(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0072711
(43) 공개일자 2021년06월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 9/0841 (2013.01)
(21) 출원번호 10-2020-0168143
(22) 출원일자 2020년12월04일
심사청구일자 없음
(30) 우선권주장
1020190162485 2019년12월09일 대한민국(KR)

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
김영갑
서울특별시 광진구 능동로 209, 대양AI센터 701호
아비짓 타카레
서울특별시 광진구 능동로 209, 대양AI센터 732호
이의종
서울특별시 광진구 능동로 209, 대양AI센터 732호
(74) 대리인
특허법인이상

전체 청구항 수 : 총 14 항

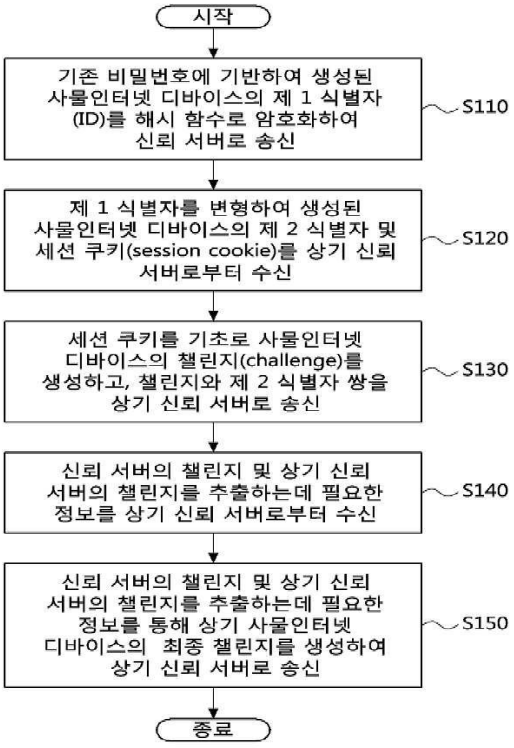
(54) 발명의 명칭 **사물인터넷 디바이스와 신뢰 서버 간 상호 인증 방법 및 장치**

(57) 요 약

본 발명은 상호 인증 방법을 개시한다. 예를 들어, 신뢰 서버(trusted server)와 연동하는 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법으로서, 기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하는 단계; 상기 제 1 식별자를 변형하여 생성된 사물인터넷 디

(뒷면에 계속)

대 표 도 - 도1



바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하는 단계; 상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하는 단계; 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하는 단계; 및 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하는 단계를 포함하는, 상호 인증 방법을 개시한다.

(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/3236 (2013.01)
H04L 2209/122 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711103210
과제번호	2019-0-00231
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발사업
연구과제명	공공 인프라 안전을 위한 인공지능 기반 영상보안 기술 및 시스템 개발
기 여 율	1/1
과제수행기관명	세종대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

신뢰 서버(trusted server)와 연동하는 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법으로서,

기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하는 단계;

상기 제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하는 단계;

상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하는 단계;

신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하는 단계; 및

상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하는 단계를 포함하는, 상호 인증 방법.

청구항 2

청구항 1에 있어서,

사물인터넷 디바이스에서 새로운 비밀번호를 선택하는 단계;

상기 새로운 비밀번호에 기반한 사물인터넷 디바이스의 제 3 식별자를 해시 함수로 암호화하는 단계;

세션키(session key)를 활용하여 상기 제 3 식별자를 상기 신뢰 서버로 송신하는 단계; 및

상기 제 3 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 4 식별자 및 세션 쿠키를 상기 신뢰 서버로부터 수신하는 단계를 더 포함하는, 상호 인증 방법.

청구항 3

청구항 1에 있어서,

상기 제 2 식별자 및 상기 세션 쿠키는,

상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성되는, 상호 인증 방법.

청구항 4

청구항 1에 있어서,

상기 사물인터넷 디바이스의 챌린지(challenge)는,

타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 1 챌린지, 및

상기 비밀값을 세션 쿠키에 은닉한 제 2 챌린지를 포함하는, 상호 인증 방법.

청구항 5

청구항 1에 있어서,

상기 사물인터넷 디바이스의 최종 챌린지는,

상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 상기 신뢰 서버의 챌린지를 검증하고,

상기 검증 후 세션키를 활용하여 생성되는, 상호 인증 방법.

