공공 IaaS 클라우드 인증제도에 적용할 위험분석 방법에 대한 연구

김선집* · 김기영**

요 약

클라우드 컴퓨팅은 서버의 추가 구축에 대한 비용절감, 데이터 스토리지 확대에 대한 비용 절감, 컴퓨터 자원에 대한 공유, 새로운 기술의 적용에 대한 편의성 등의 장점을 가지고 있다. 그러나 서비스 모델의 다양성으로 인하여 새로운 보안의 우려사항이 높아지고 있어, 이용자가 서비스의 안정성을 신뢰할 수 있도록 인증제도가 운영되고 있다. 이에 본 논문에서는 인증제도의 신뢰성을 확보하기 위해 기존 IT환경에서 적용되던 위험 분석 방법과 달리 공공 IaaS(Infrastructure as a Service) 클라우드 서비스 특징을 고려, 새로운 위험분석 방법을 제안한다.

A Study of Security Risk Analysis for Public IaaS Cloud Certification

Sun-Jib Kim* · Ki-Young Kim**

ABSTRACT

Cloud computing has emerged with promise to decrease the cost of server additional cost and expanding the data storage and ease for computer resource sharing and apply the new technologies. However, Cloud computing also raises many new security concerns due to the new structure of the cloud service models. Therefore, several cloud service certification system were performed in the world in order to meet customers need which is the safe and reliable cloud service. This paper we propose the new risk analysis method different compare with existing method for secure the reliability of certification considering public IaaS(Infrastructure as a Service) cloud service properties.

Key words : Cloud Computing, Risk Analysis, Security, Certification

접수일(2015년 8월 31일), 수정일(1차: 2015년 9월 15일), 게재확정일(2015년 9월 16일)

* 한세대학교 IT학부 정보통신공학과(제1저자)
** 서일대학교 컴퓨터소프트웨어과(교신저자)

1. 서 론

클라우드 컴퓨팅은 IT자원을 사용자의 단말기에 직접 설치하지 않고 '원격으로 빌려 사용하는' 새로운 형태의 컴퓨팅 패러다임이다[1].

기존 IT 환경은 컴퓨터의 자원이 중앙 집중적으로 회사의 자산으로 구매되어 구축함에 따라 돈, 시간, 노력이 집중되는 형태였으나 산업의 변화와 IT를 기반으로 다양한 산업의 융·복합이 가능해짐에 따라, 클라우드 컴퓨팅은 서버의 추가 구축 및 데이터 스토리지 확대의 비용 절감, 컴퓨터 자원에 대한 공유, 새로운 기술의 적용의 편의성 등의 장점을 보유하고 있어 그 활용도가 증가되고 있다.

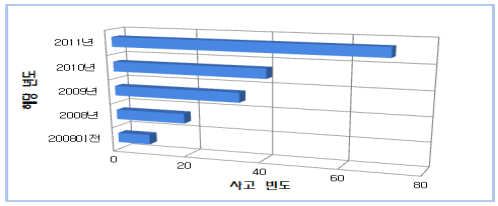
그러나, 이러한 클라우드 컴퓨팅은 다양한 고객의 데이터 및 시스템 집중의 특성으로 인하여 기존의 형태와 다른 새로운 유형의 공격이 발생될 수 있어 악의적인 공격자에겐 더 많은 관심의 대상이 될 수 있다. 이러한 보안상의 문제점으로 인하여 클라우드 서비스 환경에서는 기존 시스템에 적용되었던 보안관리 방법과 다른 방법의 적용의 필요성과 클라우드 서비스 제공자에 대한 대외적인 신뢰도 향상을 위한 인증제도의 활성화가 대두되고 있다[2,3,4].

이에 본 논문에서는 클라우드 서비스 인증제도의 신뢰성 확보를 위해 기존 IT환경에서 적용되었던 위험분석 방법과 달리 다양한 클라우드 서비스 특성을 반영한 위험분석 방법을 제시한다. 2장에서 최근 클라우드 보안사고 분석, 3장에서는 관련연구로 클라우드 서비스 인증제도와 기존 위험분석 방법에 대해 살펴보고, 4장에서는 클라우드 서비스 인증제도에 적용 가능한 위험분석 방법을 제안하며 5장에서는 결론과 향후연구에 대해 기술한다.

