Journal of Korea Spatial Information Society Vol.21, No.4 : 15-24, August 2013 ISSN 2287-9242(Print)
http://dx.doi.org/10.12672/ksis.2013.21.4.015 ISSN 2287-9250(Online)

GeoXACML 기반의 접근 제어 시스템 설계 및 구현

Design and Implementation of an Access Control System Based on GeoXACML

반 현 오* 신 인 수** 김 정 준*** 한 기 준****
Hyun O Ban In Su Shin Jeong Joon Kim Ki Joon Han

요 약 최근 공간정보와 다양한 멀티미디어 등이 융합되어감에 따라 고부가가치의 공간정보 콘텐츠에 대한 수요와 공간정보 보안을 위한 각종 기술의 필요성이 증대되고 있다. 그러나 현재의 보안 정책은 각각의 시스템에서 독립적으로 관리되고 있기 때문에 보안 정책의 수정에 많은 비용이 소요되거나 신뢰성이 떨어지는 문제점이 있으며, 국내외 공공기관 및 기업에서 사용되는 공간정보 관리 시스템에서도 시스템의 연계 및 통합 과정 중 이와 같은 문제점들이 빈번히 발생하고 있다. 따라서, 본 논문에서는 국제 표준화 기구인 OGC에서 제시한 GeoXACML을 기반으로 문법 및 의미의 확장이 용이하고 많은 공간 플랫폼 및 시스템에 대해 통합된 보안 정책을 제공할 수 있는 접근 제어 시스템을 설계 및 구현하였다. 본 논문에서 설계 및 구현한 GeoXACML 기반 접근 제어 시스템은 국제 표준 스펙을 따르기 때문에 높은 이식성과 함께 상호운용성을 제공한다. 마지막으로 본 논문에서는 본 시스템을 접근 권한이 요구되는 군사 지역에 대한 가상 시나리오에 적용해 봄으로써 그 효용성을 입증하였다.

키워드 : GeoXACML, XACML, 공간 접근 제어 언어, 접근 제어 시스템, 접근 제어 정책

Abstract Recently, as the spatial information and various multimedia are fused together, the demand for the high value-added spatial information contents and the necessity of technology for spatial information security are increasing. However, since the current security policy is being managed independently by each system, there is a problem with unreliable or costly to modify or revise the security policy. Such problems occur frequently in the process of coordination or integration of the spatial information management systems that are used in public institutions and private companies. Therefore, in this paper, the access control system that could provide an integrated security policy for many spatial platforms and systems with expandable grammar and semantics was designed and implemented based on GeoXACML proposed by OGC. As the GeoXACML-based access control system designed and implemented in this paper follows the international standard specifications, it provides high portability and interoperability. Finally, in this paper, the efficiency of the system was proved by applying it to a virtual scenario on the military area requiring the access control.

Keywords : GeoXACML, XACML, Spatial Access Control Language, Access Control System, Access Control Policy

1. 서 론

최근 공간정보와 다양한 멀티미디어 등이 융합되어감에 따라 고부가가치의 공간정보 콘텐츠에 대한 수요가 증가하면서 보안 미비로 인한 피해 사례도 급증하고 있다. 각국에서는 공간정보에 대한 침해가 이루어지는 것을 막고자 국가 GIS법을 비롯한 다양한 지리정보 보안 및 유지관리 관련제도가 추진되었으며 공간정보 보안을 위한 각종 기술의 필요성이 증가함에 따라 사고를 미연에 방지하기 위한 보안 솔루션의

† This work (Grants No. C0027296) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2012.

* Hyun-O Ban, Master, Dept. of Computer Science and Engineering, Konkuk University. hoban@db.konkuk.ac.kr
** In-Su Shin, Ph.D. Candidate, Dept. of Computer Science and Engineering, Konkuk University. isshin@db.konkuk.ac.kr
*** Jeong-Joon Kim, Assistant Professor, Dept. of Computer Science and Engineering. Konkuk University, jjkim9@db.konkuk.ac.kr
**** Ki-Joon Han, Professor, Dept. of Computer Science and Engineering, Konkuk University, kjhan@db.konkuk.ac.kr (Corresponding Author)

개발도 활성화 되었다. 이에 따라 공간정보에 대한 관리와 정보보안을 위하여 정밀한 접근 제어가 가능하고 다양한 보안 정책을 표현할 수 있는 접근 제어 시스템의 필요성이 증가하고 있다[3,4,11,15].

그러나 현재의 보안 정책은 각각의 시스템에서 독립적으로 관리되고 있기 때문에 보안 정책의 수정에 많은 비용이 소요되거나 신뢰성이 떨어지는 문제점이 있다[1,7]. 특히 국내외 공공기관 및 기업에서 사용되는 공간정보 관리 시스템에서도 시스템의 연계 및 통합 과정 중 이와 같은 문제점들이 빈번히 발생하고 있다[4].

이렇게 국내외 공공기관 및 기업에서 공간정보에 대한 관리와 정보보안을 위하여 정밀한 접근 제어의 필요성이 부각되고 보안 정책을 표현하기 위한 공통된 언어에 대한 필요성이 높아졌다[6]. 따라서 국제 표준화 기구인 OGC에서는 OASIS에서 제시한 접근 제어 언어인 XACML(eXtensible Access Control Markup Language)[8]에 공간정보 타입 및 함수를 확장한 GeoXACML(Geospatial eXtensible Access Control Markup Language)[12,13]을 제시하였다.

따라서, 본 논문에서는 국제 표준화 기구인 OGC에서 제시한 GeoXACML을 기반으로 접근 제어 시스템을 설계 및 구현하였다. 이러한 GeoXACML 기반의 접근 제어 시스템은 OGC가 제시한 국제 표준을 사용함으로써 GeoXACML을 사용하는 타 시스템과의 연동에 따른 비용과 시간의 소모가 적다는 것과 특히 공간 연산이 가능한 접근 제어 시스템이라는 장점을 갖는다.

