스마트워크 환경에서 안전한 디바이스 인증 프로토콜에 관한 연구

정수영*, 곽 진*

요약

스마트워크는 사람들에게 좀 더 편리한 근무환경을 제공해주는 유연한 근무형태이다. 이미 국내·외 많은 국가에서는 편리한 근무환경 제공을 위해 스마트워크 도입을 추진하고 있다. 이렇게 스마트워크에 대한 관심이 높아지면서 보안 위협에 대한 중요도 또한 높아지게 되었다. 특히 인증되지 않은 디바이스를 통해 공격자에게 기업의 기밀정보가 유출될 가능성이 있다. 따라서 본 논문에서는 사용자와 디바이스의 ID를 기반으로 XOR 연산과 해쉬연산을 이용한 경량화된 인증 프로토콜을 제안한다.

A Study on Secure Device Authentication Protocol in Smart Work Environment

Su-Young Jung*, Jin Kwak**

ABSTRACT

Smart work is flexible work type providing convenient work environment to people. Many countries are promoting introduction of smart work provide for convenient work environment. This importance about security threat was increased while interest about smart work was increased. Especially, if not authentication device, the attacker possible leak data for company's secret information. In this paper, we propose user and device based light-weight authentication protocol using XOR operation and hash operation.

Key Words : Smart work, Remote work, Device authentication, Authentication protocol, Security

* 순천향대학교 정보보호학과 정보보호응용및보증연구실(✉syjung@sch.ac.kr)
** 순천향대학교 정보보호학과
· 제1저자(First Author) : 정수영 · 교신저자(Correspondent Author) : 곽 진
· 접수일(2011년 9월 21일), 수정일(1차 : 2011년 10월 28일), 게재확정일(2011년 10월 31일)

Ⅰ. 서 론

IT 기술의 발전과 더불어 편리한 업무환경에 대한 관심이 높아지면서 다양한 디바이스를 활용한 기술이 연구되고 업무환경의 발전에 따른 스마트워크 환경으로의 변화가 진행되고 있다. 스마트워크는 시간과 공간의 제약을 받지 않고 업무를 수행할 수 있도록 도와주는 유연한 근무 형태로, 기업의 예산 절감, 출·퇴근 시간 단축 및 탄소 배출량 감소 등의 효과를 제공하는 친환경적인 업무환경이다[1, 2].

스마트워크는 자택에 있는 컴퓨터를 활용해 업무를 수행하는 재택근무, 스마트폰 및 태블릿 PC를 이용한 이동근무, 댁내에 가까운 스마트워크센터에 출근해 업무를 수행하는 스마트워크센터근무로 구분할 수 있다.

스마트워크는 이미 국내·외에서 많은 관심을 갖고 도입을 추진하고 있다. 국외에서는 미국, 일본, 네덜란드 등이 국가적인 차원에서 스마트워크를 도입하여 실제로 많은 효과를 입증하였다. 국내에서는 2010년 11월 스마트워크 센터 1호 개설을 시작으로 2012년에는 12개소를, 2015년까지는 공공 50개, 민간 450개의 스마트센터 구축을 목표로 추진하고 있다[5, 6].

앞서 언급한 것과 같이 스마트워크는 많은 효과를 제공하기 때문에 많은 국가가 도입을 추진하고 있지만 스마트워크로 제공되는 근무환경에는 다양한 IT기술의 접목으로 많은 보안 위협이 존재하게 된다. 특히 사용자가 디바이스를 이용해 기업의 디바이스 인증 서버와 통신할 때 인증이 제대로 이루어지지 않아 디바이스 위장 공격, 불법 프로그램 전송 등의 문제가 발생할 수 있다.

따라서 본 논문에서는 스마트워크 환경에서 디바이스와 기업의 디바이스 인증 서버 간 상호인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 스마트워크에 대한 개념과 ID기반 및 PKI 기반 방식을 살펴보고, 3장에서는 스마트워크 환경에서 발생할 수 있는 보안 문제점에 대해 서술한다. 4장에서는 보안 위협에 대비할 수 있는 보안 요구사항을 서술하고, 5장에서는 스마트워크 환경에서 안전한 디바이스 인증 프로토콜을 제안한다. 6장에서는 제안한 프로토콜에 대해 안전성 및 효율성을 분석하고, 마지막으로 7장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 스마트워크 개념

스마트워크는 기존의 사무실이라는 한정된 공간에서 업무를 수행하는 개념과는 다르게 스마트폰, 태블릿 PC, 클라우드 컴퓨팅, 광대역 통신 등의 정보통신기술(ICT : Information and Communication Technology)을 활용하여 시간과 공간의 제약 없이 언제, 어디서나 업무를 수행하는 환경을 말한다[7].

