Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1239

클라우드 컴퓨팅 보안의 취약성에 관한 연구

전 정 훈†‡
동덕여자대학교

A study on the vulnerability of the Cloud computing security

Jeong-hoon Jeon†‡
Dongduk Woman University

요 약

최근 클라우드 컴퓨팅 기술은 전 세계적으로 중요한 이슈로 부각되고 있으며, 기술과 서비스에 있어, 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 위협과 취약성에 대해 실험 및 사례연구를 통해 관리 모델들을 분석함으로써, 향후, 클라우드 컴퓨팅의 보안 설계와 성능 향상을 위한 자료로 활용될 것으로 기대한다.

ABSTRACT

Recently, The cloud computing technology is emerging as an important issue in the world, and In 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 management models through case studies and experiments to the threats and vulnerabilities of the cloud computing. and In the future, this is expected to be utilized as a basis for the security design and performance improvement.

Keywords: Cloud Computing, Cloud Service, Vulnerability, Security threat, Hypervisor, Virtualization

I. 서 론

최근 클라우드 컴퓨팅(cloud computing) 기술의 등장은 기존 서비스와 네트워크 체계에 매우 큰 변화를 가져오고 있다. 이와 같은 변화는 기존의 네트워크 패러다임(paradigm)을 변화시키고, 서비스와 하드웨어 및 소프트웨어 분야에도 혁명을 일으키고 있으며, 클라우드 컴퓨팅은 현재 IT기술에 대한 견인차 역할을 하고 있다고 해도 과언이 아닐 정도의 파급 효과를 갖고 있다. 클라우드 컴퓨팅 기술은 스마트 기기와 신기술(그리드 컴퓨팅, 홈 네트워킹 등)들과 함께, 유비쿼터스(ubiquitous) 시대의 구현을 점차 앞당기고 있으며, 여러 기술들과의 유기적인 결합을 통해, 새롭고 다양한 서비스들을 만들어 가고 있는 주요 기술 중에 하나로 자리 잡아 가고 있다. 이러한 클라우드의 대표적인 기술로는 가상화(virtualization)와 자원의 공유(sharing) 및 임대(tenancy) 등이 있으며, 이러한 기술들을 응용한 가상 서버(virtual server)와 스토리지(storage) 서비스들은 유동적 물리매체의 개념과 함께, 스마트 기기를 이용한 다양한 서비스들로 다시 태어나고 있다. 또한 클라우드 서비스들은 편의성과 신속성, 이동성 등의 장점들을 포함하고 있어, 더욱 대중화의 확산속도를 높이고 있다. Table 1.은 국내외 클라우드 컴퓨팅기술의 동향을 나타낸 것으로 향후, 전 세계의 클라우드 시장이 활성화 될 것으로 예상된다.

접수일(2013년11월 4일), 게재확정일(2013년 12월 4일)
† 주저자, nerdrandy@dongduk.ac.kr
‡ 교신저자, nerdrandy@dongduk.ac.kr(Corresponding author)

Table 1. National and international trends in the cloud

국내	- 한국인터넷진흥원, 한국정보화진흥원, 정보통신정책연구원 등에서 IT트렌드 분석과 관련, 클라우드를 중점 과제로 제시 - '12년 국내 클라우드 컴퓨팅 시장은 2009년 대비 221%가 성장한 4조 2천억원 규모로 성장을 예상(KT경제연구소)
국외	- '12년 주목해야 할 10대 IT 전략기술로 클라우드 컴퓨팅 선정(가트너,'11. 10.) - '12년전 세계 클라우드 서비스 시장 규모는 420억 달러로 예측(IDC,'11. 11.) - ICT 2012 전망에 따르면, 클라우드 컴퓨팅은 아태지역에서 주류를 이룰 것으로 전망 (프로스트 앤 설리번, '12. 1.) - 퍼블릭 클라우드에 대한 소비자와 관련한 기업들의 지출이 '10년 230억 달러에서 '15년 1,100억 달러로 약 5배 증가 전망('11. IHS iSuppli)

