韓國 컴퓨터情報學會 論文誌
第13卷 第5號, 2008. 9.

2008-13-5-3-3

역할기반 접근제어시스템에 적용가능한 민감한 개인정보 보호모델

문 형 진*, 서 정 석**

Sensitive Personal Information Protection Model for RBAC System

Hyung-Jin Mun*, Jung-Seok Suh**

요 약

전자상거래의 발달로 인해 옥션과 같은 쇼핑몰은 효율적인 서비스를 위해 고객의 개인정보를 수집하고 관리하고 있다. 하지만 옥션의 개인정보 유출로 인해 그 피해가 기업이미지 손상뿐만 아니라 유출된 정보주체인 개인까지 피해를 주고 있다. 기관과 기업에서 개인정보를 DB에 평문상태로 저장하고, 역할기반 접근제어기술을 이용하여 개인정보를 보호하고 있지만 DB관리자의 권한만 획득하면 옥션과 같이 개인정보가 쉽게 유출된다. 또한 역할기반 접근제어기술은 정보주체의 민감한 정보에 대한 보호기술로 적합하지 않다. 이 논문에서는 정보 주체가 지정한 민감한 정보를 암호화하여 DB에 저장하고, 정보주체의 개인별 정책에 따라 자신의 정보에 대한 접근을 엄격하게 제한하는 개인별 정책 기반의 접근제어 기법을 제안한다. 제안 기법을 통해 DB관리자로부터 안전하고, 개인정보 보호기술인 역할 기반 접근제어의 문제점을 보완하여 정보주체의 자기정보 제어권을 가진다.

Abstract

Due to the development of the e-commerce, the shopping mall such as auction collects and manages the personal information of the customers for efficient service. However, because of the leakage of the personal information in auction, the image of the companies as well as the information subjects is damaged. Even though the organizations and the companies store the personal information as common sentences and protect using role based access control technique, the personal information can be leaked easily in case of getting the authority of the database administrator. And also the role based access control technique is not appropriate for protecting the sensitive information of the information subject. In this paper, we encrypted the sensitive information assigned by the information subject and then stored them into the database. We propose the personal policy based access control technique which controls the access to the information strictly according to the personal policy of the information subject. Through the proposed method we complemented the problems that the role based access control has and also we constructed the database safe from the database administrator. Finally, we get the control authority about the information of the information subject

▸ Keyword : 개인정보(Personal Information), Access Control, Privacy, SpRBAC, SIMS

• 제1저자 : 문형진
• 접수일 : 2008. 6. 9, 심사일 : 2008. 7. 3, 심사완료일 : 2008. 9. 25.
* 충북대학교 초빙전임강사 **나사렛대학교 정보통신학과 부교수

Ⅰ. 서 론

전자상거래의 발달로 인해 많은 쇼핑몰이 생겨 났고, 쇼핑몰에서는 더 나은 서비스를 목적으로 고객으로부터 많은 개인정보를 요구하고, 수집하여 저장하고 있다. 최근에 옥션의 개인정보 유출로 인하여 매스컴을 통해 이슈가 되고 있다. 이렇게 개인정보가 유출되어 기업은 기업의 이미지가 손상되었고, 관련 소송으로 인해 경제적인 피해까지 발생하고 있다. 또한 유출된 정보의 주체인 개인은 유출에 의한 피해뿐만 아니라 스팸메일, 스팸문자의 2차 피해와 피싱, 전화사기와 같은 3차 피해까지 발생하여 경제적 피해와 정신적인 피해까지 주고 있다. 뿐만 아니라 구글과 같은 검색엔진의 발달로 개인정보가 노출되는 사례가 발생한다[1]. 이는 기관에서 개인의 정보를 수집하여 평문상태로 DB에 저장하고 관리하기 때문이다. DB에 저장된 정보는 RBAC 기술을 이용하여 정보사용자의 역할에 따라 정보 접근이 가능하게 되어 있다. DB관리자의 권한이 크기 때문에 DB관리자의 권한을 획득하면 제 2의 옥션사태가 계속적으로 발생 가능하다. 개인정보 유출을 막고자 개인정보 보호를 위한 연구들이 접근제어와 암호화 기술을 중심으로 활발하게 수행되고 있다.

