Journal of Convergence for Information Technology
Vol. 9. No. 9, pp. 27-32, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.9.027

CloudHIS의 개인 의료정보를 위한 보안강화에 관한 연구

조영성[1], 정지문[2], 나원식[2*]
[1]한양여자대학교 스마트 IT학과 교수, [2]남서울대학교 컴퓨터소프트웨어학과 교수

A Study on the Security Enhancement for Personal Healthcare Information of CloudHIS

Young-Sung Cho[1], Ji-Moon Chung[2], Won-Shik Na[2*]
[1]Professor, Department of Smart IT, Hanyang Woman University
[2]Professor, Department of Computer Science, Namseoul University

요 약 유비쿼터스-헬스케어의 발전과 함께 사이버 공격에 대처하기 위한 개인의료정보 처리를 위한 CloudHIS의 망분리를 기반으로 한 보안 강화를 제안한다. 모든 보안 위협으로부터 보호하고 명확한 데이터 보안 정책을 수립하기 위해 CloudHIS용 데스크톱 컴퓨팅 서버를 클라우드 컴퓨팅 서비스에 적용한다. 하이퍼 바이저 아키텍처를 갖춘 두 대의 PC를 사용하여 물리적 망분리를 적용하고 KVM 스위치를 사용하여 네트워크를 선택할 수 있다. 다른 하나는 두 개의 OS가 있는 하나의 PC를 사용하는 논리적 망분리이지만 네트워크는 가상화를 통해 분할된다. 물리적 망 분리는 인터넷과 업무망 모두에서 액세스 경로를 차단하기 위해 각 네트워크에 대한 PC의 물리적 연결이다. 제안된 시스템은 사용자의 실제 데스크톱 컴퓨터에서 서버 가상화 기술을 통해 인트라넷 또는 인터넷에 액세스하는 데 사용되는 독립적인 데스크톱이다. 보안 강화를 처리하기 위해 네트워크 분리를 통해 의료병원 정보를 처리하는 클라우드 시스템인 CloudHIS를 구성하여 해킹을 방지하는 적응형 솔루션을 구현할 수 있다.

주제어 : 전자의료기록, CloudHIS, 환자정보, 클라우드 컴퓨팅, 클라우드 서비스

Abstract Along with the growth of u-Healthcare, we propose a security enhancement based on network separation for CloudHIS with for handling healthcare information to cope with cyber attack. To protect against all security threats and to establish clear data security policies, we apply desktop computing servers to cloud computing services for CloudHIS. Use two PCs with a hypervisor architecture to apply physical network isolation and select the network using KVM switched controller. The other is a logical network separation using one PC with two OSs, but the network is divided through virtualization. Physical network separation is the physical connection of a PC to each network to block the access path from both the Internet and the business network. The proposed system is an independent desktop used to access an intranet or the Internet through server virtualization technology on a user's physical desktop computer. We can implement an adaptive solution to prevent hacking by configuring the CloudHIS, a cloud system that handles medical hospital information, through network separation for handling security enhancement.

Key Words : EMR, CloudHIS, PHI, Cloud Computing, Cloud Service

*Corresponding Author : Won-Shik Na(winner@nsu.ac.kr)
Received July 15, 2019 Revised August 20, 2019
Accepted September 20, 2019 Published September 28, 2019

1. 서론

첨단 의료 IT 및 응용 RFID, 모바일 EMR 및 클라우드 기반 가상화 기술의 발전은 의료기관 수준을 향상시켰다. 유비쿼터스 의료의 패러다임의 변화로 인간 지향적인 활발한 연구가 진행되어 의료정보시스템과 의료 IT의 긴밀한 협조하에 ICT 기반의 의료산업에 많은 진보와 응용을 가져왔다. u-헬스케어시스템의 성장[1]으로 의료정보시스템을 위한 의료업계와 관련된 사람들에게 정보를 제공하는 안전한 PHI(Personal Healthcare Information) 통합시스템 기반의 클라우드 컴퓨팅 기반 보안강화 시스템이 요구된다. 요즘은 국공립 병원 및 그외 병원들도 EMR을 사용하는 것이 기본이다. 클라우드 병원정보시스템(CloudHIS)은 가상서버에 위치한 프로그램으로서 인터넷상의 유틸리티 데이터 서버기능을 가지며 가상화 컴퓨팅 기술을 이용하는 의료정보 소프트웨어(mediware)이다. 요즘은 병원이나 의원마다 정보화 기기를 도입하고 의료정보 데이터를 기록 관리하고는 있지만, 각 병원마다 사용되는 EMR(Electronic Medical Record) 시스템이 달라 관리되는 의료정보 데이터가 상호 이질적인 형태로 생성되는 문제점을 갖는다. 또한 의료정보 데이터는 의료정보를 취급하는 기관들 사이 상호 연계성은 있지만, 데이터의 상호 연동이 불가능하여 동일 업무에 대한 반복적 처리로 시간과 인력의 오버헤드가 발생되는 경우가 많고 정보시스템의 기능적 연동이 매우 미흡한 실정이다[1-4]. 통합 관리된 개인의료정보는 보안이 강화되어 관리 되어야 하며 해커의 공격에 안전해야 한다. 본 논문에서는 클라우드 컴퓨팅 환경에서 CloudHIS를 위한 시스템 차원의 보안 강화 방법을 제안한다.

