PKI 인증서기반 방송 프로그램 유통시스템

박기철* · 이주영** · 남제호** · 정회경*

Broadcast Program Distribution System of PKI Certificate-based

Ki-Chul Park* · Joo-Young Lee** · Je-Ho Nam** · Hoe-Kyung Jung*

본 연구는 지식경제부 및 정보통신연구진흥원의 IT신성장동력핵심기술 개발사업의 일환으로 수행하였음.
[2007-S-003-03, 지상파 DTV 방송프로그램 보호 기술개발]

요 약

디지털 방송을 두고 IPTV와 디지털 CATV의 경쟁이 계속되는 가운데 방법과는 상관없이 방송된 콘텐츠 프로그램의 불법복제와 인터넷을 통한 배포의 피해 또한 커지고 있다. 디지털 CATV는 콘텐츠의 품질이 뛰어나 판매되는 DVD등의 고밀도 저장매체의 콘텐츠와 품질에서 차이가 없기 때문에 불법배포 시 문제가 크다. 하지만 사용자의 입장에서 방송프로그램의 녹화 및 재이용은 보장된 권한이고, 교육자료 등의 공정의 목적에서 녹화와 배포는 불법의 그것과는 구분이 필요하다.

본 논문에서는 디지털 인증서를 이용해 녹화된 사용자 및 공정목적의 이용을 보장하고 불법배포를 제약하는 방송프로그램 유통시스템을 설계 및 구현하였다.

ABSTRACT

Digital broadcasting and digital CATV and IPTV will continue in the competition, regardless of how the content of the program was broadcast over the Internet distribution and the damage of piracy is also growing. Excellent quality of the content of the digital CATV sales of DVD and high-density storage media because there is no difference in content and quality is the problem of illegal distribution. However, users can record and reuse program in the position of the guaranteed rights, and the purpose of training in fair and illegal recording and distribution needs to be separate from it.

In this paper using a digital certificate recorded by the user and the process to ensure the purpose of illegal distribution of pharmaceutical distribution system design and implementation of the program was broadcast.

키워드

DCATV, DRM, PKI Certification, OpenSSL, SSL

* 배재대학교 컴퓨터공학과 (교신저자 : 정회경)
** 한국전자통신연구원

접수일자 2009. 03. 18
심사완료일자 2009. 04. 21

Ⅰ. 서 론

지상파방송의 디지털 전환과 방송통신의 융합으로 IPTV와 DMB가 등장하는 등 미디어 시장이 변화하면서 CATV 또한 디지털 전환이 적극 추진되고 있으며, 전국의 1,700 만 가구 가운데 1,400 만 가구가 케이블 방송을 통해 지상파 방송을 수신하고 있고 아날로그에서 디지털 방송으로 전환의 완료를 위해 디지털 CATV가 큰 부분을 차지하고 있다[1]. 그러나 디지털 방송은 그 디지털의 특성상 복제와 배포가 쉽고 복제로 방송되는 프로그램의 품질도 매우 뛰어나다. 이는 방송의 형태가 아닌 다른 저장매체를 통한 방송프로그램 콘텐츠의 녹화 배포가 유통시장에 치명적인 문제가 될 수 있다. 하지만 개인이 방송프로그램의 녹화 및 재이용은 개인이 가진 고유의 권한이므로 개인의 재이용 권한을 보장하되 불법적인 배포를 제안할 신뢰성 있는 콘텐츠의 유통모델이 필요하고 이러한 유통모델을 표현 할 시스템이 요구되어진다.

이에 본 논문에서는 공개키 기반의 인증서를 이용하여 적법한 콘텐츠의 이용자가 이용권한을 SSL(Secure Socket Layer) 통신을 통해 서버로 부터 얻어오는 유통모델과 이 모델을 구현한 시스템에 대해서 설명한다.

Ⅱ. 관련연구

2.1 PKI(Public Key Infrastructure) 인증서

PKI는 인증서 기반 공개키 암호시스템의 구현 및 운영을 지원하기 위한 환경을 의미하며, 온라인상에서 안전한 통신이 가능하게 하는 암호화 서비스와 공개키의 인증서를 발행하고 그에 대한 접근을 제어하는 인증서 관리 서비스를 의미한다[2]. 온라인상에서 상대방을 인증하고 무결성과 부인방지를 보장해준다. 다음 표 1은 PKI 인증서 시스템의 구성 객체에 대한 설명이다.

