A SECURE VIRTUALIZATION MODEL FOR CLOUD COMPUTING TO DEFEND AGAINST DISTRIBUTED DENIAL-OF SERVICE ATTACK

SARA FARAHMANDIAN

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name: SARA FARAHMANDIAN

Date of birth : 08 SEPTEMBER 1984

Title : A SECURE VIRTUALIZATION MODEL FOR CLOUD COMPUTING TO DEFEND AGAINST DISTRIBUTED DENIAL-OF SERVICE ATTACKS

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**
L13487370	**Dr. Mazdak Zamani**
(NEW IC NO. / PASSPORT NO.)	**NAME OF SUPERVISOR**

“I declare that I have read this project, in my
Opinion this project report has satisfied the scope and quality for the
Award of Master Degree in Computer Science (Information Security).”

Signature :

Name of Supervisor : DR. MAZDAK ZAMANI

Date : JANUARY 2013

A SECURE VIRTUALIZATION MODEL FOR CLOUD COMPUTING TO DEFEND AGAINST DISTRIBUTED DENIAL-OF SERVICE ATTACKS

SARA FARAHMANDIAN

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

I declare that this project report entitled "A SECURE VIRTUALIZATION MODEL FOR CLOUD COMPUTING TO DEFEND AGAINST DISTRIBUTED DENIAL-OF SERVICE ATTACKS" is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

SIGNATURE:

Name : SARA FARAHMANDIAN

Date : JANUARY 2013

To My Beloved Mother, Father and my Sister

ACKNOWLEDGEMENT

First of all thanks God for his blessing that grant me the chance and the ability to successfully complete this project. Second and foremost I wish to express my deepest gratitude to my supervisors Dr Mazdak Zamani for his valuable advice and guidance of this work. His precious help of constructive comments and suggestions throughout the experiment and thesis works have contributed to the success of this project. Special acknowledgments to my examiners, Dr. Teddy Mantoro and Dr. Bharanidharan Shanmugam, for their clarifications and critics that make this study more comprehensive and valuable. Also a deep gratitude to the supervisory staff of UTM AIS with their continuous help and kind assistance during my presence in UTM AIS. I am indebted to all my good friends and classmate for their valuable help and support.

Last but not least, I would like to pay high regards to my parents, and my dear sister for their sincere encouragement and inspiration through my journey to complete this study.

.

DECLARATION of PROJECT STATUS FORM

Student Name	**:**	**Sara Farahmandian**	
Student ID	**:**	**MC101285**	
Supervisor Name	**:**	**Dr. Mazdak Zamani**	
Course code	**:**	**MCU1016**	
Academic	**:**	**Semester 3**	**Year 2012**

Title of Project : A SECURE VIRTUALIZATION MODEL FOR CLOUD COMPUTING TO DEFEND AGAINST DISTRIBUTED DENIAL-OF SERVICE ATTACKS

The above project work *has / has not**** fulfilled the necessary criteria towards the completion of the project, hence the mentioned student is *ready / not ready**** to submit the project report and orally present his/her project work.

*** **Additional Remarks**

____

SUPERVISOR’S SIGNATURE

Date :

***Choose appropriately
This form MUST be submitted a week before the drop date in the UTM academic calendar.

ABSTRACT

Cloud computing is based on three principles which are distributed systems, grid computing and utility computing. It provides high performance infrastructure according usage of Virtualization to offer capabilities such as on demand self-service, pay per use, highly scalable, rapid elasticity and huge amount of resource pools through the Internet. Everything in cloud environment is used as a service. The cloud technology transformed the desktop computing into service based computing by getting advantages of using data centers and server cluster technology. Even with all advantages which could bring for both Cloud Providers and Cloud consumers still security is one of the most significant concerns in this environment such as Confidentiality, Integrity, Availability, Authenticity, and privacy. A lack of security in Infrastructure as a Service (IaaS) as a fundamental delivery layer in cloud computing has an effective impact on the others delivery layers which are built on top of this layer. One of the most serious threats against the availability of cloud resources comes from Distributed Denial-of Service (DDoS) attack. This kind of attack is a large scalable and organized attack against availability of services and resources of the victim. This attack is launched by getting usage of sending tremendously large volumes of request to the target through the huge number of distributed compromised systems. The purpose of this study is to propose a new model for preventing disruption of available resources in terms of attack period. Based on previous research there is not a proper model that completely defense against DDoS attack, so the aim of this model is proposed to enhance the availability of cloud resources.

