전자도서관을 위한 전자책 교환 시스템 개발

나재무[0] 백혜선 이광재 이정훈 하동훈 이은정
경기대학교
ejlee@kyonggi.ac.kr

Development of an E-Book Exchange System for Digital Library

J.Na, H.Paik, K.Lee, J.Lee, D.Ha, Eunjung Lee
Dept. of Computer Science, Kyonggi Univ.

요 약

본 논문에서는 전자 도서관을 위한 저작권 보호 기능을 가진 전자책 교환 시스템 개발을 소개한다. 전자책은 암호화에 기반한 리더 시스템을 통해 저작권이 안전하게 보장되도록 하는 디지털 컨텐츠 유통을 위한 기술 표준이다. 전자책의 안전한 유통과 사용을 위해서 전자 도서관은 보유한 디지털 컨텐츠에 대해 적법한 사용 권한을 이용하여 대출을 해 줄 수 있어야 한다. 이를 위해 본 연구에서는 EBX(E-Book Exchange) 프로토콜에서 정의한 대출 기능을 구현한 도서관 서버를 개발하였고 전자책 리더 클라이언트를 통해 이러한 권한을 보호하면서 사용자가 전자책을 이용할 수 있게 지원하는 기능을 구현하였다.

1. 서 론

전자책 기술은 디지털 컨텐츠의 효과적인 생성, 배포 및 저작권 보호를 위한 인프라를 구축하려는 노력의 한 형태이다[5,6]. 이 기술은 현재의 도서관 시스템에 큰 영향을 미칠 것으로 예상된다. 기존의 오프라인 도서에 비하여 도서관이 보유한 전자책은 무한 권 대출할 수 있고 대출 및 반납을 위해 도서관에 직접 올 필요 없이 전자책을 다운로드 받고 반납하는 것이 가능하다. 이 외에도 다른 많은 장점을 가지는 전자도서관의 가능성은 저작권 보호를 위한 안정적이고 신뢰성 있는 시스템의 구축을 필요로 한다.

이러한 요구를 만족하기 위해 최근 전자적 저작권 보호(Digital Rights Management)를 위한 다양한 연구가 진행되고 있으며[3,4,5] 특히 몇몇 전자책 유통 시스템 개발사[6,7,8]를 중심으로 저작권 서버 구축이 활발히 진행되고 있다.

디지털 컨텐츠의 저작권을 보호하면서 전자책을 대출하여 사용자에게 전달할 수 있는 방식으로 제안된 표준이 전자책 교환(E-Book Exchange : EBX) 프로토콜이다[6]. 이것은 Open E-book 포럼에서 제시한 일차적인 프로토콜로서 전자책이 유통 및 사용 전 과정에서 암호화되어 있고 사용자가 전자책 리더 프로그램을 통해서만 전자책 컨텐츠에 접근하도록 허용하여 효과적인 저작권 보호를 가능하게 한다.

본 논문에서는 위의 전자책 교환 프로토콜에 기반하여 도서관에서 전자책을 대출하고 반납할 수 있는 시스템을 구축하였다. 도서관 서버는 사용자 DB와 책 DB를 가지고 책DB에는 전자책 파일 뿐 아니라 전자책들에 대해 도서관이 가진 권한과 대출할 수 있는 권한 정보를 포함한 Voucher를 보관하고 있다. 이 Voucher의 권한 정보는 사용자가 책을 대출했을 때 가질 수 있는 권한 정보를 정하게 되고 이를 기반으로 사용자의 대출한 책에 대한 권한 정보를 가지는 새로운 Voucher가 생성된다. 이러한 과정이 아래 그림 1에 나타나 있다.

본 논문의 구조는 다음과 같다. 2절에서는 전자책 표준 및 전자책 교환 프로토콜을 소개하고 3절에서는 본 시스템의 구조와 설계의 세부 사항을 소개한다. 4절에서는 구현된 시스템을 소개하고 5절에서 결론을 맺는다.

