한국사물인터넷학회논문지 Vol. 1, No. 1, pp. 39-44, 2015 http://dx.doi.org/10.20465/KIOTS.2015.1.1.039

공인인증서와 바이오인증 연계를 위한 연구

류갑상
동신대학교 컴퓨터학과

Study on the Connection with Public Authentication and Bio Authentication

Gab-Sang Ryu
Division of Computer Science, Dongshin University

요 약 공인인증서와 바이오 정보를 활용하여 인증과정을 처리하고 있는 기관이 증가하고 있고 휴대용 바이오 인증 기기를 배급하여 공인인증서와 바이오인증을 병행할 수 있도록 발전하고 있다. 개인의 PC나 스마트 디바이스를 이용한 인증이 범용화 되어가면서 인증에 대한 편의성이 증대되어가고 있는데 비해 네트워크 레벨에서의 보안과의 연계성에 대한 검토는 미약한 실정이다. 공인인증서와 바이오 정보의 연계를 통한 인증방식이 현재 네트워크 접근제어와 연계된다면 좀 더 강력한 보안정책으로 발전할 수 있다. 본 논문에서는 보안토큰에서의 취약한 개인인증 기법에 대한 취약점을 바이오인식과 같은 확실하고 안전한 개인인증 기법으로 연계함으로써 바이오 정보 노출 방지 및 바이오정보 본인 확인 수행 여부를 검증할 수 있는 방법론을 제시하였다. 아울러, 802.1x 네트워크 인증방식과 연계할 수 있는 시나리오를 정리하고 이의 실현을 위한 방안을 제시하였다.

주제어 : 사물인터넷, 공인인증서, 바이오인증, 정보보호

Abstract Organization is increasing the authorizing process to use public certificate and bio information. Certificate, has evolved to be able to parallel distributes the bio authentication and portable bio-authentication device. Authentication using an individual's PC and smart devices continue to generalize, while convenience for authentication is increased by comparison Study on cooperation with the security at the network level's a weak situation. If ask authentication method through the cooperation of the public certificate and bio information work with current network access control, there is a possibility to develop a more powerful security policy. by cooperation weaknesses against vulnerable personal authentication techniques on security token in a reliable and secure personal authentication techniques, such as bio-recognition, Bio Information for identification and to prevent exposing a methodology suggest to validate whether or not to carry out in this paper. In addition, organize the scenario that can work with the 802.1x network authentication method, and presented a proposal aimed at realization.

Key Words : IoT; Public certification, Bio certification, Information security

1. 서론

공인인증서는 전자서명의 일환으로 신원확인, 위변조 방지, 거래사실 부인방지 등의 기능을 제공하고 있으며 전자서명법에 기반을 두어 법적 보호도 받을 수 있다[1]. 현재의 공인인증서는 스마트폰 기반의 모바일 환경으로 급속히 전환되면서 취약한 보안 환경으로 인한 정보보호에 대한 우려가 증가하고 있다. 본인 여부 확인을 위해

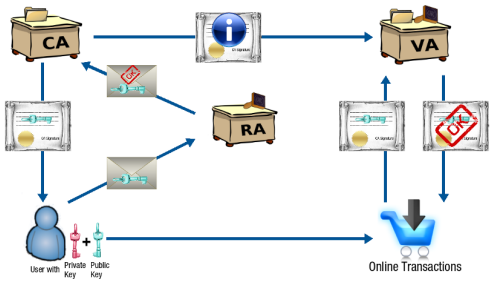
교신저자 : 류갑상(gsryu@dsu.ac.kr)
접수일 : 2015년 12월 10일

공인인증서를 사용하더라도 이와 관련하여 운용 제약 사항이 존재하는 실정이다. 이러한 운용 제약 사항이 발생하는 이유는 공인인증서 사용자들에 의해 공인인증서가 오 남용되고 있기 때문에 주로 발생한다. 또한 공인인증서를 발급하는 과정에서도 인증된 사용자가 실제 해당 사용자 본인이 맞는지 확인할 방법을 적절히 제공하지 못하기 때문에 발생한다. 이를 해결하기 위해서는 인증처리과정에서 바이오정보와 같이 사용자 본인임을 직접적으로 확인할 수 있는 방법을 공인인증서 처리 과정에 도입 및 이용하여 사용자 인증을 진행하는 것이 필요하다. 이와 같이 바이오 정보를 이용하여 해당 사용자 본인이 맞는지 확인하고 난 뒤에 공인인증서 발급 진행이나 전자서명 생성을 진행할 수 있도록 운용한다면 사용자 본인 여부 확인을 강화한 형태로 공인인증서 서비스 제공이 가능해진다. 이에 본 논문에서는 보안토큰에서의 취약한 개인인증 기법에 대한 취약점을 바이오인식과 같은 확실하고 안전한 개인인증 기법으로 연계하는 방법을 살펴보고 아울러 802.1x 네트워크 인증방식과 연동된 강력한 보안정책을 제안하고자 한다.