GeoXACML 기반의 접근 제어 시스템은 공간정보 접근 제어를 위해 정책(Policy)이나 정책 집합(Policy Set)을 생성하기 위한 Geo PAP(Policy Administration Point), 공간정보 접근 제어에 대한 결정 요청을 생성하고 권한부여 결정을 시행하여 접근 제어를 수행하기 위한 Geo PEP(Policy Enforcement Point), 공간정보 접근 요청에 대한 적용 가능한 정책을 평가하고, 접근 권한 여부를 판단하기 위한 Geo PDP(Policy Decision Point), 공간정보 접근 제어 결정에 따라 사용자 질의에 대한 결과를 관련 시스템 WMS(Web Map Service) 또는 WFS(Web Feature Service)로부터 추출하기 위한 Geo PIP(Policy Information Point), 요청 및 응답 문맥을 변환하는 Context Handler로 구성된다.

본 논문에서는 GeoXACML 기반의 공간정보 접근 제어 시스템은 XACML 요청을 처리하는 방법과 속성들 및 관련 데이터들을 관리하기 위해 Sun의 오픈소스 XACML API[12]를 기반으로 확장하였다. 그리고 GeoXACML을 사용함으로써 공간연산 기능을 지원하고 문법 및 의미의 확장이 용이하며 많은 공간 플랫폼과 시스템에 대해 통합된 보안 정책을 제공한다. 마지막으로, GeoXACML 기반의 접근 제어 시스템을 접근 권한이 요구되는 군사 지역에 대한 가상 시나리오에 적용해 봄으로써 본 시스템의 효용성을 검증하였다.

본 논문의 구성은 다음과 같다. 제1장 서론에 이어 제2장에서는 관련 연구로 XML 기반의 접근 제어 정책 언어인 OASIS의 XACML과 시스템 개발시 기반이 되는 Sun의 XACML, OGC의 GeoXACML에 대하여 분석한다. 제3장에서는 접근 제어 시스템의 전체 구조와 그에 따른 설계에 대하여 설명한다. 제4장에서는 설계에 따라 구현된 내용에 대해 상세히 언급하고, 접근 요청 가상 시나리오를 통해서 본 논문에서 개발한 접근 제어 시스템의 효용성을 검증한다. 마지막으로 제5장에서는 결론에 대하여 기술한다.

2. 관련연구

본 장에서는 XML 기반의 접근 제어 정책 언어인 XACML, XACML을 구현한 오픈 소스인 Sun의 XACML, XACML에 공간정보 개념을 확장한 GeoXACML에 대하여 알아본다.

2.1 XACML

OASIS에서 제시한 접근 제어 언어인 XACML은 접근 제어 정책을 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공하는 언어이다. 즉, XACML은 접근 요청자의 역할에 기반하여 정당한 자원 요청 개체에게만 권한을 부여하고 자원들을 접근할 수 있도록 하는 XML 기반의 접근 제어 정책 언어이다[8].

XACML은 인터넷 상의 접근 제어 서비스를 위한 다양한 제품들 및 그 제품들의 서로 다른 환경들 사이에서 일관되게 적용할 수 있는 권한부여 정책을 제공하고, 그 정책을 통하여 기존의 다양한 환경 및 방식을 가진 접근 제어 제품들에 상호운용성을 제공한다. Fig. 1은 XACML 기반 접근 제어 순서도를 보여준다.

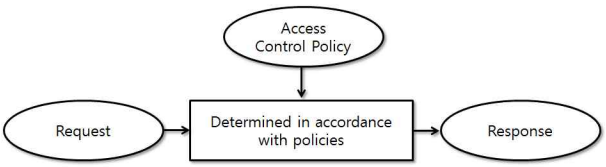

Figure 1. Access Control Flow Chart Bases on XACML

Fig. 1에서는 이용자가 특정 자원에 대한 접근 요청을 하면 접근 제어 정책을 통하여 접근 요청에 대한

권한을 판단하고, 접근 요청에 대한 집행을 수행하기 위해 필요한 권한 정보를 담은 응답을 반환한다. XACML은 일련의 과정에서 사용되는 접근 요청, 접근 제어 정책, 요청 응답을 위한 문법적 구조가 XML 스키마의 형태로 정의되어 있다. 또한 XACML에서 사용되는 정책은 각각의 사용자별 자원에 대한 단계별 접근 제어를 수립하여 구체적이고 미세한 접근 제어 정책 모델을 제공한다[5,16].

접근 제어 정책 모델은 규칙, 정책 및 정책집합 등에 관한 통상적인 접근 제어 요구사항들에 대해 기술하고 있으며 함수, 데이타 타입 및 조합 논리 등에 대해서도 정의하고 있다. 요청 언어는 어떤 주체가 특정 자원에 대해서 특정한 동작을 수행할 수 있는지에 대한 질의를 구성할 수 있게 하고, 응답 언어는 요청에 대한 결과를 표현하는데 사용된다[14].

현재 XACML은 공통의 산업 명세를 만드는 국제적인 컨소시엄인 OASIS에 의해 2005년 2월 버전 2.0의 표준안이 완성된 상태이고, 버전 3.0의 개발이 진행중에 있다.

2.2 Sun의 XACML API

Sun Microsystems에서 제공하는 XACML API는 단순히 XACML 언어의 구현만이 아닌 요청들을 처리하는 방법과 속성들 및 기타 다른 관련된 데이타들을 관리하기 위한 방법에 대한 규칙들을 구현한 Java 클래스들의 집합이다[12]. Sun의 XACML API는 현재 오픈 소스로서 자바 2 플랫폼 JDK 1.4 혹은 그 이상의 버전에서 사용될 수 있다.

