情 報 保 護 學 會 誌
第22卷 第7號, 2012. 11

클라우드 컴퓨팅 환경 기반의 가상화 기술 및 네트워크 분석 기법 관련 동향

서 정 준*, 신 영 상*, 정 현 철**

요 약

가상화 기술은 클라우드 컴퓨팅 환경에 있어서 주요 기술 가운데 하나이며, 최근 가상화 관련 연구가 활발히 이루어지고 있다. 특히 클라우드 컴퓨팅 환경 기반의 가상화 구현에 있어서 중요한 기술로는 하이퍼바이저가 있다. 또한 클라우드에서의 주요 이슈 중에 하나인 정보의 보호와 관련하여, 악의적인 공격을 탐지하고 대처할 수 있는 가상화 시스템의 분석에 대해 연구되고 있다. 본 논문에서는 클라우드 컴퓨팅 환경에서의 주요 기술과 대표적인 가상화 플랫폼에 대해 알아보며, 가상화 시스템에서의 네트워크 분석 기법과 관련된 동향을 통해 클라우드 컴퓨팅 환경에 있어 정보의 보호 측면에 대해 전반적으로 논의해 보도록 한다.

Ⅰ. 서 론

IT 관련 기술이 급격하게 발전함에 따라, 사용자에게 IT 서비스를 어떻게 제공할 수 있는지에 대해 관심이 높아지고 있다. 사용자에게 이러한 서비스를 제공하는데 있어서 이용될 수 있는 다양한 IT 기술 중에, 최근 클라우드 컴퓨팅이라는 기술이 대표적으로 떠오르고 있다. 클라우드 컴퓨팅 기술은 인터넷을 이용하여 IT 관련 자원 및 서비스를 사용자에게 제공하는데 있어서, 사용자가 요구하는 만큼 이용하게 되는 기술이다. 활용적인 측면에서 예를 들면 중소기업에서는 제품 구입 비용을 줄이기 위한 방안으로, 사용한 만큼 빌려서 사용 및 지불한 후 필요한 서비스라고 판단되면 제품을 구입하면 될 것이다. 오늘날 IT 분야 뿐만 아니라 에너지 관련 분야 등 다양한 분야에서 경제적으로 비용을 줄이는 방안에 대해 논의되고 있으며, 그 중에서 IT 분야에서는 클라우드 컴퓨팅 환경이 이러한 비용 절감 측면에서 적합한 기술로 활용될 수 있을 것으로 기대되고 있다.

그러나 최근 인터넷을 통한 악의적인 공격으로 피해가 늘어나는 가운데, 클라우드 컴퓨팅 환경에서도 클라우드에서의 정보에 대한 보호 측면에서는 아직 해결되어야 될 부분이 남아있는 실정이다. 예를 들어, 사용자의 정보가 클라우드의 서버에 저장이 되는 경우에 있어 보안 관련 고려사항에 대한 논의가 있을 수 있다.

이러한 클라우드 컴퓨팅 기술이 발전되기 위해서는 사용자 서비스를 제공하기 위한 플랫폼 관련 연구에 대한 부분과 클라우드에서의 정보와 관련된 보호 측면 부분으로 크게 나누어서 고려할 수 있을 것이다. 기본적으로 먼저 클라우드 컴퓨팅 환경에서 다양한 사용자 서비스를 제공하기 위한 플랫폼에 대한 연구를 들 수 있다. 물리적인 서버의 활용도를 높이기 위한 측면에서 최근 가상화 기술에 대한 연구가 관심을 받고 있으며, 이러한 가상화 기술은 클라우드 컴퓨팅 환경 관련 기술 요소에 있어 중요한 부분을 차지한다. 결국 가상화 기술에 대한 최근 연구 동향에 대해 파악이 요구되며, 가상머신 및 플랫폼과 관련되어 이러한 가상화 기술을 통해 다수의 사용자에게 다양한 서비스가 어떻게 제공될 수 있는지에 대한 기술 동향 파악이 필요할 것이다. 다음으로, 클

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음. [10041872, 클라우드 컴퓨팅 환경 하에서 내부 가상화 영역에서 발생하는 해킹 공격을 분석·탐지·차단하기 위한 가상 네트워크 침입 대응 기술 개발]

