Research on a Security Enhancement System for Cloud Service of Cloud Computing Environment

Young-Sung Cho,Wonshik Na

Abstract*: *Lately, a DDoS attack paralyze Internet systems with access attacks and conquer the network itself. We need a solution to build a security enhancement system for cloud computing service.The proposed method uses the desktop PCs to enhance the information security for cloud service through two network separation to defend against cyber attacks. One is physical network separation using 2 PCs using hypervisor architecture, select the network using KVM(Keyboard, Video monitor, Mouse) switched controller to select the network. The other is logical network partition using one PC with two kind of OSs, but network is divided through virtualization. Though a DDoS attack occurs on the HOST PC2 of the external network, the CPU and memory for the internal HOST PC1 are not affected by DDoS attack. It is confirmed that the CPU and memory for the internal network and the external network are processed independently of each other. The results of HOST CPU usage and PC1 memory usage measured during DDoS attack on HOST's PC2 were measured low because they were not executed in normal network environment. The HOST PC2 malicious code infection caused HOST PC1 CPU usage and memory usage to be measured with low performance and HOST PC1 performance will not change. It can be seen that the CPU usage of PC2 increases rapidly when it is infected with malicious code of HOST PC2. It is confirmed that the internal and external network for the HOST PC operate independently of each other through CPU and memory overload test. The proposal system using network separation is a security enhancement system that can provide security information about cloud service of cloud computing environment for cyber attack.

Index Terms*: *DDoS, Cloud Computing, Cloud Service, Visualization, Network Separation

I. INTRODUCTION

Nowadays, DDoS attacks paralyze Internet systems with access attacks and spoofed traffic to steal information through security boundaries and conquer the network itself.Network separation has the effect of blocking the attack from the outside and risk of leaking internal information but the inconvenience caused by that also exists. Recently, military data of South Korea has been leaked, including confidential information from the military. Military intranets were hacked by North Korea. "The code used for cyber attacks is similar to those used by North Korean hackers in the past," the ministry said.So, network-linked equipment solution was created and a number of national organizations and companies adopt network separation and network link altogether recently has beenconsidered for the security enhancement system and the protection of medical healthcare information. For examples, as the security enhacement system and the protection system of medical healthcare information, CloudHIS is designed to maximize resource pooling and sharing through visualization. It allows cloud service providers to minimize the maintenance costs of their cloud data centers and provide a high level of service at a reasonable cost-per-cost.IT resources is effectively managed and widely used cloud computing services, which are expanding more than ever and are expected to be actively researched on cloud computing security[1]. It is safety information integration system based on IaaS cloud computing based on security information.Cloud computing becomes a true trend in a cost-effective enterprise IT service model[2].In this paper, we review the cloud computing and security enhancement using networkseparation. Users need a solution that can protect confidential information that they can block from hackers.We make the adaptive solution to prevent hacking to configure security enhancement system for cloud service. Finally, we can suggest the adaptive confiuration of security enhancement system for cloud service of cloud computing environment to cope with a cyber-attack.

The development on Internet spends a large data in the cloud computing environment[3].The cloud is the integration of computing devices. It includes hardware and software infrastructure to provide reliable, cost-effective and continuous high-speed access computational ability. We can change the way of computing and data.It follows the path from standalone systems to highly-linked clusters, enterprise-class clusters, and geographically distributed computing environments.Electronic identity applications and developments in the cloud service platform enable more efficient use of the cloud service platform[4]. In this part, we can review the concept of cloud service and the visualization to consider computing service for security enhancement system for cloud service of cloud computing environment. Cloud computing is usually described by two ways as follows. It is offering the cloud location and the cloud service as well. First, it takes some kinds to make the cloud location such as public cloud, private cloud, hybrid cloud, and community cloud. Cloud computing model is convenient to network access on-demand for a shared pool of computing resources[3].There is a study on prediction models for

Revised Manuscript Received on May 23, 2019.

Young-Sung Cho, Professor,Department of Computer Engineering Education, NeoInTec Research Institute, 353, Yeok-Jun Ro, Siheung-City, Kyonggi-do, 15026, Republic of Korea

WonshikNa(Corresponding author), Professor, Department of Computer Science, Namseoul University, 91, Daehak-ro, Seonghwan-eup, Seobuk-gu, Cheonan, Chungcheongnam-do, 31020, Republic of Korea

computing end-to-end QoS values for vertically configured services consisting of three cloud services[5].Next, there are some kinds of cloud servicesas cloud computing framework as seen in Table 1.