프라이버시보호를 위한 OECD 가이드라인 8원칙 , UN 개인정보 가이드라인 , EU 개인정보보호 지침은 정보주체가 자신의 정보에 대한 제어권을 가져야 한다고 명시하고 있다[2]. 즉, 자신의 정보를 수집, 사용에 있어 정보주체의 동의를 구해야 한다. 공공기관이나 기업에서는 정보수집시에만 정보주체의 동의를 구하는 시스템으로 되어 있다. 기존 RBAC 기술이 적용된 시스템에서 정보주체의 민감한 정보를 접근시 주체의 동의하에 정보사용이 가능한 새로운 접근제어기술이 필요하다.

이 논문에서는 정보주체가 자신의 보호정책을 기관에게 제시하고, 기관에서는 정보주체의 개인별 정책에 근거하여 개인정보를 보호할 수 있는 모델을 제안한다. 기존의 RBAC시스템을 그대로 사용할 수 있는 개인정보보호를 위한 역할기반의 접근제어 모델을 제안한다. 이 논문의 구성은 다음과 같다. 2장에서는 개인정보 보호기술에 대한 관련 연구를 소개하고, 3장에서는 개인별 정책기반의 역할기반 접근제어기술모델(SpRBAC : subject-wise policy based RBAC)을 소개하고, SpRBAC를 이용한 SIMS (sensitive information management system)을 설계 및 동작과정을 설명하고, 4장에서는 시나리오 분석 및 평가를 하고 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

PGP과 같은 암호화 소프트웨어는 암호화를 통해 전자메일, 저장된 파일, 그리고 온라인에서의 안전한 통신을 제공한다. 복호화 키를 가진 사용자만이 암호화된 정보를 접근할 수 있다[3]. 최근에 암호화 기술을 이용한 개인정보를 보호하는 연구들이 진행되고 있다[4-10].

접근제어기술은 접근 권한이 있는 사용자만 접근을 허용하는 기술로 MAC(Mandatory Access Control) 과 DAC (Discretionary Access Control)같은 고전 기술이 있으나 다양하고, 복잡해지는 기관이나 기업에 적용하기가 부적합하다. 다양하고 복잡한 기관이나 기업에 적용 가능한 접근제어 기술로 RBAC (Role based Access Control)가 D.F.Ferraiolo와 D.R,Kuhn에 처음 제안되었고, R.Sandhu 에 의해 RBAC96으로 체계화되었다[11-14]. RBAC은 <그림1>에서 보듯 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없고, 대신에 접근 권한이 역할에 부여되어, 사용자는 적절한 역할에 소속됨으로 역할의 수행에 필요한 최소 자원만을 접근이 가능하다. RBAC은 복잡한 조직의 구조에 자연스럽게 매핑시켜 기관이나 기업마다 서로 다른 보안 요구사항을 만족시킬 수 있다[12].

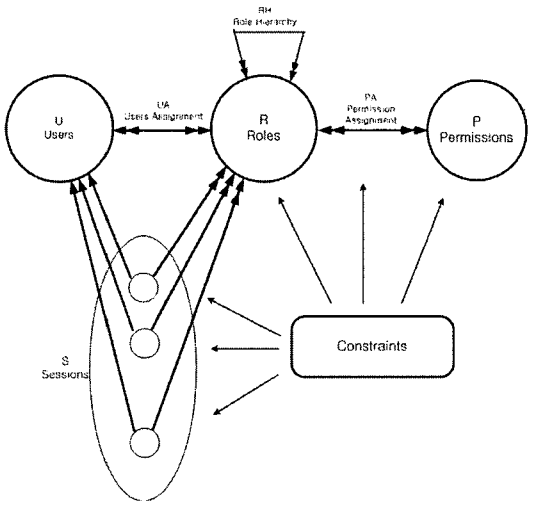

그림 1. RBAC 모델
Fig 1. RBAC Model

하지만 정보의 주체가 기관이나 기업인 경우 RBAC 모델이 적합하나 정보주체가 개인인 경우 개개인의 요구가 다르고

정보 유출시 그 피해가 개인에게 전가되어 기존 RBAC모델이 적용하기에는 부적합하다.

III. SpRBAC모델을 이용한 SIMS설계

개인은 기업이나 기관에게 자신의 정보를 민감한 정보(노출시 피해가 크다고 정보주체가 생각하는 정보)와 그렇지 않은 정보로 구분하여 제공한다. 제공된 개인정보는 DBMS에 의해 관리되고 있다. 정보 사용자는 DBMS에 의해 관리되는 개인정보를 주어진 권한 안에서 사용 목적에 따라 개인정보에 접근한다. 개인정보 주체가 개인정보를 관리하는 기관이나 기업 내의 정보사용자별로 접근 가능한 정보항목을 결정하여 개인별 정책에 기록한다. 정보사용자는 개인별 정책에 의해 지정된 정보만을 접근할 수 있다.