2.2 OpenSSL

OpenSSL은 SSL통신용 라이브러리로서 SSL은 인터넷상의 보안통신 표준이며, 통신내용은 전송 전에 암호화되고, 목적지에 도착해서 복호화 된다. OpenSSL은 이를 위한 인증기능과 암호화 알고리즘으로 구성되어 있다[3].

표 1. PKI 인증서 시스템의 객체
Table 1. PKI certificate system's object

인증기관(CA: Certification Authority)	- 인증정책을 수립 - 인증서 및 인증서 취소 목록 관리 (생성,공개,취소 등) - 다른 CA와 상호 인증
등록기관(RA: Registration Authority)	- 사용자 신분 확인 - PKI를 이용하는 응용과 CA간 인터페이스
디렉토리 (Directory)	- PKI 관련 정보 공개
PKI이용하는 응용 시스템	- 인증서 생성, 취소 등을 요구/인증경로 검증 - 인증서 활용(전자서명) - 디렉토리로부터 인증서 및 인증서 취소
인증 정책	- 특정한 형태의 인증서를 발행하기 위한 절차들을 기술

2.3 ATSC A/57 Standard

DCATV는 기존의 아날로그 CATV를 디지털로 업그레이드한 CATV이다. 국내에서 사용되는 DCATV 표준은 미국에서 표준으로 채택한 오픈 케이블 방식이다[4]. ATSC(Advanced Television Systems Committee) A/57 표준은 가상채널로 전송되는 방송프로그램의 식별과 콘텐츠 ID를 전달하는 방법에 대한 표준이다[5,6]. 본 논문에서는 새로 변경된 ATSC A/57b 표준의 식별자 정보를 기준으로 방송사와 방송사의 콘텐츠에 대한 이름과 정보를 식별한다[7].

Ⅲ. 방송 프로그램 유통 시스템 설계

본 시스템은 녹화된 DCATV의 방송프로그램 콘텐츠를 녹화자 또는 녹화자를 제외한 사용자가 이용하는 경우 재생 권한의 제공과 불법적인 이용으로부터 콘텐츠를 보호하는데 그 목적을 두고 있다. 녹화자의 사적이용범위는 본인으로 한정하고, 녹화자를 제외한 이용자는 녹화된 방송프로그램 콘텐츠만 소유한 것으로 한정한다. 콘텐츠의 배포는 인터넷 또는 휴대용 저장장치 등을 통해 사용자 스스로 획득하도록 하는 것으로 한정하였다.

3.1 녹화된 방송프로그램 콘텐츠의 구성

방송프로그램은 영상데이터의 일부가 암호화 되어 저장되는데, 이는 셋톱박스 또는 별도의 녹화 장치가 수

행할 내용이다. 녹화장치는 암호화된 방송프로그램 콘텐츠와 프로그램 식별정보를 담은 PID 파일, 녹화자의 이용을 위한 Domain 파일, 송출 방송사의 공개키로 암호화한 Package 파일로 구성된다. 구성요소에 대한 정보는 표 2와 같다. 구현과 테스트 및 검증을 위해 각각의 구성요소는 하나의 디렉토리에 정해진 파일로 보관을 하고, 디렉토리를 하나의 콘텐츠로 인식하도록 하였다.

표 2. 녹화된 콘텐츠 구성 파일
Table 2. Files of recorded program

파일이름	내용 및 포함 정보 설명
Domain	- 녹화자가 생성 - 콘텐츠 암호화 키를 사용자의 공개키로 암호화
PID	- 방송프로그램 콘텐츠 정보
Package	- 녹화자가 생성 - 콘텐츠 암호화 키를 방송국 공개키로 암호화
License	- 유통서버가 생성 재생권한 파일 - 콘텐츠의 암호화 키로서 제3자의 공개키로 암호화되어 제공 - 녹화 시에는 생성 안됨
Mpeg2ts.tp	- 영상만 암호화된 미디어 파일

3.2 녹화된 콘텐츠의 유통 시나리오

본 시스템에서 녹화된 방송프로그램의 소비는 크게 세 가지로 구분 하도록 하였다. 프로그램 녹화자 본인이 이용하는 경우, 이용권한이 없고 콘텐츠만 소유한 이용자가 이용하는 경우 그리고 공정한 목적으로 이용하는 경우로 구분하도록 하였다. 그림 1은 녹화된 프로그램의 3가지 유통유형 시나리오를 표현한 그림이다.

