ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 1, Issue 5, November 2012

A Survey on Security Assurance Architecture in Virtualization implementation on Cloud

E.Bijolin Edwin*, Dr.P.Uma Maheswari**,M.Roshni Thanka***

*(Assistant Professor, Department of Information Technology,Karunya University, Coimbatore,India-46)
** (Professor & Head, Department of Computer science and Engineering, Info Institute of Engineering, Coimbatore, India)
***(Assistant Professor, Department of Computer Science and Engineering,Karunya University, Coimbatore,India-46)

Abstract:Cloud computing is a natural extension of virtualisation technologies that enable scalable management of virtual machines over a massive physically connected systems. The virtualisation-based cloud computing paradigm offers a practical approach to green IT/clouds, which emphasise the construction and deployment of scalable, energy-efficient network software applications (NetApp) by virtue of improved utilisation of the underlying resources. This is typically achieved through increased sharing of hardware and data in a multi-tenant cloud architecture/environment, and accentuates the critical requirement for enhanced security. This paper analyses the key security challenges faced by cloud computing environments,also it gives detail on the security architecture on Cyber Security which being implemented in Cloud Protection System Architectures. It provides enhanced secure virtualization which is designed to address several key security problems within the cloud computing context.

General Terms
Cloud computing, virtual machine, security,Cyber Security

Keywords:
Virtualization, CyberSecurity,Cloud Protection System, NetApp.

I. INTRODUCTION:

CyberGuarder provides three different kinds of services; namely, a virtual machine security service, a virtual network security service and a policy based trust management service. Specifically, the proposed virtual machine security service incorporates a number of new techniques which include (1) A VMM-based integrity measurement approach for NetApp trusted loading, (2) Here multi-granularity NetApp isolation mechanism to enable OS user isolation, and (3) a dynamic approach to virtual machine and network isolation for multiple NetApp's relied on energy-efficiency and security requirements. Secondly, a virtual network security architecture service has been developed here to provide an adaptive virtual security appliance deployment in a NetApp execution environment, then a traditional security services such as IDS and firewalls can be included as VM images and deployed over a virtual security network in accordance with the practical configuration in virtualised infrastructure architecture. Thirdly, the security service providing policy based trust management is proposed to facilitate access control to the resources pool and a trust federation mechanism to support/optimise task privacy and cost requirements across multiple resource pools can be made. Preliminary studies of these services have been carried out on iVIC platform, with promising results.

II. RELATED WORK

The survey paper on cloud computing presented in Armbrust et al. (2009) makes a clear view on Cloud architectures.There are many research papers on integrity checking mechanisms and intrusion detection solutions which will make the security assurance architecture a clear one to implement. Those mechanisms can be successfully applied to cloud computing as well to virtualization techniques also. For example, the Filesystem Integrity Tools and Intrusion Detection Systems such as Tripwire (Kim and Spafford, 1994) and AIDE (AIDE team, 2005) can be deployed and also implemented in virtual machines. But these are subject to attacks possibly coming from a guest machine user who has turned the machine into a malicious one which will detect the entire architecture. In addition to this, when an attacker

finds out that the target machine is in a virtual environment, it may attempt to break out of the virtual environment incloud through vulnerabilities (Secunia, 2009) in the Virtual Machine Monitor (VMM) available in architectures.

III. VIRTUALIZATION TECHNIQUE:

Cloud Virtualization helps multiple instances of same application that can be run on one or more cloud resources in a virtualization environment. It automatically provides scalability when more number of user wants to run their application in a secure environment in same development area. It gives each user that their application is running on a single virtual machine in that environment. Here, end user cannot see other user's data properly. Proper isolation of Virtual machine is important than others. As like with Fig 1 with most virtualisation-based cloud platforms that operate in a multi-tenant cloud environment, the successful adoption of such a green computing architecture strongly depends on its security assurance mechanisms.The impact on the deployment and operations of the Virtual system, that are, inevitably used, also energy-consuming.