ABSTRAK

Pengkomputeran awan adalah berdasarkan kepada tiga prinsip yang diedarkan sistem, pengkomputeran grid dan pengkomputeran utiliti.Ia menyediakan infrastruktur sangat Prestasi penggunaan mengikut virtualisasi untuk menawarkan keupayaan seperti atas permintaan layan diri, membayar setiap penggunaan, yang sangat berskala, keanjalan pesat dan sejumlah besar kolam sumber melalui Internet. Segala-galanya dalam persekitaran awan digunakan sebagai satu perkhidmatan. Teknologi awan mengubah pengkomputeran desktop ke dalam pengkomputeran perkhidmatan berasaskan dengan mendapat kelebihan menggunakan pusat data dan pelayan kelompok teknologi. Walaupun dengan semua kelebihan yang membawa awan bagi kedua-dua Pembekal Awan dan pengguna Awan masih keselamatan adalah salah satu kebimbangan yang paling penting dalam persekitaran ini seperti Kerahsiaan, Integriti, Ketersediaan, Tha, privasi dan. Satu kekurangan keselamatan dalam Infrastruktur sebagai Perkhidmatan (IaaS) sebagai lapisan penghantaran asas dalam perkomputeran awan mempunyai impak yang berkesan pada lapisan lain penyampaian yang dibina di atas lapisan ini. Salah satu ancaman paling serius terhadap ketersediaan sumber awan datang dari Distributed Penafian Perkhidmatan (DDoS) serangan. Ini jenis serangan adalah serangan besar berskala dan teratur terhadap ketersediaan perkhidmatan dan sumber mangsa. Serangan ini dilancarkan dengan mendapatkan penggunaan menghantar pesat besar jumlah permintaan untuk sasaran melalui sebilangan besar sistem dikompromi diedarkan.Tujuan kajian ini adalah untuk mencadangkan model baru untuk mencegah gangguan sumber yang ada dari segi tempoh serangan. Berdasarkan penyelidikan sebelumnya tidak ada model yang betul yang benar-benar pertahanan terhadap serangan DDoS, jadi matlamat model ini dicadangkan untuk meningkatkan ketersediaan sumber awan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

SOA	Service Oriented Architecture
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
VM	Virtual Machine
OS	Operating System
VMM	Virtual Machine Monitor
DoS	Denial-of Service
DDoS	Distributed Denial-of Service
XML	Extensible Markup Language
HTTP	Hypertext Transfer Protocol
NIST	National Institute of Standard and Technology
APPs	Applications
CTB	Cloud Trace Back
IDS	Intrusion Detection system
NIDS	Network Intrusion Detection System
SKI	Single Kernel Image
RAID	Redundant Array of Independent Disk
TCP	Transmission Control Protocol
IP	Internet Protocol
TTL	Time to Live
FFDRF	Feedback Filtering with Dual-Resource fairness
SP	Service Provider
IDR	ID Receiver
IDPM	ID Packet Marking
IDG	ID Generator
RC	Request Checker

T	Threshold
CRU	Current Resource Usage
DC	Data Center

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud computing was a very old dreaming of computing as a service which would be used for transforming a huge portion of the IT industry, and also updated the usage of software pretty attractive as a service. It even created a great change in design and purchases of hardware and virtual technology in IT world (Armbrust *et al.*, 2010).

In recent years, this technology is basically used as a platform for sharing resources such as software, application, Infrastructure resources, and even for business processes (Zhang and Zhou, 2009).

