클라우드 컴퓨팅 환경에서 취약점에 따른 보안 요구사항 분석

박민우*, 김남욱*, 조신영*, 엄정호*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:mwpark@imtl.skku.ac.kr

An Analysis of Security Requirement Based on Vulnerabilities in Cloud Computing System

Min-Woo Park*, Nam-Uk Kim*, Sinyoung Cho*, Jung-Ho Eom*,
Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information Communication Engineering,
Sungkyunkwan University

요 약

본 논문은 클라우드 컴퓨팅 시스템의 필수적인 보안 요구사항에 대해 분석한다. 클라우드 컴퓨팅은 수 많은 자료와 방대한 자원을 다루는 시스템이다. 클라우드 컴퓨팅은 이와 같은 특징으로 인해 쉽게 해커의 공격 대상이 된다. 따라서 클라우드 컴퓨팅 산업에서는 무엇보다도 보안이 매우 중요한 요소이다. 본 논문에서는 잠재적인 위협으로부터 클라우드 컴퓨팅이 보유한 자료와 자원을 보호하기 위한 필수적인 보안 요구사항에 대해 분석한다.

1. 서론

클라우드 컴퓨팅은 대규모 분산 컴퓨팅 장치를 가상화하여 ISP 고객의 요구에 맞춰 컴퓨팅 자원, 플랫폼 서비스, 어플리케이션 등을 네트워크를 통해 인터넷 서비스를 동적으로 제공하는 새로운 컴퓨팅 패러다임이다[1, 2]. 최근에는 무선 통신 발달과 스마트폰 등장으로 시간과 장소에 구해 받지 않고 인터넷에 접속할 수 있게 되면서 클라우드 컴퓨팅 산업을 촉진시키고 있다. 클라우드 컴퓨팅은 다음과 같은 장점들로 인해 최근 이슈가 되고 있다. 첫째, 클라우드 컴퓨팅 서비스를 이용할 경우, 보다 적은 비용으로 초기 IT 체계를 구축할 수 있고 향상된 성능으로 컴퓨터 자원을 사용할 수 있어서 경제적이다. 둘째, 인터넷에 연결된 장치들을 이용하여 서비스를 받을 수 있기 때문에 서비스 이용 측면에서 편리하다.

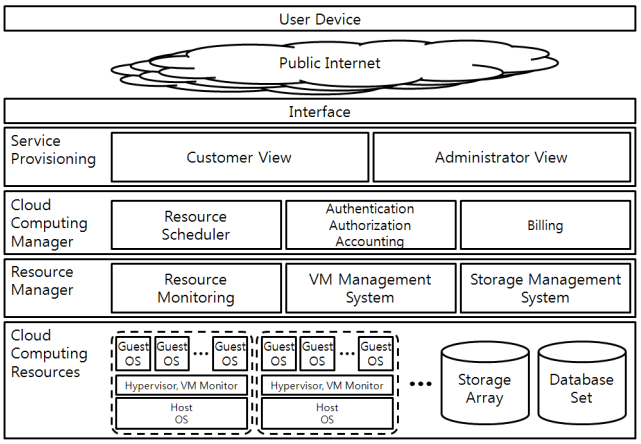
클라우드 컴퓨팅 시스템은 가상화된 자원들을 인터넷 상에서 서비스 형태로 제공되면서 컴퓨터의 자원을 다수의 사용자와 공유하여 높은 자원 효율성을 달성할 수 있지만, 이를 이용하는 사용자 측면에서는 자신의 정보와 데이터를 신뢰할 수 없는 제 3자와 함께 사용하는 시스템에 위탁해야 하는 위험 부담을 갖게 된다. 또한, 클라우드 컴퓨팅 시스템은 많은 자원을 보유하고 있으며, 방대한 사용자의 정보를 저장하고 있어 해커들에게 주 공격 대상이 되기 쉽다. 따라서 기존의 컴퓨팅 환경에서 클라우드 컴퓨팅 환경으로 전환되면서 해결해야 할 문제 중에 대표적인 것이 보안 문제이다. 본 논문에서는 클라우드 컴퓨팅 환경에서 다양한 관리 장치들이 복잡하게 연계하여 동작하는 가운데 업무처리 과정에서 다양한 취약점이 발생한다. 이에 따른 보안 취약점을 바탕으로 잠재적인 위협을 방지하기 위해서 기술적인 보안 요구사항을 제안한다.

