# 클라우드 컴퓨팅 가상화 기술: 보안이슈 및 취약점

강대훈* · 김상구* · 김현호** · 이훈재***

*동서대학교 정보통신공학과

**동서대학교 유비쿼터스 IT

***동서대학교 컴퓨터정보공학부

# Cloud Computing Virtualization: It's Security Issues and Vulnerability

Dea-Hoon Kang* · Sang-Gu Kim* · HyunHo Kim** · HoonJae Lee***

*Dept. of Information and Communication Engineering Dong University

**Dept. of Ubiquitous IT, Graduate School of Dong University

***Division. of Computer and Engineering Dong University

E-mail : kdh4997@naver.com, tkdrn910903@naver.com, feei_@naver.com, hjlee@dongseo.ac.kr

## 요 약

IT 핵심 전략기술로써 클라우드 컴퓨팅 서비스가 많은 기업들 사이에서 공간 및 IT원가절감을 위한 해결책으로 관심이 커지고 있고, 이런 클라우드 서비스를 가능하게 해주는 핵심 기술로써 가상화 기술 또한 이목이 집중되고 있다. 다수의 사용자가 접속해서 서비스를 이용하고 데이터가 집중되는 만큼 데이터의 관리와 무결성, 그리고 해커에 의한 공격 등 취약점에 대한 보안과 개인정보 유출에 대한 문제점이 있다. 서비스의 확산을 위해선 방화벽과 보안솔루션 그리고 백신을 이용한 서버 및 가상화된 다수의 Host, 사용자 편의의 애플리케이션 등에 대한 보안대책과 기술이 필요하다. 본 논문에서는 다양한 가상화 기술 및 기능, 위협요소와 취약점 그리고 이를 보완하기위한 보안기술과 여러 보안솔루션의 기술에 대해서 알아보겠다.

## ABSTRACT

The increasing of Cloud Computing technology among several companies has been a key strategy for IT services to provide desirable IT solutions to consumers of cloud services. More attention is concentrated to these core technologies that enable cloud services and more particularly to the virtualization aspect. The accessibility to a larger number of users is possible because of the usage of the data-intensive, data management and data integrity. Unfortunately, those useful services are vulnerable to kind of attacks by hackers, thus the security of personal information is in critical situation. To solve this to leakage vulnerability, and with the proliferation of cloud services, the cloud service providers adopt a security system with firewall, antivirus software and a large number of virtualized servers and Host. In this paper, a variety of virtualization technologies, threats and vulnerabilities are described with a complement of different security solutions as countermeasures.

키워드

클라우드 컴퓨팅, 가상화 환경, 가상화 솔루션, 클라우드 보안

## Ⅰ. 서 론

최근 많은 기업에서 IT 비용의 원가절감에 대한 생존전략으로 클라우드 컴퓨팅 기술이 IT핵심 전략기술로 급부상되고 있다. 클라우드 컴퓨팅(Cloud Computing)은 인터넷기반의 컴퓨팅 기술로 웹상의 유틸리티 및 데이터를 서버에 두고 사용자가 필요시에 실시간으로 모바일이나 PC등 디지털 기기에서 사용할 수 있는 웹에 기반 한 소프트웨어 서비스이다. 이러한 클라우드 컴퓨팅 서비스를 가능하게 해주는 핵심 기술인 가상화 기술은 오늘날

컴퓨팅 시스템에 광범위하게 이용되고 있는데 컴퓨터 리소스의 물리적인 특징을 추상화하고 사용자에게 논리적 리소스를 제공하는 기술이다. 하지만 가상화 환경의 가장 큰 장애요소는 보안사고에 대한 우려이며, 이를 해결하기 위해서는 보안 문제에 대한 대응이 시급한 실정이다.

## Ⅱ. 클라우드 컴퓨팅 환경 가상화 기술

가상화(virtualization)는 최근 인터넷과 스마트 단말을 통한 클라우드 컴퓨팅이 확산되면서 주목 받고 있는 기술로 클라우트 컴퓨팅 환경의 핵심 기술이다. IT자원(서버, 스토리지 등)부터 시작해 전송을 위한 스위치, 라우터 등과 같은 각종 네트워킹 자원 그리고 사용자 단말기에 걸쳐 광범위하게 적용되고 있고, 서비스 아키텍처를 위한 기반 기술로서 위치하고 있다[1]. 이런 가상화 기술은 하드웨어 비용과 공간을 줄여주고, 운영체제 서비스 활용, 멀티코어 프로세서 사용, 베타 소프트웨어의 테스트 등 다양한 기술적/관리적 이점을 제공해 준다[2][7]. 또한 가상화 계층을 통한 게스트 간 분리(isolation)을 지원함으로 게스트 OS마다 개별적인 OS 및 어플리케이션을 구동할 수 있는 환경을 제공한다.