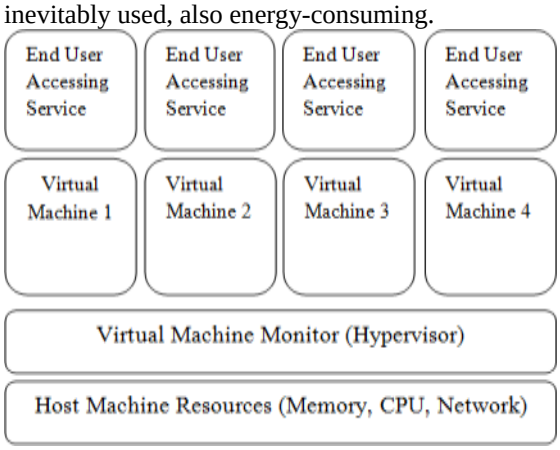

Figure:1 Virtualization Technique

Consequently, an integrated security solution would not help in providing the necessary security services, but also in reducing the overall energy consumption. Using our iVIC platform as a testbed, three key challenges have been identified and must be addressed, as follows. First, a NetApp should be loaded without malicious tempering. Various malwares, such as virus, worms, Trojans and rootkits, continue to threaten the security of a VM. In particular, rootkit malware can hide its own process, or disguise it as a legal process, to escape the detection from a virus scanner or an intrusion detection system(IDS).Second,conventional network security systems including IDSs,firewalls, should be virtualised in cloud and also easily deployed in a cloud environment through NetApp execution environment. There are several limitations; namely, (a) The deployment cost of a security system in an cloud environment(e.g., IDS) is generally high, and cannot be adaptively redeployed in that same architectures(e.g., Hardware IDS); (b) In place of the traditional security appliance, the virtual security appliance has become a new way of being rapidly enhanced and dynamically deployed within the distributed IT infrastructure amoung that architectures. Third, a policy-based access control service for the virtualization technique should be put in place to protect the security of the virtual resources amoung them. Some NetApps often require scalable computing power, but a single resource pool often found in private clouds may not be able to provide adequate resources for a large number of users.

IV. CYBER SECURITY INITIATOR:

To address these challenges, we propose a novel security assurance architecture, known as Cyber Security Initiator, which enables the trusted loading of NetApps, isolation of different NetApps, virtual security appliances for the NetApp operating environment, and resource access control and remote access to NetApp. We design Cyber Security Initiator, a security assurance architecture designed for NetApp operating systems, as a truly virtualisation based security solution developed for green cloud computing environments. A virtual machine security service, which includes mechanisms for software integrity measurement and multi-level security isolation, has also been developed. The Virtual Machine Manager (VMM) based integrity measurement approach named VMInsight can provide load-time and run-time monitoring of system processes. VMInsight intercepts system calls and process behaviours by monitoring changes in VM CPU registers.It is implemented in the hypervisor, which is completely transparent to the software and operating system running in the VM. We design a virtual network security service, which provides an adaptive mechanism to deploy virtual security appliances in a virtual network of the NetApps running environment. To enable flexible network traffic detection, we develop a dynamic software mirror port mechanism to facilitate detections of the virtual network interface.

V. CLOUD PROTECTION SYSTEM .

In the proposed Cloud Protection System (CPS)[10], the guest virtual machine is monitored by the host to ensure that the integrity of the virtual machine is protected. We mainly monitor the kernel code or data that would be targeted (or) affected by attacks to provide protection to the virtual machines and the cloud infrastructure. Thus

any modification to the kernel code and data is detected by monitoring the cloud components and the kernel (of virtual machine). This monitoring guarantees that the integrity of the virtual machine kernel and the cloud middleware have not been compromised.