스마트워크는 근무 장소 및 방식에 따라 재택근무, 이동근무, 스마트워크센터근무로 구분할 수 있다[8].

그림 1. 스마트워크 개념
Fig. 1. Smartwork Concept

• 재택근무

자택에 구축되어 있는 정보통신망을 이용해 본사에 접속하여 업무를 수행하는 형태로 출·퇴근 시간을 허비하거나 교통비에 대한 부담을 감소시킬 수 있다. 또한 별도의 공간이 필요 없다.

사무실에서 근무하기 불편한 장애인, 육아 휴직자, 노약자 등에게 유용한 업무 환경이다.

• 이동근무

스마트폰, 태블릿 PC 등을 이용하여 무선통신서비스를 사용하는 것으로 대부분의 업무시간을 밖에서 보내는 영업, 컨설팅 등의 직종에 종사하는 인원들에게 유용한 근무형태이다. 시간과 공간의 제약 없이 업무를 신속하게 처리할 수 있다.

• 스마트워크센터근무

자택 근처에 사무실과 적합하거나 유사한 환경이 구축되어 있는 곳에 출근하여 업무를 수행할 수 있는 형태이다. 근태관리가 용이하고 보안성이 높으며, 육아 놀이시설, 편의시설 등이 마련되어 있어 업무의 효율성이 향상될 수 있다[9].

2.2 PKI 기반 인증방식

PKI 기반 인증방식은 클라이언트에서 홈 네트워크를 제어하기 위한 인증기술로 인증서를 이용한다. 사전에 사용자가 홈 클라이언트 디바이스를 통해 인증서를 직접 발급받고, 서버에 직접 디바이스를 등록한 후 디바이스에 해당하는 대칭키를 발급받아 인증 절차에 사용한다. 또한 인증서를 이용하여 홈 네트워크에 접근 권한을 설정할 수 있어 허가받지 않은 사람의 접근을 차단할 수 있다[10].

PKI 기반 인증방식은 인증 스니핑, 재전송 공격 등에 안전성을 제공하고 있지만 통신 횟수가 많고 생성 및 전송단계에서 연산량이 많다.

2.3 ID 기반 인증방식

ID 기반 인증방식은 동적 ID 기반의 원격사용자 인증으로 연산량이 적은 XOR 연산 및 해쉬연산을 이용한다. 동적 ID 기반을 통해 ID가 유출되어도 다른 ID를 이용할 수 있어 ID 유출에 대비할 수 있다. 중간자 공격에 대응하기 위해 타임스탬프 값을 사용하고 자유롭게 패스워드를 수정할 수 있는 것이 특징이다. 하지만 실시간 재사용 공격이 가능하다는 문제점을 갖고 있다[11].

인증 방식에서 적은 통신 횟수와 해쉬연산 및 XOR 연산을 이용하여 연산량이 적다는 장점이 존재한다.

III. 문제점 분석

스마트워크는 시간과 공간의 제약 없이 언제 어디서나 업무를 처리할 수 있는 환경을 말한다. 스마트폰과 태블릿 PC를 이용해 이동근무가 가능하고 스마트워크센터나 재택근무를 통해 출·퇴근 시간을 절약할 수 있다.

앞에서 언급한 것과 같이 스마트워크는 많은 편리함이 있지만 기업의 내부자료 유출에 쉽게 노출되어 있어 기업에게 금전적으로 큰 피해를 입을 수 있다.

다음은 스마트워크 환경에서 발생할 수 있는 문제점을 나타낸다.

• 위장 공격

사용자와 서버간의 통신하는 과정에서 사용자의 정당성을 인증하지 않거나 인증에 필요한 ID가 노출될 경우 공격자가 정당한 사용자로 위장이 가능한 문제점이 있다.

• 정보 변조

디바이스 인증 과정에서 악의적인 공격자가 중간자 공격과 재전송 공격을 통해 정보를 가로채 정보가 포

함하고 있는 내용을 변조, 유출할 가능성이 존재한다.

