민감한 개인정보 보호를 위한 효율적인 접근제어 기법

정회원 문 형 진*, 준회원 김 기 수*, 정회원 엄 남 경*, 준회원 이 영 진*, 정회원 이 상 호**°,

Effective Access Control Mechanism for Protection of Sensitive Personal Information

Hyung-Jin Mun* ***Regular Member***, Ki-Soo Kim* ***Associate Member***, Nam-kyung Um* ***Regular Member***, Yong-Zhen Li* ***Associate Member***, Sang-ho Lee**° ***Regular Member***

요 약

은행, 병원과 같은 기관이나 기업은 효율적인 개인별 서비스를 위해 정보주체의 동의하에 개인정보를 수집·관리하고 있다. 저장된 개인정보는 정보주체마다 민감도의 차이가 존재한다. 같은 속성정보 누출시 개인이 느끼는 민감도에 따라 프라이버시 침해정도가 다르다. 그러나 현재 기관이나 기업에서 민감도에 상관없이 일괄적으로 보호하고 있다. 이 논문에서는 정보주체의 민감한 정보 항목을 개인별정책에 반영하고 개인에 의해 지정된 민감한 개인정보 접근에 대해 엄격하게 제한하는 프라이버시 정책 기반의 접근제어 기법을 제안한다. 제안 기법에서 개인정보는 정보주체별로 각기 다른 키로 암호화하여 데이터베이스에 저장된다. 정보주체는 자신의 민감한 정보의 접근권한에 대한 정책을 세우며, 개인별정책과 기관 프라이버시정책에 따라 허가된 정보사용자에게 정보를 제공하므로 써 정보 접근의 통제가 가능하다.

Key Words : SIMS, Access Control, Sensitive Personal Information, Privacy, Information Encryption

ABSTRACT

In order to provide the efficient personalized services, the organizations and the companies collect and manage the personal information. The stored data have some slight differences among each subject. Even though the same attribute information leaks out, the personal privacy violation is different according to personal sensitivity. However, currently the organizations or the companies protect all the information as the same level. This paper reflects the sensitive attribute information of the information subject to each personal policy by the encrypting techniques. And then we propose a policy-based access control mechanism for the personal information which strictly prevents unauthorized information users from illegally accessing the personal information. In the proposed mechanism, the individuals' personal information which is encrypted with different keys is stored into the database. For the access control, information subjects set up their own access control policy for their sensitive personal information. Then it is possible to control the information access by providing the information to the information users according to personal and organizational privacy policy.

Ⅰ. 서 론

은행이나 병원과 같이 개인의 민감한 정보를 수집, 저장하고 금융 및 진료 서비스와 같은 개인을 위한 개인별 서비스를 제공하기위해 개인정보를 사용하고 있다. 편리성과 효율성이라는 명목아래 개인

* 충북대학교 전산계산학과 네트워크 연구실 (jinmun@gmail.com)
** 충북대학교 전기전자컴퓨터학부 정교수 (shlee@cbnu.ac.kr) (°:교신저자)
논문번호 : KICS2007-03-127, 접수일자 : 2007년 3월 20일, 최종논문접수일자 : 2007년 7월 2일

정보 주체의 동의 없이 사용되며 이런 개인정보들이 유출되어 정보 주체에게 인권 침해 뿐만 아니라 경제적 피해까지 준다. 최근 프라이버시 침해 사례들이 매스컴을 통해 전달되면서 개인정보 주체들은 프라이버시에 대한 관심이 고취되었고, 개인정보 보호를 위한 연구들이 접근제어 기술과 암호화 기술을 중심으로 활발하게 수행되고 있다.

개인정보보호를 위한 OECD 지침과 CSAPP (Canadian Standard Association's Model Code for the Protection of Personal Information) 에 보면 정보주체의 동의 없이 사용이나 이동이 금지되고 있고, 이를 위해 기관이나 기업은 정책에 의한 접근제어로 개인정보를 보호하고 있지만 정보 사용시 개인의 동의를 구하기 어렵다. 또한 개인마다 민감한 정보가 다르기 때문에 획일적인 보호가 아닌 개인의 요구에 따른 보호 및 저장된 개인정보 사용시 개인의 동의를 구하는 새로운 접근제어 기술이 필요하다.

