情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

사용자 속성의 위임, 철회 가능한 속성기반 암호기술

송 유 진*, 도 정 민**

요 약

최근 인터넷에서 취급되는 데이터들은 개인의 프라이버시를 침해할 수 있으므로 암호화 등의 보안기술 도입이 필수적이다. 특히, u-헬스케어 서비스 사용자는 자신의 데이터에 대한 접근 권한을 위임한 사용자에 한해서만 데이터에 접근가능하도록 하고 상황에 따라 접근 권한을 박탈하는 능력이 필요하다. 이러한 서비스의 접근권한 요구사항에 근거하여 본 논문은 개인정보에 대한 접근 권한을 위임, 철회 가능한 속성기반 암호기술을 소개하고 검토한다.

Ⅰ. 서 론

정보기술의 발달로 인간의 삶의 질이 향상되었지만 개인의 편의를 위해서 공유되는 정보로 인해 개인정보 유출과 같은 보안 침해 사례가 발생하고 있다. 현재 인터넷에서 공유, 유통되어지는 정보는 개인의 프라이버시를 침해할 수 있고 이러한 프라이버시에 민감한 개인정보들이 아무런 조치없이 그대로 데이터베이스에 저장되어 보관되고 있다. 이 때문에 외부 공격자나 악의적인 내부 사용자에 의해서 개인정보 유출문제가 발생되고 있는 실정이다. 이러한 문제를 방지하기 위해서는 암호기술의 도입이 필수적이다.

암호방식으로 공개키 암호방식, ID기반 암호방식, 속성기반 암호방식이 실제 환경에 응용되기 위해서 연구중에 있다. 특히, 속성기반 암호방식은 각 개체의 속성을 이용하여 암복호화를 실행할 수 있고 기존의 공개키 암호방식, ID기반 암호방식과 달리 하나의 개체가 여러 개의 속성을 가질 수 있다. 예를 들어 소속이 '병원'이고 직위가 '원장'인 두 개의 속성을 만족해야지만 권한을 부여받을 수 있다. 속성기반 암호방식의 이러한 성질을 활용하여 접근 권한을 부여하기 위해 사용자 속성의 위임, 철회 가능한 속성기반 암호방식[6]이 제안되었다.

본 논문에서는 사용자 속성의 위임, 철회 가능한 속성기반 암호방식을 소개하고 u-헬스케어 서비스에의 응용에 대해서 검토한다. u-헬스케어 서비스는 의료정보화를 통한 의료서비스 질의 향상, 생산성과 작업의 효율화, 의료사고의 감소 등을 목표로 하고 있다[1][2][3][9].

u-헬스케어 산업이 활성화되기 위해서 개인의 진료정보 보관 및 관리가 중요하다. 현재 의료기관에서 진료기록을 관리하는 방법에 있어서도 문제점이 많다. 의료기관별로 정보가 분산돼 있고, 환자가 아닌 의료기관 방문 중심으로 꾸며져 있으며, 환자가 필요할 때 접근이 불가능하고 현행법상 정보에 대한 소유권이 의료기관에 있으며, 표준화작업이 전혀 진행돼 있지 않은 상태이다. 또한, 의료기관 중심이 아닌 환자 중심의 표준화 작업이 시급하다. 따라서 언제, 어디서나 대인 진료기록에 접근할 수 있고, 중복검사를 방지하며, 환자의 평생건강관리(PHR, Personal Health Record)를 지원하고, 개인의 진료정보를 의료기관이 공동으로 활용할 수 있도록 하는 방향으로의 개선이 필요한 시점이다[10].

u-헬스케어 서비스는 기존 유비쿼터스 컴퓨팅 서비스와는 다른 보안 요구사항들이 존재한다. 개인 의료정보가 여러 사용자 그룹(Primary care, Secondary use)에 의해 공유되어야 하며 정확한 진료를 위해서는 정보의 공유 및 2차 활용이 필수적이다. 이러한 정보의 공유 때문에 보안 취약사항이 노출되고 u-헬스케어 서비스에 대한 보안 이슈가 제기되고 있다[4][5][7][9].

현재 진료목적으로 제공하는 정보가 모든 사용자 그

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.(No. 2010-0028122)
* 동국대학교 정보경영학과 (song@dongguk.ac.kr)
** 동국대학교 전자상거래협동과정 (havdrim@hotmail.com)

룹(의사뿐만 아니라 간호사나 물리치료실 관계자, 약사, 행정직원 등 병원에 종사하는 모든 사람들)이 열람가능하며 정부기관을 비롯 보험회사, 제약회사, 해커 등 제3자도 충분히 침입가능한 문제가 발생되고 있다[10].

