情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

클라우드 컴퓨팅 보안 기술 동향

은 성 경*

요 약

클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅으로 최근 많은 관심을 받고 있다. 클라우드 컴퓨팅이 널리 사용되기 위해서 해결해야 할 첫 번째 문제는 보안인 것으로 조사된바 있다. 클라우드 컴퓨팅의 보안은 사용자의 영역에 따라 개인 사용자와 기업 사용자 분야로 나눌 수 있으며, 개인 사용자는 익명성에 관심을 두고 있고, 기업 사용자는 컴플라이언스에 관심을 두고 있다. 클라우드 컴퓨팅은 플랫폼, 스토리지, 네트워크, 단말로 구성되어 있고, 각각의 위치에서 필요한 보안기능이 따로 존재한다. 본 고에서는 클라우드 컴퓨팅의 보안 이슈, 사례, 표준, 연구 방향에 대하여 기술한다.

I. 서 론

클라우드 컴퓨팅이란 '인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 컴퓨팅'으로 정의할 수 있다[1]. 주요한 특징으로는 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 것을 들 수 있다.

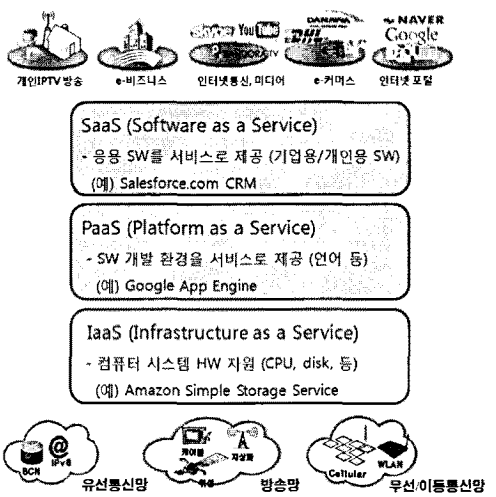
이러한 컴퓨팅을 제공하기 위한 서비스로 그 추상화 정도에 따라 분류해보면 [그림 1]과 같다.

IaaS는 CPU, Disk등 컴퓨터 시스템의 HW자원을 가상화하여 여러 사용자에게 제공하는 것으로 아마존의 Elastic Compute 서비스가 이에 해당한다. PaaS는 HW 자원을 추상화하고 그 위에 SW 개발과 수행환경을 제공하는 것으로 구글의 App Engine과 아마존의 Simple Storage Service 등이 이에 해당한다. SaaS는 응용 SW를 서비스형태로 제공하는 것으로 대표적인 서비스로 Salesforce.com과 구글의 Docs 등을 들 수 있다.

이러한 클라우드 서비스들을 수요자 별로 시장을 구분하고 각각의 사례와 주요한 사업자를 [표 1]에서 확인할 수 있다[2].

클라우드 컴퓨팅을 구성하는 요소들은 [그림 2]에서 확인해 볼 수 있다.

단말은 서비스를 요청하거나 그 결과를 보는 장비이며, 여기에는 개인용 컴퓨터를 비롯하여 노트북과 이동형 기기인 휴대전화 등을 들 수 있다. 서버는 실제 작업을 수행하는 장비를 지칭하며 여기에는 서버 컴퓨터를 비롯하여 운영체제 등이 포함된다. 스토리지는 결과를 저장하는 곳으로 디스크 및 데이터베이스 등을 포함한다. 응용프로그램은 서버와 스토리지를 이용하여 원하는 작업을 수행하는 프로그램이다. 단말과 클라우드 그리고 한 클라우드와 다른 클라우드는 네트워크로 연결한다.

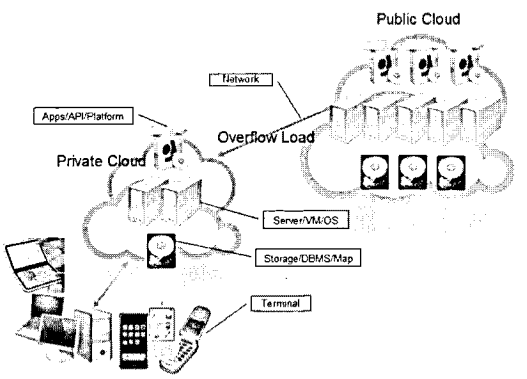


〔그림 1〕 클라우드 컴퓨팅 서비스 모델

* 한국전자통신연구원 암호기술연구팀 (skun@etri.re.kr)

