情報保護學會論文誌
第16卷 第2號, 2006. 4

암호기법을 이용한 정책기반 프라이버시보호시스템설계*

문 형 진[1†], 이 건 명[1‡], 이 영 진[1], 이 동 희[2], 이 상 호[1]
[1]충북대학교, [2]극동정보대학

Design of a Policy based Privacy Protection System using Encryption Techniques*

Hyung-jin Mun[1†], Keon-myung Lee[1‡], Yong-zhen Li[1], Dong-heui Lee[2], Sang-ho Lee[1]
[1]Chungbuk University, [2]Keukdong College

요 약

기관이나 기업은 효율적인 개인별 서비스를 위해 정보주체의 동의하에 개인정보를 수집·관리하고 있다. 그러나 데이터베이스 관리자를 비롯한 정보사용자들은 저장된 개인정보를 무분별하게 접근하여 개인정보 오남용과 유출가능성을 높아지고 있다. 개인정보 보호를 위해 기관이나 기업이 자체 정책에 따라 개인정보에 대한 접근제어를 하는 시스템이라 할지라도 정보주체 자신의 정보에 대한 접근제어가 의도를 충분히 반영하기가 어렵다. 이 논문에서는 암호기법을 이용하여 정보사용자의 불법적인 접근을 차단하고 정보별로 접근제한을 할 수 있는 프라이버시 정책 기반의 접근제어 기법을 제안한다. 제안 기법에서 개인정보는 각기 다른 키로 암호화하여 데이터베이스에 저장된다. 정보주체는 자신의 정보 접근권한에 대한 정책을 세우며, 그 정책에 따라 정보사용자에게 키를 부여하므로써 정보 접근의 통제가 가능하다.

ABSTRACT

In order to provide the efficient personalized services, the organizations and the companies collect and manage the personal information. However, there have been increasing privacy concerns since the personal information might be misused and spread over in public by the database administrators or the information users. Even in the systems in which organizations or companies control access to personal information according to their access policy in order to protect personal information, it is not easy to fully reflect the information subjects' intention on the access control to their own personal information. This paper proposes a policy-based access control mechanism for the personal information which prevents unauthorized information users from illegally accessing the personal information and enables the information subjects to control access over their own information. In the proposed mechanism, the individuals' personal information which is encrypted with different keys is stored into the directory repository. For the access control, information subjects set up their own access control policy for their personal information, and the policies are used to provide legal information users with the access keys.

Keywords : P[2]MS, *privacy, access control, personal information*

Ⅰ. 서 론

정보통신기술의 발전과 사회가 다양해짐에 따라 새롭게 개인정보들이 생겨나고, 그 개념이 확장되고 있다. 개인정보를 이용한 전자상거래 및 개인별 서비스를 제공하고자 기관이나 기업들은 고객이나 직원, 파트너 등의 개인정보들을 요구한다. 개인별 서비스를 목적으로 저장된 개인정보들은 효율성이라는 명목아래 개인정보 주체의 동의 없이 사용되며 이런

접수일: 2005년 10월 26일; 채택일: 2006년 3월 31일
† 주저자. hjmun@cbnu.ac.kr
‡ 교신저자. kmlee@cbnu.ac.kr

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 암호화 기술과 접근제어 기술을 중심으로 활발하게 수행되고 있다.

개인정보보호를 위한 OECD 지침에 개인정보의 동의 없이 사용이나 이동이 금지되고 있고, 이를 위해 기관이나 기업은 정책에 의한 접근제어로 개인정보를 보호하고 있지만 정보 사용시 개인의 동의를 구하기 어렵다. 따라서 개인정보의 보호를 위하여 기관이나 기업이 저장된 개인정보 사용시 개인의 동의를 구하게 하는 새로운 접근제어 기술이 필요하다.

이 논문에서는 암호화 기술을 이용하여 개인정보 각 속성마다 각기 다른 키를 이용하여 암호화시킴으로써 개인별 정책을 통해 세밀한 접근제어를 가능해지고, 개인정보 사용시 정보 주체의 동의를 반영시킬 수 있다. 즉 개인별 정책을 기반으로 하여 접근권한을 부여할 수 있는 새로운 개인정보 보호를 위한 접근제어 모델을 제안한다. 제안 모델은 DB관리자조차도 정보 주체의 동의가 없으면 개인정보 속성이나 식별정보를 볼 수 없어 효과적으로 개인정보를 보호할 수 있다. 이 논문의 구성은 다음과 같다. 2장에서는 개인정보 보호를 위한 기술을 살펴보고, 3장에서는 개인별 정책기반 관리시스템(P^2MS: Personal Policy based Privacy Management System)을 소개하고, 4장에서는 3장에서 소개한 P^2MS의 동작과정과 프라이버시 측면에서 제안모델의 안정성 분석을 한 뒤 5장에서는 결론을 맺는다.

II. 관련연구

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. P3P시스템에서 이용자가 사이트를 검색할 때, 사용자측의 에이전트는 방문 사이트의 P3P 정책 파일을 요구하고 이에 대응하여 해당 사이트에서는 프라이버시 정책파일을 보내게 된다. 이 과정에서 이용자가 설정한 프라이버시선호수준과 방문한 웹사이트간에 협상하게 되고 만일 이용자가 설정한 기준에 맞게되면 요청된 웹 페이지가 전송되게 된다[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].

