ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

가상화 환경 위험도 관리체계화를 위한 취약점 분석☆

The Vulnerability Analysis for Virtualization Environment Risk Model Management Systematization

박 미 영[1] 승 현 우[1] 임 양 미[2*]
Mi-Young Park Hyen-Woo Seung Yang-mi Lim

요 약

최근 IT분야에서 클라우드 컴퓨팅 기술은 유연성, 효율성, 비용절감이라는 특징을 갖고 있어 현 사회에 빠르게 보급되고 있다. 그러나 클라우드 컴퓨팅 시스템은 보안의 취약점을 크게 갖고 있다. 본 연구에서는 클라우드 컴퓨팅 시스템 보안의 취약점 해결을 위해, 가상머신의 취약점에 대한 유형 및 영향분석 타입(impact type)을 정하고, 가상머신의 취약점에 대한 위험도 평가에 따른 우선순위를 정하였다. 취약점 분석을 위해서는 오픈프레임워크인 CVSS2.0을 기반으로 취약점에 대한 위험도 측정 기준을 정의하고 해당 취약점마다 점수를 매겨 위험도 측정을 체계화하였다. 제시된 취약점 위험도 기준은 취약점의 근본적인 특징을 제시하고 취약점에 대한 위험도를 제공하여 취약점 최소화를 위한 기술적 가이드를 작성하는 데에 활용 가능할 것으로 판단된다. 또한 제시된 취약점 위험도 기준은 연구내용 자체로 의미가 있으며 향후 추진될 기술 정책프로젝트에서 활용될 수 있다.

주제어 : 가상화 환경, 취약점, 위험도

ABSTRACT

Recently in the field of IT, cloud computing technology has been deployed rapidly in the current society because of its flexibility, efficiency and cost savings features. However, cloud computing system has a big problem of vulnerability in security. In order to solve the vulnerability of cloud computing systems security in this study, impact types of virtual machine about the vulnerability were determined and the priorities were determined according to the risk evaluation of virtual machine's vulnerability. For analyzing the vulnerability, risk measurement standards about the vulnerability were defined based on CVSS2.0, which is an open frame work; and the risk measurement was systematized by scoring for relevant vulnerabilities. Vulnerability risk standards are considered to suggest fundamental characteristics of vulnerability and to provide the degree of risks and consequently to be applicable to technical guides to minimize the vulnerability. Additionally, suggested risk standard of vulnerability is meaningful as the study content itself and could be used in technology policy project which is to be conducted in the future.

☞ keyword : virtulaization environment, vulnerability, risk model

1. 서 론

최근 IT분야에서 새로운 기술 트랜드는 클라우드 컴퓨팅이다. 클라우드 컴퓨팅의 정의는 여러 가지 개념으로 정의되고 있지만, 헤이저와 니콜렛에 의하면 "대용량의 데이터 및 응용프로그램들이 확장 가능하고 가상화된 자원들이 인터넷 상에서 e-business의 형태로 제공되는 컴퓨팅의 한 형태"라고 정의하고 있다.[1] 클라우드 컴퓨팅과 가상화 기술은 물리적 자원을 논리적으로 할당하고 관리하는 기술로서 유연성, 효율성, 비용절감이라는 특징을 갖고 있다. 그러나 기존환경에서 클라우드 환경으로 전환하면서 많은 문제점들이 발생되고 있는데 그 중 가장 두드러지게 나타나는 것이 보안문제이다. 현재 클라우딩 컴퓨터 시스템에서의 보안 문제는 가상화 취약점(악성코드 및 서비스 가용성 침해), 정보위탁(소유와 관리 분리)에 따른 정보 유출 위협, 자원공유 및 집중화에 따른 서비스 장애, 단말기 다양성에 의한 정보 유출, 분산 처리에 따른 보안 적용의 어려움, 법규 및 규제의 문제 등을 들 수 있다. 이 중에서 가장 핵심 기술인 가상화 기술에 대한 보안 취약점은 시급히 해결해야할 가장 큰 문제이다.[2] 가상

1 Computer Sicence, Seoul Women's University, Nowon-gu, Seoul, 139-774, Korea
2 Digital Media, Duksung Women's University, Dobong-gu, Seoul, 132-714, Korea
* Corresponding author (yosimi@duksung.ac.kr)
[Received 13 February 2013, Reviewed 20 February 2013, Accepted 3 June 2013]
☆ This work was supported by a special research grant from Seoul Women's University(2013).

http://dx.doi.org/10.7472/jksii.2013.14.3.23

화 취약점의 해결은 클라우드 컴퓨팅 환경의 보안을 위해서 반드시 고려되어야 하는 사항이다. 이 해결을 위하여 우선적으로 취약점에 대한 위험도 측정을 수행해야 한다. 국외에서도 이러한 취약점을 DB로 관리하고 해당 취약점마다 점수를 매겨 위험도 측정을 체계화하고 있다.

본 연구에서는 클라우드 컴퓨팅의 가상화 환경에서 발생 가능한 보안 취약점을 파악하기 위해 현재 상용되는 가상머신의 취약점을 분석하고 각 취약점에 대해 가장 많이 사용하고 있는 오픈프레임워크인 CVSS 2.0을 기반으로 취약점 우선순위를 분석하여 가상화 환경에 특화된 위험도 측정 기준을 정의하고 위험도를 측정할 수 있도록 다음과 같은 세부 내용을 수행하고자 한다. CVE, CVSS는 미국의 Mitre에서 제안한 방식이지만, 일본, 캐나다, 영국 등으로 국제적으로 참조하여 사용하고 있어 이들의 표준을 본 연구에서도 참조하고자 한다.

- CVE(정보보안취약점표준) 기반으로 가상머신의 취약점 유형(type)을 분석한다.
- CVE기반으로 가상머신의 취약점 영향(impact)을 분석한다.
- CVSS를 기반으로 클라우트 컴퓨팅 환경을 고려한 취약점 우선순위 분석을 통해 위험도 측정 기준을 개발한다.

2. 관련연구

정보보호 및 취약점에 관한 연구들은 개별정보보호 분야와 정보보안에 대한 정책방안에 대한 전략적 접근으로 크게 두 분야로 볼 수 있다. 개별정보보호 분야의 연구는 기술개발 및 기술정책에 관한 연구[3], AHP를 통한 정보보호 인력의 양성방안 [4], 개인정보보호 방안 [5] 등이 있으며, 정보보호에 관한 정책 연구 분야로 기본적인 유형이나 법률, 제도, 예산, 조직관리, 기술적 표준화 정책 연구들이 있다.[6-8] 본 연구에서는 이들 두 분야의 연구들을 종합하여 취약점 분류를 체계화하였으며, 조사된 분류체계 외에 클라우드 컴퓨팅 특징을 시스템 모형에 추가하여 분석하였다.

