Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures

Sarfraz Nawaz Brohi, Mervat Adib Bamiah
Universiti Teknologi Malaysia, Malaysia
nbsarfraz2@live.utm.my, abmervat3@live.utm.my

Muhammad Nawaz Brohi, Rukshanda Kamran
Preston University Ajman, UAE
mnbrohi@preston.ae, ruks.faculty@preston.ae

***Abstract*— A multi-tenant Cloud Computing Infrastructure (CCI) consists of several Virtual Machines (VMs) running on same physical platform by using virtualization techniques. The VMs are monitored and managed by kernel based software i.e. Virtual Machine Monitor (VMM) or hypervisor which is main component of Virtualized Cloud Computing Infrastructure (VCCI). Due to software based vulnerabilities, VMMs are compromised to security attacks that may take place from inside or outside attackers. In order to formulate a secure VCCI, VMM must be protected by implementing strong security tools and techniques such as Encryption and Key Management (EKM), Access Control Mechanisms (ACMs), Intrusion Detection Tools (IDTs), Virtual Trusted Platform Module (vTPM), Virtual Firewalls (VFs) and Trusted Virtual Domains (TVDs). In this research paper we describe the techniques of virtualizing a CCI, types of attacks on VCCI, vulnerabilities of VMMs and we critically describe the significance of security tools and techniques for securing a VCCI.**

***Keywords*— Virtualization, Virtual Machine Monitor, Attacks and Vulnerabilities, Security Tools and Techniques**

I. Introduction

Considering the reduction in global warming cloud computing is moving towards the platform of virtualization [1]. Under this technique hardware or software resources such as memory, CPU, storage, network are logically portioned and provided to multiple tenants. However virtualization is complex and has a considerable attack surface. It is prone to bugs and vulnerabilities [2]. The applications of clients are running on VMs residing on VCCI. Since the VMs are not permitted to access the underlying physical hardware directly, hypervisor or VMM is used to manage, monitor and isolate VMs from each other and the host OS [3]. One of the primary benefits that virtualization brings is isolation. This benefit, if not carefully deployed will become a threat to the operating environment [4]. However, Cloud Service Providers (CSPs) undertake a substantial effort to secure their systems in order to minimize the threats to infrastructure but still hypervisors has flaws of weak security isolation [5]. If an attacker is able to gain access over the hypervisor, whole service could be at risk and all the VMs running over the hypervisor would be compromised [6-7]. Due to inappropriate security standards used for hypervisors at infrastructure level, there are security gaps that can be exploited by the inside or outside malicious attackers to misuse the infrastructure [8]. Since public cloud provides open global accesses to heterogeneous clients, confidentiality, integrity, security, availability, authenticity and privacy are essential concerns for both CSP and clients as well. Security and privacy are the most significant challenges that may impede the cloud computing adoption. Violating the security of any component will impact the other components consequently the security of the entire system will collapse [3]. CCI must be secure at each layer such as physical, network, virtualization and application layers. However, the focus of this research paper is to identify and analyze the security issues and threats only on VCCI.

II. Virtualizing The Cloud Computing Infrastructure

The adoption of virtualization in cloud computing brought up several advantages compared to traditional computing infrastructure where one resource was allocated to a single VM at a time [9]. The clients are interacting with the physical infrastructure by accessing their applications on their personal VMs running on a hypervisor as shown in Fig.1 [9].

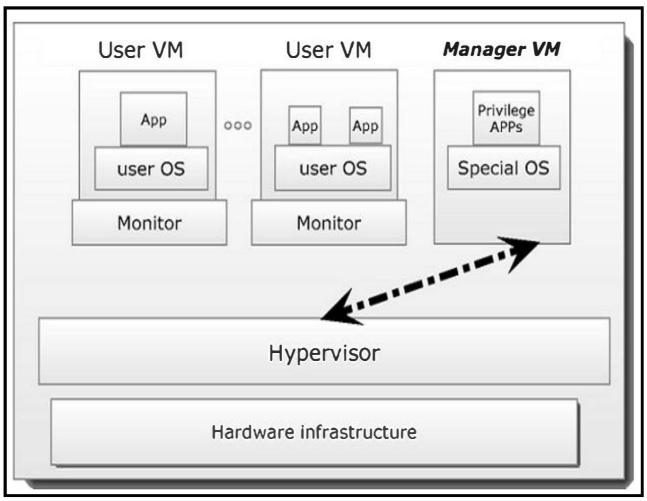

Figure 1. Cloud Virtualization [9]