2. 관련연구

2.1 EMR (Electronic Medical Record)

국내 의료정보 시스템은 크게 PACS (Picture Archiving Communication System), EMR (Electronic Medical Record), 국내 의료정보시스템(Medical Information System)은 초기부터 활발히 참여하고 있는 처방전달시스템 OCS(Ordering Communication System)으로 구성되어있다. PACS 시스템은 캡처 된 의료영상을 의료정보에 대한 디지털화로 변환한다. 환자의 질병을 치료하기 위해 의료정보를 사용하는 것이 유용하다. 현재 의학 이미지는 DICOM (Digital Imaging and Communication for Medicine)의 국제 표준에 따라 제작된다. 프로토콜은 전송 메커니즘 및 형식을 정의하며 대부분의 의료영상 장비 및 솔루션은 호환이 가능하다. 국제표준 HL7(Health Level Seven)을 기반으로 이미지 수집, 이미지 저장, 데이터베이스가 호환된다[4]. EMR은 병원 관리 프로세스를 자동화하고 PACS와 자동으로 연결되어 병원 관리 효율성을 극대화하여 이전보다 더 빨리 병원에서 절차를 제공했다. 처방전달시스템 OCS는 의사가 환자의 치료 후 처방 과정을 알리는 시스템으로 환자의 시술 과정을 단순화하고 대기 시간을 단축한다. 의사들은 다양한 진료 검사가 정확하게 처리되며 의료정보 공유 및 의료통계 차트 보고가 용이하다. 또한 의료정보 교환을 위해 다른 의료기관과 통신도 가능하다. EMR, OCS, PACS 등의 전산화된 의료정보는 필수 요소이다[5-8]. 일부 의료데이터 형식과의 호환성은 EMR/OCS 시스템의 제조업체 및 개발자에 따라 다르나 2000년 초부터 국내 대형 병원 기반 통합 건강 정보 시스템이 전자의료기록 시스템으로 발전했다. 최근 모바일 컴퓨팅 등장, 글로벌 의료업체의 경쟁 심화 및 의료수요의 폭발적 증가로 의료 환경이 급속히 변했다. 모바일 의료시스템은 스마트폰과 같은 휴대용 장치를 사용하며 소형 컴퓨팅 장치로 소형화 된다[9].

클라우드 컴퓨팅은 인터넷을 통해 구성되고 많은 다양한 서비스 모델 및 인프라 자원을 효과적으로 전달할 수 있는 방법을 제공하고 있다[10]. CloudHIS는 시각화를 통해 의료정보 리소스 및 공유를 극대화하도록 설계가 되었다. 이를 통해 클라우드 서비스 제공 업체는 클라우드 데이터 센터의 유지 관리 비용을 최소화 하고 저렴한 비용으로 높은 수준의 서비스를 제공한다. CloudHIS의 컴퓨팅 서비스를 고려하기 위해 클라우드 서비스의 개념과 시각화를 검토할 수 있다. 클라우드 컴퓨팅은 대개 다음 두 가지 방법으로 클라우드 위치 및 클라우드 서비스가 제공된다. 첫째 퍼블릭 클라우드, 프라이빗 클라우드, 하이브리드 클라우드 및 커뮤니티 클라우드와 같은 클라우드 위치를 만들기 위해 몇 가지 종류가 필요하다. 다음 Table 1은 클라우드 서비스의 종류와 특징을 나타낸 것이다.

