클라우드 컴퓨팅 서비스 침해사례 분석 및 정보보안 기술 동향

July 2013

박진호, 이재휘

경북대학교 컴퓨터학부

요 약

Hypervisor의 발전으로 가상화 기술이 흔해졌고 이에 따라 네트워크와 가상화를 합쳐 클라우드 시스템이 발전하기 시작했다. 아직은 클라우드 시스템 구축이 초기 단계에 머물고 있어 대부분의 서비스가 스토리지 제공 정도의 역할을 하고 있지만, 점진적인 시스템 구축으로 멀지 않은 미래에 진정한 클라우드 컴퓨팅 시대가 열릴 것이다. 이에 따라 점점 클라우드라는 원격 서버에 대한 의존도가 높아지게 되면서 수 많은 정보가 하나의 서버에 존재하게 될 것이므로 고려해야 될 보안 요구사항 또한 높아질 수 밖에 없는 것은 당연한 일이다. 본 고에서는 국내외에서 발생한 클라우드 관련 침해사고 사례들과 클라우드 서비스의 활성화에 따른 클라우드 컴퓨팅 환경에서의 보안 기술 동향에 대해 소개하고, 관련 정보보호 정책 수립에 대하여 기술하고자 한다.

Table of Contents

1. 서론

클라우드 서비스는 더 이상 일반인들에게 전문적이고 어려운 용어가 아니다. 클라우드 서비스 시장의 규모는 스마트 기기 보급 확산에 따라, 스마트워크, 모바일 오피스 환경 구축이 본격화됨에 따라 점점 커지고 있다. 최근에는 많은 포털 회사들이 클라우드 서비스의 준비 단계로 클라우드 스토리지 서버를 구축하고 있으며, 전 세계 가상 머신의 수는 2011년 2억 대에서 2015년 까지 5배 이상 증가할 것으로 전망된다. 현재 일반 각 사용자들이 널리 이용하고 있는 클라우드 하드디스크 서비스는 사용자가 각 클라우드 서비스 제공자가 제공하는 서비스를 독립적으로 이용하는 비교적 단순한 구조이지만 여러 사용자들의 서비스를 연동하여 제공하는 형태로 발전 될 전망이다. 현재 서비스 중인 클라우드 스토리지 서버에는 많은 양의 데이터가 쌓이고 있으며 앞으로도 계속 정보의 양은 증가할 것으로 보인다. 이러한 환경에서는 하나의 클라우드 서버에 대한 공격으로도 막대한 양의 데이터를 얻어낼 수 있게 되므로 강력한 보안이 요구된다.

클라우드 컴퓨팅 및 서비스 보안에 대한 연구는 시작단계에 있으며, 국외에서도 클라우드 보안 요구사항들에 대응하는 기술적, 관리적 대응방안들에 대한 연구가 진행되고 있어 우리나라도 클라우드 컴퓨팅 보안 관련 기술 개발과 함께 표준 및 규정 제정이 필요하다. 본 고에서는 국내외에서 발생한 클라우드 관련 침해사고 사례들과 클라우드 서비스의 활성화에 따른 클라우드 컴퓨팅 환경에서의 보안 기술 동향에 대한 소개를 하고, 관련 정보보호 정책 수립에 대하여 기술할 것이다.