본 논문의 구성은 2장에서 일반적인 클라우드 컴퓨팅 환경에 대해 설명하고 3장에서는 클라우드 컴퓨팅 환경에서 사용되는 자원에 대해 간략하게 언급한다. 4장에서는 클라우드 컴퓨팅 환경에서의 보안 취약점을 설명하고 5장에서는 본 논문에서 제안하는 보안 요구사항을 제안한다. 마지막으로 6장에서는 결론을 맺는다.

2. 클라우드 컴퓨팅 구조

현재 클라우드 컴퓨팅 환경은 실제 서비스를 제공하고 있는 기업에 의해 독자적으로 구축되어 있어 그 구성 요소나 형태가 각기 다양하다. 일례로 현재 적극적으로 클라우드 컴퓨팅 산업을 주도하고 있는 글로벌 기업 Google(구글)이나 Amazon(아마존)의 경우 각각 독자적인 분산 데이터 관리 시스템을 구축하여 사용하고 있다. 분산 데이터 관리 시스템은 분산 환경에서 정보 저장 및 저장된 정보를 대상으로 질의 서비스를 수행하기 위한 시스템으로 구글과 아마존은 각각 독자적인 Bigtable과 Dynamo 시스템을 구축하여 사용하고 있다[3].

본 장에서는 클라우드 컴퓨팅 서비스를 제공하기 위한 최소한의 구성 요소를 정의하고 그의 기능에 대해 설명한다. (그림 1)은 클라우드 컴퓨팅 환경을 일반화한 것으로 4 개의 계층으로 이루어진다.



(그림 1)

서비스 프로비저닝 계층은 사용자의 요청이나 관리자의 요청을 접수하여 서비스를 제공할 수 있도록 지원하는 계층이다. 서비스 프로비저닝 계층은 서비스를 요청하는 대상에 따라 고객 뷰와 관리자 뷰로 구분할 수 있다.

클라우드 컴퓨팅 매니저 계층은 사용자를 인증하거나 자원을 할당하고, 사용자의 시스템 이용 내역을 기록하는 업무를 처리하는 계층으로, 자원 스케쥴러, AAA, 과금 모듈으로 구성된다.

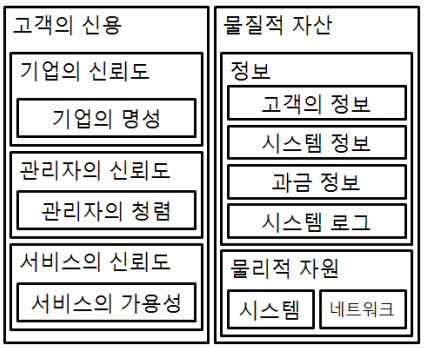
자원 관리 계층은 클라우드 컴퓨팅의 자원과 저장된 데이터를 관리하기 위한 계층으로, 자원 모니터링, VM 관리 시스템, 저장소 관리 시스템으로 구성된다.

클라우드 컴퓨팅 자원 계층은 클라우드를 구성하는 물리적인 시스템 자원들을 의미한다. 일반적인 컴퓨팅 장치들로 이루어진 컴퓨팅 자원과 저장소의 집합으로 이루어진 저장소 배열이나 데이터베이스 집합으로 구성된다.

