情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

셋톱박스 가상화를 통한 향상된 IPTV 사용자 인증 시스템

고 웅,† 곽 진‡
순천향대학교 정보보호응용및보증연구실

STB Virtualization based Enhanced IPTV User Authentication System

Woong Go,† Jin Kwak‡
Information Security Application & Assurance Lab, Soonchunhyang University

요 약

인터넷과 방송 통신과의 융합으로 IPTV서비스가 제공되면서, 사용자는 멀티미디어 콘텐츠를 시간에 상관없이 이용할 수 있게 되었다. 또한, 기존의 단방향 서비스에서 양방향 서비스로 변화하면서 사용자에게 좀 더 효율적이고 유용한 서비스 제공이 가능하게 되었다. 그러나 기존의 IPTV 서비스가 단말에 설치된 셋톱박스를 통해 멀티미디어 콘텐츠를 제공하면서, 개별적 사용자 인증이 이루어지지 않아 개별적 서비스에 한계점이 나타났다. 또한 셋톱박스가 방송 통신 사업자마다 달라 서비스 변경 시 호환성 문제도 대두되었다. 따라서 본 논문에서는 개별적 사용자 인증 및 서비스 호환성 향상을 위한 셋톱박스 가상화를 통한 향상된 IPTV 사용자 인증 시스템을 제안한다.

ABSTRACT

Because of the convergence between Internet and broadcast communication, users are able to use multimedia contents anytime. In addition, with the change of existing one-way service to two-way service, the provider can offer efficient and useful broadcast communication. However, As multimedia contents is provided by STB, it can validate only end-node STB. Thus, this method is limiting possibilities of individual service. Also, providers' STB are different, so problem of compatibility is emerging as an issue. Therefore, in this paper we proposed STB virtualization based enhanced IPTV user authentication system to improve individual authentication and compatibility of services.

Keywords: IPTV, STB, Virtualization, User Authentication

I. 서 론

초고속 인터넷의 발달은 방송통신과의 융합으로 인해 기존의 단방향 서비스만 제공하던 TV 방송에서 양방향성을 제공하는 IPTV로 발전하게 되었다. IPTV (Internet Protocol TeleVision)는 초고속 인터넷 망을 이용하여 사용자의 요청에 따라 양방향으로 멀티미디어 콘텐츠를 제공하는 방송통신 서비스이다. IPTV 서비스가 활발하게 진행됨에 따라 국내외적으로 기술 연구 및 표준화 활동이 이루어지고 있으며, 모바일 단말에서의 IPTV 서비스를 제공할 수 있는 연구도 활발히 진행되고 있다[1][2].

그러나 기존의 IPTV 서비스는 셋톱박스(STB : Set-Top Box)가 필수적으로 요구되며, 이를 통해 콘텐츠를 제어하고 있다. 이와 같은 환경에서는 개개인에 맞추어 콘텐츠를 제공하거나 차단하지 못하고, 셋톱박스에 따라 변경되는 실정이다. 따라서 맞춤형 방송 콘텐츠 제공이 어렵고, 정당한 콘텐츠 구매자 이

접수일(2011년 5월 30일), 게재확정일(2011년 7월 18일)
† 주저자, wgo@sch.ac.kr
‡ 교신저자, jkwak@sch.ac.kr

외의 사용자가 이를 이용하게 될 수도 있다. 이는 양방향성을 추구하는 IPTV 서비스의 한계점이라고 할 수 있다.

또한, 기업 마다 셋톱박스의 상호 호환성도 문제가 되고 있다. A 기업의 서비스에서 B 기업의 서비스로 이전하기 위해서는 셋톱박스 또한 바꾸어 주어야만 가능하다. 이러한 문제점은 확장성 및 가용성의 문제뿐만 아니라 경제적인 영향까지 미칠 수 있다[3].

따라서 본 논문에서는 기존의 IPTV 서비스를 클라우드 환경에 적용하여, 셋톱박스 가상화 기반의 개별적인 방송 콘텐츠 제공 사용자 인증 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 IPTV 서비스 및 셋톱박스에 대해 분석하고, 3장에서는 기존의 IPTV 문제점을 분석한다. 4장에서는 셋톱박스 가상화 및 사용자 인증 기법을 제안하고, 5장에서 제안 기법의 보안성 및 효율성을 분석한다. 그리고 6장을 결론으로 끝을 맺는다.

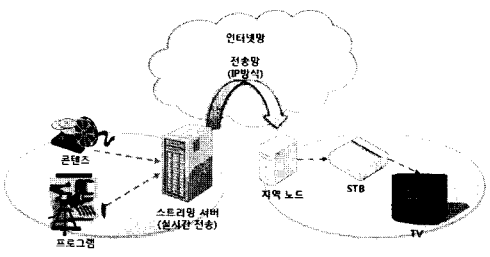
II. 관련연구

2.1 IPTV 서비스

IPTV 서비스는 초고속인터넷망을 통하여 양방향 통신으로 사용자의 요청에 따른 다양한 멀티미디어 콘텐츠를 제공하는 융합서비스를 의미한다. IPTV는 기존 공중파 방송에서 사용하는 전파가 아닌 인터넷망에서 사용되는 프로토콜을 이용하여 멀티미디어 스트리밍 방식으로 방송 프로그램을 제공한다. 이와 같은 방식은 기존 아날로그 시대의 단방향적 방송이 갖고 있던 시·공간적 제약을 해결함으로써 보다 적극적이고 능동적으로 여러 부가 서비스를 이용할 수 있는 장점을 가진다[4].

이러한 IPTV를 시청하기 위해서는 인터넷과 TV 사이에 셋톱박스를 설치해야 한다.