서비스 대상자(환자)의 입장에서는 본인의 의료정보가 정당한 사용자에 의해 의료 서비스 목적에 맞게 최소한의 공유가 이루어지고 상황에 따라서는 데이터에 대한 접근 권한을 제어할 필요가 있다. 즉, 환자의 동의에 따른 의료정보의 안전한 공유 및 활용을 요구하고 있으며 이를 만족시키기 위해서 암호방식의 도입이 필수적이다[6]. 이러한 서비스 대상자의 요구사항을 고려하여 서비스 대상자가 자신의 속성을 기반으로 암호화된 건강기록정보에 대해 정당한 사용자에게 복호 권한을 위임, 철회 가능한 암호방식이 요구된다[8].

본 논문에서는 이러한 문제에 대한 기술적인 대책으로서 정당한 속성을 갖는 사용자만이 진료정보에 접근이 가능하도록 의료정보를 암호화하는 방법을 강구한다. 그리고 u-헬스케어 환경에서 속성을 위임, 철회 가능한 사용자 속성기반 암호방식을 검토한다.

본 논문의 2장에서는 관련연구배경을 알아보고 3장에서는 사용자 속성의 위임, 철회 가능한 속성기반 암호방식을 검토한다. 4장에서는 이를 활용한 시스템 시나리오를 살펴보고 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구배경

2.1 쌍선형 사상(Bilinear Mapping)

2개의 순환군(Cyclic Group) G_1, G_2에 대해 쌍선형 사상 $e: G_1 \times G_2 \rightarrow G_T$(G_T는 쌍선형 사상의 출력 공간)는 다음의 성질을 갖는다.

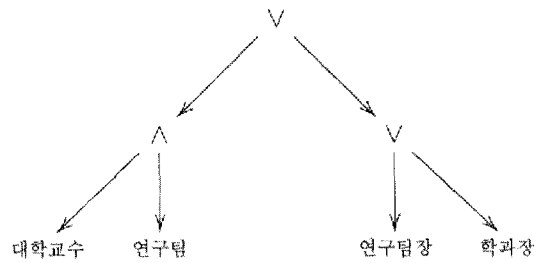
(1) 쌍선형성(bilinear) : 모든 $u \in G_1$, $v \in G_2$ 및 모든 a, $b \in Z$에 대해 $e(u^a, v^b) = e(u, v)^{ab}$가 성립된다.

(2) 비퇴화성(non-degenerate) : G_X $(X = 1, 2)$의 생성원 $g \in G_X$에 대해 $e(g, g) \neq 1$이다.

(3) 계산가능성(computable) : 모든 $u \in G_1$, $v \in G_2$에 대해서 $e(u, v)$를 계산하는 효율적인 알고리즘이 존재한다.

2.2 접근구조

기존 속성기반 암호화(CP-ABE, Ciphertext Policy Attribute Based Re-Encryption)[11]에서 사용자 비밀키는 속성집합과 관련되며 암호문은 속성 접근구조와 관련이 있다[6]. 암호문 내의 특정 복호정책에 대해서 사용자의 비밀키 속성집합이 만족되면 암호문은 복호된다.



* 접근구조=(대학교수∧연구팀)∨(연구팀장∨학과장)

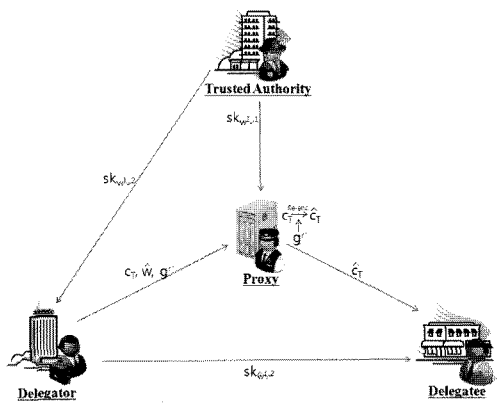
〔그림 1〕 접근구조

예를 들어, 의과대학에서 신종플루에 대한 연구를 수행하고 있다. 의과대학의 연구자가 그동안 연구해 왔던 데이터에 대한 접근을 원한다면 비밀키는 대학교수이고 연구팀 또는 연구팀장이나 학과장의 속성을 기반으로 만들어져야 하며 접근구조 (대학교수∧연구팀)∨(연구팀장∨학과장)는 [그림 1]과 같이 만들어져야 한다. 비밀키가 이러한 접근구조를 만족하면 연구자는 데이터를 복호할 수 있다.

