http://dx.doi.org/10.14400/JDC.2014.12.4.259

체내 삽입장치를 위한 위임장 기반의 인증 프로토콜

정윤수
목원대학교 정보통신공학과

Authentication Protocol based on Credential for Implantable Medical Device

Yoon-Su Jeong
Dept. of Information Communication & Engineering, Mokwon University

요 약 최근 센서 기술의 발달로 인하여 체내삽입장치를 부착한 환자가 언제, 어디서나 의료 서비스를 받을 수 있는 환경으로 변화하고 있다. 그러나, 체내삽입장치를 부착한 환자의 생체정보가 병원관계자(의사, 간호사, 약사 등)에게 전달할 때, 환자의 정보가 제 3자에게 쉽게 노출되어 악용될 수 있는 문제점이 발생되고 있다. 본 논문에서는 제3자가 환자로 위장하여 병원관계자로부터 환자 정보를 쉽게 획득할 수 없도록 유헬스케어 서비스 센터로부터 환자의 위임장을 병원관계자가 전달받는 위임장 기반의 서명 인증 프로토콜을 제안한다. 제안 프로토콜은 환자의 민감한 정보를 제 3자에게 노출시키지 않도록 환자의 민감한 정보를 유헬스케어 서비스 센터와 환자가 생성한 랜덤수로 해쉬한 서명키로 환자의 민감한 정보를 암호화한다. 또한 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원관계자 사이의 동기화를 유지함으로써 환자의 생체 정보 유출을 예방할 수 있다.

주제어 : 체내삽입장치, 키 분배, 프로토콜, RSA

Abstract Body insertion due to the recent development of sensor technology, the device is attached patients to receive medical services from anywhere, anytime environment is changing. Body insertion devices for the hospital, the patient's vital information attached personnel (doctors, nurses, pharmacists, etc.) to pass, however, when a problem occurs, a patient's information to a third party that can be exploited easily exposed. In this paper, we proposed signature authentication protocols mandate based on the patient's power of attorney from the center of the u-Healthcare services, hospital officials FormHelper third party disguised as a patient, the hospital patient information easily obtained from the officials to prevent. The proposed protocol, the patient's sensitive information to a third party, do not expose the patient's sensitive information to the random number generated by the u-Healthcare service centers and patients hash signature key to encrypt sensitive information of patients. From third parties to maintain synchronization between the patients and the hospital personnel in order to prevent patient information from being exploited illegally by the patient's vital information leakage can be prevented.

Key Words : IMD, Key Distribution, Protocol, RSA

Received 20 February 2014, Revised 20 March 2014
Accepted 20 April 2014
Corresponding Author: Yoon-Su Jeong(Mokwon University)
Email: bukmunro@mokwon.ac.kr

ISSN: 1738-1916

1. 서론

최근 유헬스케어 서비스는 IT 기술이 발달함에 따라 체내삽입장치를 환자의 신체에 삽입하여 언제, 어디서나 의료서비스를 제공받을 수 있는 환경으로 변화하고 있다[1]. 현재, 체내삽입장치는 병원에서 불치병(심장병, 당뇨병, 심근경색 등)을 치료하기 위해 사용되고 있으며, 유・무선 온라인 네트워크를 활용하여 전자적 의료정보 및 진료 예약관리 등에서 서비스를 제공하고 있다[2]. 그러나, 체내삽입장치는 무선 구간에서 병원관계자(의사, 약사, 간호사 등)이 환자의 정보를 수집하여 의료행위를 수행하기 때문에 무선 의료기기에서 송신되는 의료 정보를 해커에게 악용될 수 있는 보안 문제가 발생되고 있다[3].

유헬스케어 서비스에서 사용되고 있는 심장 페이스메이커나 제세동기와 같은 체내삽입장치는 환자의 신체에 부착되어 동작되기 때문에 환자의 생명과 개인 정보가 직접적으로 연관되어 있어 제3자로부터 쉽게 환자의 개인정보가 노출될 수 있는 보안 문제가 존재한다. 체내삽입장치는 다양한 센서들로 구성되어 있어 의료기기와 안전하게 통신하기 위해서 보통 환자의 생체정보를 공개키로 암호화하고 있다[4].