셋톱박스란 디지털 콘텐츠를 TV 또는 이용자 단말



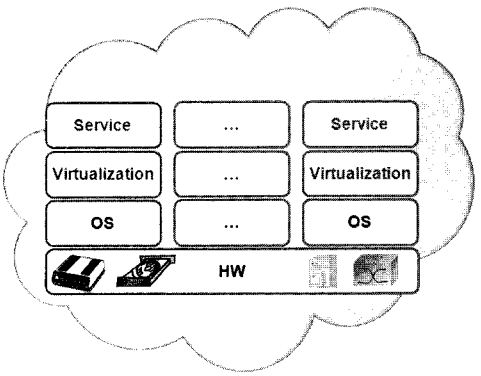
[그림 1] IPTV 서비스 개념도

장치를 통해 시청할 수 있게 해주는 장치로서 IPTV의 핵심요소이다. 셋톱박스에는 제한수신시스템(CAS : Conditional Access System)이 포함되는데, 유료 방송 서비스에 대한 정당한 사용자의 접근 여부를 제어하는 기본 시스템이다. 주로 방송사업자가 신호를 스크램블하여 멀티캐스트 방식으로 송출하면 셋톱박스가 이를 다시 디스크램블하여 화면에 보이는 방식이다.

따라서 서비스에 가입한 사용자의 셋톱박스만이 암호화된 멀티미디어 콘텐츠를 복호화 할 수 있다[5][6].

2.2 클라우드 컴퓨팅 가상화

클라우드 컴퓨팅은 인터넷 기술을 활용하여 가상화된 IT 자원을 서비스로 제공하는 컴퓨팅이다. 또한 개별적으로 저장하던 프로그램이나 문서를 인터넷으로 접속할 수 있는 컴퓨터에 분산 저장하고, 다양한 단말기로 원격작업을 수행하는 이용자 중심의 컴퓨팅이다. 클라우드 환경의 기본적인 구성 형태는 다음과 같다[7].



[그림 2] 클라우드 구성 형태

모든 하드웨어는 각각의 서비스가 공유해서 사용하고 개별적인 OS(Operating System)와 가상화를 통하여 실제 서비스를 제공하고 있다. 클라우드 컴퓨팅은 한정된 자원을 가장 효율적으로 사용하기 위해 가상화를 제공하는데 이것이 전체 환경에서 가장 핵심적인 요소이다.

가상화는 물리적으로 분리되어 있는 컴퓨터 리소스들을 논리적으로 통합하거나 반대로 하나의 자원을 논리적으로 분할해 자원을 효율적으로 사용하게 하는 기술이다[8][9].

III. 문제점 분석

3.1 비합법적인 사용자의 서비스 이용 방지 불가

기존의 IPTV의 방송 콘텐츠는 멀티캐스트 방식을 이용하여 사용자에게 전송한다. 멀티캐스트 방식은 동일 네트워크에 여러 사용자가 있는 경우 하나의 전송으로 모두 수신할 수 있는 특징을 가지고 있다. 현재 콘텐츠 보호를 위해 제한수신 시스템, 스크램블링 시스템 기능 등으로 정당한 사용자의 경우에만 시청이 가능하도록 하고 있지만, 이와 같은 특징으로 인해 정당하지 않은 사용자가 셋톱박스 인증을 위한 스마트카드 복제 및 불법적인 복호화 등을 통해 서비스를 이용하는 경우가 발생할 수 있다. 이와 같은 문제는 단순히 불법적인 서비스 이용뿐만 아니라 정당한 사용자로 위장하여 멀티미디어 콘텐츠 결제 등 금전적인 손실을 가져올 수도 있다.

따라서 기존의 셋톱박스를 통한 단일 인증은 취약하기 때문에 가입자 정보를 기반으로 채널 인증을 하는 방식 등을 통하여 동일 네트워크의 다른 사용자가 접근하는 것을 방지하여야 한다.

3.2 시스템 공격에 대한 대응 방안 미비

셋톱박스를 통하여 사용자 인증 및 콘텐츠를 제공함에 따라 특정 공격으로 셋톱박스의 취약점이 노출된 경우, 모든 셋톱박스와 관련 기능을 갱신하거나 교체해야하는 문제점이 발생할 수 있다. 개별적인 가정의 모든 셋톱박스에 대하여 이를 수행하는 것은 상당한 어려움이 따른다. 때문에 수신 제한 시스템을 개발하는 많은 기업들은 케이블카드(스마트카드의 일종)에 관련 모듈을 탑재하고 해킹 등의 문제점이 발견되면 케이블카드를 교체하는 방식을 취하고 있다.

그러나 이와 같은 방식으로도 모든 셋톱박스의 케이블카드를 교체해야한다는 불편함이 따른다. 따라서 한 번에 이와 같은 문제점을 해결하기 위한 시스템 구성이 필요하고, 통합적인 유지 보수 관리가 필요하다.

3.3 셋톱박스로 인한 개별적 사용자 인증 불가

현재의 IPTV는 기존의 TV에 셋톱박스를 연결하여 수신기로 활용하고 있으며, IC 카드, Java 카드, 하드웨어 등을 통해 정당한 사용자를 인증하고 방송 콘텐츠를 제공하고 있다. 따라서 개별적인 사용자 인증을 수행하지 못하고 하나의 인증 수단으로 가정 내 모든 인원이 콘텐츠를 시청하게 된다.

이와 같은 문제점은 제3자가 지불하지 않은 콘텐츠를 이용하거나, 미성년자가 시청할 수 없는 채널을 시청하는 등의 문제를 발생시킬 수 있다. 또한, 개별적인 사용자 인증이 불가능하기 때문에 사용자의 취향 및 과거 시청 내역 등을 통한 맞춤형 서비스 등을 제공하기 어려워진다. 따라서 개별적 사용자 인증을 위한 인증 수단 및 프로세스, 접근 제어 기술 등이 필요하다.

3.4 방송 단말 사이의 상호 호환성 부재

IPTV 서비스를 제공하는 방송 통신 사업자들은 방송 콘텐츠 제공 및 수신 제한을 위하여 자체적인 셋톱박스를 개발하여 사용하고 있다. 그러나 각 방송 통신 사업자가 제공하고 있는 셋톱박스는 동일한 콘텐츠를 제공하더라도 서로 다른 수신 제한 기술을 사용하고 있기 때문에 호환성의 문제가 있다. 이러한 문제점은 IPTV 사용자가 통신 사업자를 변경할 경우, 매번 셋톱박스를 새로 구입해야하는 문제점이 발생한다. 또한 상이한 내부 구조로 인해 동일한 수준의 보안 서비스를 제공하기 어렵다는 문제점도 존재한다.

