안전한 클라우드 컴퓨팅 환경 구축을 위한 보안 시스템 연구

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

A Study of Security System for secure Cloud Computing System

Min-Woo Park*, Dong-Min Kang*, Jun-Ho Lee*, 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 시스템을 안전하게 보호하기 위한 보안 시스템을 제안한다. 클라우드 컴퓨팅은 방대한 자원을 보유하고 있으며, 자원 가상화를 통해 다수의 사용자에게 그들이 원하는 서비스를 제공하는 시스템이다. 클라우드 컴퓨팅은 보유한 자원과 시스템내에 저장된 사용자들의 정보로 인해 공격자의 공격 대상이 되기 쉬우며, 공격이 성공할 경우 단일 컴퓨팅 시스템이나, 엔터프라이즈 컴퓨팅 시스템에서의 피해 규모에 비할 수 없는 막대한 손실을 일으킬 수 있다. 본 논문에서는 클라우드 컴퓨팅의 보안을 위협하는 다양한 공격들로부터 클라우드 컴퓨팅 시스템을 보호하기 위한 보안 시스템을 설계하고 제안한다.

1. 서론

클라우드 컴퓨팅은 대규모 분산 컴퓨팅 장치들을 이용하여 다양한 ISP 고객에게 요구사항에 맞춰 서비스를 제공할 수 있는 새로운 컴퓨팅 패러다임이다.[1,2]

클라우드 컴퓨팅은 다음과 같은 특징들로 인해 최근 각광을 받고 있다. 기업의 경우 클라우드 컴퓨팅를 이용하여 서비스를 제공하는 원가 절감을 할 수 있다. 클라우드 컴퓨팅은 과금 방식에 있어서 사용자가 원하는 만큼의 자원을 이용하고, 사용한 양 만큼에 대해서만 과금을 하기 때문에, IT 기기들을 의 구입비용을 줄일 수 있어, 비교적 적은 비용으로 서비스를 시작할 수 있다. 최근 네트워크가 발달하고 스마트폰과 같은 소형 전자장치들이 발달하면서 언제 어디에서든 인터넷에 접속할 수 있는 환경이 갖추어 졌다. 그 결과 비교적 낮은 자원을 가진 휴대기기를 사용하더라도 클라우드 컴퓨팅 서비스를 이용할 경우 높은 연산력을 요구하는 다양한 서비스들을 휴대기기를 통해 이용할 수 있게 되었다.

이러한 환경 변화에 따라 클라우드 컴퓨팅 산업에 많은 기업들이 참여하고 있다. 다국적 인터넷 기업인 Google(구글)이나 Amazon(아마존)이 적극적으로 참여하고 있으며, 그 외에도 IBM, Microsoft와 같은 큰 규모의 IT 벤더들이 클라우드 컴퓨팅 산업에 참여하고 있다[5]. 그 외 국내 다양한 기업들이 클라우드 컴퓨팅 서비스를 제공하고 있어, 국내외 클라우드 컴퓨팅 시장 규모가 나날이 커지고 있다.

