Challenges of Virtualization with Security and Management

Aqsa Bilal, Amina Islam, Kainat Nawaz, Amreena Sadaf

Abstract: With the use of cloud computing the complexity and cost of owning and operating computers and networks can be significantly reduced. In the developing age of cloud computing demand of cloud services in almost all the areas like TV channel to online shopping to educational institution etc., the cloud infrastructure cost goes very high. The cloud services customization is now possible and it is flexible to use. Providers offer advance services so that an individual might not need to spend any cost or expertise to develop advance services. Cloud computing and virtualization has been briefly introduced for this purpose. The virtualization is fundamental part of cloud computing which the virtualization is a fundamental part of cloud computing, different unused computing resources are joined into shared pools and for different tasks ,different virtual machines are created,In this way maximum number of resources are used and hence cost is reduced. Virtualization becomes significant as to provide a system security. However, Virtualization faces some challenges which includes the challenge of management and safety. In management challenges there is a challenge of **server consolidation** in which number of physical server are reduced but it increases the number of virtual servers in it that becomes tough to control. Another management problem is sharing of **IT resources** in which there is threat of losing control of one's own resources. This paper will focus on the challenges that virtualization faces and we have proposed solutions for that challenges.

Keywords— Server Consolidation, Site Visitor Monitor, Virtual Prime Layer, Hypervisor, IT Resources, Data Centers, Digital Device(DD), Environment Monitor(EM), Security Mechanism

Introduction

Cloud computing is a technology that is development of distributed computing, grid computing and is combination of development of virtualization, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) [8]. The virtualization is a rudimentary part of cloud, various unemmployed computing resources including memory ,CPUs , network etc are combined togather and different virtual machines are formed to perform different specific tasks,hence resources are used at there maximum level with a decreased cost. [2]. But there still issues in Virtualization. Management and Security is not suitable in virtual environment.

- *Aqsa Bilal is currently pursuing MS Degree Program in Information Technology in University Of Lahore, Pakistan , Email:aqsabilal@live.com,*
- *Amina Islam is currently pursuing Bachelor Degree Program in Computer Science in Government College Women University Sialkot, Pakistan,Email:aminaislam869@gmail.com,*
- *Kainat Nawaz is currently pursuing Bachelor Degree Program in Computer Science in Government College Women University Sialkot, Pakistan, Email:kainat.kat.1996@gmail.com*
- *Amreena Sadaf is currently pursuing Bachelor Degree Program in Computer Science in Government College Women University Sialkot, Pakistan, Email: laibacs1996@yahoo.com*

These are two virtualization challenges that were very superficial in the virtualization events.In this paper we have proposed solutions for above mentioned challenges.

One management challenge is server consolidation that is reducing the number of bodily servers increases the number of digital servers and it grows to be tough to control. Solution for this problem is make sets of virtual machines of the same type. A controller is introduced that will recognize the request for resource and will provide the requested resources. If time limit reaches but more resources are needed then a "borrow resource" technique is also allowed.

Another management challenge is "Sharing of IT resources". Data can reside anywhere on the network and the person/organization who share resources have fear of losing control of their own resources. Solution for the first problem is to encrypt private data before sharing resources. Solution for second problem is "Automatic Monitoring" of shared resources and "User authentication" before allotting resources to users. If user is authentic, he will get requested resources for a specific time period and after that time period resources will be automatically de-allocated and control moves back to organization who shared the resources.

Another challenge is "security of virtual prime layer". If prime layer goes down then whole system has to compromise. The solution is to place some security measures at the virtual prim layer so that site visitor can't

get access the system. Three types of monitoring are involved in the internal system "Environment Monitoring" "Device and Network Monitoring" and "Site Visitor Monitoring". This solution will make the system fully secured.

