IPTV 서비스를 위한 수신 제한 키 관리 시스템 설계

황경민* · 김창수** · 김서균*** · 김철원**** · 박기철* · 정회경*

*배재대학교 컴퓨터공학과 · **청운대학교 인터넷학과 · ***정보통신연구진흥원

· ****호남대학교 컴퓨터공학과

The Design of Key Management Module for IPTV Service

Kyung-min Hwang* · Chang-soo Kim** · Seo-kyun Kim*** · Chul-won Kim****

· Ki-chul Park* · Hoe-kyung Kim*

*Dept. of Computer Engineering, Paichai University · **Dept. of Internet, Chungwoon University

***IITA· ****Dept. of Computer Engineering, Honam University

E-mail : *{koukyo, kcpark, hkjung}@pcu.ac.kr, **ddoja@chungwoon.ac.kr, ***skkim@iita.re.kr,

****cwkim@honam.ac.kr

요 약

영상압축 기술의 발달로 시작된 멀티미디어 시장의 성장은 방송 환경이 아닌 IP 네트워크 환경으로까지 영역이 확대되고 있다. 이는 IPTV 서비스라는 형태로 나타나고 있으며 기존의 방송환경이 아닌 IP 환경에서 방송, 통신, 전화의 트리플 서비스(Triple Service)를 제공한다. 현재 IPTV 서비스에 사용되는 IPTV 셋탑박스(Settop Box)는 수신 제한 기능에 고정된 키를 사용하고 있어 관리와 운용에 자원이 낭비되는 측면이 있다. 이는 MPEG-21의 REL(Right Expression Language)과 XML 전자서명을 활용하여 유동적인 IPTV 셋탑박스 운용이 가능하다.

이에 본 논문에서는 MPEG-21 REL과 XML 전자서명을 사용하여 소비자의 수신 제한 권한이 관리 가능한 IPTV 서비스를 위한 수신 제한 키 관리 시스템을 설계하였다.

ABSTRACT

The Growth of Multimedia Digital Content market is extending to IP network environment. this is realized via IPTV service which provide Triple-Service that is broadcasting, communication, telephone service. Recently on IPTV Settop box has fixed key for control access permission. and this is cause of Wasting resource to operation and management. it can be resolved to apply DRM System which mixed MPEG-21 REL(Rights Expression Language) and XML Signature. In this paper, we designed Permission Management Module for IPTV Service which can control permission to access via MPEG-21 and XML Signature.

키워드

IPTV, DRM

Ⅰ. 서 론

영상/음성 정보의 압축 기술이 개발되기 시작하면서 멀티미디어 디지털 콘텐츠 시장 또한 꾸준한 성장을 거듭해왔다. 초창기에는 단순히 영상/음성 정보를 디지털화하여 저장하는 것이 목적이었지만, 현재 단순한 저장의 목적이 아닌 디지털 방송, 영상 통화, 교통 실황 정보 등 다양한 분야에서 활용되고 있다. 더불어 네트워크 통신 기술의 발달로 멀티미디어 디지털 콘텐츠는 고정된 환경에 국한되지 않고 인터넷 환경에서의 소비 경향으로써 자리 잡아 가고 있다. 이를 배경으로 방송과 통신의 융합이 진행되고 있으며 이는 방송, 통신, 전화 3가지 서비스가 통합된 IPTV 서

비스로 등장 하였다. IPTV는 컴퓨터와는 달리 셋탑박스라는 수신기를 통해 사용자에게 서비스된다. 현재 IPTV는 국제적으로 표준화가 진행되고 있으며 일부 국가에서는 상용 서비스로서 제공되고 있다[1].

IPTV를 국내에 서비스하기 위해서는 안정적인 네트워크망의 구축이 필요하며 이는 케이블 디지털 방송으로 제공되고 있는 방송망을 통해 실현이 가능하다. 또한 인터넷 서비스를 동시에 제공하고 있어 양방향 서비스 제공의 문제점을 해결하고 있다. 하지만 IPTV는 멀티미디어 디지털 콘텐츠의 개인정보 보안에 취약점이 존재하며 이는 주요 IPTV 표준화의 중요 이슈로서 CAS 시스템과 DRM 시스템을 병합하여 해결하려는 노력이 시도되고 있다[2].

