CLIENT TO CLIENT ATTACKS PROTECTION IN CLOUD COMPUTING BY A SECURE VIRTUALIZATION MODEL

AHAD AKBAR ABADI

UNIVERSITI TEKNOLOGI MALAYSIA

CLIENT TO CLIENT ATTACKS PROTECTION IN CLOUD COMPUTING BY A SECURE VIRTUALIZATION MODEL

AHAD AKBAR ABADI

A thesis submitted in partial fulfillment of
the requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

January 2013

ACKNOWLEDGEMENT

First and foremost, I would like to thank God for giving me the ability to accomplish this project. Apart from the efforts of me, the success of any project depends largely on the encouragement and guidelines of many others. I take this opportunity to express my sincere gratitude to the people who have been helpful in the successful completion of this project. I would like to show my greatest appreciation to Dr. Mazdak Zamani. Saying thank you is not enough for his tremendous support and help. I feel motivated and encouraged every time I attend his meeting. Without his encouragement and guidance this project would not have materialized. The guidance and support received from all of my friends who contributed was vital for the success of the project. I am grateful for their constant support and help. I am sincerely thanking to my examiners, Dr. Bharanidharan Shanmugam and Dr. Teddy Mantoro, for their appropriate comments.

Last but not least I wish to express a sense of gratefulness to my beloved parents and my dear sisters for their manual support, strength, and help and for everything. I always feel them beside myself in all good times, bad times.

ABSTRACT

Cloud computing was the long held dream of computing which has the potential to transform a large part of the IT industry, shaping the way that IT hardware designed and purchased and making software even more attractive as a service. Without Virtualization cloud computing cannot achieve to its incredible goals. VMware, Xen and KVM are some hypervisor software which provides server Virtualization ability for cloud computing structure. Although cloud computing brings gigantic advantages, the security issues still the considerable difficulties for customers. This means the attacks which can threat the computer networks also can be threats for cloud computing environment.VM to VM attack is one of the common types of attacks that classified into two different groups such as VM hopping and VM mobility. Port scanning comes in the first step of a computer attack. The aim of port scanning is to find the open ports that can be exploited by attackers, in addition, in attacker view getting information about the other port's status can be useful for further exploitation. The goal of this project is to propose a new model for achieving the better method to realize port scanning attempts and find out the information about suspicious port scanner virtual machine in cloud computing.

ABSTRAK

Pengkomputeran awan adalah impian yang lama dipegang pengkomputeran yang mempunyai potensi untuk mengubah sebahagian besar daripada industri IT, membentuk cara bahawa IT perkakasan yang direka dan dibeli dan membuat perisian lebih menarik sebagai pengkomputeran awan service.Without virtualisasi tidak boleh mencapai untuk yangmatlamat yang luar biasa. VMware, Xen dan KVM adalah beberapa hypervisor perisian yang menyediakan virtualisasi pelayan keupayaan untuk struktur perkomputeran awan. Walaupun pengkomputeran awan membawa kelebihan gergasi, isu-isu keselamatan yang masih menjadi masalah besar bagi pelanggan. Ini bermakna serangan yang boleh ancaman rangkaian komputer juga boleh menjadi ancaman untuk persekitaran pengkomputeran awan. VM serangan VM adalah salah satu jenis biasa serangan yang dikelaskan kepada dua kumpulan yang berbeza seperti VM melompat dan VM mobility.Port pengimbasan datang dalam langkah pertama serangan komputer. Tujuan imbasan pelabuhan adalah untuk mencari pelabuhan terbuka yang boleh dieksploitasi oleh penyerang, di samping itu, memandangkan penyerang mendapat maklumat mengenai pelabuhan status lain boleh menjadi berguna untuk matlamat lanjut exploitation.The projek ini adalah untuk mencadangkan satu model baru bagi mencapai kaedah yang lebih baik untuk menyedari percubaan pengimbasan pelabuhan dan mengetahui maklumat tentang pengimbas port mencurigakan mesin maya dalam perkomputeran awan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

