논문 2010-47CI-6-2

추상화 기반 상황정보 접근 제어 프레임워크

(Abstraction Based Context Data Access Control Framework)

김 윤 삼*, 조 은 선*, 조 위 덕**

(Yun-Sam Kim, Eun-Sun Cho, and We-Duke Cho)

요 약

유비쿼터스 시스템의 발달에 따라 시스템이 다루는 상황정보의 숫자 또한 크게 증가하고 있다. 이러한 상황정보 중에는 정보보호 관점에서 중요한 데이터들이 다수 존재한다. 이러한 중요한 상황정보가 다른 사용자 또는 서비스에게 제공됨에 따라 개인정보의 과도한 노출 가능성 또한 크게 증가되고 있다. 이러한 과도한 정보의 노출을 위하여 여러 시스템은 접근 제어 기법을 주로 이용하나 이러한 기존 기법은 허가되지 않은 정보의 접근을 막을 수는 있으나 허가된 정보의 제공에서 발생하는 과도한 정보의 노출은 막을 수 없다는 문제점을 가지고 있다. 본 논문은 이러한 개인정보의 과도한 노출을 막기 위하여 상황정보를 추상화하여 제공하는 접근 제어 프레임워크를 제안한다. 상황정보의 과도한 노출을 막기 위하여 협상 프로토콜과 RDF를 이용한 상황정보 추상화를 제공하며, 이를 통하여 개인정보의 보호와 동시에 서비스의 연속성을 유지한다.

Abstract

As Ubiquitous systems are developed, the number of context data which are dealt with systems also grow rapidly. In these data, some are vary important in privacy view. As these data are given to users or services of systems, probability of excess exposing of data is exist. To solve this problem, many systems use access control method like RBAC. But even this method can avoid unauthenticated access, can not prevent excess exposing of authenticated access. To prevent this exposing of context data, this paper suggests context data access control framework which abstracts context data when system gives these data to users or services. Using negotiation protocol and context data abstraction technique using RDF, our framework prevents excess exposing important data. This happens protecting privacy and keeping service continuity.

Keywords : 상황정보, 추상화, 접근제어, 협상, 정보보호

Ⅰ. 서 론

유비쿼터스 시스템의 발전에 따라 시스템의 적용범위가 집 또는 사람에서 벗어나 빌딩, 학교 등과 같이 점차 넓어지고 있으며 이에 따라 시스템의 사용자 수가 증대되고 시스템에서 제공하는 서비스 또한 다양해지고 있다[1]. 이에 따라 유비쿼터스 시스템에서 다루는 상황정보의 숫자는 꾸준히 증가하고 있으며, 이러한 정보 중에는 날씨, 온도와 같이 개인정보보호의 측면에서 중요하지 않은 정보뿐 아니라 주민등록번호, 위치 정보와 같이 개인의 사생활과 관련된 정보들 또한 존재한다.

이러한 상황정보 중 개인정보보호에 민감한 상황 정보에 대한 접근은 엄격한 제한을 두어야 하며, 그렇지 않은 경우 정보의 노출에 의한 직접 또는 간접적인 문제가 발생할 수 있다. 예를 들어 경찰이 검문의 목적으로 운전면허증을 가지고 있지 않은 운전자에 대하여 지문을 통하여 운전자의 정보를 파악할 경우 경찰은 자신에게 직접적으로 필요한 정보인 주민등록번호, 이름 등의 정보 뿐 아니라 주소, 전화번호와 같은 운전자의 신

* 정회원, 충남대학교 컴퓨터공학과
(Dept. of Computer Science and Engineering, Chungnam National University)
** 정회원, 아주대학교 유비쿼터스시스템연구센터
(Center of excellence for Ubiquitous System, Ajou University)
※ 본 연구는 지식경제 프론티어기술개발사업의 일환으로 추진되고 있는 지식경제부의 유비쿼터스컴퓨팅 및 네트워크원천기술개발사업의 09C1-T3-10M 과제로 지원된 것임
접수일자: 2010년9월23일, 수정완료일: 2010년10월25일

분 파악을 위해 필요하지 않은 정보를 요청할 때 시스템이 상황 정보의 요청에 대하여 적절히 거르지 않고 무분별적으로 중요한 정보를 제공할 경우 불필요한 정보의 노출이 발생할 수 있다. 그러나 주소, 전화번호와 같은 상황정보 같이 운전자의 신분 파악을 위해서는 필요하지 않은 정보이지만 다른 업무에서는 필요한 정보일 수 있으므로 무조건 해당 정보에 대한 접근을 금지시킬 수는 없다.

이러한 정보의 노출을 해결하기 위하여 여러 시스템들은 RBAC[2~3]이나 TMAC[4~5]과 같은 접근 제어 시스템을 사용한다. 이러한 접근 제어 시스템은 사용자 또는 서비스가 특정 상황정보에 접근하려 하는 경우 미리 기술된 정책을 토대로 하여 상황정보에 대한 접근을 허가 또는 불허한다. 상황정보에 대하여 접근이 허가된 경우에는 해당 상황정보를 사용자 또는 서비스에게 제공하고, 불허인 경우 해당 정보를 제공하지 않고 접근이 불허되었음을 알린다. 즉, 경찰이 시스템에게 요청하는 운전자의 정보에 대하여 주민등록번호, 이름에 대하여 정책을 통하여 접근을 허가하고 주소, 전화번호에 대하여 접근을 불허하는 방식으로 상황정보의 접근을 통제할 수 있다. 그러나 이러한 접근제어 시스템은 상황정보에 대한 접근만을 통제하므로, 접근이 허가되는 상황정보에 대한 과도한 정보의 노출은 막을 수 없다는 단점이 있다. 즉, 예를 들어 주민등록번호는 사람을 구별할 수 있는 가장 강력한 정보 중 하나로써 주민등록번호는 인터넷 및 여러 환경에서 개인을 인증할 때 사용하기도 한다. 따라서 주민등록번호가 완전히 공개되는 경우 경찰이 시스템에서 접근 가능한 정보 중 하나인 주민등록번호와 이름을 임의의 장소에 저장하여 이를 악용할 수 있다는 문제가 있으며, 시스템과 사용자 또는 서비스 간의 상황정보의 전달을 중간에서 가로채 악용할 수도 있다. 그러나 이러한 문제를 방지하기 위하여 주민등록번호를 제공하지 않는 경우 경찰은 업무를 지속할 수 없다. 따라서 이러한 문제를 해결하기 위한 방법으로 접근 제어 시스템에서 허용하는 상황정보의 경우에도 목적에 따라 데이터의 일부분을 보여주거나 범위의 형태로 정보를 제공함으로써 정보의 노출을 제어 할 필요가 있다. 정보의 노출 정도를 제어함으로써 과도한 정보의 노출을 어느 정도 방지할 수 있으며 서비스의 연속성도 유지할 수 있다. 예를 들어 경찰이 주민등록번호를 알려는 이유가 나이를 알기 위한 경우인 경우 111111-2222222와 같은 정확한 정보보다 11XXXX-XXXXXXX와 같이 연도만 알려주거나 본인 확인을 위하여 111111-XXXXXXX와 같이 앞자리만 알려줄 수 있다. 이렇게 상황정보를 추상화하여 일부만 제공하는 경우 기존 접근 제어 시스템에서는 정보의 과도한 노출 발생할 수 있어 정보의 접근을 불허하는 경우를 해결할 수 있어 상황정보에 대한 개인정보를 보호하는 동시에 서비스의 연속성을 높일 수 있다는 장점이 있다.

