Design of Internal Traffic Checkpoint of Security Checkpoint Model in the Cloud Computing

Jung ho Eom and Min woo Park

Military Studies, Daejeon University, 62 Daehakro, Dong-Gu, Daejeon,
School of Information and Communication Engineering, Sungkyunkwan University,
Chunchun-dong 300, Jangan-gu, Suwon, Kyunggi-do, Republic of Korea
eomhun@gmail.com, mwpark@imtl.skku.ac.kr

Abstract

In this study, we proposed design of internal traffic checkpoint in security checkpoint model for preventing security threats. Our architected security checkpoint model is a system that performs firstly check process on all incoming traffic from outside network. And it identifies almost threats and prevents them for protecting a cloud computing resources. The security checkpoint model consists of three components such as incoming traffic checkpoint, internal traffic checkpoint, and host-based threat checkpoint. The proposed model checks the safety of incoming traffic and binary file, and tracks traffic including threat factors. And it also judges threat traffics on system and storage. In this paper, we focused on structure, inspection procedures and functions of internal traffic checkpoint. Internal traffic checkpoint is important because it blocks threat traffic into internal network and ensures stable and reliable traffics.

Keywords: *Security Checkpoint, Internal Traffic Checkpoint, Abnormal Behavior*

1. Introduction

Cloud computing, which provide reliable, customized and QoS guaranteed service without direct installation of high performance computing devices, emerges as a new computing paradigm. The users want to move their information and applications to cloud system and then access them easily and comfortably. So, many internet service providers are participating in the development and trying to provide various services. Cloud computing system is a complex form of fusion computing technology such as resource virtualization, grid computing, utility computing, server-based computing, and network computing technologies [1, 2, 3]. But cloud computing has been exposed to new types of security threats due to its structural characteristics with the potential security threats in existing computing systems. It also will be added security threats by virtualization engine hypervisor, administrator, and the network in the course of transmission unlike the existing computing environment [4]. In cloud computing environment, security issues may be raised necessarily because it is in the form of outsource some or all of IT resources without owning. So, for protecting cloud computing environment which provides services in conjunction with several management devices and computing resources, it is needed to strong security countermeasures that include inspection process against the incoming traffic and audits on all traffic generated by the system components.

In this research, we proposed a security checkpoint model that can protect management devices and storage area, and block an influx of traffic to cause malfunction by checking all the traffic. Especially, we focus on checking internal threat

traffics caused leakage of data and system & application information. The leakage of information is very sensitive elements for users to use cloud computing services. Therefore, security service is very important to protect information stored within the system. In this paper, we explain the overall concept and design of a security checkpoint, and present design of internal traffic checkpoint in detail. We describe the concept of cloud computing system and security requirements in Section 2. In Section 3, security checkpoint model is presented. We propose internal traffic checkpoint module in Section 4 and conclude in Section 5.

2. Related Works

2.1. Cloud Computing

Cloud computing is defined as technology that provides virtualized IT resources to users as a service by using internet. The user uses IT resources such as software, storage, server, and network at pay-per-use service, and receive flexible support depending on the usage of the service. Figure 1 describes the concept of cloud computing.

