JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 12 : 2305~2309 Dec. 2016

비즈니스 연속성을 위한 클라우드 컴퓨팅 서비스에서의 데이터 백업과 데이터 가용영역 아키텍쳐 연구

박영호[1] · 박용석[2*]

Business Continuity and Data Backup in Cloud Computing Service and Architecture Study for Data Availability Zone

Young-ho Park[1] · Yongsuk Park[2*]

[1]Graduate School of Information Security, Sejong Cyber University, Seoul 05000, Korea
[2*]Graduate School of Information Security, Sejong Cyber University, Seoul 05000, Korea

요 약

클라우드 컴퓨팅 서비스는 그 효율성과 안정성이 기반이 되어야 한다. 한 예로 미국은 클라우드 컴퓨팅 서비스의 안전성을 위하여 FedRAMP 인증을 제시하고 클라우드 컴퓨팅 서비스 산업의 성장은 많은 기업들에게 비용 절감과 업무의 효율성을 제공하고 있으나, 그에 따른 위험성 역시 높아지고 있다. 해킹 등으로 클라우드 서비스 특징상 데이터에 대한 통제성을 잃게 되고, 많은 데이터가 한 곳에 몰리는 현상은 장애가 발생하면 모든 기기의 데이터가 일제히 삭제되는 되는 문제점이 있다. 본 논문에서는 클라우드 보안 인증 제도의 비즈니스 연속성의 문제점을 알리고 이를 위한 솔루션인 서비스 가입자 내부에 백업과 외부 백업의 장단점을 비교한다. 결론적으로 외부 백업이 구조상으로 우위에 있음을 보인다.

ABSTRACT

Cloud Computing Service should support efficiency and stability. United States of America, for example, provides FedRAMP (Federal Risk and Authorization Management Program) accreditation to certify cloud computing service and hence growth of computing service industry is giving benefits of cost reduction and efficiency to companies. However, the use of computing service brings more risk than ever. Because cloud computing holds all the data of multiple companies, problems such as hacking bring out control loss of service and as a result total data of companies can be lost. Unfortunately, cloud computing certification programs do not have any good solutions for this data loss and companies may lose all the important data without any proper data backup. This paper studies such problems in terms of backup problem and provides Data Availability Zone solution for recovery and safe saving of data so that computing service can offer better efficiency and stability.

키워드 : 클라우드 컴퓨팅 서비스, 데이터 가용영역, 서비스 가용영역, 클라우드 보안

Key word : Cloud Computing Service, Data Availability Zone, Service Availability, FedRamp

Received 30 October 2016, **Revised** 01 November 2016, **Accepted** 10 November 2016

* **Corresponding Author** Yongsuk Park(yongspark@gmail.com, Tel:+82-2-2218-8452)
Graduate School of Information Security, Sejong Cyber University, Seoul 05000, Korea

Open Access http://doi.org/10.6109/jkiice.2016.20.12.2305 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

클라우드 컴퓨팅 서비스는 그 효율성과 안정성이 기반이 되어야 한다. 세계 각국은 이를 위하여 인증 제도를 제시하고 있다. 한 예로 미국은 클라우드 컴퓨팅 서비스의 안전성을 위하여 FedRAMP 인증을 제시하고 클라우드 컴퓨팅 서비스 산업의 성장은 많은 기업들에게 비용 절감과 업무의 효율성을 제공을 지향하고 있으나, 위험성 역시 높아지고 있다.

2012년 8월 애플 공동 창업자 스티브 워즈니악은 “클라우드 서비스를 이용할 경우 어떤 것도 가질 수 없고 클라우드 제공업체의 컴퓨터 자산을 빌려 이용할 수 밖에 없다고 지적했다. 모든 것이 내 컴퓨터에 있는 것처럼 보이지만 사실은 웹(클라우드)에 전송된 것뿐이고 통제권조차 없는 것이다” 라고 말했다[1].