3.1 프레임 워크

SpRBAC는 정보주체의 개인별 정책이 포함되어 있는 RBAC96모델의 확장모델이다. <그림 2>는 SpRBAC 모델의 프레임워크로서 사용자는 개인정보 사용시 정보주체의 동의를 구하는 모델이다.

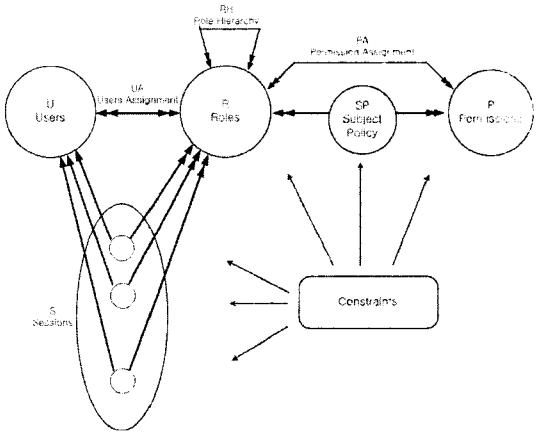

그림 2. SpRBAC 모델
Fig 2. SpRBAC Model

정보사용자의 권한이 개인정보를 접근할 수 있는 역할에 할당이 되어 있어도 정보 접근은 정보주체의 정책에 부합할 경우에만 허가된다.

3.2 개인별 정책에 의한 접근제어 모델

<그림 3>은 SpRABC을 기반한 민감한 개인정보 관리시스템의 구조를 나타낸 것이다. 정보주체(Subject)가 제공한 정보를 SIMS를 통해 Info.DB에 저장하고 정보사용자(User)는 SIMS을 통해 저장된 정보를 접근할 수 있다. SIMS의 구성요소는 <그림 3>에서 보듯이 크게 인증모듈, 정책저장소, Enc/Dec 모듈, 키관리, 감사로그로 이루어져 있다.

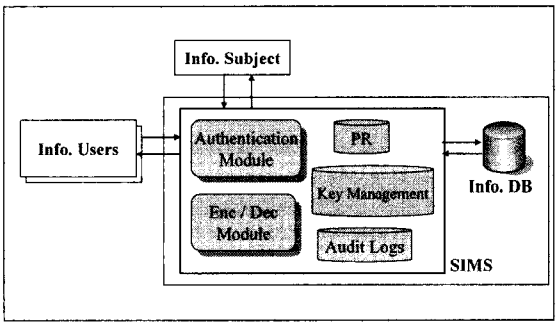

그림 3. 프레임 워크
Fig 3. FrameWork

3.2.1 인증모듈

인증 모듈은 SIMS 접근자의 인증을 담당한다. 정보주체와 정보사용자는 한 번의 인증을 통해 많은 권한이 제한없이 수행할 수 있기 때문에 ID/password 방식이 아닌 안전성이 검증된 인증서기반의 인증을 통해 사용자 인증을 한다.

3.2.2 정책저장소

정책저장소는 개인별 정책(ISp : Information Subject-wise policy)과 기관정책(EPp : Enterprise Privacy policy)이 저장되어 있는 곳이다. 전자는 개인이 자신의 정보에 대한 접근 권한 및 정보 유출시 민감한 정보를 지정하는 정책이고, 후자는 수집된 정보에 대해 RBAC 기반으로 프라이버시 관련 법규 및 치침에 의거하여 정보사용자의 역할에 따른 접근권한을 할당한다.

정보 주체는 자신의 정보에 대한 자기정보 제어권을 갖기 위해 개인별 정책을 세워야 한다. 많은 사용자에 대한 접근권한을 부여하는 것은 복잡하고 어렵기 때문에 효과적으로 개인별 정책을 수립하기 위해 기관은 정보주체에게 <그림 4>과 같이 정보사용자 그룹 카테고리(역할)를 제공하고, 정보 주체는 카테고리를 이용하여 역할에 따라 접근권한을 부여하고, 정보주체가 주치의와 같이 이미 알고 있는 특정사용자에 대한 접근권한을 추가적으로 구분하여 개인별 정책을 생성한다.