〔표 1〕 시장별 서비스 유형과 주요 사업자

시장 유형		제공서비스 사례	주요 사업자 서비스
소비자 시장	웹기반 서비스	• 인터넷 기반 서비스 (Blog, Wiki, Social Service)	• 구글 • Myspace.com
	SW 서비스(SaaS)	• Office 생산성 애플리케이션 • 협업 솔루션 • 기타 클라이언트 애플리케이션	• 구글 Apps for your Domain • MS Office Live • IBM Bluehouse
IT구매자 시장 (클라우드 인프라)	애플리케이션 컴포넌트 서비스	• 서비스나 애플리케이션 개발을 위한 API와 웹기반 SW모듈 (애플리케이션 레이어 수준)	• 아마존 flexible payment API • 구글 Calendar API • 세일스포스닷컴 AppExchange API
	SW 플랫폼 서비스 (PaaS)	• 신규 애플리케이션 개발을 위한 개발 플랫폼 (미들웨어 레이어 수준) - Hosted App Platform Server, Hosted DB - Hosted Data 관리, Message Queue 등	• 아마존 SimpleDB, Simple Storage Service(S3), simple Queue Service • 구글 App Engine • MS SQL Server Data Service • 세일스포스닷컴 Force.com
	가상인프라 서비스	• 가상 서버, 가상 Storage, 가상 네트워크 • 시스템 관리	• 아마존 Elastic Compute Cloud(EC2)



〔그림 2〕 클라우드 컴퓨팅 구성 요소

클라우드 컴퓨팅은 이용 목적에 따라서 Public Cloud와 Private Cloud로 나눈다. Public Cloud는 일반사용자에게 공개되어있는 클라우드 컴퓨팅 서비스로 구글과 아마존의 서비스가 이에 해당한다. 이러한 종류의 서비스는 대규모로 이루어지는 특성이 있다. 반대로 Private Cloud는 기업 내부와 같이 폐쇄된 환경에서 특정사용자만 사용하는 클라우드 서비스를 지칭한다. 또, Private Cloud를 운영하다 서비스가 감당할 수 있는 한계에 다다르면, 넘치는 서비스 요구를 외부의 Public Cloud 서비스를 이용하여 처리하는 형태를 생각할 수 있는데, 이러한 형태를 Hybrid Cloud로 부르기도 한다.

Ⅱ. 클라우드 컴퓨팅 보안 이슈

클라우드 컴퓨팅은 IT자원을 소유하지 않고 일부 또는 모두를 아웃소싱하는 형태이다. 이런 경우 필연적으로 보안 문제가 제기될 수 밖에 없는데, [표 2]는 이를 잘 대변해준다.

이 표는 시장 조사 기관인 IDC에서 244명의 IT 관련 임원들에게 IT Cloud 서비스에 관하여 그들의 견해와 활용에 대하여 조사한 것 중의 하나로, 보안을 해결해야 할 첫 번째 과제로 꼽고 있다[3].

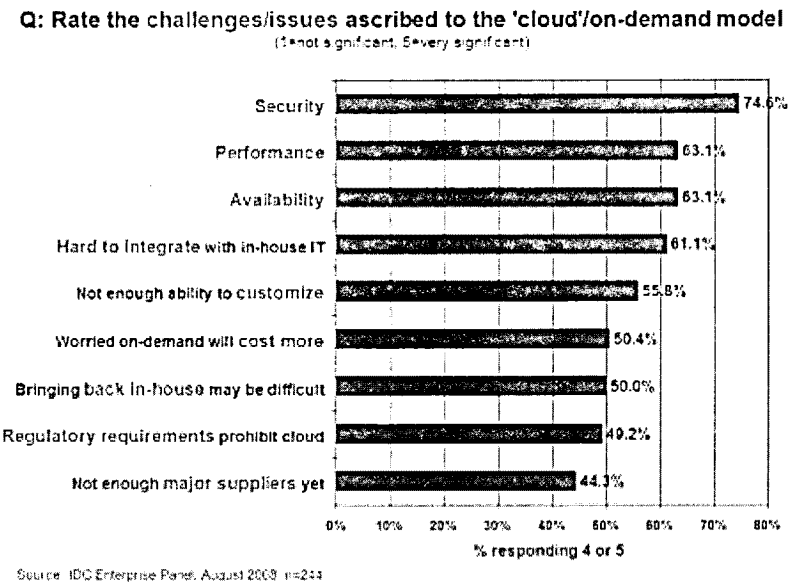
클라우드 컴퓨팅의 보안 이슈는 개인과 기업 사용자의 두 가지 소비자 영역으로 나누어서 생각해볼 수 있다.

2.1 개인 사용자 관점의 보안

개인 사용자는 E-mail, 블로그, 동호회, 사진 및 파일 저장과 공유 서비스를 주로 이용하며, 무료로 제공하는 서비스를 선호하는 특성을 갖는다. [표 1]의 웹 기반 서비스 들이 주로 이들을 위한 것이다. 개인 사용자 관점에서 우려하는 보안 문제를 열거하면 다음과 같다.

