한국항행학회 논문지 제17권 제3호 2013년 6월 (JKONI 17(3): 314-324, Jun. 2013)

스마트워크 환경에 적합한 얼굴인식 기반 사용자 인증 기법

Secure User Authentication Scheme Based on Facial Recognition for Smartwork Environment

변연상*, 곽 진**

Yun-Sang Byun*, Jin Kwak**

요 약

스마트워크는 사용자들에게 신속한 업무처리와 편리한 근무환경을 제공해주는 미래지향적인 업무환경으로 이미 국내·외에서 스마트워크 도입을 추진하고 있다. 스마트워크 환경은 기존의 클라우드 컴퓨팅 환경과 유사한 형태의 클라이언트/서버 환경으로 외부에서 사용자들이 수시로 접근하여 업무를 처리한다. 특히 스마트워크 환경에서는 비 인가된 사용자들에 의해 악성코드가 내부로 유입되거나 기업의 기밀 정보를 유출할 가능성이 있기 때문에 이러한 보안 문제점을 해결할 수 있는 사용자 인증에 대한 필요성이 증가하고 있다. 그러므로 본 논문에서는 기존의 사용자 인증 기법 분석을 통해 스마트워크 환경에 적용 가능한 얼굴인식 기반의 사용자 인증 기법을 제안한다.

Abstract

Smartwork is future-oriented work-environment to bring swift business transaction and convenient for users. In domestic and foreign various countries, It's already prompting introduction of smartwork. Users process work to access frequently from the outside in smartwork that's a similar client/server environment to existing Cloud Computing environment. Necessary of user authentication is increasing to be solvable to security vulnerability because there is possibility that malware flows in and leaks company's confidential information by unauthorized users especially in smartwork environment. Therefore we propose User Authentication scheme based face recognition is applicable to smartwork environment to analyze established User Authentication scheme. environment.

Key words : Smartwork, User Authentication, Facial Recognition, Secure Smartwork

I. 서 론

최근 업무환경 개선에 대한 사람들의 관심이 증가하면서 다양한 환경에서 업무를 처리할 수 있는 스마트워크에 대한 연구가 빠르게 진행되고 있다. 스마트워크는 다양한 디바이스를 이용하여 시간과 공간의 제약을 받지 않고 업무를 수행할 수 있는 유연한 근무형태로 기업의 예산 절감, 출·퇴근 시간 단축으로 인한 탄소 배출량 감소 등 기존의 업무방식에서 탈피

* 순천향대학교 정보보호학과 정보보호응용및보증연구실(ISAA Lab. Department of Information Security Engineering Soonchunhyang University)
** 순천향대학교 정보보호학과(Department of Information security Engineering, Soonchunhyang University)
· 제1저자 (First Author) : 변연상(Yun-Sang Byunl, Tel : +82-70-7516-6293, email : ysbyun@sch.ac.kr)
· 접수일자 : 2013년 5월 15일 · 심사(수정)일자 : 2013년 5월 15일 (수정일자 : 2013년 6월 25일) · 게재일자 : 2013년 6월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.3.314

한 친환경적이고 미래지향적인 업무환경이다[1].

스마트워크는 클라이언트/서버 환경 기반으로 많은 사용자들이 외부에서 기업의 내부 데이터에 접근하여 업무를 처리하기 때문에 정당한 사용자 인증 과정이 필요하다. 만약 안전한 사용자 인증이 이루어지지 않을 경우 비인가 된 사용자가 접근하여 직원들의 개인 정보 획득 및 유출, 내부 네트워크에 악성코드 유포와 같은 피해가 발생할 수 있다. 또한 이로 인해 업무와 연관된 중요 데이터의 손실 및 유출될 가능성이 존재하고, 유출된 데이터를 통해 스팸메일, 스팸문자, 기업내부에 악성코드 유포와 같은 문제가 발생할 가능성이 존재한다[1],[2]. 이를 해결하기 위해 기존 네트워크 환경에서는 아이디/패스워드 기반의 인증 기법, 스마트카드와 같은 인증매체 기반의 인증 기법을 사용하고 있지만, 별도의 인증매체를 소지해야 하는 번거로움과 패스워드 엿보기 공격, 패스워드 추측 공격 등과 같은 간단한 공격에도 취약하다는 단점이 있다. 따라서 본 논문에서는 기존의 사용자 인증 기법 분석을 통해 스마트워크 환경에 적합한 얼굴인식 기반의 사용자 인증 기법을 제안한다.

본 논문은 2장에서 스마트워크 환경의 개념과 얼굴인식기술, 기존의 사용자 인증 기술 등에 대해서 분석한다. 3장에서 기존 인증 기법들을 분석하고, 4장에서 얼굴 인식 기반의 사용자 인증 기법을 제안한다. 5장에서는 제안 기법의 안전성 및 효율성에 대하여 분석하고, 끝으로 6장에서 결론을 맺는다.

Ⅱ. 관련연구

2-1 스마트워크

스마트워크는 기존의 한정된 사무실에서 업무를 수행하는 근무방식을 탈피하여 언제 어디서나 효율적으로 업무를 처리할 수 있는 미래지향적인 업무형태이다. 근무 방식 및 장소에 따라 회사가 아닌 가정에서 업무를 처리하는 재택근무, 다양한 디바이스를 이용하여 현장에서 업무를 수행하는 이동근무, 회사에서 별도로 구축한 장소로 출근하여 업무를 수행하는 스마트워크센터 근무로 구분할 수 있다. 근무형태의 유연성으로 인해 능력이 뛰어난 노약자, 임산부와 같은 취업이 힘든 계층의 취업기회 확대와 같은 효과를 기대할 수 있으며, 또한 현장에서 신속하게 업무처리가 가능하기 때문에 업무속도와 생산성 향상, 실시간 업무 처리, 신속한 의사결정 및 문제해결이 가능하다[1],[2].

2-2 얼굴인식기술

얼굴인식기술은 생체정보를 이용하여 인증을 수행하는 방식으로 신분조회, 출입통제, 무인감시 또는 범죄자 검색 등과 같은 응용분양에서 다양하게 사용되고 있는 기술이다. 초기에는 정지된 영상이나 사진을 이용하는 경우가 대부분이었지만 관련 연구가 활발하게 진행되어 지속적으로 발전되고 있다.