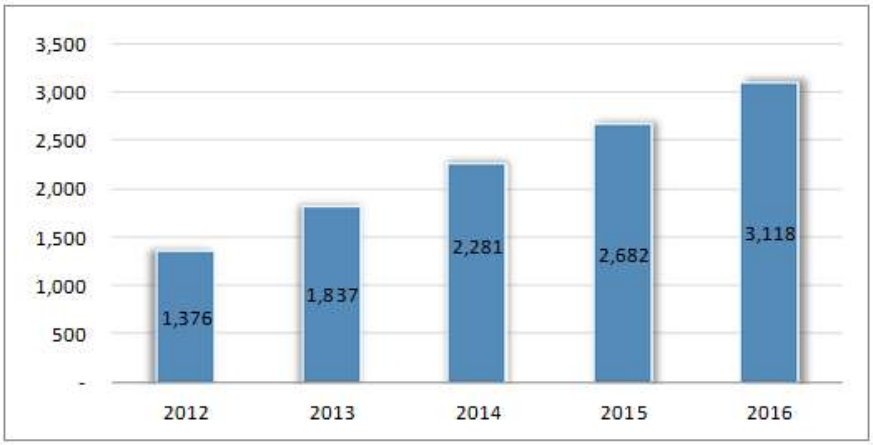

그림 1. 국내 클라우드 환경 지원을 위한 스토리지 솔루션 시장 전망

2. 클라우드 컴퓨팅 서비스 상의 침해사례

2.1. 가상화 시스템의 보안 공격

가상화 기술을 통해 이용자의 가상 머신들이 상호 연결되어 있기 때문에 다양한 공격 경로가 존재한다. 그림2를 보면 하나의 hypervisor가 zero-day 공격에 의해 감염되면 해당 hypervisor 상에서 작동하고 있는 가상 머신들 또한 악성코드에 감염되어 사고 범위가 확산될 수 있다. Hypervisor를 직접 공격하는 방법인 경우에는 클라우드 서버 내의 가상 머신 간의 도청 및 해킹도 가능하게 된다.

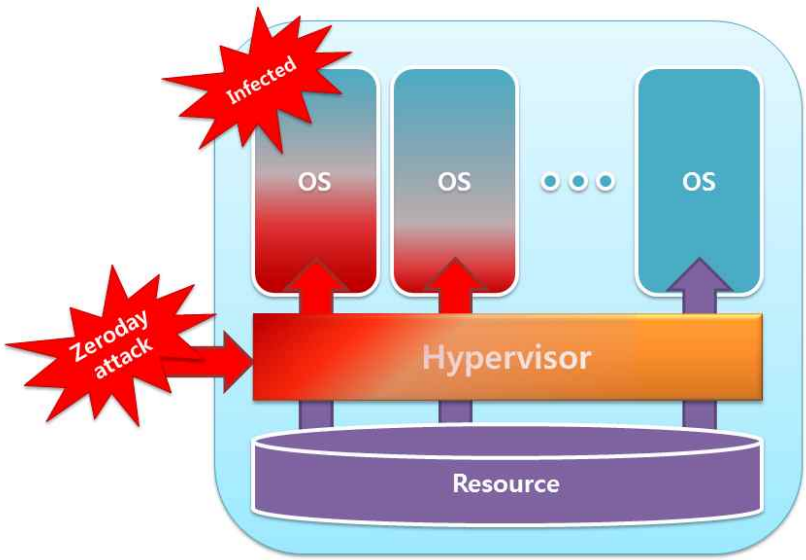

그림 2. Hypervisor 감염에 의한 감염 확산

2.2 자원의 공유 및 집중화

물리적 자원의 공유 및 집중화로 물리적 자원에 장애 발생 시 해당 자원을 공유하는 모든 사용자의 서비스가 중단될 수 있는 위협이 존재한다. 서버가 가지고 있는 물리적 자원의 양보다 더 많은 양의 요청이 들어오는 경우, 서버가 클라이언트에 자원을 제때 할당해 주지 못하게 되어 서비스가 제대로 이루어 지지 않게 되어 물리적 자원 분배 장애가 발생한다. 그림3을 보면 서버가 가진 물리적 자원의 양은 100이지만 수많은 사용자가 동시에 10의 자원을 요청하여 요청 받은 총 자원양이 100을 넘어가고 있다. 그로 인해 자원 분배에 장애가 발생하게 되고 정상적인 서비스가 불가능하게 된다.