CLOUD VIRTUALIZATION

Virtualize technology deflects human's point of view for the use of computing resources from corporal to rational.The objective of virtualization is to mutually use the computing resoucres(memory, CPUs netwrorks etc) to their maximum capacity and to diminish the rate of IT assets. this is made by joining unemployed IT assets into distributed pools and to grow unique virtual machines that can perform a lot of tasks concurrently. The resources will also be allotted or altered dynamically. Consumer should be conscious of common tactics comparable to "Eulation, Hypervisor, Full, Para and hardware assisted virtualization" even as making use of virtualization in cloud computing environment [1]. Cloud computing, and particularly the use of public clouds, brings advantages on the technical, environmental and business sides. A cloud provider can manage physical resources in a very efficient way by scaling on the several hundreds and thousands of customers with dynamically changing workload requirements, by re-optimizing the infrastructure in a completely automated (or semi-automated) fashion whenever needed, providing high levels of availability and reliability. "One of the most important technologies that enabled this paradigm shift in computing is virtualization, and particularly machine virtualization". Machine virtualization (also referred to as processor virtualization) allows a single physical machine to emulate the behavior of multiple machines, with the possibility to host multiple and Heterogeneous operating systems (called guest operating systems or guest OSs) on the same hardware. Virtualization allows for server consolidation in data centers, where multiple operating systems can be moved to the same physical resources. This enables the achievement of a reduction of the number of required physical hosts, and their improved exploitation at higher saturation levels, thus saving costs and energy [3]. Virtualization is very useful in cloud computing. Its provide abstraction for lower level functions of hardware. The virtualization enable of high level function and sharing physical resources. Virtualization has been applied of computing memory, storage, processor, software, network and all services that IT offers. Virtualization reduce the cost of all physical resources [7].

Emulation

Emulation is a technique that changes the conduct of a laptop 'hardware' to 'software'.emulation lies/resides on the virtual process layer on the hardware.Guest operating system receives/achieves big flexibility from emulation but as compared to hypervisor its speed of translation process is low. In order to run a program ,emulation requires an excessive hardware configuration.

Hypervisor or Virtual Computer Display

Hypervisor is a program layer which consuls to user specifications and disclose and virtualize the assets of a "host machine".Between the operating process and hardware, hypervisor plays the role of an intermediary layer.This layer generates "virtual resources" such as(memory, processors,drives and reminiscence).

Para Virtualization

Para virtualization supplies distinctive hyper calls. In order to strenghten the efficiency and performance , para virtualization relates verbal exchange between "Hypervisor and Guest operaing system".The drawbaack of this technique is to moddify the kernel of guest running approach utilizing hypercalls.This is only applicable with open supply working programs.

Full Virtualization

An unaccompained atmosphere is created by Hypervisor between the guest and host Or virtual server and server hardware.The fulll virtualization technique is directly access the hardware controllers[1].

Desktop virtualization

This makes it possible for to modify between various operating on the identical running systems, which makes the venture easier for application builders and different tester staffs. This reduces the necessity for replica hardware and has different reasonably priced elements.

Economic aspects of virtualization

The system of virtualization system reduces the requirement of physical machines like number of computer systems, server's storage quantity and so on. The businesses which furnish information centers use this process for storing data, software and so forth. Which in flip raises the revenue of the corporations? This proposal reduces the necessities of gigantic numbers of servers and related parameters like electricity, cooling expenditures etc. Which results improvement for the customers additionally as there will probably be colossal price reduction in the cloud utilization?

Virtualization in data centers

Knowledge centers form the basis of a huge variety of offerings furnished by means of the internet including net-web hosting, ecommerce and basic services corresponding to application as a service (SAAS), platform as a carrier (PAAS), and grid/cloud computing. They consist of targeted apparatus to perform one-of-a-kind capabilities like retailer, control, method, and trade digital knowledge and understanding. Data centers are commonly run through significant companies or government companies. This is a simple cage or rack of gear for some and a room inclusive of few cabinets for others. There may be steady develop in the demand for both the bodily infrastructure and IT equipment due to fast progress of knowledge centers. This results in continuous develop in vigor consumption. Computer systems require electrical power, as well as security from theft ie the unintentional or intentional manipulation of hardware. So, one has to safeguard data centers in opposition to outside influences and provide them with enough cooling. Virtualization technology provides the answer but it has many overheads, like complete fee of ownership, power and efficiency calculations and return of investment done. The difficulty confronted by using IT managers is suitable implementation of virtualization technology in data centers [5].

Virtualization Challenges

There are still many disorders with virtualization technologies. For illustration, in usual environments there are many tools that facilitate administration and safety for IT infrastructures. However, for digital environments ordinary administration and safety technologies are almost always not suitable. These are two virtualization challenges that had been very obvious within the virtualization events.