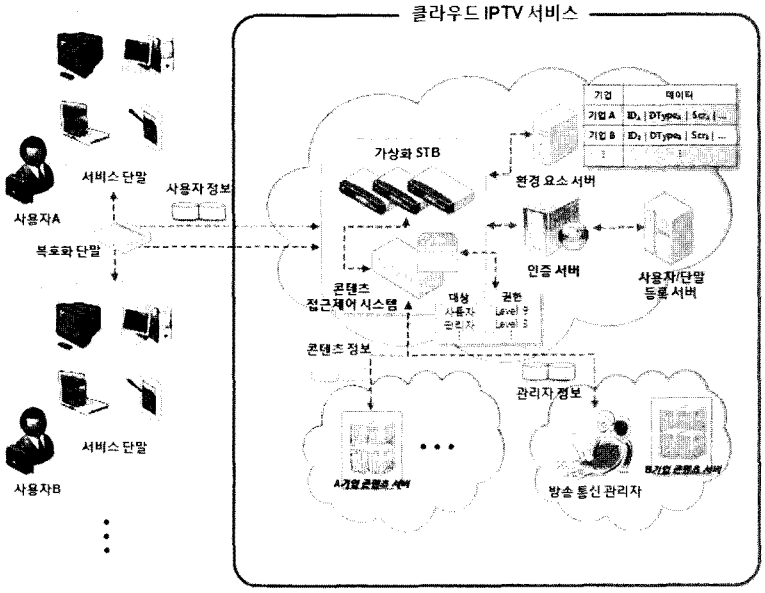
따라서 통신 사업자에 따라 다양한 형태의 수신 제한 서비스 및 접근 제어 기술을 적용하더라도 사용자는 추가적인 셋톱박스 구매 없이 해당 보안 기술을 기반으로 하는 방송 콘텐츠를 제공받을 수 있는 구성 기술이 필요하다.

IV. 제안 방안

4.1 제안하는 IPTV 서비스 및 셋톱박스 구성

본 논문에서는 IPTV 서비스의 개별적 사용자 인증 및 서비스 제공과 각 방송 통신 사업자들 간의 호환성 해결을 위하여 IPTV의 셋톱박스를 클라우드 환경에서 가상화하는 방안을 제안한다. [그림 3] 은 제안하는 IPTV 서비스의 구성도를 나타낸다.

기존의 IPTV 서비스는 방송 통신 사업자가 전송하는 콘텐츠를 처리하여 사용자에게 보여주고, 정당한 사용자만 이용 가능하도록 하기 위하여 셋톱박스를 각 단말에 연결하도록 하였다. 그러나 이러한 경우, 사용자 개개인의 인증 및 서비스 제공이 불가능하고 방송 통신 사업자간 상호 호환성이 없어 보안성 및 효율성



〔그림 3〕 제안하는 IPTV 서비스 구성도

측면에서 문제점이 발생하였다. 이를 해결하기 위하여 사용자의 최종 단말에 사용자 정보 전송 및 콘텐츠 디스크램블/복호화, 그리고 압축된 영상 복원을 위한 역할만 수행하는 모듈을 포함한다.

제안하는 IPTV 서비스는 클라우드 환경에서 가상화된 셋톱박스를 구성하며, 다음과 같이 5가지 모듈이 포함된다.

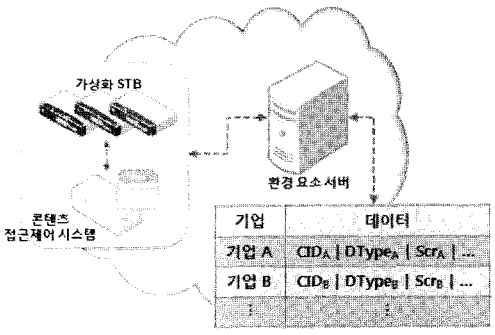
〔표 1〕 가상화 셋톱박스 모듈 구성

모듈	역할
셋톱박스 환경 구성 모듈	방송 통신 사업자 마다 상이한 콘텐츠 제공 방식 및 구성 형태를 선택하여 셋톱박스에 설정되도록 하는 모듈
암호 모듈	사용자/방송 통신 사업자와 클라우드 환경 간 안전한 채널 형성을 위한 암호 모듈
스크램블/압축 모듈	방송통신 사업자가 전송한 콘텐츠를 사용자에게 전송하기에 앞서 지불되지 않은 콘텐츠를 스크램블 및 압축하는 모듈
보안 채널 연결 모듈	사용자 복호화 단말과 방송 통신 사업자의 콘텐츠 정보를 각각 검증하여 세션 연결 승인 및 거절을 위한 모듈
접근제어 모듈	사용자 및 방송 통신 사업자가 셋톱박스에 접근하여 자신이 원하는 일정 범위(콘텐츠 결제, 삭제, 추가 등)의 기능을 수행하고자 할 때, 접근 제어 수행 모듈

4.1.1 셋톱박스 환경 구성 모듈

셋톱박스 환경 구성 모듈은 기존의 서로 상이한 방송 통신 사업자들의 셋톱박스 구성 형태 및 전송 방식 등에 대한 정보를 통하여 셋톱박스 환경을 구성하는 역할을 수행한다. 이와 같은 방식은 어떠한 방송 통신 사업자가 추가되더라도 별도의 환경 구성 및 처리 절차 없이 정보 교환만으로 추가를 가능하게 한다. 사용자 또한 별도의 환경 설정 및 단말 변경 없이 방송 통신 사업자간의 이동이 자유롭다.

이를 위하여 가상화된 셋톱박스는 제안하는 IPTV 환경에서 환경 요소 서버와 연계되어 서비스 제공 환경을 구성한다. 환경 요소 서버에는 사업자 고유 정보



〔그림 4〕 환경 요소 서버 데이터

와 데이터 구성 형태, 스크램블 방식 등의 데이터가 저장된다. 환경 구성 정보(Com_n)는 다음과 같다.