본 논문은 이러한 유비쿼터스 시스템에서 제공하는 상황정보에 대하여 협상 프로토콜을 이용하여 서비스의 연속성을 높이는 동시에 상황정보를 추상화하는 접근 제어 프레임워크를 제안한다. Ⅱ장의 관련연구는 기존의 개인정보보호를 위한 기법들을 설명하고, Ⅲ장은 본 논문에서 제안하는 추상화 기반 상황정보 추상화 프레임워크를 논한다. Ⅳ장은 본 논문의 결론을 이야기한다.

Ⅱ. 관련 연구

1. 온톨로지를 이용한 추상화

개인정보보호를 위하여 널리 쓰이는 기법 중 하나는 온톨로지를 이용하는 방법이다[6]. 온톨로지를 이용한 정보의 보호는 정보의 추상화를 위한 온톨로지를 만들고 상황정보를 이에 대입하여 추상화한다. 온톨로지는 레벨의 개념을 가지고 있으며, 레벨이 높을수록 상황정보의 추상화 정도가 높음을 나타낸다. 이러한 온톨로지를 이용한 기법은 모든 상황정보에 대하여 각각 온톨로지를 정의해야 하며, 추상화되는 값이 자동적으로 계산되는 것이 아니라 사용자가 손으로 정해줘야 하기 때문에 사용자의 오버헤드가 크게 증가하는 문제가 있다. 또한 보안을 위한 정책과 추상화를 위한 정책이 따로 존재하기 때문에 접근제어 정책 기술에 대한 복잡도가 높아지는 단점도 있다.

2. 상황정보의 블러링

I.T. Emin[7]은 상황정보를 두 가지로 분류하여 중요한 상황정보에 대한 보호를 하고 있다. 하나는 보호되어야 하는 상황정보이며, 또 하나는 계산된 상황정보이다. 이 중 보호되어야 하는 상황정보를 전달할 경우 계산된 상황정보와 주변의 상황을 보고 상황정보의 전달 상태를 결정한다. 이러한 전달 상태는 정직한 정보, 블러링된 정보, 해당 정보가 없음, 그리고 거짓된 정보의 네 가지 형태 중 하나의 형태를 지닌다. 이러한 형태 중

정보가 없음은 서비스의 연속성을 저해시킬 수 있으며, 거짓된 정보는 사용자 또는 서비스가 잘못된 행동을 할 수 있기 때문에 거짓된 정보를 함부로 제공하는 것은 위험할 수 있다.

3. K-Anonymity

K-Anonymity[8~9]는 대량의 데이터에 대한 추상화를 위하여 연구된 최근 기법 중 하나로써, 제공하는 정보들을 k개 이상의 똑같은 정보의 셋을 포함하도록 함으로써 그 정보의 소유자가 누구인지 알 수 없게 하는 기법이다. 이러한 k-Anonymity는 일반화와 삭제를 통하여 정보보호를 이룬다. 일반화는 각각의 정보를 추상화된 값으로 만들며 삭제는 하나의 행 또는 튜플을 삭제한다. 삭제는 정보를 가진 개체 자체를 삭제하므로 정보에 대한 신뢰성이 낮아질 수 있다. 이러한 k-Anonymity는 그 자체의 문제점으로 인하여 이를 해결하기 위한 l-Diversity[10]나 t-Closeness[11]과 같은 기법들이 소개되고 있다. 이러한 k-Anonymity는 데이터베이스 또는 대량의 표와 같이 대량화 되고, 정형화된 정보들에 대하여 추상화를 하기 때문에 유비쿼터스와 같은 상황정보의 요청에 이를 대입하는 것은 무리가 있다. 또한, k-Anonymity의 일반화는 모든 데이터를 일정한 레벨의 형태로 추상화함에 따라 k-Anonymity 이하로 일반화된 정보를 얻을 수 없다. 따라서 유비쿼터스 시스템에서 일반화된 상황정보를 제공할 경우 서비스의 연속성이 크게 저하될 수 있다.

4. 시간 기반 추상화

의학적인 데이터의 추상화를 위한 기법으로 주로 쓰이는 시간 기반 추상화[12]는 일정 주기로 스캔되는 의학 데이터를 추상화하여 알려주는 방법으로써, 추론을 통하여 데이터를 추상화한다. 그러나 추상화의 데이터는 미리 정해진 값들로만 추상화가 되므로 상황에 따른 다양한 추상화가 불가능하다. 또한 일정기간을 통해서 수집되고 평균이 계산되는 형태의 정보만 사용이 가능하므로 유비쿼터스 시스템의 대부분의 상황정보에 이용하기에는 힘든 면이 있다. 또한 추상화 레벨이 단순함으로써 다양한 서비스에 적용하기 힘들다는 문제가 있다.

5. View 기반 상황정보 추상화

View 기반 상황정보의 추상화[13]은 RDF에 대한 질의 결과의 View에 추상화를 진행하는 방법으로써 View에 대한 추상화를 RDF의 형태에서 제공한다. 이러한 기법의 장점은 View의 제어를 통하여 자유로운 추상화가 가능함이 있다. 그러나 추상화가 RDF 작성과 View 제어로 나뉨에 따라 데이터베이스와 View에 대한 이해가 부족한 경우 사용이 힘들며, 추상화를 위한 복잡도가 증가하게 된다. 이에 비하여 RDF와 추론을 이용할 경우 사용자는 RDF만을 작성하면 되며, 또한 이러한 RDF는 일정한 패턴을 가지며, 추상화를 위한 값들만 지정을 하면 되므로 RDF의 작성이 자동화될 수 있는 여지가 크다.

