클라우드 컴퓨팅 보안에관한 연구 및 고찰

박지수*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
e-mail:{jisoo08,jhpark1}@seoultech.ac.kr

A Study on Cloud Computing Security

Ji Soo Park*, Jong Hyuk Park*
*Dept of Computer Science & Engineering, Seoul National University of Science and Technology

요 약

클라우드 컴퓨팅은 사용자가 편리하게 자원들을 활용하고 필요한 만큼 사용하고 비용을 지불하게 하기위해 등장하였다. 하지만 클라우드 컴퓨팅은 완전히 새로운 것이 아닌 기존의 웹서비스를 이용하기 때문에 이미 존재하는 보안적인 문제점과 클라우드 컴퓨팅에서의 새로운 보안 문제점 등 여러 보안적인 문제점이 존재한다. 본 논문에서는 클라우드 컴퓨팅에서 고려할 수 있는 보안 위협과 보안 이슈에 대해 논의한다.

1. 서론

클라우드 컴퓨팅의 개념이 확산되면서 국내의 여러 포탈에서도 클라우드라는 이름의 서비스들이 증가하고 있다.

클라우드 컴퓨팅이란 사용자가 고정적인 IT 자원을 보유하고 사용하는 것이 아닌 필요시에 적절한 IT 자원을 사용하고 사용한 만큼 지불할 수 있게 하는 것으로 IT자원을 가상화하여 웹상에서 서비스 하는 것이다 [1]. 그렇기 때문에 클라우드 컴퓨팅을 이용하면 개인 사용자는 불필요한 자원을 위해 자원을 미리 구매할 필요가 없어지고 기업 사용자는 사무실 이전이나 인력 상황이 변하여도 전산시스템을 재구성해야하는 비용과 시간을 절감할 수 있다.

하지만 클라우드 컴퓨팅은 IT자원을 웹상에서 가상화하여 제공하기 때문에 여러 보안 위협들이 존재한다. 대표적인 보안 문제로는 웹상의 가상화된 스토리지를 사용하기 때문에 발생하는 개인 및 기업 정보 유출이 있다 [2].

본 논문에서는 클라우드 컴퓨팅에 대한 최근 이슈 사항 및 클라우드 컴퓨팅에서의 보안 위협과 이에 대응하기 위한 해별방안 등에 대해 살펴본다.

본 논문은 2장 클라우드 컴퓨팅의 개념 및 최근 이슈 사항, 3장 클라우드 컴퓨팅에서의 위협 및 해결 방안, 4장 결론 및 고찰로 구성된다.

2. 클라우드 컴퓨팅

본장에서는 클라우드 컴퓨팅의 대표적인 서비스와 클라우드 컴퓨팅의 종류에 대해 논의한다.

2.1 클라우드 컴퓨팅 서비스

클라우드 컴퓨팅의 대표적인 서비스로 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service) 세가지가 있다.

SaaS는 인터넷상에서 응용 소프트웨어를 서비스로 제공하는 것이다. SaaS는 단순 문서 작업 같은 OA 기능과 기업의 회계, 영업 관리 등의 기업 단일 기능, ERP, CRM 기업내 통합 기능 그리고 기업 간에 거래를 위한 기업 간 통합 기능을 제공한다. 구글의 Apps for Your Domain, 마이크로소프트의 Office Live, IBM의 Bluehouse가 대표적인 서비스라고 할 수 있다 [1,2].

PaaS는 소프트웨어 개발 환경을 서비스로 제공하는 것이다. 제공되는 자원으로는 프로그래밍 언어, 개발 툴, 파일 시스템, 데이터 베이스 등이 있다. 아마존의 S3, 구글의 App Engine, 세일즈포스닷컴 등에서 서비스를 제공하고 있다 [1,2].

IaaS는 컴퓨터를 구성하는 하드웨어적인 자원을 서비스로 제공하는 것이다. 자료 저장을 위해 스토리지를 제공하거나 컴퓨팅에 필요한 CPU 같은 자원을 제공한다. 아마존의 EC2(Elastic Compute Cloud) 등이 있다 [1,2].

2.2 클라우드 컴퓨팅 종류

클라우드 컴퓨팅은 사용 용도에 따라 Public Cloud, Private Cloud, Hybrid Cloud로 구분할 수 있다.

Public Cloud 은 External Cloud로 불리고 다수의 일반 사용자들에게 공개되어 인터넷을 기반으로 운영되는 클라

우드 컴퓨팅 서비스를 의미한다. Public Cloud는 일반 포털 사이트처럼 외부에 있는 데이터 센터를 사용하고 사용 대상을 특별히 제한하지 않는다. 구글과 아마존이 제공하는 서비스가 Public Cloud에 속한다 [1,2]. Public Cloud의 장점은 SaaS의 활용의 용이, 적은 투자로 높은 성과, 사용량 만큼만 사용료를 지불, 활용도 증가, 서비스를 적기에 제공 받음, 높은 수준의 탄력성 등이 있다. 단점으로 고객의 통제 권한이 부족하고, 이용료를 매월 납부하는 번거로움, 지원 비용의 증가, 전문적인 서비스 제공의 어려움 등이 있다 [3].