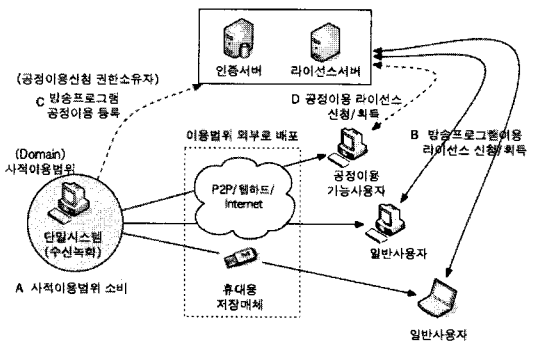

그림 1. 녹화된 콘텐츠의 유통 시나리오
Fig. 1 Distribution scenario of recorded content

• 녹화자 본인의 소비

방송프로그램의 녹화 시 Domain 파일에 콘텐츠를 암호화한 대칭키를 녹화자 인증서의 공개키로 암호화되어 Domain 파일에 저장한다. 사적이용범위 안에서 녹화된 콘텐츠의 재생을 요청하면 단말시스템은 Domain 파일에서 콘텐츠를 복호화 할 수 있는 대칭키를 추출한다. 추출에 실패하면 재생이 시도된 콘텐츠는 사적이용범위 밖의 이용으로 인식하거나 콘텐츠만 소유한 이용자의 재생요청으로 간주한다. 콘텐츠를 복호화 할 키를 얻었다면, 콘텐츠의 복호화 및 재생을 수행한다.

• 콘텐츠만 소유한 이용자의 소비

콘텐츠만 소유한 이용자는 Domain 파일에서 키를 얻을 수 없기 때문에, 재생을 위해서 유통서브시스템과의 보안통신 과정을 거쳐 재생권한을 발급 받아야 한다. 이용자는 PID 파일에 포함된 콘텐츠의 정보를 유통서버로 전송하고, 유통서버는 이용자의 단말시스템으로 재생권한을 획득 과정에 필요한 정보를 입력 할 수 있는 URL을 전송하고, 단말시스템은 서버가 전송한 URL의 웹페이지에서 이용기간 등의 정보를 입력한다. 입력완료 후 유통서버는 트랜젝션 코드를 생성 및 저장하고 이용자의 웹페이지에 출력한다. 이후 단말시스템은 트랜젝션 코드와 Package 파일의 정보와 자신의 정보를 유통서버로 전송하면 유통서버는 전송받은 내용이 정상 유무를 확인 후 첨부한 Package 파일의 정보를 소유한 방송국의

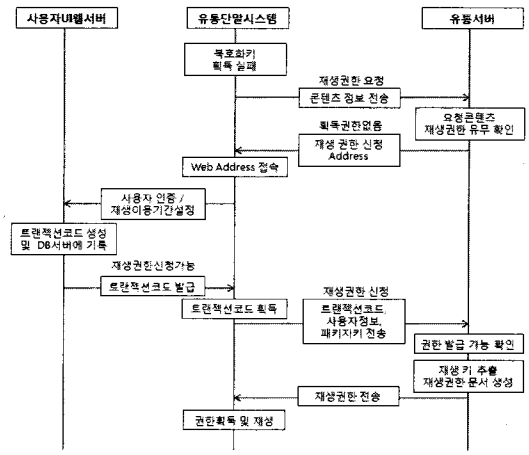

그림 2. 제3자의 재생권한 획득 과정
Fig. 2 The process of obtaining other's permission

개인키로 복호화하고 콘텐츠의 암호화키를 얻어낸 후 요청자의 공개키로 암호화하고 재생권한 문서를 생성 후 전송한다. 그림 2는 제3자의 재생권한 획득과정을 간략하게 나타낸 다이어그램이다. 발급받은 권한 문서는 이용자의 개인키를 사용하여 콘텐츠를 복호화하기 위한 대칭키를 획득할 수 있다. 다음으로 재생을 원하는 콘텐츠의 복호화 및 재생을 진행한다. 그림 3은 이용자 단말의 콘텐츠 획득에서 소비까지의 과정을 활동다이어그램으로 나타낸 것이다.