2012년 6월 20일 일본 클라우드 서비스 제공 업체인 ‘퍼스트 서버’가 전산장애를 낸 것인데 무려 5,698개 기업의 데이터를 날려버렸다. 당시 자사 서비스 버그를 해결하기 위해 소프트웨어 업데이트를 진행하다가 일어난 사고로 데이터 복구 소프트웨어를 통해서 데이터를 복원하였으나, 고객사별 접근 권한 설정이 불가능해 다른 회사 데이터까지 내려 받을 수 있게 된 것이다. 이에 따른 데이터 분실사고는 각 기업마다 천문학적인 비용의 손해를 겪게 되었고, 데이터 통제성을 잃게 된 대표적인 사례가 되고 있다[2]. 또한 데이터를 잃어버린 기업들이 손해배상을 청구하였으나, 계약당시 약관에 따르면 클라우드 서비스 중단에 따른 서비스 제공적인 측면에서의 보상은 약속되어 있으나, 데이터 분실에 따른 보상에 대해서는 기술되어 있지 않았다. 이는 일본만이 아니라 클라우드 제공하는 업체 대다수의 약관에 데이터에 대한 보상은 명시되어 있지 않다. 즉, 현재의 인증제도로는 이러한 문제가 극복 될 수가 없다.

데이터의 복구가 되지 않으면 비즈니스의 연속성이 보장 되지 않는다. 따라서 비즈니스의 연속성의 가장 중요요소는 데이터이다. 서버가 고장 나면 새로운 서버로 교체할 수 있지만, 데이터가 분실되면 기업은 경영의 운명이 달라질 수 있다.

이에 본 논문에서는 이러한 문제점을 해결하기 위해서 클라우드 서비스의 데이터 저장의 문제점과 서비스 가용영역에 대한 분석, 그리고 데이터 가용영역에 대한 구조 분석 및 향후 연구 과제를 기술한다.

Ⅱ. 관련연구

2006년 Amazon에서 클라우드 컴퓨팅을 활용한 클라우드 재해복구 서비스를 사용자들에게 선보인바 있다[3]. 클라우드 데이터의 안전을 위한 가상 저장 기술에 관한 연구도 진행되었다[4]. IT 자원의 일부 또는 빌려 쓰는 클라우드 컴퓨팅의 근본적인 속성 때문에 보안 문제가 항상 해결해야할 우선 과제로 꼽히고 있으며[5], 클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구로 데이터 센터 운용과 재해발생시 클라우드 복구에 대해 연구가 진행되었다[6]. [7]에 클라우드 컴퓨터의 데이터 및 시스템 보안기술을 논의한 바 있다. 또한 본 연구는 [8, 9]를 기반으로 한 연구이다.

Ⅲ. 클라우드 컴퓨팅 서비스와 문제점

3.1. 클라우드 서비스의 종류

먼저 클라우드 서비스의 종류는 크게 3가지로 분류되는데, 표 1 과 같이 IaaS(Infrastructure as a Service), SaaS(Software as a Service), 그리고 PaaS(Platform as a Service)로 구분하는 것이 대표적이다.

Table. 1 CLOUD Service Classification

Type	Characteristics
Iaas	virtualization of Infra Resources
SaaS	various software services through web
PasS	software platform for users apps

현재 가장 많이 제공되고 있는 클라우드 서비스는 IaaS인데 SaaS와 PaaS의 경우도 결국은 저장되는 공간이 클라우드 서비스내 IaaS이기 때문이다. 또한 개인적으로도 IaaS만 이용하는 사람도 많다.

3.2. 클라우드 데이터 저장의 문제점

클라우드 컴퓨팅 서비스 데이터 저장에 문제점은 클라우드 컴퓨팅 서비스의 단점들을 보면 알 수 있다[10]. 첫째, 지속적인 인터넷 연결이 필요하며, 둘째 저장된 데이터가 안전하지 않고, 셋째, 고객사의 통제 권한이 부족하고, 넷째, 다수의 클라우드 센터가 존재 하므로 수많은 장치와 여러 저장 공간에 분산됨에 따른 보안

문제가 발생할 수 있고, 마지막으로 여러 회사의 데이터의 중앙 집중화로 클라우드센터의 장애는 여러 회사의 위험성을 야기한다.

저장된 데이터가 안전하지 않다는 부분에 대해서 그림 1을 보면 이해하기 쉽다.