청구항 6

사물인터넷 디바이스와 연동하는 신뢰 서버(trusted server)에 의해 수행되는 상호 인증 방법으로서,

기존 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 1 식별자(ID)를 사물인터넷 디바이스로부터 수신하는 단계;

상기 제 1 식별자를 변형하여 사물인터넷 디바이스의 제 2 식별자를 생성하고, 세션 쿠키(session cookie)를 생성하여 상기 사물인터넷 디바이스로 송신하는 단계;

상기 세션 쿠키를 기초로 생성된 사물인터넷 디바이스의 챌린지(challenge) 및 제 2 식별자 쌍을 상기 사물인터넷 디바이스로부터 수신하는 단계;

상기 사물인터넷 디바이스의 챌린지를 검증하고, 검증 결과에 따라 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 생성하는 단계;

상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 사물인터넷 디바이스로 송신하는 단계; 및

상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 생성된 상기 사물인터넷 디바이스의 최종 챌린지를 수신하는 단계를 포함하는, 상호 인증 방법.

청구항 7

청구항 6에 있어서,

새로운 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 3 식별자를 세션키(session key)를 활용하여 수신하는 단계; 및

상기 제 3 식별자를 변형하여 사물인터넷 디바이스의 제 4 식별자를 생성하고, 세션 쿠키를 생성하여 상기 사물인터넷 디바이스로 송신하는 단계를 더 포함하는, 상호 인증 방법.

청구항 8

청구항 6에 있어서,

상기 제 2 식별자 및 세션 쿠키(session cookie)는,

상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성되는, 상호 인증 방법.

청구항 9

청구항 6에 있어서,

상기 신뢰 서버의 챌린지는,

타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 3 챌린지, 및

상기 비밀값을 세션 쿠키에 은닉한 제 4 챌린지를 포함하는, 상호 인증 방법.

청구항 10

신뢰 서버(trusted server)와 연동하여 상호 인증을 수행하는 사물인터넷 디바이스로서,

프로세서; 및

상기 프로세서를 통해 실현되는 적어도 하나의 명령을 저장하는 메모리를 포함하고,

상기 적어도 하나의 명령은,

기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하도록 하는 명령;

상기 제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하도록 하는 명령;

상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하도록 하는 명령;

신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하도록 하는 명령; 및

상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하도록 하는 명령을 포함하는, 상호 인증 장치.

청구항 11

청구항 10에 있어서,

사물인터넷 디바이스에서 새로운 비밀번호를 선택하도록 하는 명령;

상기 새로운 비밀번호에 기반한 사물인터넷 디바이스의 제 3 식별자를 해시 함수로 암호화하도록 하는 명령;

세션키(session key)를 활용하여 상기 제 3 식별자를 상기 신뢰 서버로 송신하도록 하는 명령; 및

상기 제 3 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 4 식별자 및 세션 쿠키를 상기 신뢰 서버로부터 수신하도록 하는 명령을 더 포함하는, 상호 인증 장치.

청구항 12

청구항 10에 있어서,

상기 제 2 식별자 및 세션 쿠키는,

상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성되는, 상호 인증 장치.

청구항 13

청구항 10에 있어서,

상기 사물인터넷 디바이스의 챌린지(challenge)는,

타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 1 챌린지, 및

상기 비밀값을 세션 쿠키에 은닉한 제 2 챌린지를 포함하는, 상호 인증 장치.

청구항 14

청구항 10에 있어서,

상기 사물인터넷 디바이스의 최종 챌린지는,

상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 신뢰 서버의 챌린지를 검증하고,

상기 검증 후 세션키를 활용하여 생성되는, 사물인터넷 디바이스.

발명의 설명

기 술 분 야

[0001] 본 발명은 사물인터넷 디바이스와 신뢰 서버 간 상호 인증을 수행하는 방법 및 장치에 관한 것으로, 더욱 상세하게는 비밀번호에 기반하여 사물인터넷 디바이스와 신뢰 서버 간 상호 인증을 수행하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 사물인터넷(Internet of Things; IoT)은 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을

의미한다. 즉, 사물인터넷은 무선 통신을 통해 각종 사물을 연결하는 기술로서, 인터넷으로 연결된 디바이스들이 데이터를 주고받아 스스로 분석하고 학습한 정보를 사용자에게 제공하거나 사용자가 이를 원격 조정할 수 있다.

[0003] 다만, 사물인터넷 디바이스들이 서버와 데이터를 주고받을 때 보안이 문제될 수 있다. 따라서, 종래에는 사물인터넷 디바이스와 서버 간 인증 또는 인가 기술을 활용하여 보안 문제 해결을 시도하였으나, 보안을 위한 다양한 요소들이 고려하지 않는 문제점이 있다.