이 논문에서는 정책에 근거한 접근제어와 암호화 기술을 이용하여 개인이 지정한 민감한 정보를 각기 다른 키로 암호화시킴으로써 개인별 정책을 통해 무분별한 접근을 차단하여 정보 주체의 동의를 반영시킬 수 있다. 즉 민감한 정보를 개인별 정책에 반영하여 이를 암호화 기술로 보호하고, 정보주체의 정책에 부합할 경우에만 접근할 수 있는 접근제어 모델을 제안한다. 이 논문의 구성은 다음과 같다. Ⅱ장에서는 개인정보 보호기술들을 살펴보고, Ⅲ장에서는 민감한 정보 관리 시스템(SIMS : sensitive information management system)을 소개하고, Ⅳ장에서는 Ⅲ장에서 소개한 SIMS의 동작과정과 프라이버시 보안 요구사항에 대한 평가를 한 뒤 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 관련 연구

P3P(Platform for Privacy Preference)는 W3C(the World Wide Web Consortium)에서 기존의 OPS (Open Profiling Standard) 기술의 Collaborative Filtering과 RDF(Resource Definition Framework) 애플리케이션에서 XML (eXtensible markup language) 등장과 함께 이를 혼합적용하기 위해 고안되었다. P3P는 웹사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨주는 것이며 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어 진 것이다. 따라서 P3P의 기능은 웹 브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자가 이미 설정해 놓은 정보공개 수준과 비교하여 정보를 선별적으로 제공함으로써 어떠한 때에 개인정보를 제공해야 하는지 이용자가 선택과 결정을 하는데 도움을 준다[1].

XACML(eXtensible Access Control Markup Language)은 OASIS(Organization for the Advancement of Structured Information) 표준중의 하나로 접근제어정책을 통해 보안이 요구되는 자원에 대한 미세한 접근제어 서비스를 제공할 수 있는 XML 기반의 언어이다. XACML은 SAML (Security Assertion Markup Language) PDP의 일부로서 역할을 수행할 수 있다. XACML의 정의에 따라 각각의 사용자 별 XML문서 접근정책을 수립하고 적용할 수 있다. XACML은 2005년 2월 XACML v2.0표준이 완성되었다[2].

접근제어기술는 권한이 있는 사용자에게만 접근을 허용하는 기술로 강제적 접근제어(MAC : Mandatory Access Control)과 임의적 접근제어(DAC : Discretionary Access Control)같은 고전 접근제어기술이 있으나 복잡해지는 기관이나 기업의 다양한 정책이나 관리를 위해 사용하기가 부적합하다. 기관이나 기업에 적용될 수 있는 역할기반 접근제어(RBAC : Role-based Access Control)가 R.Sandhu, E.Coyne, H.Feinstein, and C.Youman에 의해 제안되었다. 역할기반 접근제어는 복잡한 조직의 구조에 자연스럽게 매핑시켜 기관이나 기업마다 서로 다른 보안 요구사항들과 정책들의 요구를 만족시킬 수 있다. RBAC은 사용자의 역할에 맞는 권한을 부여하므로써 역할에 맞지 않은 데이터에 대해 접근을 통제하는 기술이다[3~7].

암호화 소프트웨어는 암호화를 통해 자신의 전자메일 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공한다. 키를 가지고 있는 당사자만이 암호화된 정보를 접근할 수 있다[8]. 암호화 기술을 이용한 개인정보를 보호하는 연구들이 진행되고 있다[9~11]. HP Lab[9]에서는 DB안에 프라이버시정책과 관련패키지를 암호화된 개인정보와 함께 저장한다. 저장된 프라이버시정책과 부합할 경우에만 복호화키를 제공하므로써 개인정보를 보호하고 있지만 대량의 개인정보를 저장될 경우 복잡한 구조로 인해 효율성 떨어진다. P^2MS[10]는 개인의 모든 정보를 암호화하여 DB에 저장하고, 정보주체의 개인별정책을 통해 사용자 접근을 통제함으로써 DB관리자를 비롯한 정

보 사용자로 부터 보호하고자 하였다. Sesay,S.[11]에 의해 제안된 기술은 개인정보를 민감한 정보(private data), 분류된 정보(classified data), 분류되지 않은 정보(unclassified data)로 나누어 민감한 정보와 분류된 정보만을 각기 다른 키를 이용하여 암호화하여 DB에 저장하였다. 개인마다 민감한 정보가 다름에도 불구하고 이를 반영하지 못하였고, 적용된 접근제어기술 역시 기관의 복잡한 조직에 적합하지 않은 MAC기술을 사용하였다.