Ⅲ. 본 론

1. 시나리오

홍길동은 자신의 건강에 관심이 많으며, 운동추천 서비스를 제공하는 의사를 통하여 자신에게 맞는 운동을 처방해주는 서비스를 제공받고 싶어 한다. 이를 위하여 홍길동은 운동추천 서비스를 제공하는 의사에게 자신이 운동 추천을 받고 싶음을 알리고 서비스를 요청한다. 이 때 홍길동은 의사가 자신의 어떠한 정보를 이용하여 운동추천을 하는지 알 수 없으므로 홍길동이 운동추천을 요청할 때 필요한 상황정보가 동시에 의사에게 전달되지는 않는다. 의사는 홍길동이 운동추천 서비스를 요청했음을 알고, 운동 추천을 위하여 홍길동의 시스템에게 키, 몸무게, 나이, 근력 등과 같은 필요한 정보를 요청하고, 시스템은 필요한 정보를 의사에게 전달한다. 의사는 시스템에게서 받은 홍길동의 정보를 바탕으로 각각의 정보를 미리 정의된 테이블과 비교하여 홍길동의 현재 상태를 파악하고 홍길동에게 맞는 운동을 처방한다. 처방된 결과는 홍길동의 휴대폰에 전달되며, 홍길동은 받은 정보를 바탕으로 운동을 한다.

2 간략한 시스템의 구성

앞 절의 시나리오는 정보보호의 관점에서 큰 문제점을 지니고 있다. 즉, 홍길동의 시스템은 서비스를 제공하는 의사가 요청하는 상황정보의 접근에 대하여 아무런 판단을 하지 않고 사용자의 정보를 제공하므로 의사가 악의를 가지는 경우 의사는 홍길동의 이름, 주민등록번호 및 카드 번호 등과 같이 의사에게 필요가 없는 정보를 요청할 수 있으며, 홍길동의 시스템이 이러한 악의적인 정보의 접근에 대하여 아무런 조치를 하지 않기 때문에 홍길동의 중요한 정보들이 의사에게 유출되

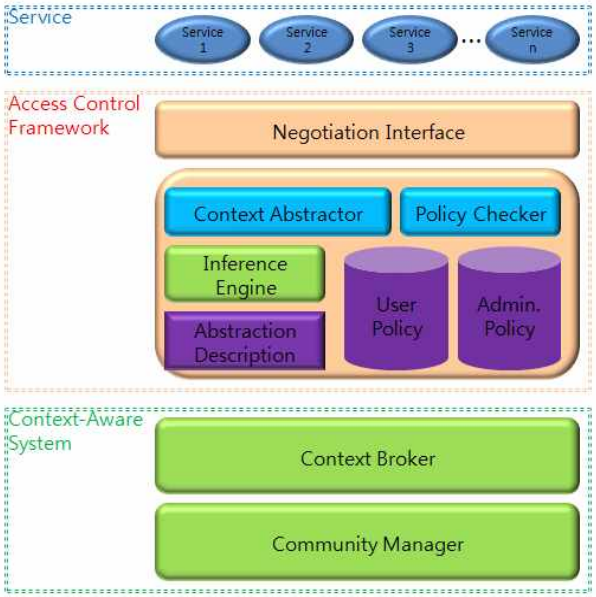


그림 1. 접근 제어 프레임워크가 포함된 시스템
Fig. 1. Access control framework and applied context-aware system.

게 된다. 또한, 의사가 운동추천을 위하여 적합하게 사용하는 키, 몸무게, 근력과 같은 정보들은 미리 작성된 데이터 테이블에 의하여 이상 상태를 파악하기 때문에 홍길동의 경우 키, 몸무게 등에 대하여 자신의 정확한 값을 전달할 필요가 없이 결과에 이용될 수 있을 정도의 범위 내에서 추상화된 값을 전달할 경우 서비스의 연속성은 유지하면서 정확한 값을 노출하지 않으므로 정보보호의 효과를 동시에 누릴 수 있다. 이를 위하여 본 논문은 추상화를 이용한 접근제어 프레임워크를 제안하며, 상황 정보 추상화를 위한 전체 시스템은 그림 1과 같다. 제안하는 접근 제어 프레임워크는 상황정보의 추상화와 협상에 대한 아이디어를 학회에서 발표를 하였으며, UCN 시스템[14]과 연동하여 동작중이다. 접근 제어 프레임워크는 하단의 유비쿼터스 시스템의 Context Broker에서 추상화에 필요한 정보를 전달받아 추상화하고 이를 사용자 또는 서비스에게 전달한다. 이러한 접근제어 프레임워크는 모듈의 형태로 개발이 되어 다른 여러 시스템에 쉽게 적용이 가능하다.

접근 제어 프레임워크는 크게 상황정보를 추상화하는 부분과 사용할 수 있는 한도 내에서 최대한 추상화된 상황정보를 사용자 또는 서비스에게 제공하기 위한 협상 부분으로 나누어진다. 협상은 사용자 또는 서비스가 상황 정보를 요청할 때 자신이 필요로 하는 상황 정보의 종류와 사용 목적, 자신이 감내할 수 있는 최대 추상화 레벨 등의 정보를 XML[15] 형태로 적어 보내면 시스템은 그 정보를 상황정보 추상화 부분으로 넘겨 추상화된 결과를 받게 된다. 협상 부분은 받은 정보에 대하여 그 정보의 형태와 추상화된 값을 사용자 또는 서비스에게 전달한다.

상황정보 추상화는 먼저 텍스트 형태로 작성되는 사용자 정의 정책(User Policy)과 관리자 정의 정책(Admin Policy)을 이용하여 사용자 또는 서비스의 접근이 가능하지 파악하고, 접근이 가능한 경우 정책에서 정의한 상황정보와 추상화 레벨, 상황정보의 소유자 그리고, 상황정보를 이용하려는 사용자 또는 서비스 등을 RDF로 기술한 추상화 기술 파일(Abstraction Description)에 넘긴다. 그러면 추상화 기술 파일은 받은 정보를 RDF[16]의 형식으로 저장하고 이를 추론하여 추상화 가능한 최솟값을 정하고, 사용자 또는 서비스에게서 받은 추상화 문서를 이용하여 추상화 가능한 최댓값을 정하여 최대화된 추상화 정보를 협상 부분에게 전달한다.

3. 상황정보의 추상화

(1) 상황정보의 분류 및 추상화

이러한 상황정보의 추상화를 자동화하기 위하여서는 상황정보의 특성에 맞게 추상화 방법을 선택하여야 한다. 본 연구의 선행 연구[16]은 이러한 상황정보를 추상화 온톨로지에 연결되는 형태에 따라서 세 가지 형태로 분류하고 있다. 그 각각을 Class I과 Class II 및 Class III로 나타내며, Class I과 Class II는 R. Wishart[6]의 분류를 이용하고 있다. Class I은 추상화 온톨로지의 값 그 자체가 추상화된 상황정보를 의미하는 상황정보를 나타낸다. 그림 2의 (a) Activity Ontology의 경우 Watching TV은 Watching Program의 추상화된 값을 나타낸다. Class I은 상황정보와 추상화된 값이 의미상으로 추상화되는 형태로 연결되며, 추상화 온톨로지 또한 사용자에 따라 각각 다르기 때문에 Class I은 자동으로 추상화를 하는 것이 불가능하다.