SOA	Service Oriented Architecture
VM	Virtual Machine
NIST	National Institute of Standards and Technology
IPS	Intrusion Prevention System
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
DaaS	Data as a Service
API	Application Programming Interface
ROI	Return of Investment
CAPEX	Capital Expenditure
OPEX	Operational Expenditure
VMM	Virtual Machine Manager
NAT	Network Address Translation
DDoS	Distributed Denial of Services
TIFS	Time Independent Feature Set
ICMP	Internet Control Message Protocol
DHCP	Dynamic Host Configuration Protocol
QoS	Quality of Services
TFIDF	Term Frequency Inverse Document Frequency
EPSD	Embedded Port Scan Detector
SBC	Single Board Computer
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
IANA	Internet Assigned Numbers Authority
vTPM	Virtual Trusted Platform Module
TC	Trusted Computing
TCG	Trusted Computing Group
TCB	Trusted Computing Base

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud computing has become a controversial subject in the next generation of computing. Cloud computing is driven from two research areas such as Service Oriented Architecture (SOA) and Virtualization. It is a computing paradigm in order to various resources such as computing, software, infrastructure, and storage are provided as paid services over the Internet as it shows in Figure 1.1. The cloud has a capability which provides the users elastic and scalable resources in the pay-as-you-use fashion at relatively low prices as Figure 1.2 shows. Also with its infrastructure, company able to cut down expenditures. Although cloud provides saving in terms of finance and manpower, new security risks are coming along with it. The main security concern is loss of control over sensitive and confidential data. Few amount of research has been done with specific focus on insider attacks on the cloud environment (Sundararajan, Narayanan, Pavithran, Vorungati, & Achuthan, 2011).

Cloud computing should include all the different types of applications and computer programs from little data processing programs to email services. Usually servers do not run with the same operating systems. In fact they work independent of operating systems. Central management such as cloud provider should monitor VMs and provide the services that everything runs well without any problem of confliction. Therefore cloud middleware software is created for this purpose in order to follow the rules that called protocols. By using the perfect middleware cloud

computing activities will be as normal as a single computer program run (Jose & Sajeev, 2011).

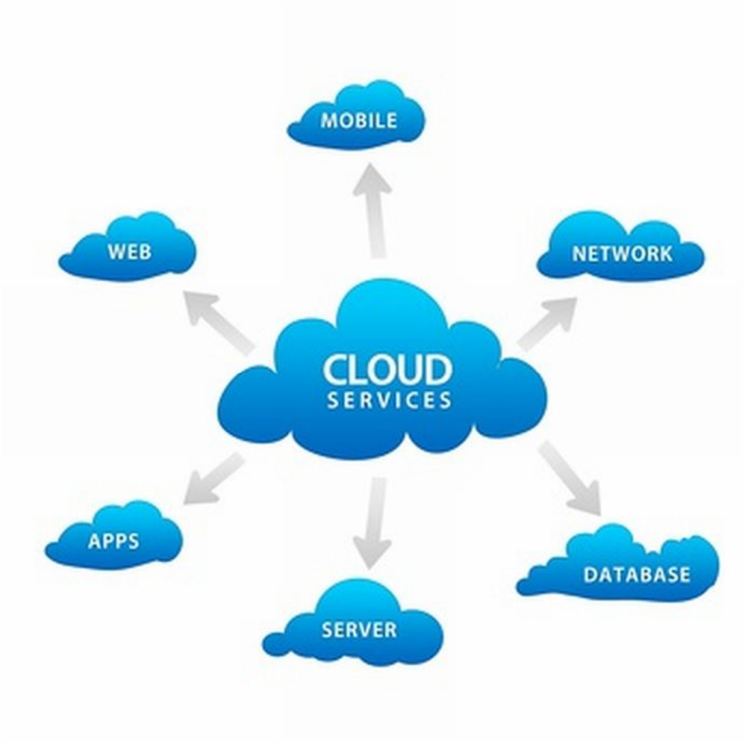

Figure 1.1: Overall View of Cloud Computing (Armbrust et al., 2010)

The data and applications which exist in the cloud are stored and run on pools of web servers. Another categorization of cloud computing is separate it into two parts. First part is the front end and the second one is back end. Front end contains all the stuff that a tenant or a computer user can see, in contrast the back end include different types of server pools, data storage pools and infrastructure that creates clouds computing and services and connect throughout the internet to each other (Kramer, Goré, & Okamoto, 2010).