Ⅲ. SIMS를 이용한 접근제어모델

이 장에서는 정보사용자로부터 개인이 추가적으로 보호를 받기 원하는 정보 즉 개인의 민감한 정보를 보호하기 위한 접근제어 모델을 제안한다. 이 모델은 SIMS를 이용하여 정보 주체가 자신의 정보 접근에 관한 정책을 세우고 그 정책에 따라 접근제어하므로써 정보사용자로부터 민감한 개인정보를 보호한다.

3.1 적용환경

개인은 기업이나 기관에 자신의 정보를 민감한 정보와 그렇지 않은 정보를 구분하여 제공하며, 제공된 정보는 DBMS에 의해 관리되고 있다. 정보사용자는 제공된 정보를 사용 목적에 따라 개인정보를 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.

3.2 개인별 정책에 의한 접근제어 모델

그림 1은 민감한 개인정보를 개인별 정책에 의한 보호하는 프레임워크이다. 정보주체가 제공한 정보를 SIMS를 통해 DB에 저장하고 정보사용자는 SIMS을 통해 저장된 정보를 접근할 수 있다. SIMS의 구성요소는 그림 1에서 보듯이 크게 인증모듈, pDB(policy Database), Enc/Dec 모듈, 키관리모듈로 이루어져 있다.

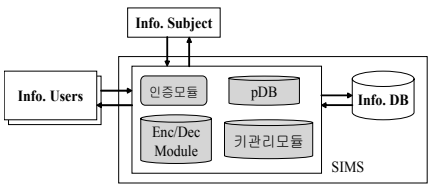


그림 1. 프레임워크

3.2.1 인증모듈

인증 모듈은 SIMS 접근자의 인증을 담당한다. 인증은 정보를 제공하거나 수정하는 정보주체의 인증과 정보사용을 목적으로 접근하는 정보사용자의 인증이 있다.

3.2.2 pDB

pDB는 ISpDB(정보주체의 개인별정책 DB)와 EPp(기관이나 기업내의 프라이버시 정책)으로 나눈다. EPp는 프라이버시 관련 제도나 법규에 의해 세워지고 정책안에 보호해야 할 정보의 항목들을 지정한다. ISp(개인별 정책)은 자신의 정보에 대해 민감한 정보와 그렇지 않은 정보를 구분하고, 민감한 정보에 대해서 정보사용자별로 접근여부를 결정하는 정책이다.

3.2.3 암·복호화모듈

암호화모듈은 정보 주체가 제공한 정보중 EPp과 ISp에서 민감한 정보로 지정된 정보를 암호화하는 모듈로 키DB에서 생성된 키를 이용하여 정보속성마다 암호화하여 개인정보DB에 제공한다. 접근자에 정당한 요구에 따라 암호화된 정보를 복호화하는 모듈이다. 복호화된 정보는 안전한 채널을 통해 접근자에게 제공한다.

3.2.4. 키관리모듈

키관리모듈은 키생성모듈과 키DB 2가지로 구성된다. 민감한 개인정보를 안전하게 보호하기 위해 SIMS는 개인의 각 속성정보를 암호화하기 위해 많은 키들이 필요하다. 키생성모듈은 개인별로 마스터키을 생성하고, 마스터키로부터 개인의 속성정보를 암호화하기 위해 민감한 정보의 수만큼 암호화키(속성키)를 생성한다. 정보 요청시 SIMS은 마스터키로부터 요청 정보에 대한 속성키를 생성하여 암호화된 요청정보를 복호화하여 정보사용자에게 제공한다. 키DB는 키생성모듈을 통해 생성된 개인별 마스터 키들을 안전하게 저장하는 공간이다.

