(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0072032
(43) 공개일자 2012년07월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2010-0133796
(22) 출원일자 2010년12월23일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
박영수
대전광역시 서구 계룡로571번길 65, 101동 907호 (탄방동, 산호아파트)
김영일
대전광역시 유성구 어은로 57, 135동 704호 (어은동, 한빛아파트)
(뒷면에 계속)
(74) 대리인
특허법인 신지

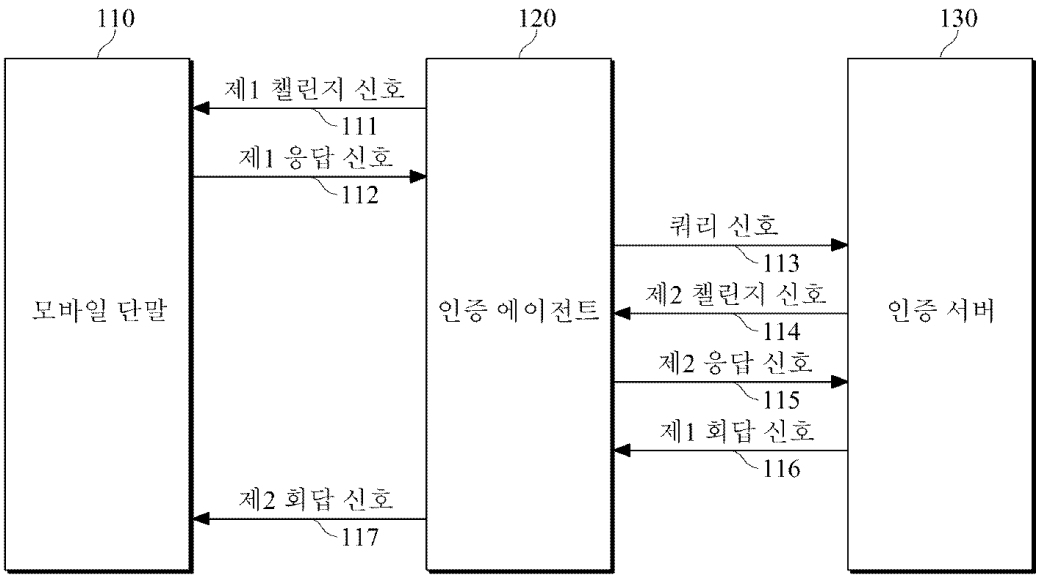
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **모바일 단말의 상호인증 시스템 및 상호인증 방법**

(57) 요 약

본 발명은 사람과 사람, 사람과 장치(디바이스, 기기, 단말 등), 장치(디바이스, 기기, 단말 등)와 장치(디바이스, 기기, 단말 등)간과 같은 다양한 인증 대상의 확대로 인한 이 기종 장치(디바이스, 기기, 단말 등) 간의 상호인증 기술을 제공한다.

대 표 도



(72) 발명자

조철희

대전광역시 유성구 어은로 57, 105동 606호 (어은동, 한빛아파트)

박대근

대전광역시 유성구 엑스포로 448, 510동 602호 (전민동, 엑스포아파트)

이용수

대전광역시 유성구 지족로 317, 반석마을아파트 110동 1504호 (지족동)

전선심

대전광역시 유성구 엑스포로 501, - 108동 1501호 (전민동, 나래아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	KI002187
부처명	지식경제부/방송통신위원회
연구사업명	정보통신산업원천기술개발사업
연구과제명	IPTV 융합단말 고도화 지원기술 개발
주관기관	한국전자통신연구원
연구기간	2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

모바일 단말과 인증서버 간에 위치하는 인증 에이전트를 통해 상호인증을 수행하는 방법에 있어서,

제1임의정보를 이용하여 생성한 제1챌린지 신호를 상기 모바일 단말로 전송하는 단계;

상기 모바일 단말로부터 상기 모바일 단말에 대한 정보에 기초하여 생성한 제1응답 신호를 수신하는 단계;

상기 모바일 단말 및 상기 인증 에이전트에 대한 인증을 위한 쿼리 신호를 상기 인증서버로 전송하는 단계;

상기 인증서버로부터 제2임의정보를 이용하여 생성한 제2챌린지 신호를 수신하는 단계;

상기 인증 에이전트에 대한 정보에 기초하여 생성한 제2응답 신호를 상기 인증서버로 전송하는 단계;

상기 인증서버로부터 상기 인증 에이전트에 대한 정보에 기초하여 생성한 제1회답 신호를 수신하는 단계; 및

상기 모바일 단말에 대한 정보에 기초하여 생성한 제2회답 신호를 상기 모바일 단말로 전송하는 단계;를 포함하는 상호인증 방법.

청구항 2

제 1 항에 있어서,

상기 인증 에이전트와 상기 모바일 단말에 각각 시드값(SEED_M, SEED_AG), 키 값(KEY_M, KEY_ID), 식별정보(ID_M, ID_AG)를 부여하고, 상기 부여된 시드값(SEED_M, SEED_AG), 키 값(KEY_M, KEY_ID), 식별정보(ID_M, ID_AG)를 상기 인증서버에 저장시키는 단계;를 더 포함하는 상호인증 방법.

청구항 3

제 1 항에 있어서, 상기 제1챌린지 신호를 상기 모바일 단말로 전송하는 단계는

Nonce값, 난수, 시간 중 어느 하나를 포함하는 제1임의정보에 대한 해쉬값으로 제1챌린지 신호를 생성하여 상기 모바일 단말로 전송하는 상호인증 방법.

청구항 4

제 1 항에 있어서, 상기 제1응답 신호를 수신하는 단계는

상기 모바일 단말에서 상기 제1챌린지 신호를 수신하면, 상기 모바일 단말의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 및 상기 제1 챌린지 신호 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 생성된 제1응답 신호를 수신하는 상호인증 방법.

청구항 5

제 1 항에 있어서, 상기 쿼리 신호를 상기 인증서버로 전송하는 단계는

상기 제1응답 신호를 수신하면, 상기 인증 에이전트와 상기 모바일 단말 대한 인증을 요청하는 쿼리 신호를 생성하여 상기 인증서버로 전송하는 상호인증 방법.

청구항 6

제 1 항에 있어서, 상기 제2챌린지 신호를 수신하는 단계는

상기 인증서버에서 상기 쿼리 신호를 수신하면, Nonce값, 난수, 시간 중 어느 하나를 포함하는 제2임의정보에 대한 해쉬값으로 생성된 제2챌린지 신호를 수신하는 상호인증 방법.

청구항 7

제 1 항에 있어서, 상기 제2응답 신호를 상기 인증서버로 전송하는 단계는

상기 인증 에이전트의 시드값(SEED_AG), 키 값(KEY_AG), 식별정보(ID_AG) 및 상기 제2챌린지 신호 중 어느 하

나를 포함하는 인증 에이전트에 대한 정보를 기초로 제2응답 신호를 생성하여 상기 인증서버로 전송하는 상호인증 방법.