Private Cloud은 Internal Cloud ,Local Cloud 또는 Enterprise로도 불리고 Public과는 다르게 기업같은 폐쇄적인 환경에서 제한된 사용자가 사용하는 클라우드 컴퓨팅 서비스를 의미한다 [1,2,3]. 장점으로는 서비스 수준의 관리 가능, 특정 임무 중심의 어플리케이션 구성, 보안 및 신뢰성 제고, 네트워크의 대역폭에 대한 제약 없음, 인터넷 접속 가능에 대한 제약 없음 등이 있다. 또한, 단점으로는 장비와 하드웨어, 가상화를 위한 기술 비용의 필요, 데이터 센터의 구축 비용, 인력 발생으로 인한 비용, 낮은 탄력성 등이 있다 [3]

Hybrid Cloud는 Private Cloud와 Public Cloud를 혼용하는 형태이다[1]. 기업 내부에서는 Private Cloud를 구성하고 추가적으로 필요한 IT 자원을 Public Cloud와 연동하여 사용한다.

2.3 클라우드 컴퓨팅 이슈

본 절에서는 클라우드 컴퓨팅의 보안 이슈와 클라우드 모델에 대한 실제 보안관리 사례에 대해 살펴본다.

IDG는 2011년 보안 이슈로 허술한 스마트폰 데이터, 액세스 제어 및 ID 관리의 개선, 계속되는 컴플라이언스 우려, 다수의 클라우드 테넌트에 따른 위험, 클라우드 표준과 인증의 출현 5가지를 들었다. 첫째로 모바일 디바이스를 이용한 클라우드 컴퓨팅의 경우 모바일에 대한 데이터가 다른 환경에 비해 데이터가 안전하게 보관되지 않고 디바이스 분실시 이용하고 있는 클라우드 서비스를 통해 정보가 유출될 가능성과 규모가 커진다. 둘째, 기존의 시스템과 클라우드 컴퓨팅의 혼합한 구조에서 적합한 ID관리 기술이 존재하지 않는 문제가 있다. 셋째, 컴플라이언스 문제는 자신이 갖고 있는 데이터와 프로세스를 다른 조직의 프로세스와의 연결에서 문제가 존재한다. 넷째, 가상화로 인해 하나의 물리적 시스템에 여러 조직의 데이터가 저장되어 단편화 대책이 없다면 문제가 존재한다. 다섯째, 데이터를 안전하게 저장할 수 있는가에 대한 정책과 표준이 중요한 요소로 작용한다 [4].

클라우드 모델에 대한 실제 보안관리 사례를 보면 SaaS에서 보안상의 우려점인 SSO를 해결한 것, IaaS에서 데이터 암호화를 해결한 것, Private Cloud에서 가상화 문제를 해결한 것이 있다. SSO 문제를 해결하기 위해 방화벽 내에서 심플리파이드가 관리하는 라우터를 사용하여 한 번 로그인 하면 추가적인 로그인을 요구하지 않게 시스템을 구현하고 어플리케이션은 클라우드로 서비스하여도 엑세스 통제권은 클라우드가 아닌 방화벽 뒤의 시스템에서 관리하도록 하였다. IaaS에서 데이터 암호화는 외부의 데이터 저장소를 이용할 때 송신자와 수신자의 암호화 방식이 다른데에 따른 문제와 어느 곳에 저장되는지 알 수 없는 클라우드 컴퓨팅의 특징을 해결하기 위해 공급업체에서 모든 암호화 과정이 이루어지고 저장위치를 알려주는 것으로 해결하였다. Priavte Cloud에서 가상화 문제는 기존 방화벽을 사용하면 100%가상환경을 구축할 수가 없어서 방화벽도 가상화를 하여 완전한 가상환경을 구축하였다 [5].

3. 클라우드 컴퓨팅 보안

클라우드 컴퓨팅에서 주요하게 고려되어야할 보안 고려사항으로는 데이터 암호화, 사용자 인증과 접근제어, 데이터 무결성, 가용성과 복구, 가상 머신 보호, 네트워크 보안, 공격 모델 및 시뮬레이션, 보안 정책 등이 있다[6].

본 장에서는 클라우드 컴퓨팅의 보안 기술 중 플랫폼, 스토리지, 네트워크, 단말 보안에 대해 알아본다.

3.1 플랫폼 보안

플랫폼 보안 기술로 사용자 인증 기술과 접근제어 기술이 있다. 사용자 인증은 사용자가 정당한 권한을 부여 받은 사용자인지를 인증하는 기술로 Id/password, Multi-factor 인증, PKI, SSO, i-PIN 등이 있다. 접근제어는 특정 프로세스가 다른 프로세스로의 접근을 통제하는 기술이고 DAC, MAC, RBAC이 있다[2].

