개인정보시스템에서 접근제어 모델 설계

박익수 조아앵 이경효 서재현 오병균
목포대학교 정보공학부
{upark○, agcho, mediakh, jhseo, obk}@mokpo.ac.kr

Design of Access Control Model in Personal information System

Ik-Su Park○ A-Aeng Cho kyoung-Hyo Lee Jea-Hyun Seo Byeong-Kyun Oh
Division of Information Engineering, Mokpo National University

요 약

유비쿼터스는 다양한 상황 정보들에 따라 여러 가지 형태의 서비스들이 요청되어 처리되어야 하는 환경이며, 이러한 환경의 태생적인 한계로 인해 사용자가 인지 못하는 사이에 야기 되어지는 개인정보 침해는 해결되어야 하는 직면된 문제 중 하나이다. 유비쿼터스 컴퓨팅은 원활한 정보 공유와 서비스 이용을 위한 환경으로 정보 공유가 필요하며, 정보에 대한 접근제어 정책으로 정제된 정보 공유를 적용하여 개인정보 보호가 가능하다. 본 논문에서는 개인정보 보호를 위한 해결방안들에 관하여 고찰하고, 정보주체에 대한 자기정보결정권을 지닌 개인정보 보호 접근제어 모델을 제안한다.

1. 서 론

최근 개인정보보호에 대한 인식이 DB에 수집된 개인정보가 부당하게 유출되거나 오·남용되는 것을 방지한다는 비교적 단순한 의미에서 벗어나 점차 정교해지고 있다[1, 2].

프라이버시도 오랫동안 '홀로 남아 있을 권리' 혹은 '사생활 보호' 라는 좁은 의미로 해석되었으나, 최근에는 정보주체의 자기정보결정권이라는 의미로 해석되는 경향이 있다. 즉, 프라이버시가 개인이 자신의 어떤 정보가, 누구에 의해, 어떻게 수집되고, 어떻게 보관되며, 어떻게 이용되는가에 대해 스스로 결정할 수 있는 권리로 인식되고 있다[3].

개인정보를 제공하는 일반 사용자들은 자신의 개인정보를 보호하기 위해 개발된 일부 보안 도구들을 사용하고 있지만, 개인정보를 수집하고 저장, 관리하는 정보통신사업자 등 개인정보 사용자가 운영하는 시스템에 대한 보안 요구사항 분석이나 개발에 대한 연구는 미진한 형편이다. 따라서 현실의 환경에서 완전하게 개인의 프라이버시가 보장되기는 어렵다.

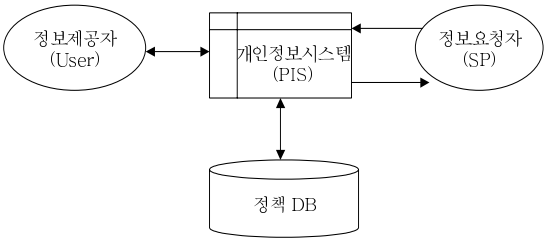
본 논문에서는 관련연구로 개인정보보호를 위한 해결방안들에 관하여 고찰하고, 정보주체에 대한 자기정보결정권을 지닌 개인정보시스템에서 접근제어 모델을 제안한다.

2. 관련 연구

2.1 개인정보시스템 위한 요구사항

개인정보보호를 위해서는 개인이 허용하는 범위 내에서만 개인정보가 사용되어야 함으로 개인정보의 생성부터 활용, 폐기까지의 단계에서 개인정보를 고찰 할 수 있는 기본 모형이 필요하다[3]. 본 절에서는 개인정보 생명 주기와 개인정보시스템 설계 요구사항을 분석한다.

개인정보시스템의 구성요소는 정보제공자, 정보요청자, 개인정보정책관리시스템인 개인정보시스템, 개인정보 저장과 관리를 위한 정책 DB가 있다. 그림1에서 개인정보시스템 환경에서 구성요소를 나타내었다.



[그림 1] 개인정보시스템 환경 구성요소

2.1.1 개인정보 생명 주기

개인정보보호 시스템과 연관된 구성요소들로는 개인정보를 제공하는 개인정보제공자, 개인정보의 수집 주체인 서비스제공자, 수집된 개인정보를 요청하는 내외부사용자 등이 있다. 또한, 개인정보 생명주기에 따라 정보의 수집, 정보의 저장, 정보의 관리, 정보의 이용, 정보의 제공, 정보의 폐기로 구분할 수 있다[4].

