

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2013-0027360 (43) 공개일자 2013년03월15일
(51) 국제특허분류(Int. Cl.) H04N 21/4367 (2011.01)		(71) 출원인 고려대학교 산학협력단 서울 성북구 안암동5가 1
(21) 출원번호	10-2011-0090893	(72) 발명자 이동훈 서울특별시 종로구 사직로8길 34, 경희궁의아침3 단지 아파트 1404호 (내수동)
(22) 출원일자	2011년09월07일	전은아 서울특별시 성북구 종암로25길 30, 110동 502호 (종암동, 삼성래미안아파트)
심사청구일자	2011년09월07일	(74) 대리인 특허법인충현

전체 청구항 수 : 총 9 항

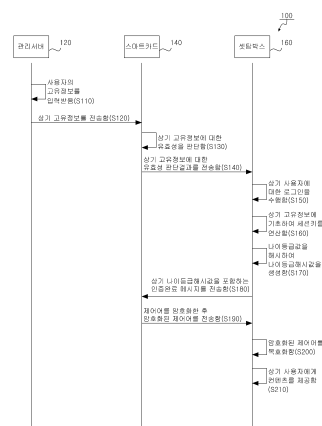
(54) 발명의 명칭 IPTV의 가입자 인증에 따른 접근제어 방법

(57) 요약

본 발명은 IPTV의 가입자 인증에 따른 접근제어 방법에 관한 것으로, 보다 구체적으로는 관리서버가 IPTV의 콘텐츠를 전송받고자 하는 사용자로부터 적어도 하나의 고유정보를 입력받아 상기 고유정보를 스마트카드에 전송하는 고유정보입력단계; 상기 셋탑박스가 상기 고유정보에 기초하여 세션키를 연산하고, 상기 콘텐츠를 수신할 수 있는 나이등급값을 해시한 후, 나이등급해시값을 포함하는 인증완료메시지를 상기 스마트카드에 전송하여 상기 사용자에게 대한 인증을 수행하는 인증단계; 및 상기 셋탑박스가 상기 스마트카드로부터 암호화된 제어어(CW: Control Word)를 수신하여 상기 세션키를 통해 복호화한 후, 인증이 완료된 상기 사용자에게 상기 콘텐츠를 제공하는 콘텐츠제공단계;를 포함한다.

이러한 구성에 의해, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 지문으로부터 측정된 지문값을 이용하여 상기 지문값에 대응하는 나이정보를 획득함으로써, 상기 사용자가 정당한 가입자인지를 확인할 수 있는 효과가 있다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 20100029121

부처명 한국연구재단

연구사업명 중견연구자지원_도약연구(전략)

연구과제명 속성 기반 공개키 시스템에 관한 연구

주관기관 고려대학교 산학협력단

연구기간 2010.09.09 ~ 2011.08.31

특허청구의 범위

청구항 1

관리서버가 IPTV의 콘텐츠를 전송받고자 하는 사용자로부터 적어도 하나의 고유정보를 입력받아 상기 고유정보를 스마트카드로 전송하는 고유정보입력단계;

상기 셋탑박스가 상기 고유정보에 기초하여 세션키를 연산하고, 상기 콘텐츠를 수신할 수 있는 나이등급값을 해시한 후, 나이등급해시값을 포함하는 인증완료메시지를 상기 스마트카드로 전송하여 상기 사용자에게 대한 인증을 수행하는 인증단계; 및

상기 셋탑박스가 상기 스마트카드로부터 암호화된 제어어(CW: Control Word)를 수신하여 상기 세션키를 통해 복호화한 후, 인증이 완료된 상기 사용자에게 상기 콘텐츠를 제공하는 콘텐츠제공단계;

를 포함하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 2

제1항에 있어서,

상기 등록단계 수행 후 상기 로그인단계 수행 전

적어도 하나의 비밀키 및 접근제어키를 생성하는 키생성단계;

를 더 포함하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 3

제2항에 있어서,

상기 고유정보입력단계는

상기 관리서버가 상기 사용자로부터 적어도 하나의 고유정보를 입력받는 고유정보입력과정;

상기 관리서버가 상기 적어도 하나의 비밀키 및 접근제어키를 이용하여 상기 고유정보를 해시한 후, 해시값을 생성하는 해시값연산과정;

상기 관리서버가 상기 적어도 하나의 비밀키 및 접근제어키를 이용하여 상기 고유정보가 기저장된 가족 구성원 정보에 해당하는지를 확인하는 제1함수를 연산하고, 상기 사용자의 나이에 따라 접근제어 여부를 결정하는 제2함수를 연산하는 함수연산과정; 및

상기 관리서버가 입력받은 상기 고유정보, 해시값, 제1함수 및 제2함수를 연산하여 생성된 제1함수값 또는 제2함수값 중 적어도 하나의 정보를 상기 스마트카드로 전송하는 전송과정;

을 포함하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 4

제3항에 있어서,

상기 제2함수는

상기 적어도 하나의 고유정보 중 복수 개의 고유정보를 이용하여 상기 사용자의 콘텐츠에 대한 접근제어 여부를 결정하거나, 상기 적어도 하나의 고유정보를 상호 조합한 후, 그 조합결과에 기초하여 상기 사용자의 콘텐츠에 대한 접근제어 여부를 결정하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 5

제2항에 있어서,

상기 로그인단계는

상기 스마트카드가 상기 고유정보의 유효성 확인을 위해, 상기 고유정보를 이용하여 적어도 하나의 유효값을 연산하는 유효값연산과정;

상기 스마트카드가 상기 유효값을 해시하거나, 상기 유효값과 랜덤수간 배타적 연산을 통해 적어도 하나의 로그인값을 생성하는 로그인값연산과정; 및

상기 스마트카드가 상기 적어도 하나의 로그인값을 포함하는 로그인메시지를 상기 셋탑박스로 전송하는 로그인 메시지전송과정;

을 포함하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 6

제5항에 있어서,

상기 인증단계는

상기 셋탑박스가 상기 스마트카드로부터 수신한 상기 사용자의 고유정보가 기저장된 고유정보와 동일한지 비교하는 고유정보비교과정;

상기 셋탑박스가 상기 고유정보 및 비밀키에 기초하여 로그인값을 연산하고, 연산한 로그인값을 수신한 로그인 메시지에 포함된 로그인값과 상호 비교하여 상기 사용자의 고유정보를 검증하는 고유정보검증과정;

상기 셋탑박스가 해당 콘텐츠를 수신할 수 있는 나이등급값을 해시하여 나이등급해시값을 생성하는 연산과정; 및

상기 셋탑박스가 생성된 상기 나이등급해시값을 포함하는 인증완료메시지를 상기 스마트카드로 전송하는 인증완료과정;

을 포함하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 7

제2항에 있어서,

상기 콘텐츠제공단계는

상기 스마트카드가 해당 콘텐츠를 수신할 수 있는 나이등급값을 해시하여 나이등급해시값을 생성하는 연산과정;

상기 스마트카드가 연산한 나이등급해시값과, 상기 인증완료메시지에 포함된 나이등급해시값을 상호 비교하는 비교과정;

상기 스마트카드가 상기 제어어를 암호화한 후, 암호화된 상기 제어어를 상기 셋탑박스로 전송하는 암호화과정; 및

상기 셋탑박스가 암호화된 제어어를 복호화하여, 상기 사용자에게 콘텐츠를 제공하는 콘텐츠제공과정;

을 포함하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 고유정보는

상기 사용자에 대한 아이디정보, 패스워드정보, 나이정보 또는 지문값정보 중 적어도 하나의 정보를 포함하는 것을 특징으로 하는 IPTV의 가입자 인증에 따른 접근제어 방법.