2.1 클라우드 컴퓨팅의 특징

클라우드 컴퓨팅은 먼저 사용자가 자신의 필요에 따라 무한정의 컴퓨터 자원을 사용할 수 있는 환경을 제공한다. 이것은 초기에 하드웨어와 소프트웨어 시스템을 제공하는 기획을 미리 할 필요 없다. 필요시기에 증가할 수 있고 사용한 후에 비용을 지불하여도 되고 더 이상 자원을 사용하지 않을 수도 있다. 또한 클라우드는 가상화된 컴퓨터 자원들의 풀(pool)을 백앤드잡(back-end job)이나 대화식 잡과 같은 다양한 종류의 워크로드를 수행할 수 있다. 워크로드 최적화 시스템은 서버, 스토리지, 네트워크, 어플리케이션 등 IT인프라 전체를 가상화한 클라우드 컴퓨팅 환경에서 사용자의 다양한 업무 특성에 맞춰 신속히 인프라를 구성할 수 있도록 해주는 특성이 있으며, 많은 하드웨어, 소프트웨어 고장으로부터 복구가 용이하게 이루어지는 특성이 있다. 또한 클라우드 컴퓨팅은 컴퓨팅 자원을 실시간으로 모니터링 할 수 있어 필요에 따라 자원 할당을 재구성하는 것이 용이하다.

위의 내용을 기반으로 클라우드 컴퓨팅의 특징을 두 가지로 요약하였다. 첫째, 워크로드의 확장성 및 신뢰성이다. 워크로드를 최적화할 경우 서버, 스토리지, 네트워크, 어플리케이션 등의 인프라 환경 전체를 클라우드 컴퓨팅 환경하에서 취약점 없이 신속하게 사용자 요구에 따라 확장 가능한지의 여부와 인프라의 신뢰도를 의미한다. 둘째, 자원할당의 확장성이다. 정보자원을 실시간으로 모니터링 함으로써 필요에 따라 자원을 재구성할 수 있는 확장성을 의미한다. 앞서 정의된 클라우드 컴퓨팅의 두 가지 특징인 자원할당 확장성(impact scalability), 워크로드 확장성 및 신뢰성(workload scalability, confidence)은 3장에서 본 연구의 취약점 점수화 시스템 모형에 추가되어 분석될 것이다.

2.2 취약점 분석 기준

취약점이란 정보 시스템의 기밀성(confidentiality), 무결성(Integrity), 가용성(availability)이 눈에 보이거나 보이지 않게 훼손되는 결과를 초래하거나 초래할 수 있는 일련의 상태라 정의할 수 있으며, 최근 직무세분화 작업을 통해 취약점 표준 목록화를 추진하고 있다.[9]

취약점 영향 분석을 위해서는 보안가이드라인을 제시하고 있는 CSA(cloud security alliance)에서 발표한 '클라우드 컴퓨팅 남용 및 불손한 사용', '안전하지 않은 애플리케이션 프로그래밍 인터페이스', '악의를 가지고 있는 내부 관계자', '공유기술의 취약점', '데이터 유실 및 유출, 계정', '서비스 및 트래픽 하이재킹', '공개되지 않은 위협 프로파일'인 클라우드 컴퓨팅 7대 위협 요소를 기반으로 분석하였다. [10]

본 연구에서는 CVE(common vulnerability and exposures) 기반으로 분석하였다. CVE는 시간에 따라 감지된 보안취약점을 정리해 둔 목록이다. 컴퓨터취약점에 대해서 표준화된 이름을 제공하기 위한 네이밍 스키마(naming schema)로써 미국의 Mitre에서 제안하여 현재 많은 보안업체들이

참여하여 취약점 이름의 표준화 작업을 진행하고 있다.[11, 12] 본 연구에서는 CVE 기반의 유형 분류와 원인별로 분류하는 CWE 기반으로 분석하였다. CWE는 다양한 취약점 유형을 분류하여 'CWE-ID'와 같은 식별자를 부여하여 계층구조로 체계화한다[13]. 취약점 분류에 관한 모든 모호성을 방지하기 위해서는 위험도 측정을 CVSS(Common Vulnerability Scoring System, 공통 취약점 점수화 시스템)로 사용하였다. CVSS는 공식, 기본 척도 및 시간척도를 토대로 취약점의 심각성과 위험도를 평가하고 확인할 수 있도록 제공된 오픈프레임워크의 산업표준이다 [14, 15]. CVSS v2 Bse score, Base Metric 취약점의 위험도를 평가하고 취약점 공격에 필요한 조건을 명시하는데 NVD, OSVDB, JVN iPedia의 경우 MITRE의 CVSS v2중 Base score, base Metric을 사용한다. 일본의 국가 취약점 DB인 JVN(Japan Vulnerability Notes)와 JVN iPedia에 수집된 취약점을 공개한다. JVN에서는 자체적인 취약점 평가 및 분류 체계를 사용하는데 반해 JVN iPedia은 미국의 취약점 분류 체계인 CWE와 취약점 위험도 평가 방법인 CVSS, 각 취약점에 유일성을 부여하는 번호체계인 CVE등을 사용한다. CVSS, CWE 등은 모두 기존의 정보기술에 대한 취약점을 고려하여 개발된 것으로 실재 관리체계 구축 시에는 이를 그대로 적용하는 것이 문제가 될 수 있다. 즉, CVSS는 정량적 수치화는 가능하지만 복잡한 다기준의사결정상황에서 수량화가 어렵기 때문에 정성적 요소들을 동시에 합리적이고 체계적인 방법으로 의사결정에 반영할 수 있도록 AHP를 적용하였다.[16] AHP 외에 이들 평가 방법이 최적화 되었는지는 별도의 추가적인 연구가 필요하기 때문에 본 연구에서는 CVSS v2의 Base score와 기본 매트릭스(Base metric), 임시 매트릭스(temporal metric), 환경매트릭스(environmental metric)를 적용하고 AHP를 추가하였다. CVSS는 가장 이용도가 높으며, 기본 매트릭스의 목적은 취약점의 근본적인 특징을 정의하고 전달한다. 따라서 취약점에 특징을 부과하는 목적을 가진 사용자들에게 분명하고 객관적으로 취약점 정보를 제공한다. 더욱 정확하게 자신들의 환경에 존재하는 위험이 반영된 정황정보를 제공받기 위해서는 임시 매트릭스와 환경매트릭스 그룹을 사용하게 된다. [12].

