디지털 저작권 보호를 위한 멀티미디어 데이터 관리 및 감시 시스템의 설계

조현섭, 오명관, 전호익
청운대학교 전자공학과
혜전대학 디지털서비스과
혜전대학 국방전자부사관과
e-mail: chohs@chungwoon.ac.kr, mkoh@hj.ac.kr, report@hyejeon.ac.kr

The Design of a Multimedia Data Management and Monitoring System for Digital Rights Protection

Hyun-Seob Cho, Myoung-Kwan Oh, Ho-Ik Jun
[1]Dept of Electronics Engineering Chungwoon University
[2]Dept of Digital service, Hyejeon College
[3]Dept. of Military Electronics for Non Commissioned Officer, Hyejeon College

요 약

This paper propose an interested digital rights protection scheme to address problems facing contemporary DRM approached : static digital rights management, and limited application to on-line environment. We introduce a dynamic mission control technology to realize dynamic digital rights management. And we incorporate license agent to on- and off-line monitoring and tracking. The proposed system prevent illegal access and use by using PKI security method, real time action monitoring for user, data security for itself.

1. 서론

컨텐츠 보호와 관리를 위해서는 안정성, 보안성 확보를 위한 정보보호 기술과 저작권을 관리하고 컨텐츠 츄통 전반을 감시, 추적하는 디지털 저작권 관리(DRM:Ditital Right Management) 기술이 필요하다(James et al., 1998: Jai, 1997). DRM은 저작권 보호 기술을 이용하여 허가되지 않은 사용자로부터 디지털 컨텐츠를 안전하게 보호함으로써 저작권 관련 당사자의 권리 및 이익을 지속적으로 보호 및 관리하는 관리 기술로 정의할 수 있다[1-3].

사용자 프라이버시 침해는 사용자의 동의나 인가를 받지 않은 상태에서 한 개인의 정보를 수집하고, 인증에 필요한 정보 외에 개인을 식별할 수 있는 불필요한 정보를 수집한다든지 혹은 정보 이용에 대한 충분한 동의나 사전인지 없이 이를 사용하거나, 저장된 정보를 무단으로 공개하는 것으로 인해 발생한다. 최근 스팸 메일등과 같은 여러 피해사례가 높아짐에 따라 사용자 프라이버시에 침해에 대한 인식이 증가하고 있다[4-5]. 이에 따라 DRM에서도 기존의 저작권 보호뿐만 아니라 사용자의 프라이버시 보호가 DRM 분야의 새로운 연구 과제가 되고 있다.

본 논문에서는 온라인과 오프라인 상에서 멀티미디어 컨텐츠에 대한 사용자 인증과 원 데이터 자체의 암호화를 통해 불법적인 실행, 복사, 이동을 방지할 수 있는 통합적인 DRM 시스템을 설계하고자 한다.

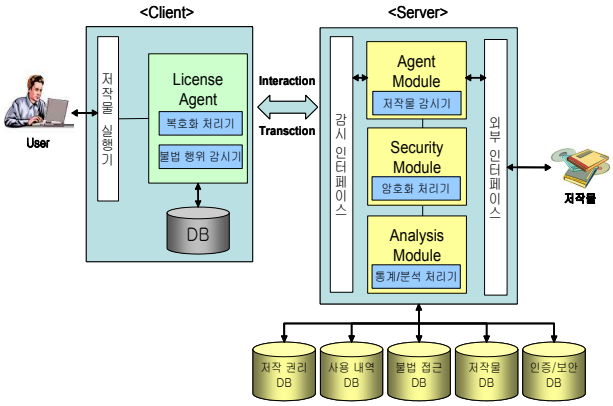
Ⅱ. LA를 이용한 DRM 시스템 설계

2.2 시스템 구조

디지털 컨텐츠의 유통을 위해서는 상용화된 전자상거래 시스템들과 상호 연결을 통해서 저작물 유통과 결재가 가능하도록 표준화된 분류 체계와 저작권 보호와 관리를 위해서는 저작물에 대하여 온라인 환경과 오프라인 환경에서 저작권 이용에 대한 위법 여부를 판단할 수 있도록 저작권 사용 내역을 자동으로 감시하고 추적할 수 있는 기능과 저작권 사용에 대한 자동 통계 기능 및 분석 기능이 제공되어야 한다. 특히, 법적인 문제 발생시 저작권 위법 사례에 대하여 이를 입증할 수 있는 객관적인 자료의 유지 및 제공 기능이 저작권 보호 및 관리 시스템의 설계 요소로서 고려되어야 한다.

