클라우드 컴퓨팅 보안 동향

이석철, 손태식
아주대학교 컴퓨터공학과
e-mail:go467913@ajou.ac.kr

Cloud Computing Security Trends

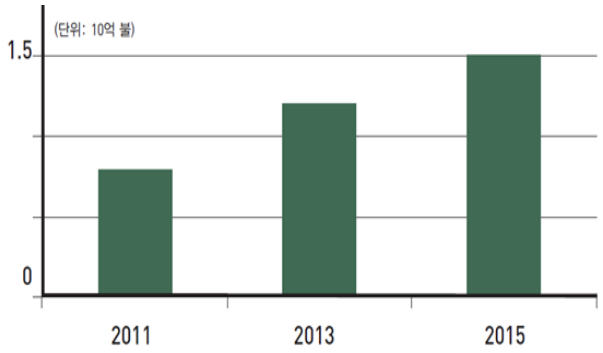
Seokcheol Lee, Taeshik Shon
Dept of Computer Engineering, Ajou University

요 약

최근 각광받고 있는 가상화 서비스 기술은 클라우드 컴퓨팅 기술에는 기존 IT환경에서 존재하던 보안 취약성뿐만 아니라, 서비스 적인 측면과 환경적인 측면에서 보안 취약점이 존재한다. 클라우드 컴퓨팅은 사회 여러분야에 적용되어 사용되므로, 보안 기술 적용의 중요성은 매우 크다. 본 논문에서는 클라우드 컴퓨팅 기술 보안 취약점의 서베이와 클라우드 컴퓨팅 보안 기술 표준화 및 개발 동향에 대해 살펴보고 클라우드 컴퓨팅 보안 연구가 향후 어떤 방향으로 진행되어야 하는지 제시할 것이다.

1. 서론

현대의 정보화 환경은 다양한 분야에 융합되어, 현대 경제·산업의 패러다임인 규모의 경제를 뒷받침하고자 대용량의 빠른 처리, 새로운 저장매체, 양질의 서비스 등을 제공하기 위해 클라우드 컴퓨팅 서비스가 각광받고 있다. 클라우드 컴퓨팅이란 구름과 같이 상호연계 및 연동된 서비스 망을 통해 서비스 제공자가 가상화된 IT자원을 서비스로 제공하고, 소비자는 IT자원을 필요한 만큼 빌려서 사용하고, 사용한 만큼의 비용을 지불하는 가상화 기반 컴퓨팅 기술이다. 클라우드 컴퓨팅의 장점으로는 사용자를 위한 저비용·고효율의 컴퓨터 환경, 접근기기의 다양함(PC, 스마트폰, PMP, 노트북 등), 정보의 접근성, 활용성, 안정성, 스마트 워크 및 작업의 편리성, 그리고 소프트웨어 비용 절감과 편리한 업데이트를 지원하는 것이다. 이와 같이 강력한 장점을 제공하는 클라우드 컴퓨팅은 초기 도입기를 지나 본격적인 성장단계에 있지만, 클라우드 컴퓨팅의 보안에 대한 연구는 이에 미치고 있지 못한 현황이다.



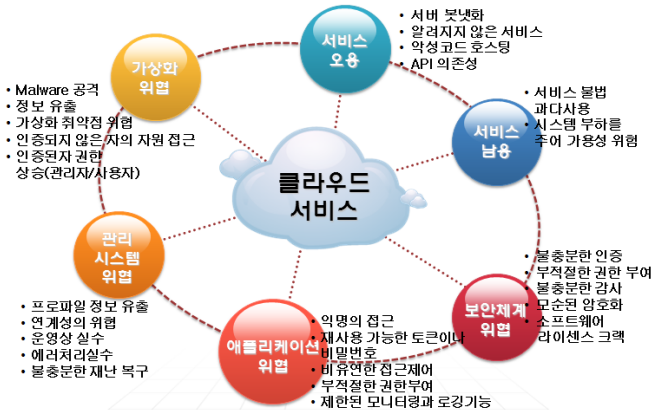
(그림1) 전 세계 가상화 보안 시장 예상규모[7]

특히 국제 시장 조사 기관인 IDC의 IT 분야 임원을 대상으로 조사를 한 결과 클라우드 컴퓨팅 서비스가 사회의 보다 많은 분야에 적용되기 위해 선행되어야 하는 연구 과제가 클라우드 컴퓨팅 보안이라고 응답하였다.[1] 또한 클라우드 컴퓨팅 환경에서는 기존 IT 환경에 존재하는 보안 위협을 포함한 다양한 보안 취약점이 존재하고 클라우드 시장 및 세계 가상화 보안 시장의 규모가 점점 커지는 추세이기 때문에 클라우드 컴퓨팅 환경에서 발생 가능한 위협 및 대응방안에 대한 연구가 필요하다.

