클라우드 컴퓨팅 서비스의 취약성과 대응기술 동향에 관한 연구

전정훈*

요 약

최근 클라우드 컴퓨팅 기술은 전 세계적으로 중요한 이슈가 되고 있으며, 기술과 서비스에 있어서도 많은 주목을 받고 있다. 그러나 클라우드 컴퓨팅의 긍정적인 측면과는 달리, 여러 취약점들로 인해 해킹기술의 진화에 따른 다양한 공격과 피해가 예상되고 있다. 따라서 본 논문은 클라우드 컴퓨팅의 보안기술에 대해 실험 및 사례연구를 통해 동향을 분석함으로써, 향후 클라우드 컴퓨팅의 보안 체계의 구축과 대응기술 개발을 위한 자료로 활용될 것으로 기대한다.

A study on the vulnerability and corresponding technique trends of the cloud computing service

Jeon Jeong Hoon*

ABSTRACT

Recently, the cloud computing technology is emerging as an important issue in the world, and In the technology and services has attracted much attention. However, the positive aspects of cloud computing unlike the includes several vulnerabilities. For this reason, the hacking techniques according to the evolution of a variety of attacks and damages is expected. Therefore, this paper will be analyzed through case studies and experiments to the security technology trends of the cloud computing. and In the future, this is expected to be utilized as a basis for the security system design and corresponding technology development.

Key words : Cloud computing security, Cloud service security, Security System, Virtualization, Vulnerability

접수일(2013년 11월 25일), 수정일(1차: 2013년 12월 15일), 게재확정일(2013년 12월 23일)

* 동덕여자대학교 컴퓨터학과

1. 서 론

최근 클라우드 컴퓨팅(cloud computing) 기술은 기존 서비스와 네트워크 체계에 매우 큰 변화를 가져오고 있으며, 편의성과 신속성, 이동성, 성능의 향상 등 여러 장점들을 갖고 있다. 이와 같은 클라우드 컴퓨팅의 기술에는 가상화(virtualization)와 자원의 공유(sharing) 및 임대(tenancy) 등이 있으며, 가상 서버(virtual server)와 스토리지(storage), 시스템 자원의 공유 등의 형태로 응용 서비스들을 제공하고 있다. 그러나 클라우드 컴퓨팅은 보안성 확보가 가장 큰 문제로 떠오르고 있다. 이와 같은 보안 문제는 서비스에 대한 신뢰성을 저하시키는 요인으로 클라우드 서비스의 활성화에 가장 큰 걸림돌이 되고 있다. 예로, 클라우드 서비스 제공자와 사용자는 클라우드 기술과 함께 해킹 기술도 함께 진화하고 있다는 점을 염두 해 둘 필요가 있다. 최근 클라우드 서비스의 취약성(vulnerability)을 악용한 새로운 공격들이 등장하면서, 이에 대한 우려와 관심이 높아지고 있다. 특히, 클라우드 보안은 서비스들을 악용한 새로운 취약성들이 새롭게 등장함에 따라, 기존 IT체계에서의 보안기술만으로는 한계를 갖는다. 따라서 클라우드 환경에 적합한 보안기술의 표준화와 호환성, 이식성 등이 반영된 개발이 필요한 실정이다. 그러나 클라우드 서비스는 사용범위가 글로벌하고, 아직까지 진화 과정 중이기 때문에, 지금의 보안 기술이 효과적인지의 여부를 판단하기는 어렵다. 그리고 아직까지 잠재된 취약성들에 대해 구체적인 분석이 필요하다. 또한, 대부분의 클라우드 보안 기술들은 서비스를 제공하는 몇몇 글로벌 기업들에 의해 주도되고 있어, 보안 기술의 의존성과 종속성이 높아지고 있는 추세이다. 이러한 상황에서, 국내 보안 기술은 아직까지 미흡한 상황이어서, 서비스에 대한 구체적인 연구와 효율적인 대응기술 마련에 초점을 맞추어야 할 것이다. 따라서 본 논문은 클라우드 컴퓨팅의 취약성과 보안기술들에 대한 분석과 비교를 함으로서, 향후, 클라우드 컴퓨팅의 보안 체계 구축 및 표준화에 필요한 자료로 활용될 수 있을 것으로 기대한다. 그리고, 연구내용에 대한 논리적 근거를 위해, 논문의 2장은 관련연구로 클라우드 컴퓨팅 서비스 및 특징과 주요 보안 관점을 알아보고, 3장은 클라우드 서비스의 취약성에 대해 알아본다. 그리고 4장은 클라우드 서비스의 취약성에 대한 대응방안기술들의 동향을 알아보고, 5장의 결론 부분으로 이글을 마치도록 한다.