Management

Companies that have adopted virtualization applied sciences are facing a quantity of management issues. One in all administration quandary in group is **server consolidation** in which the quantity of (physical) servers can also be greatly reduced to smaller number of (physical) servers which might be running a couple of virtual servers. Even as the hardware can vastly be lowered, an organization nonetheless has to manage the huge number of digital servers. In addition, server virtualization allows for organizations to simply installation new virtual servers with the clicking of a mouse button. Even though server consolidation reduces number of bodily server however because of a huge number of digital servers it grow to be tough to control.

One other problem is the sharing of IT resources. As resources are shared, the functions and data of specific departments of a group can reside anywhere in the digital atmosphere. Specific departments of a group are customarily additionally reluctant of the inspiration on sharing assets with other departments and losing control of their own assets. Nonetheless, new development in management instruments has addressed a few of these problems.

Physical and Virtual machine issues

In case of strolling quantity of physical machines in a single physical host, hardware requirements were reduced.Protection obstructions prevails between server machines and physical systems. For example if one physical machine is running a number of servers and if RAID controller removes all hard disk then there will loss of data and records.This is due to a trouble with safety between digital gadgets running on one physical machine..

Issues of virtual applications and virtual machines

if the virtualization layer, that exists between the physical and digital machine is compromised then all hosted workloads and their safety will also be compromised.In this example the virtual layer is susceptible that can be

withpout dificulty tormented by risk thus lowering the protection of complete virtual surroundings. To allow virtual machines to talk without delay within the physical host ,maximum virtualization structures encompasses the capability to initiate software based virtual networks and switches for effectiveness in verbal exchange among virtual machines.

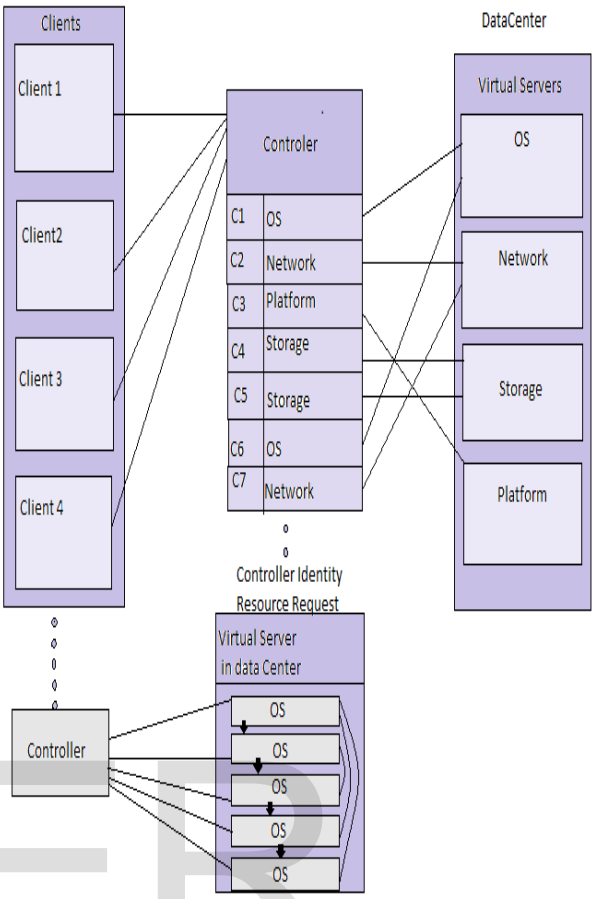
The visitor will now not be detectable to network primarily based safety gadgets.Current safety techniques won't correspond with virtual environment, as a result virtual environment is troublesome.

Problem No.1

Even though server consolidation reduces number of bodily server however because of a huge number of digital servers it grows to be tough to control.

Here, we have proposed a solution for this problem and will discuss how to easily control the huge number of digital servers.