청구항 9

제1항 내지 제7항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

[0001] 본 발명은 IPTV의 가입자 인증에 따른 접근제어 방법에 관한 것으로, 특히 사용자의 아이디 및 패스워드를 외부로 노출하지 않으면서, 사용자의 나이에 따라 접근 가능한 콘텐츠로의 접근을 허용하는 IPTV의 가입자 인증에 따른 접근제어 방법에 관한 것이다.

배경기술

[0002] IPTV란, 인터넷 프로토콜 텔레비전(Internet Protocol Television)의 약자로서, 초고속 인터넷을 이용한 정보서비스, 동영상 콘텐츠 및 방송을 텔레비전의 수상기로 제공하는 서비스를 말한다. 이러한 IPTV는 시청자가 자신이 편리한 시간에 보고 싶은 특정 프로그램을 볼 수 있다는 점에서 일반 케이블 방송과 차이점을 갖는다. 특히, IPTV는 인터넷과 텔레비전의 융합이라는 점에서, 디지털 컨버전스의 한 유형이라고 할 수 있다.

[0003] 이와 같은 IPTV를 이용하기 위해서는 텔레비전 수상기와 셋탑박스, 인터넷 회선이 연결되어야 한다. 즉, 텔레비전에 셋탑박스 또는 전용 모뎀을 부착하고, 텔레비전을 켜듯이 전원만 인가하면, IPTV를 이용할 수 있다. 이에 따라, 컴퓨터에 익숙하지 않은 사람이라도 리모컨을 사용하여 인터넷 검색은 물론, 영화감상, 홈쇼핑, 홈뱅킹, 온라인게임 및 MP3 등 인터넷이 제공하는 다양한 콘텐츠 및 부가서비스를 제공받을 수 있다.

[0004] 또한, 이러한 IPTV는 비디오를 비롯한 다양한 방송 콘텐츠를 제공한다는 점에서는 일반 케이블 방송 또는 위성 방송과 유사하지만, 양방향성이 추가된다는 점에서 차이점을 갖는다. 예를 들어, IPTV는 일반 공중파 방송, 케이블 방송 또는 위성방송과 달리, 시청자가 편리한 시간에 자신이 보고싶은 프로그램만을 볼 수 있도록 하는 것이, 양방향성의 대표적인 예라고 할 수 있다.

[0005] 이처럼 편리하고 다양한 장점을 가진 IPTV는 수 많은 콘텐츠에 대하여 정당한 시청자(즉, 사용자 또는 가입자)만이 콘텐츠에 접근할 수 있도록 한다.

[0006] 따라서, 상기 셋탑박스와 스마트카드를 서로를 상호 인증하고, 접근한 가입자에 대한 가입자 인증을 완료한 후, 세션 키 설정을 통해 콘텐츠에 접근할 수 있도록 하고 있다.

[0007] 하지만, 이와 같은 이러한 가입자 인증방법은 공개키 기반 구조로 생성되는 공인인증서 및 일회성 비밀번호(OTP: One Time Password) 중 적어도 하나 이상을 조합하여 가입자의 인증을 수행하는데, 이때, 상기 가입자가 반드시 공인인증서를 사용해야 한다는 불편함이 존재하며, 뿐만 아니라, 상기 일회성 비밀번호의 해킹에 대한 문제점이 발생하였으며, 더불어, 상기 가입자의 다양한 속성에 대한 고려가 이루어지지 않는 등의 다양한 문제점이 발생했다.

[0008] 상술한 바와 같이, IPTV의 사용자 인증에 따른 접근제어 방법에 대한 선행기술을 살펴보면 다음과 같다.

[0009] 선행기술 1은 한국공개특허공보 제2011-0051734호(2011.05.18)로서, 지문스캐너를 갖춘 셋탑박스를 이용한 인터넷TV의 시청제한, 개인 맞춤형 광고 및 개인 맞춤형 프로그램 가이드 제공방법 및 시스템에 관한 것이다. 이러한 선행기술 1은 지문스캐너를 통해 지문을 스캔하여 사용자에게 관한 식별정보를 식별하고, 상기 식별된 식별정

보를 인터넷 TV 제공서버로 전송하는 셋탑박스; 상기 전송된 식별정보에 상응하는 개인맞춤 프로그램 가이드를 상기 셋탑박스로 전송하는 인터넷 TV 제공서버; 및 상기 전송된 개인맞춤 프로그램 가이드를 제공하는 인터넷 TV를 포함함으로써, 인터넷 TV의 사용자를 쉽고 편하게 식별하고, 획득한 개인 식별 ID(식별정보)를 활용하여, 개인별 시청이력, 구매이력, 검색이력 등을 인터넷 TV 제공서버의 데이터베이스에 저장하고, 통계를 분석하여 개인맞춤 광고, 개인맞춤 프로그램 가이드를 생성하여 송출함으로써, 사용자로 하여금 수백개의 채널 중에서 자신이 선호하는 채널을 자신만의 개인맞춤 프로그램 가이드를 활용하여 보다 편안하게 선택할 수 있으며, 개인맞춤 광고를 보고 원하는 쇼핑을 할 수도 있다.

[0010] 또한, 선행기술 2는 한국공개특허공보 제2001-0081451호(2001.08.29)로서, 지문인식기를 이용한 카드리더 인터페이스 셋탑박스 제어 시스템에 관한 것이다.

