International Journal of Hybrid Information Technology
Vol.8, No.2 (2015), pp.237-246
http://dx.doi.org/10.14257/ijhit.2015.8.2.22

Virtualization Security: Analysis and Open Challenges

Muhammad Arif [1,2] and Haroon Shakeel[2],

[1]*Faculty of Computer Science and Information Technology, University of Malaya 50603 Kuala Lumpur, Malaysia*
[2]*Computer Science Department, Comsats Institute of Information and Technology Islamabad Pakistan*
[3]*School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad Pakistan*
arifmuhammad36@siswa.um.edu.my
haroon.shakeel@pral.com.pk

Abstract

Virtualization is a term that refers to the abstraction of computer resources. Virtualization has many applications within any organization. This makes possible virtual storage network and utilizing hardware resources efficiently. Virtualization also makes the foundations of cloud computing services, allowing users to use the hardware as an on-demand service. With all such advantages, there are also some security and privacy issues for utilizing any form of virtualization. The aim of this survey is to highlight such threats and techniques to solve these issues.

Keywords: *Virtualization Security; Survey on Virtualization; Virtualization privacy*

1. Introduction

Virtualization is creation of virtual environment of something such as hardware platform, operating system, storage, processing power, memory or network resource. While a physical computer in the classical sense is a complete actual machine.

Virtualization can deliver many benefits by providing abstraction of computer resources by inclusion of software abstraction layer. Virtualized computing environment gives the capability to the host operating systems to run multiple operating systems over same physical computer [1]. There are various applications of virtualization in the field of cloud computing, high performance computing. Scalability and efficient resource utilization could be achieved through virtualization technologies [2]. Main benefit of virtual environment is resource sharing. In non-virtualized environment, physical machine or parent machine uses all the resources but in case of virtual environment, all the resources are shared among multiple guest virtual machines. However, this must be made possible with isolation, which is the ability of a VM to isolate data from other VMs, which is programs running in one machine cannot see programs running on second VM [17]. Virtualization security means that virtual machine running over physical servers must be isolated from each other and shouldn't interfere in any of the neighbors working space. There exist vulnerabilities in Virtual machine monitors which might give access to the malicious user to gain privileges. Perfect isolation between multiple virtual machines must be achieved for enhanced security.

Guest OS and host OS are two main concepts explained in context of virtualization. Virtual machine monitor provides virtualization layer, performs process scheduling, I/O Management, process scheduling and network management [3]. By exploiting the strength of

ISSN: 1738-9968 IJHIT

virtualization, cloud computing provides various services such as Software as a Service, Infrastructure as a service and platform as a service [4]. There are various approaches to virtualization such as Operating system-based virtualization, Application-based virtualization, and Hypervisor-based virtualization explaining the ways how VM is being controlled [5]. Security threats has been emerged while rapid development of cloud computing. Information security becomes vital part of cloud computing and virtualization environment. Security issues of virtualizations are widely being addressed because of the popularity of the concept of cloud computing thus virtualization security becoming an important research area [6].

As explained earlier, cloud computing moves the applications and data to a data center. That data center offers various services for hosting application and data on their servers at cost relatively economical to maintaining own servers. Being an evolving field, cloud computing is still exposed by various threats compromising the confidentiality, integrity and authentication of data kept in cloud environment. Cloud computing offer its services in three main areas which are software as a service (Saas), platform as a service (PaaS) and Infrastructure as a service (IaaS). All of these service models require security mechanism in place to provide reliable services to the end user.

2. Virtualization Models

In normal circumstances, computing resources are utilized for very less time period and most of percentage of these resources remains free. Virtualization intends to utilize all available resources efficiently and effectively keeping computing machine as busy as possible. Virtualization also forms the basis of cloud computing where each user is assigned his own virtual resources to work on, isolated from other users from a pool of virtualized computer resources [12]. There are two forms of virtualization server implementation. One is that a hypervisor is installed on a host operating system and then guest operating systems are installed on that hypervisor. This guest operating system interacts with hypervisor, hypervisor interacts with host operating system and host operating system communicates with hardware. Hypervisor cannot directly communicate with hardware. Top layer have less privileges as compared to bottom layer i.e. guest operating system is less privileged then hypervisor and hypervisor is less privileged from host operating system. VMware workstation is an example of such environment [9].