3. 가상머신 취약점 분석

3.1 취약점 유형분석

클라우드 컴퓨팅을 사용하는 사용자들은 네트워크를 통해 자신만의 독립된 환경을 구축하여 고성능 컴퓨팅 시스템을 사용할 수 있게 되어 장소에 구애받지 않고 컴퓨팅 작업을 할 수 있으며 시스템 관리 부담을 덜고 필요한 자원을 할당 받아 자원 활용 효율성을 높일 수 있다. 그러나 가상화 소프트웨어의 경우 소프트웨어 자체에서 발생할 수 있는 보안 취약점이 존재하고 있어 보안위협 요소가 가상화 환경 기반의 클라우드 컴퓨팅 서비스의 신뢰도를 현격히 저하시킬 수 있다.

본 연구에서는 VMware, Xen, VirtualBox 세 종류의 가상머신이 갖는 취약점을 CVE(common vulnerability and exposures) 기반으로 분석하여 보안 위협을 정의하였고 그 결과는 (표 1)과 같다.

(표 1) 가상머신 제품별 취약점 분석
(Table 1) Virtual Machine Products Vulnerability Analysis

제품	VMware	Xen	VirtualBox	합계
취약점 수	381	78	8	467

(표 2)는 VMware, Xen, VirtualBox들의 취약점 유형을 18개로 분류한 결과이다. 이 결과에는 취약점 유형이 나타나지 않은 경우와 불충분한 정보의 경우는 제외시켰다. VMware의 경우 가장 많은 비중을 차지하는 취약점은 버퍼에러(Buffer Errors)로 전체 15%를 차지하는 것으로 나타났으며 Xen의 경우 SQL인젝션 12%, 크로스사이트 스크립트(Cross-Site Scripting) 9%, 버퍼에러 9%를 차지하는 것으로 나타났다. 마지막으로 VirtualBox의 경우 링크 팔로윙(Link Following) 25%, 권한 이슈(Authentication Issues) 12% 순으로 나타났다. 분석결과에 의하면 가장 많은 비중을 차지하는 취약점으로는 버퍼에러 14%, 허용/권한 접근통제(Permissions, Privileges, and Access Control) 9% 순으로 나타났다. 버퍼에러는 버퍼오버플로우의 취약점이며, 사용/권한 접근통제는 자원에 접근하는 공격자나 인가된 사용자의 접근 제어를 위한 보안 정책의 적용이 어려운 경우이다. 가상화 환경에서는 인가되지 않은 자 뿐 아니라 인가된 자에 의한 위협이 발생하는데 여기서 말하는 인가된 자는 서비스 사용자뿐만 아니라 관리자도 포함 된다. 공격자가 시스템 자원에 접근하여 영향을 미치는 자산 관리 에러(Resource Management Errors), 공격자에 의해 민감한 정보유출이 가능한 정보유출/공개(Information Leak/Disclosure)의 취약점 유형도 나타났다.

(표 2) 가상머신 취약점 유형 분석
(Table 2) Virtual Machine Vulnerability Type Classification

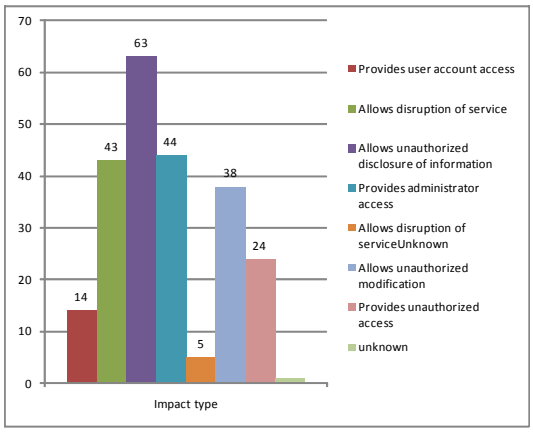
제품 / 취약점유형	VMware	Xen	VirtualBox
Permissions, Privileges, and Access Control	29	4	1
Buffer Errors	48	6	
Resource Management Errors	20	1	
Information Leak / Disclosure	10		
Input Validation	19	2	1
Design Error	12	3	
Numeric Errors	22		
Path Traversal	7	1	
Cryptographic Issues	3	1	
Configuration	9		
Cross-Site Scripting (XSS)	4	6	
Authorization Issues	2		1
Format String Vulnerability	4		
Other	12	1	
Insufficient Information	45	3	3
-	69	24	
SQL Injection	-	8	
Code Injection		1	
Cross-Site Request Forgery		1	
Link Following		3	2
합계	315	65	8

3.2 취약점 영향분석

본 연구에서는 가상머신에 존재하는 취약점으로 인해 발생할 수 있는 피해 결과인 취약점 영향을 분석하였다. 취약점 영향 분석은 분석방법에 따라 범위와 분류가 달라질 수 있지만, 본 연구에서는 CVE 기반의 영향분석 유형(Impact Type)으로 분석하고자 한다.

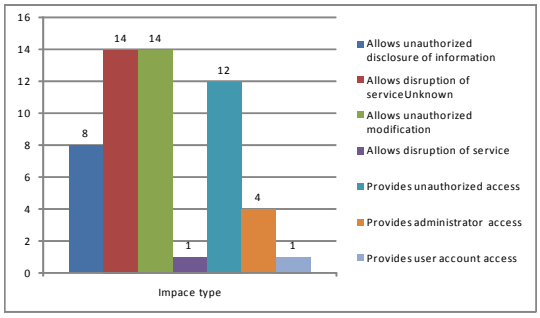
CVE 기반의 영향분석 유형은 사용자 계정 제공(Provides user account access), 서비스 중단 (disruption of Service), 비인가된 자에 의한 정보유출(unauthorized disclosure of information), 관리자 접근(administrator access), 알 수 없는 서비스 중단 허용(Allows disruption of service unknown), 비 인가된 자에 의한 파일 조작 수정, 변경(unauthorised modification), 미인증 접근(unauthorized access), 기타(unknown) 7개로 나타나고 있으며 취약점 영향 유형 294개가 존재한다.

VMware의 경우 사용자 계정 제공 14개, 서비스 중단 허용 43개, 정보 무단공개허용 63개, 관리자 접근 제공 44개, 알 수 없는 서비스 중단 허용 5개, 비 인가된 자에 의한 파일 조작 수정, 변경 38개, 인증 접근 제공 24개, 기타 1개로 분석되었다. 가장 많은 영향 유형으로는 비인가된 자에 의한 정보유출 63개로 분석되었다.