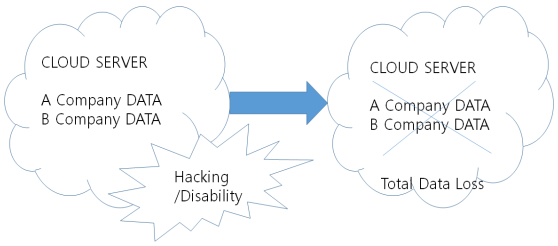

Fig. 1 Problem of CLOUD DATA Saving

클라우드라는 거대한 웹 환경에서 저장된 자료들은 각각 저장된 위치는 달라도 하나의 환경에 저장되어 있음을 알 수 있다. 만약 이 거대한 웹 환경이 악의적인 해킹이나 장애가 발생한다면 모든 데이터가 사라지는 엄청난 사태를 겪게 될 것이다. 이에 대해서 일부 전문가들은 백업에 대한 중요성을 강조 하고 있으며, 클라우드 서비스와 별도로 물리적인 스토리지 백업전용 서버를 사내에 두어 그림 2와 같이 안전한 클라우드 사용을 권장하고 있다[8].

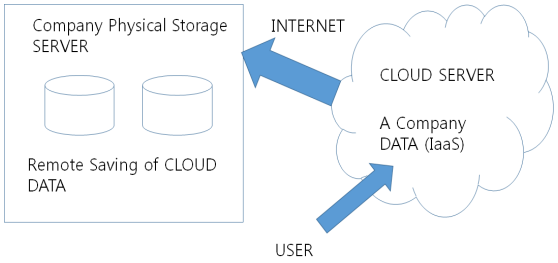

Fig. 2 CLOUD Data Backup in Company

그러나 사내에 물리적인 서버를 두어 백업하는 방법은 보안상 문제점이 있을 수 있다. 인터넷을 통해서 원격으로 저장하기 때문에 악의적인 해커의 공격이 가능하게 되며, 이를 막기 위해서 VPN(Virtual private network)과 같은 보안장비를 사용해도 기업입장에서는 장비의 사용료와 일정간격 수동으로 백업해주어야 하는 불편성, 그리고 사내 스토리지 서버 구축에 따른 유지보수 비용과 회사 내부에서만 사용가능한 점, 다수가 사용할 경우 VPN장비가 가지는 트랙픽 처리의 한계성 등 여러 가지 단점들이 생길 수 있으며, 이에 따라 사용하는 기업입장에서는 백업을 멀리 할 수밖에 없다. 클라우드 제공기업 입장에서도 전체적인 클라우드 서버 네트워크 사용량이 증가하기 때문에 부담이 된다. 이러한 단점들을 보완하기 위해 본 논문에서는 데이터 가용영역(Data Availability Zone)의 방법론을 사용한다는데, 먼저 아마존에서 서비스하는 가용영역(Availability Zone)에 대해 알아보아야 한다.

3.3. 아마존 서비스 가용 영역

아마존에서 서비스하는 가용영역은 하나의 거대한 웹 환경인 클라우드 서비스를 분리된 또 하나의 웹 환경을 구성하여 복수의 클라우드 환경을 구성하고 독립된 전력망과 환경을 만든 시스템이다. 아래 그림 3과 같이 한쪽의 클라우드가 서버가 정지하더라도 다른 가용영역의 클라우드 서버가 서비스를 대체하는 방식이다[8].

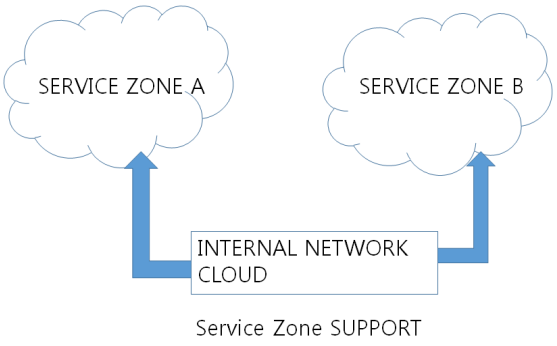

Fig. 3 Amazon Availability Zone

아마존 서비스 가용영역은 게임개발을 비롯한 여러 개발자들을 위한 서비스로 PaaS와 SaaS기능을 정지하지 않도록 해주고 있다. 한 가지 단점이라면 IaaS 부분이다. 즉, 서비스 가용영역에서 일부 데이터는 백업 해주고 있으나 전체적인 데이터 백업은 제공하고 있지 않다. 그 이유는 네트워크 속도가 저하되고 저장용량이 부족한 사태로서, EC2 내부 장애문제가 실제로 발생한 적이 있기 때문이다[11].

