# IPTV 서비스를 이용하는 사용자의 효율적인 성인인증 모델 설계

정윤수* · 김용태**

# Design of Efficient Adult Authentication Model for prevent of illegal Service of Child in IPTV Service Environment

Yoon-Su Jeong* · Yong-Tae Kim**

본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.


## 요 약

최근 멀티미디어 콘텐츠를 초고속 인터넷, 케이블 TV 망 그리고 위성 망 등을 통해 실시간으로 전송되는 IPTV 서비스가 각광을 받고 있다. 그러나 다양한 매체를 통해 사용자에게 서비스를 제공하는 IPTV 서비스는 사용자 인증을 완벽하게 지원할 수 없는 문제가 있다. 본 논문은 IPTV 환경에서 청소년이 IPTV 콘텐츠를 제공받기 위해서 불법적으로 성인 인증 정보를 IPTV 콘텐츠 서버에 전송하여 IPTV 서비스의 접근 허가를 부여받는 것을 예방하는 인증 모델을 제안한다. 제안 모델은 기존 IPTV 환경에서 수행하고 있는 단순 성인 인증 시스템의 단점을 극복하기 위해서 IPTV 콘텐츠 서버에 사용자의 등급 분류 체계를 갖추고 IPTV 콘텐츠 서버와 인증 서버의 데이터베이스에 저장된 사용자 인증 정보를 동기화하여 성인 인증 과정을 수행한다. 또한, 제안 모델은 이중 해쉬 체인 기법을 적용하여 IPTV 콘텐츠 관리자의 승인키를 청소년이 불법적으로 획득하더라도 관리자의 동의없이 콘텐츠를 불법적으로 다운로드 하지 못하도록 하고 있다.

## ABSTRACT

Recently IPTV that transmits multimedia contents in real time through internet, cable TV net and satelite net gets the limelight. But IPTV service that gives service to users by various media has a problem of not supporting user certification fully. This paper suggests a certification model which prevents getting access permission of IPTV service by sending illegal certification information by adolescent through integrating mobile communication technique with RFID(Radio Frequency IDentification) technique which is a key technique of Ubiquitous environment. This model performs the process of adult certification by keeping synchronization with user's certificaiton information that is saved in data-base of certification server and contents server after getting the system of class categorization in contents server to overcome disadvantage of simple adult certification system that is popular in the existing internet. Also, it adapts double hash chain technique not to down load illegally contents without the permission of manager even if an adolescent gets manager's approval key.



키워드

IPTV 서비스, 인증, RFID, 프로토콜

Key word

IPTV Service, Authentication, RFID, Protocol



* 정회원 : 목원대학교 정보통신공학과 교수 (제1저자, bukmunro@gmail.com)

** 정회원 : 한남대학교 멀티미디어학부 교수 (교신저자)



접수일자 : 2012. 10. 18

심사완료일자 : 2012. 11. 14

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.1.68



ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

## Ⅰ. 서 론

최근 대용량의 동영상 정보를 집안에서 편리하게 송・수신할 수 있는 IPTV(Internet Protocol Tv)가 이동통신 기술의 발전과 함께 각광을 받고 있다[1]. IPTV 기술은 기존 초고속 인터넷망을 기반으로 고선명 동영상 서비스를 가정의 TV와 연결하여 제공하는 서비스로 주문형 서비스(Video on Demand, VOD) 뿐만 아니라 위성 DMB, 지상파 DMB 등의 방송 서비스를 인터넷 환경에서 제공하는 방송기술을 의미한다[2].

IPTV 시스템은 플랫폼(headEnd), IP 네트워크, 단말장치 등으로 구성되며, IPTV 시스템은 Triple Play의 서비스를 제공할 수 있는 장비로 [그림 1]과 같이 IPTV 시스템이 구성된다.

