IPTV 서비스를 위한 수신권한 인증 및 관리 시스템 설계 및 구현

조용순* · 진두석* · 최봉규* · 정회경*

*배재대학교 컴퓨터공학과

The Design and Implementation of Conditional Access Authentication and Management System for IPTV Service

Yong-soon Cho* · Du-seok Jin* · Bong-Kyu Choi* · Hoe-Kyung Jung*

*Dept. of Computer Engineering, Paichai University

E-mail : *{inadvanceof, dsjin, bongkyu1963, hkjung}@pcu.ac.kr

요 약

최근 들어 통방융합이 진행되고 있는데, 이는 방송, 통신, 전화 서비스가 통합된 TPS(Triple Play Sevice)를 제공하는 IPTV(Internet Protocol TV) 서비스를 등장시켰다. IPTV는 방송 서비스와 VOD(Video on Denmand) 서비스를 제공하며, 이에 대한 보안을 위해 IPTV 포럼에서는 CAS(Conditional Access System)와 DRM(Digital Rights Management) 보안 솔루션 인터페이스 표준화를 진행 중에 있다. CAS는 실시간 방송 보안에 적합하고, DRM은 VOD 서비스 보안에 적합하다. 그러나 이 보안 시스템들은 제작자에 따라 권한정보의 표현 및 관리가 서로 상이하여 상호운용 부재를 야기한다. 또한 CAS와 DRM의 인터페이스 표준화 작업이 완료되면 표준 인터페이스를 기반으로 이기종 보안 시스템간의 통합 운용 요구가 발생할 것으로 사료된다. 이는 보안 시스템과 플랫폼에 독립적으로 상호 운용 가능한 권한 관리 시스템의 필요성을 의미한다.

이에 본 논문에서는 멀티미디어 디지털 콘텐츠의 보호와 유연한 IPTV 서비스를 위해 CAS와 DRM을 연계하여 권한 정보를 관리하는 수신권한 관리 시스템을 설계 및 구현하였다.

ABSTRACT

Currently broadcasting and telecommunication has integrated, And IPTV Service has appeared who called TPS(Triple Play Service) which integrated with broadcasting, telecommunication and Phone Service. IPTV provide braodcasting service and VOD(Video on Demand) service, and it must be satisfied digital content security. For this condition, IPTV Forum working on standardization of interface for digital content security. The Security solution for broadcasting and VOD are CAS(Conditional Access System) and DRM(Digital Rights Management). But these solutions manufactured by many vendors, so there is no inter-operablity. And after finished standardization of interface for CAS and DRM system, the problem of inter-operability with them will be issued. For this reason, Rights management system which possible to operate independently with platform is necessary. In this paper, To protect multimedia digital content, we designed and implemented Conditional Access Management System.

키워드

MPEG-21, 디지털 방송, IPTV, XML

Ⅰ. 서 론

멀티미디어 디지털 콘텐츠는 고정된 환경에 국한되지 않고 인터넷 환경에서의 소비 경향으로 자리를 잡아가고 있으며, 통방융합을 통한 IPTV 서비스가 이슈화되고 있다. IPTV 서비스는 콘텐츠 보호를 위해 보안성이 충족되어야 하며, 이를 위해 IPTV 포럼에서 보안 솔루션인 CAS와 DRM의 인터페이스를 표준화 중에 있다[1,2].

현재 CAS 시스템과 DRM 시스템은 보안 서비

스 운용을 위해 필요한 정보들을 권한 정보 관리 시스템으로부터 제공받고 있다. 권한 정보 관리 시스템은 제작업체들이 독자적으로 개발 및 운용하고 있어 CAS 시스템과 DRM 시스템간의 권한 정보 상호 운용성의 부재를 야기한다. 또한 CAS 시스템과 DRM 시스템의 인터페이스 표준화 작업이 완료되면 표준 인터페이스를 기반으로 이기종 보안 시스템간의 통합 운용 요구가 발생할 것으로 예상된다[3]. 이는 보안 시스템에 독립적으로 상호 운용 가능한 권한 정보 관리 시스템의 필요성을 야기하며, 플랫폼에 독립적인 권한 정보 표현 언어의 표준화를 요구한다.