2. 최근 클라우드 보안사고 분석

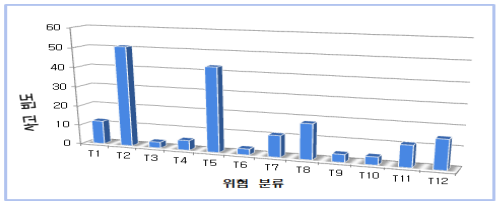
가트너사의 보고서에 따르면 클라우드 컴퓨팅 관련 보안 문제에 있어 사용자에 대한 정보 수집 관리, 규정 준수, 데이터의 물리적 위치, 사용자 데이터 구분, 복구, 조사 지원, 장시간의 생존성 확보 등의 7가지 사항을 거론하고 있다[5]. 즉 클라우드 컴퓨팅은 자원을 보유하지 않고 외부 자원을 사용한다는 특성에 의해 보안적인 측면에서 다양한 문제점이 발생될 수 있음을 보여준다.

컴퓨팅의 안전성 증진과 사용자 교육을 목적으로 설립된 CSA(Cloud Security Alliance)의 2013년 3월의 CSA의 클라우드 컴퓨팅 취약성 사고의 통계자료를 보면 (그림 1)에서 보듯 2011년도의 클라우드 컴퓨팅 취약성 사고의 빈도가 2009년도에 비해 거의 두 배에 이른다[6].



(그림 1) 년도 별 클라우드 컴퓨팅 보안사고 빈도

또한 (그림 2)에서 보듯 주요 사고의 유형은 [표 1]의 기준에 의거 3가지 주요 위협으로 T2가 전체의 29%, T5가 25% 그리고 T8가 10%로 전체의 69%를 차지하고 있다.



(그림 2) 위협 분류별 사고 빈도

또한, 클라우드 컴퓨팅 사고의 75%에 대해 알려진 것으로 분석되고 있으며, 이 중 T2와 T5의 빈도가 두드러지게 증가하고 있는 것으로 분석되고 있다.

다음의 <표 1>은 CSA에 의해 분석된 위협과 언론에 보도 된 클라우드 보안사고의 관계성을 보여주는 매칭 테이블이다.

<표 1> 위협에 관련된 보안사고

구분		보안사고						
		'08	'09	'10	'11	'12	'13	'14
T1	Abuse and Nefarious Use of Cloud Computing							
T2	Insecure Interface and APIs							
T3	Malicious Insiders							
T4	Shared Technology Issues					FS		
T5	Data Loss	A		MS	G			
T6	Account or Service Hijacking							
T7	Unknown Risk Profile							
T8	Hardware Failure		G, MS		A, AP	SF, A		MS
T9	Natural Disasters				A, AP			
T10	Closure of Cloud Service	M						
T11	Cloud-related Malware				F, S	AP, D	E, AD	AP, C
T12	Inadequate Infrastructure Design and Planning				N			

<표 1>의 보안사고 대상 중 A는 아마존, AD는 아도브, AP는 애플, C는 코스트페이스, D는 드롭박스, E는 에버노트, F는 후지쯔, FS는 퍼스트서버, G는 구글, M은 미디어맥스, MS는 마이크로소프트, N은 노키아, S는 소니, SF는 세일즈포스닷컴을 의미하며 알려진 보안사고의 대표적인 특성을 위협에 매칭 하여, 일부의 보안 사고는 다양한 위협과 매칭 되기도 한다.

3. 관련 연구

3.1 클라우드 서비스 보안 인증제도

FedRAMP(Federal Risk and Authorization Management Program)은 미 연방정부에 도입되는 클라우드 제품 및 서비스에 대한 보안성 평가·인증 제도로서[7] 미국 정부기관들이 클라우드 컴퓨팅을 사용하여 서비스를 제공시 안전성, 신뢰성, 비용 효과성을 확보하여 서비스를 사용할 수 있는 근거로 삼고 있다. NIST 800-53r4에서는 17개 분야 225개의 보안 통제사항으로 <표2> 같이 구성되어 있어 광범위하면서, 상(High), 중(Mod), 하(Low)의 영향 및 처음(First), 다음(Next), 마지막(Last), 순서에 관계없는(None)의 적용 우선순위 등의 상세 내용을 포함하고 있다.