* 한국인터넷진흥원 인터넷침해대응센터 침해예방단 연구개발팀 ({jjun2, ysshin}@kisa.or.kr)
** 한국인터넷진흥원 인터넷침해대응센터 침해예방단 연구개발팀/팀장 (hcjung@kisa.or.kr)

라우드에서의 정보를 어떻게 보호하는지에 대한 연구는 네트워크 분석과 관련된 사항일 것이다. 클라우드 컴퓨팅 시스템에서 정보를 보호하기 위해서는 패킷의 흐름을 분석하여 네트워크 기반에서의 악의적인 공격을 막을 수 있는 방안이 요구된다. 이러한 정보의 보호라는 관점을 바탕으로, 클라우드 컴퓨팅 환경에서 고려될 수 있는 네트워크 분석 관련 기법에 관한 연구가 요구될 것이다.

본 논문은 다음과 같은 구조로 이루어진다. 2장에서는 클라우드 컴퓨팅 시스템과 관련하여 서비스 분류 및 주요 기술에 대해 설명하고 클라우드 관련 해외 표준화 동향 및 보안/가상화 관련 기술에 대해 살펴보도록 한다. 이어지는 3장은 클라우드 가상화 기술의 특징 및 가상화와 관련된 대표적인 플랫폼에 대해 소개하고, 4장에서는 클라우드 가상화 시스템에서의 보안 관련 사항 및 네트워크 분석 기법에 대해 기술한다. 그리고 5장에서는 본 논문의 결론이 내려지도록 한다.

Ⅱ. 클라우드 컴퓨팅 시스템 관련 주요 기술

먼저 2장에서는 클라우드 컴퓨팅 시스템과 관련된 주요 기술을 소개한다. 클라우드 컴퓨팅 서비스의 분류와 설계 고려사항을 기술하고, 클라우드 컴퓨팅에서의 주요 기술과 해외 표준화 동향을 살펴본다. 또한 보안 관련 사항 및 가상화 기술에 대해 알아보도록 한다.

2.1. 클라우드 컴퓨팅 서비스 관련 분류 및 설계 고려사항

클라우드 컴퓨팅은 서비스가 제공되는 모델에 따라 주로 SaaS (Software as a Service), PaaS (Platform as a Service), 그리고 IaaS (Infrastructure as a Service)로 구분한다[1][2]. SaaS는 애플리케이션을 서비스로 제공하는 것이라고 고려할 수 있고, PaaS는 소프트웨어를 개발할 수 있는 플랫폼을 서비스로 제공하는 것이라고 할 수 있으며, IaaS는 인프라를 서비스로 제공하는 것이라고 볼 수 있다.

또한 클라우드 컴퓨팅은 제공되는 서비스의 목적에 따라 일반 사용자들에게 서비스를 제공하는 방식인 공공 클라우드(Public Cloud), 기업처럼 제한된 환경에서의 서비스를 제공하는 방식인 사설 클라우드(Private Cloud), 그리고 공공 클라우드와 사설 클라우드를 혼합하여 각각의 장점을 얻게 되는 방식인 하이브리드 클라우드(Hybrid Cloud)로 분류한다[1].

이러한 클라우드 컴퓨팅 산업의 활성화를 위해서는 우선적으로 신뢰성, 가용성, 호환성과 같은 사항들을 처리하는 일이 요구된다[2]. 신뢰성은 물리적인 데이터 관리 부분과 관리하는 사람 측면으로 나누어서 볼 수 있으며, 가용성은 서비스를 지속적으로 활용할 수 있는지 여부와 관련 있게 되고, 또한 호환성은 플랫폼을 이전하는 상황에서의 표준화와 연관되어 있다. 그리고 클라우드 컴퓨팅의 설계에 있어서는 대규모의 시스템을 운영할 수 있는 기술, IDC에 언제든지 접근될 수 있는 능력 및 H/W 결함 상황에서의 대처 방안, 데이터의 저장 측면에서의 기술, IT 자원 절감 방안 등이 요구될 수 있을 것이다[2].

2.2. 클라우드 컴퓨팅 관련 주요 기술 및 해외 표준화 동향

클라우드 컴퓨팅과 관련된 주요 기술로는 분산 컴퓨팅 기술, 가상화 기술, 시스템 관련 관리 기술, 서비스 플랫폼, 보안 및 과금 측면 사항 등이 있게 된다[2]. 이러한 클라우드 컴퓨팅 관련 주요 기술들 가운데 본 논문에서는 주로 가상화 기술 및 보안 측면을 설명하도록 한다.