청구항 8

제 1 항에 있어서, 상기 제2응답 신호를 상기 인증서버로 전송하는 단계는

상기 제1응답 신호, 상기 모바일 단말의 식별정보(ID_M), 상기 인증 에이전트의 식별정보(ID_AG) 및 상기 제2챌린지 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 제2응답 신호를 생성하여 상기 인증서버로 전송하는 상호인증 방법.

청구항 9

제 7 항 또는 제 8 항에 있어서,

상기 인증서버로부터 상기 제2응답 신호를 이용하여 상기 모바일 단말 및 상기 인증 에이전트를 인증받는 단계; 및

상기 모바일 단말 및 상기 인증 에이전트가 인증되면, 상기 인증서버로부터 상기 모바일 단말의 키 값(KEY_M) 및 상기 인증 에이전트의 키 값(KEY_AG)을 이용하여 각각의 시드값(SEED_M, SEED_AG)을 새로운 시드값(SEED_M', SEED_AG')으로 갱신받는 단계;를 더 포함하는 상호인증 방법.

청구항 10

제 1 항에 있어서, 상기 제1회답 신호를 수신하는 단계는

상기 모바일 단말의 시드값(SEED_M), 식별정보(ID_M), 상기 인증 에이전트의 시드값(SEED_AG), 식별정보(ID_AG), 제2응답 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 생성된 제1회답 신호를 수신하는 상호인증 방법.

청구항 11

제 1 항에 있어서, 상기 제1회답 신호를 수신하는 단계는

상기 모바일 단말의 키 값(KEY_M)에 의해 암호화한 상기 모바일 단말의 시드값(SEED_M) 및 상기 인증 에이전트의 시드값(SEED_AG)을 포함하는 인증 에이전트에 대한 정보를 기초로 생성된 제1회답 신호를 수신하는 상호인증 방법.

청구항 12

제 9 항에 있어서, 상기 제1회답 신호를 수신하는 단계는

상기 모바일 단말의 새로운 시드값(SEED_M'), 식별정보(ID_M), 상기 인증 에이전트의 새로운 시드값(SEED_AG'), 식별정보(ID_AG), 제2응답 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 생성된 제1회답 신호를 수신하는 상호인증 방법.

청구항 13

제 10 항 내지 제 12 항 중 어느 한 항에 있어서, 상기 제1회답 신호를 수신하는 단계는

상기 모바일 단말에 대한 정보를 상기 인증 에이전트의 키 값(KEY_AG)에 의해 암호화한 암호화 데이터를 생성하여 상기 제1회답 신호와 함께 수신하는 상호인증 방법.

청구항 14

제 13 항에 있어서,

상기 인증 에이전트의 키 값(KEY_AG)을 이용하여 상기 암호화 데이터를 복호화한 복호화 데이터를 생성하는 단계;를 더 포함하는 상호인증 방법.

청구항 15

제 10 항 내지 제 14 항 중 어느 한 항에 있어서,

상기 제1회답 신호를 이용하여 상기 인증서버를 인증하는 단계; 및

상기 인증서버가 인증되면, 상기 인증 에이전트의 시드값(SEED_AG)을 새로운 시드값(SEED_AG')으로 갱신하는 단계;를 더 포함하는 상호인증 방법.

청구항 16

제 1 항에 있어서, 상기 제2회답 신호를 상기 모바일 단말로 전송하는 단계는

제1응답 신호, 상기 모바일 단말의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 생성한 제2회답 신호를 상기 모바일 단말로 전송하는 상호인증 방법.

청구항 17

제 1 항에 있어서, 상기 제2회답 신호를 상기 모바일 단말로 전송하는 단계는

상기 인증 에이전트의 새로운 시드값(SEED_AG'), 식별정보(ID_AG), 제1응답 신호 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 제2회답 신호를 생성하여 상기 모바일 단말로 전송하는 상호인증 방법.

청구항 18

제 16 항 또는 제 17 항에 있어서,

상기 모바일 단말에서 상기 제2회답 신호를 이용하여 상기 인증서버를 인증하는 단계; 및

상기 인증서버가 인증되면, 상기 모바일 단말의 시드값(SEED_M)을 새로운 시드값(SEED_M')으로 갱신하는 단계;를 더 포함하는 상호인증 방법.

청구항 19

모바일 단말과 인증서버 간에 위치하는 인증 에이전트를 통해 상호인증을 수행하는 시스템에 있어서,

Nonce값, 난수, 시간 중 어느 하나를 포함하는 제1임의정보에 대한 해쉬값으로 제1챌린지 신호를 생성하여 상기 모바일 단말로 전송하고, 상기 모바일 단말로부터 상기 제1챌린지 신호에 대응하는 제1응답 신호를 수신하며, 상기 제1응답 신호를 이용하여 상기 모바일 단말에 대한 인증을 위한 쿼리신호 및 제2응답 신호를 생성하여 상기 인증서버로 전송하여 상기 모바일 단말 및 상기 인증서버를 상호인증시키는 인증 에이전트;

상기 쿼리 신호를 수신하면, Nonce값, 난수, 시간 중 어느 하나를 포함하는 제2임의정보에 대한 해쉬값으로 제2챌린지 신호를 생성하여 상기 인증 에이전트로 전송하고, 상기 인증 에이전트로부터 상기 제2챌린지 신호에 대응하는 제2응답 신호를 수신하며, 상기 제2응답 신호를 이용하여 상기 모바일 단말 및 상기 인증 에이전트에 대한 시드값(SEED_M', SEED_AG')을 갱신하여 생성한 제1회답신호를 상기 인증 에이전트로 전송하여 상기 모바일 단말을 인증하는 인증서버; 및

상기 제1챌린지 신호를 수신하면, 상기 모바일 단말의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 및 상기 제1 챌린지 신호 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 제1응답 신호를 생성하여 상기 인증 에이전트로 전송하고, 상기 제1응답 신호, 상기 제2회답 신호를 이용하여 상기 모바일 단말의 시드값(SEED_M')을 갱신하여 상기 인증서버를 인증하는 모바일 단말;을 포함하는 상호인증을 수행하는 시스템.

청구항 20

제 19 항에 있어서,

상기 모바일 단말, 상기 인증 에이전트 및 상기 인증서버에서 송수신되는 챌린지 신호, 응답 신호 및 회답 신호는 해쉬 함수를 이용하여 생성되는 상호인증을 수행하는 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 인증 기술에 관한 것으로, 특히, 모바일 단말의 상호인증 시스템 및 상호인증 방법에 관한 것이다.

배 경 기 술

[0002] 양방향 통신망 기반에서 멀티미디어 데이터(콘텐츠)를 전송하는 데이터 서버(인증서버)와 수신 단말(또는 사용자) 사이에 상호인증이 수행되어야 한다. 일반적으로 상호인증을 위한 수단으로는 관련 정보를 오프라인으로 발급한 저장/입출력 장치(스마트카드, PCMCIA 카드 등)을 이용한다. 이러한 저장된 정보의 갱신은 재발급으로 가능하므로 시간 및 추가 비용이 소요된다.

