연결 데이터 환경에서 접근제어를 위한 RBAC 모델

이종현*, 김장원*, 정동원**†, 백두권*†

*고려대학교 컴퓨터·전파통신 공학과

**군산대학교 정보통계학과
e-mail : momoline@korea.ac.kr, ikaros1223@korea.ac.kr, djeong@kunsan.ac.kr, baikdk@korea.ac.kr

A RBAC Model for Access Control in Linked Data Environments

Chonghyeon Lee*, Jangwon Kim*, Dongwon Jeong**, Doo-Kwon Baik*
* Dept. of Computer and Radio Communications Engineering, Korea University
**Dept. of Informatics & Statistics, Kunsan National University

요 약

이 논문에서는 Linking Open Data 프로젝트를 기반으로 개발된 어플리케이션들의 접근제어를 위하여 기존 RBAC 모델을 연결 데이터에 적용 가능하도록 확장한 모델을 제안한다. 제안 모델은 온톨로지의 구조에 RBAC 모델에 적용할 수 있도록 RBAC 모델에 사용자를 위한 제약조건을 온톨로지로 표현하였으며, 지능형 엔진을 통해 사용자에게 적합한 권한을 추론한다. 사용자에 적합한 접근권한을 주기 위해 FOAF, flickr, 트위터 등의 데이터가 연결되어있는 연결 데이터로부터 사용자 프로파일을 확장할 수 있는 정보를 획득할 수 있으며, 이를 기존 정보에 확장하여 사용자의 권한을 부여한다. 본 논문에서 제안한 모델의 실효성을 검증하기 위하여 DBpedia Mobile을 위한 접근제어 시스템을 설계하였으며 안드로이드 SDK 환경에 프로토타입을 구현하여 제안 모델을 연결 데이터 환경의 어플리케이션에 적용 가능함을 보였다.

1. 서론

연결 데이터(Linked Data)는 다양한 서로 다른 자원의 데이터를 링크로 연결시킨 구조화된 데이터 집합을 의미한다[1-3]. 이러한 데이터 레벨의 링크는 다른 자원에 있는 데이터를 하나로 연결시켜 브라우저를 통해 접근 가능하게 하며 시맨틱웹 검색 엔진이 크롤링 할 수 있도록 한다. 연결 데이터의 핵심 기술은 HTTP URI로서 웹 자원과 현실 세계의 객체를 식별할 수 있다[4]. 웹 자원의 데이터는 Resource Description Framework(RDF)를 통해 표현되며 이는 다른 데이터 소스의 객체를 가리키는 트리플 형식의 링크를 포함한다[5,6]. 이러한 연결 데이터가 포함하는 개념을 기반으로 다양한 어플리케이션들이 개발되어 웹 리소스들의 의미를 파악하는데 보다 풍부한 정보 및 서비스를 제공한다. 그러나 현재까지의 연구들은 이러한 연결 데이터를 이용한 어플리케이션 및 서비스 개발 및 활용에 집중되어 있을 뿐 데이터 서비스의 중요한 요소 중 하나인 보안에 관한 연구는 미비한 실정이다. 따라서 보안 측면에서 발생할 수 있는 이슈에 대한 연구가 요구되며, 특히 다양한 웹 인스턴스 간의 연결인 연결 데이터에 대한 접근제어에 대한 연구는 매우 중요한 연구분야이다. 이 논문에서는 RBAC 기반의 접근제어 모델을 제안한다. 또한 프로토타입 시스템을 구현하여 제안한 접근제어 모델의 적용 사례를 보인다.

이 논문의 구성은 다음과 같다. 제2장에서 관련연구에 대하여 언급하고 제3장에서 이 논문에서 제안하는 접근제어 모델의 전반적인 구조를 정의한다. 제4장에서는 제안 모델을 구현을 위한 개념 모델과 함께 구현된 프로토타입 시스템에 대하여 기술한다. 마지막으로 제5장에서는 결론 및 향후 연구에 대하여 기술한다.

2. 관련연구

2.1 Linking Open Data 프로젝트

W3C Linking Open Data 커뮤니티에서 시맨틱웹 기술들을 이용한 정보 취합의 목적으로 Linking Open Data 프로젝트를 추진하고 있다[7]. 이 프로젝트의 목적은 RDF로 기술되어있는 오픈 라이센스 데이터 집합을 링크로 연결하여 웹을 확장시키는 것이다[8]. 2009년 통계 자료에 따르면 연결 데이터 집합은 이미 수백만의 자원의 데이터로 77억개의 RDF 트리플을 가지고 있다.