표준화에 대한 필요성을 고려한 클라우드 컴퓨팅 환경에서의 주요 관련 분야로는 크게 클라우드 클라이언트 관련 분야, 클라우드 서비스 및 응용 관련 분야, 클라우드 플랫폼 관련 분야, 클라우드 인프라 관련 분야로 나눌 수 있다[5]. 클라우드 클라이언트 관련 분야는 사용자가 직접적으로 클라우드 서비스를 활용하는 것이며, 모바일 클라우드 부분을 예로 들 수 있다. 또한 클라우드 서비스 및 응용 관련 분야는 사용자와 제공자 간의 서비스 수준과 관련된 협약이 중요한 부분으로, 정부 차원에서 표준화를 주도해 나가는 분야이다. 그리고 클라우드 플랫폼 관련 분야는 클라우드 서비스 개발과 데이터 처리 및 관리에 대한 것이며, 클라우드 보안과 관련 있는 부분이다. 마지막으로 클라우드 인프라 관련 분야는 사용자에게 제공 되어지는 컴퓨팅 자원에 대한 관리 표준 및 자원의 가상화와 연관된 표준이라고 할 수 있다.

그리고 해외 표준화와 관련하여서는 크게 공적 표준

화 기구와 사설 표준화 기구로 나눌 수 있다[5]. 공적 표준화 기구로는 ITU-T FG (Focus Group) Cloud와 ITU-T Q.23/13, 그리고 ISO/IEC JTC 1 SC38이 있다. ITU-T FG Cloud는 주로 ITU-T 기술 이슈 및 ITU-T 권고 개발 목적의 선행 관련 연구 등을 수행하며, ITU-T Q.23/13은 주로 ITU-T SG13에서의 클라우드 컴퓨팅 관련 가이드라인 개발과 연관이 있다. 또한 사설 표준화 기구의 예로는 클라우드 간 상호호환을 목적으로 하는 OCC (Open Cloud Consortium), 글로벌 클라우드 컴퓨팅 생태계를 위하는 CCIF (Cloud Computing Interoperability Forum), 클라우드 스토리지 시장 확대 목적의 SNIA (Storage Networking Industry Association), 그리고 클라우드 컴퓨팅 보안을 위해 모범 사례 및 보안 가이드라인 개발과 함께 교육을 제공하는 CSA (Cloud Security Association) 등이 있다.

2.3. 클라우드 컴퓨팅 시스템에서의 보안 관련 기술 및 가상화 기술

최근 IT 기술이 급속하게 발전함에 따라 더욱 각광받고 있는 부분은 보안 관련 기술일 것이다. 보안은 기존의 컴퓨팅 환경에서도 고려되는 이슈인데, 클라우드 컴퓨팅 시스템에서는 기존의 보안 위협은 물론 클라우드 컴퓨팅 시스템에서 내재하는 보안 위협도 추가적으로 고려될 필요가 있다[1]. 즉, 클라우드 컴퓨팅 시스템 자체적인 특징에 따른 보안 위협이 될 수 있는 부분으로는 프로세스, 커널, 하이퍼바이저, 가상머신, 네트워크, 관리자를 들 수 있는데, 이 중에서 특히 이슈가 되고 있는 부분은 하이퍼바이저와 가상머신이라고 할 수 있다. 하이퍼바이저는 단일 운영체제가 아닌 다양한 운영체제를 지원하기 위한 방안으로, 최근 정보의 보호와 관련해서는 하이퍼바이저로의 공격 침입에 대한 탐지 또는 대응 관련 사항들이 이슈가 되고 있다. 가상머신은 하이퍼바이저의 위에서 각 운영체제가 탑재되는 것으로, 이러한 가상머신 상의 피해로 인해 전체 시스템에 영향을 줄 수 있으므로 역시 보안 측면에서 이슈가 되는 부분이다. 클라우드에서의 보안은 다른 관점에서 본다면 데이터 자체에 대한 보안 기술과 시스템 측면에서의 보안 기술로 나눌 수 있게 되는데, 데이터 자체로는 무결성, 기밀성, 그리고 가용성과 연관되며, 시스템 측면의 보안 기술은 무결성의 확인, 신뢰성을 보장하는 H/W 지원 기술, 가상화 기반에서 보안성을 향상시키는 기술이라고 할 수 있다[1].