[0004] 또한, 기존 사물인터넷 디바이스와 서버 간 인증 또는 인가 기술의 경우 대규모 인증 또는 인가를 위해 수많은 계산 작업이 필요하고 컴퓨팅 능력이 필요하다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 사물인터넷을 위해 낮은 컴퓨팅 환경에서도 사물인터넷과 서버 간 인증 또는 인가가 가능한 방법을 제공하는 데 있다.

과제의 해결 수단

[0006] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 상호 인증 방법은 신뢰 서버(trusted server)와 연동하는 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법으로서, 기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하는 단계; 상기 제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하는 단계; 상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하는 단계; 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하는 단계; 및 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하는 단계를 포함할 수 있다.

[0007] 여기서, 본 발명의 일 실시예에 따른 상호 인증 방법은 사물인터넷 디바이스에서 새로운 비밀번호를 선택하는 단계; 상기 새로운 비밀번호에 기반한 사물인터넷 디바이스의 제 3 식별자를 해시 함수로 암호화하는 단계; 세션키(session key)를 활용하여 상기 제 3 식별자를 상기 신뢰 서버로 송신하는 단계; 및 상기 제 3 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 4 식별자 및 세션 쿠키를 상기 신뢰 서버로부터 수신하는 단계를 더 포함할 수 있다.

[0008] 한편, 상기 제 2 식별자 및 상기 세션 쿠키는, 상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성될 수 있다.

[0009] 또한, 상기 사물인터넷 디바이스의 챌린지(challenge)는, 타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 1 챌린지, 및 상기 비밀값을 세션 쿠키에 은닉한 제 2 챌린지를 포함할 수 있다.

[0010] 한편, 상기 사물인터넷 디바이스의 최종 챌린지는, 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 상기 신뢰 서버의 챌린지를 검증하고, 상기 검증 후 세션키를 활용하여 생성될 수 있다.

[0012] 상기와 같은 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 상호 인증 방법은, 사물인터넷 디바이스와 연동하는 신뢰 서버(trusted server)에 의해 수행되는 상호 인증 방법으로서, 기존 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 1 식별자(ID)를 사물인터넷 디바이스로부터 수신하는 단계; 상기 제 1 식별자를 변형하여 사물인터넷 디바이스의 제 2 식별자를 생성하고, 세션 쿠키(session cookie)를 생성하여 상기 사물인터넷 디바이스로 송신하는 단계; 상기 세션 쿠키를 기초로 생성된 사물인터넷 디바이스의 챌린지(challenge) 및 제 2 식별자 쌍을 상기 사물인터넷 디바이스로부터 수신하는 단계; 상기 사물인터넷 디바이스의 챌린지를 검증하고, 검증 결과에 따라 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 생성하는 단계; 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 사물인터넷 디바이스로 송신하는 단계; 및 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 생성된 상기 사물인터넷 디바이스의 최종 챌린지를 수신하는 단계를 포함할 수 있다.

[0013] 여기서, 본 발명의 다른 실시예에 따른 상호 인증 방법은, 새로운 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 3 식별자를 세션키(session key)를 활용하여 수신하는 단계; 및 상기 제 3 식별자를 변형하여 사물인터넷 디바이스의 제 4 식별자를 생성하고, 세션 쿠키를 생성하여 상기 사물인터넷 디바이스로 송신하는 단계를 더 포함할 수 있다.

[0014] 한편, 상기 제 2 식별자 및 세션 쿠키(session cookie)는, 상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성될 수 있다.

[0015] 또한, 상기 신뢰 서버의 챌린지는, 타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 3 챌린지, 및 상기 비밀값을 세션 쿠키에 은닉한 제 4 챌린지를 포함할 수 있다.

[0017] 상기와 같은 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따른 상호 인증 장치는, 신뢰 서버(trusted server)와 연동하여 상호 인증을 수행하는 사물인터넷 디바이스로서, 프로세서; 및 상기 프로세서를 통해 실현되는 적어도 하나의 명령을 저장하는 메모리를 포함하고, 상기 적어도 하나의 명령은, 기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하도록 하는 명령; 상기 제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하도록 하는 명령; 상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하도록 하는 명령; 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하도록 하는 명령; 및 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하도록 하는 명령을 포함할 수 있다.