2. 관련 연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅에 대한 정의는 기업 및 연구기관, 리서치 기관들에 따라, 조금씩 달리 하고 있다. 그러나 공통적으로는 자원의 공유 및 임대 서비스를 통한 성능의 극대화와 시스템 운영 등의 경제적 비용의 절감 등을 장점으로 다루고 있다. 이러한 클라우드 컴퓨팅 서비스는 표1에서와 같이 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)로 분류해 볼 수 있으며, 운영 형태에 따라, 퍼블릭(public)과 프라이빗(private), 하이브리드(hybrid) 클라우드로 구분해 볼 수 있다[1].

<표 1> 클라우드 컴퓨팅 서비스

구분		주요개념
서비스유형	IaaS	하드웨어 자원 임대・제공
	PaaS	플랫폼 임대・제공
	SaaS	소프트웨어 임대・제공
서비스운용형태	퍼블릭	불특정 다수 대상
	프라이빗	기업 및 기관 내부
	하이브리드	결합형태

2.2 가상화 기술

가상화 개념은 1960년대부터 연구되어져 왔던 기술로서 IBM은 'Time Sharing'이라는 주제로 연구하여 왔다. 특히, 서버 가상화(server virtualization)기술은 운영체제의 가상화로 시작하여, 물리적이지 않은 2대 이상의 컴퓨터의 기능을 한 대의 컴퓨터에서 운영할 수 있도록 한다. 이와 같은 가상화 기술은 한 대 시스템의 완전한 설치로 다른 것들을 수행하는 Full-virtualization과 단일 하드웨어 장치에 다중 운영체제를 변경해가며, 시스템 자원을 효율적으로 동시에 사용할 수 있도록 하는 Para-virtualization으로 나누어 볼 수

있다. 가상화는 물리적인 기기를 대신할 가상 머신(VM:vitrual machine)을 통해, 물리적인 네트워크 통신을 대신한다. 보다 구체적인 내부 기술로는 운영체제가 설치되고, 버추얼 머신 모니터(virtual machine monitor)라는 소프트웨어가 운영체제의 최상위에 설치됨으로써, 애플리케이션 윈도우 내에서 다양한 게스트의 운영체제를 실행할 수 있도록 하는 호스티드(hosted) 방식과 1대의 시스템에 사용자의 운영체제 외에 여러 개의 게스트 운영체제(guest os)를 운용할 수 있는 OS방식이 있다. 또한 VMM이 호스트 운영체제에 의존하지 않고, 시스템 하드웨어와 직접 통신하도록 설치함으로써, 운영체제를 악용한 공격에 강한 특징을 갖는 베어메탈(bare-metal)은 방식이 있다[2]. 이와 같은 가상화 기술들은 자원의 접근 방식이나 모니터링 방식에 따라, 성능(performance) 및 부하(overhead)에 차이를 갖고 있어, 효율성을 판단하기가 어려우며, 잠재된 취약점들의 예측과 기존 보안기술로의 대응을 어렵게 하는 요인이 되고 있다[3].

2.3 공유 및 임대 기술

클라우드 컴퓨팅은 복잡한 내부 기술들이 함께 운영되는 복합 기술로서 가상화 기술 외에 공유 및 임대 기술이 있다. 공유 및 임대 기술은 시스템 자원을 여러 가상 머신들이 공유할 수 있도록 해주며, 다양한 운영체제를 지원한다. 그리고 사용자는 특정 소프트웨어나 스토리지, 기타 서비스의 사용료를 납부하도록 하는 서비스이다[4]. 그러나 공격에 매우 취약하여, 새로운 공격으로의 변이나 진화가 예상된다. 서비스의 효율성과 안정성은 제공형태 및 환경에 따라 다르기 때문에 세밀한 보안기술 적용이 요구된다. 이러한 예로 [5]는 단일 임대 방식의 데이터베이스가 효율성 측면에서 다중 임대 데이터베이스보다 우수하며, 안정성 측면에서는 다중 데이터베이스 임대 방식이 오히려 우수한 것으로 분석하고 있다. 결과적으로 공유 및 임대 기술은 서비스별 취약성 분석과 효율성을 고려한 보안기술 개발이 필요함을 알 수 있다 .