얼굴인식은 사용자에게 특별한 행동이나 행위를 요구하지 않으며, 사용자와 인식장치의 접촉 없이 인증을 수행하기 때문에 사용자의 거부감이 적다는 장점이 있으며, 각 사용자들 마다 서로 다른 특징을 기반으로 높은 안전성을 확보할 수 있다[3].

2-3 클라이언트/서버 아키텍처 기반 사용자 인증 기법

스마트워크 환경은 기존에 개발된 클라우드 컴퓨팅 환경이 진화된 환경으로 수많은 사용자가 동일한 인프라를 기반으로 업무를 처리하거나 서비스를 제공받을 수 있는 클라이언트-서버 아키텍처와 유사한 환경이다. 또한 클라우드 컴퓨팅 환경과 유사한 가상화 기술을 기반으로 구성되기 때문에 클라우드 컴퓨팅 관련 기술들이 스마트워크 환경에 대부분 적용 가능할 것으로 예상된다. 따라서 본 절에서는 기존 클라이언트/서버 아키텍처 기반의 사용자 인증 기법에 대해서 분석을 통해 문제점을 분석한다.

클라이언트-서버 아키텍처 기반의 인증 기법은 1981년 Lamport[4]에 의해 처음으로 제안되었으며, 이를 기점으로 인증 기술의 효율성이나 안전성에 대한 연구가 지속적으로 수행되기 시작하였다. Lamport가 제안한 인증 기법은 패스워드 테이블을 이용하여 사용자의 정당성을 확인하는 방법이지만 이 암호 테이블이 손상되거나 도난, 타인에 의해 수정될 경우

시스템이 사용자를 인식하지 못하는 경우가 발생하는 문제점이 있다. 그 이후 스마트카드를 이용한 패스워드 기반의 인증 기법이 Hwang [5] 등과 Khan [6] 등에 의해 새롭게 제안되었고, Hwang 등과 Khan 등의 제안 인증 기법은 안전성 및 효율성 등을 향상시켜 다시 제안되었다[5],[6]. 그 이후 Kim 등이 제안한 스마트카드와 지문을 이용한 ID 기반 패스워드 인증 기법은 도청에 의해 스마트카드와 지문, 아이디/패스워드를 이용하지 않고 로그온이 가능하다는 문제점이 있었다[7]. 이 외에도 제안된 많은 인증 기법이 취약한 것으로 분석되었다 [7],[8]. 이 후에도 지속적으로 클라이언트-서버 아키텍처기반의 사용자 인증 방법에 대한 연구가 활발하게 진행되었으며, 클라우드 컴퓨팅 환경이 널리 확산되면서 대규모 사용자들이 동일한 인프라를 사용하는 클라이언트-서버 아키텍처의 변형된 형태로 기존의 클라이언트-서버 간 네트워킹 시스템보다 강력한 인증을 요구되었다. 이에 따라 Lee [9] 등은 클라우드 컴퓨팅 환경에서 공개키 기반구조와 모바일 아웃 밴드를 이용한 인증 기법을 제안하였다. 그러나 Lee 등이 제안한 인증 기법은 사용자를 검증하기 위해 사용되는 수단인 아이디와 패스워드를 암호화하지 않고 평문 형태로 전송하여 도청과 같은 공격에 쉽게 노출될 수 있으며, 이를 통해 위·변조가 가능하다는 문제점이 존재한다.

Ⅲ. 문제점 분석

3-1 무결성(Integrity)

네트워크 환경에서는 기본적으로 데이터를 송·수신 할 경우뿐만 아니라 기존에 저장되어 있는 데이터에 대해서도 무결성이 보장되어야 한다. 스마트워크 환경은 외부에서 내부 데이터에 접근하기 위해 인터넷과 같은 공개된 네트워크를 이용하게 되며, 이러한 경우 가상 사설망(VPN)을 이용하여 데이터를 전송하는 경우보다 악의적인 사용자의 접근이 가능해지며, 그로 인한 다양한 취약점이 노출될 수 있으며, 악의적인 사용자가 내부 네트워크에 접근하여 데이터의 위·변조, 파괴 등 보안사고 발생 가능성이 증가하게 된다. 스마트워크 환경에서 이용하는 내부 데이터의 경우 데이터의 위·변조로 인해 잘못된 정보의 전파와 그로인한 업무 방해 등이 발생할 수 있기 때문에 이러한 문제점을 방지하기 위해서는 데이터의 무결성이 보장되어야 한다[2].

Lee 등이 제안한 인증 기법은 사용자를 검증하기 위해 사용되는 수단인 아이디/패스워드 등을 암호화되지 않은 평문 형태로 전송한다. 만약 평문 형태로 사용자의 아이디/패스워드가 전송될 경우, 악의적인 사용자가 해당 정보를 탈취하여 개인저보 유출, 변형, 위조 및 변조가 발생할 수 있으며 이로 인한 데이터 무결성을 보장할 수 없다.

3-2 기밀성(Confidentiality)

스마트워크 환경은 외부에서 내부 데이터에 접근하는 사용자가 대부분이므로, 만약 해당 데이터에 대한 기밀성이 확보 되지 않는다면 악의적인 사용자의 네트워크 무단 접근 및 침입으로 인한 개인 프라이버시 침해, 데이터 유출 등과 같이 데이터 안전성에 영향을 미치게 된다. 또한 유출된 데이터로 인한 스팸메일, 스팸문자, 피싱과 같은 추가적인 피해가 발생할 가능성이 있기 때문에 기밀성 보장은 필수적으로 요구된다[2]. Lee 등의 제안 기법에서는 앞서 분석한 바와 같이 아이디/패스워드 등을 악의적인 사용자가 쉽게 가로챌 수 있는 평문 형태로 전송하기 때문에 해당 데이터의 전송과정에서 도청과 같은 공격으로 습득하여 해당 사용자의 정보를 획득할 수 있기 때문에 데이터의 기밀성을 보장할 수 없다.