- 개인정보 노출
- 개인에 대한 감시
- 개인 데이터에 대한 상업적 목적의 가공

〔표 2〕 IT Cloud 서비스의 해결 과제



2.2 기업 사용자 관점의 보안

기업 사용자는 자신이 소유하던 IT자산을 클라우드 형태로 제공받기를 원하지만, 자신의 데이터가 타인과 공유되기를 원하지 않는다. [표 1]에서 웹 기반 서비스를 제외한 다른 서비스들이 기업 사용자를 위한 것이다. 기업 사용자는 안정성과 안전성을 제공하면 비용을 지불할 의사가 있으며, 때에 따라서는 Private Cloud와 같이 자신이 직접 운영하기도 한다. 기업 사용자 입장에서 우려하는 보안 문제를 열거하면 다음과 같다.

- 서비스 중단
- 기업 정보 훼손
- 기업 정보 유출
- 고객 정보 유출
- 법/규제 준수
- e-discovery 대응

이와 같이 개인 사용자와 기업 사용자는 클라우드 컴퓨팅에 대한 보안 요구사항이 다르다. 개인 사용자는 익명성 보장에 중점을 두는 반면, 기업 사용자는 컴플라이언스에 중점을 두는 경향이 있다.

기업 사용자의 보안 고려사항은 Cloud Security Alliance에서 가이드로 제시한 것을 참고해 볼 수 있다[4]. Cloud Security Alliance는 클라우드 컴퓨팅의 안전성 증진과 사용자 교육을 목적으로 만든 비영리 기관으로, 다음과 같은 보안 고려사항을 제시하고 있다.

- Governance and Enterprise Risk Management
- Legal
- Electronic Discovery
- Compliance and Auit
- Information Lifecycle Management
- Portability and Interoperability
- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Storage Virtualization

Ⅲ. 클라우드 컴퓨팅 보안 사례

클라우드 컴퓨팅 보안 사례로 Amazon Web Serivce(AWS)

의 보안 기능을 알아보면 다음과 같다[5].

3.1 Certifications and Accreditations

법률이나 규정 또는 규격에 부합함을 인정받는 것으로, AWS에서는 미국의 회계관련법인 SOX와 기업 내부 제어에 대한 인증인 SAS70 Type II 그리고 의료관련 법률인 HIPAA 지원을 목표로 하고 있다.

3.2 Physical Security

시설물 보호를 위하여 경비원, CCTV 및 침입감지 시스템을 두고 있으며, 모든 직원은 데이터 센터에 들어갈 때까지 3번 이상의 two-factor 인증을 거친다.

3.3 Backups

S3와 SimpleDB 그리고 Elastic Block Store의 모든 데이터는 복수개의 원격지에 중복 저장하고 있으며, 따로 backup을 수행하지는 않는다.

3.4 EC2 Security

EC2 instance로의 접근은 SSH에 의하여 보호하며, 네트워크 접속은 Firewall을 이용하여 통제하고 있다. instance의 생성 및 제거와 firewall 설정 변경 등 주요한 EC2 API 호출은 X.509 인증서나 Amazon Secret Access Key에 의하여 서명된 것만 처리된다. instance들은 Xen hypervisor를 이용하여 격리하고 있다. EC2의 네트워크 보안 기능으로 syn cookie, connection limiting, bandwidth limitation등에 의한 DDoS 공격 방지, SSL 사용에 의한 MITM 공격 방지, firewall에 의한 IP spoofing 방지와 port scanning 방지 등이 있다.

3.5 S3 Security

S3의 모든 데이터는 bucket 또는 object 별로 Access Control List에 의하여 접근이 통제된다. 외부로의 데이터 이동 시에는 SSL을 사용하여 데이터를 보호한다. S3에 데이터를 저장할 때 자동으로 암호화해서 저장하지는 않는다. S3에서 데이터를 삭제하면, 해당 영역은 다시 덮어쓸 때까지 write operation으로만 접근 가능하다.

3.6 SimpleDB Security

SimpleDB는 AWS의 계정 ID 별로 접근이 통제되는 Access Control List를 가지고 있다. 외부와의 통신시에는 SSL을 이용하여 데이터를 보호한다. SimpleDB에 데이터를 저장할 때는 자동으로 암호화를 수행하지는 않는다. 사용자가 암호화해서 저장할 수 는 있지만, 이런 경우 query의 조건으로는 사용할 수 없다. SimpleDB에서 데이터를 삭제하면, 해당 영역은 다시 덮어쓸 때까지 write operation으로만 접근 가능하다.

Ⅳ. 클라우드 컴퓨팅 보안 표준

국제 표준 기관인 ISO에서는 2009년 ISO/IEC JTC1 SC38에 SGCC(Study Group on Cloud Computing)를 만들어 클라우드 컴퓨팅 표준을 준비하면서 보안 이슈를 다루고 있다.

