유비쿼터유비쿼터스 환경에서 프라이버시 보호를 위한 사용자 직접 관리 방식의 접근 기록 관리 시스템

An Access Log Management System by User Directed Managing in Ubiquitous Environment

이제훈, J.Lee*, 김상욱, S.Kim**

요약 유비쿼터스 환경에서 사용자는 도메인간의 이동이 자유롭고 다른 도메인에서의 활동이 많아진다. 이런 환경에서 서비스 제공자들은 사용자들에게 서비스를 제공하면서 접근 및 동작에 관한 기록을 남긴다. 이 기록은 추후에 개인을 식별하거나 행적을 추적할 수 있는 프라이버시 침해 문제를 일으킬 수 있다. 따라서 이러한 정보를 서비스 제공자가 가지는 것이 아니라 개인이 보관하고 관리할 수 있도록 하여야 한다. 본 논문에서는 개인의 접근이나 제공받은 서비스에 대한 기록을 서비스 제공자의 도메인에서 자신이 관리하는 도메인 서버로 가져와서 관리할 수 있는 시스템을 제안한다. 또한 원격 도메인 관리자가 해당 정보를 적법한 절차에 의해 해당 정보를 요청 시에 시스템은 개인이 허용하는 범위의 정보만을 전달하도록 하여 개인의 프라이버시를 지킬 수 있도록 한다.

Abstract In ubiquitous environments, clients move between domains freely and its activities in the other domains are growth. Like this environment, the service provider makes access or activity records what they are provided to clients. This record can make a privacy problem to recognize a person or trace some works. So this record must be kept and managed by user instead of the service provider. In this paper, we propose a system that can gather those records from the service provider to home domain server which client's managing by themselves. In addition, if remote domain manager requests that record by the legal process, system can transfer only a range of information which allowed by client to keep personal privacy.

핵심어: Ubiquitous, Privacy, Security, Context-Awareness, Access Information.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0026)

*주저자 : 경북대학교 전자전기컴퓨터학부 석사 e-mail: newsky@cs.knu.ac.kr

**공동저자 : 경북대학교 전자전기컴퓨터학부 교수 e-mail: swkim@cs.knu.ac.kr

1. 서론

유비쿼터스 환경에서 사용자는 이동이 자유롭고 여러 도메인에서 제공하는 서비스를 편하게 이용하기를 원한다. 사용자는 자신에게 적합한 서비스를 제공받기 위하여 개인 정보를 자신이 모르는 사이에 서비스 제공자에게 제공하고 있다[1]. 사용자 정보를 제공하는 단계에서 개인의 익명성을 보장하기 위한 연구들은 진행되고 있다. 하지만 제공받은 서비스 내역을 보관함으로 인해 생기는 프라이버시 침해도 생각해보아야 한다.

예를 들어 사용자가 이동하면서 비디오 콘텐트를 제공받기를 원할 때, 서비스를 제공하는 도메인에서는 사용자에게 콘텐트를 제공하였기 때문에 결제를 원하거나 차후에 개인화된 서비스를 제공하기 위하여 결제 정보 등의 기록을 사용자 정보와 함께 가지고 있어야 한다. 하지만 이러한 정보가 서비스 제공자가 악의적인 목적이나 불법적인 방법을 통하여 유출된다면 개인의 프라이버시가 침해될 수 있는 위험이 있다. 또한 사용자는 자신의 정보가 언제 어떻게 사용되는지에 대한 자기 통제권을 가질 필요가 있다.

이와 관련하여 개인 정보에 대한 인식은 차츰 커지고 있지만 제도적인 뒷받침은 제대로 이루어지지 못하고 있다. 법적으로 개인 정보 또는 정보프라이버시의 보호를 위한 법령들이 이곳 저곳에 산재되어 법적 보호의 공백을 야기하고 있다[2]. 더욱이 문제는 법으로 제정된다고 하여도 서비스 제공자를 통한 정보유출도 심각한 문제로 남아있다[3]. 미국에서는 전자지불 업체의 서버 해킹으로 인한 4000 만 명 이상의 고객 신용카드 정보가 유출되어 현재까지 일본에서만 약 12 억 원 이상의 도용피해가 있었다.