3. 클라우드 컴퓨팅 자산

클라우드 컴퓨팅 환경은 다수의 사용자에게 인터넷 서비스를 제공하는 패러다임으로 사용자나 기업의 관점에서 다양한 자산이 발생한다[4, 5]. (그림 2)는 클라우드 컴퓨팅의 자산을 나타낸 것이다.

- 기업의 신뢰도: 사용자로부터 개인의 정보를 위탁받는 형태의 서비스 중에 가장 중요한 자산으로 보안사고가 발생할 경우 고객들로부터 기업의 신뢰를 잃게 된다.
- 관리자의 신뢰도: 고객의 자원을 취급하고 전체 시스템을 관리하는 관리자에 대한 신뢰가 형성될 때 비로소 고객은 안심하고 시스템을 이용한다.
- 서비스의 신뢰도: 서비스의 가용성. 즉, 언제 어디서든지 사용자가 서비스를 요청할 때 즉시 요구한 서비스를 신속 정확하게 제공해야 한다.
- 고객의 정보: 고객의 신원정보나 개인정보, 서비스를 이용하면서 생산, 가공, 저장 되는 고객의 각종 정보 등이 클라우드 컴퓨팅 시스템 내에 유통되거나 저장되는데 이는 중요한 자산이다.
- 시스템 정보: 클라우드 컴퓨팅 시스템을 동작하기 위해 필요한 정책, 관리 장치들의 설정 정보 등도 중요한 자산의 하나이다.
- 과금 정보: 고객의 신용정보나 과금의 근거가 되는 시스템 사용량 등에 대한 저장 정보로 유출·변조될 시 치명적이다.
- 물리적 하드웨어: 클라우드 컴퓨터를 구성하는 다수의 컴퓨팅 장치로 서버나 저장장치 등이 이에 해당한다.
- 네트워크: 클라우드 컴퓨터는 인터넷을 통해 서비스를 제공하기 때문에 충분한 네트워크 자원이 필요하다. 네트워크의 자원이 고갈될 경우 서비스나 기업의 신뢰도에 심각한 영향을 끼칠 수 있다.
- 어플리케이션: 서비스 제공자의 어플리케이션 소스 코드는 클라우드 컴퓨팅 시스템에 저장된 중요한 지적 자산이다.
- 로그: 시스템 동작 과정에서 발생하는 로그나 보안 관련 로그들이 저장된다.



(그림 2) 클라우드 컴퓨팅 자산

4. 클라우드 컴퓨팅 보안 요구사항

본 장에서는 클라우드 컴퓨팅의 자산과 취약점으로 인해 발생할 수 있는 잠재적인 위협을 방지하기 위해 클라우드 컴퓨팅의 특징에 따라 새로운 상황에 적용될 수 있는 보안 요구사항을 제안한다.

- AAA Security(RQ1): 기존의 아이디와 비밀번호를 통해 사용자를 인증하는 수단은 정적인 비밀정보를 사용하기 때문에 비밀번호가 노출되면 악의적인 사용자가 부정한 인증 과정을 저지를 수 있다. 따라서 One-Time Password와 같이 시간에 따라 비밀번호가 변경되는 동적인 비밀정보를 인증에 적용함으로써 부정한 사용자가 다

른 사용자의 명의로 인증 과정을 통과하는 행위를 막을 수 있다. 특히, 시스템 동작에 치명적인 영향을 끼칠 수 있는 관리자의 인증 과정은 OTP와 같은 강력한 고등 인증기술을 적용해야 한다. 사용자 인증 과정이 정확하게 이루어져 정당한 사용자가 시스템에 접근할 경우 AAA 장치가 해커에 의해 제어권을 빼앗긴 경우를 제외하면, 권한 인증이나 과금 과정은 항상 정확하게 동작한다.

