하이브리드 클라우드 컴퓨팅 환경에 적합한 인증시스템 설계★

이 극* · 지재원* · 천현우* · 이규원*

요 약

클라우드 컴퓨팅은 자원을 편리하고 효율적으로 사용하기 위해 만들어진 시스템이다. 본 논문에서는 PKI와 ID_PW 그리고 지리정보 조합을 이용한 2-factor 인증방법을 제안한다. 제안한 방법은 하이브리드 클라우드 환경에 적합하며 자원과 데이터를 보다 안전하게 관리할 수 있다.

Design of An Authentication System Proper for Hybrid Cloud Computing System

Geuk Lee* · Jae-Won Ji* · Hyun-Woo Chun* · Kyu-Won Lee*

ABSTRACT

Cloud computing is a system which efficiently utilizes resources. In this paper, we propose 2-factor authentication system combing PKI, ID_PW and location information. The proposed method improve the security of hybrid cloud systems and manage resources more safely.

Key words : 2-Factor authentication system, cloud computing

접수일(2011년 12월 09일), 수정일(1차: 2011년 12월 21일), 게재확정일(2011년 12월 22일)

★ 이 논문은 2011년 한남대학교 학술연구조성비 지원에 의하여 연구되었음

* 한남대학교 컴퓨터공학과

1. 서 론

클라우드 컴퓨팅은 원거리에 있는 서버에 나의 데이터를 저장시켜놓고 내가 필요할 때 언제 어디서건 자료를 이용할 수 있다[1].

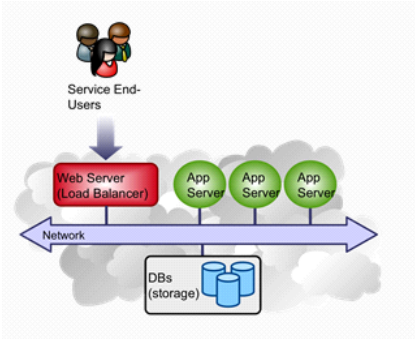
그러나 정보 유출의 염려 때문에 기업들은 자신의 중요 데이터를 자신이 관리하지 않는 원격의 장소에 저장하기를 꺼려하면서도, 장소에 무관하게 정보에 접근할 수 있는 클라우드 환경에 매력을 느끼고 사용하고 싶어하는 딜레마가 있다. 이러한 문제를 해결하기 위한 한 가지 방안이 하이브리드 클라우딩이 될 수 있다[2].

본 논문에서는 하이브리드 클라우드 컴퓨팅 환경에서 효율적 인증방법을 제안한다. 2장에서는 여러 가지 클라우드에 대해 설명하고, 클라우드 환경에서의 사용자인증과 보안에 대해 논의한다. 3장에서는 하이브리드 클라우드 시스템에서의 효율적인 인증 방법을 설계하고 4장에서는 결론을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅의 정의

NIST(National Institute of Standard Technology)는 클라우드 컴퓨팅을 “최소한의 관리 노력과 서비스 제공자의 연동으로 빠르게 제공되고 보급될 수 있는 컴퓨팅 자원(네트워크, 서버, 스토리지, 애플리케이션 그리고 서비스)의 저장고에 가용, 편리, 온 디멘드 네트워크 접근이 가능한 모델”로 정의하고 있다[3].



(그림 1) 클라우드 구동 동작

아마존이나 구글, MS가 실제 클라우드 환경을 제공하고 있지만 클라우드 컴퓨팅은 다양한 방향으로 발전하고 있으며 최종적으로 어떻게 안착할지는 아직 알 수가 없다.

2.2 구성 모델에 따른 클라우드 분류

구성 모델에 따라 클라우드 컴퓨팅을 크게 다음의 4가지로 분류 할 수 있다[2].

2.2.1 공공 클라우드

공공 클라우드는 아마존이나 구글 등에서 사용하는 방식으로, 사용자들에게 대규모의 IT자원을 빌려주고 일정금액의 과금을 받는 방식이다.