Technology of cloud computing is based on using the internet and remote servers for preserving data and applications. Being able to use the application without any installation on personal systems by just accessing to internet is an interested part in cloud computing. High progress and integration of computer technology like a high speed microprocessor, massive memory, trustworthy system architecture and fast networks are the basic foundation of the existence of cloud computing (Jain *et al.*, 2011).

The grid computing, distributed computing and parallel computing in Service Oriented Architecture (SOA) are as application operation in cloud computing. This technology could be accessible everywhere just by using any digital devices such as laptops, smart phones, cell phones which are capable of connecting to the internet and cloud base services such as social networking, webmail and video viewing. It also allows more well-organized by following centralized storage, memory, processsing and bandwidth (Bakshi and Yogesh, 2010).

The system layer (is a virtual machine concept of a server), the platform layer (a Virtualization operating system of a server), and application layer (which include web applications) are three fundamental layers in cloud computing. Three services model which is involved in cloud computing are named as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) (Roschke *et al.*, 2009).

SaaS gave ability for users to work with their software far from any anxiety of installing and running their applications on their own systems. In addition, it gives opportunity to vendors for only using their cloud Infrastructure and platforms, which provide software applications for their customers. In fact, in SaaS it is the duty of providers to control and maintains software applications, operating systems, and computer hardware. So, users have only a limited access to application configuration such as using Email (Roschke *et al.*, 2009).

The PaaS layer provides a platform for users that their application can be run like Java platform. Actually, PaaS makes customer able to utilize of the provider's cloud infrastructure for deploying their web applications and other software by using supported vender's programming languages. The only controls and maintains that customers have been on their software applications and the other parts such as operating systems, physical computer hardware and even server applications is in the hands of providers (Roschke et al., 2009).

In fact, IaaS provides a large Infrastructure, managing networks and maintaining user's information in a protected way. In IaaS, providers by using virtualization software share their hardware among multiple customers, which refer as "multiple tenants". The customers are able to run their choices of operating systems and software applications. However, it is still the duty of providers to control and maintains the physical computer hardware (Roschke *et al.*, 2009).

In cloud computing one of the critical parts is virtualization which plays a significant role in constructing efficient and flexible usage of hardware devices. Actually, an abstraction of computer resources named as Virtualization. In recent years, Virtualization is used in majority level such as networks, and system storage, CPU, memory, application stack and databases which are also useful for improving security of systems, availability, reliability, and especially in terms of reducing costs and present a superior flexible system (Xing and Zhan, 2012).

By simulating the hardware, virtualization gave permission to multiple virtual machines to run different operating system and application on single computers which achieve multi tenancy and high scalability (Sabahi, 2011).

There are some phrases and layers which are pretty useful in virtual environments such as Virtual Machine (VM) that refers to a software computer, which exactly shows as a physical computer, for running an operating system and the other applications. Virtual machines have permission for sharing the resources of host machine but in a way which can be able to provide isolation between the virtual machines and the host (Sabahi, 2011).

An operating system which is run on the VM is named as a guest operating system. To be able to control and monitors the others Virtual machines which are running on the virtual network there is a layer called VM monitor or manager (Dong *et al.*, 2010).

The relation between cloud computing and virtualization technology is pretty crucial. In the virtual world when a client utilizes a system, actually dealing directly with a view which is present in the operating system with an abstraction of all the available physical elements (Dong *et al.*, 2010).

The clients have the ability to achieve all their necessary information from that logical view without any trouble in accessing of data. With Inspiration of this logical view description of what virtualization technology tries to do is more understandable which is building a few different logical views from a physical machine which would be used by several users at the same time. Actually, virtualization technology by engaging the structure of an isomorphism tries to map a virtual guest system to a real host. It connects two guest state and host state together (Dong *et al.*, 2010).