Class II는 키, 몸무게와 같이 그 추상화 값이 온톨로지의 특성에 따라 변화되는 상황정보를 나타낸다. 즉, 키가 174cm인 경우 값을 170~180cm와 같은 형태로 나타내어 추상화시킨다. 그림 2의 (b), (c)인 장소를 나타내는 상황정보와 사람의 이름을 나타내는 상황정보 등이 그 예를 나타낸다. 제안하는 접근 제어 프레임워

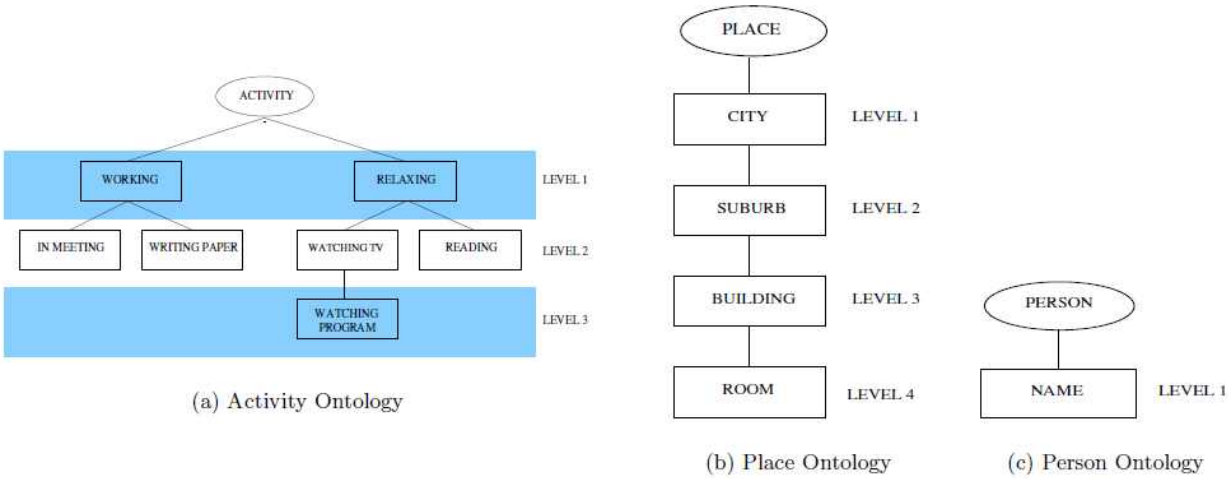


그림 2. Obfuscation을 위한 온톨로지
Fig. 2. Ontologies for obfuscation[6].

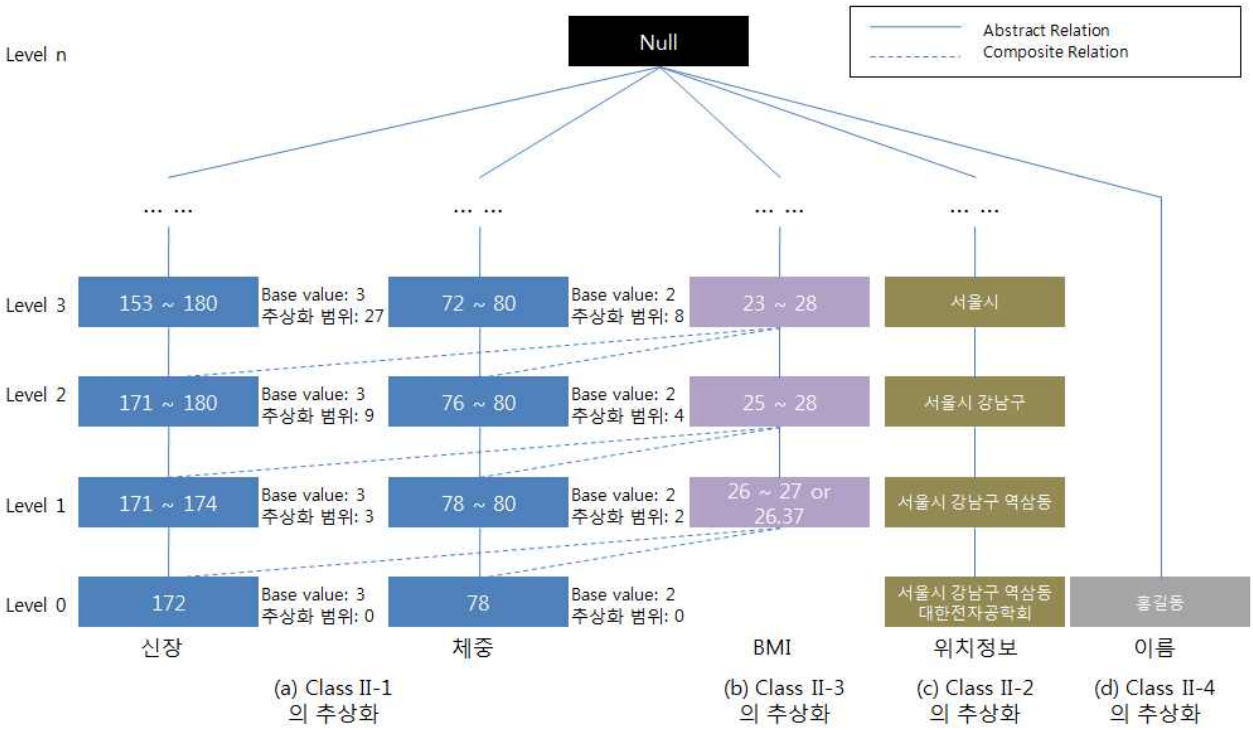


그림 3. Class II 상황정보의 분류 및 추상화
Fig. 3. Classifying and abstraction of context data of Class II[17].

크는 이러한 Class II에 해당하는 상황정보를 다시 4가지의 형태로 나누어 이를 각각 다른 방법으로 추상화한다. 우리는 이러한 상황정보의 집합을 Class II-1, Class II-2, Class II-3, Class II-4로 다시 분류한다[17]. 그림 3은 각 클래스에 해당하는 상황정보의 예이다. Class II-1은 키, 몸무게와 같이 상황정보가 숫자의 형태로 되어있으며, 그 정보가 센서 또는 사용자의 직접 기록에 의하여 만들어지는 상황정보를 나타낸다. 이러한 상황정보는 범위 값으로 추상화하며, 추상화는 사용자가 지정하는 기본 값의 차승형태로 추상화된다. 즉, 키가 174cm이며 키에 대한 기본 값이 2인 경우 추상화 레벨이 1인 경우 174cm~176cm의 값을 가지고, 추상화 레벨이 2인 경우 172cm~176cm의 값으로 추상화가 진행된다. 선행 논문의 논문에서 정의된 Class II-1의 경우

추상화 값을 사용자가 각 레벨에 대한 추상화 값을 지정하였으나 이 경우 각 레벨에 따른 상황정보를 획득할 수 있는 경우 원래의 값을 알 수 있는 경우가 있으며, 레벨을 추상화하기 위한 RDF의 작성의 자동화가 힘들기 때문에 추상화 값은 일률적인 계산을 통하여 추상화를 이루게 된다.