Sun의 XACML API는 정책간 충돌을 막기 위한 정책 결합 알고리즘과 정책들의 파싱, 요청과 응답의 관리, 요청에 적합한 정책의 적용 등 XACML 명세 상의 필수 요소만을 구현하였다. 그러나 이것은 XACML의 핵심만을 구현한 것이기 때문에 SAML, LDAP 등의 다른 보안 관련 제품들과의 연동성은 제공하지 않고 있다. 또한 XACML 명세에서 언급된 데이타 타입들 및 함수들에 대해서 전체를 지원하지 않으므로 사용하고자 하는 부분이 미구현이라면 개발자로 하여금 별도의 추가 구현을 요구한다. Table 1은 Sun의 XACML API를 구성하는 패키지를 보여준다.

Table 1. XACML API Package of Sun

Packages	Description
com.sun.xacml	This is the root package, which contains the PDP class where most people will want to start.
com.sun.xacml.attr	Contains many of the classes related to attributes and attribute retrieval.
com.sun.xacml.combine	All of the combining algorithm support is in this package.
com.sun.xacml.cond	Support for Conditions is in this package.
com.sun.xacml.ctx	All of the classes that support the context schema are in this package.
com.sun.xacml.finder	The finder package supports all of the pieces of the XACML specification that require custom implementation.

Table 1과 같이 Sun의 XACML에서 제공하는 패키지는 요청을 변환하고 정책을 검색하여 이를 판단하기 위한 PEP와 PDP에 한정되어 있다.

2.3 GeoXACML

GeoXACML은 분산 지리 정보의 개발 및 통합을 위해 접근 제어 표준인 XACML에 공간 연산 기능을 확장한 언어이다[9,10,13]. 이것은 2007년 OGC에서 1.0이 채택되었으며 2011년 수정을 통하여 1.0.1으로 갱신되었다. GeoXACML은 공간 연산을 통해서 접근을 제어하고 상호운용성을 가지는 접근 제어 시스템의 구현을 가능하게 하며, 객체별 접근 제한 및 특정 지역에서만 해당 공간정보에 접근할 수 있도록 공간적 범위와 조건에 의거한 접근 제한 또한 가능하다.

GeoXACML은 XACML을 확장한 형태이므로 기존 XACML의 정책언어 허가 모델과 정보흐름 모델, XML 정책 스키마 및 정책과 관련된 PAP, PDP, PEP, PIP 등의 컴포넌트 개념 등을 그대로 따른다. 정책은 접근을 제어하기 위한 규칙들의 집합으로 복수의 정책 결합 알고리즘에 의하여 결정을 생성하게 된다. PAP는 접근을 제어하기 위한 규칙을 생성 및 관리하는 요소이고, PEP는 결정요청을 생성하고 권한부여 결정을 시행하여 접근 제어를 수행하는 시스템 요소이다. PDP는 적용 가능한 정책을 평가하고 권한부여 결정을 만드는 시스템 요소이며, PIP는 공간정보 서비스에 접근하여 판단에 필요한 속성을 가져오는 시스템 요소이다.

GeoXACML에서 확장된 공간 데이타 타입과 공간 함수는 XACML 기반의 정책에 대한 추가적인 공간 제약조건을 정의하는데 사용된다. GeoXACML은 OGC의 단순 기하에 따른 공간 데이타 모델을 사용하며, XACML의 정책언어를 따르면서 GML 3.0의 단순 기하를 표현하기 위한 구조화된 <AttributeValue> 타입을 정의한다. 새로 추가된 데이타 타입은 모든 기하 데이타 타입의 상위 클래스로서 urn:ogc:def:dataType:geoxacml:1.0:geometry 하나로 하였는데, 이는 많은 데이타 타입을 도입하는 복잡함을 피하면서 함수 선언부를 단순화하고 접근 제어 시스템의 구현을

쉽게 하기 위한 의도이다.

3. 시스템 설계

본 장에서는 GeoXACML 기반의 접근 제어 시스템의 전체 구조에 대하여 기술하고, 또한 이러한 접근 제어 시스템의 각 모듈에 대해 자세히 설명한다.

3.1 시스템 구조

GeoXACML 기반의 접근 제어 시스템은 요청 받은 리소스에 대한 접근이 허락되었는지를 결정하고 그 결정을 집행하는데, 본 논문에서는 사용자의 요청에 따라 WMS, WFS 등의 서비스를 대상으로 정책에 기반한 공간 연산을 수행하여 접근을 제어하는 기능을 제공한다. Fig. 2는 본 논문에서 개발한 전체 시스템의 구성도를 보여준다.

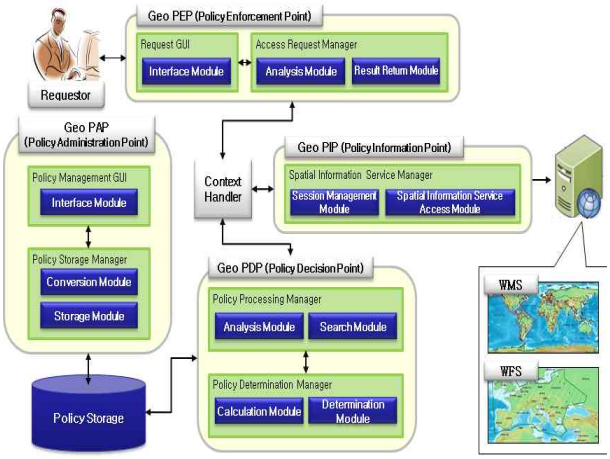

Figure 2. Structure of Access Control System Based on GeoXACML

Fig. 2와 같이 GeoXACML 기반 접근 제어 시스템은 Sun의 XACML API를 확장하였으나 표준 준수를 통한 상호 운용성과 경쟁력을 이유로 XACML 표준의 데이터 흐름도와 유사하게 설계되었다. 그러므로 GeoXACML 기반 접근 제어 시스템은 정책 생성을 위한 Geo PAP, 요청 생성 및 권한부여 결정을 시행하는 Geo PEP, 접근 권한 여부를 판단하는 Geo PDP, 판단에 필요한 속성을 서비스로부터 가져오는 Geo PIP, 요청과 응답의 형식을 변환하는 Context Handler의 구성으로 시스템 구조도로 구성된다.