이에 본 논문에서는 멀티미디어 디지털 콘텐츠를 보호하고 유동적인 IPTV 서비스를 제공하기 위해 CAS 시스템을 DRM 시스템과 연계하여 IPTV 서비스를 위한 수신 제한 키 관리 시스템을 설계 및 구현하였다.

II. 관련연구

2.1 MPEG-2 TS(Transport Stream)

MPEG-2 TS에서 정의하고 있는 TS 패킷은 데이터를 전송하는 컨테이너로서 디지털방송을 서비스하기 위한 188바이트 단위의 패킷으로서 4바이트의 헤더와 184바이트의 페이로드(payload)로 이루어져 있다. MPEG-2 TS의 구조는 그림 1과 같다[3].

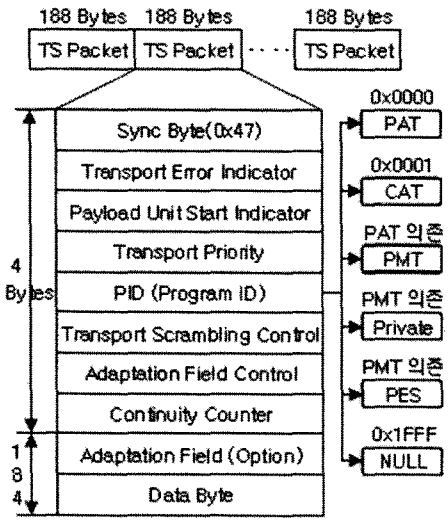

그림 1. MPEG-2 TS 전체 구조

TS 패킷은 영상정보와 음성정보를 전송하는 PES(Packetized Elementary Stream)와 특화된 프로그램의 방송정보를 전송하는 PSI(Program Specific Information)로 구분된다. PSI 정보는 모든 PMT에 대한 정보를 가지고 있는 PAT(Program Associated Table), 유료방송을 위한 조건부 접속을 위한 정보를 가지고 있는 CAT(Condition Access Table), 방송프로그램의 영상 및 음성에 대한 정보를 가지고 있는 PMT(Program Map Table), 그리고 해당 방송 서비스를 제공하는 네트워크 환경에 대한 정보를 가지고 있는 NIT(Network Information Table) 등 4개의 정보로 이루어져 있다.

2.2 MPEG-21 REL(Rights Expression Language)

REL은 RDD와 함께 MPEG-21 지적 재산권 관리 및 보호(IPMP)의 세부 요소로 분류 된다. REL은 MPEG-21 Multimedia Frameworks 내에서 디지털 컨텐츠 이용, 유통, 관리 및 사용 규칙 등에 관한 표현 언어로 저작권 처리 관련 용어에 대하여 신뢰도 높은 시스템을 제시한다. 또한 표준화된 용어를 제공함으로 타 시스템간의 상호 운용성 증대와 유연성과 함께 확장성을 제공하는 것을 목표로 한다. REL의 스키마는 REL Core, REL Standard Extension, REL Multimedia Extension으로 구성된다. REL Core에서는 루트 엘리먼트 License를 비롯한 핵심 요소 및 REL 전체의 개념 정의 등을 포함하고 있고, REL Standard Extension 부분은 REL 소비에서 일반적이고도 광범위하게 사용할 수 있는 정보들을 정의 하고 있다. REL Multimedia Extension 부분에서는 멀티미디어 자원에 대한 사용, 삭제 및 수정 등의 자원에 대한 확장 처리 정보가 정의되어 있다. 각각은 필요한 경우 REL Core를 확장하여 사용할 수 있다. 하위 계층에서 RDD가 REL의 용어를 정확하게 정의하고 각각의 의미를 제공하게 된다[4].

REL은 XML 스키마 기술을 사용하여 XML 네임스페이스와의 호환성을 가질 수 있어 디지털 콘텐츠 제공자들에게 비즈니스 확장성을 크게 높여준다. 따라서 확장에 대한 요구를 고려하여 REL은 광범위하게 정의 되어 있으며 현존하는 모든 멀티미디어 자원에 관한 저작권 정보를 처리 할 수 있도록 설계 되어 있다. REL의 모델 범위는 기존의 타 시스템 보다 비즈니스 모델의 수용 범위가 확대되어 기존의 컨텐츠 중심 모델을 벗어나 서비스 중심 모델이나 개별 엔티티 또는 그룹의 권리 결합, 라이프사이클 비즈니스 시나리오 등 다양한 모델로의 확장을 지원한다.