그러나 서비스의 제공자나 사용자 모두 클라우드의 긍정적인 측면만을 보아서는 안 될 것이다. 클라우드 컴퓨팅 기술의 발전과 병행하여 해킹기술 또한 진화하고 있다는 점도 염두해 두어야 하기 때문이다. 최근 클라우드 서비스의 취약성(vulnerability)을 악용한 새로운 공격들이 증가함에 따라, 클라우드 컴퓨팅 보안에 대한 우려와 관심이 깊어지고 있다. 특히, 클라우드 컴퓨팅은 기존 IT체계와 많은 차이점을 갖고 있어, 가상화와 공유 및 임대 등을 응용한 서비스들에 새로운 취약성들을 나타나고 있다. 보안 분야에 있어, 취약성은 대응기술개발과 방어 전략의 수립에 매우 중요하며, 취약성을 어느 정도 빨리 발견하느냐 하는 문제는 클라우드 서비스의 안전성에 매우 큰 영향을 미치게 된다. 그러나 이와 같은 취약성을 예측하는 것은 쉽지 않다. 특히 클라우드 컴퓨팅의 경우, 계속해서 진화해 가고 있기 때문에 서비스의 종류와 방식에 따라, 다양한 취약성이 잠재할 가능성이 매우 높다. 그리고 이러한 클라우드의 취약성에 대해서는 여러 기관 및 기업들이 자체 서비스에 대한 취약성들을 일관성이 결여된 취약 항목들만을 나열하고 있기 때문에 취약성에 대한 대응방안을 모색하기 어렵다. 그리고 취약성에 대한 포괄적이고, 일관성 있는 분석과 취약성 관리 모델이 필요하며, 클라우드 컴퓨팅 환경에 적합한 대응기술의 개발 및 표준화 작업과 서비스의 취약성에대한 효율적인 대응방안을 위한 분석이 함께 요구된다. 따라서 본 논문은 클라우드 컴퓨팅 기술에 필요한 위협(threat)및 취약성들의 비교분석을 통해, 향후, 클라우드 컴퓨팅의 보안 체계 및 네트워크의 구축에 필요한 자료로 활용될 수 있을 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해, 논문의 Ⅱ장은 클라우드 컴퓨팅 서비스 및 특징들을 알아보고, Ⅲ장은 클라우드 서비스의 보안적인 관점에 대해 알아본다. 그리고 Ⅳ장은 클라우드 서비스의 보안 위협요인과 취약성에 대해 비교분석을 통한, 효과적인 취약성 분류 모델과 대응방안을 알아보며, Ⅴ장의 결론 부분으로 이글을 마치도록 한다.

II. 관련 연구

2.1 클라우드 컴퓨팅 기술

클라우드 컴퓨팅에 대한 정의는 기업 및 연구기관, 리서치 기관들에 따라, 조금씩 달리하고는 있지만, 공통적으로 자원의 공유 및 임대 서비스를 통한 성능의 극대화와 시스템 운영 등의 경제적 부담의 경감 등을 장점으로 다루고 있다. 이와 같은 클라우드 서비스는 다음 Table 2.와 같이 IaaS(Infrastruc ture as a Service), PaaS(Platform as a Ser vice), SaaS(Software as a Service)로 분류하고, 운영형태에 따라, 퍼블릭(public)과 프라이빗(private), 하이브리드(hybrid) 클라우드로 구분할 수 있다[1]. 또한 클라우드의 주요 기술로는 가상화와 공유 및 임대 등이 있으며, 이에 대해서는 다음 절에서 알아본다.

Table 2. Cloud Computing Services

구분		주요개념
서비스 유형	IaaS	하드웨어자원임대・제공
	PaaS	플랫폼 임대・제공
	SaaS	소프트웨어 임대・제공
서비스 운용 형태	퍼블릭 클라우드	불특정 다수 대상
	프라이빗 클라우드	기업 및 기관 내부
	하이브리드 클라우드	결합형태

2.2 가상화 서비스

가상화는 1960년대 IBM에서 'Time Sharing'이라는 주제로 연구되어져 왔으며, 서버 가상화(server virtualization)로도 불리는 운영체제의 가상화로부터 시작하여 물리적이지 않은 2대 이상의 컴퓨터의 기능을 1대의 물리적 컴퓨터에서 운영할 수 있도록 하였다.

