클라우드 컴퓨팅의 기술 및 보안서비스 연구

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

A study on technology and the security service of the Cloud Computing

Nam Yong Kim, Jong Hyuk Park*
Dept. of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul, 139-743, REPUBLIC OF KOREA
e-mail : {nykim, jhpark1}@seoultech.ac.kr

요 약

컴퓨터가 점차 발달하면서 클라우드 컴퓨팅(Cloud Computing)이 미래에 핵심적인 기술로 이슈가 되고 있다. 클라우드 컴퓨팅 기술 발전을 통해 스마트 기기와 신기술 또는 다른 분야의 항목들과 융합이 가능해지며, 무한한 가능성을 보여주고 있다. 본 논문에서는 클라우드 컴퓨팅 기술 및 구조를 설명하였고, 클라우드 컴퓨팅 보안 위협과 보안사고 사례를 나타냈다. 또한 클라우드 보안 서비스인 SecaaS를 통해 클라우드 컴퓨팅 보안서비스를 연구하였고, 이를 통해 앞으로 클라우드 기술을 적용 및 확장 가능한 미래 기술을 전망한다.

1. 서론

최근 클라우드 컴퓨팅 기술의 등장으로 기존 서비스 및 네트워크 체계에 패러다임(paradigm)의 변화를 가져오고 있다. 컴퓨터 산업이 시작되면서 하드웨어와 소프트웨어를 사용한 만큼 요금을 지불하는 형태의 유틸리티 컴퓨팅을 지향하였다. 그래서 효율적이면서 저렴하게 컴퓨터 시스템을 사용하고자 클라우드 컴퓨팅을 비롯한 새로운 기술들이 개발되고 있다. 클라우드 컴퓨팅 기술은 스마트 기기(스마트 폰, 스마트 TV, 스마트 냉장고 등)와 신기술(IoT, 빅데이터, 블록체인, 로봇 등)들과 같이 미래 IT 시대의 중심을 맡고 있으며, 다른 분야의 항목들(의료, 바이오, LED, 보안 등)과 융합을 통해 새롭고 다양한 서비스들(방송, 통신, 콘텐츠 등)을 만들어 가는 주요 기술이 되고 있다 [1].

전 세계 공공 클라우드 서비스 시장 규모는 '16년 965억 달러에서 2020년에는 1,950억 달러 규모로 연평균 20.4% 증가할 것으로 전망되며, 현재 글로벌 시장은 아마존, MS 등 주도 중이나, 향후 높은 잠재 수요를 가지고 있는 중국 시장이 급성장할 것으로 전망이다. 국내 클라우드 시장 규모는 1.19조원으로 전년 대비 55.2% 증가하였으며, 클라우드 기업도 전년 대비 51.6% 증가(353→535개, 182개↑) 하여 클라우드 컴퓨팅은 무한한 가능성을 보이고 있으며 계속적으로 투자를 하고 있다 [2].

본 논문에서 클라우드 컴퓨팅 기술 및 구조에 대해 살펴보고, 클라우드 컴퓨팅 보안 위협과 사고 사례 분석한다. 또한 Security as a Service(SecaaS)를 통해 클라우드 컴퓨팅이 보안 패러다임의 변화로 핵심적인 역할을 담당할 것이다.

Acknowledgments

이 논문은 2016년도 정부 (미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016R1A2B4011069)

2. 클라우드 컴퓨팅

클라우드 컴퓨팅은 인터넷상에서 유틸리티 컴퓨팅과 IT 기술, 자원 또는 서비스 제공을 말한다.

그림 1을 보면, 미국 National Institute of Standards and Technology(NIST)는 참조모델 경제 안보를 강화와 삶의 질을 개선하는 방식으로 각종 산업 기술과 측정 분야의 국가 기준이 되는 표준을 선정하여 개발하는 연구소이며, 클라우드 컴퓨팅을 배치 모델(Hybrid, Private, Public, Community), 서비스 모델(SaaS, PaaS, IaaS, BaaS), 주요 특성(Rapid Elasticity, On Demand Self-Service 등), 공통 특성(Massive Scale, Resilient computing 등)으로 구분하였다 [3].