• User Provisioning/De-provisioning Security(RQ2): 사용자 계정의 생성·삭제 및 계정 정보의 수정 과정에 필요한 사용자의 신원 확인을 믿을 수 있는 기관에서 발급한 공인인증서나 사용자 명의의 휴대전화, 오프라인 확인 등 제 3자가 거짓으로 사용자 확인 과정에 참여할 수 없으며, 믿을 수 있는 기관에서 사용자에 대해 공증해 주는 정보를 통해 수행하면 안전하다. 또한 위와 같이 사용자 확인 과정에서 송·수신 되는 정보가 공격자에게 노출되지 않도록 사용자 확인 과정을 암호화하여야 한다.

• Remote Access Security for Management(RQ3): SSH, SSL, IPSec과 같은 보안 프로토콜을 이용하는 VPN을 통하여 원격 제어를 수행하면, 부정한 사용자가 원격 제어 과정에 참여하는 것을 막을 수 있다. 또한, 세션의 정보가 암호화 되어 부정한 사용자가 다른 사용자와 사업자간의 통신에 참여할 수 없으며, 원격 제어 과정에서 송·수신 되는 정보를 훔쳐볼 수 없다.

• Access Management(RQ4): 시스템 자원에 대한 사용자의 접근 제어가 정확하게 이루어지기 위해서는 먼저, 자원의 명확한 구분과 사용자에 대한 정확한 인증이 이루어져야 한다. 이러한 보안 요구사항은 위의 RQ1과 아래 RQ5 RQ6에서 설명한다. 명확하게 구분된 자원에 대한 사용자의 접근 제어는 Role Based Access Control(RBAC)을 통해 가능하다. 각 사용자는 이용하고자 하는 서비스에 따라 역할을 활성화하며, 이 때 활성화 된 역할에 따라 AAA 모듈이 자원에 대한 접근 여부를 허가한다. 따라서 보안 요구사항 RQ1, RQ5, RQ6이 만족하는 경우 RBAC을 통해 정확한 접근 제어를 수행할 수 있다.

• Hypervisor Security(RQ5): 악의적인 사용자에 의한 하이퍼바이저의 오동작이나 하이퍼바이저 자체의 문제로 인해 자원이 명확하게 구분 되지 않을 수 있다. 악의적인 사용자에 의한 하이퍼바이저의 오동작을 막기 위해서는 하이퍼바이저가 동작하는 Host 레벨에서 침입탐지 시스템을 설치하여 Host내에 악의적인 사용자의 활동을 조기에 발견하고 차단하는 방법이 있다. 하이퍼바이저 자체의 문제로 인해 오동작이 일어날 수 있으며, 이를 예방하기 위해서는 하이퍼바이저의 업데이트를 주기적으로 확인하고 수행하는 방법이 있다[6,7,8,9].

• Perfect Resource Isolation(RQ6): 자원의 직접적인 할당은 보안 요구사항 RQ4, RQ5를 통해 안전하게 수행할 수 있다. 하지만 전체 시스템에 공통적으로 동작하는 어플리케이션에 존재하는 취약성으로 인해 부정한 사용자가 다른 사용자의 정보 침해를 막기 위해서는 어플리케이션의 취약성을 보완하기 위한 업데이트를 정기적으로 수행하고, 문제가 될 수 있는 요청을 사전에 검사하여 어플리케이션에 전달되는 것을 막는 방법이 있다. 대표적으로 문제가 되는 어플리케이션으로는 SQL 등이 있다.

• Secure Communication(RQ7): 사용자와 시스템 간의 통신은 공개된 인터넷을 통해 수행되기 때문에 통신의 기밀성과 무결성을 보장하기 위한 암호화가 요구된다. 기밀성의 위한 암호화 방법으로는 DES, AES, IDEA와 같은 표준 암호 알고리즘을 사용하여 평문을 암호화 하거나, SSL이나 IPSec과 같은 보안 프로토콜을 사용하는 방법이 있다.