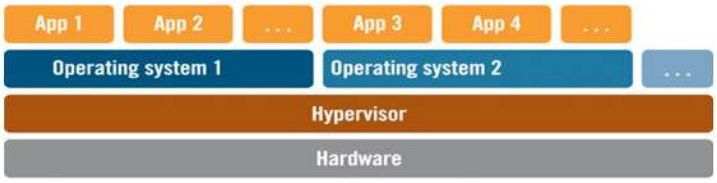

Figure 1. Type 1 Hypervisor

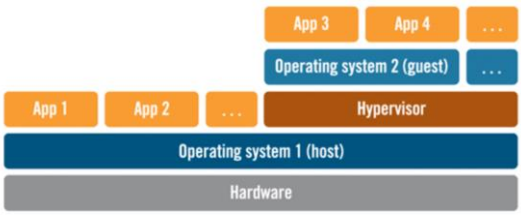

Figure 2. Type 2 Hypervisor

Other form of virtualization implementation is to implement hypervisor and Virtual Machine Monitor directly on hardware and then install guest operating system on that hypervisor. VMM intercepts all the requests from guest operating systems and provide necessary response by communicating with hardware and provides resources as requested by virtual machines. VMM is responsible for isolation and resource management between virtual machines implemented [11]. Figures 1 & 2 illustrate both types of hypervisors.

Enterprises across various sectors are eager to adopt cloud services to accelerate their business. For the protection of their critical information and data, organizations need to examine the security issues of cloud services critically. Although, security of corporate data over cloud is not guaranteed but it's not impossible. Every service model has its own security issues and needs to be dealt carefully.

Software as a service also known as on-demand software is a software deployment model in which software and data are being hosted over cloud. SaaS reduces cost by offering operational efficiency and various significant benefits. Although SaaS is quite emerging delivery model in cloud computing and efficiently meets the needs for enterprises but still it lacks transparency in storage of enterprise sensitive application and data. Security concerns in Saas become the challenging question for cloud service providers. Vendors must address the issues of data confidentiality, integrity and authenticity of data to gain confidence of the enterprise management for using cloud services.

IaaS provides virtual machines along with other resources as a service to the customer. Instead of spending amount over servers, data centers and maintaining them, this whole of the resources are being offered by cloud service provider to the customer for nominal cost. Scaling and infrastructure growth is no more an issue for enterprise after having IaaS. Motivation behind IaaS is to enable business focused over there competencies instead of worrying about infrastructure management. Despite the services being offered by IaaS delivery model, it only provides basic security services such as firewall, load balancing etc. Security measures in Iaas must be concrete so that intruders and malicious programs could not take control of the cloud infrastructure and putting enterprise sensitive information and data in jeopardy.

One layer above over Iaas, computational platform and integrated development environment is being provided in a service delivery model names as Platform as a Service PaaS. Software development life cycle, design and development of application and testing are type of services provided via paas. Being helpful for the programmers and software developer, Paas also give some advantage to hacker to leverage the Paas delivery model and run malicious programs to gain control over the application running over PaaS [8].

3. Threats in Virtualization

Any forms of above discussed virtualization implementation create some security and privacy concerns. As suggested in [9] traditional Virtual Machine Monitors (VMM) and operating systems cannot handle virus infection threats and not even infamous Linux's Mandatory Access Control (MAC) can meet security requirements of different application. When virtualization is implemented for a storage area network (SAN), it is most likely to transfer security threats like Trojans, viruses and malicious codes across the storage area network because every host is required to install virtualization client to provide a uniform platform and communication between heterogeneous systems and operating systems, making it vulnerable for malicious software, viruses and Trojans to infiltrate [10]. However, some threats can be avoided by splitting features and functionalities among different VMMs running on different systems [15].

Cloud computing has changed the way enterprises use to think about data handling, infrastructure development, platform maintenance, developing and maintaining data centers. Now everything is being treated as a service for which companies give away quite economical budget as compared to developing and maintaining the required services at their own premises. One of the major concerns of enterprise is data security. In cloud environment, they are giving away their sensitive applications and data to be taken care of by cloud service provider. Hackers and malicious intruders can exploit their breach in deployment models of service provider and putting endangers sensitive information and data of enterprises. Cross side scripting, cookie manipulation, SQL injection, insecure configuration and storage and various other kinds of attacks could be made possible by malicious users.