기본적으로 클라우드 컴퓨팅은 기존 IT 기술에서 더 나아간 것으로, 보안 부분도 기존 보안 기술들 중 클라우드 컴퓨팅과 관련된 요소들로 구분할 수 있는데, 클라우드 컴퓨팅 보안 기술은 플랫폼, 스토리지, 네트워크, 단말의 네 부분으로 나누어서 고려할 수 있다[4]. 특히 플랫폼 부분은 접근 제어, 사용자 인증, 네트워크 상의 사용자 인증을 말하며, 네트워크 부분은 SSL, DDoS 관련 방어 기술 등이 포함된다.

클라우드 컴퓨팅 시스템에서 보안 기술과 함께 중요한 부분은 가상화 기술이다. 가상화 기술에는 데이터 센터 안에서의 서버 및 스토리지와 같은 IT 자원, 스위치, 라우터, 보안 장치 등의 전송 관련 네트워크 장치, 그리고 PC, 스마트폰 등과 같은 사용자 관련 단말기처럼 고려해볼 수 있는데, 이러한 가상화 기술의 종류로는 주로 애플리케이션 가상화, 데스크톱 가상화, 서버 가상화, 스토리지 가상화, 그리고 네트워크 가상화가 있다[3]. 이 가운데 대표적인 기술인 서버 가상화는 데이터센터에서의 많은 물리적 서버를 가상 서버로 합하는 것이며, 이러한 서버 가상화 기술은 비용 측면에서 상당한 이점을 주게 되는 기술이라고 볼 수 있다.

기상화 기술은 보안, 그린 IT, 그리고 비용의 절감 등처럼 다양한 목적을 위한 이슈로 부각되고 있는데, 결국 클라우드 컴퓨팅 시스템의 구축을 위해서는 SaaS, PaaS, IaaS와 같은 각 가상화 요소 기술 자체도 중요한 사항이지만, 가상화 기반의 클라우드 인프라 관리 관련 능력이 더욱 중요한 핵심 사항이 될 것이다[3].

2장에서는 클라우드 컴퓨팅 시스템에서의 주요 기술 이슈에 대해 언급하였다. 다음의 3장에서는 클라우드 컴퓨팅에서의 가상화 기술 관련 플랫폼 소개로 가상화 기술에 대해서 전반적인 설명을 전개해 나갈 것이다. 그리고 4장에서는 보안 측면에서의 네트워크 분석 동향 및 기법에 대해 알아보도록 하여 이러한 결과를 통해 정보가 어떻게 보호될 수 있는지 살펴볼 것이다.

Ⅲ. 클라우드 가상화 기술 관련 플랫폼

3장에서는 클라우드 가상화 기술과 관련된 대표적인 플랫폼에 대해 소개한다. 주로 가상화에 대한 개념과 함께 대표적인 가상화 관련 플랫폼인 Xen[7]의 특징 및

구조에 대해 살펴본 후, Xen에서의 모니터링 기법으로 LibVMI[6]에 대해 알아볼 것이다.

3.1. 클라우드 컴퓨팅 환경에서의 가상화 기술

가상화 기술은 최근 클라우드 시스템과 관련하여 많은 관심을 보이고 있는 기술 중 하나이다. 이러한 가상화 기술에 있어 메모리와 관련된 주소가 있다. 주소에는 물리 주소와 가상 주소가 있는데, 주소 변환은 가상 주소를 물리 주소로 매핑하게 되는 것이다. 그리고 가상 주소 공간은 페이지로 이루어지며, 물리 주소 공간은 프레임으로 구성된다.

이러한 가상화는 반가상화와 전가상화로 구분될 수 있는데, 반가상화는 운영체제를 수정한 형태이며, 이와는 다르게 전가상화는 운영체제를 수정하지 않은 형태이다. 그리고 다양한 가상화 종류 가운데 서버 가상화와 데스크톱 가상화를 고려하면, 서버 가상화에서는 효과적인 자원 활용을 위해서 자원 사용 때 시간적으로 제대로 분배되는지 여부가 중요한 사항이 될 것이다. 반면 서버 가상화와 달리 데스크톱 가상화는 가상머신에 설치되는 OS가 클라이언트 OS이다.