이에 본 논문에서는 멀티미디어 디지털 콘텐츠의 보호와 유연한 IPTV 서비스를 위해 수신권한 정보 관리 시스템을 설계 및 구현하였다.

II. 관련연구

2.1 MPEG-21 REL(Rights Expression Language)

REL은 RDD와 함께 MPEG-21 지적 재산권 관리 및 보호(IPMP, Intellectual Property Management and Protection)의 세부 요소로 분류된다. REL은 MPEG-21 Multimedia Frameworks 내에서 디지털 콘텐츠 이용, 유통, 관리 및 사용 규칙 등에 관한 표현 언어로 저작권 처리 관련 용어에 대하여 신뢰도 높은 시스템을 제시한다. 또한 표준화된 용어를 제공함으로 타 시스템간 상호 운용성의 증대 및 유연성과 함께 확장성을 제공하는 것이 목표이다. REL의 스키마는 REL Core, REL Standard Extension, REL Multimedia Extension로 구성된다[4].

2.2 XML 전자서명

XML 전자서명은 임의의 디지털 콘텐츠에 대한 디지털 서명을 표시하기 위해 쓰이는 XML 문법으로 다양한 유형의 데이터 타입에 대해 전자서명을 처리한다[5].

XML 전자서명은 Signature 엘리먼트로 모든 것을 포함하는 구조로 되어 있으며 전자서명에 관련된 정보를 기술하는 SignatureInfo 엘리먼트와 서명된 데이터를 저장하는 SignaureValue 엘리먼트를 기본적으로 포함하도록 구성되어 있다. SignedInfo 엘리먼트는 전자서명에 관련된 정보를 기술하며, XML 정규화에 사용된 알고리즘을 명시하는 CanonicalizationMethod 엘리먼트, 전자서명에 사용된 알고리즘을 명시하는 SignatureMethod 엘리먼트, 서명에 사용된 Digest값과 Digest값 추출을 위해 사용된 알고리즘을 명시하는 DigestMethod 엘리먼트와, DigestValue 엘리먼트, 그리고 Digest관련 엘리먼트를 포괄하며 전자서명을 적용한 원본 문서의 위치를 기술하는 Reference 엘리먼트로 구성된다. XML 전자서명은 동봉된 서명, 동봉한 서명, 분리된 서명 3가지 형식으로 나뉜다.

III. 수신권한 관리 시스템 설계

3.1 시나리오

현재 IPTV는 CAS 시스템과 DRM 시스템을 동시에 지원하는 방향으로 발전하고 있으며, CAS 시스템을 통한 실시간 방송의 보호와 DRM 시스템을 통한 프로그램 단위의 보호를 통해 IPTV 서비스를 사용자에게 제공한다. 이를 위한 시스템과 사용자와의 관계 구성도를 그림 1에 나타내었다.

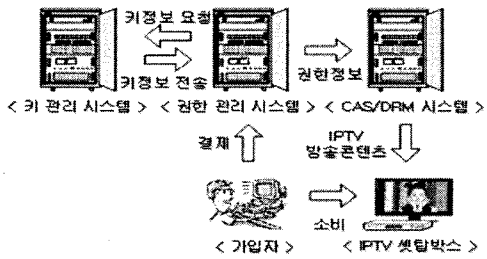

그림 1. 시스템/사용자 관계 구성도

시스템과 사용자의 관계를 기반으로 가상 시나리오를 설정하여 설계를 진행하였다.

3.2 시스템 설계

본 논문에서의 설계는 크게 키관리 시스템, 권한 관리 시스템으로 나뉘며 이를 테스트하기 위한 권한 정보 테스트 클라이언트로 구성된다. 수신권한 관리 시스템의 전체 아키텍처는 그림 2와 같다.