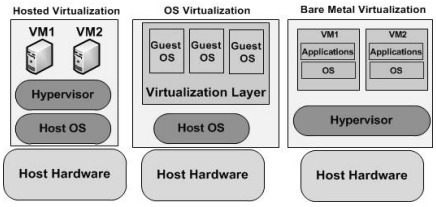


Fig.1. Virtualization computing

Fig.1.에서와 같이 가상화의 종류에는 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. 이러한 가상화 기술은 물리적인 기기를 대신할 가상화 머신(vitrual machine)들과 하이퍼바이저(hypervisor)를 통해, 물리적인 네트워크 통신을 대신한다.

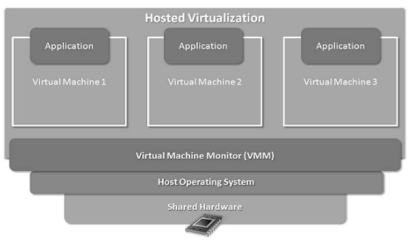


Fig.2. Hosted method

가상화의 내부기술로는 호스티드(hosted)와 베어메탈방식으로 나누어 볼 수 있는데, 여기서 호스티드 방식은 Fig.2.에서와 같이 운영체제가 설치되고, 하이퍼바이저나 버추얼 머신 모니터(virtual machine monitor)라는 소프트웨어가 운영체제 상의 최상위에 설치됨으로써, 애플리케이션 윈도우 내에서 다양한 게스트의 운영체제를 실행할 수 있도록 하는 방식이다[2]. 그리고 베어메탈(bare-metal)방식은 Fig.3.에서와 같이 VMM(Virtual Machine Monitor)이 호스트 운영체제에 의존하지 않고, 시스템 하드웨어와 직접 통신하도록 설치함으로써, 운영체제를 악용한 공격에 강한 특징을 갖고 있다[2].

이러한 가상화 방식들은 자원의 접근 방식이나 모니터링 방식에 따라, 성능(performance) 및 부하(overhead)의 정도에 차이를 갖고 있으며, 어떠한 방식이 효율적인지를 정의하기가 어렵다. 이와 같은

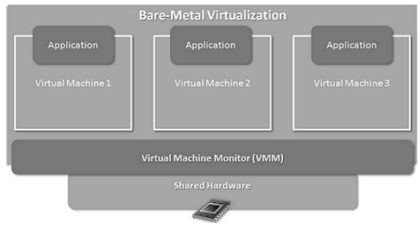


Fig.3. Bare-metal method

클라우드 서비스의 특징들은 어떠한 취약점들이 포함되어 있는지를 예측하기가 어려우며, 기존의 IP와 패턴에 의한 보안기술만으로 대응하기 어려운 원인이기도 하다[3].