• 취약한 보안 환경

스마트워크센터는 일정 수준의 보안 관리가 이루어지고 있지만 이동근무, 재택근무의 경우 개인적으로 관리를 해야 하기 때문에 대부분의 경우 악성코드 등에 쉽게 노출되어 있다.

Ⅳ. 스마트워크 보안 요구사항

스마트워크 환경에서는 많은 IT기술을 이용하기 때문에 다양한 보안위협이 존재하고 있다. 이러한 보안위협은 사용자 및 기업의 측면에서 많은 피해를 입을 수 있기 때문에 보안 요구사항에 대한 연구가 필요하다.

스마트워크 환경에서의 보안 요구사항들은 다음과 같다.

4.1 무결성

통신상에서 전송되는 데이터들은 업무 내용을 포함하고 있기 때문에 기업의 기밀정보가 포함되어 있다. 따라서 이러한 정보가 중간자 공격, 재전송 공격 등에 의해 위·변조될 경우 기업에 많은 피해가 발생할 수 있다. 따라서 통신 과정에서는 무결성이 보장되어야 한다.

4.2 기밀성

디바이스와 기업의 인증 서버의 통신 과정에서 인증을 위해 사용되는 값은 직접적으로 노출되지 않아야한다. 사용자와 DB 시스템에서 서로를 인증하기 위한 값이 노출될 경우 이 값을 이용하여 암호화된 데이터를 복호화 할 수 있으며, 공격자가 정상적인 사용자로 위장하는 위장공격이 발생할 수 있다.

4.3 상호인증

스마트워크 환경에서 사용자가 디바이스를 이용하여 기업 내부 서버에 접근하기 위해서는 디바이스와 기업 내부 서버간의 상호인증이 필요하다. 인증이 이루어지지 않을 경우 위장 공격을 통한 불법적인 프로그램, 악성코드 등의 문제가 발생할 수 있다.

Ⅴ. 안전한 디바이스 인증 프로토콜

사용자의 디바이스를 사용하여 기업 내부 서버에 접근할 때 정당한 디바이스 및 인증 서버에 대해 확인하지 않으면 내부 서버에 불법 프로그램, 악성코드 등으로 인한 문제가 발생할 수 있다.

본 논문에서는 앞에서 분석한 보안 요구사항을 기반으로 안전한 스마트워크 환경을 위한 디바이스/디바이스 인증서버 상호간의 인증 프로토콜을 제안한다. 제안한 인증 프로토콜은 디바이스 등록 과정에서 사용하는 공개키 암호화를 제외하고는 XOR 연산 및 해쉬함수를 이용한 인증을 통해 경량화된 인증 기법을 제공한다.

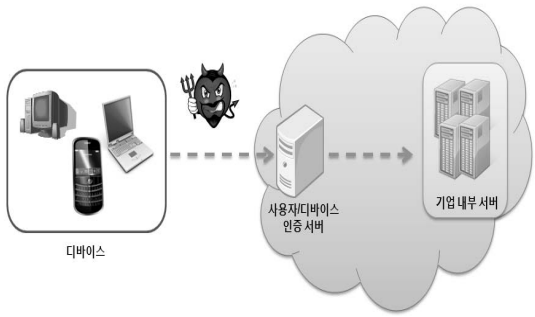

그림 2. 제안방안 흐름도
Fig. 2. Suggestion Flow Chat

표 1은 제안된 인증 프로토콜에서 사용하는 시스템 파라미터이다.

표 1. 시스템 파라미터
Table 1. System Parameters

계수	설명
ID_*	사용자가 갖고 있는 ID
PW_U	사용자의 패스워드
R	디바이스에서 생성한 랜덤값
pk	디바이스 인증 서버의 공개키
sk	디바이스 인증 서버의 비밀키
$E[\bullet]$	암호화
$D[\bullet]$	복호화
$h(\bullet)$	일방향 해쉬 함수
T_*	타임스탬프 값
$\oplus$	배타적 논리합 연산
$\|\|$	연접 연산

5.1 디바이스 등록 단계

등록 단계는 기업의 디바이스 인증 서버에 등록하기 위한 사용자 아이디와 패스워드를 연접하여 해쉬함수한 N값을 생성한다. 사용자 아이디 ID_U와 패스워드 PW_U에 대한 정보는 사전에 디바이스 인증 서버에 저장되어 있다고 가정한다. 생성한 N값은 디바이스 인증 서버에 저장하여 디바이스와의 인증 과정에서 사용하고, 디바이스 아이디는 디바이스 인증 서버에서 N값을 얻기 위한 용도로 사용한다.