3-3 상호인증(Mutual Authentication)

다양한 사용자들이 외부에서 실시간으로 기업 내부로 접근하여 문제를 해결하거나, 각종 업무를 처리하는 스마트워크환경에서 사용자와 서버 사이에서 상호인증을 수행하지 않을 경우, 보안 문제점이 발생할 수 있다. 사용자가 악의적인 피싱 서버에 접근하여 사용자 정보를 입력하는 경우 서버 개설자가 사용자의 정보를 손쉽게 획득 가능하며, 획득한 정보를 악용하여 내부에 접근하는 것이 가능해진다. 또한 악의적인 사용자가 정당한 서버에 위장 접근할 경우 악

성코드 유포, 직원들의 개인정보 탈취, 기밀문서 유출과 같은 보안사고가 발생할 수 있다[2]. 따라서 이러한 피해를 예방하기 위해서는 사용자 인증 과정을 수행하는 경우에도 사용자와 서버 간에 상호인증과정이 필요하다. Hwang 등이 제안한 인증 기법은 사용자와 서버 사이에 상호인증 과정을 수행하지 않는다. 이로 인해 서버 또는 사용자로 위장하여 정보를 탈취하는 것이 가능하다.

3-4 위장공격(Impersonation Attack)

공개적인 네트워크를 이용하는 스마트워크 환경에서는 사용자 데이터를 불법 습득하여 정당한 사용자로 내부로 접근할 경우, 직원들의 개인정보, 기업 핵심 데이터 유출과 같은 문제점이 발생할 수 있다[2]. 그러나 Lee 등의 제안 기법에서는 아이디/패스워드를 암호화 과정 없이 평문 형태로 전송하며, 또한 사용자와 서버사이에서 상호인증 과정이 수행되지 않는다. 이러한 경우 악의적인 사용자가 손쉽게 아이디/패스워드를 탈취하고, 도용 또는 도난을 통해 정당한 사용자의 휴대전화를 이용해 정당한 사용자로 위장해 서버로 접속하는 것이 가능하고, 휴대전화를 통해 일회성 인증코드를 전송받는 것도 가능하다.

3-5 도청

Lee 등이 제안한 사용자 인증 방법에서는 사용자가 웹 서버로 전송하는 사용자의 아이디와 패스워드를 암호화 과정 없이 평문 형태로 전송한다. 따라서 악의적인 사용자가 일반 사용자의 아이디와 패스워드를 도청하는 것이 가능하다.

악의적인 사용자가 사전에 클라우드 서버에 정당한 사용자로 등록을 한 공격자가 사용자와 서버사이에서 도청을 통해 아이디와 패스워드를 확인하고 본인의 아이디와 패스워드를 전송하여 사용자 인증 과정을 수행하고, 정당한 사용자에게는 악성코드가 감염된 사이트로 접속을 유도하거나, 사용자의 개인정보를 이용한 스팸메일, 문자 전송 등 악성 행위를 하는 것이 가능해 진다.

표 1. 보안 취약점 분석
Table. 1. Analysis of Security Problems

	Hwang et al	Khan et al	Lee et al
무결성	O	O	X
기밀성	O	O	X
상호 인증	X	O	X
위장 공격	O	O	X
도청	X	X	X

O: 제공 / X:제공하지 못함

Ⅳ. 제안 기법

본 절에서는 스마트워크 환경에서 사용 가능한 얼굴인식 기반의 사용자 인증 기법을 제안한다. 제안 기법은 다양한 디바이스를 이용하여 외부에서 자유롭게 내부 데이터로 실시간으로 접속하여 업무를 처리 가능하고, 서비스를 제공받을 수 있는 스마트워크 환경에서 주로 사용되는 스마트 디바이스의 카메라를 이용한 얼굴 인증 기법이다. 본 논문에서 제안하는 인증 기법은 등록 단계와 로그인 및 인증단계로 구분되며, 등록 단계는 안전한 통신과 사용자 정보의 안전을 위해 최초 1회만 수행되며, 로그인 및 인증 단계는 서버에 접근할 때 마다 수행된다. 전체적인 제안 기법을 도식화하여 표현하면 아래 그림 1과 같다.

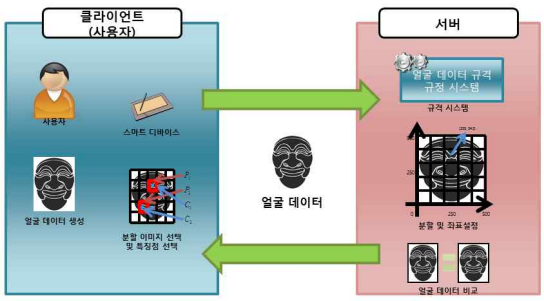

그림 1. 전체 흐름도
Fig 1. Proposed scheme concept

4-1 데이터 중심 추출과 규격 설정

본 논문에서 제안하는 사용자 인증 기법에서 얼굴 데이터를 사용하기 위해 최초의 데이터베이스에 저장되는 얼굴 데이터와 인증 과정에서 입력되는 데이터들의 다양한 크기의 데이터를 일정한 크기로 출력할 수 있는 규격 설정 과정과 정확한 인증 과정을 수행하기 위한 중심추출 과정을 진행한다.

4-1-1 얼굴 데이터의 중심 추출

입력된 얼굴 데이터의 경우 위치 및 크기가 계속 변경되기 때문에 얼굴 데이터의 크기를 규격화시키기 위한 기준이 되는 데이터의 중심이 필요하다. 따라서 본 논문에서는 얼굴 데이터의 규격화가 진행된 데이터의 중심점을 선택한다.

① 얼굴의 중심점은 코를 중심으로 상하좌우의 x, y좌표 기준점을 설정한다.
② 기준점을 중심으로 X축을 설정하고, 설정된 X축을 중심으로 Y축을 설정한다.
③ X축과 Y축이 설정되면 각 축의 중심을 기준으로 눈과 입의 위치를 파악하여, 상하를 구분한다.

얼굴 데이터의 중심이 추출된 다음 수평정렬, 입력받은 데이터의 규격 설정 과정이 진행된다.

