제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

전자도서관 인증과 인가에 대한 연구

원형석, 김태성, 조상래, 진승헌
한국전자통신연구원
e-mail : (moho,taesung,sangrae,jinsh)@etri.re.kr

A study on a digital library authentication and authorization architecture

Hyung Suk Won, Taesung Kim, Sangrae Cho, Seunghun Jin
Electronics and Telecommunications Research Institute

요 약

전자도서관에서 기존의 자료 및 새로운 자료들이 디지털화되어 사용자에게 제공되고 있다. 하지만 디지털 자료에 대한 접근시 기존의 도서관 서비스와는 달리 많은 제약 조건 때문에, 사용자의 접근이 어려워 유용한 정보를 가진 많은 양의 디지털화된 자료들의 서비스들이 아주 제한적으로 이루어지고 있다. 이것은 디지털 자료 접근시 기존의 오프라인 도서관에서 사용하는 인증인가 방식을 그대로 사용하고 있기 때문이다. 전자도서관 인증과 인가에 대한 연구가 외국은 활발한 반면, 우리나라에서는 이에 대한 연구가 행해지고 있지 않다. 이에 본 논문은 전자도서관의 디지털 자료나 웹 서비스 접근 시 인증 인가가 필요한 이유와 인증인가 모델 개발시 고려사항들을 설명하고 이를 해결하기 위한 여러 인증 인가 모델들을 소개한다. 그리고 향후 개발될 전자도서관 인증인가 예상 모델과 개발에 필요한 향후과제를 제시한다.

1. 서론

이용자에게 보다 나은 자료와 정보를 제공하기 위해 도서 외에 디지털 자료와 웹 서비스를 제공할 수 있는 전자도서관 구축 사업이 정부, 연구기관, 대학을 중심으로 활발하게 시행되었다. 하지만, 이렇게 구축된 디지털화된 자료를 이용자에게 서비스하기에는 복제나 배포 등과 관련된 license 나 저작권 등의 문제로 아주 제한적인 이용만이 가능하게 되어 전자도서관 운영의 본래의 취지를 살리지 못하고 있다. 이것은 기존의 오프라인 도서관에서 쓰던 인증과 인가 방식을 그대로 사용함으로써 디지털 자료에 대한 관리와 서비스가 불가능하게 되어 적절하게 대처할 수 없기 때문이다. 이에 외국에서는 여러 인증인가 모델들이 제시되고 있다. 하지만 국내에서는 이러한 연구가 미흡하다. 따라서 본 논문에서는 전자도서관에서 인증과 인가가 필요한 이유와 고려사항들을 설명하고, 지금까지 제시된 여러 모델들을 살펴보고 국내 전자도서관에 적용이 가능한 인증인가 모델을 제시한다.

2. 전자도서관에서의 인증과 인가

2.1 인증과 인가

한국정보통신기술협회(TTA)[1]의 정보통신 용어정의에 따르면, 인증(authentication)이란 망을 통해 컴퓨터에 접속해 오는 사용자가 등록된(허가받은) 사용자인지를 확인하는 것이고, 인가(authorization)란 특정한 프로그램, 데이터 또는 시스템 서비스 등에 접근할 수 있는 권한이 주어지는 것을 말한다.

2.2 필요한 이유

이용자의 입장에서 전자도서관은 원격이용이 가능하고 이용시간의 제한을 받지 않고 여러 사람이 동시에 자료를 이용할 수 있고 검색의 도움을 받아 정보탐색의 시간을 줄일 수 있다는 장점을 가진다[2]. 이러한 서비스는 전자도서관 구축 사업의 일환으로 기존의 자료를 디지털 자료로 변환하고 이것을 웹을 통해 서비스함으로써 가능해진다.

일반적으로 전자도서관에서 제공하는 자료, 서비스들과 그에 따른 제한사항을 나열해보면 아래 [표 1]과 같다.

