안전하고 편리한 온라인 도서관 설계 및 구현

고성종, 박성욱, 이선호, 이임영
순천향대학교 소프트웨어 공학과
e-mail:[lunatics, swpark, sunho431, imylee]@sch.ac.kr

Design and Implementation of Secure and Efficient Online Library System

Seoung-Jong Ko, Sung-Wook Park, Sun-Ho Lee, Im-Yeong Lee
Dept. of Computer Software Engineering, Soonchunhyang University

요 약

인터넷이 발달함으로써 기존에 아날로그 콘텐츠들을 디지털 콘텐츠로 이용하게 되고, 오프라인의 불편한 점을 온라인으로 이용함으로써 해결하게 되었다. 디지털 콘텐츠의 발달로 인해 다양한 분야에서 디지털 콘텐츠를 이용하여 오프라인 시스템을 대체하게 되었다. 기존의 오프라인 온라인 도서관의 경우 사용자가 직접 도서관을 방문하여 이용해야 하고 도서관이 보유하고 있는 책의 종류가 적고, 부족한 장서로 인한 불편함이 있다. 이를 디지털 콘텐츠화하여 e-Book으로 이용하게 되었으며, 온라인으로 디지털화된 콘텐츠를 이용함으로써 편리하게 도서관을 이용할 수 있게 되었다. 하지만 디지털 콘텐츠의 공유가 쉽다는 특성으로 인해 무분별한 유포로 출처를 찾기 어렵고, 해당 콘텐츠의 저작권 문제, 무단 복제로부터 안전한 시스템이 필요하게 되었다. 본 논문에서는 위와 같은 문제점을 해결하고자 디지털 콘텐츠 서비스를 이용하고, 콘텐츠를 암호화하여 DRM 시스템을 이용하여 무단 배포를 방지하고 저작권을 보호할 수 있는 안전하고 편리한 온라인 도서관을 이용하도록 하는 시스템을 설계 및 구현하였다.

1. 서론

교보문고는 자사의 e-book이 2006년부터 2011년 8월까지 누적 판매량 292만 권 중 2011년 1월 1일부터 8월 1일까지 판매량이 43.4%를 차지함으로 시장이 급격하게 커지고 있음을 알 수 있다[1].

e-book 서비스가 활발히 제공되면서 최근 일상에서 PC나 휴대용 단말기를 통해 손쉽게 전자책을 접할 수 있게 되었고, 콘텐츠 복제, 배포, 전송이 쉬운 디지털자료의 특성 탓에 저작권 관련 문제점들이 발생하고, 도서관에서의 콘텐츠 제공이 관련업계의 수익성을 침해한다는 부정적인 우려가 제기되고 있다[2].

위와 같은 배경으로 본 연구는 기존의 오프라인 도서관을 시간과 공간의 제약과 부족한 장서의 문제점을 해결하기 위해 디지털 콘텐츠로 서비스를 제공한다. 전송이 쉬운 디지털 자료를 암호화하여 무분별한 유포를 방지하며, DRM을 적용하여 저작권 관련 문제를 해결할 수 있는 시스템을 설계 및 구현하였다.

2. 관련 연구

온라인 도서관은 주로 WWW(World Wide Web)를 통하여 사용자가 시간과 공간에 제약 없이 문헌 열람 등 기존 도서관 기능뿐만 아니라, 온라인의 장점을 살린 여러 기능을 활용할 수 있게 해준다.

가장 주요한 기능 중 하나로 데이터베이스에 접속하여 해당 콘텐츠 및 등록된 사용자 정보를 검색하는 방식을 사용하고 있다. 인증 과정을 통하여 무단 배포 및 비인가 사용자의 사용을 제한하고 저작권을 보호하기 위해 DRM 기술을 이용한다.

2.1 DRM(Digital Right Management)

인터넷 환경에서 디지털 콘텐츠에 대한 지적 재산권을 관리하고 제어하기 위해 주로 사용되는 기술이다. 불법 복제를 방지하기 위하여 디지털 콘텐츠의 데이터를 암호화하여 유통하고, 인증된 사용자 또는 단말기에 대해서만 라이센스를 발급함으로써 콘텐츠의 이용을 제한한다.

라이센스는 콘텐츠에 대한 사용 권한과 해독키를 포함하는데, 사용 권한에 의한 제한 조건이 만족하는 경우에만 복호화를 수행할 수 있도록 제한한다. 이러한 전체 관정을 위조 방지 기술에 의해 보호함으로써 콘텐츠 불법 유출을 차단한다[3].