[0003] 또한, IT 인프라를 기반으로 하는 서비스들은 사용자의 위치 정보 및 신원 정보 등의 개인 정보들을 많이 다루게 되며, 이로 인하여 유출 위험도 크게 증가되고 있다. 이에 각종 장치(디바이스, 기기, 단말 등)의 인증 관리의 필요성이 증가하고 있으며, 사람과 사람, 사람과 장치(디바이스,기기, 단말 등), 장치(디바이스,기기, 단말 등)와 장치(디바이스,기기, 단말 등)간과 같은 인증 대상 확대로 이 기종 장치(디바이스,기기, 단말 등)간의 인증 기술도 필요하다.

[0004] 또한, 단순 인증서 기반 솔루션은 인증 정보가 탑재된 디바이스 하드웨어 정보를 포함하지 않아서 복제에 취약하다. 하드웨어 기반 인식 솔루션은 하드웨어 정보만으로 장치(디바이스,기기, 단말 등)를 인식하여 장치(디바이스,기기, 단말 등)와 사람간의 상호연동 및 보안성이 미흡하다.

[0005] 한편, 인증 보안 시스템은 인증서버 및 모바일 단말 등을 포함하여 구성되며, 보안 및 신원(또는 장치) 인증 등에 널리 사용되고 있다.

[0006] 인증서버는 각 모바일 단말에 대한 식별정보(ID), 키(KEY) 및 데이터를 저장하는 식별정보 목록을 가지고 있다. 또한 모바일 단말은 자신의 식별정보(ID) 및 키(KEY)를 저장한다.

[0007] 또한, 인증서버는 모바일 단말로 식별정보 요청 명령과 함께 챌린지에 대한 해쉬값을 함께 전송하고, 모바일 단말은 해쉬값 및 자신의 식별정보(ID)와 키(KEY)를 해쉬한 단말 해쉬값을 인증서버로 전송한다.

[0008] 또한 인증서버는 모바일 단말로부터 수신된 단말 해쉬값, 챌린지 해쉬값, 데이터를 이용하여 식별정보 목록으로부터 해당하는 모바일 단말에 대한 식별정보(ID) 및 키(KEY)를 검출한다. 또한, 인증서버는 챌린지를 생성하여 모바일 단말로 전송하며, 상기 챌린지를 이용하여 해당 모바일 단말과 공유하는 새로운 키를 생성하여 저장한다.

[0009] 그러나, 모바일 단말에서 인증서버로 단말 해쉬값, 챌린지에 대한 해쉬값, 및 데이터를 전송하는 부분에서는 암호화가 이루어지지 않는다. 따라서, 도청 및 트래픽 분석을 통해 인증서버에서 확인을 해야 하는 사항인 챌린지에 대한 해쉬값과 및 데이터, 즉 입력과 출력이 노출될 수 있으며, 도청 및 트래픽 분석을 통해 해쉬 함수의 노출로 이어져, 인증서버에서 모바일 단말로 전송하는 데이터를 취득할 수 있다는 문제가 발생할 수 있다.

발명의 내용

해결하려는 과제

[0010] 본 발명은 인증 보안 시스템의 객체인 모바일 단말, 인증 에이전트 및 인증서버가 챌린지를 이용하여 상호 인증하며, 인증된 객체들 사이에서만 데이터를 주고받도록 함으로써, 데이터 유출을 방지하고자 한다.

[0011] 또한, 본 발명은 각 객체에 저장된 데이터의 갱신은 온라인으로 챌린지 및 응답을 주고 받음으로써 효과적인 데이터 갱신 방법을 제공하고자 한다.

[0012] 또한, 본 발명은 사람과 사람, 사람과 장치(디바이스, 기기, 단말 등), 장치(디바이스, 기기, 단말 등)와 장치(디바이스, 기기, 단말 등)간과 같은 다양한 인증 대상의 확대로 인한 이 기종 장치(디바이스, 기기, 단말 등) 간의 상호인증 기술을 제공하고자 한다.

[0013] 또한, 본 발명은 멀티미디어 데이터(콘텐츠) 전송 서버와 수신 단말간의 송수신되는 데이터의 안전함을 보장받을 수 있기 때문에 도청 등의 보안 위협에 따른 공격을 방어할 수 있다.

[0014] 또한, 본 발명은 안전한 멀티미디어 데이터(콘텐츠) 송수신을 제공할 수 있는 방법을 제공하고자 한다.

과제의 해결 수단

[0015] 본 발명의 일 양상에 따른 모바일 단말과 인증서버 간에 위치하는 인증 에이전트를 통해 상호인증을 수행하는 방법은 제1임의정보를 이용하여 생성한 제1챌린지 신호를 모바일 단말로 전송하는 단계, 모바일 단말로부터 모바일 단말에 대한 정보에 기초하여 생성한 제1응답 신호를 수신하는 단계, 모바일 단말 및 인증 에이전트에

대한 인증을 위한 쿼리 신호를 인증서버로 전송하는 단계, 인증서버로부터 제2임의정보를 이용하여 생성한 제2챌린지 신호를 수신하는 단계, 인증 에이전트에 대한 정보에 기초하여 생성한 제2응답 신호를 인증서버로 전송하는 단계, 인증서버로부터 인증 에이전트에 대한 정보에 기초하여 생성한 제1회답 신호를 수신하는 단계 및, 모바일 단말에 대한 정보에 기초하여 생성한 제2회답 신호를 모바일 단말로 전송하는 단계를 포함할 수 있다.

[0016] 또한, 인증 에이전트와 모바일 단말에 각각 시드값(SEED_M, SEED_AG), 키 값(KEY_M, KEY_ID), 식별정보(ID_M, ID_AG)를 부여하고, 부여된 시드값(SEED_M, SEED_AG), 키 값(KEY_M, KEY_ID), 식별정보(ID_M, ID_AG)를 인증서버에 저장시키는 단계를 더 포함할 수 있다.

[0017] 또한, 제1챌린지 신호를 모바일 단말로 전송하는 단계는 Nonce값, 난수, 시간 중 어느 하나를 포함하는 제1임의정보에 대한 해쉬값으로 제1챌린지 신호를 생성하여 모바일 단말로 전송한다.

[0018] 또한, 제1응답 신호를 수신하는 단계는 모바일 단말에서 제1챌린지 신호를 수신하면, 모바일 단말의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 및 제1 챌린지 신호 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 생성된 제1응답 신호를 수신한다.

[0019] 또한, 쿼리 신호를 인증서버로 전송하는 단계는 제1응답 신호를 수신하면, 인증 에이전트와 모바일 단말 대한 인증을 요청하는 쿼리 신호를 생성하여 인증서버로 전송한다.

[0020] 또한, 제2챌린지 신호를 수신하는 단계는 인증서버에서 쿼리 신호를 수신하면, Nonce값, 난수, 시간 중 어느 하나를 포함하는 제2임의정보에 대한 해쉬값으로 생성된 제2챌린지 신호를 수신한다.

[0021] 또한, 제2응답 신호를 인증서버로 전송하는 단계는 인증 에이전트의 시드값(SEED_AG), 키 값(KEY_AG), 식별정보(ID_AG) 및 제2챌린지 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 제2응답 신호를 생성하여 인증서버로 전송한다.