암호화 소프트웨어는 암호화를 통해 자신의 전자메일 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공한다. 한번 암호화가 이루어지면 오직 그 당사자만이 암호화된 정보에 대한 키를 가지고 그 정보를 접근할 수 있다. 암호화 소프트웨어는 하드디스크나 파일 암호화, 전자메일 암호화, 개인방화벽, 인증수단과 커뮤니케이션 도구 등 다양한 형태로 이용 가능하다[3].

강제적 접근제어(MAC : Mandatory Access Control)는 군사 환경이나 매우 제한적인 환경에서 제한된 수의 보안 관리자들에 의해 일정한 규칙에 따라 사용자의 정보에 대한 접근 권한을 통제하는 기술이다. 임의적 접근제어(DAC : Discretionary Access Control)는 각 정보의 소유자들이 그들 임의의 판단으로 접근 권한을 다른 사용자들에게 위임하거나 취소시킬 수 있어 강제적 접근제어보다 유연성이 있고, 분산된 접근제어 기능을 수행할 수 있다. 하지만 MAC와 DAC은 복잡해지는 기관이나 기업의 다양한 정책이나 관리를 위해 사용하기가 부

적합하다. 기관이나 기업에 적용될 수 있는 대안으로 역할기반 접근제어(RBAC : Role-based Access Control)가 제안되었다. R.Sandhu, E.Coyne, H.Feinstein, and C.Youman이 제안한 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[4]. 행위기반 접근제어(ABAC : Activity based Access Control)는 워크플로우(workflow)와 같은 협력 작업 환경을 위한 접근제어 기술이다[5]. 과업-역할기반 접근제어(TRBAC : Task -Role based Access Control)는 복잡한 구조 및 많은 사용자와 많은 양의 정보를 가진 기관이나 기업 환경에 맞는 접근제어 기술로 역할 기반 접근제어와 행위기반 접근제어를 통합한 기술이다[6-8].

HP 연구소에서는 기관이나 기업 내에서 저장되어 있는 대량의 개인정보 DB를 시스템적으로 보호할 수 있는 기술을 제안하였다[9]. 그림 1에서 보듯이 개인정보의 특정정보가 암호화되어 저장되고, 프라이버시 관리 서비스(Privacy Management Service)는 키를 소유하고 있다. 이 모델에서는 개인정보가 암호화 되어 있어 권한이 없는 사람들은 정보를 접근할 수 없고, 권한이 있더라도 정보 사용목적이 정책에 맞지 않으면 프라이버시 관리서비스에서 복호화 키를 제공하지 않기 때문에 안전하게 개인정보DB를 보호할 수 있다.

그러나 HP모델은 권한이 있는 정보 사용자가 기관의 정책에 맞으면 언제든지 정보주체의 동의 없이 원하는 정보를 접근할 수 있는 문제점이 있다. 또한 원하는 정보를 검색하기 위해 식별정보가 평문형태로 DB에 저장이 되어 있어 DB관리자의 무조건 접근이 가능하다.

Ⅲ. P²MS를 이용한 접근제어모델

이 장에서는 정보사용자로부터 개인정보 DB를 보호하기 위한 접근제어 모델을 제안한다. 이 모델은 P²MS를 이용하여 정보 주체가 자신의 정보에 대한 정책을 설정하고 그 정책에 따라 접근 제어하므로써 정보사용자로부터 개인정보를 보호한다.

3.1 적용환경

개인은 기업이나 기관에 개인정보를 제공하며, 제공된 정보는 DB 관리시스템에 의해 관리되고 있다. 정보 사용자는 제공된 정보를 사용 목적에 따라 개인정보를 접근한다. 개인은 자신의 정보를 사용할 수 있도록 정보 사용자에게 권한을 설정한다. 정보사용자에게 차등하게 권한을 설정하여 개인은 개인정보의 오용 및 유출을 막고자 한다.

개인정보 주체가 개인정보를 관리하는 기관이나 기업 내의 정보사용자별로 접근 가능한 정보항목을 결정하여 개인별 정책에 기록한다. 정보사용자는 개인별 정책에 의해 접근 가능한 정보가 지정되어 그 정보만을 접근할 수 있다. 그림 2는 정보사용자가 정보주체의 개인별 정책을 통해 부여된 권한을 가지고 개인정보에 접근한 모습을 나타낸다.

3.2 개인별 정책에 의한 접근제어 모델

그림 3은 정보주체가 제공한 정보를 안전하게 정보사용자에게 권한에 맞게 정보를 제공하는 제안 모델이다.