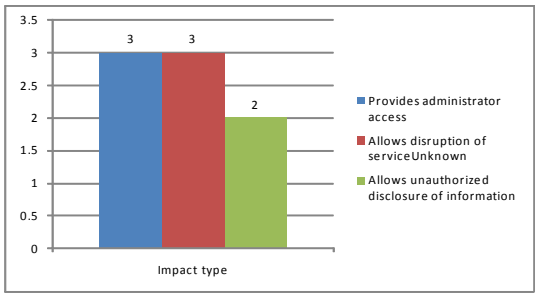
(그림 1) VMware 영향 분석 유형(Impact Type)
(Figure 1) VMware Impact Type Analysis

Xen의 경우 사용자 계정 제공 1개, A서비스 중단 허용 1개, 비인가된 자에 의한 정보유출 6개, 관리자 접근 제공 4개, 알 수 없는 서비스 중단 허용 14개, 비 인가된 자에 의한 파일 조작 수정, 변경 14개, 미인증 접근 제공 12개로 분석되었다. 가장 많은 영향 유형으로는 알 수 없는 서비스 중단 허용, 비 인가된 자에 의한 파일 조작 수정, 변경으로 분석되었다.



(그림 2) Xen 영향 분석 유형 (Impact Type)
(Figure 2) Xen Impact Type Analysis

VirtualBox의 경우 비인가된 자에 의한 정보유출 2개, 관리자 접근 제공 3개, A알 수 없는 서비스 중단 허용 3개로 분석되었다.



(그림 3) VirtualBox 영향 분석 유형(Impact Type)
(Figure 3) VirtualBox Impact Type Analysis

(표 3)은 세 개의 가상머신의 취약점 영향 유형을 분석한 결과로 비인가된 자에 의한 정보유출 73개, 비인가된 자에 의한 파일 조작 수정, 변경 52개, 관리자 접근 제공 51개, 서비스 중단허용 44개 순으로 나타났다.

(표 3) VMware, Xen, VirtualBox 취약점영향비교분석
(Table 3) Impact Type caused by VM Vulnerability

제품 / 취약점유형	VMware	Xen	VirtualBox	
Provides user account access	14	1	-	15
Allows dService Interruption	43	1	-	44
Allows unauthorized disclosure of information	63	8	2	73
Provides administrator access	44	4	3	51
Allows disruption of serviceUnknown	5	14	3	22
Allows unauthorized modification	38	14	-	52
Provides unauthorized access	24	12	-	36
unknown	1	-	-	1
합계	232	54	8	294

3.3 취약점 결과 분석

취약점 분석 결과를 기반으로 가상화 환경의 발생 가능한 주요 보안 위협 요소를 살펴보면 다음과 같다.[17] 우선 가상머신의 취약점을 이용하여 공격자가 권한을 획득하거나 기타 경로를 통해 임의의 악성코드가 실행되는 경우 악성코드는 가상머신의 상호커뮤니케이션 과정에서 다른 사용자 영역에 악성코드를 감염 시킬 수 있다. 가상화 환경에서 호스트는 보안이 확보되어야 할 가장 기본적이고 핵심적인 부분으로서 가상화 환경을 위협하는 공격에 대응해야 한다. 즉, 항상 보안 패치를 최신으로 유지하고 방화벽 뒤에 백신 툴을 배치해야 한다. 그러나 가장 큰 첫 번째 문제로 현재 가상화 기술을 도입하는 영역이 확대되면서 가상머신의 수가 지수적으로 늘어나고 복잡도 증대에 따른 패치 설치관리를 어떻게 할 것인가와 같은 문제가 제기되고 있다. 둘째, 가상머신은 호스트의 파일시스템에 직접 접근할 수 없으므로 다른 가상머신의 가상 디스크에 접근하거나 다른 가상머신의 네트워크 패킷을 볼 수 없다. 그러나 가상머신의 취약점을 이용하여 허가되지 않은 권한을 획득한 경우에는 물리적 디스크에 대한 접근이 가능하고 이로 인한 정보유출이 가능해진다. 실제로 위에서 취약점 분석 결과 취약점을 이용한 공격으로 인해 민감한 정보유출의 사례가 다수 발행하는 것을 확인할 수 있다. 셋째, 취약점 영향 분석 결과 서비스 중단(Service Interruption)로 서비스 거부 및 혼란을 야기 할 수 있다. 이는 분산서비스 공격(DoS, Denial of Service) 의 형태로 볼 수 있는데 이는 각 가상머신이 호스트의 자원을 공유하고 있기 때문에 발생한다. 만일 하나의 가상머신에서 자원을 남용하거나 가상머신에서 실행되는 프로그램이 가상머신 계층을 통과하여 호스트의 권한을 획득하여 악의적인 행위를 하는 경우에는 호스트 또는 다른 가상머신에 서비스 거부 등 서비스 혼란을 야기 할 수 있다. 이는 각 가상머신별로 자원의 사용량을 제한하거나 디스크 파티셔닝을 통해 호스트와 가상머신 영역을 분리함으로써 감소시킬 수 있다. 마지막으로 취약점 유형 분석결과 비 인가된 자에 의한 파일 조작 수정(unauthorized modification)과 같이 가상화 환경에서는 가상머신이 인증되지 않은 자에 의해 변경됨으로써 보안 위협이 발생되기도 한다. 악의적인 목적을 가진 공격자가 또는 사용자가 가상머신을 실행하여 임의로 설정을 변경하고 권한을 획득하는 경우이며, 이는 가상머신의 실행 전 전자성명을 통해 인증하는 과정을 추가함으로써 대응할 수 있다. 단 이를 위해서는 하이퍼바이저가 전자 서명확인이 가능하도록 설계되어야 하고 전자 서명을 위한 키(key) 관리가 필요하다.[18]

3.4 CVSS 기반의 취약점 우선순위 분석

3.4.1 취약점 우선순위 설문조사 개요 및 방법

본 연구에서는 가상머신의 취약점 위험도의 우선순위에 대한 의견수렴을 위하여 설문조사를 실시하였다. 설문조사는 NTIS(국가과학기술지식정보서비스)를 기반으로 본 연구에서 선정한 정보보안 관련 출연(연) 연구원과 국,

공립, 사립대학교 박사급 이상 연구원, 교수들를 대상으로 실시되었다. 특히, 클라우드 컴퓨팅 관련 연구분야를 고려하여 설문대상자를 선정하였다.

설문조사기간은 2010년 10월 4일부터 11월 13일 까지 약 40일 동안 실시되었으며 이메일을 통한 회수방법을 적용하여 설문지를 회수 분석되었다.