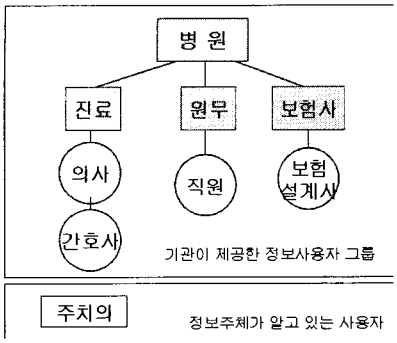

그림 4. 정보사용자 그룹별 카테고리
Fig 4. Information User group category

3.2.3 암·복호화모듈

암호화모듈은 추가적인 보호장치로 개인이 개인별 정책에서 지정한 민감한 정보를 암호화하는 모듈이다. 키관리에서 생성된 키를 이용하여 SIMS에서 암호화하여 개인정보 DB에 저장한다. 〈그림 5〉은 개인의 속성정보를 암호화하는 과정에 대한 의사코드이다.

```
// 정책에서 지정된 속성정보 암호화과정
Leb be number of attribute_information : n
Be K_ji and M={M_1,M_2,...,M_n}
  // K_ji : IS_j 의 i번째 속성키
Be A={A_1,A_2,...,A_n}
  //A_i : 속성정보 식별자
For i=1 to n
If (A_i∈ISpL) //ISpL : 민감한 정보목록
     Encrypt M_i^* = E_Kji(M_i)
Else
     M_i^* = M_i
Endif
Save M_i^* to Info.DB
```

그림 5. 속성정보의 암호화 알고리즘
Fig 5. Attribute Information Encryption Algorithm

복호화모듈은 정보사용자(정보접근자)의 정당한 요구에 따라 암호화된 개인정보를 복호화하는 모듈이다. 복호화된 정보는 안전한 채널을 통해 접근자에게 제공한다. 〈그림 6〉은 정보접근자의 요청시 암호화여부를 확인하여 암호화된 정보는 복호화하여 접근자에게 제공하고, 그렇지 않은 정보는 복호화과정없이 제공하는 과정을 의사코드이다.

```
// 암호화된 정보의 복호화 과정
Be K_ji and M_i and A_i
// K_ji : IS_j 의 i번째 속성키, A_i :속성정보 식별자
Receive M_i^* to Info.DB
If (A_i∈ISpL)  // ISpL : 민감한 정보목록
     Decrypt M_i = D_Kji(M_i^*)
Else
     M_i = M_i^*
Endif
Send M_i to Requestor
```

그림 6. 속성정보의 복호화 알고리즘
Fig 6. Attribute Information Decryption Algorithm

3.2.4 키관리

키관리는 키생성모듈과 KeyDB 2가지로 구성된다. SIMS는 민감한 속성정보를 안전하게 보호하기 위해 암호화를 하는데 많은 키를 필요로 한다. 키DB는 키생성모듈을 통해 생성된 개인별 마스터 키들을 안전하게 저장하는 공간이다.

키생성모듈을 통해 개인별로 마스터키(MK_{IS_i})를 생성한다. 개인별 정책에서 지정한 속성정보를 암호화하기 위한 키(속성키)가 필요하다. 〈그림 7〉은 개인별 마스터키와 속성키를 생성하는 과정을 나타낸 의사코드이다.

```
// 개인별 마스터 키 및 속성키 생성과정
Be ID_i , A_j and EMK  // ID_i : IS_i의 식별자
Generate T   // T 타임스팸프
Compute ID_i⊕T, ID_i⊕A_i
     MK_ISi = h_EMK(ID_i⊕T)
     key_ij = h_MKISi(ID_i⊕A_j)
     // IS_i의 j번째 속성키 생성
Save MK_ISi to KeyDB
```

그림 7. 개인별 마스터키 생성 알고리즘
Fig 7. Subject-wise Masterkey generation Algorithm

키생성모듈을 통해 생성된 개인별 마스터키는 키 DB에 저장하고, 개인별 마스터키를 통해 생성한 속성키는 암호화키로 사용한다. 키 길이가 짧고 암호화 속도가 빠른 대칭키 암호알고리즘을 이용하여 정책에 의해 지정된 속성정보를 암호화한다. 개인별 마스터키만 있으면 언제든지 생성이 가능하므로 속성키는 사용 후에 삭제한다.