그 중 몇 가지 살펴보면, 사설 클라우드(Private cloud)는 폐쇄적으로 운영되어 정보 유출이 민감한 기관에서 선호하는 방식이며, 특정 사용자만 사용하는 클라우드 서비스이다. 공용 클라우드(Public cloud)는 일반 사용자에게 공개된 대규모 클라우드 서비스이며, 기업들은 사용량에 따라 사용료를 내고 이용하는 방식이다. 혼용 클라우드(Hybrid cloud)는 사설과 공용 클라우드를 동시에 제공한다. 클라우드 컴퓨팅의 주요특성 5가지가 나타난다. 주문형 셀프 서비스(On Demand Self-Service)는 필요할 때 사용자와 클라우드 서비스 공급자는 온라인으로 컴퓨터 자원을 사용할

수 있다. 광대역 네트워크 접근(Broad Network Access)은 네트워크를 통해 컴퓨터 자원 또는 서비스 어디서나 접근이 가능하고 사용 할 수 있다. 신속한 탄력성(Rapid Elasticity)은 자원들을 빠르고 유연하게 대응이 가능하다. 자원공유(Resource Pooling)는 멀티테넌트(multi-tenant)을 통해 자원 할당을 의미한다. 측정된 서비스(Measured Service)는 측정시스템을 기반으로 사용자는 사용량, 대역폭 등 서비스를 사용한 만큼 비용을 지불한다 [4].

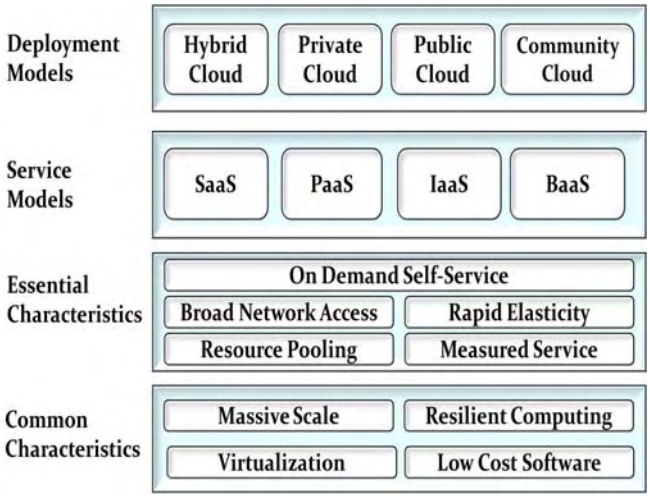

그림 1. NST의 클라우드 컴퓨팅 구조

그림 2 을 통해, 클라우드 서비스는 제공하는 자원의 형태에 따라 X as a service(XaaS) 로 정의하며, 일반적으로 Infrastructure as a Service(IaaS), Platform as a Service(PaaS), Software as a Service(SaaS), Backend as a Service(BaaS) 로 분류한다 [5].

IaaS는 가상 머신, 가상 인프라, 가상 저장장치와 같은 하드웨어 자원을 사용자에게 제공하며, IaaS 서비스 모델의 예는 Linode, GoGrid, EC2(Amazon Elastic Compute Cloud) 등이 있다. PaaS는 IaaS를 포함하고 운영체제, 개발 프레임워크 등을 사용자에게 제공한다. PaaS 서비스 모델의 예는 Google AppEngine, Windows Azure Platform 등이 있다. SaaS는 PaaS를 포함하며 애플리케이션, 관리, 사용자 인터페이스를 포함하는 서비스를 말하고 Google Apps, Oracle On Demand, Office 365 등이 있다. BaaS는 SaaS를 포함하며 애플리케이션에 Backend를 제공하는 클라우드 컴퓨팅에 대한 접근 방식이며, API와 Backend를 통합 할 수 있는 다양한 컴퓨터 언어용 도구를 제공한다. BaaS 서비스 모델의 예는 Parse, Firesbase 등외에도 다양하게 있다 [6].

2.1. 클라우드 보안 위협

클라우드 컴퓨팅에서는 다양한 보안 위협이 존재하며 클라우드 서비스 관련 사고들이 잇따라 나타나고 있다. Cloud Security Alliance(CSA)는 클라우드 컴퓨팅에서의 안정성 증진과 보안 이슈를 해결하기 위한 비영리 단체이며, 2008년 Information Systems Security Association (ISSA)의 Chief Information Security Officer(CISO) 포럼을 계기로 설립되었다.