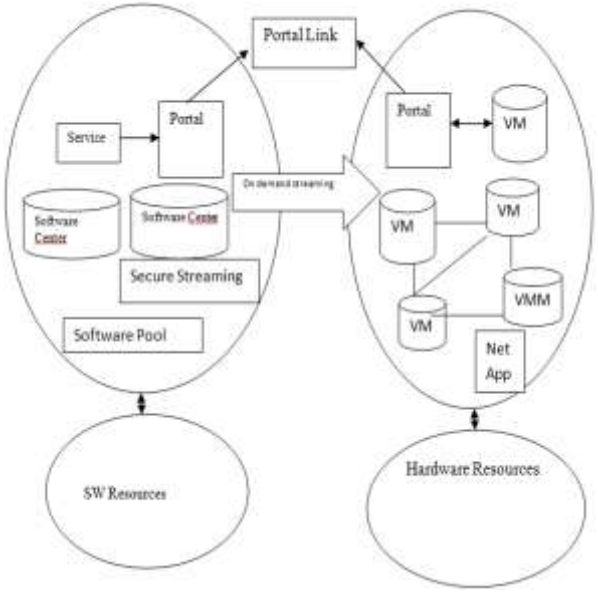

Figure:2 Deployment architecture of Cyber Security

Now how we monitor the integrity of cloud components is by logging in and verifying the checksum of cloud libraries and executable files periodically while the data is being analysed. The high level description of CPS is shown in Figure 3. The monitoring data flows are depicted as continuous lines in green color where as the dangerous data flows are shown as lines (red). All the CPS[10] modules- with the Interceptor, with the Warning Recorder, along with Warning Queue and the Evaluator are located on the base machine (host) to encapsulate them. The Interceptor component notices any suspicious guest activities like for example, system_call invocation and it is recorded by the Warning Recorder into the Warning Queue (WQ) which gives a warning signal present in that same queue. Then the threat will be evaluated by the Evaluator component which identifies and evaluates . Our protection system called CPS is implemented over Eucalyptus cloud environment. Eucalyptus (Nurmi etal.,2009) consists of: a Node Controller (NC) that controls the execution, inspection, and termination of VM instances on the host where it runs; a Cluster Controller (CC) that gathers information about VM and schedules VM execution on specific node controllers; further, it manages virtual instance

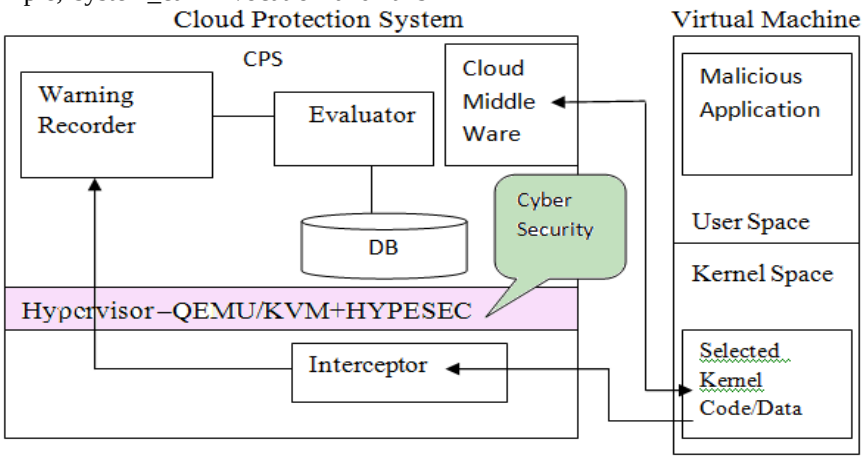

Figure: 3 Cloud Protection Systems

networks; there is a Storage Controller (SC)—Walrus—that is, a storage service providing a mechanism for storing and accessing VM images and user data; a Cloud Controller (CLC), the web services entry point for users and administrators that make high level scheduling decisions in that same aspects. The NC runs on every node hosting VM instances with in that same architectures. The NC activity and integrity is mainly monitored periodically, as it is the key component for our cloud implementation in virtualization environment. Now, if any dangerous alteration in the guest VM is detected in that particular area, CPS can take actions like shutting down the VM or restarting a clean image with in them. An attack can be implemented by inserting a rootkit with in the guest virtual machines. For instance we can insert Sebek, which is a kernel module rootkit that hides its presence and intercepts file system and network activity within them. It also alters the syscall table which acts as a system calls and changes the execution flow to execute any malicious code. CPS can detect both the alteration of the syscall table and the change in the checksum of kernel files on virtual storage through the system calls. Now if there are many virtual machines installed in a single system and one virtual machine has gone malicious, then it will affect the remaining virtual machines in no time. That is, the co-location of multiple virtual machines increases the attack surface and risk of virtual machine-to-virtual machine compromise. Hence along with CPS, we can include a security feature in the hypervisor Qemu that provides a good security assurance to provide better protection. We kept the name as HypeSec since we add the security feature in the hypervisor that enables a good assurance architecture.