2. 관련 연구

2.1 공인인증서 시스템

전자상거래시에 신원을 확인하고, 문서의 위조와 변조, 거래사실의 부인 방지 등을 목적으로 공인인증기관이 발행하는 전자서명 정보이다. 공인인증서 내에는 인증서 버전, 인증서 일련번호, 인증서 유효기간, 발급기관 이름, 가입자의 전자서명 검증정보, 가입자 이름 및 신원확인 정보, 전자서명 방식 등의 정보가 포함되어 있다[2,3].



[Fig. 1] Public key infrastructure

전자서명은 비밀키와 공개키로 구성된 공개키 기반구조(PKI, Public Key Infrastructure)로 이루어진다. PKI는 인증기관, 인증서, 등록기관, 인증서 관리시스템 등으로 구성되며[4] 각 요소별 수행 기능 및 연관성은 Fig. 1과 같다[5]. 공개키기반구조는 인터넷 환경을 이용한 전자상거래 등에서 사용가능하며, 전자서명을 통해 전자상거래 부인 방지 서비스가 가능하고 개인정보나 거래 정보가 외부에 노출되지 않도록 기밀성 서비스가 가능하다.

2.2 바이오 보안토큰

보안토큰(HSM : Hardware Security Module)이란 전자서명생성키 등 비밀 정보를 안전하게 저장, 보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 기기로 외부로 나오지 않기 때문에 피싱과 해킹 등으로부터 공인인증서 유출을 방지할 수 있는 휴대용 저장장치이다[6,7].

[Fig. 2] Bio-security token device model

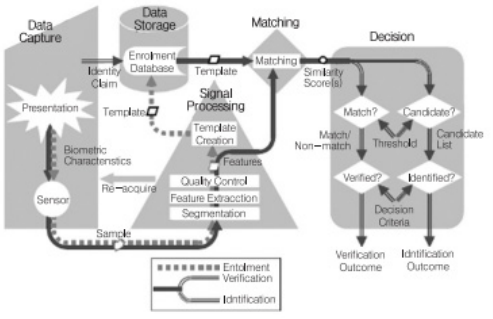
HSM의 기능은 서버의 공개키, 개인키 쌍을 생성하고 서버에 공개키를 전달하며, 서버의 개인키는 HSM에 저장함으로써 외부 유출이 불가능해 안전한 키 관리를 제공한다. 또한, 서버의 공개키로 암호화된 세션키를 HSM에 저장해 둔 서버 개인키로 복호화해 저장함으로써 공인전자서명 시 세션키로 암호화된 데이터를 복호화할 수 있다. 바이오 보안토큰 장치는 바이오정보 처리를 위한 MCU, 생체정보인식을 위한 Bio센서, 개인식별정보, 전자서명 생성키 등의 정보가 저장되는 스마트카드, 통신을 위한 USB 및 UART인터페이스 등의 장치로 구성된다[8]. 바이오보안토큰의 외부 인터페이스 장치로는 PC 환경에 접속할 수 있는 USB장치와 휴대폰의 24핀 컨넥터에 접속할 수 있는 장치로 구성되어야 한다.

2.3 바이오정보 인식처리

바이오정보 인식 기술이란 사람의 고유한 신체적 특

징을 이용하여 신원확인의 수단으로 사용하는 사용자 인증 기술이다. 바이오정보 인식기술에서 사용되는 바이오정보는 신체적 특성을 이용하는 정보와 행동학적 특성을 이용하는 정보가 있다.

