboot or any modification is required in BIOS. BluePill Cannot be detected offline.
Malicious. (Sec, 2017)	They introduce a pernicious hypervisor in runtime. Adjust the code or information structures of a legitimate hypervisor, we may accomplish capacities like the ones accessible for Vitriol.
Doxware. (Sec, 2017)	The activity of exposing files that are sensitive to someone. Instead of encrypting files, the malware writers focused on the private files of users, threatening to leak them to friends on social media or sell them online.
RIG Exploit Kit. (Joanna, 2016)	The EK used the domain shadowing technique and the HTTPS open redirector from Rocket Fuel.
Hypervisor Based Isolation (Sec, 2017)	Mainly impact on software and device to get access of physical OS in a cloud.
Firmware Rootkit. (Sec, 2017)	Firmware rootkit can open a backdoor for an attacker VM to access all other VMs. At some point system firmware got infected with a rootkit During each boot rootkit installs a backdoor for an attacker controlled VM.
Qemu/KVM (Not a Malware) CVE-2014-3689	Drawback Of Qemu/KVM: vulnerabilities in the vmware-vga driver in QEMU allows local guest to write to QEMU memory and gain host/hypervisor privileges via unspecified parameters related to rectangle handling.
Xen Attack via boot script (Not a Malware)	Xen attack via S3 boot script, Changing the boot script to access Xen hypervisor pages, Found S3 boot script table in memory accessible to Dom0.

3.1. Attacks on cloud

Over the period of time cloud has noted various attack on each level of cloud. In this section we are describing the known attack which are placed over the period of time on the cloud. (Issa M. Khalil, 2014)

- **Theft-of-Service:**
  Consequences related to this attack is Cloud service usage without billing Cloud resource stealing with less/no cost and this attack falls in Cloud Infrastructure category.
- **Denial of service :**
  DDoS Http-Based DDoS Xml-Based DDoS REST Based-DDoS Shrew attack (light traffic) DoS are the attack incident. Consequences related to this attack is Service/hardware Unavailability wrapping a malicious code in Xml signature to gain unauthorized access to information accessing a browser history or any other private information through unsecure Http browsing and this attack falls in network and Cloud Infrastructure category.

Electronic copy available at: https://ssrn.com/abstract=3170188

- **Cloud malware injection:**
  Consequences related to this attack is Credential information leakage User data leakage Cloud machine abnormal behavior and this attack falls in Cloud Infrastructure category.
- **Cross VM side channels:**
  Timing side channels Energy consumption side channels are attack incident. Consequences related to this attack is User data/information leakage Cloud resources/infrastructure information leakage and this attack falls in Cloud Infrastructure category.
- **Targeted shared memory:**
  Consequences related to this attack is Cloud resource's information leakage User information/data leakage Provides open window for other attacks such as side channels and cloud malware injection and this attack falls in Cloud Infrastructure category.
- **Phishing:**
  Consequences related to this attack is Unauthorized access to personal information Installing a malicious code into user computer Force cloud computing structure to behave abnormally Make server unavailable for end user and this attack falls in Cloud Infrastructure, Network, Access category.
- **Botnets:**
  Consequences related to this attack is stepping stone attack & unauthorized access to cloud resources Make cloud system work abnormally stealing sensitive information Stealing user data and this attack falls in Cloud Infrastructure, Network, Access category.
- **Audio Steganography:**
  Consequences related to this attack is Unavailability of cloud storage system accessing user data User data deletion and this attack falls in Cloud Iaas, Access category.
- **VM rollback attack:**
  Consequences related to this attack is Launch brute force attack Damage cloud infrastructure Leakage of sensitive information and this attack falls in Cloud Infrastructure, Network, Access category.
- **Oracle Virtual Box (Not a Malware) CVE-2014-6588 CVE-2015-0427:**
  Consequences related to this attack is Drawback Of Oracle Virtual Box:.1)Memory corruption in VMSVGAGMRTRANSFER 2)Integer overflow memory corruption in VMSVGAFIFOGETCMDBUFFER and this attack falls in Cloud Infrastructure category.
- **Attacking Hypervisors through System Firmware (Not a Malware):**
  Consequences related to this attack is 1) Pointer Vulnerabilities in SMI Handlers.2) Exploiting firmware SMI handler to attack VMM.3) Root cause? Port B2h is open to VM in I/O bitmap.4) Attacking VMM by proxying through SMI handler and this attack falls in Cloud Infrastructure, Network, Access category.

4. System Architecture

System Architecture of any framework describe the overall flow of the system in which manner it will work and flow to perform the given task. In this section of cloud system architecture we have describe the flow of cloud while providing various service to the users. Fig. 1 Cloud flow describe the flow of cloud toward hypervisors and the service provided by the hypervisor while allocating the VMs and monitoring the services.