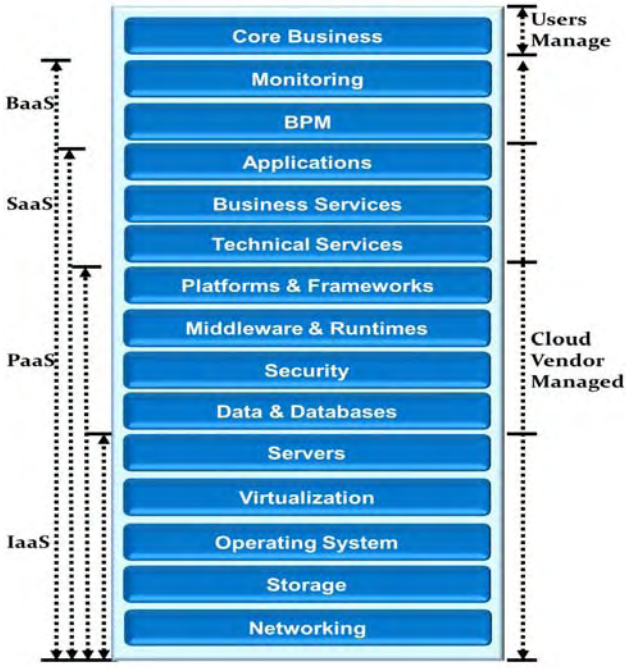

그림 2. 클라우드 서비스별 자원제공 범위

표 1 에서는 CSA가 발표한 The treacherous 12 cloud computing top threats in 2016을 통해 12가지의 위험할 수 있는 항목을 제시하였다. 데이터 유출(Data Breaches), 불충분한 ID, 자격 증명 및 접근 관리(Insufficient Identity, Credential and Access Management), 안전하지 않은 인터페이스 및 API (Insecure Interfaces and APIs), 시스템 취약점(System Vulnerabilities), 계정 도용(Account Hijacking), 악의적인 내부자(Malicious Insiders), 지능적 지속 위협(Advanced Persistent Threats), 공유된 기술 문제(Shared Technology Issues), 클라우드 서비스의 남용 및 사소한 사용(Abuse and Nefarious Use of Cloud Services), 서비스 거부(Denial of Service), 불충분한 조사(Insufficient Due Diligence), 데이터 손실(Data Loss) 과 같이 클라우드 12가지의 위험유형을 발표하였다. 이 발표는 자주 일어나는 위협항목을 나타낸 것이며 다양한 보안 사고 사례가 기반이 되었다 [7].

2.2. 클라우드 보안사고 사례

최근 클라우드 서비스 보안사고 사례가 매년 다양하고 향상된 공격으로 나타난다. 2014년, 애플의 iCloud에 업로드된 유명 여배우들의 계정 해킹을 통한 개인자료 및 사진 유출, 공격자가 소니에 침입하여 개인 식별 정보 및 전자메일 교환과 같은 기밀 정보가 소니 직원들 사이에서 누출 등 클라우드 보안사고에 큰 이슈가 되었다. 2015년, 아마존에서 BitDefender는 AWS 에서 호스팅되는 공용 클라우드 애플리케이션의 보안상 취약점으로 다수의 개인정보 유출 사례, 미국 국세청(IRS)의 취약한 API("Get Transcript")를 통해 30 만 건 이상의 데이터 노출이 있었다.

표 1. CSA에서 발표한 12가지의 클라우드 위협

위 협	설 명
Data Breaches	응용 프로그램 취약성과 취약한 보안 등을 통한 민감한 데이터 유출
Insufficient Identity, Credential and Access Management	데이터 침해 및 공격 가능성은 ID 액세스 관리, 자격증명, 암호 및 인증서 인증 등을 사용하지 않기 때문에 발생
Insecure Interfaces and APIs	인증 및 접근 제어, 활동 모니터링 등의 인터페이스는 정책을 우회하는 위협
System Vulnerabilities	데이터 유출 또는 시스템 제어하거나 서비스 작업을 방해하기 위해 시스템 취약점을 통한 침투
Account Hijacking	사기, 피싱 및 소프트웨어 취약점 등 공격으로 인한 계정 탈취
Malicious Insiders	악의적인 내부자에 의한 위협
Advanced Persistent Threats(APTs)	특정 목표에 대한 지능적이고 지속적인 위협 공격
Shared Technology Issues	전송 모델에서 잠재적으로 악용될 수 있는 공유된 기술 취약점
Abuse and Nefarious Use of Cloud Services	클라우드 서비스를 이용한 악의적인 공격
Denial of Service	DoS 및 DDoS 공격으로 인한 클라우스 서비스 위협
Insufficient Due Diligence	클라우드 기술 및 서비스제공자 등에 불충분한 조사
Data Loss	재해, 해킹 등의 사고로 인한 데이터 손실 또는 유출