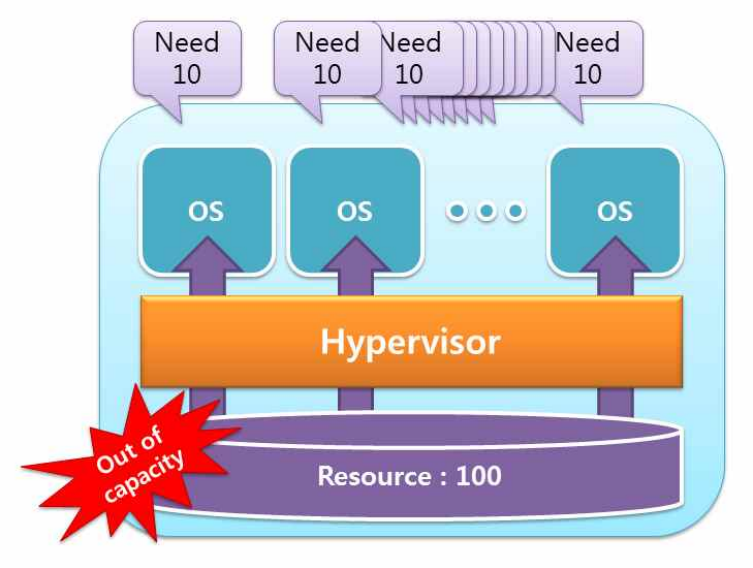

그림 3. 수용 능력 이상의 자원 요청

2.3 데이터 접근제어의 어려움

데이터 저장 및 관리의 측면으로는 정보의 위탁관리로 인해 이용자의 정보가 복사, 이동, 수정 되어도 이용자가 확인이 불가능하며 서비스 제공사의 내부자에 의한 정보 유출 가능성이 존재한다. PC, 스마트 폰, 스마트 TV 등 다양한 단말의 접속을 허용하기 때문에 각각의 단말이 갖는 보안 위협을 그대로 상속한다. 특히 모바일 단말의 경우 특성상 분실 시 이용자의 정보가 유출될 가능성이 크다. 사용자의 인증 및 접근제어 측면으로는 대용량 데이터가 분산 파일 시스템을 통해 많은 서버들에 분산 저장/관리 됨에 따라 데이터 암호화, 이용자 인증, 접근제어 등의 어려움이 증가한다.

유형	내용	사례
가상화 시스템의 위협	시스템 및 가상화의 측면으로는 하나의 hypervisor가 악성코드에 감염되면 동일한 hypervisor 상에서 작동하고 있는 가상 머신들에 의해 악성코드 감염의 범위가 확산	2009 국내 년 6월 영국의 한 클라우드 서비스가 사용하는 가상 머신 관리 소프트웨어의 취약점을 이용한 공격을 통해 관리자 권한을 획득한 후 10만 고객의 정보를 삭제
자원의 공유 및 집중화	물리적 자원의 공유 및 집중화로 장애 발생 시 해당 자원을 공유하는 모든 사용자의 서비스가 중단	2008년 여름 아마존의 클라우드 서버가 인증요청 쇄도로 인하여 7~8시간 동안 서비스 장애가 발생해 일시적으로 서비스가 중단
데이터 접근제어의 어려움	대용량 데이터가 분산 파일 시스템을 통해 많은 서버들에 분산 저장/관리 됨에 따라 데이터 암호화, 이용자 인증, 접근제어 등 관리의 어려움이 증가	2010년 12월, MS의 서비스 환경설정 오류로 클라우드 상의 기업정보가 타입에게 열람

표 1. 침해사고 유형별 사례

2.4 침해사례로 본 새로운 대안의 필요성

기존 보안 장비는 물리 컴퓨터 내부에서 네트워크 패킷을 감시하여 공격을 탐지하지만, 클라우드 시스템 내부에서 발생되는 공격은 hypervisor와 같은 새로운 계층이 추가되어 있어 공격 탐지에 어려움이 있다. Rookt kit과 같은 악성 프로그램을 hypervisor 영역에 설치하는 경우 가상화 시스템의 kernel 영역보다 더 높은 권한을

갖기 때문에 가상 머신 상의 유저 영역에서 동작하는 백신은 소용이 없다.

클라우드 환경에서는 유저가 사용하는 가상 머신이 이미지 파일 형태로 존재하므로 간단히 생성, 이동, 삭제가 가능하다. 그러므로 새로운 가상 머신을 생성하거나 이전의 이미지를 복구하는 등의 빈번한 자원변동이 발생하게 되며 이에 따른 보안 정책 적용이 어렵다.