Networks over which data, application and information is transferred from enterprise to cloud service provider end is prone to attacks if not well protected. Hacker can sniff networks, penetrate the network, exploit weakness in the network or find an insure connection. Encryption technique, Secure socket layer and Transport layer security is normally used to transmit data over network.

Integrity of the data is quite important aspect, which should be taken care of while transferring to cloud environment. Developers and database designer makes sure that they conforms to the ACID property of databases (atomic, consistency, isolation, transaction). There exist multiple databases in cloud environment and lack of integrity control would result in serious loss of important information and data of enterprise.

Existence of data over same environment from multiple users poses serious threat. Loophole in the application of one user could give a way to intruder, thus comprising the application and databases residing at the same server. Employees databases and records are usually kept using LDAP servers protected by firewall but this is not normally the case with cloud service provider where such data is being kept outside the corporate firewall. For any data given to cloud service provider, enterprise should make sure the confidentiality of the data they are going to host over cloud. Enterprise should check with the cloud service provider, how they are protecting the confidently of data being hosted at their environment.

When virtualization is used for providing pool of cloud computing services, there is a threat to virtual machines from external hackers as well as clients do not trust the cloud computing provider administrator for the security and privacy of their data on the virtual machines created on that cloud [11]. Ideas addressing the security of virtual machines work under assumption that client will always trust the cloud computing services provider for the privacy of his data but reality is opposite [12]. An administrator of virtual host can view VMs running inside that host, can monitor applications inside VMs, can start, pause or restart the VM. In this case even administrator of cloud computing service provider is not able to be trusted [18]. Therefore, there is need of research for security and privacy protection in virtual environments, no matter if they are implemented for experiments on workstations, for centralized storage area network in organization or for cloud computing. End user is also in fear of loss of control over its VM or important data. The user does not aware of where his data or VM is stored and processed in the cloud. Data is usually mobile over cloud i.e it can be migrated from one server to another, which can expose it for hacking from outside source [20].

Existing kernel integrity-checking mechanisms work under certain assumptions. For example assumption that guest system is clean when it starts being monitored but reality is that a VM can be created already infected by any virus or can be compromised by any malicious code. It is assumed that guest OS is known in priori but reality is that VMs can be

created using any one or multiple OS configurations. So there is a need of an architecture, which avoids as many assumptions as possible [19].

Table: 1. Virtualization Threats

Source	Explanation
NW → VMM	Attack from outside the network to VMM
NW → VM	Attack from outside the network to guest VM
VMM → VM	Threat from VMM attacks to VM
VM → VM	Threat from one VM to another VM
Admin → VMM	Cloud service providor admin threat to VMM
Admin → VM	Cloud service provder admin threat to VM

4. Solution to Threats

As discussed earlier, there is always a security threat to a virtual machine of virus and Trojan attacks no matter if that virtual machine is configured in desktop environment or at cloud computing. On solution to this threat is provided by [9] by suggesting that a second level virtual machine monitor or SeVMM should be used which acts as security control mechanism for virtual resources like network or virtual processor and inter-domain communication should also be monitored by this new layer (SeVMM) based on isolation capability of Vkernel. This will provide strong isolation between multiple machines, control and management of virtual resources and inter-domain communication. This new virtual layer is also responsible for deploying security policies automatically and also support multiple security policies to be implemented for enhanced flexibility. It supports multiple security policies and models such as Bell–LaPadula model (BLP), CW and TE and to configure security a strategy, Flask Framework is used which is a micro framework for Python [14]. SeVMM takes control of all security policy making and implementation from traditional VMM by intercepting all security related calls between guest and host operating system. It has three modules. Security policy management module to manage and update security policies as needed. Safety hook for controlling the sharing of virtual resources among multiple VMs by taking some information about virtual machines like attributes of virtual resources, types of operations etc. and then passes these information to third module called Security policies enforcement module which makes decisions based on the security information provided by the safety hook. Fig. 3 illustrates its architecture. This technique was quite successful and performed well on the System Call Delay benchmark Test, First-in-First-out communication delay benchmark test [9]. However, as compared to traditional Virtual Machine Monitors, it has performance penalty on overall performance of the system at the rate of 5%. It is tradeoff between performance of the host and security of the virtual machines on that host.