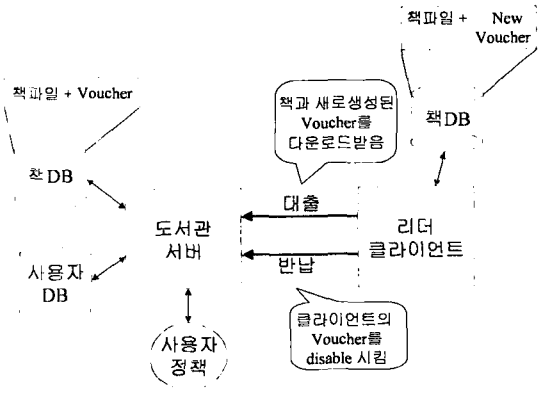

그림 1 저작권 보호 기능을 가진 도서관 시스템 구조

2. 저작권 보호를 위한 전자책 교환 프로토콜의 구성

전자책 교환 프로토콜은 전자책의 배포를 위한 EBX 서버 시스템과 사용자가 전자책을 접근할 수 있게 해 주는 EBX 리더 시스템으로 구성된다[5,6]. 서버 시스템은 제작자가 생성한 전자책 파일은 권리 증서(Voucher)와 함께 배포하는데, 이 때 전자책 파일은 비밀키로 암호화되어 있고 권리 증서는 이 비밀키를 포함하고 있는 파일이다. 권리 증서 파일은 전자책의 소유권 또는 사용권을 가진 사용자 클라이언트의 리더 시스템의 공개키로 암호화되고 전자책을 복호화할 수 있는 비밀키는 대응되는 비밀키를 가진 EBX 리더 시스템에 의해서만 얻어질 수 있다. 권리 증서는 비밀키를 저장하는 역할 뿐 아니라 이 전자책에 대해 해당 사용자가 가진 권한을 표현하는 역할을 한다. 유효기간이나 접근할 수 있는 책의 부분, 또는 사용할 수 있는 기능 등을 여기서 명시할 수 있다.

그러므로 전자책 교환 서버에서는 사용자를 위하여 전자책의 비밀키를 포함한 Voucher를 생성하고 이를 클라이언트 리더 시스템의 공개키로 암호화하게 된다. 이렇게 암호화된 Voucher는 전자책과 함께 클라이언트로 다운로드된다.

클라이언트 리더 시스템은 다운로드 받은 Voucher에서 비밀키를 얻어내어 전자책을 복호화하여 사용자에게 보여주어야 하며, 또한 Voucher에 의해 명시되어 있는 사용권한과 제약 사항이 만족되도록 감시할 책임이 있다.

3. 전자도서관을 위한 저작권 보호 시스템의 설계

전자책 교환 프로토콜 표준은 도서관의 대출과 개인간의 대여 프로토콜도 제시하고 있다. 전자책은 대여할 수 있는 권한과 대여 가능한 책의 권 수를 voucher에 명기하고 있다. 대출 또는 대여 시에 전자책 리더 시스템은 그 시스템의 voucher에서 사용 또는 대여 가능한 권수를 줄이고 새로운 voucher를 생성하여 그 책이 가진 권한 정보를 그대로 생성하여 넘긴다.

전자도서관에서 대출을 위해 처리해야 하는 일도 기본적인 대여 프로토콜의 과정과 같다. 전자도서관의 보유 도서는 무제한의 대출이 가능한 것도 있고 제한된 카피만 보유하고 있는 경우도 있을 것이다. 또한 해당 전자책에 대해 보유하고 있는 권한의 종류도 다양할 수 있다. 이것은 일반적인 리더 시스템과 마찬가지로 도서관 서버 시스템에 의해 지켜져야 하는 제약사항이며, 대출할 때 생성되는 voucher는 이러한 제약 사항을 그대로 반영하게 된다.

한편 도서관 시스템은 자체적으로 대출을 위한 정책을 가질 수 있다. 예를 들어 대학도서관에서 학생은 2주간 대출할 수 있고 한번에 대출 가능한 권수가 3권이며, 대학교원은 3달까지 대출가능하고 한번에 대출할 수 있는 권수의 제약이 없다. 또한 사용자의 대출 정지나 신분 상의 변경 등은 도서관이 가진 정책에 따라 반영되어야 하며, 이는 대출 가능한가를 나타내는 정보이다. 전자도서관에서는 이러한 정보도 더욱 세분화되어서 대출할 수 있는 책의 종류나 권한 정보의 허용 방식도 달라질 수 있다. 이것은 도서관의 정책 파일에 기록되어 대출 Voucher를 생성할 때 반영될 수 있다.