In a virtual environment, when clients work with a specific resources via a virtual view, it does not matter that the view is a sketch of physical resources or even just a diagram of a logic set of resources. The user is just interacted with the logic view which prepared by Virtual Machine Monitor (VMM), a layer of virtualization technology.

Although using virtualization brings more benefits in cloud computing technology, there are critical security issues which should be concerned in cloud computing such as Denial-of Service (DoS) and Distributed Denial-of Service (DDoS) attack which can demolish the availability of cloud networks by attacking to virtual servers and resources.

The biggest purpose of an attack such as Denial-of-service (DoS attack) and also Distributed Denial-of Service is to make network resources such as servers, and storage inaccessible for all intended clients. In the majority of cases of DoS attacks, the attacker usually targets sites or services, which are on high-profile web servers such as banks, credit card payment gateways and even in some cases Domain Name Servers (DNS Servers) but it is not just restricted to this field. It even used to attack on CPU, Storages, and the other resources on Networks (Cha and Kim, 2011).

One of most jeopardy threat for service availability of cloud computing is Distributed Denial-of Service. DDoS attacks actually are same as DoS attacks but in a way which a massive amount of hosts in network executes Dos attacks via a synchronized behavior to one or more targets. These kind of attacks enormously increased based on bandwidth and technique (Muhai and Ming, 2010).

In cloud, environment DDoS attacks harshly decreased the performance of cloud services. One of the usage of DDoS attacks for the attacker is that make them able to freely control information through the networks and even by creating specific information on specific time decided that which information can be accessible for clients and which one not. Base on ability which gave to intruder DDoS attacks are the number one security threats in all kinds of network and especially in cloud networks in a distributed environment which make it so attractive for attackers to compromise it (Gul and Hussain). Figure 1.1 illustrated an attacker which by getting access control to other systems creates a zombie network against a victim system.

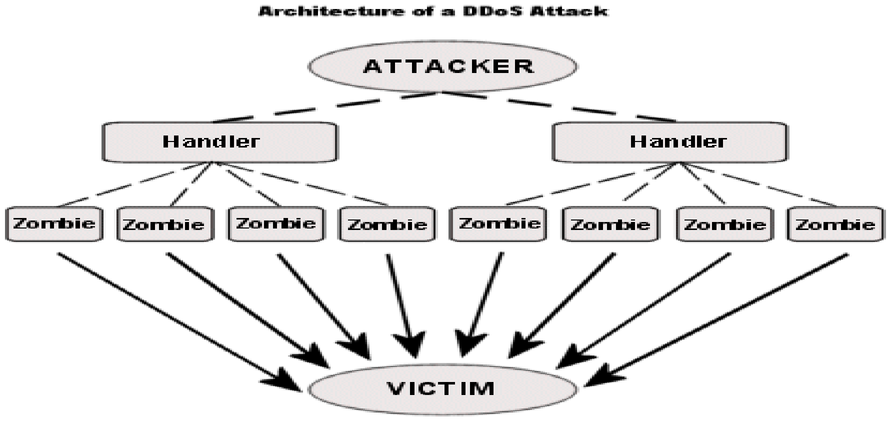

Figure 1.1: Architecture of a DDoS attack (Mirkovic and Reiher, 2004)

1.2 Background of Problem

Internet- based computing makes cloud computing abilities to share services, interfaces, and data which enable vendors to hire their space on their physical machines (Armbrust *et al.*, 2010).

Services and other interfaces shared based on customer demand. Pursuant to study based on e-crime in 2000, by the E-crime Congress in partnership with KPMG, the rate of Crime increased especially on online customer, which used cloud computing for their business. So security of cloud is a big concerned in cloud computing (Armbrust *et al.*, 2010).

In fact, with new technology always there are people who want to compromise the systems and even whole network. One of crucial attack that can bring down the entire of network in cloud named Distributed denial-of service (DDoS) which means many of systems attacks to one system in at the same time by sending exhausted request to target system. An example of such attacks is on the BitBuket.com cloud which according to a report went down for 20 h (Chonka *et al.*, 2010).