2.2라이센스 관리(License Management)

배포자는 사용자 식별정보를 헤더에 삽입하여 콘텐츠를 제공하고, 라이센스에는 사용자의 장치 식별자, URL 등의 식별정보와 해독키가 사용자의 공개키로 암호화되어 있다. 라이센스는 구매 여부에 따라서 라이센스를 정규 라이센스와 동료 라이센스로 나누어 관리한다[4].

3. 요구사항

3.1 보안 요구사항

본 연구는 기밀성, 무결성, 사용자 인증에 대하여 다음과 같은 보안 요구 사항을 가진다.

- 기밀성 : 클라이언트에 전송되는 정보가 허가되지 않은 사용자에게 노출되지 않도록 기밀성이 보장되어야 한다.
- 무결성 : 클라이언트에 전송되는 정보가 권한이 없는 사용자에 의해 악의적 또는 비 악의적 접근에 의해 변경되지 않아야 한다.
- 사용자 인증 : 이용하려는 사용자나 응용프로그램의 정보를 확인하여 불법적인 사용자가 이용할 수 없도록 하여야 한다.
- 부인 방지 : 서버가 데이터를 보낸 사실에 대한 부인을 방지 할 수 있어야 하며, 클라이언트는 데이터를 받은 사실에 대한 부인을 방지할 수 있어야 한다.

3.2 콘텐츠 요구사항

본 연구는 상호 작용성, 즉시 연결성, 이용 제한성에 대하여 다음과 같은 콘텐츠 요구사항을 가진다.

- 상호 작용성 : 클라이언트와 서버 간의 원활한 통신이 이루어져야 한다.
- 즉시 연결성 : 사용자는 시간 및 공간의 제약 없이 서버와 통신 서비스를 원활히 제공받아야 한다.
- 이용 제한성 : 라이센스에 포함되어 있는 사용 권한에 의해 이용이 제한되며 인증된 사용자만 이용이 가능해야 한다.

4. 제안방식

본 연구는 사용자가 원하는 e-book 콘텐츠를 전송받아 이용하지만, 보안상 안전을 위해 사용자 인증을 통하여 정당한 사용자만 암호화된 콘텐츠를 사용한다. 콘텐츠는 DRM 기술을 적용하여, 사용 권한에 의하여 기간제로 이용함으로써 저작권을 보호할 수 있는 방안으로 설계하였다.

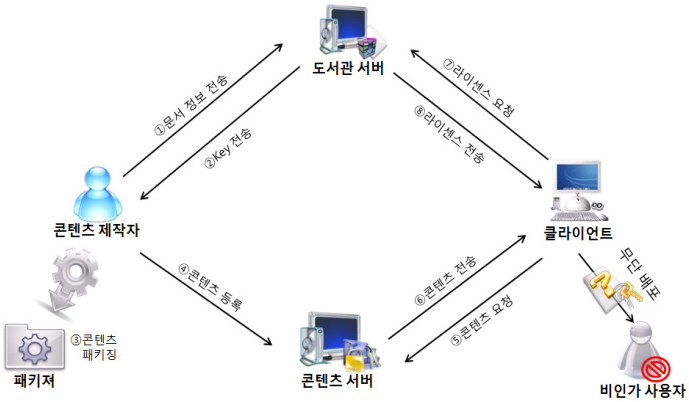
4.1 시나리오

본 연구는 사용자 인증을 통해 세션 키 분배가 완료되면 클라이언트를 통하여 원하는 콘텐츠를 선택하여 콘텐츠와 라이센스를 발급받아 콘텐츠를 이용한다.

Step 1. 콘텐츠 제작자는 도서관 서버에 도서 정보를 전송한다.

Step 2. 도서관 서버는 도서 정보를 등록하고 암호화 콘텐츠를 생성하기 위한 키를 전송한다.

Step 3. 콘텐츠 제작자는 전송받은 키로 패키져를 이용하여 콘텐츠를 생성한다.



(그림 1) 시나리오

Step 4. 콘텐츠 제작자는 생성한 콘텐츠를 콘텐츠 서버에 등록한다.

Step 5. 클라이언트는 콘텐츠 서버에 원하는 콘텐츠를 요청한다.

Step 6. 콘텐츠 서버는 클라이언트에서 요청한 콘텐츠를 클라이언트로 전송한다.

Step 7. 클라이언트는 도서관 서버에 해당 콘텐츠의 라이센스를 요청한다.

Step 8. 도서관 서버는 클라이언트가 요청한 라이센스를 전송한다.

Step 9. 클라이언트는 전송받은 라이센스를 이용하여 해당 콘텐츠를 복호화하여 이용한다.

