클라우드 컴퓨팅 서비스 백업을 위한 데이터 가용영역 방법론

박영호* · 박용석*

*정보보호대학원, 세종사이버대학교

Data Availability Zone for backup system in Cloud computing service

Young-ho Park* · Yongsuk Park*

*The Graduate School of Info Security. Sejong Cyber University

E-mail : ngel007@naver.com, yongspark@sjcu.ac.kr

요 약

최근 클라우드 컴퓨팅 서비스는 IT업계의 핵심기술로 전망되고 있다. 클라우드 서비스 산업의 시장규모는 매년 18.9%의 성장률을 보이며 2013년 1,330억 달러의 규모를 형성하였고, 2015년에는 1,768억 달러 규모를 형성할 것으로 전망되고 있다. 클라우드 컴퓨팅 서비스 산업의 성장은 많은 기업들에게 비용 절감과 업무의 효율성을 제공하고 있으나, 그에 따른 위험성 역시 높아지고 있다. 클라우드 서비스 특징상 데이터에 대한 통제성을 잃게 되고, 많은 데이터가 한 곳에 몰리는 현상은 장애가 발생하면 모든 기기의 데이터가 일제히 삭제되는 되는 문제점이 있다.

이에 본 논문에서는, 클라우드 컴퓨팅 서비스의 안전한 데이터 저장과 문제 발생에 따른 신속한 복구가 가능하도록 클라우드 서비스 데이터 전용의 가용영역에 대해서 연구하였다.

ABSTRACT

Recently been viewed as a core technology of the IT industry, cloud computing services. It is expected that the market for cloud services industry showed a growth rate of 18.9% annually, to form a scale of $ 1,330 billion dollars in 2013, and to form a 1,768 billion dollars in 2015. Growth of cloud computing services industry, provides the operational efficiency and reduce costs for many companies, but the risks associated with it is also increasing. There is a problem that phenomenon is to lose control of the data on features of the cloud service, more data is gathered in one place, when a failure occurs, it is removed simultaneously the data of all devices.

therefore, in the present paper is investigate the area a quick recovery with up to the problem and secure data storage INT the cloud computing service is available in only the data in the cloud service possible.

키워드

클라우드 컴퓨팅 서비스, 데이터 가용영역, 서비스 가용영역, 클라우드 보안

Ⅰ. 서 론

2012년 8월 애플 공동 창업자 스티브 워즈니악이 클라우드 컴퓨팅 서비스에 대해서 향후 5년 내에 큰 문제를 겪게 될 것이라고 우려를 표했다. 그는 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 것이라고 말했다[1].

2012년 6월 20일 일본 클라우드 서비스 제공업체인 ‘퍼스트 서버’가 전산장애를 낸 것인데 무려 5,698개 기업의 데이터를 날려버렸다. 당시 자사 서비스 버그를 해결하기 위해 소프트웨어 업데이트를 진행하다가 난 사고로 데이터 복구 소프트웨어를 통해서 데이터를 복원하였으나, 고객사별 접근 권한 설정이 불가능해 남의 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].

데이터는 기업 경영의 생명이자 심장이다. 서버가 고장 나면 새로운 서버로 교체할 수 있지만, 데이터가 분실되면 기업 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 구현 방법 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 보안문제가 항상 해결해야 할 우선 과제로 꼽히고 있으며[5], 클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구로 데이터 센터 운용과 재해발생시 클라우드 복구에 대해 연구가 진행되었다[6]. 김태형(2012)은 클라우드 컴퓨터의 데이터 및 시스템 보안기술을 논의한 바 있다[7].