■ 수집 단계

수집 단계는 정보사용자가 정보를 요청하면 정보의 주체는 정보사용자가 요청하는 개인정보의 사용목적을 확인하고 어떠한 목적에 의해 정보데이터가 수집되고 사용될 것인지 확인한다. 정보의 주체가 허용하는 범위 내에

서 개인정보를 요청한 사용자에게 제공한다.

■ 정보의 저장

수집된 개인정보는 서비스제공자가 정보수집 목적에 부합하도록 정제과정을 거쳐서 데이터유형, 데이터사용목적, 데이터유지시간 등의 추가 정보와 함께 저장된다.

■ 정보의 관리

저장된 정보는 서비스제공자의 개인정보보호 정책에 의해 관리된다. 또한, 개인정보제공자에 의해서 수정되거나 삭제될 수 있다.

■ 정보의 이용・제공

정보사용자는 다른 서비스제공 혹은 업무를 위해 필요한 개인정보를 서비스제공자에게 요구한다. 서비스 제공자는 정보사용자가 요구하는 개인정보를 개인정보제공자가 지정한 사용목적 등을 참조하여 제공여부를 결정하고 필요에 따라 사용자에게 동의를 구한 후 정보사용자에게 개인정보를 전송한다. 추후 정보사용자의 개인정보 활용은 서비스제공자에게 통보되고 서비스제공자는 감사기능을 수행하여 개인정보의 정확한 사용여부를 기록・보관한다.

■ 정보의 폐기

개인정보제공자의 정보폐기 요청이나 관리단계에서 정한 유지기간이 지나면 개인정보를 폐기하고, 정보사용자에게 정보폐기를 요청하고 그 결과를 받는다. 최종 결과를 개인정보제공자에게 통보한다.

2.1.2 개인정보시스템 설계를 위한 요구사항[6]

유비쿼터스 환경에서 접근제어 요구사항은 다음과 같다.

■ 유비쿼터스 컴퓨팅 환경에 포함된 주체, 객체, 접근형태(권한)를 식별(identify)하고 정보로 표현할 수 있는 방법이 있어야 한다.

참조 모니터가 접근제어를 수행할 수 있기 위해서는 기본적으로 주체, 객체, 접근 형태(권한)가 식별될 수 있어야 한다. 유비쿼터스 컴퓨팅 환경에서는 주체, 객체, 접근의 형태가 일반 정보 시스템과는 다르므로 어떻게 이들을 식별하고 정보를 관리할 것인가를 고민해야 한다. 주체나 객체의 식별은 비교적 쉽겠지만 접근의 형태에 대한 식별은 쉽지 않다. 유비쿼터스 컴퓨팅 환경에서는 단순히 하나의 장치만 포함된 것이 아니라 기능과 성격이 다른 여러 장치들이 포함되어 있고 장치마다 접근 특성이 다르므로 이들에 대해 전체적 차원에서 접근제어를 시행하는 것은 어려운 일이다. 주체, 객체, 접근의 형태에 대한 식별과 표현 방법에 대한 연구가 필요하다.

■ 컨텍스트 정보를 기반 동적 제어 규칙을 표현할 수 있는 방법이 있어야 한다.

유비쿼터스 컴퓨팅 환경에서는 기본적으로 컨텍스트 정보에 의해 접근제어가 이루어지는 매우 동적인 접근제어를 필요로 한다. 따라서 컨텍스트 정보를 어떻게 효과적으로 접근제어에 접목 시킬 수 있는가가 문제해결의 관건이다. 유비쿼터스 컴퓨팅 환경에서 접근제어에 대한 기존의 연구가 이 부분에 집중되어 있다는 사실은 컨텍스트 정보의 처리가 매우 중요함을 입증한다. 컨텍스트 정보가 접근제어에 접목되기 위해서는 제어 규칙의 형태로 표현되어야 한다.

■ 분산 환경의 특성을 구현하기 위한 방법이 제공되어야 한다.