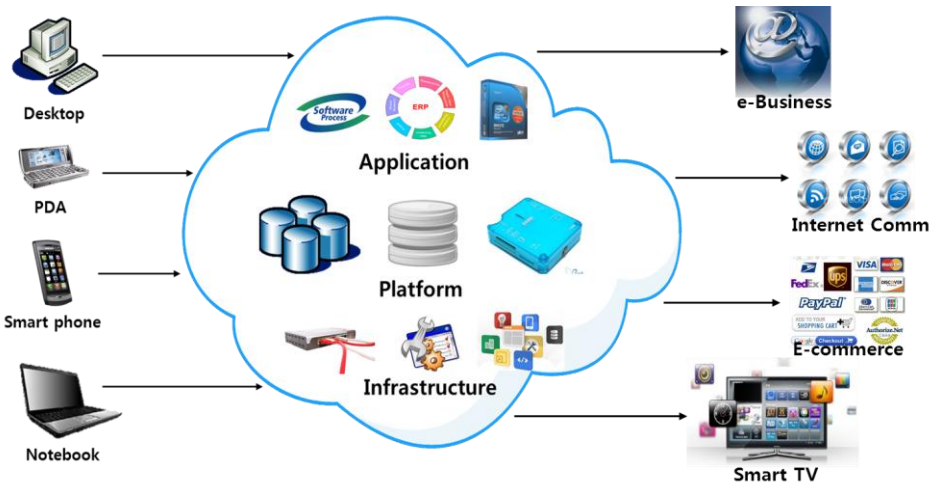

Figure 1. Cloud Computing [5]

Cloud computing has the following characteristics [1, 6].

- On-demand service: Users access and employ computing resources such as server, network storage on demand. Users can customize their computing environments without human interaction with service providers.

- User centric access: Users can access computing platforms simply and pervasively.

- Guaranteed QoS offer: Cloud computing can provide guaranteed QoS for users. Service level agreement (SLA) is included the levels of availability, serviceability, performance, etc.

- Rapid elasticity: Cloud computing can be rapidly and flexibly provisioned to quickly scale out, and rapidly released to quickly scale in. It should be elasticated to adapt to various requirements of a large number of users.

- Autonomous service: Cloud computing can be automatically reconfigured, orchestrated and consolidated by leveraging a metering capability.

Cloud computing services is representative such as SaaS (Software as a Service), PaaS(Platform as a Service), and IaaS (Infrastructure as a Service).

SaaS is a software delivery model in which software and associated data are centrally hosted on the cloud computing. And Users typically access remotely by using a thin client via a web browser. So, it sometimes referred to as "on-demand software".

PaaS provides a computing platform and a solution stack as a service. The user creates the software using tools and libraries from the provider. The user also controls software deployment and configuration settings.

IaaS is a platform through which businesses can avail equipment in the form of hardware, servers, storage space, operation and process functions, etc. at pay-per-use service [5, 7].

2.2. Security Requirements

Cloud computing does not yet guaranteed security perfectly. It must be met the following security requirements for use cloud computing safely [8, 9].

First, it should be checked the safety of the incoming traffic into cloud computing system. It should be determined whether the kinds and delivery path of traffic is safe or not. And it also should be determined whether traffic generated system is safe or not.

Second, the binary files from the outside should be able to verify the safety. Incoming upload binary files through the legitimate process flows should be examined. And it should be examined e-mail attached to the binaries and safety of files through protocols possible to transfer files such as HTTP, FTP, SCP, and RSYNC, etc.

Third, it should be able to track traffic including threat factors. It is required to additional tracking process of threat traffic because it can leak information stored in system or cause secondary aggressive behavior using cloud computing resources.

Fourth, it should be able to verify the safety of the message designated management system to destination address. The cloud computing system is caused a serious problem whether it is out of control or is happened malfunction by attacking management system. For example, they are such as abnormal billing, authentication, and resources management.

Fifth, it should be able to verify the safety of messages delivered directly the storage system. If the control of the system is lost, it can break out the user's information disclosure, alteration, and deletion, etc.

Finally, it must be able to detect attacks by the virtual machine or host. It is very difficult to keep the virtual machine safely in advance because traffic to access the virtual machine is irregular. Thus, even though the virtual machine loses control right and is used to a second attack, attack detection techniques are needed to protect other systems from these attack

3. Security Checkpoint Model

A security checkpoint model inspects on incoming traffic from outside to meet the security requirements. It performs inspection to incoming traffic into cloud computing system through service-oriented interface technology. And it inspects traffic generated from virtual machine or host running virtual machine. The security checkpoint model consists of three checkpoints such as incoming traffic checkpoint, internal traffic checkpoint, and host-based threat checkpoint like as following Figure 2. The detailed function and components of the security

checkpoint model are explained Park's paper 'A study on architecture of a cyber checkpoint model in the cloud computing environment [10]'.