3.4.2 평가기준의 선정과 분석 방법

클라우드 컴퓨팅 환경의 가상머신 취약점 위험도의 우선순위를 분석하기 위하여 기존의 문헌 조사 내용과 CVSS 2.0 내용을 참조하고 AHP 분석을 병행하여 수행하였다. 표 4는 본 연구에서 개발한 취약점 위험도 우선순위 선정 평가 모형으로 기존 CVSS 2.0를 기반으로 클라우드 컴퓨팅 환경의 특징을 반영하여 3개의 평가 요소(기본, 임시, 환경 매트릭스)와 14개의 평가기준(항목)으로 구성되어 있다. 표4는 CVSS2.0을 참조한 본 연구의 평가모형이다

(표 4) 본 연구의 평가 모형
(Table 4) Evaluation Model of the Paper

그룹	평가기준 (매트릭스 항목)	세부내용	평가매트릭스 값
기본 매트릭스 (Base Metrics)	공격 수행위치 (Access Vector)	취약점이 공격되는 위치	local, Adjacent network, network
	공격복잡도 (Access Complexity)	공격자가 취약점을 공격하기 위해 목표 시스템 접근에 필요한 접근방법	high, medium, low
	인증 필요여부 (Authentication)	공격자가 취약점을 공격하기 위해 목표시스템에 인증 필요 여부를 평가. 인증 요구가 적을 수 록 더 높은 취약점 점수를 받음.	Multiple, Single, none
	공격영향 - 기밀성 (Confidentiality Impact)	취약점의 성공적인 공격이 기밀성에 미치는 영향을 의미. 기밀성에 미치는 영향이 증가하면, 취약점 점수는 증가함.	none, partial, complete
	공격영향 - 무결성 (Integrity Impact)	취약점의 성공적인 공격이 무결성에 미치는 영향. 무결성에 미치는 영향이 증가할수록 취약점 점수는 증가함.	none, partial, complete
	공격영향 - 가용성 (Availability Impact)	취약점의 성공적인 공격이 가용성에 미친 영향. 가용성은 정보 자원의 접근성, 가용성에 미치는 영향이 클수록 취약점 점수가 높음.	none, partial, complete
	공격영향 - 자원할당 확장성 (Scalability Impact)	취약점의 공격이 자원 확장성에 미치는 영향.	none, partial, complete
임시 매트릭스 (Temporal Metrics)	공격코드 공개여부 (Exploitability)	현재의 공격 기술이나 코드의 이용여부를 의미	unproven, proof of concept, functional, high, not defined
	취약점 패치 단계 (Remediation Level)	취약점 패치에 대한 것으로 개별적인 패치 단계가 마지막 단계로 되면 긴급한 위험이 감소되어 임시 매트릭스 점수를 하향 조절함.	official fix, temporary fix, workaround, unavailable, not defined
	취약점 신뢰도 (Report Confidence)	기술 세부사항의 신뢰성과 취약점 실체에 대한 신뢰도를 측정	Unconfirmed, uncorroborated, confirmed, not defined
환경 매트릭스	피해 (Collateral Damage Potential)	재산이나 도구의 손상을 통한 물리적 자산이나 개인적 잠재적 손실 의미	non, low, l-m, m-h, high, not defined
	취약점영향 시스템분포도 (Target Distribution)	취약점 시스템들의 영역을 의미함	non, low, medium, high, not defined
	보안 요구사항 (Security Requirement)	기본 매트릭스의 공격 영향 - 기밀성, 무결성, 가용성 매트릭스와 대응 관계에 의해 결정됨.	non, low, medium, high, not defined
	워크로드 확장성 및 신뢰성 (workload Scalability)	워크로드를 최적화 할 경우 서버, 스토리지, 네트워크, 애플리테이션 등 IT 인프라 환경 전체를 클라우드 컴퓨팅 환경하에서 취약점 없이 다이내믹하게 사용자 요구에 따라 인프라 확장가능성과 신뢰성 평가 매트릭스	non, low, medium, high, not defined

3.4.3 취약점 우선순위 평가

취약점 위험도 우선순위 분석을 위한 평가 요소별 상대적 우선순위 분석은 정량적 분석 외에 정성적 요소를 체계적인 방법으로 수행하기 위해 AHP 분석을 활용하였으며 ExpertChoice 11.5를 이용하여 분석하였다.[19] AHP는 단순성, 명확성, 간편성, 범용성이라는 특징으로 인해 의서결정 분야에서 널리 사용되고 있다. 이를 위해 다음과 같은 단계를 거친다.

- 1단계 : 목표의 설정 및 의사결정요소의 도출 및 의사결정모델의 설정 - 참여자들의 쌍대비교를 통해 계층의

요소를 총 표본수 만큼 기하평균을 통해 A=[aij ′] 행렬을 구한다.

$$aij = \frac{1}{a_{ij}} \quad (1)$$

• 2단계 : 쌍대비교를 통한 요소들의 판단 - n개의 요소들은 각각 A1, A2, A3,...,An이라 하고 각 요소의 중요도를 w1, w2, w3, wn이라 하면 다음과 같은 행렬로 표현된다.

$$A = \begin{array}{c} \\ A_1 \\ A_2 \\ A_3 \\ \\ A_n \end{array} \begin{array}{c} \begin{array}{ccccc} A_1 & A_2 & A_3 & .. & A_n \end{array} \\ \begin{bmatrix} w_1/w_2 & w_1/w_2 & w_1/w_3 & .. & w_1/w_n \\ w_2/w_1 & w_2/w_2 & w_2/w_3 & .. & w_2/w_n \\ w_3/w_1 & w_3/w_2 & w_3/w_3 & .. & w_3/w_n \\ . & . & . & .. & . \\ . & . & . & .. & . \\ w_n/w_1 & w_n/w_2 & w_n/w_3 & .. & w_n/w_n \end{bmatrix} \end{array} \quad (2)$$

• 3단계 : 논리적 일관성의 검증 - 고유값을 산출하고, 이를 통해 가중치 행렬(W)을 산출한다. 고유값 =l A'-λ · I , l=0 을 만족시키는 값으로 다중 해일 경우, 그 중 최대값을 고유값으로 설정한다.

$$W = \begin{bmatrix} W1 \\ W2 \\ W3 \end{bmatrix} \rightarrow A' \cdot W = \lambda \cdot W \rightarrow (A' - \lambda \cdot I) \cdot W = 0 \quad (3)$$