2.4 보안적 관점

클라우드 컴퓨팅의 보안성은 제공자나 사용자 모두에게 중요한 이슈가 되고 있다. 이에 대해 가트너(Gartner)의 최근 보고서를 인용해 보면, 가상화를 적용한 서버가 물리적인 서버보다도 약 60%정도 안전성이 떨어질 것으로 전망하고 있으며, 가상화 서버의 위험성을 2015년까지 약 30%정도로 감소시키는 것을 목표로 하고 있다[3]. 또한 [6]은 1999년부터 2009년까지의 취약성 노출에 관한 보고내용에서 2002년 이후부터 취약성이 지속적으로 증가하고 있음을 나타내고 있다. 위험도별 보고내용에서도 2005년부터 위험성이 높은 취약성들이 급속히 증가하고 있으며, 2008년부터 2009년 사이 위험도가 급증하였음을 나타내고 있다. 이러한 자료를 살펴 볼 때, 운영체제에 의존적인 가상머신의 보안성은 운영체제의 안전성과 보안성으로 예측해볼 수 있으며, 결과적으로 가상화와 공유 및 임대 기술은 비슷한 보안요인들로 이슈가 되고 있다. 따라서, 새로운 보안 취약점들이 증가할 것으로 예상되며[3], 향후 운영체제의 진화가 클라우드 보안에 큰 영향을 미칠 것으로 전망된다.

3. 위협과 취약성 분석

클라우드 서비스는 다양성과 편의성, 성능개선 등을 강점으로 다양한 서비스들이 개발되고 있다. 이들 서비스들의 대부분은 서비스를 제공하는 몇몇 글로벌 기업들이 주축이 되고 있으며, 다양한 기기들을 활용한 서비스들로 편의성과 신속성, 이동성 등을 제공하고 있다. 그러나 클라우드 서비스의 다양화는 잠재된 취약성으로 서비스의 표준화 모델과 표준화를 통한 보안기술의 기반마련이 요구된다. 따라서 본 절에서는 다양한 취약성들에 대해 알아본다.

3.1 보안 위협요인

국・내외의 기관 및 기업들은 클라우드 서비스를 위협하는 요인들을 다양하게 정의하고 있으며, 이러한 위협요인들은 서비스의 진화와 함께 생성과 소멸을 반복하고 있다. 이와 같은 클라우드 서비스의 위협들에 대해 [7]과 [8]은 <표2>와 같이 6가지로 정의하고 있으며, 이러한 위협들은 기존 IT체계의 위협요인들과 차이가 없음을 알 수 있다.

<표 2> 클라우드 서비스의 보안 위협

보안위협	· 클라우드 컴퓨팅의 악의적인 사용과 남용 · 악성 내부사용자 · 공유기술의 취약성 · 데이터 손실 및 누출 · 계정, 서비스와 트래픽 하이재킹 · 알려지지 않은 위험 프로파일

가트너 보고서는 위협요인들을 <표3>과 같이 7가지로 정의하고 있다. <표3>은 <표2>의 위협 요인들보다, 클라우드 서비스에 대한 보안 위협들을 일부 포함하고 있으며, 데이터에 대한 접근과 복구, 저장에 대해 정의하고 있다[8][9].

<표 3> Gartner의 보안 위협

보안위협	· 권한 관리자의 접근 · 정책 · 데이터 저장위치 · 조사자원 · 데이터 분리 · 복구 · 장기적 생존 가능성

UC Berkely는 <표4>와 같이 보안 위협에 대해 10가지로 정의하고 있으며, 앞서 언급된 위협들보다 클라우드 서비스에 관련한 정의를 하고 있다. 그리고 전반적으로 데이터에 대한 접근과 서비스 유지, 모니터링, 전송에 관한 위협들을 열거하고 있다[9].

<표 4> UC Berkely의 보안 위협

보안위협	· 서비스 가용성 · 데이터 lock-in · 데이터 기밀과 감시 · 데이터 전송장애 요소 · 불확실한 성능 예측 · 확장 가능한 스토리지 · 대규모 분산 시스템 버그 · 신속한 스케일링 · 평판 공유 · 소프트웨어 라이센싱

EINSA는 <표5>와 같이 서비스 사용자에 대한 위협들을 다루고 있으며, 서비스의 사용 중, 발생할 수 있는 위협들에 대해 정의하고 있다. 그리고 주요 요인으로 서비스 제공자에 대한 신뢰성 확보와 사용자의 데이터에 대한 보안성 유지에 대해 열거하고 있다[9].