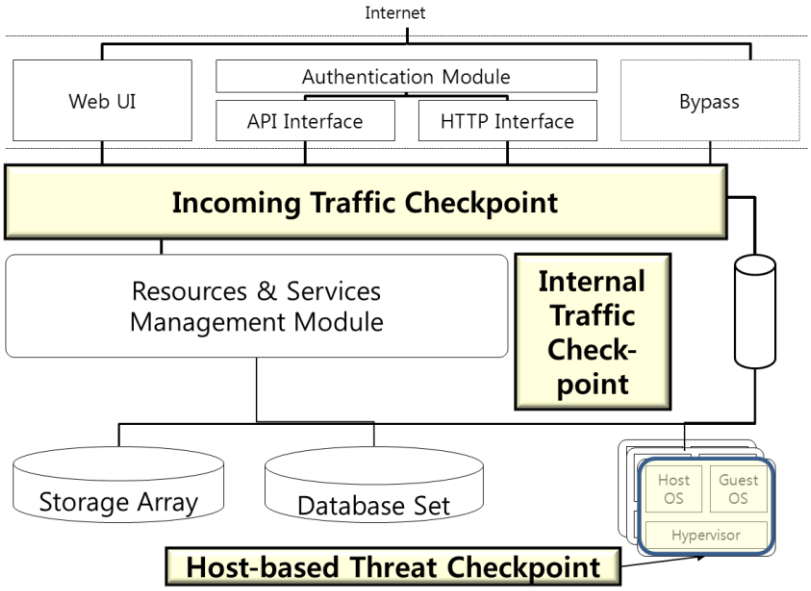

Figure 2. Architecture of a Security Checkpoint

Incoming traffic checkpoint blocks threat traffic coming into the cloud computing system. It classifies traffic that could be used to attack and determines the safety of traffic by performing inspection process. Incoming traffic checkpoint consists of six modules such as certificate verifier module, quarantine verifier module, user abnormal behavior check module, traffic classification module, database query analyzer module, and binary file abnormality check module.

Internal traffic Checkpoint blocks the delivery of threat traffic into internal system. It consists of two modules such as traffic classification module and abnormal traffic identification module.

Host-based threat checkpoint detects attacks that can occur by virtual machine and hypervisor. It can specify the boundary of rule set by security level of each user and security strength. It consists of two modules such as hypervisor threat detection module and virtual machine security module.

4. Internal Traffic Checkpoint

4.1. Design of Internal Traffic Checkpoint

It consists of two modules such as traffic classification module and abnormal traffic identification module, as shown Figure 3.

Traffic Classification Module determines whether the traffic goes through any inspection process. The traffic passed to internal traffic checkpoint is sent to the traffic abnormality check module or transmitted to the first destination by bypass user interface of cloud computing. Abnormal Traffic Identification Module judges whether traffic destined for the internal system for managing cloud computing in the traffic generated by the virtual machine or traffic destined for the unknown host is normal.