[표 1] 전자도서관 서비스와 제한사항

자료 및 서비스		이용제한
웹 관련 서비스	검색	웹 접속하는 사용자 모두
	개인 정보변경, 갱신, 예약, 예약취소	기관 소속자, 협정기관 소속자
	도서신청	기관 소속자만 가능
	원문복사신청	기관소속자, 협정기관 업무담당자
학위논문		저자가 배포에 동의한 것만 서비스 가능
학술데이타베이스 (CD net service)		기관 소속자만 가능
전자저널		기관 소속자만 가능
ebook		기관 소속자만 가능
VOD (기존 analog 자료인 audio/video tape 을 디지털 자료로 변환한 것)		analog 소스가 기관이 생성한 것일 경우에만 서비스 가능

디지털 자료와 웹 서비스에 여러 제한사항이 있다는 것을 알 수 있다. 이러한 제한 사항은 앞에서 언급한 바와 같이 자료의 license 나 저작권 등의 이유에서 비롯된 것으로 모든 전자도서관에 해당하는 일반적인 사항이다. 이러한 전자도서관의 서비스나 자료에 대한 적절한 이용을 가능하게 하기 위해서는 디지털 자료에 대한 인증인가 모델이 필요하다. 또한, 한기관의 디지털 자료는 한정되어 있으므로, 보다 나은 서비스를 위해서 타기관 또는 현재 일반적으로 전자도서관에서 서비스 되고 있는 전자저널 상용서비스와 도서구매를 위한 출판사와의 연계가 필요한데 이를 위해서 기관간의 인증인가도 전자도서관의 인증인가 모델 구조에 필수적인 내용이다.

2.3 고려사항

일반적으로 전자도서관의 인증과 인가 모델에서 다음의 내용들을 고려사항으로 제시하고 있다[3].

(1) Privacy : 소속기관외에 아이디를 포함한 어떤 개인정보도 서비스를 제공하는 사이트에 제공되지 않아야 한다.

(2) Partitioning of information : 만약 정보의 공유가 필요할 때라도 그 중복을 최소화해야 한다. 아이디 대신 pseudo anonymous identity 를 사용해야 한다.

(3) Separation of authentication and authorization : 개인의 신분과 권한이 계속 변화하기 때문에 변화에 맞게 인증과 인가가 따로 분리되어 운영되어야 한다.

3. 인증인가방식

인증인가 방식은 다음과 같이 분류할 수 있다[3][4].

3.1 아이디/패스워드 방식

사용자마다 부여된 아이디와 패스워드를 확인하여 인증과 인가를 하는 방식이다. 전통적인 도서관 시스템 이용시 많이 사용되는 형태로써 이용자들이 친숙한 방식이다. 기관간 자료 이용시 개인에 따라 맞춤 서비스가 가능한 장점이 있지만 타기관에 아이디와 패스워드가 노출되므로 privacy 에 문제가 있고 아이디/패스워드 관리 또한 여러기관에서 중복되어 관리되어야 하는 단점이 있다.

3.2. IP 방식

등록된 IP 를 가진 컴퓨터에서만 자료에 대한 접근을 허가하는 방식으로 현재 전자도서관에서 가장 일반적으로 쓰이고 있는 방식이지만 물리적인 위치로 접근을 제한하는 방식이기 때문에 기관에 소속된 사용자가 집이나 외부에 나가서 자료를 이용할 수 없는 단점이 있다.

3.3. Proxy 방식

IP 방식의 특별한 경우로 볼 수 있는데, 사용자가 proxy 를 통해 정보에 접근하게 하는 것이다. 사용자는 proxy 에 접근시 인증 과정을 거쳐야 한다. proxy 를 이용할 경우 서비스 제공자는 사용자를 구분할 수 없으므로 사용자 개인별로 맞춤 서비스를 할 수 없고 proxy 의 관리가 매우 어렵다.

3.4 인증서 방식

최근에 많이 연구되고 있는 방식으로 인증서(certificate)[5]를 이용하는 방식이다. 모든 웹 브라우저에서 지원되고 가장 보안이 뛰어난 방식이다. 최근에 국가적으로 인증서를 기반으로 하는 안전한 정보보호 기반 구축을 활발히 하고 있다. 하지만 인증서 관리와 운용 및 연동의 어려움과 응용 서비스의 부재는 인증서 확산에 장애가 되고 있다. 현재 이와 같은 문제점을 해결하기 위한 방안들이 활발히 제안되거나 적용되고 있다.