3.2 스토리지 보안

스토리지 보안 기술에는 검색 가능 암호시스템과 PPDM이 있다. 검색 가능 암호시스템은 키의 사용에 따라 대칭키 기반 검색 가능 암호시스템과 공개키 기반 검색 가능 암호시스템으로 구분된다. 대칭키 기반 검색 가능 암호시스템은 효율성이 높아 대용량 처리에 적합하고 공개키 기반 검색 가능 암호시스템은 다양한 검색기능을 제공하지만 대칭키 기반에 비해 효율성이 떨어진다. PPDM(Privacy Preserving Data Mining)은 기존의 Data Mining이 정보 유출과 프라이버시 침해의 문제가 발생하여 이러한 문제를 해결하기 위해 개발되었다. PPDM은 많은 양의 데이터에서 Data Mining을 수행하지만 프라이버시를 침해하지 않게 한다 [2].

3.3 네트워크 보안

네트워크 보안 기술에는 SSL과 IPsec, application firewall, DDoS 방지 기술이 있다. IPsec은 네트워크 계층의 보안 프로토콜로서 기밀성 기능과 무결성 기능을 제공하고 가상 사설망 등에서 널리 사용되고 있다. IPsec는 강한 보안성을 제공하고 IPv4 에서는 선택적으로 IPv6에서는 필수로 설정된다. SSL의 표준 명칭은 TLS로 인증서를 통한 인증, 기밀성, 무결성을 제공하여 보안성을 강화한다. Application Firewall은 기존의 Firewall에서 응용 계층을 효과적인 방어를 지원하지 않기 때문에 개발되었고 Web Firewall과 DB Firewall이 있다. DDoS(Distribute Denial of Service) 방지 기술은 취약점을 이용하여 서비스의 이용을 불가능하게 만드는 DDoS를 방어하기 위한 기술이다. 비정상적인 Port, Option, Packet의 사용을 차단하는 기술이 있다 [2].

3.4 단말 보안

단말보안에는 TCG의 TPM, Discretix의 CryptoCell, SafeNet의 SafeXcel IP-Trusted Module 등의 상용기술이 있다. 최근 가상화와 재생화를 통한 보안 기술이 개발되고 있으며 가상화는 통신서비스와 개인서비스를 분리하여 공격이나 장애시에도 통신 서비스를 제공할 수 있도록 하고 재생화는 양방향 통신환경에서 단말의 무결성이나 보안 업데이트를 수행하여 보안성을 향상시킨다 [2].

4. 결론

본 논문에서는 클라우드 컴퓨팅의 개념 및 종류, 서비스, 최근 이슈 사항 및 보안 기술에 대해 살펴보았다. 클라우드 컴퓨팅은 기존의 IT 기술을 이용하여 IT 자원의 활용과 효율을 증가하지만 기존 IT 기술을 이용하기 때문에 기존의 보안 위협을 갖고 있다. 그 외에도 여러 기술이 복합되면서 새로운 보안 위협을 불러올 수 있다.

앞에서 살펴본 클라우드 컴퓨팅 이슈와 보안 문제를 해결하기 위한 방법들에서도 보았듯이 클라우드 컴퓨팅은 물리적인 장비의 가상화 문제와 기존에 사용하는 ID관리 시스템과 다른 ID 관리 기술이 필요하고 클라우드 서비스를 제공하는 업체와 서비스를 제공받는 업체 간의 연동 문제, 그리고 표준이나 인증 기준 등에 대한 문제들이 존재한다.

클라우드 보안 위협이 해소되기 위해서는 보안 표준과 인증 기준을 확립하여 기존 보안 기술을 강화하고 서비스하는 소프트웨어, 플랫폼, 인프라, 스토리지, 데이터 베이스 등의 보안과 통합적인 서비스를 제공할 경우 발생할 수 있는 보안 문제점에 대한 지속적인 연구가 필요하다. 그리고 보안성을 강화할 경우 필연적으로 발생하는 서비스 효율성의 저하되는 Trade-Off를 고려하여 클라우드 컴퓨팅의 보안 기술이 연구되어야 할 것이다.

감사의 글

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1131-0004)

참고문헌

[1] 민옥기, 김학영, 남궁한, “클라우드 컴퓨팅 기술 동향”, 전자통신동향분석 제24권 제4호 2009년 8월

[2] 은성경, 조남수, 김영호, 최대선, "클라우드 컴퓨팅 보안 기술", 전자통신동향분석 제24권 제4호 2009년 8월

[3] 이호현, 이기훈, “IBM의 클라우드 컴퓨팅 동향 및 전략”, 정보통신연구원, 방송통신정책, 제22권, 제21호, 통권 497호, 2010년 11월

[4] “2011년에 등장할 클라우드 보안 이슈 5선” http://www.idg.co.kr/newscenter/common/newCommonView.do?newsId=63667, 2010년 12월

[5] “현실에서의 클라우드 보안 : 4가지 사례“ http://www.idg.co.kr/newscenter/common/newCommonView.do?newsId=62005, 2010년 6월

[6] 임철수, "클라우드 컴퓨팅 보안 기술" , 정보보호학회지 제19권 제3호, 2009년 6월