[0011] 이러한 선행기술 2는 카드데이터를 읽어들이기 위한 카드리더부와 각종 모드를 선택하기 위한 모드선택부를 포함하고, 카드데이터를 저장하기 위한 저장부와, 상기 카드데이터 및 모드선택신호를 통신단자를 통하여 송수신하도록 제어하는 제어부와, 송신데이터의 처리결과를 수신하여 표시하기 위한 표시부를 포함하는 카드리더와, 상기 카드리더와 데이터를 송수신할 수 있도록 통신라인을 통해 연결되고, 지문데이터를 읽어들이는 지문인식기와, 상기 카드리더로부터의 카드데이터와 지문데이터를 저장하는 저장부와, 상기 카드리더의 모드선택신호에 따라 지문데이터 및 카드데이터를 보내거나 또는 카드데이터만을 선택적으로 송신하고 처리결과를 수신하여 상기 카드리더에 송신하는 제어부를 포함하는 지문인식 셋탑박스와, 상기 지문인식 셋탑박스와 데이터 송수신이 가능하도록 통신선로를 통해 연결되고, 지문인식 셋탑박스로부터의 카드데이터 및 지문데이터를 수신하고 미리 저장된 데이터와 비교처리하여 송신하는 카드랜시스템으로 구성됨으로써, 본인 확인이 확실하게 이루어지므로 카드사용으로 인한 피해를 줄일 수 있는 효과가 있다.

발명의 내용

해결하려는 과제

[0012] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 사용자 즉, 가입자의 지문값을 이용하여 정당한 가족구성원 여부 및 연령대를 측정하고, 이를 통해 상기 가입자가 시청할 수 있는 적절한 콘텐츠를 상기 가입자에게 제공함으로써, 가입자의 콘텐츠 접근을 용이하게 제어할 수 있는 IPTV의 가입자 인증에 따른 접근제어 방법을 제공하고자 한다.

과제의 해결 수단

[0013] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 IPTV의 가입자 인증에 따른 접근제어 방법은 관리서버가 IPTV의 콘텐츠를 전송받으려 하는 사용자로부터 적어도 하나의 고유정보를 입력받아 상기 고유정보를 스마트카드로 전송하는 고유정보입력단계; 상기 셋탑박스가 상기 고유정보에 기초하여 세션키를 연산하고, 상기 콘텐츠를 수신할 수 있는 나이등급값을 해시한 후, 나이등급해시값을 포함하는 인증완료메시지를 상기 스마트카드로 전송하여 상기 사용자에게 인증을 수행하는 인증단계; 및 상기 셋탑박스가 상기 스마트카드로부터 암호화된 제어어(CW: Control Word)를 수신하여 상기 세션키를 통해 복호화한 후, 인증이 완료된 상기 사용자에게 상기 콘텐츠를 전송하는 전송단계;를 포함한다.

[0014] 보다 바람직하게는 상기 등록단계 수행 후 상기 로그인단계 수행 전, 적어도 하나의 비밀키 및 접근제어키를 생성하는 키생성단계;를 더 포함할 수 있다.

[0015] 보다 바람직하게는 상기 관리서버가 상기 사용자로부터 적어도 하나의 고유정보를 입력받는 고유정보입력과정; 상기 관리서버가 상기 적어도 하나의 비밀키 및 접근제어키를 이용하여 상기 고유정보를 해시한 후, 해시값을 생성하는 해시값연산과정; 상기 관리서버가 상기 적어도 하나의 비밀키 및 접근제어키를 이용하여 상기 고유정보가 기저장된 가족 구성원정보에 해당하는지를 확인하는 제1함수를 연산하고, 상기 사용자의 나이에 따라 접근제어 여부를 결정하는 제2함수를 연산하는 함수연산과정; 및 상기 관리서버가 입력받은 상기 고유정보, 해시값, 제1함수 및 제2함수를 연산하여 생성된 제1함수값 또는 제2함수값 중 적어도 하나의 정보를 상기 스마트카드로 전송하는 전송과정;을 포함하는 고유정보입력단계를 포함할 수 있다.

[0016] 특히, 상기 적어도 하나의 고유정보 중 복수 개의 고유정보를 이용하여 상기 사용자의 콘텐츠에 대한 접근제어

여부를 결정하거나, 상기 적어도 하나의 고유정보를 상호 조합한 후, 그 조합결과에 기초하여 상기 사용자의 콘텐츠에 대한 접근제어 여부를 결정하는 제2함수를 포함할 수 있다.

[0017] 보다 바람직하게는 상기 스마트카드가 상기 고유정보의 유효성 확인을 위해, 상기 고유정보를 이용하여 적어도 하나의 유효값을 연산하는 유효값연산과정; 상기 스마트카드가 상기 유효값을 해시하거나, 상기 유효값과 랜덤 수간 배타적 연산을 통해 적어도 하나의 로그인값을 생성하는 로그인값연산과정; 및 상기 스마트카드가 상기 적어도 하나의 로그인값을 포함하는 로그인메시지를 상기 셋탑박스로 전송하는 로그인메시지전송과정;을 포함하는 로그인단계를 포함할 수 있다.

[0018] 보다 바람직하게는 상기 셋탑박스가 상기 스마트카드로부터 수신한 상기 사용자의 고유정보가 기저장된 고유정보와 동일한지 비교하는 고유정보비교과정; 상기 셋탑박스가 상기 고유정보 및 비밀키에 기초하여 로그인값을 연산하고, 연산한 로그인값을 수신한 로그인메시지에 포함된 로그인값과 상호 비교하여 상기 사용자의 고유정보를 검증하는 고유정보검증과정; 상기 셋탑박스가 해당 콘텐츠를 수신할 수 있는 나이등급값을 해시하여 나이등급해시값을 생성하는 연산과정; 및 상기 셋탑박스가 생성된 상기 나이등급해시값을 포함하는 인증완료메시지를 상기 스마트카드로 전송하는 인증완료과정;을 포함하는 인증단계를 포함할 수 있다.

[0019] 보다 바람직하게는 상기 스마트카드가 해당 콘텐츠를 수신할 수 있는 나이등급값을 해시하여 나이등급해시값을 생성하는 연산과정; 상기 스마트카드가 연산한 나이등급해시값과, 상기 인증완료메시지에 포함된 나이등급해시값을 상호 비교하는 비교과정; 상기 스마트카드가 상기 제어어를 암호화한 후, 암호화된 상기 제어어를 상기 셋탑박스로 전송하는 암호화과정; 및 상기 셋탑박스가 암호화된 제어어를 복호화하여, 상기 사용자에게 콘텐츠를 전송하는 콘텐츠전송과정;을 포함하는 전송단계를 포함할 수 있다.

[0020] 특히, 상기 사용자에 대한 아이디정보, 패스워드정보, 나이정보 또는 지문값정보 중 적어도 하나의 정보를 포함하는 고유정보를 포함할 수 있다.

발명의 효과

[0021] 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 지문으로부터 측정된 지문값을 이용하여 상기 지문값에 대응하는 상기 사용자의 나이정보를 획득함으로써, 상기 지문값 및 나이정보를 통해 상기 사용자가 정당한 가입자인지 여부를 용이하게 확인할 수 있는 효과가 있다.

[0022] 또한, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 지문을 통해 이에 대응하는 연령대를 확인함으로써, 상기 사용자가 정당한 가입자라고 하더라도 해당 연령대가 시청할 수 있는 콘텐츠만을 제공받도록 하는 효과가 있다.

