The Solution of Disaster Recovery System on Cloud Computing Environment

Chang Yup Choo 1 and Kwang Sik Chung 2,*

1 KT Corp., Enterprise Business Performance Unit, BunDang-gu, GyeongGi-Do, seongnam, Republic of Korea
2 Dept. Of Computer Science, Korea National Open University, Jongno-gu, Dongsung-Dong, Seoul, Republic of Korea

*E-mail : kchung0825@knou.ac.kr

Abstract. As the number of cases of cloud environment development in the financial industry has increased, cases of disaster recovery system in the financial industry are increasing. However, the establishment of the cloud environment for the main tasks in the financial industry is being restricted or limited in the cloud environment due to the security restriction regulation on the personal information and the financial business information. Unlike the establishment of a disaster recovery system for a general enterprise cloud environment, the financial industry of the cloud environment has a wide range of personal information security and protection regulations, and there are many limitations according to the respective country. Therefore, it is necessary to consider the existing one in constructing the disaster recovery system of the cloud environment in the financial industry. This research analyzes the solution and technology trends for existing cloud disaster recovery system, and extracts the problems of existing cloud disaster recovery system. In addition, the financial business classification criteria based on the services to be provided in the cloud environment, and determine the scope of introduction of the legacy system and the cloud system according to the cloud business classification standard are defined in this paper. In the standard of financial service to be provided in the cloud environment, the classification standard of the financial business is newly defined based on the range of influence of the personal information and the service continuity of the financial service from the core/context theory. Lastly, disaster recovery system in cloud environment for financial business services is defined.

1. Introduction

In order to minimize the loss of financial services due to natural or man-made disasters, a disaster recovery system has been established and operated in financial industry. The current disaster recovery system is mostly built and operated with the same computer architecture of the main data center. However, the change management of the disaster recovery system against the change of the computerized environment is not performed smoothly. In order to compensate for this situation, there is a growing interest in building a disaster recovery system in the cloud environment and the number of cases of disaster recovery system in the cloud environment has been gradually increasing. However, there is a limitation in constructing a disaster recovery system for the cloud environment. In this paper, cloud deployment environment is defined based on financial business classification in order to build a disaster recovery system in a cloud environment, and a disaster recovery system operation scheme is proposed.
This paper is organized as follows. First, previous related cloud disaster recovery techniques and vendors are analyzed. Then, the financial tactics classification metrics for cloud system adaptation and operations of cloud disaster recovery systems are proposed. Finally, research conclusions in Chapter 4 are presented.

2. Related Works

The cloud market has not reached the maturity stage, and the public cloud service is mainly provided by the telecom companies. But it does not include the disaster recovery service in the cloud service. In terms of hardware of disaster recovery systems, main components are divided into server, storage, and network. Servers and networks are cloud environments that can be configured to provide a virtual environment by cloud services while maintaining fail-over or active-active state during the data center disaster. However, in the case of storage, since the data is continuously generated and changed through the server providing the main service, remote data replication should be performed through the data replication function provided by the cloud service.

Figure 1 shows the basic concept of configuring a disaster recovery system in a cloud environment. The disaster recovery system activates resources to replicate critical data between the primary and disaster recovery centers normally. Server resources are allocated and maintained as a minimum resource. At disaster, the cloud system in the disaster recovery center allocates resources to the server using the resource provisioning function and operates the disaster recovery system to provide continuous business services to the customer.

3. Building Disaster Recovery System for Cloud

3.1. Core / Context Analysis Framework for Disaster Recovery System

’Core/Context Analysis’ is a framework proposed by Jeffrey A. Moore[3,4]. Core means the core business of a corporation. Core business is an important part of enhancing a company’s competitive advantage. Context is defined as all activities other than the core. And context tasks are not pursuing differentiation, but rather ‘as efficient as possible in the standard way as possible’ [5].

[Core / Context Analysis] is used as a framework for building a disaster recovery system in this research. The specified conditions in the Core are defined by ‘The Guide to Using the Cloud Services in the Financial Services’ printed by the Financial Security Institute[6]. In addition, the definition specified in mission-critical is selected through Business Impact Analysis (BIA).

The Business impact analysis is a series of analysis activities that define the tier matrix by analyzing the RTO / RPO for each business function and define the mission-critical (core or important
task) according to the tier level connected to each business function. The results of business impact analysis can be defined a little differently depending on the consulting method, but the basic concept is applied equally[7,8].

Core task means that an IT system for processing, transmitting, receiving and delivering unique identification information or personal credit information. Context task means all other IT system.