2.3 공유 및 임대 서비스

클라우드 기술은 하나의 기술로 완성된 것이 아닌, 세부적인 내부 기술들이 포함되어, 여러 기술들이 조화롭게 운영되는 기술이다. 하드웨어만 보더라도, CPU와 메모리, 기타 저장장치 등 많은 구성 요소들이 서로 조화를 이루며, 상호 연관성을 갖고 있다. 이와 같은 컴퓨팅 자원들은 IaaS, PaaS, SaaS 등의 서비스 모델 형태로 제공되며, 이러한 서비스들의 내부기술이나 하드웨어의 취약 요인으로 인해, 전체 클라우드의 취약점으로 나타나게 된다. 특히, 공유(share) 및 임대(tenancy) 기술은 1대의 시스템 자원을 여러 VM들이 공유하여 사용하거나, 여러 운영체제를 지원하며, 특정 소프트웨어나, 스토리지, 기타 클라우드 서비스에 대한 사용료를 납부하도록 한다[4]. 따라서 공유 및 임대 서비스는 기존에 존재하였던 공격유형들에게도 취약하지만, 컴퓨팅 자원공유에 따른 새로운 공격유형으로의 진화가 예상되고 있기 때문에, 이에 대한 대응이 요구된다. 클라우드의 공유 및 임대 서비스의 예를 통해, 예측하기 어려운 취약성들에 대해 알아본다. 다음의 Fig.4.는 다중과 단일 데이터베이스 임대의 효율성과 안정성을 나타낸 것으로, 단일 임대 방식의 데이터베이스는 효율성 측면에서 다중 임대 데이터베이스보다 우수하며, 안정성 측면에서는 다중 임대 방식의 데이터베이스 사용이 오히려 우수한 것으로 나타내고 있다[5].

이와 같은 클라우드의 공유 서비스는 단일 및 다중 서비스에 따라 효율성과 안정성을 달리하고 있어, 적용 서비스의 종류와 기능, 성능, 환경 등에 따라, 보안 취약성들의 분석과 예측이 어렵다는 것을 알 수 있다.

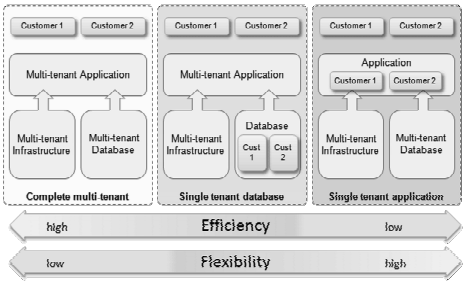


Fig.4. Multi. Single Database Tenancy

그리고 클라우드 서비스의 보안을 위해서는 포함하고 있는 서비스의 특성에 따라, 다양한 취약성들을 효과적으로 분류하고, 이를 체계화한 보안 기술의 개발이 필요함을 알 수 있다.

III. 클라우드 서비스의 보안적 관점

클라우드 컴퓨팅의 특징 중에 하나인 가상화의 보안적 관점은 가트너[GAR10c]의 최근 보고서를 인용해 볼 수 있다. 이 보고서에서는 가상화를 적용한 서버가 물리적인 서버보다도 약 60%정도 안전성이 떨어질 것으로 전망하고 있으며, 가상화 서버의 안전성을 높이기 위해서는 향후, 2015년까지 위험성을 약 30%정도로 감소시키는 것을 목표로 하고 있다[3]. 그리고 [6]은 클라우드 서비스에 대한 취약점들에 대해 취약성들의 노출과 위험이 증가하고 있음을 그림을 통해 나타내고 있으며 1999년부터 2009년까지의 가상화 취약성의 노출에 관한 보고내용에서는 2002년 이후부터 취약성이 지속적으로 증가하였음을 나타내고 있다. Fig.5.는 가상화 시스템에 대한 취약성의 위험도별 보고내용으로 2005년부터 위험성이 높은 취약성들이 급속히 증가하였으며, 2008년부터 2009년 사이 위험도가 높은 취약성들이 급속히 증가했음을 알 수 있다.