<표 2> FedRAMP 보안 통제 베이스라인 구조

Control Name	Control Baselines
Access Control	23
Awareness and Training	4
Audit and Accountability	16
Security Assessment and Authorization	8
Configuration Management	11
Contingency Planning	13
Identification and Authentication	11
Incident Response	10
Maintenance	6
Media Protection	8
Physical and Environmental Protection	19
Planning	6
Personnel Security	8
Risk Assessment	5
System and Services Acquisition	20
System and Communication Protection	41
System and Information Integrity	16
Total	225

CSA(Cloud Security Alliance)는 클라우드 구조, 관리 운영, 보안에 대한 가이드라인을 제공하고, 애플리케이션 & 인터페이스 보안, 감사 보증과 준거성, 비즈니스 연속성 관리, 변경 통제와 구성관리, 데이터 보안과 정보 라이프사이클 관리, 데이터센터 보안, 암호와 키 관리, 위험관리, 휴먼 자원 보안, 인식 및 접근 관리, 인프라 및 가상화, 상호 운영성 및 이동성, 모발 보안, 사고 관리, E-Disc와 클라우드 포렌식, 공급망 관리, 위협과 취약성 관리의 136개 통제항목으로 구성하여 인증 프레임워크에 적용하고 있으며, NIST SP800-53r3, r4의 통제항목간의 관계를 제시하고 있다[8, 9, 10].

일본의 총무성에서는 2008년 4월부터 SaaS(Software as a Service)의 안전과 신뢰성에 관한 정보 공개 인증제도를 도입하여 실행하고 있으며, 2012년 8월부터 기존의 인증제도와 더불어 데이터 센터 안전·신뢰성에 관한 정보 공개 인증제도와 IaaS(Infrastructure as a Service)·PaaS(Platform as a Service)의 안전·신뢰성에 관한 정보 공개 인증제도를 시행함에 따라 이 세 가지 정보 공개 인증제도를 클라우드 서비스의 안전·신뢰성에 관한 정보 공개 인증제도라고 총칭하고 있다.

ASP·SaaS는 비즈니스의 장소, 휴먼 리소스, 재정적 조건, 자본 관계, 서비스의 기본적 특징, 애플리케이션, 인프라구조와 스토리지, 네트워크, 하우징, 서비스 지원의 9개 도메인의 93개 통제항목에 대해, IaaS·PaaS는 107개 통제항목에 대한 기준을 설립하고 인증

을 부여하고 있다[11].

3.2 기존 위험 분석 방법 및 문제점

미국 정부 조직인 NIST(National Institute of Standards and Technology)의 가이드라인인 Special Publication(SP) 800-30에서 9가지 단계의 위험 평가 방법론에 대해 소개하고 있으며, 위험의 필수적 요소인 소스와 이벤트, 취약성 및 발생조건, 영향, 위협 발생 가능성에 대해 다루고 있다. 또한 SP800-39에서는 조직에서 필요한 보안위험 관리 종류에 대한 포괄적인 가이드라인은 제시하고 있다[12].

ENISA(European Network and Information Security Agency)는 ISO/IEC 27005 표준을 기반으로 클라우드 컴퓨팅 보안 위험에 대한 위험등급 평가에 대해 발표하였으며, 정책과 조직의 위험, 기술적 위험, 법적 위험의 세 가지 범주에 대한 35가지 위험에 대한 리스트를 보고하고 있다[13].

또한, 많은 기존의 연구가 클라우드 컴퓨팅 환경에서의 위험 분석 방법에 대해 연구되었다. 내부자에 의한 공격과 가상화 위협에 대한 연구와 클라우드 환경에서의 데이터 전송, SLA(service level agreement)에 대한 연구, 클라우드 컴퓨팅 환경에서의 서비스거부공격에 대한 연구 및 신원 관리에 관한 연구가 진행되고 있다[14]. 즉, 기존 연구는 내부자에 의한 공격, 클라우드 상의 서비스 거부 공격 등 특정 취약성에 초점을 맞춘 연구가 대부분으로 클라우드 서비스 모델의 특징을 고려한 연구는 부족하다.

