Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1131

멀티클라우드 환경에서 사용자에게 서비스의 투명성을 제공하는 인증 기법*

이 재 경,† 손 정 갑, 김 훈 민, 오 희 국‡
한양대학교

An Authentication Scheme for Providing to User Service Transparency in Multicloud Environment*

Jaekyung Lee,† Junggab Son, Hunmin Kim, Heekuck Oh‡
Department of Computer Science and Engineering, Hanyang University

요 약

클라우드 컴퓨팅 모델은 대부분이 단일 서버 모델로 가용성, 내부자 공격, vendor lock-in 등의 해결하기 어려운 문제점을 가지고 있다. 이를 해결하기 위해 최근 멀티클라우드 모델에 관한 연구가 진행되고 있다. 멀티클라우드 모델은 기존 클라우드 모델의 단점을 보완하고, 새로운 서비스를 제공할 수 있는 장점이 있다. 본 논문에서는 멀티클라우드 모델에서 발생하는 사용자 인증 문제에 초점을 맞추고 이를 해결하기 위한 기법을 제안한다. 클라우드 브로커 기반의 멀티클라우드 모델을 정의하고, 여기에 적용할 수 있는 인증 프로토콜을 제안하였다. 제안한 프로토콜은 사용자에게 서비스의 투명성을 제공하고, 서비스 제공자의 위장 공격을 방지할 수 있다.

ABSTRACT

Most of the single server model of cloud computing services have problems that are hard to solve, such as a service availability, insider attack, and vendor lock-in, etc. To solve these problems, the research about multicloud has emerged. Multicloud model can supplement previous cloud model's weakness and provides new services to user. In this paper, we focus on a user authentication problem in multicloud model and propose a scheme to resolve it. We define a cloud broker-based multicloud model. And we propose an authentication protocol that is applicable at presented model. The proposed scheme can provide service transparency to user and prevent an impersonation attack by service provider.

Keywords: cloud computing, multicloud, authentication, cloud broker

I. 서 론

클라우드 컴퓨팅은 네트워크 기술을 기반으로 하여 하드웨어나 소프트웨어와 같은 컴퓨팅 자원을 가상화된 형태로 제공하는 기술을 말한다[1]. 클라우드 컴퓨팅 기술은 현재의 컴퓨터 구조와 서비스에 많은 영향을 미쳤으며 많은 변화를 가져왔다. 클라우드 컴퓨팅 기술로 인해 데이터나 어플리케이션에 대해 시간, 장소, 기기에 관계없이 빠르고 쉬운 접근이 가능하게 되었으며, 효율적인 관리 또한 가능하게 되었다. 그리고

접수일(2013년 10월 1일), 게재확정일(2013년 11월 14일)
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0301-13-1002)
* 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)
† 주저자, jklee85@hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr(Corresponding author)

컴퓨팅 자원을 빌려 사용할 수 있기 때문에 기업이나 조직에 필요한 컴퓨팅 인프라의 초기 구축비용과 유지비용의 절감시켜주는 장점을 가지고 있다[2]. 이러한 클라우드 컴퓨팅의 장점으로 인해 사용량이 급증하게 되었고, 급격한 발전을 이루었다.

현재 상용화된 대부분의 클라우드 컴퓨팅 서비스는 단일 클라우드 컴퓨팅 서비스이다. 이 또한 기존의 서버/클라이언트 환경과 동일하게 사용자 인증, 접근제어, 데이터 공유, 사용자 프라이버시 등의 해결해야할 다양한 보안 문제가 존재한다. 이러한 문제를 해결하기 위해 많은 연구가 진행되고 있다. 하지만 이외에도 단일 클라우드 컴퓨팅 서비스 환경에서는 해결하기 어려운 문제점이 존재한다. 바로 서비스 가용성 문제와 악의적인 내부자 문제, vendor lock-in 문제이다[3,4,5].

단일 클라우드 컴퓨팅 서비스의 문제점으로 인해 아직은 기업이나 조직에서 중요한 업무나 데이터를 다루는 경우에는 이용하기를 꺼려한다[6]. 최근에는 단일 클라우드 컴퓨팅 서비스의 문제점을 완화하기 위해 'cloud-of-clouds', 'cross-cloud', 'federated clouds', 'intercloud' 등의 멀티클라우드 모델에 관한 연구가 진행되고 있다[7]. 멀티클라우드 모델은 단일 클라우드 컴퓨팅 서비스의 단점을 보완할 수 있으며, 여러 서비스 간의 상호작용으로 인한 시너지 효과를 기대할 수도 있다.

멀티클라우드의 개념은 두 개 이상의 서로 다른 클라우드 컴퓨팅 서비스가 특정 계약에 의해 서로 상호작용하는 모델을 말한다. 이로 인해 사용자는 하나의 서비스를 이용하지만 여러 개의 서비스로부터 기능을 제공받을 수 있게 된다. 그리고 서비스 제공자는 자신의 서비스를 이용하는 사용자에게 더 나은 서비스를 제공할 수 있게 된다. 하지만 멀티클라우드 역시 단일 클라우드 컴퓨팅 서비스 환경에서 발생할 수 있는 사용자 인증 문제, 프라이버시 침해 등의 문제점이 동일하게 발생할 수 있다. 본 논문에서는 사용자 인증에 관한 문제를 다룬다.