M. Mambo et. al[5]은 이산대수문제에 기반한 대리서명기법을 제안하였지만, 공개키 기반구조 하에서 대부분 RSA 전자서명 알고리즘을 사용하고 있어 이중의 서명 알고리즘을 사용해야 하는 점과 기본적인 안정성인 강한 위조 불가능성을 충족하지 못한다는 단점이 있다. R. Lu et. al[6]은 변형된 형태의 Rabin 기반 대리서명을 제안하였으며, 이 기법은 소인수 분해 문제의 어려움에 기반하고 있다. [6] 기법은 원 서명자가 대리서명자에게 위임장과 그에 대한 서명을 전송하면 대리서명자는 인증서의 유효성을 확인한다. Zhou. Cao. et. al[2]은 RSA와 소인수분해문제에 기반한 대리서명기법들이 위임 검증 가능성 측면에서 인증서가 직접 대리 서명키를 사용하여 위임장을 스스로 생성해서 이를 이용하여 대리서명을 할 수 있음을 보였다.

최근 센서 기술의 발달로 인하여 체내삽입장치를 부착한 환자가 언제, 어디서나 의료 서비스를 받을 수 있는 환경으로 변화하고 있다. 그러나, 체내삽입장치를 부착한 환자의 생체정보가 병원관계자(의사, 간호사, 약사 등)에게 전달할 때, 환자의 정보가 제 3자에게 쉽게 노출되어 악용될 수 있는 문제점이 발생되고 있다[7,8].

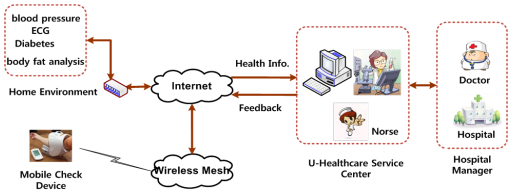
본 논문에서는 유헬스케어 환경에서 체내삽입장치를 부착한 환자의 생체정보를 제3자가 환자로 위장하여 병원관계자로부터 환자 정보를 악용하는 것을 예방하기 위한 위임장 기반의 서명 인증 프로토콜을 제안한다. 제안 프로토콜은 유헬스케어 서비스 센터와 환자가 생성한 랜덤수로 해쉬한 서명키로 환자의 민감한 정보를 암호화하여 환자의 민감한 정보를 제 3자에게 노출시키지 않는다. 또한 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원관계자 사이의 동기화를 유지하여 환자의 생체 정보 유출을 예방하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어 환경의 체내삽입장치에 대해서 알아본다. 3장에서는 환자의 체내삽입장치의 정보를 제3자가 악용하여 사용할 수 없는 위임장 기반의 서명 인증 프로토콜을 제안하고, 4장에서는 유헬스케어 환경에서 발생하기 쉬운 보안 공격유형에 따른 안전성을 평가하고, 마지막으로 5장에서 결론을 맺는다

2. 관련연구

2.1 유헬스케어 환경의 체내삽입장치

유헬스케어 환경에서 병원관계자(병원/의사/간호사/약사 등)는 환자의 신체에 부착한 장치를 이용하여 언제, 어디서나 환자의 상태정보를 수집 처리, 전달, 관리 할 수 있다. 유헬스케어 서비스는 기존 의료 서비스 뿐만 아니라 유・무선 온라인 네트워크를 활용한 전자적 의료정보 및 진료 예약관리 등을 서비스할 수 있다[2]. 노인의 고령화에 따라 유헬스케어 서비스는 기업을 중심으로 다양한 애플리케이션을 개발하고 있다. 그러나 첨단 센서 제품 개발에 어려움이 많아 상용화에는 어려움을 겪고 있는 문제점이 있다. 이러한 문제점은 센서와 통신・의료 인프라 간 연계가 부족, 기술적 한계, 고비용, 소비자 친화적인 'Easy-to-USE' 시스템의 부재 등이 그 원인으로 들 수 있다[6]



[Fig. 1] Structure of U-Healthcare System

그림 1은 유헬스케어 시스템의 일반적인 동작 구조를 보여주고 있다. 그림 1에서 유헬스케어 시스템은 가정 환경에서 환자 자신의 상태를 혈압, 당뇨, 심전도, 체지방 분석 등의 정보를 인터넷을 통해 유헬스케어 서비스 센터에 전달한다. 의사에게 전달된 환자의 생체정보는 의사가 환자의 상태정보를 분석하여 유헬스케어 서비스 센터를 통해 처방을 환자에게 피드백하는 과정을 수행한다. 만약 환자가 가정 이외의 장소에 있을 경우 이동형 측정장치를 이용하여 환자의 상태를 모니터할 수 있다.