대표적인 데이터 자원인 DBpedia는 Wikipedia로부터 추출하여 260만개의 객체들과 30가지의 언어로 기술된 주석, 이를 연결하는 60만개의 이미지 링크와

※ 이 논문은 '2 단계 BK21 사업'과 정보통신산업진흥원의 SW 공학 요소기술 연구개발사업에 의해 지원되었음을 밝힙니다.
† 공동 교신 저자

315만개의 웹 페이지 링크를 포함한다[9]. DBpedia의 데이터들은 Freebase, flickr^{TM}wrappr, GeoNames 등과도 서로 링크로 연결되어 있다[10-12]. 하지만 이러한 연결 데이터 집합을 기반으로 한 Faceted Wikipedia Search, DBpedia Relation Finder, DBpedia Navigator, OpenLink Virtuoso built-in Faceted Browser 등과 같은 어플리케이션은 활용성을 위한 개발 및 연구에만 초점을 두고 있을 뿐, 접근제어에 대한 연구는 미비한 실정이다[13-16]. 즉 사용자의 권한을 고려하지 않기 때문에 보안이 중요시 되는 정보 혹은 특정 사용자 그룹에게만 공개되어야 하는 정보에 대한 접근 제한이 불가능하다. 아울러 사용자 역할에 따른 접근제어가 불가능함으로써 보다 세밀한 접근제어 정책을 지원할 수 없다.

2.2 DBpedia Mobile

DBpedia Mobile은 시맨틱 웹 기반의 위치기반 클라이언트 환경으로서 스마트폰의 브라우저나 표준 웹 브라우저를 통하여 연결 데이터 기반의 서비스를 제공한다[17-19]. 사용자는 단순한 지도 정보뿐만 아니라 특정 위치와 링크로 연결 되어있는 정보 또한 얻을 수 있다. 예를 들면 YAGO의 박물관, 지하철역 정보와 flickr^{TM}wrappr의 데이터 요약, 이미지 정보 등이 있다[11,20]. 사용자의 정보는 FOAF(Friend of a Friend) 프로파일과 같은 프로파일 데이터 집합으로 관리되며 이는 이 논문에서 제안하는 시스템에서 사용자의 권한을 판단하기 위하여 사용된다[21].

2.3 RBAC

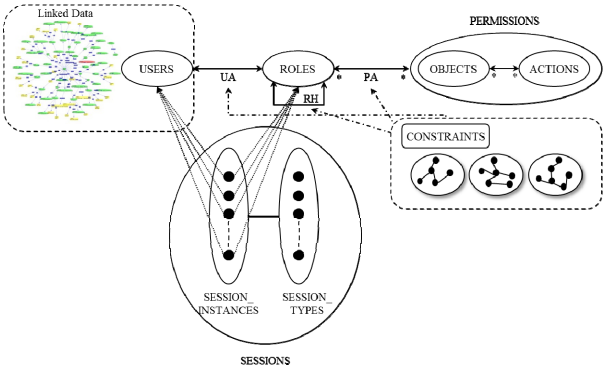
RBAC(Role-Based Access Control)은 역할(Role)의 개념을 사용함으로써 사용자의 권한을 효과적으로 관리하기 위한 모델이다[22]. 사용자의 역할기반 접근통제 방식은 임의적 접근통제와 강제적 접근통제에 비하여 정교함과 유연성을 제공한다[23]. RBAC은 1970년대에 다중 어플리케이션에서의 적용을 시작으로 의료 정보 보호 시스템부터 분산 가상환경까지 다양한 분야에서 권한 접근제어를 위해 사용되고 있다[24-25]. 이러한 RBAC 기반의 시스템에 대한 수요를 바탕으로 벤더들은 데이터 베이스, 웹 기반 어플리케이션, 시스템 관리 등 다양한 제품에 적용 가능한 다양한 RBAC 모델들을 제안하고 구현하고 있다[26].

RBAC은 조직 수준에서 보안 관리를 증진시키기 위해 사용자 식별 수준이 아닌 추상화 수준을 제공하여 시스템의 실제 환경에 자연스럽게 적용 가능하도록 한다. RBAC에서 사용자는 특정 정보나 자원에 대한 접근 권한을 얻기 위하여 해당 접근 권한이 배정된 역할 집합의 구성원이 되어야 한다. 권한 부여 및 관리 단위가 역할이라는 이 특성은 사용자로 구성된 시스템의 효율적 권한관리를 가능하게 할 뿐만 아니라 역할간 계층구조를 통해 하위 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한상속을 제공한다. RBAC이 제공하는 권한상속은 계층구조 별 권한 관리를 단순화 시키고 특정한 보안정책을 유연하게 구현할 수 있도록 한다. 하지만 기존 RBAC 모델은 온톨로지를 고려하지 않고 설계되었기 때문에 연결 데이터 기반의 어플리케이션에 적용 시 다양한 온톨로지 자원을 활용할 수 없다. 이 논문에서 제안하는 확장 RBAC 모델은 연결 데이터 온톨로지의 구조적인 측면을 RBAC 모델에 적용하기 위하여 제약조건을 온톨로지로 표현하고 Jena와 같은 지능형 엔진을 활용하여 사용자에게 적합한 역할을 배정한다.