3.3 개인정보 구조

개인정보 DB는 개인정보를 저장하는 곳으로 민감한 정보는 암호화되어 있고, 그렇지 않은 정보는 평문상태로 저장되어 있다. 암호화된 정보의 경우 개인마다 속성마다 다른 키를 이용하여 암호화 되어 있고, 그 키는 SIMS에서 관리되고 있다. DB에 저장된 정보는 SIMS에 의해서만 정보를 제공하거나 제공받는다.

개인정보 주체가 그림 2 (a)와 같이 자신의 정보를 제공한다. 제공된 정보는 ISp과 EPp에 따라 민감한 정보가 결정되고 SIMS을 통해 Info.DB에 저장된다. 그림 2 (b)은 속성정보 M_2, M_3, M_5, M_n 은 ISp와 EPp에 의해 결정된 민감한 정보를 나타내고 있다.

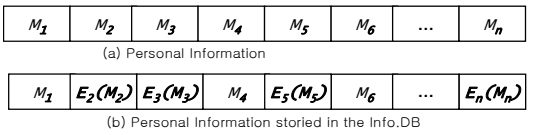


그림 2. Info.DB에 저장된 개인정보 구조

Ⅳ. 제안모델에서의 프로토콜

동작과정기술의 가독성을 위하여 그림 3과 같이 표기법을 정의한다.

4.1 키관리

개인정보를 안전하게 보호하기 위해 키관리가 필요하다. 키생성모듈을 통해 개인마다 마스터키 MK_{IS_i}를 생성한다. 개인의 민감한 속성정보를 암호화하기 위해 민감한 정보 수만큼 속성키가 필요하다. 정보주체 식별자 ID_i와 민감한 속성정보의 식별자 A_j라 할 때 속성키는 다음과 생성한다.

$$key_{ij} = E_{MK_{IS_i}}(ID_i \oplus A_j)$$

생성된 속성키는 대칭키 암호알고리즘을 이용하여 속성정보를 암호화하는데 사용하고 개인별 마스터키만을 키 DB에 저장한다. 정보사용자의 정보요청시 저장된 마스터키로부터 속성키를 생성하여 암호화된 민감한 정보를 복호화하여 그 정보를 정보사용자에게 제공한다. 키 DB에 저장된 키는 마스터키로서 정보를 제공한 정보주체의 수와 같고, 마스터키는 오직 속성키를 생성할 때만 사용되어 안전하다.

IU : 정보사용자 , IS : 정보주체
IS_{info} : 정보주체의 개인정보
HL : 정책에 따른 속성정보목록
EP_pL : 기관의 프라이버시 정책에 따른 속성정보목록
IS_pL : 정보주체의 정책에 따른 속성정보목록
$M = M_1 \| M_2 \| \cdots \| M_n$: 개인속성정보
$A = \{A_i \mid 1 \le i \le n\}$
: 개인정보의 속성정보 목록집합
PL : 정책에서 지정한 정보 목록
$fr\_IS_{info} = IS_{info}|_{EPp \wedge ISp}$
: EPp와 ISp 정책에 의해 필터링된 개인정보
$fr\_IS_{info}L$: fr_IS_{info} 의 속성정보 목록
IU_{ID}: 정보사용자 식별자, IS_{ID} : 정보주체 식별자
[]: 메시지전송
K : 키 , $E()$: 암호화 , $D()$: 복호화

그림 3. 약어 설명

4.2 개인정보 등록

정보 주체는 n개의 속성정보를 SIMS에 제공하고, SIMS는 개인별 성향에 따라 자신이 지정한 민감한 속성정보와 기관의 프라이버시 정책에 입각하여 민감한 정보를 암호화한다. 즉 그림 4과 같이 ISp와 EPp 두 가지 정책에서 지정된 속성정보만을 암호화한다. 정보 주체의 개인정보 M에 대해 암호화해야 할 정보는 다음과 같이 정의한다.

$$E_{PL}: M_i \rightarrow E_{PL}(M_i) = \begin{cases} E(M_i) & i \in PL \\ M_i & i \notin PL \end{cases}$$

이를 통해 정보주체인 개인은 자신의 정보사용에 대한 통제권을 반영할 수 있고, 개인이 지정하지 않은 정보에 대해 추가로 기관에서 중요한 정보를 암호화하여 보호한다.