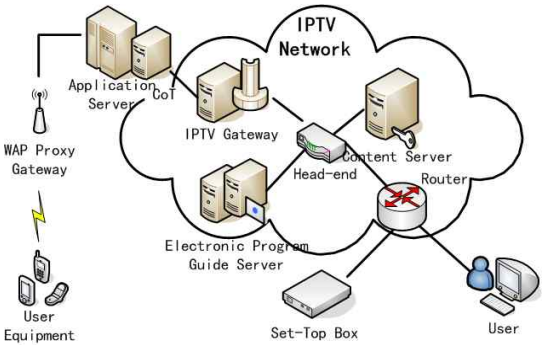


그림 1. IPTV 시스템의 기본 구성
Fig. 1 Structure of IPTV System

휴대전화와 같은 통신기술이 발전함에 따라 사용자는 휴대폰에 RFID 리더를 탑재하여 사용자의 지리적 위치에 상관없이 IPTV 서비스를 제공받고 있다. IPTV 서비스는 개인 단위의 미디어 특성을 갖는 것과는 달리 일반적인 TV처럼 가구중심 단위의 미디어 특성을 갖고 있어 사용자 인증의 문제점을 가지고 있다. IPTV 서비스는 기존 인터넷 서비스와 유사한 플랫폼 환경으로 서비스가 제공되고 있기 때문에 다른 플랫폼 기반으로 사용자 개별 인증이 가능하다.

IPTV 서비스는 기존 방송 서비스보다 다양한 콘텐츠를 제공하고 있어 청소년이 부모의 동의없이 부모의 권한정보를 이용하여 IPTV 콘텐츠 서비스를 불법적으로 이용하는 경우가 많다. 불법적으로 IPTV 서비스를 제공받으려는 청소년의 인증처리 문제를 해결하기 위해서는 휴대전화와 같은 이동통신장비에 RFID 기술과 청소년의 성인인증 기술을 적용하여 IPTV 서비스를 제공할 필요가 있다[3,4,5,6].

IPTV 서비스에서 수행되고 있는 성인 인증은 주민등록번호를 이용하는 방식을 사용하고 있다. 이 방식은 주민등록번호만을 이용하여 주민등록번호 알고리즘에 적용하는 단순 계산 방법, 이름과 주민등록번호를 갖고 금융정보기관에 문의하는 방법, 실명 이름을 입력하여 로그인(log-in)를 수행하는 방법 등 3가지고 있다. 그 이외에 휴대전화번호, 공인인증서를 이용하는 방법도 있다. 그러나 IPTV 콘텐츠를 제공받으려는 청소년이 부모의 성인 인증 정보를 우회적으로 획득할 경우 기존 방법에서 행해지고 있는 성인 인증과정은 무의미하게 된다[7,8,9].

이 논문에서는 유비쿼터스 환경의 핵심 기술인 RFID(Radio Frequency IDentification) 기술과 이동통신 기술의 접목하여 IPTV 환경에서 청소년이 불법적으로 성인 인증 정보를 전송하여 IPTV 서비스의 접근 허가를 부여받는 것을 예방하는 인증 모델을 제안한다. 제안 모델은 기존 인터넷에서 수행하고 있는 단순 성인 인증 시스템의 단점을 극복하기 위해서 콘텐츠 서버에 등급 분류 체계를 갖추고 콘텐츠 서버와 인증 서버의 데이터베이스에 저장된 사용자 인증 정보와 동기화를 유지하여 성인 인증 과정을 수행한다. 또한, 제안 모델은 청소년이 관리자의 승인 키를 불법적으로 획득하더라도 관리자의 동의없이 콘텐츠를 불법적으로 다운로드 못하도록 하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 연구의 동기와 IPTV 서비스에 대해서 알아본다. 3장에서는 IPTV 환경에서 청소년이 불법적으로 성인 인증을 수행하려는 것을 예방하기 위한 인증 모델을 제안한다. 4장에서는 제안 프로토콜의 안전성을 분석하고 마지막으로 5장에서 결론을 맺는다.

