논문 2012-49CI-3-7

스마트 카드를 이용한 패스워드 기반의 검색 가능한 암호화 기술

(A Password-Based Searchable Encryption using Smart Cards)

이 동 근*, 이 현 숙*, 임 종 인**

(Dongkun Lee, Hyun Sook Rhee, and Jong In Lim)

요 약

사용자 인증은 인터넷 상의 많은 리소스를 인가된 사용자만 사용하도록 안전한 시스템 구축의 필수 요소이며 암호화 기법은 데이터 프라이버시를 제공하는 것을 목적으로 한다. 또한, 검색 가능한 암호화 기법은 데이터의 프라이버시와 함께 키워드를 이용한 검색으로 데이터의 효율적인 관리를 목적으로 한다. 공개키 기반의 검색 가능한 암호화 시스템은 사용자의 공개키에 대한 인증이 미리 이루어져야 하고 사용자 별 공개키/개인키에 대한 안전한 관리가 요구된다. 클라우드 환경에서는 다양한 디바이스를 통해 인터넷 클라우드 환경의 다양한 리소스를 사용가능하도록 하는 것이 목적이며 이에 반해서 다양한 디바이스들은 실제로 공개키/개인키에 대한 관리 및 인증서를 관리하기에는 리소스가 부족할 수 있으며 디바이스마다 이러한 클라이언트를 구현한다는 것은 쉽지 않다. 이러한 문제점들을 해결하기 위해서 H/W적인 안전성을 보장하는 temper-resistant한 device인 스마트 카드(smart card)를 이용한 암호화된 데이터에서의 패스워드 기반의 인증된 사용자의 검색 기술을 제안한다.

Abstract

User authentication is a necessity to set up secure system which only an authorized user can use various resource on the Internet. Encryption is to provide data privacy. Also, searchable encryption is to provide both data privacy and efficient management of data by searching with a keyword. The public key based searchable encryption requires in advance the authentication of user's public key as well as the secure management of a publlic/private key of a user, respectively. In cloud, it is purpose to use cloud various resources by using various devices, meanwhile, it is not sufficient resource that some devices manage public/private keys and certificates and it is not easy to implement these clients. To solve this problem, we propose a password-based saerchable encryption using smart cards which are temper-resistant devices.

Keywords : Searchable Encryption, Smart Cards, Password-Based User Authentication

Ⅰ. 서 론

클라우드 서비스는 크게 web-based service, software-as-a-service (SaaS), 그리고 클라우스 스토리지 서비스(cloud storage service)로 나눌 수 있다. 이 중 클라우드 스토리지 서비스는 각 개인들이자신의 정보를 클라우드 스토리지에 저장하고 언제 어디서나 이용할 수 있다는 측면에서 매력적이다. 클라우드 스토리지 서비스의 예로는 Amazon Simple Storage Service (S3), Verizon Online, Backup and Restore service, Live Mesh, Box.net, and a DlopBox가 있다.

네트워크 망에 접속 가능한 다양한 전자 장치들은 많은 정보를 전송 및 저장하고 있으며 안전성을 제공하기 위해서 암호화 기법 및, SSL 또는 IPSec과 같은 기존의 많은 보안 전송기술을 적용하고 있다. 이러한

* 정회원, 삼성전자 무선사업부
(Samsung Electronics),
** 정회원-교신저자, 고려대학교 정보보호대학원
(Korea University)

접수일자: 2012년2월20일, 수정완료일: 2012년5월2일

네트워크 망은 클라우드 환경으로 확장되었을 때 새롭게 고민되는 보안이슈 및 사용자 프라이버시에 대해서 고려되어야 한다. 따라서, 이러한 클라우드 스토리지 서비스의 주요 보안 이슈는 데이터 프라이버시이며 데이터에 대한 권한을 갖은 정당한 사용자만이 민감한 데이터에 접근하도록 하는 사용자 인증과 암호화 기법의 적용이 요구된다. 즉, 데이터를 저장한 사용자 혹은 저장한 사용자가 권한을 위임한 정당한 사용자만이 데이터에 접근할 수 있도록 해야 한다. 이러한 다양한 클라우드 스토리지 서비스를 고려한 클라우드 환경에서는 개개인의 정보들이 안전하지 않은 채널을 통해서도 전송되고 있으며 다양한 채널에서도 데이터에 대한 프라이버시를 제공하기 위한 기술인 데이터 암호화는 클라우드 환경 및 클라우드 스토리지(Cloud Storage)에서 전송 및 저장되어지는 데이터들에게 고려되어야 될 기반기술이다. 또한 클라우드 서비스를 제공하는 디바이스의 종류가 다양화 되면서 서비스의 종류도 더욱 다양해 질 것이다.