따라서 본 논문에서는 사용자가 서비스를 제공받았을 때 그러한 정보를 사용자가 통제할 수 있도록 하기 위한 시스템을 제안한다. 도메인간을 이동할 때 자신의 정보를 자동으로 전달하고 그 정보를 토대로 자신의 홈 도메인 서버로 서비스 제공 내역을 전달하여 전달된 정보를 자신의 도메인에서 관리할 수 있도록 한다. 또한 서비스 제공자나 적법한 절차에 의해서 서비스 내역을 요청 시에는 제공할 수 있는 시스템을 제안한다.

본 논문의 2 장에서는 기존의 연구를 살펴보고 3 장에서는 제안하는 접근 기록 관리 시스템을 설명한다. 마지막으로 4 장에서는 구현에 대해 설명하고 5 장에서 결론을 기술한다.

2. 관련 연구

유비쿼터스 환경에서 동적인 환경에서 접근 기록 관리 서비스 제공에 관련된 연구를 살펴본다

2.1 OpenID

OpenID 는 개인의 인증 정보를 사용자가 관리할 수 있는 분산형 공개 표준 기술이다[4]. 하나의 아이디로 여러 웹 사이트를 로그인 할 수 있는 기술이다. 즉 고유한 URI 형태의 자신만의 아이디를 자신이 운영하는 도메인이나 서비스 제공자의 도메인에서 발급받는다. 그런 후 사이트를 이용하기 위해 로그인하게 되면 서비스 제공자와 OpenID 서버와 협상에 의해 로그인 절차를 거치게 된다. 이때 사용자는 개인 정보를 자신이 허락하는 수준의 개인정보만을 제공할 수 있도록 대화식 접근 방법을 사용하여 제어할 수 있다.

2.2 Gaia

Gaia[5]는 Illinois 대학에서 제안한 시스템으로 스마트 공간을 제공하는 기본구성을 제공한다. Cerberus 는 Gaia 에서 중심 서비스로 신분 증명, 인증, 상황 인지 등을 통합하는 시스템이다. GAMM(Gaia Authentication Device Modules)는 일반적인 방법을 통해서 사용자를 인증한다. 사용되는 인증 방법으로는 Kerberos 인증이나 사용자아이디와 비밀번호를 통한 인증 등이 있다. Gaia 에 포함되어 유비쿼터스 어플리케이션의 보안성을 향상한다. 하지만 이 시스템에서 개인의 프라이버시에 대한 고려는 부족하다. 인증된 개인의 정보의 관리와 접근 기록의 관리에 대한 고려를 하지 않고 있다.

2.3 Privacy Preferences Project

Privacy Preferences Project(P3P)[6] 는 웹 사이트의 프라이버시를 보호하기 위해 World Wide Web Consortium(W3C)에서 정한 표준 기술 플랫폼이다. 사용자의 웹 브라우저에 설치된 에이전트가 자동으로 사용자의 개인정보 보호 정책과 서비스 제공자의 개인 정보 사용 정책을 비교해 정보 제공을 결정한다. 개인 정보 노출 수위를 조절할 수 있고 서비스 제공자가 개인 정보를 어떤 목적으로 사용되는 지를 쉽게 알아볼 수 있도록 하는 것이다. 사용자는 자신의 개인 정보 보호 요구사항을 서비스 제공자가 충족시키는지를 판별할 수 있도록 하고 있다. 하지만 이 방법은 웹 사이트 환경에 국한되고 제공된 사용자 정보가 추후에 악의적인 목적으로 사용되었을 경우에 이를 방지하거나 추적할 수 없다.

3. 접근 기록 관리 시스템

본 논문에서 제안하는 시스템은 자유롭게 이동하는 환경에서 서비스를 제공받을 때 제공받은 서비스에 대한 상세한 기록을 서비스 제공자가 기록/관리하는 것이 아니라 개인이 자신의 홈 도메인에 기록하여 자신이 직접 관리할 수 있도록 하는 시스템을 제안한다.

3.1 시스템 구조

제안하는 시스템 구조는 다음과 같다.