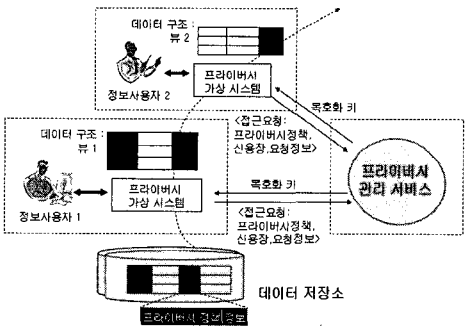


그림 1. HP 프라이버시 관리모델

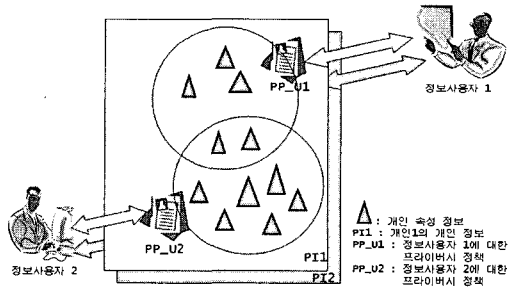


그림 2. 개인정보에 대한 정보사용자의 접근권한

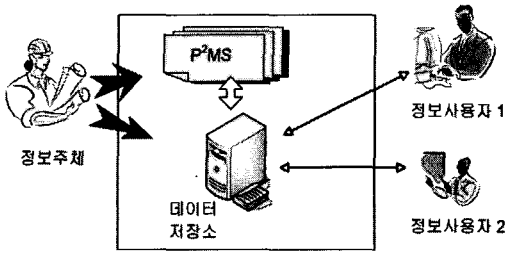


그림 3. 제안 모델

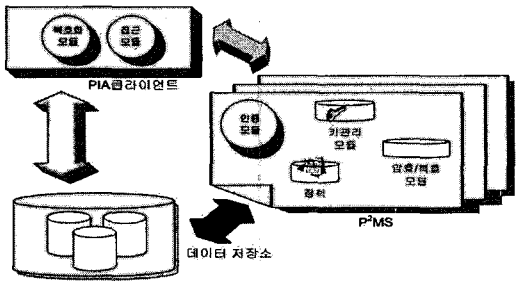


그림 4. 제안 모델의 구성요소

제안 모델은 그림 4에서 보듯이 크게 PIA 클라이언트(PIA : Personal Information Access), P²MS, 데이타저장소 3가지 구성요소를 가지고 있다.

3.2.1 PIA 클라이언트

정보 주체는 PIA 클라이언트를 이용하여 자신의 정보를 제공하고, 정보 사용자의 무분별한 접근을 막기 위해 개인별 정책을 세운다. 정보사용자는 PIA 클라이언트를 이용하여 자신을 인증하고, 원하는 개인정보를 요청하여 그 정보를 접근한다.

PIA 클라이언트는 접근모듈과 복호화모듈 2가지 모듈로 구성되어 있다.

접근모듈은 P²MS와 데이타저장소에 접근하는 모듈이다. P²MS에 접근하여 원하는 정보의 항목을 요청하고 복호화키를 가지고 오는 기능을 수행한다. 데이타저장소에 접근하여 원하는 정보 검색하여 암호화된 정보를 가지고 오는 기능을 수행한다.

복호화모듈은 요청한 정보를 복호화하는 모듈이다. P²MS에서 제공한 키를 이용하여 데이타저장소에서 제공받은 개인정보 암호문을 복호화하므로써 원하는 정보를 접근한다.

3.2.2 P²MS

PIA 클라이언트에서 개인이 세운 개인별 정책에 맞게 개인정보를 보호하고 관리하는 책임을 맡고 있다. P²MS는 PIA 클라이언트를 통해서만 접근이 가능하고 P²MS를 통해 정보사용자의 요청된 정보를 제공하는 기능을 하고 있다. P²MS는 인증모듈, 정책, 암·복호화모듈, 키모듈 4가지 기본 구성으로 되어 있다.

가. 인증과 정책

인증모듈은 정보접근자의 인증을 담당한다. 인증에는 정보주체의 인증과 정보사용자의 인증으로 나누어 처리한다. 정책은 2가지 종류로 나눈다. 기관이나 기업 내의 프라이버시 보호를 위한 정책과 정보 주체가 작성한 개인별 정책이 있다. 기관이나 기업 내의 프라이버시 정책은 프라이버시 관련 제도나 법규에 의해 세워지고, 개인별 정책은 정보 주체인 개인이 자신의 정보에 대한 접근을 정보사용자별로 정책을 세운다.

나. 암·복호화

암호화모듈은 정보 주체가 제공한 정보를 암호화하는 모듈로 키DB에서 생성된 키를 이용하여 각 정보 속성마다 암호화하여 데이타저장소에 제공한다. 복호화모듈은 요청한 정보를 복호화하는 모듈이다. 이 모듈은 개인별 기관별 정책 수정시, 개인정보 유출시 피해를 최소화하기 위해 정보를 수정할 필요가 있다. 이때 복호화모듈을 이용하여 암호화된 정보를 복호화하여 수정을 한다.

다. 키관리모듈

키관리모듈은 키생성모듈과 키DB 2가지로 구성된다.

개인정보를 안전하게 보호하기 위해 P²MS는 개인정보의 각 속성값을 암호화하기 위해 많은 키들이 필요하다. 키생성모듈은 개인별로 마스터키을 생성하고, 마스터키로부터 개인정보의 속성정보를 암호화하기 위한 속성암호화키를 생성한다. 정보 요청시 P²MS은 마스터키로 부터 요청 정보에 대한 속성키를 생성하여 정보사용자에게 제공한다. 키DB는 키생성모듈을 통해 생성된 개인별 마스터 키들을 안전하게 저장하는 공간이다.

3.2.3 데이타저장소

데이타저장소는 개인정보를 저장하는 곳으로 저

장된 모든 정보는 해쉬값과 암호문으로 이루어져 있다. 개인 정보 속성마다 서로 다른 키를 이용해 암호화 되어 있고, 그 암호화 키는 P²MS에 저장되어 있다. 개인정보 암호문은 P²MS으로부터 제공받아 PIA 클라이언트에서 정보를 요청시 요청된 암호화된 정보를 제공한다.

3.3 개인정보 구조

개인정보 주체가 PIA 클라이언트에 그림 5 (a)와 같이 자신의 정보를 제공한다. 제공된 정보는 여러 단계를 걸쳐 데이타저장소(DR : Data Repositories)에 최종적으로 그림 5 (b)과 같이 식별자의 해쉬값과 식별자 및 개인정보에 대한 암호화된 정보로 저장이 된다.

