情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

클라우드 컴퓨팅 보안 기술

임 철 수*

요 약

최근 IT 분야에서 클라우드 컴퓨팅에 대한 관심과 연구가 진행되고 있다. IT 기술의 기술적/산업적 성장은 유비쿼터스 컴퓨팅의 실현을 목표로 확장가능하고 자원의 연동을 위한 클라우드 컴퓨팅의 관심을 높이고 있다. 그러나 클라우드 컴퓨팅의 실현을 위해서는 보안적인 문제점 해결이 선결 과제이다. 클라우드 컴퓨팅을 통해 데이터가 연동되고 자원을 다양하게 활용하는 것에는 데이터 보호와 자원의 관리 정책, 기업 비밀 관리나 개인의 프라이버시 측면에서의 문제점도 존재한다. 따라서 본 고에서는 클라우드 컴퓨팅의 분류 체계와 보안적인 문제점을 분석하여 클라우드 컴퓨팅 이용자를 위한 보안 가이드라인을 제시한다. 가이드라인을 기반으로 클라우드 컴퓨팅의 산업적 확장성을 강화하고 활용성을 높임으로써 서비스의 확대 및 자원의 효율적인 활용을 강화하고자 한다.

Ⅰ. 서 론

최근 IT 분야의 새로운 기술적/산업적 트랜드를 형성해가고 있는 클라우드 컴퓨팅은 여러 가지 개념으로 정의되고 있으나, "대용량의 확장 가능(scalable)하고 가상화된(virtualized) 자원들이 인터넷 상에서 서비스의 형태로 제공되는 컴퓨팅의 한 형태"라는 가트너(Gartner)의 정의가 널리 받아들여지고 있다[1,2]. 아마존(Amazon)의 AWS (Amazon Web Service), EC2 (Elastic Compute Cloud), S3 (Simple Storage Service)나 구글(Google)의 Apps등은 이미 잘 알려진 클라우드 컴퓨팅의 예이며, 최근에 Microsoft, IBM, HP, SUN 등 IT 관련 글로벌 기업들이 참여하면서 Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) 등 다양한 형태의 클라우드 컴퓨팅 서비스 및 제품들이 선보이고 있다.

그러나 기존의 컴퓨팅 환경이 클라우드 환경으로 전환되면서 해결되어야 할 많은 이슈들이 있는데, 그 중 대표적인 것이 보안(security) 문제이다. 클라우드 컴퓨팅 서비스는 데이터를 보호하기 위해 별도의 자원을 할당하고 관리하므로 개별 기업이나 개인이 직접 데이터를 관리하는 것보다 안전성이 높아지는 것이 일반적이나, 반면에 민감한 데이터에 대한 직접 제어권(control)을 포기해야 하며 사고시 피해의 파급효과가 크기 때문에 기업 비밀 관리나 개인의 프라이버시 측면에서 많은 문제점 또한 존재한다.

아울러 클라우드컴퓨팅 서비스 산업의 활성화를 위해서는 보안문제 해결이 선결해야할 주요 이슈가 되는 것은 이론적이고 기술적인 문제뿐만 아니라, 2008년 2월의 아마존 AWS S3 서비스의 중단(outage) 사고, 2008년 Carbonite 사의 백업저장소 손상으로 인한 데이터의 영구적 손실 및 2008년 9월의 Google Docs의 데이터 유출 문제 등과 같은 유사 사례들이 재발하지 않도록 하는 방안 마련이 시급하다.

Ⅱ. 클라우드 컴퓨팅 기술 분류

지식경제부 차세대컴퓨팅 분야에서는 클라우드컴퓨팅 기술 및 제품에 대한 로드맵을 작성하였는데, 이중 클라우드 보안기술은 프라이버시 및 데이터 보안 기술, 신뢰성(Trustworthy) 컴퓨팅 기술, 클라우드 SSO 기술 및 클라우드 네트워크 보안 기술을 포괄하는 중분류 기술로서 포지셔닝 되어 있다.