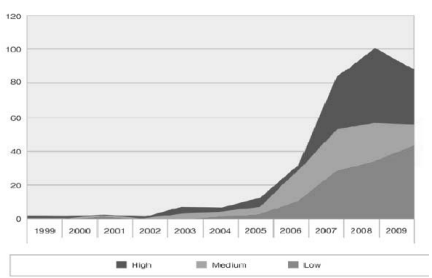


Fig.5. Virtualization vulnerabilities

이러한 가운데, 클라우드 서비스의 가장 핵심기술인 가상화 서비스의 가상머신(virtual machines)의 사용은 운영체제에 매우 의존적이기 때문에 운영체제의 안전성과 보안성을 통해, 가상머신의 보안성을 예측해볼 수 있다. 이와 같이 가상화는 비슷한 보안요인들과 함께 이슈화 되고 있으며, 공유 및 임대 서비스는 다중 임대 구조로 경계가 무너지고 있는 추세이기 때문에 이에 따르는 새로운 보안 취약점들이 증가할 것으로 예상된다[3]. 이러한 전망은 클라우드 컴퓨팅의 보안 관점을 2가지 이슈로 나누어 볼 수 있다. 첫 번째는 서비스를 사용하는 개인 사용자와 두 번째는 서비스를 제공하는 기업 제공자에 대한 보안적 관점이다[6]. 여기서 사용자 입장의 보안적 이슈로는 개인정보의 노출과 감시, 개인 데이터에 대한 상업적 목적의 가공 등에 대한 보안성 보장 등의 문제들이다. 서비스를 제공받기 위해서 제공자에게 개인 정보를 제공해야 하는 부담과 개인 데이터의 관리 및 보안에 대한 신뢰성이 가장 큰 이슈가 되고 있기 때문이다. 또한 제공자의 입장에서는 서비스의 지속, 정보의 훼손 및 유출, 법과 규제의 준수 등이 보안이슈가 되고 있다[8][9]. 결과적으로 클라우드 컴퓨팅은 사용자와 제공자의 두 가지 측면에서 보안적인 접근이 필요하며, 위협 및 취약성이 다루어져야 한다. 다음 장에서는 클라우드 컴퓨팅의 위협과 취약성들의 유형들을 분석하고, 이를 통합할 수 있는 분류모델에 대해 알아본다.

IV. 클라우드 서비스의 위협 및 취약성 분석

최근 클라우드 컴퓨팅은 다양한 서비스들을 선보이며, 클라이언트들의 시선을 모으고 있다. 이전 웹 하드의 형태에서 클라우드 스토리지나, 웹과 모바일 기기를 이용한 소프트웨어 임대 사용 등 다양한 형태의 서비스들을 제공하고 있으나, 서비스를 사용하는 사용자와 제공자의 입장에서는 무엇보다도 상호 신뢰성이 보장되어야만 한다. 클라우드의 스토리지 서비스의 경우, 서비스 제공자가 모든 사용자의 정보 및 데이터를 관리하고 있기 때문에 이에 대한 보안이 매우 중요하다. 그러나 공격은 제공자의 시스템뿐만 아니라, 사용자의 시스템을 이용한 다양한 공격들이 시도되고 있으며, 새롭게 등장하는 서비스들로 인한 다양한 취약성들이 나타나고 있어, 이에 대한 분석과 대응방안이 요구된다. 이에 대해 본 장에서는 다양한 위협과 취약성들에 대해 알아본다.

4.1 보안 위협 분석

본 절에서는 국·내외 클라우드 컴퓨팅의 보안을 위협하는 다양한 요인들을 기관 및 기업별로 분석해 본다. [9]와 [10]은 클라우드 컴퓨팅에 대한 보안 위협요인들을 Table 3.과 같이 나타내고 있다.

Table 3. Cloud service's security threat

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

이러한 요인들을 분석해 보면, 클라우드 서비스에 대한 보안 위협들이라 보기 보다는, 기존 IT체계의 응용서비스에 대한 보안 위협들로써 가상화와 임대 기술에 의한 위협들이 배제되어 있다. 그리고 앞서 언급되었던 바와 같이 클라우드 서비스에 대한 대응 입장이 사용자보다는 서비스 제공자 입장에서의 위협들로 나열되어 있음을 알 수 있다.

다음의 Table 4.는 가트너(gartner) 보고서의 클라우드 서비스 보안 위협 7가지로서, Table 3. 보다는 클라우드 서비스에 대한 보안 위협들에 대해 열거하고 있으며, 가상화나 공유 및 임대에 관련한 위협보다는 데이터에 대한 접근제어와 복구, 저장에 치우친 위협요인들을 다루고 있음을 알 수 있다[10][11].