• Encryption of Data(RQ8): 클라우드 컴퓨팅 시스템에서 주요 통신 메시지나 저장되는 데이터는 반드시 표준 암호화 알고리즘을 이용하여 암호화한 뒤에 저장하며, 메모리에 로드될 때에는 필요한 부분만 복호화하여 메모리에 로드한다. 이때 메모리에 머무는 시간은 최소한으로 하며, 사용이 끝난 즉시 NULL로 메모리값을 치환한다. 이와 같은 방법은 매번 메모리에 접근 시 마다 복호화와 메모리에 로드하는 과정을 거쳐야 하기 때문에 연산 과정이 효율적이지 못하다. 따라서 사용자에게 메모리에 정보를 유지하는 시간을 조절할 수 있도록 함으로써 연산 효율과 정보의 기밀성의 trade-off를 선택할 수 있도록 한다.

• Secure Key Generation & Management (RQ9): 클라우드 컴퓨팅 환경에서는 사용자 인증, 정보 암호화, 통신 암호화 등 다양한 영역에서 키(key)를 사용한다. 난수를 이용한 안전한 키 생성과 Key Recovery Mechanism을 구축하여 키의 유실 시 암호화된 정보가 소실되는 것을 막는다. 키는 사용자의 선택에 따라 사용하며 ISAKMP나 PKI와 같은 표준 키 분배 알고리즘을 통해 분배한다.

• Resource Management(RQ10): 실질적으로 Virtual Machine에 자원을 할당하는 것은 보안 요구사항 RQ5를 통해 안전하게 이루어진다. 이때 충분히 안전하게 자원이 할당되더라도, 다수의 사용자에게 자원 할당, 해제하는 과정에서 자원 할당 단위가 불명확할 경우 자원의 누수가 발생할 수 있다. 따라서 관리자에 의해 자원의 최소 단위를 지정하고, 하이퍼바이저가 이를 따르도록 한다.

• Secure Network(RQ11): 네트워크는 DDoS, 스푸핑, 스니핑, Man-In-The-Middle Attack, ARP poisoning, 웜 등 다양한 공격으로부터 위협받게 된다. 따라서 기존의 엔터프라이즈 환경에서 사용되는 Firewall, IDS, IPS, Anti-DDoS와 같은 보안 장치들을 통하여 보안 공격을 막는다.

• Internal Network Probing Prevention (RQ12): 클라우드 컴퓨팅 시스템은 내부에서 발생하는 트래픽에 대해서도 침입탐지 시스템을 통한 감시가 필요하다. Virtual machine을 할당 받은 악의적인 사용자는 내부 네트워크에 공격 트래픽을 발생 시킬 수 있기 때문이다. 공격 여부를 탐지할 수 있는 침입탐지 시스템뿐만 아니라 주요 시스템의 프록시 서버를 설정하여 운영함으로써 내부 네트워크

에 발생하는 네트워크 공격을 막을 수 있다.

• Forensic Readiness(RQ13): 클라우드 컴퓨팅 환경에서 관리의 목적과 보안의 목적으로 시스템 내에 발생하는 많은 트렌잭션을 기록한다. 하지만 정작 보안 사고가 발생할 경우 무수히 많은 기록 정보들로 인해 보안 사고의 진원지와 공격 원인을 밝혀내기 어렵다. 효율적인 보안 기록을 남기기 위해서는 먼저 비정상 탐지 기법을 기반으로 평소 이용 시간이 아닌 시간에 접속하거나, 다른 지역의 네트워크를 통해 접속하는 등 비정상 경로를 통해 서비스를 사용하는 고객들에 대한 정보를 따로 기록한다. 가능한 포렌식 서비스의 예로는 SaaS의 경우 서비스 사용자의 콘텐츠 접근에 관한 IP 로그 정보 저장 및 접근 서비스, IaaS의 경우 최근 가상 머신 및 디스크 이미지에 대한 포렌식 서비스 등이 있다.