## Ⅱ. 관련 연구

### 2.1. IPTV

IPTV(Internet Protocol TV)는 유・무선 IP망에 연

결된 셋탑박스, 단말 등을 통해 TV 수상기로 제공하는 방송형 및 통신형 서비스로써 사용자에 맞는 '개인 맞춤형 서비스'와 '양방향 데이터 서비스'를 제공하는 대표적인 융합 서비스이다[1]. IPTV는 통신사업자 측면에서 기존의 통신서비스 기반 위에 주문형 비디오 (VOD), 디지털영상저장 (DVR) 서비스뿐만 아니라 TV 스크린을 통한 인스턴트 메시지 전송서비스 등을 제공함으로써 단일 회선망을 통하여 데이터, 음성, 영상을 한꺼번에 묶어 동시에 제공한다.

IPTV는 버전에 따라 협의의 IPTV(IPTV 1.0)와 광의의 IPTV(IPTV 2.0)로 구분된다. 협의의 IPTV는 IP-STB을 기반으로 한 거실 TV형 유선방송 서비스를 의미하며, 광의의 IPTV는 ALL-IP 기반의 유선과 무선이 통합된 거실 TV형, 이동 TV형, 유무선 방송 서비스를 의미한다. [그림 2]은 협의의 IPTV의 전체 구성도를 나타내고 있다[1].

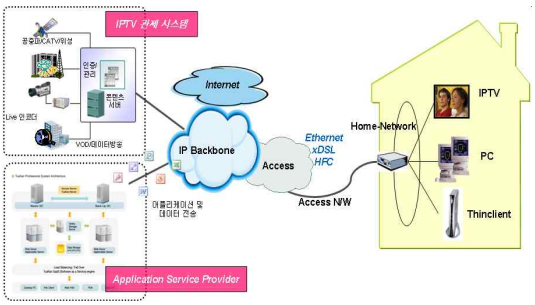


그림 2. IPTV 개요 및 서비스 구성도
Fig. 2 IPTV Concept and Service Constructure

IPTV는 T-Commerce나 온라인 게임, 채팅, 이메일 등의 양방향 서비스가 가능하고, Point-to-Point 전달 방식으로 개인화된 채널을 볼 수도 있다. IPTV는 개인의 취향에 따른 TPS, QPS 등의 제공이 가능하고 그 외 다양한 서비스가 지속적으로 창출될 수 있다.

### 2.2. IPTV 서비스 보안

IPTV 서비스는 사용자와 셋톱박스 사이에서 인증을 수행할 때 데이터가 셋톱박스 내에서 처리되기 때문에 맥코맥 핵 공격에 대한 보안이 취약하다. IPTV 환경에서 맥코맥 핵 공격은 사용자로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 공격을 의미한다.

IPTV 환경에서 발생가능한 공격유형은 [표 1]과 같다. IPTV 서비스 보안과 관련하여 많은 연구자들은 무결성(Integrity), 보안(Security), 감사(Auditing), 프라이버시(Privacy), 부인방지(Non-reputation), 인증(Authentication), 기밀성(Confidentiality), 권한(Authorization), 면역(immunity), 이용성(Availability), 신원확인(Identification) 등의 보안 요소들에 대해 연구해왔다[4,5,10,11].

IPTV 콘텐츠 제공자가 제공하는 콘텐츠를 불법 유출은 일반적으로 영화, 비디오, 방송 등을 이용하여 사용자에게 전송하는 과정 중에 발생한다. 콘텐츠 불법 유출을 예방하기 위해서는 일정 수준 이상의 수신 제한 기술이 요구된다. IPTV 콘텐츠 제공자의 요구에 맞는 수신 제한 기술을 적용하기 위해서 콘텐츠 제공자는 서버 제품과 방송 수신 제어 모듈에 탑재된 단말 및 케이블 카드를 일괄 구입하여 수신 제한 기술을 적용해야 한다.

### 2.3. 논문의 기여

이 논문은 크게 2가지 측면에서 기여가 있다. 첫째, 제안 프로토콜은 RFID 시스템을 사용하여 USN과 같은 환경에 사용하기 위한 안전하고 확장 가능한 보안 프로토콜이며 AES 메커니즘을 사용하기에 적합하다.