바이오정보 인식 처리 모델은 바이오정보 등록 단계와 바이오정보 인식 단계로 이루어져 있다. 바이오정보 인식은 바이오정보 등록 단계에서 사용자 인식 또는 인증에 사용할 바이오정보를 등록하게 된다. 이렇게 등록된 바이오정보와 바이오정보 인식 단계에서 사용자로부터 획득한 바이오정보를 이용하여 사용자 일치 여부 등을 판단하게 된다[8]. 사용자 인식 또는 인증에 사용되는 바이오정보 종류에 관계없이 바이오정보 인식처리 모델의 바이오정보 등록 및 인식 단계는 크게 데이터 획득, 이미지 처리, 비교 및 판단의 절차를 거치도록 구성한다.



[Fig. 3] Bio information recognition model

2.4 ISO ACBio 모델

바이오인식 인증 컨텍스트(ACBio)는 ISO/IEC 24761[9]에 정의된 메커니즘으로, 바이오인식이 사용된 장치와 원격지에서 실행된 과정들에 대한 정보를 확인자에게 보냄으로써 원격에서의 바이오인식 검증에서 발생할 수 있는 문제에 대한 해결책을 제공해 준다. ACBio는 확인자가 바이오인식 검증 과정 결과의 신빙성 정도를 결정하는데 도움을 주는 BPU(BPU, Biomertic Processing Unit)에 대한 인증된 정보를 제공하기 위하여, 센서, 스마트카드, 비교기 등 BPU에 의해 생성되는 보안 데이터를 위한 데이터 포맷을 정의한다. ACBio는 PKI 기술과 PKIX(X.509, Public Key Infrastructure)를 기본으로 하며, 신뢰성 확보와 부인 방지를 위하여 전자서명을 사용한다.

바이오인식 검증 과정에서 각각의 BPU는 BPU 인증서 정보, BPU 보고서 정보 및 BR 인증서 정보를 담은 ACBio 인스턴스를 채워야 한다. 확인자는 BPU 인증서에 있는 전자서명 혹은 메시지인증코드를 확인함으로써 ACBio 인스턴스의 확실성과 무결성을 확인할 수 있다[10]. 확인자는 BPU 보고서에 따라 BPU의 보안 레벨과 기능적 성능 레벨을 알 수 있고, BRT(Biometric Referece Template) 인증서에 따라 바이오인식 검증 과정에서 사용된 바이오인식 레퍼런스의 확실성도 알 수 있게 된다.

ACBioContentInformation
Version
BPU Information Block
BPU Certificate Referrer Information
BPU Report Information
Control Value
Biometric Process Block
SubprocessIndex[1]
:
SubprocessIndex[L]
BPUIOExecutionInformation[1] (for input)
:
BPUIOExecutionInformation[M] (for input)
BPUIOExecutionInformation[1] (for output)
:
BPUIOExecutionInformation[N] (for output)
BRT Certificate Information

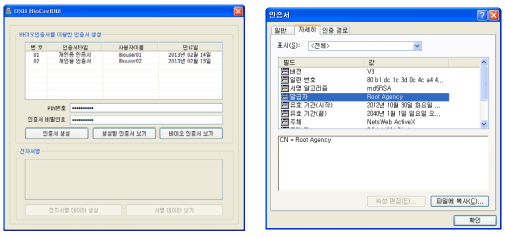
[Fig. 4] ACBio Instance data format

3. 바이오정보 연계 방안

3.1 바이오정보 연계 프로타입

본 연구에서는 바이오정보를 인식하기 위해 QC인증서버에 보관하고 있는 바이오정보가 사용자 등록 단계에서 등록한 바이오인식장치 내부에서만 복호화 되도록 강제함으로써 바이오인식처리 결과를 직접적으로 신뢰할 수 있게 운용하는 모델을 제안한다. 이 모델에서는 전자서명 생성 및 검증 절차에서 기존 전자서명 생성 검증뿐만 아니라 서명 생성자에게 발급된 바이오인증서를 기반으로 한 전자서명 생성 및 검증도 처리하여 서명 생성자의 본인 여부를 직접적으로 확인할 수 있다.

바이오 정보 연계 프로토타입의 운영 절차는 1)인증서 발급 정책 등록, 2)사용자 등록, 3)바이오인증서 발급, 4) 발급된 바이오인증서로 사용자 인증서 발급 (그림5), 5) 전자서명 데이터 생성, 6)전자서명 검증 단계로 진행된다. [Fig. 5]는 바이오인증서 발급을 위한 프로세서를 실행하는 화면과 생성된 인증서 내용을 설명한 예이다.