3.2.5 개인정보 DB

DB는 개인정보를 저장하는 곳으로 정책에서 지정한 정보는 암호화되어 있고, 그렇지 않은 정보는 평문상태로 저장되어 있다. 정책에 의해 지정된 속성정보는 개인마다 속성마다 다른 키를 이용하여 암호화하고, 그 키는 SIMS에서 관리한다. 평문상태로 저장된 개인정보는 RBAC이 적용되어 접근권한이 없는 역할의 사용자로부터 보호를 받는다. 개인은 자신의 정보($M = M_1 \| M_2 \| \cdots \| M_n$)를 〈그림8(a)〉와 같이 SIMS에 제공한다. 〈그림8(b)〉에서 보듯이 속성정보 M_2, M_5, M_n 은 개인별 정책에 의해 지정된 민감한 정보로 암호화되어 있다.

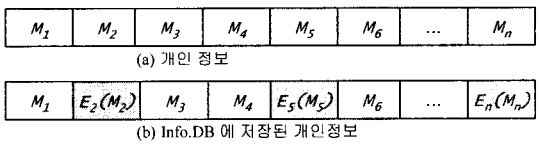

그림 8. Info.DB에 저장된 개인정보 구조
Fig 8. Structure of Personal Information stored in the info.DB

3.2.6 감사로그

감사로그(Audit Logs)는 정보주체의 정보수정을 비롯한 정보사용자에 의한 정보접근에 관련된 정보들을 기록한다. 감사로그는 기록된 자료를 근거로 정보주체나 정보사용자의 부인봉쇄 기능을 제공한다. 개인정보의 유출이나 프라이버시 침해가 발생할 때 수집된 감사로그의 분석을 통해 책임소재를 파악하는 기초자료로 활용된다. 감사로그에 대한 기록형태는 다음과 같다.

〈Req, Subj, Obj, fpL(Req), intent, time, IP〉

Req는 접근자이고, Subj는 접근하는 정보주체 식별자이고 Obj는 정보요청 목록이다. fpL(Req)는 Req에게 정보접근이 허용된 정보목록이고 intent는 접근목적을 나타낸다. time은 접근시간이고 IP은 접근하는 컴퓨터의 인터넷 주소를 나타낸다.

3.3 제안모델에서의 프로토콜

3.3.1 개인정보 등록

정보 주체는 n개의 속성정보를 SIMS에 제공하고, SIMS는 개인별 성향에 따라 자신이 지정한 민감한 속성정보를 〈그림 9〉와 같이 암호화한다. 지정된 정보를 암호화하는 암호화함수(E_{pL})를 다음과 같이 정의한다.

$$E_{pL} : M_i \rightarrow E_{pL}(M_i) = \begin{cases} E(M_i) & i \in pL \\ M_i & i \notin pL \end{cases}$$
$(pL$: 정책에 기록된 속성정보목록$)$

이는 정보주체인 개인에게 자신의 정보사용에 대한 제어가 부여되고, 개인이 지정하지 않은 정보는 기관의 정책에 근거하여 RBAC 시스템을 통해 접근을 통제하여 정보를 보호한다.

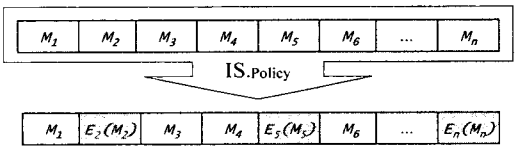

그림 9. 개인정보 등록
Fig 9. Personal Information Registration

3.3.2 정보 검색

정보사용자의 역할과 개인별 정책에 의해 접근할 수 있는 정보가 제한될 수 있다. 역할이나 정책 등에 의해 정보목록이 선택되어지는 필터링함수(fr_{pL})를 식(3.3.1)과 같이 정의한다.

$$fr_{pL} : A \rightarrow fr_{pL}(A) = A \cap pL \quad \cdots\cdots\cdots\cdots (3.3.1)$$
(단, A : 속성정보목록 식별자 집합)

〈그림 10〉에서는 정보 사용자가 정보주체(IS)의 개인정보를 검색하는 과정을 나타낸 것이다. 정보사용자(IU)가 IS의 정보를 검색하는 과정은 다음과 같다.

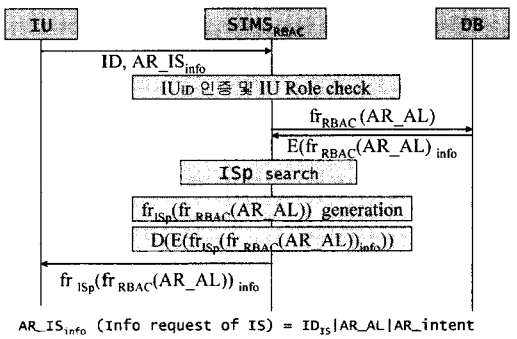

그림 10. 특정인의 정보 검색
Fig 10. Information Retrieval

① 정보사용자는 SIMS에게 자신의 ID와 함께 검색할 정보항목(AR_ISinfo:Access Request_IS information)를 제공

한다. AR_ISinfo에는 검색할 정보주체 ID와 요청정보목록(AR_AL:Access Request_attribute List), 정보요청목적(AR_intent)으로 구성되어 있다. AR_intent는 목적에 부합되는 정보를 정보사용자에게 제공하지 않기 위함이다.