VI. IMPLEMENTING CYBER SECURITY IN CPS

According to the requirements analysis of a network-based software operating system, we design the architecture of Cyber-Security in iVIC The iVIC is one in which the network computing platform that is based on a distributed virtual resource container to implement the individual computing and storage devices so that they can provide virtualised entities, such as VMs or vDisks on an virtual environment. Virtual machines are dynamically deployed and connected into virtual networks. Users may allocate their own virtual clusters or even complex virtual networks (vLabs) in iVIC to support hardware as a service (vHaaS) and software as a service (vSaaS) application scenario.In iVIC platform the relied software and hardware resources are organised in respective resource pools, and software in a software pool (SW Pool) can be downloaded and installed into VMs in a hardware pool (HW pool) on-demand basis. There are four key security components in this architecture: NetApp trusted loading, multi-level NetApp isolation,virtual security appliance (e.g., vIDS), and NetApp resource trust management. Virtual machine security service In this VM security service, we not only provide a VMM-based NetApp trusted loading approach-VMInsight, but also a multilevel security isolation approach based on the virtual machine technologies.

A. VMM-based software integrity verification

In VMImsight, we leverage the VMM-based system call interception approach to provide load-time and run-time integrity protection for a NetApp. **Firstly**, VMInsight intercepts and analyses the system call sequence to identify and control the loading of software including user applications, shared libraries and kernel modules.

Secondly, a system call correlation method is designed to establish the relationship of multiple system calls. Finally, VMInsight monitors the behaviour of NetApp processes to recognise the malicious attacking patterns. For example, VMInsight can find hidden processes using the cross-view theory by collecting a real VM process list and comparing them with that coming from the OS user's tool. The VMM-level protection mechanism ensures that the VM system can maintain its correctness and security even if the guest OS kernel has been comprised. The VMInsight system also supports legacy or commodity guest operating systems, and it requires no modification to the guest OS.VMInsight has three main components: System Call Interpreter (SCI), System Call Analyzer (SCA) and Integrity Measure Module (IMM). The VMInsight works using the following two steps (1) SCI intercepts a

system call instruction (i.e. INT 80h or sysenter) invoked from the user mode in the guest OS, and identifies a binary-executing related system call, resolves system call arguments to get executable path information.

The arguments and path information are passed to SCA and IMM for further analysis. SCA analyses the system call information based on configurable patterns to monitor the

run-time behaviour of processes. IMM receives executable paths from SCI, locates the disk file using path information,and then measures the file content. IMM takes measurements

using the SHA-1 hash algorithm, and the fingerprint is then compared with known values stored in the fingerprint library

It can be implemented VMInsight in two majorVMMs (Qemu and KVM). We can evaluate its effectiveness to detect malicious processes, and the performance and energy-consumption overhead.**First**, we use some malware samples to evaluate the effectiveness of VMInsight.We simulate the malicious software's behaviour of tampering with the already known software to test whether VMInsight can detect such an integrity exception.The results show that VMInsight can identify processes, detect network traffic, and monitor CPU usage and file operations. Such information will be exploited and integrated to identify malicious software behaviours. For example, the hidden processes which steal users' information can be located by analysing the network packet's receive/send status, thus resulting in the reporting of malicious software.**Second,** we use some benchmark applications to evaluate the performance overhead of VMInsight for Qemu and KVM. VMInsight incurs less than a 10% performance overhead. According to the above analysis, we can conclude that the monitoring information provided by VMInsight can be used to develop a third-party security system.

B. Multi-granularity NetApp sandbox mechanism

Here the Isolation is an important factor to improve the availability and security of applications running in a virtual environment [3],and is more far than a superior to applications running in a traditional, nonvirtualised system. While the virtual machines in a cloud environment can share the physical resources of a single computer with in a virtualized architecture, they remain completely isolated from each other as if they were in separated physical machines. If, for example, there are four virtual machines running on a single physical server and one of the virtual machines crashes in one particular time , the other three virtual machines remain available within that .There is a scenario called a multi-granularity NetApp sandbox mechanism[3] in Cyber Security, which can provide security isolation at different levels. The isolation at the user and application levels is achieved with existing tools, and the virtual network level isolation is achieved with CyberGuarder ERVIN. In response to the user isolation requirement in an OS, we use chroot