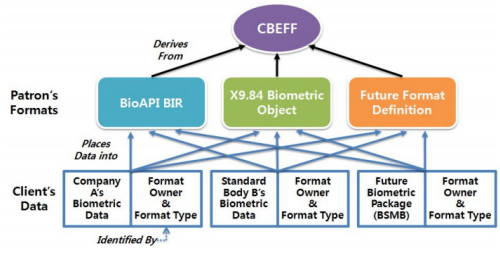


[Fig. 5] Creating a Bio-certification

3.2 바이오 정보교환을 위한 데이터 형식

CBEFF(Common biometric Exchange File Format)는 상이한 바이오정보 인식 소프트웨어/장치들에게 어떤 형식으로 사용할 것인가에 대한 어플리케이션의 표준 형식이다[11,12]. 바이오 정보 인증 시스템의 어플리케이션 간의 생체 정보의 상호교환은 호환성 측면에서 매우 중요하며 제품 개발 시 API와 더불어 범용성을 지원하기 위해서 반드시 필요하다. Biometric consortium과 NIST, NSA가 CBEFF의 개발을 후원하고 있다.

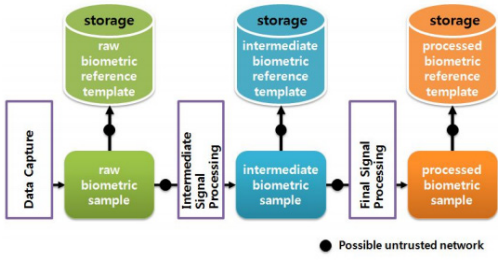
CBEFF의 자료 형식은 다른 바이오정보 인식 기술들 간의 호환성을 목적으로 하지 않으며, 한 시스템 또는 응용 어플리케이션 내에서 각 바이오정보 인식 기술을 식별하고 활용 가능하도록 한다. 바이오정보 인식업체 또는 고객들이 CBEFF에서 정의된 바이오정보 인식 자료 구조 내에서 공용표준 템플릿 포맷에 동의할 수 있으나 바이오정보 인식 데이터 구조의 내용에 대한 정의는 포함되지 않는다. [Fig. 6]은 CBEFF, CBEFF Patron 포맷 및 CBEFF 클라이언트 간의 관계이다.



[Fig. 6] CBEFF, CBEFF Patron format

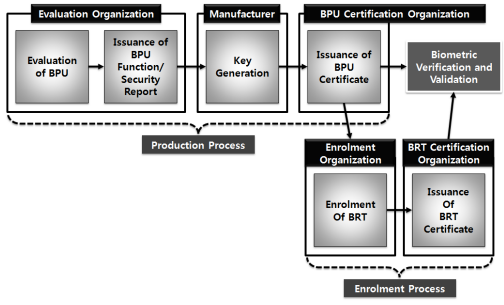
3.3 802.1x와 바이오인증정보 연계방안

ACBio 사용을 위한 일련의 준비 작업들은 생산/등록 과정과 뒤이어 일어나는 검증 과정으로 나누어진다. 이러한 ACBio 프레임워크를 통하여, 확인자는 비교결과, 바이오인식 검증 결과 뿐 만아니라 수행된 바이오인증 검증 결과의 유효성을 확인할 수 있는 ACBio 인스턴스도 얻을 수 있다. 바이오인식 검증 과정에서 각각의 BPU는 BPU 인증서 정보, BPU 보고서 정보 및 BR 인증서 정보를 담은 ACBio 인스턴스를 채워야 한다. ACBio 인스턴스란 XML 인코딩룰(XER, XML Encoding Rules) 또는 흔히 암호용 툴킷 제공업체들로부터 제공되는 ASN.1 기본 인코딩룰(BER, Basic Encoding Rules)을 이용하여 인코딩된 것으로, 구문은 알고리즘 독립적이며, 데이터 무결성과 데이터 원본 인증을 지원한다[10].



[Fig. 7] ACBio registration model

확인자는 BPU 인증서에 있는 전자서명 혹은 메시지 인증코드를 확인함으로써 ACBio 인스턴스의 확실성과 무결성을 확인할 수 있다. 확인자는 BPU 보고서에 따라 BPU의 보안 레벨과 기능적 성능 레벨을 알 수 있고, BRT(Biometric Referece Template) 인증서에 따라 바이오인식 검증 과정에서 사용된 바이오인식 레퍼런스의 확실성도 알 수 있게 된다.