2.2 기존 연구분석

체내삽입장치를 부착한 환자의 생체정보를 병원관계자가 안전하게 사용하기 위해서 환자 대신 대리로 서명할 수 있는 다양한 대리서명 기법의 필요성이 증가하고 있다[2, 5, 6]. Zhou. Cao. et. al[2]은 RSA와 소인수분해 문제에 기반한 대리서명기법들이 위임 검증 가능성 측면에서 인증서가 직접 대리 서명키를 사용하여 위임장을 스스로 생성해서 이를 이용하여 대리서명을 할 수 있음을 보였다. M. Mambo et. al[5]은 이산대수문제에 기반한 대리서명기법을 제안하였지만, 공개키 기반구조 하에서 대부분 RSA 전자서명 알고리즘을 사용하고 있어 이중의 서명 알고리즘을 사용해야 하는 점과 기본적인 안정성인 강한 위조 불가능성을 충족하지 못한다는 단점이 있다. R. Lu et. al[6]은 변형된 형태의 Rabin 기반 대리서명을 제안하였으며, 이 기법은 소인수 분해 문제의 어려움에 기반하고 있다. [6] 기법은 원 서명자가 대리서명자에게 위임장과그에 대한 서명을 전송하면 대리서명자는 인증서의 유효성을 확인한다.

3. 위임장 기반의 인증 프로토콜

이 절에서는 체내삽입형 장치를 부착한 사용자의 민감한 생체정보를 제3자의 개인키로 환자의 동의 없이 대리서명이 생성되지 않도록 위임장 기반의 인증 프로토콜을 제안한다.

3.1 개요

체내삽입장치를 부착한 환자가 인증 서버로부터 병원관계자(의사/간호사/약사 등)와의 안전한 통신을 위해 제안 프로토콜에서는 사용자의 위임서를 환자의 개인키로 환자의 동의나 인증 없이 유효한 대리서명의 생성이 가능하도록 제안프로토콜을 적용한다.

제안 프로토콜은 제3자가 환자로 위장하여 병원관계자로부터 환자의 민감한 생체정보를 획득하지 못하도록 공격자의 개인키로 환자의 동의나 인증없이 유효한 대리서명이 생성되지 못하도록 인증서버에서 체크한다. 만약 제3자가 불법적으로 환자의 개인정보를 획득하려는 시도가 발생할 경우 제안 프로토콜에서는 관리자와 환자가 생성한 랜덤수를 이용하여 새로 대리 서명키를 생성하여 환자의 생체 정보를 암호화한다. 또한 유헬스케어 서비스센터는 제 3자로부터 환자 정보가 불법적으로 악용되는 것을 예방하기 위해서 환자와 병원관계자 사이의 동기화를 유지하는 역할을 담당한다.

3.2 용어 정의

표 1은 제안된 프로토콜에서 사용하는 용어에 대한 설명이다.

〈Table 1〉 Notations

Notation	Definition
SC	Service Center
U_i	ith user
P_i	ith Provider
ID_i, ID_j	Identification of U_i and P_i
e_X, d_X	Public/Private key of RSA of Identification X
S_i	Certificate of U_i generated through SC
Se_{SC}, Sd_{SC}	Public/Private key of SC
$E_K(M)$	symmetric key cipher of plain text M using K
$D_K(C)$	symmetric key cipher of plain text C using K
SK_i	signature key of i
$\sigma_i(SK_i, M)$	signature of signatured M through P_i with Signature key
$Ver(PK_i, M, \sigma_i)$	Validate signature σ_i of M with public key PK_i
$h(\bullet)$	one-way hash function
$\|$	concatenation

3.2 대리서명 프로토콜

제안 프로토콜에서는 환자와 병원관계자사이에서 환자의 동의 없이 환자의 대리서명자를 통하여 환자의 생체정보를 안전하게 사용할 수 있다.