등록 단계는 다음과 같이 진행된다.

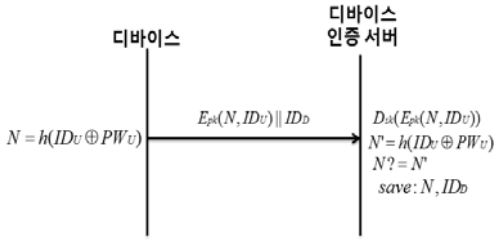

그림 3. 디바이스 등록 단계
Fig. 3. Device Registration Phase

Step 1. 디바이스는 사용자의 아이디인 ID_U와 패스워드인 PW_U를 XOR 연산 후 해쉬연산을 하여 N을 생성한다.

$$N = h(ID_U \oplus PW_U) \quad (1)$$

Step 2. 디바이스는 앞에서 생성한 N과 사용자의 아이디인 ID_U, 디바이스의 아이디인 ID_D를 공개키를 이용해 암호화하여 디바이스 인증 서버로 전송한다.

$$E_{pk}(N,\ ID_U) \| ID_D \quad (2)$$

Step 3. 디바이스 인증서버는 자신의 비밀키를 이용하여 전송받은 $E_{pk}(N, ID_U)\|ID_D$를 복호화한다. 복호화하여 얻은 사용자 ID인 ID_U를 사전에 등록되어 있는 정보를 통해 해당 PW_U를 찾는다. 검색하여 얻은 ID_U와 PW_U를 XOR 연산 후 해쉬연산하여 N'를 생성한다. 생성한 N'과 디바이스에서 전송 받은 N을 비교하여 확인한다. 확인 후이상이 없을 경우 N과 함께 디바이스 인증 서버에 ID_D를 저장한다.

$$D_{sk}(E_{pk}(N, ID_U)) \quad (3)$$
$$N' = h(ID_U \oplus PW_U) \quad (4)$$
$$N? = N' \quad (5)$$
$$save: N, ID_D \quad (6)$$

5.2 디바이스 인증 단계

등록 단계를 통해 디바이스 인증 서버에 저장된 값을 이용하여 인증한다. 랜덤 값인 R을 생성하고 N을 이용하여 S를 생성하고 R과 함께 디바이스 인증 서버로 전송한다. N의 값이 직접적으로 노출되지 않기 때문에 인증을 위해 사용하는 S를 추측하기 어려워 안전성을 보장할 수 있다.

인증 단계는 다음과 같이 진행된다.

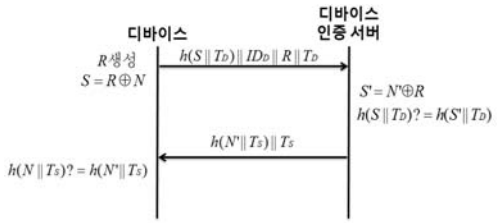

그림 4. 디바이스 인증 단계
Fig. 4. Device Authentication Phase

Step 1. 디바이스는 랜덤 값인 R을 생성한다. 디바이스 인증 서버에서 디바이스를 인증하는데 사용하기 위한 S를 앞에서 생성한 R과 N을 XOR 연산하여 생성한다.

$$R \text{ 생성} \tag{7}$$
$$S = R \oplus N \tag{8}$$

Step 2. 디바이스는 앞에서 생성한 S를 디바이스의 타임스탬프값 T_D 와 연접한 후 해쉬연산을 한다. 해쉬연산한 값 $h(S \| T_D)$, 디바이스의 아이디인 ID_D, 랜덤한 값 R을 타임스탬프 값 T_D와 함께 연접하여 디바이스 인증 서버에 전송한다.