본 논문에서는 클라우드 컴퓨팅 환경의 보안성 강화를 위한 미래 연구 방향을 제안하기 위해 2장에서는 클라우드 환경의 보안 취약점을 분석하며, 3장에서는 클라우드 컴퓨팅 환경에서 보안 연구 동향에 대해 살펴보고, 4장에서 결론 및 향후 연구방향을 제시한다.

2. 클라우드 컴퓨팅 보안 취약점

클라우드 컴퓨팅 환경에는 기존 IT 환경에 존재하는 보안 위협 외에도 여러 가지 보안 취약점이 존재한다. 대표적으로 클라우드 컴퓨팅 서비스 측면에서는 봇넷과 같이 악성코드가 알려지지 않은 서비스 등으로 인한 서비스 오용, 자원 및 서비스를 불법적으로 과다하게 사용하거나 시스템에 부하를 주어 가용성을 위협하는 서비스 남용, 불충분한 인증 및 감사와 사용자에게 권한을 부적절하게 부여함으로써 발생하는 보안 체계 위협, 비인가 사용자의 접근과 보안 토큰 및 비밀번호의 재사용 등과 같은 문제로 인한 애플리케이션 위협, 에러처리 및 운영상의 실수, 불충분한 재난 복구 등으로 인한 관리 시스템 위협, 그리고 가상화 취약점을 이용한 Malware 공격 등의 가상화 위협, 이렇게 6가지 위협요소가 있다.



(그림 2) 클라우드 컴퓨팅 서비스 측면 주요 취약성

클라우드 컴퓨팅 서비스에서 뿐만 아니라 클라우드 컴퓨팅 환경 자체에서 발생할 수 있는 보안 위협들 또한 존재하는데, 이에 대해서 Gartner, CSA(Cloud Security Alliance), 그리고 ENISA(Eroupean Network and Information Security Agency)와 같은 해외 기관들에서 각각 Top Risks, Top Threats, 그리고 Top Security Risks를 발표하였다.

● Gartner: Top Risk (2008)
- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

● CSA: Top Threats (2010)
- Abuse and nefarious use of cloud
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

● ENISA: Top Security Risks (2009)
- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

위의 세 기관에서 발표한 클라우드 컴퓨팅 환경에서의 보안 취약성들을 종합하면 다음과 같은 보안 위협/위험 가능성들을 도출할 수 있다.

1) Data 분리 및 Privacy
2) 악의적 내부 사용자에 의한 특권 남용
3) 클라우드 관리 시스템 공격에 의한피해 확산
4) 인터페이스, API의 보안성 부족
5) 데이터 저장 위치에 대한 불확실성
6) 데이터 보호 및 보안
7) 데이터 복구 및 resiliency
8) 데이터 삭제의 불완전성
9) 계정 혹은 서비스 Hijacking
10) 가상화 인프라의 보안 취약점
11) 클라우드 서비스의 남용
12) 준수성(Compliance) 부재
13) 거버넌스(Governance) 부재

이와 같이 클라우드 컴퓨팅 환경에서 발생할 수 있는 보안 위협은 다차원적이므로 기존 IT환경에서의 보안 기술을 클라우드 컴퓨팅 환경에 직접적으로 적용하는데에는 그 한계가 있기 때문에, 클라우드 컴퓨팅 환경에 특화된 보안 기술의 연구가 필요하다.

3. 클라우드 컴퓨팅 보안 연구 동향

클라우드 컴퓨팅 서비스를 이용하는 사용자들은 클라우드 컴퓨팅 서버로부터 인프라(Infra as a Service), 플랫폼(Platform aS a Service), 그리고 소프트웨어(Software As a Service)를 제공받는데, 클라우드 컴퓨팅의 구성요소가 악의적인 공격을 받을 경우 사용자들은 이용하고 있는 서비스를 제공받지 못하고 사용자들의 중요 정보가 외부로 유출될 가능성이 크다. 이에 따라 국내·외의 표준제정기관, 각종 기관, 그리고 대학 연구소에서는 클라우드 컴퓨팅 보안을 위한 표준 및 기술 개발을 위한 연구를 진행하고 있다.

3.1 국내·외 클라우드 컴퓨팅 보안 표준 동향[7]

국외 표준화기관은 미국 국립표준기술연구원(NIST), CSA, 그리고 ITU-T 등이 있으며 2008년 클라우드 컴퓨팅이 부각된 이래 꾸준히 클라우드기술 및 보안기술의 표준화를 선도하고 있다.

국내의 경우 한국정보통신기술협회(TTA)를 중심으로 한국클라우드 서비스협회(KCSA), CSA 한국지부 등이 국내 클라우드 컴퓨팅 보안 표준화를 진행하고 있다.

국내·외 클라우드 컴퓨팅 보안 표준화 동향은 다음 <표 1>, <표 2>와 같다.