4. 전자도서관 시스템의 구현

본 시스템은 자바 언어로 개발되었으며, 도서관 서버와 리더 클라이언트 시스템으로 구성된다.

아래에서는 서버 시스템과 통신 부분, 클라이언트 시스템으로 나누어 시스템의 구현을 살펴본다.

도서관 서버 시스템은 (1) 책 DB와 사용자 DB를 관리하고 (2) 책의 대출 여부와 사용자의 대출 가능 여부를 검사할 수 있어야 하며, (3) 책의 대출을 위해 voucher를 생성할 수 있어야 한다. (4) 책 파일과 voucher 파일을 다운로드해 줄 수 있어야 한다.

한편 서버 시스템은 도서관 시스템은 사용자들의 공개키를 관리하기 위한 키 관리기능을 가져야 하며, 다운로드 시점 전에 클라이언트 시스템의 공개키를 가져와 저장해야 한다. 공개키는 Voucher를 암호화하는데 사용되며 이것은 클라이언트 시스템이 가진 개인키에 의해서만 복호화될 수 있다. Voucher 파일은 책 파일을 다운로드 하기 전에 먼저 다운로드 되고 클라이언트 DB에 저장된다.

클라이언트와 서버의 통신은 XML RPC 프로토콜을 이용하였다. 이것은 XML 에 기반한 전통적인 원격함수 호출(Remote Procedure Call :RPC)을 지원하기 위한 표준으로 HTTP 위에 구현되어 함수의 호출을 위한 매개변수와 반환값의 직렬화를 처리해주는 표준이다. XML RPC는 언어에 독립적이며 HTTP 기반이어서 방화벽에 독립적이라는 장점을 가진다. 본 연구에서는 아파치 그룹에서 제공하는 자바 XML RPC API를 사용하였다[10].

책 파일의 다운로드는 별도의 소켓을 사용하고 있다. 책 파일은 생성할 때 비밀키로 암호화되어 서버에 저장되어 있으며 다운로드 요청이 오면 책을 구성하는 파일들을 압축하여 전송한다. 전송된 책 파일은 클라이언트의 지정된 디렉토리에 압축을 푼다.

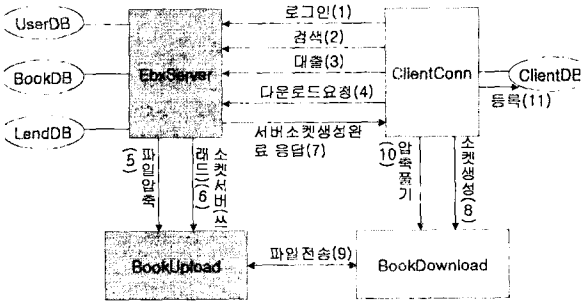

그림 2 도서관 서버와 클라이언트의 실행 과정

클라이언트 시스템은 전자책의 랜더링과 사용자 인터페이스를 가지는 리더 부분과 책의 다운로드, 책꽂이 관리, 권한 제어, 암호화된 전자책의 복호화 등의 기능을 담당하는 책관리 부분으로 나누어진다. 리더의 랜더링 부분은 본 연구팀에서 기개발한 자바 API를 사용하였다[2].