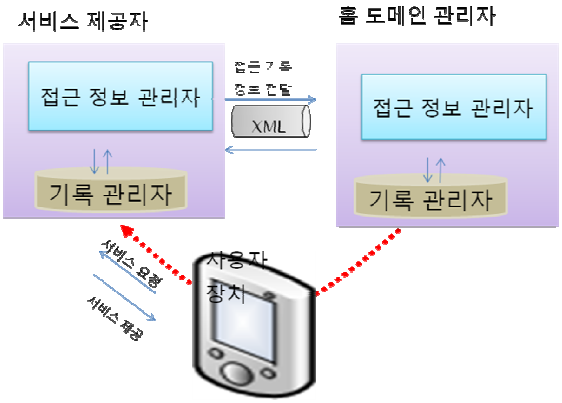

그림 1. 시스템 구조

사용자는 서비스 제공자에게 서비스를 요청하게 된다. 이때 사용자를 인증 할 수 있는 인증도 같이 한다. 인증 요청과 서비스 요청에 대한 내용은 "프라이버시 보호를 위한 동적 접근 제어 시스템"을 따른다[7]. 이 시스템은 도메인간의 이동을 할 때 홈 도메인의 인증 서버를 통하여 자신의 인증 정보를 전달하는 시스템이다. 홈 시스템과 다른 도메인의 시스템은 모두 신뢰기관으로부터 인증된 상태인 제 3 기관을 통한 신뢰 시스템이다. 접근에 대한 인증이 끝나면 서비스를 요청한다. 서비스 제공자는 해당 요청에 따라서 서비스를 제공하기 전에 사용자가 직접 전근 기록 정보를 관리하는지 확인한다. 사용자는 자신의 접근 기록 정책을 서비스에 맞게 전달한다. 서비스 제공자는 전달받은 정보를 바탕으로 자신의 서비스에 맞게 협상을 한 후 사용자 홈 도메인 관리자에게 접근 기록 정보를 전달한다. 그런 후 사용자에게 서비스를 제공하게 된다.

3.2 접근 정보 전달 알고리즘

위 과정을 흐름도로 나타내면 다음과 같다.

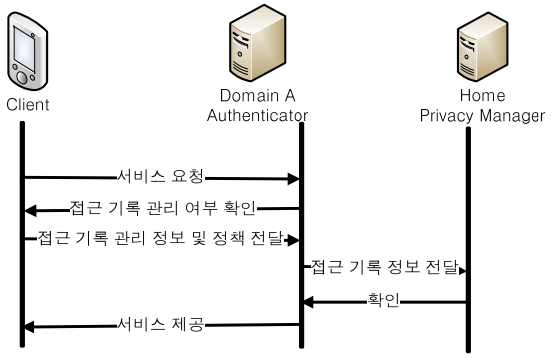

그림 2. 접근 정보 전달 흐름도

그림 2 는 접근 정보를 사용자 홈 도메인으로 전달하는 과정을 나타낸다. 사용자는 이동하면서 이동한 도메인에 서비스를 요청한다. 서비스 제공자는 접근 기록 정보를 사용자가 관리하는지에 대해 사용자에게 확인한다. 사용자는 접근 기록 정보를 전달할 수 있는 홈 도메인 서버의 URI 와 접근 기록 정보에 대한 사용자의 정책을 전달한다. 서비스 제공자는 해당 정책과 서비스 제공자의 접근 기록 정보 사이에서 협상을 통해서 전달할 정보를 결정한다. 홈 도메인 서버로 접근 기록 정보를 전달한 후 사용자가 요청한 서비스를 제공한다. 서비스 제공자는 자신의 접근 기록 정보를 저장할 때 사용자를 식별할 수 있는 코드와, 과금이 필요할 경우 해당 금액에 대한 정보, 추후 서비스 내역의 추적을 위해서 서비스 제공에 대한 해쉬 코드를 포함한다. 이러한 정보들이 최소화 되도록 한다. 이 외의 정보들에 대해서는 사용자가 관리할 수 있도록 홈 도메인 서버로 전달하도록 한다.