그림 2. 데이터 중심 추출 과정
Fig 2. Data center extraction process

4-1-2 데이터 규격 설정

사용자의 얼굴 데이터가 디바이스를 통해 입력될 경우 해당 데이터의 인식과정을 수행하기 위해 입력되는 사용자의 얼굴 데이터는 일정한 크기로 입력되지 않는다. 따라서 인증 과정에서 새로 얼굴 데이터를 입력한 후에도 동일한 크기를 유지하기 위해 특정 기준을 설정하고 기준에 따라 데이터의 크기를 일정하게 생성한다.

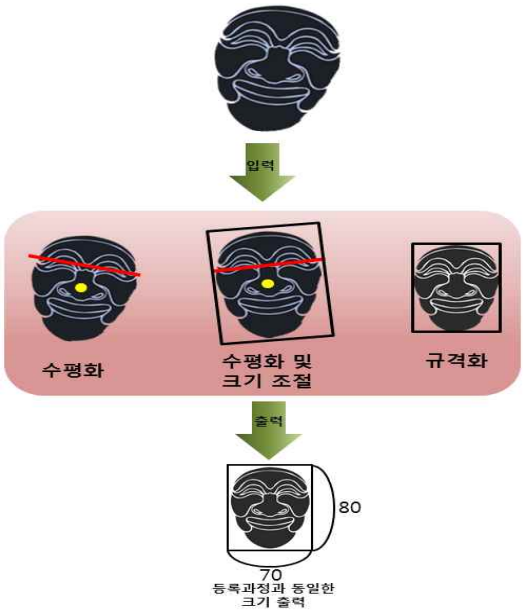

그림 3. 얼굴 규격 설정
Fig 3. Face standard setting process

4-2 이미지 분할

서버는 입력받은 얼굴 데이터의 크기 규격 설정과정을 진행하고, 인증 과정에서 사용하기 위한 이미지 분할 과정을 진행한다. 이미지 분할은 사용자의 얼굴을 중심으로 원형 테두리 내부에 격자를 적용하여 아무런 특징점이 없는 데이터를 최소화 시킨다. 또한 이미지의 분할 개수는 사용자가 선택 가능하며, 선택하지 않을 경우 시스템에서 일괄적으로 지정된 크기로 분할된다. 얼굴 데이터의 분할의 예는 다음 그림 4와 같다.

4-2-1 좌표 지정 및 특징점 도출

좌표지정 및 특징점 도출은 원형 테두리 내부에서 분할된 이미지에 좌표를 부여하는 과정으로 기준은 얼굴의 좌측 상위부분을 시작으로 분할된 이미지가 해당되는 행과 열에 따라 좌표가 부여된다.

또한 서버는 사용자가 선택 가능한 특징점과 임의로 생성한 거짓 특징점을 무작위로 출력하여 특징점 후보군을 형성하고 특징점 후보들 중에서 희망하는 특징점을 선택할 수 있도록 그림 5와 같이 출력을 하게 된다.

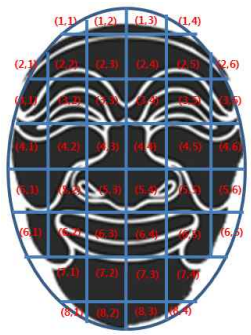

그림 4. 얼굴 분할
Fig 4. A split face

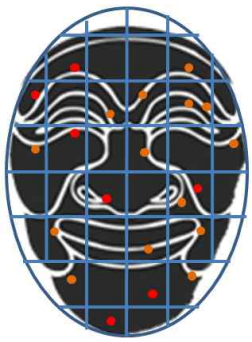

그림 5. 후보군 도출
Fig 5. Candidate search

4-3 용어 정의

- ID_i : 사용자 식별자
- PW_i : 사용자 패스워드
- DID_i : 사용자 디바이스 식별자
- SN_i : 사용자 디바이스 시리얼넘버
- b : 랜덤넌스 값
- UF_i : 사용자의 얼굴데이터
- $G(UF_i)$: 격자가 적용된 얼굴 데이터
- x : 서버의 비밀키
- P_n : 사용자가 희망하는 이미지 $(n = 1,2,3,....)$
- C_n : P_n에서 희망하는 특징점 $(n = 1,2,3,....)$
- G_n : 사용자 로그인 정보
- $h(\bullet)$, $||$: 해시연산, 연접연상
- $\oplus$: XOR 연산

4-4 등록 단계

사용자는 등록을 하기 위해 사용자 기본 정보와 얼굴 데이터를 안전한 채널을 통해 전송하면, 서버는 해당 데이터들을 통해 키 값을 생성하여 사용자에게 전송한다. 사용자는 네트워크 환경에서 발생할 수 있는 도청, 해킹 등과 같은 공격을 방지하기 위해 네트워크 자원을 이용하지 않고, 사용자 등록을 수행하는 부서에서 얼굴 데이터를 생성하고, 사용자 등록에 필요한 정보를 제출함으로써 안전한 채널을 만들 수 있다.