$Com_n = CID_n | DType_n | Scr_n | Reservation$
CID_n = 방송 통신 사업자 고유 식별 정보
$DType_n$ = 콘텐츠 압축 형식
Scr_n = 스크램블 방식
$Reservation$ = 추가 옵션

4.1.2 암호 모듈

기존의 셋톱박스가 각 가정에서 독립적으로 구성되면서 콘텐츠 복호화 및 디스크램블, 인증 등의 암호 모듈 과정이 상당부분 여기에서 수행되었다. 그러나 본 제안 방식에서는 주요 기능이 클라우드 환경에서 구성되므로 가상화된 셋톱박스와 사용자 간의 안전한 채널 형성이 필수적으로 요구된다. 또한, 방송 통신 사업자가 가상화된 셋톱박스 기반의 IPTV 서비스를 통해 사용자에게 콘텐츠를 제공하므로 이 구간에도 동일한 채널 구성이 필요하다. 따라서 셋톱박스와 사용자/방송 통신 사업자간 보안 채널 형성을 위한 세션 키 생성 및 교환, 관리 등을 수행하는 암호 모듈을 포함한다. 사용되는 키 관리 기술은 업계 표준인 Cisco의 ISAKMP(Internet Security Association and Key Management Protocol)를 준수한다.

4.1.3 스크램블/압축 모듈

방송 통신 사업자가 콘텐츠 제공 시 정당한 사용자만 서비스를 이용할 수 있도록 스크램블/압축 모듈을 이용하여 콘텐츠를 전송한다. 데이터에 대한 스크램블은 기존의 IPTV 서비스에서 제공하고 있는 모든 기술을 적용할 수 있다. 스크램블 모듈은 이와 같은 스크램블 기술을 집합한 형태이며, 사용자에게 가상화된 셋톱박스 제공 시 필요한 기능이 선택되어 제공된다. 스크램블 기술의 선택은 셋톱박스 환경 구성 모듈에 의해 방송 통신 사업자가 제공하는 스크램블 기능을 선택한다. 또한 가상화된 셋톱박스로 인해 클라우드 환경에서 사용자 단말로 콘텐츠가 제공될 때, 대용량의 영상을 전송하게 되므로, 이를 해결하기 위하여 영상의 압축을 함께 수행한다.

이 때, 콘텐츠 압축에 사용하는 정보는 환경 구성 정보에 포함된 콘텐츠 압축 형식($DType_n$)을 따르게 되며, 다른 사용자가 동일 네트워크상에서 콘텐츠를 가로채더라도 이용할 수 없도록 사용자 정보(UID_n)를 키 값으로 사용한다.

4.1.4 보안 채널 연결 모듈

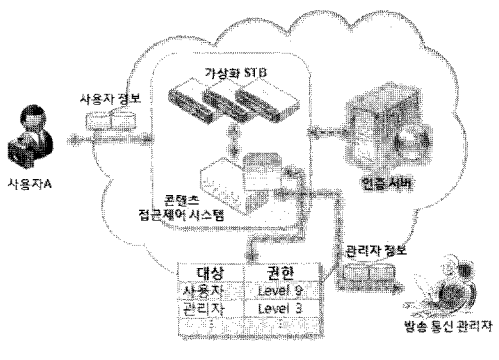
보안 채널 연결 모듈은 사용자 및 방송 통신 사업자와 제안하는 IPTV 환경과의 보안 채널 형성을 위한 기능을 수행한다. 보안 채널 형성 시 사용자와의 채널은 응용프로그램에서의 세션을 구축하고, 방송 통신 사업자와 IPTV 환경간은 전용회선 기반의 세션을 구축한다. 여기에는 암호 모듈을 통한 세션 키와 3계층 터널링 기술인 IPSec(Internet Protocol Security Protocol)을 활용하여 보안 채널을 형성한다.

본 기능은 사용자 단말의 고유 식별 번호(Serial No.) 및 사용자 비밀키와 방송 통신 사업자의 고유 정보 및 비밀키를 활용하여 보안 채널을 형성한다.

4.1.5 접근제어 모듈

사용자 및 방송 통신 사업자가 가상화된 셋톱박스에 접근하여 서비스 이용 및 제공을 수행할 때, 접근 권한에 따라 수행 범위가 상이할 필요가 있다. 이는 사용자에게 개별적인 IPTV 서비스를 제공하기 위해서 필수적인 기능으로, 셋톱박스의 기본적인 연결/변경 등의 설정과 결제된 멀티미디어 콘텐츠, 연령 제한 등 사용자 맞춤형 서비스 제공을 위해 사용된다. 그리고 방송 통신 사업자 내의 다수의 관리자들은 각각의 셋톱박스 구성 변경, 콘텐츠 제공 방식 변경 등의 기능을 권한에 따라 나누어 적용하기 위해 적용된다.

따라서 본 모듈에서는 사용자 개인의 식별 정보, 패스워드를 통하여 사용자 접근 권한을 식별하고, 방송 통신 사업자의 고유 식별 정보, 관리자 식별 정보, 패



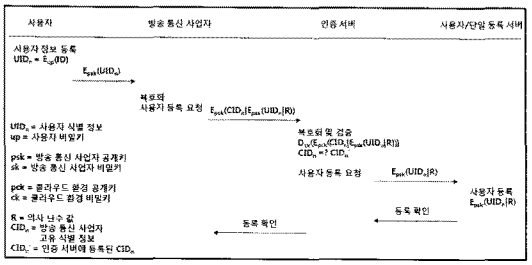
〔그림 5〕 접근제어 모듈 흐름도

스워드를 통해 관리자를 식별한다. 사용자 및 관리자의 권한은 접근 제어 기능에 포함된 권한 제어 리스트와 사용자 인증 서버의 인증 정보를 통해 IPTV 서비스 환경에서 제어된다. 단, 사용자가 이용하는 콘텐츠에 대한 제어는 방송 통신 사업자에서 수행한다.

4.2 사용자/단말 등록 및 인증 절차

인증 서버는 사용자 및 관리자의 신원을 확인하여 정당한 사용자가 서비스를 이용하고 관리자가 서비스를 제어할 수 있도록 하기 위한 기능을 수행한다. 이를 위해 사용자/단말 등록 서버를 두고 사용자 및 관리자와 복호화 단말의 등록 및 삭제 등을 수행한다.

다음은 사용자 등록 절차를 나타낸 것이다.



〔그림 6〕 사용자 등록 절차

전제 조건으로 방송 통신 사업자는 서비스 제공을 위해 셋톱박스 가상화 기반의 IPTV 서비스 환경과 신뢰관계를 맺고 보안 채널이 구성되어야 한다. 이는 방송 통신 사업자의 정보가 해당 환경에 등록됨을 의미한다. 최초 사용자가 IPTV 서비스 이용을 위하여 특정 방송 통신 사업자와 계약을 수행하며 이때, 사용자의 ID가 저장된다. 그 후 사용자의 정보를 암호화하여 사용자/단말 등록 서버에 등록을 수행한다.