종래 암호화 기술은 데이터 프라이버시는 제공하지만 데이터를 효율적으로 관리하지 못하며 원하는 데이터를 검색하는 데 있어서 사용자 편리성을 제공하지 못한다. 이러한 문제점을 해결하기 위해서 2000년 Song et al.[S00]에 의해서 제안된 검색 가능한 암호 기법을 시작으로 암호화된 데이터에서의 equality, range, subset 그리고 inner product와 같은 다양한 쿼리(query)가 가능한 검색가능한 암호화 기법에 대한 연구는 최근 연구의 주요 이슈이다.

검색 가능한 암호화 기법은 암호화된 데이터에 검색어 암호문(Searchable Ciphertext)를 첨부하여 저장소에 저장한 후 사용자가 선택한 검색어 쿼리(ex, Trapdoor 혹은 Capability)를 생성해서 테스트 서버에게 주면 테스트 서버는 검색어 암호문 (Searchable Ciphertext)와 검색어 쿼리(ex, Trapdoor 혹은 Capability)를 테스트 함수에 입력해서 테스트 결과(예를 들면, quality, range, subset 그리고 inner product의 결과)를 얻는 형태로 제안되어 진다.

이러한 기술들은 기존에 잘 알려진 안전한 문제(Hardness Assumption)들에 기반을 두고 기술에 대한 안전성을 증명해 왔다. 하지만 이러한 기술들을 현실적인 기술로 접목시키는데 있어서 기술의 한계점은 효율성 측면 뿐 아니라 어떻게 안전하게 secret key (symmetric encryption key) 혹은 private key (asymmetric decryption key)를 관리하고 이용하여 구현하는가의 문제를 여전히 갖는다.

예를 든다면 공개키를 이용한 검색 가능한 암호화 시스템 Boneh et al. 에 의해서 제안된 Public-key encryption with keyword search [BCOP04]가 있다. 이러한 시스템을 구축하기 위해서는 사용자의 공개키에 대한 인증이 미리 이루어져야 하고 사용자 별 공개키/개인키에 대한 안전한 관리가 이루어져야 한다. 이에 반해서 다양한 디바이스들은 실제로 공개키/개인키에 대한 관리 및 인증서를 관리하기에는 리소스가 부족할 수 있으며 디바이스마다 이러한 클라이언트를 구현한다는 것은 쉽지 않다.

이러한 문제점들을 해결하기 위해서 H/W적인 안전성을 보장하는 temper-resistant한 device인 스마트 카드(smart card)를 이용한 암호화된 데이터에서의 패스워드 기반의 인증된 사용자의 검색 기술을 제안한다. 즉, ID/PW를 이용한 인증과 동시에 검색어를 이용한 암호화된 데이터에서의 안전한 검색이 가능하도록 하는 것이 목적이다.

1. 관련 연구

가. 패스워드 기반의 사용자 인증 기술

인터넷 상의 많은 시스템들은 인가된 사용자만이 어떠한 리소스를 이용할 수 있도록 하기 위해서는 정당한 사용자인지를 확인하게 되고 이를 위해서 가장 널리 이용되는 기술은 아이디와 패스워드를 이용한 사용자 인증이다. 이러한 패스워드 기반 사용자 인증 기법에 대한 연구는 안전한 패스워드를 어떻게 설정하며 사용자가 인증을 위해서 입력한 정보들을 이용하여 가공된 인증정보들로부터 패스워드 정보가 들어나지 않도록 설계하는 것이 중요하다. 안전한 패스워드는 제3자가 쉽게 추측할 수 없으며, 시스템에 저장되어 있는 사용자 정보나 인터넷을 통해 전송되는 정보를 해킹하여 사용자의 패스워드를 알아내기 어렵도록 설계되어야 한다. 이러한 패스워드 기반의 사용자 인증 기법의 안전성은 (1) 오프라인 사전공격에 안전하도록 인증서버 관리자에 의해서 패스워드 정책이 수립되어야 하며 (2) 프로토콜 메시지를 병행적으로 악용하는 공격(Parallel session attack)이나 재사용 공격(Replay attack)에 안전하도록 설계되어야 한다. 하지만 스마트 카드를 이용한 패스워드 기반의 인증된 사용자 검색 기술은 인증된 사