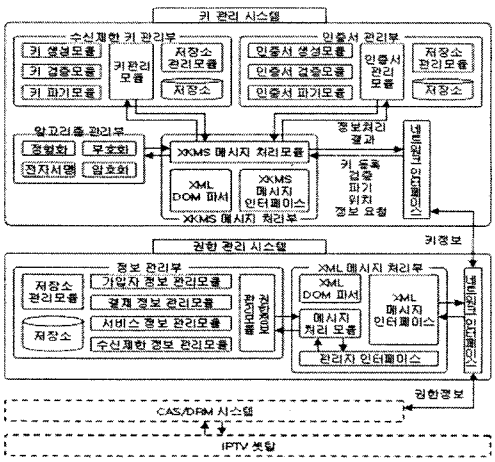

그림 2. 수신권한 관리 시스템

3.3 키 관리 시스템

키 관리 시스템은 네트워크 인터페이스, XKMS (XML Key Management Specification) 메시지 처리부, 인증서 관리부, 수신권한 정보 관리부, 알고리즘 관리부로 구분된다.

XKMS 메시지 처리부는 XKMS 메시지 인터페이스를 통해 네트워크 인터페이스로부터 XML 형식의 요청 메시지를 전송받는다. 전송된 메시지는 XKMS 메시지 처리모듈로 전달된다. 이후 XKMS 메시지 처리모듈은 적재된 XKMS 요청 메시지를 분석하여 등록, 검증, 파기, 위치정보 요청 메시지로 분류한다.

인증서 관리부는 DRM 시스템의 권한 정보에 필요한 인증서 정보를 저장 및 관리한다. XKMS 메시지 처리부의 XKMS 메시지 처리모듈로부터 인증서의 생성, 검증, 파기에 대해 요청받을 경우, 전달받은 파라미터를 통해 인증서에 적용될 알고리즘을 판별하며, 알고리즘 관리부의 알고리즘을 사용하여 인증서에 대한 요청 메시지를 처리한다. 처리된 결과는 다시 XKMS 메시지 처리모듈로 반환한다.

수신권한 정보 관리부는 인증서 관리에 필요한 키를 저장 및 관리한다. XKMS 메시지 처리부의 XKMS 메시지 처리모듈로부터 생성할 키의 알고리즘 정보를 전달받으며 생성된 키는 저장소 관리모듈을 통해 저장소에 저장된다. 키 생성 외에 키에 대한 검증 요청과 파기 요청을 처리하며, 검증 시 해당 알고리즘을 사용하여 키의 유효성 검사를 진행하고, 파기 시 저장소 관리모듈로 해당 키 정보를 검색하여 파기한다.

알고리즘 관리부는 XML 전자서명과 XML 암호화를 지원하기 위해 RSA, DSA 전자서명 알고리즘과 AES, Triple-DES 암호화 알고리즘, Base64 부호화 알고리즘, XML 정형화 알고리즘을 제공한다.

3.4 권한 관리 시스템

권한 관리 시스템은 네트워크 인터페이스, 관리자 인터페이스, XML 메시지 처리부, 정보 관리부로 구성된다.

관리자 인터페이스는 권한 관리 시스템에 등록되어 있는 정보를 관리자가 접근하여 관리할 수 있는 인터페이스를 제공한다. 관리자는 이 인터페이스를 통해 가입자 정보, 결제 정보, 유료 콘텐츠 서비스 정보, 수신 제한 정보, 권한 정보를 관리한다. XML 메시지 처리부는 메시지를 네트워크 인터페이스로부터 수신하여 메시지 처리모듈로 전달한다. 메시지 처리모듈은 적재된 XML 메시지의 유형을 분석하여 정보 관리부에 저장된 정보를 관리한다.

정보 관리부는 권한 관리 시스템이 CAS 시스템과 DRM 시스템, 수신권한 정보 관리 시스템과 연계하여 정보를 제공하기 위한 정보를 보유하고 있으며, 정보의 관리를 위해 가입자 정보, 결제 정보, 서비스 정보, 수신제한 정보, 권한 정보를 저장소 관리모듈을 통해 관리한다.

3.5 권한 정보 테스트 클라이언트

CAS 시스템과 DRM 시스템은 각 벤더(Vendor)들의 독자 기술로 제작되어 운용되기 때문에 실제로 구현하는데 있어 어려움이 있고, 본 논문에서 제안한 연구의 범위를 고려하여 수신권한 관리 시스템이 생성하여 전송한 권한 정보를 수신하여 해당 정보에 대한 검증을 진행하기 위해 설계하였다. 권한 정보 테스트 클라이언트는 그림 3과 같이 네트워크 인터페이스, XML 메시지 처리부, 권한 정보 처리부, 사용자 인터페이스로 구성된다.