표 1. 공격 유형과 보안 요소 분석
Table. 1 Attack Category and Security Component Analysis

| 공격 유형 | 보안 요소 | 새로운 보안 요소 |
|---|---|---|
| Interruption | Access Control | Availability |
| Interception | Access Control, Communication Security | Authorization |
| Modification | Data Confidentiality | Integrity, Privacy |
| Fabrication | Data Confidentiality, Non-Repudiation | Privacy, Authentication, Authorization |

특히, 제안 프로토콜에서는 AES을 사용하는 디바이스가 안전한 통신을 위해 통신 파티 사이에 키 쌍-AES의 경우에 공유된 비밀 키-을 유지하고 분배할 때 오버헤드를 줄이고 있다. 둘째, 제안 프로토콜은 RFID의 동작 속도와 통신량을 향상시키기 위해 태그에서 생성되는 난수를 공장에서 초기 입력한 값과 사용자 자신이 제품을 초기 사용할 때 입력한 값을 조합한 난수를 이용하여 태그에서 생성되는 난수와 관련된 보안 문제점을 해결하고 있다.

## Ⅲ. 성인 인증 서비스를 지원하는 IPTV 시스템 인증 모델 설계

청소년이 불법적으로 사용자의 성인 인증 정보를 전송하여 IPTV 서비스에 접근 허가를 부여받는 것을 예방하기 위한 IPTV 접근 보안 모델을 제안한다. 제안 모델은 기존 인터넷에서 처리되고 있는 성인 인증 시스템의 단점을 극복하기 위해서 콘텐츠에 등급 분류 정보를 추가하여 서비스를 제공받으려고 할 때 인증허가 요청 정보를 사용자에게 전달하여 시스템에 등록되어 있는 정보와 사용자의 인증 권한 위임 정보를 비교하여 정보의 무결성을 보장받을 수 있도록 이중 해쉬 체인 기술을 사용한다.

### 3.1. 제안 프로토콜 설계 구성

제안 프로토콜에서는 청소년이 성인 인증을 불법적으로 수행하지 못하도록 하기 위해서 제안 프로토콜에서는 [그림 3]과 같은 동작을 수행한다. [그림 3]처럼 제안 프로토콜이 RFID 기술을 이용하는 이유는 2가지이다. 첫째, 휴대폰 단말을 사용하는 사용자가 IPTV 서비스를 사용할 때 낮은 통신 오버헤드와 서비스 지연을 제공하기 위해서이다. 둘째, 휴대폰 단말과 RFID 리더 사이에 제안 프로토콜이 XOR 연산을 사용하는 이유는 RFID 태그의 계산 비용을 낮추면서 계산 속도를 높이기 위해서이다.

제안 프로토콜은 [그림 3]처럼 IPTV 콘텐츠 제공자, 셋톱박스, IPTV 인증서버, 데이터베이스, RFID 리더, RFID 태그 등으로 구성된다.

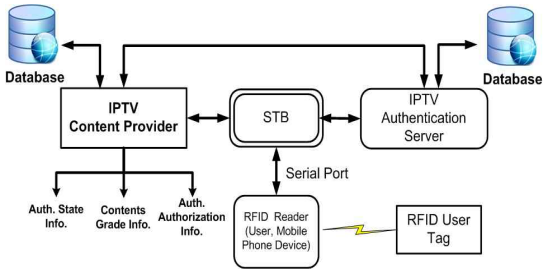


그림 3. 제안 프로토콜의 인터페이스 구조
Fig. 3 Interface Structure of Proposed Protocol

[그림 3]에서 RFID 리더는 사용자 또는 휴대폰 단말의 역할을 수행하며 STB와 직접 시리얼 포트를 통해 연결한다. 만약 RFID 리더가 시리얼 포트를 통해 연결이 안될 경우 USB 포트를 통해 연결을 시도한다. IPTV 콘텐츠 제공자는 RFID 사용자 태그에 포함된 컨텐트 등급 정보를 확인한 후 IPTV 인증서버에게 사용자의 인증 상태와 인증권한의 위임정보를 요청하여 사용자에게 IPTV 콘텐츠를 정상적으로 제공할 것인지를 결정한다. 셋톱박스는 플로그 앤 플레이(Plug and Play) 기능을 통해 RFID 리더를 인식하는 기능을 수행한다. IPTV 인증서버는 RFID 사용자의 정상 유·무를 판별하고, 데이터베이스에게 태그정보와 인증정보의 쌍을 전달하여 저장하도록 한다. 데이터베이스는 RFID 태그정보를 저장하며 RFID 태그 정보는 인식자와 인증정보 쌍으로 구성된다.