기존에 제안된 클라우드 컴퓨팅을 위한 인증 기법은 사용자가 직접 서비스에 등록하여 인증 받는 방식으로, 만약 사용자가 다수의 서비스를 이용하기 위해서는 각각의 서비스에 등록해야 하며 여러 번의 인증 과정을 거쳐야 하는 불편함이 발생한다[8]. 이를 해결하기 위해 Single Sign-On(SSO) 인증 방식을 이용할 수 있다. 하지만 SSO 서버가 공격당하면 그 피해 규모가 크고, 많은 사용자의 인증을 처리하다보면 병목 현상이 발생할 수 있다. 따라서 본 논문에서는 클라우드 브로커 기반 멀티클라우드 모델을 제시하고, 제시한 모델에 적절한 인증 프로토콜을 제안한다.

제시한 클라우드 브로커 기반 멀티클라우드 모델에서는 클라우드 브로커가 각 클라우드 컴퓨팅 서비스 간 중개와 인증을 담당한다. 이 모델에 적용하기 위해 제안하는 인증 프로토콜은 사용자 대신 서비스 제공자가 클라우드 브로커의 인증 과정을 거치기 때문에 사용자에게 서비스의 투명성을 제공할 수 있다. 또한 사용자의 서명값을 이용하여 서비스 제공자의 위장 공격을 방지하고, 사용자로 인해 시스템에 문제가 발생한 경우 해당 사용자에게 책임을 물을 수 있도록 설계하였다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드 컴퓨팅 기술과 단일 클라우드 컴퓨팅 서비스의 한계에 대해 알아본다. 3장에서는 멀티클라우드 모델에 대해 알아보고, 기존 인증 기법들에 대해 분석한다. 4장에서는 제안하는 기법에 대해 설명하고, 5장에서 기법에 대한 분석을 한다. 마지막으로 6장에서 결론을 맺는다.

II. 연구 배경

이 장에서는 클라우드 컴퓨팅과 그 배치 모델에 대해 설명하고, 기존의 단일 클라우드 컴퓨팅 서비스의 한계점을 알아본다.

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅에 대한 공식적인 정의는 학계와 업계 모두에서 많이 제안되었지만 핵심적인 공통 요소를 포함하는 정의를 U.S. NIST(National institute of Standards and Technology)에서 제안하였다. NIST에서 제안한 클라우드 컴퓨팅 서비스란 네트워크, 서버, 스토리지, 응용프로그램 등 다

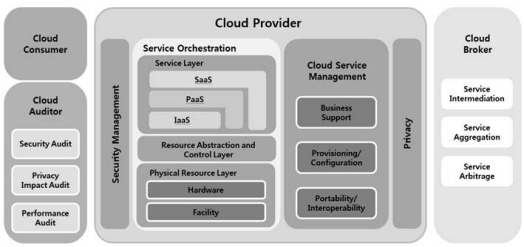

Fig.1. NIST Cloud Reference Model

양한 가상화된 컴퓨팅 자원들의 공유된 풀에 네트워크를 통해 접근하여 언제든지 편리하게 사용이 가능한 컴퓨팅 방식이다[9]. 이러한 컴퓨팅 자원은 Fig.1.의 서비스 계층 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service)별로 제공된다.

클라우드 컴퓨팅의 서비스는 주문형 아웃소싱(On-Demand) 방식으로 사용자에게 제공된다. 즉, 사용자는 서비스 제공자가 구축하고 관리하는 컴퓨팅 자원을 네트워크를 통해 필요한 만큼 빌려 사용할 수 있다. 따라서 사용자들은 컴퓨팅 자원의 초기 구축비용과 유지비용을 절감할 수 있게 된다.

2.2 클라우드 배치 모델의 종류

클라우드 컴퓨팅은 배치 상태에 따라 크게 사설(private) 클라우드, 공용(public) 클라우드, 그리고 사설과 공용이 혼합된 혼합(hybrid) 클라우드, 이 세 가지로 구분할 수 있다. 세 가지 모델에 대한 설명은 다음과 같다[10].

2.2.1 공용 클라우드

공용 클라우드는 클라우드 서비스 제공자가 IT 자원을 구축하고 관리해주는 모델이다. 어플리케이션, 스토리지 등의 서비스가 On-Demand 방식으로 일반 대중에게 제공된다. 이는 IT 자원을 아웃소싱하는 방식으로 사용자의 주요 데이터 노출, 저작권 침해 등의 보안 위험이 존재할 수 있지만, IT 자원의 구축 및 유지보수 비용이 저렴하다는 장점이 있다.

2.2.2 사설 클라우드

사설 클라우드는 하나의 기업이나 조직을 위해 운영되는 클라우드 모델이다. 특정 업무 중심의 어플리케이션으로 구성할 수 있고, 기업이나 조직이 요구하는 서비스 수준으로 관리할 수 있어 업무에 효율적이다. 또한 외부로부터의 접근을 최대한 차단하기 때문에 데이터 노출 등의 보안 위협을 줄일 수 있다. 사설 클라우드는 공용 클라우드에 비해 IT 자원의 구축 및 유지보수 비용이 높은 편이지만, 공용 클라우드에 비해 안전한 관리가 가능한 장점을 가지고 있다.