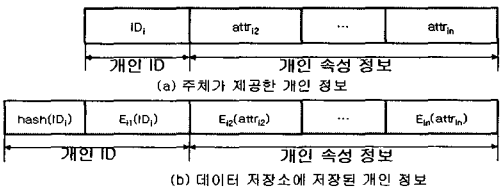


그림 5. 데이터 저장소에 저장된 개인정보 구조

식별정보를 해쉬값과 암호문을 생성해 해쉬값은 개인별 ID로 새롭게 저장을 하고, 전화번호, 주소 등의 다른 개인정보들을 각각의 다른 키를 이용해 암호화하여 저장한다. 식별정보를 해쉬값과 암호문을 생성하므로써 해쉬값을 이용하여 쉽게 정보를 검색하고, 정상적인 방법이 아닌 우회적인 방법으로 DB관리자가 식별정보를 손쉽게 얻지 못하게 하여 개인 식별정보를 보호한다.

Ⅲ. P²MS를 이용한 접근제어모델

동작과정기술의 가독성을 위하여 그림 6과 같이 표기법을 정의한다.

4.1 키관리

개인정보를 안전하게 보호하기 위해 키관리가 필요하다. 키생성모듈을 통해 개인별로 마스터키(k_{ID_i})를 생성한다. 개인의 속성정보를 암호화하기 위한 속성정보 수만큼 속성키가 필요하다. 속성키를 ID_i와 난수R_j을 가지고 다음과 같이 속성키 ($key_{ij} = E_{key_i}(ID_i \| R_j)$)를 생성한다. 생성된 속성키를 대칭키 암호시스템의 대칭키로 속성정보를 암호화하는데 사용하고 개인별 마스터키만을 키 DB에 저장한다. 이는 키 생성 및 키 사이즈를 비롯한 암·복호화 시간이 제안 모델에 적합하기 때문이다. 정보사용자의 정보요청시 저장된 마스터키로부터 속성키를 생성하여 정보사용자에게 제공한다. 키 DB에 저장된 키는 마스터키로서 정보를 제공한 정보주체의 수와 같고, 마스터키는 오직 속성키를 생성할 때만 사용되어 안전하다.

개인정보를 접근권한에 대해 시간이나 기간이 설정되었을 경우 이를 위해 P²MS에서 티켓을 발행한

PIA (*Personal information Access client*) : *PI* 접근클라이언트	*MRAL* (*Modification Request Attribute List*) : 수정요청 정보항목 목록
IS (*Information subject*): 정보주체	*MRALI* (*MRAL Informtion*): *MRAL*의 정보
DR (*Data Repositories*): 데이타저장소	*EP_P* (*Privacy Policy of Enterprise*) : 기업내의 프라이버시 보호 정책
IU (*Information User*): 정보사용자	ID_{IS}_P : *IS* 의 프라이버시 보호 정책
IU_{ID} : 정보사용자 식별자	$\bigcup_{j=2}^{n} attr_{ij} = (attr_{i2}, attr_{i3}, \cdots, attr_{in})$
ID_{IS}(*Identity of Information subject*) : 정보주체 식별자	*AR_intent* (*Access Request intent*): 정보요청 목적
ARAL (*Access Request Attribute infomration List*) : 접근요청 정보항목 목록	$T()$: *P²MS* 의 서명(티켓)
fr_ARAL(*filtered result of ARAL*) : 필터링된 접근요청 정보항목 목록	*IT* : 티켓의 유효기간
fr_ARALI(*fr_Access Request Attribute List Information*) : *fr_ARAL*의 정보	[ ] : 메시지전송 K : 키 , E : 암호화 , D : 복호화 , R_i : 난수

그림 6. 약어 설명

다. 이 티켓은 P^2MS의 개인키로 서명되어 있다. 이는 공개키 암호시스템의 장점인 누구나 볼 수 있지만 변조가 되지 않은 서명을 손쉽게 생성할 수 있기 때문이다.

4.2 개인정보 등록

정보 주체는 PIA에게 자신의 ID와 $n-1$ 개의 정보 속성값을 제공한다. 정보 주체는 PIA를 통해 자신의 정책을 세워 정보 사용자들이 무분별하게 사용하는 것을 제한한다. 개인별 정책을 통해 자신의 정보에 대한 통제권을 기관이 아닌 개인이 갖게 된다. 그림 7은 개인정보 주체가 자신의 정보를 DR에 저장하는 과정을 설명하고 있다.

정보주체(IS_i)가 자신의 정보를 등록하는 과정은 다음과 같다.

① 정보주체는 자신의 정보를 PIA에게 제공한다.

$$IS_i \rightarrow PIA : [DataSet_i] \quad where\ DataSet_i = (ID_i | \bigcup_{j=2}^{n} attr_{ij})$$

② PIA는 정보주체의 개인별 정책 P_i를 세운다.

③ PIA는 P^2MS에게 $DataSet_i$과 정책 P_i를 제공한다.

$$PIA \rightarrow P^2MS : [DataSet_i | IS_i\_P]$$

④ P^2MS는 제공받은 정보 항목마다 각기 다른 키를 이용하여 암호화하고, 정책 P_i를 정책 DB에 저장한다.

$$P^2MS: E_{key ij}((ID_i | \bigcup_{j=2}^{n} attr_{ij}), \bigcup_{j=1}^{n} key_{ij})$$

$$= E_{key i1}(ID_i) | \bigcup_{j=2}^{n} E_{key ij}(attr_{ij})$$

⑤ P^2MS는 DR에게 ID_i 와 함께 암호화된 정보를 제공한다.

$$P^2MS \rightarrow DR : [ID_i | E_{key i1}(ID_i) | \bigcup_{j=2}^{n} E_{key ij}(attr_j)]$$

⑥ DR은 제공받은 ID_i 의 해쉬값을 생성하여 저장하고 ID_i 은 삭제하여 ID_i 의 유출을 막는다. 나머지 정보는 DB에 저장한다.