Benefits of virtualization are also being reaped in Storage Area Network (SAN). Traditional SAN had limitations like no support for heterogeneous environment. So here virtualization plays the role to make Storage Virtualization Network in which each server must install a virtualization client and provide one storage area based on heterogeneous hardware. That client opens a door for virus and malicious software attacks. System Administrators cannot know whether booting such network was secure or not. So a model is introduced based on trusted computing [10]. It takes into account that how a particular devices is expected to behave for a specific purpose and then builds a trusted computing platform (TCP). In this TCP, a trusted root is built whose security trust is ensured by physical security. Then from that root, a trust chain is built to hardware, from hardware to operating

system, from operating system to application in a manner that higher level is authenticated by the lower level extended to entire computer system making a trusted computing platform. Out-of-band virtualization controller is used to scan for any factor that might do harm to SAN and then built TCP. This platform is built before all the servers accessing Virtual Storage Network boot up.

Out of band virtualization controller is a computer which will connect to all the servers as soon as it powers on and then makes trusted measurements. First of all it ensures a trusted booting process of virtual controller by establishing trusted root and notes that booting process behaved as expected. It is done before the OS kernel is loaded because otherwise it would have already been communicated with servers so we cannot be sure whether its trusted or not. On second stage, it executes Network Self-recognition Model which is embedded in the virtualization controller and can scan the storage network and protect it against viruses and other malicious codes. Although this model has higher performance and scalability, but it delays overall boot up time of whole virtual storage network.

By utilizing virtualization, cloud computing can provide its users dynamically shared and scalable resources over internet. However, clients are always worried about confidentiality, security threats and loss of their control over their data. So on cloud computing, there is also need of a model that can prevent data theft or other security attacks [11]. Technique proposed by [11] is that the virtual machine of a particular user over cloud computing should be configured in such a way that only a valid user can boot it. Otherwise it cannot be booted hence it is more secure. The architecture is implemented in three parts. In trusted part which includes hardware platform, a trusted bootloader and a XEN Hypervisor. Untrusted part includes dom0 driver because dom0 driver is controlled by cloud computing services providers so it cannot be trusted. Protected part which includes all guest VM environment. This technique also involves making a Trusted Platform Module which ensures authenticated booting, secure I/O and secure storage. Input/output memory management unit (IOMMU) prevents dom0 device drivers and to prevent dom0 driver from hacking into guest VM, VM-kernel is modified in such a way that mouse, VGA console, frame buffer, keyboard, serial port and sound is disabled for local use. ACPI and kernel debugging is disabled to prevent hacking into kernel by any means. For each guest VM, encryption is enabled to protect virtual disks and all drivers are removed except of those which are necessary to keep the guest VM running. To ensure that only a valid user boots up the guest VM, user needs to prepare two disk images at the time of creation of VM. One disk image is called root disk image which contains password file for the user and other image is called boot disk image which contains password file for booting the VM. Both images are encrypted and uploaded to dom0 driver on the cloud server. To boot the VM, client sends request to dom0 driver, which launches the guest VM and grub bootloader loads the encrypted kernel. Kernel executes kernel wrapping code that executes a hypercall asking hypervisor to decrypt the images. Hypervisor asks for public key for decrypting the password boot file. User provides the key and hypervisor decrypts it and transfers the control to VM. After kernel is loaded, user password image is executed and again it asks user to provide decryption key to decrypt the image to obtain user password. User provides and then this user password file is used to mount encrypted file system. Now the host operating system starts. In this whole process, dom0 only sees encrypted images and passwords making it impossible to hack. Evaluation shows that this model performs well in terms of system confidentiality, memory isolation, storage protection, network protection, guest VM boot process security and virtual devices control.