III. 본 론

3.1 클라우드 서비스 종류

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

표 1. 클라우드 서비스의 계층별 분류

유형	특성
IaaS	서버, 스토리지, 네트워크 등 인프라 자원을 가상화하여 사용하도록 제공
SaaS	다양한 소프트웨어를 웹을 통해 사용자가 임대하여 사용하도록 제공
PaaS	이용자가 애플리케이션을 개발 및 구축할 수 있는 통합된 플랫폼을 제공

현재 가장 많이 제공되고 있는 클라우드 서비스는 IaaS로 SaaS와 PaaS사용 때마다 저장되는 공간이 클라우드 서비스내 IaaS이기 때문이다. 또한 개인적으로도 IaaS만 이용하는 사람도 많다.

3.2 클라우드 데이터 저장에 문제점

클라우드 컴퓨팅 서비스 데이터 저장에 문제점은 클라우드 컴퓨팅 서비스의 단점들을 보면 알 수 있다[8].

표 2. 클라우드 컴퓨팅 서비스의 단점

구분	내용
단점	지속적인 인터넷 연결이 필요하다.
	저장된 데이터가 안전하지 않다.
	고객사의 통제 권한이 부족하다.
	수많은 장치와 여러 저장 공간에 분산됨에 따른 보안문제가 발생할 수 있다.
	데이터의 중앙 집중화에 따른 위험성이 크다.

[표 2]에서 설명하고 있는 저장된 데이터가 안전하지 않다는 부분에 대해서 [그림 1]을 보면 이해하기 쉽다.

그림 1. 클라우드 데이터 저장의 문제점

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 2]와 같이 안전한 클라우드 사용을 권장하고 있다[9].

.

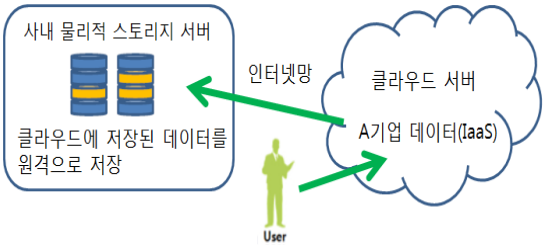

그림 2. 클라우드 사내 스토리지 백업

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 일정 간격 수동으로 백업해주어야 하는 불편성, 그리고 사내 스토리지 서버 구축에 따른 유지보수 비용

과 회사 내부에서만 사용가능한 점, 다수가 사용할 경우 VPN장비가 가지는 트랙픽 처리의 한계성 등등 여러 가지 단점들이 생길 수 있으며, 이에 따라 사용하는 기업입장에서는 백업을 멀리할 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 제시하는데, 먼저 아마존에서 서비스하는 가용영역(Availability Zone)에 대해 알아보아야 한다.

3.3 아마존 서비스 가용영역

아마존에서 서비스하는 가용영역은 하나의 거대한 웹 환경인 클라우드 서비스를 분뢰된 또 하나의 웹 환경을 구성하여 복수의 클라우드 환경을 구성하고 독립된 전력망과 환경을 만든 시스템이다. 아래 [그림 3]과 같이 한쪽의 클라우드가 서버가 정지하더라도 다른 가용영역의 클라우드 서버가 서비스를 대체하는 방식이다[10].

그림 3. 아마존 서비스 가용영역

아마존 서비스 가용영역은 게임개발을 비롯한 여러 개발자들을 위한 서비스로 PaaS와 SaaS기능을 정지하지 않도록 해주고 있다. 한 가지 단점이라면 IaaS 부분이다.

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].

3.4 데이터 가용영역 방법론

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.

데이터 가용영역의 구조는 [그림 4]와 같이 아마존의 서비스 가용영역과 비슷하다. 구조는 비슷하지만 백업하는 방식이 다르다. 아마존의 서비스 가용영역은 지속적으로 백업과 이중화 구성을 위해 연결되어 있으나, 데이터 가용영역은 일정시간마다 데이터를 백업하는 점이 다르다. 클라우드 간에 지속적인 연결은 서비스 가용영역에서 보여준 것과 같이 네트워크 속도에 영향을 미치기 때문에 데이터 가용영역은 지속적인 연결을 하지 않는 것이 특징이다.