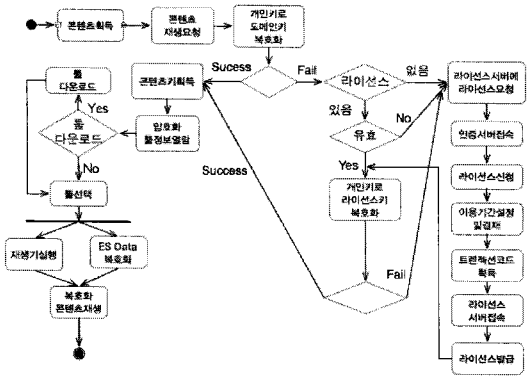

그림 3. 콘텐츠 소비 과정 다이어그램
Fig. 3 Diagram of content consumption process

• 공정이용을 위한 허가 요청과 소비

교육 목적의 참고자료와 같은 공정 목적으로 녹화된 방송프로그램을 이용하는 경우 공정이용 허가 요청과 이를 재생하는 소비 과정을 거친다. 공정이용 허가 요청은 공정이용 권한을 가진 교사가 자신의 수업 참고자료 목적으로 일정기간동안 임의의 그룹에 재생권한을 부여하도록 요청하는 것을 의미한다. 그림 4는 공정이용 허가 과정을 간략히 나타낸 것이다.

공정이용 요청을 하면 유통서버는 공정이용 용청자의 요청권한을 확인 후 요청한 콘텐츠에 대한 요청 과정을 완료할 수 있는 URL을 전송하고 요청자의 단말시스템은 수신한 URL로 이동한다. 요청자는 공정이용 기간과 공정이용 재생권한 발급 범위 등을 설정하는데 유통시스템은 이때 트랜젝션 코드를 생성해 요청자의 단말시스템에 출력한다. 공정이용 허가 요청자의 공정이용 재생권한 발급범위에 해당되는 사용자는 공정이용 콘텐츠를 소유한 상태에서 재생을 요청하면 단말시스템은 유통시스템으로 공정이용 재생권한을 요청하고 이때 유통서버로 전송하는 정보는 트랜젝션 코드, Package 파일의 내용, 자신의 정보를 포함하여 전송한다.