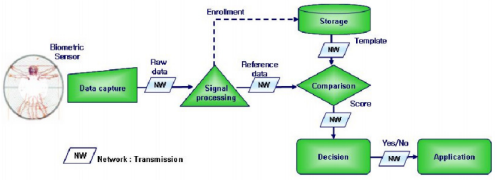


[Fig. 8] Biometric verification process

3.4 바이오정보 기술 연계 보안 요구사항

바이오정보 인식 기반 정보시스템도 다양한 취약성과 위협에 노출 될 수 있다. 바이오 정보 인식 기반 환경 내에서 모든 가능한 위협으로부터 바이오정보 자료와 해당

정보를 보호하기 위해 시스템의 취약 포인트 정의 및 각 취약 포인트별 시스템 보호를 위한 가이드라인이 필요하다. [Fig. 9]는 바이오정보 인식 기능을 네트워크를 통하여 구현하는 경우에 요구되는 기능의 각 부분을 설명하고 있다. 바이오정보 인식 기능 모델은 바이오정보 인식을 위해 각 단계에서 바이오정보를 생성 및 전송하는 과정에 포함되어야 하는 기능을 모델링한 것이다. 한 개의 바이오정보 인식 기능은 이전 단계의 출력을 입력받아서 각 기능을 독립적으로 수행한다.



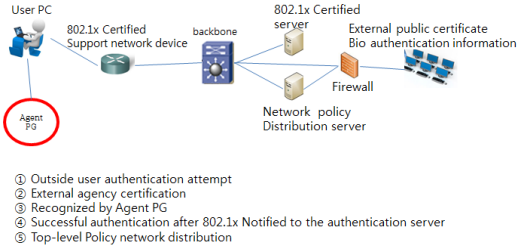
[Fig. 9] Bio information recognition

3.5 802.1x와 바이오인증정보 연계방안

개인의 PC나 스마트 디바이스를 이용한 인증이 범용화 되어가면서 인증에 대한 편의성이 증대되어가고 있는데 비해 네트워크 레벨에서의 보안과의 연계성에 대한 검토는 이루어지지 않고 있다. 앞에서 제안한 바이오연계 프로타입이 802.1x 네트워크 접근제어와 연계된다면 좀 더 강력한 보안정책으로 발전할 수 있다. 802.1x 네트워크 인증은 사용자가 사용하는 개인PC나 스마트 디바이스는 네트워크에 접속하기 전에 사용자 인증을 통해서 사용자별 네트워크 접근권한이 주어지고 사용자는 본인에게 적용된 정책에 따라 내외부 네트워크 리소스에 접근할 수 있다[13,14,15]. 공개키 기반구조를 보면 사용자가 공개키 기반에서 인증되는 방식과 802.1x 인증방식의 연계방안은 다음 시나리오로 정리할 수 있다.

다음에 제시된 시나리오를 통해 사용자 인증 및 네트워크 레벨에서의 정책이 연계되고자 할 때 가장 중요한 기능은 사용자의 인증시도를 어떻게 802.1x 인증 디바이스(스위치허브, 무선AP)에서 인식할 수 있는가에 대한 것이다. 이 기능의 구현은 사용자 PC에서 동작중인 특정 Agent 를 활용하는 방식으로 가능하다.

1. 사용자가 PC등를 이용해 네트워크에 접근할 때 일단 네트워크 레벨에서 사용자를 인식하고 기본 네트워크 정책을 적용
2. 사용자가 특정기관(공인인증서와 바이오정보 연계 인증 요구)에 접속하려고 시도
3. 사용자의 공인인증서와 바이오정보 연계인증 요청을 네트워크 레벨에서 인식
4. 사용자의 공인인증서와 바이오정보 연계인증 완료
5. 네트워크 레벨에서 최상위 보안정책 적용
6. 사용자 접속 종료
7. 네트워크 레벨에서 기본 보안정책 적용



[Fig. 10] Bio information linkages with 802.1x

이 Agent 프로그램은 PC에서 항상 동작하여 사용자의 공인인증서 사용이나 바이오 인증 디바이스 사용을 감시하여 인증이 이루어질 시 네트워크 레벨에 기존 802.1x 인증 재요청을 통보하고 인증이 성공할 시 최상위 레벨의 보안정책이 네트워크 디바이스(스위치 허브, 무선AP)에 적용되도록 동작한다.