용자를 제외한 제 3자로부터의 암호문의 기밀성을 목표로 한다. 본 논문에서 제안한 스마트 카드를 이용한 패스워드기반의 검색 가능한 암호화 기법은 암호문이 평문에 대한 기밀성을 제공하기 때문에 사용자가 인증 및 검색 정보를 재사용하여 암호문을 얻을지라도 암호문으로부터 평문에 대한 정보를 획득할 수 없다.

나. 암호화된 데이터에서의 검색 기술

검색 가능한 암호화 기법은 암호화된 데이터에 검색어 암호문(Searchable Ciphertext)를 첨부하여 저장소에 저장한 후 사용자가 선택한 검색어 쿼리(ex, Trapdoor 혹은 Capability)를 생성해서 테스트 서버(MFP가 직접 수행할 수도 있다.)에게 주면 테스트 서버는 검색어 암호문 (Searchable Ciphertext)와 검색어 쿼리(ex, Trapdoor 혹은 Capability)를 테스트 함수에 입력해서 테스트 결과(예를 들면, quality, range, subset 그리고 inner product의 결과)를 얻는 형태로 제안되어 진다.

이러한 기술들은 기존에 잘 알려진 어려운 문제(Hardness Assumption)에 기반을 둔(즉, 제안된 기술을 공격하면 잘 알려진 어려운 문제를 풀수 있다는 것을 보임) 안전성을 증명해 왔다. 하지만 이러한 기술들을 현실적인 기술로 접목시키는데 있어서 기술의 한계점은 효율성 측면뿐 아니라 어떻게 안전하게 secret key (symmetric encryption key) 혹은 private key (asymmetric decryption key)를 관리하는가의 문제를 여전히 갖는다.

즉, 암호화된 데이터에서의 검색 기술은 사용자 별 공개키/개인키를 가정하고 이러한 공개키/개인키 쌍이 안전하게 사용자에게 제공되며 공개키 인증서 및 개인키의 안전한 저장 및 관리에 대한 가정 및 구현이 요구된다.

2. 논문의 공헌도

본 논문에서는 temper-resistant한 device인 스마트 카드(smart card)를 이용한 암호화된 데이터에서의 패스워드 기반의 인증된 사용자의 검색 기술을 제안한다. 즉, ID/PW를 이용한 인증과 동시에 검색어를 이용한 암호화된 데이터에서의 안전한 검색이 가능하도록 하는 것이 목적이다.

이 경우, 클라우드 환경에 노출되어져 있는 다양한 device에서 가공, 생성, 저장되는 다양한 데이터들에 대한 데이터 프라이버시와 이들 데이터에 대한 편리한 접근을 가능하게 한다. 또한, 아래와 같은 추가적인 보안적인 장점을 갖는다.

(1) 사용자의 (ID, PW) 테이블을 따로 관리하지 않기 때문에 Server Compromise 공격에 대해서 안전하다.
(2) 사용자의 공개키/개인키에 대한 안전성 및 공개키 인증서 관리에 대한 요구가 없다.
(3) 서버의 공개키도 스마트 카드에 저장하여 발급하기 때문에 서버의 공개키에 대한 인증서가 요구되지 않는다.

Ⅱ. 스마트 카드를 이용한 패스워드 기반의 인증된 사용자의 검색 가능한 암호화 기술

스마트 카드를 이용한 암호화된 데이터에서의 패스워드 기반의 인증된 사용자의 검색 프로토콜은 사용자가 스마트 카드를 꽂을 수 있는 스마트 카드 리더기를 보유하거나 USIM과 같은 형태로 내장하고 있는 Tablet PC나 모바일 폰에서 구현 가능하다. 사용자는 자신의 ID/PW와 서버로부터 발급받은 스마트 카드(서버의 공캐키와 사용자의 ID/PW를 입력되면 정당한 인증정보들을 계산하여 테스트 서버에 저장하는 스마트 카드)를 이용하여 사용자 인증과 함께 검색어를 생성하고 검색된 암호문을 복호화 할 수 있게 된다.