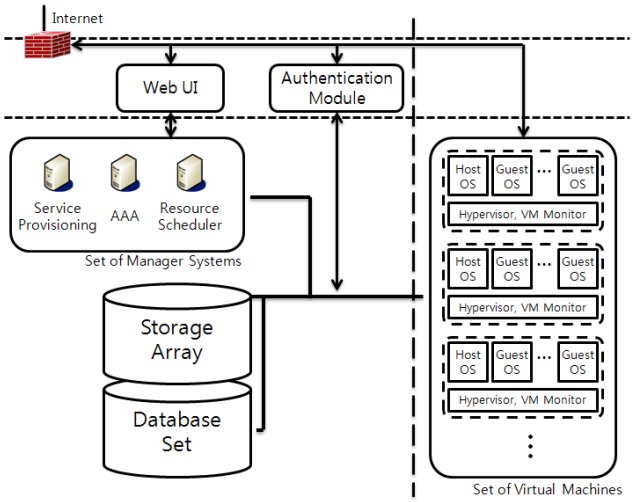
클라우드 컴퓨팅 시장의 지속적인 발전을 위해서는 안전한 클라우드 컴퓨팅 환경을 구축하는 것이 중요하다[6, 7]. 클라우드 컴퓨팅 시스템은 사용자의 정보를 위탁받아 저장하고 이를 가공하는 등 사용자가 요구하는 다양한 서비스를 처리한다. 이 때문에 서비스 과정에서 사용자의 정보가 노출되거나 변조되는 등 보안 사고가 발생하게 되면 해당 시스템의 신뢰도가 크게 손상되며, 이는 나아가 클라우드 컴퓨팅 시스템 자체에 대한 소비자들의 불신으로 이어질 수 있다. 특히 클라우드 컴퓨팅은 다수의 사용자들의 정보를 저장하고 있으며, 많은 자원을 보유하고 있기 때문에 공격 대상이 되기 쉽다. 게다가 자원 가상화나 사용량을 실시간으로 확인하는 등 여러 장치들이 복잡한 형태로 얽혀 동작하기 때문에 자칫 취약점이 발생하기 용이하다. 따라서 클라우드 컴퓨팅 환경은 유입되는 트래픽들에 대한 총체적인 강력한 통합 보안 시스템이 필요하다. 본 논문에서는 클라우드 컴퓨팅 시스템을 구성하는 장치들에 대해 개념적으로 서술하고 클라우드 컴퓨팅 시스템을 보호하기 위한 보안 시스템 모델을 제시한다.

본 논문의 구성은 다음과 같다. 먼저 2 장에서는 클라우드 컴퓨팅 시스템의 개념적 구조에 대해 서술하고, 3장에서는 서비스 유형별 보안 요구사항에 대해 설명하고, 4장에서는 본 논문에서 제안하는 클라우드 컴퓨팅 시스템의 보안 시스템 모델을 제시한다. 마지막으로 5 장에서는

본 연구의 결론을 맺는다.

2. 클라우드 컴퓨팅 시스템의 개념적 구조

현재 클라우드 컴퓨팅은 각각 서비스를 제공하는 회사별로 독자적인 형태로 구축되며, 제공하는 서비스에 따라 다른 형태로 구축되고 있다. 따라서 각 클라우드 컴퓨팅 시스템이 가지는 공통적인 시스템 구조를 개념적으로 정의하고, 시스템 구조를 바탕으로 보안 시스템을 설계한다. (그림 1)은 클라우드 컴퓨팅 시스템의 구조를 개념적으로 나타낸 것이다.



(그림 1) 클라우드 컴퓨팅 시스템의 개념적 구조

클라우드 컴퓨팅 시스템은 크게 네 부분으로 구분할 수 있다. 첫째, 사용자와 직접 적인 통신을 담당하는 Web UI나 Authentication Module이 존재한다. 내부 네트워크에 존재하는 주요한 장치들을 외부로부터 보호하기 위한 장치로 사용자나 요청 트래픽이 정당한 대상인지 인증을 수행하거나 서비스 요청에 따라 내부에 위치한 여러 장치들과 통신하여 요청 결과를 사용자에게 전달하는 역할을 한다. 둘째, 클라우드 컴퓨팅 시스템들을 관리하고, 사용자에게 서비스를 할당하는 주체로 관리 장치들이 있다. 관리 장치는 정당한 사용자의 목록 관리, 사용자의 자원 사용량 확인, 실질적인 사용자 인증 과정, 사용자에게 자원 할당 및 반환 등 클라우드 컴퓨팅 서비스가 정상적으로 제공되고 그에 대한 과금 처리가 명확하게 이루어 질 수 있도록 전체 시스템을 유지, 관리 하는 기능을 가지는 장치이다. 셋째, 데이터를 저장하기 위한 저장 영역이나 데이터베이스가 있다. 저장 영역이나 데이터베이스는 개인 사용자가 직접 접근하여 이를 이용하거나, 클라우드 컴퓨팅 서비스를 제공하기 위해 내부적으로 사용되는 장치로 저장 영역의 경우 자원 가상화를 통해 대용량의 정보들을 저장하거나 읽기에 적합한 형태의 자원이며, 데이터베이스의 경우 많은 량의 작은 크기의 정보들을 질의에 따라 빠르게 탐색, 추가, 삭제 하기에 적합한 형태의 자원이다. 마지막 자원은 사용자에게 실질적인 자원을 제공하기 위한 자원들의 집합이다. 하이퍼바이저를 통해 하나의 시스템에서 다수의 게스트 OS 생성시켜 각 사용자에게 하나씩 할당하는 형태로 서비스가 제공된다.