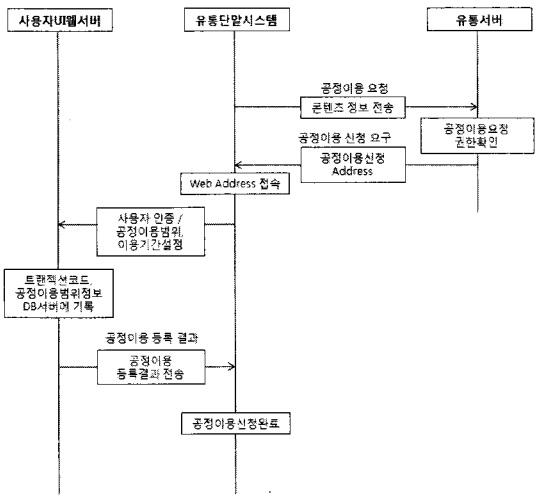

그림 4. 공정이용 허가 과정
Fig. 4 Authorization process of public usage

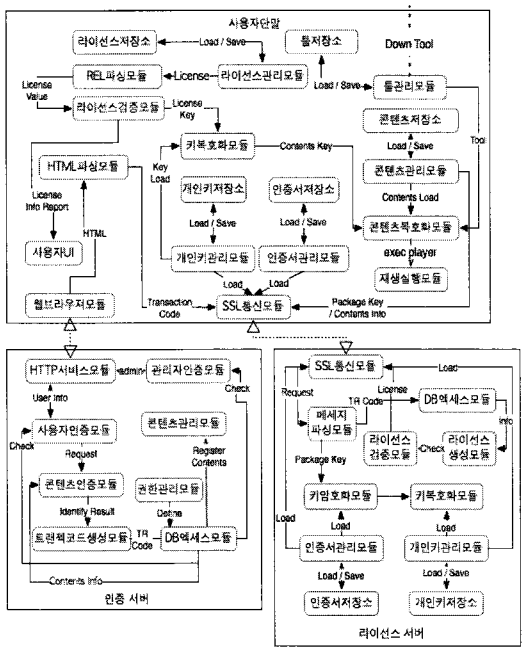

그림 5. 유통 시스템의 전체 구성도
Fig. 5 Architecture of distribution system

유통시스템은 공정이용 재생권한 요청자가 공정이용 범위에 해당되는지의 여부를 검사한 후 요청자의 Package 정보를 해당 방송국의 개인키로 복호화 한 후 다시 요청자의 공개키로 암호화하여 재생권한 문서를 생성하여 권한요청자의 단말시스템으로 전송한다. 이를 수신한 단말시스템은 자신의 개인키로 콘텐츠 복호화 키를 추출하고 콘텐츠 복호화과정과 재생과정을 수행한다. 그림 5는 유통시스템의 전체 구조이다.

Ⅳ. 시스템 구현

본 시스템은 IBM-PC 호환 컴퓨터에서 MS Windows XP 플랫폼에서 구현되었고, OpenSSL API는 x86 단일 CPU 환경에서 빌드 하였다. 콘텐츠는 AES-CBC 알고리즘으로 암호화 하였고 키의 길이는 128bit로 한정하였다. 재생권한 획득을 위한 이용자의 웹 UI를 위해 Ruby On Rails 2.2.2가 사용 되었으며, 추가적인 Ruby의 패키지로 uuid 2.0.1와 Mongrel 1.1.5가 사용 되었다. 재생권한 문서의 생성과 파싱을 위해 Libxml 2.7.3이 사용되었고, 단말시스템과 유통서버는 MS Visual Studio C++ 6.0으로 구현되었다.

4.1 인증서의 생성

구현에서 사용된 인증서는 OpenSSL을 통해 자기 서명된 인증서를 사용하였으며, 각각의 방송국에 따른 샘플 인증서와 유통유형을 가정한 이용자별로 인증서를 생성하였다. 그 외에 키교환을 위한 Diffie-Hellman과 Random Seed 파일을 생성하여 구현에 사용되었다[8].

4.2 방송프로그램 콘텐츠의 암호화

본 연구에서는 ATSC A/57b의 표준을 기준으로 구현했으며, ATSC A/57b 표준은 구현 당시 DCATV에 반영되지 않았으므로, 프로그램식별 정보와 프로그램 영상의 암호화는 별도로 생성하였다. 콘텐츠의 암호화에는 한국전자통신연구원에서 제공한 암호화 툴을 사용하여 콘텐츠를 암호화 및 복호화 과정을 수행하였다.

4.3 유통시스템의 구현

유통시스템의 구현에 SSL통신을 구현하기 위해 일반적인 통신 소켓에 OpenSSL에서 제공하는 SSL API를 추가해 구현하였으며, 단말시스템과 유통서버 간의 통신에 사용되었다[9]. 재생권한 문서는 MPEG21-REL 표준을 따르는 형식의 문서로 생성하였으며, 재생권한 문서에는 이용자의 공개키로 암호화된 대칭키를 Base64로 인코딩되어 첨부하였다. 단말시스템에서 동영상 재생을 위한 재생기는 OS에서 지원하는 미디어 재생기와 MPEG2-TS 재생을 지원하는 코덱을 설치하여 구현하였다.

4.4 유통시나리오의 구현

유통시나리오의 구현을 위해 서로 다른 두대의 PC가 사용되었다. 하나는 유통서버시스템이 설치되었으며, 나머지 PC는 사용자단말시스템이 설치되었는데, 유통서버시스템에는 방송국의 인증서와 개인키를 관리 하도록 하였고, 단말시스템에는 여러 조건의 사용자로 가정하여 각각의 사용자의 인증서를 이용하여 서로 다른 사용자로 인식하도록 설정하였다. 그림 6은 유통단말이 이용권한을 요청하는 과정을 캡쳐한 화면이다.