Table 1 : The type of cloud computing framework

Service Type	Service Unit	Service Resource	Examples
SaaS(Software-as-a-Service)	Application	Business application, Web service, etc.	Gmail, Google Apps, Facebook etc.
PaaS(Platform-as-a-Service)	Platform	Software framework, Storage, etc.	GooleAppEngine etc.
IaaS(Infrastructure-as-a-Service)	Infrastructure	Computation device(VM), Storage, etc.	NaverNDrive etc.
	Hardware	CPU, Memory, Disk, Network, etc.	Amazon Data Center etc.

We can briefly explain three service models of cloud computing as follows.

- SaaS (Software as a Service): In this case, the providermakes your customers use only their own applications. The software interacts with the user to use the application. The software interacts with the user through the user interface.

These applications are web-based e-mail, applies to applications like Twitter[6]. The SaaS provider that subscribers can access both resources and applications.You do not need to have a physical copy of the software to install on your device for you.

- PaaS (Platform as a Service): PaaS providers give subscribers how to accesss components required todevelop and operate applications through the Internet.This is a collection of software and development tools hosted on the providers' servers. The Google app is one of the most popular Platforms as a Service providers. It is an application for development and deployment platform that is delivered as a service to the web by developers.It has several functions of services including application design, application development, testing, deployment and hosting, as well as application services integration.

- IaaS(Infrastructure as a Service) : IaaS creates servers, storage, and networks into virtualized environments, and enable them to use infrastructure resources as needed. Instead of purchasing servers, software, data centre space or networkequipment, clients can buy these resources as outsourcedservice. In other words the client uses the third partyinfrastructure services to support its operations includingstorage, hardware, servers and networking components.For example, IBM's bare metal cloud is an example. Typical technologies include server virtualization and desktop virtualization.

There are two kind of logical network partition: SBC(Server-based Computing) and CBC(Client-based Computing) according to the base of virtualization. Physical network partition is using one PC to connect to internet for external businesses, and the other for internal work without connecting to the internet. It has the merit of good safety as well excellent security. Logical network separation combines virtualization technology with a network already built, the use of the Internet in a single user PC. It is a technology that enables the use of internal business network based on virtualization technology, mainly by virtualization.It is divided into internet area and internal area, and it is possible to separate the business area from one PC through network separation of virtualization area. Network separation is logically constructed using network virtualization [7,8,8,10].VDI-based network separation is a virtualization of the desktop to the server, which provides on-line.It does not support physical network separation. Security policy enforcement and centralized control are used, and adaptation time is needed.The virtualization-based technology is a method of accessing a server through a user authentication or a secure area access method.A series of processes that are downloaded can not escape from a central server or a security zone,Event history management is possible, and data and user management are possible according to enterprise security policy.

- Logical Network Separation: The server-based logical network separation uses SBC to connect to a server equipped with a virtual machine and uses the internal business network. When the Internet is used, the existing PC is used in the same manner as the environment. It is a method that each user PC connects to a central server and processes work by centering a server equipped with a virtual machine [11,12,13] such as VMware. Users must access the business virtual machine server for internal business processing, and documents created or viewed can not escape from the central server, preventing document leakage.This method requires only one physical PC, and the central server controls each work environment for high maintenance efficiency.This means that if the storage device of the PC is damaged, the work can not be performed immediately, and if there is serious risk, the entire data may be lost. Also, it takes time to repair the PC, reinstall the operating system, reinstall the business software, and during this time, the work is paralyzed and the continuity of the business is deteriorated, but even if the PC is physically damaged. If you have a PC, you can work immediately. All the data and work environment is stored in the server, and since it can be used only by connecting to the central server, it can work in mobile environment instead of PC.

- SBC (Server Based Computing) :It uses a PC terminal to connect to a server that has a virtual machine installed in the center, and uses the application program of the server and stores data.The advantage is that the user's work is performed on the server and can be controlled by the centralized management of the server.The disadvantage is that there is no utilization of user PC and many users use

the server, which can cause data sharing and work environment violation.