And Mission-Critical task means processes shortfall creates serious and immediate risk. Non-Mission –Critical means all other processes.

Core-Mission-Critical task requires that a system that maintains direct relationships with customers in financial services and maintains competition with competitors. Context-Mission-Critical task requires that there is no direct relationship with financial services (A system that causes the business crisis when it does not work properly.). Core-Non-Mission-Critical task requires that a system that indirectly support financial services and require to maintain differentiation from competitors, but may be failed to deliver. Context-Non-Mission-Critical task requires that a System with low importance for corporate management.

| Core/Context Analysis | Core                      | Context       |
|-----------------------|---------------------------|---------------|
| Mission-critical      | Legacy System             | Public Cloud  |
| Non-mission-critical  | Private Cloud             | Public Cloud  |

In table 1, the comparison between the mission-critical task and the non-mission-critical tasks is classified according to the importance of the task. For mission-critical operations, contracts must be made with cloud providers to enable continuous business services through redundancy or SLA recovery activities. Relatively non-mission-critical tasks are less impacted by the disability, so that contracts for disability recovery activities can be additionally provided through contracts that take economic considerations into account. Although the mission-critical and non-mission-critical tasks corresponding with the core conditions are classified according to the importance of work, they do not use the public cloud environment, so that they are applied to the maintenance of the legacy system environment and the private cloud environment. However, for mission-critical tasks, the transition to the cloud environment should be considered depending on the utilization of the business.

3.2. Core / context model based disaster recovery system

The method of constructing the disaster recovery system according to the system configuration type derived through the core / context analysis is differently configured. Generally, the scope of building a disaster recovery system will be different depending on the construction time and the operation time of disaster recovery system. However, since the mission-critical service has a great impact on the management of the financial company even, the disaster recovery system should be built in the advance.

- Definition of locations for providing disaster recovery services
  ‘Mission-critical’ services and ‘non-mission-critical’ services are in the same space from the view of Core system. ‘Mission-critical’ services and ‘non-mission-critical’ services that are associated with the ‘Context’ system and are also in the same space. However, the ‘Core’ system and the ‘Context’ system do not exist in the same space.

In the public cloud environment, the space of the ‘mission-critical’ service may be different from the space of the ‘mission-critical’.

- Define when to provide disaster recovery services
  Disaster of ‘Mission-Critical’ services can affect to whole financial business even in a temporary disruption situation so that disaster recovery systems should be con-figured and prepared in the advance. The ‘Core’ and ‘Context’ systems that provide ‘non-mission-critical’ services can be pre-configured and operated in accordance with the financial company's management policies and service
priorities. And according to RTO (recovery time objective), the system may be newly configured and operated after a disaster occurs.

- Classification of services under the Public Cloud environment

‘Context’ systems with public cloud services have different ‘mission-critical’ and ‘non-mission-critical’ services. ‘Mission-Critical’ services should be provided for disability or disaster in the aspect of temporary interruption, while relatively ‘non-mission-critical’ services can be selected for low-level services in table 2.

| Service                     | SLA                                                                 |
|-----------------------------|----------------------------------------------------------------------|
| ‘Mission-critical’ service  | Service recovery within the due time in case of a service failure   |
|                             | Automatic Fail-Over in case of H/W failure                          |
|                             | Disaster recovery service (transition within RTO)                   |
|                             | Minimum data loss (data recovery within RPO), etc.                  |
| ‘Non-mission-critical’ service | Service recovery within the due time in case of a service failure |
|                             | Automatic Fail-Over in case of H/W failure                          |

3.3. Operate Disaster Recovery System with Core/Context Model

Disaster of ‘Mission-critical’ with ‘Core’ system and ‘mission-critical’ & ‘Context’ system can affect to whole financial business even in a disruption situation so that disaster recovery systems should be configured and prepared in the advance. How-ever, since the provision locations of the services are different from each other, the ‘Core’ and ‘Context’ systems do not cause the same disaster situation from the perspective of disaster.

‘Mission-critical’ services and ‘non-mission-critical’ services that are classified as ‘Core’ systems. And the services are directly affected when a disaster occurs. And the service continuity is maintained as shown in figure 2. It also connects with ‘mission-critical’ services using public cloud to provide continuous services.