다음 4단계는 통합 및 그룹 판단 경로가 도출, 5단계 민간도 분석 및 피드백의 분석단계를 거친다. AHP 분석은 쌍대비교를 통한 요소들의 판단결과를 통합하기 전에 각 의사결정 참여자의 판단에 대한 타당성의 검증이 필요하며, 타당성의 검증은 각 의사결정자의 논리적 판단 일관성을 검증하게 된다. 본 분석에서는 의사결정 참여자의 쌍대비교를 통한 평가기준과 대안에 대한 판단 결과, 몇 개 부분에서 논리적 일관성이 낮게 나타났다. 이에 따라, 판단결과를 피드백하여 비논리적인 부분을 재검토 및 보완하는 과정을 수행하였으며, 그 결과 참여자의 논리적 일관성이 크게 향상되어, AHP 분석 모델 전체에서의 비일관성비율이 기준치인 0.1 이내로 개선되었다. 다음은 비일관성비율 계산식이다.

$$\text{비일관성비율: } CR = \frac{CI}{RI}, \quad CI = \frac{\lambda - n}{n-1} \quad (4)$$

(λ: 고유값(Eigen Value), n : 요소의 수)

여기서, CR Consistency Ratio(일치성 비율)

CI : Consistency Index(일치성 지수)

RI : Random Index(확률지표)

확률지표

n	2	3	4	5	6	7	8	9	10
RI	0.00	0.52	0.90	1.12	1.24	1.32	1.41	1.45	1.51

다음은 취약점 우선순위 평가에 따른 중요도와 위험도 우선순위 분석을 정리하였다.

가) 각 매트릭스의 중요도 우선순위 분석

(표 5)는 기본, 임시, 환경 매트리스들의 평가기준 우선순위가 높은 순으로 9순위까지 정리한 것이다. 평가기준들을 종합적으로 살펴보면 인증 필요여부가 26.4%로 가장 중요한 기준으로 나타났으며 이어 공격영향-기밀성 15.2%, 취약점 신뢰도 14.1%, 공경영향-무결성(11.3%) 순으로 나타났다. 반면 공격수행위치, 공격 복잡도, 취약점 영향 시스템 분포도, 피해 등은 2% 미만으로 상대적으로 우선순위가 낮게 나타났다.

(표 5) 각 매트릭스의 평가기준 중요도 우선순위

(Table 5) Importance Priority of Evaluation Criteria

평가지표	중요도	우선순위
인증 필요여부 (기본)	26.4%	1
공격영향-기밀성(기본)	15.2%	2
취약점 신뢰도(임시)	14.1%	3
공격영향-무결성(기본)	11.3%	4
공격영향-가용성(기본)	7.7%	5
워크로드 확장성 및 신뢰성 (환경)	5.0%	6
공격코드 공개여부(임시)	4.7%	7
공격영향-자원할당 확장성(기본)	4.2%	8
취약점 패치 단계(임시)	2.8%	9

(표 6)은 (표 5)의 평가지표 우선순위의 중요도를 기반으로 결과를 종합한 것으로 클라우드 컴퓨팅 환경의 가상머신 취약점 중 3가지 매트릭스 그룹에서는 기본 매트릭스가 68.5%로 가장 중요한 것으로 나타났으며 이어 임시 매트릭스가 21.6% 순으로 나타났다. 반면 환경 매트릭스는 9.8%로 상대적으로 중요도가 낮은 것으로 나타났다.

(표 6) 각 매트릭스 그룹의 중요도
(Table 6) Importance of Each Matrix Group

Goal: 클라우드 컴퓨팅 환경의 가상머신 취약점 우선순위	중요도
기본 매트릭스	68.5%
임시 매트릭스	21.6%
환경 매트릭스	9.8%

나) 각 매트릭스의 위험도 우선순위 분석

아래의 (표 7, 8, 9)는 각 매트릭스의 취약점 위험도에 대한 우선순위를 분석한 결과 위험도 기준에 대해 high, medium, low 3가지 기준을 적용한 것이다. 또한 취약점을 계산할 때 별도의 가중치를 부여하여 각 평가기준치의 오차 범위를 최소화하였다. 표 7의 기본메트릭스 위험도가 가장 높은 것은 인증필요여부(38.6%)였으며, 표 8의 임시 매트릭스의 취약점 위험도 우선순위는 취약점신뢰도(65.2%), 환경매트릭스에서는 워크로드 확장성 및 신뢰성(51.1%)였다. 워크로드 확장성 및 신뢰성은 본 연구에서 클라우드 환경의 특징을 반영하여 추가한 평가기준이다. 각 매트릭스 그룹들에 대한 점수화 계산식은 CVSS 점수화를 토대로 계산하였다.

(표 7) 기본 매트릭스의 취약점 위험도 우선순위
(Table7)Vulnerability Risk Priority of Basic Matrix

기본 매트릭스	중요도	위험도 기준	가중치 (weight)
공격 수행위치	2.7%	low	0.02
공격 복잡도	2.7%	low	0.02
인증 필요여부	38.6%	high	0.3
공격영향-기밀성	22.2%	high	0.2
공격영향-무결성	16.5%	Medium	0.1
공격영향-가용성	11.2%	Medium	0.1
공격영향-자원할당 확장성	6.1%	low	0.06

공격영향-자원할당 확장성은 본 연구에서 클라우드 환경의 특징을 반영하여 추가한 평가기준이다.

(표 8) 임시 매트릭스의 취약점 위험도 우선순위
(Table 8) Vulnerability Risk Priority of Temporary Matrix

임시 매트릭스	중요도	위험도 기준	가중치 (weight)
공격코드공개여부	21.7%	low	0.2
취약점 패치 단계	13.1%	low	0.1
취약점 신뢰도	65.2%	high	0.6

(표 9) 환경 매트릭스의 취약점 위험도 우선순위
(Table 9) Vulnerability Risk Priority of Environment Matrix

환경 매트릭스	중요도	위험도 기준	가중치 (weight)
피해	7.7%	low	0.07
취약점 영향 시스템 분포도	14.0%	low	0.1
보안 요구사항	27.2%	Medium	0.2
워크로드 확장성 및 신뢰성	51.1%	high	0.5

워크로드 확장성 및 신뢰성은 본 연구에서 클라우드 환경의 특징을 반영하여 추가한 평가기준이다.

(표 10)은 각 매트릭스 그룹의 중요도, 위험도, 가중치를 종합하여 정리한 것이다.