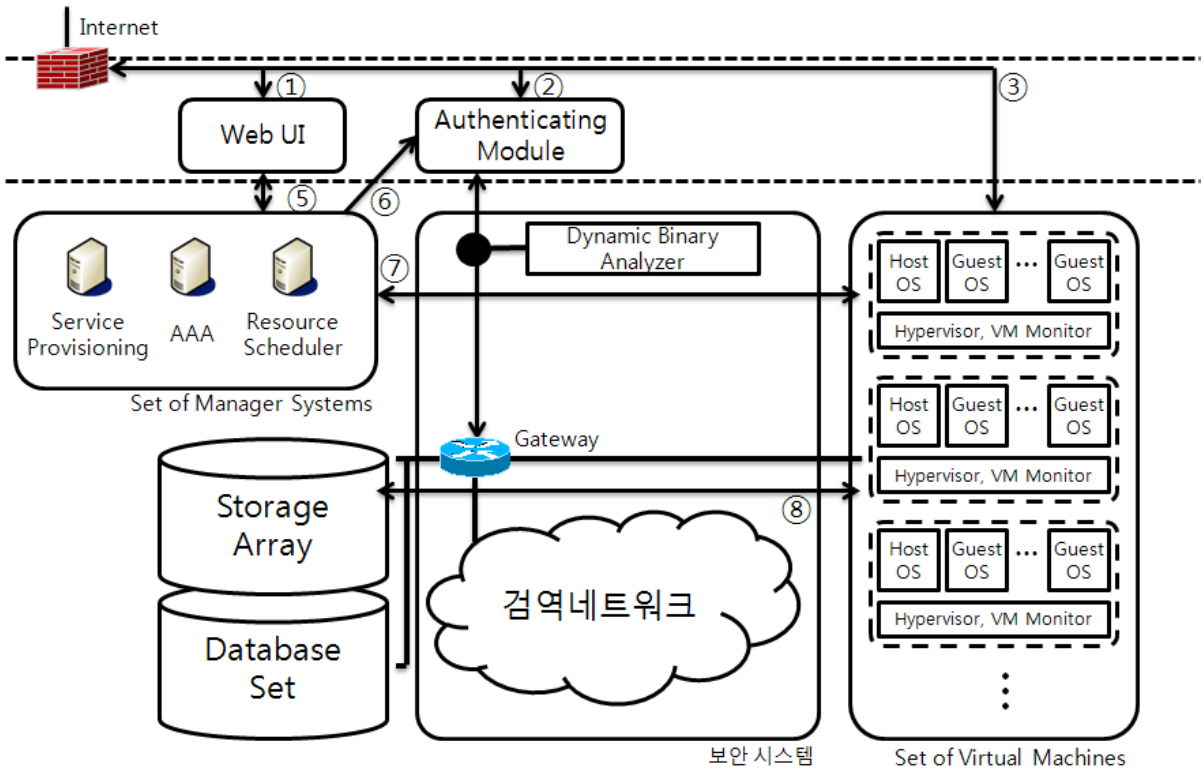
3. 서비스별 보안 요구사항

클라우드 컴퓨팅 시스템은 서비스 유형에 따라 구조가 달라지며, 그에 따라 필요한 보안 요구사항 또한 크게 달라진다. 본 장에서는 서비스 유형별 필요한 보안 요구사항에 대해 서술한다. 통상적으로 클라우드 컴퓨팅은 서비스의 유형에 따라 Infrastructure as a Service(IaaS), Platform as a Service(PaaS), Software as a Service(SaaS)로 구분된다. 아래 <표 1>은 서비스별 특징과 대표적인 클라우드 컴퓨팅 서비스를 나타낸 것이다.