프로토콜의 구성은 (1) 사용자 등록 단계 (2) 암호화된 검색어 생성단계 (3) 로그인 및 인증검색정보 생성단계 (4) 인증 및 트랩도어를 이용한 검색 단계 (5) 암호문 복호화 단계이다.

1. A Password-Based Searchable Encryption using Smart Cards (PBSE-SC)

가. 사용자 등록 단계

서버는 p=2q+1 을 만족하는 큰 소수 p, q를 선택하여 서버 자신의 비밀키 $x \in (Z_q^*)$와 일방향 해쉬함수 $h : \{0,1\}^* \rightarrow Z_q^*$ 를 선택한 후 다음 과정을 수행한다.

(1) 사용자는 자신의 ID와 PW를 선택한 후 안전하게 서버에게 전송한다.
(2) 서버는 자신의 비밀키 x를 이용하여 다음의 값들

을 계산하여 (ID, A, h(), p, q, Y)를 저장한 스마트 카드를 사용자에게 발급한다.

$$A = h_1(ID)^x + h_1(PW) \bmod p$$

여기서, Y=g^{t}는 서버의 공개키이고 t (in Z_q^*) 는 서버의 비밀키이고, 서버는 사용자의 (ID, PW) 테이블을 따로 관리하지 않는다.

나. 암호화된 검색어 생성단계

제공자는 자신의 스마트카드를 카드리더기에 꽂고 (Insert), 아이디 ID' 와 패스워드 PW' 그리고 선택한 검색어 KW를 입력한다. 스마트카드는 검색 암호문 (Searchable Ciphertex) CT_{KW}를 생성하여 검색 서버에 전송한다.

$$CT_{KW} = [C_1, C_2] = [h_2(e(h_1(KW)^r, Y)), g^r]$$
$$C = [C_3, C_4] = Enc (h_2(e((h_1(ID')^x)r', h_1(ID))), m), h_1(ID')^{r'}$$

여기서, 정당한 제공자는 ID', PW'을 자신의 스마트 카드에 입력하게 되고 정당한 ID', PW'값을 입력받은 스마트카드는 $h(ID')^x$ 값을 이용하여 키 값 $h_2(e((h_1(ID')^x r', h_1(ID)))$ 를 계산할 수 있다.

다. 로그인 및 인증검색정보 생성 단계

사용자는 자신의 스마트카드를 카드리더기에 꽂고 (Insert), 아이디 ID 와 패스워드 PW 그리고 선택한 검색어 KW' 를 입력한다.

(1) 스마트카드는 내장된 테스트 서버의 공개키 Y와 랜덤값 w를 선택하고 현재시각 T에 대해서 다음을 계산한다.

$$A' = (A - h_1(PW))^w * h_1(KW)$$
$$B = h_1(ID)^w$$
$$B' = Enc(Y, B, A')$$

여기서 Enc(., .)은 공개키 암호화 알고리즘이다.

(2) 스마트 카드는 인증검색정보 (I1, I2, I3)= (ID, T, B') 를 검색 서버에게 전송한다.

라. 인증 및 트랩도어를 이용한 검색 단계

인증검색정보 (I1, I2, I3)=(ID, T, B')를 전송받은 서버는 저장된 검색암호문 $CT_{KW} = [C_1, C_2]$를 이용하여 다음을 확인하여 (2)번식의 등호를 만족하는 검색암호문에 대응하는 암호문을 사용자에게 전송한다.

(1) $(B, A') = Dec(t, B')$

(2) $D = (A'/B^x)^t = h_1(KW)^t$

(3) Check if $h_2(e(D, C_2)) = ? C_1$

여기서 Dec(., .)은 공개키 복호화 알고리즘이다.

마. 복호화 단계

암호문을 전송받은 사용자는 $C_4 = h_1(ID')^{r'}$를 스마트카드에 입력하면 스마트 카드는 $h_1(ID)^x$를 이용하여 복호화 키 $h_2(e(h_1(ID')^{r'}, h_1(ID)^x))$ = $h_2(e((C_4, h_1(ID)^x))$ 계산하여 사용자에게 준다. 사용자는 C_3와 스마트카드로부터 얻은 복호화키를 이용하여 메시지 $Dec(h_2(e(C_4, h_1(ID)^x)), C_3) = m$ 을 얻는다.