<표 5> EINSA의 보안 위협

보안위협	· 관리부재 · 고립의 어려움 · 서비스 제공자 의존 · 규제 위협 · 데이터 보호 · 관리 인터페이스 보완 · 안전하지 않은 데이터 삭제 · 악의적인 내부자

국내 한국인터넷진흥원은 <표6>과 같이 클라우드 서비스의 핵심 보안 위협들에 대해 6가지의 위협들을 정의하고 있다. 이러한 위협들은 클라우드 서비스의 특성인 가상화와 공유 및 임대에 대한 위협들과 서비스 사용자와 제공자에 대한 위협들을 포함하고 있다.

<표 6> KISA의 보안 위협

보안위협	· 가상화 취약점 · 정보위탁에 따른 정보유출 위협 · 자원 공유 및 집중화에 따른 서비스 장애 · 단말 다양성에 따른 정보유출 · 분산 처리에 따른 보안 적용의 어려움 · 법규 및 규제의 문제

결과적으로 보안 위협들은 제공하는 서비스 및 주요 관점에 따라, 다양하다는 점을 확인할 수 있다. 이에 대해 보안 위협들의 분류체계 구축의 필요성과 사용자 및 제공자 관점의 분석이 필요함을 알 수 있다.

3.2 보안 취약성

클라우드의 취약성은 기존 취약성과 많은 차이를 보인다. 특히, 가상화에 따른 취약성은 새로운 보안 기술들이 요구되며, 운영체제의 보안성에 매우 의존적이다. 이러한 이유로 클라우드의 취약성은 시스템의 성능 및 보안에 매우 큰 영향을 미친다. 다음 표7에서는 가상 머신의 취약성들에 대해 알아본다.

<표 7> 가상머신의 취약성

VM 취약성	· 전형적인 네트워크 보안 통제방식으로 VM을 모니터링 할 수 없다. (VM상호간의 공격)
	· 즉각적인 보안 적용이 어렵다.(Instant on gaps) · 여러 VM들은 서로 다른 보안 레벨을 갖고 있다. (혼재된 신뢰 레벨의 VM) · 자원의 공유로 인해 비인가자에 의해 사용될 수 있다.(리소스의 경합) · 이전의 방식보다 VM의 관리가 복잡하여 관리가 어렵다. (관리의 복잡성) · 악의적이거나, 알려지지 않은 VM이 함께 존재한다.(다중 임대) · VM들의 활동에 대해 로그나 모니터링이 어렵다. (감사 추적의 미흡)

<표7>은 가상 머신의 구성 및 운영상에 복잡함과 가상 머신 상호간의 공격 가능성을 취약요인으로 다루고 있다. 그리고 가상 머신들 간의 시스템 자원 경합으로 자체 취약성 발생 가능성 등을 포함하고 있다. 이러한 요인들은 대부분 외부로부터의 직접적인 공격 가능성을 고려한 것보다는 가상 머신들 간의 취약 요인들이다[10]. 따라서 클라우드 서비스는 다양한 취약성들이 잠재되어 있음을 알 수 있으며, 이에 대한 대응을 위해, 지속적인 취약성의 분석과 분류체계의 구축, 취약성 관리를 통해 보다 예측된 대응체계의 마련이 필요함을 알 수 있다.

4. 대응 기술 분석

클라우드의 대응 기술에는 어떤 것들이 있는지를 알아보기 위해, 본 장은 인증과 네트워크, 스토리지(storage), 접근통제(access control), 단말 시스템, 관리 기술, 기타 기술로 분류하고 이들을 분석해본다.

(1) 인증

인증기술은 인가된 자와 그렇지 않은 자를 검증하는 기술로 매우 다양한 종류들이 있다. 최근 클라우드의 인증에서는 SSO(Single-Sign On)를 사용하고 있으나, 가상화와 SAML(Security Assertion Markup Language)의 적용에 따른 문제가 발생하고 있다[4]. 기존 인증 기술과는 달리, 가상화 기술로 인해 복잡하고, 다양한 취약성들이 존재하기 때문에 효율성이 저하되고 있다.

	보안대응기술
인증	- ID/Password - 공개키 인증서 - Multi-factor - I-PIN - IAM (identity Authentication Management) - SSO - SAML - Kerberos - KMIP(Key Management Interoperability Protocol) - IdMS(Identity Management System) - WSDL(Web Service Description Language)

(2) 네트워크

기존의 IT체계에서 사용되었던 기술들은 클라우드에서도 네트워크의 보안을 위해 사용되고 있다. 그러나 단순히 전송되는 데이터를 보안하는 기능에서 가상화와 공유 기술의 적용에 적합한 기술로 개발이 진행 중에 있다[4].