<표 1> 서비스별 특징

서비스 분류	서비스별 특징	대표 서비스
Software as a Service(SaaS)	응용 소프트웨어, 웹 기반 서비스 등을 사용자에게 제공하는 클라우드 컴퓨팅 서비스	Google Apps, MS office live
Platform as a Service(PaaS)	개발 환경, 웹 서비스 환경 등 사용자가 어플리케이션을 제작, 제공할 수 있는 환경을 제공하는 서비스	Google AppEngine, Amazon EC2
Infrastructure as a Service(IaaS)	저장소, 데이터베이스 등 대용량의 인프라스트럭쳐를 제공하는 서비스	Amazon S3, Amazon SimpleDB, Google Base

서비스의 유형별로 각각 보안 시스템 구축 시 요구사항이 달라진다. 서비스 유형별 특징을 살펴보면, SaaS의 경우 주로 웹 또는 API를 통해 클라우드 컴퓨팅 시스템에서 제공하는 응용 프로그램을 이용하는 형태로 개인 사용자가 직접 클라우드 컴퓨팅 시스템 내에 각각의 자원들을 이용하거나 접근할 수 없다. 따라서 SaaS의 경우 다른 서비스에 비해 폐쇄적인 서비스 구조를 가지기 때문에 보안 시스템 구축 시 요구사항이 보다 간단하다. 이에 비해 IaaS나 PaaS는 사용자가 API나 HTTP를 통해 직접 시스템 자원에 접근하여 이를 이용하기 때문에 보안 시스템 구축 시 요구사항이 복잡하다. 특히 두 서비스 유형의 경우 자원 가상화를 통한 각 사용자에게 할당되는 자원들의 구분이 명확하게 이루어 져야 한다. PaaS는 시스템 자원에 인증을 거친 사용자만 접근하는 것이 아니라, 해당 사용자가 개발한 응용 프로그램을 통해 제 3자가 시스템 자원에 접근할 수 있다. 따라서 자원의 구분도 중요하지만, 제 3자에 의한 루팅 행위나, 사용자에 의한 의도적인 악성 프로그램의 구동을 검사하고 규제하여야 한다.



(그림 2) 클라우드 컴퓨팅 시스템을 위한 보안 시스템 모델

4. 클라우드 컴퓨팅 시스템을 위한 보안 시스템

클라우드 컴퓨팅 시스템을 보호하기 위해서는 다음 세 가지 기능이 필수 적이다. 첫째, 클라우드 컴퓨팅으로 유입되는 트래픽들을 대상으로 안전성 검증을 통해 외부로부터 악성 코드의 유입을 막는 기능과 Guest OS 또는 Host OS에 의해 발생하는 트래픽들을 대상으로 안전성 검증을 통해 가상 머신에 의해 내부 장치들이 공격받는 것을 막는 기술이 필요하다. 마지막으로 각 Host OS 또는 Guest OS에서 발생하는 제어권 침탈을 위한 행위들을 감시하고 이를 조기에 판단할 수 있는 기능이 필요하다.