- CBC (Client Based Computing) : It is separation of servers based on centralized desktop virtualization. It is used for the hypervisor of the central server. It is a way to use a virtualized OS running on the user server using a client connection program installed on your PC.When the client OS for each user is packaged using the profile and application information of the user and stored in the server storage to execute the client program installed in the user PC. The comparison between the physical network and the logical network is seen in Table 2.

Table 2 : The comparison between the physical network and the logical network

division	system	strength	weakness
physical network separation	. using 2 different PCs ·	. highly secure	· high cost(networks, PCs)
			· Increase the space andenergyconsumption
			. security management is required for additionalequipment
	.network switchingdevices used	. highly secure	. high cost(networks, PCs)
		. suitable for limited officespace	. declining work effiency(user hostile as reboot)
logical network separation	. Internet network separation based on server virtualization	. user control andmanagement policy to beapplied in batches	. high cost
			. internet traffic in crease as mass transactions
		. mininization malwareinfections	. compatibility of security programs should be reviewed
	. biz. network separation based on server virtualization	. centralized managementof business data coursepreventing internalinformation leakage	. high cost
			. biz. network traffic increase as mass transactions
		. user control andmanagement policy to beapplied in batch	. compatibility of securityprograms should be reviewed
	. internetnetwork separation based on terminalserver	. integrate securitymanaging would bepossible for settingsecurity level of terminalservers	. high cost
			. internet traffic increase as mass transactions
			. countermeasures tovulnerabilities and malwareinfections are required
	. Internet network separation based on PC virtualization	. user control and management policy to be applied in batches	. compatibility of security programs should be reviewed
		. low cost	. other network equipment areneeded

- Client-based Virtualization Network Separation :It is based on virtualization, but it is a method of virtualization on a personal desktop rather than a server. By using two NICs, they are allocated to the host operating system and the virtual machine, respectively.Compared to the SBC method, there is no merit of centralization of data and central control, but it has the advantage of using all hardware resources of user PC. The following two configuration methods are introduced. The first, virtualize the PC desktop OS to configure the host OS and guest OS, and separate networks by setting up different networks for each area. The O.S is not required additionally, a virtual space is created on the currently used the O.S, and only applications executed in the virtual space are connected to the Internet, thereby realizing network separation. Since this method does not use much system resources, it can be applied to a basic PC any number of times, so that network separation can be constructed at a minimum cost. The second, it uses a separate virtual network for two or more operating systems using the client hypervisor.

- Physical network separation: It is to connect the PCs to each network physically to block access paths from both the Internet and business networks; i.e., it is divided into an Internet network and an internal business network physically. Finally, it has high security, but, the separation of the physical network requires a separate network, PC and network equipment as well. It can degrade efficiency using dual PCs.

- Virtualization based multi-user connectivity :It looks like one PC in appearance, but it consist of two PC structures based on one PC motherboard inside; By physically duplicating the HDD, NIC, VGA, and USB hubs.It allows two different operating systems to run on a single board PC. Multi-user can configure one PC environment to be used independently.

The network separation is performed by separating the internal network and the external network to prevent intrusion into the outside and to prevent leakage of internal information.Malicious code infections may not be completely blocked even when the network is disconnected. For example, the following managements are suggested as effective security management to maximize the effectiveness of network separation. The security management for configuring a system based on network separationis as follows:

- PC security management :It is necessary to separate the PCs that access the Internet network and the business network, and perform security management for the Internet PC and the business PC, respectively.

- Using Internet Mail :The mail server for sending / receiving external e-mail is connected to the business network is separated and accessible only from Internet PC.

- Patch Management System Management : The patch management system operates separately from external internet.

- Network access control : The unauthorized devices (PC, notebook, etc.)It must be controlled so that it can not be connected.

- Auxiliary memory management : The authorized auxiliary enterprise devices (USB memory, CD, removableHard disk, etc.).

- Data transmission between networks: The data transmission or disclosure between Internet PC and business. The data transmission between

real-time business connected servers and so on.

- Operate peripherals printers-like : The peripherals printers-like should be operated separately for the Internet network or business network.