Since a VCCI consists of numerous clients VMs that, are controlled by VMM to ensure fair scheduling, memory and resource allocation etc. The VMM itself is running on the physical infrastructure by utilizing the host OS [10]. The VCCI is similar to the OS environment, where multiple processes are running on a single OS which is responsible for monitoring and managing the processes. There are two main types of hypervisors used on a VCCI i.e. Type-1 and Type-2. A Type-1

978-1-4673-4416-6/12/$31.00 ©2012 IEEE

hypervisor runs directly upon the hardware with a separated layer from the host OS. Type-2 hypervisor runs together with the host OS. Due to the isolation from the host OS, the security, performance and scalability features in Type-1 are enhanced than Type-2 [11]. The highly used industry based type-1 and type-2 hypervisor include Xen and KVM respectively.

A. Xen Hypervisor

Xen resides between the VMs and underlying physical hardware. In order to create a secure operating environment, Xen hypervisor divides the VMs into two domains i.e. Domain0 (Dom0) and DomainU (DomU) according to the accessibility privileges. The Dom0 VM has higher privileges and it can access the hardware whereas DomU VMs have lower privileges and cannot directly access the hardware. When Xen hypervisor starts, for the first time it loads Dom0 VM. Normally the user of Dom0 is a system administrator who has privilege to use the hypervisor interface to create, delete or manage any DomU VMs. Each DomU VM contains a modified Linux kernel that includes front-end drivers that communicates with the Xen hypervisor, instead of communicating directly with hardware. For each DomU VM, CPU and memory access operations are handled directly by the Xen hypervisor. However, I/O is directed to Dom0 since Xen hypervisor itself is not able to perform any I/O operation [12].

B. Kernel Virtual Machine (KVM) Hypervisor

KVM is developed by implementing Linux kernel module with enhanced hypervisor functionalities. Each Linux process has two modes of execution, user and kernel mode. The user mode is considered as unprivileged while kernel mode is considered as privileged process. The default mode for a process is user mode. It changes to the kernel mode when it requires some sort of services from kernel such as request for writing to hard disk. While implementing the KVM, the developers added a third mode for process, called as guest mode. The guest mode itself has two normal modes user and kernel, can be called as guest-user and guest-kernel mode. When a guest process is executing non-I/O guest code, it will run in guest-user mode. In guest-kernel mode, the process handles exits from guest-user mode due to I/O or other special instructions. In user mode, the Linux process performs I/O on behalf of a guest. In the KVM model each guest VM is implemented as a simple Linux process and that process itself is able to run multiple applications concurrently because it is acting as a virtual OS [13]. Each VM is scheduled by standard Linux scheduler.

III. ATTACKS ON VCCI AND VULNERABILITIES OF VMMS

Due to inappropriate security standards used for hypervisors at infrastructure level, there are several security gaps that can be exploited by the inside or outside malicious attackers to misuse the infrastructure as shown in Fig. 2 [8].

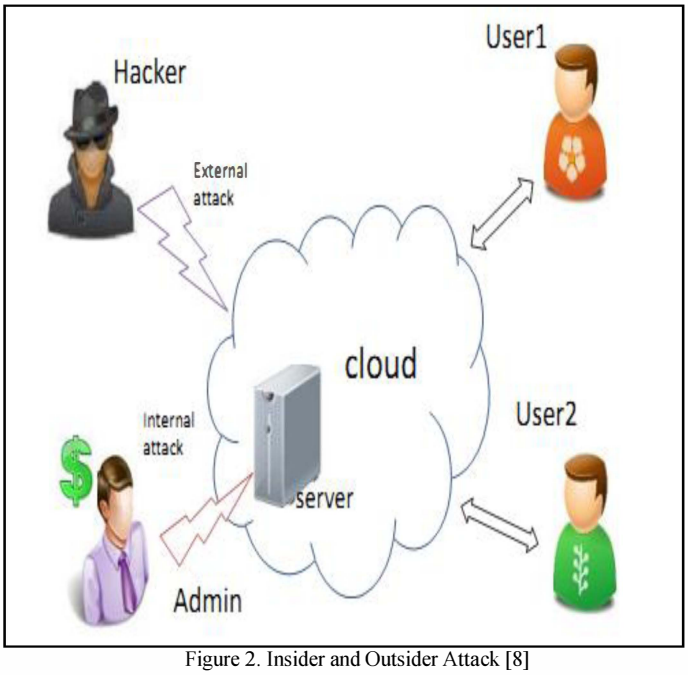

Figure 2. Insider and Outsider Attack [8]

Attack on any component of VCCI may affect the others. In order to overcome this issue, the infrastructure needs to be secured by implementing security tools and techniques that isolates the VMM, guest/ host OS and physical hardware from the side-effects of each other. [2] Identified two major attacks on VCCI (VM to VM and VM to Hypervisor) as shown in Fig. 3 [2].