4.3 정보 검색

그림 8에서는 정보 사용자가 정보주체인 특정인의 원하는 정보를 검색하는 과정을 나타낸 것이다.

정보사용자가 특정인의 정보를 검색하는 과정은 다음과 같다.

① 정보사용자는 특정인의 개인정보를 검색 정보 항목 리스트(ARAL)과 함께 자신의 ID와 특정인의 ID인 ID_{IS}, 정보요청목적(AR_intent)을 P^2MS에게 제공한다. 정보요청목적을 P^2MS에게 제공하는 이유는 P^2MS가 불필요한 정보를 정보사용자에게 제공하지 않기 위해 위함이다.

$$IU \rightarrow P^2MS: [ARAL | IU_{ID} | ID_{IS} | AR\_intent]$$

② P^2MS는 제공 받은 정보사용자 ID를 인증한다.

③ P^2MS는 정보사용자에게 정보 항목을 얼마나 제공할지 결정하기 위해 기관의 정책을 조회하여 권한과 요청목적에 근거하여 요청정보 목록이 축소되고, 축소된 목록에서 ID_{IS}의 개인별 정책을 통해 해당되는 정보만을 접근할 수 있다. 새롭게 생성된 fr_ARAL 와 정책에 맞는 유효기간(IT)을 개인키로 암호화하여 티켓(T)을 생성한다.

$$P^2MS: EP\_P, ID_{IS}\_P\ search, fr\_ARAL, T(fr\_ARAL, IT)$$

$$where\ fr\_ARAL = ARAL \cap ID_{IS}\_P \cap EP\_P \cap AR\_intent$$

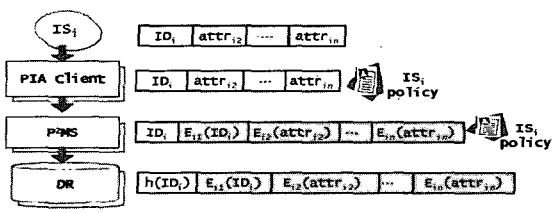


그림 7. 개인정보 등록

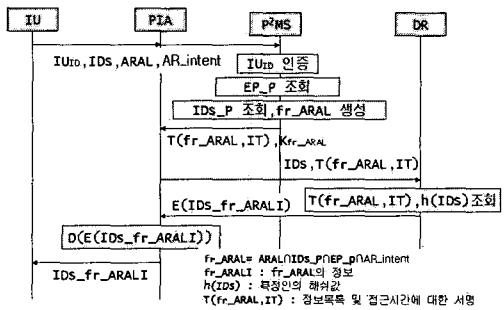


그림 8. 특정인의 정보 검색

$personal\ information \supseteq ARAL \supseteq fr\_ARAL$

$T(fr\_ARAL,IT) = E_{P^2MS}(fr\_ARAL,IT)$

$where = (time, vaild\_util)$

④ P^2MS는 PIA에게 티켓과 fr_ARAL 키들을 제공한다.

$P^2MS \rightarrow PIA : [T(fr\_ARAL,IT) | K_{fr\_ARAL}]$

⑤ PIA는 DR에게 ID_{IS}와 티켓을 제공한다.

$PIA \rightarrow DR : [IDs | T(fr\_ARAL,IT)]$

⑥ P^2MS공개키로 티켓을 복호화하여 요청정보 목록 및 티켓 유효기간을 확인후 ID_{IS}의 해쉬값을 생성하여 DB를 조회한다.

$DR: D_{P^2MS}(T(fr\_ARAL,IT)), h(IDs)$

⑦ 유효기간내의 정보 요청시 DR은 PIA에게 IDs의 fr_ARALI정보만을 제공한다.

$DR \rightarrow PIA: [E_{sj}(DataSet_{sj} \cap fr\_ARALI)\ ]$

⑧ PIA는 DR에서 제공받은 정보를 P^2MS에서 제공한 공개키를 이용하여 복호화한다.

$PIA : D(E_{key_{sj}}(DataSet_{sj} \cap fr\_ARALI)$

⑨ PIA는 정보사용자에게 복호화된 특정인의 정보를 제공한다.

4.4 개인정보 수정

그림 9는 개인정보 주체가 자신의 정보를 수정하는 과정을 나타낸 것이다.

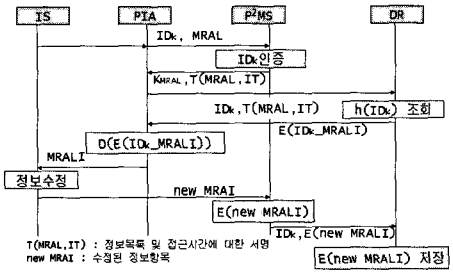


그림 9. 개인 정보 수정

정보 주체(IS_k)가 자신의 정보를 수정하는 과정은 다음과 같다.

① 정보주체의 ID_k와 정보수정 요청항목리스트(MRAL)를 P^2MS에게 제공한다.

$IS \rightarrow P^2MS: [ID_k | MRAL]$

② P^2MS에서 IS_k 인증 한다.

③ P^2MS는 PIA에게 MRAL의 키와 티켓을 제공한다.