1.2.1 DDoS Attacks in Cloud Computing

VeriSign Commissioned Forrester Consulting did a survey on the manner of Distributed denial-of Service (DDoS) attacks in March 2009. In this study which was involved around 400 cases in the US and Europe was planned for preparing a quantitative data base on DDoS threats and methods which companies chosen to defense against these attacks (Cha and Kim, 2011).

Approximately 124-survey respondent's confession that their organizations had an experiment of DDoS attacks one or more which cause damage to their services. The time duration to bring back their information was different in every organization that related to policy and strategy of that particular company against such attack. For example around 64 organizations reported that it took between 1 and 5 hours for restoring their systems, whereas 41 organizations reported that time to be able to recover their services was between 5 to 8 hours (Cha and Kim, 2011).

As it shows in Figure 1.2 there are different recovering time for companies to repair themselves of the impact of DDoS attack.

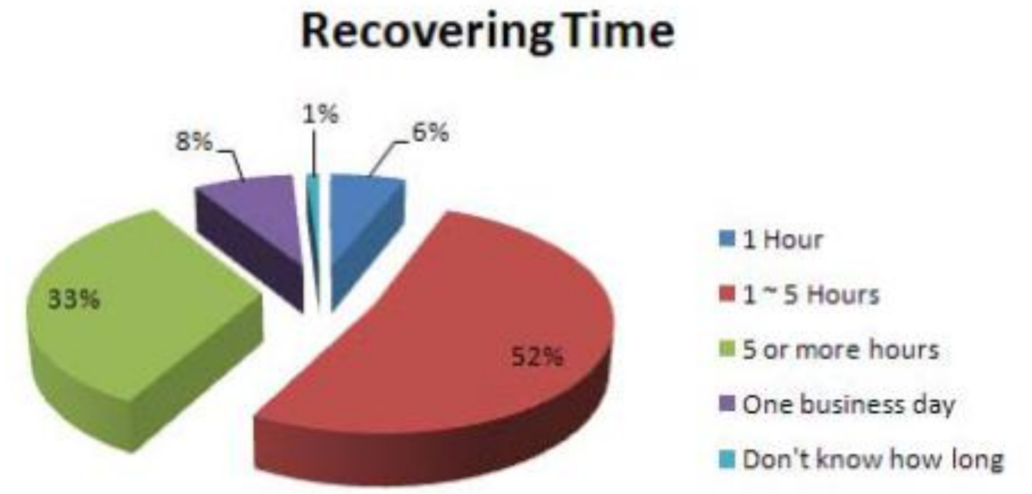

Figure 1.2: The time duration for recovering information in different organization (Cha and Kim, 2011)

There are various kinds of DDoS attack tools such as Agobot (F-Secure, 2003; Sophos, 2009), MStream (Dittrich, 2000), and Trinoo (Dittrich, 1999) that still used by attacker today. But using the less complex web based attack tools such as Extensible Markup Language (XML) based Denial of Service or even Hypertext Transfer Protocol (HTTP) based Denial-of Service attack which have simple implementation and so difficult to detect and also because lake of the existing defense method against them are more prevalent among attackers (Chonka et al., 2010).

An XML-based DDoS attack happened when a lot of XML message is sent to a web server or web service which their content poisoned with malicious codes aiming to achieve control of their resources. Such attack concentrate on disrupting availability of servers or services from legitimate user who go for accessing and using of that resource (Chonka *et al.*, 2010).

Figure 1.3 illustrated a DDoS attack in a cloud where intruder has full control over both networks and starts with sending massive numbers of XML-based message to a web server on another cloud network.