Cloud computing use pools of storages and servers to distribute the services and stored data such as a list of clients, clients' information. These several copies enable servers to gain access to backup data in various locations. Thus clients can access to their data from anywhere which linked to the Internet (Sundararajan, et al., 2011).

Reducing cost and hardware dependency is an aim in network technology and business. With cloud computing system need for hardware on client side sharply decreased. Tenants do not need for advanced hardware such as fast computer with a bigger size of memory because cloud system prepares these requirements (Jose & Sajeev, 2011).

Cloud is an Internet-based and tries to cover the difficulties for users. Virtualization plays a pivotal role in cloud computing infrastructure that combined with self-service abilities computing resources. Due to its ability to decrease the amount of spending time, energy, installing and maintaining racks of servers many organizations using Virtualization to satisfy their requirements with fewer resources and costs (Turner, 2008).

The logic behind the Virtualization is the abstraction of physical resources into many separate virtual computing environments which called a virtual machine. The permission of the users in a virtual environment is created copy, save, read, modify, share, migrate and roll back the running VMs. By allocating these abilities administrator of the system can easily manage the system (Garfinkel & Rosenblum, 2010; Li, Raghunathan, & Jha, 2011).

Multiple Virtual Machines (VM) hosted on the same physical server in a cloud environment. Applications delivered as a service over the Internet and hardware in data centers provides these services. Companies try to provide benefits like energy efficiency and performance without compromising security to achieve successful fertilization. Although virtualization provides intrusion isolation, accessing to share storages that contain sensitive personal or corporate data typically possible for VMs. In other word, VMs still are vulnerable for the cloud. The vital role of Virtualization makes it a prime target for attacks (Kirch, 2007).

Virtualization layer is based on a large complex trusted computing. Most of the listed reports in NIST's National Vulnerability Database show the difficulty of transferring bug-free hypervisor code. Therefore, an attacker can achieve these bugs and exploit Virtualization software. This is just the first step, after exploiting, the

attacker gets the ability to thwart or access other VMs and poison confidentiality, integrity, and availability of data (Reuben, 2009).

One of the most sufficient points of Virtualization is the elasticity. Virtualization technology provides the scalable computing capacity environment for tenants which need the lower cost in contrast to physical one as Figure1.2 shows. Virtualization also provides load balancing via provisioning and migration of virtual machines among physical parts (Li, et al., 2011).

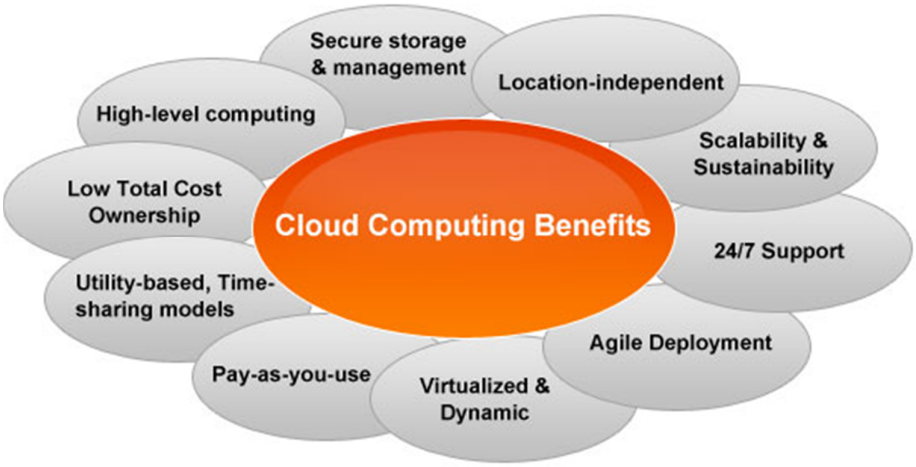

Figure 1.2: Benefits of Cloud Computing (Jansen, 2011)

Two basic types of Virtualization architecture are introduced in cloud computing. In the first type, the virtual machine monitor put on the hardware and captures the communication between the guest VMs and hardware. On top of the virtual machine monitor there is a VM which manages the other virtual machines. This virtual machine is responsible for all the communication between VMs. In the second type the virtual machine monitor executes as an application within the host operating system. In other word the host operating system place above the hardware and the virtual machine monitor place on above host operating system. Even though these two architectures are different, how VM can trust to execution environment is the same security concern in both of them (Li, et al., 2011).