[0022] 또한, 제2응답 신호를 인증서버로 전송하는 단계는 제1응답 신호, 모바일 단말의 식별정보(ID_M), 인증 에이전트의 식별정보(ID_AG) 및 제2챌린지 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 제2응답 신호를 생성하여 인증서버로 전송한다.

[0023] 또한, 인증서버로부터 제2응답 신호를 이용하여 모바일 단말 및 인증 에이전트를 인증받는 단계 및, 모바일 단말 및 인증 에이전트가 인증되면, 인증서버로부터 모바일 단말의 키 값(KEY_M) 및 인증 에이전트의 키 값(KEY_AG)을 이용하여 각각의 시드값(SEED_M, SEED_AG)을 새로운 시드값(SEED_M', SEED_AG')으로 갱신받는 단계를 더 포함할 수 있다.

[0024] 또한, 제1회답 신호를 수신하는 단계는 모바일 단말의 시드값(SEED_M), 식별정보(ID_M), 인증 에이전트의 시드값(SEED_AG), 식별정보(ID_AG), 제2응답 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 생성된 제1회답 신호를 수신한다.

[0025] 또한, 제1회답 신호를 수신하는 단계는 모바일 단말의 키 값(KEY_M)에 의해 암호화한 모바일 단말의 시드값(SEED_M) 및 인증 에이전트의 시드값(SEED_AG)을 포함하는 인증 에이전트에 대한 정보를 기초로 생성된 제1회답 신호를 수신한다.

[0026] 또한, 제1회답 신호를 수신하는 단계는 모바일 단말의 새로운 시드값(SEED_M'), 식별정보(ID_M), 인증 에이전트의 새로운 시드값(SEED_AG'), 식별정보(ID_AG), 제2응답 신호 중 어느 하나를 포함하는 인증 에이전트에 대한 정보를 기초로 생성된 제1회답 신호를 수신한다.

[0027] 또한, 제1회답 신호를 수신하는 단계는 모바일 단말에 대한 정보를 인증 에이전트의 키 값(KEY_AG)에 의해 암호화한 암호화 데이터를 생성하여 제1회답 신호와 함께 수신한다.

[0028] 또한, 인증 에이전트의 키 값(KEY_AG)을 이용하여 암호화 데이터를 복호화한 복호화 데이터를 생성하는 단계를 더 포함할 수 있다.

[0029] 또한, 제1회답 신호를 이용하여 인증서버를 인증하는 단계 및, 인증서버가 인증되면, 인증 에이전트의 시드값(SEED_AG)을 새로운 시드값(SEED_AG')으로 갱신하는 단계를 더 포함할 수 있다.

[0030] 또한, 제2회답 신호를 모바일 단말로 전송하는 단계는 제1응답 신호, 모바일 단말의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 생성한 제2회답 신호를 모바일 단말로 전송한다.

[0031] 또한, 제2회답 신호를 모바일 단말로 전송하는 단계는 인증 에이전트의 새로운 시드값(SEED_AG'), 식별정보(ID_AG), 제1응답 신호 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 제2회답 신호를 생성하여 모바일 단말로 전송한다.

[0032] 또한, 모바일 단말에서 제2회답 신호를 이용하여 인증서버를 인증하는 단계 및, 인증서버가 인증되면, 모바일 단말의 시드값(SEED_M)을 새로운 시드값(SEED_M')으로 갱신하는 단계를 더 포함할 수 있다.

[0033] 본 발명의 일 양상에 따른 모바일 단말과 인증서버 간에 위치하는 인증 에이전트를 통해 상호인증을 수행하는 시스템은 Nonce값, 난수, 시간 중 어느 하나를 포함하는 제1임의정보에 대한 해쉬값으로 제1챌린지 신호를 생성하여 모바일 단말로 전송하고, 모바일 단말로부터 제1챌린지 신호에 대응하는 제1응답 신호를 수신하며, 제1응답 신호를 이용하여 모바일 단말에 대한 인증을 위한 쿼리신호 및 제2응답 신호를 생성하여 인증서버로 전송하여 모바일 단말 및 인증서버를 상호인증시키는 인증 에이전트, 쿼리 신호를 수신하면, Nonce값, 난수, 시간 중 어느 하나를 포함하는 제2임의정보에 대한 해쉬값으로 제2챌린지 신호를 생성하여 인증 에이전트로 전송하고, 인증 에이전트로부터 제2챌린지 신호에 대응하는 제2응답 신호를 수신하며, 제2응답 신호를 이용하여 모바일 단말 및 인증 에이전트에 대한 시드값(SEED_M', SEED_AG')을 갱신하여 생성한 제1회답신호를 인증 에이전트로 전송하여 모바일 단말을 인증하는 인증서버 및 제1챌린지 신호를 수신하면, 모바일 단말의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 및 제1 챌린지 신호 중 어느 하나를 포함하는 모바일 단말에 대한 정보를 기초로 제1응답 신호를 생성하여 인증 에이전트로 전송하고, 제1응답 신호, 제2회답 신호를 이용하여 모바일 단말의 시드값(SEED_M')을 갱신하여 인증서버를 인증하는 모바일 단말을 포함할 수 있다.

[0034] 또한, 모바일 단말, 인증 에이전트 및 인증서버에서 송수신되는 챌린지 신호, 응답 신호 및 회답 신호는 해쉬함수를 이용하여 생성된다.

발명의 효과

[0035] 상호인증 장치의 객체인 모바일 단말 및 인증서버가 챌린지를 이용하여 상호 인증하고, 인증된 객체들 사이에서만 데이터를 주고받도록 하여, 데이터 유출을 방지할 수 있다.

[0036] 또한, 모바일 단말과 인증서버의 인증은 인증 에이전트를 통하여 이루어짐으로써 인증서버의 부하를 줄이고, 다수의 모바일 단말들과의 상호인증을 수행할 수 있다.

[0037] 또한, 사람과 사람간, 사람과 장치간, 장치와 장치간 등 상호인증을 통해 인식이 이루어지도록 하며, 출입통제, 신원확인, 키 배포 등의 다양한 보안 시스템에 적용하여 보안을 강화할 수 있다.

도면의 간단한 설명

[0038] 도 1은 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 시스템 및 그 동작과정을 나타낸 도면이다.

도 2는 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 모바일 단말을 나타낸 블록도이다.

도 3은 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 인증 에이전트를 나타낸 블록도이다.

도 4는 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 인증서버를 나타낸 블록도이다.

도 5는 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 과정을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0039] 이하, 첨부된 도면을 참조하여 본 발명의 일 실시예를 상세하게 설명한다.

[0040] 도 1은 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 시스템 및 그 동작과정을 나타낸 도면이다.

[0041] 초기 상태에서 모바일 단말(110)과 인증 에이전트(120)는 각각 시드값(SEED), 키 값(KEY), 식별 정보(ID)를 보유하고 있으며, 각각의 시드값(SEED), 키 값(KEY), 식별 정보(ID)는 인증서버(130)에 저장된다.