II. PROPOSED WORK

A. Our Proposal for Configuration of SecurityEnhancement System

Virtualization improves information security for cloud service by creating physical and logical network separaration solution to create adaptive solutions that prevent hacking based on network separation. Security enhancement systems are created by desktop PCs to enhance information security for cloud service through network separation in a physical and logical way.We can consider the network separation method to improve the security of information for the cloud computing system to cope with a cyber attack. There are two network partition; One is a physical network partition using two PCs using a hypervisorarchitecture as Xen HVM, and uses a KVM (keyboard, video monitor, mouse) switch controller to select the network. The other is a logical network partition using one PC with two OSs, but the network is partitioned through virtualization. One is physical network partition using 2 PCs using hypervisor architecture, select the network using KVM(Keyboard, Video monitor, Mouse) switched controller as the Hybrid PCI Contoller and the other is logical network partition using 1 PC with 2 OS, but network is divided through virtualization as follows Figure1.

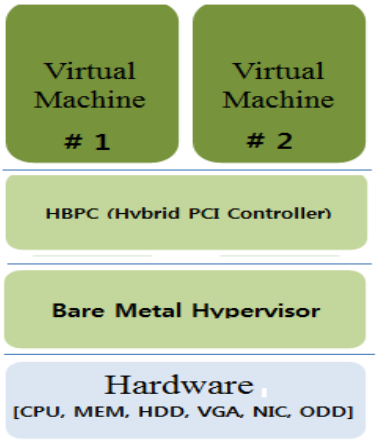

Fig1 :The system configuration for virtualization based multi-user

We can apply the PCI Pass-through method to assign the actual PCI device directly to the virtual machine. Virtual machines use their own virtual address space and support PCI passthrough, which allows them to connect to VT-D for physical H / W and virtual machine 1: 1 connections with I / O performance enhancement technology. The PCI pass-through method of the motherboard's BIOS and virtualization kernel is fully supported. So far, virtualization provides 60-70% utilization for hypervisors, but there is no technology that can optimize related servers and clients involved [14]. We can configure the PCI pass-through on the motherboard's BIOS and virtualization kernel to fully support it through the hypervisor. So, we propose an adaptive structure of security enhancement system using network separation for cloud service of cloud computing environment to cope with a cyber attack. Our suggestion is needed to isolate the physical network from the virtual desktop service using HW direct allocation to overcome some problems. The proposed system provides two operating system environments by dualizing HDD, NIC, VGA and USB on one motherboard. It is a dual PC that solves heat, power consumption, space problems, costs and a physical network separated physical network.The proposed system is an independent desktop used to access an Intranet or the Internet using the virtualization technology of a physical desktop computer. The system can also support network separation without compromising the ability to cope with cyber attacks.We did the experiment of the proposed system for the cause of performance degradation to inspect network packets for the logical network separation.

B. The security design for configuring a system based on network separation

The malicious code infections may not be completely blocked even when the network is disconnected. For example, the following managements are suggested as effective security management to maximize the effectiveness of network separation. The security management for configuring a system based on network separationis as follows:

- Internet PC security management (URL filtering) :Internet PC can not generate and store information related to business. External e-mail and web server connection are performed only through internet PC.- Access to internet sites that are not related to business should be restricted by using security system.

- Business PC security management : The Business PCs can create and store business-related information, and block access to the Internet, including external e-mail and Web server access.The portable devices such as notebook computers should be prevented from connecting to unauthorized auxiliary memory devices such as restriction on use of business PC, blocking of wireless Internet connection, smart phone, USB. We should permit data access on the work PC using the manganese data transmission system with limited administrator approval.

- E-MAIL :The mail server that sends and receives Internet mail should be constructed in the Internet network area and accessible only from the Internet PC to prevent the harmful network from malicious code infection.If private mail is required for the company, it should be built and operated in the business network separately and the access of the Internet PC should be blocked.Th mail server blocks malicious code or spam mail.

- Patch management system :Patch management system should block external

internet connection and install and operate in internet and business network for security enhancement.The patch file is manually downloaded by the administrator and verifies the integrity verification and infection of the malicious code and applies it to the patch management system.The Patch Management System performs network access control (server access control) so that it can access only from the authorized administrator PC.Patch performance log management should be done for more than 1 year (integrated log management).4) Patch management systemPatch management system should block external internet connection and install and operate in internet and business network for security enhancement.The patch file is manually downloaded by the administrator and verifies the integrity verification and infection of the malicious code and applies it to the patch management system.The Patch Management System performs network access control (server access control) so that it can access only from the authorized administrator PC.- Patch performance log management should be done for more than 1 year (integrated log management).