[0018] 여기서, 적어도 하나의 명령은, 사물인터넷 디바이스에서 새로운 비밀번호를 선택하도록 하는 명령; 상기 새로운 비밀번호에 기반한 사물인터넷 디바이스의 제 3 식별자를 해시 함수로 암호화하도록 하는 명령; 세션키(session key)를 활용하여 상기 제 3 식별자를 상기 신뢰 서버로 송신하도록 하는 명령; 및 상기 제 3 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 4 식별자 및 세션 쿠키를 상기 신뢰 서버로부터 수신하도록 하는 명령을 더 포함할 수 있다.

[0019] 한편, 상기 제 2 식별자 및 세션 쿠키는, 상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성될 수 있다.

[0020] 또한, 상기 사물인터넷 디바이스의 챌린지(challenge)는, 타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 1 챌린지, 및 상기 비밀값을 세션 쿠키에 은닉한 제 2 챌린지를 포함할 수 있다.

[0021] 한편, 상기 사물인터넷 디바이스의 최종 챌린지는, 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 신뢰 서버의 챌린지를 검증하고, 상기 검증 후 세션키를 활용하여 생성될 수 있다.

발명의 효과

[0022] 본 발명의 일 실시예에 따르면 기존 인증, 인가 기술에 비해 컴퓨팅 비용(computation cost), 통신 비용(communication cost) 및 저장 비용(storage cost)를 감소시킬 수 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법의 동작 순서도이다.

도 2는 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법의 동작 순서도이다.

도 3은 사물인터넷 디바이스의 식별자를 신뢰 서버에 등록하는 방법을 설명하기 위한 도면이다.

도 4는 사물인터넷 디바이스와 신뢰 서버 간 상호 인증하는 방법을 설명하기 위한 도면이다.

도 5는 사물인터넷 디바이스의 새로운 식별자를 신뢰 서버에 등록하는 방법을 설명하기 위한 도면이다.

도 6은 본 발명의 또 다른 실시예에 따른 상호 인증 장치의 블록 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고

상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0025] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는"이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0026] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0027] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0028] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0030] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0031] 도 1은 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법의 동작 순서도이다.

[0032] 도 1을 참조하면, 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법은, 기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하는 단계(S110)를 포함할 수 있다.

[0033] 또한, 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법은 상기 제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하는 단계(S120)를 포함할 수 있다,

[0034] 여기서, 상기 제 2 식별자 및 상기 세션 쿠키는, 상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성될 수 있다.

[0035] 한편, 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법은 상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하는 단계(S130)를 포함할 수 있다.

[0036] 여기서, 상기 사물인터넷 디바이스의 챌린지(challenge)는, 타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 1 챌린지, 및 상기 비밀값을 세션 쿠키에 은닉한 제 2 챌린지를 포함할 수 있다.

[0037] 또한, 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법은, 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하는 단계(S140)를 포함할 수 있다.

[0038] 마지막으로, 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법은, 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하는 단계(S150)를 포함할 수 있다.

[0039] 여기서, 상기 사물인터넷 디바이스의 최종 챌린지는, 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 상기 신뢰 서버의 챌린지를 검증하고, 상기 검증 후 세션키를 활용하여 생성될 수 있다.

[0040] 또한, 본 발명의 일 실시예에 따른 사물인터넷 디바이스에 의해 수행되는 상호 인증 방법은 사물인터넷 디바이스에서 새로운 비밀번호를 선택하는 단계; 상기 새로운 비밀번호에 기반한 사물인터넷 디바이스의 제 3 식별자를 해시 함수로 암호화하는 단계; 세션키(session key)를 활용하여 상기 제 3 식별자를 상기 신뢰 서버로 송신하는 단계; 및 상기 제 3 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 4 식별자 및 세션 쿠키를 상기 신뢰 서버로부터 수신하는 단계를 더 포함할 수 있다.

[0042] 도 2는 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법의 동작 순서도이다.

[0043] 도 2를 참고하면, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은, 기존 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 1 식별자(ID)를 사물인터넷 디바이스로부터 수신하는 단계(S210)를 포함할 수 있다.

[0044] 또한, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은 상기 제 1 식별자를 변형하여 사물인터넷 디바이스의 제 2 식별자를 생성하고, 세션 쿠키(session cookie)를 생성하여 상기 사물인터넷 디바이스로 송신하는 단계(S220)를 포함할 수 있다.

[0045] 여기서, 상기 제 2 식별자 및 세션 쿠키(session cookie)는, 상기 제 1 식별자, 임의의 난수(random number) 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 생성될 수 있다.