3.2 Geo PAP

본 절에서는 Geo PAP를 구성하는 정책 관리 GUI인 인터페이스 모듈과 정책 저장 관리자인 정책 변환 모듈, 정책 저장 모듈에 대해서 설명한다.

3.2.1 인터페이스 모듈

인터페이스 모듈은 공간정보 접근 요청에 사용될 공간정보 접근 제어 정책과 정책 집합을 생성 및 관리하는 기능을 제공한다. Fig. 3은 접근 제어 정책 생성을 위한 사용자 인터페이스를 제공하는 Geo PAP의 인터페이스 모듈 실행 화면을 보여준다.

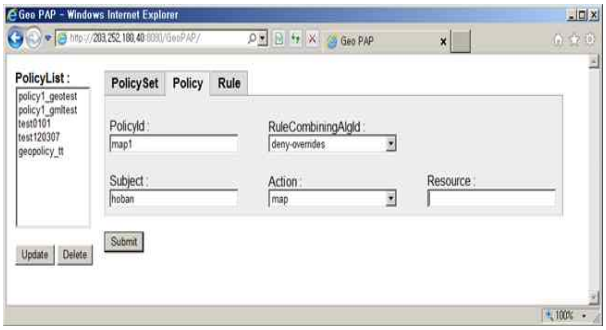

Figure 3. Execution Screen of Geo PAP Interface Module

Fig. 3의 Geo PAP 인터페이스 모듈에서 생성된 정책은 ID로 map1, 조합 알고리즘으로 deny-overrides를 갖게 되는데, 이 정책은 Subject가 hoban이고 Action이 map인 요청을 입력받을 때 부합하게 된다. 정책 속성을 입력하는 창 외에도 탭을 통하여 정책 및 정책 집합을 추가 및 제거할 수 있는 정책 관리 창, 정책을 확인 및 수정할 수 있는 정책 창으로 구성된다.

3.2.2 정책 변환 모듈

정책 변환 모듈은 새로운 접근 제어 정책을 저장하기 위해 접근 제어 정책 모델에 따라서 GUI에서 입력받은 값을 GeoXACML의 Policy 형태로 변환하며, 정

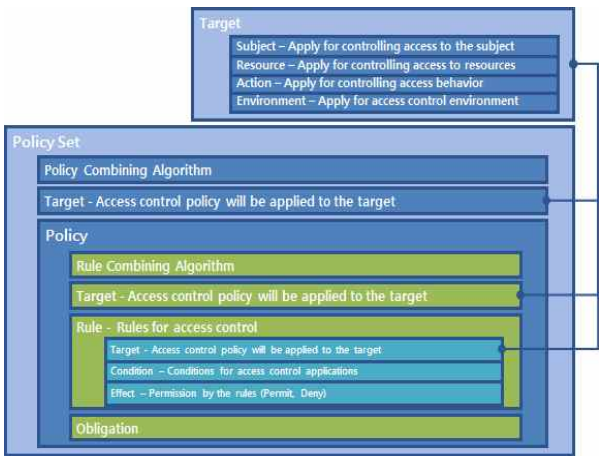

Figure 4. Access Control Policy Model of GeoXACML

책 저장소에 기록된 GeoXACML Policy 형태의 정책을 인터페이스 모듈에서 관리할 수 있도록 분석한다. Fig. 4는 GeoXACML의 접근 제어 정책 모델을 보여준다.

Fig. 4와 같이 정책 변환 모듈에서 사용되는 GeoXACML 정책은 정책, 정책 집합으로 구성되며, 정책은 하나의 Target과 하나 혹은 다수의 규칙, 그리고 의무조항(Obligation) 등을 포함한다. 여러 개의 정책들은 Rule Combining Algorithm에 의해서 결합되어 사용될 수 있다. Table 2는 GeoXACML의 주요 정책 구성 요소에 대한 설명을 보여준다.

Table 2. Component of GeoXACML Policy

Component	Description
Policy	- A set of rules, an identifier for the rule-combining algorithm and (optionally) a set of obligations.
Policy Set	- A set of policies, other policy sets, a policy-combining algorithm and (optionally) a set of obligations.
Target	- The set of decision requests, identified by definitions for resource, subject and action, that a rule, policy or policy set is intended to evaluate
Rule	- A target, an effect and a condition. A component of a policy.
Obligation	- An operation specified in a policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision
Combining Algorithm	- The procedure for combining the decision and obligations from multiple policies and multiple rules.

Table 2와 같이 정책 변환 모듈에서 작성되는 새로운 정책은 정책 구성 요소에 기준하여 GeoXACML로 변환된다. GeoXACML은 정책 구성간 사용되는 데이타 타입과 함수를 시스템에서의 필요에 의해 새로 추가하는 방법 또한 제공한다.

3.2.3 정책 저장 모듈

정책 저장 모듈은 정책 변환 모듈을 통하여 GeoXACML로 변경된 공간정보 접근 제어 정책을 정책 저장소에 저장 및 관리한다. 생성된 GeoXACML 정책은 WMS 또는 WFS 중 어떤 서비스를 위한 정책인지 구별하여 관리하게 되며, 하나의 정책 집합을 하나의 파일로서 관리한다.

3.3 ANP 평가 구조 설계

본 절에서는 Geo PEP를 구성하는 접근 요청 GUI인터페이스 모듈과 접근 요청 관리자인 요청 분석 모듈, 결과 반환 모듈에 대해서 설명한다.

3.3.1 인터페이스 모듈

인터페이스 모듈은 질의 생성을 위한 사용자 인터페이스를 제공하며, Fig. 5는 Geo PEP의 인터페이스 모듈 실행 화면을 보여준다.