(표 10) 각 매트릭스 그룹의 취약점 위험도 우선순위
(Table 10) Vulnerability Risk Priority of Each Matrix Group

Goal: 클라우드 컴퓨팅 환경의 가상머신 취약점 우선순위	중요도	위험도 기준	가중치
기본 매트릭스	68.5%	high	0.7
임시 매트릭스	21.6%	Medium	0.2
환경 매트릭스	9.8%	low	0.08

4. 결과 분석

본 연구에서는 첫 번째로 클라우드 컴퓨팅 환경에서 발생 가능한 보안 취약점 최소화를 위해 클라우드 컴퓨팅의 핵심기술인 가상화 기술의 보안 취약점 유형 및 영향을 분석하였다.

전체적으로 분석해보면 가장 많은 비중을 차지하는 취

약점으로는 버퍼에러 14%, 허용, 권한접근 통제 9% 순으로 나타났다. 버퍼에러는 버퍼오버플로우의 취약점이며 허용, 권한접근 통제는 자원에 접근하는 공격자나 인가된 사용자의 접근 제어를 위한 보안 정책의 적용이 어려운 경우이다. 가상화 환경에서는 인가되지 않은 자 뿐 아니라 인가된 자에 의한 위협이 발생하는데 여기서 말하는 인가된 자는 서비스 사용자뿐만 아니라 관리자도 포함 된다. 공격자가 시스템 자원에 접근하여 영향을 미치는 자산관리 에러, 공격자에 의해 민감한 정보 유출이 가능한 정보유출/공개의 취약점 유형도 나타났다.

이에 외부에서 처리되는 민감한 데이터들은 해당 데이터를 내부에서 처리할 때 일반적으로 수행하는 물리적, 논리적, 인적 통제를 거치지 않는 상태이므로 항상 잠재적 위험성을 가지고 있다고 볼 수 있다. 따라서 보안 관리 정책적인 면에서 클라우드 컴퓨팅을 이용하는 조직은 클라우드 내에서 실제 데이터를 다루는 인력 및 이들에 대한 관리 정보를 서비스제공자에게 요청하여 얻을 수 있어야 한다. 또한 클라우드 서비스 제공자가 데이터를 관리하고 있지만 궁극적으로 해당 데이터의 안전성 및 무결성에 대한 책임은 클라우드 이용자에게 있다. 따라서 전통적인 IT 서비스에서와 같이 클라우드 서비스 제공자에 대한 외부 감사나 보안 기능에 대한 인증이 보장되어야 한다. 이어 클라우드 컴퓨팅 환경에서는 다수사용자의 데이터와 로그 정보가 공존하고 이들이 위치하는 호스트나 데이터 센터들이 지속적으로 변하기 때문에 불법 행위에 대한 조사나 책임 소재 규명이 어려운 경우가 많다. 따라서 클라우드 서비스 제공자는 이러한 조사기능을 보장할 수 있어야 한다.

이어서 가상머신에 존재하는 취약점으로 인해 발생할 수 있는 피해 결과인 취약점 영향 분석은 (표 3)과 같이 7개와 취약점 영향 유형 294개가 존재한다.

VirtualBox의 경우 가장 많은 영향 유형으로는 관리자 접근 제공, 알 수 없는 서비스 중단 허용으로 분석되었다. 비인가된 자에 의한 정보유출 73개, 비 인가된 자에 의한 파일 조작 수정 52개, 관리자 접근 제공 51개, 알 수 없는 서비스 중단 허용 44개 순으로 나타났다.

두 번째로 취약점 위험도 우선순위 분석 결과, 기본 매트릭스가 68.5%로 가장 우선순위가 높은 것으로 나타났으며, 임시 매트릭스가 21.6%, 환경 매트릭스는 9.8%로 상대적으로 중요도가 낮은 것으로 나타났다.

기본 매트릭스 평가 기준에서는 인증 필요여부의 중요도가 38.6%로 가장 높게 나타났으며 이어 공격영향-기밀성(22.2%), 무결성(16.5%), 가용성(11.2%) 순으로 나타났다. 반면, 공격영향-자원할당 확장성, 공격수행위치, 공격복잡도는 10% 미만으로 상대적으로 우선순위가 낮게 나타났다. 임시 매트릭스 평가기준에서는 취약점 신뢰도가 65.2%로 가장 높게 나타났으며, 공격코드 공개여부 21.7%, 취약점 패치 단계는 13.1%로 상대적으로 우선순위가 낮게 나타났다. 환경 매트릭스의 평가기준에서는 워크로드 확장성 및 신뢰성이 51.1%로 가장 높게 나타났으며, 보안요구사항이 27.2%, 취약점 영향 시스템 분포도와 피해는 각각 14.0%, 7.7%로 상대적으로 우순순위가 낮게 나타났다.

인증필요여부는 공격자가 취약점을 공격하기 위해 목표시스템에 인증필요 여부를 여러 번에 걸쳐 평가하기 때문에 이 매트릭스는 인증 프로세스에 대한 복잡성이나 강도를 측정하는 것이 아니라 단지 공격자가 공격 발생 전에 인증을 거치는 지를 말하며 인증 요구가 적을 수 록 더 높은 취약점 점수를 받는다. 위에서 분석한 취약점으로 인해 발생할 수 있는 피해 결과인 취약점 영향을 분석결과에서도 비인가된 자에 의한 정보유출, 비 인가된 자에 의한 파일 조작 수정, 변경의 결과가 나타난 것처럼 인증 필요여부가 취약점 위험도가 가장 높다는 결과와 같다고 볼 수 있다.

취약점 신뢰도는 기술 세부사항의 신뢰성과 취약점 실체에 대한 신뢰도를 측정 하는 것으로 취약점이 솔루션 업체나 다른 신뢰된 곳에 의해 입증될수록 더 높은 점수를 받으며, 이에 따라 위험도 높다고 볼 수 있다.

보안요구사항은 기본 매트릭스의 공격 영향- 기밀성, 무결성, 가용성 매트릭스와 대응 관계에 의해 결정되며, 기본 매트릭스의 공격영향- 기밀성, 무결성, 가용성 매트릭스를 재 측정함으로써 환경 매트릭스 점수를 수정할 수 있다. 공격영향-기밀성은 취약점의 성공적인 공격이 기밀성에 미치는 영향을 의미하며, 기밀성은 비권한자에게 공개하고 접근하는 것을 막을 뿐만 아니라 권한자에게도 제한적인 정보 공개와 접근만을 허가하는 것을 말한다. 기밀성에 미치는 영향이 증가할 수 록 취약점 점수는 증가한다. 공경영향-무결성은 취약점의 성공적인 공격이 무결성에 미치는 영향을 말한다. 무결성은 정보의 신뢰성을 보장할 수 있는 척도를 의미하며, 무결성에 미치는 영향이 증가할수록 취약점 점수는 증가한다. 공격영향-가용성은 취약점의 성공적인 공격이 가용성에 미친 영향을 말한다. 가용성은 정보 자원의 접근성을 말하며 가용한 시스템에 영향을 줄 수 있는 네트워크의 대역폭, 프로세스 사이클, 디스크 공간 소모하는 공격등이며 가용성에 미치는 영향이 클수록 취약점 점수가 높다.