2.2.3 혼합 클라우드

사설 클라우드, 공용 클라우드 각각의 장점을 결합한 모델이다. 기업이나 조직의 주요 데이터는 직접 구축한 사설 클라우드의 IT 자원을 활용하고, 그 외에는 공용 클라우드를 활용하는 것이다. 이로 인해 데이터 노출 등의 위협을 최소화하여 보안성을 향상시킬 수 있고, IT 장비 구매 및 유지보수 비용을 절감할 수 있는 장점이 있다.

2.3 단일 클라우드 컴퓨팅 서비스의 한계

단일 클라우드 컴퓨팅 서비스는 하나의 서비스 제공자가 서버를 구축한 뒤 서비스하는 형태이기 때문에 자연 재해나 정전, 하드웨어 오류, 네트워크 과부하 등의 문제로 인해 서비스 자체가 중단될 수 있다. 이는 처리 중이던 데이터의 손실을 발생시킬 수 있다. 그리고 클라우드 컴퓨팅 서비스를 이용하여 컴퓨팅 인프라를 구축한 기업이나 조직의 경우 서비스 중단 시간에 따른 피해가 막대할 수 있다. 또한 클라우드 컴퓨팅 서비스를 이용하여 이미 자신들의 컴퓨팅 인프라를 구축한 기업이나 조직은 그 인프라를 다른 클라우드 컴퓨팅 서비스로 옮겨서 다시 구축하는 것이 쉽지 않다.

클라우드 컴퓨팅 서비스는 아웃소싱 방식이기 때문에 앞서 언급한 문제점은 기업이나 조직에 미치는 파급효과가 클 수 있다. 이에 따라 아직은 기업이나 조직은 자신의 주요 데이터나 어플리케이션을 위해 단일 클라우드 컴퓨팅 서비스를 이용하는 것을 꺼려한다[11]. 이러한 문제점을 완화시키고, 클라우드 컴퓨팅 서비스 간 상호작용으로 인한 시너지 효과를 얻기 위해 멀티클라우드 모델에 대한 연구가 시작되었다.

III. 관련 연구

이 장에서는 멀티클라우드에 대해 알아보고, 지금까지 연구된 인증 기법에 대해 설명하고 멀티클라우드에 적용할 경우 발생하는 문제점에 대해 알아본다. 그리고 멀티클라우드 모델을 구성하기 위해 클라우드 브로커에 대해 알아본다.

3.1 멀티클라우드

멀티클라우드는 두 개 이상의 서로 다른 클라우드

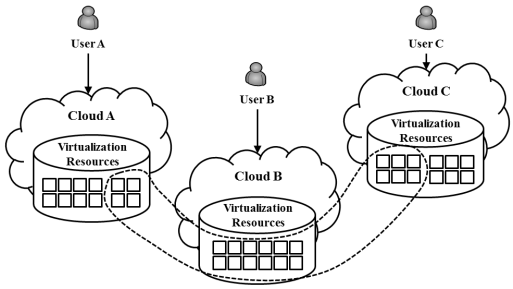

Fig.2. Conceptual Model of Multicloud

컴퓨팅 서비스가 계약에 의해 상호작용하는 모델로 클라우드 컴퓨팅 서비스의 연합이라 할 수 있다. 즉, Fig.2.와 같이 어떤 클라우드 컴퓨팅 서비스의 가상화된 자원을 다른 클라우드 컴퓨팅 서비스가 사용할 수 있는 것을 의미한다. 멀티클라우드는 컴퓨팅 능력, 스토리지 등의 자원이 부족한 클라우드 서비스 제공자에게 다른 클라우드 컴퓨팅 서비스로부터 가상화된 자원을 빌려서 사용할 수 있는 기회를 제공한다. 이로 인해 클라우드 서비스 제공자는 자신의 사용자에게 더 나은 서비스를 제공할 수 있는 이점이 있다. 그리고 사용자는 하나의 서비스에만 등록하여 사용하지만, 실제로는 다수의 서비스를 사용하게 되면서 폭넓은 서비스를 제공받을 수 있다[12].

3.2 기존 클라우드 컴퓨팅을 위한 인증 기법

현재까지 클라우드 컴퓨팅 환경에 적용하기 위해 많은 사용자 인증 기법이 제안되었다. Kerberos를 이용한 인증 기법[13], PKI(Public Key Infrastructure)를 이용한 인증 기법[14], 스마트 카드를 이용한 인증 기법[15] 등 클라우드에 적용 가능한 다양한 인증 기법들이 제안되었다. 하지만 현재까지 제안된 인증 기법의 적용 범위는 단일 클라우드 컴퓨팅 서비스에 한정되어 있어, 멀티클라우드 환경에 적용하기에는 부적절하다. 기존의 클라우드 컴퓨팅을 위한 사용자 인증 방식은 사용자가 자신이 사용할 클라우드 컴퓨팅 서비스에 직접 등록한 뒤 인증 과정을 거쳐야 한다. 멀티클라우드 환경에서는 사용자가 두 개 이상의 클라우드 컴퓨팅 서비스를 사용하게 된다. 이때 각 클라우드 컴퓨팅 서비스마다 독자적인 인증 모듈과 사용자 관리 모듈을 가지고 있다. 이로 인해 멀티클라우드 환경에서는 Fig.3.과 같이 사용자가 다수의 서비스를 이용하기 위해서 각각의 서비스에 등록해야 하며, 각 서비스를 이용할 때마다 인증 과정을 거쳐야 하는 불편함이 발생한다. 그리고 사용자가 사용하는 서비스가 증가할 때마다 직접 유지해야 하는 인증 정보 또한 증가하게 된다. 이에 따라 멀티클라우드 환경에서는 한 번의 인증 과정을 통해 다수의 서비스에 접근이 가능한 인증 시스템이 요구된다.

