하이브리드 클라우드 서비스 모델에 대한 연구*

이재경, 손정갑, 은하수, 오희국
한양대학교 컴퓨터공학과
e-mail:jklee85@hanyang.ac.kr

A Research about Hybrid Cloud Service Models*

Jaekyung Lee, Junggab Son, Hasoo Eun, Heekuck Oh
Dept. of Computer Science and Engineering, Hanyang University

요 약

클라우드 컴퓨팅은 인터넷 기술을 기반으로 소프트웨어, 스토리지, OS 등의 가상화된 IT 자원 서비스로서 이용한 만큼 비용을 지불하는 방식으로 제공된다. 따라서 이를 이용하는 사용자 또는 조직이 IT 자원의 유지비용을 절감할 수 있는 이점이 있다. 하지만 기존의 단일 클라우드 서비스 모델은 가용성 문제, vendor lock-in 문제 등의 해결하기 어려운 문제점을 가지고 있다. 이에 따라 최근 클라우드 서비스 간 상호작용을 통해 기존 단일 클라우드의 문제를 해결하고자 하는 모델에 대한 연구가 진행되고 있다. 본 논문에서는 앞서 언급한 모델을 hybrid 클라우드 서비스 모델이라 칭한다. 현재까지 hybrid 클라우드 서비스 모델은 multi-cloud, inter-cloud, collaborative-cloud 등 크게 세 가지 형태로 제안되었다. 본 논문에서는 hybrid 클라우드 서비스 모델에 대한 전반적인 내용을 분석하고, 서로 다른 클라우드 서비스 간 상호작용 과정에서 새롭게 발생할 수 있는 보안 문제를 분석한다.

1. 서론

클라우드 컴퓨팅은 인터넷 기술을 기반으로 소프트웨어, 스토리지, OS 등의 가상화된 IT 자원 서비스를 이용한 만큼 비용을 지불하는 방식으로 제공된다. 따라서 클라우드 컴퓨팅 서비스를 이용하면 사용자와 조직은 자신의 어플리케이션에 대한 빠른 접근과 IT 자원의 유지비용을 절감시킬 수 있다. 이러한 장점 때문에 클라우드 컴퓨팅은 현대 IT 환경에서 중요한 기술로 자리 잡았고, 자연스럽게 이용률이 증가하였다. 이는 클라우드 컴퓨팅 기술의 급격한 발전의 토대가 되었다. 하지만 급격한 발전에 함께 발생하는 보안 위협과 데이터 및 시스템 제어에 대한 손실 문제의 해결은 클라우드 컴퓨팅 환경에서 중요한 과제가 되었다[1].

기존의 단일 클라우드 서비스 환경에서 안전성을 보장하기 위한 다양한 연구가 진행되었고, 많은 기술이 개발되었다. 하지만 단일 클라우드 서비스는 여전히 자연 재해나 정전, 네트워크 과부하, 또는 하드웨어 고장으로 인한 서비스 중단 문제를 가지고 있다[1,2]. 현재 클라우드 서비스에 의존하는 기업이 많기 때문에 만약 서비스가 중단된다면 이를 사용하는 기업의 손실에 대한 위험 부담이 크다. 기업은 이와 같은 상황에 대처하기 위해 예비로 사용할 수 있는 클라우드 서비스를 필요로 하게 될 수 있다[2]. 또한 단일 클라우드 서비스 환경에서는 성능을 위해 서비스를 확장하는 비용의 부담이 크다[3, 4].

최근 단일 클라우드 서비스의 문제 해결의 한계를 극복하고, 이점을 확대하기 위해 여러 클라우드 서비스가 혼합되어 있는 모델이 제안되었다. 이는 서로 다른 클라우드 간 상호작용을 통해 여러 클라우드 서비스를 하나의 서비스처럼 사용한다는 목적을 가지고 있다. 기존의 hybrid 클라우드 용어는 둘 이상의 클라우드 모델(private, community, 또는 public)이 혼합된 형태의 클라우드 모델을 의미하지만, 본 논문에서는 기존 용어의 의미를 확장하고, 서로 다른 클라우드 서비스 모델이 혼합된 형태의 모델을 총칭하여 'hybrid 클라우드 서비스 모델'이라 칭한다.