[0023] 더불어, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 인증 시 사용되는 아이디 및 패스워드와 같은 고유정보를 노출하지 않더라도 사용자인증을 용이하게 수행할 수 있도록 하는 효과가 있다.

[0024] 이와 더불어, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 비밀키를 스마트카드 내 안전하게 저장함으로써, 전방향 안전성(forward secrecy) 및 디피 헬먼(Diffie-Hellman) 키 교환에 대한 공격을 방지할 수 있으며, 스마트카드와 셋탑박스 간에 상호 인증 시, 중간자 공격(Man-In-The-Middle)을 방지할 수 있는 효과가 있다.

[0025] 또한, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 셋탑박스가 스마트카드와의 상호인증 및 키교환과정을 수행하지 않고 세션키만을 이용하여 데이터를 복호화할 수 없도록 함에 따라, 상기 스마트카드의 인증 시 발생하는 맥코맥 해킹(McCormac Hacking) 및 상기 스마트카드의 복제 공격을 방어할 수 있는 효과가 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 일 실시 예에 따른 IPTV의 가입자 인증에 따른 접근제어 방법의 순서도이다.

도 2는 도 1의 고유정보입력단계의 세부순서도이다.

도 3은 도 1의 로그인단계의 세부순서도이다.

도 4는 도 1의 인증단계의 세부순서도이다.

도 5는 도 1의 콘텐츠제공단계의 세부순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0028] 이하, 도 1을 참조하여, 본 발명의 일 실시 예에 따른 IPTV의 가입자 인증에 따른 접근제어 방법에 대하여 자세하게 살펴보도록 한다.
- [0029] 도 1은 본 발명의 일 실시 예에 따른 IPTV의 가입자 인증에 따른 접근제어 방법의 순서도이다.
- [0030] 도 1에 도시된 바와 같이, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 먼저, 관리서버(120)가 IPTV의 콘텐츠를 전송받으려 하는 사용자(가입자)로부터 상기 사용자에게 대한 적어도 하나의 고유정보를 입력받는다(S110). 이때, 상기 고유정보란, 상기 사용자에게 대한 아이디정보, 패스워드정보, 나이정보 또는 지문값정보 중 적어도 하나의 정보를 말한다.
- [0031] 이후, 상기 사용자로부터 상기 사용자에게 대한 고유정보를 입력받은 상기 관리서버(120)는 입력받은 상기 고유정보를 스마트카드(140)로 전송한다(S120).
- [0032] 상기 스마트카드(140)가 상기 고유정보에 대한 유효성을 판단한 후(S130), 그 판단결과를 셋탑박스로 전송한다(S140).
- [0033] 이에 따라, 상기 셋탑박스(160)는 유효하다고 판단한 상기 고유정보를 갖는 상기 사용자에게 대한 로그인을 수행한다(S150).
- [0034] 이후, 상기 셋탑박스(160)는 상기 고유정보에 기초하여 추후 암호화된 제어어의 복호화 시, 사용되는 세션키를 연산한다(S160).
- [0035] 이어서, 상기 셋탑박스(160)가 상기 콘텐츠를 수신할 수 있는 나이대별 각 등급에 대한 나이등급값을 해시하여, 나이등급해시값을 생성한다(S170).
- [0036] 이후, 상기 셋탑박스(160)는 생성한 상기 나이등급해시값을 포함하는 인증완료메시지를 상기 스마트카드(140)로 전송한다(S180).
- [0037] 이와 같이, 나이등급해시값을 포함하는 인증완료메시지를 수신한 상기 스마트카드(140)는 제어어(CW: Control Word)를 암호화하고, 암호화된 제어어 CW를 상기 셋탑박스(160)로 전송한다(S190).
- [0038] 이후, 상기 셋탑박스(160)가 상기 스마트카드(140)로부터 수신한 암호화된 제어어를 앞서 S160과정에서 연산한 세션키를 통해 복호화한 후(S200), 인증이 완료된 상기 사용자에게 상기 사용자가 수신하고자 하는 해당 콘텐츠를 제공한다(S210).
- [0039] 이하, 도 2 내지 도 5를 참조하여, 본 발명의 일 실시 예에 따른 IPTV의 가입자 인증에 따른 접근제어 방법의 세부과정에 대하여 보다 구체적으로 살펴보도록 한다.
- [0040] 도 2는 도 1의 고유정보입력단계의 세부순서도이다.
- [0041] 상기 관리서버(120)가 콘텐츠를 수신하고자 하는 상기 사용자로부터 상기 사용자 자신에 대한 적어도 하나의 고유정보를 입력받는다(S111). 이때, 상기 고유정보는 상기 사용자 개인에 대한 아이디정보 ID, 패스워드정보 PW, 나이정보 a 또는 지문값정보 f 중 적어도 하나의 정보를 말한다.
- [0042] 이어서, 상기 관리서버(120)는 적어도 하나의 비밀키 및 접근제어키를 생성한다(S112). 예를 들어, 두 개의 비밀키 x_s , y_s 와 한 개의 접근제어키 z_s 를 랜덤수로부터 생성하고, 생성한 상기 두 개의 비밀키 x_s , y_s 및 한 개의 접근제어키 z_s 를 셋탑박스(160)에 저장한다.
- [0043] 이후, 상기 관리서버(120)는 앞서 생성한 두 개의 비밀키 x_s , y_s 및 한 개의 접근제어키 z_s 를 이용하여, 입력받은 상기 고유정보를 해시하여 상기 고유정보에 대한 해시값을 생성한다(S113). 이때, 상기 해시값은 제1 해시값 A, 제2해시값 B 및 제3 해시값 R의 총 3개의 값으로 연산할 수 있는데, 상기 제1 해시값 A은 $A =$

$h(ID \oplus x_s) \oplus h(h(ID \parallel pw) \parallel y_s)$ 이다. 즉, 상기 제1 해시값 A는 상기 고유정보 중 아이디정보 ID와 비밀키 x_s 를 XOR 연산을 수행하고, 이를 다시 해시하여 해시값을 생성한다.

[0044] 또한, 상기 아이디정보 ID와 패스워드정보 PW를 OR 연산하고, 연산한 값을 비밀키 y_s 와 OR 연산을 수행하여, 해시한다. 이와 같이 해시한 값을 앞서 상기 아이디정보ID와 비밀키 x_s 를 XOR 연산을 수행한 후 해시한 값과 XOR 연산을 수행함으로써, 획득할 수 있다.

[0045] 또한, 상기 제2 해시값 B는 $B = h(h(ID \oplus x_s) \parallel y_s)$ 이다. 즉, 상기 제2 해시값 B는 상기 아이디정보 ID와 비밀키 x_s 를 XOR 연산하고, 이를 해시한 후, 해시한 값을 비밀키 y_s 와 OR 연산을 수행한 후 해시함으로써, 획득할 수 있다.