to create and host a separate virtualised copy of the software system. Now, we are also adopting Linux kernel seccomp to allow processes to call a very small subset of system calls, e.g., read, write, Three-level NetApp isolation in CyberSecurity.sigreturn, and exit. For the NetApps isolation requirement among VMs, we assign security policies for a resource pool and a scheduler (deployed with the Web Portal) can automatically deploy VMs according to the NetApps' isolation policies. For the virtual network isolation requirements, we design the ERVIN which uses a layertwo tunnel VPN between distributed vBridges, and the metadata

such as virtual network topologies is maintained in a central node to optimise the traffic between VMMs. CyberGuarder ERVIN provides a data transmission mechanism in a P2P manner for a virtual network, the network packets between different virtual machines do not transit through a central server, thus making full use of the network bandwidth between the hosts to improve the efficiency of virtual machines' network packet transmission.

VII. CONCLUSION.

Cloud computing is an extension of virtualisation technologies which enable scalable management of virtual machines being present on distributed hosts giving maximal utilisation of re-sources . As well as providing a much improved hardware efficiency it also raises some issues related to security and data integrity within the cloud environment, and in

an open NetApp operating system. This paper proposes a architecture named Cloud Protection System that can provide security to the cloud resources via virtualization. CPS monitors the guest and the middleware components and ensures that the integrity has not been compromised. To enhance the security provided, HypeSec architecture is proposed which is integrated along with the hypervisor Qemu[3]. CPS combined with HypeSec can be deployed on any cloud implementation.A virtualisation security assurance architecture, CyberSecurity [3], which is designed to address several key security problems. Several techniques concerning the provision of integrity verification, multi-level NetApp isolation, virtual security appliance (e.g., vIDS), and NetApp resource trust management services have been implemented. Preliminary results obtained on our iVIC platform are promising.Future work concerns the construction of a reliable and scalable utilization of NetApp operating system that will support all other advanced virtualisation technologies, a greater federation of cloud services to facilitate the seamless integration of private and public cloud systems.

VIII . REFERENCES.

[1] Armbrust M, Fox A, Griffith R. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, February 2009.

[2] Seshadri A, Luk M, Qu N, Perrig A. Secvisor: a tiny hypervisor to provide life time kernel code integrity for commodity oses. In SOSP'07: Proceedings of twenty first ACM SIGOPS symposium on operating systems principles, ACM, New York, NY, USA, 2007. p. 335–50

[3] Jianxin Li , Bo Li, Tianyu Wo, Chunming Hu, Jinpeng Huai, Lu Liu , K.P. Lam,CyberGuarder : A virtualization security assurance architecture for green cloud computing, Future Generation Computer Systems,Elsevier, 11 May 2011,PP.379-390

[4] Payne BD, Carbone M, Sharif M, Lee W. Lares: An architecture for secure active monitoring using virtualization. In SP '08: Proceedings of the 2008 IEEE symposium on security and privacy (sp2008), IEEE Computer Society, Washington, DC, USA, 2008. pp. 233-47

[5] Lombardi F, Di Pietro R. Kvmsec: a security extension for linux kernel virtual machines Proceedings of the 2009 ACM symposium on applied Computing, ACM, New York, , NY, USA, 2009. pp. 2029–34

[6] Dimitrios Zissis, DimitriosLekkas, Addressing cloud computing security issues,Future Generation Computer Systems (2011), pp-583-592

[7] Lombardi F, Di Pietro R. Transparent security for cloud. In SAC'10: Proceedings of the 2010 ACM symposium on applied computing

[8] Marc Fouquet , Heiko Niedermayer , Georg Carle , Cloud Computing for the Masses, , U-NET'09, December 1, 2009, Rome, Italy copy right 2009 ACM

[9] Marc Fouquet , Heiko Niedermayer , Georg Carle , Cloud Computing for the Masses, , U-NET'09, December 1, 2009, Rome, Italy copy right 2009 ACM

[10] Niranjana Padmanabhan,Bijolin Edwin E,An Architecture for providing security for cloud resources,International Journal of Computer Applications, 2011; pp. 34-37