유비쿼터스 컴퓨팅 환경은 기본적으로 분산 환경이다. 하나의 단일 하드웨어 혹은 단일 시스템으로 구현되는 것이 아니라 단일 하드웨어 혹은 단일 시스템으로 구현되는 것이 아니라 다양한 기능과 역할을 하는 지능형 장치들과 센서들이 네트워크로 연결되어 하나의 '환경'을 형성한다. 따라서 접근제어 모델 역시 이러한 분산 환경의 특성을 지원해야 한다. 분산 환경이라는 특성은 접근제어를 실제 구현할 때 다양한 유형의 구현이 가능하게 한다.

2.2 개인정보보호 해결 방안들

2.2.1 P3P

P3P는 컴퓨터 프로그램에 내장되어 특정웹사이트와 이용자의 웹브라우저 간 개인정보 보호 정책들을 검색하여 적정선에서 요구하고 적절하게 관리하고 있는지를 알 수 있도록 하기 때문에 이용자측면에서는 안전성과 편리성을 추구할 수 있고 서비스제공자측면에서는 개인정보보호정책의 내용을 구체적으로 명확하게 알려주고 이용자들의 개인정보를 수집하여 서비스제공에 활용하는 등 상호 신뢰를 쌓을 수 있게 한다. 그러나 이용자에게 개인정보보호 설정을 하도록 되어 있어 컴퓨터 운영지식이 미숙한 사용자에게 부적절한 방법이며, 강제성이 없다는 문제가 있다. 또한 개인정보보호는 인터넷 상에서만 일어나는 것이 아니므로 오프라인에서도 가능한 개인정보보호 기술이 필요하다.

2.2.2. E-P3P(Enterprise P3P)

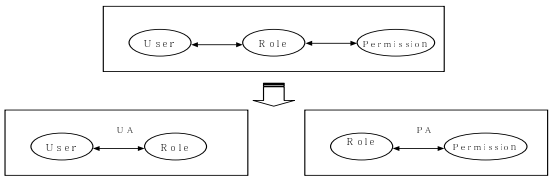
E-P3P는 IBM에서 제안한 기술로서, 기업 내에서 사용자들의 신원 정보의 오・남용을 막기 위한 정책의 정형화 및 집행을 가능하게 하는 프레임워크이다. 즉, 기업이 수집한 민감한 개인 정보를 신뢰할 수 있는 방법으로 관리할 수 있도록 하는 새로운 프레임워크이다[4].

3. 개인정보시스템 접근제어 모델 설계

유비쿼터스 환경에서의 접근제어는 사용자의 상황 정보가 반영되어야 하며, 다양한 사용자의 요구가 따른 적절한 접근 제어가 수행되어야 한다[1].

3.1 제안된 RBAC 모델 개념

기존의 역할 기반 접근제어 모델에서는 보안 관리자에 의해서만 역할과 해당 권한을 생성, 관리할 수 있다. 이에 따라 사용자의 개입이 배제되어 사용자의 다양한 요구를 처리하는데 한계가 있었으며, 사용자의 의도되지 않은 개인 정보까지 노출될 위험이 있다. 본 논문에서는 [1]에서 제안한 접근제어 모델의 개념을 바탕으로 개인정보시스템에서 접근제어 모델을 설계한다. 그림1은 보안 관리자의 권한부여 정책 작성 권한의 일부분을 사용자에게 이양하여 사용자에게 자신의 데이터 접근에 대한 통제권한을 보유하게 하여 사용자의 의도가 반영되는 접근제어 모델 개념이다.

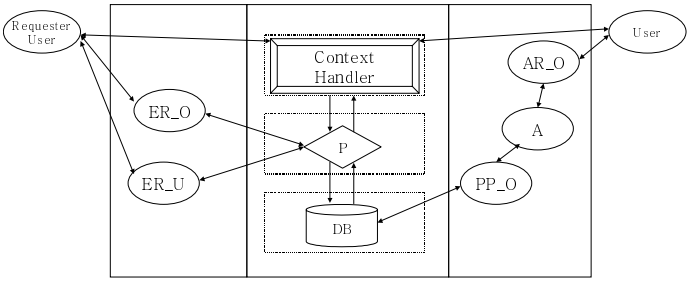


[그림 2] 적용 모델 개념[1]

3.2 개인정보보호 접근제어 모델

개인정보보호 접근제어 모델은 그림2와 같다. 개인정보시스템에서 개인정보를 이용하기 위해서는 정보제공자의 협의를 거쳐야 한다. 개인정보보호 접근제어 모델은 그림2와 같다. 이 모델에서는 개인정보시스템에 접근할 수 있는 경우는 개인정보 제공자, 개인정보 관리자, 외·내부 개인정보 사용자로 구성된다.