$IU \rightarrow SIMS$: $[IU_{ID} | AR\_IS_{\infty o}]$

② SIMS는 제공 받은 정보사용자 ID를 인증하고 정보사용자의 역할을 확인한다.

③ SIMS는 RBAC시스템에서 정의된 IU의 역할에 따라 접근할 수 있는 정보목록을 추출하여 DB에 제공한다.

$$fr_{RBAC}(AR\_AL) = AR\_AL \cap AL_{RBAC}$$
$$where\ \ AL_{RBAC}: access\ list\ by\ IU's\ role$$

④ DB는 $fr_{RBAC}(AR_AL)$에 해당되는 암호화된 정보를 SIMS에 제공한다.

$$DB \rightarrow SIMS: [E(fr_{RBAC}(AR\_AL)_{info})]$$
$$E(fr_{RBAC}(AR\_AL)_{info}) = \bigcup_{i=1}^{n} E_{fr_{RBAC}(AR\_AL)}(M_i)$$

⑤ SIMS는 ISp를 조회한다.

⑥ SIMS는 $fr_{RBAC}(AR_AL)$에서 ISpL(ISp에 기록된 속성정보 목록)에 의해 필터링된 개인정보목록($fr_{ISpL}(fr_{RBAC}(AR\_AL))$)을 생성하고 그 목록에 대한 속성정보를 복호화 한다.

⑦ SIMS는 IU가 요청한 정보중에 프라이버시 정책들에 의해 필터링된 정보만을 안전한 채널을 통해 제공한다.

3.3.3 개인정보 수정

〈그림 11〉는 개인정보 주체가 자신의 정보를 수정하는 과정을 나타낸 것이다. 정보 주체(IS_k)가 자신의 정보를 수정하는 과정은 다음과 같다.

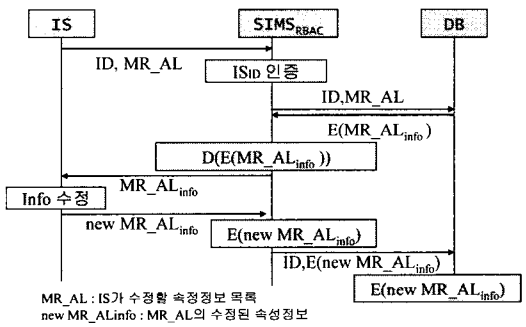

그림 11. 개인정보 수정
Fig 11. Personal Information Modification

① 정보주체가 ID와 정보수정요청항목리스트(MR_AL:Modification Request Attribute information List)를 SIMS에게 제공한다.

② SIMS는 정보주체 ID를 인증한다.

③ SIMS는 DB에 ID와 MR_AL를 제공한다.

④ DB는 SIMS에게 ID의 MR_AL에 해당되는 암호화된 정보(E(MR_ALinfo))를 제공한다.

⑤ SIMS는 암호된 정보를 복호화한다.

⑥ SIMS는 복호화된 수정할 정보를 안전한 채널을 통해 IS에게 제공한다.

⑦ IS는 이전 정보(MR_ALinfo)를 새로운 정보(new MR_ALinfo)로 수정한다.

⑧ IS는 수정된 정보(new MR_ALinfo)를 저장하기 위해 SIMS에게 안전한 채널을 통해 제공한다.

⑨ SIMS는 IS로부터 제공받은 정보를 암호화 한다.

⑩ SIMS는 정보주체의 ID와 함께 암호화된 정보를 DB에게 제공한다.

⑪ DB는 제공받은 정보(E(new MR_ALinfo))를 ID 확인 후 정보를 갱신한다.

3.3.4 개인 정보의 재암호화 및 정책변경

개인정보의 재암호화는 키의 유출이나 정보주체가 자신의 정보 변경시에만 이루어진다. 키의 유출시 민감한 정보를 복호화하여 새로 생성된 속성키로 민감한 정보를 재암호화해야 하며, 정보수정시에는 기존 속성키로 수정된 정보만을 재암호화한다.