따라서 현재 사용되고 있는 가상화 기술의 취약점 분석을 통해 보안 위협을 정의하고 취약점에 대해 CVSS를 기

반으로 위험도 측정 및 기준 매트릭스를 개발하였다. 이를 통해 클라우드 컴퓨팅 환경에서 발생할 수 있는 취약점으로 인한 위험도의 우선순위를 정의하여 보안 위험에 실질적으로 대응할 수 있다.

5. 결과 및 향후 연구 방향

본 연구의 결과를 기반으로 향후 연구에서는 클라우드 컴퓨팅의 취약점 유형별 대응체제를 정책적인 면에서 설계 구축하는 것이 필요하며, 또한 취약점으로 인해 발생할 수 있는 피해 결과인 취약점 영향에 따른 대응체제 안을 마련하는 연구가 계속되어야 할 것이다. 즉, 클라우드 공급업체의 경우 자신의 클라우드에 대해 철저한 보안 검토와 취약점 시험을 수행하고 있는지와 한 고객이 다른 고객에게 제공된 자원을 볼 수 없는 것이 보장되는지에 대한 실질적이고 구체적인 보안의 정책적 대응체제가 필요하며 이에 대한 연구 또한 병행되어야 할 것이다. 이를 위해 국가차원에서 현재 추진하고 있는 지경부『클라우드 컴퓨팅 활성화 종합계획』등의 동향을 파악하고 클라우드 컴퓨팅의 신뢰성 및 안전성제고를 위한 보안 및 인증체계 구축을 통해 클라우드 환경에서 개인정보보호 등 보안 강화를 위한 기준안을 마련하는 연구가 계속되어야 할 것이다. 또한 본 연구에서 개발한 취약점 우선순위 분석에 따른 위험도 기준을 기반으로 취약점 점수화 시스템 구현에 적용할 수 있는 세부적인 매트릭스에 대한 연구 가 계속되어야 할 것이다.

참 고 문 헌(Reference)

[1] Jay Heiser and Mark Nicolett, “Assessing the Security Risks of Cloud Computing”’, Research Gartner, June 2008.

[2] C.S Lim, “Cloud Computing Security Technology”, Institute of Information Security and Cryptology, Vol.19, No.3. pp.14-17, 2009.

[3] J.I lim, “‘A Study on Technological Development and Policy for Privacy Protection”, Research Report, National Information Society Agency, 2004

[4] T.S Kim, H.J Jun, “Analysis on Information Security Manpower Policy by the Analytic Hierarchy Process”, Institute of Communications and Information Sciences, Vol.31, No.5B, pp. 486-493, 2006.

[5] J.Y Na, “Use and Protection of Personal Information in Ubiquitous Computing Environment”, Research Report, Korea Internet & Security Agency, 2009.

[6] E.J Yu, M.Y Yun, “‘Cyber Security Strategies and Implications of Major Nation”, CIO Report Vol.15, National Information Society Agency, 2009.

[7] K.C Kim, O. Heo, S.J Kim, “A Security Evaluation Criteria for Korean Cloud Computing Service”, Institute of Information Security and Cryptology, Vol. 23, No. 2, pp.1-17, 2013.

[8] S.Y Shin, S.H Song, “A Priority Study for Applying Public Cloud Services in Korea by Mapping the SRM with Overseas Cloud Services in the Public Sector”, Internet and Information Security, Vol.3, No. 3, pp.67~89, 2012

[9] K.Y kim, H.M Na, “The Job Analysis for Information Security Manager”, Institute of Information Security and Cryptology, Vol. 10, No. 3, pp. 63-74, 2000.

[10] CSA(Cloud Security Alliance), “Top Threats to Cloud Computing V1.0”, March 2010.

[11] CVE, http://cve.mitre.org/cve/index.html

[12] D.J Kim, S.J Cho, “An Analysis of Domestic and Foreign Security Vulnerability Management Systems based on a National Vulnerability Database”, Internet and Information Security, Vol. 2, No.2, pp.130-147, 2010.

[13] CWE, http://cwe.mitre.org

[14] FIRST(Forum of Incident Response & Security Teams), http://www.first.org/cvss/cvss-guide.html

[15] Peter Mell, Sasha Romanosky, “A Complete Guide to the Common Vulnerability Scoring System Version 2.0”, 2007

[16] K.T Jho. ‘*Analytic* Hierarchy Process’, Published Dong-hyen. 2003.

[17] Joel Kirch, “Virtual Machine Security Guidelines”, The Center for Internet Security, September 2007

[18] J.Y Kim, “The Virtualization Technology Vulnerability Analysis of Cloud Computing Environment”, Institute of Information Security and Cryptology, Vol. 19, No. 4, pp.72-77, 2009.

[19] Expertchoice Manuak. http://www.expertchoice.co.kr.

◐ 저 자 소 개 ◑

박 미 영(Park Mi Young)
1994년 숙명여자대학교 경영학과 졸업(학사)
2003년 서울여자대학교 대학원 컴퓨터학과 졸업(석사)
2009년 서울여자대학교 대학원 컴퓨터학과 졸업(박사)
2004년~현재 서울여자대학교 정보미디어대학 컴퓨터학과 초빙교수
2008년~현재 과학기술정책연구원 연구개발정책본부 전문연구원
관심분야 : 데이터베이스, 지역과학기술정책, etc.
E-mail : ollive@stepi.re.kr

승 현 우(Hyen-Woo Seung)
1981년 서강대학교 영문학과 졸업(학사)
1988년 일리노이대학교 공대대학원 전산학과 졸업(석사)
1991년 일리노이대학교 공대대학원 전산학과(박사)
1994년~현재 서울여자대학 컴퓨터학과 교수
관심분야 : 데이터베이스, 데이터마이닝, 빅데이터분석, 소프트웨어공학.
E-mail : hwseung@swu..ac.kr

임 양 미(Yang-mi Lim)
1993년 서울과학기술대학교 매체학과 졸업(학사)
1998년 큐슈대학교 대학원 정보전달학과 졸업(석사)
2009년 중앙대학교 대학원 첨단영상대학원 졸업(박사)
2010년~현재 덕성여자대학교 디지털미디어학과 교수
관심분야 : 멀티미디어, 인터랙티브아트, UX/UI etc.
E-mail : yosimi@diksung..ac.kr