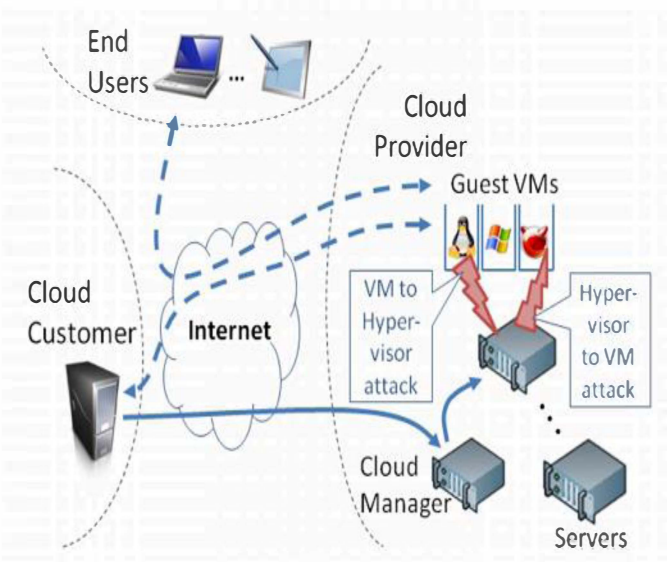

Figure 3. Attack Surface [2]

The attacks visualized in Fig.3 can take place due to three major vulnerabilities (VM hopping, VM escape and VM mobility) identified in hypervisors [7] [4].

A. VM Hopping

When several VMs are running on the same host OS, a malicious attacker such as remote un-trusted cloud user on one VM can obtain the access of other VM just by knowing its IP address. Once a VM is attacked, the attacker can monitor the traffic going over the VM and change the flow of traffic or manipulate it. This attack can create a major issue of Denial of Service (DOS) that is actually an attempt to make a computer resource unavailable to its intended users [4]. If VM is running since a long time, an attacker can modify the configuration file such that VM goes off state. Therefore the ongoing communication to that VM could be stopped. When the connection is resumed, the VM needs to start the entire communication again [7].

B. VM Escape

This vulnerability allows a guest-level VM to attack its host. Under this an attacker such as an un-trusted user of cloud services can run a code on a VM that allows an OS running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker access to the host OS and all other VMs running on that host [4]. If an attacker gains access to the host running multiple VMs, he/she can access the resources which are shared by the other VMs. The host can monitor the memory being allocated and the CPU utilization. If necessary an attacker can bring down these resources and turn off the hypervisor and if the hypervisor fails, all the other VMs turn off eventually [7].

C. VM Mobility

Under a VCCI, VMs can move from one physical host to another is called as VM mobility. However, VM mobility can be risky for security attacks, VM files can be stolen without physical theft of the host machine [3]. VMs can be moved over the Network or copied through a USB. Since VM are not essentially present on the physical machine, the threat for an attack increases. The contents of the VM are stored in a file on the hypervisor. If the VM is moved to another location, then the virtual disk is also recreated and an attacker can then modify the source configuration file and alter the VMs activities. VM can also be compromised if the VM is offline. An attacker can modify the configuration file of the VM. Gaining access to the virtual disk, attacker has sufficient time to break in all the security measure such as passwords, important credentials, etc. Since this VM is a copy of the actual VM, it is difficult to trace the attacker with this threat [7]. This attack is normally caused by a malicious cloud administrator.