2.3 XML 전자서명

XML 전자서명은 서명이 포함된 XML 문서에 존재하거나 또는 그 이외의 위치에 존재하는 다양한 형식의 데이터에 대해 무결성, 메시지 인증 및 서명 인증 서비스를 제공한다[5]. XML 전자서명은 디지털 콘텐츠의 형식에 상관없이 모두 적용 가능하며 하나 이상의 리소스에 대해서도 적

용될 수 있다. XML 전자서명은 서명시 Enveloped, Enveloping, Detached 3가지 형태로 서명된다.

XML 전자서명은 Well-formed XML 문서로 이루어져 있으며 이로 인해 바이너리 포맷일 때와는 달리 서명 처리에 필요한 모든 정보를 서명 안에 담을 수 있다. XML 전자서명은 최소한의 처리만으로 XML 서명정보를 처리할 수 있으며 암호키나 서명 검증을 위한 X.509 인증서를 XML 전자서명 문서 내에 포함 가능하다. XML 전자서명은 XML 문서의 특성을 포함하기 때문에 물리적으로는 다른 문서를 논리적으로 완전히 동일한 문서로 인식한다. 이를 해결하기 위해 XML 정형화를 통해 항상 동일한 XML 문서를 추출하여 처리하며, 정규화 처리된 XML 문서는 해쉬함수를 통해 해당 XML 문서만이 가질 수 있는 고유의 값으로 변형된다. XML 전자서명은 이 고유의 해쉬값을 서명에 사용하여 무결성, 메시지 인증 및 서명 인증 서비스를 제공할 수 있게 된다.

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 Digest 값과 Digest값 추출을 위해 사용된 알고리즘을 명시하는 DigestMethod 엘리먼트와, DigestValue 엘리먼트, 그리고 Digest관련 엘리먼트를 포괄하며 전자서명을 적용한 원본 문서의 위치를 기술하는 Reference 엘리먼트로 구성된다. 특히 Reference 엘리먼트는 Transform 엘리먼트를 통해 XML 문서가 서로 동일함을 증명하는 XML 정규화에 대해서 어떤 알고리즘이 사용되었는지를 명시할 수 있다. DigestMethod 엘리먼트와 DigestValue 엘리먼트는 XML 전자서명 문서의 해쉬값과 해쉬값 추출에 사용된 방법에 대해서 정보를 제공하며 DigestValue 엘리먼트는 해쉬값을 Base64 인코딩 형식으로 부호화해서 값을 저장한다. SignatureValue 엘리먼트는 DigestValue 값을 SignatureMethod 엘리먼트에 명시된 서명 알고리즘을 사용하여 서명한 값을 Base64 인코딩하여 서명 값을 저장한다. KeyInfo 엘리먼트는 서명에 사용된 인증키에 대한 정보를 기술할 수 있는 엘리먼트로서 현재 공개키 기반의 키구조와 정보를 명시할 수 있는 X.509 형식의 표현을 X509Data 엘리먼트를 통해 지원한다. 또한 공개키 기반 구조에 대한 정보를 SPKIData 엘리먼트를 통해 기술하며, 기타 키에 대한 정보를 제공하기 위한 엘리먼트로 구성되어 있다. Object 엘리먼트는 Enveloping 구조의 전자서명에서 사용되는 구성요소로서 XML 전자서명 문서내부에 서명 원본 데이터를 포함하는 구조에 사용된다.

III. 시스템 설계

IPTV 서비스를 위한 수신 제한 키 관리 시스템의 전체 아키텍처는 그림 2와 같다.