### 3.2. 용어 정의

[표 2]는 제안된 프로토콜에서 사용하는 용어에 대한 설명이다.

표 2. 용어 정의
Table. 2 Definition of Terminology

| 용 어 | 정 의 |
|---|---|
| IPTV | 인터넷 프로토콜 TV |
| RFID | 근거리 주파수 인식 장치 |
| TLV | Type, Length, Value의 약어 |
| MCU | 마이크로 회로 장치 |
| PIN | 개인 인식 넘버 |

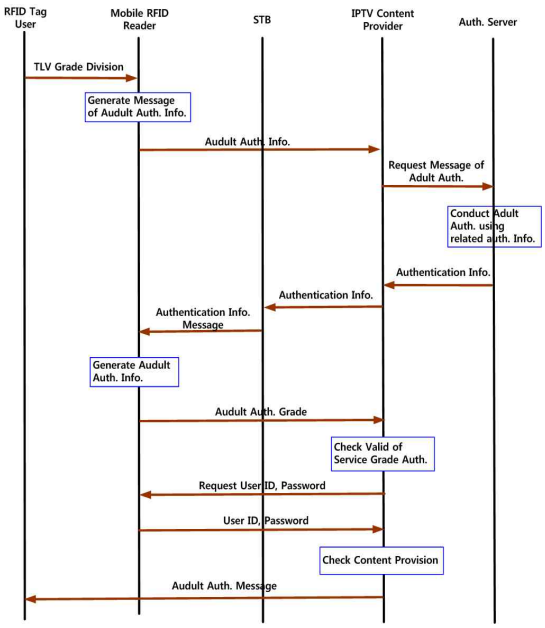


그림 4. 제안 프로토콜의 처리 흐름도
Fig. 4 Process of Proposed Protocol

3.3. 이동 IPTV 환경에서의 성인 인증 프로토콜

제안 프로토콜에서 사용되는 이동 RFID 리더는 성인 인증 기능이 내장되어 있으며, 이 기능을 통해 성인 콘텐츠의 RFID 태그에 기록된 성인인증에 대한 등급정보를 추출한다. 이동 RFID 리더는 RFID 태그로부터 추출된 정보를 이용하여 태그 ID와 성인인증 등급정보를 포함한 정보를 인증서버에게 전달하여 사용자의 성인 인증을 과정을 수행한다. 정상적으로 성인 인증이 수행되면 인증 메시지가 생성되어 생성된 인증 메시지를 콘텐츠 제공자에게 전달한다. 만약 정상적인 성인 인증 과정이 수행되지 못한다면 프로세스는 종료한다. 콘텐츠 제공자는 전달받은 인증 정보를 이용하여 사용자에게 콘텐츠 서비스 유·무를 결정한다. [그림 4]처럼 제안된 성인 인증 시스템의 인증 처리 절차는 다음과 같다.

· 단계 1 : RFID 태그 사용자 → 이동 RFID 리더

사용자는 휴대폰 단말과 같은 장비에 부착된 이동 RFID 리더를 통하여 RFID 태그 내에 포함된 성인 인증 정보를 읽는다. 이 때, 이동 RFID 리더가 읽은 데이터의 각 카테고리 값은 한국정보통신기술협회[7,8]에서 정의한 TLV(Type, Length, Value) 등급 체계 분류로부터 획득할 수 있다.