[0046] 더불어, 상기 제3 해시값 R은 $R = h(ID \parallel PW) \oplus y_s$ 이다. 즉, 상기 제3 해시값 R은 상기 아이디정보 ID를 상기 패스워드정보 PW와 OR 연산한 후 해시하고, 해시한 값과 비밀키 y_s 를 XOR 연산함으로써, 획득할 수 있다.

[0047] 또한, 상기 관리서버(120)는 앞서 연산한 상기 비밀키 x_s , y_s 및 접근제어키 Z_s 를 제1함수 $g(x)$ 에 적용하여 상기 사용자로부터 입력받은 고유정보가 기저장된 가족구성원 정보에 해당하는지 여부를 확인한다(114). 이때, 상기

$$g(x) = \prod_{i=1}^t (x - h(f_j)) \oplus y_s$$

제1함수 $g(x)$ 란, 이다. 즉, 상기 사용자로부터 입력받은 고유정보 x 에서 기저장된 지문값정보 f_j 를 해시한 값을 뺀 후, 앞서 생성한 비밀키 y_s 와 XOR 연산을 수행함으로써, 입력받은 상기 고유정보 x 가 기저장된 가족구성원에 해당하는 정보인지 확인할 수 있도록 한다.

[0048] 이어서, 상기 관리서버(120)는 상기 비밀키 x_s , y_s 및 접근제어키 z_s 를 제2함수 $l(x)$ 에 적용하여 상기 사용자의 나이에 따른 콘텐츠 접근여부를 결정한다(S115). 이때, 사용되는 상기 제2함수 $l(x)$ 란,

$$l(x) = \prod_{i=1}^t (x - h(f_j)h(a_j)) \oplus z_s$$

이다. 즉, 상기 사용자의 지문값 x 로부터 기저장된 지문값정보 f_j 를 해시한 값과, 나이정보 a_j 를 해시한 값을 뺀 후, 접근제어키 z_s 와 XOR 연산을 수행하여, 특정 콘텐츠에 접근하고자 하는 사용자의 나이에 따라 상기 콘텐츠의 접근여부를 결정하도록 한다.

[0049] 특히, 상기 제2함수 $l(x)$ 는 가입자의 고유정보를 이용하여 그 속성을 확장할 수 있다.

[0050] 먼저, 사용자로부터 입력받은 적어도 하나의 고유정보 중 나이정보 외에도 사용자에 대한 학년정보, 연령대정보 등과 같은 고유정보 (attribute)_j를 하기의 수학적 식 1에 적용하여 상기 사용자의 콘텐츠에 대한 접근제어 여부를 결정할 수 있다.

[0051] [수학적 식 1]

$$l(x) = \prod_{i=1}^t (x - h(f_j)h((attribute)_j)) \oplus z_s$$

[0052] 즉, 사용자의 고유정보 x 에서, 기저장된 지문값정보 f_j 를 해시한 값에 상기 사용자의 고유정보 중 2개의 정보 예를 들면, 나이정보, 학년정보를 나타내는 를 해시한값을 곱한 값을 뺀 후, 이를 다시 접근제어키 z_s 와 XOR 연산을 수행하여 특정 콘텐츠에 접근하고자 하는 사용자의 나이에 따라 상기 콘텐츠의 접근여부를 결정한다.

[0054] 또는 이와 달리, 하기의 수학적 식 2와 같이, 사용자로부터 입력받은 고유정보를 2개씩 n 개의 쌍, 예를 들면 나이, 성별, 나이, 가입패키지정보 등을 상호 조합하여 생성한 값 $h(attribute)_{jc}$ 들의 합을 연산하여 상기 사용자의 콘텐츠에 대한 접근제어 여부를 결정할 수 있다.

[0055] [수학식 2]

$$I(x) = \prod_{i=1}^t [(x - h(f_j) \prod_{c=1}^q h(attribute_{j_c}))] \oplus z_s.$$

[0057] 즉, 상기 사용자의 고유정보 x 에서, 기저장된 지문값정보 f_j 를 해시한 값과상기 사용자에게 대한 고유정보 중 나이정보, 학년정보, 연령대정보, 콘텐츠 패키지 정보 등을 상호 조합하여 해시한 값의 합 을 곱한 값을 뺀 후, 이를 다시 접근제어키 z_s 와 XOR 연산을 수행하여 특정 콘텐츠에 접근하고자 하는 사용자의 고유정보들에 따라 상기 콘텐츠의 접근여부를 결정한다.

[0058] 이와 같이, 상기 관리서버(120)가 생성한 제1 내지 제3해시값 A, B, R 과, 상기 제1함수 및 제2함수를 연산하여 생성된 제1함수값 $g(x)$ 또는 제2함수값 $l(x)$ 와, 사용자로부터 입력받은 고유정보 즉, 지문값 x 를 스마트카드(140)로 전송한다(s116).

[0059] 이어서, 도 3을 참조하여, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법 중 로그인단계에 대하여 보다 구체적으로 살펴보도록 한다.

[0060] 도 3은 도 1의 로그인단계의 세부순서도이다.

[0061] 도 3에 도시된 바와 같이, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법 중 로그인단계는 먼저, 스마트카드(140)가 가입자로부터 입력받은 고유정보가 유효한지 여부를 확인하기 위해, 상기 고유정보를 이용하여 적어도 하나의 유효값을 연산한다(S131). 이때, 상기 스마트카드(140)는 제 1 내지 제3 유효값 C_1, C_2, C_3 을 연산할 수 있다. 상기 제1 유효값 C_1 은 $C_1 = g(h(f_j))$ 와 같으며, 이러한 제1 유효값 C_1 은 비밀키 y_s 와 대응되는 y_s' 가 된다. 즉, 상기 제1 유효값 C_1 은 기저장된 지문값정보 f_j 를 해시한 값에 대한 제너레이터값을 생성함으로써, 획득할 수 있다.

[0062] 또한, 상기 제2 유효값 C_2 는 $C_2 = C_1 \oplus R$ 이다. 즉, 상기 제2 유효값 C_2 는 상기 제1 유효값 C_1 과 상기 제3 해시값 R 을 XOR 연산한 값이다. 또한, 상기 제3 유효값 C_3 은 $C_3 = A \oplus h(C_2 \parallel C_1)$ 이다. 즉, 상기 제3 유효값 C_3 은 상기 제2 유효값 C_2 와 제 1 유효값 C_1 을 상호 OR 연산을 수행한 후, 이를 해시한 값을 상기 제1 해시값 A 와 XOR 연산을 수행함으로써 획득할 수 있다.