4.1 유입되는 트래픽 검역

클라우드 컴퓨팅에는 총 3가지 경로로 트래픽이 유입된다. 그 경로는 각각 (그림 2)의 ①, ②, ③과 같다. 경로 ①은 Web UI를 통해 이루어지는 서비스로 서비스 이용을 위한 가입, 서비스 요청, 변경, 또는 Web을 통한 SaaS 서비스 등이 이에 해당한다. 경로 ①의 트래픽은 목적지가 Web UI이며, 내부 장치들과 직접 통신은 Web UI에서 담당한다. 즉, 경로 ①을 통해 서비스를 이용하는 사용자들은 네트워크 내부에 위치한 관리 장치들의 정확한 존재를 알 수 없으며, 직접 통신이 불가능하다. 따라서 경로 ①을 통해 유입되는 트래픽은 검역 대상이 되지 않는다. 경로 ②를 통해 유입되는 트래픽은 인증 코드를 발급 받은 HTTP, API 등을 통해 저장 영역, 데이터베이스에 접근하는 트래픽이나, 가상 머신을 할당, 해제, 구동, 정지와 같은 동작을 지시하기 위한 트래픽, 또는 가상머신에서 작동할 사용자의 어플리케이션을 업로드하기 위한 트래픽이나, 첨부파일이 포함된 e-mail 등 다양하다. 경로 ②를 통해 유입되는 트래픽 중 API를 통한 요청/응답 형태의 정형화된 메시지는 검역 대상에서 벗어난다. 그 외 HTTP나 응용 프로그램 업로드 과정, e-mail의 첨부파일 등은 동적 바이너리 분석을 통해 사전에 위험성을 검사하고 이를 예방할 수 있도록 한다. 동적 바이너리 분석은 주로 에뮬레이팅을 통해 가상 머신에서 직접 바이너리 파일을 실행하면서 발생되는 이상 행위를 통해 공격을 판단하는 방법[3]이 있으며, 샌드박스를 통해 특정한 host에서 바이너리 파일을 실행시키는데 이때 각각 함수들을 후킹을 통해 추적하며 이상 행동을 취하는 지를 검사하는 방법[4]이 있다. 경로 ③을 통해 유입되는 트래픽은 계약 관계를 맺은 사용자과 서비스 제공자 사이의 통신 보다는 제 3자와 PaaS 서비스 사용자의 웹 어플리케이션 간의 통신과 같이 별다른 인증 과정을 거치지 않고 직접 가상 머신과 통신하는 트래픽을 나타낸다. 따라서 경로 ③을 통해 유입되는 트래픽들은 검역 대상에서 벗어난다.

4.2 가상머신에서 발생하는 트래픽 검역

가상 머신에서 발생하는 트래픽은 총 세 가지, 첫째 외부 네트워크로 향하는 트래픽, 둘째 관리 장치로 향하는 트래픽, 셋째 저장 장치로 향하는 트래픽으로 구분할 할 수 있다. 검역 대상이 되는 트래픽은 관리 장치나 저장 장치로 향하는 트래픽이다. PaaS를 제공하는 클라우드 컴퓨팅의 경우 사용자가 제작한 웹 어플리케이션의 취약점이

나, 가상 머신을 구성하는 Guest OS 자체의 취약점 등을 통해 제 3자가 특정 가상 머신의 제어권을 획득할 수 있다. 이 경우 공격자는 Guest OS를 통해 관리 장치나 저장 장치를 공격할 수 있다. 이러한 위협으로부터 관리 장치와 저장 장치를 보호하기 위해, Guest OS로부터 발생하는 트래픽 중 관리 장치나 저장 장치를 향하는 트래픽들에 대해 검역을 수행한다. Guest OS나 Host OS가 직접 관리 장치나 저장 장치와 통신하는 경우는 매우 제한적이다. 이는 클라우드 컴퓨팅 구축 결과에 따라 달라지게 되지만, 대부분 모든 경우는 요청/응답 형태의 정형화된 메시지로 구성된다. <표 2>는 정형화된 메시지의 예를 나타낸 것이다. 따라서 정형화된 형태의 메시지가 아닌 경우 또는 정형화된 메시지라도 상황에 맞지 않는 경우, 또는 존재 하지 않은 장치를 향한 트래픽 등은 트래픽을 에뮬레이팅 할 수 있는 검역 네트워크로 보내진다. 검역 네트워크는 honeypot의 일종으로 스캔을 포함한 자신을 대상으로 하는 모든 공격들에 대해 알람을 발생시킨다.