Table 4. Gartner's security threat

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

Table 5.는 UC Berkely의 10가지 보안 위협요인으로써, 앞서 언급된 보안 위협들보다 클라우드 서비스와 관한 위협들을 다루고 있으며, 전반적으로 데이터에 대한 접근과 서비스 유지, 모니터링, 전송에 관한 위협들을 열거하고 있다[11].

Table 6.은 EINSA의 클라우드 사용자 관점에서의 위협들로써, 클라우드 서비스를 사용하는 사용자 입장에서 서비스의 사용 중, 발생할 수 있는 위협들을 정의하고 있다. 주요 내용으로는 서비스 제공자에 대한 신뢰성 확보와 사용자의 데이터에 대한 보안성 유지를 열거하고 있음을 알 수 있다[11].

Table 5. UC Berkely's security threat

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

Table 6. EINSA's security threat

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

마지막으로 Table 7.은 국내 클라우드 컴퓨팅에 대한 보안 위협에 대해 한국 인터넷진흥원에서는 클라우드 서비스의 핵심 보안 위협들로써, 6가지를 정의하고 있다. 이러한 위협들은 클라우드 서비스의 특성인 가상화와 공유 및 임대에 대한 위협들과 서비스 사용자와 제공자에 대한 위협들에 대해 포괄적으로 언급하고 있다.

Table 7. KISA's security threat

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

이와 같이 여러 기업 및 기관들이 정의하고 있는 다양한 보안 위협들에 대해 알아보았다. 결과적으로 클라우드 서비스의 사용자와 제공자 입장을 반영한 통합적이고, 구체적인 위협요인들의 정의가 필요하며, 이

를 기반 한, 위협요인들의 경감 및 대응방안이 반영된 정의 및 표준모델이 필요함을 알 수 있다.

4.2 보안 취약성 분석

클라우드 컴퓨팅의 보안 취약성은 기존 체계와 많은 차이점을 갖고 있다. 특히, 가상화에 따른 가상머신은 시스템의 성능에 큰 영향을 미치며, 운영체제와의 호환성과도 세밀한 조율이 요구되기 때문이다. 다음의 Table 8.에서는 가상머신의 취약성들에 대해 나타내고 있다[12].

Table 8. Vulnerabilities in a virtual machine

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)

Table 8.은 가상머신의 구성 및 운영상에 복잡함과 가상머신 상호간의 공격 가능성을 취약요인으로 하고 있으며, 가상머신들 간의 자원(resource) 경합으로 인한 자체 취약성 발생 가능성 등을 포함하고 있다. 표8의 취약요인들은 대부분 외부로부터의 직접적인 공격가능성을 고려한 것이 아닌 가상머신들 간의 취약요인들에 대해서 다루고 있음을 알 수 있다[12].

Table 9. Virtualization system vulnerabilities

가상화 취약성	· Footprinting of Virtualized Target Systems
	· Virtualized Botnets
	· Hypervisor Tranversal Attacks
	· Virtual Code Injection Attacks

Table 9.의 가상화 취약성은 앞서 표8에서 기술되고 있지 못한 가상화 시스템의 내·외부 취약성에 대해 기술하고 있다. 가상화 봇넷(botnet)이나, 가상 코드 삽입 공격 등은 가상화에 대한 향후 취약성에 대해 구체적으로 언급하고 있음을 알 수 있다[2].

Table 10. KISA IaaS Checklist

보안 취약성	모바일 웹	· 어플리케이션 변조
		· 입력값 검증
		· 암호화 통신 여부 확인
		· 개인정보취급방침 게시 및 수집 동의 구현
		· 비정상(탈옥, 루팅)단말기의 실행제한
		· 중요정보 평문저장
	웹	· 명령어 삽입 가능성
		· Cross Site Scripting
		· SQL Injection
		· 쿠키 스니핑/조작 가능성
		· 디렉터리 인덱싱
		· 관리자 페이지 접근
		· 백업파일
		· 디폴트 페이지
		· 파일 업로드
		· 파일 다운로드
		· 인증우회
		· 히든필드 점검
		· 취약한 계정/패스워드
		· 에러처리 미흡
		· 사용자 개인정보 노출 취약점
		· 기타 취약점
	어플리케이션	· 어플리케이션 변조
		· 입력 값 검증
	공통	· 중요정보 노출
		· 인증 처리