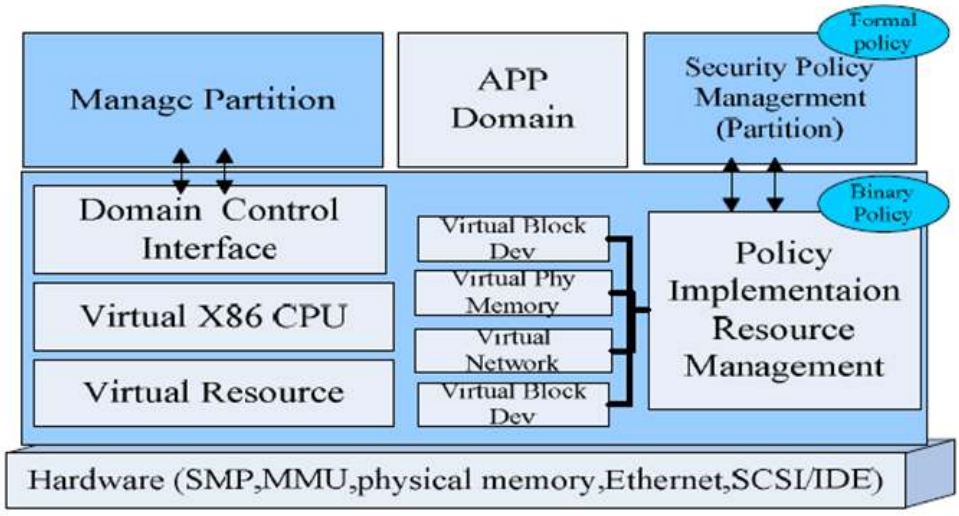

Figure 1. Architecture of SeVMM

To secure a VM in cloud computing from cloud computing service provider administrators, there is another technique proposed by [12]. Administrators can access a virtual machine by using dom0 driver. The idea is to seal system boot to dom0 driver by using TPM hardware. It mainly involves securing all steps involved in booting up guest virtual machine by encryption or moving certain drivers to safe location. The idea and implementation is similar to [10]. It is supposed that hardware and hypervisor is trusted but dom0 is not because it can be used by cloud computing service providers to access the VM, it can destroy or create VMs, they can access the memory being used by virtual machines, can access contents of virtual disk and can monitor all network packets. To secure system boot, a chain of trust is developed from bios to bootloader and from bootloader to hypervisor. Bios is enhanced with a core root of trust management (CRTM), which will be the first instance of boot process, then bios loads and after that bootloader of the system. To secure DMA, I/O memory management units are used to isolate and restrict device access to assigned resource. Hypervisor is responsible to restrict DMA from an I/O device to physical memory owned by dom0, by using DMA remapping hardware. To provide Trusted Computing Functionality (TCF), a software instance Virtual TPM is created at the time of creation of VM and is associated with that guest VM. Kernel and initrd are encrypted using a secret key by user, then kernel is wrapped using a wrapper code which involves only a hyper call which asks hypervisor to decrypt the kernel and intird images. User first attest cloud server, if succeeds sends boot request to dom0 and guest VM is booted. Then the guest VM executes wrapping code to decrypt the kernel and initrd images. But there is another issue that an administrator can suspend a virtual machine and during that period, memory used by guest VM is totally exposed to dom0. To make this memory inaccessible to dom0, page based encryption method is used in which a secret key is used by KVMM to encrypt all the pages. Before decryptions of these pages, hash is checked to detect any temper to saved image. This way data privacy and integrity is protected. However there is a drawback of this approach. While suspending the VM, encryption and decryption is involved, this makes the save/restore process slower. So more the memory allocated to a virtual machine, more extra overhead would be. Fig. 4 illustrates overall architecture of this technique of securing confidentiality of cloud computing service client.