2.2.2 개인 클라우드

CC(Cloud Computing)원리에 따라 서비스가 제공되지만, 개인 네트워크 내에서만 접근 가능한 클라우드 환경이다. 이것은 상당한 관리 비용과 구축비용이 필요하다. 개인 클라우드 환경은 자원을 효율적으로 사용할 수 있고, 보안에 강하기 때문에 큰 규모의 기업에서는 선호한다.

2.2.3 커뮤니티 클라우드

커뮤니티 클라우드는 몇몇 기관이 유사한 요구사항을 갖고 인프라를 공유하여 CC의 장점을 이용하고자 할 때 사용한다. 이것은 많은 비용이 들지만 고수준의 프라이버시, 보안성을 제공한다. 예로서는 구글의 gov 클라우드이다.

2.2.4 하이브리드 클라우드

하이브리드 클라우드는 개인 클라우드 처럼 개인 네트워크 내에서 작동하지만 더 강한 컴퓨팅 파워나 저장 공간이 필요할 때는 벤더들의 서비스를 빌려서 사용할 수 있는 형태이다.

2.3 클라우드에 필요한 기술

2.3.1 가상화

(그림 2) VMware 가상화 구조.

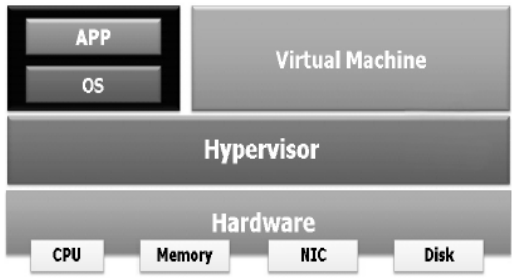
가상화 기술은 서버, 운영체제, 어플리케이션, 스토리지 및 네트워크 등 IT 인프라 거의 모든 측면에서 복잡했던 환경을 단순화 시킨다. 이 가상화 기술을 이용하면 작업처리의 분산, 관리 수단의 통합을 통하여 비용절감과 관리 능률 향상 등의 긍정적인 효과를 얻을 수 있다[4].

가상화 기술을 이용하는 방식은 크게 세 가지로 나누어 볼 수 있다. 시스템 자원의 추상화, 분배 그리고 병합으로 구분한다. 먼저, 자원의 추상화는 자원을 이용하는 주체에게 복잡한 물리적인 속성을 숨기고, 주체가 필요로 하는 형태로 논리적인 자원을 제공하는 것으로, 자바 가상머신을 대표적인 예로 들 수 있다. 그리고 서버 가상화와 같이 하나의 시스템 자원을 다수의 접근 주체들에게 독립적인 자원으로 인식시켜 이용할 수 있도록 하는 자원의 분배 방식이 있다. 또한 분리되어 있는 자원들을 하나의 자원으로 인식 할 수 있도록 하여 방대한 자원을 효율적으로 이용할 수 있도록 가상환경을 만들어 주는 것이 병합이다[5].

대표적인 가상화 기술 활용 사례는 SANDBOX이다. 이것은 제한적 환경을 만들어 놓고, 악성코드를 수행해 보면서 시스템에 영향을 주지 않으면서 악성코드를 정밀하게 분석하는 것이 가능하고, 서버 운영 시에도 중요 업데이트 등을 현실과 똑같이 구성한 가상머신 상에서 미리 수행해 본 후 실제 서버에 적용하는 방법 등으로 활용된다.

2.3.2 Hypervisor

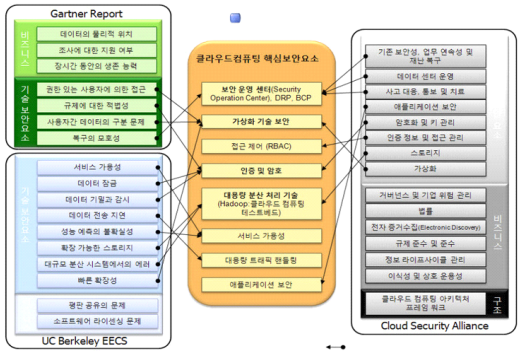
Hypervisor는 가상화를 가능하게 하는 핵심기술이다. 호스트 컴퓨터에서 다수의 운영체제가 동시에 실행되게 하기 위한 가상 플랫폼을 의미한다. 이것은 로드 밸런싱(load balancing)의 기능도 함께 한다[6].