4. 최근 연구

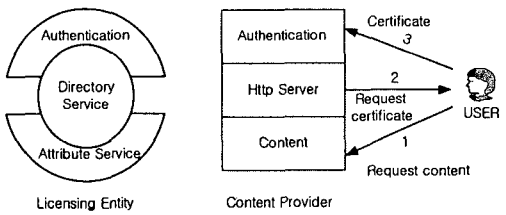
최근에 연구되고 있는 모델들의 구조를 살펴보면 주로 인증서를 이용한 방식이 많고, 특히 접근관리를 위해 인가가 많이 연구되고 있는데, 일반적으로 access model 이라는 이름으로 연구되고 있다. 그리고, 3 장에서 언급된 여러 방식들을 혼합하여 적용하는 hybrid 모델도 많이 연구되고 있다.

4.1 인증서 이용 모델[5],[6]

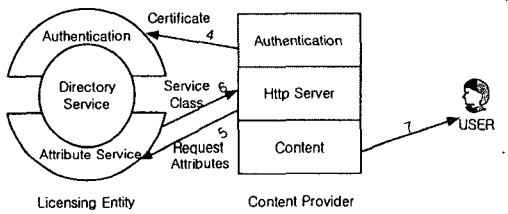
사용자가 자료에 접근시, 웹서버는 개인의 인증서를 이용하여 개인을 인증하고 개인의 권한을 권한내용이 저장되어 있는 디렉토리에서 확인하여 자료 접근 권한을 웹서버에 다시 알려주면 권한에 따라 웹서버는 자료에 접근을 시도한 사용자에게 가능한 서비스를 하게 된다. 그 절차는 [그림 1] [그림 2]의 번호 순서대로 진행되고, 각각의 과정의 자세한 설명은 다음과 같다.

1. 사용자가 웹을 통해서 원하는 자료에 접근을 시도한다.
2. 웹서버가 사용자에게 인증서를 요구한다.
3. 사용자가 인증서를 제공한다.
4. 인가에 필요한 정보를 인증서에서 추출한다.

5. 웹서버가 Attribute server 에 연결하고 서버의 인증서를 제시하면 attribute server 는 요청 서버를 확인하고 요청한 서버의 자료에 대한 사용자의 권한을 결정한다.
6. 접근 권한이 요청 서버에게 리턴된다.
7. 웹서버는 사용자에게 부여된 권한을 가지고 접근을 허가한다.



[그림 1] 인증서 이용 모델 (1)



[그림 2] 인증서 이용 모델 (2)

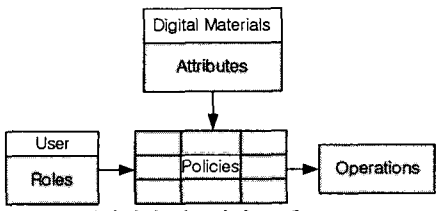
4.2 접근관리 모델 (Access model)

자료에 접근하는 사용자의 적절한 관리를 위한 것으로, [그림 3]과 같이 user, digital material, policy, operation 으로 구성된다. 기관내의 어떤 role 을 가진 사용자에게 어떤 attributes 를 가진 digital material 에 대해 어떤 operation 을 할 수 있게 할 지를 policy 로 정해놓은 뒤 사용자의 접근을 policy 로 제어하는 것이 목적이다[7]. 이렇게 하면 role, attribute, policy 가 다이나믹하게 반영될 수 있다.

형식언어로 기술하면,

if (role) and (attribute) then (operation)

으로 표현할 수 있다.