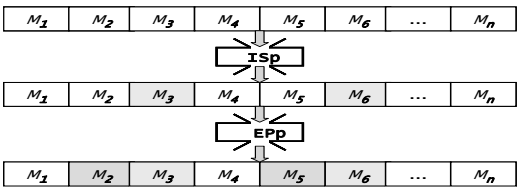


그림 4. 개인정보 등록

4.3 정보 검색

그림 5에서는 정보 사용자가 정보주체 IS의 개인정보를 검색하는 과정을 나타낸 것이다.

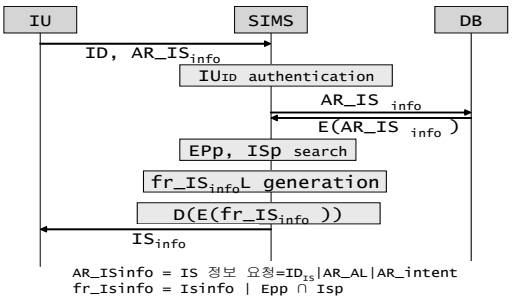


그림 5. 특정인의 정보 검색

정보사용자가 IS의 정보를 검색하는 과정은 다음과 같다.

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

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

② SIMS는 제공 받은 정보사용자 ID를 인증한다.

③ SIMS는 DB에 AR_ISinfo를 제공한다.

④ DB는 AR_ISinfo에 해당되는 암호화된 정보(E(AR_ISinfo))를 SIMS에 제공한다.

⑤ SIMS는 EPp, ISp를 조회한다.

⑥ SIMS는 AR_AL에서 EPp, ISp에 의해 필터링된 개인정보목록을 생성하고 그 목록에 대한 정보를 복호화 한다.

$SIMS: D(E(fr\_IS_{info}), fr\_IS_{info})$

⑦ SIMS는 IU가 요청한 프라이버시 정책들에 의해 필터링된 정보만을 제공한다.

4.4 개인정보 수정

그림 6는 개인정보 주체가 자신의 정보를 수정하는 과정을 나타낸 것이다.

정보 주체(IS_k)가 자신의 정보를 수정하는 과정은 다음과 같다.

① 정보주체가 ID와 정보수정요청항목리스트(MRAL)를 SIMS에게 제공한다.

② SIMS는 정보주체 ID를 인증한다.

③ SIMS는 DB에 ID와 MRAL를 제공한다.

④ DB는 SIMS에게 ID의 MRAL에 해당되는 암호화된 정보(E(MRALinfo))를 제공한다.

⑤ SIMS는 암호된 정보를 복호화한다.

⑥ SIMS는 복호화된 수정할 정보를 IS에게 제공한다.

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

⑧ IS는 수정된 정보(new MRALinfo)를 저장하기 위해 SIMS에게 제공한다.

⑨ SIMS는 IS로부터 제공받은 정보를 암호화 한다.

⑩ SIMS는 정보주체의 ID와 함께 암호화된 정보를 DB에게 제공한다.

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

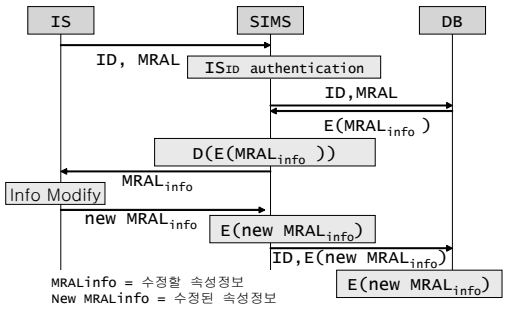


그림 6. 개인 정보 수정

4.5 개인 정보의 재암호화

개인정보의 재암호화는 정보주체가 자신의 정보 변경시와 키의 유출이 발생할 경우에만 이루어진다. 키의 유출이 아닌 개인정보 변경시에는 기존 암호화키를 이용하여 암호화하여도 안전한 SIMS에서 키를 관리하기 때문에 개인정보는 안전하다.