(그림 3) Hypervisor

2.4 클라우드 환경의 보안

미국의 Pew Internet R American Life Project 에서 08년 4월에 조사한 바에 의하면, 사람들은 기업들이 사전에 알리지 않고 고객의 데이터를 사용할지도 모른다며 심각하게 걱정 하고 있었으며, 고객의 데이터가 매매되거나 마케팅 목적으로 이용될 가능성에 대해서도 우려를 하고 있는 실정이다. 보안에 관련된 다른 문제로는 서버에 문제가 생겼을 때 벤더에서 직접 나서서 시스템을 점검할 때까지 고객들이 할 수 있는 일이 거의 없다는 것이다[7]. 또한 대규모의 데이터들이 한곳에 밀집해 있기 때문에, 해커들의 집중 공격 대상이 되기에도 너무나 쉬우며, 대규모 DDos 공격이 상당한 부담이 될 것이라 생각된다[8].



(그림 4) 클라우드 컴퓨팅 핵심 보안 요소기술

2.5 클라우드에서 인증

2.5.1 클라우드 환경의 사용자 인증과 종류

클라우드 컴퓨팅 사용자는 새로운 클라우드 서비스를 사용할 때마다 매번 서비스 제공자가 요구하는 개인 인증 과정을 완료해야 한다. 일반적으로 개인 인증 과정은 고유하고 민감한 개인정보를 서비스 제공자에게 제공하여 등록하는 과정을 거치고, 등록이 완료되면 서비스 제공자는 개인 인증을 위한 고유한 식별자를 제공한다. 이후 사용자는 클라우드 컴퓨팅서비스를 이용하고자 접근 할 때 마다 서비스 제공자로부터 제공받은 식별자를 사용하여 개인 인증을 수행하게 된다[9].

식별자가 임의의 공격에 의해 고유성과 안전성이 침해되었을 경우에는, 데이터베이스에 저장되어 있는 개인 정보와 기업의 정보들이 공격자에게 노출되는 것은 물론이고, 개인이 해당업무처리 서비스를 제공받는 사실, 개인 정보 및 업무처리에 연관된 개인 과 단체 정보까지 노출되어 심각한 피해가 뒤따르게 된다.

그에 비하여 하이브리드 클라우드 환경에서는 중요 데이터는 개인 클라우드에 보관한다. 하이브리드 클라우드 환경은 사설 네트워크 안에 데이터를 저장하기 때문에 공개되어있는 다른 클라우드 환경보다는 높은 보안수준을 보장 할 수 있다. 그러나 개인 클라우드에서 공공 클라우드에 접근하여 서비스를 제공 받을 때 많은 취약점이 발생 할 수 있다. 그러므로 하이브리드 클라우드를 구성할 때는 개인 정보는 물론 개인 클라우드와 공공 클라우드 사이에서도 상당히 높은 수준의 인증 방법을 제공하여 정보가 노출되지 않도록 해야 한다.

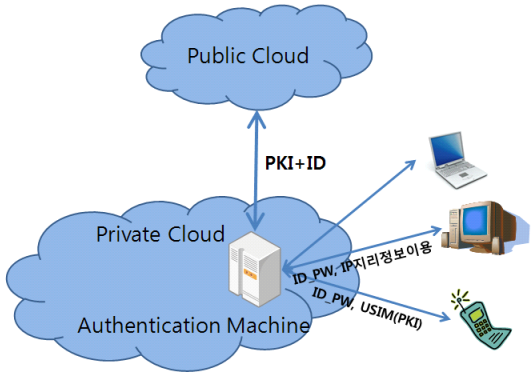
일반적이며 대표적인 인증 보안 기술은 다음과 같이 ID/PW를 이용한 방법, SSO(Single Sign On), MTM(Mobile Trusted Module), 공개키 인증서(PKI)를 이용한 방법 그리고 Multi-factor인증이 있다. 이 중 Multi-factor인증 방법은 표준이 없어 보안요구 정도에 따라 인증방법을 택하기가 쉽지 않다.