종래에 CP-ABE 방식은 철회(Revocation)와 위임(Delegation)에 대한 문제를 실용적인 면에서 다루지 못하고 있다.

Ⅲ. 사용자 속성의 위임, 철회 가능한 속성기반 암호방식[6]

사용자 속성의 위임, 철회 가능한 속성기반 암호방식



〔그림 2〕 CP-ABTD의 개념도

(CP-ABTD, Ciphertext Policy Attribute Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes)은 속성기반 암호화의 확장된 형태로서 유연한 속성 위임과 동시에 속성 철회 기능을 수행할 수 있다. 이러한 CP-ABTD는 3가지 특징을 가지고 있다. 첫째, 속성집합과 관련된 비밀키를 가지는 위임자는 피위임자에게 자신의 권한을 위임할 수 있다. 둘째, 위임자는 피위임자에게 자신의 권한을 위임할 수 있도록 결정할 수 있다. 셋째, 제안된 방식은 속성철회가 가능하다. [그림 2]는 CP-ABTD의 개념도이다.

사용자 속성의 위임, 철회 가능한 속성기반 암호방식은 Setup, KeyGen, Encrypt, Delegate, m-Delegate, m-Decrypt, Decrypt로 총 7개의 알고리즘으로 구성되고 참가자는 위임자, 피위임자, 인증기관(TA, Trusted Authority), 프록시다.

각 알고리즘에 대해서 Setup과 KeyGen은 TA, Encrypt와 Delegate는 위임자, m-Delegate와 m-Decrypt는 프록시, Decrypt는 피위임자에 의해서 수행된다.

① Setup(k) : 보안파라메터 k를 입력받아서 생성자 g, 소수 위수 p인 G_0를 생성한다. bilinear map은 $\hat{e}: G_0 \times G_0 \rightarrow G_1$이고 시스템 속성 집합 $\Omega=(a_1, a_2, \ldots a_n)$ (n은 정수)이며 $a_j \in \Omega$는 임의의 요소 $t_j \in Z_p^*$를 선택한다.

- $y=\hat{e}(g,g)^{\alpha}$ ($\alpha \in_R Z_p^*$, $T_j=g^{t_j} (1 \le j \le n)$)
- 공개키 $pk=\left(\hat{e}, g, y, T_j (1 \le j \le n)\right)$
- 마스터키 $mk=(\alpha, t_j (1 \le j \le n))$

가 생성된다.

② KeyGen(mk, w, I_u) : 속성 집합 w와 위임자의 식별자 I_u로 비밀키를 생성한다.

(a) 비밀키의 베이스 콤포넌트 :

$d_0=g^{\alpha-u_{id}}$ ($u_{id} \in_R Z_p^*$)를 계산.

(b) 비밀키의 속성 콤포넌트 :

속성 $a_j \in w$, $u_j \in_R Z_p$를 선택하고 $d_{j,1}=g^{u_j t_j^{-1}}$와 $d_{j,2}=g^{(u_{id}-u_j)t_j^{-1}}$를 계산.

첫 번째 비밀키 쉐어 $sk_{w I_u 1}=(\forall a_j \in w: d_{j,1})$를 프록시에게 전송하고, 두 번째 비밀키 쉐어 $sk_{w I_u 2}=(d_0, \forall a_j \in w: d_{j,2})$를 위임자에게 전송한다.

③ Encrypt(m, τ, pk)($m \in G_1$) : $s \in Z_p^*$를 임의로 선택하고 $c_0=g^s, c_1=m \cdot y^s=m \cdot \hat{e}(g,g)^{\alpha s}$를 계산한다. 최종 사용자 속성(leaf attribute) $a_{j,i} \in \tau$, $c_{j,i}=T_j^{s_i}$를 계산한다. 위임자의 암호문 $c_\tau=(\tau, c_0, c_1, \forall a_{j,i} \in \tau: c_{j,i})$를 만들어낸다.