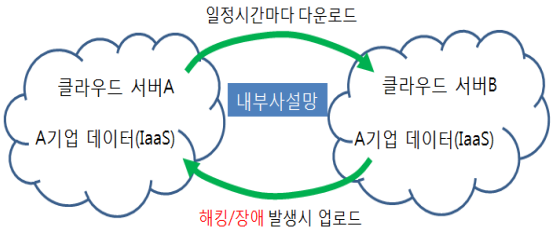

그림 4. 데이터 가용영역

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 데이터 가용영역 구현에 핵심이 될 장비이다. 데이터 가용영역의 구현은 하드웨어적인 부분보다는 소프트웨어적인 부분을 구현할 것이며, 이는 비용절감 측면에서 많은 도움이 될 것이다.

그렇다면 데이터 가용영역과 전문가들이 권장하는 사내 스토리지 서버 백업과의 비교분석을 해보면 아래 [표 3]과 같다.

표 3. 사내 백업과 데이터 가용영역 비교분석

구분	사내 물리적 스토리지 백업	데이터가용영역
데이터 복구	가능	가능
네트워크 속도	느림	빠름
보안성	낮음	높음
편의성	낮음	높음
협업성	보안성을 높일수록 낮음	보안성과 상관없이 제공
유지보수 비용	높음	보통

데이터 복구 면에서는 둘 다 가능하며, 네트워크 속도 면에서는 일정시간마다 연결하는 데이터 가용영역이 빠를 수밖에 없다. 보안적인 측면에서 사내 스토리지 서버는 인터넷이 연결된 외부망으로 보안성이 낮지만, 데이터 가용영역은 내부 사설망을 사용하기 때문에 보안성이 높다. 편의적인 측면에서도 수동적인 백업을 하는 사내 스토리지보다 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 높지 않다.

Ⅳ. 결 론

데이터 가용영역은 클라우드 제공업체 입장에서는 부담되는 시스템이기도 하다. 백업을 위한 클라우드를 따로 유지보수 해야 되기 때문이다. 물론 비용은 사용자가 부담하나 백업에 대해서는 적극적으로 권장 할 수 없게 된다. 그러나 일본의 클라우드 대란처럼 제 2의 클라우드 대란이 발생할 수도 있다. 이를 막기 위해서 클라우드 제공업체에서는 데이터 가용영역을 통해 안전하고 신뢰성 있는 클라우드를 제공한다면, 클라우드 서비스 산업은 더욱 발전할 것으로 전망된다.

향후 연구과제로는 데이터 가용영역 구현에 대한 구체적인 연구가 필요하다.

참고문헌

[1] Steve Wozniak, “Cloud disaster leading to terrible within five year”, http://www.ciorea.com/news/13542, 2012

[2] Sim jae-seok, “Lessons learned in the cloud Tairan of Japan ”, http://www.ddaily.co.kr/cloud/news/article.html? no=94571

[3] H. min-seop, “A Study on setup Disaster Recovery Environment using by Cloud Service” Soongsil University Master’s thesis, pp. 35-40, 2012

[4] C. Jae-Hyun, L.Dae-Sung, “A Study on Virtual Storage Technology for the Safety of the Cloud Data ” Korea Society of Computer and Information, 2013

[5] “Asia Pacific End-User Cloud Computing Security Survey”, International Data Corporation, 2009

[6] Kim hak-bun, “Study on security management in cloud computing environment”, KNU, pp 127~144, 2011

[7] T.H.Kim, I.H.Kim, “Security Technology Trend in Cloud Computing”, Korea Information Science Society Review, Vol30, No.1, pp 30-38, 2012

[8] Lee suk-woo, “A study of convergence security framework designing on cloud computing environment in military”, hanse university, pp. 17, 2013

[9] Kim jae suk, “Cloud environment data security”, CSA summit korea, 2013

[10] Amazon “Amazon web service F&Q”, pp 6, 2012

[11] Jon Brodkin, “Amazon EC2 problem Availability zone effected?”, ITWorld, http://www.itworld.co.kr/tags/53016