- Network access control : The network access control only permits access of the devices (PC, northbook) to the Internet network and the business network, thus preventing the network-to-PC inter-network use. The network access control is controlled by network access control (server access control). The log record of network access control history management should be kept for more than 1 year (integrated log management).

- Auxiliary storage management :Only the authorized auxiliary storage device (USB, CD, hard disk, etc.) is used to prevent important data stored on the PC from being leaked to the outside.It should be used for Internet PC and work PC.Network access control (server access control) so that the management server can access only from the authorized administrator PC.When using the authorized auxiliary storage device, record the data transmission history for more than 3 years (integrated log management).

- Manganese data transmission : The transmission control server is constructed for internet network and business use respectively, and data transmission is performed only through transmission control server. The transmission control server performs data transmission and service linkage code checkingWhen transmitting data using secure USB, prohibit the use of USB as security USB after registering general USB etc. on management server. Insert secure USB into Internet PC and
work PC to identify and authenticate users and automatically detect malicious code Set up a vaccine program to scan. The perform security measures against loss of security USB. The secure USB / Internet Log records of data transmission between PC and work PC should be kept for more than 3 years (integrated log management).

- Peripherals such as printers : The printers and other peripherals should be installed in the Internet and business networks. In case of sharing, additional equipment such as a printer server should be used. The security should be enhanced by using a different connection port.The printer server controls network access so that it can be accessed only from an authorized administrator PC.The printer server performs identification and authentication so that only authorized administrators can connect to it, and remote access from the outside such as a service company isprohibited.

III. EXPERIMENT & RESULT

The experiment for systen in network separation consist of the seven items (ICMP communication, shared folder access, port discovery, DDoS attack, malware infection, CPU and memory overload, SSH and FTP access) for access control and independence testing and performance testing. Then check the results.

A. Application Analysis for Experiment

Typically, the network separating system can perform tests on multiple items for access control, independent testing, and performance testing, as shown in Table 3.

Table 3 : Testing and checking items for the network separating system

Testing item	The aim of testing	Points to be checked
ICMP communication test	Internal and external network independence test using ICMP	Confirm that the internal network and the external network of the HOST PC are independent from each other using the ICMP communication test.
Shared Folder Access Test	Mutual access control test of internal and external network for accessing shared folder	Through mutual access experiment of shared folder, the internal and external network of HOST PC is confirmed that it is independent.
Port inspection test	Access Control Experiment Using Port Scanning (Zenmap) for Internal Network Hacking Through the Internet	Through the port scan test, the internal and external networks of the HOST PC is confirmed that it is independent.
DDoS attack test	Internal network CPU and memory independence test due to DDoS attack through external network	Through the DDoS attack, the internal and external networks of the HOST PC are independent of each other.
Malicious code infection test	Internal network CPU / memory independence test due to malicious code infection through external network	Through the malicious code infection test, it is confirmed that the internal network and the external network of the HOST PC are independent from each other.
Access control test in network separation such as CPU and memory overload	Internal and external network CPU and memory overload due to external network CPU and memory overload test	CPU and memory overload tests confirm that the internal and external networks of the HOST PC operate independently of each other.
SSH and FTP access testing	Kernel environment access control test using SSH and FTP connection tool:	Through SSH and FTP kernelenvironment connection, it confirms that the HOST PC is safe from external access.

B. Experimental Environment for System in Network Separation

In this paper, we focuse on experiments of hacker attacks through the application analysis for experiment.The experiment of hacking test should be measuredto cope with a cyber-attack. The Internal network and the external network Independent testing results for hacking measures.Several kinds of testing such as independent testing, access control testing, CPU and memory independence testing, inter-access control testing, etc. Thease testing results should be confirmed by prepared method to cope with a cyber-attack as follows.The basic experimental environment for the system using network separation was constructed as seen in Figure 2.The DDoS experimental environment for the system using network separation was constructed as seen in Figure 3.