Table 1. Types of Cloud Services

Service Type	Service Unit	Service Resource	Examples
SaaS (Software-as-a-Service)	Application	Business application, Web service, etc.	Gmail, Google Apps, Facebook etc.
PaaS (Platform-as-a-Service)	Platform	Software framework, Storage, etc.	Goole AppEngine etc.

IaaS (Infrastructure-as-a-Service)	Infrastructure	Computation device(VM), Storage, etc.	Naver NDrive etc.
	Hardware	CPU, Memory, Disk, Network, etc.	Amazon Data Center etc.

2.2 정보보호를 위한 망분리

일반적으로 인터넷에 연결된 망은 외부의 유해한 요소로부터 많은 위험에 노출되게 된다. 외부로부터의 침입 및 악의적인 공격으로부터 안전한 환경을 제공하고 내부 사용자로부터 중요 자료를 보호해야 하는 필요성은 계속적으로 요구되어 왔으며, 그 동안 기업과 관공서의 주요 정보를 보호하기 위한 방안으로 정보보안 솔루션이 많이 도입되어 왔다. 이메일 보안, DB 암호화, 문서 보안, 내부정보유출 방지, 출력물 보안 등 다양한 방안의 솔루션이 제시되고 있으나 시스템 차원의 원칙적인 내부 정보 보호를 위한 업무망과 외부망의 네트워크 분리의 필요성이 부각되었고 이에 따라 물리적인 망 분리가 요구되어 왔다.

2.2.1 물리적인 망분리

한 사람이 두 대의 PC를 사용하거나 전환 스위치로 망을 완전히 분리하는 방식이다. 각각의 망에 연결된 PC가 별도로 필요하지만, 논리적 망분리를 사용하면 하나의 PC로도 내부망과 외부망을 분리하여 운영할 수 있다. 분리된 망은 자료이동, 외부로부터의 침입 등이 차단되므로 높은 수준의 보안을 유지할 수 있으며 관리도 용이하다.

2.2.2 논리적인 망분리

PC의 운영체제 환경과 Desktop 서버에 구성된 데스크탑 가상환경 2개의 운영체제를 각 개인이 보유할 수 있어, 보안이 보장된 망분리를 구축할 수 있다. 가상화 기술을 활용한 VDI(Virtual Desktop Infrastructur)방식과 하나의 PC에 두개의 OS를 설치하는 OS커널 분리방식이 있다. 가상환경의 특성에 따라 외부 인터넷 접속을 위하여 가상환경이 동작하는 서버를 경유하므로 관리가 용이하다. 구축 비용도 절약할 수 있으며 물리적 방안에 비해 기본 비용이 저렴하다. 또한 재난 복구도 용이하며 서버에 저장되어 있는 가상환경은 오류 상황이 발생해도 쉽게 복구할 수 있다.

2.3 보안강화 시스템 설계 기준

2.3.1 클라이언트 기반 가상화 망분리

가상화를 기반으로 하지만 서버가 아닌 개인용 데스크톱에서의 가상화 방법이다. 두 NIC(N/W Interface Card)를 사용하여 호스트 운영 체제와 가상 시스템에 각각 할당된다. SBC 방식에 비해 데이터 중앙 집중식 관리의 장점은 없지만 사용자 PC의 모든 하드웨어 자원을 사용하는 장점이 있다. 구성 방법으로는 첫째는 PC 데스크톱 OS를 가상화하여 호스트 OS 및 게스트 OS를 구성하고 각 영역마다 다른 망을 설정하여 망분리 한다. OS는 부가적으로 요구되지 않으며, 현재 사용되는 OS에 가상공간이 생성되고 가상공간에서 실행되는 애플리케이션들만이 인터넷에 연결되어, 망분리를 실현한다. 이 방법은 많은 시스템 자원을 사용하지 않고 기본 PC에 여러 번 적용 할 수 있으므로 최소 비용으로 망분리를 구성 할 수 있다. 둘째 클라이언트 하이퍼바이저를 사용하는 두 개 이상의 운영체제에 별도의 가상 망을 사용한다.