2. 정확성(Correctness)

위에서 제안한 기법은 정확성을 가짐을 쉽게 보일 수 있다.

가. 검색 단계

저장된 암호문 CT_{KW} =$[C_1, C_2]$ = $[h_2(e(h_1(KW)^r, Y)), g^r]$ 와 인증검색정보 (I1, I2, I3)=(ID, T, B') 그리고 자신의 비밀키 t를 이용하여 $Dec(t, B') = (B, A')$ 를 얻는 서버는 $D = (A'/B^x)^t$ = $h_1(KW)^t$ 를 얻은 후 $h_2(e(D, C_2)) = ? C_1$ 인지를 체크하면 아래와 같은 과정을 통해서 확인 할 수 있다.

$$\begin{aligned} h_2(e(D, C_2)) &= h_2(h_1(KW)^t, g^r) \\ &= h_2(e(h_1(KW)^r,\ g^t)) \\ &= h_2(e(h_1(KW)^r, Y)) \\ &= C_1 \end{aligned}$$

나. 복호화 단계

데이터의 암호문 C = $[C_3, C_4]$ = $Enc(h_2(e((h_{1(ID')}^x)r',$

$h_1(ID))),m),h_1(ID')^{r'}$ 를 전송받은 사용자는 스마트 카드로부터 전송받은 $h_2(e(h_1(ID')^{r'},h_1(ID)^x)$를 이용하여 메시지를 얻는것을 확인할 수 있다.

$$h_2(e((C_4,h_1(ID)^x)) = h_2(e(h_1(ID')^{r'},h_1(ID)^x))$$
$$= h_2(e((h_1(ID')^x)r',h_1(ID)))$$

Ⅲ. 안전성 분석 (Security)

본 절에서는 제안된 프로토콜 PBSE_SC이 스마트 카드의 temper-resistant한 성질에 기반하여 알려진 공격들에 대해서 안전함을 분석한다.

가. 서버 가장 공격

공격자가 서버만의 비밀값 x 와 t값에 대한 정보없이 인증검색정보 $(A,B,B) = (ID,T,B')$ 로부터 $h(ID)^{xw}$를 계산할 수 없고, $h_1(KW)^t$ 를 유추하거나 계산할 수 없다. 즉, 서버가 아니고는 저장된 암호문 $CT_{KW} = [C_1,C_2] = [h_2(e(h_1(KW)^r, Y)), g^r]$으 로 부터 검색어 KW에 대한 정보를 유추할 수 없다. 즉, 서버 가장 공격에 대해서 안전하다.

나. 암호문의 안전성

본 논문에서 제안된 프로토콜에서 저장된 검색 암호문 $CT_{KW} = [C_1,C_2] = [h_2(e(h_1(KW)^r, Y)), g^r]$으로부터 검색어에 대한 정보를 노출하지 않는다는 것은 BCOP04논문에서 검색 암호문으로부터 검색어의 정보가 노출되지 않는다는 것을 보이는 것과 동일하게 증명된다. 즉, 암호문에 대한 기밀성(confidentiality)을 보장한다.

Ⅳ. 결 론

본 논문에서는 temper-resistant한 device인 스마트 카드(smart card)를 이용한 암호화된 데이터에서의 패스워드 기반의 인증된 사용자의 검색 기술을 제안하였다. 제안된 스킴은 다양한 공격들에 대해서 안전성을 제공하고 사용자의 공개키와 개인키에 대한 안전성 및 공개키 인증서 관리에 대한 요구가 없다. 또한, 서버의 공개키도 스마트 카드에 저장하여 발급하기 때문에 서버의 공개키에 대한 인증서가 요구되지 않는다.

사용자에게 다양한 편리성을 제공할 것으로 기대하며 연구되고 있는 클라우드 연구 분야는 다양한 디바이스에서 가공, 생성, 저장되는 다양한 데이터들에 대한 데이터 프라이버시와 이들 데이터에 대한 편리한 접근을 가능하게 한다. 하지만 다양한 디바이스들이 일정 수준 이상의 안전성을 제공하는 것이 쉽지 않고 이러한 디바이스들에 사용자의 공개키 및 개인키 정보가 저장된다는 것은 많은 문제를 야기할 수 있다. 반면 스마트 카드를 내장한 디바이스에서 본 기술을 적용하여 중요한 데이터에 대해서 관리한다면 클라우드 환경에서 사용자에게 자신의 데이터 정보를 효율적으로 관리하면서도 자기정보 통제권을 갖게 한다는 측면에서 매우 큰 의미가 있다.