사용자의 디바이스에 전송받은 데이터의 일부를 저장하고 얼굴 인식을 통해 필요한 정보를 서버로 전

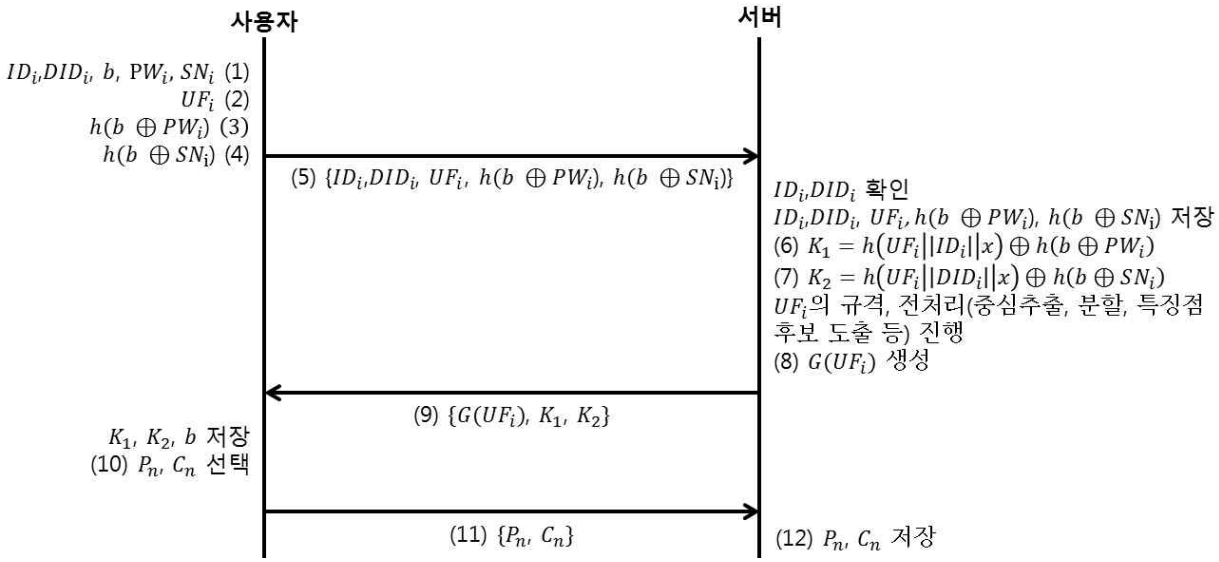

그림 6. 등록단계 프로토콜
Fig 6. Registration Protocol

송하면 등록 단계가 마무리 된다. 등록 단계의 자세한 과정은 그림 6과 같다.

[단계 1] 등록을 하기 위해 사용자 정보 및 디바이스 정보, 랜덤넌스 값을 생성한다.

$$ID_i,\ DID_i,\ b,\ PW_i,\ SN_i \tag{1}$$

[단계 2] 사용자는 자신의 얼굴 데이터와 패스워드 및 시리얼넘버를 랜덤넌스 값과 연산을 통하여 패스워드 및 시리얼넘버 검증자를 생성하여 사용자가 정보와 함께 안전한 채널을 통해 서버로 전송한다.

$$UF_i \tag{2}$$

$$h(b \oplus PW_i) \tag{3}$$

$$h(b \oplus SN_i) \tag{4}$$

$$ID_i,\ DID_i,\ UF_i, h(b \oplus PW_i), h(b \oplus SN_i) \tag{5}$$

[단계 3] 서버는 사용자 및 디바이스 정보를 확인하고 저장한다. 그 후 검증자를 이용하여 사용자와 디바이스의 키 값을 생성한다.

$$K_1 = h(UF_i \| ID_i \| x) \oplus h(b \oplus PW_i) \tag{6}$$

$$K_2 = h(UF_i \| DID_i \| x) \oplus h(b \oplus SN_i) \tag{7}$$

[단계 4] 서버는 전송받은 얼굴 데이터를 중심 설정 및 규격화 과정을 수행하고, 격자를 적용시켜 각 키 값과 함께 전송한다.

$$UF_i \Rightarrow G(UF_i) \tag{8}$$

$$G(UF_i), K_1, K_2 \tag{9}$$

[단계 5] 사용자는 전송받은 키 값과 랜덤넌스 값 b를 디바이스에 저장하고, 전송받은 얼굴 데이터에서 희망하는 이미지와 특징점을 선택하여 서버로 전송한다.

$$P_n,\ C_n \text{ 선택} \tag{10}$$

$$P_n, C_n \text{ 전송} \tag{11}$$

[단계 6] 서버는 전송받은 이미지와 특징점을 저장하고 등록과정을 마무리 한다.

$$P_n,\ C_n \text{ 저장} \tag{12}$$

4-5 로그인 및 인증 단계

사용자는 로그인을 위해 자신의 정보와 랜덤넌스 값 및 얼굴 데이터를 생성하고, 검증자를 생성하여 서버로 전송한다. 전송받은 서버는 식별자 확인 및 키 값을 생성하여 정당성을 확인하고, 얼굴 데이터를 비교한다. 또한 격자가 적용된 얼굴 데이터를 생성하여 사용자로부터 데이터를 전송받아 사용자의 정당성을 확인한다. 로그인 및 인증단계의 자세한 내용은 그림7과 같다.

[단계 1] 사용자는 서버에 접속하여 자신의 정보와 디바이스 정보 생성 및 얼굴 데이터를 생성한다.

$$ID_i,\ PW_i,\ DID_i,\ SN_i,\ b \tag{13}$$

$$UF_i' \tag{14}$$

[단계 2] 사용자는 각각의 검증자를 생성하고, 검증에 필요한 파라미터를 생성하여 서버로 전송한다. ([단계 2]에서 생성된 파라미터들은 XOR 연산과 해시연산을 통해 생성된 데이터이다.)

$$h(b \oplus PW_i),\ h(b \oplus SN_i) \tag{15}$$

$$Z_1' = k \oplus h(b \oplus PW_i) \tag{16}$$

$$Z_2' = k \oplus h(b \oplus SN_i) \tag{17}$$

$$Z_3 = h(k||h(b \oplus PW_i)||h(b \oplus PW_i) \quad (18)$$

$$Z_4 = h(k||h(b \oplus SN_i)||h(b \oplus SN_i) \quad (19)$$

$$ID_i, DID_i, Z_1, Z_2, Z_3, Z_4, UF_i' \quad (20)$$

[단계 3] 서버는 전송받은 식별자를 확인하기 위해서 키 값을 생성하여, 전송받은 식별자를 확인한다. [단계 3]은 전송받은 식별자를 확인하기 위한 단계로 기존에 서버에 저장되어 있던 데이터를 이용하여 데이터를 생성한 다음, 전송받은 식별자와 일치여부를 확인하는 과정이다.

$$K_1 = h(UF_i||ID_i||x) \oplus h(b \oplus PW_i) \quad (21)$$

$$K_2 = h(UF_i||DID_i||x) \oplus h(b \oplus SN_i) \quad (22)$$

$$h(b \oplus PW_i) = K_1 \oplus Z_1 \quad (23)$$

$$h(b \oplus SN_i) = K_2 \oplus Z_2 \quad (24)$$

$$Z_1? = Z_1' \quad (25)$$

$$Z_2? = Z_2' \quad (26)$$

[단계 4] 서버는 저장되어 있는 얼굴 데이터와 전송받은 얼굴 데이터를 비교하여, 추가 검증자와 격자가 적용된 얼굴 데이터를 사용자에게 전송한다. [단계 4]에서 검증 결과가 일치하지 않을 경우 세션을 종료한다.

$$UF_i? = UF_i' \quad (27)$$

$$G(UF_i) \quad (28)$$

$$Z_5 = h(ID_i||h(b \oplus PW_i) \quad (29)$$

$$Z_6 = h(DID_i||h(b \oplus SN_i) \quad (30)$$

$$ID_i, G(UF_i), Z_5, Z_6 \quad (31)$$

[단계 5] 사용자는 파라미터를 이용하여 전송받은 추가 검증자를 생성하여 값을 비교한다.