2.3.2 물리적 망 분리

PC를 각각의 망에 물리적으로 연결하여 인터넷망 및 업무망의 액세스 경로를 차단한다. 즉 인터넷망과 내부 업무망으로 구분된다. 보안성은 높지만 물리적 망분리를 하려면 별도의 네트워크, PC 및 네트워크 장비가 필요하다. 듀얼 PC를 사용하면 효율성이 떨어질 수 있다.

외관상으로는 하나의 PC 처럼 보이지만 내부에 하나의 PC 마더 보드를 기반으로 하는 두 개의 PC 구조로 구성된다. HDD, NIC, VGA 및 USB 허브를 물리적으로 복제한다. 두 개의 서로 다른 운영체제가 단일 보드 PC에서 실행될 수 있다. 다중 사용자는 하나의 PC 환경을 독립적으로 구성 할 수 있다. 망분리는 내부망과 외부망을 분리하여 외부로의 침입을 방지하고 내부정보의 유출을 방지한다. 악의적인 코드 감염은 네트워크 연결이 끊어진 경우에도 완전히 차단되지 않을 수 있다. 다음과 같은 관리방법은 망분리의 효과를 극대화하기 위한 효과적인 보안관리로 제안된다.

2.3.3 PC 보안 관리

인터넷망과 업무망에 액세스하는 PC를 분리하고 인터넷 PC와 업무 PC에 대한 보안 관리를 각각 수행해야한다.

2.3.4 인터넷 메일 사용

외부 전자 메일을 송수신하는 메일 서버는 업무용 망에 연결되어 있으며 인터넷 PC에서만 분리하여 접속할 수 있다.

2.3.5 패치 관리 시스템

패치 관리 시스템은 외부 인터넷과 별도로 운영된다.

2.3.6 네트워크 액세스 제어

인증되지 않은 장치(PC, 노트북 등)는 연결할 수 없도록 제어되어야 한다.

2.3.7 보조 메모리 관리

인증된 보조 엔터프라이즈 장치(USB 메모리, CD, 이동식 장치, 하드 디스크 등) 별도로 제어관리 한다.

3. CloudHIS를 위한 보안강화 시스템 제안

원격진료 및 고립된 분산 클라우드 컴퓨팅 환경의 CloudHIS에서 의료정보 보호를 위한 시스템 차원의 보안강화 시스템 구축을 위한 보안강화 방법을 제안한다.

3.1 물리적 망 분리 적용

물리적 망분리는 PC를 각 네트워크에 물리적으로 연결하여 인터넷망 및 업무망의 액세스 경로를 차단하는 것이다. 즉, 인터넷망과 내부 업무망으로 구분된다. 마지막으로 보안성은 높지만 물리적 망을 분리하려면 별도의 네트워크, PC 및 네트워크 장비가 필요하다. 많은 구축 비용과 듀얼 PC를 사용하기 때문에 효율성이 저하된다.

3.2 가상화 기반 다중 사용자 연결성 적용

다중 사용자는 Fig. 1과 같이 하나의 PC 환경을 독립적으로 구성 할 수 있다.

Fig. 1. Dual PC server configuration on board of network disconnect

H/W를 직접 할당하는 방법으로 물리적PCI(Peripheral Component Interconnect)장치를 가상 컴퓨터에 직접 할당하기 위해, PCI 통과(Pass-through) 방법을 적용 할 수 있다. 이 방식은 NIC, 디스크 컨트롤러, USB 컨트롤러와 사운드 카드 등의 PCI 장치를 직접적으로 Guest에게 할당하여 바로 제어하고 접근 할 수 있다. 가상 머신은 자체적인 독립적인 가상주소 공간을 사용하고 I/O 성능향상 기술로 물리적 H/W 및 가상 머신의 1:1 연결을 위해 VT-D에 연결할 수 있는 PCI 통과를 지원한다. 마더 보드의 BIOS 및 가상화 커널의 PCI 통과 방법이 완벽하게 지원된다[11].