사용자는 자신의 ID를 비밀키(up)로 암호화하여 사용자 식별 정보(UID_n)를 생성한다.

$$UID_n = E_{up}(ID) \tag{1}$$

생성된 사용자 식별 정보를 방송 통신 사업자의 공개키(psk)로 암호화하여 전송한다.

$$E_{psk}(UID_n) \tag{2}$$

방송 통신 사업자는 전송된 정보를 복호화하여 사용자 식별 정보와 의사 난수 값(R)을 연접하여 공개키로 재 암호화한다. 그리고 방송 통신 사업자 고유 식별 정보(CID_n)를 연접하여 클라우드 환경 공개키(pck)를 이용하여 암호화 한 후 인증 서버에 전송한다. 의사 난수 값은 암호화된 사용자 식별 정보가 노출되더라도 정확한 식별 정보를 알아낼 수 없도록 하기 위하여 사용된다.

$$E_{pck}(CID_n|E_{psk}(UID_n|R)) \tag{3}$$

인증서버는 이를 복호화한 후 정당한 방송 통신 사업자가 전송한 정보인지를 검증한다. 이 때, 인증서버는 방송 통신 사업자는 클라우드 환경을 통해 서비스를 제공하기 위하여 사전 협약이 완료되어 있으므로 인증 서버가 이에 대한 정보(CID_n')를 가지고 검증할 수 있다.

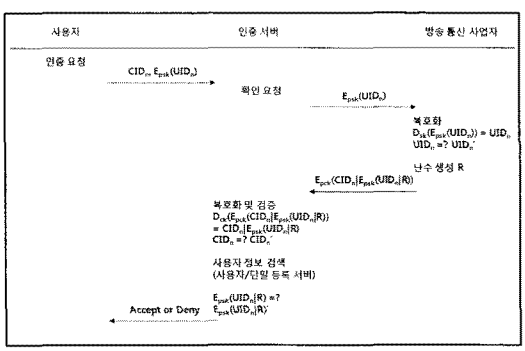
$$\begin{aligned} &D_{ck}(E_{pck}(CID_n|E_{psk}(UID_n|R))) \\ &CID_n = ?\ CID_n' \end{aligned} \tag{4}$$

검증이 완료되면 인증 서버는 사용자 정보를 등록하기 위하여 사용자/단말 등록 서버에 방송 통신 사업자의 공개키로 암호화된 정보($E_{psk}(UID/R)$)를 전송한다. 해당 정보는 방송 통신 사업자의 비밀키 없이는 인증 서버에서 알아낼 수 없으므로 사용자의 개인 식별 정보 노출 및 프라이버시 침해를 방지할 수 있다.

$$E_{psk}(UID_n|R) \tag{5}$$

사용자의 등록이 완료되면 인증 서버 및 방송 통신 사업자는 사용자에게 등록 확인 메시지를 전송한다.

모든 과정이 완료되면 사용자는 단말 등록을 위해 사용자 인증을 수행한다. 다음은 사용자 인증 절차에 대해 나타낸 것이다.



〔그림 7〕 사용자 인증 절차

사용자는 자신의 신원을 인증하기 위하여 방송 통신 사업자의 고유 식별 정보와 해당 사업자의 공개키로 암호화한 사용자 식별 정보를 인증 서버에 전송한다.

$$CID_n,\ E_{psk}(UID_n) \tag{6}$$

인증 서버는 해당 정보가 유효한 방송 통신 사업자의 공개키로 암호화 되었는지 확인하고, 사용자의 신원을 검증하기 위하여 방송 통신 사업자에게 확인을 요청한다.

$$E_{psk}(UID_n) \tag{7}$$

방송 통신 사업자는 이를 복호화하여 사용자의 식별 정보를 알아내고 사전에 등록된 사용자의 정보와 일치하는지 여부를 확인한다.

$$\begin{aligned} &D_{sk}(E_{psk}(UID_n)) \\ &UID_n = ?\ UID_n' \end{aligned} \tag{8}$$

동일한 사용자 정보가 있을 경우, 최초 사용된 의사 난수 알고리즘을 동일하게 사용하여 의사 난수를 생성하고 이를 연접하여 재암호화 한다. 그리고 해당 정보와 방송 통신 사업자의 식별 정보를 연접한 후 클라우드 환경 공개키를 통해 암호화하여 이를 인증 서버에 전송한다.

$$\begin{aligned} &\text{난수 생성 } R \\ &E_{pck}(CID_n|E_{psk}(UID_n|R)) \end{aligned} \tag{9}$$

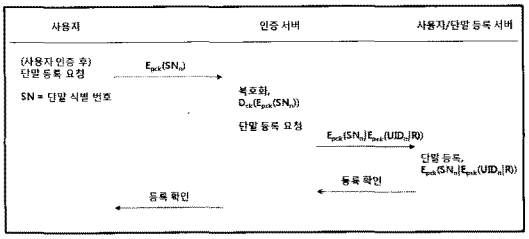
인증 서버는 전송받은 정보를 통해 방송 통신 사업자를 검증하고 사용자/단말 등록 서버에 저장된 정보와 비교하여 사용자를 식별한다. 이는 인증 서버가 방통 통신 사업자와 사용자 모두를 식별하고 이를 통하여 상호 인증이 가능하다. 또한 이를 통해 불법적인 상용자 및 사업자의 접근을 차단한다.

$$\begin{aligned} &CID_n = ?\ CID_n' \\ &E_{psk}(UID_n|R) = ?\ E_{psk}(UID_n|R)' \end{aligned} \tag{10}$$

모든 사용자 및 사업자의 신원 식별이 완료되면 사용자에게 접근 허용 또는 거부 메시지를 전송한다.

다음은 사용자 인증 후, 실제 사용하기 위한 사용자 단말의 등록 절차를 나타내고 있다.

최초 사용자는 자신의 단말 식별 번호(SN)를 클라우드 환경 공개키로 암호화하여 전송한다.