3. 제안 모델

이 논문에서 제안하는 연결 데이터 환경의 어플리케이션을 위하여 확장된 RBAC 모델은 [그림 1]과 같다. 이 모델은 사용자(USER), 역할(ROLE), 권한(PERMISSION), 세션(SESSION)으로 구성되어 있다.

사용자는 프로파일 정보를 바탕으로 하는 인간의 행동이나 자율적인 에이전트를 나타내며 시스템은 사용자 정보를 연결 데이터의 온톨로지 프로파일 정보로부터 획득한다. 이때 연결 데이터의 온톨로지 프로파일은 FOAF 등을 주로 사용한다[21].



(그림 1) 연결 데이터 환경을 위한 RBAC 모델

역할은 조직에서 같은 역할을 갖는 사용자들의 공통된 권한과 책임을 표현하는 의미적 구조이다. 권한은 시스템에서 하나 또는 그 이상의 객체에 대한 접근에 대한 읽기, 쓰기, 수정 등의 허가를 의미하며 특정 객체들과 허가된 행위들의 다-대-다 관계로 객체에 해당 권한을 나타낸다. 역할 계층(RH: role hierarchy)은 역할의 계층구조를 구성하여 권한상속을 제공 가능하게 한다. 권한상속은 조직 내에서 권한과 책임의 순서를 반영하기 위하여 역할을 구조화한다. 권한상속에서는 상위의 역할을 역할 계층 다이어그램의 위 부분에 위치시키고 하위의 역할들을 아래 부분에 배치함으로써 권한의 계층을 나타낸다.

모델에서 이러한 권한과 역할의 관계를 유지하고 관리하는 것은 매우 중요하다. 역할에 부적절한 권한을 할당하는 것은 시스템에 심각한 문제를 초래할 수 있기 때문이다. 효과적으로 역할에 해당하는 권한을 유지하기 위하여 모델은 권한과 역할의 관계를 명확히 식별해야 할 뿐만 아니라 해당 관계를 표현하는 리뷰를 제공받아야 한다. 특히 리뷰는 사용자가 역할에서 제외되거나 권한이 너무 오랫동안 방치된 경우 등 다양한 관리적 상황을 고려하기 위해 반드시 필요하다.

세션은 한 사용자와 여러 개의 권한을 매칭하는 역할을 수행하며, 세션 인스턴스(session_instance)와 세션

타입(session_type)을 요소로 갖는다. 세션 인스턴스는 실제 사용자가 권한을 부여 받기 위하여 수행하는 로그인 인스턴스이다. 한 사용자는 동시에 여러 개의 세션 인스턴스를 가질 수 있으며 시스템은 세션 인스턴스를 유일하게 식별한다.

사용자는 해당 역할의 구성원이 됨으로써 사용자 할당(UA: user assignment) 을 받고 시스템으로부터 구성원에 적합한 권한 할당(PA: permission assignment)을 받는다. 모델의 제약조건(constraint)은 온톨로지로 표현되며 UA와 PA를 수행을 위해 만족되어야 하는 규칙으로 이루어져있다. 또 이 규칙은 사용자 집단의 역할에 해당하는 적절한 권한 이상을 가지는 것을 방지하기 위한 이해와 상충에 대한 정책으로 사용된다. 특정 행위에 해당하는 권한들은 분리된 규칙에 의해 다양한 역할에 분배됨으로써 한 사용자의 독단적인 권한 획득을 방지한다. 제안 모델에서의 온톨로지 규칙은 RBAC 시스템의 최소 특권의 원리를 지원하기 위하여 사용자가 자신의 업무를 수행하기 위해 필요한 기능 이상의 특권을 가지지 않도록 관리되어야 한다. 시스템은 이러한 온톨로지 제약조건을 기반으로 지능형 엔진의 추론을 통하여 자동으로 사용자에게 적합한 역할을 부여한다.