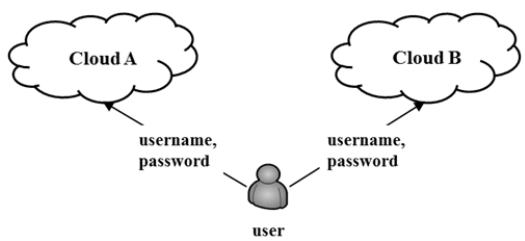

Fig.3. Existing Authentication Scheme

3.3 Single Sign-On (SSO)

SSO는 하나의 인증 정보를 이용하여 여러 서비스를 이용할 수 있는 통합 인증관리 시스템이다. 즉, 사용자는 한 번의 인증 과정을 거친 후 접근 권한이 있는 연관 서비스에 자동으로 인증 처리됨으로써 접근이 가능하다[16]. 이 기술은 사용자로 하여금 인증 정보 관리에 대한 부담을 줄여주고, 재인증 과정을 거칠 필요가 없기 때문에 사용자에게 편의를 제공할 수 있다. 그리고 서비스 제공자 측면에서는 인증 정보 관리를 위한 비용을 줄이고, 인증과 인증 정보의 중앙관리가 가능하게 된다. 현재 SSO를 지원하기 위해 많이 사용되는 프로토콜이나 방법은 SAML(Security Assertion Markup Language), OAuth(Open Authorization) 등이 있다.

SAML은 인증과 권한 정보 교환을 위해 OASIS에서 제정한 XML 기반의 표준이다. 이는 표준 언어로서 상호운용성과 각종 프로토콜과의 호환 서로 다른 서비스 간의 SSO를 구축하기에 적합하다. OAuth는 OpenAPI로 개발된 제 3자가 사용자의 비밀번호 없이도 사용자 데이터에 액세스할 수 있도록 해주는 개방형 표준 인증 프로토콜이다. 사용자가 비밀번호를 어플리케이션과 직접 공유하는 대신 OAuth가 '보조키' 역할을 한다. 이로 인해 어플리케이션은 사용자를 대신하여 사용자 데이터에 접근할 수 있다.

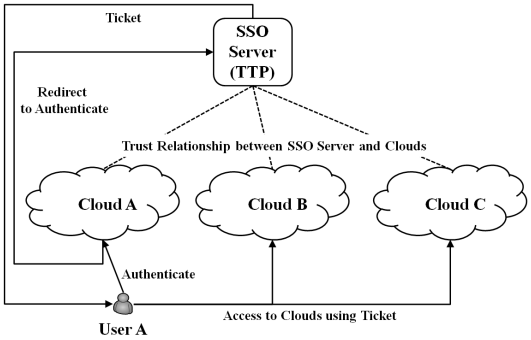

Fig.4. SSO Authentication Scenario in Multicloud

3.3.1 멀티클라우드에 SSO 인증 방식 적용 시나리오

멀티클라우드 환경에서 SSO 인증의 시나리오는 Fig.4.와 같이 사용자 A가 클라우드 A에 인증을 요청하면 클라우드 A는 인증을 위해 SSO Server로 redirection을 시킨다. 그리고 사용자 A는 SSO Server에 의해 인증을 받는다. 유효한 사용자로 판단되면 SSO Server는 사용자 A에게 티켓을 전송하고, 사용자 A는 받은 티켓을 이용하여 클라우드 A, B, C 모두 접근이 허용된다. 하지만 이때 SSO Server는 클라우드 A, B, C의 모든 사용자의 인증 정보를 가지고 있어 쉽게 공격 대상이 될 수 있다. 만약 SSO Server가 공격을 당하면 연결된 모든 클라우드 컴퓨팅 서비스의 사용자 정보가 노출되기 때문에 그 파급효과가 크다. 그리고 SSO Server는 연결된 모든 클라우드 컴퓨팅 서비스에 등록된 사용자의 인증을 수행해야 하기 때문에 병목(bottle neck) 현상 발생의 가능성이 있고, 이에 따라 전체 시스템이 마비될 수 있다.

3.4 클라우드 브로커

클라우드 브로커는 사용자와 서비스 제공자 사이에서 클라우드 컴퓨팅 서비스의 부가가치를 창출하기 위해 사용자를 대신해 일하는 중개자의 의미를 지닌다. 즉, 클라우드 브로커는 사용자와 서비스 제공자 간 관계 조율 및 소비자의 요구에 맞춰 최적의 클라우드 컴퓨팅 서비스를 제안하고 다양한 클라우드 컴퓨팅 서비스의 활용, 성능 관리, 전달 등의 역할을 담당한다.

클라우드 브로커 서비스는 클라우드 컴퓨팅 서비스 제공자 또는 특정 업체가 서비스를 구성하고 운영할 수 있다. 따라서 클라우드 브로커의 기능 구성은 브로커 서비스를 구성하여 운영하는 브로커 서비스 제공자에 의해 이루어진다. 클라우드 브로커는 서비스 제공 측면에서 서비스 중개 브로커(Service Intermediation Broker), 서비스 결합 브로커(Service Aggregation Broker), 서비스 차익 브로커(Service Arbitrage Broker) 세 가지의 유형으로 분류될 수 있다. 각 유형별 설명은 다음과 같다.