[0046] 또한, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은 상기 세션 쿠키를 기초로 생성된 사물인터넷 디바이스의 챌린지(challenge) 및 제 2 식별자 쌍을 상기 사물인터넷 디바이스로부터 수신하는 단계(S230)를 포함할 수 있다.

[0047] 한편, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은 상기 사물인터넷 디바이스의 챌린지를 검증하고, 검증 결과에 따라 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 생성하는 단계(S240)를 포함할 수 있다.

[0048] 여기서, 상기 신뢰 서버의 챌린지는, 타원 곡선 암호 생성자 및 비밀값을 통해 생성된 제 3 챌린지, 및 상기 비밀값을 세션 쿠키에 은닉한 제 4 챌린지를 포함할 수 있다.

[0049] 또한, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 사물인터넷 디바이스로 송신하는 단계(S250)를 포함할 수 있다.

[0050] 또한, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 생성된 상기 사물인터넷 디바이스의 최종 챌린지를 수신하는 단계(S260)를 포함할 수 있다.

[0051] 또한, 본 발명의 다른 실시예에 따른 신뢰 서버에 의해 수행되는 상호 인증 방법은 새로운 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 3 식별자를 세션키(session key)를 활용하여 수신하는 단계; 및 상기 제 3 식별자를 변형하여 사물인터넷 디바이스의 제 4 식별자를 생성하고, 세션 쿠키를 생성하여 상기 사물인터넷 디바이스로 송신하는 단계를 더 포함할 수 있다.

[0053] 도 3은 사물인터넷 디바이스의 식별자를 신뢰 서버에 등록하는 방법을 설명하기 위한 도면이다.

[0054] 도 3에 사용된 문자의 의미는 다음과 같다.

[0055]

Notations	Description
Psw_i	Secret password of the embedded device
P_{ke}	Public key of the embedded device
P_{ks}	Public key of the server
I_i	Hashed embedded device ID
CID_i	Server-generated embedded device ID
CK	Session cookie
E_{ki}, D_{ki}	Communication encryption key / decryption key
$D=< x_1,.,x_n >$	Dictionary of ephemeral secretes
s	Server private key
H	Hash function
$X_i, Y_i, X_j, X_j, Y_j, C$	Challenges
x_{i1}, x_{j1}	Ephemeral secretes
E_t	Expiration time of the cookie
A, T	Equations
S_K	Session key

[0056] 도 3을 참조하면, 먼저, 사물인터넷 디바이스는 비밀번호(Psw_i)를 선택할 수 있다. 이어서, 사물인터넷 디바이스는 선택된 비밀번호를 토대로 사물인터넷 디바이스의 식별자(ID_i)를 해시 함수로 암호화할 수 있다. 이어서, 사물인터넷 디바이스는 암호화된 사물인터넷 디바이스의 식별자를 신뢰 서버로 송신할 수 있다(S110).

[0057] 한편, 신뢰 서버는 사물인터넷 디바이스의 식별자를 수신할 수 있다(S210). 또한, 신뢰 서버는 사물인터넷 디바이스의 식별자가 신뢰 서버에 저장되어있는지 확인할 수 있다. 이어서, 신뢰 서버는 사물인터넷 디바이스의 식별자가 신뢰 서버에 저장되어 있지 않은 경우, 임의의 난수(R)를 선택할 수 있다.

[0058] 또한, 신뢰 서버는 사물인터넷 디바이스의 식별자, 임의의 난수 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 사물인터넷 디바이스의 새로운 식별자(CID_i) 및 세션 쿠키(session cookie, CK)를 생성할 수 있다. 한편, 신뢰 서버는 사물인터넷 디바이스의 새로운 식별자 및 세션 쿠키를 생성하면서 사용한 매개 변수를 신뢰 서버에 저장할 수 있다. 또한, 신뢰 서버는 사물인터넷 디바이스의 새로운 식별자 및 세션 쿠키를 사물인터넷 디바이스로 송신할 수 있다(S220).

[0059] 한편, 사물인터넷 디바이스는 사물인터넷 디바이스의 새로운 식별자 및 세션 쿠키를 수신할 수 있다(S120).

[0061] 도 4는 사물인터넷 디바이스와 신뢰 서버 간 상호 인증하는 방법을 설명하기 위한 도면이다.