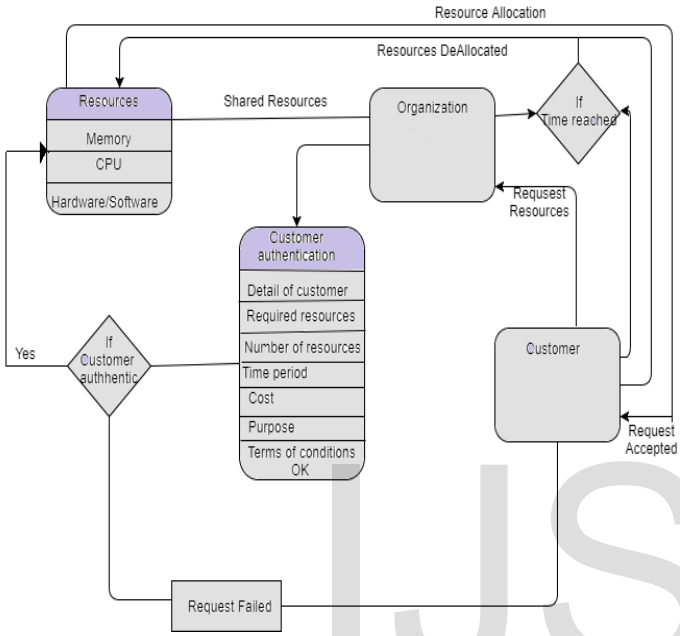
Solution: As we know that in one physical server there a huge number of virtual servers. If there are many **requests** for different resources(OS, network, memory etc), for each type of request there is a specific type of virtual machine that handles that specific **request**. It is not necessary that for one specific request there in only one virtual machine. There may be more than one virtual machines for each type of requests. These virtual machines provide resources for a specific time period in response to request. We can make parts of data centers like storage, operating system,platform, networking etc. to control different parts of data centers we have to introduced a "controller" that will control the incoming and outgoing processes. In every individual part, there are many virtual machines. If one virtual machine is working but the time limit of its allocated resources reaches but work is still pending, then it can borrow resources from some other virtual machine of its area whose time limit for resources is remaining and resources are free. In this way, it will be easy to control digital servers.



Problem No.2

We are facing a problem of "sharing of IT resources". When different IT resources are shared then Data and Functions of an organization can reside anywhere on the digital atmosphere. Many organizations don't share their extra unused resources with the fear that they will lose control of their own resources. We have proposed a solution for this problem. When an organization share it's resources, it is suggested that they secure their private data. For this purpose, they can use Data Encryption so that data remains inaccessible to others. When an organization share its IT resources there should be a mechanism that maintains organization's control over its shared resources. There should be an automatic monitoring of these shared resources. When a customer request for the resources shared by an organization first it's authentication will be performed. If user is authentic then resources will be allocated for a specific period of time and when this specific time period reached, resources will be deallocated automatically and control moves back to the organization which shared the resources. During the authentication user

customer /user can also register himself. Customer has to provide every detail about him, required resources, number of resources, time period for (which resources are required), purpose for getting these resources, cost and at last have to sign an agreement. if the whole procedure is done successfully then resources will be alloted. The whole scenario is described as:



Safety

Security disorders associated with virtualization have end up extra significant to address. In fact, virtualization provides new challenges for businesses that require involvement of expertise safety measures in preliminary stages of virtualization projects. Virtualization provides a new layer of application on a (physical) server and like several application that's written with the aid of a “man or women” it will possibly contain embedded and but to be learned vulnerabilities which may be exploitable. When hackers get access to the virtualization layer, which includes the hypervisor, all the digital machines could be compromised. Furthermore, normal protection and management tools inside an OS will not be aware or designed to entry, scan or protect the virtualization layer. There are safety instruments for virtualization, known as virtual protection appliances. Digital security appliances are security packages that are areas within VMs. The VM is packaged with an OS and protection utility, which will offer better efficiency, than putting in safety application in each VM, as a result of its dedicated technique. Nonetheless, the security instruments are nonetheless positioned on prime of the virtualization layer, which has its drawbacks, peculiarly if the virtualization layer is compromised. One other risk is the verbal exchange between digital machines. Many digital environments comprise the capacity to create digital networks and switches throughout the host (or physical server) to permit digital machines to be in contact directly. This site visitors will not be obvious to ordinary physical community-centered security safety gadgets as the site visitors goes through a virtual community inside the host. Monitoring the site visitors between virtual machines on the identical server requires safety measures placed within the host [2]. The virtualization not only provides us security benefits but also it is detrimental. Virtualization is a very high and wide field of new research which provide us solution of new coming threats of daily life but it does not cover every aspect of security. By using of virtualization system. Its work is related to concern consideration and implication. It includes sensitive data for security but does not provide complete security [6].