### 2.1 Hypervisor

일반적인 계층화 아키텍처에서 플랫폼 가상화를 지원하고 가상서버와 하드웨어 사이에 추상화 계층을 배치하는 구조로써 가장 널리 보급되어 있는 가상화 솔루션이다. 가상 시스템 모니터 또는 VMM(Virtual Machine Monitor)이라고도 하고 클라우드 컴퓨팅 환경에서도 보편적으로 적용되는 기술로 호스트 컴퓨터 1대에서 다수의 운영체제를 동시에 실행하기 위한 논리적 플랫폼을 말한다[6].

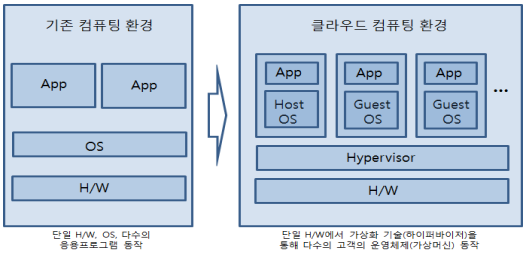


그림 1. 하이퍼바이저의 구성

일반적으로 호스트베이스 하이퍼바이저 방식과 베이메탈 하이퍼바이저 방식으로 나뉜다.

#### 2.1.1 베어메탈(Bare-Matal Hypervisor)방식

베어메탈 방식은 시스템 하드웨어 상에서 직접 구동 되면서 하나 이상의 운영체제를 가상머신으로 하이퍼바이저 상에서 구동되는 방식으로 Xen, VMWare ESX Server, HP Integrity VM 등이 있다.

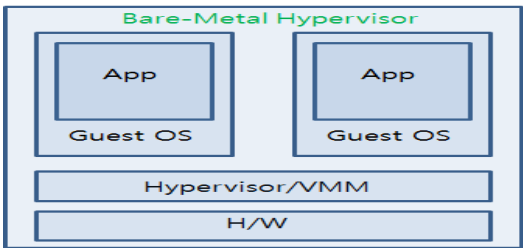


그림 2. Bare-Metal 방식의 구성

#### 2.1.2 호스트베이스(Hosted Hypervisor) 방식

호스트베이스 방식은 일반 애플리케이션처럼 프로그램으로 설치되는 방식으로 단일 호스트 OS상에 가상서버가 존재해 물리적 서버와 하드웨어를 공유하는 형태이다. 대표적으로 VMWare Workstation, VMWare Server, Virtual PC 등이 있다.

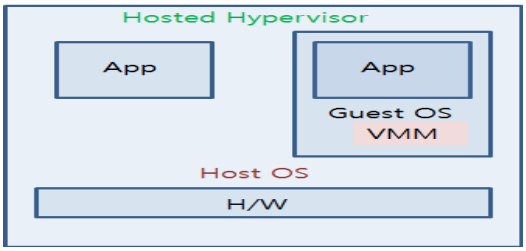


그림 3. Hosted 방식의 구성

### 2.2 vSwitch

물리적 NIC를 다수의 가상머신이 공유하여 가상머신에 가상 NIC가 부여되고 가상 스위치를 통해 물리적 NIC와 연결된다[6]. 가상스위치는 MAC 또는 IP주소를 바탕으로 트래픽 필터링이 제공되므로 가상네트워크의 ACL설정을 통해 격리 시킬 수 있고, 스푸핑 방지를 통한 다른 VM의 IP를 훔치기 위해 ARP스푸핑을 사용하는 악성 VM으로부터 보호할 수 있다[9].

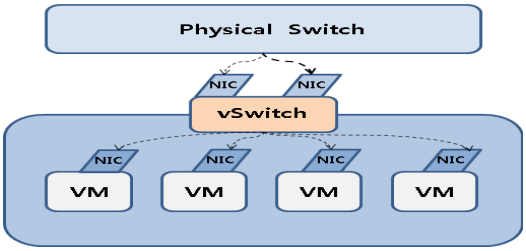


그림 4. 가상스위치의 구성

### 2.3 vMotion

물리적 PC의 장애 발생, 과부하, 이용률 저조시 중단 없이 서비스를 제공하기 위해 가상머신을 power-off 하지 않고 다른 물리적 컴퓨터로 이동시키는 기술로 호스트, 클러스터 또는 데이터 센터 간에 전체 가상 머신을 라이브 마이그레이션을 수행하여 네트워크 ID 및 활성 네트워크 연결이 정확하게 유지되며 업무 중단 없이 사용할 수 있다는 장점이 있다[9].