④ Delegate($sk_{w I_u 2}, \hat{w}, I_j$) : $r' \in Z_p$를 임의로 선택하고 $a_j \in \hat{w}$로 $g^{t_j r'}=g^{r_j''}$을 설정한다. 속성 전환키 $sk_{w \rightarrow \hat{w}}=g^{r'}$을 설정하고 $a_j \in \hat{w}$로 $\widehat{d_{j,2}}$을 계산한다.

$\widehat{d_{j,2}}=g^{(u_{id}-u_j)t_j^{-1}-r'}=g^{(u_{id}-u_j)t_j^{-1}-r_j''t_j^{-1}}$

$=g^{(u_{id}-\hat{u_j})t_j^{-1}} (\hat{u_j}=u_j+r_j'')$

비밀키 쉐어 $sk_{\hat{w} I_j 2}=(d_0, \forall a_j \in \hat{w}: \widehat{d_{j,2}})$를 피위임자에게 전송하고 $\hat{w}$와 $sk_{w \rightarrow \hat{w}}$를 프록시에게 전송한다.

⑤ m-Delegate($sk_{w I_u 1}, \hat{w}, sk_{w \rightarrow \hat{w}}$) : 속성 위임 리스트(Attribute Delegation List)를 체크하고 속성 위임대상이라면 $a_j \in \hat{w}$로 $sk_{\hat{w} I_j 1}$을 계산한다. 속성 위임 리스트에 확인되지 않으면 계산은 진행되지 않는다.

$\widehat{d_{j,1}}=g^{u_j t_j^{-1}+r'}=g^{\hat{u_j} t_j^{-1}}$

비밀키 쉐어 $sk_{\hat{w} I_j 1}=(\forall a_j \in \hat{w}: \widehat{d_{j,1}})$를 피위임자에게 전송한다.

⑥ m-Decrypt($c_\tau, sk_{w I_j 1}, I_t$) : 속성 철회 리스트(Attribute Revocation List)를 체크하고 속성 철회대상이 아니라면 $\hat{c_\tau}$를 계산한다. 철회대상이라면 계산이 진행되지 않는다. 모든 속성 $a_j \in w'$로 계산한다.

$\hat{c_\tau}=\prod_{a_j \in w'} \hat{e}\left(T_j^{s_i}, g^{u_j t_j^{-1}}\right)=\hat{e}(g,g)^{\sum_{a_j \in w} u_j s_i}$

⑦ Decrypt($\hat{c_\tau}, sk_{w I_j 2}$) :

(a) 모든 속성 $a_j \in w'$로 계산:

$$c_\tau''=\prod_{a_j \in w'} \hat{e}\left(T_j^{s_i}, g^{(u_{id}-u_j)t_j^{-1}}\right)$$
$$=\prod_{a_j \in w'} \hat{e}\left(g^{t_j s_i}, g^{(u_{id}-u_j)t_j^{-1}}\right)$$
$$=\hat{e}(g,g)^{\sum_{a_j \in w'}(u_{id}-u_j)s_i}$$

(b) 계산:

$$\hat{e}(c_0, d_0) \cdot \hat{c_\tau} \cdot c_\tau''$$
$$=\hat{e}\left(g^s, g^{\alpha-u_{id}}\right) \cdot \hat{e}(g,g)^{\sum_{a_j \in w} u_j s_i} \cdot \hat{e}(g,g)^{\sum_{a_j \in w'}(u_{id}-u_j)s}$$
$$=\hat{e}\left(g^s, g^{\alpha-u_{id}}\right) \cdot \hat{e}(g,g)^{u_{id} s} = \hat{e}\left(g^s, g^{\alpha}\right)$$

(c) m의 반환

$$m = \frac{c_1}{\hat{e}(g^s, g^\alpha)} = \frac{m \cdot \hat{e}(g, g)^{\alpha s}}{\hat{e}(g^s, g^\alpha)}$$

Ⅳ. 사용자 속성의 위임, 철회 가능한 속성기반 암호기술을 활용한 시스템의 시나리오

4.1 시스템 개요

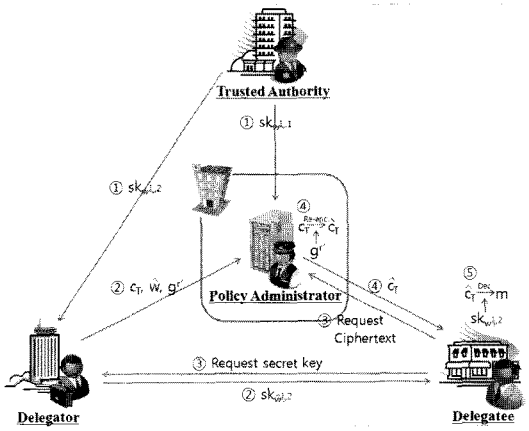
기존의 원격 헬스케어 시스템은 서비스 사용자에 대한 데이터가 평문 형태로 저장되어 사용자가 접근하여 사용했다. 진정한 유비쿼터스 헬스케어 서비스가 이루어지려면 데이터의 공유 및 활용은 필수적이다. 이때 사용되는 데이터는 개인에게 있어 치명적일 수 있는 정보다.