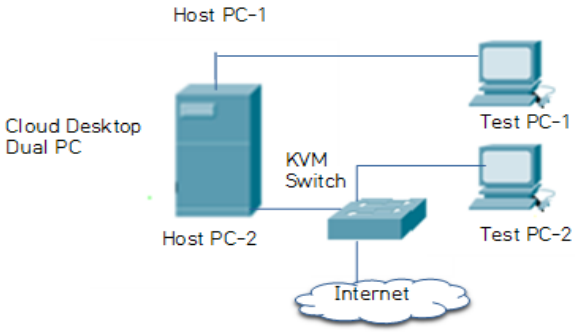

Fig2 :The configuration of the basic experimental environmentfor system in network separation

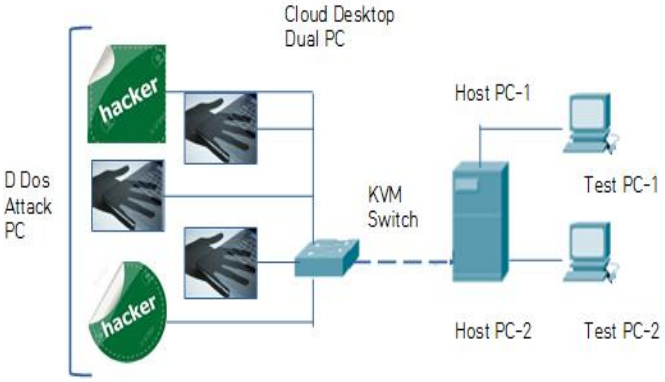

Fig3 : The configuration of the DDoS experimental environmentfor system in network separation

C. Experiment & Result Analysis for a Cyber Attack

We should perform an experiment of hacking tests to cope with a cyber attack. We can apply two script test tools and remote desktop processing. First, there is the "internet-startall.cmd" script that can run three websites simultaneously. Second, it is a script that allows you to run five office files "office-startall.cmd" with different extensions at the same time. The results of the independence test against the DDoS attack shall conform to the security certification procedure according to the DDOS test environment.

1) We check the independent test result for CPU and memory in internal network, due to DDoS attack through external network even if DDOS attack occurs in HOST PC2 of external

network.The CPU and memory of the internal network HOST PC1 are not affected by DDoS, and the CPU and memory of the internal network and the external network are confirmed to be processed independently of each other. The following is the result of measuring HOST's CPU usage and memory usage for PC1 during DDoS attack against HOST's PC2. The results of the remote desktop execution test were measured lower because it was not running in a normal network environment, as shown in Figure 4.

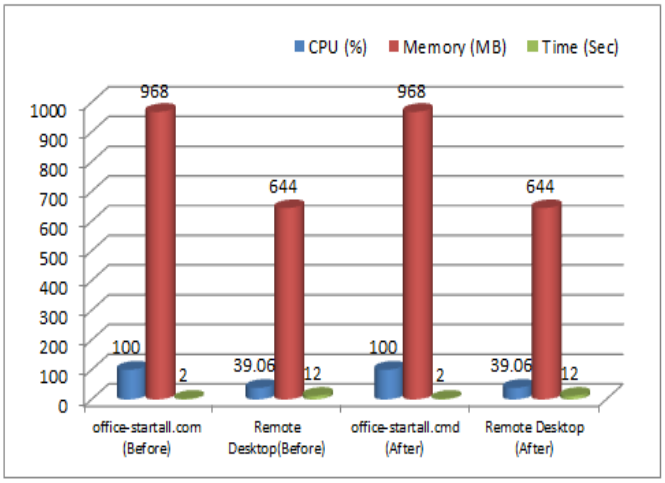

Fig 4 : The result of CPU usage and memory usage for PC1 of HOST before and after during the DDoS attack of PC2 of HOST

2) This is the result of measuring CPU usage and memory usage of HOST PC2 during DDoS attack against HOST's PC2. There was little change in CPU usage and memory usage due to network overload after a DDoS attack, as seen in Figure 5.

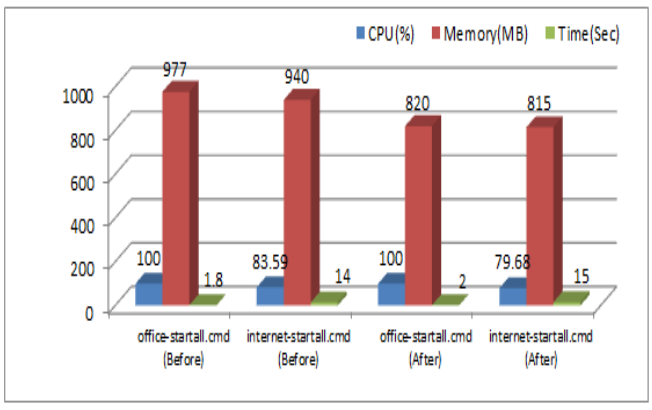

Fig 5: The result of CPU usage and memory usage for PC2 of HOST before and after during the DDoS attack on PC2 of HOST.