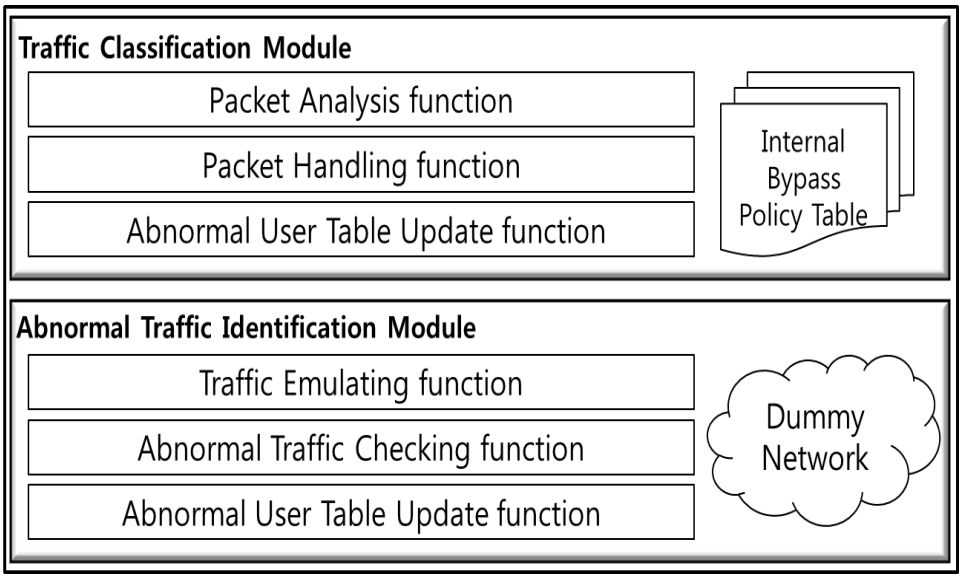

Figure 3. Internal Traffic Checkpoint

Traffic classification module consists of three functions and a table as above Figure 3. Packet analysis function extracts incoming packet header into internal traffic checkpoint and determines protocol. Packet handing function searches internal bypass policy table and determines whether the packet passes, disposes, and quarantines. Abnormal user table update function updates the abnormal level of the users when specific traffic is discarded in traffic classification module. Internal bypass policy table specifies policy for distinguish traffic to quarantine in internal traffics. It contains the information of message waiting to receive from cloud computing management device or a storage device. It also stores the information about the traffic policy to prevent the influx.

Abnormal traffic identification module consists of three functions and a dummy network. Traffic emulating function decides the emulating order for fair traffic emulation, and passes traffic to fake device of dummy network according to the scheduled order. As doing so, internal traffic checkpoint can be performed quarantine process of a large amount of traffic in a short period of time. Abnormal traffic checking function receives checking results from fake management device, fake storage device and honeypot, and finally determines whether traffic is abnormal or not. Abnormal user table update function updates the abnormal level of the users caused the threat traffic if it is determined traffic is dangerous. Dummy network is fake network for emulating traffic. It includes fake management and storage device with same IP address of real device. Honeypot is located on there for detecting attack.

4.2. Quarantine Process of Internal Traffic Checkpoint

The quarantine process of internal traffic checkpoint is as shown Figure 4. If the virtual machine passes traffic to the internal network of cloud computing system, the all internal traffic will pass through internal traffic checkpoint. In the process, as internal traffic checkpoint blocks traffic is determined as a potential threat, it protects securely management and storage device, and derives attack pattern could threaten the system.