4. 구현

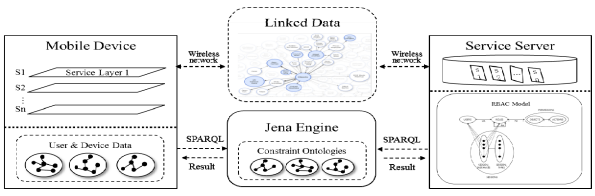
4.1 시스템 개념 모델

시스템 구현을 위한 환경은 [표 1]과 같다. 모바일 디바이스는 안드로이드 2.1 플랫폼에서 구현하였으며 서버를 Java SE 환경으로 구축하였고 Jena Framework 2.6.3을 통해 지능형 처리를 수행하고 온톨로지를 저장 및 관리한다.

<표 1> 시스템 환경

Mobile platform	안드로이드 2.1 (API level 7)
Operating System	Microsoft Windows 7 Enterprise K
Language	Java SE Runtime Environment <build 1.6.0_18-b07>
Inference Engine	Jena Semantic Web Framework2.6.3

연결 데이터를 위한 RBAC 기반의 접근제어 개념 모델은 [그림 2]와 같다. 모바일 디바이스는 RBAC 모델의 사용자로서 서비스 서버에 무선 통신을 통하여 접속하고 연결 데이터의 프로파일 정보를 서비스 서버에 전달한다.



(그림 2) 연결 데이터 환경의 어플리케이션을 위한 접근제어 개념 모델

서비스 서버는 사용자의 역할을 판정하기 위하여 Jena 지능 엔진에 사용자의 프로파일 정보와 제약조건을 포함하는 SPARQL CONSTRUCT 질의문를 보낸다[27]. Jena 지능 엔진은 SPARQL 질의에 대한 응답으로 사용자의 역할을 전송하고 서비스 서버는 사용자에게 해당 연산을 허용함으로써 특정 연결 데이터에 접근 가능하도록 한다.

4.2 프로토타입 시스템

이 절에서는 제안한 접근제어 시스템을 다음과 같은 시나리오를 기반으로 테스트한다. 사용자는 모바일 디바이스를 통해 DBpedia Mobile 서버에 접속하고 서버는 접근제어가 필요 없는 기본적인 연결 데이터 정보들을 사용자에게 전송한다. 사용자는 추가로 학교 내 열람실의 좌석 현황 정보를 요청하며 자신의 프로파일 정보를 서버에 전송한다. 서버는 프로파일 정보를 Jena 지능 엔진을 통해 분석하여 사용자의 역할을 배정하고 이에 적합한 권한을 부여한다.

(그림 3) DBpedia Mobile 접속과 사용자 역할 요청

[그림3]의 좌측 화면은 사용자가 DBpedia Mobile 서버에 접속하여 기본적인 정보들을 전송 받은 화면을 나타낸다. 모바일 디바이스의 화면에는 지도정보 외에도 YAGO, flickr 등 다양한 정보들이 매쉬업 되어 표시되어 있다. 사용자는 자신이 접근 가능한 추가적인 정보들을 얻기 위하여 [그림 3]의 우측 화면과 같이 서버에 프로파일 정보를 보낸다. 서버는 이와 같은 정보를 Jena 지능 엔진에 SPARQL로 질의하며 이에 대한 결과는 [그림 4]와 같다.

```
S: Connecting...
S: Receiving...
S: Received: 'what is my role'
S:163.152.39.158:5555's Role is Korea Univ. Student
```

(그림 4) 서버의 사용자 역할 지정

서버에서 지정한 역할이 해당 대학의 학생이므로 [그림 5]의 좌측 화면과 같이 접근 권한을 부여 받아 열람실의 좌석 정보를 확인할 수 있다. 반면 [그림5]의 우측 화면과 같이 해당 학생이 아닌 경우 특정 정보에 접근할 수 없다.

(그림 5) 사용자 역할에 적합한 정보 제공

5. 결론

이 논문에서는 연결 데이터 환경의 어플리케이션의 접근제어 관리의 문제점을 해결하기 위하여 RBAC 모델을 확장함으로써 연결 데이터 온톨로지의 구조적인 측면을 RBAC 모델에 적용 가능하게 하였고, 지능형 엔진을 활용하여 사용자에게 적합한 접근권한을 할당하도록 하였다. 제안 모델을 적용 가능성을 확인하기 위하여 제안 모델을 기반으로 하는 시스템을 설계하였고 이를 안드로이드 SDK에 구현하여 적합한 접근제어를 제공할 수 있음을 보였다.

향후 연구로는 시스템의 세부 요소들을 상세히 구체화하고 제안 모델을 연결 데이터 전체 집합에 적용할 계획이다.