4.6 정책 등록 및 변경

정보 주체가 자신의 정보에 대한 접근을 제어할 수 있는 정책을 생성한다. 즉 자신의 정보를 기관이나 기업에게 제공하기 전에 정책을 세워 그 정책에 맞게 자신의 정보를 사용할 수 있도록 한다. 효과적으로 정책을 세우기 위해 기관은 정보주체에게 그림 7과 같이 정보사용자 그룹 카테고리를 제공하고, 정보 주체는 카테고리를 이용하여 그룹별로 접근권한을 부여하고, 정보주체인 개인이 이미 알고 있는 특정사용자에 대한 접근권한을 구분하여 정책을 생성한다. 개인별정책에서 정보주체가 알고 있는 사용자의 정책이 사용자그룹별 접근권한과 충돌시 특정 사용자에 대한 접근권한이 우선한다.

정보 주체의 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

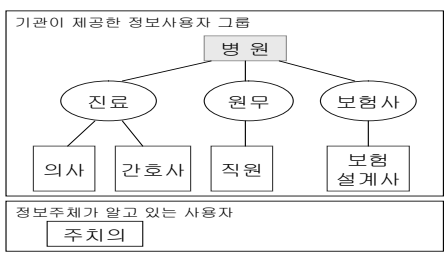


그림 7. 정보사용자 그룹별 카테고리

SIMS에게 정보주체의 정책변경을 요청한다. SIMS는 수정된 정책을 확인하여 추가된 민감한 정보는 암호화하여 DB에 저장한다.

4.7 프라이버시 보안 분석

개인정보보호를 위한 접근제어 기법을 위해서는 정보사용시 주체에 의한 동의, 정보사용을 위한 편이성, 보호를 위한 효율성 평가등이 필요하다.

1) 정보주체의 동의: 개인별정책을 통해 민감한 정보를 지정하고 이를 접근할 수 있는 정보사용자를 결정하여 동의가 있을 경우에만 접근을 허용한다.
2) 정보사용의 편이성: 민감한 정보만을 암호화하므로써 암복호화하는 시간이 단축되어 합법적인 정보사용자에게 빠른 정보제공이 가능하다.
3) 보호를 위한 효율성: 암호화키는 개인정보보호를 위한 핵심요소이다. 키유출시에만 마스터키를 변경하여 불필요한 키변경은 없다.
4) 정보 재암호화: 저장된 정보에 대한 재암호화는 정보변경시에만 한다.

표 1. 기존기법과의 프라이버시 보안 분석

	HP	P²*MS*	Sesay	제안 기법
주체동의	○	○	×	○
정보사용 편이성	△	△	○	○
키변경	매번	매번	매번	유출시
재암호화	정보 정책	정보 정책	정보 정책	정보

표 1은 기존기법과 비교분석한 결과이다. Sesay[11] 기법은 정보주체의 동의를 구하지 않고, 기관에 의해 결정된 정보만을 보호하는 기법이다. HP[9], P²MS[10]기법은 모든 정보를 암호화하기 때문에 정보사용에 대한 편이성이 다른 기법보다 떨어진다. 기존기법은 암호화키를 정책에 부합하는 정보사용자에게 제공하고, 정보사용 종료시마다 키변경 및 재암호화를 해야한다. 제안기법에서는 키유출시 키변경과 재암호화를 하고, 정보변경시에는 재암호화만 하므로 정보사용에 효율적임을 알 수 있다.

V. 결 론

기관이나 기업들은 여러 가지 목적으로 개인정보를 수집하여 저장된 DB에 대해 기관별 정책을 이용한 접근제어와 암호화 기술을 이용하고 있지만 정보주체의 다양한 요구에 만족시키지 못하다. 그러나 개인정보보호 관련 법률이나 제도는 정보 주체의 동의 및 제어 권한을 주체에게 제공할 것을 계속적으로 요구하고 있다.

이 논문에서는 DB에 저장되어 있는 개인정보를 개인별 정책을 이용하여 개인의 동의를 구하고, 정책에 입각하여 접근제어하므로써 자신의 정보를 보호할 수 있는 모델을 제안하였다. 이 모델은 정보수집과정에서 개인마다 민감한 정보가 다르므로 민감한 정보만을 암호화하므로 정보검색 및 정보사용에 있어 효율성을 높이고자 하였다.