4. 클라우드 서비스 인증을 위한 위험분석 방법

4.1 서비스 모델과 위험 및 관리통제와의 관계

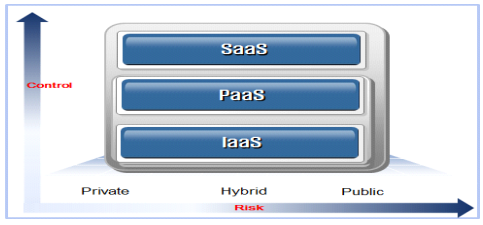
NIST(National Institute of Standard Technology)에 의한 클라우드 서비스 모델은 응용소프트웨어나 웹 애플리케이션을 제공하는 SaaS, 애플리케이션이 동작하는 플랫폼 및 개발 환경이나 도구들을 사용자에게 제공하는 서비스인 PaaS, 고객에게 서비스를 위한 서버의 컴퓨팅 능력, 스토리지, 네트워크 등의 기본적인 컴퓨팅 자원을 제공하는 IaaS로 구분할 수 있으며, 구축 모델로는 클라우드 사용자 혹은 기관 전용의 클라우드인 사설 클라우드(Private Cloud), 클라우드 서비스 제공자가 구축한 서비스를 사용자가 사용하는 공공 클라우드(Public Cloud), 커뮤니티 클라우드 사용자 전용의 커뮤니티 클라우드(Community Cloud), 서로 다른 클라우드를 2개 이상 조합한 하이브리드 클라우드(Hybrid Cloud)로 나누어 질 수 있다[15].

이러한 클라우드의 다양한 서비스 모델과, 구축 모델로 인하여 보안의 위험과 관리 통제사항은 매우 다양해 질수 밖에 없다.

IaaS 모델의 경우 서비스 제공자는 온 디맨드 가상머신, 스토리지, 데이터 베이스 서비스를 고객에게 제공하게 되므로, 클라우드 인프라에 대한 관리를 수행, 고객의 자원에 대한 접근 허용 등의 기능을 하는 반면 고객은 서버의 구동과 정지, 소프트웨어 패키지의 설치, 가상 네트워크 설정, 접근제어 및 방화벽 정책의 설정 등의 다양한 기능을 수행할 수 있어 그 수행 기능과 보안상의 책임이 달라진다.

SaaS모델에서는 대다수의 기능과 책임은 서비스 제공자가 수행함에 따라 보안의 기능과 책임 또한 서비스 제공자가 수행하며 고객은 본인의 데이터에 대한 책임을 가지게 된다. 또한 클라우드 서비스를 받고자 하는 고객에 따라 그 보안의 요구사항 또한 서로 상이할 수밖에 없다.

(그림 3)은 클라우드 서비스 모델에 따른 위험과 관리통제 사항의 상관관계를 보여준다.



(그림 3) 클라우드 서비스별 위험과 관리 관계

4.2 공공 IaaS 클라우드에 적용할 위험분석 방법

본 논문에서는 다양한 클라우드 서비스 중 공공 클라우드 모델의 IaaS 클라우드 서비스에 대해 서비스 제공자가 클라우드 서비스 인증 취득 시 활용할 수

있는 위험분석 방법에 대해 논하며, 이에 다음의 수식을 기반으로 위험분석을 수행하도록 한다.

Risk= SM ◦ CR ◦ AS ◦ VN ◦ TH ◦ PR

SM(Service Model) 행렬은 클라우드 컴퓨팅 구축 방법에 따라 서비스 모델과 구축 모델로 세분화 할 수 있으나, 본 논문에서는 다음의 표와 같이 SaaS, PaaS, IaaS로 서비스 모델로만 간단히 구분하였다. 이에 다음의 <표 3>은 서비스 모델과 이를 사용하는 고객에 대한 행렬을 보여준다.

<표 3> SM(Service Model) 행렬

	기업	정부	개인
SaaS	SM_S1	SM_S2	SM_S3
PaaS	SM_P1	SM_P2	SM_P3
IaaS	SM_I1	SM_I2	SM_I3

보안 요구사항인 CR(Client Requirement)행렬은 SM(Service Model) 행렬의 고객에 대응하는 가용성, 무결성, 기밀성으로 세분하고[16, 17] 그 가중치를 기업, 정부, 개인의 이해관계자가 중요시 하는 부분에 대해 가중치를 H(High), M(Medium), L(Low)로 부여할 수 있으며 본 논문에서는 기업과, 정부, 개인의 클라우드 서비스 이용 시 중요하게 보는 관점을 <표 4>와 같이 가정한다.

