UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name: **KAMBIZ MOHAMMAD HOSSEINI**

Date of birth : **08.05.1977**

Title : A MODEL TO ENHANCE SECURITY OF LIVE VIRTUAL MACHINE MIGRATION IN CLOUD COMPUTING

Academic Session: 2012/2013

declare that this thesis is classified as :

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

■ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

SIGNATURE	**SIGNATURE OF SUPERVISOR**
(NEW IC NO. /PASSPORT NO.)	**MAZDAK ZAMANI** **NAME OF SUPERVISOR**
Date :	Date :

"I declare that I have read this project, in my opinion this project report has satisfied the scope and quality for the award of the degree of Master of Computer Science (Information Security)."

Signature	:	
Name of Supervisor	:	DR. MAZDAK ZAMANI
Date	:	JANUARY 2013

A MODEL TO ENHANCE SECURITY OF LIVE VIRTUAL MACHINE MIGRATION IN CLOUD COMPUTING

KAMBIZ MOHAMMAD HOSSEINI

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

Advanced Informatics School (AIS)
Universiti Teknologi Malaysia

JANUARY 2013

I declare that this thesis entitled: “A MODEL TO ENHANCE SECURITY OF LIVE VIRTUAL MACHINE MIGRATION IN CLOUD COMPUTING” is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is degree and is not concurrently submitted in candidature of any other degree.

Signature :

Name : KAMBIZ MOHAMMAD HOSSEINI

Date : 10th JANUARY 2013

Dedicated to My Beloved wife

ACKNOWLEDGEMENT

IN THE NAME OF GOD, MOST GRACIOUS, MOST COMPASSIONATE

May I express my appreciation to GOD, for giving me the blessing for health, strength and earnestness to accomplish and fulfil this project report.

I would like to take this opportunity to say the highest appreciation to Dr. Mazdak Zamani as my supervisor who always gives full support and faithfulness in all guidance, advice and commitment upon on the effort for this project.

This appreciation also goes to my beloved wife, because of her uninterrupted support during my study.

ABSTRACT

Cloud Computing has become a new effective technology in IT industries to reduce the costs and increase the quality of service of any sort of services including Platform as a Service (PaaS), Infrastructure as a Service(IaaS) and Software as a service(SaaS). Virtual Machine is a basic unit of each cloud and as far as the security is concerned, maintaining and reducing the vulnerabilities of Virtual Machines is a must. In order to provide a cloud with the highest performance and least fault tolerance, VM Live Migration was introduced, and it is being used many times in a daily maintenance of a cloud, so keeping the process of Live Migration secure is a principle in securing a cloud. Different approaches have been put forward for live migration however, more investigation and concentration needs to be taken on the concept of security on them. In this research MITM attacks are analysed and a new model is introduced to enhance security of Virtual Machine Live Migration against MITM which is using SSL to secure its connection.

ABSTRAK

Pengkomputeran awan telah menjadi satu teknologi baru yang berkesan dalam industri IT untuk mengurangkan kos dan meningkatkan kualiti perkhidmatan apapun perkhidmatan termasuk Pelantar sebagai Perkhidmatan (PaaS), Infrastruktur sebagai satu Perkhidmatan (IaaS) dan Perisian sebagai perkhidmatan (SaaS). Mesin maya adalah satu unit asas setiap awan dan sejauh yang sebagai cagaran conserned, maintaning dan mengurangkan kelemahan Mesin Virtual adalah satu kemestian. Dalam usaha untuk menyediakan awan dengan prestasi hightest dan telorence bersalah kurangnya, VM Live Migrasi telah diperkenalkan, dan digunakan banyak kali dalam maitenance harian Awan 1, jadi menjaga proses Migrasi selamat Live adalah prinsip dalam mendapatkan awan.Pendekatan yang berbeza telah dikemukakan untuk Walau bagaimanapun, penghijrahan hidup, penyiasatan dan cencentration yang lebih perlu diambil ke atas konsep keselamatan kepada mereka. Dalam kajian ini serangan MITM dianalisis dan model baru yang diperkenalkan untuk meningkatkan keselamatan Migrasi Virtual Machine Live terhadap MITM yang menggunakan SSL untuk mendapatkan sambungan.