3.2. Xen 플랫폼 특징 및 구조

클라우드 컴퓨팅 환경 기반의 시스템에 있어서 가상화 기술과 관련된 대표적인 플랫폼으로는 Xen과 VMware[8]가 있다. 두 가지 플랫폼 중에, 본 논문에서는 Xen 기반의 플랫폼에 대해 살펴본다[7].

Xen은 관리 모듈을 하이퍼바이저와 분리되도록 한 것이며, Xen 하이퍼바이저는 하드웨어 위에서 다수의 게스트 OS를 구동시킬 수 있는 소프트웨어 형태의 레이어이다. 게스트 OS의 종류로는 리눅스, 윈도우즈 등이 있으며, Xen 관련 구조에서의 주요 구성요소로는

〔그림 1〕 게스트 도메인 부분의 VM 수가 5개인 Xen 시스템 기본 구조 예 (〔7〕 참고)

Xen 하이퍼바이저, Dom0, DomU가 있다. Dom0는 하드웨어와 직접 접근하고 게스트 도메인 부분의 관리를 담당하며, 특권이 있게 된다. 반면 DomU는 하드웨어와 직접 접근을 못하며, 특권이 없는 형태이다. [그림 1]은 Xen 시스템의 기본 구조 예를 나타내며, 게스트 도메인 부분에서의 VM (Virtual Machine) 수가 5개인 경우를 보여준다.

3.3. Xen에서의 LibVMI 기법을 통한 모니터링 방안

Xen 시스템이 구축되면 시스템 모니터링을 통해 가상머신의 CPU, 메모리 등과 같은 정보를 얻게 된다. 시스템 모니터링 기법으로 본 논문에서는 LibVMI를 통한 가상머신의 정보 획득에 대해 살펴본다[9].

LibVMI 프로그램 내에서 주로 고려하게 될 파일은 헤더 파일인 'libvmi.h' 파일이다. 이 파일은 libvmi-0.8을 기준으로 libvmi 폴더 속에 위치하는 파일이다[9]. 또한 가상머신 분석은 시스템 레벨 가상머신의 런타임 상태를 외부에서 모니터링할 수 있는 기술이라고 할 수 있다. 여기서 런타임 상태는 CPU 레지스터, 메모리, 디스크, 네트워크, 그리고 하드웨어 이벤트를 포함한다.

XenAccess는 Xen 시스템에서 운영되고 있는 OS들의 라이브러리를 모니터링하는 것으로, 모니터링 목적 OS의 메모리 또는 디스크를 안전하고 효율적인 형태로 접근하기 위한 모니터링 애플리케이션이 되도록 하는 것이다. 그리고 XenAccess는 libxc, libxenstore, 그리고 BlkTap 구조로 이루어져 있다. 또한 XenAccess 모니터링 라이브러리는 크게 가상 메모리 분석과 가상 디스크 모니터링으로 나눌 수 있다. 가상 메모리 분석은 현재의 메모리 페이지 상황을 모니터링하며 XenControl library와 관련 있는 것으로, 이러한 가상 메모리 분석에 있어서는 xc_map_foreign_range()를 사용하여 다른 가상머신의 메모리를 파악한다. 또한 가상 디스크 모니터링은 디스크로부터 데이터의 오고 가는 것을 캡쳐하는 것으로 BlkTap과 관련 있게 된다. 즉, DomU에서의 프론트앤드 드라이버와 Dom0에서의 백앤드 드라이버를 활용하여 가상 디스크 모니터링이 이루어진다.

[표 1]은 가상 메모리 분석에서의 메모리 분석 API와 가상 디스크 모니터링에서의 디스크 모니터링 API를 나타낸다.