3.4.1 서비스 중개 브로커

서비스 중개 브로커는 특정 기능 개선을 통해 서비스의 향상과 소비자에게 부가가치 서비스를 제공한다. 성능 향상의 예로는 ID 및 접근제어 관리, 성능 보고, 안전성 향상 등의 기능을 포함한다.

3.4.2 서비스 결합 브로커

서비스 결합 브로커는 다양한 서비스를 하나 이상의 새로운 서비스로 통합하여 제공한다. 이는 데이터 통합, 사용자와 다수의 서비스 제공자 간 데이터의 이동의 안전성을 보장한다.

3.4.3 서비스 차익 브로커

서비스 결합 브로커와 유사하지만 결합되는 서비스가 고정되어 있지 않다는 차이점을 가지고 있다. 따라서 클라우드 브로커에게 유연성을 제공하여 사용자가 특정 서비스를 원하는 그 상황에서 가장 최적의 서비스를 선택하여 사용자에게 제공할 수 있다.

IV. 제안하는 기법

4.1 제안하는 멀티클라우드 사용자 인증 모델

제안하는 멀티클라우드 사용자 인증 모델은 클라우드 브로커를 기반으로 한다. Fig.5.와 같이 멀티클라우드 환경에서의 클라우드 A, B, C는 클라우드 브로커를 중심으로 서로 상호작용을 한다. 각 서비스를 이용하는 사용자 A, B, C가 자신이 사용하는 서비스 외에 다른 서비스의 기능을 이용하고자 할 때, Fig.6.과 같이 클라우드가 사용자를 대신하여 클라우드 브로커에게 인증을 받는다.

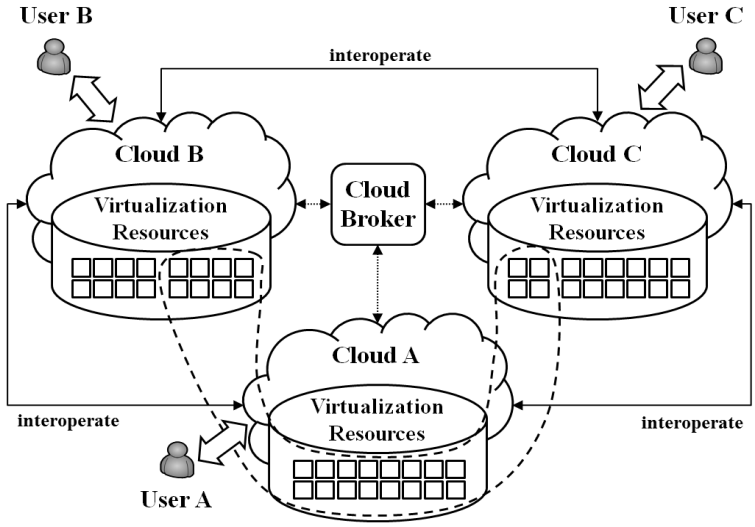

Fig.5. Conceptual Model of Multicloud

4.2 인증 프로토콜 설계 고려사항

제안하는 멀티클라우드 사용자 인증 모델에 적용할 수 있는 인증 프로토콜을 설계하기 위해서 고려해야 할 사항은 다음과 같다.

4.2.1 서비스의 투명성 보장

멀티클라우드 환경에서 사용자는 하나의 서비스에만 등록한 상태에서 다른 클라우드 컴퓨팅 서비스의 기능을 이용하게 된다. 이 때 사용자가 자신이 등록한 클라우드 컴퓨팅 서비스 외에 다른 클라우드 컴퓨팅 서비스에 접근하기 위한 인증 과정을 거치게 된다면 사용자는 여러 개의 서비스를 이용하고 있다는 것을 인식하게 될 수 있다. 따라서 사용자는 자신이 등록한 클라우드 컴퓨팅 서비스의 인증 과정 한 번으로 다른 클라우드 컴퓨팅 서비스의 기능을 제공받을 수 있어야 한다.

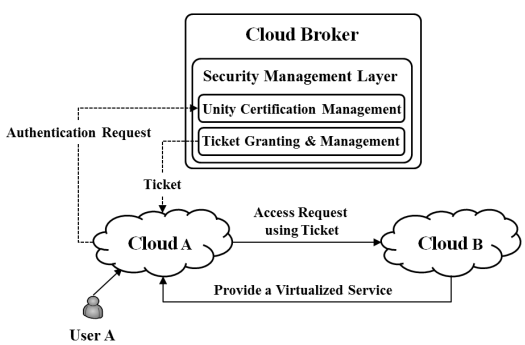

Fig.6. Authentication Model Scenario based on Cloud Broker

4.2.2 위장 공격 방지

제안하는 멀티클라우드 사용자 인증 모델에서는 사용자의 인증 정보를 가진 악의적인 서비스 제공자가 사용자인척하여 다른 클라우드 컴퓨팅 서비스에 접근할 가능성이 있다. 이러한 행위로 인해 사용자에게 부당한 과금이 발생할 수 있다. 클라우드 컴퓨팅에서는 사용한 만큼 비용을 지불하는 방식이기 때문이다.