· 단계 2 : 이동 RFID 리더 → IPTV 콘텐츠 제공자

이동 RFID 리더는 RFID 태그로부터 전달받은 성인 인증 정보 중 태그 ID와 성인 인증 등급정보를 추출하여 메시지를 생성한다. 이동 RFID 리더에 의해 생성된 메시지는 사용자에게 콘텐츠 서비스 제공 유·무를 판별하기 위해서 셋톱박스를 통해 IPTV 콘텐츠 제공자에게 전달한다.

· 단계 3 : IPTV 콘텐츠 제공자 → 인증서버

IPTV 콘텐츠 제공자는 셋톱박스로부터 전달받은 서비스 요청 메시지를 수신 받은 후 인증서버에게 사용자의 성인 인증 요청 메시지를 전달한다.

· 단계 4 : 인증서버

인증서버는 데이터베이스에 저장된 사용자 정보 중 인증 관련 정보(주민번호, 나이 등)를 이용하여 성인 인증을 수행한다.

· 단계 5 : 인증서버 → IPTV 콘텐츠 제공자, 셋톱박스

인증서버로부터 성인 인증이 완료된 후 인증서버는 IPTV 컨텐트 제공자와 셋톱박스에게 인증 정보를 전달한다. STB에게 사용자의 인증정보를 전달하는 이유는 IPTV 콘텐츠 제공자의 부인 방지를 예방하기 위해서이다.

· 단계 6 : 이동 RFID 리더 → IPTV 콘텐츠 서버

셋톱박스로부터 인증정보 메시지를 수신한 이동 RFID 리더는 수신된 메시지를 해석하여 카테고리 값을 얻는다. 이동 RFID 리더는 카테고리 값을 이용하여 사용자의 성인인증 등급을 생성한다. 이동 RFID 리더는 생성된 성인인증 등급을 셋톱박스를 통해 IPTV 콘텐츠 서버에게 전달한다.

· 단계 7 : IPTV 콘텐츠 서버 → 이동RFID 리더

IPTV 콘텐츠 서버는 셋톱박스로부터 전달받은 성인 인증 등급 메시지를 최종 등급 결정 정책에 따라 최종 등급과 태그 ID를 서비스 등급 인증의 유효성 검사를 수행한다. IPTV 콘텐츠 서버는 사용자의 서비스 등급 인증

의 유효성 검사를 위해 사용자에게 ID와 패스워드의 입력을 요청한다.

· 단계 8 : 이동 RFID 리더 → IPTV 콘텐츠 서버

이동 RFID 리더는 IPTV 콘텐츠 서버의 요청에 따라 사용자의 ID와 패스워드를 입력한다. IPTV 콘텐츠 서버는 IPTV 콘텐츠 서버의 데이터베이스에 저장되어 있는 사용자의 주민번호와 ID를 조회하여 사용자의 성인 유·무를 판별한다. 이 때, IPTV 콘텐츠 서버는 최종 등급과 사용자의 나이를 통해 해당 콘텐츠 제공 유·무를 결정한다.

· 단계 9 : IPTV 콘텐츠 서버 → 사용자

IPTV 콘텐츠 서버는 결정된 성인 인증 메시지를 이동 RFID 리더에게 전달한다. 이동 RFID 리더는 사용자에게 IPTV 콘텐츠 서버로부터 전달받은 성인 인증 확인 메시지를 사용자에게 전달한다. IPTV 콘텐츠 서버는 성인 인증 판단 결과에 따라 사용자에게 해당 콘텐츠를 제공하거나 제공하지 않는다.

## Ⅳ. 평가

IPTV 서비스를 제공하는 환경에서 제안 프로토콜의 안전적인 성인인증을 위해 제사용 공격, Forward 보안, RFID 태그 추적, 맥코맥 핵 공격 등에서 평가한다.