〔표 1〕 XenAccess에서의 메모리 분석 API 및 디스크 모니터링 API 관련 주요 내용 (〔9〕 참고)

	API 종류	주요 내용
메모리 분석 API	xa_init()	메모리 분석과 관련된 초기화
	xa_destroy()	인스턴스의 지움 관련
	xa_access_virtual_address()	주소 변환 시 페이지 테이블 룩업 필요
	xa_access_kernel_symbol()	커널 symbol을 가상 주소로 변환
	xa_access_user_virtual_address()	사용자 공간 메모리 접근
디스크 모니터링 API	xadisk_init()	디스크 모니터링 관련 초기화
	xadisk_destroy()	모니터링 인스턴스 종료
	xadisk_set_watch()	watchpoints 설정
	xadisk_unset_watch()	watchpoints 지움
	xadisk_activate()	inference 엔진 생성
	xadisk_deactivate()	inference 엔진 중지

Ⅳ. 클라우드 가상화 시스템의 네트워크 분석 기법 관련 동향

그러면 4장에서는 클라우드 컴퓨팅 환경 기반 관련 연구 이슈 중에 네트워크 분석 기법 동향에 대해 알아본다. 우선적으로 네트워크 보안 동향에 대해 전반적으로 살펴보며, 그 다음으로 Open vSwitch[10]를 통해 네트워크 상황을 분석하는 기법에 대해 소개한다.

4.1. 클라우드 가상화 시스템에서의 네트워크 보안

네트워크 환경 상의 증가하는 악의적인 공격에 대비하기 위해서는 가상화 시스템 내에서의 패킷 이동과 관련된 사항이 우선적으로 이루어질 필요가 있다. 기본적으로 가상머신 사이에 데이터를 주고받기 위한 소프트웨어 형태의 스위치가 있을 것이다.

보안 측면에서 고려하면, 보안 상황이 다른 다양한 가상머신들을 관리하는 일이 보안 위협으로 다가올 수 있을 것이다. 보안 위협으로부터 대처하기 위한 주요 방안으로, 가상머신 사이에서 주고받는 트래픽을 분석하는 기술과 접근을 제어하는 기술이 있다.

4.2. Open vSwtich 기법을 통한 네트워크 상황 분석

가상화 시스템에서의 네트워크 상황 분석 기법 중에 Open vSwitch라는 기법이 있으며, 주요 특징을 소개하도록 한다[10].

클라우드 환경에서의 가상화 시스템 관련된 Open vSwitch는 멀티 레이어 형태의 가상 스위치로, KVM, Xen 등의 오픈소스 하이퍼바이저 솔루션들을 지원하며, 기본적으로 보면 플로우 기반의 스위칭을 관리한다. 이러한 Open vSwitch가 주로 지원될 수 있는 분야로는 보안, 모니터링, QoS 등이 있다. 특히 보안 측면에서는 트래픽 관련 필터링 기능이 지원되며, 모니터링에서의 기능들로는 NetFlow, sFlow 등이 가능하다.

또한 Open vSwitch의 주요 구성요소로는 ovs-vswitchd, ovsdb-server를 고려할 수 있다. 여기서 ovs-vswitchd는 플로우 기반의 스위칭을 위한 리눅스 커널 모듈과 연계되며, ovsdb-server는 설정을 위한 ovs-vswitchd 요청과 관련된 가벼운 타입의 데이터베이스 서버이다. 그 이외에도 ovs-vswitchd 설정 요청 및 업데이트를 위한 유틸리티인 ovs-vsctl이 있다. 그리고 Open vSwitch가 지원하는 주요 사항은 ovs-controller와 ovs-ofctl이라고 볼 수 있다.

Ⅴ. 결 론

유비쿼터스 환경에서, 경제적인 측면으로 IT 자원을 최대한 활용할 수 있는 방안이 최근 이슈가 되고 있으며, 이러한 측면에서 클라우드 컴퓨팅 환경 기반의 시스템 도입이 많은 관심을 받고 있다. 클라우드 컴퓨팅 시스템은 가상화라는 기술을 활용하여 물리적인 서버의 사용이 최대화될 수 있는 특징을 지닌다. 특히 클라우드 컴퓨팅 환경 기반의 시스템 구축에 있어 기본적으로 필요한 부분은 가상화 기술을 활용한 가상머신의 관리가 될 것이다. 본 논문에서는 클라우드 컴퓨팅 시스템과 관련된 주요 기술을 먼저 소개하고, 대표적인 가상화 기술 관련 플랫폼인 Xen 기반 시스템에 대해 설명하였다. 그리고 Xen의 모니터링 기법인 LibVMI를 알아보았으며, 클라우드 가상화 시스템에서의 네트워크 분석 기법과 관련하여 Open vSwitch 기술을 살펴보았다.