공격 경로 역시 물리 컴퓨터와는 달리 다양하게 존재하는 만큼 보안에 투자해야 하는 시간과 노력이 상당하며, 수많은 사용자의 가상 머신이 하나의 클라우드 시스템 상에 존재하므로 작은 실수가 서비스 전체를 마비시키는 큰 재해로 되돌아 올 수도 있다.

기존의 보안 기술들은 클라우드 환경의 보안 위협에 대응하기에는 가상화 기술의 구조적 특성을 인식하지 못하는 한계가 있으므로 클라우드 컴퓨팅 환경에 적합한 새로운 보안 기술을 개발할 필요가 있다.

3. 보안 기술 동향

클라우드 시스템 환경에 적합한 새로운 보안 기술을 개발하기 위한 국내외적 연구가 계속 진행되고 있는 중이다.

3.1. 가상화 시스템의 위협

스탠포드 대학에서는 2003년 클라우드 시스템의 구조적 특성을 고려해 호스트 외부에서 호스트에 대한 공격 탐지를 하는 기법을 연구했다. 모니터링 하는 호스트는 가상 머신 상에서 동작시키고, 가상 머신 모니터를 통해 가상 머신 내부 상태를 분석하는 기법을 연구했다.

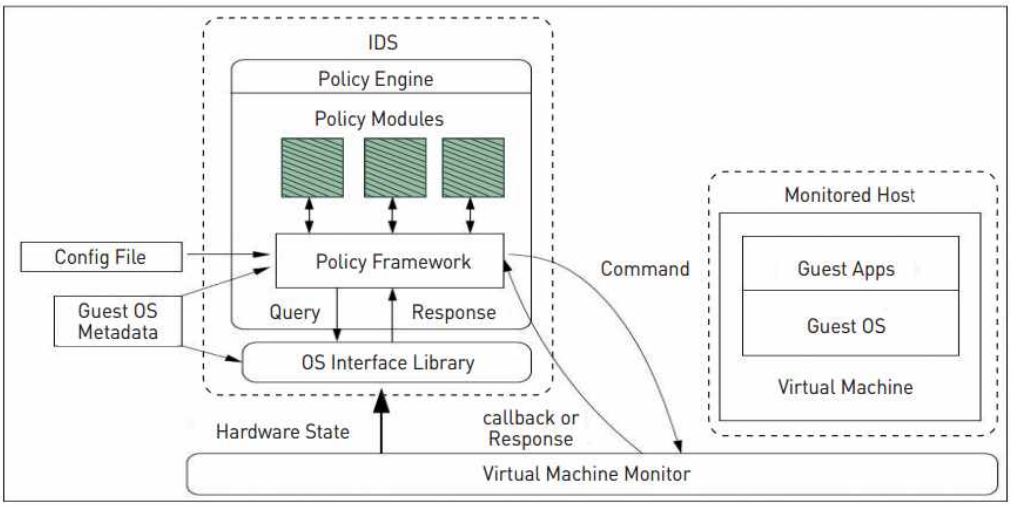

그림 4. 가상 머신 내부 상태 분석(VMI) 기반 IDS 구조

3.2. 자원의 공유 및 집중화

한 연구진은 클라우드 컴퓨팅 환경에서의 DDoS 공격이 발생한 상황에 대한 대비책을 연구했다. 그림5를 보면 front-end 클라우드 서버 밑으로 세 대의 가상 머신이 작동 중이다. Front-end는 하위 가상 머신들을 관리하는 hypervisor 역할로 자원 관리 등을 담당한다. Front-end 하위의 각 가상 머신의 내부에는 개별적으로 IDS가 작동하고 있으며, 공격을 평가하는 attack assessment는 front-end 내부에 존재한다.