<표 1> 국외 클라우드 컴퓨팅 보안 표준화 동향

기관	표준명(표준번호)	제정일자
NIST	Guidelines on Security and Privacy in Public Cloud Computing (SP 800-144)	2011.12
	Guide to Security for Full Virtualization Technologies (SP 800-125)	2011.01
Cloud Security Alliance	Security Guidance for Critical Areas of Focus in Cloud Computing (V3.0)	2011.11
	Cloud Control Matrix Trusted Cloud Initiative (V1.2)	2011.08
	Trused Cloud Initiative Reference Architecture Model (V1.1)	2011.01
	Top Threats to Cloud Computing (V1.0)	2010.03
ITU-T	Cloud Security, ITU-T FG Cloud	2011.12

<표 2> 국내 클라우드 컴퓨팅 보안 표준화 동향

기관	표준명(표준번호)	제정일자
TTA	퍼스널 클라우드 컴퓨팅 개인정보보호 참조모델	개발 중
	퍼스널 클라우드 컴퓨팅의 접근제어	개발 중
	협업 클라우드 환경에서의 침입탐지 프레임워크 (TAK.KO-10.0534)	2011.12
	퍼스널 클라우드 보안 프레임워크 (TAK.KO-10.0533)	2011.12
	모바일 사용자 상황 정보 수집 및 전달 구조 (TAK.KO-10.0175)	2011.12
	공공 클라우드 컴퓨팅의 보안 및 프라이버시 보호 지침 (TAK.KO-10.0015)	2011.12
	클라우드 컴퓨팅 위협 및 요구사항 분석 (TAK.KO-10.0466)	2010.12

3.2 국내·외 클라우드 컴퓨팅 보안 기술 개발 동향

클라우드 컴퓨팅 보안 기술을 개발하고 있는 국외 기업은 Symantec, CSA Security Congress 참가 기업 등이 있으며 대학 연구소로는 Symantec, University of British Columbia, CSA Security Congress, 그리고 North Carolina State University 등이 있다. 국내의 경우 아주대학교, 고려대학교, 서울여자대학교 등의 대학 연구소와 한국인터넷진흥원, 안철수연구소 등의 기업에서 클라우드 보안 기술 및 제도의 연구를 진행하고 있다.

● Symantec(2011년)

Symantec Endpoint Protection(SEP)를 클라우드 컴퓨팅 환경과 같은 가상화 환경에 적합하게 변형하고, 다중 사용자에 의한 병목현상의 제어를 위해 클라우드를 구성하는 각 가상머신 별 백신 프로세싱 스케쥴을 조정하는 기술을 개발했다.

● University of British Columbia(2011년)

UBC에서는 동적으로 생성된 가상머신의 보안 관리 및 접근제어 시스템에 관한 연구를 진행하여 부팅 시 서비스를 위해 생성한 가상머신들을 가상머신 사용자들의 서비스 시작 전에 안전하게 삭제하여 부팅과정의 보안성을 확립하고, 서비스 수행 가상머신과 일반 사용자들의 가상머신 간 권한을 분리, 그리고 가상머신 간 통신을 수행하는 모듈에 대한 고립성 강화를 통해 가상머신 간 통신에서 사용되는 데이터 유출을 방지하는 기술을 개발했다.

● CSA Security Congress(2011년)

CSA Security Congress에서는 구글 및 트렌드마이크로 등 글로벌 업체뿐 아니라 신생 보안업체들을 포함한 총 40여개 업체들이 전시회에 참여하여 다중임차(Multi-Tendency) 환경을 고려한 ID 관리, 암호키 관리, 가상화보안, 컴플라이언스 관련 제품들을 선보였다.

● North Carolina State university(2010년)

North Carolina State University에서는 하이퍼바이저의 무결성 보장을 통한 하이퍼바이저 보안 연구를 진행하여 하이퍼바이저와 같은 레벨의 권한에서의 무결성을 테스트하고, 하이퍼바이저가 외부에 노출되지 않도록 고립된 구조를 연구했으며, 하이퍼바이저의 상태 정보에 접근 가능한 독립된 구조를 연구했다.

● 아주대학교 & 고려대학교(2012년)

아주대학교와 고려대학교에서는 클라우드 기반 분산 대용량 파일시스템 보안 연구를 통해 클라우드 컴퓨팅 환경에서 포렌식 기술을 이용하여 파일 및 자원을 복구하는 등의 관리 기술과 다양한 분산 파일 시스템에 대한 개인정보보호 기법을 연구하고 있다.

● 서울여자대학교(2010년)

한국인터넷진흥원과 연계하여 모바일 클라우드 서비스 위협을 분류/분석하고 정책적 대응 방안에 대한 연구를 진행하고 있다.