Class II-2는 위치정보, 시간 등과 같이 그 정보 자체가 추상화를 가지는 상황정보의 집합을 나타낸다. 시간의 경우 '년-월-일-시-분-초'의 형태의 경우 월은 연도의 하위 정보이며, 일은 월의 하위 정보라고 볼 수 있다. 이러한 정보들의 경우 하위 정보를 하나씩 제거함으로써 상황정보의 추상화를 이룰 수 있다. 즉, 시간의 경우 '년-월-일-시'의 경우 '년-월-일-시-분'에 대하여 좀 더 추상화된 시간을 나타내므로 사용자 또는 서비스가 시간에 대한 상황정보를 요청할 경우 '년-월-일-시-분'이 아닌 '년-월-일-시'의 형태의 정보를 제공함으로써 좀 더 추상화된 값을 전달 할 수 있다.

Class II-3은 다른 상황정보에 의하여 만들어지는 상황정보의 집합을 나타낸다. 다른 상황정보들이 센서 등에 의하여 생성되는 기본적인 정보임과 다르게 Class II-3은 BMI 등과 같이 센서 등에 의하여 생성되지 않고 다른 상황정보를 조합하여 새롭게 생성된 상황정보를 나타낸다. 이러한 조합된 상황정보는 시스템에서 존재하지 않을 가능성이 많으며, 해당 정보가 존재하지 않는 경우 키, 몸무게와 같이 상황정보의 계산에 쓰이는 기본적인 정보를 직접 전달하여 사용자 또는 서비스가 처리하는 방법이 있으나 조합된 상황정보를 제공할 경우 계산의 바탕이 되는 기본적인 상황정보의 값을 유추할 수 없어 그 값이 외부로 유출 될 경우 기본적인 정보를 제공하는 것보다 상황정보의 소유자에 대한 익명성을 높일 수 있으며, 기본적인 상황정보를 조합하여 새로운 상황정보를 만드는 것 자체가 기본적인 정보에 대한 또 다른 방법의 추상화가 되므로 조합된 상황정보를 제공함으로써 향상된 개인정보보호를 이룰 수 있다.

Class II-4는 추상화할 필요가 없거나 추상화를 하면 안 되는 상황정보를 나타낸다. 예를 들어 날씨 또는 외부의 온도와 같은 상황정보의 경우 Class I의 형태로 추상화 하거나 Class II-1의 형태로 추상화를 할 수는 있다. 그러나 이러한 정보들은 유비쿼터스 시스템이 아니라도 다른 일반적인 시스템이나 직접적인 관찰이 가능하므로 추상화하여 얻을 수 있는 효과는 거의 없으며, 추상화를 함에 따라 발생하는 추론에서 불필요한 오버헤드가 생기게 된다. 또한 이름과 같은 정보의 경우 이름을 추상화시킬 경우 그 의미가 없어지게 되며, 시스템에 따라 시스템의 특정 상황정보를 접근하려면 그 사람의 이름을 알아야 하기 때문에 추상화된 이름을 알려줄 경우 시스템의 서비스를 이용할 수 없는 경우도 발생하게 된다. 이러한 특징을 가진 상황정보들은 추상화를 하지 않은 상태에서 정보를 전달하거나 그 결과를 전달하지 않는 방법을 취한다.

Class III는 Class I과 Class II의 조합에 의하여 생성되는 상황정보로써 본 논문은 Class I과 Class II에 해당되는 상황정보의 추상화를 각각 제공함으로써 추상화를 해결한다.

(2) 접근 제어 정책의 기술

접근 제어 프레임워크의 정책의 정의는 기존 RBAC이나 TMAC과는 다르게 정책을 사용자 정의 정책과 관리자 정의 정책의 2단계로 나누어 정의한다. 기존 RBAC등의 접근 제어 기법은 상황정보의 소유자 또는 시스템의 관리자가 모든 정책을 기술함에 따라 소유자가 정책을 기술할 경우 시스템을 사용하는 각각의 소유자가 시스템에서 동작하는 모든 서비스의 종류와 각각의 서비스가 요구할 수 있는 소유자의 상황정보를 알고 있어야 하며, 관리자가 정책을 기술할 경우 시스템을 이용하는 각각의 사용자들이 가지고 있는 상황정보를 알아야 하기 때문에 기존 접근 제어 기술의 정책은 시스템의 크기가 클 경우 적절히 적용하기 힘들다. 이를 해결하기 위하여 제안하는 접근 제어 프레임워크는 정책을 사용자 정의 정책과 관리자 정의 정책으로 나누어 사용하며, 관리자는 '특정 역할(Role)을 가진 사용자 또는 서비스가 어떠한 목적으로 접근을 할 수 있다 또는 없다'를 나타내는 정책을 기술하며, 상황정보의 소유자는 '특정 목적에 대하여 자신이 가지고 있는 상황 정보에 대하여 접근이 가능하거나 불가능하며, 접근이 가능한 경우에는 어떠한 레벨까지 접근이 가능하다'라는 사용자 정의 정책을 기술한다. 정책의 기술은 표 1과 같다.

*Role*은 사용자 또는 서비스가 시스템에서 맡은 역할을 의미하며, 사용자 또는 서비스에 대하여 직접 정책을 기술하지 않음으로 하여 정책 기술에 대한 효율성을 높일 수 있다. 관리자 정의 정책의 *Permission1*과 사용자 정의 정책의 *Permission2*는 Allow 또는 Deny의 단어를 가지며, Allow는 상황정보에 대한 접근 가

표 1. 접근제어 정책의 기술 및 예
Table 1. Description of access control policies and an example.