〔그림 8〕 사용자 단말 등록 절차

$$E_{psk}(UID_n) \tag{11}$$

인증 서버는 전송된 정보를 복호화하여 단말 식별 번호를 알아내고 이를 사용자의 식별정보와 난수로 암호화된 정보와 연접하여 재암호화 후 사용자/단말 등록 서버에 전송한다. 사용자를 식별하기 위한 정보를 함께 암호화하면서 인가되지 않은 사용자가 해당 단말을 이용하여 접근하지 못하도록 할 수 있다.

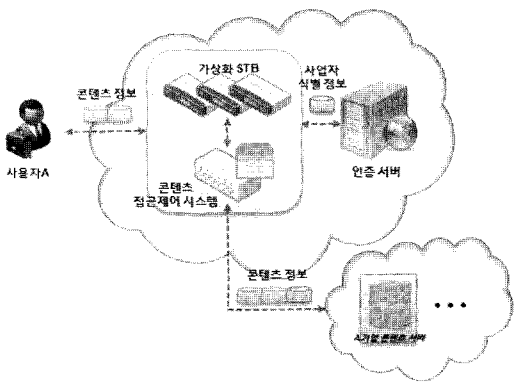
$$E_{pck}(SN_n|E_{psk}(UID_n|R)) \tag{12}$$

사용자/단말 등록 서버는 해당 단말을 서버에 등록하고 이에 대한 등록 확인 메시지를 사용자에게 전송한다.

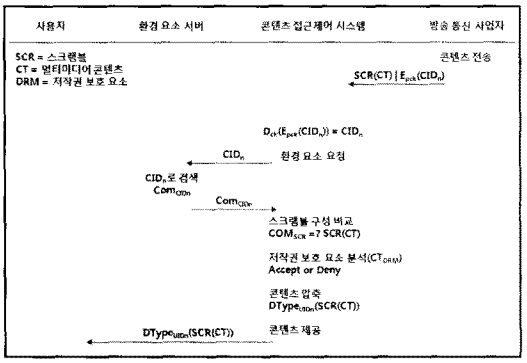
위 절차와 같이 모든 사용자 등록/인증, 단말 등록이 완료되면 멀티미디어 콘텐츠를 제공하기 위한 단계가 수행된다.

4.3 콘텐츠 접근제어 시스템

콘텐츠 접근제어 시스템은 앞서 기술한 사용자와 관리자의 접근제어 기능뿐만 아니라 방송 통신 사업자가



〔그림 9〕 콘텐츠 접근제어 시스템 구성



〔그림 10〕 콘텐츠 접근제어 및 서비스 제공

제공하는 콘텐츠에 대한 접근 허용 및 거부 기능을 포함한다. 보안 채널을 통해 서비스가 제공되지만, 네트워크 취약성 및 악의적인 공격자에 의한 공격 가능성이 전혀 없는 것은 아니기 때문에 정당한 콘텐츠 여부를 검증할 필요가 있다. 이를 위해서는 콘텐츠 정보에 방송 통신 사업자의 정보를 포함하고 이를 검증한다.

방송 통신 사업자는 서비스 제공을 위해 멀티미디어 콘텐츠와 식별 정보를 함께 보내게 되고 제안하는 IPTV 서비스 환경에서는 식별 정보 추출 후 인증 서버에 보낸다. 인증 서버는 방송 통신 사업자 목록에서 정당한 사업자임을 확인하여 알려준다. 콘텐츠 접근제어 시스템은 전송된 콘텐츠 정보의 환경 설정 정보와 사업자가 설정한 환경 정보가 동일한지 확인하고, 사업자마다 설정한 저작권 보호 요소를 확인한다. 이를 통해 정당한 콘텐츠 여부를 확인한다. 이를 완료하면 콘텐츠 전송을 위하여 환경요소에 포함된 콘텐츠 압축 형식에 따라 압축을 수행한다. 이 때, 사용자 정보를 키를 이용하여 동일 네트워크상의 다른 사용자가 콘텐츠 가로채기 공격을 시도하더라도 압축을 해제하고 콘텐츠를 이용할 수 없도록 한다.

V. 안전성 및 효율성 분석

□ 비합법적인 사용자 서비스 이용 방지

현재 IPTV 서비스는 방송 통신 사업자가 멀티미디어 콘텐츠를 동일 네트워크에 멀티캐스트 방식으로 전송한다. 따라서 동일 네트워크 내에 있는 모든 사용자의 셋톱박스에 콘텐츠가 전송되나, 인증을 거친 정당한 셋톱박스만 콘텐츠를 이용할 수 있다. 이는 셋톱박스를 인증하기 위한 정보를 위조하거나, 콘텐츠를 불법으로 복호화 하여 서비스를 이용하는 등에 문제를 발생시킬 수 있다. 그러나 본 논문의 제안 방식에서는 콘텐츠를 개별 사용자에 따라 특정 사용자에게만 전달하고, 압축형식과 사용자 정보 키를 이용한 암호화 통하여 비합법적인 서비스 이용을 방지할 수 있다.

멀티미디어 콘텐츠는 특정 사용자에게만 전달되기 위하여 사용자의 단말 식별 번호(SN)와 사용자 정보(UID_n)가 이용되며, 타 사용자의 단말 식별 정보 및 사용자 정보가 이와 상이하므로 해당 콘텐츠를 사용할 수 없다. 또한, 콘텐츠가 가상화된 셋톱박스에서 재압축되어 전송될 때 콘텐츠 압축 형식($DType_n$)과 사용자 정보가 키로 활용되므로, 콘텐츠를 도청하여도 해당 정보를 알 수 없어 사용할 수 없다.

□ 셋톱박스 시스템 공격으로 인한 갱신/변경 문제 해결

현재 IPTV 서비스는 콘텐츠 제공을 위하여 셋톱박스에 하드웨어 모듈을 포함하거나 케이블카드에 관련 모듈을 탑재하여 삽입하는 방식을 이용하고 있다. 그러나 셋톱박스의 취약점을 통한 해킹, 악성코드 등이 발생할 경우에는 모든 셋톱박스 관련 기능을 갱신하거나 제품 자체를 교체해야하는 문제점이 발생할 수 있다. 그러나 본 제안 방식에서는 셋톱박스의 기능은 가상화를 통하여 제공하고 콘텐츠 복호화 및 디스크램블 등으로 최소화한 사용자 단말을 통해 콘텐츠를 이용하도록 하여, 셋톱박스에 대한 공격으로 인한 갱신, 변경 등의 문제점을 해결한다.