4.2.3 부인 방지

멀티클라우드 환경에서는 악의적인 사용자가 악성 데이터를 사용하는 경우 그 파급효과가 크다. 여러 개의 클라우드 컴퓨팅 서비스가 상호작용하는 환경이기 때문에 악성데이터의 유포가 빠르고 쉽기 때문이다. 이로 인해 시스템에 문제가 발생한 경우, 사용자가 부인하는 것을 방지할 수 있어야 한다.

4.3 인증 프로토콜 설계

이 절에서는 4.2절에서 정리한 고려사항을 바탕으로 사용자 인증 프로토콜을 설계한다.

4.3.1 표기법

본 논문에서는 Table 1.의 표기법을 따른다.

Table 1. Notation

Notation	Description
UID_i	identifier of user i
CP_A, CP_B	identifiers of service provider A and B
SI_{CP_A}, SI_{CP_B}	information of cloud A and B
PK_{U_i}, PR_{U_i}	public/private key of user i
PK_{CP_A}, PR_{CP_A}	public/private key of cloud A
PK_{CB}, PR_{CB}	public/private key of cloud broker
$Sign_x$	signature of participant x
$Auth$	authorization from cloud broker
$TC_{A \leftrightarrow B}$	contract between cloud A and B
T	timestamp
$Ticket$	ticket

4.3.2 인증 프로토콜

본 논문에서 제안하는 인증 프로토콜에 대한 설명에 앞서 사용자는 이미 각자 자신이 사용하는 클라우드 컴퓨팅 서비스에 등록된 상태라 가정한다. 제안하는 프로토콜은 Fig.7.과 같이 크게 계약 과정과 인증 과정으로 나뉜다. 각 단계별 설명은 다음과 같다.

4.3.2.1 계약 과정

계약 과정에서는 클라우드 컴퓨팅 서비스 A와 B 간의 상호작용을 위해 클라우드 브로커를 통해 계약을 진행한다. 이 과정을 거쳐야 각 서비스의 사용자는 다른 서비스의 기능을 사용할 수 있게 된다. 계약 과정의 각 단계별 설명은 다음과 같다.

- 단계 ①: 서비스 제공자 A는 클라우드 브로커에게 자신에게 부족하거나 없는 컴퓨팅 자원(하드웨어, 소프트웨어 등)을 가진 서비스에 대한 검색을 요청한다.
- 단계 ②: 클라우드 브로커는 서비스 제공자 A로부터 받은 요청에 맞는 서비스를 검색하고, 해당 서비스에 대한 식별자 CP_B와 정보 SI_{CP_B}를 서비스 제공자 A에게 전송한다.
- 단계 ③: 서비스 제공자 A는 클라우드 브로커로

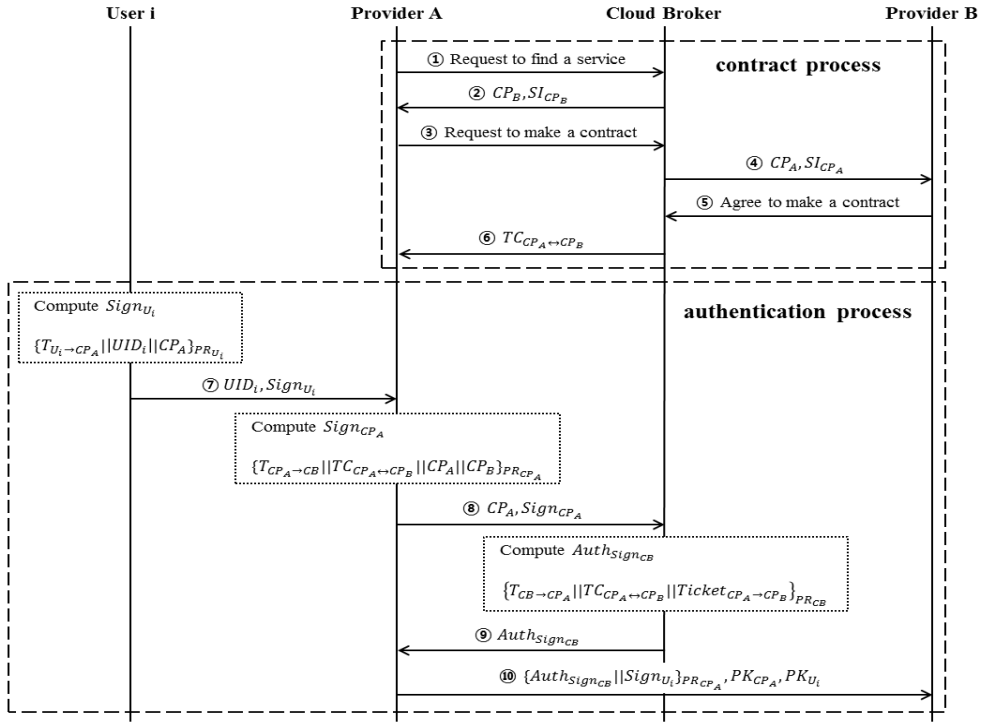

Fig.7. Proposed Authentication Protocol

부터 받은 정보 SI_{CP_B}를 확인하고, 자신이 원하는 서비스가 맞으면 클라우드 브로커에게 서비스 제공자 B와의 계약을 위한 중개를 요청한다.