$$h(S \| T_D) \| ID_D \| R \| T_D \tag{9}$$

Step 3. 디바이스 인증 서버는 디바이스에서 전송받은 타임스탬프 값 T_D를 비교하여 시간 차이를 확인한다. 확인 후 디바이스로부터 전송 받은 ID_D를 자신이 저장하고 있는 값과 비교를 통해 N을 찾는다. 찾은 N을 디바이스에서 전송받은 R과 XOR 연산하여 S'를 생성한 후 디바이스로부터 전송받은 타임스탬프 값 T_D와 연접하여 해쉬연산하고 그 값을 디바이스에서 전송받은 $h(S \| T_D)$와 비교하여 확인한다.

$$S' = N' \oplus R \tag{10}$$
$$h(S \| T_D) ? = h(S' \| T_D) \tag{11}$$

Step 4. 디바이스 인증 서버는 N'을 디바이스 인증 서버의 타임스탬프 값 T_S와 연접하여 해쉬연산한다. 해쉬연산한 값을 타임스탬프 값 T_S와 연접하여 디바이스에게 전송한다.

$$h(N' \| T_S) \| T_S \tag{12}$$

Step 5. 디바이스는 디바이스 인증 서버로부터 전송받은 타임스탬프 값 T_S를 이용하여 재전송 공격 여부를 확인한다. 확인 후 T_S와 N을 연접하여 해쉬연산한다. 해쉬연산한 값과 $h(N' \| T_S)$를 비교하여 확인한다. 확인 후 이상이 없을 경우 인증을 완료한다.

$$h(N \| T_S) ? = h(N' \| T_S) \tag{13}$$

VI. 제안사항 분석

본 논문에서는 스마트워크 환경에서 안전한 디바이스 인증 프로토콜을 제안하였다. 표2는 안전성 및 효율성에 대한 비교·분석을 나타낸다.

표 2. 안전성 및 효율성 비교·분석
Table 2. Comparison·analysis of Security and Efficiency

구분	PKI	Das	제안사항
상호인증	O	X	O
	인증서를 통한 인증	원격 시스템 인증 불가	사용자 ID를 통한 인증
무결성	O	O	O
기밀성	O	O	O
연산량	2h+3U	12h+2E	6h+1U
통신횟수	4	3	3

- h: 해쉬연산, E: 대칭키 연산, U: 공개키 연산

6.1 안전성 분석

무결성, 기밀성, 상호인증을 증명하는데 활용되는 값인 N은 사전에 사용자와 디바이스 서버가 갖고 있기 때문에 통신상에서 직접적으로 노출이 되지 않아 추측하기 어려워 공격자가 임의의 값을 만들어도 인증을 완료할 수 없다.

- 무결성

디바이스와 기업의 디바이스 인증 서버 간의 통신에서 $h(S \| T_D)$와 $h(S' \| T_D)$ 확인을 통하여 디바이스의 무결성이 보장된다. 또한 $h(N \| T_S)$와 $h(N' \| T_S)$ 비교를 통해 디바이스 인증 서버의 무결성이 확인된다.

따라서 디바이스와 디바이스 인증 서버는 무결성을 제공한다.

- 기밀성

디바이스와 기업의 디바이스 인증 서버간의 등록과정에서 인증을 위해 사용하는 값인 N, ID_U을 공개키로 암호화하여 $E_{pk}(N, ID_U)$을 전송한다. 전송과정에서 직접적으로 N과 ID_U가 노출되지 않기 때문에 공격자가 유추하기 어렵고 인증 과정을 통해 정당한 사용자에게만 데이터가 공유된다.

- 상호인증

디바이스 인증 서버는 디바이스에서 전송받은 $h(S \| T_D)$를 $S' = N' \oplus R$ 과정을 거쳐 $h(S' \| T_D)$와 비교하여 무결성이 확인되기 때문에 디바이스를 인증한다.

디바이스는 디바이스 인증 서버에서 전송받은 $h(N' \| T_S)$를 디바이스 인증 서버에서 받은 T_s를 이용하여 생성한 $h(N \| T_S)$와 비교하여 무결성이 확인되고 디바이스 인증서버를 인증한다.

따라서 디바이스와 디바이스 인증 서버는 상호 인증을 제공한다.

6.2 효율성 분석

- Das

동적 ID 기반 인증방식은 통신 횟수는 3번으로 적지만, 12번의 해쉬연산과 2번의 암호화로 인해 연산량이 많다. 또한 인증과정에서 같은 사용자가 인증메세지를 식별할 수 있기 때문에 효과적으로 사용자 익명성을 보장할 수 없다.