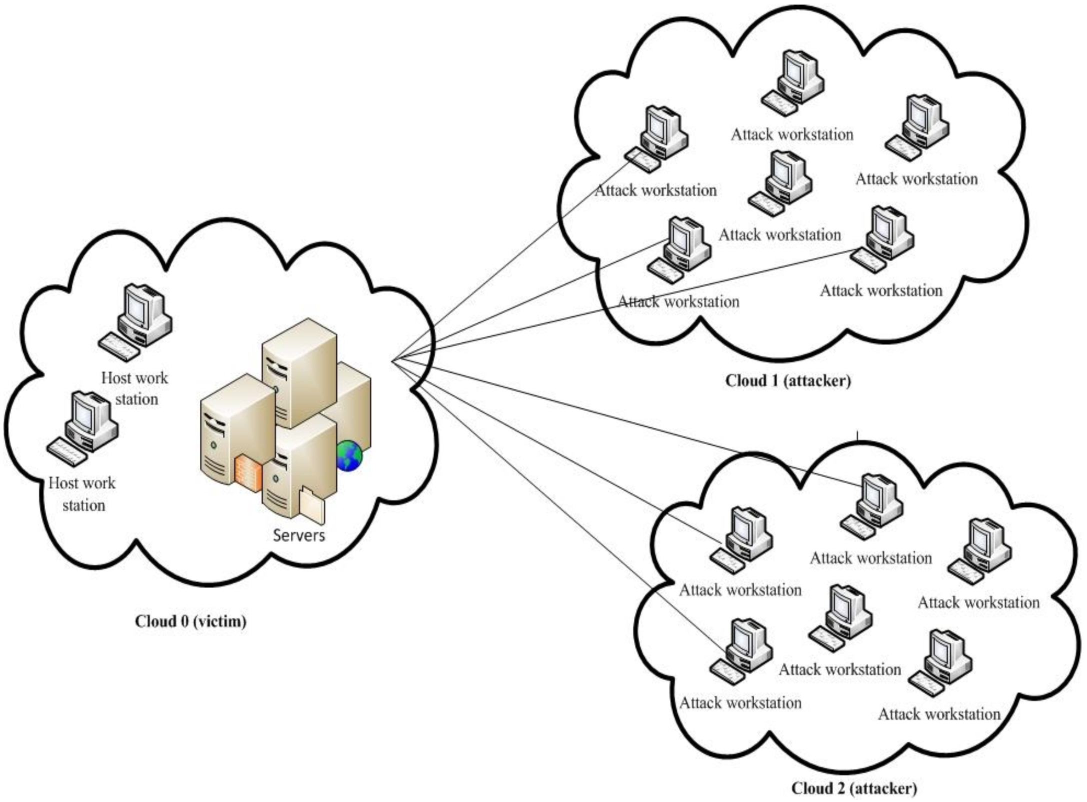

Figure 1.3: A DDoS attacks against cloud computing (Chonka *et al.*, 2010)

1.3 Problem statement

Cloud computing is based on essential portion as named virtualization which still has security vulnerabilities in the cloud networks have not adequately been studied. Even though, there are so many researches on cloud security just a few of them related to virtualization security issues such as DDoS attack which is one of most serious threat to the distributed environment. Physical resources can be shared by using virtualization such as CPU, memory disk, and network bandwidth. DDoS attack could be more successful where infrastructure shared among large numbers of Virtual machine (VM) clients. The unwanted DDoS attack occurred in terms of weak security in cloud technology and especially the level of Virtualization security in the aim of disrupting the availability of cloud resources (Sabahi, 2011).

Figure 1.4 shows the architecture of DDoS attack to a special target that it can be a pool of servers which provide services for cloud users.