IV. Security Tools and Techniques for Securing the Virtualized Cloud Computing Infrastructure

There are numerous security tools and techniques available to overcome the malicious threats on VCCI and hypervisor vulnerabilities. During our analysis, we have identified some major approaches for securing a VCCI by reviewing the past and present literature. These include EKM, ACMs, IDTs, vTPM, VFs and TVDs. The significances of these techniques to secure a VCCI are described as follows:

A. Encryption and Key Management (EKM)

The protection of data against the loss and theft is a shared responsibility of cloud customer and CSP. Nowadays, encryption is one of the strongly recommended techniques in cloud Service Level Agreements (SLAs) [26]. The confidential data of customer must be encrypted at three different stages i.e. encryption of data- at- rest (encrypting the customer's data on disk storage as cipher text that will protect the data from malicious CSP and illegal use), encryption of data-at-transit (encrypting the confidential information such as credit cards while transmitting over a network) and encryption of data on backup media such as external or internal storages, this can protect against misuse of lost or stolen media [14]. However, encryption only is not enough to keep the data secure, there must be proper key management practices to ensure the safe and legal access of encryption keys. For-instance encryption keys must be protected same as sensitive data itself and these keys should be accessed only by limited and authorized personalities and proper procedures must be followed if encryption keys are lost or stolen [14]. It is the customer's responsibility to enforce the use of encryption and key management in their SLAs. However, type of encryption technique used depends upon the requirements and objectives. The common encryption methods that can be used on VCCI include symmetric and asymmetric algorithms. From symmetric cryptography family, Triple Data Encryption Algorithm (TDEA) also known as Triple-DES or (3DES) and Advanced Encryption Standard (AES) are most common types of encryption techniques. These types of encryption and decryption process use a secret key. From asymmetric cryptography, RSA and Elliptic Curve Cryptography (ECC) are mostly used encryption techniques, unlike symmetric these methods uses two different keys, a public key for encryption and a private key for decryption [24]. If data encryption practices are followed accurately, the data will be saved from the illegal accesses or theft of a malicious CSP's administrator and remote hackers.

B. Intrusion Detection Tools (IDTs)

The multi-tenant and distributed nature of the cloud makes it an attractive target for potential intruders. Appropriate IDTs should be used at VCCI which continuously collects and analyzes data from a computing system, aiming to detect intrusive actions. There are two main approaches for IDTs i.e. Network-based IDTs (NIDTs) and Host-based IDTs (HIDTs), NIDTs are based on monitoring the network traffic flowing through the systems and examining events as packets of information exchange between computers. While, HIDTs are based on monitoring local activity on a host like processes, network connections, system calls, logs, etc and examining events like what files were accessed and what applications were executed [16]. Both IDTs tools should be used at VCCI to ensure safe and secure operating environment in order to block the intruders.

C. Virtual Firewall (VF)

It is a firewall service running in a virtualized environment which provides usual packet filtering and monitoring services that a physical firewall provides [18]. VFs can execute in various modes typically hypervisor-mode (hypervisor resident) and bride-mode. In order to protect the VMs and VMM, hypervisor-resident VFs must be implemented on the VMM where it is responsible to capture malicious VM activities including packet injections. These VFs require a modification to the physical host hypervisor kernel to install process hooks or modules allowing the VF system access to VM information and direct access to the virtual network switches as well as virtualized network interfaces moving packet traffic between VMs. The hypervisor-resident VF can use the same hooks to then perform all firewall functions like packet inspection, dropping, and forwarding but without actually touching the virtual network at any point. Hypervisor-resident VFs can be faster as compared to bridge-mode VFs because they are not performing packet inspection in VFs, but rather from within the kernel at native hardware speeds [19].

D. Trusted Virtual Domains (TVDs)

A TVD is security technique formed at VCCI by grouping the related VMs running on separate physical machine into a single network domain with a unified security policy. The multiple instances of TVDs co-exist on a single platform under a shared resource policy. The use of TVD provides strong isolation among un-related VMs as the communication among TVDs takes places only according to the security policies defined by administrator configured in the VMM. A malicious VM cannot join any TVD because in order to join TVD, a VM should fulfil the requirements of the policy so no malicious VM can affect the VMs of trusted users on cloud [20]. Normally the VMs residing in a TVD are labeled with a unique identifier. For-instance the VMs of one customer will be labeled differently from the other customer. The labeling is used to identify the assigned VMs to a particular customer and to allow the same labeled VMs to run on inside the same TVD that must be designed by following a proper security guidelines and policies that doesn't exhibit any loop holes.