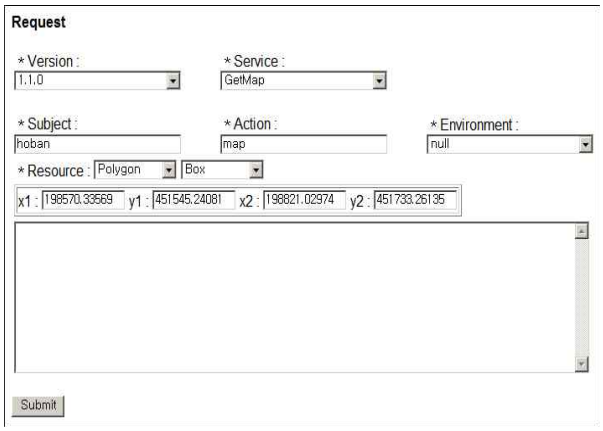

Figure 5. Execution Screen of Geo PEP Interface Module

Fig. 5와 같이 사용자는 인터페이스 모듈을 통해서 요청 및 질의를 입력할 수 있다. WMS Version 1.1.0에 GetMap 연산을 선택한 이 요청에서는 Subject가 hoban이고, Action이 map이며, Resource가 (198570.33569, 451545.24081 198821.02974, 451733.26135) 좌표를 갖는 Box 타입의 Polygon으로 GetMap 연산을 요청하게 된다. 또한 인터페이스 모듈은 WMS 또는 WFS 접근 요청에 대한 응답 결과를 반환된다.

3.3.2 요청 분석 모듈

요청 분석 모듈은 사용자로부터 입력받은 공간 요청을 분석하는 역할을 수행한다. 또한 접근 서비스와 연산 종류, 요청자의 Target 정보, 공간정보 등으로 분석된 서비스 접근 요청 정보를 인스턴스에 담아 Context Handler로 전송한다. 이때 공간정보는 GeoXACML에서 명시된 GML을 사용하여 표현되며, GML은 OGC의 단순기하에 따른 공간 데이타 모델을 사용한다.

3.3.3 결과 반환 모듈

결과 반환 모듈은 입력받은 요청이 Geo PDP의 공간 연산을 거쳐 생성된 응답을 요청자에게 반환한다. 즉, Geo PDP의 공간 연산에 따라 Context Handler로부터 전송받은 WMS 또는 WFS 질의 결과와 정책에 포함된 Obligation을 요청자에게 반환한다.

3.4 Geo PDP

본 절에서는 Geo PDP를 구성하는 정책 처리 관리자인 정책 분석 모듈, 정책 검색 모듈과 정책 판별 관리자인 공간 연산 모듈, 정책 판별 모듈에 대해서 설명한다.

3.4.1 정책 분석 모듈

정책 분석 모듈은 요청에 해당하는 정책을 분석하여 정책 적용 대상에 해당하는 Target의 4요소인 개체, 자원, 동작, 환경과 연산을 위해 필요한 공간정보를 DOM을 사용하여 추출한다. Fig. 6은 DOM API를 이용한 GeoXACML 분석 과정을 보여준다.

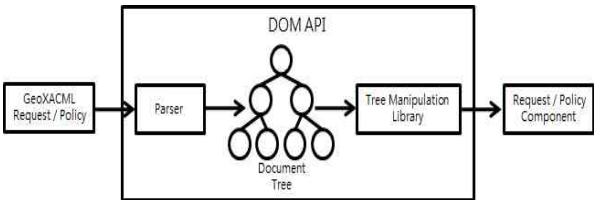

Figure 6. Analysis Process of GeoXACML

Fig. 6과 같이 DOM은 GeoXACML 문서를 문서 트리 구조로 변환한 후, 생성된 트리 구조에 DOM API를 이용하여 GeoXACML 문서의 조작(생성, 수정, 삭제 등)을 수행한다.

3.4.2 정책 검색 모듈

정책 검색 모듈은 정책 분석 모듈에서 분석한 접근 요청 컨텍스트의 개체, 자원 및 동작의 내용을 타깃의 내용인 개체, 자원 및 동작과 비교하여 정책 저장소로부터 공간정보 접근 제어 정책을 조회한다. GeoXACML은 XML에 기반하므로 정책 검색 모듈은 XPath와 XQuery를 이용하여 정책 저장소에서 관련 정책을 검색한다.

3.4.3 공간 연산 모듈

공간 연산 모듈은 GeoXACML 기반 정책에 대한 추가적인 공간 제약 조건을 정의하기 위해 확장 정의된 함수이다. 공간 연산 모듈은 접근 요청과 접근 제어 정책의 비교 분석을 위한 Table 3의 GeoXACML의 공간 데이타 타입과 Table 4의 공간 함수를 지원한다.

Table 3 및 Table 4와 같이 GeoXACML은 XACML 기반 정책에 대한 추가적인 공간 제약 조건을 정의하기 위해 확장 정의된 공간 데이터 타입과 공간 함수를 지원한다.

3.4.4 정책 판별 모듈

정책 판별 모듈은 정책 검색 모듈에서 전달된 공간 접근 제어 정책들과 다수의 요청 컨텍스트에 대하여 각 규칙들의 결과를 정책 결합 알고리즘(Policy combining algorithm)에 적용하여 접근여부를 결정한다. 또한 정책 판별 모듈에서 사용되는 정책 및 정책 집합들은 개체, 자원, 동작, 환경으로 정의된 Target을 포함하고 있다. Table 5는 정책 판별 모듈이 사용하는 GeoXACML의 규칙 평가표를 보여준다.

Table 3. Spatial Data Types of GeoXACML

Type	Description
Point	Point is 0-dimensional geometric objects and represented by a single coordinate.
LineString	Linestring is a path between locations. It takes the form of an ordered series of two or more points.
Polygon	Polygon is a representation of an area. The outer boundary of the polygon is represented by a ring.
MultiPoint	MultiPoint is set of point.
MultiLine String	MultiLineString is set of lineString.
MultiPolygon	MultiPolygon is set of polygon.