$P^2MS \rightarrow PIA: [K_{MRAL} | T(MRAL,IT)]$

$where \quad T(MRAL,IT) = E_{P^2MS}(MRAL,IT)$

④ PIA는 DR에게 IS_k와 티켓을 제공한다.

$IIA \rightarrow DR : [IS_k | T(MRAL,IT)]$

⑤ DR은 티켓을 복호화하여 요청정보목록 및 티켓 유효기간을 확인 후 IS_k의 해쉬값을 생성하여 DB를 조회한다.

$DR : D_{P^2MS}(T(MRAL,IT)), h(IS_k)$

⑥ DR은 PIA에게 암호화된 IS_k 정보에서 MRAL에 해당되는 정보만을 제공한다.

$DR \rightarrow PIA: [E(IS_k\_MRALI)]$

$where\ E(IS_k\_MRALI) = E_{kj}(DataSet_{kj} \cap MRALI)$

⑦ PIA는 제공받은 암호화된 자신의 정보를 P^2MS에서 제공한 키를 이용하여 복호화 한다.

$PIA: D(E(IS_k\_MRALI))$

$$= D(\bigcup_{j=2}^{n}(K_{MRAL}, E_{kj}(DataSet_{kj} \cap MRALI)))$$

⑧ PIA는 IS_k에게 수정할 자신의 정보를 제공한다.

$PIA \rightarrow IS: [DataSet_k \cap MRALI]$

⑨ IS_k는 자신의 정보를 수정한다.

$IS: modify(DataSet_k \cap MRALI)$

⑩ IS_k는 P^2MS에게 수정한 정보를 제공한다.

$IS \rightarrow P^2MS : [new\ MRAL]$

$where\ new MRAI = modified(DataSet_k \cap MRALI)$

⑪ P^2MS는 새로운 키를 생성하여 IS_k가 제공한 수정된 정보를 암호화한다.

$P^2MS: [E(new\ MRAI)]$

$$= E(\bigcup_{j=2}^{n}(new\,key_{kj}, modified(DataSet_{kj} \cap MRALI)))$$

$where\ new\,key_{kj}: jth-new\ key$

⑫ P^2MS는 DR에게 IS_k와 함께 암호화된 정보를 제공한다.

$$P^2MS \rightarrow DR : [IS_k | E(\bigcup_{j=2}^{n}(new\,key_{kj}, modified(DataSet_{kj} \cap MRALI)))]$$

⑬ DR은 제공받은 정보를 IS_k의 정보에 갱신한다.

4.5 개인 정보의 재암호화

P^2MS는 정보사용자의 정당한 정보 요청시 해당 정보의 복호화키인 세션키를 제공한다. 정보사용자

는 키와 티켓을 소유하여 DR에 계속적인 접근이 가능하다. P²MS는 정보사용자의 오남용을 막기 위해 정보변경이나 정책조건의 변경시 P²MS에서 개인별 마스터키 새롭게 생성하여 속성정보를 암호화 시킴으로써 접근을 차단한다.

4.6 정책 등록

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 10과 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 특정사용자에 대한 접근권한이 우선한다.

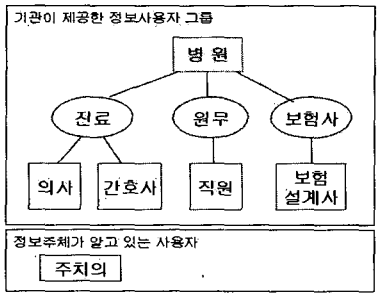


그림 10. 정보사용자 그룹별 카테고리

그림 11은 홍길동이 병원에서의 제공한 정보 사용자 그룹별로 다르게 권한을 부여한 예이다. 홍길동은 이미 알고 있는 주치의에 대해 질병내역과 같은 민감한 정보를 접근할 수 있도록 권한을 부여하였다.