3) This is the result of measuring CPU usage and memory usage of HOST PC1, due to infection of HOST PC2 malicious code. Test results for execution were measured at low performance because they did not run in a typical network environment. The performance of the HOST PC1 due to malicious code infections of HOST PC2 is not changed as shown in Figure 6.

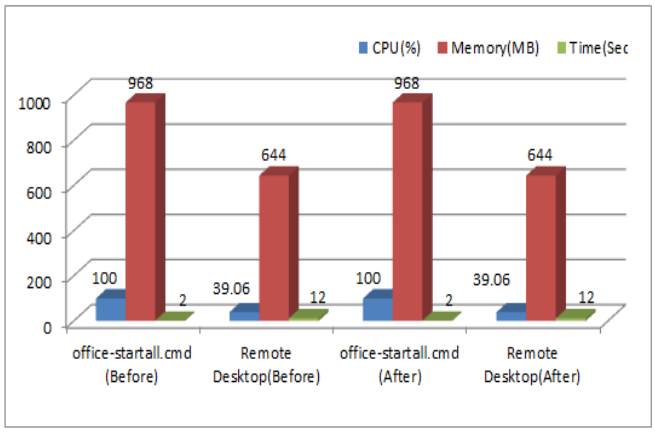

Fig 6 :The result of CPU usage and memory usage for PC1 of HOST before and afterby malicious code infection of HOST PC2

4) It is a result of measuring CPU usage and memory usage of HOST PC2, due to malicious code infection of HOST PC2. If the CPU usage rate of HOST PC2 is infected with malicious code of HOST PC2, it can be seen that it increases rapidly, as seen in Figure 7.

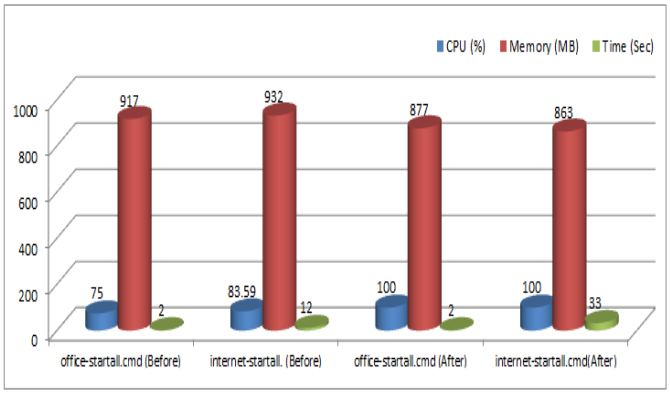

Fig 7 : The result of CPU usage and memory usage for PC2 of HOST before and afterby malicious code infection of HOST PC2

5)We make independent tests on CPU and memory on internal and external networks, due to CPU and memory overload on the external network. We make sure that the internal and external networks of the HOST PC work independently of each other through CPU and memory overloadingtests, as seen in Figure 8. This is the result of a test to check whether each of the CPUs of the HOST PC2 is affected when they are overloaded. We confirmed that the test results do not affect each other and operate independently.