Ⅳ. 데이터 가용영역 아키텍쳐

본 논문에서 제안하는 데이터 가용영역이란 아마존에서 제공하는 가용영역에서 데이터 백업만을 위한 데이터 자동저장 시스템으로, 기업들의 천문학적인 손실을 막고 안전하고 신뢰성 있는 클라우드 서비스를 위한 백업 시스템이다. 본 논문에서 제시하는 데이터 가용영역의 구조는 그림 4와 같이 아마존의 서비스 가용영역과 비슷하지만, 백업하는 방식이 다르다. 아마존의 서비스 가용영역은 백업과의 이중화를 위해 지속적으로 백업과 이중화 구성을 위해 연결되어 있으나, 본 논문이 제시한 데이터 가용영역은 일정시간마다 데이터를 백업하는 점이 다르다. 클라우드 간에 지속적인 연결은 서비스 가용영역에서 보여준 것과 같이 네트워크 속도에 영향을 미치기 때문에 본 논문이 제시하는 데이터 가용영역은 지속적인 연결을 하지 않아 네트워크의 속도에 미치는 영향이 적다.

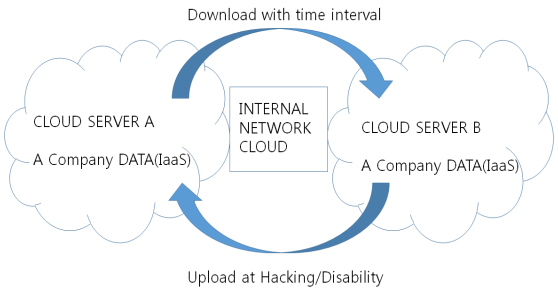

Fig. 4 Data Availability Zone Architecture Amazon

일정시간 마다 백업하는 기능은 미국 쿼럼(Quorum)사의 온큐(onQ)장비가 하드웨어적인 부분으로 적용하고 있는데, 이 장비는 서버를 이중화하는 장비로서 데이터 백업시 중복자료들을 무시하고 새로 저장된 자료들만 저장하는 기능과 자동 데이터 백업 기능이 있어 본 논문에서 제시한 데이터 가용영역 구현에 핵심이 될 장비이다. 데이터 가용영역의 구현은 하드웨어적인 부분보다는 소프트웨어적인 부분을 구현할 것이며, 이는 비용절감 측면에서 많은 도움이 될 것이다.

본 논문이 제시하는 데이터 가용영역과 전문가들이 권장하는 사내 스토리지 서버 백업과의 비교분석을 해보면 아래 표 2 과 같다. 데이터 복구 면에서는 둘 다 가능하며, 네트워크 속도 면에서는 일정시간마다 연결하는 데이터 가용영역이 빠를 수밖에 없다.

데이터 가용역의 경우 클라우드 내부망을 사용하게 되지만, 다른 경우는 내부 네트워크, 인터넷망 그리고 클라우드 내부망을 사용하게 된다. 보안적인 측면에서 사내 스토리지 서버는 자체 솔루션을 사용하기 때문에 보안성이 낮을 가능성이 높고 또한, 인터넷이 연결된 외부망을 거쳐야하기 때문에 중간 유출 가능성 등으로 보안성이 낮지만, 데이터 가용영역은 내부 사설망을 사용하기 때문에 보안성이 높다. 편의적인 측면에서도 수동적인 백업을 하는 사내 스토리지 보다 자동백업인 데이터 가용영역이 높다. 협업성은 사내 스토리지는 보안장비를 늘릴수록 협업성이 낮아지게 되나, 데이터 가용영역은 협업 기능에 상관없이 서비스 제공이 가능하다. 마지막으로 유지보수 측면에서는 사내 물리적 스토리지 백업은 장비구입과 유지보수 비용이 많이 드나, 데이터 가용영역은 가상화 저장으로 비교적 높지 않다.