또한, 원 저작물의 데이터 보호와 인증을 위해 기

존의 저작물에 대한 단순한 사용권한 제한이나 패스워드 인증 방식이 아닌 PKI 기법을 이용한 사용자 인증과 데이터 암호화를 이용하여 원 저작물에 삽입하여 데이터를 보호해야 한다. 제안하는 시스템은 클라이언트/서버로 구성되어 운용되며 <그림 2-1>는 전체 구조도를 나타낸다.



[그림 2-1] 제안 시스템 구성도

인증된 사용자라 할지라도 사용권한에 따라 제한적인 사용을 위해 저작물 자체 암호화에 의해 저작물을 보호하게 된다.

Ⅲ. 인증 및 암호화 기법

3.1 동영상 파일의 암호화 및 복호화

동영상 데이터 자체의 암호화를 위해 LA는 다음과 같은 요구사항을 필요로 한다.

첫째, Agent는 클라이언트 시스템 내부에 존재한다. 클라이언트 내부에 존재하게 되며 Agent를 사용자 임의적으로 종료하게 되면 다운로드한 동영상의 정상적인 재생을 할 수 없다.

둘째, Agent는 클라이언트 사용자가 서버에 처음으로 접속하였을 때 서버로부터 다운 로드 하여 실행하며 클라이언트 시스템의 부팅과 동시에 실행되거나 사용자에 의해 실행되어 사용한다.

셋째, Agent는 동영상의 실행 시 실행동영상의 사용자정의 데이터를 체크하여 암호화되어 있는 동영상과 일반 동영상을 구분하여 암호화되어 있는 동영상일 경우 서버에 사용요청을 수행한다. 사용요청을 받은 서버가 사용자 인증을 하게 되면 복호화에 필요한 대칭키를 사용자의 공개키로 암호화 하여 클라이언트로 전송하게 되고 에이전트에 의해 암호화 되어 있는 동영상의 I 프레임을 복호화 하여 재생할 수 있도록 한다.

넷째, Agent는 사용자의 정보와 실행하고자 하는 동영상의 정보를 서버로 보내게 되고 서버는 사용자와 동영상정보를 통하여 실행 횟수 제한을 수행 할 수 있다.

3.2 라이센스 인증 기법

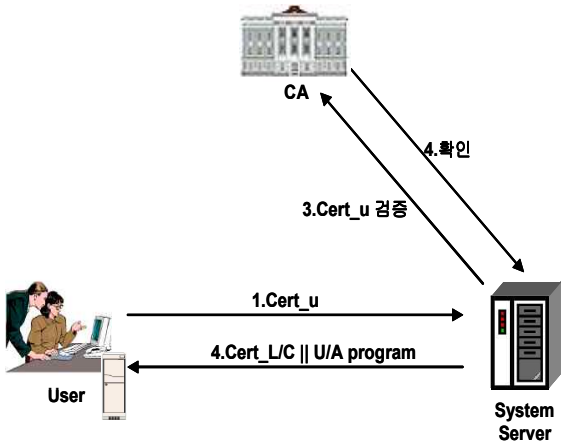
저작물 저작자는 창작한 저작물을 컨텐츠 출판업자에게 전송한다. 그러면 컨텐츠 출판업자는 해당 저작물을 임의의 대칭키 Ks로 암호화하여 암호화된 저작물 C를 컨텐츠 제공자에게 전송하여 컨텐츠 제공자의 서버에 저장한다.

$$C = EKs[data]$$

사용자는 원하는 저작물을 컨텐츠 제공자의 서버에서 다운로드 받아서 사용할 수 있다. 그러나 다운로드 된 컨텐츠는 암호화 되어 있으므로 사용자가 임의로 실행할 수 없다. 그러므로 다음의 단계를 거쳐서 사용할 수 있다.

1) Step 1 : 사용자 등록 프로토콜

사용자는 컨텐츠를 사용하기 위하여 우선 사용자 등록을 한다. 사용자 등록 과정은 <그림 3-2>과 같다.

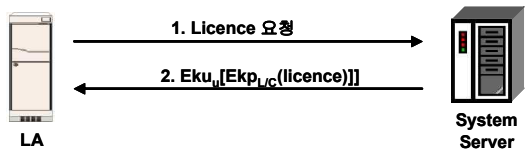


[그림 3-2] 사용자 등록 프로토콜

사용자는 라이센스 서버 기능을 갖는 시스템 서버에 접속하여 자신의 인증서 cert_u를 전송한다. 시스템 서버는 사용자의 인증서 cert u를 인증경로를 통하여 검증하고 올바른 인증서이면 사용자 에이전트 프로그램과 클리어링 하우스의 인증서를 전송한다.