Step 10. 무단 배포 시 비인가 클라이언트는 암호화된 콘텐츠를 이용할 수 없다.

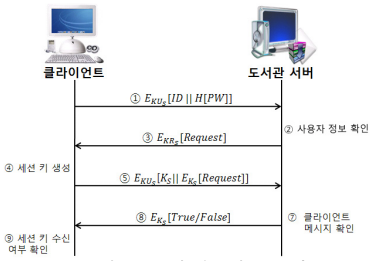
4.2 시스템 계수

- * : 참여 개체(S : 서버, C : 클라이언트, P : 제작자)
- KU* : *의 공개키
- KR* : *의 개인키
- KS* : 서버와 클라이언트 간의 세션 키
- E*[ ]: *의 키로 암호화
- D*[ ]: *의 키로 복호화
- H[] : 해쉬
- UI : 사용자 정보
- Contents : .pdf파일을 암호화한 콘텐츠
- CI: 콘텐츠 정보
- License : 콘텐츠 사용 라이센스
- Request : 요청 메시지
- True/False : 확인 여부 메시지

4.3 사용자 인증 방식

본 연구는 Client에서 회원 가입을 통하여 사용자 정보를 입력하여 사용자 정보를 등록한다. 등록하는 과정에서 사용자 정보를 안전하게 관리하기 위해 패스워드는 해쉬 과정을 거치게 된다. 로그인 요청 시 입력된 ID와 패스워드와 등록된 사용자 정보와 비교하여 사용자 인증을 한다.

4.4 세션 키 분배



(그림 2) 세션 키 분배

클라이언트 서버와 안전한 통신을 암호화 통신을 한다. 클라이언트에서 생성된 세션 키는 공개키와 대칭키 분배 방식을 이용하며 교환하며 프로토콜은 다음과 같다[5].

Step 1. 클라이언트 프로그램은 ID와 패스워드를 입력받아 도서관 서버의 공개키로 암호화하여 전송하여 사용자 인증을 요청한다.

$$C \rightarrow E_{KU_S}[ID \| H[PW]]$$

Step 2. 도서관 서버는 서버의 개인키로 암호화된 메시지를 확인하여 등록되어 있는 사용자 정보와 비교하여 사용자 인증 과정을 거친다.

$$D_{KR_S}[E_{KU_S}[ID \| H[PW]]] = ID \| H[PW]$$

$$ID \| H[PW] \equiv ID \| H[PW]'$$

Step 3. 도서관 서버는 정당한 사용자이면 클라이언트로 세션 키를 요청 메시지를 개인키로 암호화하여 전송한다.

$$S \rightarrow E_{KR_S}[Request]$$

Step 4. 클라이언트는 서버의 공개키로 암호화된 메시지를 확인하여 세션 키를 생성한다.

$$D_{KU_S}[E_{KR_S}[Request]] = Request$$

Step 5. 클라이언트는 세션 키와 세션 키로 암호화된 요청 메시지를 도서관 서버의 공개키를 이용하여 암호화해 전송한다.

$$C \rightarrow E_{KU_S}[K_S \| E_{K_S}[Request]]$$

Step 6. 도서관 서버는 전송받은 암호문을 서버의 개인키로 복호화하여 세션 키를 획득하고, 세션 키로 암호화된 메시지를 확인한다.

$$D_{KR_S}[E_{KU_S}[K_S \| E_{K_S}[Request]]]$$

$$K_S \| E_{K_S}[Request]$$

Step 7. 도서관 서버는 획득한 세션 키로 메시지를 확인한다.

$$D_{K_S}[K_S \| E_{K_S}[Request]] \equiv Request'$$

$$Request \equiv Request'$$

Step 8. 도서관 서버는 클라이언트에 *step 6*의 결과를 획득한 세션 키로 암호화하여 전송한다.

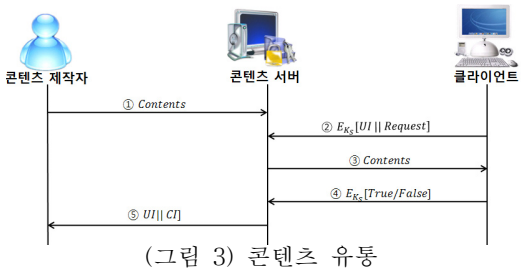
$$C \rightarrow E_{K_S}[True/False]$$

Step 9. 클라이언트는 전송받은 메시지를 세션 키로 확인하여 서버의 처리를 확인한다.

$$D_{K_S}[E_{K_S}[True/False]] \equiv True/False'$$

$$True/False \equiv True/False'$$

4.5 콘텐츠 유통



(그림 3) 콘텐츠 유통

세션 키가 안전하게 분배되면 클라이언트는 콘텐츠 서버로 콘텐츠를 요청하여 전송받을 수 있고, 콘텐츠 서버는 콘텐츠 이용 정보를 콘텐츠 제작자에게 제공한다.

Step 1. 콘텐츠 제작자는 세션 키로 암호화된 콘텐츠를 콘텐츠 서버에 등록하게 된다.

$$P \rightarrow Contents$$

Step 2. 클라이언트는 콘텐츠 서버에 등록된 콘텐츠를 요청 메시지와 사용자 정보를 세션 키로 암호화 하여 전송한다.

$$C \rightarrow E_{K_S}[UI \| Request]$$

Step 3. 콘텐츠 서버는 요청한 콘텐츠 정보를 확인 후 콘텐츠를 클라이언트로 전송한다.

$$D_{K_S}[\| E_{K_S}[UI \| Request]] = UI \| Request$$

$$S \rightarrow Contents$$

Step 4. 클라이언트는 요청된 콘텐츠를 전송받으면 콘텐츠 수신 여부를 세션 키로 암호화하여 전송한다.

$$C \rightarrow E_{K_S}[True/False]$$

Step 5. 서버는 콘텐츠 수신 여부를 확인하면 콘텐츠 이용 정보와 사용자 정보를 콘텐츠 제작자에게 제공한다.

$$D_{K_S}[E_{K_S}[True/False]] \equiv True/False'$$

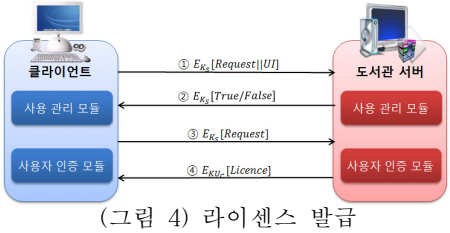
$$S \rightarrow UI \| CI$$

4.6 라이센스 발급

클라이언트는 사용 정보를 도서관 서버로 전송하여 사용자 인증 후 도서관 서버는 라이센스를 생성하여 클라이언트로 발급한다.

Step 1. 클라이언트는 특정 콘텐츠를 이용하기 위한 사용 정보를 도서관 서버로 전송한다.

$$C \rightarrow E_{K_S}[Request \| UI]$$



(그림 4) 라이센스 발급

Step 2. 서버는 사용자 정보를 확인하여 사용 여부를 전송한다.

$$D_{K_S}[E_{K_S}[Request \| UI]] \equiv Request \| UI'$$

$$S \rightarrow E_{K_S}[True/False]$$

Step 3. 클라이언트는 사용 여부를 확인받으면 라이센스를 요청한다.

$$D_{K_S}[E_{K_S}[True/False]] \equiv True/False'$$

$$C \rightarrow E_{K_S}[Request]$$

Step 4. 서버는 요청된 콘텐츠의 라이센스를 클라이언트의 공개키로 암호화하여 전송한다.

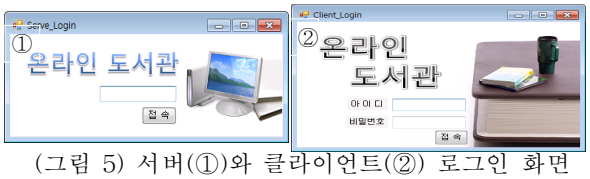
$$D_{K_S}[\| E_{K_S}[Request]] = Request$$

$$S \rightarrow E_{KU_C}[License]$$

5. 제안방식 구현

5.1 클라이언트, 서버 접속화면

본 연구는 패스워드를 입력하여 서버를 시작할 수 있으며, 클라이언트는 사용자 ID와 패스워드를 입력하여 인증 과정 통과해야 이용할 수 있다[6].