ITU에서는 보안 연구 그룹인 ITU-T SG17에서 클라우드 컴퓨팅 보안을 새로운 연구 주제로 정할 것인지를 논의하고 있다.

미국의 NIST에서는 클라우드 컴퓨팅의 보안 이슈, 아키텍처 보안, 응용 보안, 컴플라이언스, 포렌식 등을 다루는 문서를 발간할 예정으로 있다.

Ⅴ. 클라우드 컴퓨팅 보안 기술 연구 방향

클라우드 컴퓨팅 보안 기술의 연구 방향은 다음의 네 가지를 생각해 볼 수 있다.

5.1 클라우드 컴퓨팅 환경 보호

클라우드 컴퓨팅 구성 요소는 [그림 2]에서와 같이 서버, 소프트웨어, 스토리지, 네트워크, 단말로 나누어 볼 수 있다. 각 구성 요소별로 보안 기술이 필요한데, 서버에는 운영체제 및 Hypervisor 보안 기술이, 소프트웨어에는 응용프로그램 인증, 사용자 인증 및 결재 기술이, 스토리지에는 접근제어 및 암호화 기술이, 네트워크에는 암호화 및 DDoS 공격 방어 기술이, 단말에는 악성코드 방지 및 개인정보 보호 기술이 필요하다. 또한 클라우드

컴퓨팅 서비스 전체로는 물리보안, 보안 SLA(Service Level Agreement)보장, 보안인증 등이 필요하다.

5.2 기존 보안 기술의 클라우드 적용

Anti-virus, 방화벽, IDS/IPS, DLP(Data Loss Prevention), E-discovery 등 기존 IT 환경을 위한 보안 기술은 클라우드 컴퓨팅 환경에 맞게 수정하고 적용하려는 노력이 필요하다.

5.3 Security as a Service

IT 자원을 소유하지 않고 외부에서 서비스 받아 사용한다는 클라우드 컴퓨팅의 특징을 이용하여, 보안도 외부 서비스 형태로 제공하는 Security as a Service는 새로운 보안 기술 분야로 생각할 수 있다.

5.4 새로운 보안 이슈

IT 자원의 공유로 인한 비용 절감이 클라우드 컴퓨팅의 큰 특징인 반면, 보안 기술 적용으로 인한 효율 저하는 풀어야할 숙제로 남아있다. 예를 들어 중복 데이터 제거 기술을 이용한 스토리지 효율성 향상은 각기 다른 키로 암호화된 데이터에는 적용되지 않는다. 또한, 보안을 위한 암호화가 한 번에 이루어지지 않고 통신 계층별 또는 단계별로 중복 수행되는 것에 따른 자원 낭비도 해결해야할 문제이다.

IT 자원을 서비스 형태로 외부로부터 제공받는다는 특징은 사용자의 데이터가 담겨있는 스토리지의 지리적 위치가 법적인 문제를 야기할 수 있어 위치 파악이 필요하고, 자신의 통제권 밖에 있는 데이터의 존재성 및 무결성 확인을 쉽고 빠르게 수행할 수 있는 기술적 장치가 필요하다.

VI. 결 론

클라우드 컴퓨팅의 핵심은 IT자산을 타 사용자와 공유함으로써 얻는 효율성 증대와 그로 인한 비용절감이다. 서버, 네트워크, 소프트웨어, 스토리지등 대부분의 IT 자산은 타 사용자와 공유하여 사용할 수 있지만, 가장 큰 자산이라 할 수 있는 데이터는 타 사용자와 공유할 수 없다. 따라서, 클라우드 컴퓨팅에서 보안은 IT 자산을 타 사용자와 공유함으로써 얻는 효율성 향상을 유지하면 데이터를 안전하게 보호하는 기술에 초점을 맞추어야할 것이다.

참고문헌

[1] 김명준, "Korea's Cloud Computing Strategy", IT21 글로벌 컨퍼런스, 2009.

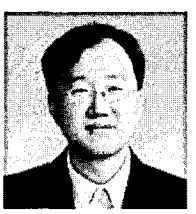
[2] 정재호, 클라우드 컴퓨팅의 현재와 미래 그리고 시장 전략, 한국소프트웨어진흥원, 2008.

[3] Asia Pacific End-User Cloud Computing Survey, IDC, 2009.

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, 2009.

[5] Amazon Web Services: Overview of Security Processes, Amazon, 2008.

〈著者紹介〉



은 성 경 (Un, SungKyong)

1990년 8월: 전북대학교 전자계산기공학과 졸업

1993년 2월: 포항공과대학교 전산학과 석사

1993년 3월~현재: 한국전자통신연구원 책임연구원

<관심분야> 정보보호, 클라우드 컴퓨팅, 디지털 포렌식