• Secure Data Deletion(RQ14): 데이터를 저장 매체로부터 삭제할 때에는 물리적인 완벽 삭제가 가능하도록 해야 한다. 이것이 가능하지 않다면 정보 저장 시에 표준 암호 알고리즘을 이용하여 암호화함으로써 정보 유출의 위험을 줄일 수 있다.

• Business Continuity and Disaster Recovery Plan(RQ15): 기업의 신뢰성은 보안 사고로 인한 정보 유실이나 변경에 의해 손상되기도 하지만, 서비스 가용성이 제대로 이루어지지 않을 경우에 크게 손상된다. 보안 사고가 발생하더라도 지속적으로 사용자에게 충분한 서비스를 제공할 수 있도록 용인가능최대정지시간(Maximum Tolerable Downtime, MTD)를 은행, 증권사의 복구 시간과 동일한 수준의 3시간 이내로 설정하여, 관리자로 하여금 신속하게 오류 여부를 파악하고 이를 복구할 수 있도록 시스템을 설계하여 업무의 연속성을 보장한다.

• Application/OS Security and Patch Management(RQ16): 운영체제와 사용 소프트웨어의 무결성 여부 확인, 악성코드에 대한 확인 및 대응, 각 소프트웨어의 취약성 관리, 침입탐지 등이 가능하도록 보안 시스템을 구성해야 한다. 또한 패치 관리 프로세스가 네트워크와 서버 운영체제, 가상화 소프트웨어, 어플리케이션, 보안 시스템 전 영역에 걸쳐 동작해야 한다.

• Security Monitoring System(RQ17): 클라우드 컴퓨팅 인프라 내부 네트워크의 트래픽, 시스템 내부 동작의 세부사항, 발견된 시스템 취약점 등에 보안 관련 정보들을 저장·분석·관리할 수 있는 시스템이 존재해야 한다.

5. 결론

본 논문에서는 최근 이슈가 되고 있는 클라우드 컴퓨팅 환경 구축 시 반드시 고려되어야 하는 보안 요구사항을 클라우드 컴퓨팅 자산과 취약점에 따라 제안하였다. 클라우드 컴퓨팅 환경의 경우 일반적인 단일 시스템에 비해 대량의 정보와 자원을 취급하기 때문에 보안 서비스가 매우 중요한 요소이다.

클라우드 컴퓨팅이 IT 자원의 공유로 인한 저비용 컴퓨팅 환경 구축이 장점인 반면에 각 자원과 서비스에 따른 보안 요구사항은 해결해야 할 문제이다. 아울러 보안 요구사항을 적용할 경우에 클라우드 컴퓨팅의 효율성 저하에 따른 문제점도 발생할 수 있다.

향후 제시한 보안 요구사항을 만족할 수 있는 클라우드 컴퓨팅 환경에서의 보안 시스템의 구조를 설계 및 연구할 계획이다. 또한, 시뮬레이션을 통해서 보안 요구사항을 적용할 경우에 클라우드 컴퓨팅에 대한 효율성도 점검할 것이다.

참고문헌

[1] 김의중, “IT 6 Mega Trend: Green IT&Cloud Computing" p.25, 2008.

[2] 민옥기 외, “훤히 보이는 클라우드 컴퓨팅”, 2009.

[3] 문상철, 김형준, "클라우드 컴퓨팅을 위한 분산 데이터 관리 시스템 및 데이터 서비스 기술", 정보처리학회지, 16권 제 2호, Mar. 2009.

[4] ENISA, "Benefits, Risks and recommendatations for information secuirty", Nov. 2009.

[5] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", 2009.

[6] Joel Kirch, "Virtual Machine Security Guidelines", WBB Consulting, 2007.

[7] Tal Garfinkel and Mendel Rosenblum, "When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments", In 10th Workshop on Hot Topics in Operating Systems, 2005.

[8] Jenni Susan Reuben, "A Survey on Virtual Machine Security", Seminar on Network Security, 2007.

[9] Doug Hyde, "A Survey on the Security of Virtual Machines", 2009.