단일 클라우드 서비스 환경에서 hybrid 서비스 클라우드 환경으로 변화하게 된 이유는 다음과 같다. hybrid 클라우드 서비스 환경에서는 클라우드 서비스 제공자가 자신의 서비스에는 없는 기능을 다른 클라우드 서비스를 통해 빌려 사용할 수 있다. 이로 인해 저렴한 비용으로 사용자에게 새로운 기능을 제공할 수 있다는 이점이 있다[3]. 또한 클라우드 서비스를 이용하여 서비스 인프라를 구축한 기업 측면에서는 인프라 구축에 이용된 서비스에 종속되는 vendor lock-in 문제가 발생한다. 하지만 hybrid 클라우드 서비스 환경에서는 서로 다른 클라우드 서비스 간 상호작용을 통해 vendor lock-in 문제를 피하고 서비스를 개선할 수 있어 고객들에게 보다 나은 서비스 제공이 가

* 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-R1A2A2A01046986)
* 이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(No. 2012-R1A1A2009152)

능하다[5].

현재까지 hybrid 클라우드 서비스 모델은 'multi-cloud,' 'inter-cloud,' 'collaborative-cloud,' 등 세 가지 명칭으로 제안되었다. 명칭은 서로 다르지만 세 가지 모델 모두 기존 단일 클라우드 서비스를 결합하여 서비스 간 상호작용이 가능한 모델을 의미한다. 이에 따라 기존 단일 클라우드 환경과 동일한 문제점뿐만 아니라 클라우드 서비스 간 상호작용 과정에서 새로운 문제점이 발생할 수 있다. 본 논문에서는 hybrid 클라우드 서비스 모델에 대해 분석하고, 발생할 수 있는 문제점을 분석해본다.

본 논문의 구성은 다음과 같다. 2장에서는 연구 배경을 서술하고, 3장에서는 hybrid 클라우드 서비스 모델에 대해 살펴본다. 그리고 4장에서 hybrid 클라우드 환경에서의 상호작용 과정에서 발생할 수 있는 보안 문제를 분석해보고, 마지막으로 5장에서 결론을 맺는다.

2. 연구 배경

2.1 클라우드 컴퓨팅 배치 모델

클라우드 컴퓨팅 배치 모델은 다음과 같이 크게 세 가지의 모델이 있다.

- *Public-cloud*

서비스 제공자에 의해 어플리케이션, 스토리지 등의 서비스를 일반 대중이 쉽게 이용할 수 있는 모델이다. 이 서비스는 무료로 사용할 수 있거나 서비스를 사용한 만큼 비용을 지불하는 방식으로 제공된다.

- *Private-cloud*

하나의 조직을 위해 운영되는 클라우드 구조로, 내부 또는 제 3집단에 의해 관리되는 모델이다. 특정 업무 중심의 어플리케이션으로 구성할 수 있어 업무에 효율적이며, 조직의 구성원에게 안전성 및 신뢰성을 제공할 수 있다.

- *Hybrid-cloud*

둘 이상의 클라우드 모델(private, public)이 혼합된 구조로 여러 배치 모델의 고유한 특성을 유지하고 있는 모델이다. 혼합된 각 클라우드 모델의 장점을 모두 제공할 수 있으며, 단점을 완화시킬 수도 있다.

2.2 단일 클라우드 서비스의 문제점

클라우드 컴퓨팅 환경에서 안전성은 중요한 요소이다. 클라우드 컴퓨팅 기술이 발전하고 사용자가 증가함에 따라 안전성을 보장하기 위한 다양한 연구가 진행되었다. 이로 인해 많은 기술이 개발되었지만 단일 클라우드 서비스 환경에서는 해결하기 어려운 문제점이 존재한다.