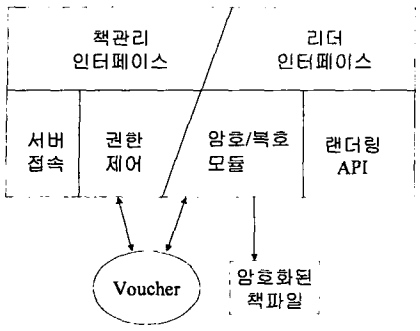

그림 3 클라이언트 시스템 구조

아래 그림은 리더와 책관리부의 암호화 및 복호화 처리 과정을 보여준다. 권리증서의 권한 검사와 책파일을 복호화하는 일을 담당하는 클래스가 EbxSecurityMgr 이다. 이 클래스는 DB에서 voucher를 꺼내 시스템의 개인키를 이용하여 암호를 풀고 voucher에 의해 명시된 권한만 허용하도록 관리한다. 책 관리 클래스에서 보유한 책의 리스트로부터 사용자가 원하는 책을 선택하게 되면 (1) EbxSecurityMgr에게 권리 증서 파일을 요청하고 (2) 권리 증서 파일을 DB에서 읽어 암호를 풀고 (3) Voucher 객체를 생성한다. 여기서 선택된 책에 대해 기간, 열기 권한 여부 등 주어진 기본 권한을 검사한다. 그리고 볼 수 있는 챕터를 구분하여 목차 페이지에서 이동 가능한 챕터들을 보여준다. (4) 사용자는 리더 시스템을 사용하여 이동, 프린트, Copy & Paste, 대출 등을 할 수 있는데, 사용자가 이러한 액션을 요청할 때 리더 시스템은 EbxSecurityMgr에게 권한이 있는지 검사한 후 허용된 것만 처리한다. (5) 사용자가 다른 페이지로 이동할 때는 목표 시점에 해당하는 파일을 읽어들여 랜더링한다. 그러므로 EbxSecurity Mgr에게 해당 챕터를 복호화해 줄 것을 요청한다.

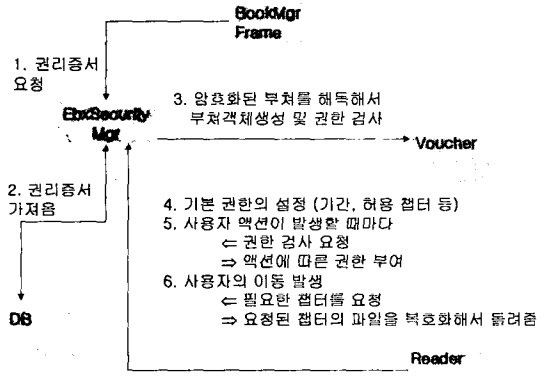

그림 4 리더 시스템의 권한 제어

본 연구에서 사용한 자바 암호 모듈은 JDK에서 제공되는 JSA와 JCE에 기반을 하고 있으며, PKI에 의한 Voucher의 암호화는 RSA에서 제공하는 제품의 SDK를 사용할 계획이다[11].

5. 결론

본 논문에서는 전자도서관 시스템을 위한 저작권 보호 교환 프로토콜의 구현을 소개하였다. 이 시스템은 도서관 서버와 리더 클라이언트 시스템으로 구성되며, 전자책 교환 프로토콜의 권리 증서 암호화 방식을 기반으로 하고 있다. 본 시스템은 자바 언어로 개발되었고 XML RPC 프로토콜을 이용하여 HTTP 상에서 사용될 수 있는 장점을 가진다.

참고문헌

[1] 김준범 외, "인터넷 EDI 문서 전송을 위한 보안 시스템," '99 봄 학술발표논문집(A) 1999, 04 v.26, n.1 pp.696-698, 1999.

[2] 이은정, 조수선, "전자책 리더를 위한 자바 API 개발," 정보처리학회 논문지 A, Vol.12, No.4, pp.91-103, December 2001.

[3] S.Cheng, P.Litva, A.Main, "Trusting DRM Software, " W3C Wokshop on DRM, January 2001

[4] R.Iannella, "Digital Rights Management Architecture," D-Lib Magazine, Vol. 7, No. 6, June 2001.

[5] E. Neylon, "Digital Rights Management in the emerging EBook environment," D-Lib Magazine, Vol. 7, No.1, January 2001.

[6] Open eBook Forum(OeBF), http://www.openebook.org .

[7] Electronic Book Exchange(EBX) Working Group. http://www.ebxwg.org .

[8] Extensible rights Markup Language(XrML) http://www.xrml.org .

[9] Microsoft eBook Reader http://www.microsoft.com/reader.

[10] Apache Software Foundation, XML RPC Implementation http://xml.apache.org/xmlrpc/ .

[11] J.Knudsen, Java Cryptography, O'Reilly Press, 1986.