Table 10.의 내용은 서비스 별 취약성들을 나열하고 있다. 이러한 분류는 새로운 서비스에 따른 취약성이 추가될 경우, 필요한 정보보호 요소와 적용 기술을 구분하기에 다소 용이하지 못하다. 또한 분류된 취약성들은 기존 IT체계에서의 취약성들을 함께 포함하고 있어, 클라우드 서비스에 대한 취약성분석이 모호하다. 따라서 클라우드 서비스에는 다양한 취약성들이 포함되어 있음을 알 수 있으며, 효과적인 보안대응을 위해서는 취약성들에 대한 분류기준의 마련과 기존 보안기술의 적용가능성에 대한 분석이 요구된다.

4.3. 효과적인 대응을 위한 취약성 분류 모델

클라우드 컴퓨팅 기술은 여러 국가 및 기업들이 주도되어 다양한 서비스를 개발하고, 주도권을 얻기 위해 치열한 경쟁을 벌이고 있다. 이러한 가운데 클라우드의 위협 및 취약성들에 대해, 각기 다양한 정의들을

하고 있어, 클라우드 서비스 보안을 위한 대응방안이나 표준화에 큰 영향을 미치고 있다. 따라서 이제까지의 취약성에 대한 분류방식을 서비스나 일관성이 결여된 단순한 나열보다는 이해하기 쉽고, 개발이 용이한 분류체계가 필요하다. 다음에서는 제안하고자 하는 분류 모델에 대해 알아본다. Table 11과 같이 취약성 분류 모델은 기존 분류체계와 달리, 취약성을 클라우드 서비스에 대해 정보보호의 3요소라 부르는 기밀성(confidentiality)과 무결성(integrity), 가용성(availability)에 대해 1차 분류를 하고, 클라우드 서비스를 고려하여, 세부 항목으로 가상화와 공유 및 임대, 기타에 대해 2차로 분류한다. 그리고 Table 11.과 같이 영문표기의 첫 철자를 분류코드의 기호로 사용하여, 취약성 분류코드를 작성한다. 또한 취약성에 대한 상세 내용을 마지막으로 기록한다.

Table 11. Vulnerability classification model

1차 분류	2차 분류	대응방식	취약성 분류코드	취약 내용
기밀성 (C)	- 가상화(V)	차단(B)	CV_B	
	- 공유/임대(T)	탐지(D)	CT_D	
	- 기타			
무결성 (I)	- 가상화(V)	B	IV_B	
	- 공유/임대(T)	B,D	IT_BD	
	- 기타			

취약성에 따른 대응기술을 찾기 위해서는, Table 12.와 같이 취약성 분류코드에 따른, 취약성 코드상세에 따라, 대응기술들을 매칭 시킨다.

Table 12. Response system classification Model

취약성 분류코드	취약성 코드상세	대응기술
CV_B	CV_B_	VMM Firewall
	CV_BD_	VMM IPS
	CV_E_	VMM crypto
	CV_BE	VMM VPN

이와 같은 분류체계는 대부분의 공격유형들을 보안요소와 대응하여 분류해 볼 때, 대응 및 공격 유형의 분석이 쉽고, 새로운 취약성의 발견 시, 추가 및 삭제가 용이하다. 또한 대응 기술의 개발 시에도 대응모델의 제시가 용이하다.