멀티미디어 콘텐츠를 복원하기 위한 콘텐츠 압축 형식은 사용자의 키를 이용하여 압축 후 콘텐츠와 함께 전송($DType_{UIDn}(SCR(CT))$)된다. 따라서 악의적인 공격자가 사용자 단말에 대한 변경을 수행하더라도 전송되는 정보를 통해 정상적으로 복원이 가능하다.

또한, 사용자 단말을 사용할 수 없도록 만들어도 기존의 모든 모듈의 변경 없이 적은 수의 모듈 변경 및 갱신으로 처리가 가능하다. 마지막으로 가상화되어 있는 셋톱박스에 대한 직접적인 공격이 발생하더라도 가상화된 다른 셋톱박스를 통해 서비스 제공이 가능하므로 서비스 가용성 측면도 향상된다.

□ 개별적 사용자 인증 및 서비스 제공

기존의 IPTV 서비스의 경우, 사용자 인증 및 양방향 서비스 제공을 위해 단말에 설치한 셋톱박스에 IC 카드, 자바카드, 하드웨어 모듈 등을 이용한다. 이와 같은 방식은 사용자 개개인을 식별하고 서비스를 제공

〔표 2〕 안전성 및 효율성 분석

	기존 IPTV 서비스	제안하는 IPTV 서비스	관련 요소
비합법적인 사용자 서비스 이용 방지	- 멀티캐스트 전송 방식 - 동일 네트워크의 모든 사용자에게 콘텐츠 전송 - 셋톱박스 인증 정보 위조 가능 - 콘텐츠 불법 복호화 가능	- 특정 사용자에게만 콘텐츠 전송 - 단말 정보 및 사용자 정보를 통한 개별 인증 - 사용자 정보를 가상화 환경에 전송하여 인증하므로 사용자 단말의 복제 무의미 - 사용자 키로 암호화된 콘텐츠 압축 형식을 통해 콘텐츠 복호화 방지	- 단말 식별 번호(SN) - 사용자 정보(UID_n) - 콘텐츠 압축 형식 ($DType_n$)
셋톱박스 시스템 공격으로 인한 갱신/변경 문제 해결	- 셋톱박스 시스템에 직접적인 공격 가능 - 내부 모듈 정보의 임의 변경 및 악성코드를 통한 공격 가능 - 셋톱박스 문제 발생 시 하드웨어 변경 또는 기능 갱신 필요	- 셋톱박스 가상화로 특정 가상 셋톱박스 공격 시 교체가 간단함 - 셋톱박스 교체로 인한 서비스 중지 없음(다른 셋톱박스를 통해 전송) - 사용자가 직접 셋톱박스에 대한 물리적인 갱신/변경 필요 없음	- 콘텐츠 압축 형식 ($DType_n$) - 가상 셋톱박스 - 사용자 정보(UID_n)
개별적 사용자 인증 및 서비스 제공	- 셋톱박스 인증을 통한 콘텐츠 제공 - 개별적인 사용자에 대한 인증 및 서비스 제공 불가 - 동일 셋톱박스를 이용하는 다양한 사용자에 대한 개별적 접근제어 불가(연령 제한 등) - 제한적인 양방향 통신 수행 - 셋톱박스 단위의 정보 수집만 가능	- 사용자 정보를 기반으로 개별적 사용자 인증 및 서비스 제공 가능 - 개인 단위의 정보 수집 및 특화 서비스 제공 가능 - 진정한 양방향 서비스 제공 가능 - 연령 제한과 같은 콘텐츠 접근 제어 가능	- 사용자 정보(UID_n) - 사용자 비밀키(up) - 콘텐츠 압축 형식 ($DType_n$)
사업자간 호환성 제공	- 독자적인 서비스 제공으로 셋톱박스가 상이함 - 사업자 변경 시 셋톱박스 변경 필수 - 셋톱박스 재활용이 제한적	- 셋톱박스 구성 환경 변경용이 - 가상화된 셋톱박스에 환경 구성을 변경함으로써 동일한 단말로 접근 가능 - 사업자 변경 시 별도의 시스템 변경 없음 - IPTV 사업자가 지원하는 세톱박스의 추가, 삭제, 변경용이	- 환경 구성 정보(com_n) - 방송 통신 상업자 고유 식별 정보(CID_n)

하는 것이 아니기 때문에 한정적인 양방향 서비스를 제공한다. 즉, 사용자 개인에 대한 식별 보다는 서비스 이용이 가능한 단말임을 인증한다고 할 수 있다. 사용자가 이용하는 콘텐츠 정보를 수집하고 서비스를 제공할 수는 있지만, 사용자 개인의 취향, 성향, 등에 따른 서비스 제공이나 연령 제한에 따른 서비스 제공 등의 차별화된 서비스를 제공하기 어렵다. 그러나 본 논문에서 제안한 방식은 사용자 정보와 단말의 정보를 통해 개별적인 인증과 서비스를 제공할 수 있다.

IPTV의 콘텐츠는 사용자 요청에 따라 각각 암호화 및 압축 과정을 거치므로 이를 위해 사용된 사용자 비밀키(up)를 알아야만 이용할 수 있다. 또한, 사용자의 연령에 따라 이용 가능한 콘텐츠의 제한을 위한 접근제어 모듈이 가상화된 셋톱박스에 존재하므로 정당하지 않은 사용자의 단말까지의 전송 자체를 차단할 수 있다. 이처럼 개별적인 인증 과정을 이용함으로써 성향, 취향 등의 정보를 수집하여 개별적인 서비스를 제공하고 진정한 양방향 서비스를 제공할 수 있다.