### 4.1. 재사용 공격

제안 프로토콜에서는 이동 RFID와 셋톱박스가 논리적으로 동작하면서 다수의 RFID 태그와 연동하고 있다. 이 때, 셋톱박스는 제3자에게 노출되지 않도록 이동 RFID 리더가 범위 안에 접근할 때마다 이동 RFID 리더의 ID와 RFID 사용자 태그가 생성한 랜덤수를 해쉬한 토큰값을 암호화한다. 또한, 셋톱박스는 사용자의 성인등급 정보를 IPTV 콘텐츠 서버와 인증서버에게 전달하는 게이트웨이 역할을 함으로써 IPTV 콘텐츠 서버와 인증서버와의 인증과정을 통해 제3자가 인증 정보를 재전송하는 것을 예방한다. 제3자는 이동 RFID 리더와 RFID 태그 사이에서 생성된 랜덤값 정보를 얻는다 하더라도 사용자의 인식 정보를 얻을 수 없기 때문에 인증 세션이 성공적으로 완성된 후에는 자동 갱신을 통해 트래킹과 재전송의 안전성을 보장받는다.

### 4.2. Forward 보안

제안 프토콜에서는 이동 RFID 리더와 RFID 사용자 태그 사이에 생성된 랜덤수를 해쉬한 토근값과 셋톱박스와 IPTV 콘텐츠 서버, 셋톱박스와 인증서버 사이에 생성되는 랜덤수를 사용하여 성인인증 등급 정보, 사용자 인증 정보를 암호화하기 때문에 forward security을 예방한다. 또한 IPTV 콘텐츠 서버의 데이터베이스와 인증서버의 데이터베이스에 각각 저장되어 있는 사용자 정보를 등급 결정 정책에 따라 최종 등급과 사용자 정보(태그 ID 정보등)의 유효성 검사를 수행한다. 검사과정에서 정보가 일치하면 IPTV 콘텐츠 서비스를 제공하고 정보가 일치하지 않으면 처리를 종료하게 된다.

### 4.3. RFID 태그 추적

셋톱박스는 다중 사용자의 공개키를 저장하고 있어 MCU로부터 PIN 정보를 체크하고 해쉬 결과로부터 랜덤 코드를 검색한 후 검색된 코드를 셋톱박스가 저장하고 있는 정보와 비교하여 정보가 일치한다면 IPTV 콘텐츠 서버에게 사용자의 성인등급 서비스를 요청한다. 이 때, 제3자가 RFID 태그 사용자의 정보를 기록하여 RFID 태그를 추적할 경우 제안 프로토콜에서는 토큰을 사용하여 제3자의 공격을 예방한다. 이동 RFID 리더의 ID와 RFID 사용자 태그가 생성한 랜덤수를 해쉬한 토큰값이 공격자에 의해 캡처되더라도 사용자의 성인인증등급 정보는 셋톱박스와 IPTV 콘텐츠 제공자 사이의 랜덤값을 제3자가 모르기 때문에 안전하며 사용자의 성인인증등급의 요청정보가 새로운 RFID 리더 인식자의 메모리에 갱신하려고 할 때도 새로운 RFID 리더 인식자는 이전 리더 인식자와 함께 암호화되기 때문에 제3자에 의해 통신이 도청되더라도 안전성을 보장받는다.

### 4.4. 맥코맥 핵 공격

제안된 프로토콜에서는 RFID 리더에 의해 서도 다른 인식자를 사용하기 때문에 제3자가 복제한 태그를 사용하더라도 IPTV 콘텐츠 서버에 저장된 정보와 일치하지 않은 경우 성인인증등급의 IPTV 콘텐츠를 제공받지 못한다. IPTV 콘텐츠 서버에 저장된 사용자 정

보와 인증서버에 등록된 정보가 해쉬함수에 의해 생성된 인식자 값과 서로 다르기 때문이다. 따라서, 복제된 성인인증등급 정보를 사용하는 제3자는 제안 프로토콜에서 생성된 해쉬함수의 인식자를 판별하기 어려워 성인인증등급의 IPTV 콘텐츠를 제공받는 것은 사실상 불가능하다.