클라우드 컴퓨팅은 인터넷을 기반으로 사용자에게 제공되는 서비스이므로 자연 재해나 정전, 네트워크 과부하, 또는 하드웨어의 고장으로 인해 서비스가 중단될 수 있다. 즉, 가용성 문제가 발생한다[1,2]. 만약 클라우드 서비스를 이용하여 고객에게 서비스를 제공하는 기업인 경우 서비스 중단 시간에 따른 손실에 대한 위험 부담이 크다.

클라우드 서비스 제공자 측면에서는 고객에게 더 나은 서비스를 제공하기 위해 하드웨어나 소프트웨어, 기능 등의 서비스 확장을 위한 비용 부담이 크다. 만약 클라우드 서비스를 이용하는 기업이 고객의 요구 사항을 충족시키려 한다면 클라우드 서비스 제공자에게 서비스 확장을 요구할 수 있다. 하지만 앞서 말한 확장을 위한 비용 부담이 크기 때문에 서비스 확장이 쉽지 않다. 하지만 클라우드 서비스의 확장이 불분명하더라도 이미 서비스 인프라를 구축한 기업의 경우 타 클라우드 서비스 업체로 이주하는 것은 쉽지 않다. 따라서 단일 클라우드 환경에서는 기업이 이용하는 클라우드 서비스 제공자에게 종속적이 될 수 있는 vendor lock-in 문제점이 있다[5].

3. hybrid 클라우드 서비스 모델

3.1 hybrid 클라우드 서비스 모델의 출현 배경

클라우드 컴퓨팅의 기본적인 배치 모델인 hybrid 클라우드 배치 모델은 public 클라우드와 private 클라우드를 혼합하여 각각의 장점을 확대시키고, 단점은 완화시킬 수 있다. 최근에는 기존 hybrid 클라우드 배치 모델을 확장하여 서로 다른 클라우드 서비스 간의 상호작용을 통해 2.2절에서 언급한 단일 클라우드 서비스의 문제를 해결하고자 hybrid 클라우드 서비스 모델이 제안되었다.

3.2 hybrid 클라우드 서비스 모델의 정의

서로 다른 클라우드 간 상호작용을 위해 현재까지 제안된 hybrid 클라우드 서비스 모델은 다음과 같다.