E. Access Control Mechanisms (ACMs)

ACMs are responsible of protecting of a VCCI by limiting, denying or restricting access to a system or an entity such as processes, VM and VMMs according to the well defined security policies [15]. Most common ACMs used in VCCI include Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these techniques are known as identity based ACMs as user subjects and resources objects are identified by unique names. Identification may be done directly or through roles assigned to the subjects [25]. ACMs guarantees integrity and confidentiality of the resources. Access control must be performed by a trusted party which can be also the CSP or third party in association with the cloud customer. Moreover, the collaboration and the expression of access control at each layer e.g. hypervisor or OS must be achieved in a dedicated and neutral language to allow a unification policy regardless of the layer.

F. Virtual Trusted Platform Module (vTPM)

IBM researchers proposed TPM virtualization that is based on certificate chain linking vTPMs to the physical TPM in order to provide its capabilities and make it available to all VMs running on a platform. vTPMs can be located in a specific layer over the hypervisor. A vTPM instance is created for each VM by vTPM Manager which is built in a specific VM and may invoke its own vTPM through the hypervisor [17]. Each VM has its associated vTPM instance that emulates the TPM functionality to extend the chain of trust from the physical TPM to each vTPM via careful management of signing keys and certificates. A vTPM has its own virtual Endorsement Key (EK) and virtual Storage Root Key (SRK) beside some software on the host. In multi-tenant VCCI the system of vTPM virtualizes a physical TPM to be used by a number of VM on a single hardware platform [23].

V. Implementation of Security Tools and Techniques for Formulating a Secure VCCI

The security tools and techniques discussed in previous section have been implemented by various researchers to design and develop secure VCCI. This section describes some of the valuable contributions by the researchers. [21] designed Trusted Virtual Datacenter (TVDc). The aim of TVDc is to provide a safety net that reduces the risk of security issues that take place by misusing the VMs with the help of malicious software. [22] Proposed a trusted VMM with the use of encryption methods. This technique is referred as CloudVisor. It is implemented as a security monitor that runs in the highest privileged mode even more than the hypervisor. Once the CloudVisor runs then it starts the hypervisor that executes in the least privileges mode. In order to enforce protection and isolation, CloudVisor monitors the use hardware by VMM and VMs. CloudVisor uses security authentication TPM for secure boot-up and encryption of VMs data. [8] Proposed the TVMM by using TPM as root of trust by implementing it on Xen hypervisor. The vTPM provides the isolation security between VMs so no any VMs can access the resources of others. [8] Also proposed a page-based encryption method. This method uses the secret key managed by the hypervisor to encrypt all pages. Encryption uses AES-128 in CBC mode, and hashing uses SHA-256 before the pages are handed over to Dom0. These are few of the valuable contributions however there is tremendous amount of research being carried out by several researchers for securing the VCCI.

VI. Conclusion and Future Work

Multi-tenancy is one of the significant characteristics of cloud computing that refers to the mechanism of sharing a cloud platform and resources to the several clients. In order to achieve the benefits of this technique, cloud computing has moved towards virtualization, where each clients is assigned with one or multiple VMs. Beside the benefits, multi-tenant cloud environments is also vulnerable to attacks that have impede the trust on adopting cloud computing. Attacks have

been identified from outsiders and insiders. The major targeted point for attack on VCCI includes the VMM. In order to secure the VMM, several techniques have been introduced that are implemented by various researchers from academia and industry to secure the VCCI. The adoption of cloud computing is an un-stopping task so the challenge is to formulate a secure CCI. In order to contribute in the field of cloud computing we analyzed the security issues on VCCI, however security is not only limited to virtualization components. A CCI must be secure at various layers physical, network, application, management and organizational layers by considering the governmental policies and SLAs etc. However, the future direction of our research is to conduct an analysis identifying and overcoming the security issues on cloud computing from governance and operational perspectives.

ACKNOWLEDGMENT

We are thankful to God Almighty for giving us the knowledge and wisdom to complete this work. We are also thankful to our parents for their encouraging support.

REFERENCES

[1] Yamini, B. & Selvi, D.V., 2010. Cloud virtualization: A potential way to reduce global warming. *In Recent Advances in Space Technology Services and Climate Change (RSTSCC), 2010.* Recent Advances in Space Technology Services and Climate Change (RSTSCC), 2010. pp. 55–57.

[2] Szefer, J., et al. 2011. Eliminating the hypervisor attack surface for a more secure cloud. *Proceedings of the 18th ACM conference on Computer and communications security. Chicago, Illinois, USA, ACM:* 401-412.