□ 사업자간 호환성 제공

IPTV 서비스 이용을 위해서는 셋톱박스 설치가 필수적인데, 현재 IPTV 서비스를 제공하는 사업자들은 독자적으로 구성한 셋톱박스를 제공하고 있다. 따라서 특정 셋톱박스는 특정 방송 통신 사업자가 전송하는 데이터만 이용할 수 있다. 이는 서비스 제공 사업자간 보다 좋은 서비스 제공을 위한 셋톱박스 개발 등의 이점을 가져올 수 있지만, 방송 통신 사업자 변경 시 항상 새로운 셋톱박스를 설치해야하는 번거로움이 발생된다. 또한, 기존의 셋톱박스 재활용이 제한되는 등

효율성이 좋지 못하다. 그러나 본 제안 방식에서는 사용자가 이용하는 방송 통신 사업자의 셋톱박스 구성 환경을 클라우드 환경에서 가상화하여 제공하므로 구성 변경이 용이하며, 방송 통신 사업자를 변경하더라도 셋톱박스의 직접적인 변경 없이 서비스를 이용할 수 있다.

사용자는 단순 복호화 및 디스크램블 단말만 사용하므로 셋톱박스에서 전송되는 정보에 포함된 환경 구성 정보(com_n)를 통해 단말의 변경 없이 콘텐츠를 정상적으로 이용할 수 있다. 또한, 가상화된 셋톱박스를 통한 서비스 제공은 방송 통신 사업자가 독자적으로 지원하는 셋톱박스의 추가, 삭제, 변경이 용이하며, 기존의 셋톱박스 구성 형태의 변경 없이 적용할 수 있다.

VI. 결론

초고속 인터넷과 방송 통신의 융합으로 인해 IPTV 서비스가 제공되면서 많은 사용자들이 안전하고 효율적인 서비스를 제공받고자 하는 요구가 증가하게 되었다. 또한, 차별화된 개별 서비스 제공에 대한 기대 증가와 서비스 이용 시 발생할 수 있는 문제점들에 대한 요구도 증가하였다.

IPTV 서비스가 셋톱박스와 네트워크를 통한 양방향 통신을 통해 다양한 서비스를 제공받게 되었으나, 방송 통신 사업자의 콘텐츠 제공 환경이 다르고, 셋톱박스 구성 형태 등이 달라 타 서비스 업체 간의 호환성 문제가 대두되었다. 또한, 개별적으로 사용자를 인증하는 것이 아니라 셋톱박스의 인증 모듈을 통해 서비스가 제공되면서, 정당하지 않은 사용자가 특정 콘텐츠에 접근하는 등 사용자 인증 및 개별적 서비스에 대한 문제점도 발생하였다. 이와 같은 문제점들은 IPTV 서비스의 발전에 악영향을 미치며, 보다 효율적인 서비스 제공을 어렵게 하고 있다.

따라서 본 논문에서는 이를 해결하기 위해 셋톱박스를 클라우드 환경에서 가상화하여 방송 통신 사업자 간 호환성을 향상시키고, 개별적 사용자 인증을 통한 보안성 및 개별적 IPTV 서비스 제공이 가능한 시스템을 제안하였다.

제안 방식을 통하여 사용자가 IPTV 서비스를 이용할 때, 방송 통신 사업자를 변경하더라도 별도의 시스템 및 셋톱박스 변경 없이 서비스 이용이 가능하여, 서비스 제공에 대한 가용성을 제공할 수 있다. 그리고 사용자 정보를 기반으로 개개인을 인증하고 서비스를 제공함으로써 정당한 사용자에 대한 식별성 향상 및 개별적 서비스 제공이 가능하다. 이를 통해 콘텐츠 제공 시 불법적인 접근 및 사용을 방지하고, 사용자의 셋톱박스 변경에 따른 불편과 방송 통신 사업자의 서비스 제공에 대한 문제점 해결 등의 보안성 및 효율성을 향상 시킬 수 있을 것으로 기대된다.

참고문헌

[1] ATIS, "IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification," ATIS-0800006, 2007.

[2] 최현우, 정영곤, 염홍열, "(Mobile) IPTV 보안 기술 및 표준화 동향," 한국정보보호학회지, 20(2), pp. 65-77, 2010년 4월.

[3] 정윤수, 정윤성, 김용태, 박길철, 이상호, "IPTV 환경에서 가입자의 인증 상태정보를 이용한 인증 보안 모델 설계," 한국통신학회논문지, 35(3), pp. 421-430, 2010년 3월.

[4] WiMAX Forum Network Working Group, "WiMAX Forum Network Architecture-Stage 3: Detailed Protocols and Procedures-Release 1, Version 1.2," WiMAX Forum, Jan 2008.

[5] EBU Project Group B/CA, "Functional model of a conditional access system," EBU Technical Review, pp. 64-77, Winter. 1995.

[6] 여상수, "SDCS: 유비쿼터스 환경의 안전한 콘텐츠 다운로드를 위한 안전한 D-CAS 시스템," 한국멀티미디어학회 논문지, 13(2), pp. 249-257, 2010년 2월.

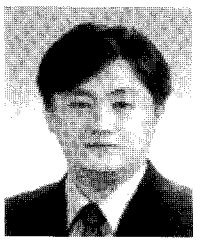
[7] Dave Thomas, "Enabling Application Agility-Software as a Service, Cloud Computing and Dynamic Languages," Journal of Object Technology, Vol. 7, No. 4, pp. 29-32 , May-Jun. 2008.

[8] George Lawton, "Developing Software Online with Platform-as-a-Service Technology," IEEE Computer Society, pp. 13-15 , Jun. 2008.

[9] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," Dec. 2009.

〈著者紹介〉

고 웅 (Woong Go) 학생회원
2008년 2월: 순천향대학교 정보보호학과 졸업
2010년 2월: 순천향대학교 정보보호학과 석사
2010년 3월~현재: 순천향대학교 정보보호학과 박사과정
〈관심분야〉 클라우드 컴퓨팅, IPTV, 정보보호, 개인정보보호, 융합보안 등



곽 진 (Jin Kwak) 종신회원
성균관대학교 (공학사 공학석사, 공학박사)
2006~2006년: 일본 큐슈대학교 방문연구원
2006~2006년: 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007년: 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009년: 정보통신연구진흥원 집필위원
2007~현재: 순천향대학교 정보보호학과 교수
2009~2009년: 순천향대학교 공과대학 교학부장
2009~2010년: 순천향대학교 정보보호학과 학과장
2010~2010년: 교육과학기술부 국가기술수준평가 전문위원
현재: 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장
〈관심분야〉 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등