- *Multi-cloud*

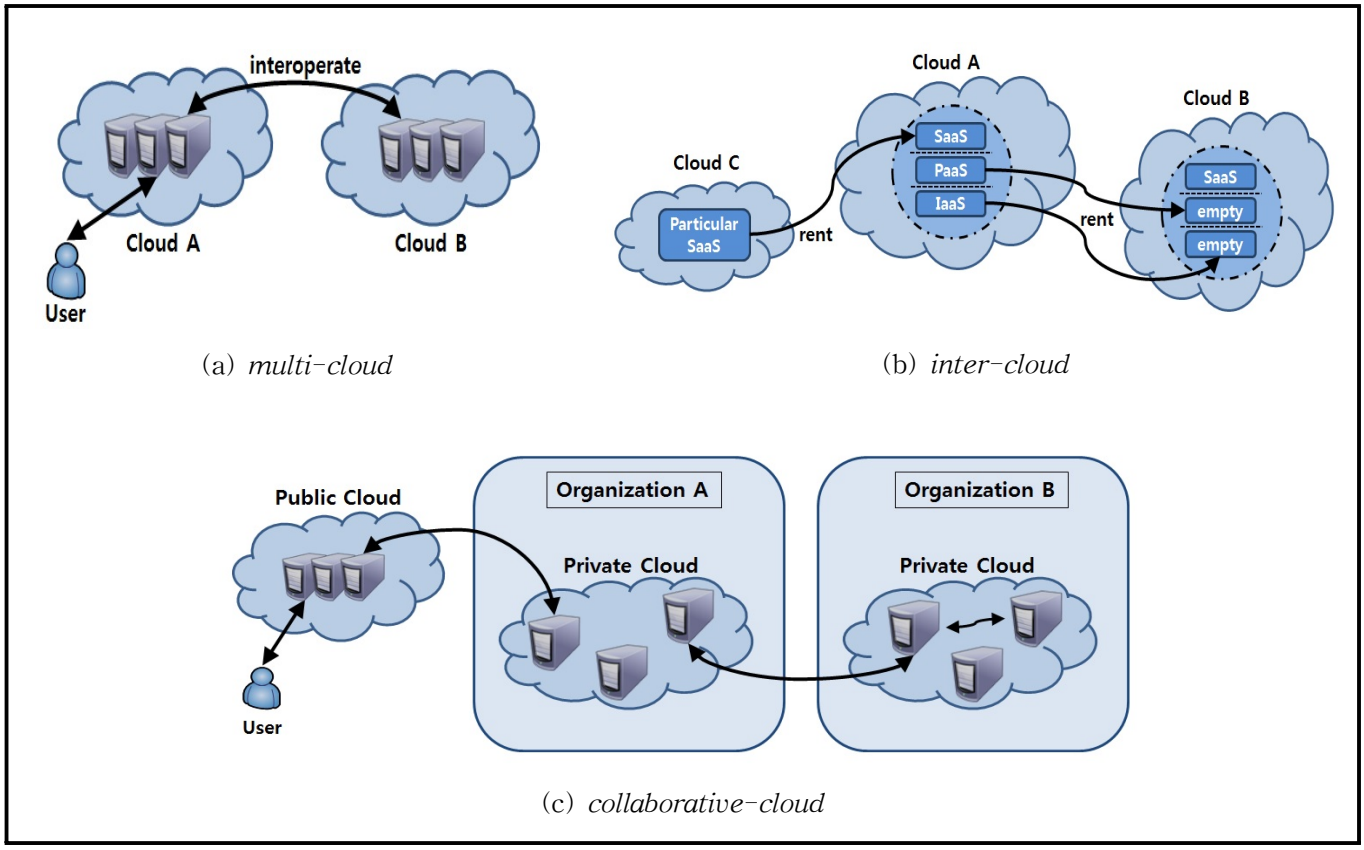
(그림 1)의 (a)와 같이 두 개 이상의 클라우드 서비스를 동시에 하나의 클라우드 서비스처럼 사용이 가능한 모델이다. 단일 클라우드 서비스 환경에서 발생하는 서비스 중단에 의한 위험을 최소할 수 있다[2].

- *Inter-cloud*

각 클라우드 서비스의 성능과 가용성과 같은 서비스 품질 보장의 목적을 가지고 있으며, (그림 1)의 (b)와 같이 서로 다른 서비스 제공자의 클라우드 구조(SaaS, PaaS, IaaS) 간 상호 연동이 가능한 모델이다[6]. 만약 SaaS 제공자가 인프라를 필요로 한다면, 직접 인프라를 구축하는 것보다 IaaS 제공자로부터 인프라를 획득하는 것이 더 효율적이며 비용 절감을 가능하게 한다. 이처럼 서로 다른 클라우드 서비스 간 연동을 통해 서비스의 안전성과 품질을 개선하여 고객의 요구 사항을 충족시킬 수 있는 서비스 제공을 보장한다.

- *Collaborative-cloud*

(그림 1)의 (c)와 같이 public cloud와 private cloud 간, 그리고 서로 다른 조직의 private cloud 간 협업을 위한 클라우드 서비스 모델이다[5]. 각 조직에 이미 구축되어 있는 private cloud 간 상호작용을 통하여 둘 이상의 조직의 협업 인프라를 구축할 수 있다. 따라서 상호 간 협



(그림 1) hybrid 클라우드 서비스 모델

업 과정이 효율적으로 이루어질 수 있고, 협업을 관리하기가 편리해진다는 이점이 있다.

최근에는 특정 소프트웨어에 초점을 두고 서비스를 제공하여 다른 클라우드와 상호작용을 하는 모델에 대한 연구가 진행되고 있다[7]. 예를 들어 (그림 1)의 (b)과 같이 A와 C클라우드 서비스가 있다. C는 보안관리 인프라 제공에 초점을 두고 서비스를 하고, A는 이를 구축하려 하지만 비용 측면에서 부담을 가지고 있다. 이때 위의 hybrid 클라우드 서비스 모델의 특징 중 클라우드 구조 간 상호 연동이 가능하다는 점을 이용하면 A클라우드는 C클라우드와 상호작용을 통해 보안관리 인프라를 구축하지 않고 빌려서 사용이 가능하게 된다.