[그림 3] 일반적인 접근관리 모델

대학을 예로 들어, 도서관 자료가 일반, 지정, 참고도서로 구분되어 있고, 교수는 일반도서는 30 일 대출, 지정도서는 10 일 대출가능하고 참고도서의 경우 도서관내에서만 열람이 가능하다. 그리고, 학생은 일반도서는 10 일대출, 지정도서와 참고도서는 도서관내에서만 열람이 가능하다고 가정하자. 이것을 접근관리모델로 바꾸어 생각해보면, User 의 role 에는 교수, 학생이 있고, material 에 일반도서, 참고도서, 지정도서가 있고, operation 에는 10 일대출, 30 일대출, 도서관내에서만 열람가능이 있는 것이다. 이 내용을 policy 테이블로 만들면 다음과 같다.

Role	Attribute	Operation
교수	일반도서	30 일 대출
교수	지정도서	10 일 대출
학생	일반도서	10 일 대출
학생	지정도서	도서관내에서만 열람
교수 또는 학생	참고도서	도서관내에서만 열람

만약, 도서관이 교수와 학생에게 동일한 권한을 적용하기로 정하고 일반도서의 경우 모두 30 일대출, 참고도서와 지정도서의 경우 도서관내에서만 열람이 가능하도록 한다면, role, attribute, operation 에는 변함이 없고 policy 테이블만 아래와 같이 수정되면 된다.

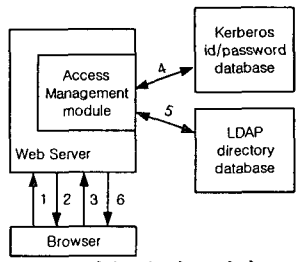
Role	Attribute	Operation
교수 또는 학생	일반도서	30 일 대출
교수 또는 학생	지정/참고도서	도서관내에서만 열람

5. 인증인가모델

5.1 인증인가 모델 예[8]

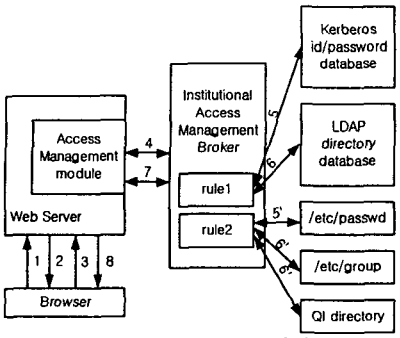
인증인가 모델에는 앞에서 살펴본 기본적으로 인증서와 접근관리 모델을 적용한 여러가지 다양한 변형이 제시될 수 있다.

먼저 사용자와 서비스 제공자가 동일 기관 소속일 경우일 때, [그림 4]와 같이 가장 간단한 웹 접근 관리 형태로 구성된다. 이 방식은 사용자가 웹 브라우저를 닫거나 로그아웃 하지 않으면 다른 사람이 그대로 그 권한을 사용하게 되는 문제가 있다. 그리고, 일반적으로 한 기관 내에 두개 이상의 웹서버나 두개이상의 인증이나 디렉토리 시스템이 존재하게 되는데, 이런 경우 관리가 매우 복잡하거나 불가능해진다.



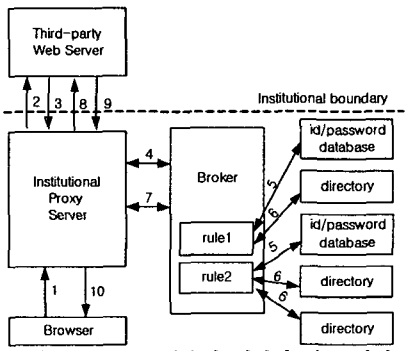
[그림 4] 단순 웹 접근 관리

두개이상의 디렉토리 시스템이 있을 경우 디렉토리에 상관없이 접근을 하나로 통합하려면 [그림 5]와 같이 "브로커(broker)"를 도입하여 사용자가 어느 디렉토리에 속하는지를 처리하게 한다. 이 방식으로 앞의 모델의 문제점을 해결할 수 있다.



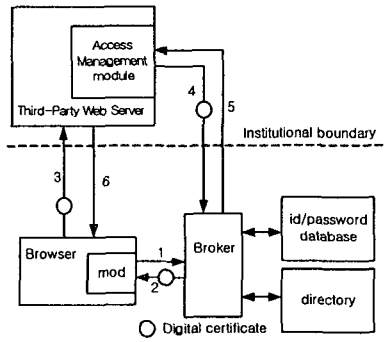
[그림 5] 브로커를 통한 접근 관리

두개이상의 기관이 연결될 경우, [그림 6]처럼 proxy 를 통해 외부 서비스를 제공할 수 있다. 현재 많이 쓰이는 방식이지만 앞에서 언급한 바와 같이 proxy 자체의 단점을 가지고 있다.