클라우드 컴퓨팅 환경은 사용자에게 다양한 서비스를 제공함에 있어 자원 사용의 줄임을 고려하는 것으로 볼 수 있을 것이다. 이러한 서비스를 제공함에 있어 최근 부각되는 이슈는, 정보를 보호하는 측면에서의 보안 관련 문제일 것이다. 특히 가상화 관련 시스템에서의 보안 문제는 악의적인 공격으로부터 침입을 탐지할 수 있는 기술에 대한 부분과 함께 이에 따르는 대처 방안 기술에 대한 부분이 될 것이다. 그러므로 본 논문에서 설명했던 가상화 관련 기술 및 네트워크 분석 기법을 고려하여 가상화 시스템 내의 악의적인 공격에 있어서 탐지 및 대처가 제대로 이루어질 수 있도록 꾸준히 노력해야 될 것이다.

덧붙여서, 최근 다양한 IT 기술의 활용에 따라 서비스를 제공하는 측면에서의 클라우드 컴퓨팅 관련 수요는 늘어나게 될 것으로 예측된다. 결국 앞으로 클라우드 컴퓨팅을 지속적으로 발전시키기 위해서는 클라우드 컴퓨팅 환경에서의 기술적인 연구 이외에도 활발한 표준화 활동 참여 및 정책적인 측면에서의 적극적인 의견이 요구될 것으로 예상한다.

참고문헌

[1] 김태형, 김인혁, 민창우, 엄영익, “클라우드 컴퓨팅 보안 기술 동향”, *정보과학회지*, 30(1), pp. 30-38, 2012년 1월.

[2] 민옥기, 김학영, 남궁한, “클라우드 컴퓨팅 기술 동향”, *전자통신동향분석*, 제24권 제4호, pp. 1-13, 2009년 8월.

[3] 오경, “클라우드 서비스와 가상화 기술”, *TTA Journal*, No. 125, 2009.

[4] 은성경, 조남수, 김영호, 최대선 “클라우드 컴퓨팅 보안 기술”, *전자통신동향분석*, 제24권 제4호, pp. 79-88, 2009년 8월.

[5] 이강찬, 이승윤 “클라우드 컴퓨팅 표준화 동향 및 전략”, *정보과학회지*, 28(12), pp. 27-33, 2010년 12월.

[6] LibVMI, http://code.google.com/p/vmitools/.

[7] Xen, http://xen.org/.

[8] VMware, http://www.vmware.com/.

[9] Bryan D. Payne, Martim D. P. de A. Carbone, and Wenke Lee, “Secure and Flexible Monitoring of Virtual Machines,” http://www.acsac.org/2007/abstracts/138.html.

[10] Open vSwitch, http://openvswitch.org/.

〈著者紹介〉

서 정 준 (Jeong-Jun Suh)
정회원
1999년 2월 : 중앙대학교 제어계측공학과 학사
2001년 8월 : 연세대학교 전기전자공학과 석사
2010년 8월 : 연세대학교 전기전자공학과 박사
2010년 11월~2011년 3월 : 대구경북과학기술원 박사후연수연구원
2011년 5월~2012년 4월 : 한국에너지기술평가원 연구원
2012년 7월~현재 : 한국인터넷진흥원 선임연구원
<관심분야> 무선 센서 네트워크 라우팅 및 포워딩, Wireless PANs, 위성 ATM 망, 클라우드 컴퓨팅

신 영 상 (Youngsang Shin)
비회원
1998년 2월 : 부산대학교 컴퓨터공학과 학사
2000년 2월 : 부산대학교 컴퓨터공학과 석사
2004년 5월 : 미국 University of Wisconsin - Madison, Computer Science M.S.
2011년 8월 : 미국 Indiana University - Bloomington, Computer Science Ph.D.
2011년 12월~현재 : 한국인터넷진흥원 인터넷침해대응센터 연구개발팀 선임연구원
<관심분야> 네트워크 보안, 클라우드 보안, 웹 보안, 모바일 보안

정 현 철 (Hyun-Cheol Jeong)
정회원
1996년 2월 : 서울시립대학교 전산통계학과 졸업
1999년 8월 : 광운대학교 전자계산학과 석사
2006년 9월~2008년 8월 : 고려대학교 정보보호대학원 박사과정 수료
1996년 7월~현재 : 한국인터넷진흥원 인터넷침해대응센터 연구개발팀장
<관심분야> 웹취약성 분석, 인터넷전화 보안, 악성코드 분석, 클라우드 보안