3.3 hybrid 클라우드 서비스 모델의 장점

hybrid 클라우드 서비스 모델을 이용하면 다음과 같은 이점을 얻을 수 있다.

- 단일 클라우드 환경에서 서비스 중단 문제로 인한 손실의 위험을 최소화하여 서비스를 이용하는 기업이나 고객의 신뢰를 높일 수 있다. 하나의 클라우드 서비스가 중단되었더라도 예비의 클라우드 서비스를 이용할 수 있기 때문이다.
- 클라우드 서비스 제공자 측면에서는 더 나은 서비스를 원하는 고객의 요구 사항을 충족시키기 위해 소프트웨어, 하드웨어, 그리고 기능 등의 서비스 확장에 드는 비용을 절감시킬 수 있으며, 서로 다른 클라우드 서비스 간 상호작용을 통해 새로운 기능을 제공할 수 있다는 이점이 있다.
- 클라우드 서비스를 이용하는 기업 측면에서는 단일 클라우드 환경에서 이미 서비스 인프라가 구축된 상태에서 발생할 수 있는 vendor lock-in 문제를 피할 수 있다. 또한 더 나은 서비스를 원하는 고객의 다양한 요구를 충족시키기 위해 서로 다른 클라우드 서비스의 인프라를 이용하여 새로운 기능을 도입할 수 있다. 따라서 고객의 요구사항에 맞추어 개선된 서비스를 제공할 수 있다.

4. 보안 문제

hybrid 클라우드 서비스 환경에서는 서로 다른 클라우드 서비스 간 상호작용에 의해 기존의 단일 클라우드 서비스 환경보다 더 복잡한 보안 문제가 발생 할 수 있다[8]. hybrid 클라우드 서비스 환경에서 발생할 수 있는 보안 문제는 다음과 같다.

- 악의적인 서비스 제공자의 데이터 분석 문제

hybrid 클라우드 서비스 환경에서는 악의적인 목적을 가진 서비스 제공자가 다른 클라우드 서비스 제공자에게 상호 연동을 제안할 수 있다. 예를 들어 A클라우드 서비스 제공자가 상호 연동을 통해 B클라우드 서비스의 스토리지에 접근할 수 있다. 이 때 A클라우드 서비스 제공자

가 악의적인 목적을 가지고 있다면, B클라우드 서비스의 스토리지에 저장되어 있는 데이터를 분석하여 새로운 정보를 추출할 수 있다.

- 서로 다른 클라우드 간 사용자 인증 문제

hybrid 클라우드 서비스 환경에서는 사용자의 요청에 의해 서로 다른 클라우드 서비스와의 상호작용이 가능해야 하기 때문에 사용자 인증정보를 통해 인증이 이루어져야 한다. 하지만 클라우드 서비스마다 서로 다른 사용자 인증 인터페이스를 가질 수 있다. 각 인터페이스마다 인증에 요구되는 사용자 정보의 속성이 다르거나 정보의 양이 다를 수 있다. 예를 들어 A클라우드 서비스는 인증에 아이디와 패스워드를 요구하지만, B클라우드 서비스는 공인인증서를 요구할 수 있다. 또한 A클라우드 서비스는 사용자 정보 중 두 가지 속성(e.g. 아이디, 비밀번호)을 요구하지만, B클라우드 서비스는 사용자 정보 중 세 가지 속성(e.g. 아이디, 비밀번호, One-time password)을 요구할 수도 있다. 따라서 A와 B클라우드 간 상호작용을 위해 인증 횟수가 증가하게 될 수 있다.