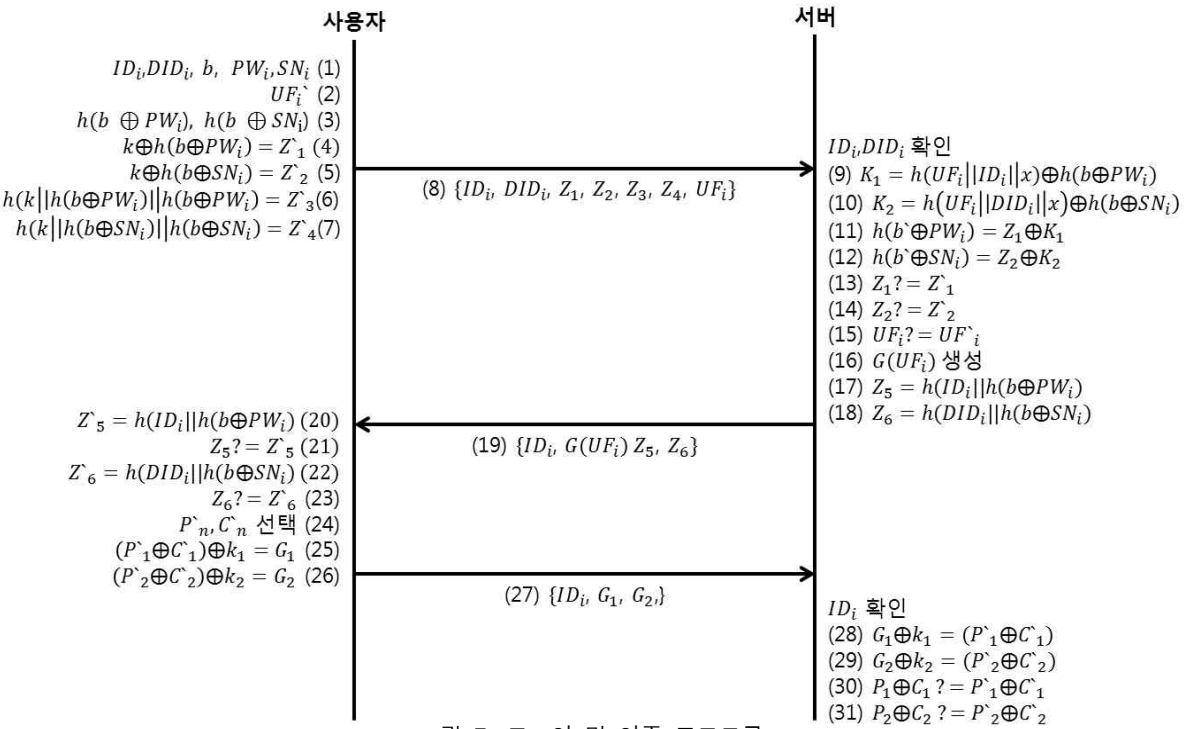

그림 7. 로그인 및 인증 프로토콜
Fig 7. Login and Authentication Protocol

$$Z_5' = h(ID_i \| h(b \oplus PW_i)) \quad (32)$$

$$Z_5 ? = Z_5' \quad (33)$$

$$Z_6' = h(DID_i \| h(b \oplus SN_i)) \quad (34)$$

$$Z_6 ? = Z_6' \quad (35)$$

[단계 6] 격자가 적용된 얼굴 데이터에서 희망하는 이미지와 특징점을 선택하여 키 값을 이용하여 로그인 정보를 생성하여 서버로 전송한다.

$$P_n', C_n' \text{ 선택} \quad (36)$$

$$(P_1' \oplus C_1') \oplus k_1 = G_1 \quad (37)$$

$$(P_2' \oplus C_2') \oplus k_2 = G_2 \quad (38)$$

$$ID_i, G_1, G_2 \text{ 전송} \quad (39)$$

[단계 7] 서버는 전송받은 로그인 정보와 키 값을 이용하여 로그인 정보의 정당성을 확인하고 서비스 제공 여부를 결정한다. 확인 결과 및 오차 범위에 따라 세션을 종료한다.

$$G_1 \oplus K_1 = (P_1' \oplus C_1') \quad (40)$$

$$G_2 \oplus K_2 = (P_2' \oplus C_2') \quad (41)$$

$$P_1 \oplus C_1 ? = P_1' \oplus C_1' \quad (42)$$

$$P_2 \oplus C_2 ? = P_2' \oplus C_2' \quad (43)$$

Ⅴ. 안전성 및 효율성 분석

5-1 안전성 분석

제안 방식을 앞서 분석한 문제점에 맞추어 분석하면 다음과 같이 정리하여 표 2.와 같이 나타낼 수 있다. 본 논문에서 제안한 사용자 인증 기법은 안전한 채널에서 등록과정을 수행하게 된다. 안전한 채널은 기업 내 사용자 등록을 수행하는 부서에서 직접 사용자의 얼굴 데이터를 생성하고, 사용자 정보를 직접 제출하기 때문에 안전한 채널이 구성된다.

o 무결성 : 사용자 등록 과정은 앞서 Lee 등이 제안한 인증 기법과 달리 안전한 채널에서 진행되며 인증에 필요한 파라미터들은 스마트카드에 저장된다.