4.6 정보 검색 시나리오

정보사용자가 DR에 있는 정보를 얻고자 하여 P²MS에 접근요청을 하게 되면 P²MS는 기관내의 정책과 개인별 정책에 맞게 요청된 정보를 필터링하여 제공한다. 그림 12은 정보사용자가 DR에 있는 Table T에서 특정 사람의 정보에 대한 검색과정을 도식화한 것이다.

```
- <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  - <xsd:element name="Hong's Policy">
    - <xsd:complexType>
      - <xsd:sequence>
          <xsd:element name="Info_user" type="xsd:string" />
          <xsd:element name="ID" type="xsd:string" />
          <xsd:element name="name" type="xsd:string" />
          <xsd:element name="tel" type="xsd:string" />
          <xsd:element name="health_checkup" type="xsd:string" />
          <xsd:element name="job" type="xsd:string" />
          <xsd:element name="sex" type="xsd:string" />
          <xsd:element name="medical_fee" type="xsd:string" />
          <xsd:element name="prescription" type="xsd:string" />
          <xsd:element name="disease_name" type="xsd:string" />
          <xsd:element name="disease_history" type="xsd:string" />
        </xsd:sequence>
      </xsd:complexType>
    </xsd:element>
  - <xsd:Policy Info_user="doctor">
    - <xsd:AttributeInformation>
        <xsd:Attribute ID="read" />
        <xsd:Attribute tel="read" />
        <xsd:Attribute disease_name="modify" />
        <xsd:Attribute job="read" />
        <xsd:Attribute health_checkup="read" />
      </xsd:AttributeInformation>
    - <xsd:Constraint>
        <xsd:Time>AM 9:00~PM 6:00</xsd:Time>
      </xsd:Constraint>
    </xsd:Policy>
  - <xsd:Policy Info_user="nurse">
    - <xsd:AttributeInformation>
        <xsd:Attribute ID="read" />
        <xsd:Attribute prescription="read" />
      </xsd:AttributeInformation>
    - <xsd:Constraint>
        <xsd:timeDuration>under medical treatment</xsd:timeDuration>
      </xsd:Constraint>
    </xsd:Policy>

  - <xsd:Policy Info_user="hospital clerk">
    - <xsd:AttributeInformation>
        <xsd:Attribute prescription="read" />
        <xsd:Attribute tel="read" />
        <xsd:Attribute medical_fee="write" />
      </xsd:AttributeInformation>
    </xsd:Policy>
  - <xsd:Policy Info_user="Insurance consultant">
    - <xsd:AttributeInformation>
        <xsd:Attribute name="read" />
        <xsd:Attribute tel="read" />
        <xsd:Attribute address="read" />
        <xsd:Attribute job="read" />
        <xsd:Attribute medical_fee="read" />
      </xsd:AttributeInformation>
    - <xsd:Constraint>
        <xsd:Time>AM 9:00~PM 6:00</xsd:Time>
      </xsd:Constraint>
    </xsd:Policy>
  - <xsd:Policy Info_user="family doctor">
    - <xsd:AttributeInformation>
        <xsd:Attribute ID="read" />
        <xsd:Attribute tel="read" />
        <xsd:Attribute health_checkup="modify" />
        <xsd:Attribute disease_history="modify" />
        <xsd:Attribute disease_name="write" />
      </xsd:AttributeInformation>
    - <xsd:Constraint>
        <xsd:IPaddress>192.168.0.100</xsd:IPaddress>
        <xsd:Time>AM 9:00~PM 5:00</xsd:Time>
        <xsd:timeDuration>2006.6.31</xsd:timeDuration>
      </xsd:Constraint>
    </xsd:Policy>
</xsd:schema>
```

그림 11. 홍길동의 개인별 프라이버시 보호 정책

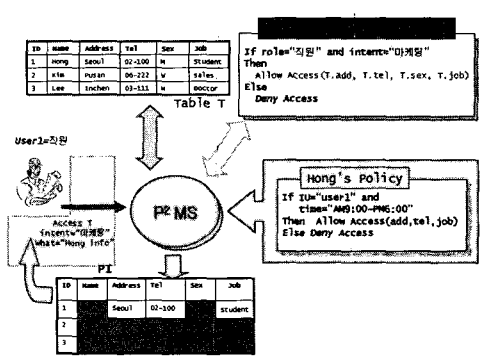


그림 12. "Hong" 정보를 검색하는 시나리오

그림 12은 정보사용자 user1은 직원으로 마케팅을 목적으로 P²MS에 "Hong"의 정보요청을 하고 있다. P²MS는 정보사용자의 요청을 분석한 후 2가지 수행한다. 먼저 기관의 정책을 조회하고 난 후, Hong의 정책을 검색하여 요청된 정보를 제공할 것인지 결정한다. P²MS는 User 1이 요청한 정보중에 접근할 수 있는 정보에 대한 키를 제공한다. User 1은 DR에 있는 Table T에서 원하는 정보를 요청하여 암호화된 정보를 제공받는다. 제공받은 정보는 암호화가 되어 있기 때문에 정보를 볼 수 없다. 암호화된 정보를 User 1은 P²MS에서 받은 키로 복호화하여 해당 정보를 볼 수 있다.

$$
\begin{aligned}
&\text{요청정보목록}(=ARAL) = hong\text{'s } info\\
&=[Name|Address|Tel|Sex|Job]\\
&\text{제공정보목록}(=fr\_ARAL)\\
&=EP\_P \cap (Hong\_P \cap ARAL)\\
&=[Address|Tel|Sex|Job] \cap ([Address|Tel|Job]\\
&\quad \cap [Name|Address|Tel|Sex|Job])\\
&=[Address|Tel|Job]\\
&\quad where\ Hong\_P = Hong\text{의 개인별 정책}
\end{aligned}
$$

4.7 프라이버시 보호측면에서 비교

제안모델을 민감한 개인정보를 암호화하여 기관이나 기업의 정책에 따라 개인정보를 보호하는 시스템인 HP모델[7]과 4가지 측면에서 비교하면 다음과 같은 특성이 있다.

첫째, 제안모델에서는 개인정보 사용시 정보주체의 의도를 반영할 수 있다. HP 모델은 기관의 자체 정책에 따라 접근제어를 이용하여 정보를 보호하고 있지만 정보 주체의 동의없이 정보가 제공되고 있으나 제안 모델에서는 정보 주체가 작성한 정책에 부합될 때만 정보가 제공되므로 정보 주체의 의도가 반영된다.

둘째, 제안모델에서는 세밀한 접근 제어가 가능하다. HP 모델은 역할 및 업무에 의한 접근제어를 하나, 제안 모델에서는 기관의 정책뿐만 아니라 개인별 정책을 통해 보다 세밀한 접근제어가 가능하다.

셋째. 제안모델은 DB 관리자로부터 안전하다. HP 모델은 DB의 정보 검색을 위해 식별자는 평문으로 되어 있다. 식별자를 이용하여 원하는 정보 검색이 가능하지만 DB 관리자는 권한없이 식별정보를 볼 수 있다. 제안모델에서는 식별정보을 해쉬값으로 대치하여 DB 관리자의 불법적 접근으로부터의 보호가 가능하다.