[0042] 본 발명의 일 양상에 따른 상호인증을 수행하는 시스템은 모바일 단말(110), 인증 에이전트(120) 및 인증서버(130)는 초기 상태에서 모바일 단말(110) 및 인증 에이전트(120)는 각각 {SEED_M, KEY_M, ID_M}, {SEED_AG, KEY_AG, ID_AG}를 가지며, 인증서버(130)는 {데이터, SEED_M, KEY_M, ID_M, 다른 모바일 단말 정보, SEED_AG,

KEY_AG, ID_AG, 다른 인증 에이전트 정보}를 가진다. 이때, 상술한 바와 같이, SEED는 시드값, KEY는 키 값, ID는 식별 정보를 나타낸다.

[0043] 인증 에이전트(120)는 제1챌린지 신호를 생성하여, 제1챌린지 신호를 모바일 단말 측으로 송신한다(111). 이때, 제1챌린지 신호는 상호인증을 위한 임의의 정보(Nonce, 난수, 시간 등)의 해쉬값으로 이러한 정보는 인증 에이전트(120)에서 생성된다.

[0044] 모바일 단말(110)은 제1챌린지 신호에 대한 응답으로서, 모바일 단말(110)에 관련된 시드값(SEED_M), 키 값(KEY_M), 식별 정보(ID_M) 및 제1챌린지 신호 중에서 적어도 어느 하나에 기초하여 생성된 제1응답 신호를 인증 에이전트(120) 측으로 송신한다(112).

[0045] 제1응답 신호를 수신한 인증 에이전트(120)는 인증 에이전트(120) 및 모바일 단말(110)의 인증을 위한 쿼리 신호를 인증서버(130) 측으로 송신한다(113).

[0046] 인증서버(130)는 쿼리 신호에 대한 응답으로서, 제2챌린지 신호를 생성하여, 제2 챌린지 신호를 인증 에이전트(120)측으로 송신한다(114). 이때, 제2챌린지 신호는 상호인증을 위한 임의의 정보(Nonce, 난수, 시간 등)의 해쉬 값으로 그 정보는 인증서버(130)에서 생성한다.

[0047] 인증 에이전트(120)는 인증 에이전트(120)에 관련된 시드값(SEED_AG), 키 값(KEY_AG), 식별 정보(ID_AG) 및 제2 챌린지 신호를 이용하여, 제2 응답 신호를 생성한다. 이때, 인증 에이전트(120)는 제1응답 신호, 모바일 단말(110)에 관련된 식별 정보(ID_M), 인증 에이전트(120)에 관련된 식별정보(ID_AG), 제1챌린지 신호 중에서 적어도 어느 하나를 포함하여, 제2응답 신호를 생성할 수 있다.

[0048] 인증 에이전트(120)는 이렇게 생성된 제2응답 신호를 인증서버(130) 측으로 송신한다(115).

[0049] 인증서버(130)는 수신된 제2응답 신호를 검증한다. 다시 말해, 인증서버(130)에서 모바일 단말(110) 및 인증 에이전트(120)의 각각 식별 정보(ID_M) 및 식별 정보(ID_AG), 시드 값(SEED_M) 및 시드 값(SEED_AG), 그리고 키 값(KEY_M) 및 키 값(KEY_AG)을 이용하여, 모바일 단말(110) 및 인증 에이전트(120)를 검증하게 된다.

[0050] 인증서버(130)는 모바일 단말(110) 및 인증 에이전트(120)가 검증되면, 모바일 단말(110)에 관련된 키 값(KEY_M) 및 키 값(KEY_AG)을 이용하여 모바일 단말(110) 및 인증 에이전트(120)에 관련된 각각의 시드 값(SEED_M) 및 시드 값(SEED_AG)을 갱신한다(SEED_M´, SEED_AG´).

[0051] 또한, 갱신된 시드값(SEED_M´, SEED_AG´)과 모바일 단말(110)의 식별 정보(ID_M) 및 인증 에이전트(120)의 식별 정보(IDR_AG)를 이용하여 제1회답 신호를 생성한다. 즉, 제1회답 신호는, 모바일 단말(110)의 키 값(KEY_M)에 의하여 암호화한 모바일 단말(110)의 시드값(SEED_M) 및 모바일 단말(110)의 식별 정보(ID_M)에 기초하여 생성될 수 있다.

[0052] 이후, 인증서버(130)는 모바일 단말(110)에 관련된 데이터를 인증 에이전트(120)의 키 값(KEY_AG)에 의하여 암호화한 암호화 데이터(EDATA-KEY_AG)를 생성한다.

[0053] 인증서버(130)는 상기와 같이 생성된, 제1회답 신호 및 암호화 데이터(EDATA-KEY_AG)를 인증 에이전트(120) 측으로 송신한다(116).

[0054] 인증 에이전트(120)는 제2응답 신호에 대한에 대한 회답으로서, 인증서버(130)로부터, 인증 에이전트(120) 및 모바일 단말(110)의 검증 여부에 기초한 제1회답 신호를 수신한다(116). 즉, 인증 에이전트(120)는 제1회답 신호 및 암호화 데이터를 수신하고, 인증서버(130)에 대한 검증을 수행하게 된다.

[0055] 인증 에이전트(120)는 상기 인증서버(130)를 정당한 인증서버인 것으로 검증한 경우에는, 키 값(KEY_AG)을 이용하여 암호화 데이터를 복호화하여 복호화 데이터(DATA)를 얻는다.

[0056] 인증 에이전트(120)는 인증 에이전트(120)에 관한 키 값(KEY_AG´)을 계산하고, 인증에이전트(120)에 관한 시드값(SEED_AG) 및 키 값(KEY_AG)을, 인증을 수행하기 위한 새로운 시드값(SEED_AG´) 및 키 값(KEY_AG´)으로 업데이트 한다.

[0057] 이후, 인증 에이전트(120)는 모바일 단말(110)에 관련된 제2회답 신호를 모바일 단말(110) 측으로 송신한다(117).

[0058] 이후, 모바일 단말(110)는 인증 에이전트(120)로부터 수신한 제2회답 신호를 이용하여 시드값(SEED_M´)을 계산하고, 인증서버(130)를 검증할 수 있다.

[0059] 모바일 단말(110) 측에서 인증서버(130)에 대한 검증이 이루어진 경우에는, 키 값(KEY_M´)을 계산하고, 모바일 단말(110)에 관한 시드값(SEED_M) 및 키 값(KEY_M)을 각각 시드값(SEED_M´) 및 키 값(KEY_M´)으로 업데이트한 후 종료한다.

[0060] 이후, 모바일 단말(110), 인증 에이전트(120), 및 인증서버(130) 각각의 시드값(SEED)과 키 값(KEY)이 모두 업데이트 되어있기 때문에, 다수의 모바일 단말(110)이 있는 경우, 그 수에 맞추어 인증 에이전트(120) 및 모바일 단말(110) 간의 제1 챌린지 단계(111)부터 다시 수행하게 된다.

[0061] 또한, 모바일 단말, 인증 에이전트 및 인증서버에서 챌린지/응답/회답 신호는 해쉬 함수를 이용하여 송수신하고, 데이터 암호화 및 복호화는 XOR(exclusive or) 연산 또는 대칭키 암호 알고리즘(DES, 3DES, AES 등) 등을 이용할 수 있다.