.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

OS	-	Operating System
IT	-	Information Technology
TLS	-	Transport Layer Security
SSL	-	Secure Socket Layer
CA	-	Certificate Authority
DNS	-	Domain Name System
STP	-	Spanning Tree Protocol
CAM	-	Content Addressable Memory
VM	-	Virtual Machine
MiTM	-	Man in the Middle
CPU	-	Central Processing Unit
VMM	-	Virtual Machine Monitor
JVM	-	Java Virtual Machine
TCP	-	Transmission Control Protocol
PaaS	-	Platform as a Service
IaaS	-	Infrastructure as a Service
SaaS	-	Software as a Service

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cloud Computing, one of the emerging technologies, has changed the world of IT significantly by providing more affordable and effective computer services and resources, which is beneficial for both providers and customers. There are three different distinct layers in cloud computing, system layer, platform layer and application layer and three service models, Platform as a Service (PaaS), Infrastructure as a Service(IaaS) and Software as a service(SaaS)(Foster *et al.*, 2008).

1.1.1 History of Cloud Computing

Cloud computing is a model which, provide different part of services including hardware such as servers, networks or software like applications and other aspects which could be find in data centres. By doing this users and companies, that use these services via Internet, are able to pay only for the amount of services that they need not to hire a huge server and network and pay huge amount of money for using only part of the capability of servers and pay for whole potential. In other word, it is provided to enable convenient, network access when it is necessary to a shared resources which are easy to configure and safe to use, that could be rapidly served and start services with the least need of management by customers or service provider communicating(Fogarty, 2009).

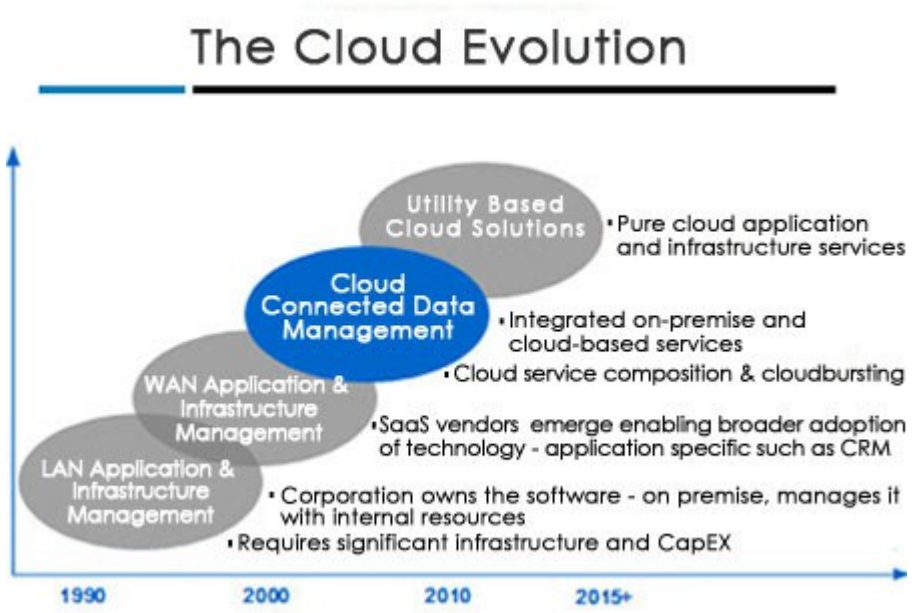

Figure 1.1 Evolution of Cloud Computing

The History of Cloud Computing went back to 1990 with an idea for making computer power easy to access with Grid Computing. In this case accessibility was supposed to be as easy as an electric power grid (Senthil Kumar S. , 2012). (Prof.