Although the managing of the cloud system is becoming easier through the Virtualization environment, the security concerns are appearing. If the hacker attacks the VM that manage the system attacker can easily copy, modify and compromised all the VMs. In addition when attacker compromise the management of the environment by getting a high level of permissions, can bypass the mechanisms in guest VMs (Borders, Weele, Lau, & Prakash, 2009).

The cloud provides an environment which is completely huge and internet base, therefore the vulnerabilities for cyber-attacks are more than traditional solutions. If the environment has some limitation in scaling then the services, applications and also the users who got access control are under complete controlling and monitoring but cloud computing environment are built on the internet connection, so all the services which contain in internet is running in the same condition. In addition the cyber-attacks on the internet are becoming a potential threat in cloud computing (Lombardi & DI Pietro, 2010).

One of the most harmful attacks is Man-in-the-Middle. It is an active overheard in order to make an independent connection with the victim. The attacker makes the victims believe that they have a straight connection with servers in private zone, however in fact the total connection is controlled by the attacker. Attackers significantly affect the security of organization by injecting new messages. Owing to these problems it is vital to use the techniques in order to protect against those attacks (Whalen, Engle, & Romeo, 2009).

Patching offline VMs are security vulnerability in Virtualization environment. Some patch management tools are introduced but they cannot patch offline VM images. Also making updating signature and protecting offline VMs and VM appliance images become a problem for providers. VMs may be off, on, suspended or allocated in storage; so, information about the life cycle of VMs and their changes is essential for providers to access the VMs' vulnerabilities in order to apply security patches to VMs (Owens, 2009).

Because of the loss of virtual network discovery approaches, model the configuration of a virtual server has become a considerable problem. In the optimistic viewpoint the virtual devices, virtual network, all VMs and services should be discoverable follows by their relationship to other ones. The system should gather the information about the devices and their configuration, then confirm the correct configuration and create a baseline. Because of the loss of configuration baseline it is not possible yet (Owens, 2009).

Most of the attacks on cloud computing are using the detrimental vulnerability which is the lack of traffic monitor in a virtual environment. The inter VM traffic movement are not visible to intrusion prevention system (IPS) and other traditional security devices through the network based environment. To secure the virtual infrastructures virtualized security capabilities should place between the guest operating system and virtual network to protect against attacks (Owens, 2009).

1.2 Background of the problem

Virtualization is the most essential technology aspect in cloud computing, however its security vulnerabilities and potential threats which can compromised by attackers has not been enough studies (Kirch, 2007). As Figure 1.3 shows cloud computing services categorized into three types of layers such as Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a service (IaaS). SaaS presents an application-level interface. PaaS offers development environment for applications. IaaS provides shared infrastructures without accessing for upper layers. Nowadays attackers focus on IaaS on access to the forbidden environment of infrastructures (L. J. Zhang & Zhou, 2009).

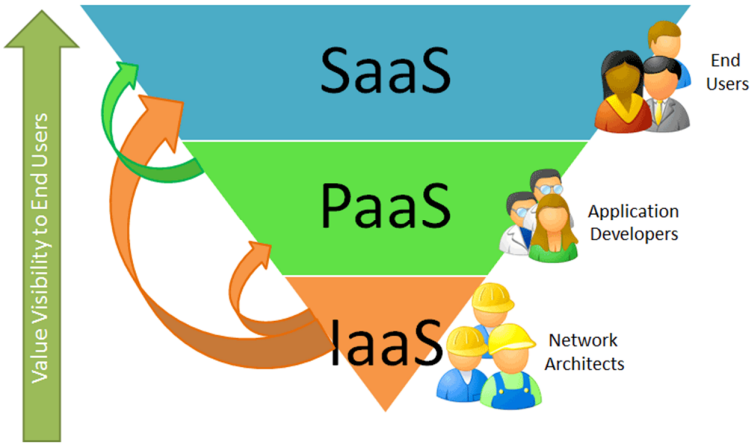

Figure 1.3: Cloud Computing Services (Jin et al., 2010)

Generally IaaS made resources available in the form of VMs instances. Tenants have full control over these VMs; however they do not have visibility into the lower level of the infrastructure like hypervisors (virtual machine monitor) or data center manager systems (Hyde, 2009).

Hypervisors create to present a view which appears both operating system and application inside a VM running on the same hardware to the guest VM. Hypervisors gain this by matching the original hardware and referring access to it. Requirements for this purpose are a complex body of software and significant interaction between VM and hypervisor. Hence the interaction is the basic security threat. Malicious VM can operate to attack the hypervisor via exploiting its bugs or supporting Virtualization software to attack another VM (Fish et al., 2010).

Although the security vulnerabilities do not exist in one type of cloud, the main security concern is in public cloud. Multi-tenancy creates sharing of resources. As clouds implement logical isolation through tenants, they multiplex tenants across the infrastructure. Realistic threat of data theft in public clouds presents via this practice (Christodorescu, Sailer, Schales, Sgandurra, & Zamboni, 2009). One of the

biggest questions from cloud providers is even they offer assurance of physical isolation for their tenants how tenants can verify that their VMs and resources are physically isolated?

1.3 Problem Statements

The main security concern is loss of control over sensitive and confidential data. One malicious virtual machine could poison all existed virtual machines in the physical server. The intruder who attacks a VM can simply transfer to another hosted VM in the same physical server. Attackers have to access one VM for contaminating other VMs and escaping the hypervisor that legitimacy is not accessible from VM level (Sabahi, 2011).

Attack from one VM to another VM can categorize in two different types such as VM Hopping and VM Mobility.

VM hopping is the action of jumping from one VM to another one on the same host. To achieve this hopping the attacker should know the IP address of the second VM or gaining access over the host as Figure 1.4 shows. Because of deploying on the same host, if attacker monitors the network traffic going to the victim could violate the traffic and attack as Table 1.1 illustrates. In addition, an attacker can change the configuration file, thus change the files of the victim. An attacker can stop the ongoing communication, so when the connection resumed, the whole connection should start again (Hyde, 2009; Tsai, Siebenhaar, Miede, Huang, & Steinmetz, 2011).

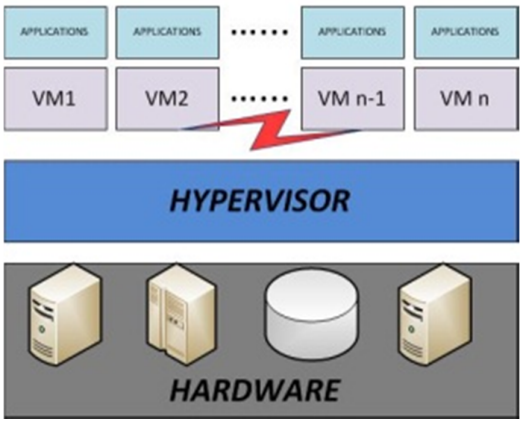

Figure 1.4: VM Hopping

Another type of VM to VM attack is VM Mobility. VMs are portable, so clients can move them from one location to another one. Also they can copy VMs through a network or move them via USB disks. VMs are not inherently present on the physical machine therefore the potential of the threats is suddenly increased. Hypervisor has a file which contains the content of the stored VMs. When the VM moves the virtual disk should be recreated, this is the best situation for an attacker to modify the configuration file of the VM as Table 1.1 shows. Also as Figure 1.5 illustrates, if the VM is offline the attacker gain the access to virtual disk and get the sufficient time to break all the security walls. As this VM is a copy of real VM, tracing the attacker with this threat is difficult (Hyde, 2009; Tsai, et al., 2011).

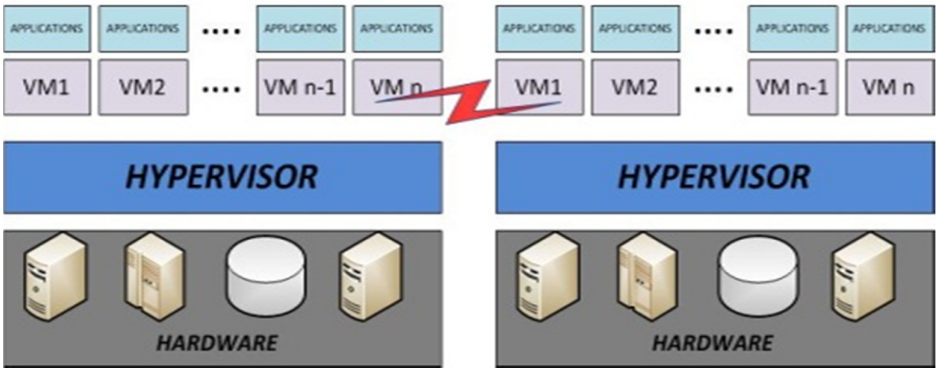

Figure 1.5: VM Mobility

Table 1.1: Security Impacts of Virtualization(Tsai, et al., 2011)

Virtual machine (VM) vulnerability	Conventional environment	Cloud computing environment		
		SaaS	PaaS	IaaS
VM hopping	Confidentiality	—*	Confidentiality	Confidentiality
	Integrity		Integrity	Integrity
	Availability		Availability	Availability
VM mobility	Confidentiality	—	x**	Confidentiality
	Integrity			Integrity
	Availability			Availability
	Security management			

Port scanning is one of the VM to VM attacks which provides useful information for attackers to compromise the VMs. Normally port scan does not do direct damage just by port scanning in cloud computing . Potentially a port scan helps the attacker find which ports are available to launch various attacks. By compromising the target VM port scanning can break the confidentiality, by performing further attacks such as DDoS it can break the availability and by changing the compromised data it can break the integrity (Tsai, et al., 2011).

1.4 Project Objectives

The objective of this study is as below:

i. To investigate existing models of virtualization in cloud computing
ii. To propose a model for cloud computing against port scanning in Client to Client attack field in cloud comuting
iii. To test the proposed model against port scanning in Client to Client attack field.

1.5 Research Questions

The main questions this research motivates to answer are as follows:

i. What are the potential attacks for Virtualization in a cloud computing environment?
ii. What are the secure models to defend against port scanning in Client to Client attack fields?
iii. How to test and validate the proposed secure model against port scanning in Client to Client attack fields?

1.6 Project Aim

The aim of this project is to investigate the existing models with currently examined by providers. Then analyze the types of attacks which affect the cloud environment from a VM to another VM. In addition, identify the vulnerabilities that can be a window for port scanning attackers to achieve unexpected access and violate the target VM. After that propose a model for cloud computing environment against port scanning in Client to Client field and test the proposed model. Although confidentiality is the main goal of this project, availability and performance is vital to a cloud environment.

1.7 Project Scope

The scope of the project is focused on the lowest layer of cloud computing architecture which is an Infrastructure as a Service (IaaS). Tenants do not have visibility on this level. VM to VM attacks is the family of attacks that discussed in this project. VM hopping is the main type of VM to VM attacks that will explain during this project. The specific attacks of VM to VM in VM hopping field is port scanning. In the port scanning type the focused will be on the vertical scans which

explained as a single IP scanner for multiple ports in a cloud environment. The proposed model will build to detect the port scanning which is performed on VM. VMware is the platform which will be used for simulation in this project. ESXi and vSphere client are the products which prepare cloud environment are using through simulation.

In addition, some areas which are excluded from the scope of this project are:

- VM mobility attacks (attack from one VM to another one on the different hypervisors).
- Horizontal port scanning (group of IP scans for single port)
- Pre detection of port scanning

1.8 Summary

Overall view of cloud computing and its business characteristics which make the cloud environment as an undeniable environment for use by organizations and enterprises were introduced in this chapter.

Actually this chapter was classified into different aspects such as the background of the problem which review the creation of problems, problem statement that states the problem, project objectives, project aim and final project scope. Security vulnerabilities are the main concern in a cloud environment. Using Virtualization in this area brings some attacks which related to virtual machines. The main problem in cloud environment is about attacking from one virtual machine to another one that called VM to VM attack.

REFERENCES

Ahmed, N., Khalib, Z., Ahmad, R., Sudin, S., & Asi, S. (2008). *Low-End Embedded Linux Platform for Network Security Application–Port Scanning Detector.* Paper presented at the Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on.

Andrzejak, A., Kondo, D., & Yi, S. (2010). *Decision model for cloud computing under sla constraints.*

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Baig, H. U., & Kamran, F. (2007). *Detection of Port and Network Scan Using Time Independent Feature Set.* Paper presented at the Intelligence and Security Informatics, 2007 IEEE.

Baumann, A., Barham, P., Dagand, P. E., Harris, T., Isaacs, R., Peter, S., et al. (2009). *The multikernel: a new OS architecture for scalable multicore systems*.

Berger, S., Cáceres, R., Goldman, K., Pendarakis, D., Perez, R., Rao, J. R., 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.

Borders, K., Weele, E. V., Lau, B., & Prakash, A. (2009). *Protecting confidential data on personal computers with storage capsules*.

Briscoe, G., & Marinos, A. (2009). *Digital ecosystems in the clouds: towards community cloud computing*.

Chen, J. Q., Williams, B., & Samake, A. A. (2009). Teaching Intrusion Detection and Intrusion Prevention on the Virtual Platform: Hands-On Laboratory Exercises.

Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., & Zamboni, D. (2009). *Cloud security is not (just) virtualization security: a short paper*.

Dabbagh, M., Ghandour, A. J., Fawaz, K., Hajj, W., & Hajj, H. (2011). *Slow port scanning detection.* Paper presented at the Information Assurance and Security (IAS), 2011 7th International Conference on.

Das, T., Padala, P., Padmanabhan, V. N., Ramjee, R., & Shin, K. G. (2010). *Litegreen: Saving energy in networked desktops using virtualization*.

Endo, P. T., Gonçalves, G. E., Kelner, J., & Sadok, D. (2010). *A survey on open-source cloud computing solutions*.

Fish, T. E., Blumberg, B., Mathis, A., Theobald, K., Busco, J., Makarick, L., et al. (2010). FUTURE ISSUES Winter 2009-2010.

Gadge, J., & Patil, A. A. (2008). *Port scan detection.* Paper presented at the Networks, 2008. ICON 2008. 16th IEEE International Conference on.

Garfinkel, T., & Rosenblum, M. (2010). *When virtual is harder than real: Security challenges in virtual machine based computing environments*.

Harold, D., Abraham, R., Hollingworth, P., Sims, R., Gerrish, A., Hamshere, M. L., et al. (2009). Genome-wide association study identifies variants at CLU and PICALM associated with Alzheimer's disease. *Nature genetics, 41*(10), 1088-1093.

Hyde, D. (2009). A Survey on the Security of Virtual Machines. *Dept. of Comp. Science, Washington Univ. in St. Louis, Tech. Rep*.

Jansen, W. A. (2011). *Cloud Hooks: Security and Privacy Issues in Cloud Computing*.

Jin, H., Ibrahim, S., Bell, T., Gao, W., Huang, D., & Wu, S. (2010). Cloud types and services. *Handbook of Cloud Computing*, 335-355.

Jose, G. J. A., & Sajeev, C. (2011). Implementation of Data Security in Cloud Computing.

Kaushik, A. K., Pilli, E. S., & Joshi, R. (2010). *Network forensic system for port scanning attack.* Paper presented at the Advance Computing Conference (IACC), 2010 IEEE 2nd International.

Khajeh-Hosseini, A., Sommerville, I., & Sriram, I. (2010). Research challenges for enterprise cloud computing. *Arxiv preprint arXiv:1001.3257*.

Kifayat, K., Merabti, M., & Shi, Q. (2010). Future security challenges in cloud computing. *International Journal of Multimedia Intelligence and Security, 1*(4), 428-442.

Kikuchi, H., Kobori, T., & Terada, M. (2009). *Orthogonal Expansion of Port-scanning Packets.* Paper presented at the Network-Based Information Systems, 2009. NBIS'09. International Conference on.

Kim, J., & Lee, J. H. (2008). *A slow port scan attack detection mechanism based on fuzzy logic and a stepwise p1olicy.* Paper presented at the Intelligent Environments, 2008 IET 4th International Conference on.

Kirch, J. (2007). Virtual machine security guidelines. *The Center for Internet Security*.

Kiyanclar, N. (2008). A survey of virtualization techniques focusing on secure on-demand cluster computing. *Arxiv preprint cs/0511010*.

Kotsovinos, E. (2009). Method and system for automatic and remote server provisioning using virtual machine appliances: EP Patent 2,043,320.

Kramer, S., Goré, R., & Okamoto, E. (2010). Formal definitions and complexity results for trust relations and trust domains fit for TTPs, the Web of Trust, PKIs, and ID-Based Cryptography. *ACM SIGACT News, 41*(1), 75-98.

LaRoche, P., Zincir-Heywood, N., & Heywood, M. I. (2009). *Evolving tcp/ip packets: a case study of port scans.* Paper presented at the Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on.

Li, C., Raghunathan, A., & Jha, N. (2011). A Trusted Virtual Machine in an Untrusted Management Environment. *Services Computing, IEEE Transactions on*(99), 1-1.

Li, C., Raghunathan, A., & Jha, N. K. (2010). *Secure virtual machine execution under an untrusted management OS*.

Lombardi, F., & Di Pietro, R. (2010). Secure virtualization for cloud computing. *Journal of Network and Computer Applications.*

Louridas, P. (2010). Up in the Air: Moving Your Applications to the Cloud. *Software, IEEE, 27*(4), 6-11.

Luo, Y. (2010). Network I/O Virtualization for Cloud Computing. *IT Professional, 12*(5), 36-41.

Motika, G., & Weiss, S. (2012). Virtio network paravirtualization driver: Implementation and performance of a de-facto standard. *Computer Standards & Interfaces, 34*(1), 36-47.

Owens, K. (2009). Securing Virtual Compute Infrastructure in the Cloud. *white paper, Savvis Communications Corporation*.

Reuben, J. S. (2009). A survey on virtual machine security. *Helsinki University of Technology*.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*.

Sabahi, F. (2011). *Cloud computing security threats and responses*.

Sahoo, J., Mohapatra, S., & Lath, R. (2010). *Virtualization: A survey on concepts, taxonomy and associated security issues*.

Santos, J. R., Turner, Y., Janakiraman, G., & Pratt, I. (2008). *Bridging the gap between software and hardware techniques for i/o virtualization*.

Scarfone, K. (2011). *Guide to Security for Full Virtualization Technologies*: DIANE Publishing.

Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., et al. (2011). Challenges for Cloud Networking Security. *Mobile Networks and Management*, 298-313.

Smith, M. A., Pieper, J., Gruhl, D., & Real, L. V. (2008). *IZO: applications of large-window compression to virtual machine management*.

Soniya, B., & Wiscy, M. (2008). *Detection of TCP SYN Scanning Using Packet Counts and Neural Network*. Paper presented at the Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on.

SUBASISH, M., & PRASANNA, P. S. (2010). A SECURITY FRAMEWORK FOR VIRTUALIZATION BASED COMPUTING ENVIRONMENT.

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management, 30*(2), 109-116.

Sundararajan, S., Narayanan, H., Pavithran, V., Vorungati, K., & Achuthan, K. (2011). Preventing Insider Attacks in the Cloud. *Advances in Computing and Communications*, 488-500.

Tsai, H., Siebenhaar, M., Miede, A., Huang, Y., & Steinmetz, R. (2011). Threat as a Service? The Impact of Virtualization on Cloud Security. *IT Professional*(99), 1-1.

Turner, A. (2008). Andy Turner's Blog 2008-04 Web Page@ School of Geography, University of Leeds. *Thought, 2008*, 04-24.

Wang, G., & Ng, T. S. E. (2010). *The impact of virtualization on network performance of amazon ec2 data center*.

Whalen, S., Engle, S., & Romeo, D. (2009). An Introduction to Arp Spoofing., 2001.

Zeng, W., Zhao, Y., Ou, K., & Song, W. (2009). *Research on cloud storage architecture and key technologies*.

Zhang, L. J., & Zhou, Q. (2009). *CCOA: Cloud computing open architecture*.

Zhang, Y., Juels, A., Oprea, A., & Reiter, M. K. (2011). *Homealone: Co-residency detection in the cloud via side-channel analysis*.