<표 2> 클라우드 컴퓨팅 환경에서 발생 가능한 요청/응답 메시지 예

이름	SRC	DST	설명
Login_req	Web UI	Manager	사용자의 로그인을 위한 확인 요청
Login_rep	Manager	Web UI	로그인을 위한 확인 결과 반환
Auth_req	Web UI	Manager	사용자의 Authentication Code 요청
Auth_rep	Manager	Web UI	Authentication Code 반환
Serv_req	Web UI	Manager	사용자의 서비스 요청
Serv_rep	Manager	Web UI	서비스 요청 결과 반환
Alloc_VM	Manager	Hypervisor	Hypervisor에게 인스턴스 할당 요청
Alloc_VM_Ack	Hypervisor	Manager	인스턴스 할당 요청에 대한 결과 반환
Start_VM	Manager	Hypervisor	인스턴스의 실행 요청
Start_VM_Ack	Hypervisor	Manager	인스턴스 실행 요청 결과 반환
Abort_VM	Manager	Hypervisor	인스턴스의 중지 요청
Abort_VM_Ack	Hypervisor	Manager	인스턴스 중지 요청 결과 반환
VM_Img_Req	Hypervisor	Storage Array	인스턴스 이미지 요청
VM_Img_Rep	Storage Array	Hypervisor	인스턴스 이미지 요청에 대한 결과 반환
Store_VM_Img	Hypervisor	Storage Array	인스턴스 이미지 저장 요청
Store_VM_Img_Ack	Storage Array	Hypervisor	인스턴스 이미지 저장 요청 결과 반환

4.3 가상머신의 침입 탐지

PaaS를 제공하는 클라우드 컴퓨팅 서비스의 경우 가상머신에서 불특정 다수가 접근할 수 있는 웹 어플리케이션이 동작한다. 이 경우 웹 어플리케이션의 취약점이나 해당 어플리케이션이 동작하는 guest OS의 취약점으로 인해 가상머신이 동작하는 host의 제어 권한이 공격자에게 넘어갈 수 있다[8, 9]. 경로 ③을 통해 유입되는 트래픽들은 그 형태가 예측할 수 없어, 트래픽 단위에서 검역은 매우 어려우며, 이 경우 각각 host OS에서 해당 시스템을 위협하는 행위들에 대한 침입 탐지를 수행해야 한다.

5 결론

본 논문에서는 클라우드 컴퓨팅 환경을 보호하기 위한 보안 모델에 대해 제안하였다. 클라우드 컴퓨팅 환경을 안전하게 보호하기 위해서는 다음의 기본적인 3 가지 보안 기능을 만족하여야 한다. 첫째, 유입되는 바이너리 파일들에 대한 안전성 검증이 이루어져야 한다. 둘째, 가상머신으로부터 발생하는 트래픽 중 관리 장치나 저장 장치로 향하는 트래픽에 대해 안전성 검증이 이루어져야 한다. 셋째, 각 가상머신 수준에서 host에 대한 침입 탐지 과정이 필요하다. 이러한 요구 사항을 충족할 경우 클라우드 컴퓨팅 환경은 외부의 공격자로부터 안전하게 시스템을 보호할 수 있다.

향후 연구 방향으로는 클라우드 컴퓨팅 환경에 적합한 각각의 세부 검역 장치들에 대한 설계와 동작 알고리즘에 대한 연구를 진행할 계획이다.

참고문헌

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

[2] 민옥기 외, “훤히 보이는 클라우드 컴퓨팅”, 2009.

[3] Ulrich Bayer, Andres Moser, Christopher Kruegel, and Engin Kirda, "Dynamic analysis of malicious code", 2008.

[4] Willems C, Holz T, and Freiling F, "Toward Automated Dynamic Malware Analysis Using CWSandbox", Security & Privacy IEEE, 2007.

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

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

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

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

[9] 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.