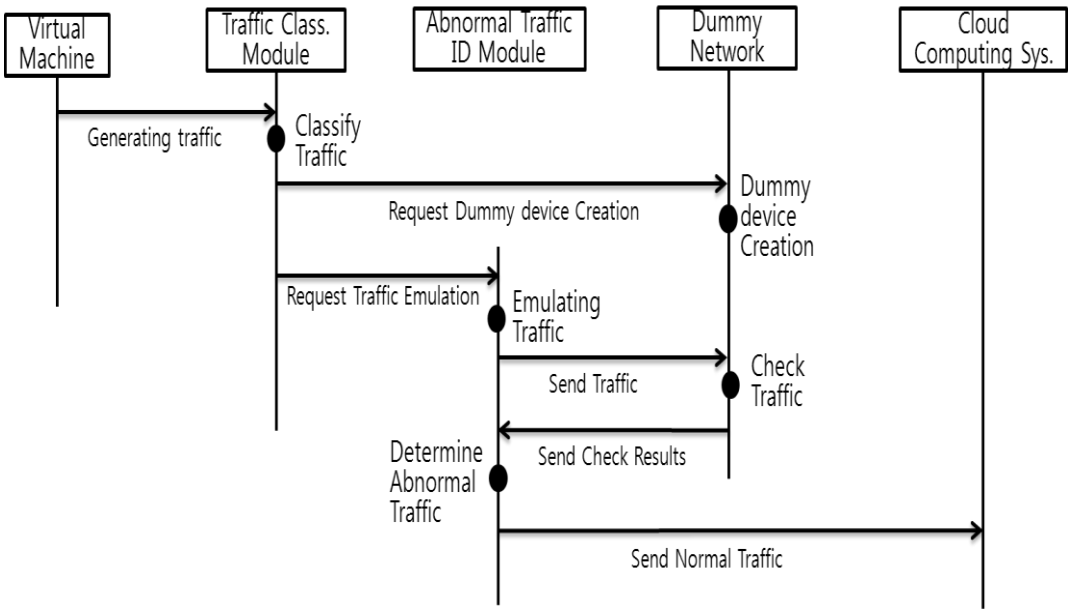

Figure 4. Quarantine Process of Internal Traffic Checkpoint

All packets which virtual machine sent to communicate with management and storage device are delivered to destination via internal traffic checkpoint. Internal traffic checkpoint classifies incoming traffic according to its characteristics. Classification standard are a response waiting packet for the management device, a response waiting packet for the storage device, packets related to routing, etc. Internal traffic checkpoint determines firstly whether management or storage device is waiting for a response of virtual according to internal bypass policy table. While management or storage device is waiting for response, if the level of user's abnormal behavior is not risk, packet is immediately sent to the first destination for alleviating system performance degradation by security checkpoint. If packet was classified as packet related to routing, it is promptly disposed and information is sent to security administrator. A response non-waiting packet or all other packets are performed sequentially traffic safety inspection by scheduling. In particular, if packet's destination is management device or storage device, dummy network generates virtual management or storage management and emulates. If packet is not threat in the quarantine result, it is disposed. If packet is threat, internal traffic checkpoint increases the abnormality level of virtual machine user who generated the packet, and save threat pattern.

Traffic classification module classifies incoming traffic for regulating quarantine object and method. For example, it classifies packet including potential threat as follow table.

Table 1. Potential Threat Packet Classification

Object	Port	Threat
HTTP Request Packet	80	Invalidated Input Value URL attack
SMTP	25	Mail Server attack User PC attack using client vulnerability
IMAP	143	Mail Server attack User PC attack using client vulnerability Checked messages on the mail server still exists
POP	110	Mail Server attack User PC attack using client vulnerability
DHCP	67	Attacker disguised as a DHCP server and assigns users to spoofed DHCP address to send data A buffer overflow attack
.	.	.
.	.	.

Internal Traffic checkpoint can early detect a potential attack by tracking the user's traffic classified as abnormal users even if direct attack pattern does not appear. Criteria examples for abnormal behavior of the users are shown in the following table.

Table 2. Criteria Examples for Abnormal Behavior of the User

Criteria for abnormal behavior of the user
- The runtime and usage of a specific resource used by the user
- High frequency of system calls statistically
- The more number of login attempts than three times
- System resource related CPU, I/O, Memory usage
- The information of use hours per connection as the user ID
- The more number of flows with the same origin or same destination for last 90 sec. than 200
- The case of incoming suddenly traffic to a particular port more than the average value of incoming traffic
- Significantly increased billing for the services of a particular user
- Access to customer data by user logged in as the administrator ID even if error reporting
- Log in at the same time as the same ID
.
.

We drew up the matrix to quantitatively estimate the abnormal behavior of the user based on Table 2. The matrix includes application rate, the score, and valid number and time according to detailed abnormal behavior.

Table 3. The Example of Estimation

Abnormal behavior	Application rate	Score	Valid number / time
Access by the same ID	100%	10	1/unlimited
Access by the same IP	100%	10	1/unlimited
Login attempt more than 4 times	100%	5	1/unlimited
Access except for the primary use time zone	1/number* 100%	10	unlimited / unlimited
Behavior classified as attacks	100%	30	unlimited / unlimited
. . .	. . .	. . .	. . .