<표 4> SM(Service Model) 행렬

	가용성	무결성	기밀성
기업	H	M	H
정부	M	M	H
개인	M	H	H

또한, 보안 요구사항에 대한 자산 구성 요소 간 행렬인 AS(Asset) 있어서는 본 논문이 IaaS환경에 대한 위험분석에 대해 논의함에 따라, 가상적인 자원보다는 실 구성요소에 대해 고려해야 함으로 <표5>와 같이 자산 항목을 정의할 수 있다. 다만, 추가적으로는 그 동안의 보안사고가 시사하는 것과 같이 물리적인 보안의 문제점이 매우 큰 이슈임에 따라 시설 부문과 IaaS상의 가상 클라이언트 환경을 제공해주는 하이퍼바이저(Hypervisior)에 대해서는 자산 항목에 포함하여야 할 것이다.

<표 5> AS(Asset) 행렬

	어플리케이션	서버	네트워크	DB	보안솔루션	시설	하이퍼바이저
가용성	H	H	H	H	H	H	H
무결성	H	M	M	H	H	M	H
기밀성	M	M	M	H	H	M	H

취약성에 대한 행렬인 VU(Vulnerability)에 대해서는 IaaS상의 물리적인 자산에 대해서는 기존 IT환경의 위험분석에서 활용되었던 취약성을 매핑할 수 있으며, 하이퍼바이저에 대한 취약성은 가상화 기반 취약성, 가상화 기반 보안장비 운영의 취약성, 운영 관리의 취약성 등을 고려할 수 있다[18].

보안위협에 대한 행렬인 TH(Threat) 있어서는 <표1>의 CSA의 12가지 보안 위협요소에 대해 반영한다.

위에서 논의하였듯 클라우드 컴퓨팅 보안사고 중에서 투명하게 알려진 사고는 전체 사고의 75%이므로 위협의 가능성은 발생빈도와 심각도 중 높은 것을 선택하도록 계산한다.

위협 가능성(PR) = Max(심각도 or 발생빈도)

이에 따라 위협의 가능성 PR는 <표 6>의 기준표를 작성하고 <표 7>과 같이 도출할 수 있다.

<표 6> 심각도와 발생빈도 등급기준

구분	등급(점수)	기준	평가요소
발생빈도	H(3)	10회 이상	보고된 보안사고 건수 또는 관련 사건
	M(2)	4 ~ 9회	
	L(1)	0 ~ 3회	
심각도	H(3)	80 ~ 100%	CSA의 설문조사
	M(2)	20 ~79%	
	L(1)	0~19%	

<표 7> 위협 가능성

CSA기준	발생빈도	심각도	가능성
T1	12(H)	91%(H)	H
T2	51(H)	91%(H)	H
T3	3(L)	87%(H)	H
T4	5(M)	90%(H)	H
T5	43(H)	81%(H)	H
T6	3(L)	88%(H)	H
T7	11(H)	84%(H)	H
T8	18(H)	81%(H)	H
T9	4(M)	82%(H)	H
T10	4(M)	unknown	M
T11	11(H)	unknown	H
T12	15(H)	unknown	H

5. 결 론

클라우드 서비스의 지속적인 성장에도 불구하고, 다양한 이해관계자가 하드웨어 자원을 공유하는 이유로 클라우드 서비스는 악의적인 공격자에 의해 기존의 시스템에 비해 더 매력적인 공격대상으로 여겨질 수 있다. 이에 다양한 서비스 모델과 구축 모델을 기준으로 클라우드 서비스 제공자의 보안수준을 이해관계자에게 명확하게 제시할 수 있는 보안인증제도 도입이 필요하다. 또한, 이러한 보안인증제도의 신뢰성을 확보하기 위해 가장 중요한 것은 클라우드 서비스별 위험분석 방식이다. 그러나 기존의 기업이 자체 IT자산을 운영하던 전통방식과 클라우드 환경의 가장 큰 차이점인 하이퍼바이저를 활용한 가상 환경에 대한 위험 분석이 적절하게 수행되지 않는다면, 클라우드 서비스 보안인증제도의 실효성 문제가 발생될 수 있다. 다시 말해서 위험분석이 적절하게 수행되지 않는다면, 다른 통제사항에 대한 적절한 통제수행 방법이 설정 될 수 없기 때문에 위험에 대한 적절한 대응책을 수립할 수 없게 된다.