Figure 2. Configuration for Data Center Disaster

In the event of a disaster in a cloud service provider as shown in figure 3, business services resume within RTO and RPO through a disaster recovery service contracted with a cloud service provider. A disaster recovery center operated by a cloud service provider provides business continuity for business services with a disaster recovery service contract.
Figure 3. Configuration for Cloud Service Provider Disaster

If situations as shown in figure 2 and figure 3 occur, the disaster recovery system for each business service defined in the category is operated according to the operating procedure specified in tables 3 and table 4.

Table 3. Pre- and post-disaster Core/Context service Activities [Figure 2]

| Category                  | Normal Operation                                                                 | Disaster Recovery Operation                                                                 |
|---------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Core & Mission-critical   | Disaster recovery system exists. The Disaster Recovery center is operated at a distance from the data center. | Start disaster recovery system within RTO. Resume service after data recovery according to RPO. |
| Context & Mission-critical| Disaster recovery system exists. Disaster recovery service contract through public cloud provider. | In case of own data center disaster, link with disaster recovery system Maintain existing services. |
| Core & Non-mission-critical| Disaster recovery system exists (possible). The Disaster Recovery center is operated at a distance from the data center. | If the disaster recovery system is operated, the disaster recovery system is operated within the RTO, Resume service after data recovery according to RPO. |
| Context & Non-mission-critical| Disaster recovery system does not exist.                                         | In case of self-center disaster, link with disaster recovery system, Maintain existing services. |

Table 4. Pre- and post-disaster Core/Context service Activities [Figure 3]

| Category                  | Normal Operation                                                                 | Disaster Recovery Operation                                                                 |
|---------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Core & Mission-critical   | Disaster recovery system exists. The Disaster Recovery center is operated at a distance from the data center. | Integration of Disaster recovery system of public cloud center.                               |
| Context & Mission-critical| Disaster recovery system exists.                                                 | Operate disaster recovery system of public cloud center(RTO level assurance).                |
Disaster recovery service contract through public cloud provider.

Resume target data recovery and according to RPO and business services.

Integration of Disaster recovery system of public cloud center.

Disaster recovery system exists (possible).
The Disaster Recovery center is operated at a distance from the data center.

Rebuilding public cloud services.

Resume business services.

Context & Non-mission-critical

Disaster recovery system does not exist.

4. Conclusion

Personally identifiable financial information dealt with in the financial industry requires the highest level of information security [9]. Therefore, adaptation of the cloud environment in the financial industry has many limitations. However, it is possible to derive information or financial services that can be handled in the cloud environment through business analysis of the financial industry.

In this paper, the criteria for classifying the business and financial information services of the financial industry are defined based on the [Core / Context Analysis] theory. In addition, those that can be deployed in the cloud environment and those that should be provided as legacy systems according to the newly defined [core / context classification criteria]. The disaster recovery system for financial services and financial business supported is designed and proposed in the cloud environment. In particular, an operational frame for the normal operation of financial information services for disaster recovery is proposed. Through this design, it will be possible to establish a financial system cloud system that can manage personal information and financial information efficiently and establish a disaster recovery system.

References

[1] Jongbeom Jeon, ‘A Research for the New Disaster Recovery Method on Cloud Environment’, 2014, Korea University
[2] Timothy Wood, Emmanuel Cecchet, K.K. Ramakrishnan, Prashant Shenoy, Jacobus van der Merwe, and Arun Venkataramani, ‘Disaster Recovery as a Cloud Service:Economic Benefits & Deployment Challeges’, In proceedings of the Conference on Hot Topics in Cloud Computing (HotCloud),August 2010
[3] ‘Living on the Fault Line, Revised Edition:Managing for shareholder Value in Any Economy’, August 20, 2002, Harper Business, Geoffrey A. Moore
[4] ‘Dealing with Darwin : How Great Companies Innovate at Every Phase of Their Evolution’, 2005, Penguin, Geoffrey A. Moore
[5] ‘CLOUD NO SHOUGEKI’, 2009, TOYO KEIZAI INC., Makoto Shirota
[6] ‘The guide for using financial service in the Cloud’,2016.10.14,Financial Security Institute
[7] Omar H. Alhazmi , Yashwant K. Malaiya, ‘Evaluating Disaster Recovery Plan Using the Cloud’,In proceeding of Reliability and Maintainability Symposium (RAMS), 2013
[8] Mr.A.Srinivas, Y.Seetha Ramayya, B.Venkatesh, ‘A Study on Cloud Computing Disaster Recovery’, International Journal of Innovative Research in Computer and Communication Engineering, August 2013, Vol. 1,pp1383-1384
[9] ‘Financial Supervisory Regulation’,Amended on 2016.10.15