개인정보보호 접근제어 모델은 개인정보 관리를 위한 정책관리 모듈과 개인정보 사용의 허가를 받기위한 정책 실행 모델로 구성된다.



[그림 3] 개인정보시스템 제안 모델

개인정보시스템에서 정책 관리 모듈은 개인정보소유자와 개인정보서비스관리자가 수행한다. User는 개인소유자로 소유하는 개인정보를 관리하며 개인정보소유자정책(PP_O)을 생성하고 관리한다.

개인정보시스템에서 DB는 개인정보를 저장하고 있다. Requester User는 개인정보 DB 모듈과 사용목적 접근리스트 P 모듈 정책을 적용하여 개인정보 사용허가를 얻을 수 있다.

3.3 개인정보 정책 기술

개인정보시스템에서 사용자가 작성해야 하는 정책의 항목은 표 1과 같다.

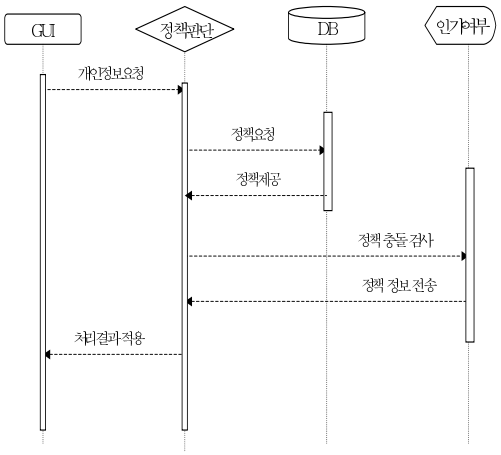
이들 항목은 역할기반 접근제어 모델의 제약사항의 일부로서 보안 관리자의 권한 배정 정책과 비교되어 사용자에게 적절한 권한을 배정하게 된다.

[표 1] 프라이버시 정책

정책	설명
User	사용자
Requester	요청자
AR_O	소유자의 역할
A	Access mode
PP_O	개인정보보호 소유자정책
ER_O	제공자의 역할
ER_U	사용자의 역할
Context handler	개인정보시스템에서 핵심적인 부분
P	사용목적
DB	개인정보 저장

3.4 개인정보 정책 허가 및 시스템 설계

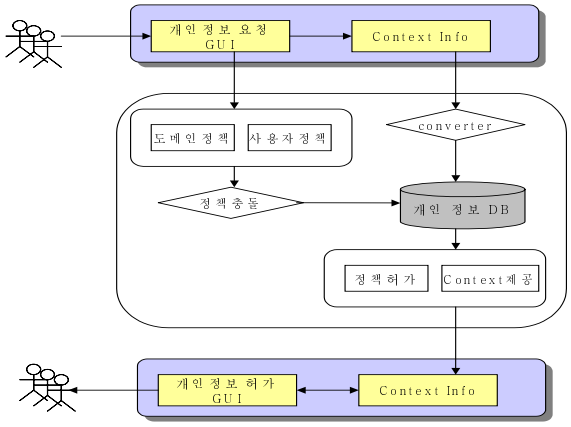
제안된 시스템은 3.2 에서 정의한 개인정보시스템 접근제어 모델을 적용하며, 제안된 시스템의 정책 허가는



[그림 4] 개인정보 정책 허가 시나리오

[그림4]와 같다. 개인정보 요청자가 GUI를 통하여 개인정보를 요청한다. 정책판단에서는 개인정보 요청 정보를 DB에 있는 정책을 요청한다. 요청된 정책에 기반 하여 개인정보 허가 결정을 수행한다. 만약 정책 충돌이 발생하면 정책 중동 규칙으로 허가를 결정한다. 결정된 개인정보 정책은 개인정보의 인가 요청자에게 전송한다.