[0063] 이어서, 상기 스마트카드(140)는 제2 해시값 B 를 연산하여, 상기 관리서버(120)가 연산한 제2 해시값 B 와 동일한지 여부를 비교하여 확인한다. 이때, 상기 스마트카드(140)가 연산한 제2 해시값 B 와, 상기 관리서버(120)가 연산한 제2 해시값 B 가 상호 동일하지 않으면, 상기 사용자에게 대한 로그인을 수행하지 않도록 한다.

[0064] 이후, 상기 스마트카드(140)는 랜덤수 r_1 을 생성하고, 적어도 하나의 로그인값을 생성한다(s132). 이때, 상기 스마트카드(140)는 제1 로그인값 C_4 및 제2 로그인값 C_5 을 각각 생성한다. 상기 제1 로그인 값 C_4 는 $C_4 = h(C_3 \parallel h(T_1)(\text{mod}p))$ 이다. 이를 통해, Z_{p^*} 그룹에서 p 로 나누면 나머지가 $h(C_3 \parallel h(T_1))$ 가 되는 것을 알 수 있다.

[0065] 또한, 상기 제2 로그인값 C_5 은 $C_5 = C_3 \oplus r_1(\text{mod}p)$ 이다. 마찬가지로, 상기 Z_{p^*} 그룹에서 p 로 나누면 나머지가 $C_3 \oplus r_1$ 이 되는 것을 알 수 있다.

[0066] 더불어, 상기 스마트카드(140)는 상기 랜덤수 r_1 의 제너레이터값을 연산한 후, 이를 세션키 K_2 로 사용하며, 기설정된 시간동안에만 유효하도록 설정된 현재시간 T_1 을 생성한다.

$$(T_1 - T'_1) \geq \Delta T$$

[0068] 즉, 현재 시간 T_1 과 임의의 시간 T'_1 시간 간격이 기설정된 시간간격 ΔT 와 같거나 큰지 여부를 확인하여, 기설정된 시간동안에만 유효한 현재시간 T_1 이 생성될 수 있다.

[0069] 이에 따라, 상기 스마트카드(140)는 연산한 상기 제1 로그인값 C_4 , 제2 로그인값 C_5 , 아이디정보 ID, 세션키 K_2

및 현재시간정보 T_1 를 포함하는 로그인메시지를 생성하고, 이를 셋탑박스(160)로 전송한다(S133).

- [0070] 이와 같이, 상기 사용자에게 대한 로그인 단계가 완료되면, 이어서, 상기 사용자에게 대한 인증단계가 수행되는데, 이하, 도 4를 참조하여 본 발명의 인증단계에 대하여 자세히 살펴보도록 한다.
- [0071] 도 4는 도 1의 인증단계의 세부순서도이다.
- [0072] 도 4에 도시된 바와 같이, 본 발명의 인증단계는 먼저, 셋탑박스(160)가 상기 스마트카드(140)로부터 수신한 상기 사용자의 고유정보가 기저장된 고유정보와 동일한지 여부를 비교한다(S161). 이때, 셋탑박스(160)가 스마트카드(140)로부터 수신한 고유정보가 기저장된 고유정보와 동일하지 않는 경우, 상기 고유정보를 전송한 사용자에게 대한 인증을 수행하지 않는다.
- [0073] 상기 셋탑박스(160)가 상기 스마트카드(140)로부터 수신한 고유정보가 기저장된 고유정보와 동일한 경우, 상기 셋탑박스(160)는 상기 고유정보 중 아이디정보 ID 및 비밀키 x_s 에 기초하여 로그인값을 연산한다(S162).
- [0074] 상기 셋탑박스(160)가 연산하는 상기 제1 로그인값 C_4 는 $C_4 = h(h(ID \oplus_{x_s}) \parallel h(T_1))$ 이다. 즉, 상기 제1 로그인값 C_4 는 상기 아이디정보 ID와 비밀키 x_s 간 XOR 연산을 수행한 후 이를 해시한 값과, 현재시간정보 T_1 을 해시한 값을 상호 OR 연산한 후, 이를 다시 해시하여 제1 로그인값 C_4 을 획득한다. 즉
- [0075] 이후, 상기 셋탑박스(160)는 자신이 연산한 제1 로그인값 C_4 와, 상기 스마트카드(140)로부터 수신한 로그인메시지에 포함된 제1 로그인값 C_4 가 상호 동일한지 비교한다. 이때, 상기 셋탑박스(160)가 연산한 제1 로그인 값 C_4 와, 상기 스마트카드(140)로부터 수신한 로그인메시지에 포함된 제1 로그인값 C_4 가 상호 동일한 경우, 상기 셋탑박스(160)는 상기 랜덤수 r_1 과 대응하는 랜덤수 r_1' 을 $r_1' = C_5 \oplus h(ID \oplus_{x_s})$ 를 통해 연산하고, 이와 같이 연산된 상기 r_1' 이 상기 r_1 과 동일한지 여부를 비교한다. 이때, 상기 r_1' 과 r_1 이 동일한 경우, 상기 셋탑박스(160)는 사용자에게 대한 고유정보 즉, 아이디정보 ID, 패스워드정보 PW 및 지문값 f 를 인증한다.
- [0076] 이후, 상기 셋탑박스(160)는 DLP(Discrete Logarithm Problem, 이산대수문제)를 기반으로 하는 세션키 K_1 에 대응하는 K'_1 을 $K'_1 = (k_1)^{x_s}$ 을 통해 연산한다. 이와 같이, 상기 k_1 에 대응하는 K'_1 을 연산하고, 연산된 K'_1 을 k_1 와 상호 비교하여 동일한 경우에 추후 세션키 SK를 연산할 수 있도록 하여, 정당한 세션키 SK값을 획득한 사용자(가입자)만이 제어어 CW를 복호화할 수 있도록 한다.
- [0077] 이와 같이, 상기 K'_1 를 연산한 상기 셋탑박스(160)는 상기 K'_1 과, 아이디정보 ID 및 상기 셋탑박스(160)의 고유정보 ID_s 를 해시하여 공개세션키 SK를 연산한다.
- [0078] 상기 셋탑박스(160)가 기설정된 나이등급값을 해시하여 나이등급해시값을 생성한다(S165). 이때, 상기 셋탑박스(160)는 제1 내지 제3 나이등급해시값 C_6 , C_7 , C_8 을 각각 생성할 수 있다.
- [0079] 상기 제1 나이등급해시값 C_6 은 $C_6 = h(K'_1 \oplus_{r_2}) \oplus h(\text{grade}_c)$ 이다. 이때, 상기 grade_c 는 특정 콘텐츠의 시청가능한 시청자의 연령대값을 나타냄에 따라, 앞서 연산한 상기 k_1 에 대응하는 K'_1 과 랜덤수 r_2 를 XOR연산하고 이를 해시한 값과, 특정 콘텐츠의 시청가능한 시청자의 연령대값을 해시한값을 XOR연산을 수행함으로써, 연산된다.
- [0080] 또한, 상기 제2 나이등급해시값 C_7 은 $C_7 = h(r_2 \oplus Z_s)$ 이다. 즉, 랜덤수 r_2 와 접근제어키 Z_s 를 XOR연산한 후, 이를 다시 해시함으로써 연산된다.
- [0081] 더불어, 상기 제3 나이등급해시값 C_8 은 $C_8 = h(r_2 \parallel h(\text{grade}_c) \parallel T_2)$ 이다. 즉, 랜덤수 r_2 와 특정콘텐츠의 시청가능한 시청자의 연령대값을 해시한값 $h(\text{grade}_c)$ 및 시간정보 T_2 를 상호 OR연산하고, 이를 다시 해시함으로써 연산된다.
- [0082] 이후, 상기 셋탑박스(160)는 연산한 상기 제1 내지 제3 나이등급해시값 C_6 , C_7 , C_8 및 현재시간정보 T_2 를 포함하여 인증완료메시지를 스마트카드(140)로 전송한다(S166).
- [0083] 이와 같이, 상기 셋탑박스(160)가 인증완료메시지를 스마트카드(140)로 전송함에 따라, 상기 셋탑박스(160)는