Table 4. Spatial Functions of GeoXACML

Type	Function
Topological Functions	Disjoint, Touches, Crosses, Within, Overlaps, Intersects, Equals, Contains
Geometric Functions	Buffer, Boundary, Centroid, ConvexHull, Difference, SymDifference, Intersection, Union
Scalar Functions	Area, Distance, IsWithinDistance, Length
Functions of Check Special Characteristics	IsSimple, IsColsed, IsValid
Bag Functions	GeometryOneAndOnly, GeometryBagSize, GeometryIsIn, GeometryBag
Set Functions	GeometryBagIntersection, GeometryBagAtLeastOneMemberOf, GeometryBagUnion, GeometryBagSubset, GeometrySetEquals
Conversion Functions	ConvertToMetre, ConvertToSquareMetre

Table 5. Policy Estimation Table of GeoXACML

Target	Condition	Rule Value
Match	True	Effect
Match	False	Not Applicable
Match	Indeterminate	Indeterminate
No-match	Don’t care	Not Applicable
Indeterminate	Don’t care	Indeterminate

Table 5와 같이 정책 판별 모듈은 규칙 평가표에 의거하여 규칙 결과를 산출하며, 규칙의 결과는 규칙 요소에 포함된 Effect에서 정의된 Permit, Deny, Indeterminate, Not Applicable이 된다. 또한 공 GeoXACML 기반의 접근 제어 시스템에서는 공간 연산에 의한 부분 반환도 허용한다. Table 6은 GeoXACML의 결합 알고리즘을 보여준다.

Table 6. Combination Algorithm of GeoXACML

Algorithm	Description	Applicable range
Deny-Overrides	If a single "Deny" result is encountered, then the combined result is "Deny".	Rules, and policies applicable
Permit-Overrides	If a single "Permit" result is encountered, then the combined result is "Permit".	
First-Applicable	First element in the list of rules whose target and condition is applicable to the decision request.	
Only-one-Applicable	Ensures that one and only one policy or policy set is applicable by virtue of their targets.	Only policies applicable

Table 6과 같이 정책 판별 모듈에서 사용되는 대표적 정책 결합 알고리즘은 Deny 우선의 Deny-Overrides, Permit 우선의 Permit-Overrides, 제일 처음 나온 결과가 최종 결과로 반환되는 First-Applicable, 적용 가능한 정책이 하나 이상이면 Indeterminate이 되는 Only-one-Applicable 등이 있다.

3.5 Geo PIP

본 절에서는 Geo PIP를 구성하는 공간정보 서비스 관리자인 세션 관리 모듈과 공간정보 서비스 접근 모듈에 대해서 설명한다.

3.5.1 세션 관리 모듈

공간 연산을 통해 접근 요청자에게 서비스의 접근이 허가되면 세션 관리 모듈은 공간정보 서비스와 Geo PEP 사이의 요청자 세션 정보를 관리한다. 세션 정보는 요청자의 Subject, Action, Resource, Environment에 근거하며 잔여 시간, 최대 세션 시간, 유휴 시간, 최대 유휴 시간 등을 포함한다.

3.5.2 공간정보 서비스 접근 모듈

공간정보 서비스 접근 모듈은 Context Handler를 통하여 Geo PDP로부터의 공간정보 서비스 접근 질의를 WMS 또는 WFS에 전달하며, 또한 질의에 대한 응답을 WMS 또는 WFS로부터 추출하여 Geo PDP로 반환한다.

3.6 Context Handler

Context Handler는 서비스 접근 요청을 GeoXACML 정규 표현식으로 변환하거나 GeoXACML 정규 표현식인 권한부여 결정을 외부의 응답 형식으로 변환하는 시스템 구성요소이다. 즉, 요청자의 속성이 선택적으로 포함된 접근 요청을 Geo PEP로부터 받으면 이러한 접근 요청을 GeoXACML 요청 문맥으로 변환하여 Geo PDP로 보낸다. 또한 Geo PDP로부터 받은 연산 결과를 GeoXACML 응답 문맥으로 변환하여 Geo PEP로도 전송한다.

4. 시스템 구현

본 장에서는 시스템의 구현 환경을 살펴보고, GeoXACML 기반의 접근 제어 시스템의 주요 기능에 대하여 상세히 설명한다. 또한, 본 접근 제어 시스템의 효용성을 검증하기 위하여 가상 시나리오를 적용한 내용에 대해서 기술한다.

4.1 구현 환경

본 논문에서 시스템을 구현하기 위하여 구축한 구현 환경은 다음과 같다. 운영체제로는 Microsoft Windows 7을 사용하였고 프로그래밍 언어로는 Java 1.6.0_10-b33을 사용하였다. 그리고 웹 서버를 구축하기 위하여 Apache 2.2.11과 Tomcat 6.0.35를 사용하였으며, WMS/WFS를 위해 GeoServer 2.1.3을 사용하였다. 또한 접근 제어를 위한 요청 접수 및 연산을 확장하기 위하여 SUN에서 Sun XACML 2.0을 사용하였다. 그리고 공간 데이타 처리를 위해 JTS Topology Suite 1.8.0[2]과 질의 및 정책 분석을 위해 DOM 1.0을 사용하였다.

4.2 가상 시나리오

본 논문에서는 GeoXACML 기반의 접근 제어 시스템에 대한 효용성을 검증하기 위해 접근 권한이 중요시되는 전시 군사지역이 포함된 공간정보에 대하여 접근 요청 가상 시나리오에 대해서 적용해 보았다. Fig. 7은 가상 시나리오의 정책 설계 화면을 보여준다.