[3] Dawoud, W., Takouna, I. & Meinel, C., 2010. Infrastructure as a service security: Challenges and solutions. In *Informatics and Systems (INFOS), 2010 The 7th International Conference on*. Informatics and Systems (INFOS), 2010. pp. 1–8.

[4] Shengmei, L., et al., 2011. Virtualization security for cloud computing service. In *Cloud and Service Computing (CSC), 2011 International Conference on*. Cloud and Service Computing (CSC), 2011 International Conference on. pp. 174–179.

[5] Takabi, H., Joshi, J.B.D. & Ahn, G., 2010. Security and Privacy Challenges in Cloud Computing Environments. *Security & Privacy*, IEEE, 8(6), pp.24-31.

[6] Wang, Z. & Jiang, X., 2010. HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity. *In Security and Privacy (SP), 2010 IEEE Symposium on*. Security and Privacy (SP), 2010 IEEE Symposium on. pp. 380–395.

[7] Jasti, A., et al. 2010. Security in multi-tenancy cloud. In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*. Security Technology (ICCS T), 2010 IEEE International Carnahan Conference on. pp. 35–41.

[8] Jinzhu Kong, 2010. Protecting the Confidentiality of Virtual Machines Against Untrusted Host. In Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on. Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on. pp. 364–368.

[9] Fu Wen & Li Xiang, 2011. The study on data security in Cloud Computing based on Virtualization. In IT. In Medicine and Education (ITME), 2011 International Symposium on. pp. 257–261.

[10] Suryanarayana, V., Jasti, A. & Pendse, R., 2010. Credit scheduling and prefetching in hypervisors using Hidden Markov Models. In Local Computer Networks (LCN), 2010 IEEE 35th Conference on. Local Computer Networks (LCN), 2010 IEEE 35th Conference on. pp. 224–227.

[11] Naughton, T., et al. 2010. Loadable Hypervisor Modules, System Sciences (HICSS), 2010 43rd Hawaii International Conference on, vol., no., pp.1-8.

[12] Peijie Yu. et al., 2010. Real-time Enhancement for Xen Hypervisor. In Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on. Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on. pp. 23-30.

[13] Pham, C., et al. 2011. CloudVal: A framework for validation of virtualization environment in cloud infrastructure. In Dependable Systems & Networks (DSN), 2011 IEEE/IFIP 41st International Conference on. Dependable Systems & Networks (DSN), on. pp. 189-196.

[14] CSA, 2010, Domain 12: Guidance for Identity & Access Management V2.1.Cloud Security Alliance. Available at: http://www.cloudsecurityalliance.org/guidance/csaguide- dom12.pdf

[15] Afoulki, Z.,et al. 2012. MAC protection of the Open Nebula Cloud environment, High Performance Computing and Simulation (HPCS), 2012 International Conference on, vol., no., pp.85.

[16] Harley Kozushko, Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems, Available from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf.

[17] Achemlal, M., et.al. 2011. Trusted Platform Module as an Enabler for Security in Cloud Computing, Network and Information Systems Security (SAR-SSI), 2011 Conference on , vol., no., pp.1-6.

[18] Wiki, Virtual Firewall, Available from http://en.wikipedia.org/wiki/Virtual_firewall.

[19] Clement Berthelot, Evaluation of a Virtual Firewall in a Cloud Environment, Available from http://buchananweb.co.uk/09014406_MSc_VirtualFirewall.pdf.

[20] Luigi, C., et al. Trusted Virtual Domains – Design, Implementation and Lessons Learned, Available from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf.

[21] Berger, S., R. Caceres, et al. 2009. Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal of Research and Development 53(4): 6:1-6:12.

[22] Zhang, F., et al. 2011. CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. Cascais, Portugal, ACM: 203-216.

[23] Dongxi, L., et al. 2010. A Cloud Architecture of Virtual Trusted Platform Modules, Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on, vol., no., pp.804-811.

[24] Jing-Jang h., et al. 2011. A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, Information Science and Applications (ICISA), 2011 International Conference on , vol., no., pp.1-7, 26-29.

[25] Khan, A., 2012. Access Control in Cloud Computing Environment, In ARPN Journal of Engineering and Applied Sciences, vol-7, no-5., pp.613-615.

[26] Jansen, W., and Grance, T., 2011, Guidelines onSecurity and Privacy in Public Cloud Computing. N*ational Institute of Standards and Technology Special Publication 800-144.* NIST Special Publication 800-144.