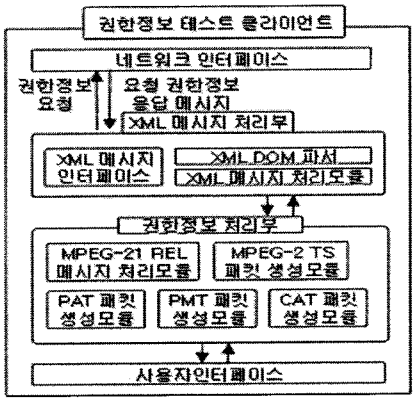

그림 3. 권한정보 테스트 클라이언트

XML 메시지 처리부는 XML 메시지 인터페이스, XML DOM 파서, XML 메시지 처리모듈로 구성되며, 메시지를 네트워크 인터페이스로부터 수신하여 메시지 처리모듈로 전달한다. 메시지 처리모듈은 적재된 REL 권한 정보를 권한 정보 처리부로 전달한다.

권한 정보 처리부는 MPEG-21 REL 메시지 처리모듈, MPEG-2 TS 패킷 생성모듈, PAT 패킷 생성모듈, PMT 패킷 생성모듈, CAT 패킷 생성모듈로 구성된다.

사용자 인터페이스는 권한 정보 처리부로부터 REL 권한 정보 문서를 전달받아 출력창에 권한 정보를 출력하는 역할을 담당한다.

IV. 수신권한 관리 시스템 구현

본 시스템은 MS사의 Windows XP 운영체제가 설치된 IBM-PC 호환 컴퓨터상에서 MS Visual Studio .NET 2003과 MSXML 4.0 SDK, MySQL Essential 5.0.45를 사용하여 구현하였다.

4.1 키 관리 시스템 구현

수신제한 키 관리 시스템의 전체적인 인터페이스는 세 개의 구조로 이루어지는데 등록된 키/인증서 정보들을 확인할 수 있는 키/인증서 정보 표시부, 권한 관리 시스템과 네트워크 접속을 담당하는 시스템 접속 제어부, 시스템에서 발생하는 모든 이벤트를 로그 파일로 저장 및 확인하는 이벤트 리포팅 표시부로 구성된다. 수신제한 키 관리 시스템을 구현한 인터페이스를 그림 4에 나타내었다.

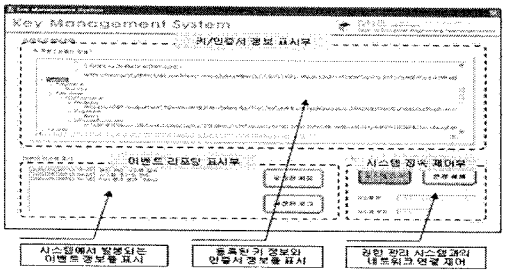

그림 4. 키관리 시스템

4.2 권한 관리 시스템 구현

권한 관리 시스템의 전체적인 인터페이스는 세 개의 구조로 이루어지는데 등록된 정보들을 확인 및 관리할 수 있는 권한 정보 관리부, CAS/DRM 시스템, 수신 제한 키 관리 시스템과 연결을 담당하는 시스템 연동 제어부, 시스템에서 발생하는 모든 이벤트를 로그 파일로 저장 및 확인하는 이벤트 리포팅 표시부로 구성된다. 권한 관리 시스템을 구현한 인터페이스를 그림 5에 나타내었다.