Fig. 7의 가상 시나리오는 다음과 같다. 임의의 부대는 area1 지역을 군 주둔 거점으로 한다. 또한 폭 150m 이내 영역인 road1과 작전계획에 의거하여 교전 예상 지역인 area2, area3, area4 내에서 가옥이 100채 이하인 교차 영역에 공병대대를 투입하여 지뢰를 매설함

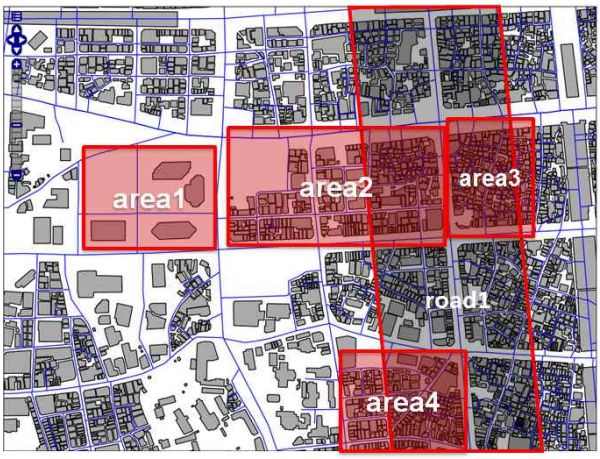

Figure 7. Policy Design Screen of Scenario

으로 적군의 습격에 대비하고자 한다. 작전이 시작되면 정책이 시행되며 임의의 일반 이용자인 hoban에게는 해당 작전 지역의 어떠한 공간 객체도 반환하지 못하도록 하였다. Fig. 8은 접근 제어 시스템의 작전 지역에 대한 서비스 접근 요청 생성 화면을 보여준다.

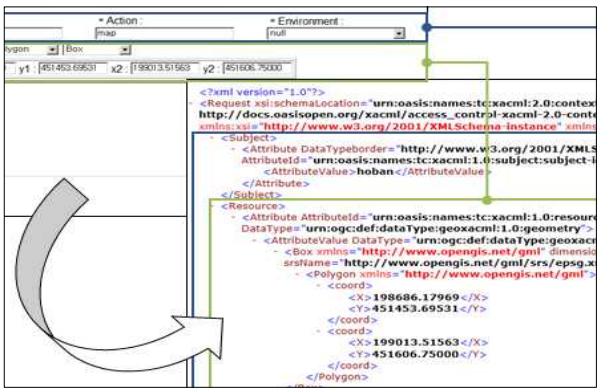

Figure 8. Creation Screen of Service Access Request

Fig. 8과 같이 요청 생성 브라우저는 서비스 종류, 서비스의 버전, Target, 서비스를 요청할 공간 좌표 등을 입력하여 제출함으로 요청을 생성하며, 생성된 요청은 Context Handler을 통해 GeoXACML의 형태로 생성되어 Geo PDP로 전달된다. 가상 시나리오의 서비스 접근 요청은 hoban이 (198686.17969, 451453.69531 199013.51563, 451606.75000) 범위의 Polygon 영역에 대하여 GetMap 연산을 질의하는 서비스 접근 요청이다. Fig. 9는 가상 시나리오의 접근 제어 시스템에서 사용되는 정책 생성 화면을 보여준다.

Fig. 9와 같이 정책 생성 브라우저는 정책 집합, 정책, 규칙별 탭을 채워서 제출하는 방식으로 정책을 생성 및 저장하고, 저장된 정책은 브라우저에서 호출하여 수정 및 삭제가 가능하다. 정책 생성 폼은 정책 단위의 Target과 Rule 단위 Target를 입력받으며, 공간 연산을 위한 속성 값을 설정할 수 있다. 가상 시나리오의 접근 제어 시스템 정책은 Fig. 7의 정책 설계에 맞추어 area1, area2, area3, area4의 4개 지역에 대한 공간 연산을 수행하는 정책이며, 자료형 선언자와 구조상 중복되는 area2, area3, area4에 대하여 area2만을 남기고 생략하였다.

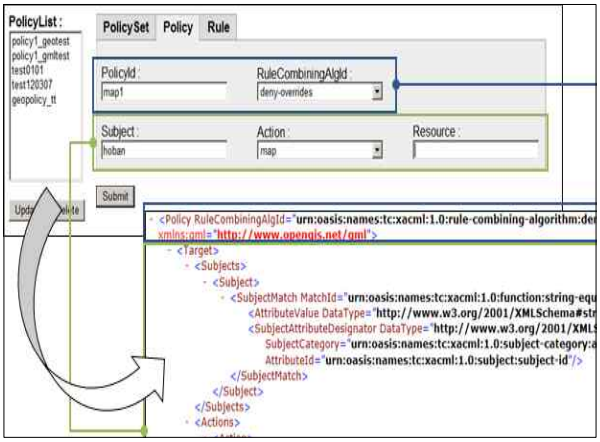

Figure 9. Policy Creation Screen of Access Control System

Fig. 7에서 군 주둔 거점인 area1은 (198570.33569, 451545.24081 198821.02974, 451733.26135)과 WMS에서 서비스 되는 공간 객체들과 Disjoint 연산을 수행함으로써 해당 영역의 공간 객체에 대한 접근을 제어한다.

road1 영역과 교전 예상지역의 교차 영역에 대한 접근 제어는 area2, area3, area4 모두에 대해서 동일한 연산을 수행한다. 교전 예상지역인 area2는 최초 (198840.35156, 451767.62500 199250.35938, 452000.00000)과 WMS에서 서비스 되는 공간 객체들과 Contain 연산을 수행한다. area2의 공간 객체를 Geometry의 Bag으로 재구성한 후 GeometryBagSize 연산을 수행하여 Bag 내 공간 객체를 측량한다. GeometryBagSize 연산의 Integer 결과 값을 XACML에서 제공하는 연산자 중 하나인 IntegerGreaterThan을 사용하여 100 이상인지 여부를 확인한다. 가옥이 100채 이하인 교차 영역에 공병대대를 투입하여 지뢰를 매설하기 위해 IntegerGreaterThan의 결과 값이 100 이하이면 참을 반환하도록 한다. 이 Boolean 값을 다시 (198840.35156, 451767.62500 199250.35938, 452000.00000) 내의 공간 객체들과 and 연산을 수행하여 area2 영역의 공간 객체가 100을 이하라면 지정된 Polygon 내의 공간 객체들을 반환하게 된다.