개인별 정책은 개인의 상황에 따라 변경될 수 있다. 즉 정보주체가 건강이 양호할때는 건강정보는 민감하지 않지만 질환이 발생시에는 해당 정보는 민감한 정보가 될 수 있다. 정보사용자에게 부여했던 접근권한을 수정해야 할 경우 정보 주체는 SIMS에게 정보주체의 정책변경을 요청한다. SIMS는 수정된 정책을 확인하여 추가된 민감한 정보가 있을 경우 해당 정보를 암호화하여 DB에 저장한다.

IV. 시나리오 및 비교 평가

4.1 시나리오

〈그림 12〉은 정보사용자가 DB에 있는 Table T에서 "김대수"의 정보에 대한 검색과정을 도식화한 것이다. 정보사용자인 보험설계사가 보험설계를 목적으로 SIMS에 김대수의 개인정보 접근요청을 하고 있다. 김대수는 자신의 개인별 정책에서 민감한 정보로 질병, 나이, 직업을 지정하여 DB에 암호화되어 저장되어 있다.

SIMS는 정보사용자의 역할(보험설계사)을 확인 후에 접근할 수 있는 정보목록(이름, 나이, 질병, 성별, 직업)중에 김대수의 개인별정책에서 보험설계사에게 민감한 정보라 암호화되어 있는 나이 정보를 비롯하여 이름과 성별 정보를 제공한다. Table T를 보면 홍길동과 같이 건강할때는 질병정보가 민감하지 않아 암호화할 필요성이 없지만 김대수는 당뇨이기 때문에 질병정보가 민감한 정보이므로 암호화하여 관리하고, 주치의에게만 그 정보를 공개할 것이다.

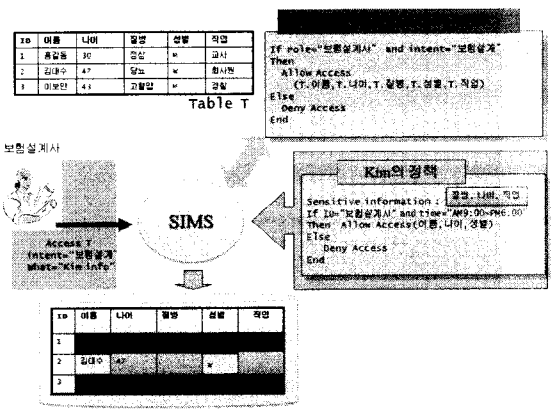

그림 12. 병원 시나리오
Fig 12. Scenario in the hospital

4.2. 기존 접근제어와의 비교 평가

개인정보의 접근측면에서 기존 역할기반 접근제어기법과 2가지 측면에서 비교하고자 한다. 개인의 민감한 정보가 많고, 보호가 필요한 병원을 대상으로 비교분석한다.

첫째, 제안모델은 정보주체가 자신의 정보에 대한 접근을 필요에 따라 제한할 수 있다. 기존 접근제어 모델에서는 기관이 지정한 역할에 따른 정보 접근을 일방적으로 결정한다. 이로 인해 개인의 정보가 주체의 동의 없이 무분별하게 사용되는 사례가 발생된다. 제안모델에서는 역할 R에 대한 접근허가 aP(r)에 개인별 정책 SP을 반영한 접근허가로 식(4.2.1)과 같이 표현된다.

$$aP(r)|_{SP} = aP(r) \cap SP \quad \cdots\cdots (4.2.1)$$

이로 인해 제안모델은 정보주체인 개인에게 자신의 정보에 대한 제어를 갖게 된다.

둘째, 제안모델은 주치의와 같이 이미 알고 있는 정보사용자에게 가족력이나 진료정보를 추가적으로 제공하고자 한다. 하지만 기존 접근제어에서는 동일한 역할이라면 접근권한도 동일하게 제공되어 특정 사용자에게 접근권한 추가할 수 없다. 동일한 역할에 접근권한을 확대하면 무분별한 접근이 가능해져 프라이버시침해가 발생한다. 제안모델에서는 특정사용자 u′ 의 역할 r에 의한 접근허가 aP(r)과 정보주체가 추가로 제공한 접근허가 $P^*(u')$에 대해 특정사용자의 접근허가는 식(4.2.2)와 같이 표현한다.

$$aP(r) \cup P^*(u') \quad \cdots\cdots (4.2.2)$$

제안모델은 주어진 역할에 따른 접근권한을 제한이 가능하고 특정 사용자에게 접근권한을 추가적 제공이 가능하므로 개인정보에 대한 세밀한 접근제어가 가능하다.