참고문헌

[1] T. Berners-Lee, "Linked Data", http://www.w3.org/DesignIssues/LinkedData.html, 2009.
[2] C. Bizer, R. Cyganiak, "How to Publish Linked Data on the Web", http://sites.wiwiss.fu-berlin.de/suhl/bizer/pub/LinkedDataTutorial/, 2007.
[3] C. Bizer, T. Heath, T. Berners-Lee, "Linked Data—the story so far", International Journal on Semantic Web & Information Systems 5 (3) 1–22, 2009.
[4] L. Sauermann, R. Cyganiak (Eds.), "Cool URIs for the SemanticWeb—W3CInterest Group Note", http://www.w3.org/TR/cooluris/,W3C, 2008.
[5] G. Klyne, J. Carroll (Eds.), "Resource Description Framework (RDF): Concepts and AbstractSyntax—W3CRecommendation", http://www.w3.org/TR/rdfconcepts/, 2004.
[6] D. Berrueta, J. Phipps (Eds.), "Best Practice Recipes for Publishing RDF Vocabularies—W3C Working Group Note", http://www.w3.org/TR/swbpvocab-pub/,W3C, 2008.
[7] W3C, "Linking Open Data SWEO Commuinity Project", http://esw.w3.org/topic/SweoIG/TaskForces/CommunityProjects/LinkingOpenData,
[8] C. Bizer, T. Heath, D. Ayers, "Y. Raimond, Interlinking Open Data on the Web", in: Poster at the 4th European Semantic Web Conference (ESWC2007), Innsbruck, Austria, June 2007.
[9] C. Bizer, J. Lehmann, G. Kobilarov, S. Auer, C. Becker, R. Cyganiak, S. Hellmann, "DBpedia—a crystallization point for the Web of data", Journal of Web Semantics 7 (3) 154–165, 2009.
[10] Metaweb, freebase, http://www.freebase.com.
[11] Freie University, flickr^{TM}wrappr, http://www4.wiwiss.fu-berlin.de/flickrwrappr.
[12] Creative Commons Attribution, GeoNames, http://www.geonames.org.
[13] Chris Bizer, Faceted Wikipedia Search, http://wiki.dbpedia.org/FacetedSearch, 2010.
[14] Philipp Heim, Steffen Lohmann, Timo Stegemann, DBpedia Relation Finder, http://relfinder.dbpedia.org/, 2009.
[15] Jens Lehmann and Sebastian Knappe, DBpedia Navigator, http://navigator.dbpedia.org/.
[16] OpenLink Software, OpenLink Virtuoso built-in Faceted Browser, http://dbpedia.org/fct/, 2010.
[17] Becker,C. and C. Bizer, "Exploring the Geospatial SemanticWeb with Dbpedia Mobile", Web Semantics: Science, Services and Agents on the World Wide Web, 2009.
[18] Christian Becker, DBpedia Mobile, http://beckr.org/DBpediaMobile, 2008.
[19] Christian Becker, Christian Bizer, "DBpedia Mobile: A LocationEnabled Linked Data Browser", In: Proceedings of the 1st Workshop about Linked Data on the Web LDOW 2008.
[20] F. Suchanek, G. Kasneci, G. Weikum, "YAGO: a core of semantic knowledge", in: WWW2007: Proceedings of the 16th International Conference on World Wide Web, ACM 697–706, 2007.
[21] D. Brickley, L. Miller, "FOAF Vocabulary Specification 0.91", http://xmlns.com/foaf/spec/, 2007.
[22] Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink, Charles E. Youmank, "Role-Based Access Control Models", IEEE Computer, Vol.29, No.2, pp.38-47, 1996.
[23] David F. Ferraiolo and D. Richard Kuhn, "Role-based access controls", 15th NIST-NCSC National Computer Security Conference, pp.554-563, Baltimore, MD, October 13-16, 1992
[24] 노승민, 이수철, 황인준, 박상진, 김현주, "RBAC에 기반한 의료정보 시스템의 설계 및 구현", 한국정보처리학회 춘계학술발표대회 논문집 제 11권 1호, 2004.
[25] 정헌만, 탁진현, 이세훈, 왕창종, "분산 가상 환경에서 역할 기반 접근제어 관리자 설계", 한국정보처리학회 춘계 학술발표 논문집 제 7권 1호, 2000.
[26] James B. D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford, "Security models for web-based applications", Communications of the ACM, Volume 44 , Issue 2, pp.38-44, 2001
[27] E. Prud'hommeaux, A. Seaborne (Eds.), "SPARQL Query Language for RDF—W3C Recommendation", http://www.w3.org/TR/rdf-sparql-query/,W3C, 2008.