[0062] 도 2는 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 모바일 단말을 나타낸 블록도이다. 도 2를 참조하면, 모바일 단말(200)은 신호 수신부(210), 신호 제어부(220), 신호 송신부(230)을 포함할 수 있다.

[0063] 신호 수신부(210)는 제1챌린지 신호를 수신한다.

[0064] 신호 제어부(220)는 제1챌린지 신호에 대한 응답으로서, 모바일 단말(200)에 관련된 시드값(SEED_M), 키 값(KEY_M), 식별 정보(ID_M) 및 제1챌린지 신호 중에서 적어도 어느 하나에 기초하여 생성된 제1응답 신호를 생성한다.

[0065] 또한, 신호 제어부(220)는 모바일 단말(200)에 관련된 제1응답 신호를 인증 에이전트 측으로 송신하여, 모바일 단말(200)이 인증서버를 검증하도록 제어할 수 있다.

[0066] 또한, 신호 제어부(220)는 모바일 단말(200) 측에서 인증서버의 검증이 이루어진 경우, 모바일 단말(200)의 시드값(SEED_M) 및 모바일 단말의 키 값(KEY_M)을 갱신하도록 제어할 수 있다.

[0067] 또한, 모바일 단말(200)은 제1챌린지 신호를 수신하면, 모바일 단말(200)의 시드값(SEED_M), 키 값(KEY_M), 식별정보(ID_M) 및 제1 챌린지 신호 중 어느 하나를 포함하는 모바일 단말(200)에 대한 정보를 기초로 제1응답 신호를 생성하여 인증 에이전트로 전송하고, 제1응답 신호 및 제2회답 신호를 이용하여 모바일 단말(200)의 시드값(SEED_M´)을 갱신하여 인증서버를 인증할 수 있다.

[0068] 도 3은 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 인증 에이전트를 나타낸 블록도이다. 도 3을 참조하면, 상호인증을 수행하는 인증 에이전트(300)는, 신호 수신부(310), 신호 제어부(320) 및 신호 송신부(330)를 포함할 수 있다.

[0069] 신호 제어부(320)는 제1챌린지 신호를 생성한다.

[0070] 신호 송신부(330)는 제1챌린지 신호를 모바일 단말 측으로 송신한다.

[0071] 신호 수신부(310)는 제1챌린지 신호에 대한 응답으로서, 모바일 단말에 관련된 시드값(SEED_M), 키 값(KEY_M), 식별 정보(ID_M) 및 제1챌린지 신호 중에서 적어도 어느 하나에 기초하여 생성된 제1응답 신호를 모바일 단말로부터 수신한다.

[0072] 이때, 신호 수신부(310)는 모바일 단말에 관련된 식별 정보(ID_M)를 포함하는 제1응답 신호를 모바일 단말로부터 수신할 수 있다.

[0073] 이후, 신호 송신부(330)는 인증 에이전트 및 모바일 단말의 인증을 위한 쿼리 신호를 인증서버 측으로 송신하고, 신호 수신부(310)는 쿼리 신호에 대한 응답으로서, 인증서버로부터 쿼리에 대한 제2챌린지 신호를 수신할 수 있으며, 신호 제어부(320)는 인증 에이전트에 관련된 시드값(SEED_AG), 키값(KEY_AG), 식별 정보(ID_AG) 및 제2챌린지 신호 중에서 적어도 어느 하나에 기초하여, 제2응답 신호를 생성할 수 있다.

[0074] 또한, 신호 송신부(330)는 생성된 제2응답 신호를 인증서버 측으로 송신하고, 신호 수신부(310)는 제2응답 신호에 대한에 대한 회답으로서, 인증서버로부터 인증 에이전트 및 모바일 단말의 검증 여부에 기초한, 제2회답 신호를 수신할 수 있다.

[0075] 이때, 신호 수신부(310)는 인증서버로부터 제1회답 신호 및 모바일 단말에 관련된 데이터를 인증 에이전트의 키 값(KEY_M)에 의하여 암호화한 암호화 데이터(EDATA-KEY_AG) 중에서 적어도 어느 하나를 포함하는, 제1회답 신호를 수신할 수 있다.

[0076] 이때, 제1회답 신호는 인증 에이전트의 키 값(KEY_AG)에 의하여 암호화한 인증 에이전트의 시드값(SEED_AG)

및 인증 에이전트의 식별 정보(ID_AG)에 기초하여 생성될 수 있다.

[0077] 또한, 모바일 단말에 관련된 제1회답 신호는, 모바일 단말의 키 값(KEY_M)에 의하여 암호화한 모바일 단말의 시드값(SEED_M) 및 모바일 단말에 관련된 식별 정보(ID_M)에 기초하여 생성될 수 있다.

[0078] 또한 신호 제어부(320)는 제2회답 신호에 기초하여, 인증서버를 검증할 수 있다.

[0079] 이때, 신호 제어부(320)는 제1응답 신호, 모바일 단말에 관련된 식별 정보(ID_M), 인증 에이전트에 관련된 식별 정보(ID_AG), 제1챌린지 신호 중에서 적어도 어느 하나를 포함하는, 제2응답 신호를 생성할 수 있다.

[0080] 또한, 신호 제어부(320)는 인증서버의 검증이 이루어진 경우, 암호화 데이터(EDATA_KEY_AG)를 인증 에이전트의 키 값(KEY_AG)에 의해 복호화하여 데이터(DATA)를 획득할 수 있다.

[0081] 또한, 신호 제어부(320)는 제1회답 신호 및 인증 에이전트의 키 값(KEY_AG)을 이용하여, 인증 에이전트의 키 값(KEY_AG)을 갱신할 수 있다.

[0082] 또한, 신호 제어부(320)는 모바일 단말에 관련된 제1회답 신호를 모바일 단말 측으로 송신하여, 모바일 단말이 인증서버를 검증하도록 제어할 수 있다.

[0083] 또한, 신호 제어부(320)는 모바일 단말 측에서 인증서버의 검증이 이루어진 경우, 모바일 단말의 시드값(SEED_M) 및 모바일 단말의 키 값(KEY_M)을 갱신하도록 제어할 수 있다.

[0084] 또한, 인증 에이전트는 Nonce값, 난수, 시간 중 어느 하나를 포함하는 임의정보에 대한 해쉬값으로 제1챌린지 신호를 생성하여 모바일 단말로 전송하고, 모바일 단말로부터 제1챌린지 신호에 대응하는 제1응답 신호를 수신하며, 제1응답 신호를 이용하여 모바일 단말에 대한 인증을 위한 쿼리신호 및 제2응답 신호를 생성하여 인증서버로 전송하여 모바일 단말 및 인증서버를 상호 인증시킬 수 있다.

[0085] 도 4는 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 인증서버를 나타낸 블록도이다. 도 4를 참조하면, 상호인증이 가능한 인증서버(400)는 신호 수신부(410), 신호 제어부(420) 및 신호 송신부(430)를 포함할 수 있다.

[0086] 신호 수신부(410)는 인증 에이전트로부터 인증 에이전트 및 모바일 단말의 인증을 위한 쿼리신호를 수신한다.