로그인 및 인증 단계에서는 사용자의 개인 식별자인 ID_i, DID_i를 사용하며, 사용자가 임의로 선택한 랜덤넌스 값 b를 기반으로 PW_i와 개인이 직접 소지하고 있는 디바이스의 시리얼 넘버 SN_i을 XOR 연산 및 해시 연산하여 패스워드와 디바이스 검증자 $h(b \oplus PW_i), h(b \oplus SN_i)$를 인증을 위한 파라미터로 사용하기 때문에 무결성을 보장할 수 있으며, 추가적으로 사용자의 얼굴 데이터 UF_i와 사용자가 선택한 이미지 P_n과 특징점 C_n을 사용자 인증 과정에서 이용하기 때문에 데이터의 무결성을 보장할 수 있다.

o 기밀성 : 사용자 인증에 필요한 모든 정보는 등록 단계에서 안전한 채널에서 진행되며, 이후 로그인 및 인증 과정에서는 필요한 정보를 다른 파라미터들과 연산을 통해 새로운 값으로 도출한 다음, 해당 값을 전송하기 때문에 기밀성을 보장할 수 있다. 뿐만 아니라 사용자가 선택한 랜덤넌스 값 b와 사용자가 선택한 이미지 P와 특징점 C를 로그인에 필요한 파라미터로 이용하기 때문에 사용자 인증에 사용되는 정보들에 대한 기밀성을 보장할 수 있다.

o 상호인증 : 사용자와 서버는 해당 개체의 정당성을 파악하기 위해 상호간에 인증을 위한 파라미터를 송·수신 하게 된다. 제안 인증기법은 K_1, K_2와 PW_i, SN_i를 기반으로 생성한 검증자를 연산하여 Z_1, Z_2, Z_3, Z_4를 생성하고 서버로 전송한다. 서버는 저장된 데이터와 생성된 값을 이용하여 파라미터를 생성하고, 생성한 파라미터와 전송받은 데이터들을

연산하여 인증에 필요한 파라미터를 도출하여 비교한다. 이를 통해 상호간에 전송된 데이터를 확인하고, 같은 사용자, 서버에서 전송된 데이터의 확인이 가능하다.

o 위장공격 : 등록 단계에서는 사용자가 안전한 채널을 기반으로 사용자 등록을 실시하기 때문에 위장공격으로부터 안전하게 파라미터 및 데이터를 보호할 수 있다. 또한 로그인 및 인증 단계에서는 사용자가 임의로 선택하는 랜덤넌스 값 b, 사용자의 얼굴 데이터 UF_i, 희망하는 얼굴 이미지 P, 특징점 C는 등록 단계에서 사용자가 직접 등록한 데이터로써 추측하거나 임의로 선택하여 로그인 정보를 생성하는 것이 불가능하다. 또한 검증자와 다양한 파라미터를 이용하여 생성한 데이터들을 상호 인증에 이용하기 때문에 위장공격으로부터 안전하다.

o 도청 : 제안한 인증 프로토콜의 등록 단계는 안전한 채널에서 진행되며, 악의적인 공격자가 사용자의 정보를 도청 및 감청하는 것은 불가능하다. 로그인 및 인증단계에서는 사용자와 서버사이에서 전송되는 데이터를 연산을 통해 해당 값이 공개되지 않기 때문에 도청으로부터 안전하다.

표 2. 안전성 분석
Table 2. Security analysis

	Hwang et al	Khan et al	Lee et al	제안 기법
무결성	O	O	X	O
기밀성	O	O	X	O
상호 인증	X	O	X	O
위장 공격	O	O	X	O
도청	X	X	X	O

5-2. 효율성 분석

본 논문에서 제안한 인증 프로토콜은 로그인 단계에서만 4번의 해시 연산을 진행하며, 2번의 XOR 연산과정이 필요하다. 인증 과정에서는 사용자 측에서 4번의 XOR 연산이 필요하고, 서버 측에서 4번의 해시 연산과 6번의 XOR 연산이 필요하다. XOR 연산의 경우 지수 연산에 비해 속도가 빠르다는 장점이 있지만, XOR 연산의 특성으로 발생 가능한 사용자/서버 위장 공격 등에 취약할 수 있다. 이러한 문제점을 해결하기 위해 본 논문에서는 XOR 연산뿐만 아니라 해시 연산을 함께 진행 하였으며, 사용자가 임의로 선택한 랜덤넌스 값 b와 얼굴 이미지의 분할된 일부분인 P, 특징점 C를 사용함으로써 이러한 취약점들을 해결하였다. 효율성 분석에 대한 내용을 정리하면 표 3과 같이 나타낼 수 있다.

표 3. 효율성 분석
Table 3. Efficiency Analysis

구분		Hwang et al	Khan et al	Lee et al	제안 기법
로그인 단계	사용자	4S, 2M, 1X	3H, 2X	-	4H, 2X
	서버	-	-	-	-
인증 단계	사용자	-	-	-	4X
	서버	1S, 2M, 1X	6H, 6X	-	4H, 6X

M: 지수연산, H: 해시연산, S:대칭키 암·복호화, X: XOR연산

Hwang 등이 제안한 인증 기법에서는 총 5번의 대칭키 암·복호화 과정과 4번의 지수 연산, 1번의 XOR 연산을 수행하였으며, Khan 등이 제안한 인증 기법에서는 총 9번의 해시연산과 8번의 XOR 연산을 수행하였다. 본 논문에서 제안한 인증 기법은 총 8번의 해시연산과 12번의 XOR 연산을 수행하게 된다. 각각의 암호화 연산 과정에 대한 속도를 비교하여 표로 정리하면 다음 표 4와 같이 정리할 수 있다.

다양한 암호화 방법들 중 널리 알려진 RSA 1024(지수연산)와 AES/CTR 256(대칭키), SHA-512(해시) 방식을 선정하여 1회 연산 속도 비교를 진행하였다.

암호화 속도비교는 Microsoft Visual C++ 2005 SP1버전으로 구현된 내용을 바탕으로 수행되었으며, 32비트의 Windows Vista 인텔 코어2 1.83GHz의 CPU에서 실행된 결과이다.

표 4. 암호화 방식 속도 비교
Table 4. Encryption speed comparison

	Cycle / Byte	Microseconds to Setup Key and IV	Cycles to Setup Key and IV
AES/CTR (256)	18.2	0.756	13.83
SHA-512	17.7	-	-
	Milliseconds/Operation	Megacycles/Operation	
RSA 1024	0.08(Enc)+1.46(Dec)	0.14(Enc)+2.68(Dec)	

아래 표 5를 통하여 기존의 사용자 인증기법과 제안된 기법의 연산속도 비교를 수행한 결과 안전성을 확보하였으면서 연산속도 또한 크게 차이나지 않는 것으로 확인할 수 있다.