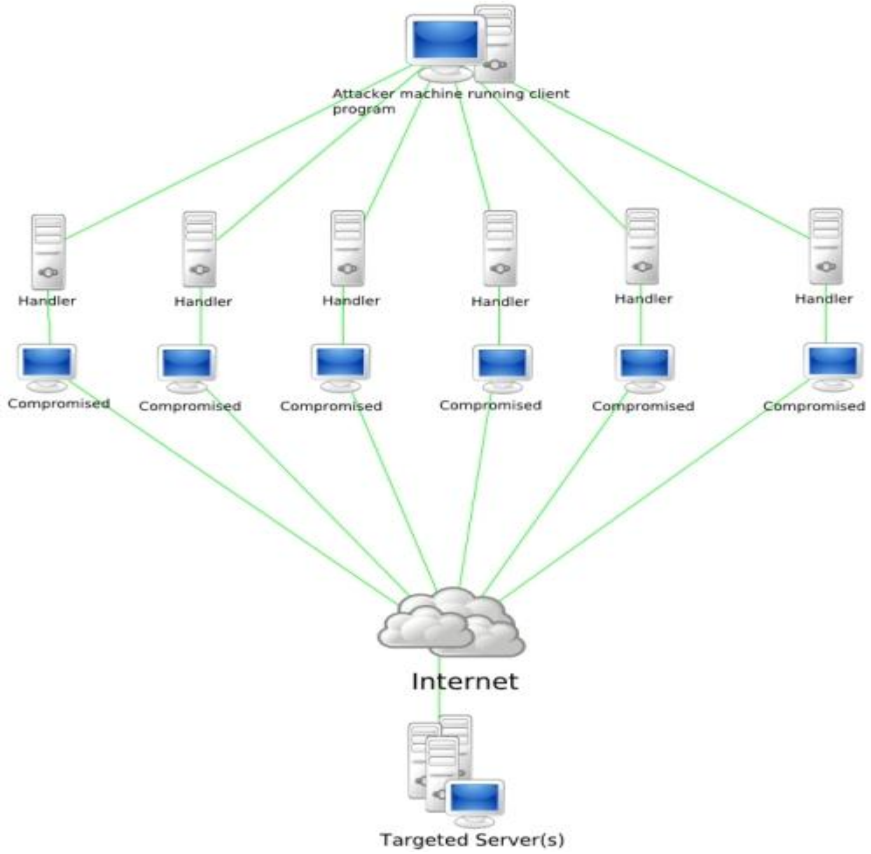

Figure 1.4: DDoS attack against cloud servers (Mirkovic and Reiher, 2004)

1.4 Project Objectives

i. To investigate previous existences defense methods against DDoS attack

ii. To propose a model for cloud computing to defend against DDoS attack.

iii. To test the proposed model which can improve the security of virtual system in cloud computing against DDoS attacks.

1.5 Research Questions

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

i. What are the approaches to defend against DDoS attack in cloud computing?

ii. How to develop a new model to enhance the security of cloud computing against DDoS attacks?

iii. How to test and evaluate the proposed model against DDoS attacks?

1.6 Project Aim

The aim of this project is to propose a model to enhance the security specially availability of cloud resources against DDoS attack. The proposed model will then be tested against the attack by simulation application.

1.7 Project scope

This project focus on security issues in cloud computing which using virtualization technology to defend against a special threat named Distributed Denial-of Service (DDoS) attack that occurred in one of service layers of cloud computing which is Infrastructure as a Service (IaaS). The public cloud is an area of research for this project. So the other types of cloud computing are not discussed in this scope.

This project is based on attacking distributed virtual machines against available resources of target victim. So the focus of this project is on the availability of resources through the cloud network.

This proposed model concentrates to prevent of occurrence of DDoS attack for disturbing cloud resources. So the detection phase of this attack is not in the area of this study. This proposed model is going to prevent disruption of cloud resources during the attack period. Also VMware will be used as a crucial technology in this area.

1.8 Summary

Security is a significant portion in a cloud environment. To make cloud perfectly secure lots of things must be done specially based on virtualized network which are used in this kind of area. Although virtualization brings numerous advantages to cloud computing, there are many security concerns which must be carefully investigated and find the best solution for them. One of most important threat to cloud is DDoS which can effect on availability of cloud and its services.

In this chapter we went through several classified groups which were as problem statement, project objectives, project scope, background of the problem, and project aim.

REFERENCES

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.