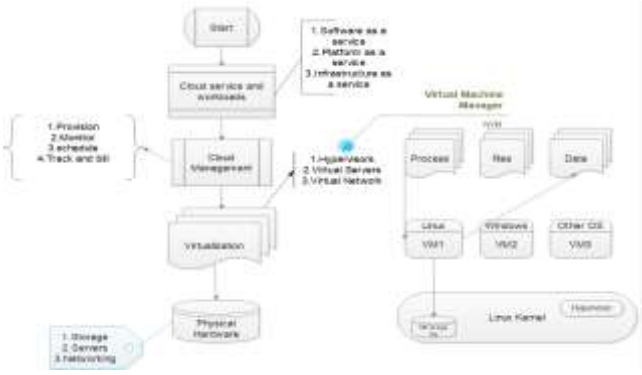

Fig. 1 - Cloud flow

Fig. 2 mainly describe about the vm how it can open the backdoor in the hyervisors to compromised the integrity of the data and security of hypervisors. This diagram mainly discussed about the solution to the backdoor in the hypervisor. which allow the engine to analysis the malware to make system more secure.

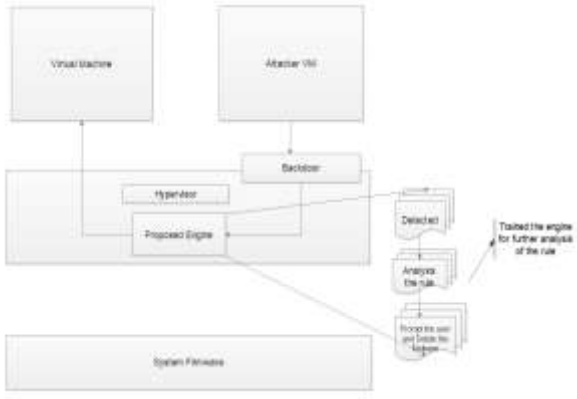

Fig. 2 - Proposed Engine for hypervisor malware detection

Fig.3 contain the information based on the user point of view how malware can be detected in the Vms. After detecting the malware it will be get classified into level of threat and according to which system will act rule on the hypervisor. High level threat have different set of rule as compare to low level threat while taking action against malware.

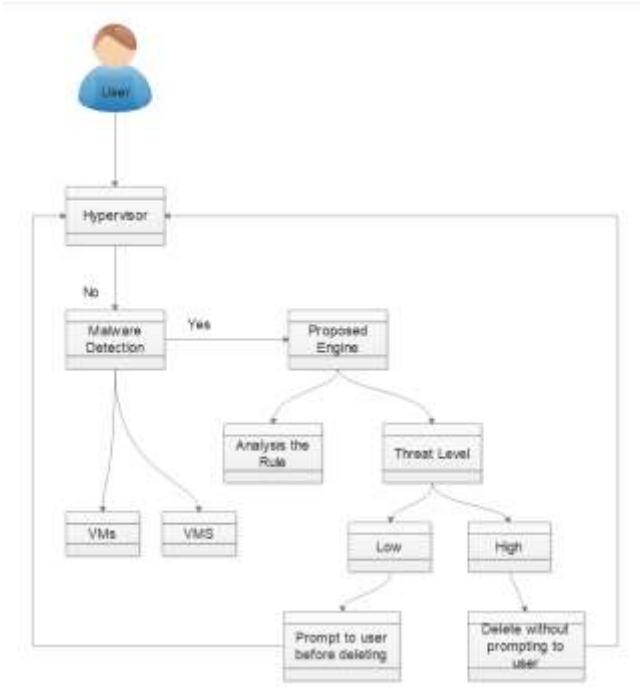

Fig. 3 - Detection of Threat Level

Fig.4 describe the flow chart of detection of malware in the system. It will first check user status if it is in idle state it will scan for the user vm memory if it is in not in a idle state it will stop monitoring the process. In a next step it will analyse the scan memory or if it unable to scan memory it will check the connection status for further analysis. It will genrate the report of found malware and give alert to the user for further action.