	보안대응기술
네트워크	- SSL - Ipsec - Application Firewall(L7) - IPS

(3) 스토리지

스토리지의 대응기술은 정보 보호 및 스토리지의 가용성 향상을 위해 제안되었다. 최근 데이터베이스의 보안 기술에 응용되고 있으며, 데이터의 암호화를 통해 보안성을 제공하고 있다. 이는 클라우드 서비스 보안뿐만 아니라, 기존 IT체계에서도 적용되고 있는 기술들이다. 이중에 PPDM은 효율성이 낮아 실용적이지 못하다는 평가를 받고 있어, 아직까지 클라우드에 실제 적용하기까지 시간이 필요할 것으로 보인다[4].

	보안대응기술
스토리지	- 암호기술응용 - PPDM(Privacy Preserving Data Mining)

(4) 접근통제

접근통제 기술에는 DAC(discretionary access control)과 MAC(mandatory access control), RBAC(roles based access control)이 있으며, 대부분 사용되어 왔던 기술들이다. 최근 웹 페이지의 개발에 XACML을 이용하여, 접근통제 기능을 제공하도록 개발이 진행 중에 있다[4].

	보안대응기술
접근통제	- DAC - MAC - RBAC - XACML(eXtensible Access Control Markup Language)

(5) 단말기

단말 시스템의 대응 기술로는 암호 및 운영체제의 보안, 백신 등이 있다. 그러나 가상화는 운영체제에 매우 의존적이기 때문에 운영체제의 보안성은 매우 중요하다[4]. 최근 클라우드 보안을 위해 기존 대응기술과는 달리, 모듈별이나 가상 머신별 기술들이 개발되고 있는 추세이다.

	보안대응기술
단말 보안	- CyptoCell - Virtualization Security - TPM(Trusted Platform Module) - Renewabel Security - SafeXcel IP

(6) 기타 대응기술

기타 대응기술은 기존 IT체계에서 사용되고 있는 기술들이 대부분으로 시스템과 데이터베이스, 감사 등의 기술이 있으며, 기능 향상을 통한 업그레이드 형태를 갖는 것이 특징이다. 예로 최근 클라우드 컴퓨팅의 기반 기술이 되었던 Hadoop은 보다 보안적인 측면에서 향상시킨 Secure Hadoop으로 재탄생되었다[4].

	보안대응기술
기타 기술	- DB 보안 - 시스템 보안 - Secure Hadoop - 감사(Auditing)

(7) 기업별 가상화 보안기술 동향

클라우드 서비스는 몇몇 글로벌 기업들이 주축이 되어 자신들의 서비스를 최적화하기 위해 기술개발을 하고 있다. 따라서 기업들마다의 보안 기술은 호환성과 이식성이 비교적 낮다[11]. 그러나 클라우드 시장이 전 세계로 확대됨에 따라, 서비스의 선점이 보안기술로 이어지고 있는 실정이며, 국내의 해외 서비스 점유에 따른 보안기술의 잠식이 진행 중에 있다.

	기업	보안대응기술
가상화 기술	- Citrix - Microsoft - Oracle - Paralles - Red Hat - VMware - Discretix - SafeNet - TCG - OASIS	- XenServer - Hyper-V - Virtual Iron - Virtuozzo Containers - KVM(Kernel-base Virtual Machine) - VMware - CryptoCell - SafeXcel - TPM - SAML

(8) 관리적 및 기술적 보안

관리 및 기술에 대한 보안은 여러 대응기술들의 통합 정리한 형태로 기술적인 부분에서 클라우드의 가상화와 공유 및 임대 기술에 따른 변화가 이뤄지고 있다. 향후 이와 같은 분류는 보안기술과 서비스의 체계적인 관리를 가능하게 할 것으로 예상된다.