[Admin Policy] *AdminPolicy = Permission 1 Role Action To Purpose* [User Policy] *UserPolicy = Permission2 Purpose Action To ContextData AtLevel AccessLevel When Condition* [System Policy] *Policy=AdminPolicy X UserPolicy* *Permission1, Permission2∈Permission* *Permission = {Allow | Deny}* *Action = CanAcess*
[Example] {*Allow* Doctor *CanAccess To* prescribeExercise} X {*Allow* prescribeExercise CanAccess To Kil-Dong's Height *AtLevel* 5}

능을 나타내며 Deny는 접근 불허를 나타낸다. 정책이 기술되지 않았을 경우에는 Deny로 판단하며, 사용자 정의 정책과 관리자 정의 정책 양쪽에서 접근을 제어함으로써 어느 한 쪽이 의도적으로 정보를 노출하는 것을 방지한다. 즉, 관리자 정책에서 서비스가 원하는 목적에 대하여 접근을 허용한다고 하여도 사용자가 목적에 대한 상황정보의 접근을 막을 경우 해당 상황정보에 대한 접근은 불가능하다. *Purpose*는 상황정보를 사용하려는 목적을 나타내며, *Purpose*를 이용하여 사용자 정의 정책과 관리자 정의 정책이 연결된다. *ContextData*는 사용자 또는 서비스가 정의된 *Role*이 요구하는 상황정보를 나타내며, 이 상황정보는 사용자 정의 정책을 기술하는 사용자가 가진 상황정보로 제한된다. *AccessLevel*은 *Role*이 접근 가능한 추상화 범위를 나타내며, 기본 값은 Abstraction Description에서 RDF의 형태로 기술되며, Class II-1은 기본 값^{AccessLevel}의 형태로 최소 추상화 값이 설정되며, Class II-2는 *AccessLevel* 이하의 레벨 정보를 제거하는 방식으로 최소 추상화 값이 설정된다. 그리고 Class II-3은 자신의 AccessLevel보다 1만큼 작은 기본 상황정보를 이용하여 값을 추상화한다.

(3) 상황정보의 요청 및 전달

본 논문에서 제안하는 접근제어 프레임워크는 상황정보의 요청과 전달은 협상을 통하여 이루어진다. 그림 4는 사용자 또는 서비스와 유비쿼터스 시스템 간의 상황정보 요청 및 전달의 과정을 나타낸다. 사용자 또는 서비스는 원하는 상황정보를 요청하기 위하여 협상 프로토콜에 준하는 문서 작성하여 유비쿼터스 시스템에게 전달하고, 문서를 받은 시스템은 접근 제어 프레임워크의 협상 인터페이스에게 그 문서를 전달한다. 협상 문서는 P3P[18] 문서와 유사한 XML 형식을 띄고 있으며,

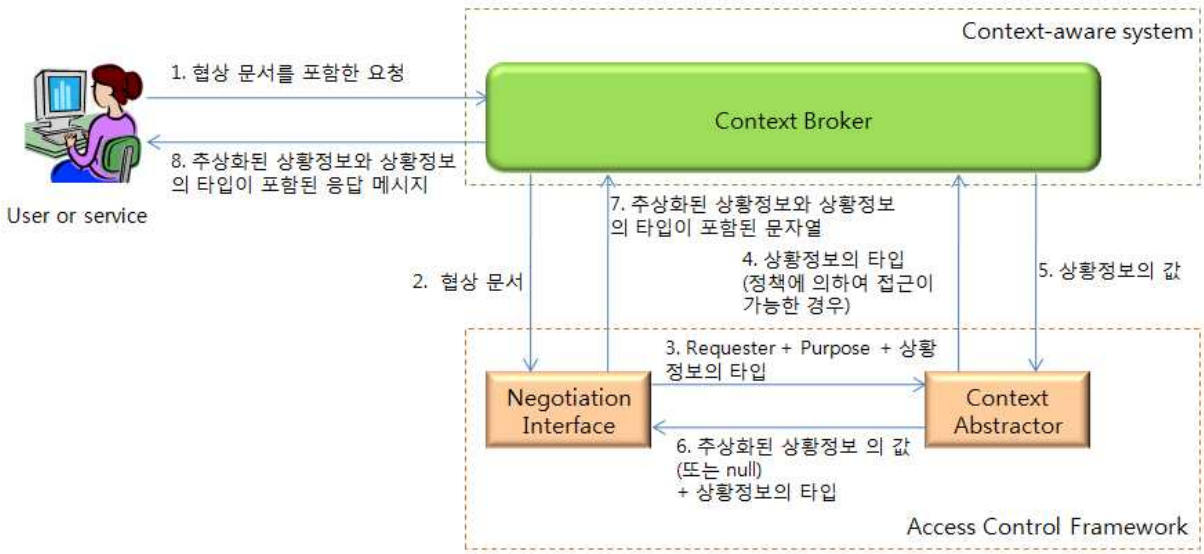


그림 4. 상황정보의 요청 및 전달
Fig. 4. Request and response of context data.

```
<META xmlns="http://plas.cnu.ac.kr/2009/07/ACv01">
   <CONTEXT-PREFERENCES>
      <METHOD>GET</METHOD>
      <REQUERSTER>U-Health</REQUESTER>
      <ISSUER>Kil-Dong</ISSUER>
      <PURPOSE>Select Exercise</PURPOSE>
      <OPTIONAL>
          <RESULT-SET>True</RESULT-SET>
      </OPTIONAL>
      <REQUEST-CONTEXTDATA>
          <CONTEXTDATA>
              <CONTEXTDATA-PRIORITY>1
              </CONTEXTDATA-PRIORITY>
              <CONTEXTDATA-TYPE>Weight
              </CONTEXTDATA-TYPE>
              <ABSTRACTION-TYPE>ClassII-1
              </ABSTRACTION-TYPE>
              <ABSTRACTION-UPPERBOUND>10
              </ABSTRACTION-UPPERBOUND>
          <AND-CONTEXTDATA>
              <CONTEXTDATA-TYPE>Height
              </CONTEXTDATA-TYPE>
              <ABSTRACTION-TYPE>ClassII-1
              </ABSTRACTIOM-TYPE>
              <ABSTRACTION-UPPERBOUND>20
              </ABSTRACTION-UPPERBOUND>
          </CONTEXTDATA>
          <CONTEXTDATA>
              <CONTEXTDATA-PRIORITY>2
              </CONTEXTDATA-PRIORITY>
              <CONTEXTDATA-TYPE>BMI
              </CONTEXTDATA-TYPE>
              <ABSTRACTION-TYPE>ClassII-3
              </ABSTRACTION-TYPE>
              <ABSTRACTION-UPPERBOUND>5
              </ABSTRACTION-UPPERBOUND>
          </CONTEXTDATA>
      </REQUEST-CONTEXTDATA>
   </CONTEXT-PREFERENCES>
</META>
```

그림 5. 협상 문서의 예
Fig. 5. An example of negotiation document.