2) Step 2 : 라이센스 발급 프로토콜

사용자는 라이센스 에이전트(LA) 프로그램을 설치하고 라이센스 에이전트를 실행한다. 사용자의 PC에 탑재된 라이센스 에이전트는 사용자가 암호화된 저작물을 실행하면 <그림 3-3>과 같이 시스템 서버에 접속하여 라이센스를 발급받는다.



[그림 3-3] 라이센스 발급 프로토콜

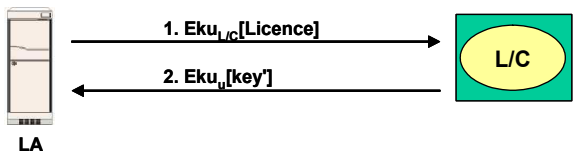
라이센스 에이전트는 시스템 서버에 접속하여 원하는 저작물에 대한 라이센스를 요청한다. 시스템 서버는 라이센스 ID, 사용자 ID, 저작물 ID, 권한 등이 담긴 라이센스를 발급한다. 이때, 보안을 위하여 다음과 같이 사용자의 공개키로 암호화하고 자신의 개인키로 서명하여 전송한다.

Ekuu[EkpL/C(licence)]]

여기서 ku는 공개키를 나타내고 kp는 개인키를 나타낸다. 그러므로 kuu는 사용자(user)의 공개키이고 kpL/C는 L/C의 개인키이다.

3) Step 3 : 라이센스 인증 프로토콜

라이센스 에이전트는 사용자가 암호화된 저작물을 실행하면 라이센스가 있는지 확인한다. 만약 라이센스가 없다면 위의 step 2에 따라서 라이센스를 발급받고 라이센스가 있다면 다음 그림과 같이 해당 라이센스에 대한 인증을 시스템 서버에 탑재된 라이센스 클리어링 하우스(L/H)에 요청한다.



[그림 3-3] 라이센스 구조

라이센스 클리어링 하우스는 라이센스 에이전트로부터 라이센스에 대한 인증 요청을 받으면 라이센스 저장 목록에서 권한을 확인한 후 인증을 하게 된다. 사용자의 라이센스가 특정일까지의 시간 라이센스이면 해당 시간이 경과 되었는지 확인하고 사용횟수에 대한 라이센스라면 횟수를 하나 줄인 후 해당 키값을 다음과 같이 사용자의 ID와 연산하여 이를 사용자의 공개키로 암호화하여 전송한다.

Ekuu[key'] (where *key'=Ks⊕userID*)

암호화된 키를 받은 사용자 에이전트는 해당 암호화된 키를 사용자의 개인키로 복호화하여 key'을 추출하고 이를 사용자의 라이센스에 있는 user ID와 연산하여 키를 얻어서 암호화된 저작물을 복호화하여 사용자에게 보여준다.

V. 결론 및 향후 연구방향

본 논문에서는 디지털 저작권 보호를 위한 멀티미디어 데이터 관리 및 감시 시스템에 대해 제안하고 설계하였다. 라이센스 에이전트는 PKI 기법을 이용하여 사용자 인증을 하며, 컨데이터 기법을 이용하여 시스템 서버에서 데이터 자체의 암호화를 한 후 클라이언트에서 버퍼 스케쥴링에 의해 복호화를 하는 멀티미디어 데이터에 대한 저작권을 보호하는 기능을 수행한다. 앞으로 시스템 설계에 있어서 멀티미디어 데이터를 사용자가 실행할 때 버퍼 관리 스케쥴링에 대한 구체적인 설계가 요구되며, 현재 설계를 기반으로 한 시스템 구현이 진행중에 있다.

참고문헌

[1] J.Dubl,"Digital Rights Management: A Defination", IDC 2001.

[2] J.Dubl, S.Kevorkian, "Understanding DRM system: An IDC White paper", IDC, 2005.

[3] Kentaro Endo, “The Building up of national Regional and International Registers for works and objects of related rights," Proc. pf International Conference on WIPO, Seoul, Korea October 25-27, 2008.

[4] V.K Gupta, "Technological measures of protection, "Proc. of International Conference on WIPO, Seoul, Korea October 28-29, 2010.

[5] P.Vora, D, Reynolds, L.Dickinson,J.Erickson, D.Banks, "Privacy and Digital Rights Managements", A Position paper for the W3C Workshop on Digital Rights Management, January 2010.