넷째, 개인정보 변경시 제안모델은 변경된 정보만을 암호화하면 된다. 그러나 HP모델은 필드 단위로 암호화되어 있어 한 개의 정보 변경시에도 필드의 모든 정보에 대해 재암호화 해야 한다.

다섯째, 제안모델은 키 하나가 유출되었을 때, 한 사람의 속성정보 하나만 유출되지만 그 정보의 주인이 누구인지는 알 수 없다. HP 모델은 개인정보의 특정정보 즉 필드 단위로 암호화하였기 때문에 그 키가 유출되면 모든 사람의 특정 정보를 볼 수 있다. 그 특정정보가 금융, 성향 등의 민감한 정보일 경우 식별자 정보를 이용하면 침해정도가 심각하게 된다. 제안모델에서는 키 하나가 유출되어도 식별정보를 모르기 때문에 프라이버시 침해를 최소화할 수 있다.

V. 결 론

기관이나 기업들은 개인정보를 수집하여 저장된 DB에 대해 암호화와 접근제어 기술을 이용하여 보호하고 있지만 개인의 요구에 맞는 보호 방법으로는 적절하지 못하다. 프라이버시 지침이나 제도는 정보주체의 동의 및 제어 권한을 주체에게 제공할 것을 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 정보주체가 자신의 정책을 세우고 정보 저장과정에서는 암호화키를 이용하여 개인별, 속성별로 암호화하여 저장하였다. DB 정보 검색을 위해 개인 식별정보는 해쉬값으로 변환하여 저장하였고, 그로 인해 DB관리자조차도 식별정보라 할지라도 개인별 정책과 기관의 정책에 부합하지 않으면 볼 수 없다.

제안한 모델은 병원과 같이 저장된 정보가 개인마다 민감하고, 유출시 그 피해가 큰 기관이나 개인정보가 저장되어 특정 정보 검색 및 개인화 서비스를 제공할 수 있는 교육행정정보시스템(NEIS)에서 사용될 수 있다. 즉 개인정보 DR에 대해 DB관리자로부터 보호가 필요한 시스템에 사용이 가능하다. 제안모델은 속성별로 암호화하는 방식이므로 세션키 생성시간과 암호화 시간을 단축시키는 연구가 필요하다.

참 고 문 헌

[1] W3C, Platform for Privacy Prefere-

nce(P3P) version1.1, http://www.w3c.org/P3P

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

[3] W. Stallings, Cryptography and Network Security, ISBN 0-13-091429-0.

[4] 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.

[5] W.k. Huan, and V. Atluri, "SecureFlow : A secure Web-enabled Workflow Management System," Proc. of 4th ACM Workshop on Role-based Access Control, 1999.

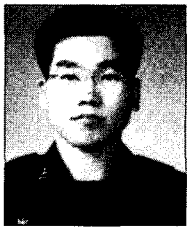
[6] P.K.Thomas, and R.S.Sandhu, "Task-based Authorization Control(TBAC) : A Family of Models for Active and Enterprise-oriented Authorization Management," Proc of the IFIP WG11.3 Workshop on Database Security. 1997.

[7] 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.

[8] S. Oh, and S. Park, "A Process of Abstracting T-RBAC Aspects from Enterprise Environment," DASFAA'01. April.2001.

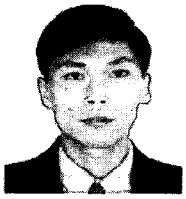
[9] M.C. Mont, S. Pearson, and P. Bramhall., "An Adaptive Privacy Management System For Data Repositories," http://www.hpl.hp.com/techreports/2004/HPL-2004 -211.html

〈著者紹介〉



문 형 진 (Hyung-Jin Mun) 학생회원
1996년 2월: 충남대학교 수학과 졸업
2002년 2월: 충남대학교 수학과 석사
2003년 3월~현재: 충북대학교 전자계산학과 박사과정
〈관심분야〉 암호학, 정보보호, 프라이버시 보호

이 건 명 (Keon-Myung Lee) 정회원
1990년 2월: KAIST 컴퓨터과학과 졸업
1992년 2월: KAIST 컴퓨터과학과 석사
1995년 2월: KAIST 컴퓨터과학과 박사
1996년~현재: 충북대학교 전기전자컴퓨터공학부 교수
〈관심분야〉 정보보호, 데이터 마이닝, 퍼지시스템



이 영 진 (Yong-zhen Li) 학생회원
1994년 6월: 중국 연변대학교 물리학과 졸업
1997년 6월: 중국 연변대학교 물리학과 석사
2003년 3월~현재: 충북대학교 전자계산학과 박사과정
〈관심분야〉 센서네트워크, 정보보호, 프라이버시 보호, 암호학

이 동 희 (Heui-dong Lee) 정회원
1988년 2월: 충북대학교 전자계산학과 졸업
1990년 2월: 충북대학교 전자계산학과 석사
2006년 2월: 충북대학교 전자계산학 박사
1994년 3월~현재: 극동정보대학 보건의료정보과 교수
〈관심분야〉 네트워크 보안, 정보보호, 접근제어

이 상 호 (Sang-ho Lee) 정회원
1976년 2월: 숭실대학교 전자계산학과 졸업
1981년 2월: 숭실대학교 시뮬레이션 석사
1989년 2월: 숭실대학교 컴퓨터네트워크 박사
1981년~현재: 충북대학교 전기전자컴퓨터공학부 교수
〈관심분야〉 정보보호, 네트워크 보안