- PKI 기반

PKI 기반 인증방식은 통신 횟수는 4회 이지만 공개키 암호를 사용하기 때문에 연산량이 많고 인증서를 통한 상호인증을 수행하기 때문에 다른 방식보다 통신 횟수가 많다.

- 제안 방식

본 논문에서 제안한 방식은 통신 횟수는 3회로 적다. 연산량은 해쉬함수를 6번사용하고 공개키 암호를 1번 사용함으로써 경량화 시켰다. 사용자 ID와 패스워드를 해쉬연산한 값 N을 이용하여 상호인증 절차를 수행한다.

Ⅶ. 결 론

스마트워크는 재택근무, 이동근무, 스마트워크센터 근무 등의 유연한 업무환경제공으로 시간과 공간을 효율적으로 활용할 수 있게 해주고 편의성을 제공해준다. 또한 기업의 예산 절약, 출·퇴근 탄소 배출량 감소 등의 효과도 제공해준다. 하지만 클라우드 컴퓨팅, 광대역 통신, 스마트폰, 태블릿 PC 등의 다양한 IT기

술을 활용하기 때문에 이에 따른 많은 보안 위협에 노출되어 있다. 특히 사용자 디바이스와 기업의 디바이 인증 서버 간 통신에서 인증이 이루어지지 않으면 공격자의 공격 목표가 될 수 있다.

이에 본 논문에서는 스마트워크 환경에서 디바이스 인증을 위한 프로토콜을 제안했다. 또한 디바이스와 서버간의 통신 과정에서 랜덤 값을 이용하여 중간자 공격을 방지하고, 상호인증을 통해 정당한 디바이스와 기업의 인증 서버가 통신을 할 수 있는 프로토콜을 제안하였다.

본 논문은 스마트워크 환경을 도입하여 안전한 디바이스 인증을 시스템을 구축하는데 활용될 수 있을 것으로 기대된다.

참고문헌

[1] NIST SP 800-46, "*Guide to Enterprise Telework and Remote Access Security*", 2009.

[2] NIST SP 800-114, "*User's Guide to Securing External Devices for Telework and Remote Access Security*", 2007.

[3] 박승권, 이주한, "스마트워크 기술과 표준화 동향", 표준 *기술동향*, July 2011.

[4] 이재성, 김홍식. "스마트워크 현황과 활성화 방안 연구", *한국지역정보화학회지*, 제13권 제4호, pp.75-96, 2010

[5] 행정안정부, "*스마트워크 추진 계획*", 2011.

[6] 스마트워크센터, http://www.smartwork.go.kr/

[7] OPM, "*Status of Telework in the Federal Government*", 2011.

[8] Robin Simpson. "*How to Keep Mobile & Remote Workers Happy in 2010*", 2010.

[9] 현욱, 강신각, "스마트워크 표준화 동향", *전자통신동향분석*, 제26권, 제2호, 2011.04.

[10] 이영구, 김정재, 김현철, 전문석, "PIK 기반 홈 네트워크 시스템 인증 및 접근제어 프로토콜에 관한 연구", *한국통신학회논문지*, Vol. 35 No. 4, 2010.

[11] M. L. Das, A. Saxena and V. P. Gulati, "*A dynamic ID-based remote user authentication scheme*", IEEE Trans. Consumer Electron., vol. 50, No. 2, pp. 629-631, May 2004.

감사의 글

본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2011-0007755).

저자소개

정수영(Su-Young Jung)

2006년~현재 순천향대학교 정보보호학과 재학

※ 관심분야 : 스마트워크, 클라우드 컴퓨팅 보안 등

곽진(Jin Kwak)

2003년 성균관대학교 컴퓨터공학과 (공학석사)

2006년 성균관대학교 컴퓨터공학과 (공학박사)

2006~2006년 : 일본 큐슈대학교 방문연구원

2006~2006년 : 일본 큐슈시스템 정보기술연구소 특별연구원

2006~2007년 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관

2007~ 현 재 : 순천향대학교 정보보호학과 교수

2007~2009년 : 정보통신연구진흥원 집필위원

2009~2009년 : 순천향대학교 공과대학 교학부장

2009~2010년 : 순천향대학교 정보보호학과 학과장

2010~2010년 : 교육과학기술부 국가기술수준평가 전문위원

현재 : 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장

※ 관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 등