* 지식경제부 차세대컴퓨팅 Program Director, 서경대학교 컴퓨터공학과 (ucom@keit.re.kr, cslim@skuniv.ac.kr)

〔표 1〕 클라우드 컴퓨팅 기술 분류

클라우드 서비스 및 응용 기술	SaaS 플랫폼 기술
	클라우드 응용 컴포넌트 기술
	클라우드서비스 개발 기술
	클라우드 클라이언트 기술
클라우드 플랫폼 기술	서비스 배치 및 관리 기술
	클라우드 분산 시스템 기술
	클라우드 보안 기술
클라우드 인프라 기술	인프라 자원 관리 기술
	인프라 자원 가상화 기술
	클라우드 네트워크 기술
	클라우드 데이터센터 기술

Ⅲ. 클라우드 컴퓨팅 보안을 위한 요소기술

클라우드 컴퓨팅에서 위와 같은 사고들 및 잠재적인 위협을 방지하기 위해서는 다음과 같은 기술적 요구사항들이 만족되어야 한다. 이들은 기본적으로는 전통적인 IT 환경에서 요구되었던 사항들이나 클라우드 컴퓨팅의 특징인 가상화나 분산화 등 새로운 상황에 맞게 재구성되어야 할 것으로 예상된다.

□ 기밀성과 데이터 암호화

개인 및 기업 데이터에 대한 기밀성(privacy) 보호를 위해서는 기본적으로 암호화(encryption) 기술이 제공되어야 한다. 특히 클라우드 컴퓨팅에서는 대용량 데이터의 암호화시 전체 시스템의 가용성이 떨어질 수 있다는 점을 고려하여 이러한 상황에 적합한 암호가 이용되어야 하는데, 예를 들어 DES나 AES와 같은 블록 암호 대용으로 스트림 암호를 사용하는 방안 등을 고려해볼 수 있다. 또한 키 저장 서버의 사고시 다수 사용자의 데이터가 접근 불가능해지므로 키 관리 방안에 대한 연구 또한 필요하다.

□ 사용자 인증과 접근 제어

다수 사용자의 데이터가 혼재되어 있는 클라우드 환경에서는 사용자에 대한 인증과 권한 관리 기술이 더욱 필요하며, 다수의 사이트와 다수의 서비스를 통합 인증하는 Single-Sign On (SSO) 형태의 인증 기술이 많이 연구되고 있다. 개방형 인증 기술인 OpenID는 이의 한 예라고 할 수 있으며, OASIS의 Security Assertion Markup Language (SAML)은 XML 기반으로 사용 권한을 제어하기 위한 프레임워크이다. 전통적으로 사용자 확인을 위해서 이용되어 왔던 전자서명 기술도 많이 활용될 수 있으나, AWS의 전자서명에서 취약점이 발견된 사례에서 보듯이 특히 웹 기반의 인터페이스를 기반으로 하는 클라우드 환경에서는 인증 프로토콜에 대한 다양한 케이스별 검증이 매우 중요하다.

□ 데이터의 무결성

2008년 7월의 AWS S3 서비스 다운 사례는 서버간에 교환되는 메시지에 대한 무결성 검사 루틴이 없었던 데서 기인하였다. 이 사례에서 확인할 수 있듯이 클라우드 컴퓨팅에서는 저장되는 데이터와 교환되는 메시지에 대한 오류 검사가 매우 중요하며, 최근에 무결성 확인을 위해 많이 사용되는 MD5와 SHA의 취약점이 발견되면서 미국 NIST에서 새로운 해쉬 알고리즘인 SHA-3의 공모 및 개발이 진행되고 있다[8].

□ 가용성 및 복구

서비스의 중단이나 데이터의 손실을 막기 위해서는 사고시 서비스를 지속할 수 있는 고장 감내성(fault tolerance) 및 데이터 복구(recovery) 기법에 대한 연구가 매우 중요하다. 클라우드 서비스 중단 및 데이터의 연구적 손실이 발생한 사례들은 이러한 메커니즘들이 제대로 동작하지 않을 때 생길 수 있는 문제들을 보여준 예라 할 수 있겠다.