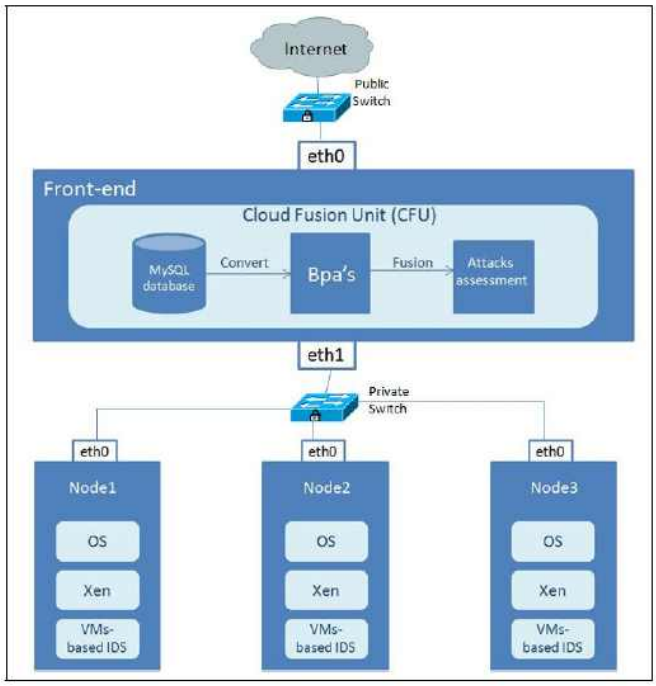

그림 5. IDS Cloud Topology

하위 가상 머신 내부의 IDS가 공격을 탐지하면 front-end에 존재하는 MySQL 데이터베이스에 해당 유형을 저장한다. 저장된 유형들은 Basic Probabilities Assignments(BPA)로 사용된다. BPA는 front-end 내부에 존재하는 Bpa's에서 공격인지 아닌지를 판별할 때 사용한다. Bpa's에서의 공격 탐지를 위해 DST operation을 사용하며, 지나간 TCP, UDP 그리고 ICMP를 분석해 사용한다.

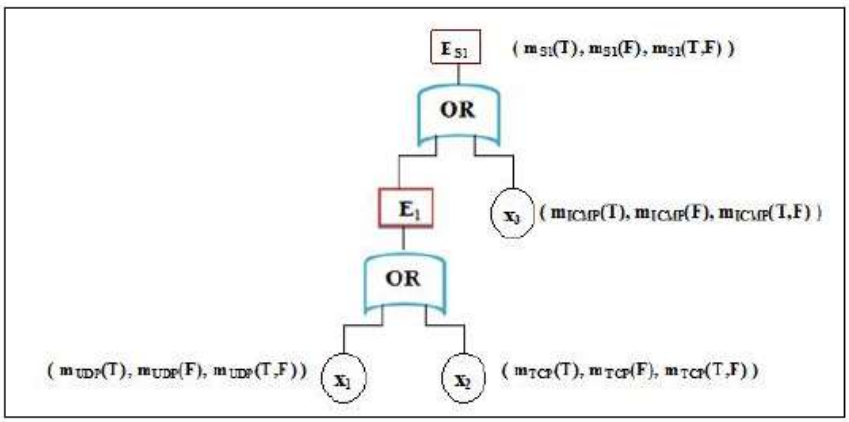

그림 6. BPA's 계산

3.3. 데이터 접근제어의 어려움

International Islamic University에서는 수많은 서비스가 각각 다른 사용 권한을 가지고 있는 클라우드 시스템에서의 사용자 인증과 자원에 대한 접근을 제어하는 기술을 연구했다. 그림7을 보면 클라우드 서비스 사용자와 직접적으로 접하게 되는 Identity Matrix(IMx)를 중심으로 사용자들이 저장한 중요한 정보들이 저장된 knowledge warehouse와 각 정보들의 권한과 인증 등이 저장된 International Regulatory Body(IRB)가 연결되어 있다.

ID카드와 여권 번호 등의 정보를 사용자가 저장하게 되면 해당 정보들은 IRB에 의해 검증된다. 검증이 완료되면 IMx는 자동적으로 해당 사용자의 정보를 knowledge warehouse에 저장하게 된다. 그리고 IMx에서는 접속중인 모든 사용자의 행위가 감시된다.