	보안대응기술
관리적	- 관리 및 관제 - 감사 - 로그 관리 - 보안 규제 관리
기술적	- 보안 시스템 - 네트워크 시스템

	- Storage 시스템 - DB 시스템 - 암호 및 인증 - Virtualization - Share & Tenancy - Secure Hadoop

앞서, 클라우드 컴퓨팅의 다양한 보안 기술들을 알아보았다. 그러나 보안 기술의 대부분은 해외 기술들로 몇몇 글로벌 기업들이 주도되고 있어, 저마다의 서비스 보호를 위해 개발되고 있다. 또한 각 기업들은 다양한 보안 기술들을 제공하여, 클라우드 시장을 선점하기 위해 치열한 경쟁을 하고 있다. 따라서 클라우드 컴퓨팅의 효율적인 대응을 위해서는 보안 기술과 서비스의 표준화, 체계적인 취약성 관리가 필요함을 알 수 있다.

5. 결 론

최근 클라우드 컴퓨팅 기술은 전 세계적으로 큰 이슈가 되고 있는 가운데, 다양한 서비스들이 새롭게 등장하고 있다. 그리고 클라우드 기술은 몇몇 글로벌 기업들에 의해 주도적으로 개발되고 있으며, 전 세계의 클라우드 시장은 이들 몇몇 기업들이 선점해 가고 있다. 이들 기업들은 자신들의 서비스에 최적화된 보안 기술들을 개발함으로서, 호환성과 이식성 측면에서 매우 낮게 평가되고 있다. 그리고 취약성은 기업 및 관련 기관들마다 다양하게 정의하고 있어, 대응기술 개발을 저해하는 요인이 되고 있다. 이러한 가운데, 클라우드 컴퓨팅 기술은 잠재된 위협과 취약성들로 향후 클라우드 서비스에 대한 공격시도가 증가할 것으로 예상되며, 기존의 보안 기술만으로 대응하기 어려울 것으로 전망되고 있다. 따라서 본 논문은 클라우드 컴퓨팅의 위협 및 취약 요인들에 대한 분석과 클라우드 컴퓨팅 보안에 필요한 대응기술들을 알아보았다. 그러나, 클라우드 컴퓨팅 기술의 진화가 계속되고 있는 시점에서 새로운 위협 및 취약 요인들이 계속해 등장할 것으로 예상되며, 클라우드의 취약성 분석 및 관리와 보안기술의 이식성과 호환성, 예측성이 포함된 연구가 필요함을 알 수 있다. 본 연구는 클라우드 컴퓨팅 환경으로의 변화에 필요한 보안체계의 구축 및 대응기술의 개발에 유용한 자료로 활용될 수 있을 것으로 기대하며, 향후, 클라우드 컴퓨팅의 보안을 위해 클라우드 서비스에 따른 다양한 공격기술의 분석과 함께 잠재된 취약요인들에 대한 지속적인 실험과 연구가 필요하다.

참고문헌

[1] 강원영, “최근 클라우드 컴퓨팅 서비스 동향,” 한국인터넷진흥원, no. 3, pp. 20-24, 2011.

[2] Tyson T. Brooks, C. Caicedo and J.S. Park, “Security Vulnerability Analysis in Virt ualized Computing Environments,” International Journal of Intelligent Computing Research, vol. 3, pp. 227-291, Mar. 2012.

[3] A. Mishra, R. Mathurm and J.S. Rathore, “Cloud Computing Security,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1(1), pp. 36-39, Jan. 2013.

[4] 은성경, 외 3인, “클라우드 보안기술,” 한국전자통신동향분석, vol. 24, no. 4, pp. 79-88, Aug. 2009.

[5] Johnson, “http://erpcloudnews.com/2010/06/multi-tenant-versus-single-tenant-erp-a-comparison/,“ Jun. 2010.

[6] B. Williams and T. Cross, “Virtualization System Security,” IBM Advanced Research, Apr. 2010.

[7] J. Archer, D. Cullinane, N. Puhlmann , A. Boehme, P. Kurtz, and J. Reavis, “Security Guidance for critical areas of focus in cloud computing v2.1,” Cloud Security Alliance, Dec. 2009.

[8] Md.T. Khorshed, A.B.M. S. Ali, S. A.Wasimi “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,” Future Generation Computer System, vol. 28(6), pp. 833-851, Jun. 2012.

[9] 이향진, ”안전한 클라우드 서비스 제공・이용을 위한 보안 고려사항,” KISA, CloudSEC, 2012.

[10] http://www.kisa.or.kr/jsp/common/downloadAction.jsp? bno=4&dno=1236&fseq=1

[11] 정현준, “가상화 기술의 동향 및 주요 이슈(Ⅱ),” 한국정보통신정책연구원, vol. 25, no. 5(550), Mar. 2013.

[저 자 소 개]

전 정 훈 (Jeong-hoon Jeon)

2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr