제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

멀티미디어 컨텐츠를 위한 온라인 정보 제공 서비스

김정환*, 이상향*, 김주연**,김진천*
*경성대학교 컴퓨터공학과
**경성대학교 멀티미디어 대학원 정보공학과
e-mail:jckim@star.kyungsung.ac.kr

On-line Information Services for Multimedia contents

Jung-hwan Kim*, Sang-hyang Lee*, Joo-youn kim**,Jin-chun Kim
*Dept. of Computer Engineering, Kyungsung University
**Dept. of Information Engineering, School of Multimedia, Kyungsung University

요 약

현재 인터넷의 활성화로 웹 페이지의 활용이 여러 분야로 확산되고 있다. 따라서 도서 및 출판물과 다양한 멀티미디어 컨텐츠도 많은 업체에서 웹을 통한 온라인 방식으로 제공되고 있다. 이러한 온라인 방식을 효율적으로 활용하기 위해서는 오프라인과 비교하여 최대의 약점인 가독성 문제를 해결하기 위한 효율적인 뷰어, 제공자가 컨텐츠 및 회원 정보 등을 체계적으로 관리할 수 있는 통합관리 시스템, 컨텐츠의 복제와 무단배포 방지를 위한 자료의 암호와 사용자의 개인정보를 포함한 클라이언트와 서버간에 전송되는 데이터의 보안을 위한 웹 보안, 온라인 상에서 지불이 가능한 전자 결제 시스템의 제공이 필수 불가결하다. 본 논문에서는 다양한 형태의 자료를 포함하는 멀티미디어 컨텐츠의 온라인 상에서의 효율적인 제공을 위한 통합시스템의 설계 및 구현에 관한 방법을 제시하였다.

Ⅰ. 서론

현재 인터넷의 활성화로 웹 페이지의 활용이 여러 분야로 확산되고 있다. 따라서 도서 및 출판물과 다양한 멀티미디어 컨텐츠도 많은 업체에서 웹을 통한 온라인방식으로 제공되고있다. 이러한 온라인방식을 효율적으로 활용하기 위해서는 오프라인과 비교하여 최대의 약점인 가독성 문제를 해결하기 위한 효율적인 뷰어, 제공자가 컨텐츠 및 회원 정보 등을 체계적으로 관리할 수 있는 통합관리 시스템, 컨텐츠의 복제와 무단배포 방지를 위한 자료의 암호와 사용자의 개인정보를 포함한 클라이언트와 서버간에 전송되는 데이터의 보안을 위한 웹 보안, 온라인상에서 지불이 가능한 전자 결제 시스템의 제공이 필수 불가결하다.

현재 많이 사용되고 있는 온라인 방식에는 단순히 웹 상에 업로드한 자료를 다운로드 받아 여러 가지의 상용 도구를 사용하여 자료를 보는 간단한 방식과 자체 개발한 뷰어를 제공하여 자료를 볼 수 있게 하는 두 가지 방식이 있다.

첫 번째 방식은 주로 공개된 자료의 제공을 목적으로 한 방식으로 암호화 및 웹 보안등의 사항을 전혀 고려하지 않은 단순한 형태이다. 두 번째 방식은 첫 번째 방식을 보완한 것으로 자체 뷰어를 제공하여 가독성문제를 해결하고 있다. 그리고 PDF포맷으로 작성된 자료가 전송될 때 대칭키 방식으로 암호화 된 새로운 자체 포맷 형태의 자료로 변환되어 사용자에게 제공되게 하여 자체 뷰어에서만 볼 수 있게 하고 병행하여 사용자 인증 절차를 통하여 자료의 복제와 무단배포 문제를 해결하고 있다. 현재 사용되고 있는 인증 절차는 ID와 Password를 이용하여 인증의 횟수에 제한을 두는 방식으로 사용자의 컴퓨터 시스템의 포맷, 뷰어의 재 설치 및 시스템 교체 시에는 업체에 연락을 하여 다시 인증을 받아야 하는 문제점이 있다. 사용자의 개인정보를 포함한 클라이언트와 서버간에 전송되는 데이터의 보안을 위한 웹 보안에는 대부분 SSL(Secure Socket Layer) 프로토콜이 사용되고 있다. 전자상거래에는 여러 가지 지불방법이 사용되고 있으나 전자현금시스템과 신용카드 지불 시스템이 주로 많이 사용된다. 제공자가 컨텐츠 및 회원 정보 등을 체계적으로 관리할 수 있는 통합관리 시스템은 제공자가 자체 제작하여 사용하고 있으며, 그 형태 및 기능도 여러 가지이다. 결론적으로 온라인 방식의 컨텐츠 제공 서비스를 위해서는 위의 모든 기능을 자체적으로 개발해야 하는 어려움이 있다. 따라서 컨텐츠의 효율적인 제공을 위한 통합시스템의 개발이 필요하다.

본 연구에서는 다양한 형태의 자료를 포함하는 멀티미디어 컨텐츠의 온라인 상에서의 효율적인 제공을 위한 통합시스템의 설계 및 구현에 관한 방법을 제시한다. 이 통합시스템은 컨텐츠 제공자가 컨텐츠 전달을 위한 웹페

이지 제작시 기본적인 위저드 형식의 템플릿을 제공하고, 추가적인 편집이 가능하도록 웹페이지 상에서 사용가능한 웹 에디터, 기능을 보완한 뷰어, 제공자가 컨텐츠 및 회원 정보 등을 체계적으로 관리할 수 있는 통합관리 시스템, 전자 결재를 위한 신용카드 결제 시스템의 인터페이스를 제공한다. 특히 위에서 언급한 발급횟수 제한에 기반한 인증 절차의 문제점을 해결하기 위하여 Mac Address(Media Access Control Address)를 사용하여 컴퓨터 시스템 수에 제한을 두는 새로운 방식의 인증 절차를 개발하였다. 따라서 위의 통합 시스템은 유료 혹은 무료로 제공할 수 있는 모든 전자 출판물을 포함한 멀티미디어 컨텐츠에 적용이 가능하여 인터넷을 통한 전자신문, 인터넷 방송국, 인터넷 서점 등에서 사용이 가능하며, 회원과 비회원의 서비스 차별화에도 적용이 가능하다. 또한 공공기관, 회사, 대학 등에서 보안이 필요한 정보의 공유를 인터넷에서 가능하게 한다.

II. 관련 연구

2.1 PDF

PDF(Portable Document Format)는 윈도우나 매킨토시, 유닉스, OS/2 등과 같은 어떤 타입의 컴퓨터 시스템 환경 하에서도 전송과 읽기가 가능하도록 지원되는 전자문서 포맷이다.

이 PDF 전자 문서 포맷은 자체의 압축기능을 포함하고 있어 인터넷/인트라넷 환경에서 원하는 작은 사이즈의 파일 문서를 만들고 전송하기에 가장 적합한 포맷이라 할 수 있다. 또한 PDF는 PostScript 언어 기반의 기술로 완성되었기 때문에 출력물에 높은 품질을 제공할 수 있으며, 자체의 압축 알고리즘을 통한 압축으로 최소한의 작은 파일 크기로 PDF를 만들 수 있다.[1]

2.2 암호화 알고리즘

암호화는 컨텐츠의 암호화 및 복호화, 전자 지불 시스템에서의 정보 보호 및 웹보안에 사용된다. 이러한 암호화 알고리즘에는 대칭키 암호화 알고리즘, 공개키 암호화 알고리즘이 있다.

대칭키 암호화 알고리즘은 암호화(encrypt)하거나 복호화(decrypt)하는 데에 쓰이는 키(key)가 동일한 것으로 속도가 빠르다는 장점이 있다.[2] 공개키 암호화 알고리즘은 암호화하거나 복호화하는 데에 쓰이는 키가 하나가 아닌 두개가 존재한다. 즉, 어느 하나의 키로 암호화한 것은 다른 하나의 키로만 복호화할 수 있는 것이다. 그 두개의 키는 각각 비밀키(secret key)와 공개키(public key)로 불리며, 비밀키는 이름 그대로 사용자 자신만이 알도록 해야 하고 공개키는 다른 사람들에게 알리도록 해야 한다. 그러나 비밀키 알고리즘보다 속도가 느리다.[3]

2.3 Viewer

현재 여러 컨텐츠 제공 업체들이 자체뷰어를 개발하여 제공하고 있다.

현재 제공되고 있는 뷰어들의 인증 절차는 소비자들에게 불편을 제공하고 있다. 기존의 인증은 발급횟수에 제한을 두어 사용자가 인증 받는데 불편한 점이 많았다. 소비자가 컨텐츠를 저장해놓은 컴퓨터를 포맷하게 되면 업체에게 연락을 해서 다시 인증을 받거나 컨텐츠를 다시 구입해야하는 번거로움이 있다.

본 논문에서는 인증 방법을 발급횟수에는 제한을 두지 않고 MAC address(Media Access Control address)를 이용해서 두 개의 시스템에 대해서만 인증을 허가한다. 즉, 시스템의 수에 제한을 두어 사용자가 인증을 받는데 있어 보다 나은 편의를 도모한다. 뷰어는 기능에서도 Acrobat Reader의 가지는 기능을 모두 포함하고 전자사전 기능, 페이지 타이머 기능, 사전기능, 시간 표시 기능, 라인 자동 스크롤 기능, 다중 책갈피 기능, 최상위창 고정 기능, 분류별 컨텐츠 관리 기능을 추가하여 기능적인 면을 개선하였다.

2.4 웹 보안

웹이 단순한 정보검색 뿐 아니라 신용카드 정보와 같이 타인에게 노출되어서는 안 될 중요한 정보의 전송과 같이 용도가 다양해짐에 따라 웹의 보안 문제는 필수사항이 되게 되었다

보안 서비스를 효과적으로 제공하기 위한 웹보안은 일반적으로 시스템 보안과 네트워크 보안 크게 두 부분으로 나눈다. 본 연구에서는 어플리케이션 또는 네트워트 부분에서 보안 서비스를 제공하기 위한 접근방식을 취하고 있다. 즉, 데이터를 처리하는 어플리케이션을 안전하게 만들거나 어플리케이션 데이터가 전송되는 통신 프로토콜을 안전하게 만드는 방식을 취한다.[4]

2.4.1 SSL(Secure Socket Layer)

SSL(Secure Socket Layer)은 보안공격으로부터 데이터를 안전하게 전송하기 위해 제안되었으며 응용 계층(HTTP, SMTP, FTP, etc)의 프로토콜과 TCP/IP사이에서 소켓 계층으로 존재한다. 기존 TCP/IP 응용 프로그램들이 쉽게 이식할 수 있도록 API를 기존의 소켓과 유사하게 정의하였다. TCP계층 바로 위에 위치하여 응용계층과 전송계층 사이에서 클라이언트와 서버간의 안전한 채널을 형성해 주는 역할을 수행하며, 클라이언트/서버 인증, 무결성 등과 같은 보안 서비스를 제공하게 된다.[5][6]

III. 시스템의 설계 및 구현

3.1 시스템의 설계

3.1.1 시스템 모듈 구성

본 시스템은 그림 1과 같이 SSL 보안 설정을 포함하고 있는 Web Server와 사용자 정보, 컨텐츠 정보등을 관리하기 위한 Database Server, 컨텐츠의 검색 및 주문에 사용되어지는 Web Browser, 컨텐츠 확인을 위한 Viewer, 그리고 지급정보 중계기관(Payment Gateway)으로 구성되어 진다.

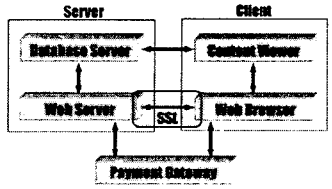

그림1. 시스템 구성요소

컨텐츠 전달 시스템은 Web Server와 Database Server를 통해 사용자에게 SSL 보안을 적용한 상태에서 컨텐츠의 주문과 같은 데이터를 교환하며, 사용자는 Web Browser를 통해 서버로부터 필요한 정보 및 컨텐츠를 획득하게 된다. 또한 사용자가 서버의 컨텐츠 전달 시스템을 통해 전달받은 컨텐츠는 Content Viewer를 통해 확인이 가능하며 이때 Viewer는 서버측의 데이터 베이스에서 필요한 인증서에 대한 정보를 검증 받은 후 인증서를 제공받게 된다. 지급정보 중계기관의 시스템은 본

연구에서는 직접 구현되지 않으나 중계기관과의 연동을 위한 인터페이스를 제공하여 관리자의 편의를 제공한다.

3.1.2 시스템 모듈 구성 및 모듈별 기능

그림 2는 시스템 구성 모듈을 나타내고 있다.

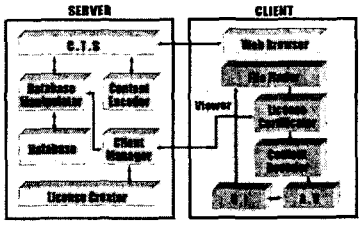

그림2 구현을 위한 모듈 구성도

(1) Content Encoder, Decoder : Encoder는 서버측에서 사용자에게 제공되어질 컨텐츠를 컨텐츠 전달 시스템을 통해 데이터베이스에 저장한 암호화키 즉, 사용자 정보 중 ID, Password를 이용하여 해당 컨텐츠를 암호화 한다. Decoder는 클라이언트의 뷰어의 기능에 포함되어 있으며 라이센스 조작기를 통해 서버로부터 전달 받은 인증서를 통해 컨텐츠를 복호화한다.

(2) Client Manager : 클라이언트 뷰어의 라이센스 조작기로부터 인증서 요청 또는 인증서 재발급 요청을 확인하여 이를 데이터베이스에서 확인하고 인증서가 할당되어질 필요가 있는 클라이언트에게는 인증서 생성기를 통해 생성된 인증서를 클라이언트 측에 전달하는 역할을 한다. 만약 인증서를 발급 받은 시스템 갯수의 초과등으로 인증서를 발급할 수 없을 때는 에러 코드를 클라이언트의 인증서 조작기에게 전달하게 된다.

(3) License Creater : 클라이언트가 컨텐츠를 복호화 하는데 사용되어질 인증서를 생성하는 모듈로 클라이언트 매니저의 요청이 있을 경우 해당 클라이언트의 인증서를 생성하게 된다.

(4) DB Manipulator : 컨텐츠 전달 시스템으로 부터의 데이터 입출력 뿐만 아니라클라이언트 매니저로 부터의 데이터 입출력을 담당한다.

(5) License Certificator : 컨텐츠를 디코딩하기 이전에 사용자의 클라이언트 측에 인증서가 있는지 확인 하고 만약 존재하지 않는다면 인증서 요청을 위한 대화상자를 제공하여 인증서를 서버의 클라이언트 매니저를 통해 제공 받는다.

(6) File Finder : 뷰어에서 사용자가 해당 컨텐츠를 오픈하기 위한 대화 상자를 제공하며 사용자로부터 입력받은 파일 정보를 License Certificator 에게 전달한다.

3.1.3 모듈의 주요기능에 대한 세부 설계

그림2의 구현을 위한 모듈 구성도를 바탕으로 주요 기능에 대한 설계사항은 다음과 같다.

(1) Document Encrytion(컨텐츠의 암호화)

서버로부터 클라이언트에게 전달되는 컨텐츠는 아이디와 패스워드를 사용하여 컨텐츠를 암호화 한 후 암호화된 컨텐츠를 클라이언트에게 전달한다.

(2) Document Decrytion(컨텐츠의 복호화)

암호화된 컨텐츠는 클라이언트에서 아이디와 패스워드를 이용하여 복호화한다.

(3) 뷰어를 통한 컨텐츠 확인

전달된 컨텐츠는 자체 제작된 뷰어에서 확인이 가능하다. 이때 서버로부터 인증절차를 거친 인증서가 필요하다. 클라이언트 측에 이미 인증서가 존재하면 인증서를 사용하여 바로 컨텐츠를 확인하고, 인증서가 클라이언트에게 존재하지 않는다면 서버의 클라이언트 매니저에게 접속하여 인증서를 요청하여야 한다. 인증서를 요청할 때 클라이언트의 뷰어에서는 사용자로부터 ID, Password를 입력 받고 여기에 MAC Address에 대한 정보를 추가하여 서버의 클라이언트 매니저에게 전달한다. 클라이언트 매니저는 데이터베이스 조작기를 통해 해당 클라이언트의 정보를 질의하여 인증서 발행 여부를 결정하게 된다. 인증서의 발행이 결정되게 되면 인증서 생성기를 통해 인증서를 생성하고 해당 인증서를 다시 클라이언트에게로 전달하게 되며 뷰어는 이 인증서를 통해 컨텐츠를 확인하게 된다. 이 과정은 그림 3과 같다.

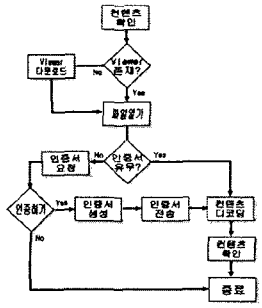

그림 3 뷰어를 통한 컨텐츠 확인 절차

(4) Mac Address를 이용한 인증

본 논문에서는 발급횟수의 제한을 기반으로한 인증절차의 문제점을 해결하기 위하여 Mac Address (Media Access Control Address)를 사용하여 컴퓨터 시스템 수에 제한을 두는 새로운 방식의 인증 절차를 개발하였다.

① 초기 인증 받기

초기인증을 받기 위해서는 서버에 ID, PASSWORD, MAC address A의 정보를 서버에 전송하여 인증을 요청한다. 정보를 전송 받은 서버에서는 뷰어의 MAC address A에 인증을 한다.

그림 4 초기 인증 받기

② 시스템이 포맷된 경우

초기인증을 받기 위해서는 서버에 ID, PASSWORD, MAC address A의 정보를 서버에 전송하여 인증을 요청한다. 그 정보를 전송받은 서버에서는 뷰어의 MAC address A에 인증을 한다.

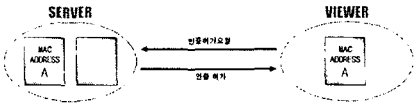

그림 5 시스템이 포맷된 경우

③ 시스템이 두 대인 경우

초기인증을 받기 위해서는 서버에 ID, PASSWORD,

MAC address A의 정보를 서버에 전송하여 인증을 요청한다. 정보를 전송 받은 서버에서는 뷰어의 MAC address A에 인증을 한다.

그림 6 시스템이 두 대인 경우

④ 시스템이 바뀌는 경우

시스템이 바뀌는 경우 시스템의 변경을 통보하고 바뀐 새 시스템의 MAC address C에 인증을 요청하게 되면, 서버에서는 서버의 기존의 MAC address 정보를 초기화 후 새로운 MAC address C에 인증을 한다.

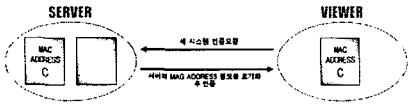

그림 7 시스템이 바뀌는 경우

⑤ MAC address가 바뀔 경우

기존의 MAC address A와 현재의 MAC address C의 정보를 서버에 전송하여 인증을 요청하면 서버는 MAC address C에 대한 인증을 한다.

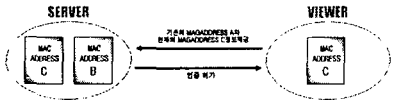

그림 8 MAC address가 바뀔 경우

3.2 시스템의 구현

3.2.1 컨텐츠 전달 시스템

컨텐츠 전달 시스템은 관라자 모드와 사용자 모드로 구분되어 진다. 사용자 모드는 사용자에게 컨텐츠를 검색 및 주문 할 수 있도록 하며 관리자는 컨텐츠 및 사용자 그리고 인증서 관리를 웹 상에서 이루어 질 수 있도록 하였다.

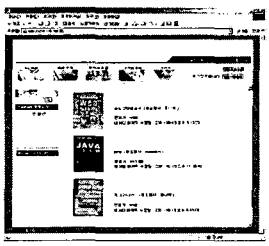

그림 9 컨텐츠 전달 시스템의 사용자 모드

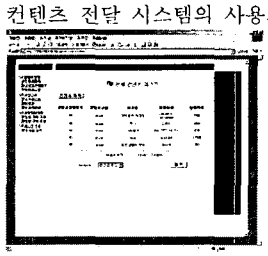

그림 10 컨텐츠 전달 시스템의 관리자 모드

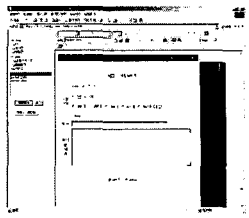

그림 11 웹 에디터

3.2.2 컨텐츠 뷰어

컨텐츠 뷰어는 다운로드 받은 컨텐츠를 확인하기 위한 도구로 컨텐츠의 관리를 위한 FileFinder와 컨텐츠를 확인하기 위한 뷰어로 구현 되었다.

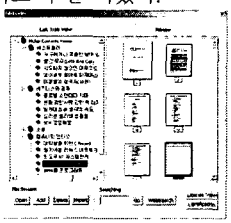

그림 12 File Finder

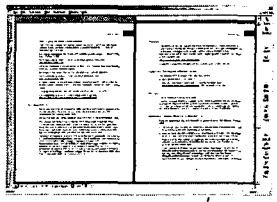

그림 13 뷰어 메인

V. 결론

본 논문에서 제시한 통합 시스템은 컨텐츠의 양적 증가를 체계적으로 관리할 수 있는 계층적 데이터베이스 관리를 가능하게 하여 컨텐츠 제공자의 컨텐츠 관리 업무를 최소 화시킬 수 있는 관리시스템과 컨텐츠 전달을 위한 웹 페이지 제작시 기본적인 위저드 형식의 템플릿을 제공하고, 추가적인 편집이 가능 하도록 웹 페이지 상에서 사용 가능한 웹 에티터, 기능을 보완하여 효율적으로 컨텐츠의 확인할 수 있는 뷰어를 제공하였으며, 특히 인증서발급 방법을 발급횟수에는 제한을 두지 않고 MAC address(Media Access Control address)를 이용해서 시스템의 수에 제한을 두어 사용자가 인증을 받는데 있어 보다 나은 편의를 도모하였다. 향후 연구 과제로는 사용자의 편의성을 보다 향상시킨 인터페이스를 제공하고, 개발 웹 에디터에서 제공하는 기능의 질적, 양적인 향상을 도모하는 것이다.

참고문헌

[1] PDF의 세계, http://www.pdf4u.co.kr/
[2] (주)퓨처시스템 암호체계 센터, "암호알고리즘 및 프로토콜의 이해", http://cnscenter.future.co.kr
[3] 이종완, "컴퓨터 시스템에서 키 분배 프로토콜에 관한 연구", 고려대 학교 석사학위 논문, 1990. 11
[4] http://mhome.shinbiro.com/~sb3216
[5] Freddric J. Hirsch, "Introducing SSL and Certificates using SSLeay" http://www.Camb.opengroup.org/RI/www/prism
[6] 이정엽, 유형소, 최승혁, 문상재 "SSL기반의 신용정보보호 전자지불 프로토콜 제안", (주) 코렉