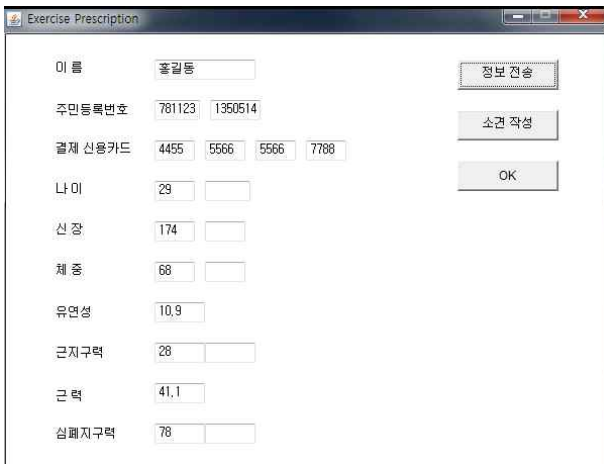
이는 추후 P3P와의 연동 및 호환이 되도록 하기 위함이다. 그림 5는 협상 문서의 예로써 BMI 정보를 얻기 위한 협상 문서이다. ***REQUESTER*** 테그는 상황정보를 얻기 위한 서비스가 U-Health임을 의미한다. ***REQUESTER***에 기술된 상황정보의 요청자 또는 서비스는 시스템에 의하여 정책에 기술되어 있는 역할(Role) 중 하나로 바뀌게 된다. ***ISSUER***는 U-Health가 요구하는 상황정보의 소유자를 나타내며, ***PURPOSE***는 상황정보를 사용하려는 목적을 나타낸다. 즉, U-Health 서비스는 운동 추천을 위하여 Kil-Dong의 상황정보를 요구하며, 그 요구하는 상황정보는 키와 몸무게 또는 BMI 정보 둘 중 하나임을 나타낸다. 키의 경우 허용 추상화 범위는 20이며, BMI의 허용 추상화 범위는 5이다. 시스템은 키와 몸무게를 전송하는 경우 키와 몸무게 양쪽의 상황정보를 전달하여야 하며, BMI를 전달하는 경우에는 키와 몸무게는 서비스에게 전달할 필요가 없다.

협상 인터페이스는 문서의 기록된 정보를 바탕으로 상황정보 추상화 모듈에 사용자 또는 서비스가 요청한 상황정보에 대하여 우선순위를 정하고 우선순위에 따라서 정보를 전달한다. 필요한 정보를 받은 상황정보 추상화 모듈은 정책 검사기를 이용하여 상황정보에 대하여 접근이 가능한지 파악하고 접근이 가능한 경우 Context Broker에게 필요한 상황정보를 요청하며, Context Broker에게서 받은 정보를 정책 문서에서 기술한 추상화 최대 허용 값을 넘지 않는 상태에서 그 값을 전달한다. 만약 추상화 모듈에서 추상화한 상황정보가 협상 문서에서 기록한 최대 허용 값을 넘어 가는 경우 협상 문서에 따라 값의 전달 여부가 결정된다. 협상 문서의 RESULT-SET이 True의 값을 가지는 경우 추상화된 값을 협상 문서의 최대 허용 값으로 나누어서 전달하고, False인 경우 접근이 불가능하다고 판단한다. 즉, 상황정보 추상화모듈에서 추상화시킨 키의 값이 160~180cm이며, 협상 문서의 최대 추상화 허용 값이 10cm이고, RESULT-SET이 True인 경우 시스템은 사용자에게 키는 160~170cm or 170cm~180cm라고 전달하고, False인 경우에는 null 값을 전달한다. 이러한 셋 기반 전달은 추천 서비스와 같이 결과의 값이 여러 개이며, 이 중 하나를 사용자가 선택을 하는 서비스에서 사용할 수 있다. 즉, 실제 키가 174cm인 경우 전달되는 결과 중 하나인 160~170cm는 잘못된 상황정보이나 이러한 상황정보를 이용할 경우에도 올바른 정보에서 얻어진 결과와 크게 다르지 않는 결과를 보여주거나 또는 사용자가 결과 값 중 일부는 잘못된 결과임을 알 수 있는 경우 서비스의 연속성을 높일 수 있다.

상황정보 추상화 모듈은 추상화가 가능한 경우 추상화 값을 협상 인터페이스에 전달하고, 그렇지 않은 경우 null 값을 전달한다. 협상 인터페이스는 null 값을 받는 경우 협상 문서에 기록된 정보를 토대로 이를 대체할 수 있는 상황정보가 있는 경우 그 값을 다시 요청하여 결과를 받고 대체할 상황정보가 없는 경우 null 값을 전송한다. Context Broker는 협상 인터페이스에서 받은 결과를 바탕으로 이를 다시 사용자 또는 서비스에게 전달하고, 사용자 또는 서비스는 받은 정보를 이용하여 자신의 일을 진행한다.

4. 실험

우리는 이러한 상황정보를 추상화하는 접근 제어 프레임워크를 UCN 시스템을 이용하여 본 논문의 시나리



(a) 접근제어를 하지 않은 상황정보의 전달 및 결과

(b) 추상화 접근제어 프레임워크를 이용한 상황정보의 전달 및 결과

그림 6. 접근 제어를 적용하지 않은 운동 처방을 위한 의사의 화면 (a)과 추상화를 이용한 접근 제어를 적용한 운동 처방을 위한 화면 (b)

Fig. 6. Views of doctor who gives exercise prescription which does not apply access control (a) and applys abstract based access control (b).

오를 기반으로 구현하였다. 또한 UCN 시스템은 역할 기반이 아닌 사용자 또는 서비스의 아이디를 이용한 정보의 전달을 하므로 본 실험에서는 역할(Role)이 아닌 사용자 또는 서비스의 아이디를 사용하며, 시스템이 Class II-3보다는 Class II-1이나 Class II-2를 선호함에 따라 실험에서는 Class II-3의 정보를 제공하지 않는다.

홍길동은 자신의 상황정보를 이용하여 자신에게 맞는 운동을 전문 의사에게 처방받길 바라며, 의사는 운동 처방 이외에 나쁜 의도로 주민등록번호, 카드번호와 같은 상황정보를 수집하려고 한다. 그림 6의 (a)는 상황정보에 대하여 접근제어를 하지 않는 경우에 의사의 화

그림 7. 운동처방에 의한 사용자의 결과

Fig. 7. User result of exercise prescription.

면에 나타는 결과이다. 이러한 경우 모든 상황정보를 허용함으로써 주민등록번호와 같은 과도한 정보가 의사에게 노출되게 된다. 이에 비하여 접근제어 프레임워크를 적용하는 경우 그림 6의 (b)와 같이 이름, 신용카드 번호와 같은 상황정보를 제공하지 않으며, 나이, 몸무게와 같은 정보는 추상화된 값을 보여준다. 각 수치에 대한 운동 처방은 서경원[19]가 제시한 식을 이용하였으며, 그림 6의 (a)와 (b)에서 사용자가 휴대폰을 통하여 받는 운동처방은 모두 그림 7과 같은 모습을 보인다. 이는 추상화에 의하여 서비스의 연속성이 하락하지 않음을 보여준다.