● 한국인터넷진흥원(2010년)

클라우드 보안 기술개발 사업, 클라우드 보안법, 제도 연구, 클라우드 침해사고 대응체계 구축, 클라우드 관련 보안 기술 개발, 클라우드 프라이버스 보호 등 다양한 클라우드 보안 관련 연구를 진행하고 있다.

● 안철수연구소(2009년)

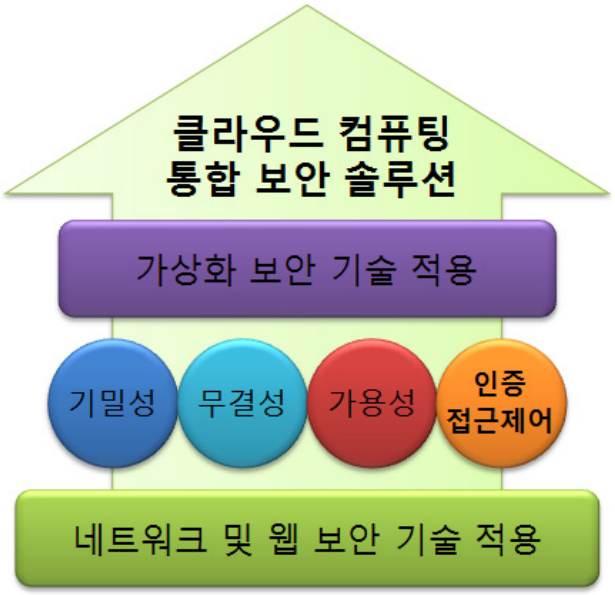
클라우드 컴퓨팅 기반 행위 분석 기술을 활용한 보안 서비스인 ACCESS(AhnLab Cloud Computing E-Security Service)를 발표했다.

4. 결론 및 향후 연구방향

본 논문에서는 클라우드 컴퓨팅 환경에서의 보안 취약성에 대한 서베이 및 클라우드 컴퓨팅 보안 기술 표준화 및 개발 동향에 대해 살펴보았다. 클라우드 컴퓨팅이 사회에 보급되는 속도에 비해 클라우드 컴퓨팅 보안관련 연구의 진행수준은 아직 미비한 수준이기 때문에, 알려진 보안 취약성에 대응하는 보안기술이 아직 확립되지 않은 단계이다. 현재상황은 악성유저 및 해커들이 클라우드 컴퓨팅 환경에 대한 공격을 시도하여 클라우드 컴퓨팅 서비스 중지 및 지연과 같은 피해를 일으킬 수 있으며, 이에 개인정보 및 기업기밀 유출과 같은 사회·경제적 피해가 발생할 수 있다.

따라서 향후에는 기존 네트워크 보안, 시스템 보안 및 응용 보안과 기술적인 부분과 클라우드 서비스, 플랫폼, 인프라 전반에 걸친 정책적인 부분을 밑바탕으로, 클라우드 컴퓨팅 보안 고려사항인 기밀성, 인증 및 접근제어, 무결성, 가용성, 가상화 보안, 그리고 네트워크 및 웹 보안을 적용하여 현재까지 밝혀진 보안 취약성에 대응할 수 있는 클라우드 컴퓨팅 통합 보안 솔루션을 개발하여 보다 안전한 클라우드 컴퓨팅 환경을 조성할 수 있도록 해야 할 것이다.

또한, 현재까지 밝혀진 보안 취약점들 외에도 많은 보안 취약점이 존재할 것이다. 이에 대응하여 클라우드 컴퓨팅 환경에 디지털 포렌식(Digital Forensic), Whitelist 기반의 네트워크 패킷 필터링 기술 등을 접목하여 차세대 클라우드 컴퓨팅 보안 위협요소에도 대비해야 한다.



(그림 3) 클라우드 컴퓨팅 통합 보안 솔루션 구성

참고문헌

[1] Asia Pacific End-User Cloud Computing Servey, IDC, 2009

[2] Cloud Computing Security - Trends and Research Directions, Sengupta, S.; Kaulgud, V.; Sharma, V.S., 2011 IEEE World Congress on Digital Object Identifier, 2011, pp 524-531

[3] Security and Privacy in Cloud Computing, Xiao, Z.; Xiao, Y., Communications Surveys & Tutorials IEEE, 2012, pp 1-17

[4] 모바일 클라우드 서비스 보안 침해 대응방안, 한국인터넷진흥원, 2010

[5] 클라우드 서비스 보안 위협 및 보안대책, 한국인터넷진흥원, 2011

[6] 클라우드 서비스 정보보호 안내서, 방송통신위원회; 한국인터넷진흥원 2011

[7] PD 이슈리포트 12-6호, 클라우드 컴퓨팅 보안 기술동향과 산업전망, 2012

[8] 클라우드 컴퓨팅 보안 기술 동향, 김태형, 한국정보과학회지, 특집원고1, 2012, pp 30-38