사용자에게 상기 사용자가 수신하고자 하는 콘텐츠를 제공한다.

- [0084] 도 5는 도 1의 콘텐츠제공단계의 세부순서도이다.
- [0085] 도 5에 도시된 바와 같이, 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법 중 콘텐츠제공과정은 먼저, 상기 스마트카드(140)가 가입자에 대한 해당 콘텐츠를 수신할 수 있는 나이등급값을 해시하여 나이등급해시값을 생성한다(S191). 이때, 상기 나이등급해시값은 $h(\text{grade}_c)' = h(K'_1 \oplus r_2) \oplus C_6$ 이다. 즉, 먼저 상기 스마트카드(140)는 DLP를 기반으로 하는 세션키 K_1 에 대응하는 K'_1 과 랜덤수 r_2 를 XOR연산한 후 이를 해시하고, 해시한 값을 제1 나이등급해시값 C_6 과 XOR연산함으로써, 나이등급값에 대응하는 해시값 $h(\text{grade}_c)'$ 를 획득한다.
- [0086] 이후, 상기 스마트카드(140)는 앞서 연산한 상기 나이등급해시값을 이용하여 제3 나이등급해시값 C_8 을 연산한다. 이때, 상기 제3 나이등급해시값 C_8 은 $C_8 = h(r_2 \parallel h(\text{grade}_c)' \parallel T_2)$ 이다. 즉, 상기 제3 나이등급해시값 C_8 은 랜덤수 r_2 와 상기 나이등급해시값 $h(\text{grade}_c)'$ 및 현재시간정보 T_2 를 상호 OR연산한 후, 이를 해시함으로써 획득된다.
- [0087] 이에 따라, 상기 스마트카드(140)는 앞서 연산한 상기 제3 나이등급해시값 C_8 을 상기 셋탑박스(160)로부터 수신한 인증완료메시지에 포함된 제3 나이등급해시값 C_8 과 상호 비교하여 동일한지 여부를 확인한다(S192).
- [0088] 이후, 상기 스마트카드(140)는 자신이 연산한 제3 나이등급해시값 C_8 과, 상기 인증완료메시지에 포함된 제3 나이등급해시값 C_8 과 동일하다고 판단한 경우, 공개세션키 SK 및 제어어 CW를 암호화하고, 암호화된 제어어 CW를 셋탑박스(160)로 전송한다(S193).
- [0089] 이에 따라, 상기 셋탑박스(160)는 암호화된 제어어 CW를 복호화하여 제어어 CW를 획득한다(S194).
- [0090] 이와 같이, 상기 제어어 CW를 획득한 상기 셋탑박스(160)는 인증이 완료된 사용자에게 상기 사용자가 수신하고자 하는 해당 콘텐츠를 제공한다(S195).
- [0091] 이러한 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- [0092] 본 발명의 IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 지문으로부터 측정한 지문값을 이용하여 상기 지문값에 대응하는 상기 사용자의 나이정보를 획득함으로써, 상기 지문값 및 나이정보를 통해 상기 사용자가 정당한 가입자인지 여부를 용이하게 확인할 수 있는 효과가 있다.
- [0093] 또한, IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 지문을 통해 이에 대응하는 연령대를 확인함으로써, 상기 사용자가 정당한 가입자라고 하더라도 해당 연령대가 시청할 수 있는 콘텐츠만을 제공하도록 하는 효과가 있다.
- [0094] 더불어, IPTV의 가입자 인증에 따른 접근제어 방법은 사용자의 인증 시 사용되는 아이디 및 패스워드와 같은 고유정보를 노출하지 않더라도 사용자인증용 용이하게 수행할 수 있도록 하는 효과가 있다.
- [0095] 이와 더불어, IPTV의 가입자 인증에 따른 접근제어 방법은 비밀키를 스마트카드 내 안전하게 저장함으로써, 전 방향 안전성(forward secrecy) 및 디피 헬멘(Diffie-Hellman) 키 교환에 대한 공격을 방지할 수 있으며, 스마트카드와 셋탑박스 간에 상호 인증 시, 중간자 공격(Man-In-The-Middle)을 방지할 수 있는 효과가 있다.
- [0096] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