그러므로 서비스 사용자의 데이터가 안전하게 공유 및 활용되기 위해서 서비스 사용자는 정당한 사용자에게 데이터에 접근할 수 있는 권한을 부여하는 위임기능과 때에 따라서 접근 권한을 부여한 사용자의 권한을 박탈하는 철회기능이 요구하게 된다. 이러한 요구사항을 감안하여 접근 권한을 위임, 철회할 수 있는 사용자 속성의 위임, 철회 가능한 속성기반 암호기술을 이용한 시스템을 소개한다.

우선, 사용자 속성의 위임, 철회 가능한 속성기반 암호기술을 이용한 시스템은 서비스 사용자의 속성을 기반으로 한 접근구조로 데이터를 암호화하여 프록시 서버에 전송한다. 서비스 사용자의 암호화된 데이터를 공유 및 활용하고자 하는 사용자는 프록시 서버에 복호권한을 요구한다. 서비스 사용자는 복호권한을 요구한 사용자가 자신의 데이터를 이용할 수 있는 정당한 사용자임을 판단한 후에 속성을 위임하는 키를 만들어 프록시 서버에게 보내준다. 이 시스템 상에서 프록시 서버는 속성위임리스트와 속성철회리스트를 보유하고 있어야한다. 프록시 서버는 속성위임리스트를 체크하고 속성을 위임하는 키로 데이터를 재암호화한 후 사용자에게 제공한다.

4.2 시나리오

사용자 속성의 위임, 철회 가능한 속성기반 암호기술을 이용한 u-헬스케어 서비스 시스템 시나리오는 다음과 같다[그림 3].



〔그림 3〕 시나리오 구성

① Trusted Authority(TA)가 Setup(k) 알고리즘을 이용해서 시스템 파라메터을 정의하고 공개키 pk와 마스터키 mk를 생성한다. 그리고 KeyGen (mk, w, I_u) 알고리즘을 이용하여 환자의 속성 w과 공개키 I_u와 연관된 두 개의 비밀키 쉐어 sk_{wI_u1}와 sk_{wI_u2}를 생성하여 프록시 서버에게 sk_{wI_u1}와 환자에게 sk_{wI_u2}를 분산한다.

② 환자는 Encrypt(m, τ, pk) 알고리즘으로 데이터 m를 암호화한 암호문 c_τ를 프록시 서버의 데이터베이스로 전송한다. 여기서, 데이터는 일반적으로 PHR(Personal Health Record) 데이터를 말한다. 환자는 의사에게 암호문 c_τ에 대한 복호 권한을 위임하기위해서 자신의 속성집합 w를 기초로 $\hat{w}$를 정의한다. 자신의 비밀키 쉐어 sk_{wI_u2}와 $\hat{w}$, 의사의 공개키 I_j로 의사를 위한 비밀키 쉐어 $sk_{\hat{w}I_j,2}$와 속성을 위임하는 프록시키 $sk_{w\to\hat{w}}$를 생성하여 각각 의사$(\hat{w},\ sk_{\hat{w}I_j,2})$와 프록시 서버$(sk_{w\to\hat{w}})$에게 보낸다.

③ 의사는 환자의 데이터 m에 접근하기 위해서 프록시 서버에 복호 토큰(속성집합과 암호문)을 요구한다.

④ 프록시 서버는 자신의 비밀키 쉐어 sk_{wI_u1}, 프록시키 $sk_{w\to\hat{w}}$와 환자가 정의한 속성집합 $\hat{w}$로 의사를 위한 비밀키 쉐어 $sk_{\hat{w}I_j1}$을 생성한다. 암호문 c_τ를 의사의 공개키 I_j, $sk_{\hat{w}I_j1}$로 재암호화한 $\hat{c_\tau}$를 의사에게 보낸다.