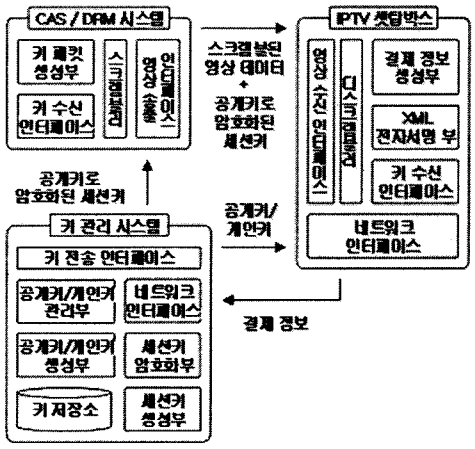

그림 2. 시스템 전체 아키텍처

IPTV 서비스를 위한 수신 제한 키 관리 시스템은 IPTV 서비스를 스크램블하여 송출하는 CAS / DRM 시스템, 스크램블된 IPTV 서비스를 서비스하는 IPTV 셋탑박스, 그리고 두 시스템의 수신 권한 키를 관리하는 키 관리 시스템으로 구성되어 있다. 본 장에서는 IPTV 서비스를 위한 수신 제한 키 시스템의 핵심 구성요소인, 키 관리 시스템, CAS/DRM 시스템의 키 패킷 생성부, IPTV 셋탑박스의 결제정보 생성부와 XML 전자서명부를 설계한다.

3.1 키 관리 시스템

키 관리 시스템은 IPTV 셋탑박스로부터 XML 전자서명을 통해 결제 정보를 전송 받으며 이를 통해 결제 정보를 공개키와 함께 키 저장소에 보관한다. 키 저장소에 저장된 공개키는 CAS/DRM 시스템에서 사용될 세션키를 암호화하며 IPTV 셋탑박스로부터 받은 결제 정보를 통해 유료 콘텐츠에 대한 MPEG-21 REL 권한 문서를 작성하여 CAS/DRM 시스템을 전송한다.

세션키 관리부는 CAS 시스템에서 사용되는 실시간 방송 스트림의 스크램블링에 사용되는 대칭키를 관리한다. 실시간 스트림의 신속한 스크램블링에 적합한 DES 알고리즘이 사용되며 DES 키를 약 4초 간격으로 생성하여 인증키 관리부로부터 콘텐츠 소비를 결제한 사용자의 공개키를 제공받아 세션키 암호화를 진행한다. 이는 스크램블된 키를 결제자가 개인키로 복호화하여 세션키를 획득하여 콘텐츠 소비가 가능하게 한다.

세션키 관리부는 세션키 생성을 위한 타이머

모듈, 스크램블링에 사용될 DES 알고리즘을 사용한 세션키 생성 모듈, 생성된 DES키를 검증하기 위한 세션키 검증 모듈, 권한이 있는 사용자가 자신의 개인키로 세션키를 획득하기 위한 세션키 암호화 모듈, 공개키로 생성된 암호화된 세션키를 검증하기 위한 세션키 암호화 검증 모듈, 사용자 콘텐츠 소비권한을 명시하는 MPEG-21 REL 문서 생성 모듈로 구성된다. 인증키 관리부는 IPTV 셋탑박스로부터 사용자의 인증키 생성 요청을 받아 공개키/개인키로 이루어진 인증키를 생성한다. 생성 인증키는 키 관리 모듈을 통해 키 저장소에 저장되며 키 관리를 위해 IPTV 셋탑박스의 네트워크 인터페이스의 MAC 어드레스를 고유 번호로 함께 저장한다. 세션키 관리부로부터 인증키 요청을 받으면 해당 인증키에 대한 권한을 결제정보 관리부를 통해 확인후 세션키 관리부로 인증키를 전송한다. 결제정보 관리부는 IPTV 셋탑박스로부터 사용자의 결제정보를 수신하여 결제를 진행하며 이때 인증키 관리부로부터 생성된 인증키를 기반으로 결제 정보를 검증한다. 결제정보 관리부는 XML 전자서명 알고리즘을 사용하며 서명정보를 처리하는 XML 전자서명부, XML 전자서명 문서의 변형을 방지하기 위한 XML 정규화 모듈로 이루어져 있다. 네트워크 인터페이스는 IPTV 셋탑박스와 CAS/DRM 시스템간의 통신을 담당하며 콘텐츠 소비권한을 명시하는 MPEG-21 REL 문서와 사용자의 공개키로 암호화된 세션키, 그리고 스크램블에 사용되는 DES 세션키를 암호화하여 CAS/DRM 시스템으로 전송한다.