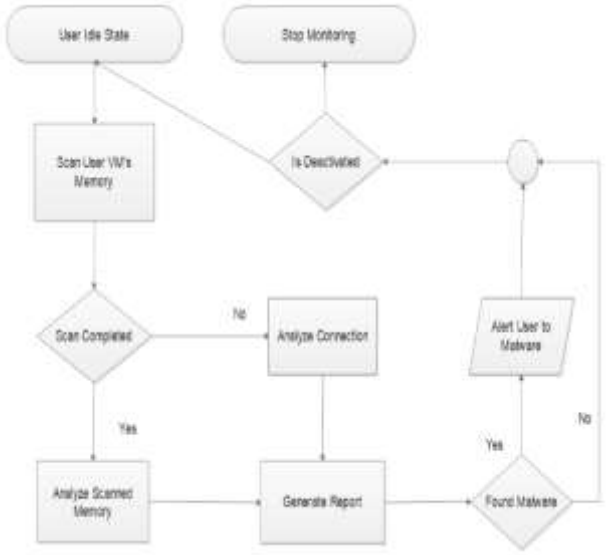

Fig. 4 - Flowchart of malware detection

5. Future Scope

This section will discussed about the requirement of work in the domain of cloud to make it more reliable for user. Currently in a cloud malware can be ejected in a cloud system by network node backdoor of a system or by firmware that can allow malware to take control of cloud. Many hypervisor still updating there system to overcome the drawback of pitfall of the system which required deep study in this domain.

Table 1 – Literature Survey.

Paper	Future Scope
A Light Weight Hypervisor For Malware Analysis	Fully Evaluate extraction technique against Linux and Windows. (Godiyal, 2014)
A framework for detecting malware in Cloud by identifying symptoms	Sample of a Mobility algorithm, a Distributed Algorithm, which allows collaboration of the FVMs in identifying multiple symptoms. (Keith Harrison, 2017)
Malware Detection in Cloud Computing Infrastructures	Respond to new threats and challenges online and in real time under minimal computational cost. (Michael R. Watson, 2017)
Evolution of Attacks, Threat Models, and	Different solutions with the same security properties using

Solutions for Virtualized Systems	their implementation strategies. (Sgandurra, 2016)
Cloud-Based Malware Detection for Evolving Data Streams	Current feature selection procedure limits its attention to the best S features based on information gain as the selection criterion. The classification accuracy could potentially be improved by leveraging recent work on dimensionality reduction techniques for improved feature selection. (Masud, 2011)
Virtual machine introspection towards bridging the semantic gap	The security weaknesses of VMI will need to be addressed to enable widespread adoption by the industry. (More, 2014)
Stealthy malware detection and monitoring through VMM-based out-of-the-box semantic view reconstruction	Reduce complexity of various techniques implemented by applying Vmwatcher. (Jiang, 2010)

6. Conclusion

The adoption of cloud computing paradigm is continuously growing. With the massive growth in cloud computing adoption, the security attracted the attention of researchers and practitioners but still has not received enough attention. In this work, we conduct a survey on the current cloud security issues and the state-of-the-art security solutions. In this paper we have discussed about the parameter about cloud security and various security implementation techniques. We have discussed about the pros and cons in recent trend of hypervisor environment, how they can be monitor and what need to be monitor. Also in this paper we have analysis malware and there working. Drawback in various hypervisor which have been detected recently. This paper also contain various know attack on a cloud. Possible flow of the cloud and how malware can be detected and prompted to the user. Threat level in the hypervisor system to detected the category of the cloud. In this it also contain future scope in domain of a cloud.

References

ECONOMICS, C. (2007). *Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other Malicious Code.* NewYork.

Godiyal, A. A. (2014). A lightweight hypervisor for malware analysis. *ACM*, 116-123.

Intel Security Tech, r. (2017). *INTEL. Intel R Virtualization Technology Specification for the IA-32 Intel R Architecture.* California: Intel Report.

Ismael, O. A. (2017). *USA Patent No. US Patent 9,736,179.*

Issa M. Khalil, A. K. (2014). Cloud computing Security: A Survey. *Computers*, 1-35.

Jiang, X. a. (2010). Stealthy malware detection and monitoring through VMM-based “out-of-the-box” semantic view reconstruction. *ACM*, 13(2), 12.

Joanna, R. (2016, August 02). *invisiblethings*. Retrieved from Bluepill: https://blog.invisiblethings.org/

Keith Harrison, B. B. (2017). A framework for detecting malware in Cloud by identifying symptoms. *IEEE 16th International Enterprise Distributed Object Computing Conference*, 164-172.

Masud, M. M.-K. (2011). Cloud-based malware detection for evolving data streams. *ACM*, 2(3), 16.

Michael R. Watson, N.-u.-h. S. (2017). Malware Detection in Cloud Computing Infrastructures. *IEEE Transaction on Dependable and Secure Computing*, 192-205.

More, A. a. (2014). Virtual machine introspection: towards bridging the semantic gap. *Journal of Cloud Computing, SpringerOpen*, 3(1), 16.

Pék, G. L. (2013). A survey of security issues in hardware virtualization. *ACM*, 45(3), 40.

Sec. (2017, september 21). *Attack on pc*. Retrieved from timeglider: http://timeglider.com/timeline/5ca2daa6078caaf4

Sgandurra, D. a. (2016). Evolution of attacks, threat models, and solutions for virtualized systems. *ACM Computing Surveys (CSUR)*, 48-57.