Assurity of Hypervisor's security

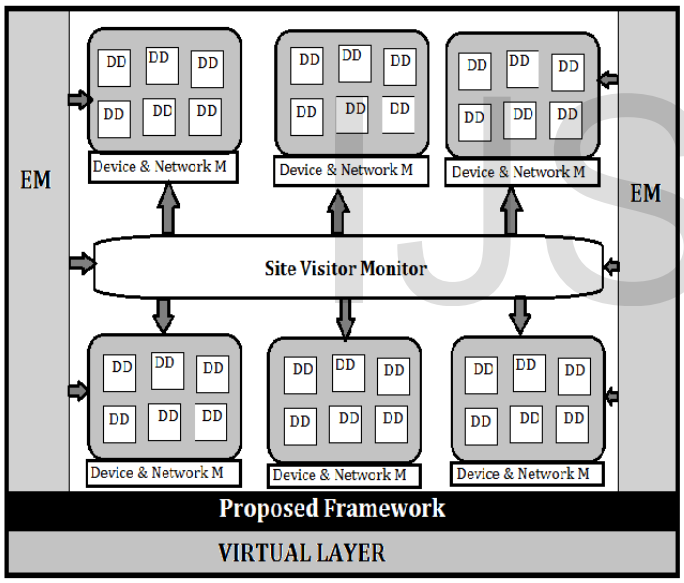
Virtual applications that are accessed through calls from the client, must have privacy within the server environment, such that every client is private from every other client in the Virtual environment. If there is no privacy, then statistics from one purchaser are posted to another patron in the virtual environment ,thus resulting in information "Insecurity". If there is no confidentiality between degital applications and client then information is insecure.

In case of physical environment ,this isn't always a trouble as all applications and customers are remote from each other.The statistics from server will become erractic when virtual programs get right of entry to data from database service.There rise up several troubles when operating system is provided as a carrier alternatively when applications are accessed On-demand .For example

the server slows down when there are many concurrent 'operating system requests' by the clients.

Problem No.3

When security instruments are positioned at prime layer of virtualization, it has some drawbacks. If these security instruments are attacked then whole virtualization layer has to compromise. Another risk is the verbal exchange between digital machines. Digital environment has enough capacity that it can create its own digital network and can switch inside the host. When a site visitor 'gets in' a digital network, the safety gadgets present in virtual community of host do not detect the "site visitors". To detect and monitor these site visitors, some safety measures should be placed in the host. Here we have proposed a security mechanism that perform the above-mentioned tasks.



DD= Digital Devices

M= monitor

EM= Environment Monitor

This mechanism will apply high security on the virtual prime layer and will be able to detect and deny any unauthorized access. The mechanism will also be applied on the other components of virtual environment like on individual digital network and on individual digital device inside this network. It will check that, is the site visitor authentic or not? Automatic monitoring will also be included in this mechanism, in which site visitors will be automatically detected that safety gadgets inside the host are unable to detect. By developing and applying this mechanism, security of virtualization can be enhanced.

Discussion

The virtualization is fundamental part of cloud computing which utilizes the IT resources to
to extreme level and minimises the charges of Computing resources (IT resources).But there still issues in Virtualization. Management and Security is not suitable in virtual environment. We addressed both of these challenges in this paper and proposed solution for these challenges. As we found the challenge of server consolidation for it we proposed the solution of borrowing resources from another virtual machine with same types of resources to complete the request. Second problem that we addressed is the sharing of IT resources where there is fear of losing control over one's own resources for it we proposed the solution of authentication and automatic de-allocation of resources when time limit reaches. The third problem is safety from site visitor and we proposed to apply such automatic monitoring mechanism on virtual layer and to each individual component of virtual machine. If the above mentioned proposed solutions will be applied it will reduce virtualization challenges.

Conclusion and Future work

In this paper ,we discussed the virtualizaion which is a fundamental part of cloud computing which uses multiple computing resources(Memory, CPUs ,Networks) to minimize the cost of resources by generating various virtual machines in order to perform a lot of tasks concurrently.But virtualization faces still some issues like security and management. Virtual machine applications and physical machine applications have some issues. If RAID controller removes all hard disk and server is running on one physical machine then all data and recordes will be lost. If there is no privacy among server applications and client then information is insecure in this case. We proposed the solution of challenges identified in the paper. In future we are intended to implement the proposed solution by applying some algorithms or hypothesis to figure out that how effective are the results we achieved.

References:

[1] Durairaj. M, Kannan.P , A Study On Virtualization Techniques And Challenges In Cloud Computing ` , volume 3, issue 11, november 2014.

[2] Bohar Singh, Jagdeep Singh, Sahil Kumar , Virtualization Techniques and Virtualization Challenges in Cloud Computing ` , Volume 2, Issue 6, June 2015.