- 단계 ④: 클라우드 브로커는 서비스 제공자 A로부터 중개 요청을 받으면, 서비스 제공자 B에게 서비스 제공자 A의 식별자 CP_A와 정보 SI_{CB_A}를 전송한다.
- 단계 ⑤: 서비스 제공자 B는 클라우드 브로커로부터 받은 정보 SI_{CB_A}를 확인하고, 계약에 대한 동의여부를 전송한다.
- 단계 ⑥: 클라우드 브로커는 서비스 제공자 B로부터 계약에 대해 동의를 받으면, 서비스 제공자 A와 B 간의 계약을 의미하는 $TC_{CP_A \leftrightarrow CP_B}$를 서비스 제공자 A에게 전송한다.

4.3.2.2 인증 과정

인증 과정에서는 클라우드 컴퓨팅 서비스 A에 등록된 사용자가 정상적인 사용자인지 검증하고, 서비스 제공자 A가 다른 클라우드 컴퓨팅 서비스 B에 접근하여 컴퓨팅 자원을 사용자에게 제공하기 위한 과정이다. 인증 과정의 각 단계별 설명은 다음과 같다.

- 단계 ⑦: 사용자는 클라우드 컴퓨팅 서비스 A에 정상적인 사용자임을 검증받기 위해 타임스탬프, 자신의 식별자, 서비스 제공자 A의 식별자를 자신의 개인키로 서명한 값 $Sign_{U_i}$를 계산하여 자신의 식별자 UID_i와 함께 전송한다. 서비스 제공자 A는 사용자로부터 받은 식별자 UID_i를 데이터베이스 내에서 검색한다. 동일한 값이 있으면 사용자로부터 받은 값을 사용자의 공개키로 복호화하여 타임스탬프와 사용자가 자신에게 보낸 메시지가 맞는지 확인한다. 이 단계가 정상적으로 수행되면 사용자는 클라우드 컴퓨팅 서비스 A에 정상적인 사용자임이 검증된다.
- 단계 ⑧: 사용자가 다른 클라우드 컴퓨팅 서비스인 B가 가진 컴퓨팅 자원을 이용하고자 할 때 진행되는 단계이다. 서비스 제공자 A는 클라우드 컴퓨팅 서비스 B에 접근하기 위해 클라우드 브로커에게 인증 요청을 한다. 자신과 B의 계약 관계를 의미하는 값과 자신의 식별자, 그리고 클라우드 컴퓨팅 서비스 B의 식별자를 자신의 개인키로 서명한 값 $Sign_{CP_A}$를 계산하여 자신의 식별자 CP_A와 함께 클라우드 브로커에게 전송한다.
- 단계 ⑨: 클라우드 브로커는 서비스 제공자 A로부터 받은 값 $Sign_{CP_A}$를 서비스 제공자 A의 공개키로 복호화하여 계약이 유효함을 확인한다. 이 단계가 정상적으로 수행되면 클라우드 브로커는 서비스 B에 접근하기 위한 티켓과 A와 B 간의 계약을 개인키로 서명한 값 $Auth_{Sign_{CB}}$를 계산하여 서비스 제공자 A에게 전송한다.
- 단계 ⑩: 서비스 제공자 A는 서비스 B에 접근하기 위해 클라우드 브로커로부터 받은 티켓과 사용자로부터 받은 인증정보를 자신의 개인키로 암호화하여 생성한 값 $\{Auth_{Sign_{CB}} \| Sign_{U_i}\}_{PR_{CP_A}}$를 계산하고, 자신의 공개키와 사용자의 공개키와 함께 서비스 제공자 B에게 전송한다. 서비스 제공자 B는 서비스 제공자 A로부터 받은 값을 이용하여 서비스 제공자 A의 접근이 유효함을 검증한다.

V. 분 석

이 장에서는 4.2절에서 정리한 프로토콜 설계 고려사항을 바탕으로 4.3절에서 제안한 인증 프로토콜을 분석한다.

5.1 서비스의 투명성 제공

본 논문에서 제안한 프로토콜에서는 사용자에게 서비스의 투명성과 편의를 제공하기 위해서 사용자 대신 서비스 제공자가 인증 과정을 거치도록 설계하였다. 따라서 사용자는 최초 한 번 자신이 등록한 서비스의 인증 과정만 수행하면 된다. 따라서 사용자는 다른 클라우드 컴퓨팅 서비스의 가상화된 컴퓨팅 자원을 이용할 수 있다.

5.2 위장 공격 방지

제안하는 프로토콜에서는 서비스 제공자가 사용자의 인증 정보를 가지고 있지만, 사용자 인증 단계에서 사용자의 개인키를 이용한 서명값이 전달되는 동시에 타임스탬프 T를 사용하여 인증과정을 수행하기 때문에 서비스 제공자의 위장 공격을 예방할 수 있다.

5.3 부인 방지

제안하는 프로토콜에서는 클라우드 컴퓨팅 서비스 A의 사용자를 인증하는 과정에서 사용자의 서명값을 이용한다. 그리고 사용자의 서명값은 상호작용하는 관계에 있는 클라우드 컴퓨팅 서비스에 전달된다. 따라서 만약 사용자로 인해 시스템에 문제가 발생한 경우 사용자만 생성할 수 있는 서명값을 이용하여 사용자에게 그 책임을 물을 수 있다.