3.2.1 초기화 과정

환자 U_i와 병원관계자 P_i는 자신들이 선택한 개인키 (p, q)와 공개키(N=pq,e)를 생성하는 RSA 기반의 공개키 기반구조를 가진다. 여기서, p와 q는 $p = 2q'+1$과 $q = 2p'+1$을 만족하는 임의로 생성되는 큰 솟수이다.

$$Select \;\; p,\; q \tag{1}$$

$0<M<N$인 정수 N, M 그리고 임의의 정수 k가 정해지면 식 (2)와 같은 식이 만들어진다.

$$M^{k\Phi(N)+1} = M^{k(p-1)(q-1)+1} \equiv M \bmod N \tag{2}$$

여기서, $\Phi(N)$은 N보다 적고 N과 서로소인 양의 정수가 되는 함수를 의미하며 p, q가 솟수일 때, $\Phi(pq)=2pq$를 이용하여 식 (3)을 구한다.

$$ed = k\Phi(N) + 1 \tag{3}$$

여기서, e와 d는 mod $\Phi(N)$의 곱셈 역원이다. 모듈러 연산 규칙에 따라 d(와 e)는 $\Phi(N)$에 서로소이다.

환자 U_i는 개인키와 공개키를 각각 (p, q)와 (N, e)를 가진다. 또한, H_U: $\{0,1\} \rightarrow Z_N$는 환자 U_i가 사용하는 안전한 해쉬함수이며 H_P:$\{0,1\}^* \times Z_N \rightarrow Z_P$는 병원관계자 P_i가 사용하는 안전한 해쉬 함수를 의미한다.

$$H_U: \; \{0,1\} \rightarrow Z_N \tag{4}$$
$$H_P: \{0,1\}^* \times Z_N \rightarrow Z_P \tag{5}$$

3.2.2 위임 과정

위임 과정은 체내삽입장치를 부착한 환자 U_i의 서명권한을 병원관계자가 대리로 서명을 위임받는 과정이다.

이 과정은 환자와 병원관계자 사이의 정보를 이용하여 대리서명을 크게 3단계로 구성된다.

- 1 단계 : 환자 U_i는 서명에 대한 권한이나 유효기간 등의 대리서명과 관련된 정보를 포함하고 있는 위임장 m_i를 생성한 후 공개한다.

$$Generate \;\; m_i \;\; (1 \le i \le n,\; n \in Z^*) \tag{6}$$

- 2 단계 : 환자 U_i는 위임장 m_i을 이용하여 식 (7) 의 과정을 통해 서명과정을 거친 후 병원관계자에게 식 (8)의 인증서를 전달한다.

$$d_1 = \begin{cases} 0, \dfrac{H(m_i, T)}{N}\%2 \\ 1, \dfrac{H(m_i, T)}{N}\%2 \end{cases} \quad d_2 = \begin{cases} 0, \dfrac{d_2, H(m_i, T)}{p}\%2 \\ 1, \dfrac{d_1, H(m_i, T)}{p}\%2 \end{cases} \tag{7}$$

여기서 T는 병원관계자가 임의로 선택한 랜덤수 $t \in Z_N$를 선택한 후 $T = t^2 \bmod N$을 통해 구한다.

$$Sig = (-1)^{d_2} \cdot e^{d_1} \cdot H(m_i, T) \bmod N \tag{8}$$

- 3 단계 : 환자 U_i는 병원관계자 P_i에게 식 (9)와 같은 인증서를 전달한다.

$$Transfer \;\; m,\; Sig,\; T,\; d_1,\; d_2 \tag{9}$$

3.2.3 서명 과정

서명 과정은 환자 U_i가 유헬스케어 서비스 센터 C_i에게 대리서명 정보를 전달하여 환자 U_i 대신 환자의 생체정보를 서명할 수 있도록 하는 과정이다.