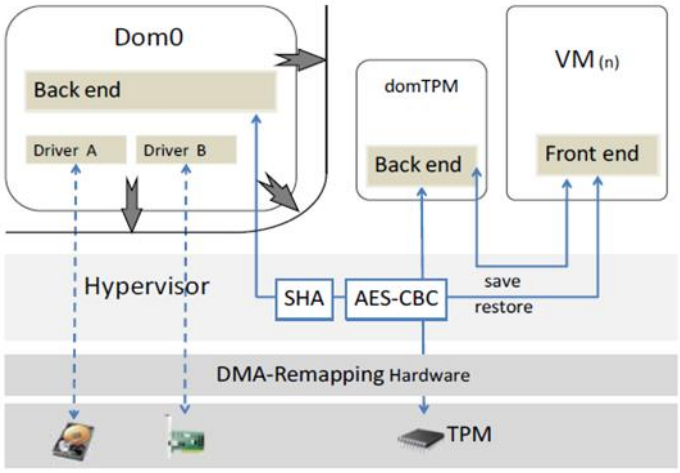

Figure 2. Securing VM against Untrusted Host

VMMs are implemented using software based approach to implement security mechanisms and hardware based approach for performance. If VMM is implemented in software based approach, it cannot be switched to hardware based approach and if it is implemented using hardware based approach, security benefits of software based approach cannot be obtained. Reference [13] proposes a technique which utilizes benefits of both software emulated (QEMU) security and hardware based (KVM) performance. Hybrid VMM switches dynamically between QEMU and KVM. QEMU supplies security and reliability to a critical software while KVM supplies performance to a performance critical software. To enable switching between these two methods, code of QEMU and KVM is modified. To switch from KVM and QEMU, para-virtualization mechanism of Linux kernel is disabled which is detects whether KVM exists or not, so it needs to be disabled in order to switch from KVM. In proposed system, the return string that detects KVM using CPUID, is changed such that KVM does not exist. Then a converted is implemented that converts processor register values of KVM to be used by QEMU because QEMU is unable to use processor state of KVM. Thirdly and arbitration mechanism is implemented for working threads of KVM and these KVM-managing threads manage all QEMU interfaces.

Now switching from QEMU to KVM is done by converting QEMU state to KVM by modifying the flag of the code segment register and flag of the task state segment register. Then execution path of QEMU is modified which detects hooks in blocks and hybrid VMM escapes from execution loop of QEMU and start switching from QEMU to KVM. Then re-initialization module of KVM kernel module is added. Hooking is done by using conventional OS switching mechanism.

Table 2. Techniques to Handle Security Threats

Technique	Advantages	Disadvantages
Using additional virtual layer for security (SeVMM)	flexible security	Performance penalty on host
Security based on TCM	Higher performance and scalibility	Virtual Storage Network boot time delay
Integrating amiddleware and encrypting boot process	Certain security and confidentiality	Technical complexities at user end
Sealing system to dom0	Data confidentiality	Encryption and decryption overhead proportional to memory allocated to VM
Hybrid of software emulated	No significant modification in	Switching overhead between VMMs

security and virtualizatoin support of CPU for performance	existing security mechanism. No modification to guest OS.	increase as system gets busier.

5. Conclusion and Recommendations

In this survey, we found that virtualization technology have been very beneficial in terms of maximum resource utilization, providing services over cloud or providing a virtual storage space enabling heterogeneous storage networks. However, there are certain security concerns to consider. If one hypervisor is compromised in a virtual environment, it is possible that it will try to hack into its underlying virtual machines or will threaten the security of other hypervisors in the network. On the other hand, if we look virtualization implementation over cloud computing, hackers are always looking to hack into cloud computing servers. Secondly, cloud computing service users also feel unsecure to put all their important data in a VM that is hosted on a cloud and cloud computing service administrator have full access to that VM.

Virtualization technology, its applications and service models discussed earlier are need for every enterprise nowadays. Scalability and infrastructure growth is no more an issue within an economical budget. With all the usefulness cloud computing and virtualization service models offers, service providers have to take precautionary measures and implement security mechanisms for the protection of sensitive business information, application and data. Service providers could only attract businesses and enterprises towards cloud environment only if they are able to build their trust in the offered services. We have discussed various threats to the cloud environment and there solutions in context of virtualization security and conclude that security in general should be an integral part of virtualization infrastructure.

Techniques to solve these problems are reviewed. We have found that no matter what technique you choose to get extra security and privacy as compared to traditional OS and VMM, you have to tradeoff in terms of performance or technical complexities. However, technique having more technical complexities is recommended because a user will learn it eventually and will understand its benefits. But performance penalty such as switching overhead in hybrid VMM cannot be tolerated because busier the system will be, more switching overhead it will cause, making its guest VMs becomes slower, which kills the objective of a virtual environment i.e. maximum utilization of computational resources for productive use.

References

[1] T. Brooks, C. Caicedo and J. Park, "Security Challenges and Countermeasures for Trusted Virtualized Computing Environments" School of Information Studies (iSchool) Syracuse University, Syracuse, NY, USA, World Congress on Internet Security (WorldCIS) (**2012**).