3.3 CloudHIS를 위한 보안강화 방법

가상화를 이용하여 물리적인 방법과 논리적인 방법으로 망분리를 적용하여 고립된 지역의 원격 의료서비스를 위한 데스크톱 컴퓨팅 서버를 CloudHIS에 적용한다. 제안 방법의 망분리 방법을 검토하여 사이버 공격에 대처할 수 있는 의료건강 관리정보의 보안강화를 도모할 수 있다. 두 개의 네트워크 파티션이 있고 하나는 하이퍼바이저 아키텍처를 이용하는 2대의 PC를 이용하는 물리적 망 파티션이며, KVM(키보드, 비디오 모니터, 마우스) 스위치 컨트롤러를 이용하여 네트워크를 선택한다. 다른 하나는 2개의 OS가 있는 1대의 PC를 이용하는 논리적 네트워크 파티션이지만 네트워크는 가상화를 통해 분할된다. 논리 네트워크 파티션에는 가상화의 기반인 SBC(Server Based Computing)와 CBC(Client Based Computing)의 두 가지 종류가 있다. 물리적 망 파티션은 하나의 PC를 사용하여 외부 업무를 위해 인터넷에 연결하고 다른 하나는 인터넷에 연결하지 않고 내부 작업을 수행한다. 본 논문에서는 사이버 공격에 대처하기 위한 개인의료 정보처리를 위한 CloudHIS의 망분리 기반의 보안강화 적응 구조로 제안한다. 이 제안은 일부 문제를 극복하기 위해 H/W 직접 할당을 이용하는 가상 데스크톱 서비스 하에서 물리적 망분리가 필요하다. 제안 시스템은 물리적 데스크톱 컴퓨터의 서버 가상화 기술을 이용하여 인트라넷 또는 인터넷에 액세스하는데 사용되는 독립적인 데스크톱 시스템이다.

4. CloudHIS를 위한 보안강화 시스템 구축을 위한 시험방법

원격진료 및 고립된 분산 컴퓨팅 환경은 개인 의료정보

보안강화를 위해 시스템 차원의 보안강화 방법이 요구된다. 다음 Fig. 2는 CloudHIS를 위한 보안강화 시스템을 위한 망분리 시스템 시험환경 구성도이다.

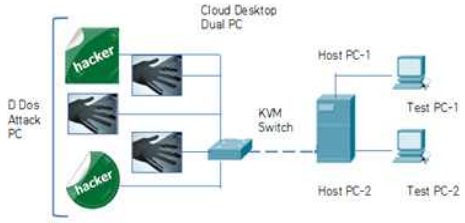

Fig. 2. Network separation system Test environment configuration diagram

해커의 사이버 공격에 대처하기 위해 해킹 테스트 시험을 실시해야 한다. 물론 일반적으로 해킹 테스트를 위한 몇 가지 방법을 사용할 수 있다. 제안하는 시험방법으로 두 가지 스크립트 테스트와 원격 데스크톱 처리를 적용 할 수 있다. 테스트 도구로 두 개의 스크립트를 사용할 수 있다. 한 스크립트는 세 개의 웹 사이트를 동시에 실행할 수 있다. "internet-startall.cmd" 다른 스크립트는 동시에 다른 확장명을 가진 다섯 개의 Office 파일 인 "office-startall.cmd"를 실행할 수 있다. DDoS 공격에 대한 독립 테스트 결과는 DDOS 테스트 환경에 따른 보안인증 방법을 준수해야 한다.

5. 결론

요즘 의료정보 시스템은 보안향상을 위해 IaaS (Infrastructure-as-a-Service) 클라우드 컴퓨팅 환경을 기반으로 하는 안전한 개인 의료정보(PHI) 통합 시스템으로 제공된다. 원격진료 및 고립된 분산 클라우드 컴퓨팅 환경에서 개인 의료정보 보호를 위해 해커의 사이버 공격에 대처하기 위한 시스템 차원의 보안강화 방안으로 망분리 기반의 보안강화 시스템 구축 방법을 제시하였다. 또한 DDoS 공격에 대한 네트워크 분리 환경을 기반으로 서로 독립적인 테스트를 수행하기 위한 보안인증 시험방법을 제시하였다. 제안 방법은 시스템 차원의 사이버 공격에 대처할 수 있는 클라우드 컴퓨팅 환경에서 개인 의료정보의 보안강화 방법이다. 개인 의료정보를 제공하는 클라우드 병원정보 시스템(CloudHIS)의 망분리 기반 보안강화 시스템으로 성능저하 없이 클라우드 데스크톱 듀얼 PC 서버로 구현 가능하였다. 보안강화 시스템 구성에 활용되는 망분리 방법은 물리적 방법이나 논리적 방법을 시스템 구축 비용과 용도를 고려하여 구성할 수 있다. 시스템 구성 후 보안관리 기준에 따른 제어관리에 중요성이 강조된다. 향후 사이버 공격에 대처할 수 있는 보안강화 시스템은 요구되는 많은 산업 분야의 솔루션으로 자리 매김 할 것으로 전망된다.