- 데이터 전달 및 처리 문제

hybrid 클라우드 서비스 환경에서는 서로 다른 클라우드 간 상호작용을 위해 사용자의 데이터를 전달하고 처리할 수 있다. 예를 들어 스토리지만을 제공하는 A서비스 제공자에게 데이터를 위임한 사용자가 있다. 이 사용자는 자신의 데이터를 이용하여 작업하기를 원하지만 작업을 할 수 있는 소프트웨어를 가지고 있지 않을 수도 있다. 클라우드 컴퓨팅 환경에서는 사용자가 작업에 필요한 소프트웨어를 제공하는 다른 서비스에 접근하여 작업을 할 수 있다. 이 때 스토리지에 위임된 사용자의 데이터는 작업을 위해 소프트웨어를 제공하는 B서비스 제공자에게 전달되어 처리될 것이다. 이 때 B서비스 제공자가 전달 받은 사용자의 데이터를 악의적인 목적을 가지고 사용할 수 있다. 이 문제는 데이터를 암호화하여 전달함으로서 해결할 수 있지만 암호화된 데이터는 작업 요청에 대한 처리를 할 수 없다는 문제점이 있다.

5. 결론

기존의 단일 클라우드 서비스 환경에서는 가용성 문제, 서비스 확장비용 문제, vendor lock-in 문제 등 해결하기 어려운 문제점이 존재한다. 최근 단일 클라우드 서비스 환경의 문제 해결의 한계점을 해결하기 위해 서로 다른 클라우드 간 상호작용이 가능한 hybrid 클라우드 서비스 모델에 대한 연구가 진행되고 있다.

본 논문에서는 현재까지 제안된 multi-cloud, inter-cloud, collaborative-cloud 등의 hybrid 클라우드 서비스 모델에 대한 분석을 수행하였다. 서로 다른 클라우드 서비스 간 상호작용이 가능한 hybrid 클라우드 서비스 모델은 혼합된 클라우드 서비스 각각의 장점을 가질 수 있으며, 단점을 보완할 수 있는 이점이 있다. 하지만 hybrid 클라우드 서비스 환경에서는 본 논문에서 분석한 바와 같이 새로운 문제가 발생할 수 있다. 이는 클라우드 서비스 간 상호작용을 방해하는 요인이 될 수도 있다. 따라서 hybrid 클라우드 서비스 환경이 활성화되기 위해서는 앞서 언급한 보안 문제는 해결되어야 할 것이다.

참고문헌

[1] M. A. Alzain, E. Pardede, B. Soh, and J. A. Thom, “Cloud Computing Security: From Single to Multi-Clouds,” 45th Hawaii International Conference on System Science, pp. 5490-5499, 2012.

[2] M. Kretzschmar, M. Golling, and S. Hanigk, “Security Management Areas in the Inter-Cloud,” IEEE 4th International Conference on Cloud Computing, pp. 762-763, 2011.

[3] M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishnan, G. J. Ahn, and E. Bertino, “Collaboration in Multicloud Computing Environments: Framework and Security Issues,” IEEE Computer Society, pp. 76-84, 2013.

[4] R. Benny, B. David, E. Amir, H. David, L. Irit, N. Kenneth, T. Johan, R. Carmelo, V. Massimo, C. Stuart, L. Eliezer, M. Alessandro, M. Philippe, H. Munoz, and G. Tofetti, “Reservoir - When One Cloud Is Not Enough,” IEEE Computer Society, pp. 44-51, 2011.

[5] M. Kretzschmar and S. Hanigk, “Security Management interoperability challenges for Collaboration Clouds,” 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management, pp. 43-49, 2010.

[6] Y. Demchenko, M. X. Makkes, R. Strijkers, and C. de Laat, “Intercloud Architecture for Interoperability and Integration,” IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 666-674, 2012.

[7] D. Krishnan and M. Chatterjee, “Cloud Security Management Suit - Security as a Service,” World Congress on Information and Communication Technologies (WICT), pp. 431-436, 2012

[8] D. Bernstein and D. Vij, “Intercloud Security Considerations,” IEEE 2nd International Conference on Cloud Computing Technology and Science, pp. 537-544, 2010.