2016년, 대형 DNS 서비스 업체인 딘(Dyn)이 대규모 DDoS 공격당했으며 아마존과 깃허브, 트위터 등 업체에 트래픽 문제가 발생, 링크드인 650만 계정 비밀번호 유출, 야후 2014년 해킹 당시 5억명의 특정 사용자 계정 정보의 사본 유출 등 이러한 보안사고 사례를 통해 꾸준히 지능적이면서 향상된 공격기법들이 증가하고 있다. 향후 미래에는 클라우드 보안 역시 안전하다고 할 수 없다.

2.3. Security as a Service(SecaaS)

SecaaS는 클라우드 시스템의 여러 종류와 모델을 기반으로 제공하는 소프트웨어 형태의 보안 서비스이다. SaaS의 한 종류이며 클라우드를 이용해서 고객이 필요로 하는 보안 서비스를 제공하기 위해 설계되었다.

SecaaS가 등장하면서 보안 패러다임의 변화가 생겨났다. 기존의 보안은 예전의 기술, 소프트웨어 구조를 고려하여 보안 위협으로부터 다양한 형태의 제품들을 추가하면서 보안해왔다. 예를 들면, 일반적인 보안은 Firewall, IDS/IPS, Anti-DDoS 등이 있고, 엔드포인트(End-Point) 보안은 Anti-virus, DB encryption 등을 통해 다양한 형태의 보안 제품들이 있다. 이렇게 기존 소프트웨어구조에서 효율적인 보안 장비로 바뀌가고 있지만 알려지지 않은 취약점들도 많을 뿐만 아니라 보안 제품 간의 호환성 문제 등 관리가 쉽지 않기에 보안이 안전하다고 답할 수 없다 [8].

SecaaS의 시장은 2015년 31억 2000만 달러에서 2020년 85억 2000만 달러로 연 평균 22.2% 성장할 전망이다. 국내외 많은 보안업계에서 SecaaS 시장에 잇따라 진입하고 있다. 해외에서는 SecaaS를 본격 공략하고 있지만 국내는 클라우드 보안에 대한 투자 규모가 작지만 일부 기업에서는 적극적으로 시장에 뛰어들고 있다 [9].

SecaaS는 빠르고 쉬우며 전문화된 보안 서비스를 제공할 수 있는 장점들이 있다. 경제적 측면에서 비용이 절감되며 사용하는 서비스에 대한 사용료를 지불하면 된다. 보안 솔루션 장비를 설치할 필요 없으며, 고객의 데스크톱과 서버, 모바일 기기 등 장비에 대한 취약점관리가 가능하다. 로그관리, 모니터링 등 반복적인 보안업무가 간소화되어 지능형 지속 위협 공격(APT), 분산 서비스 거부 공격(DDoS) 등 대응에 효과적이다. 그러나 기존 보안장비와 보안프로그램과 다르게 대용량 트래픽관리가 안돼서 큰 규모의 네트워크에서는 성능 저하, 접속 지연 등 문제가 생길 수 있다. 하지만 중소기업의 경우 대용량 트래픽이 자주 발생하지 않아 SecaaS를 효과적으로 사용가능하며 저비용, 효율적인 관리 및 보안성 강화를 통해 중소기업의 취약한 정보보안 해결책이 될 전망이다 [10].

CSA는 기존에 존재하는 SecaaS 서비스에서 보안 위협 시 소비자들에게 더 나은 보안 솔루션의 이해를 위해 표 2와 같이 12가지 항목으로 분류하였다 [11].