V. 결 론

최근 클라우드 컴퓨팅 기술은 전 세계적인 관심과 기대가 증가하고 있는 가운데, 여러 국가들과 기업들은 다양한 서비스와 응용기술들을 지속적으로 개발하고 있다. 이와 같은 클라우드 컴퓨팅의 등장은 기존 IT 체계에 큰 변화를 불러오면서, 네트워크와 시스템, 기기 등 많은 부분에 있어, 큰 변화를 요구하고 있다. 또한, 클라우드 컴퓨팅 기술로 인해, 해킹 기술이 함께 진화하면서, 기존의 보안시스템에도 큰 변화가 필요하게 되었다. 그 원인에는 클라우드 컴퓨팅만이 갖고 있는 가상화와 자원의 공유, 임대 등의 특징들로 인해, 기존 기술에 존재해왔던 위협과 취약성과는 다르기 때문이다. 이와 같은 차이점은 보안 대응 기술에도 큰 변화가 요구되고 있으며, 클라우드 컴퓨팅 보안을 위한 기술개발이 필요한 실정이다. 이러한 상황에서 클라우드 컴퓨팅의 취약성의 보안관점과 보안요소별, 서비스별 취약성의 분류를 통해, 대응 및 기술개발에 효율성을 더해줄 분류체계의 필요성을 알 수 있었다. 따라서 본 논문은 기존 IT체계와 클라우드 컴퓨팅의 위협 및 취약요인들에 대한 비교분석을 통해, 기존 취약성 관리의 한계를 통해, 분류 모델을 제안하여 보았다. 이와 같은 결과는 기존 IT체계와 클라우드 컴퓨팅 서비스를 보완하기 위한 보안시스템 및 대응 기술개발에 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 클라우드 컴퓨팅의 보안을 위해서는 클라우드 서비스에 따른 다양한 공격기술의 분석과 표준화에 대한 체계적이고, 지속적인 연구가 병행되어야 할 것이다.

References

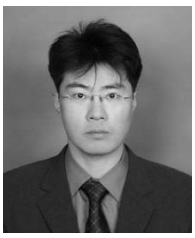
[1] Won-Young Kang, "Recently Trends in Cloud Computing Services," Internet & Security Issue, no. 3, pp. 20-24, Mar. 2012.

[2] Tyson T. Brooks, Carlos Caicedo and Joon S. Park, "Security Vulnerability Analysis in Virtualized 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," Interna-

tional Journal on Recent and Innovation Trends in Computing and Communication, vol. 1(1), pp. 36-39, Jan. 2013.
〔4〕 S.K. Un, N.S. Jho, Y.H Kim and D.S Choi, "Cloud Computing Security Technology," Electronics and Telecommunications Research Institute, vol. 24, no. 4, pp. 79-88, Aug. 2009.
〔5〕 J. Archer, D. Cullinane, N. Puhlmann , A. Boehme, and J. Reavis, "Security Guidance for critical areas of focus in cloud computing v3.0," Cloud Security Alliance, 2011.
〔6〕 Bryan Williams and Tom Cross, "Virtu alization System Security," IBM X-For ce Advanced Research, Apr. 2010.
〔7〕 Young-Jin Chio, Jong-Hei Ra and San g-Hak Lee, "Vulnerability and Security Management System from the Perspective of the Cloud Service Users," Journal of Information Technology and Architecture, vol. 9, no. 4, pp. 401-41 1, Dec. 2012.
〔8〕 Seong-Kyung Un, "Trends in Cloud co mputing security technology," Korea Institute of Information Security and Cryptology, vol. 20, no. 2, pp. 27-31, Apr. 2010.
〔9〕 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.
〔10〕 Md.Tanzim Khorshed, A.B.M. Shawkat Ali, and Saleh 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.
〔11〕 Yang-Jin Lee, "The use of secure cloud services and security considerations," CloudSEC, 2012.
〔12〕 http://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=4&dno=1236&fseq=1

〈저자소개〉



전 정 훈 (Jeong-hoon Jeon) 종신회원
1999년 2월: 숭실대학교 컴퓨터학과 공학사
2000년 2월: 숭실대학교 컴퓨터학과 공학석사
2008년 2월: 숭실대학교 컴퓨터학과 공학박사
2005년 3월~현재: 동덕여자대학교 조교수
〈관심분야〉 정보보호, 포렌식, 클라우드 보안