Ramnath Chellappa, 1977) used the term “cloud computing” for the first time in an academic lecture.

1.1.2 Virtualization and Virtual Machine

The most important part of cloud computing which enables it to work meet the goal of sharing resources is virtualization. Actually cloud computing use the technology of virtualization to attract businesses to provide services with decreasing the billing and increasing the quality of services. In virtualization software and hardware are simulated upon which other software runs which is famous as VM (virtual machine). Virtualization is greatly beneficial for both service provider and service users because it provides features like multi-tenancy, better server utilization, and data centre consolidation. Cloud providers are able to gain a great deal of capacity which in turn it offers better margins, moreover, cloud users can use virtualization to decrease expenditure on hardware and increase the performance (Saraswat and Rohini, 2009).

1.1.3 Virtual Machine Migration

A virtual machine is capable to be transfered from one physical machine and palced to another, in case that it is necessary (Voorsluys *et al.*, 2009). virtual machine cloning (to copy one virtual machine in different places), virtual machine relocation (just moving from one host to another) are two example of VM movement, generally these actions happen in case of maintenance or failure(Rogers

and Schroeder, 2008). Due to the ability of movement from one host to other hosts it is used in high availability and disaster recovery plans and it increases the value of using it. Figure 1.2 shows a virtual machine migration from one physical server to another.

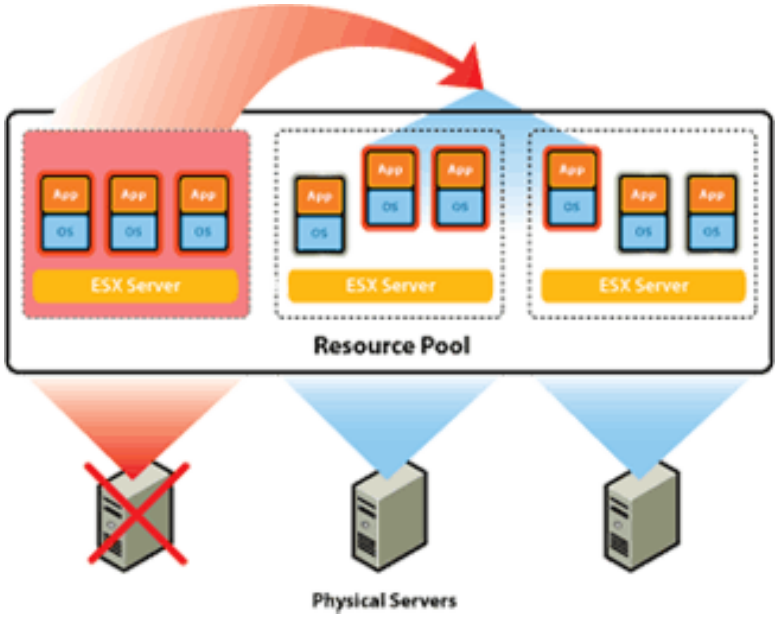

Figure 1.2: Virtual Machine Migration

1.1.4 Live Virtual Machine Migration Security

Although, advantages of cloud computing have absorbed attention of users to itself, security issues decline the pace of adoption of cloud computing. Different methods have been put forward to improve the Security of Cloud, however, still collaboration to be taken to bring peace of mind to its user. One aspect which is a concern in security in cloud is security issues during live Virtual Machine migration(Lombardi and Di Pietro, 2010).

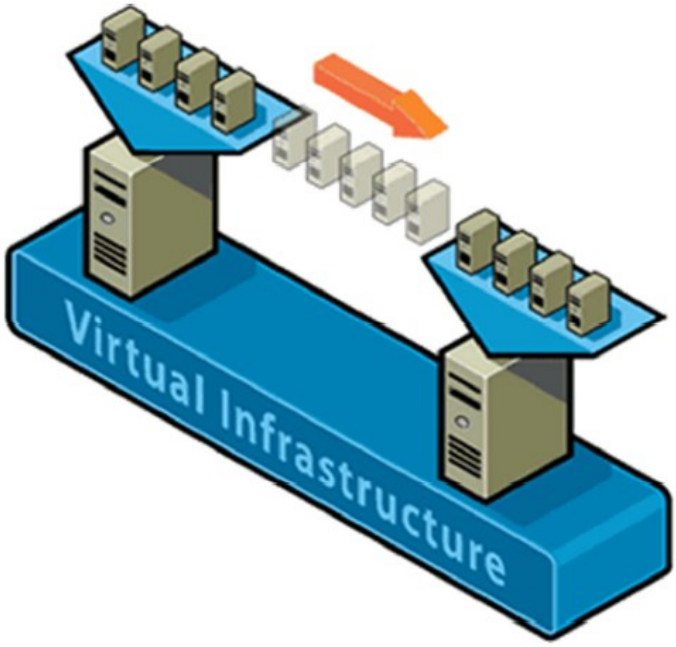

Figure 1.3: Virtual Migration

1.2 Background of the problem

There are lots of steps occur in system to perform live migration a VM however, generally it is the memory image of source server transfer to destination server (Voorsluys *et al.*, 2009). the hypervisor which is responsible to manage virtual machines pre-copies VM memory pages to destination server without disturbing the OS or applications actually users do not realize that they are serving by another server. In order to be sure that whole active memory transfer, The process of page copying is continuously occurs several times and dirty pages repeatedly are moved. Normally, the reason of repeating the process is that there are some pages that is modified during the migration process as the system is totally active, so often that the VM should be waited sometimes, until these dirty pages are fully transferred to the destination. As a result of the process, the VM can be activated in the destination server (Voorsluys *et al.*, 2009),however, it needs to be sure that no copy of data left

behind in memory and data is not compromised while it was transferring (confidentiality and integrity).

Providing integrity is the goal of securing data while they are moving. It means that data should be stopped from being modified. Moreover, another concern is to be ensuring that data remains secret when it is sending from server to client or other servers and except the sender and the receiver, no one else should be able to change or read data and in extreme case no one else should realize the data transaction. Different ways have suggested to protect data which is transferring, however, The most common and effective solution to protect it is to use encryption and authentication in order to provide a situation that data pass through in safely(Speake and Winkler, 2011).

Encryption is utilized to ensure that in case of compromising of integrity between client and server data keeps confidential. Moreover, Authentication is utilized to ensure that the data in communication of both client and server indicate that who they say, they are.

Different method of authentication use cryptography algorithm in many ways. Data transferring data by mean of programs, manual ftp, or browser by using different services like HTTPS, TLS, or SSL are different example of security protocols, which are used for that reason. PKI is used to authenticate the transaction (trusted root CAs), and encryption are used to keep the payload secure(Speake and Winkler, 2011).

1.3 Problem Statement

Different approaches have been put forwarded for VM migration, form unsecure one (just a TCP connection) to relatively secure (through SSL).the point is

that there have been several attacks for even secured one with SSL connection(El-Hajj, 2012).

1.4 Research Questions

I. What are the approaches to secure Migration of VMs to prevent Man in the middle attack in live migration in cloud computing?

II. How to design a new model for enhancement of security of VMs to prevent Man in the middle attack in VM migration in cloud computing?

III. How to evaluate the enhanced security model in migration of VMs in cloud computing?

1.5 Objectives of the Study

I. To identify and investigate approaches in secure Live Migration of VMs to keep data safe against Man In The Middle attack in cloud computing.

II. To propose and design a model for enhancement of security of VMs to prevent Man in the middle attack in VM migration in cloud computing.

III. To evaluate proposed enhanced security model in migration of VMs in cloud computing.

1.6 Project Aim

The aim of this research is to propose a method to increase confidentiality and integrity of data in motion in live VM migration and have a model for preventing Man in the middle attack and make sure that data isolation which is one of main purpose of virtualization is preserved. As a result, enhancing the overall cloud security is expected to achieve.

1.7 Scope of the Study

In cloud computing, three types of services including Infrastructure, Platform, and Software as a service are provided. this study focus on Infrastructure as a service. This research will consider security concerns of virtualization in cloud computing specially in VM migration to identify problems related to Man in the middle attack among all virtualization threats. This research would focus on Xen hypervisor which is one of the strongest and the most useable virtualization model. Xen is open source and design by Cambridge University as a research project (Barham *et al.*, 2003).

REFERENCES

Badger, L., Grance, T., Patt-Corner, R., and Voas, J. (2011). Draft cloud computing synopsis and recommendations. *NIST Special Publication.* 800, 146.

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., et al. (2003). Xen and the art of virtualization. *ACM SIGOPS Operating Systems Review.* 37(5), 164-177.

Deshpande, U., Wang, X., and Gopalan, K. (2011). Live gang migration of virtual machines 135-146.

El-Hajj, W. (2012). The most recent SSL security attacks: origins, implementation, evaluation, and suggested countermeasures. *Security and Communication Networks.* 5(1), 113-124.

Fogarty, K. (2009). Cloud Computing Definitions and Solutions.

Foster, I., Zhao, Y., Raicu, I., and Lu, S. (2008). Cloud computing and grid computing 360-degree compared 1-10.

Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., and Boneh, D. (2003). Terra: A virtual machine-based platform for trusted computing 193-206.

Lombardi, F., and Di Pietro, R. (2010). Transparent security for cloud 414-415.

Masti, R. J. (2010). *On the security of virtual machine migration and related topics.* Eidgenössische Technische Hochschule Zürich, Department of Computer Sciences.

Milojičić, D. S., Douglis, F., Paindaveine, Y., Wheeler, R., and Zhou, S. (2000). Process migration. *ACM Computing Surveys (CSUR).* 32(3), 241-299.

Oberheide, J., Cooke, E., and Jahanian, F. (2008). Empirical exploitation of live virtual machine migration.

Padala, P. (2011). Underestanding Live migration of virtual machine. *Pradeep Padala's blog*.

Rogers, D., and Schroeder, C. (2008). PROVIDING SERVICE REDUNDANCY THROUGH VIRTUALIZATION ON A CAMPUS BASED NETWORK.

Saraswat, N., and Rohini, D. (2009). VIRTUALIZATION-UNLOCKING HIDDEN CLOUD CAPABILITIES. *CHIEF PATRON CHIEF PATRON*.

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

Senthil Kumar S. , D. P., R.Ranjani. (2012). Grid Computing *International Conference on Computing and Control Engineering (ICCCE 2012)*.

Speake, G., and Winkler, V. J. R. (2011). *Securing the cloud: cloud computer security techniques and tactics*. Syngress.

Thomas, S. A. (2000). *SSL & TLS essentials*. Wiley.

Venkatesha, S., Sadhu, S., and Kintali, S. (2009). *Survey of Virtual Machine Migration Techniques*: Technical report, Dept. of Computer Science, University of California, Santa Barbarao. Document Number)

Ver, M. (2011). *Dynamic Load Balancing based on Live Migration of Virtual Machines:*

Security Threats and Effects.

Voorsluys, W., Broberg, J., Venugopal, S., and Buyya, R. (2009). Cost of virtual machine live migration in clouds: A performance evaluation. *Cloud Computing*, 254-265.

Wood, T., Ramakrishnan, K., Shenoy, P., and Van der Merwe, J. (2011). CloudNet: dynamic pooling of cloud resources by live WAN migration of virtual machines 121-132.

Zhang, F., and Chen, H. (2012). Security-Preserving Live Migration of Virtual Machines in the Cloud. *Journal of Network and Systems Management*, 1-26.