Ⅳ. 결 론

유비쿼터스 시스템이 더욱 많은 상황정보를 취급함에 따라 시스템에서의 개인정보보호의 중요성은 갈수록 증대되고 있다. 또한 이런 개인정보보호는 기존의 접근제어 기법만으로는 충분하지 못하다. 본 논문은 이러한 상황정보의 제공에 의하여 발생할 수 있는 개인정보의 과도한 노출을 막기 위한 추상화 기반 접근제어 프레임워크를 제안한다. RDF의 추론과 협상을 통하여 상황정보를 서비스의 연속성이 유지되는 한도 내에서 최대한으로 추상화하여 제공함으로써 서비스의 연속성을 높이는 동시에 개인정보를 보호한다. 또한 기존의 RBAC과 유사한 형식을 사용함으로써 사용하기 쉬우며, 모듈의 형태로 개발됨에 따라 여러 시스템에 쉽게 적용이 가능하다.

그러나 제안하는 프레임워크의 추상화는 RDF의 추론을 사용함에 따라 상황정보의 숫자의 증가에 따른 속도 저하가 발생할 수 있어 정보의 적절한 분리와 추론의 범위의 제한을 통한 처리 속도를 향상시킬 필요가 있다. 또한 현재의 상황정보의 추상화에서 발생할 수 있는 추론에 의한 정보의 유출 가능성에 대한 검증이 필요하다. 그리고 현재의 RDF의 작성은 사용자가 직접 작성을 해야 하는 번거로움이 있어 정책의 기술시 필요한 정보가 자동적으로 기술하도록 할 필요성이 있다.

참 고 문 헌

[1] 조은선, 민영목, “상황인식 시스템 모델링을 위한 정형화 프레임워크”, 전자공학회논문지, 제 46권 CI편, 제2호, 2009년 3월.

[2] R. S. Sandu, E. J. Coyne, H.L. Feinstein, and C. E. Youman, “Role-based access control models”, IEEE computer, 29(2): pp. 38-47, 1996.

[3] R. S. Sandhu, D.F. Ferraiolo and D.R. Kyhn, “The Nist Model for Role Based Access Control: Toward a Unified Standard”, in Proc. of 5th ACM Workshop on Role Based Access Control, pp. 47-63, 2000.

[4] Roshan K. Thomas, “Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments”. in Proc. of the second ACM workshop on Role-based access control, pp. 13-19, 1997.

[5] Fahad T. Alotaiby and J. X. Chen, “A Model for Team-based Access Control (TAMC 2004)”, in Proc. of the International Conference on Information Technology: Coding and Computing (ITCC’04), 2004.

[6] R. Wishart, K. Henricksen, and J. Indulska, “ Context Obfuscation for Privacy via Ontological Descriptions”, in Proc. of the International Workshop on Location and Context-Awareness 2005, pp. 276-288, 2006.

[7] I.T. Emin, “Context Data Model for Privacy”, Prime Standardization Workshop, 2006.

[8] P. Samarati, “Protecting Respondent’s Identities in Microdata Release”, IEEE Transactions on Knowledge and Data Engineering, vol. 13, pp. 1010-1027, 2001.

[9] Latanya Sweeney, “Achieving k-Anonymity Privacy Protection using Generalization and Suppression”, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), pp. 557-570, 2002.

[10] A. Machanavajjhala, J. Gehrke, D. Kifer and M. Venkitasubramaniam, “l-diversity: Privacy beyond k-anonymity”, in Proc. of 22nd International Conference of Data Engineering, page. 24, 2006

[11] N. Li, T. Ki and S. Venkitasubramaniam, “t-closeness: Privacy Beyound k-Anonymity and l-Diversity”, in Proc. of IEEE International Conference on Data Engineering, 2007.

[12] M. Ctacey and C. McGregor, “Temporal abstraction in intelligent clinical data analysis: A survey”, Artifical intelligence in Medicine, 39, pp. 1-24, 2007.

[13] E.S. Cho, Y.S. Kim, M.P. Hong and W.D. Cho, “Fine-Grained View-based Access Control for RDF Cloaking”, in Proc. of IEEE Ninth International Conference on Computer and Information Technology, 2009/

[14] 김현우, 변성호, 박희정, 이승환, 정유석, 조위덕, “유비쿼터스 지능공간에서 멀티모달센서를 이용한 향상된 u-헬스케어 서비스 구현에 대한 연구”, 전자공학회논문지, 제46권 CI편, 제 2호, 2009년 3월.

[15] Extensible Markup Language (XML), http://www.w3.org/XML/

[16] Resource Description Framework (RDF), http://www.w3.org/RDF/

[17] Y.S. Kim, E.S. Cho and W.D. Cho, “Context Data Abstraction Framework using RDF”, in Proc. of the 4th International Conference on Ubiquitous Information Management and Communication (ICUMIC 2010), January, 2010.

[18] P3P: The Platform for Privacy Preferences. http://www.w3.org/P3P/

[19] 서경원, “웹기반을 이용한 비만 학생의 운동프로그램 가발에 관한 연구”, 충북대학교 석사논문, 2005년 2월

저 자 소 개

김 윤 삼(정회원)

2004년 충북대학교 전기전자및 컴퓨터공학부 졸업
2006년 충북대학교 전자계산학과 졸업
2007년～현재 충남대학교 공과대학 컴퓨터공학과 박사과정.
<주관심분야 : 보안, 개인정보보호>

조 위 덕(정회원)

1987년 한국과학기술원 전기및 전자공학과 졸업(공학박사)
1983년～1991년 금성전기(현 LG 전자) 기술연구소 DSP 연구실장
1991년～2003년 전자부품연구원 (KETI) 시스템연구본부 본부장
1993년 미국 TCSI/Berkeley PCG Group 공동개발연구원
1994년 영국 TTP/Cambridge GSM Division 공동개발연구원
현 아주대학교 유비쿼터스시스템여구센터장
현 아주대학교 전자공학부 교수.
<주관심분야 : 통신, 컴퓨터, 신호처리, 반도체>

조 은 선(정회원)

1991년 서울대학교 계산통계학과 졸업(계산학전공)
1993년 서울대학교 전산과학과 석사
1998년 서울대학교 전산과학과 박사
1999년～2000년 한국과학기술원 연구원
2000년～2001년 아주대학교 정보통신전문대학원 조교수 대우
2002년～2006년 충북대학교 조교수
2006년～현재 충남대학교 컴퓨터공학과 조교수.
<주관심분야: 상황인지 시스템, 상황데이터 모델링 및 언어 등>