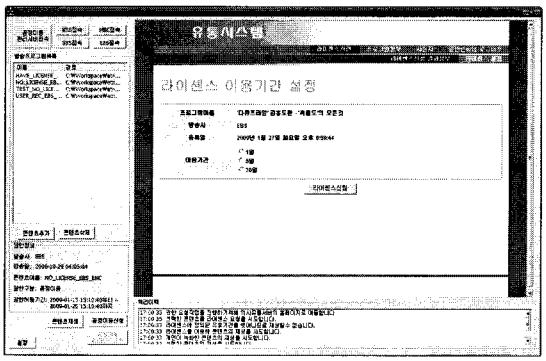

그림 6. 유통단말시스템 동작 화면
Fig. 6 Action screen of distribution terminal

콘텐츠 영상의 일부만 암호화 했으므로 이용권한이 없는 경우에도 콘텐츠의 소리와 출력되는 일부 영상을 통해 이용자가 원하는 콘텐츠인지 식별이 가능하다. 그림 7과 8은 암/복호화된 영상의 동일한 재생 시간대 스냅샷이다.

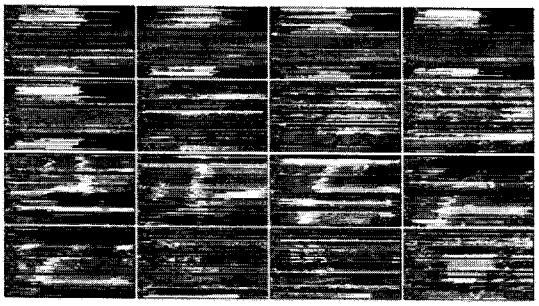

그림 7. 암호화된 콘텐츠의 스냅샷
Fig. 7 Snap-shot of encrypted content

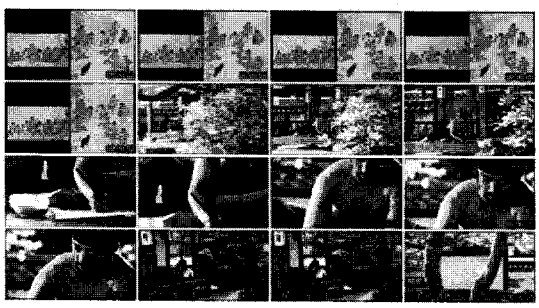

그림 8. 복호화된 콘텐츠의 스냅 샷
Fig. 8 Snap-shot of decrypted content

V. 고찰 및 결론

본 시스템에서는 콘텐츠를 대칭키 암호화 알고리즘으로 암호화하고 암호화에 사용된 키를 다시 공개키로 암호화 하는 방식을 취하였다. 암호화에 사용된 대칭키 알고리즘을 사용하는 이유는 간단한 연산을 통해 빠른 암호화와 복호화가 가능하기 때문이다. DCATV의 영상은 1920 x 1080의 해상도로 영상을 표현하기 때문에 영상파일로 직렬화 할 경우 1시간 분량의 방송프로그램은 10기가바이트 정도가 소요된다. 이러한 영상의 효율적인 암호화를 위해서는 암복호화의 성능을 위해 최소한의 암호화를 통해 정상적인 이용은 제한하도록 하고 이용 시 성능상의 문제를 최소화 하는 방법이 바람직하다. 하지만 대칭키 자체의 키 유출 문제와 최소한의 암호화로 인한 콘텐츠 보호의 취약점이 문제가 될 소지가 있다. 하지만 콘텐츠를 암호화한 키를 공개키로 다시 암호화하여 관리하면 콘텐츠 보호의 취약점을 일부 극복 가능하고 암/복호화에 사용되는 암호화 툴을 다양한 방법으로 구현 한다면 콘텐츠 보호의 효율성은 더욱 증대될 것으로 사료된다. 본 논문에서 제안한 유통시스템은 과거 보편적인 DRM(Digital Rights Management) 유통 방법과 다르게 콘텐츠의 배포는 일반 사용자의 자의에 맡기고 재생을 제한하는 방법을 제안하였다. 더욱 선명해지고 대용량화 되가는 영상 콘텐츠를 현재와 같은 방법으로 VoD 스트리밍 서버만이 제공하는 경우 제공자의 서버는 엄청난 트래픽과 유지를 위한 과도한 설비의 비용 부담에 직면하게 된다. 그리고 단일의 대칭키 알고리즘과 일정한 형식으로 암호화된 영상 콘텐츠는 암호화 키 노출에 취약한 문제점이 있다. 더욱이 이러한 DRM 방법은 하나의 단말, 플랫폼, 밴더, 제공자에 종속적이기 때문에 이용자의 구매 콘텐츠 간의 호환성 결여로 인한 이용자의 피해 확산과 콘텐츠 구매 기피로 인한 콘텐츠 시장이 위축되는 문제가 있다.