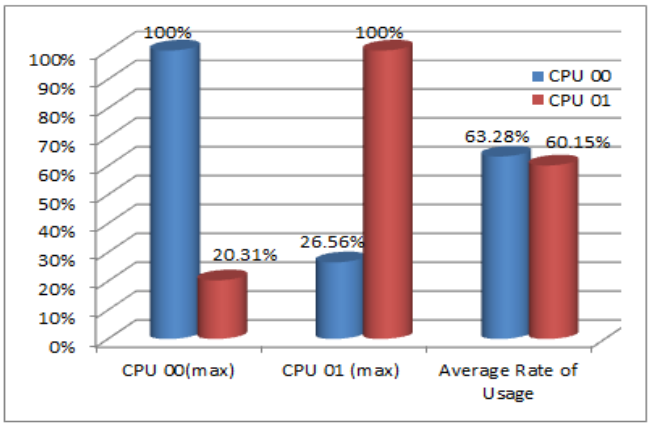

Fig 8 : The result of overloading measurement on each CPU of HOST PC2

IV. CONCLUSION

We proposed adaptive configuration of security enhancement system using network separation for security enhancement which can be information protection for cloud service that can cope with cyber attack. Build a physical network to obtain an adaptive solution to prevent hacking to build a security-enhanced system for cloud service of cloud computing environment, and apply logical network separation to the network using virtualization. We conduct experiments on common task processing based on network separation using ICMP for each network and produce some results reports. In order to cope with the cyber attacks, we prove and verify the results of testing the security enhancement system for the cloud service in the network separation environment. As a result, the results of the tests to cope with cyber attacks have ensured safety. We have been able to implement a cloud desktop dual PC server without degrading the security enforcement system in a network separation environment as a system for cloud service that can cope with cyber attacks. In the furure, our proposing system will become a more safesystem as security enhancement solution that can provide secure informationfor cloud service of cloud computing environment to cope with a cyber attack.

ACKNOWLEDGMENT

Funding for this paper was provided by Namseoul University.

REFERENCES

1. Kang AN, Barolli L, Park JH Jeong YS. A strengthening plan for enterprise informationsecurity based on cloud computing. Cluster computing, 2014; 17(3), 703-710.
2. Wang B, Zheng Y, Lou W, Hou YT. DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks, 2015; 81, 308-319.
3. Chun SH, Choi BS. Service models and pricing schemes for cloud computing. Cluster Computing, 2014; 17(2), 529-535.
4. Chen B, Tan C, Zou X. Cloud service platform of electronic identity in cyberspace. Cluster Computing, 2017; 20(1), 413-425.
5. Karim R, Ding C, Miri A, Rahman MS. Incorporating service and user information and latent features to predict QoS for selecting and recommending cloud service compositions. Cluster Computing, 2016; 19(3), 1227-1242.
6. Gajjar H. Securing User's Data in HDFS. International Journal of Computer Trends & Technology, 1(4), 1327-1335.
7. Anderson T, Peterson L, Shenker S, Turner J. Overcoming the Internet impasse through virtualization. Computer, 2005; (4), 34-41.
8. Che Y, Yang Q, Wu C, Ma L. BABAC: An access control framework for network virtualization using user behaviors and attributes. In Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing 2010 Dec; 747-754.
9. Schaffrath G, Werle C, Papadimitriou P, Feldmann A, Bless R, Greenhalgh A, Mathy L. Network virtualization architecture: Proposal and initial prototype. In Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures, 2009, Aug; 63-72.
10. Boutaba R. A survey of network virtualization. Computer Networks, 2010; 54(5), 862-876.
11. Bem D. Virtual machine for computer forensics–the open source perspective. In Open Source Software for Digital Forensics. 2010; 25-42.
12 Dorn G., Marberry C, Conrad S, Craiger P. January). Analyzing the impact of a virtual machine on a host machine. In IFIP International Conference on Digital Forensics. 2009; 69-81.
13. Bares RA. Hiding in a virtual world: using unconventionally installed operating systems. In 2009 IEEE International Conference on Intelligence and Security Informatics. 2009 Jun; 276-284.
14. Patni JC, Abhishek Sharma, Prashant Mishra and Abhishek Kumar. Datacenter Virtualization with Optimization and Customization. Indian Journal of Science and Technology, 2016, 9(44). Available from:http://www.indjst.org/index.php/indjst/article/view/105087

AUTHORS PROFILE

First Author Young-Sung Cho He is a certifiedtechnology consultant,SMEs in Korea, as well as holda adjunct professor at DongYangMirae University. Hisresearch interests include BigData, Machine Learning, Datamining, e-commerce, Bio-informatics,Ubiquitous computingand Security Server. He has aM.S. in Computer Engineeringfrom Yonsei University and aPh.D. in Computer Sciencefrom ChungbukNationalUniversity.

Second Author Wonshik Na He is a professor ofDepartment of Computer Scienceat Namseoul University inKorea. His research interestsinclude Network Security,Information Protection, MedicalInformation, Multimedia,U-computing, Wireless LAN.He has a Ph.D. in Computer Engineering fromKyunghee University in Korea.