3.2 CAS/DRM 시스템

키 수신 인터페이스는 키 관리 시스템으로부터 암호화된 세션키를 수신하며 사용자 콘텐츠 소비권한을 명시하는 MPEG-21 REL 문서를 수신하여 키 패킷 생성부로 모든 정보를 전달한다. 키 패킷 생성부는 키 수신 인터페이스로부터 암호화된 세션키 전달받아 MPEG-2 TS 패킷을 생성한다. 생성되는 TS 패킷은 private 섹션을 사용하여 사전에 예약된 PID 번호로 KEY의 정보를 구분한다.

3.3 IPTV 셋탑박스

결제정보 생성부는 IPTV 사용자로부터 소비 콘텐츠에 결제하기 위한 정보를 처리한다. 결제정보 생성시 IPTV 셋탑박스의 네트워크 인터페이스 카드의 MAC 어드레스를 병합하여 고유의 ID를 생성 및 처리한다. 이 정보는 키 관리 시스템에서 소비자를 분별하기 위한 식별자로 사용되며 또한 소비 권한의 구분을 결정하는 중요 요소가 된다. 결제정보 생성시 사용자의 개인키가 존재하지 않을 때는 키 관리 시스템의 인증서 관리부로부터 인증키를 발급받아 정보를 생성한다. 결제정보 생성부에서 생성된 정보를 XML 전자서명을 통해 서명처리를 담당하며 서명에 사용되는 개인키를 통해 고유의 소비 권한을 처리한다. 네트워크 인터페이스는 키 관리 시스템과 통신을 담당하며 IPTV 사용자의 결제 정보, 인증키 생성을 요청하며 인증을 위해 생성된 개인키를 수신하여 결제정보에 필요한 정보를 전달한다.

Ⅳ. 결 론

영상/음성 압축 기술의 발달과 정보통신 기술의 발달은 통신과 방송의 융합을 유도하여 통방융합을 통한 새로운 서비스를 촉진하였다. 이는 방송, 통신, 전화 3가지 서비스를 하나로 제공하는 트리플 플레이 서비스라는 IPTV 서비스로 나타났다. IPTV는 국내 IT839 전략의 일환으로 추진되고 있으며 IPTV 표준화 작업을 진행 중에 있다. 현재 국내 IPTV 서비스는 콘텐츠의 보안을 위해 기존 케이블 디지털 방송에서 사용하는 CAS 시스템을 도입과 DRM 시스템을 통한 보안 시스템을 도입을 놓고 보안 시스템의 표준화를 진행하고 있으며 CAS 시스템은 실시간 스트림 서비스에서 강점을 보이지만 개인정보 보호시스템에 취약점이 존재한다. 반대로 DRM 시스템은 개인정보 보안이 강점이지만 실시간 스트림에 취약하다는 단점을 가지고 있다.

이에 본 논문에서는 실시간 스트리밍의 보안에는 적합하지만 개인정보의 보호에는 취약한 CAS 시스템을 DRM 시스템으로 보완하여 개인정보를 안전하게 제공하는 수신 제한 키 관리 시스템의 참조 모델을 제안하였다.

향후 연구 과제로는 본 참조 모델에서 제안하고 있는 공개키 기반의 세션키 암호화를 통한 수신 제한 키 관리 시, 다수의 IPTV 서비스 이용자들의 공개키를 효율적으로 관리 및 운용하기 위한 시스템의 구조에 대한 연구가 필요하며 IPTV 서비스의 본격적인 이용을 위한 기반 기술로서 연구가 진행되어야 할 것이다.

참고문헌

[1] 김도연, 'IPTV 동향 조사 보고서', 2008. 2
[2] 김정태, 'IPTV 콘텐츠의 저작권 보호를 위한 핵심 요소 - CAS / DRM', 2008. 3
[3] ISO/IEC 13818-1, MPEG, 'Generic Coding of Moving Pictures and Associated Audio Information : Systems', 2000
[4] ISO/IEC 21000-5, MPEG, 'Information technology -- Multimedia framework (MPEG-21) -- Part 5: Rights Expression Language', 2004
[5] W3C, 'XML-Signature Syntax and Processing', 2002