REFERENCES

[1] Y. B. Cho, S. H. Woo & S. H Lee. (2014). The CloudHIS System for Personal Healthcare Information Integration Scheme of Cloud Computing. *Journal of the Korea society of computer and information, 19(5),* 27-35.
DOI : 10.9708/jksci.2014.19.5.027

[2] Y. S. Cho & K. H. Ryu. (2014). Predictive pattern analysis using SOM in medical data sets for medical treatment service. Computational Intelligence in Bioinformatics and Computational Biology. *IEEE Conference on. IEEE, 2014.*
DOI : 10.1109/CIBCB.2014.6845512

[3] S. C. Noh & J. H. Hwang. (2011). A Study of Software Architecture Design Methods for Multiple Access Control under Web-based Medical Information System Environment. *Journal of Information and Security, 11(4),* 43-49.

[4] I. S. Cho. & H. S. Kwon. (2009). Efficient Sharing System of Medical Information for Interoperability between PACS System. *Journal of the Korea Institute of Information and Communication Engineering, 13(3),* 498-504.

[5] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton & D. W. Bates. (2008). A research agenda for personal health records (PHRs). *Journal of the American Medical Informatics Association, 15(6),* 729-736.

[6] G. L Yau., Williams, A. S. & J. B. Brown. (2011). Family physicians' perspectives on personal health records Qualitative study. *Canadian Family Physician, 57(5),* 178-184.

[7] T. H. Kim, I. H. Kim, J. H. Kim, C. W. Min, J. H. Kim & Y. I. Eom. Security-Enhanced Local Process Execution Scheme in Cloud Computing Environments. *Journal of the Korea Institute of Information Security and Cryptology, 2010, 20(5),* 69-79.

[8] D. K. Cho & S. C. Park. (2013). Development and

implementation of monitoring system for management of virtual resource based on cloud computing. *Journal of The Korea Society of Computer and Information, 18(2),* 41-47.

[9] K. M. Kim. (2012). Implementation of patient monitoring system based on mobile healthcare. *Journal of The Korea Society of Computer and Information, 17(12),* 1-10.

[10] K. Balaji & P. S. Kiran. (2016). A Review on Cloud Security Challenges and Issues. *Indian Journal of Science and Technology, 9(43).*

[11] J. C. Patni, A. Sharma, P. Mishra & A. Kumar. (2016). Datacenter Virtualization with Optimization and Customization. *Indian Journal of Science and Technology, 9(44).*

조 영 성(Young-Sung Cho) [정회원]

· 1990년 2월 : 연세대학교 전산학과 (공학석사)
· 2008년 8월 : 충북대학교 전산학과 (공학박사)
· 1989년 11월~2017년 5월 : 미국CDC 한국지사 S.E Manager, ㈜ 네오아이엔씨 (CEO), 컴트리 기업연구소 (이사)
· 2018년 2월 ~ 현재 : 네오인텍연구소(대표), 경기대진테크노파크 전문위원, 한양여자대학교 산학겸임/교수
· 관심분야 : 데이터베이스, 빅데이터, IoT, 추천서비스
· E-Mail : youngscho@empas.com

정 지 문(Ji-Moon Chung) [정회원]

· 1990년 2월 : 연세대학교 전산학과 (공학석사)
· 2008년 2월 : 충북대학교 전산학과 (이학박사)
· 1987년~1991년 : 국방과학연구원
· 1991년~1994년 : 대전과학기술대학교
· 1994년~현재 : 남서울대학교 컴퓨터소프트웨어학과 교수
· 관심분야 : 데이터베이스, 빅데이터, 멀티미디어컨텐츠
· E-Mail : jmchung@nsu.ac.kr

나 원 식(Won-Shik Na) [종신회원]

· 2005년 8월 : 경희대학교 컴퓨터공학과 (공학박사)
· 2001년 3월 ~ 2003년 2월 : ㈜성신섬유 전산실장
· 2006년 3월 ~ 현재 : 남서울대학교 컴퓨터소프트웨어학과 부교수
· 관심분야 : 네트워크 보안, 무선 LAN, 모바일 컴퓨팅, 의료정보, 전자제어
· E-Mail : winner@nsu.ac.kr