이에 본 논문에서는 클라우드 서비스를 SaaS, PaaS, IaaS의 3가지 서비스 모델과, 사설 클라우드, 공공 클라우드, 커뮤니티 클라우드, 하이브리드 클라우드의 4가지 구축 모델을 고려한 클라우드 서비스 보안인증을 위한 위험분석 중 공공 IaaS 클라우드 서비스에 활용할 수 있는 기술부분의 위험분석 방법을 제시하였다. 물론 위험분석에 있어 관리적, 물리적인 위험분석 또한 수행되어야 하며, 향후 하이퍼바이저에 관련된 취약성에 대한 연구 및 고객 등 서비스 이해관계자의 보안요구사항들이 더욱 자세히 분석되어 제시된 위험분석 방법에 확대 적용될 필요성이 있다. 또한, 본 논문에서 논의하지 않은 서비스 모델 중 공공 클라우드 모델의 SaaS의 경우 다양한 클라우드 서비스의 이해관계자가 존재할 수 있어 더욱 세밀한 분석을 통한 위험분석이 이행될 수 있도록 연구되어야 할 것이다.

참고문헌

[1] S.K.Eun, “Cloud Computing Security Technology Trends”, Review of Korea Institute of Information Security and Cryptology, Vol.20, No2, pp.27-31, 2010.

[2] 신종회, “클라우드 보안 인증 스킴과 해결과제”, 정보보호학회지, 제22권 제6호, pp29-33, 2012.

[3] 고갑승, “보안성이 강화된 클라우드 서비스 평가·인증 체계에 관한 연구”, 보안공학연구논문지, 제9권, 제6호, 2012.

[4] 정성재, 배유미, “클라우드 보안 위협요소와 기술동향 분석”, 보안공학연구논문지, 제10권, 제2호, 2013.

[5] Jon Brodkin, “Gartner:Seven Cloud-computing security risks,” Network world, 2008.

[6] https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview

[7] FedRAMP(The Federal Risk and Authorization Management Program). http://www.fedramp.gov/resources/nist-publications/

[8] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[9] https://cloudsecurityalliance.org/research/security-guidance/

[10] https://cloudsecurityalliance.org/download/cloud

-controls-matrix-v3/

[11] Kwang-Kyu Seo, “A Comparison Study of Korea and Japanese Cloud Service Certification Systems”, The Journal of Digital Policy & Management, 2013.

[12] NIST, “Managing Information Security Risk:organization, mission, and information system view SP800-39”, National Institute of Standards and Technology(NIST), 2011.

[13] ENISA. “Cloud Computing: benefits, riska and recommendations for information security”, The European Network and Information Security Agency(ENISA), 2009.

[14] Sameer Hasan Albakri, “Traditional Security Risk Assessment Methods in Cloud Computing Envrionment: Usability Analysis”, IRICT(2014) 483-495, 2014.

[15] P. Mell and T. Grance, "The NIST Definition of Cloud Computing(Draft)", SP 800-145.

[16] Subashini, S., Kavitha, V., “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, 2010.

[17] Wooley, P., “Identifying Cloud Computing Security Risks”, University of Oregon, Master’s Degree Program, 2011.

[18] 정성재, 배유미, “클라우드 보안 위협요소와 기술 동향 분석”, 보안공학연구논문지, 제10권, 제2호, 2013.

[저 자 소 개]

김 선 집 (Sun-Jib Kim)

1999년 2월 강남대학교 전자계산학과 공학사
2001년 2월 숭실대학교 컴퓨터학과 공학석사
2010년 2월 한세대학교 IT학과 공학박사
2012년 9월 ~ 현재 : 한세대학교 IT학부 정보통신공학과 교수

email : kimsj@hansei.ac.kr

김 기 영 (Ki-Young Kim)

1996년 2월 상지대학교 전자계산학과 이학사
1999년 2월 숭실대학교 컴퓨터학과 공학석사
2003년 8월 숭실대학교 컴퓨터학과 공학박사
2004년 3월 ~ 현재 : 서일대학 컴퓨터소프트웨어과 부교수

email : ganet89@seoil.ac.kr