클라우드 컴퓨팅 환경에서 인증을 사용 할 때 전통적인 방법들은 여러 가지 문제점이 존재하기 때문에, 조금 더 높은 수준의 인증방법들이 요구된다. 그것들의 종류로는 클라이언트 SW를 사용하는 PKI-인증, 개인키 및 인증서 관리를 수행하는 클라이언트 사이드 응용프로그램, IP를 이용한 지리위치 정보 식별, 핑거프린트와 식별자, 지식기반 인증, Out-of Band, HW단말기를 사용하지 않는 OTP번호를 조합하는 순환형 OTP카드, OTP HW 토큰 등이 있다. 여러 가지 개인 인증 방법의 접근 용이성과 상호 운용성에 대한 분석과 2-factor 인증의 예상 성능에 대한 부분은 참고문헌 9번의 선행연구를 참조하기 바란다[9].

3. 하이브리드 클라우드 환경에 적합한 인증방법 설계

3.1 2-Factor 인증 시스템 설계

하이브리드 클라우드 환경은, 개인 클라우드와 공공 클라우드를 함께 사용하기 때문에 인증방법과 데이터 공유 할 때, 다른 클라우드 보다 많은 취약점이 존재 한다. 그래서 두 가지의 인증 방법을 이용하여 인증 모델을 설계 하였다.



(그림 5) 2-Factor 인증 시스템 설계 모델

우선 개인 클라우드에 인증머신(Authentication Machine)을 구축한다. 개인 클라우드가 공공 클라우드에 접근 할 때는 클라이언트 SW를 사용하여 PKI인증방법과 사용자 ID를 이용하여 인증을 한다. PKI 는 개인키만 유출 되지 않는다면 상당히 높은 수준의 보안성을 보장한다. 하지만 PKI 시스템은 키의 관리에

어려움이 있고, 클라이언트 소프트웨어는 고객이 사용하는 방대한 운영시스템 자원을 소모 하는 것, 패치 업데이트해야하는 번거로움과 키 관리비용이 높아 질 수 있다는 단점이 있다.

이러한 문제점을 인증 머신이 대신 담당하게 함으로써 키 관리에 어려움과 관리비용을 줄인다. 인증머신이 시스템 자원을 일부 소모하지만 거대한 전체 클라우드의 컴퓨팅 파워 측면에서 보면 작은 일부분이다.

개인이 노트북이나 PC로 개인 클라우드에 접속 하였을 때는 ID_PW, IP지리 정보를 이용한 2-Factor 방법으로 인증하여 보안성능을 향상 시킨다. 또한 스마트폰으로 접근 했을 때는 ID_PW와 USIM(PKI)를 이용하여 인증을 한다. 일반 사용자들에게는 최대한 사용하기 쉽고 접근성이 뛰어난 방법을 이용하여 인증을 한다. 개인 클라우드에서는 상대적으로 보안성능은 낮지만 ID_PW를 잘 관리한다면 충분한 성능을 보장 할 수 있다.