VI. 결 론

최근 인터넷을 기반으로 가상화된 서비스를 제공하는 클라우드 컴퓨팅 기술이 주목받고 있다. 하지만 현재 상용화된 클라우드 컴퓨팅 서비스는 하나의 서비스 제공자가 구축하여 제공하는 단일 서비스의 형태로 서비스 가용성 문제, 내부자 공격, vendor lock-in 등의 해결하기 어려운 문제점이 있다. 이를 해결하기 위해 최근에는 멀티클라우드에 대한 연구가 진행되고 있다. 본 논문에서는 다수의 클라우드 컴퓨팅 서비스 간의 상호작용을 위해 클라우드 브로커를 기반으로 한 멀티클라우드 모델을 제시하고, 그 모델에 적용할 수 있는 인증 프로토콜을 제안하였다. 제안하는 인증 프로토콜은 사용자 대신 서비스 제공자가 클라우드 브로커에게 인증받기 때문에 사용자에게 서비스의 투명성을 제공할 수 있다. 그리고 사용자의 서명값을 이용하여 사용자의 인증 정보를 알고 있는 서비스 제공자가 사용자인척 하여 다른 서비스에 접근하는 위장 공격을 방지하고, 사용자로 인해 시스템에 문제가 발생한 경우 사용자가 부인하는 것을 방지할 수 있도록 설계하였다.

References

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing, pp. 109-116, Sept. 2009.

[2] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of network and Computer Applications, Vol. 34, Issue 1, pp. 1-11, Jan. 2011.

[3] J. S. Babu, K. Kishore, and K. E. N. Kumar, "Migration from Single-Cloud to Multi-Cloud Computing," International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 4, pp. 1218-1225, Apr. 2013.

[4] S. Sundararajan, H. Narayanan, V. Pavithran, K. Vorungati, and K. Achuthan, "Preventing Insider Attacks in the Cloud," Advances in Computing and Communications, Springer Berlin Heidelberg, Vol. 190, pp. 488-500, 2011.

[5] B. Satzger, W. Hummer, C. Inzinger, P. Leitner, and S. Dustdar, "Winds of Change: From Vendor Lock-In to the Meta Cloud," IEEE Internet Computing, Vol. 17, Issue 1, pp. 69-73, Jan.-Feb. 2013.

[6] B. Rochwerger, D. Breitgand, A. Epstein, D. Hadas, I. Loy, K. Nagin, J. Tordsson, C. Ragusa, M. Villari, S. Clayman, E. Levy, A. Maraschini, P. Massonet, H. Munoz, and G. Tofetti, "Reservoir - When One Cloud Is Not Enough," IEEE Computer, Vol. 44, Issue 3, pp. 44-51, Mar. 2011.

[7] 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 Sciences (HICSS), pp. 5490-5499, Jan. 2012.

[8] B. Zwateendorfer and A. Tauber, "Secure Cross-Cloud Single Sign-On (SSO) using eIDs," International Conference for Internet Technology and Secured Transactions, pp. 150-155, Dec. 2012.

[9] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and D. Leaf, "NIST Cloud Computing Reference Architecture," NIST Special Publication 500 (2011): 292.

[10] B. P. Rimal, E. M. Choi, and L. Lan, "A Taxonomy and Survey of Cloud

Computing Systems," International Joint Conference on INC, IMS and IDC, pp. 44-51, Aug. 2009.

[11] M. Jensen, J. Schwenk, J. M. Bohli, N. Gruschka, and L. L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," IEEE International Conference on Cloud Computing (CLOUD), pp. 565-572, July. 2011.

[12] M. Kretzschmar and S. Hanigk, "Security Management Interoperability Challenges for Collaboration Clouds," 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management (SVM), pp. 43-49, Oct. 2010.

[13] M. Hojabri and K. V. Rao, "Innovation in Cloud computing: Implementation of Kerberos version5 in Cloud Computing in Order to Enhance the Security Issues," International Conference on Information Communication and Embedded Systems (ICICES), pp. 452-456, Feb. 2013.

[14] S. Lee, I. Ong, H. T. Lim, and H. J. Lee, "Two Factor Authentication for Cloud Computing," Journal of Information and Communication Convergence Engineering, 8(4), pp. 427-432, Aug. 2010.

[15] P. Urien, E. Marie, and C. Kiennert, "An Innovative Solution for Cloud Computing Authentication: Grids of EAP-TLS Smart Cards," International Conference on Digital Telecommunications (ICDT), pp. 22-27, June. 2010.

[16] P. Murukutla, and K. C. Shet, "Single Sign On For Cloud," International Conference on Compupting Sciences (ICCS), pp. 176-179, Sept. 2012.

〈저자소개〉

이 재 경 (Jaekyung Lee) 정회원
2012년 8월: 신라대학교 컴퓨터공학과 학사
2012년 9월~현재: 한양대학교 컴퓨터공학과 석사과정
〈관심분야〉 암호프로토콜, 클라우드 컴퓨팅 보안

손 정 갑 (Junggab Son) 학생회원
2009년 2월: 한양대학교 컴퓨터공학부 학사
2011년 2월: 한양대학교 컴퓨터공학부 석사
2011년 3월~현재: 한양대학교 컴퓨터공학과 박사과정
〈관심분야〉 암호기술 응용, 클라우드 컴퓨팅 보안

김 훈 민 (Hunmin Kim) 학생회원
2013년 2월: 한양대학교 컴퓨터공학부 학사
2013년 3월~현재: 한양대학교 컴퓨터공학과 석사과정
〈관심분야〉 가상화, 클라우드 컴퓨팅 보안

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과 학사
1989년: 아이오와주립대학 전자계산학과 석사
1992년: 아이오와주립대학 전자계산학과 박사
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안