□ 원격 확인 (remote attestation) 및 가상 머신 보호

클라우드 컴퓨팅에서는 코드가 원격으로 실행되는 경우가 많으므로, 원격 확인, 특히 소프트웨어에 대한 이진 분석(binary analysis of software)이 매우 중요한 이슈가 된다. 또한 가상 머신(VM) 상에서 프로그램의 실행 영역 및 메모리 보호(memory protection)를 위해 sandboxing 등 관련 기술이 활발히 연구되고 있다.

□ 네크워크 보안 및 웹 보안

클라우드 컴퓨팅은 기본적으로 네트워크를 기반으로 하고 있기 때문에 IDS (Intrusion Detection System), IPS (intrusion prevention system), 방화벽 (firewall), IPsec 및 가상사설망(Virtual Private Network: VPN) 등 기존의 네트워크 보안 기술을 어떻게 효율적으로 적

용할 것인가 하는 문제를 고려해야 한다. 특히 클라우드 컴퓨팅은 주로 웹 기반 인터페이스를 이용하므로 SSL/TLS (Secure Socket Layer/Transport Layer Security) 기반의 https에 대한 활용 방안 연구도 중요하다.

□ 공격 모델 및 시뮬레이션

클라우드 컴퓨팅에서 사용자의 요청에 의해 자원을 할당하는 서비스 방식은 서비스 거부 공격(Denial of Service: DoS)의 전형적인 대상이 될 수 있으며, 클라우드 환경을 가정한 공격 모델의 정립과 공격 시뮬레이션 기술은 위의 네트워크 보안 기술과 더불어 안전한 클라우드 환경을 제공하는 데 있어 필수적인 기술이다.

□ 보안 정책 관리 및 비용 분석

암호화 등 보안 기능이 적용될 경우 상당량의 컴퓨팅 자원 및 에너지를 소모하게 되므로 이에 대한 비용과 보안 사고시 예상되는 피해 규모 등을 종합적으로 평가하여 자원 및 인력을 적절히 배분하는 것이 중요하다. 클라우드는 대규모로 운영되는 경우가 많기 때문에 종합적 평가가 쉽지 않으며, 따라서 클라우드의 특성을 고려한 새로운 비용 평가 모델과 보안 정책 수립 방안의 연구가 필요하다.

Ⅳ. 클라우드 컴퓨팅 이용자를 위한 보안 가이드라인

Gartner는 클라우드 컴퓨팅의 보안 위협을 평가하기 위한 일반적인 가이드라인을 제시하였다[8]. 이 가이드라인은 보안에 관한 기술적 지식이 없는 클라우드 컴퓨팅 이용자들이 클라우드의 안전성을 판단하는 데 이용할 수 있도록 7가지 항목으로 구성되어 있는데, 본 절의 내용은 이를 재구성한 것이다.

□ 접근 권한에 관한 정보 (privileged user access)

기업 외부에서 처리되는 민감한 데이터들은 해당 데이터를 기업 내부에서 처리할 때 일반적으로 수행하는 물리적, 논리적, 인적 통제를 거치지 않은 상태이므로 항상 잠재적인 위험성을 가지고 있다. 따라서 클라우드 컴퓨팅을 이용하는 기업은 클라우드 내에서 실제 데이터를 다루는 인력 및 이들에 대한 관리 정보를 서비스 제공자에게 요청하여 얻을 수 있어야 한다.

□ 규정의 준수 (regulatory compliance)

클라우드 서비스 제공자가 데이터를 관리하고 있지만 궁극적으로 해당 데이터의 안전성 및 무결성에 대한 책임은 클라우드 이용자에게 있다. 따라서 전통적인 IT 서비스에서와 같이 클라우드 서비스 제공자에 대한 외부 감사나 보안 기능에 대한 인증이 보장되어야 한다.

□ 데이터의 위치 (data location)

클라우드 사용자는 일반적으로 데이터의 정확한 위치를 알지 못하며, 심지어는 어느 나라에 저장되어 있는지도 알 수 없다. 따라서 서비스 제공자로 하여금 데이터가 저장되고 처리되는 지역이 어디라는 점과 그 해당 지역에서 의무화하고 있는 프라이버시 규정을 준수한다는 점을 확인받을 수 있어야 한다.