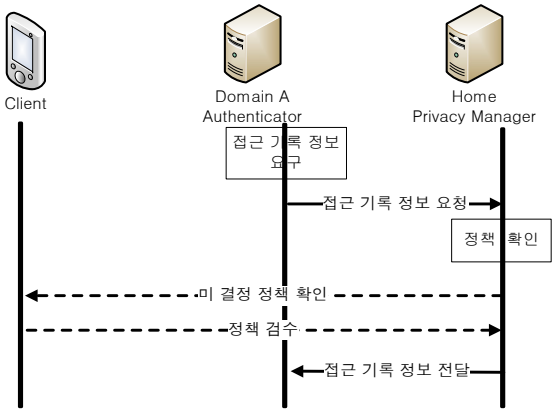

그림 3. 접근 정보 요청 흐름도

그림 3 은 사용자가 관리하는 접근 정보가 요구될 때 해당 정보를 요청하는 흐름을 나타낸다. 서비스 제공자가 필요로 하거나 적합한 절차에 의해서 해당 정보에 대한 추적이 필요하다면 홈 도메인 서버의 URI 로 해당 서비스에 대한 해쉬 코드를 보내고 홈 도메인 서버는 사용자가 미리 정의한 정책에 따라서 해당 정보를 전달할 것인가를 결정하게 된다. 이때 등급을 두어 어느 정도의 정보를 전달할 것인가를 개인의 통제하에서 전달되도록 한다. 만약 기존에 정책이 결정되어 있지 않다면 미 결정 정책에 대해서 사용자가 직접 검사할 수 있도록 한다.

4. 구현

접근 기록 관리 시스템의 구현을 위해서 UPnP 기반의 홈 엔터테인먼트 AV 시스템 상에서 구현하였다. 미디어서버는 Open Source 기반의 MediaTomb[8] 을 사용하였다. 홈 도메인서버는 윈도우 기반으로 작성되었다.

홈 도메인 서버는 다음의 기능을 가진다.

a) 사용자 인증
b) 사용자 접근 기록 정책 관리
c) 접근 기록 정보 관리
d) 접근 기록 정책 전달

미디어 서버에는 다음의 기능이 필요하다.

a) 사용자 및 서비스 제공자 정책 협상
b) 접근 기록 전달

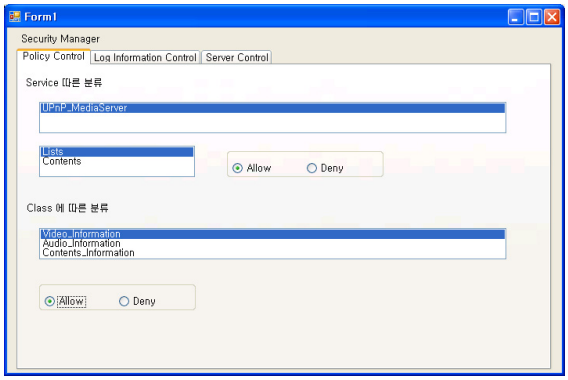

그림 4. 사용자 프라이버시 관리 서버

그림 4 는 홈 도메인 관리 서버의 동작화면이다. 정책은 서비스와 클래스에 따른 분류로 나뉜다. 접근 기록 정보는 각 서비스에 따라서 형태도 다르고 저장해야 하는 정보도 다르다. 따라서 서비스에 따른 분류를 두어 해당 서비스에 맞는 서비스 관리 정책을 지정할 수 있다. 혹은 전체 클래스에 따른 정책 결정으로 시간, 콘텐트 내역 등 에 따른 정책을 지정할 수 있다.

4.2 정보 전달 프로토콜

4.2.1 접근 기록 정보 전달 프로토콜

1) 접근 기록 정보 전달 프로토콜

접근 기록을 전달 하기 위해서는 사용자의 홈 도메인의 정보와 정책을 전달하고 해당 정책에 따라서 접근 기록 정보를 전달하는 메시지가 필요하다. 서비스를 요청하면 서비스 제공자는 사용자의 홈 도메인에게 자신의 서비스 명을 포함하여 사용자의 정책 전달을 요청한다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
  <HomeServer>155.230.118.69</HomeServer>
  <AuthCode>4302c7ee32602c88d91a3d5..</AuthCode>
  <ExpireDate>2007-12-31 23:59:59</ExpireDate>
  <Audio_Information>allow</Audio_Information>
  <ContentInformation>deny</ContentInformation>
</Client>
```

그림 5. 사용자 정책 전달 메시지

그림 5 는 사용자 정책을 전달하는 메시지이다. 홈 도메인 서버는 서비스 명을 확인하여 해당 서비스에 대한 특정 정책을 가지고 있으면 해당 정책을 전송하고 그렇지 않으면 클래스 관련 정책을 전송한다. 클래스 관련 정책으로는 Video, Audio, Contents 와 같이 일반적인 콘텐트의 정의로 구성된 정책을 의미한다. 전송하는 메시지에는 홈 도메인 서버의 주소와 인증 코드, 이 정책 메시지의 유효 기간, 정책들을 정의하고 있다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
  <AuthCode>4302c7ee32602c88d91a3d5..</AuthCode>
  <HashCode>c3557ca22ada1cca1cc...</HashCode>
  <ContentInformation>
    <RawData>Adding content disposition header:
Content-Disposition: attachment; filename="28wits-
sample.avi"</RawData>
  </ContentInformation>
</Client>
```