표 2. CSA에서 발표한 SecaaS 12가지 항목

도메인	설 명
Network Security	모니터링, 분배, 네트워크 접근 할당 등 네트워크 보안서비스 구성
Vulnerability Scanning	공용 네트워크를 통해 보안 취약점에 대한 인프라 또는 시스템 취약점 검사
Web Security	클라우드 서비스 공급자를 통해 웹 트래픽, SSL 등 공개된 애플리케이션 서비스 실시간 보안
Email Security	피싱, 악의적인 첨부 파일 등 스팸메일로부터 조직을 보호, 비즈니스 연속성 옵션 제공
Identity and Access Management(IAM)	ID관리, 신원보증 등 사용자 관리
Encryption	일반 텍스트를 암호와 숫자를 사용하여 데이터를 난독화하는 프로세스
Intrusion Management	비정상적인 이벤트 감지, 침입 시도를 방지 또는 탐지를 관리
Data Loss Prevention (DLP)	데이터 사용과 행위에 모니터링, 보호 및 검증
Security Information and Event Management (SIEM)	로그 및 이벤트 정보의 상관관계, 사고 데이터를 수용하고 실시간 분석
Business Continuity and Disaster Recovery (BCDR)	서비스 중단 시 운영상의 탄력성을 보장하도록 설계된 조치
Continuous Monitoring	조직의 현재 보안 상태를 나타내는 지속적인 위험 관리 기능 수행
Security Assessments	업계 표준을 기반으로 한 클라우드 서비스에 대한 제 3자가 감사

3. 결론

최근 다른 분야의 항목들(의료, 바이오, LED, 보안 등)에 클라우드와 기술이 융합 및 개발이 적용되고 있으나 보안사고는 지속적으로 나타나고 있어 기술적 대책이 필요한 상황이다. 기존 IT 환경을 대체하는 패러다임의 변화로 그 중 큰 화제가 클라우드 컴퓨팅 보안이다. 그리고 보안사고들을 최대한 줄이기 위해 클라우드 컴퓨팅 보안서비스를 빠르게 도입시켜 전문 보안업체들은 클라우드 컴퓨팅 보안에 힘을 써야 한다.

본 논문에서는 클라우드 컴퓨팅 개념과 구조를 소개하며 최신 보안의 위협 요소들, 클라우드 보안 서비스인 SecaaS 보안기술에 대해 살펴보았다.

클라우드 보안 서비스 기반인 SecaaS 를 통해 보안시장을 변화시키며 인력관리, 모니터링, 편의성 등 사용자와 서비스제공자에게 모두 효율적으로 사용되어야 하고, 앞으로 클라우드 컴퓨팅은 점차 IT뿐만 아니라 모든 시장에 큰 영역을 차지할 것으로 기대된다. 따라서 클라우드 컴퓨팅을 보안 문제없이 안전하면서도 효과적인 보안서비스를 제공하여 사물인터넷(IoT), 인공지능(AI), 머신러닝 등 다양한 미래 기술들과 빠르게 적용할 수 있을 것으로 전망한다.

참고문헌

[1] 신상열, 남영준, "2017년 K-ICT 클라우드컴퓨팅 활성화 시행계획 마련", 미래창조과학부, 2017

[2] Barrie Sosinsky, “클라우드 컴퓨팅 바이블”, 길벗출판사, 2012

[3] Peter Mell, Tim Grance, Lee Badger, “The NIST Cloud Definition Framework”, NIST, 2011

[4] 권혁찬, 정도영, 정병호, 김정녀, "클라우드 보안 개요", 한국전자통신연구원, 2015

[5] Ashish Singh, Kakali Chatterjee, "Cloud security issues and challenges: A survey, Journal of Network and Computer Applications, Volume 79, 2017

[6] KISA 연구개발팀, “클라우드 서비스 정보보호 안내서”, 한올출판사, 2011

[7] Top Threats Working Group, "The Treacherous 12 Cloud Computing Top Threats in 2016", CSA, 2016

[8] 정수환, “클라우드 기반 보안서비스 기술 동향”, The Magazine of the IEEK, 2013

[9] Ngoc-Tu Chau, Minh-Duong Nguyen, Seungwook Jung, Souhwan Jung, “SecaaS Framework and Architecture: A Design of Dynamic Packet Control”, International Workshop on Information Security Applications, 2015

[10] Security as a Service Working Group, "CSA Defining Categories of Security as a Service: Continuous Monitoring", CSA, 2016

[11] Deepak H. Sharma, C.A. Dhote Dr, Manish M. Potey, “Identity and Access Management as Security-as-a-Service from Clouds”, Procedia Computer Science, Volume 79, 2016