In the Table 3, application rate is defined as the extent to the score. Valid number means whether abnormal behavior is persisted during a few of login time. Valid time means whether how long score is applied after abnormal behavior occurred. The following table shows abnormal levels of user evaluation methods based on Table 3.

Table 4. The Classification by Score with the Level of Abnormal Behavior

Score	Level	Classification
Above 80	Very High	User with high attack
60~79	High	User with threat to the system
40~59	Medium	User with potential threat
20~39	Low	User with abnormal behavior lowly
Under 19	Very Low	Normal user

Internal traffic checkpoint assesses finally the level of user's abnormal behavior after calculated scores per abnormal behavior according to estimation matrix

5. Conclusion

We proposed architecture of cyber checkpoint model for preventing security threats in the Park's paper [10]. In this paper, we focused on structure, check procedures and functions of internal traffic checkpoint. Internal traffic checkpoint is important because it blocks threat traffic into internal network and ensures stable and reliable traffics. It

consists of two modules such as traffic classification module and abnormal traffic identification module. Traffic Classification Module determines whether the traffic goes through any inspection process. The traffic passed to internal traffic checkpoint is sent to the traffic abnormality check module or transmitted to the first destination by bypass user interface of cloud computing. Abnormal Traffic Identification Module judges whether traffic destined for the internal system for managing cloud computing in the traffic generated by the virtual machine or traffic destined for the unknown host is normal. Traffic classification module classifies incoming traffic for regulating quarantine object and method and abnormal behaviors even if direct attack pattern does not appear by the criteria of abnormal user behavior. We used the matrix quantitatively for estimate the abnormal behavior of the user. Internal traffic checkpoint assesses finally the level of user's abnormal behavior after calculated scores per abnormal behavior according to estimation matrix.

In the future, we finish architecture of other checkpoint and will proceed implementation. Finally, we will continue to conduct performance evaluation through simulation.

References

[1] L. Wang, G. von Laszewski, A. Younge, X. He, M. Kunze, J. Tao and C. Fu, "Cloud Computing: a Perspective Study", Ohmsha, Ltd., Springer, vol. 28, **(2010)**, pp. 137-146.
[2] M. -h. Kim, J. -w. Kim and H. -c. Chang, "The present and future of cloud computing", CSO magazine, The paper of Society of KIIC, vol. 20, no. 2, **(2010)** April, pp. 56-64.
[3] O. G. Min, H. Y. Kim and G. H. Nam, "Trends in Technology of cloud computing", The paper of ETRI, vol. 24, no. 4, **(2009)** August, pp. 1-13.
[4] T. H. Kim, I. H. Kim, C. W. Min and Y. I. Eom, "Trend of Cloud Computing Security Technology", Communications of The KISS, vol. 30, no. 1, **(2012)** January, pp. 30-38.
[5] http://en.wikipedia.org/wiki/Cloud_computing.
[6] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", Special Publication 800-145, **(2011)** January.
[7] J. H. Cheong, "The present and future of cloud computing, market strategy, Trend", NIPA, **(2008)** October, pp. 56-85.
[8] J. Kirch, "Virtual Machine Security Guidelines Version 1.0", WBB Consulting, The center for Internet Security, **(2007)** September.
[9] D. Hyde, "A Survey on the Security of Virtual Machines", A project report, **(2009)**.
[10] M.-w. Park, H.-h. Eom, S.-h. Kim, N.-u. Kim and T.-m. Chung, "A Study on Architecture of a Cyber Checkpoint Model in the Cloud Computing Environment", The proceedings of ITCS 2012, **(2012)** July, pp. 123-128.

Authors

Jung ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are information security, cyber warfare, network security.

Min Woo Park is currently a Doctor candidate at Sungkyunkwan University, Suwon, Korea. He received his B.S. degrees in Information & Communication Engineering from the SungKyunKwan University, Suwon, Korea, in 2008, respectively. He received his M.S. degrees in Department of Electrical and Computer Engineering from the SungKyunKwan University, Suwon, Korea, in 2010, respectively. His research interests include security of Sensor Networks and Cloud Computing.