그림 6. 접근 기록 정보 전달 메세지

그림 6 은 서비스 제공자가 정책에 따른 협상을 한 후 접근 기록을 전달하는 메시지이다. 접근 기록 전달 메시지에는 인증코드와 해당 기록에 대한 유니크 코드로 시간, 콘텐트 ID 를 포함하여 생성한 해쉬 코드를 삽입한다. 협상에 따라서 XML 형태로 접근 기록 정보를 바꾸어 전달한다. 이때 적합한 형태를 구성하지 못하면 Raw data 형태로 전달할 수도 있다.

사용자가 정의한 정책과 서비스 제공자가 정의하는 접근 기록정보에 따라서 전달 데이터를 협상을 한다. 만약 서비스에 대한 사용자의 정책이 존재한다면 그 정책에 따라서 정보를 전달한다. 만약 서비스에 대한 정책이 정의되어 있지 않다면 클래스에 대한 정책을 통해서 서비스가 제공하는 접근 정보와 비교하여 전달할 정보를 결정하는 과정이 필요하다. 콘텐트의 클래스는 Video, Audio, Contents 로 나눈다. 따라서 서비스 제공자가 제공하는 정보의 종류에 따라서 사용자의 정책과 비교하여 접근 정보에 대한 정책을 결정한다.