[0087] 신호 제어부(420)는 쿼리 신호에 대한 응답으로서, 인증서버로부터 쿼리에 대한 제2챌린지 신호를 생성한다.

[0088] 신호 송신부(430)는 제2챌린지 신호를 인증 에이전트 측으로 송신한다.

[0089] 이때, 신호 수신부(410)는 제2챌린지 신호에 대한 응답으로서, 인증 에이전트에 관련된 시드값(SEED_AG), 키 값(KEY_AG), 식별 정보(ID_AG) 및 제2챌린지 신호 중에서 적어도 어느 하나에 기초하여 생성된, 인증 에이전트의 제2응답 신호를 수신한다.

[0090] 신호 제어부(420)는 인증 에이전트의 제2응답 신호에 대한에 대한 회답으로서, 인증 에이전트 측으로 인증 에이전트 및 모바일 단말의 검증 여부에 기초한 제1회답 신호를 송신하도록 신호 송신부(430)를 제어한다.

[0091] 또한, 신호 제어부(420)는 모바일 단말에 관련된 회답 신호 및 모바일 단말에 관련된 데이터를 인증 에이전트의 키 값(KEY_AG)에 의하여 암호화한 암호화 데이터(EDATA-KEY_AG) 중에서 적어도 어느 하나를 포함하는 제1회답신호를 송신하도록 신호 송신부(430)를 제어하고, 인증 에이전트가 제1회답 신호에 기초하여 인증서버(400)를 검증하도록 한다.

[0092] 이때, 회답 신호는, 인증 에이전트의 키 값(KEY_AG)에 의하여 암호화한 인증 에이전트의 시드값(SEED_AG) 및 인증 에이전트의 식별 정보(ID_AG)에 기초하여 생성될 수 있다.

[0093] 또한, 인증서버는 쿼리 신호를 수신하면, Nonce값, 난수, 시간 중 어느 하나를 포함하는 임의정보에 대한 해쉬값으로 제2챌린지 신호를 생성하여 인증 에이전트로 전송하고, 인증 에이전트로부터 제2챌린지 신호에 대응하는 제2응답 신호를 수신하며, 제2응답 신호를 이용하여 모바일 단말 및 인증 에이전트에 대한 시드값(SEED_M', SEED_AG')을 갱신하여 생성한 제1회답신호를 인증 에이전트로 전송하여 모바일 단말을 인증할 수 있다.

[0094] 이상과 같이 본 발명은 비록 한정된 실시 예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시 예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0095] 도 5는 본 발명의 바람직한 일 실시예에 따른 상호인증을 수행하는 과정을 나타낸 흐름도이다.

[0096] 도 5는 모바일 단말과 인증서버 간에 위치하는 인증 에이전트를 통해 상호인증을 수행하는 방법을 나타낸 것이다.

[0097] 먼저, 인증 에이전트에서 제1임의정보를 이용하여 생성한 제1챌린지 신호를 모바일 단말로 전송한다(500).

[0098] 모바일 단말에서 모바일 단말에 대한 정보에 기초하여 생성한 제1응답 신호를 인증 에이전트로 전송하고(510), 인증 에이전트에서 모바일 단말 및 인증 에이전트에 대한 인증을 위한 쿼리 신호를 인증서버로 전송한다(520).

[0099] 인증서버에서 제2임의정보를 이용하여 생성한 제2챌린지 신호를 인증 에이전트로 전송한다(530).

[0100] 다음으로, 인증 에이전트에서 인증 에이전트에 대한 정보에 기초하여 생성한 제2응답 신호를 인증서버로 전송한다(540).

[0101] 인증서버에서 인증 에이전트에 대한 정보에 기초하여 생성한 제1회답 신호를 인증 에이전트로 전송하고(550), 인증 에이전트에서 모바일 단말에 대한 정보에 기초하여 생성한 제2회답 신호를 모바일 단말로 전송한다(560).

[0102] 또한, 인증서버에서 제2응답 신호를 이용하여 모바일 단말 및 인증 에이전트를 인증하고, 모바일 단말 및 인증 에이전트가 인증되면, 인증서버에서 모바일 단말의 키 값(KEY_M) 및 인증 에이전트의 키 값(KEY_AG)을 이용하여 각각의 시드값(SEED_M, SEED_AG)을 새로운 시드값(SEED_M', SEED_AG')으로 갱신할 수 있다.

[0103] 또한, 인증 에이전트에서 인증 에이전트의 키 값(KEY_AG)을 이용하여 암호화 데이터를 복호화한 복호화 데이터를 생성할 수 있다.

[0104] 본 발명의 일 양상은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현될 수 있다. 상기의 프로그램을 구현하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 디스크 등을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드로 저장되고 실행될 수 있다.

[0105] 이상의 설명은 본 발명의 일 실시예에 불과할 뿐, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명의 본질적 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현할 수 있을 것이다. 따라서, 본 발명의 범위는 전술한 실시예에 한정되지 않고 특허 청구범위에 기재된 내용과 동등한 범위 내에 있는 다양한 실시 형태가 포함되도록 해석되어야 할 것이다.