제안 모델은 진료정보와 같이 민감 정도가 개인마다 차이가 있는 기관에서 활용도가 크다. 향후 연구로는 민감정도를 측정하고, 민감정도에 따른 보호을 위한 접근제어기술에 대한 연구가 필요하다.

참 고 문 헌

〔1〕 W3C, Platform for Privacy Preference(P3P) version1.1, http://www.w3c. org/P3P

〔2〕 OASIS, eXtensible Access Control Markup Language(XACML) version 2.0. OASIS, Feb. 2005.

〔3〕 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.

〔4〕 P.K.Thomas, and R.S.Sandhu, "Task- based Authorization Control(TBAC) : A Family of Models for Active and Enterprise-oriented Authorization Management," *Proc of the IFIP WG11.3 Workshop on Database Security*. 1997.

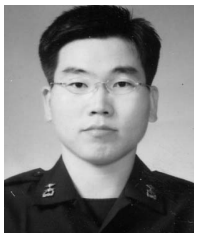
〔5〕 S. Oh, and S. Park, "An Integration Model of Role-based Access Control and Activity-based Access Control Using Task," *Proc. of 14th Annual IFIP WG11.3 Working Conference on Database Security*, Aug. April. 2000.

〔6〕 S. Oh and S. Park "Task-Role Based Access Control(T-RBAC): An Improved Access Control Model for Enterprise Environment", *Proceedings of the 11th International Conference on Database and Expert Systems Applications*, pp. 264-273, 2000.

〔7〕 E. Bertino, P.A. Bonatti and E. Ferrari, TRBAC: A Temporal Role-Based Access Control Model, *ACM Trans. Information and*

System Security, vol. 4, no. 3, pp. 191-233, Aug. 2001.
〔8〕 W. Stallings, Cryptography and Network Security, ISBN 0-13-091429-0.
〔9〕 M.C. Mont, S. Pearson, and P. Bramhall., "An Adaptive Privacy Management System For Data Repositories," *TrustBus*2005(LNCS 3592), pp.236-245, 2005.
〔10〕 H.J. Mun, K.M. Lee and S.H. Lee, "Person-Wise Privacy Level Access Control for Personal Information Directory Services," *EUC*2006(LNCS 4096), pp.89-98, 2006.
〔11〕 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.

문 형 진 (Hyung-Jin Mun) 정회원



1996년 2월 충남대학교 수학과 졸업
2002년 2월 충남대학교 수학과 이학석사
2005년 8월 충북대학교 전자계산학과 박사수료
<관심분야> 프라이버시 보호

김 기 수 (Ki-Soo Kim) 준회원

2007년 2월 충북대학교 전기전자컴퓨터공학부 졸업
2007년 3월 충북대학교 전자계산학과 석사과정
<관심분야> Wibro 모바일네트워크, 정보보호

엄 남 경 (Nam-Kyoung Um) 정회원

1999년 2월 충북대학교 컴퓨터과학과 졸업
2002년 2월 충북대학교 전자계산학과 이학석사
2007년 8월 충북대학교 전자계산학과 이학박사

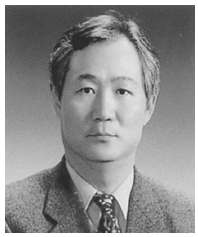
<관심분야> 네트워크 보안, 침입탐지 시스템

이 영 진 (Yong-Zhen Li) 준회원

1994년 6월 중국 연변대학교 물리학과 이학사
1997년 6월 중국 연변대학교 물리학과 이학석사
2007년 2월 충북대학교 전자계산학과 이학박사

2007년 3월~현재 충북대학교 초빙전임강사
<관심분야> 네트워크 보안, 유비쿼터스 보안

이 상 호 (Sang-ho Lee) 정회원



1976년 2월 숭실대학교 전자계산학과 졸업
1981년 2월 숭실대학교 전자계산학과 공학석사
1989년 2월 숭실대학교 전자계산학과 공학박사

1981년~현재 충북대학교 전기전자컴퓨터공학부 교수
<관심분야> 프로토콜 공학, 네트워크 보안 및 관리