4.2.2 정보 요청 프로토콜

사용자에게 기록된 접근 기록 정보가 요구될 수도 있다. 서비스 제공자가 개인화된 서비스를 제공하거나 적법한 절차에 따라서 공적인 요구에 의해 개인의 접근 기록을 요청하는 경우가 발생한다. 이 경우 서비스 제공자는 자신이 가지고 있는 해쉬 정보를 사용자의 홈 도메인 서버에 보내어 해당 정보를 요청 할 수 있다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
  <AuthCode>4302c7ee32602c88d91a3d5..</AuthCode>
  <HashCode>c3557ca22ada1cca1cc...</HashCode>
</Client>
```

그림 7. 접근 정보 요청 메시지

요청 받은 접근 정보에 대해서 정책을 확인하고 전송 가능한 정책이면 전송한다. 만약 해당 정책이 정의되어 있지 않다면 사용자의 결정을 요청하고 피드백을 받아서 결정한다.

4.2 구현 결과

UPnP 기반의 홈 엔터테인먼트 AV 환경에서 사용자는 컨트롤 포인터를 이용해서 미디어 서버에 있는 콘텐트를 미디어 랜더러를 통해 이용한다. 기존의 UPnP 환경에서

서비스 제공자는 자신이 제공한 서비스에 대해서 누가, 언제, 어떤 서비스를 제공하였는지에 대한 정보를 서비스 제공자의 데이터 베이스에 관리하고 있었다. 따라서 이러한 정보를 이용하여 사용자를 추적하면 개인의 프라이버시를 침해할 수 있는 문제점이 있었다.

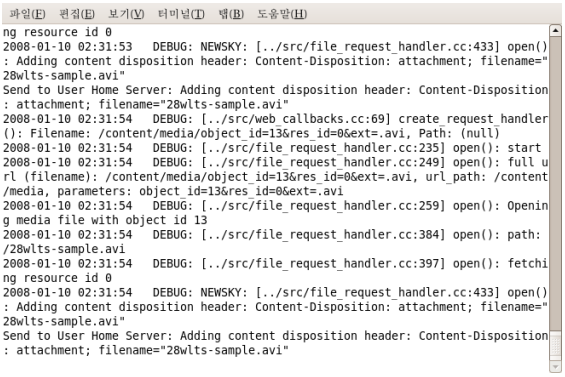

그림 8. 미디어 서버 동작 화면

컨트롤 포인터에서 미디어 서버로 콘텐트를 요청하면 미디어 서버는 컨트롤 포인터로부터 홈 도메인 서버에 대한 정보를 받는다. 해당 정보를 바탕으로 홈 도메인 서버의 사용자의 프라이버시 정책을 수신한다. 수신한 프라이버시 정책을 바탕으로 미디어 서버가 제공하는 접근 기록에서 홈 도메인 서버로 전송할 정보를 추출하고 전송한다. 그림 8 은 미디어 서버가 접근 기록 정보를 저장하고 사용자의 홈 도메인 서버로 전송하는 부분을 보여준다.

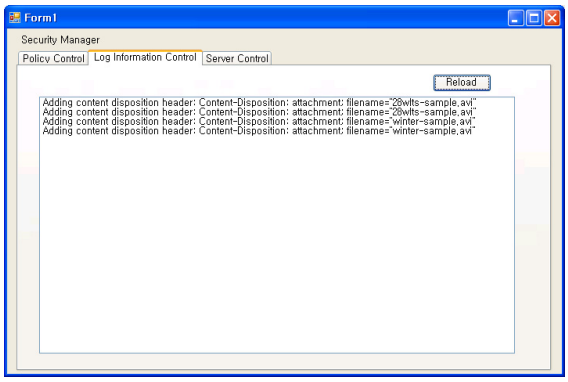

그림 9. 홈 도메인 서버의 접근 기록 관리 화면

그림 9 는 홈 도메인 서버에 서비스 제공자로부터 수신된 접근 기록 정보를 관리하는 화면이다.

기존의 프라이버시를 보호하기 위한 시스템으로 P3P 나 EPAL 의 경우 접근 기록을 관리하는 방법으로는 정책과 데이터가 한곳에 저장되므로 단순히 쿼리를 이용해서 손쉽게 사용자의 정보를 열람할 수 있다[9]. 따라서 서비스 제공자가 악의적인 목적으로 개인 정보의 유출 가능성이 있다. 하지만 제안하는 시스템을 이용하면 개인의 정보를 열람하기 위해서는 개인의 동의가 있어야 한다. 따라서 개인정보의 무분별한 유출을 막을 수 있다. 또한 적합한 권리가 있는 서비스 제공자는 기존의 시스템과 차이가 없이 서비스를 제공할 수 있다.

5. 결론

본 논문에서는 개인의 이동이 자유로운 환경에서 서비스를 제공받을 때 제공받은 서비스 내역에 대한 자기 통제권을 가질 수 있는 시스템을 제안하였다. 사용자는 자신의 서비스 내역에 대한 자기통제권을 가짐으로써 프라이버시를 지킬 수 있고 서비스 제공자는 많은 개인 정보를 보호해야 하는 부담을 덜 수 있게 되었다. 또한 접근 기록 데이터는 개인이 보관하지만 해당 데이터의 이용이 필요할 때에는 적합한 절차에 의한 검색이 이루어 질 수 있었다.

향후에는 OpenID 와 같은 표준화된 인증절차와 연결하여 실질적인 사용을 이루도록 노력하여야 한다. 또한 사용자는 서비스를 제공받을 때 프라이버시 관리 방식을 미리 인지하여 서비스를 제공받을 때 선택권을 줄 수 있도록 해야 한다.

참고문헌

[1] E. Gustafsson and A.Jonsson, "Always best connected," IEEE Wireless Communication., Vol. 10, No. 1, pp.49-55, Feb. 2003

[2] 서운석, 신순자, 구자동, 임진수 “유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향 연구,” 한국전산원, 2004

[3] 홍종현, "유비쿼터스 환경에서의 개인정보 보호", Public Law Korean Public Law Association, Vol. 32, No. 5, Jun. 2004

[4] OpenID, http://openid.net

[5] Gaia, http://gaia.cs.uiuc.edu

[6] Platform for Privacy Preferences, http://www.w3.org/P3P

[7] 이제훈, 김상욱, “유비쿼터스 환경에서 프라이버시 보호를 위한 동적 접근 제어 시스템”, 정보과학회 추계학술발표대회, Vol. 34, no. 2, pp.118-121, Oct. 2007

[8] MediaTomb, http://www.mediatomb.cc

[9] S.Sackmann, J. Struker, R.Accorsi, “Personalization in Privacy-Aware Highly Dynamic Systems”, Communications of the ACM, Vol. 49, No. 9, pp.32-38, Sep, 2006