[2] Y.-L. Huang, B. Chen, M.-W. Shih and C.-Y. Lai, "Security Impacts of Virtualization on a Network Testbed", Department of Electrical and Computer Engineering, National Chiao-Tung University, Hsinchu, Taiwan, IEEE Sixth International Conference on Software Security and Reliability (**2012**).

[3] Q. Chen, R. Mehrotra, A. Dubeyy, S. Abdelwahed and K. Rowland, "On State of The Art in Virtual Machine Security", Electrical and Computer Engineering, Mississippi State University, Miss. State, MS Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN, US Army Engineer Research and Development Center, Vicksburg, (**2012**).

[4] S. Luo, Z. Lin, X. Chen, Z. Yang and J. Chen, "Virtualization security for cloud computing service," ZTE Corporation, Shenzhen, China, Dept. of Computer Science and Technology, Shenzhen University, Shenzhen, China. International Conference on Cloud and Service Computing (**2011**).

[5] F. Wen and L. xiang, "The Study on Data Security in Cloud Computing based on Virtualization", Chongqing College of Electronic Engineering (**2011**).

[6] X. Luo, L. Yang, L. Ma, S. Chu and H. Dai, "Virtualization Security Risks and Solutions of Cloud Computing Via Divide-Conquer Strategy", 1. China Electronic System Engineering Institute, Beijing 100141,

China; 2. Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, China Third International Conference on Multimedia Information Networking and Security, (**2011**).
[7] F. Sabahi, "Virtualization-Level Security in Cloud Computing", Faculty of Computer Engineering Azad University Iran (**2011**).
[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Anna University Tirunelveli, Tirunelveli, TN 627007, India, Journal of Network and Computer Applications, July (**2010**).
[9] W.-z. Chen, H.-w. Zhu and H. Wei, "SeVMM: VMM-based Security control Model", International Conference on Cyberworlds, (**2008**).
[10] Q. Zhang, Y. Wu, D. Cui and Z. Dang, "Research on the Security of Storage Virtualization Based on Trusted Computing", International Conference on Networking and Digital Society, (**2010**).
[11] J. Kong, "A Practical Approach to Improve the Data Privacy of Virtual Machines", 10th IEEE International Conference on Computer and Information Technology, (**2010**).
[12] J. Kong, "Protecting the Confidentiality of Virtual Machines against Untrusted Host", International Symposium on Intelligence Information Processing and Trusted Computing, (**2010**).
[13] J. Sawazaki, T. Maeda and A. Yonezawa, "Implementing a Hybrid Virtual Machine Monitor for Flexible and Efficient Security Mechanisms", Pacific Rim International Symposium on Dependable Computing, (**2010**).
[14] http://flask.pocoo.org/
[15] A. V. Cleef, W. Pieters and R. Wieringa, "Security Implications of Virtualization: A Literature Study", International Conference on Computational Science and Engineering, (**2009**).
[16] D. Ramalingam and A. N. Shivashankarappa, "Effective Server Virtualization with Enchanced Security Strategy for Large Organization", World Congress on Internet Security, (**2011**).
[17] S. Mohapatra, J. Sahoo and R. Lath, "Virtualization" A Survey on Concepts, Taxonomy and Associated Security Issues", Second International Conference on Computer and Network Technology, (**2010**).
[18] N. Patra, J. Sahoo, S. Mahapatra and S. Pati Prasanna, "A Security Framework for Virtualization based Computing Environment", International Journal of Engineering Science and Technology, vol. 3, August (**2011**).
[19] M. Christodorescu, R. Sailer, D. Lee Schales, D. Sgandurra and D. Zamboni, "Cloud Security is Not (Just) Virtualization Security", Proceedings of the 2009 ACM Workshop on Cloud Computing Security, (**2009**).
[20] F. Lombardi and R. Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, (**2010**).

Authors

Muhammad Arif, he is a PhD student at Faculty of CS and IT, University of Malaya. Currently he is working on Medical image Processing. His research interests include image processing, E learning, Artificial intelligence and data mining. He joined UM as a Bright Spark Scholar in September 2013 for the period of 3 years. Before this he completed masters and bachelor degrees in Pakistan. He received his BS degree in Computer Science from University of Sargodha, Pakistan in 2011. He obtained his MS degree in Computer Science from COMSATS Islamabad 2013 Pakistan.