본 논문에서 제안한 모델을 이용하면, 콘텐츠 제공자는 자체적으로 VoD 서버나 별도의 스트리밍 서비스를 위한 설비의 부담을 줄일 수 있고 콘텐츠에 대한 재생권한만 관리하는 간단한 구조로 서비스를 단순화 할 수 있으며, 콘텐츠의 안전한 배포가 가능하고, 다양한 암호화 툴을 이용해 플랫폼과 콘텐츠 소비기 간의 호환성을 높일 수 있다. 추가적으로 공정한 목적의 콘텐츠 이용을 통해 공정한 목적에 부합할 경우 사용자 및 단체의 공익을 보장 받을 수 있다. 또한 이러한 방식의 콘텐츠의 배포나 공급은 인터넷 공유업체의 음성적인 유통 시장을 양성적인 시장으로 변화 시킬 수 있으며 인터넷 공유 시장을 올바르게 활성화 할 수 있는 방안으로 사료된다.

향후 연구로는 콘텐츠를 좀 더 복잡하고 다양한 방법으로 암호화 하는 방법에 대한 연구가 필요하며, 사용자 단말을 통한 콘텐츠 이용의 경우 좀 더 많은 플랫폼 간의 독립성의 확보에 대한 연구가 필요하며 방송프로그램의 식별 정보를 통한 콘텐츠 외에 콘텐츠의 영상 정보를 이용한 콘텐츠 식별등의 콘텐츠 식별 방법에 대한 추가적인 연구가 필요 할 것으로 사료된다.

참고문헌

[1] "케이블카드 분리 정책 고찰" - 최윤동, 김성민, 박광만, 고순주 정보통신진흥연구원

[2] "PKI의 개념과 해외 시장 현황" - 심동철 KISDI IT Focus, 2001
[3] The Open Source toolkit for SSL/TLS, http://www.openssl.org
[4] "미래 안방 방송의 주인공은? IPTV vs. CATV" - 이영수, 주간경제, 2006
[5] "ATSC A/57 규격 변경에 따른 방송프로그램 ID수정안" 한국정보통신기술협회, 2008
[6] "지상파 디지털TV방송 송수신정합표준" - 한국정보통신기술협회, 2008
[7] ATSC Standard: Content Identification and Labeling for ATSC Transport, http://www.atsc.org/standards/a_57b.pdf
[8] Secure programming with the OpenSSL API Part 1,2,3 , Kenneth Ballard 22 Jul 2004, http://www.ibm.com/developerworks
[9] An Introduction to OpenSSL Programming, Eric Rescorla, RTFM, Inc. October 5, 2001

저자소개

박 기 철(Ki-Chul Park)

2007년 배재대학교 컴퓨터공학과 (학사)
2009년 배재대학교 컴퓨터공학과 (석사)
※관심분야 : 멀티미디어 시스템, 임베디드 시스템, 소셜 네트워킹, MPEG-21

이 주 영(Joo-Young Lee)

2003년 아주대학교 미디어학과 (학사)
2006년 한국과학기술원 전산학과 (석사)
2006년~현재 한국전자통신연구원 전파방송연구단
※관심분야 : 콘텐츠 저작권 보호기술, 멀티미디어 데이터베이스

남 제 호(Je-Ho Nam)

1992년 홍익대학교 전기제어공학과(학사)
1996년 University of Minnesota, Dept. of Electrical Eng.(석사)
2000년 University of Minnesota, Dept. of Electrical Eng. (박사)
2001년 ~ 현재 한국전자통신연구원(ETRI) 방송미디어연구그룹 선임연구원, 방통융합콘텐츠보호연구팀장
2007년 ~ 현재 과학기술연합대학원대학교(UST) 이동통신 및 디지털방송공학 겸임 부교수
※관심분야 : 멀티미디어 신호처리, 디지털방송기술, MPEG, 콘텐츠 보호관리

정 회 경(Hoe-Kyung Jung)

1985년 광운대학교 컴퓨터공학과 (학사)
1987년 광운대학교 컴퓨터공학과 (석사)
1993년 광운대학교 컴퓨터공학과 (박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, XML, SVG, Web Services, Semantic Web, MPEG, 유비쿼터스 센서 네트워크, 콘텐츠 보호 관리