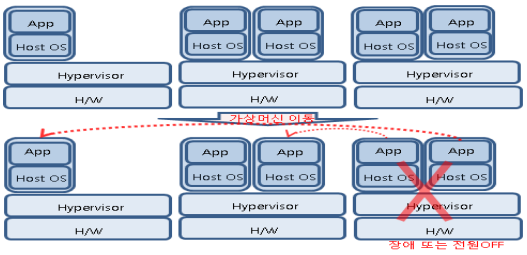


그림 5. vMotion의 구성

## Ⅲ. 클라우드 가상화 기술의 보안 위협 요소와 취약점

### 3.1 가상화 기술의보안 위협 요소

가상화는 기업의 서버 운용 효율과 비용 절감을 위해 매우 유용하지만, 보안을 고려하지 않고 수행할 경우 위협의 대상이 될 가능성이 높다. 기존 보안 제품들은 가상머신 위에서 제대로 작동하지 않고 있는데 이는 IP 혹은 MAC 주소를 정의하기가 어렵고 기존 보안 솔루션들은 하나의 서버 내부가 아닌 서버간의 트래픽을 모니터링 하도록 설계가 되어있기 때문이다[5]. 가상화 환경의 보안 위협으로는 Malware 공격, 정보유출, 서비스 거부, 가상머신 인증, VMM 보안 등이 있다.

### 3.2 클라우드 가상화 기술 취약점

가상화 기술을 통해 이용자의 가상머신들이 상호 연결되어 다양한 공격경로가 존재(가상머신 및 VMM으로 해킹, 악성코드 등 전파가 용이함)하며[4], 클라우드 환경의 가상머신은 이미지 파일 형태여서 쉽게 생성, 이동, 삭제되어 이에 따른 동일한 시스템 상에 VMM 해킹으로 통제권 상실이 되어 서버에 저장되어 있는 이용자들의 자료가 유출되고 손실된다. 빈번한 자원변동, 물리자원 공유로 가상머신 보안 관리에 어려움이 있기 때문에 VMM 호스트 시스템, 게스트 시스템, VMM 자체의 취약점 등에 의해 보안 공격에 노출될 수 있다.

#### 3.2.2 보안장비의 한계점

가상머신은 호스트에 막혀 물리적인 보안장비로는 제어할 수 없다. 가상머신은 제약없이 이동이 자유롭기 때문에 감염된 가상머신이 위치를 이동하면서 여러 시스템에 영향을 미칠 수 있다. 컴퓨터 외부에서 네트워크 패킷을 감시하여 공격을 탐지하는 방화벽, 침입탐지시스템, 침입방지시스템 등은 물리적 시스템의 영역만을 탐색하고 물리 컴퓨터 외부에서 패킷을 감시하여 공격을 탐지하지만, 가상화 내부에서 발생되는 공격행위는 탐지 및 차단이 어렵다. 또한, 가상 머신으로 운영하는 시스템이 많을 경우에 중복된 악성코드 관리를 통해 트래픽 발생과 자원의 낭비를 초래할 수 있다. 아울러, 현재 안티바이러스 제품들은 VMM 루트킷 등과 같은 공격은 탐지할 수 없다.

## Ⅳ. 가상화 보안기술 및 보안솔루션 동향

가상 OS위에 설치된 백신 솔루션은 VMM 동작에 필요한 동등한 상태의 권한을 요구하므로 가상 영역의 악성코드 탐지에 있어서 어려움을 가지게 된다. 이를 해결하기 위해 가상 OS를 컨트롤 하고 실제 데이터 통신 경로를 제어하는 특정 권한을 가진 VMM레벨에서 보안 기술이 적용되어야 하며 가상 OS와 VMM 간의 다른 권한을 가진 보안을 구현해야한다. 하지만 기존 보안업체 핵심 기술인 VMM 원천기술이 제대로 확보되지 않아 보안기술 개발이 부족한 실정이기 때문에 원천 핵심 기술을 개발 하는데 주력해야 한다.

### 4.1 가상화 기반 보안기술

#### 4.1.1 에이전트(Agent)기반 기능

가상화 보안 솔루션의 위치는 각각의 VM 레벨에 위치하는 것으로 VM내부 가상화 트래픽 보안을 향상시킬 수 있고[8], 에이전트가 게스트 시스템에서 실행되기 때문에 클라우드 간 복제, 복구 및 마이그레이션이 가능하며 데이터를 보다 세밀하게 선택할 수 있어 대역폭 및 스토리지 요구사항을 줄일 수 있다.

#### 4.1.2 VMM기반 기능

VMM 안에 있는 가상화된 트래픽도 보안이 가능하다 그러나 VMM 안에 보안 솔루션이 들어가 있기 때문에 속도 저하가 발생할 수 있다.