Ayres, P. E., Sun, H., Chao, H. J., and Lau, W. C. (2006). ALPi: A DDoS defense system for high-speed networks. *Selected Areas in Communications, IEEE Journal on, 24*(10), 1864-1876.

Bakshi, A., and Yogesh, B. (2010). *Securing cloud from ddos attacks using intrusion detection system in virtual machine*, 260-264.

Cha, B., and Kim, J. (2011). *Study of Multistage Anomaly Detection for Secured Cloud Computing Resources in Future Internet*, 1046-1050.

Chiueh, S. N. T. (2005). A survey on virtualization technologies. *RPE Report*, 1-42.

Chonka, A., Xiang, Y., Zhou, W., and Bonti, A. (2010). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of network and computer applications*.

Dong, H., Hao, Q., Zhang, T., and Zhang, B. (2010). *Formal Discussion on Relationship between Virtualization and Cloud Computing*, 448-453.

Furht, B., and Escalante, A. (2010). *Handbook of cloud computing*: Springer-Verlag New York Inc.

Gul, I., and Hussain, M. Distributed Cloud Intrusion Detection Model.

Gul, I., and Hussain, M. (2011). Distributed Cloud Intrusion Detection Model. *International Journal of Advanced Science and Technology, 34*, 71-82.

Hamlen, K., Kantarcioglu, M., Khan, L., and Thuraisingham, B. (2010). Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP), 4*(2), 36-48.

Jain, P., Rane, D., and Patidar, S. (2011). *A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment*, 456-461.

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

Karnwal, T., Thandapanii, S., and Gnanasekaran, A. A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack. *Intelligent Informatics*, 459-469.

Kim, D., Kim, B., Kim, I., Kim, J., and Cho, H. (2012). Endpoint Mitigation of DDoS Attacks Based on Dynamic Thresholding. *Information and Communications Security*, 381-391.

Kim, Y., Lau, W. C., Chuah, M. C., and Chao, H. J. (2004). *PacketScore: Statistics-based overload control against distributed denial-of-service attacks*, 2594-2604 vol. 2594.

Laplante, P. A., Zhang, J., and Voas, J. (2008). What's in a Name? Distinguishing between SaaS and SOA. *It Professional, 10*(3), 46-50.

Maveli, N. S., Walter, R. A., Costantino, C. L., Roy, S., Alonso, C., Pong, M. Y. W., et al. (2002). Method and apparatus for virtualizing storage devices inside a storage area network fabric: Google Patents.

Mell, P., and Grance, T. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology, 53*(6), 50.

Mirkovic, J., and Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53.

Muhai, L., and Ming, L. (2010). An adaptive approach for defending against DDoS attacks. *Mathematical Problems in Engineering, 2010*.

Reuben, J. S. (2007). A survey on virtual machine security. *Helsinki University of Technology*.

Roschke, S., Cheng, F., and Meinel, C. (2009). *Intrusion detection in the cloud*, 729-734.

Sabahi, F. (2011). *Virtualization-level security in cloud computing*, 250-254.

Sahoo, J., Mohapatra, S., and Lath, R. (2010). *Virtualization: A survey on concepts, taxonomy and associated security issues*, 222-226.

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

Subashini, S., and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications, 34*(1), 1-11.

Wei, W., Dong, Y., and Lu, D. (2008). *Optimal control of DDoS defense with multi-resource max-min fairness.* Paper presented at the Cybernetics and Intelligent Systems, 2008 IEEE Conference on, 1285-1293.

Xing, Y., and Zhan, Y. (2012). Virtualization and Cloud Computing. *Future Wireless Networks and Information Systems,* 305-312.

Zhang, L. J., and Zhou, Q. (2009). *CCOA: Cloud computing open architecture,* 607-616.

Zhang, Q., Cheng, L., and Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7-18.

Zhao, S., Chen, K., and Zheng, W. (2009). *Defend Against Denial of Service Attack with VMM.* Paper presented at the Grid and Cooperative Computing, 2009. GCC'09. Eighth International Conference on, 91-96.