⑤ 의사는 프록시 서버와 환자로부터 받은 키 $sk_{\hat{w}I_j 2}$와 암호문 $\hat{c}_r$으로 복호하여 데이터 m을 획득한다.

V. 결 론

본 논문은 u-헬스케어 환경에서의 사용자 속성의 위임, 철회 가능한 속성기반 암호기술의 적용 가능성에 대해서 검토하였다. 사용자 속성의 위임, 철회 가능한 속성기반 암호기술이 위임과 철회기능을 갖추고 있어 유비쿼터스 헬스케어 서비스에 활발한 응용이 예상된다.

참 고 문 헌

[1] 오정연, "의료정보화 현황 및 과제," NCA CIO REPORT, 05-11호, 한국전산원, 2006.

[2] 박건희, "보건의료정보화와 개인정보보호," 서울대 의대 2006년 상반기 토픽 리뷰, 2006.

[3] 송지은, 김신효, 정명애, 정교일, "u-헬스케어 보안 이슈 및 기술 동향," 전자통신동향분석, 제 22권 제 1호, 한국전자통신연구원, 2007.

[4] Shinyoung Lim, Taehwan Oh, Young B. Choi, T. Lakshman, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring," UMC2010, 2010.

[5] M. Tentori, et.al., "Privacy-Aware Autonomous Agents for Pervasive Healthcare," IEEE Intelligent Systems, pp.55-62, Nov.-Dec. 2006.

[6] 박광용, 송유진, "속성기반 암호기술," 정보보호학회, Feb. 2010.

[7] P. Robinson, H. Vogt, W. Wagealla, "Privacy, Security, and Trust Within the Context of Pervasive Computing," SpringerVerlag, ISBN 0387234616, 2005.

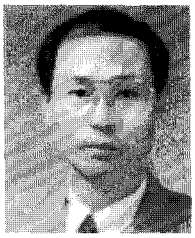
[8] L. Ibraimi, M. Petkovic, S. Nikoval, P. Hartel, W. Jonker, " Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009 University of Twente, Centre for Telematics and Information Technology, Internal Report, 2009.

[9] EHR핵심연구개발사업단, "건강정보보호 및 보안체계 개발," 5세부, 2009, 4월.

[10] 김주한, "개인정보 암호화 한 평생기록 추진," 메디칼 업저버, 창간 5주년 기념 정책토론회, Jul. 2006.

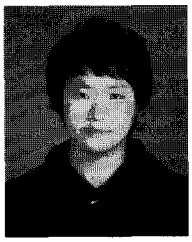
[11] X. Liang, Z. Cao, H. Lin, J. Shao, "Attribute Based Proxy Re-encryption with Delegating Capabilities," ASIACCS 2009, Sydney, Australia, ACM, pp. 276-286, Mar. 2009.

〈著者紹介〉



송 유 진 (Youjin Song)
정회원

1982년 2월: 한국항공대학교 전자공학과 학사
1987년 8월: 경북대학교 대학원 석사
1995년 3월: 일본 Tokyo Institute of Technology (동경공업대학) 정보보호학과 박사
1988년~1996년: 한국전자통신 연구원 선임연구원
2003년~2005년: 미국 University of North Carolina at Charlotte 연구교수
2006년 7월~8월: 일본 정보보호대학원대학(IISEC) 객원교수
1996년~현재: 동국대학교 정보 경영학과/대학원 교수
2005년~현재: 동국대학교 부설 전자상거래연구소 소장
1998년~현재: 한국정보보호학회 이사
2006년~현재: 국제e-비즈니스학회 이사
2006년~현재: 한국사이버테러정보전학회 이사
2001년: ICISC2001 운영위원장
2003년: 하계CISC2003 프로그램위원장
2006년: CISC-S2006 공동 프로그램위원장
2007년: 한국정보시스템학회 추계학술발표대회 공동 조직위원장
<관심분야> Secret Sharing, Privacy Protection, 전자상거래 응용보안 (Location Privacy, 디지털컨텐츠 보호, SCM/CRM 보안 등), Context Aware Application Security



도 정 민 (Jeongmin Do)
학생회원

2010년 2월: 동국대학교 정보경영학과 졸업
2010년 3월~현재: 동국대학교 석사과정(전자상거래 기술전공)
<관심분야> 암호이론, 데이터 베이스 보안, 유비쿼터스 프라이버시 보호