맨-인더-미들-어택(Man-in-the-middle attack, MITM Attack)과 같은 공격은 중간에 공격자가 중계소 행세를 하며 송신자와 수신자를 교란하는 방법이다. 송신자와 공격자 사이에 다른 키를 서로 공유하고, 공격자와 수신자 사이에 다른 키를 공유하며 중간에서 오가는 신호를 도청하는 방법이다. 제안한 2-Factor 방법에 사용되는 각각의 인증 방법은 이미 널리 인정을 받는 매커니즘들이며, 클라우드 컴퓨팅환경에서 상당히 유협적인 문제 중 하나인 MITM(Man In The Middle) 공격에 대해 서로 다른 2가지 인증 방법으로 서로 보완한다. 따라서 개인키와 ID_PW가 같이 유출되지 않는 한 보안을 유지할 수 있으며, 사용자 개인은 추가적인 큰 불편함 없이 두 가지 클라우드 환경을 사용할 수 있어 보안 수준과 효율성, 안정성 측면에서 보다 효과적인 방법으로 볼 수 있다.

4. 결 론

중요데이터는 개인 클라우드에 저장하고, 더 많은 자원이 필요할 때는 공공 클라우드에 접속하여 서비스를 받는 것이 하이브리드 클라우드 컴퓨팅이다. 이때 인증 방법에 문제가 있다면 보안에 상당히 큰 문제가 생긴다. 이것을 해결하기 위해서는 전통적인 방법과 좀 더 발전된 클라우드 인증 방법을 함께 이용하여 Multi-factor 인증방법을 취해야 한다. 본 논문에서는 PKI 와 ID를 이용하여, 개인 클라우드와 공공 클라우드 사이에 인증을 제공하고, 개인사용자와 개인 클라우드 사이에서는 사용하기 편한 ID_PW+IP지리정보 이용을 이용하는 2-Factor 인증 방법을 제안 하였다. 향후 연구로는 MITM 공격보다 더 위협이 될 수 있는 악성 내부자에 대한 인증과 대처법등에 대한 연구가 필요하다.

참고 문헌

[1] http://opennebula.org
[2] http://ko.wikipedia.org
[3] P. Mell and T. Grace, The NIST Definition of Cloud Computing(Draft), 2011.
[4] http://www.vmware.com/kr
[5] 김인혁 외 4명, “시스템 보안을 위한 가상화 기술 활용 동향”, 정보보호학회 논문지 제 19권 2호, pp.26-34, 2009.
[6] 김지연외 3명, "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구", 정보보호학회 논문지, 제 19권 4호, pp.72-77, 2009.
[7] 민옥기외 3명, "훤히 보이는 클라우드 컴퓨팅", 전자 신문, 2009.
[8] 박춘식 외, 클라우드 컴퓨팅 보안 동향, NIPA(정보통신산업진흥원) 주간기술 동향 1432호 2010.
[9] 김현승, 박춘식, "클라우드 컴퓨팅과 개인 인증 서비스", 정보과학회지, 20권 2호, pp11-19, 2010.

[저 자 소 개]

이 극 (Geuk Lee)

1983년 3월 경북대학교 전자과
컴퓨터전공(공학사)
1986년 3월 서울대학교
컴퓨터공학과(공학석사)
1993년 8월 서울대학교
컴퓨터공학과 (공학박사)
1988년~ 현재 한남대학교
컴퓨터공학과 교수
2003년~ 현재 지식경제부지정
민군겸용 보안공학
연구센터 소장

e-mail : leegeuk@hnu.kr

지 재 원 (Jae-Won Ji)

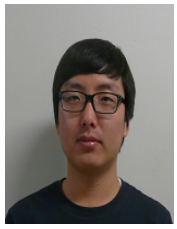
2009년도 한남대학교
컴퓨터공학과 전공
(공학사)
2011년 현재 한남대학교 대학원
컴퓨터공학전공 석사
4학기 과정.

e-mail : pepero500@hnu.kr

천 현 우 (Hyun-Woo Chun)

2009년도 한남대학교
컴퓨터공학과 전공(공학사)
2011년 현재 한남대학교 대학원
컴퓨터공학전공 석사
4학기 과정.

e-mail : chjhahaha@hnu.kr



이 규 원 (Kyu-Won Lee)

2009년도 한남대학교
컴퓨터공학과 전공(공학사)
2011년 현재 한남대학교 대학원
컴퓨터공학전공 석사
4학기 과정.

e-mail : importantman@hnu.kr