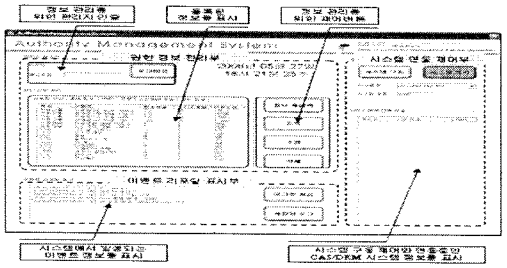

그림 5. 권한 관리 시스템

4.3 권한 정보 테스트 클라이언트 구현

권한 정보 테스트 클라이언트의 인터페이스는 세 개의 구조로 이루어지는데 등록된 정보들을 확인 및 관리할 수 있는 권한 정보 관리부, CAS/DRM 시스템, 수신 제한 키 관리 시스템과 연결을 담당하는 연동 시스템 제어부, 시스템에서 발생하는 모든 이벤트를 로그 파일로 저장 및 확인하는 이벤트 리포팅 표시부로 구성된다. 권한 관리 시스템을 구현한 인터페이스를 그림 6에 나타내었다.

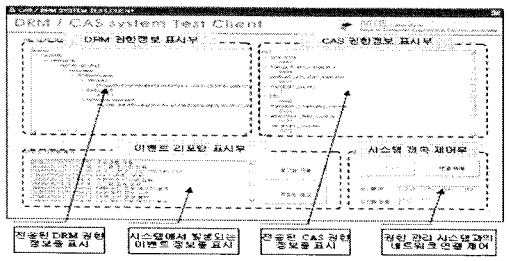

그림 6. 권한정보 테스트 클라이언트

V. 고찰 및 결론

본 논문에서는 IPTV 포럼에서 진행중인 보안 솔루션 인터페이스의 표준화 완료시 권한 정보 시스템의 상호 운용성을 보장하기 위해 CAS/DRM 시스템에서 통합적으로 운용이 가능한 권한 정보 문서를 생성할 수 있는 수신권한 관리 시스템을 설계 및 구현하였다.

본 시스템은 MPEG-21 REL 스키마를 기반으로 생성된 권한 정보 문서에 대해 DOM 객체를 생성한다. 생성된 DOM는 CAS/DRM 시스템에서 필요로하는 권한 정보를 모두 명시하고 있으며 이는 국제표준 MPEG-21 REL 문서를 기반으로 작성되어 있어 통합 운용에 대한 상호운용성을 보장한다. 그러므로 MPEG-21 REL 표준을 사용하여 구현된 개방형 시스템이라는 점과 메타데이터의 상호 운용성 보장을 통해 향후 IPTV 서비스를 위한 CAS/DRM 시스템간의 상호연동 시 권한 정보의 통합관리가 가능하다는 특징을 갖는다. 현재 IPTV의 보안 솔루션에 있어서의 콘텐츠 보호에 대한 측면으로 볼 때, CAS/DRM 시스템은 인터페이스에 대한 표준이 상이하여 상호운용성에 문제점을 가지고 있다.

이에 본 논문에서 제안 및 구현한 참조 모델은 국제 표준 규격인 MPEG-21 REL 문서로 권한 정보를 기술함으로써 권한 정보의 상호운용성을 해결하고 있다. 또한 향후 IPTV 보안 솔루션 인터페이스의 표준화 완료시 CAS/DRM 보안 솔루션의 병합 모델로서의 활용이 가능할 것으로 사료된다. 향후 연구 과제로는 CAS 시스템으로 보호되는 실시간 방송 콘텐츠를 저장하여 이를 DRM 시스템의 기술을 적용하여 재분배토록 하는 연구가 필요하며, 이는 CAS/DRM 시스템의 병합 운용에 대한 기술로서 연구가 진행되어야 할 것이다.

참고문헌

[1] 김태현, "표준화 이슈가 되고 있는 IPTV 보호기술 상호연동", 한국정보통신기술협회, 2007.9.28

[2] 우제학, "IPTV 콘텐츠 보호 기술의 비교 - CAS와 DRM 중심으로", 한국콘텐츠학회논문지 '06 Vol. 6 No. 8, p157-164, 2006.6

[3] 이준휘, "IPTV 국내 표준 규격 소개", TTA Journal No.116, Section - IT Standard & Test, p53-59, 2008.3

[4] ISO/IEC 21000-5, MPEG, 'Information technology – Multimedia framework (MPEG-21) – Part 5: Rights Expression Language', 2004

[5] XML Signature, World Wide Web Consortium, http://www.w3.org/TR/ xmldsig - core/, 2008.6