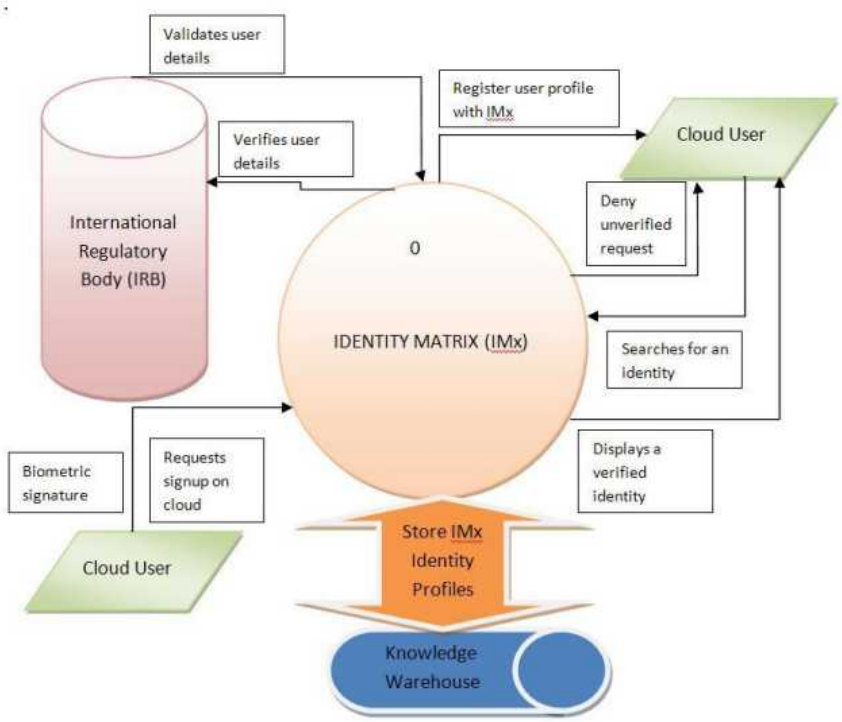

그림 7. 데이터 접근제어를 위한 diagram

3.3. 보안기술 고려사항

클라우드 시스템의 보안 기술 별 고려사항은 기밀성과 데이터 암호화로는 기본적으로 암호화 기술이 제공되어야 하며 클라우드 시스템에서 대용량 데이터의 암호화 시 가용성이 떨어질 가능성이 있으므로 적절한 암호화 알고리즘을 찾아야 할 필요가 있다. 암호 키를 저장하고 있는 서버에서 사고가 발생하는 경우 많은 사용자들의 데이터가 접근 불가능해지므로 키 관리 방안에 대해서도 대책을 세워야 한다.

프로토콜에 대한 다양한 케이스 별 검증이 필요하고 클라우드 시스템에서 저장되는 데이터와 교환되는 메시지에 대한 오류검사 또한 필요하다. 클라우드 시스템이 공격받거나 과부하가 걸려 서비스가 중단되거나 데이터의 영구적 손실들이 발생하는 경우를 막기 위해서 고장 감내성 및 데이터 복구 기법이 필요하다. 클라우드 시스템 상에서 발생하는 공격 코드는 원격으로 실행되는 경우가 많으므로 원격 확인, 특히 소프트웨어에 대한 바이너리 레벨에서의 분석이 매우 중요하다. 가상 머신 상에서 프로그램의 실행 영역 및 메모리를 보호하기 위해 샌드박스와 같은 기술들을 적용하는 것도 연구해야 한다.

4. 정책 동향

미국은 연방정부 및 산하기관에 클라우드 시스템 도입을 촉구하고 있다. 연방정부 및 산하기관의 클라우드 우선 도입 촉구를 위해 각 기관의 CIO에게 3개 서비스를 지정해 클라우드 솔루션으로 이관 계획을 세울 것을 지시했다. 최소 1개 서비스는 반드시 12개월 내에 이관 완료해야 하며, 나머지 2개 서비스도 18개월 내에 이관할 것을 지시했다. 그리고 RedRAMP(Federal Risk and Authorization Management Program)이라는 클라우드 서비스에 대한 보안성을 검증하는 클라우드 보안 인증제도를 도입하였다. FedRAMP를 통과한 서비스는 별도의 인증절차 없이 정부기관에 도입이 가능하다. FedRAMP는 연방정부가 이용하는 클라우드 컴퓨팅 서비스의 보안 요건, 지속적인 모니터링, 승인 및 인가 절차 등을 기술한다.