부호의 설명

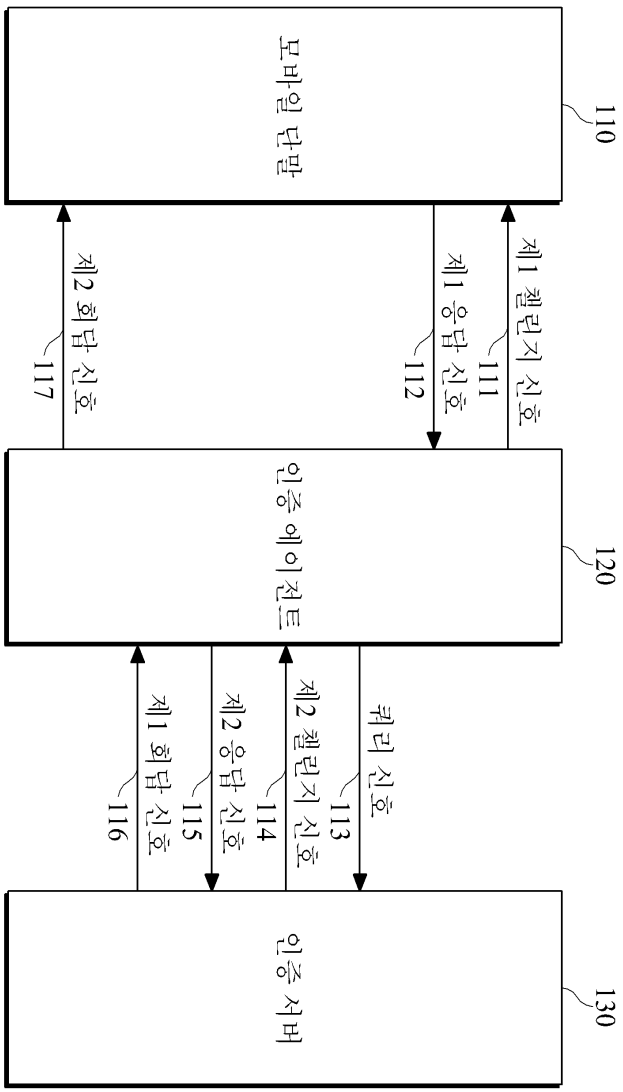
[0106] 110 모바일 단말

120 인증 에이전트

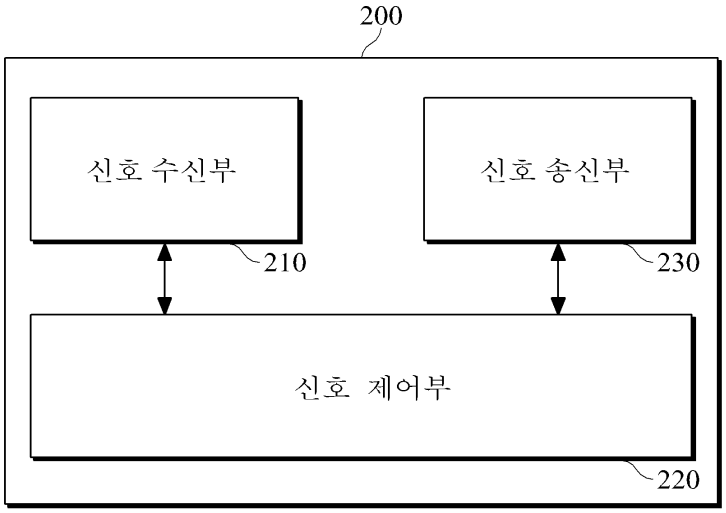
130 인증서버

도면

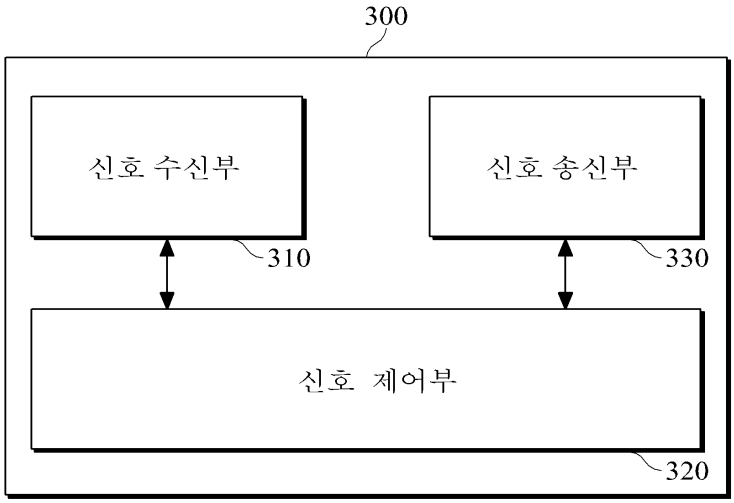
도면1


모바일 단말
110
제1 챌린지 신호
111
제1 응답 신호
112
제2 회답 신호
117
인증 에이전트
120
쿼리 신호
113
제2 챌린지 신호
114
제2 응답 신호
115
제1 회답 신호
116
인증 서버
130

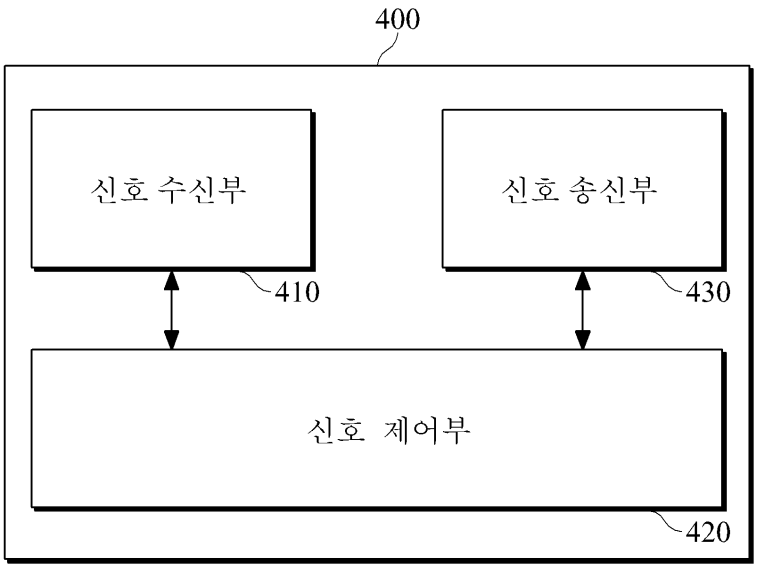
도면2


200
신호 수신부
신호 송신부
210
230
신호 제어부
220

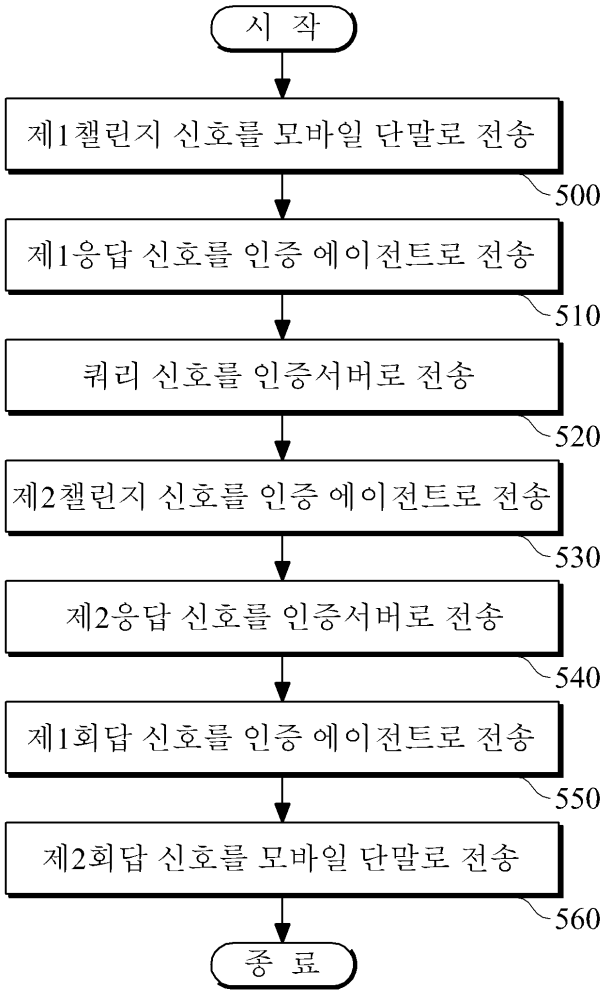
도면3


300
신호 수신부
신호 송신부
310
330
신호 제어부
320

도면4


400
신호 수신부
신호 송신부
410
430
신호 제어부
420

도면5


시 작
제1챌린지 신호를 모바일 단말로 전송
500
제1응답 신호를 인증 에이전트로 전송
510
쿼리 신호를 인증서버로 전송
520
제2챌린지 신호를 인증 에이전트로 전송
530
제2응답 신호를 인증서버로 전송
540
제1회답 신호를 인증 에이전트로 전송
550
제2회답 신호를 모바일 단말로 전송
560
종 료