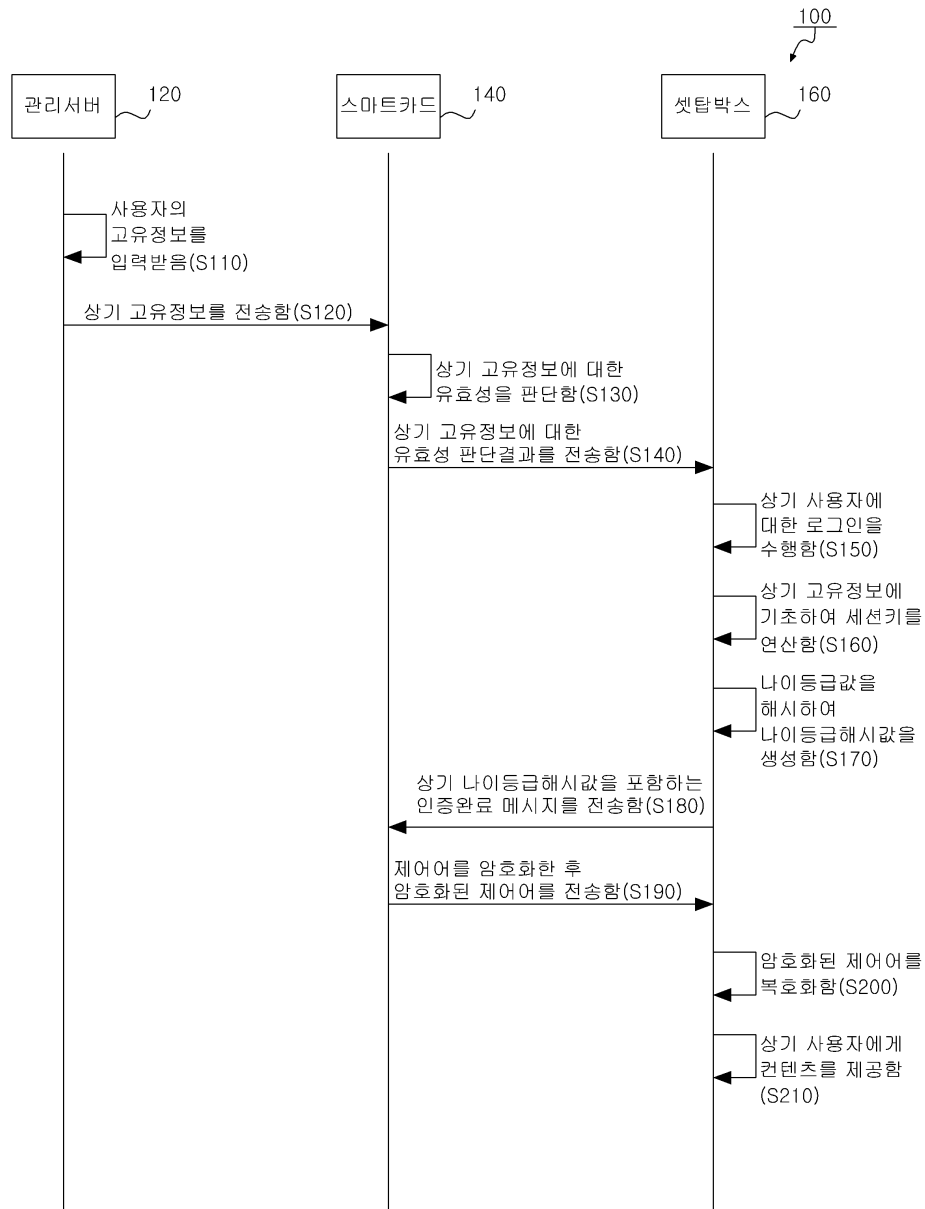
부호의 설명

- [0097] 120: 관리서버 140: 스마트카드

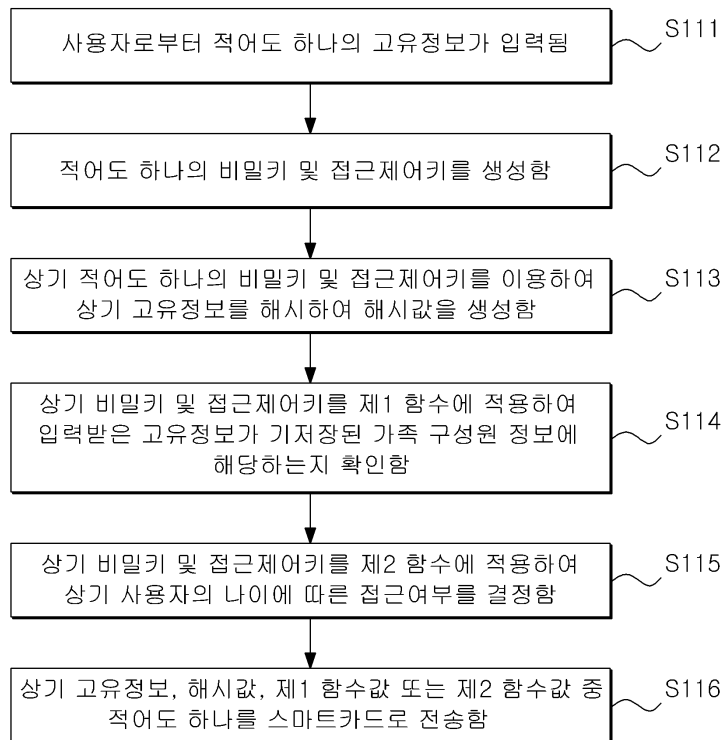
160: 셋탑박스

도면

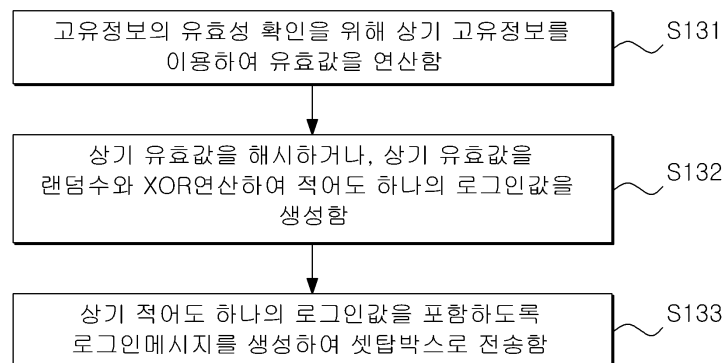
도면1



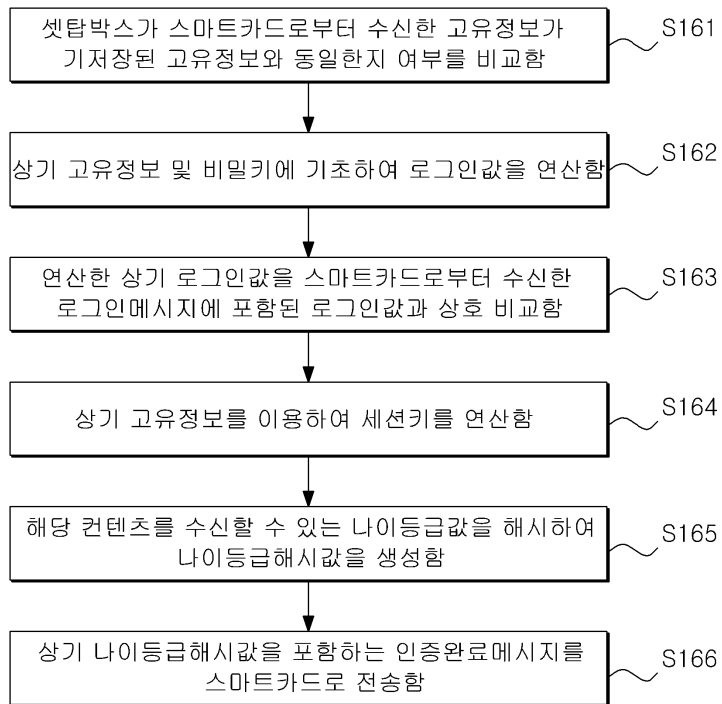
도면2



도면3



도면4



도면5