V. 결론

기관의 프라이버시 정책에 따라 접근제어와 암호화 기술을 이용하고 있지만 정보주체의 다양한 요구에 만족시키지 못하고 있다. 현 시스템은 평문상태로 저장되어 유출시 피해가 크고, 정보사용자의 무분별한 접근을 정보주체가 통제할 수 없다. 이 논문에서는 DB에 저장되어 있는 개인정보를 개인별 정책에 따라 민감한 정보를 암호화하므로써 추가적으로 보호하면서 개인별 정책에 의해 정보접근이 가능한 접근제어모델을 소개하였다. 기존의 RBAC시스템에 적용가능한 접근제어 모델을 제안하여 개인정보 검색 및 사용에 있어 효율성을 높이고자 하였다.

제안 모델은 RBAC시스템이 적용된 병원, 은행, 법률사무소와 같은 기관에서 활용도가 크다. 기업의 합병 또는 기관의 통합으로 인하여 각기 저장된 개인정보 DB을 효과적이면서 프라이버시 침해 없이 통합할 수 있는 연구가 필요하다.

참고문헌

[1] 양형규, 이강호, 최종호,"국내 검색엔진을 이용한 개인정보 해킹에 관한 연구" 한국컴퓨터정보학회, 제12권3호, 2007
[2] OECD, 2001, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www1.oecd.org/publications/e-book/9302011E.PDF
[3] W. Stallings, Cryptography and Network Security, ISBN 0-13-091429-0.

[4] M.C. Mont, S. Pearson, and P. Bramhall., "An Adaptive Privacy Management System For Data Repositories," TrustBus2005(LNCS 3592), pp.236-245, 2005.
[5] S.Sessay, Z. Yang, J. Chen and D. Xu, "A Secure Database encryption scheme," second IEEE Consumer Communications and Networking Conference, pp.49-53, 2005.
[6] H.J. Mun, K.M. Lee and S.H. Lee, "Person-Wise Privacy Level Access Control for Personal Information Directory Services," EUC2006(LNCS 4096), pp.89-98, 2006.
[7] Hyung-Jin Mun, Nam-Kyoung Um, Ning Sun, Yong-Zhen Li, Sang-ho Lee, "Subject-wise Policy based Access Control Mechanism for Protection of Personal Information," ICCIT2007(IEEE CS), pp. 2242-2247, Nov 2007.
[8] 문형진, 이건명, 이영진, 이동희, 이상호, "암호기법을 이용한 정책기반 프라이버시보호시스템 설계," 정보보호학회, 제16권 2호, pp. 33-44, 2006년 4월
[9] 문형진, 김기수, 엄남경, 이영진, 이상호,"민감한 개인정보보호를 위한 효율적인 접근제어기법",한국통신학회,제32권7호, 2007.7
[10] 문형진, "주체정책을 반영한 역할기반 개인정보 보호기법," 박사학위논문, 충북대학교 대학원, 2008년 2월
[11] D. F. Ferraiolo, D. R Kuhn, "Role-Based Access Control," Poceedings of the 15th National Computer Security Conference, pp. 554-563, 10. 1992.
[12] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role- Based Access Control Models," IEEE Computer, Vol29, No2, pp38-47. 1996.
[13] D.F.Ferraiolo, J.F.Barkley,D.R.Kuhn,"A Role Based Access Control Model and Reference Implementation within a Corporate Intranet", ACM Transactions on Information and System Security,1999
[14] Joon S. Park, Ravi Sandhu, Gail-Joon Ahn, "Role-based Access Control on the Web" ACM Transactions on Information and System Security, Vol 4 No.1 pp.37-71, Feb.2001

저 자 소 개

문 형 진 (Hyung-Jin Mun)

1996년 2월 충남대학교 수학과 졸업
2002년 2월 충남대학교 수학과 이학석사 졸업
2008년 2월 충북대학교 전자계산학과 이학박사
2008년 3월 ~ 현재 충북대학교 초빙전임강사
〈관심분야〉 개인정보보호, 접근제어, 네트워크 보안

서 정 석 (Jung-Seok Suh)

1987년 9월 Drexel University MBA(MIS) 졸업
1990년 1월 Boston University Computer Science 졸업
2000년 8월 국민대학교 정보관리학 박사
1999년 ~ 현재 나사렛대학교 정보통신학과 부교수
〈관심분야〉 정보관리