- 1 단계 : 유헬스케어 서비스 센터 C_i는 임의로 선택한 정수 $r \in Z_N$를 선택한 후 R ($=r^2 \bmod N$)을 계산한다.

$$Select \quad r \in Z_N \tag{10}$$
$$R = r^2 \bmod N \tag{11}$$

- 2 단계 : 유헬스케어 서비스 센터 C_i는 대리서명을 수행하기 위해서 식 (12)과 같이 d_1과 d_2을 계산한다.

$$d_1' = \begin{cases} 0, \dfrac{H(m_i, T)}{N}\%2 \\ 1, \dfrac{H(m_i, T)}{N}\%2 \end{cases} \quad d_2' = \begin{cases} 0, \dfrac{d_2, H(m_i, T)}{p}\%2 \\ 1, \dfrac{d_1, H(m_i, T)}{p}\%2 \end{cases} \quad (12)$$

- 3 단계 : 유헬스케어 서비스 센터 C_i는 식 (12)에서 생성된 d_1과 d_2을 이용하여 랜덤 수 r_1과 r_2를 식 (13) ~ 식 (14)처럼 생성한다.

$$r_1 = Sig \cdot t \mod N \quad (13)$$

$$r_2 = (-1)^{d_2} \cdot e^{d_1} \cdot H(m_i, T) \mod N \quad (14)$$

- 4 단계 : 유헬스케어 서비스 센터 C_i는 d_1', d_2', r_1, r_2을 이용하여 식 (15)처럼 대리서명을 생성한 후 생체정보와 함께 병원관계자에게 P_i에게 전달한다.

$$p\sigma = (m,\ T,\ d_1,\ d_2,\ d_1',\ d_2',\ r_1,\ r_2) \quad (15)$$

3.2.4 검증 과정

병원관계자 P_i는 유헬스케어 서비스 센터 C_i로부터 전달받은 대리서명 $p\sigma$를 검증하기 위하여 식 (16)~식 (18)까지의 과정을 수행한다.

$$R_1 = r_1 \mod N \quad \text{and} \quad R_2 = r_2 \mod N \quad (16)$$

$$Sig = (-1)^{d_2} \cdot e^{d_1} \cdot H(m_i, T) \mod N \quad (17)$$

$$T' = R_1 \cdot Sig \quad \text{and} \quad T'' = R_2 \cdot Sig \quad (18)$$

병원관계자 P_i는 식 (19) ~ 식 (20)을 계산하여 T와 T'''가 일치하는지를 검증한다. 만약 일치하지 않다면 병원관계자 P_i는 유헬스케어 서비스 센터 C_i로부터 다시 대래서명을 전달받는다.

$$T''' \equiv T' \mod N \quad \text{and} \quad T''' \equiv T'' \mod N \quad (19)$$

$$T \equiv T''' \mod N \quad (20)$$

4. 보안평가

4.1 재사용공격

제안 프로토콜에서는 재사용공격을 예방하기 위해서 헬스케어 서비스 센터 C_i가 임의로 선택한 정수 $r \in Z_N$를 선택한 후 R (=r^2 mod N)을 계산하기 때문에 제3자에게 도청되더라도 안전성을 보장받는다. 유헬스케어 서비스 센터 C_i는 대리서명을 수행하기 위해서 d_1', d_2', r_1, r_2을 이용하여 병원관계자에게 전달하기 때문에 재사용공격에 안전한다.

4.2 스푸핑 공격

제안 프로토콜에서는 d_1과 d_2을 이용하여 랜덤 수 r_1과 r_2를 사용하기 때문에 제3자가 환자의 대리서명 $p\sigma$를 알지 못하기 때문에 스푸핑 공격에 안전하다. 또한, 제3자가 환자의 체내삽입장치의 정보 $p\sigma$를 전달할 때 이전 대리서명 정보를 도청하더라도 랜덤 수 r_1과 r_2를 알지 못하기 때문에 검증 과정에서 R_1과 R_2 값이 서명 Sig과 조합하여 생성된 T'와 T''이 일치하지 않는다. 제안 프로토콜에서는 검증과정에서 T'와 T''를 계산하여 비교하기 때문에 제3자의 공격을 막을 수 있다.