## V. 결 론

IPTV 기술의 발전으로 사용자는 지리적 위치에 상관없이 멀티미디어 서비스를 손쉽게 제공받고 있다. 그러나 IPTV 서비스를 불법적으로 제공받으려는 사용자 또한 증가하고 있는 것이 현실이다. 본 논문에서는 IPTV 시스템에 RFID 기술과 이동통신 기술을 접목하여 청소년이 불법적으로 IPTV 콘텐츠의 성인 인증 정보를 부여받는 것을 예방하는 인증 모델을 제안하였다. 제안 모델은 기존 인터넷의 단순 성인 인증 시스템의 단점을 보완하기 위해서 IPTV 콘텐츠 서버에 성인 등급 분류 체계를 통하여 IPTV 콘텐츠 서버와 인증 서버의 데이터베이스에 저장된 사용자 인증 정보와 동기화를 유지하여 성인 인증 과정을 설계하였다. 또한, 제안 모델에서는 청소년이 불법적으로 인증정보를 획득하더라도 관리자의 동의없이 콘텐츠를 불법적으로 다운로드 못하도록 설계하였다.

향후 연구에서는 DRM의 기능을 IPTV 시스템에 결합하여 가입자의 권한 접근 및 레벨을 부여한 인증 메커니즘을 연구 수행할 계획이다.

## 참고문헌


[1] M. Pagani(2003), "Multimedia and Interactive Digital TV - Managing the Opportunities Created by Digital Convergence", IRM Press, 2003.

[2] Y. S. Jeong(2012), "RFID-based Authentication Protocol for Implantable Medical Device", The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 141-146.

[3] Y. L. Huang and S. Shieh(2004), "Efficient key distribution scheme for secure media delivery in pay-TV systems", IEEE Trans. Multimedia, vol. 6, no. 5, pp. 760-769.

[4] A. T. Sherman and D. A. McGrew(2003), "Key establishment in large dynamic groups using one-way functions trees", IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444-458.

[5] B. K. Rhee, Y. S. Jeong, S. H. Lee(2012), "Privacy Model based on RBAC for U-Healthcare Service Environment", Journal of Information & Communication, Vol. 16, No. 3, pp. 13-19.

[6] Y. S. Jeong, Y. T. Kim, G. C. Park and S. H. Lee(2009), "A Low-weight Authentication Protocol using RFID for IPTV Users", Journal of Inforamation Security & Cryptology, pp. 105-116.

[7] T.-W. Hou, J.-T. Lai and C.-L. Yeh(2007), "Based on Cryptosystem Secure Communication between Set-top Box and Smart card in DTV Broadcasting" , TENCON 2007, IEEE Region 10 Conference, 2007, pp.1-5.

[8] D. S. Wong and A. H. Chan, "Mutually authentication and key exchange for low power wireless communications", proc. IEEE MILCOM 2001, Vol. 1, pp. 39-43.

[9] T. Jiang et al(2004), "Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcastion", IEEE Trans. On Consumer Electronics, Vol. 50, No. 3, August, 2004, pp. 882-886.

[10] S. T. Wu and B. C. Chieu(2003), "A User Friendly Remote Authentication Scheme with Smart cards", Computers & Security 22 (6), 2003, pp. 547-550.

[11] S. T. Wu and B. C. Chieu(2004), "A Note on a User Freindly Remote User Authentication Scheme with Smart Cards", IEICE Transactions Fundamentals 87-A(8), Aug. 2004. pp. 2180-2181.

## 저자소개

**정윤수(Yoon-Su Jeong)**

1998. 청주대학교
전자계산학과 학사
2000. 충북대학교 대학원
전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사
2008.3 ~ 2009.8 충북대 및 한남대 시간강사
2009.9 ~ 2012.2 한남대학교 산업기술연구소
전임연구원
2012.3 ~ 현재 목원대학교 정보통신공학과 교수
※관심분야 : IPTV, 정보보호, 암호이론, Network Security, 유・무선통신보안

**김용태(Yong-Tae Kim)**

1984. 한남대학교 계산통계학과
학사.
1988. 숭실대학교 전자계산학과
석사.
2008. 충북대학교 전자계산학과 박사.
2002. 12. ~2006.2 (주)가림정보기술 이사
2010. 8 ~ 현재 한남대학교 멀티미디어 학부 교수
※관심분야 : 모바일 웹서비스, 정보보호, 센서 웹, 모바일 통신보안