데이터 가용영역과 스토리지 서버와의 효율적인 측면을 분석해보면 다음과 같다. 스토리지 백업서버는 백업 데이터 용량이 크면 클수록 필요한 서버 대수가 단계적으로 늘어 날 수밖에 없다. 그러나 데이터 가용영역은 가상화 서버로 구축하기 때문에 필요한 서버 대수가 스토리지 백업 서버에 비해 늘어나지 않으며, 백업 데이터 용량에 따라 비용이 늘어나지 않는 장점이 있다. 물론 클라우드 웹 환경 구성 자체가 비용이 많이 필요하나 한번 유지된 클라우드 웹 환경의 효율성에 대해서는 앞서 설명한 바와 같이 장점들이 많다.

Table. 2 Comparisons of in-Company Backup and Data Availability Zones (architectures)

Features	in-Company Storage Backup	Data Availability Zone
Data Back Up	YES	YES
Network Speed	Slow	Fast
Convenience	Low	High
Cooperability	Low with High Security	Independent with Security
Maintenance Cost	High	Average
Security	Low	High
Responsibility	Company	Service Provider

Ⅴ. 결 론

백업 데이터의 책임을 클라우드 컴퓨팅 서비스를 제공 받는 회사가 책임을 가지는 것과 서비스 제공자가 책임을 갖는 가는 방법의 차이로 볼수도 있다. 하지만, 클라우드 제공 업체가 제공하는 것이 장점이 많으며, 구조상으로 서비스 가용 영역과 유사하게 데이터 백업에도 가용영역을 제공하는 것이 우월하다. 또한, 비즈니스의 연속성을 위하여서는 인증제도에도 포함 시키는 것이 그 안정성을 고려했을 때 필요하다. 또한 이러한 내용이 향후 보안 인증제도에 포함 시키는 연구 등이 필요하다.

REFERENCES

[1] S. Wozniak. Cloud disaster leading to terrible within five year[Internet]. Available: http://www.ciorea.com/news/13542.

[2] J. Sim. Lessons learned in the cloud Tairan of Japan [Internet] Avaiable: http://www.ddaily.co.kr/cloud/news/article.html? no=94571.

[3] M. Whang, “A Study on setup Disaster Recovery Environment using by Cloud Service,” Master thesis, Soongsil University, Seoul, South Korea, pp. 35-40, 2012.

[4] J. Choi and D. Lee, “A Study on Virtual Storage Technology for the Safety of the Cloud Data,” in *Proceeding of Korea Society of Computer and Information*, vol. 21 no. 2, pp. 265-267, 2013.

[5] International Data Corporation. Asia Pacific End-User Cloud Computing Security Survey [Internet]. Available: https://www.idc.com/.

[6] H. Kim et al, “Study on security management in cloud computing environment,” *Korean review of management consulting*, vol. 2, no. 1, pp. 127-144, Feb. 2011.

[7] T. Kim and I. Kim, “Security Technology Trend in Cloud Computing,” *Korea Information Science Society Review*, vol. 30, no. 1, pp. 30-38, 2012.

[8] Y. Park, “Korean cloud certification system through foreign case of analysis and suggestions,” Master Thesis, SeJong Cyber University, Seoul, South Korea, 2014.

[9] Y. Park and Y. Park, “Data Availability Zone for backup system in Cloud Computing Service,” in *Proceeding of The Korea Institute of Information and Communication Engineering*, vol. 18, no. 2, pp. 0366-0369, Fall 2014.

[10] S. Lee, “A study of convergence security framework designing on cloud computing environment in military,” Ph. D. Dissertation, Hanse University, Kyungkido, South Korea, 2013.

[11] J. Brodkin. Amazon EC2 problem Availability zone effected? [Internet]. Available: http://www.itworld.co.kr/tags/53016.

박영호(Young-ho Park)

세종사이버대학교 정보보호대학원 석사
※관심분야 : 클라우드서비스, 보안 등

박용석(Yongsuk Park)

서강대학교 컴퓨터 공학학사
New York University (Poly) 컴퓨터 공학석사 및 박사
미국 AT&T (Bell) Labs, 삼성전자 연구소 등
현 세종사이버대학교 IT학부 및 대학원 주임교수
※관심분야 : 서비스보안, 빅테이터 및 IoT 서비스 보안, 사이버수사, 산업보안, 소프트웨어 보안 등