본 논문에서 제안한 기법은 Pairing연상을 요구한다. Parinig연산을 경량화하여 좀 더 현실적인 기술을 제안하는 것은 의미가 있다. 더 나아가서 암호화된 데이터에서의 Inner Product, Conjunctive와 같이 다양한 검색이 가능하도록 확장하는 것은 향후에 연구할 만하다.

참 고 문 헌

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi, \emph{Searchable Encryption Revisited : Consistency Properties, Relation to Anonymous IBE, and Extensions}, Journal of Cryptology, Volume 21, Issue 3, pages 350-391, 2008.

[2] J. Baek, R. Safavi-Naini, and W. Susilo, “Public key encryption with keyword search revisited,” Proc. ICCSA 2008, LNCS 5072, pp. 1249 - 1259, 2008.

[3] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” Proc. EUROCRYPT 2004, LNCS 3027, pp. 506 - 522, 2004.

[4] D. Boneh and B. Waters, Conjunctive, Subset, and Range Queries on Encrypted Data, In proceedings of TCC2007, LNCS vol.4392, pages 535-554, 2007.

[5] C. Blundo, V. Iovino, and G. Persiano, Private-Key Hidden Vector Encryption with Key Confidentiality, in Proc. Cryptology and Network Security 2009, LNCS vol.5888, pages 259-277, 2009.

[6] C. I. Fan, Y. C. Chan, Z. K. Zhang, Robust remote authentication scheme with smart cards, Computers & Security 24(8) pages 619-628, 2005.
[7] P. Golle, J. Staddon and B. Waters, Secure Conjunctive Keyword Search Over Encrypted Data, In Proceedings of ACNS2004, NCS vol.3089, pages 31-45, 2004.
[8] J. Katz, A. Sahai, B. Waters, Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, In Proceedings of EUROCRYPT2008, LNCS vol.4965, pages 146-162, 2008.
[9] D. Park, K. Kim and P. Lee, Public-Key Encryption with Conjunctive Field Keyword Search, In Proceedings of WISA2004, LNCS vol.3325, pages 73-86, 2004.
[10] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, Improved Searchable Public Key Encryption with Designated Tester, In Proceedings of ASIACCS2009, pages 376-379, 2009.
[11] D.E. Shen, E. Shi, and B. Waters, Predicate Privacy in Encryption Systems, In Proceedings of TCC2009, pages 457-473, 2009.
[12] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searching on encrypted data," Pro. IEEE Symposium on Security and Privacy, pp. 44-55, May 2000.
[13] C. C. Yang, H. W. Yang, and R. C. Wang, Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50(2), pages 578-579, 2004.

저 자 소 개

이 동 근(정회원)
1990년 부산대학교 기계공학과 학사 졸업.
2010년～현재 고려대학교 정보보호대학원 석사재학중.
현재 삼성전자 무선사업부 상무

<주관심분야 : 정보보호정책, 개인정보보호, 기업정보보호>

임 종 인(정회원)-교신저자
2012년 현재 고려대학교 정보보호대학원 원장 겸 교수
2012년 현재 개인정보보호위원회 위원
2012년 현재 산업기술보호위원회 위원
2012년 현재 대검찰청 디지털수사 자문위원회 위원장
2012년 현재 행정안전부 정책자문위원회 위원
2012년 현재 금융보안연구원 보안기술전문위원회 위원장
2012년 현재 국가정보원 정보보호시스템 평가인증위원회 위원
2012년 현재 한국정보보호학회 명예회장

이 현 숙(정회원)
2008년 고려대학교 정보보호대학원 박사 졸업
2008년～2009년 Wollongong University PostDoc
2009년～2010년 고려대학교 정보보호대학원 연구교수
2010년 학술진흥재단 여성과학자
2011년～현재 삼성전자 ITS사업부 보안 기술 담당.

<주관심분야 : 정보보호기술, 프라이버시보호기술>