別紙４－１（課程博士（英文））

Date of Submission (month day, year) : January 9, 2018

Department	Student ID Number	
Computer Science and Engineering		D149301
Applicant's name	Idris Winarno	

Supervisors	Yoshiteru Ishida Jun Miura

Abstract (Doctor)

Title of Thesis	A Resilient Server with a Self-Repair Network Model on the Virtualization Environment

Approx. 800 words

The performance of an information system depends on the reliability of the data center infrastructure. A computer which has a high specification and runs a service, which can be accessed by multiple users over a network, is called a server. The server is one of the most critical parts of a data center, hence can negatively affect the overall performance of an information system in cases of system failure (e.g. hang faulty, denial of service attack, and malware). Since servers play a critical role in data processing and data transmission for serving many clients, failures in servers cause not only performance degradation of the server itself but also threats to the entire computer connected to the servers. Resilient servers that can self-recognize failures, self-repair failures and self-replace failed parts are required when computer systems and networks become huge-scale as witnessed by data centers and the cloud computing. Recently, virtualization has become a popular method to develop servers for data center infrastructure. Thus, we require a model that can deal with virtual servers as a repair unit. There are two types of virtualization technology that we can use to build the resilient server: virtualization machine monitor (VMM) and container (also called as Linux Container or LXC). Container offers fast boot and efficient resource usage to deploy a server on the virtual environment. However, VMM provides higher diversity of guest operating system than container.

In this study, we introduce a new model of the resilient server by implementing a self-repair network (SRN) model in the virtualization environment to address failures that occur during the operation of the server. The SRN model offers a general framework of self-action models for the server to self-recognize, self-repair, and self-replace its own failed parts (learned from

immune system). In this study we use the following four models of SRN: (i) self-repair, (ii) mutual-repair, (iii) mixed-repair, and (iv) switching-repair. The SRN model will be applied to the script that we called as SRN manager. This script has the main responsibility to monitor and respond to the failures. We define eight types of resilient server using the combination of three parameters including application (service), guest operating system, and host operating system (virtualization engine).

The simulations show that virtualization technology is able to build a resilient server to recover the failure in the limited scenario. The first experiment shows that container outperforms the VMM since container almost ten times faster and more efficient of memory resources compared to the VMM. However, a container has lower diversity than VMM due to container uses a shared kernel. The second experiment explains that a resilient server with a homogeneous environment offers ease of replacement of the failed parts, but this resilient server has less resilience than those with heterogeneous environment since the entire server in the homogenous environment has the same vulnerability. The last experiment describes that we use multiple virtualization engines to increase the diversity of the resilient server. Moreover, the performance of our proposed method has low performance losses and high service availability.