교전 예상지역인 area2, area3, area4내에서 가옥이

100채 이하인 영역의 공간 객체들을 Bag으로 묶어 road1의 공간 객체를 담은 Bag과 Geometry BagIntersection 연산을 수행하면 두 Bag 모두에 포함된 같은 공간 객체만을 Bag으로 반환하게 되며, 이 공간 객체에 대한 접근 제어를 통하여 가상 시나리오의 정책이 완성된다. Fig. 10은 가상 시나리오의 접근 제어가 이루어진 질의 응답 화면을 보여준다.

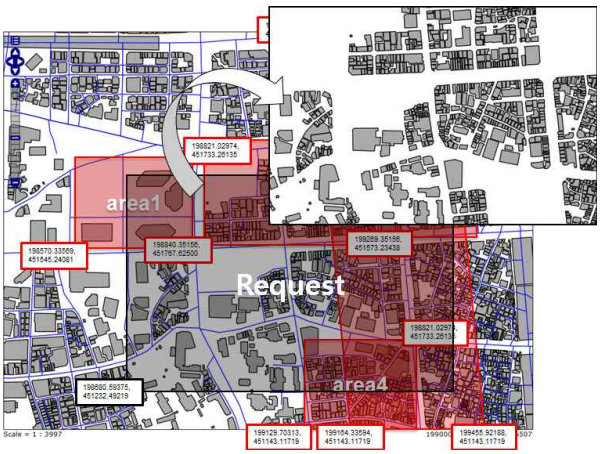

Figure 10. Request and Response Screen of Scenario

Fig. 10과 같이 군 주둔 거점인 area1과 가옥 수가 100이 넘지 않는 area3, area4의 교차 영역에 위치한 공간 객체는 반환되지 않았기 때문에 접근 제어가 제대로 이루어짐을 확인할 수 있다.

5. 결 론

최근 공간정보 보안을 위한 각종 기술의 필요성이 증대됨과 동시에 보안 서비스에서 사용되는 정책의 수정 및 통합 시 많은 비용이 소요되거나 신뢰성이 떨어지는 문제점이 큰 이슈가 되고 있다.

따라서, 본 논문에서는 공간 연산을 통해 접근을 제어하고 상호운용성을 가지는 GeoXACML 기반의 접근 제어 시스템을 설계 및 구현하였다. GeoXACML 기반의 접근 제어 시스템은 문법 및 의미의 확장이 용이하고 객체별 접근 제한도 지원한다. 특히 특정 지역에서만 해당 공간정보에 접근할 수 있도록 하는 공간적 범위와 조건에 의거한 접근 제한도 가능하다.

마지막으로, 본 논문에서 개발한 GeoXACML 기반의 공간정보 접근 제어 시스템을 접근 권한이 요구되는 군사 지역에 대해 가상 시나리오를 설정하여 적용해 봄으로써 본 시스템의 효용성을 검증하였다.

References

[1] CBDI-Forum, 2003, XACML Access Control Markup Language Ratified as OASIS Open Standard.

[2] JTS Topology Suite, http://www.vividsolutions.com/jts/jtshome.htm/.

[3] Kang, H. K; Shin, I. S; Kim, J. J; Han, K. J. 2010, MR-Tree: A Mapping-based R-Tree for Efficient Spatial Searching, Journal of KSIS, 18(4):109-120.

[4] Kim, J. H; Moon, K. Y. 2003, Trend of eXtensible Access Control Markup Language Based on XML, Korea Institute of Information Security & Cryptology, 13(4):68-73.

[5] Lorch, M.; Proctor, S; Lepro, R. 2003, First Experiences Using XACML for Access Control in Distributed Systems, Proceeding of ACM Workshop on XML Security, 25-37.

[6] Matheus, A. Access Control for Geo Web Services using GeoXACML, http://www.unibw.de/inf3/forschung/projects/opengissec/flyergeoxacml/.../down2/.

[7] Moses, T; Anderson, A; Proctor, S; Godik, S. 2003, XACML Profile for Web Service, OASIS TC Working Draft.

[8] OASIS, 2004, eXtensible Access Control Markup Language Version 2.0, http://www.oasis-open.org/specs/index.php#xacmlv2.0.

[9] Open Geospatial Consortium, 2007, GeoXACML Implementation Specification Version 1.0, http://www.opengeospatial.org/standards/geoxacml/.

[10] Open Geospatial Consortium, 2008, Geospatial eXtensible Access Control Markup Language (GeoXACML).

[11] Park, C. G; Park, H. H; Kang, H. K; Han, K. J. 2007, Development of an OpenGIS Spatial Interface based on Oracle, Journal of KSIS, 9(2):1-11.

[12] Sun Microsystems, 2006, Sun's XACML Implementation, http://sunxacml.sourceforge.net/.

[13] Technical Corporation, 2011, Functionality and Usage of GeoXACML Version 1.0.

[14] Tao, H. 2005, A XACML-based Access Control Model for Web Service, Proceeding of International Conference on Wireless Communi-

cations, Networking and Mobile Computing, 2: 1140-1144.

[15] Telecommunications Technology Association, 2010, Geospatial Information Copyright Protection-Right Expression and Access Control: Functional Requirements.

[16] Yang, K. D; Lee, H. J. 2006, Design of Access Control for Web based Enterprise Application System Using XACML, Autumn workshop presentation file of Korean Institute of Information Scientists and Engineers, 33(2C):467-471.

논문접수 : 2013.01.02
수 정 일 : 2013.06.25
심사완료 : 2013.07.25