[3] Marisol García-Vallsa, Tommaso Cucinottab, Chenyang Luc , Challenges in real-time virtualization `.

[4]:2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.254-256.

[5] K C Gouda, Anurag Patro, Dines Dwivedi , Nagaraj Bhat, Virtualization Approaches in Cloud Computing `.

[6] MICHAEL PEARCE, SHERALI ZEADALLY, RAY HUNT, Virtualization: Issues, Security Threats, and Solutions `.

[7] Deepanshu Thakral, Mahesh Singh, Virtualizati in Cloud Computing `, IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1262 – 1273.

[8]Santosh Kumar and R. H. Goudar "Cloud Computing – Research Issues, Challenges, Architecture, , Vol. 1, No. 4, December 2012.

[9] Resource Allocation in Contending Virtualized Environments through Stochastic Virtual Machine Performance Modeling and Feedback*
CONG-FENG JIANG, JIAN WAN, XIANG-HUA XU, JI-LIN ZHANG AND XIN-DONG YOU Grid and Services Computing Technology Lab Hangzhou Dianzi University Hangzhou, 310037 P.R. China

[10] A Sharing-Aware Greedy Algorithm for Virtual Machine Maximization
Safraz Rampersaud Department of Computer Science Wayne State University Detroit, MI 48202, USA Email: safraz@wayne.edu
Daniel Grosu Department of Computer Science Wayne State University Detroit, MI 48202, USA Email: dgrosu@wayne.edu

[11] A Cooperative Multi Agent Learning Approach to Manage Physical Host Nodes for Dynamic Consolidation of Virtual Machines
Seyed Saeid Masoumzadeh Research Group Entertainment Computing University of Vienna Vienna, Austria Email: Seyed.Saeid.Masoumzadeh@univie.ac.at
Helmut Hlavacs Research Group Entertainment Computing University of Vienna Vienna, Austria Email: Helmut.Hlavacs@univie.ac.at

[12] Practical effectiveness of mobile virtual machines
Lennart Beringer and Stephen Gilmore
Laboratory for Foundations of Computer Science, The University of Edinburgh, Edinburgh EH9 3JZ, Scotland. Email {lenb,stg}@lfcs.ed.ac.uk

[13] Securing Virtual Machine in Cloud Enviroment using OVF and Hashing Function Rajinder Sandhu Dr. Inderveer Chana

[14] Dynamic Environments for Virtual Machine Placement considering Elasticity and Overbooking
Jammily Ortigoza Science and Technology School Catholic University of Asunci´on jortigozaf@gmail.com Paraguay Fabio L´opez-Pires Itaipu Technological Park National University of Asunci´on fabio.lopez@pti.org.py Paraguay Benjam´ın Bar´an National University of Asunci´on Catholic University of Asunci´on bbaran@pol.una.py Paraguay

[15] Virtual Machine Migration Enabled Cloud Resource Management: A Challenging Task
Misbah Liaqata, Shalini Ninoriyab, Junaid Shujaa, Raja Wasim Ahmada, Abdullah Gania a Faculty of Computer Science and Information Technology, FSKTM, University of Malaya

[16] TREASURE: Trust Enhanced Security for Cloud Environments
Vijay Varadharajan Udaya Tupakula Information and Networked Systems Security Research Department of Computing, Faculty of Science, Macquarie University Sydney, Australia {vijay.varadharajan, udaya.tupakula}@mq.edu.au

[17] Analyzing Security Threats to Virtual Machines Monitor in Cloud Computing Environment
Ahmad Fayez S. Althobaiti
Department of Computer and Information Sciences, Al-Imam Muhammad Ibn Saudi Islamic University, Riyadh, Saudi Arabia

[18] Security Considerations for Virtual Platform Provisioning
Mudassar Aslam, Christian Gehrmann Swedish Institute of Computer Science (SICS) Isafjordsgatan 22, SE-164 29 Kista, Sweden {mudassar.aslam, chrisg}@sics.se

[19] Virtual machine security challenges: case studies
Amjad Rehman • Sultan Alqahtani • Ayman Altameem • Tanzila Saba

[20] When Virtual is Harder than Real: Resource Allocation Challenges in Virtual Machine Based IT Environments
Ludmila Cherkasova, Diwaker Gupta1, Amin Vahdat1
Enterprise Systems and Software Laboratory HP Laboratories Palo Alto HPL-2007-25 February 8, 2007*