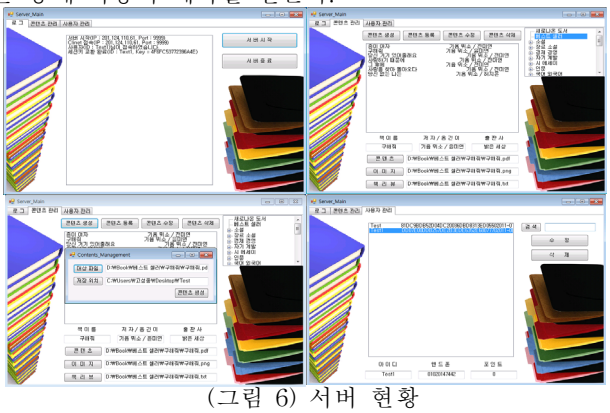


(그림 5) 서버(①)와 클라이언트(②) 로그인 화면

5.2 서버 현황

서버는 텝 컨트롤을 이용하여 로그 텝, 콘텐츠 관리 텝, 사용자 관리 텝으로 구성되어 있으며 시작과 종료 버튼을 이용하여 서버를 시작 / 종료할 수 있고 서버가 시작되면 로그 정보를 확인해서 전반적이 통신의 흐름을 알 수 있으며, 클라이언트(사용자)의 접속 및 사용 내용을 알 수 있다.

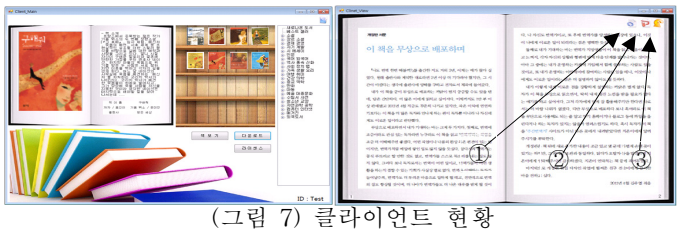
콘텐츠 관리 텝은 등록된 콘텐츠의 정보를 보여주며 콘텐츠의 생성 버튼을 선택하여 암호화된 콘텐츠와 라이센스 생성한다. 생성된 콘텐츠는 등록 버튼을 이용하여 콘텐츠 정보를 등록하게 되며 등록된 콘텐츠는 수정 및 삭제가 가능하다. 라이센스는 콘텐츠 ID, 키 정보, 사용자 정보, 사용 규칙 정보를 가지고 있으며 사용자는 라이센스를 통해 사용의 제약을 받는다.



(그림 6) 서버 현황

사용자 관리 텝은 클라이언트로 등록된 사용자의 정보를 확인하며 사용자 관리를 위해 검색 및 수정, 삭제할 수 있다.

5.3 클라이언트 현황



(그림 7) 클라이언트 현황

본 연구는 사용자 인증을 통하여 서버의 접속하게 되면 서버로부터 콘텐츠 목록을 전송받고, 목록을 선택하여 등록된 콘텐츠를 이미지를 전송받아 확인할 수 있다. 이미지를 선택하면 해당 책에 대한 정보가 나타나며, 콘텐츠와 라이센스 전송받고 콘텐츠를 이용할 수 있다.

콘텐츠를 이용할 수 있는 View 화면이 출력되면 오른쪽 위에 버튼 설명이 나온다. 오른쪽 위 라이센스 버튼(①)을 이용하여 라이센스를 선택할 수 있고, 라이센스가 확인되지 않으면 이용할 수 없다. 콘텐츠 버튼(②)을 통해 다른 콘텐츠 이용이 가능하고, 뒤로 가기 버튼(③)을 통해 콘텐츠 목록 선택 화면으로 넘어갈 수 있다.

6. 결론 및 향후 연구 방향

본 논문에서는 디지털 콘텐츠로 도서를 이용하여 안전한 키 분배 방식으로 세션 키를 교환하여 데이터를 암호화하여 통신이 이루어지며, DRM 기술을 이용하여 암호화된 콘텐츠와 생성 및 전송하여 허가되지 않은 사용자의 사용 및 무단 유포를 방지하고 라이센스를 발급받아 콘텐츠 사용 권한을 제한하여 저작권을 보호함으로써 안전한 유통 콘텐츠 방식을 구현하였다.

하지만 향후 지속적으로 온라인 도서관의 개발과 사용자를 위해 무단 복제를 방지할 수 있는 기술을 연구해야 할 것이다.

참고문헌

[1] 아이티투데이 '국내 전자책 시장, 예상보다 빠른 성장', 2011.08

[2] 독서신문 '국립중앙도서관. '디지털 시대 전자책·저작권',포럼 개최, 2011.08

[3] A. M. Eskicioglu, 'Protecting Intellectual Property in Digital Multimedia Network', IEEE Computer, Vol.36, pp.39-45, 2003

[4] 이병욱, 유종화, 'DRM 사용자간 배포를 위한 라이센스 관리 모델 설계', 인터넷정보보호논문지 제8권 제3호, 2007

[5] 최용락, 소우영, 이재광, 이임영, '컴퓨터통신보안 3rd edition', 그린출판사, 2006

[6] 최재규, 'C# Programming Bible with .Net framework 3.0', 영진닷컴, 2009