4. 결론

공인인증서와 바이오 정보를 활용하여 인증과정을 처리하고 있는 기관이 증가하고 있고 휴대용 바이오 인증기기를 배급하여 공인인증서와 바이오인증을 병행할 수 있도록 발전하고 있다. 본 논문에서는 보안토큰에서의 취약한 개인인증 기법에 대한 취약점을 바이오인식과 같은 확실하고 안전한 개인인증 기법으로 연계함으로써 바이오 정보 노출 방지 및 바이오정보 본인 확인 수행 여부를 검증할 수 있는 방법론을 제시하였다. 아울러 공인인증서와 바이오 정보의 연계를 통한 인증방식이 현재 네트워크 접근제어와 연계된다면 좀 더 강력한 보안정책으로 발전할 수 있다. 이를 위해 본 논문에서는 802.1x 네트워크 인증방식과 연계할 수 있는 시나리오를 정리하고

이의 실현을 위한 방안을 제시함으로써 전자금융 환경 등에서 바이오 보안토큰과 공인인증서의 효율적 활용을 도모하고 확장성을 제공할 수 있는 방안을 모색하였다.

REFERENCES

[1] In Bum Kim, Journal of information and security, “A Study on Enforce the Policy of User Certification in Public Certificate System“, Vol. 10, No. 4, pp. 69-76, 2010.

[2] Junghyun Lee, Journal of information and security, “A Study on Certificate-based Personal Authentification System for Preventing Private Information Leakage through Internet”, Vol. 10, No. 4, pp. 1-11, 2010.

[3] Kyoung-Soon Hong, The Journal of the Korea Contents Association, “Accessibility Evaluation of Accredited Certificate Subscriber Software“, Vol. 11, No. 2 pp. 40-53, 2011.

[4] Sun-Woo Park, Journal of the Korean Institute of Information Security and Cryptology, “Security Analysis on Digital Signature Function Implemented in Electronic Documents Software ”, Vol. 22, No. 5, pp. 945-957, 2012.

[5] http://en.wikipedia.org

[6] Changhyun No, "Study on the application of HSM to GPKI digital certification system", Changwon Univ., 2009.

[7] Hanna Choi, Journal of the Korean Institute of Information Security and Cryptology, "Improved Security for Fuzzy Fingerprint Vault Using Secret Sharing over a Security Token and a Server", Vol. 19. No. 1, pp. 63-70, 20.

[8] Yong-Nyuo Shin, Journal of Korean institute of information technology, "Privacy Preserving User Authentication Using Biometric Hardware Security Module", Vol. 22. No.2, pp. 347-3556, 2012.

[9] ISO/IEC 24761-Security techniques-ACBio, Authentication Context for Biometrics, 2009.

[10] Yong-Nyuo Shin, Journal of Korean institute of information technology, "Operational Management for Biometrics Hardware Security Module and PKI", Vol. 9. No.51, pp. 207-216, 2011.

[11] Hyo-Bin Lee, "Watermarking technique for biometric images security ", Younse Univ., 2007.

[12] Yooyoung Lee, Theory, Applications, and Systems, 2007. BTAS 2007, “Conformance Test Suite for CBEFF Biometric Information Records ”, 2007.

[13] Weilin Xu, Circuits,Communications and System (PACCS), 2010 Second Pacific-Asia Conference on "802.1x relay: A new model for authentication of nat-enabled router", Vol. 1 .2010.

[14] Tae-Yoon Kim, Kyungnam Univ., "An Efficient user authentication method in PKI system based on 802.1x", 2005.

[15] Hyun-Suk Choi, Aju Univ., "Information Security in IEEE 802.1x Wireless LAN", 2007.

류 갑 상(Gab-Sang Ryu) [정회원]

- 1983년 2월 : 전남대학교 일반대학원 컴퓨터학과 (이학석사)
- 2006년 2월 : 고려대학교 일반대학원 컴퓨터과학과 (이학박사)
- 1985년 3월 ~ 1996년 2월 : 한국기계연구원 책임연구원
- 1996년 3월 ~ 현재 : 동신대학교 컴퓨터학과 교수

<관심분야>

사물인터넷, 정보보호, 컴퓨터교육