그림 5는 개인정보시스템 구조를 보여주고 있다. 개인정보시스템은 크게 2개의 부분으로 나눠진다.



[그림 5] 개인정보시스템 설계

4. 결론

개인정보침해 기술은 IT 기술의 진보와 더불어 고도로 다양화되고 지능화되어 다수의 선진국은 개인정보침해로부터 국민의 권리를 보호하기 위해 개인정보를 보호하는 법률을 제정하였거나 제정 중에 있다. 접근통제 기술은 보안기능을 제공하는 대부분의 정보 시스템에서 정보객체에 대한 사용자의 접근권한 소유 여부를 최종적으로 판단하는 기술로서 활용되는 주요한 정보보호 기술 중의 하나이다.

유비쿼터스는 다양한 상황 정보들에 따라 여러 가지 형태의 서비스들이 요청되어 처리되어야 하는 환경이며, 이러한 환경의 태생적인 한계로 인해 사용자가 인지 못하는 사이에 야기 되어지는 개인정보 침해는 해결되어야 하는 직면된 문제 중 하나이다.

본 논문에서는 유비쿼터스 컴퓨팅 환경에서 개인정보보호를 위한 해결방안들에 관하여 고찰하여, 정보주체에 대한 자기정보결정권을 지닌 개인정보시스템에서 접근제어 모델을 제안하였다.

차세대 IT 환경인 유비쿼터스 환경에서는 언제 어디서나 사용자의 개인정보침해 사고가 발생할 수 있으며 이로 인해 언제 어디서나 프라이버시를 보호할 수 있는 자동화된 기술이 필요하다. 그러므로 자동화된 에이전트 기반 기술을 바탕으로 한 지능화 통합화 에이전트 기술이 각광받을 것은 자명하다.

참고문헌

[1] 홍성호, 조은애, 문창주, 백두권, “프라이버시 보장을 위한 RBAC 기반의 접근 제어 프레임워크”, 2006 KCC, Vol 33, No. 1(C), 2006.

[2] 김기현, "접근통제기술 개요", 한국정보보호센터, 시스템기술팀, 1999.

[3] 노승민, 이수철, 김현주, “RBAC에 기반한 의료정보 보호시스템의 설계 및 구현”, 아주대학교, 정보통신전문대학원, 대학원의학과, 제21회 한국정보처리학회, 춘계 학술발표 논문집, 제 11권, 제 1호, 2004.

[4] 박종화, 김동규, "프라이버시 보호를 갖는 확장된 역할기반접근제어 모델", 한국통신학회 논문지, Vol 29. NO. 8C, 8월, 2004.

[5] 박종화, 김지홍, 김동규, “확장된 역할 기반 접근제어 모델에서 GRBAC을 이용한 프라이버시 제어,” 한국통신학회논문지, Vol 30. No. 3C, 2005.

[6] 이동희, 이경희, “전자상거래에서 MMDB를 활용한 상품추천 시스템”, 극동정보대학, 기업경영연구소, 제 4권, pp. 175- 190, 2001.

[7] 이동희, “RBAC 개념을 이용한 역할과 허가권한의 모델 확장”, 극동정보대학 논문집, 제 9집, pp. 247 - 276, 2002.

[8] 이동희, 이성종, “RBAC 개념을 응용한 병원정보시스템”,극동정보대학, 산업경영연구소, 제 6권, pp. 181 - 206,2001.

[9] 이상하, 조인준, 천은홍, 김동규, "역할기반 접근통제에서 역할 계층에 따른 접근권한 상속의 표현," 한국정보처리학회 논문집, 제7권 제7호, 2000.

[10] 조병철, 박석, "역할기반 접근제어에서 ARBAC97의 역할관리 기법을 적용한 사용자 수준의 위임", 서강대학교 컴퓨터학과 데이터베이스 연구실, 한국통신정보보호학회, 종합학술발표회 논문집 Vol. 10. No. 1. 2000.

[11] 최만규, "병원정보시스템의 성과 및 활성화 방안", 국민보건연구소 연구논문, J. Institute Hlth. Environ. Sci. Vol. 9.No. 1. PP. 21-35, June, 1999.

[12] http://www.epic.org/privacy/tools.html