(XOR연산의 경우 1.83GHz의 연산량을 반올림 연산을 통해 약 2.00GHz로 연산을 수행하였다.)

표 5. 연산 속도 비교
Table 5. Operation speed comparison (단위 : us)

구분		Hwang et al	Khan et al	Lee et al	제안 기법
로그인 단계	사용자	75.880000003	53.100000006	-	70.800000006
인증 단계	사용자	-	-	-	0.000000012
	서버	21.280000003	106.200000018	-	70.800000018

VI. 결 론

스마트워크 환경은 다양한 디바이스와 통신 인프라를 기반으로 업무의 편리성 및 유연성을 제공하는 미래지향적인 IT서비스의 대표적인 기술이다.

업무시설 구축을 위한 비용 절감과 생산성 향상, 편리성 증대와 같은 효과로 인해 많은 기업에서 스마트워크 환경을 도입하고 있는 추세이다. 하지만 단말기의 분실이나 사용자들의 다양한 접속환경을 통한 악성코드의 감염 가능성이 있고, 감염된 악성코드로 인한 악의적인 행위로 인해 개인정보 유출사고와 같은 보안사고가 발생할 수 있다. 따라서 기업 외부 환경에서 내부 자원에 접근하는 스마트워크 환경의 사용자들에 대한 정당한 사용자 인증 과정이 필수적으로 요구된다. 본 논문에서는 기업 외부에서 네트워크를 기반으로 내부 자원으로 접근하는 수많은 스마트워크 사용자들에 대한 사용자 인증을 위해서 사용자들의 얼굴 데이터를 이용한 인증기법에 대해서 제안하였다. 본 제안 기법은 수많은 스마트워크 사용자들의 고유 얼굴 데이터와 사용자가 선택한 이미지 및 특징점을 사용하기 때문에 정확한 사용자 인증 과정을 수행하지 않은 사용자들은 사전에 차단이 가능하다. 또한 중요 정보 노출에 대해서 악의적인 내부 사용자들의 추적이 가능할 것으로 예상되며, 스마트워크 환경에서 사용 가능한 사용자 인증기법 연구에 도움이 될 것으로 예상 된다. 또한 사용자 인증 분야에서 보안성 향상에 도움이 될 것으로 기대된다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0007755)

Reference

[1] S.K. Park, J.H. Lee, “Smarwork Technology and Standardization”, *Telecommunications Technology Assocition Journal,* Vol. 136, pp.79-84

[2] M.S Jeong, D.B Lee, J. Kwak, “Analysis of Smartwork Security Threats and Security Requirements”, *Korea Institute of Information Security & Cryptology, Journal of Information Security*, Vol. 21 No. 5, pp55-63, 2011.

[3] K.H, Lee, “Facial Recognition Technology Trends"

[4] L. Lamport, "Password Authentication with Insecure Communication", *Communications of ACM 24,* Vol. 24. No.11. pp. 770-772, Nov. 1981.

[5] M.S. Hwang, L.H. Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE*

Transactions on Consumer Electronics Vol. 46. No. 1 pp. 28-.30. Feb. 2000.

[6] M.K. Khan, S.K. Kim, "Cryptanalysis and Security Enhancement of a 'more Efficient & Secure Dynamic ID-based Remote User Authentication Scheme', *Computer Communications,* Vol. 34, pp. 305-309, 2011.

[7] M. Scott, "Cryptanalysis of an ID-based Password Authentication Scheme Using Smart Cards and Fingerprints", *ACM SIGOPS Operating Systems Review,* 2004.

[8] I. E. Liao, C. C. Lee, M. S, Hwang, "A Password Authentication Scheme Over Insecure Networks", *Journal of Computer and System Sciences,* Vol. 72, pp. 727-740, 2006.

[9] S. Lee, I. Ong, H. T. Lim, H. J. Lee, "Two Factor Authentication for Cloud Computing", *International journal of KIMICS,* Vol. 8, No. 4, pp. 427-432, Aug. 2010

변 연 상 (Yun-Sang Byun)

2012년 2월 : 순천향대학교 정보보호학과(공학사)
2013년 3월~현재 : 순처향대학교 정보보호학과 석사과정
관심분야 : 스마트워크 보안, 클라우드 컴퓨팅 보안, 암호 프로토콜 등

곽 진 (Jin Kwak)

2000년 8월 성균관대학교 공학학사
2003년 2월 성균관대학교 공학석사
2006년 2월 성균관대학교 공학박사
2006년 4월 - 2006년 11월 : 일본 큐슈대학교 방문연구원
2006년 8 월 - 2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월 - 2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 3월 - 현재 : 순천향대학교 정보보호학과 교수
2009년 1월 - 2009년 12월 : 순천향대학교 공과대학 교학부장
2009년 1월 - 2010년 12월 : 순천향대학교 정보보호학과 학과장
2010년 1월 - 2012년 12월 : 순천향대학교 SCH BIT 창업보육센터장
2011년 2월 - 2012년 12월 : 순천향대학교 중소기업 산학협력센터 센터장
2007년 1 월 - 2009년 12월 : 정보통신산업진흥원 주간기술동향 집필위원
2008년 1월 - 2010년 12월 : 한국정보보호학회 논문지편집위원
2008년 1월 - 현재 : 한국정보보호학회 이사
2008년 4월 - 현재 : 한국인터넷정보학회 논문지편집위원
2008년 12월 - 현재 : 정보통신산업진흥원 기술평가위원
2009년 5월 - 현재 : TTA 표준화로드맵 기술표준기획전담반 위원
2010년 3월 - 현재 : 조달청 기술평가위원
2010년 5월 - 2010 년 7 월 : 교육과학기술부 국가기술수준 평가 위원
2011년 1월 - 현재 : 한국정보기술융합학회 이사
2011년 1월 - 현재 : 한국정보처리학회 이사
2011년 1월 - 현재 : JIPS 논문지 편집위원
2011년 7월 - 현재 : 지식경제부 지식경제기술혁신 평가단 위원
2013년 3 월 - 현재 : 금융보안연구원 보안기술 자문위원
관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 등