4.1.3 가상 어플라이언스(Virtual appliance) 연결 기능

보안 솔루션이 별도의 가상 어플라이언스에 있는 것으로 가상 스위치를 통해 보안 기능을 수행한다[8]. 기존 솔루션 구축 시 H/W와 S/W를 따로 구매하고 시스템 통합작업을 거쳐야 했다. H/W와 S/W의 연동과정에서 시행착오가 많아 서로간의 책임 구분이 명확하지 않았지만 어플라이언스는 인프라 구축과 최적화에 필요한 일정을 최소화하며 시스템의 안정적인 운영을 가능하게 함으로써 H/W와 S/W가 최적의 상태로 공급된다.

4.2 가상화 솔루션의 기능과 종류

일반적으로 잘 알려진 가상화 솔루션에는 Oracle의 virtualbox와 VMware의 Workstaion이 있다[3]. 그 밖에도 Microsoft나 CITRIX, redhat, HP, cisco등에서 만든 가상화 솔루션이 있고, 여러 기능을 제공해주어서 관리적, 가용성, 이동성의 효율을 증대시켜 준다.

솔루션 시장에서 가장 높은 점유율을 보이고 있는 기업은 VMware다. VMware는 각 항목별 기능별 여러 가지 기능을 제공하여주고 관리적, 이동성, 가용성 부분에 있어서도 다양하게 지원하고, 하이퍼바이저 부분도 다른 기업들과 비교했을 때 안정성이 가장 뛰어나다.[10]

표 1. 보안 솔루션 제품별 기능

| 보안솔루션 기능 | 보안솔루션 종류 |
|---|---|
| 가상화, 방화벽 (IPS/IDS) | · Deep Security(Trend Micro)<br>· vGW virtual Gateway(JuniperNetworks)<br>· vController IPS/IDS for virtual Environment(HP)<br>· vShield(VMwere), ASA 1000V(Cisco) |
| 가상화 환경에서의 안티바이러스 기술 | · Kaspersky Security for Virtualzation (Kaspersky)<br>· MOVE AntiVirus(MCAlee)<br>· Deep Security Anti Malware(Trend Micro)<br>· Horizon View(VMware) |
| 가상화 환경 (보안관리/관제 기술) | · vTrust for Virtual Management Center (Rellex System)<br>· Virtual Server Protection for VMware(IBM)<br>· HyTrust Appliance(HyTrust) |
| 데이터 (암호화/토큰링) | · Encryption as a Service for wan(Certes Networks)<br>· Ciphercloud(Cipher Cloud)<br>· Token Management(Cryplomathic, inc)<br>· Data Loss Prevertion(Symantec) |
| identify 관리, 인증, 접근제어, SSO | · Intel Expressway Cloud Access 360(Intel)<br>· Okia Application Network(Okia)<br>· privileged Identify Management suit (Cyber-Ark Software) |

## Ⅴ. 결 론

클라우드 컴퓨팅 서비스의 확산으로 가상화 기술이 핵심이 되어 다수의 사용자들에게 편의성을 제공해 주지만 개인정보 유출과 해킹 등 보안사고가 매년 끊이지 않고 발생하고 있다. 관리자의 관리소홀, 개발자의 실수, 천재지변, 전문해커에 의한 공격 등 사고 원인도 다양하다. 이러한 사고를 방지하고 예방하기위한 보안 솔루션들이 기능별로 출시되어 있다. 보안솔루션의 효과적인 사용과 OS 보안과 방화벽 기술을 응용해 악성코드 확산을 방지해야한다. 또한 기업의 보안전문가들을 대상으로 하는 세미나를 주최하여 보안에 대한 인식을 고취시켜야 할 것이다.

## 감사의 글

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었으며(과제번호:2013-071188),부산광역시에서 지원하는 BB21 과제에서 지원받았음.

## 참고문헌

[1] 오경, “클라우드 서비스와 가상화 기술”, TTA Journal, 58-63, 2009. 10
[2] 탁정수, “가상화 기술의 현황과 전망”, NIDA 한국인터넷진흥원. 7-10, 2010. 10
[3] http://docs.oracle.com/cd/E49215_01/html/E40607/
[4] 신영상, “KISA 클라우드 환경의 가상화 보안 위협과 대응 기술 동향“, 1-27, 2013. 1
[5] http://blog.naver.con/gojump0713?Redirect=Log&iogNo=140193504334
[6] 민영기, 고갑승, “클라우드 컴퓨팅 환경에서의 가상머신 보안 취약점 탐지도 설계”,보안공학연구논문지 제9권 제6호, 519-530, 2012. 12
[7] http://www.ni.com/white-paper/8709/ko/
[8] http://blog.naver.com/gojump0713/140193504334
[9] http://www.vmware.com/products/vsphere/features-distributed-switch
[10] http://www.virtualizationmatrix.com/