[그림 6] proxy 를 이용한 기관간 접근 관리

이것을 해결하기 위해 [그림 7]의 인증서를 이용한 방식이 제시되었다. 이 방식은 인증서가 일시적인 것이므로 인증서와 관련된 폐기, 위탁, 복구 등의 문제에서 벗어날 수 있다. 하지만 인증서가 효력기간이 너무 짧아 사용할 때마다 인증서를 받아야하므로 사용자가 불편하다.



[그림 7] 인증서를 이용한 접근 관리

5.2 향후 인증인가 모델 개발 방향

지금까지 살펴본 바와 같이, 하나의 완벽한 인증인가 모델로 정해진 것은 없다. 따라서, 필요한 상황에 맞게 모델을 구성하고 시험 후 문제점을 제거해 나가는 과정을 거쳐야 한다. 국내에서는 인증서를 기반으로 하는 안전한 정보보호 기반 구축과 이에 따른 연구가 활발하다. 따라서 향후 웹을 기반으로 하는 국내의 전자도서관의 인증인가 시스템도 인증서를 기반으로 하는 인증인가 시스템이 일반적인 모델이 될 것으로 예상된다. 최근에 미국은 Internet2[9] 프로젝트에서 미들웨어로 Shibboleth[10]라는 기관간 자료공유를 위한 인증인가 시스템을 연구개발 중에 있다. 이처럼 인증인가 모델을 실제 현장에 적용하기 위한 다양한 연구가 요구된다[3]. 사용자가 두기관 이상에 소속되어 있을 경우에 각기 다른 권한에 대한 관리를 위한 방법에 대한 연구, 기관이 CA 가 아닐 경우에 대한 연구, 3 개기관 이상의 기관간 연동을 통한 파일럿 테스트, 기타 인증서 관리와 관련된 연구, 익명을 유지하기 위한 방법에 대한 연구 등이 이에 해당한다.

6. 결론

본 논문에서는 전자도서관에서 디지털 자료를 서비스하기 위해 인증인가가 필요한 이유를 설명하고, 이 문제를 해결하기 위해 외국에서 제시된 여러 방식들을 살펴보고, 향후 인증인가 모델의 개발방향을 예상해보았다. 외국의 다양한 연구에 비해, 국내의 연구는 거의 행해지고 있지 않다. 따라서, 국내에서도 지금까지의 디지털 자료 구축 위주의 연구에서 한 발 더 나아가 전자도서관의 인증인가 모델에 대한 활발한 연구가 필요하다. 또한, 이러한 연구를 전자출판물 관리나 전자정부, 회사, 병원 등, 기관의 디지털 접근 관리에 적용하기 위한 연구도 필요하다.

참고문헌

[1] http://www.tta.or.kr/
[2] http://www.lg.or.kr/lg_docs/index330.html
[3] David Millman, "Cross-Organizational Access Management: A digital library authentication and authorization architecture", D-Lib magazine, vol.5, no.11, 1999.
[4] Clifford Lynch, "A White paper on authentication and access management issues in cross-organizational use of networked information resources", Coalition for Networked Information. Apr. 1998.
[5] Digital Library Federation (DLF) and Corporation for Research and Educational Networking (CERN), "Digital certificate infrastructure (FAQ)".
[6] A digital library authentication and authorization architecture, 2000.
[7] William Yeo Arms, "Implementing policies for access management", D-lib magazine, Feb. 1998.
[8] Ariel Glenn and David Millman, "Access management of web-based services : An incremental approach to cross-organizational authentication and authorization", D-Lib Magazine, Sep. 1998.
[9] http://www.internet2.edu/
[10] Marlena Erdos, Scott Cantor, "Shibboleth-Architecture DRAFT v05", 2002.