국내의 클라우드 정책 동향으로는 세계 최고수준의 클라우드 컴퓨팅 강국 실현을 목표로 세부 추진과제를 제시했다. 공공부문 선제도입을 통하여 범정부 클라우드 인프라를 구축하고 범정부 클라우드 플랫폼을 도입한다. 민간 클라우드 서비스 기반을 마련하기 위해 클라우드 서비스 모델을 발굴하고 클라우드 컴퓨팅 테스트베드를 구축한다. 구축된 민간 클라우드 서비스의 공경 활용을 촉진한다.

클라우드 서비스의 활성화를 위해서는 클라우드 컴퓨팅 도입 법 제도를 개선하고 신뢰성 및 안정성 제고를 위한 보안 및 인증체계를 구축해야 한다. 정부차원에서 클라우드 컴퓨팅의 표준화를 추진해야 한다.

5. 결론

새로운 IT 이슈로 자리잡은 클라우드 컴퓨팅은 아직까지는 풀어야 할 과제들이 많이 남아 있다. 그 중 정보보안과 관련된 기술들의 미비는 클라우드 컴퓨팅의 확산 속도를 낮추게 될 것으로 예상된다. 컴퓨터가 많은 비중을 차지하는 정보화시대인 만큼 클라우드 컴퓨팅 환경에서의 정보보안 침해사고는 이 사회에 미치는 영향이 클 것이라 보기 때문이다.

클라우드 컴퓨팅이 사회에 안정적으로 자리잡았을 때 기술적, 관리적 대응방안의 미비로 뒤쳐지지 않도록 우리나라도 클라우드 컴퓨팅 보안 관련 기술 개발과 함께 표준 및 규정 제정이 필요하다.

6. 참고문헌

[1] AhnLab 보안세상 http://blogsabo.ahnlab.com.
[2] ITWORLD http://www.itworld.co.kr
[3] DailySecu http:// www.dailysecu.com
[4] "클라우드 컴퓨팅 보안 기술", 한국전자통신연구원 전자통신동향분석 제 24 권 제 4 호 2009 년 8 월
http://ettrends.etri.re.kr/PDFData/24-4_079_088.pdf
[5] "클라우드 컴퓨팅 보안 기술동향과 산업전망", KEIT 2012 년 7 월
http://ants.mju.ac.kr/2012Fall/cloud2
[6] "클라우드 컴퓨팅 보안 동향과 통찰", IBM Corporation 2013
http://www.codegate.org/renew/_file/board/dr_6476251.pdf
[7] "안전한 클라우드 서비스 제공, 이용을 위한 보안 고려사항", CLOUDSEC 2012
http://www.cloudsec.co.kr/event/pdf/cloudsec2012_04.pdf
[8] 보안인닷컴 http://boanin.tistory.com
[9] "Cloud computing security", Wikipedia http://en.wikipedia.org/wiki/Cloud_computing_security
[10] "Cloud computing", Wikipedia http://en.wikipedia.org/wiki/Cloud_computing
[11] "Conceptual Cloud Computing Employing Identity Matrix and Knowledge Warehouse", September 2012
http://www.sersc.org/journals/IJEL/vol1_no2/4.pdf
[12] "Detecting DDoS Attacks in Cloud Computing Environment", ISSN 1841-9836, February 2013
http://univagora.ro/jour/index.php/ijccc/article/download/170/pdf_14

[그림 1] 한국 IDC, 국내 클라우드 스토리지 솔루션 시장 2016 년까지 연평균 29.7% 성장 전망
http://www.idckorea.com/product/Getdoc.asp?idx=540&field=PressRelease
[그림 4] 가상머신 내부 상태 분석(VMI) 기반 IDS 구조. http://ants.mju.ac.kr/2012Fall/cloud2
[그림 5] IDS Cloud Topology
http://univagora.ro/jour/index.php/ijccc/article/download/170/pdf_14
[그림 6] BPA's 계산 http://univagora.ro/jour/index.php/ijccc/article/download/170/pdf_14
[그림 7] 데이터 접근제어를 위한 diagram http://www.sersc.org/journals/IJEL/vol1_no2/4.pdf