□ 데이터의 분리 (data segregation)

클라우드 컴퓨팅 환경에서는 일반적으로 여러 사용자의 데이터들이 공용 환경에서 처리된다. Google Docs의 데이터 유출과 같은 사건이 방지되기 위해서는 기본적으로 암호화(encryption)가 이용되어야 하며, 이러한 암호 기술은 전문가들에 의해 설계되고 충분히 검증되어야 한다.

□ 복구 (recovery)

데이터를 여러 사이트에 복수로 저장하고 처리하는 것은 문제 상황 발생시 대처를 위한 가장 기본적인 전제조건이다. 서비스 제공자는 문제 상황시 데이터가 완전히 복구 가능한지, 또한 복구에 시간이 얼마가 소요될 것인지를 보장할 수 있어야 한다.

□ 불법행위 조사 (investigative support)

클라우드 컴퓨팅 환경에서는 다수 사용자의 데이터와 로그 정보가 공존하고 이들이 위치하는 호스트나 데이터 센터들이 지속적으로 변하기 때문에 불법 행위에 대한 조사나 책임 소재 규명이 어려운 경우가 많다. 따라서 클라우드 서비스 제공자는 이러한 조사 기능을 보장할 수 있어야 한다.

□ 장기 생존 가능성 (long-term viability)

클라우드 서비스 제공자가 폐업하거나 인수, 합병되는 경우에는 기존 사용자 데이터의 가용성이 보장되어

야 하며, 특히 이러한 데이터는 다른 업체가 제공하는 서비스로 쉽게 포팅 가능한 형태로 유지되어야 한다. 'The Linkup (TLU)'의 실패 사례는 온라인 스토리지 업체인 Streamload가 일반 소비자 대상의 MediaMax와 기업 사용자 대상의 Nirvanix로 분리되면서 데이터가 적절히 관리되지 않아 일부 사용자 데이터가 손실된 예이다.

V. 결 론

본 고에서는 클라우드 컴퓨팅의 보안 사고 사례와 이러한 사고를 방지하기 위한 기술적 요소들 및 클라우드 이용자들에게 권장되는 보안 가이드라인을 살펴보았다. 그러나 클라우드 컴퓨팅은 아직 시작 단계에 있으므로 새로운 서비스 모델의 개발에 따라 새로운 위협 유형이 계속 출현할 것으로 예상되며, 따라서 이에 대한 대책이 지속적으로 연구되고 보완되어야 IT 산업을 재편하고 새로운 시장 기회를 창출할 수 있는 신성장동력 산업으로 포지셔닝 가능하다고 할 수 있겠다.

참고문헌

[1] Gartner says cloud computing will be as influential as e-business, 2008. 6. http://www.gartner.com/it/page.jsp?id=707508.

[2] Cloud computing, wikipedia, http://en.wikipedia.org/wiki/Cloud_computing.

[3] The ACM Cloud Computing Security Workshop, 2009. 11 (예정), http://crypto.cs.stonybrook.edu/ccsw09/.

[4] The eSTREAM project, http://www.ecrypt.eu.org/stream/.

[5] OpenID, http://openid.net/.

[6] OASIS Security Services (SAML) TC, http: //www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[7] NIST, Cryptographic hash algorithm competition, http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

[8] Gartner, Assessing the Security Risks of Cloud Computing, 2008. 6, http://www.gartner.com/DisplayDocument?id=685308.

〈著者紹介〉

임 철 수 (Lim, CheolSu)

1985년: 서울대학교 계산통계학과 학사
1988년: 미국 인디애나주립대 컴퓨터과학과 석사
1995년: 서강대 컴퓨터공학과 박사
1997년~현재: 서경대 컴퓨터공학과 교수
2009년~현재: 지식경제부 차세대컴퓨팅 Program Director
<관심분야> 유비쿼터스 컴퓨팅, 클라우드 컴퓨팅, 네트워크 보안, 정보보호