4.3 정보노출방지

제안 프로토콜은 환자가 인증서버에 접근할 때마다 환자와 관리자가 생성하는 랜덤 수 r_1과 r_2를 사용하기 때문에 제3자에 의해서 환자의 정보가 노출되더라도 인식하지 못한다. 관리자는 환자의 체내삽입장치의 정보를 제3자가 불법적으로 사용하지 못하도록 대리 서명 Sig를 사용한다.

4.4 다단계 서비스 접근인증에 따른 공격

제안 프로토콜에서는 유헬스케어 서비스 센터가 생성한 R_1, R_2와 대리서명을 위해 d_1과 d_2을 이용하여 랜덤 수 r_1과 r_2를 생성하기 때문에 권한이 없는 제3자는 환자의 생체정보를 불법적으로 접근할 수 없다. 제안 프로토콜에서는 대리 서명에 따라 상호간 등록 및 인증 요청, 키 교환, 디바이스 인증 정보 전송, 인증 결과 전송 등이 이루어진다.

4.5 환자의 프라이버시 공격

제안 프로토콜에서는 환자의 프라이버시를 보장하기 위해서 유헬스서비스 센터가 생성한 랜덤 수 r_1과r_2를

대리서명에 적용하여 생체정보와 함께 병원관계자에게 전달하기 때문에 환자의 생체정보를 보호할 수 있다. 이 같은 방법은 병원관계자가 병원 내 여러 장소에서 환자의 생체정보를 수집하려고 할 경우 유헬스서비스 센터는 환자의 대리서명 정보를 관리하기 때문에 환자의 생체정보에 대한 가용성을 보장할 수 있어 환자의 프라이버시를 보호할 수 있다.

5. 결론

최근 의료기술의 발달로 인하여 체내삽입장치가 불치병(심장병, 당뇨병, 심근경색 등)을 치료하기 위해 사용되고 있지만 환자의 프라이버시 보안 피해 또한 증가하고 있다. 본 논문에서는 유헬스케어 환경에서 체내삽입장치를 부착한 환자의 생체정보를 제3자가 환자로 위장하여 병원관계자로부터 환자 정보를 악용하는 것을 예방하기 위한 위임장 기반의 서명 인증 프로토콜을 제안하였다. 제안 프로토콜은 헬스케어 서비스 센터가 임의로 선택한 정수를 이용하여 대리서명을 수행하기 때문에 재사용 공격, 스푸핑공격 등에 안전성을 보장받으며, 유헬스케어 서비스 센터와 환자가 생성한 랜덤수로 해쉬한 서명키로 환자의 민감한 정보를 암호화하여 환자의 민감한 정보를 제 3자에게 노출시키지 않는다. 향후 연구로 본 연구의 결과를 기반으로 체내삽입장체에 실제 적용할 계획이다.

REFERENCES

[1] Y. S. Jeong(2012), “RFID-based Authentication Protocol for Implantable Medical Device”, The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 141-146.

[2] Y. Zhou, Z. Cao, and R. Lu(2005), “Provably secure proxy-protected signature schemes based on factoring”, Appl. Math. Comput. Vol. 164, No. 1, pp. 83-98.

[3] Y. S. Jeong and S. H. Lee(2012), “u-Healthcare Service Authentication Protocol based on RFID Technology”, The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 153-160.

[4] K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta(2010), “PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks”, Vol. 14, No. 1, pp. 60-68.

[5] M. Mambo, K. Usuda, and E. Okamoto(1996), “Proxy signatures for delegating signing operation”, Proc. Third ACM Conf. on Computer and Communications Security. pp. 48-57.

[6] R. Lu, Z. Cao and Y. Zhou(2004), “A simple efficient proxy-protected signature scheme based on factoring”, Comp. Stand. Inter., withdrawn.

[7] E. J. KO(2009), “Leading health care revolution smart sensors”, LG Business Insight, pp. 37-44.

[8] Y. S. Jeong, S. H. Lee(2012), “U-Healthcare user’s privacy protection protocol with Implantable medical Device of State Information”, THE JOURNAL OF KOREA INFORMATION AND COMMUNICATIONS SOCIETY (J-KICS), Vol. 37, No. 4, pp. 277-353.

정 윤 수(Jeong Yoon-Su)

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail : bukmunro@gmail.com