[0062] 도 4를 참고하면, 먼저, 사물인터넷 디바이스는 사전(dictionary)에서 임의의 비밀값(x_i)를 선택하여 챌린지(challenge)를 생성할 수 있다. 이 때, 챌린지는 타원 곡선 암호 생성자와 비밀값을 연산하여 획득한 목표(X_i) 및 비밀값을 세션 쿠키에 은닉한 목표(Y_i)를 포함할 수 있다. 비밀값을 세션 쿠키에 은닉할 때는 해시 함수를 활용할 수 있다. 이어서, 사물인터넷 디바이스는 사물인터넷 디바이스의 챌린지와 사물인터넷 디바이스의 새로운 식별자 쌍을 신뢰 서버로 송신할 수 있다(S130).

[0063] 한편, 신뢰 서버는 사물인터넷 디바이스의 챌린지와 사물인터넷 디바이스의 새로운 식별자 쌍을 수신할 수 있다(S230). 이어서, 신뢰 서버는 사물인터넷 디바이스의 챌린지를 검증할 수 있다. 예를 들어, 신뢰 서버는 사물인터넷 디바이스의 챌린지를 계산하여 은닉한 목표가 도출되는지 확인하여 사물인터넷 디바이스의 챌린지를 검증할 수 있다.

[0064] 이어서, 신뢰 서버는 사물인터넷 디바이스의 챌린지를 검증한 후, 사전에서 임의의 비밀값(x_j)를 선택하여 챌린지를 생성할 수 있다(S240). 이 때, 챌린지는 타원 곡선 암호 생성자와 비밀값을 연산하여 획득한 목표(X_j) 및 비밀값을 세션 쿠키에 은닉한 목표(Y_j)를 포함할 수 있다. 비밀값을 세션 쿠키에 은닉할 때는 해시 함수를 활용할 수 있다.

[0065] 한편, 신뢰 서버는 사물인터넷 디바이스의 챌린지를 계산하는데 사용된 수식(equation)을 신뢰 서버의 챌린지를 추출하는데 필요한 정보로서 포함시킬 수 있다. 따라서, 신뢰 서버는 신뢰 서버의 챌린지 및 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 사물인터넷 디바이스로 송신할 수 있다(S250).

[0066] 사물인터넷 디바이스는 신뢰 서버의 챌린지 및 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 수신할 수 있다(S140). 한편, 사물인터넷 디바이스는 신뢰 서버의 챌린지를 검증할 수 있다. 예를 들어, 사물인터넷 디바이스는 신뢰 서버의 챌린지를 계산하여 은닉한 목표가 도출되는지 확인하여 신뢰 서버의 챌린지를 검증할 수 있다.

[0067] 신뢰 서버의 챌린지를 검증한 후, 사물인터넷 디바이스는 사물인터넷 디바이스의 최종 챌린지를 생성할 수 있다. 이 때, 사물인터넷 디바이스는 세션키(S_k)를 활용하여 최종 챌린지를 생성할 수 있다. 이어서, 사물인터넷 디바이스는 사물인터넷 디바이스의 최종 챌린지를 신뢰 서버에 송신할 수 있고(S150), 신뢰 서버는 이를 수신할 수 있다(S260).

[0069] 도 5는 사물인터넷 디바이스의 새로운 식별자를 신뢰 서버에 등록하는 방법을 설명하기 위한 도면이다.

[0070] 도 5를 참고하면, 사물인터넷 디바이스는 새로운 비밀번호(Psw_i*)를 선택할 수 있다. 이어서, 사물인터넷 디바이스는 선택된 새로운 비밀번호를 토대로 사물인터넷 디바이스의 식별자(ID_i)를 해시 함수로 암호화할 수 있다. 이어서, 사물인터넷 디바이스는 암호화된 사물인터넷 디바이스의 식별자를 신뢰 서버로 송신하고, 신뢰 서버는 이를 수신할 수 있다.

[0071] 한편, 신뢰 서버는 사물인터넷 디바이스의 식별자, 임의의 난수 및 타원 곡선 암호(Elliptic Curve Cryptosystem; ECC) 생성자를 활용하여 사물인터넷 디바이스의 새로운 식별자(CID_i*) 및 세션 쿠키(session cookie, CK*)를 생성할 수 있다. 한편, 신뢰 서버는 사물인터넷 디바이스의 새로운 식별자 및 세션 쿠키를 생성하면서 사용한 매개 변수를 신뢰 서버에 저장할 수 있다. 또한, 신뢰 서버는 사물인터넷 디바이스의 새로운 식별자 및 세션 쿠키를 사물인터넷 디바이스로 송신할 수 있다.

[0073] 도 6은 본 발명의 또 다른 실시예에 따른 상호 인증 장치의 블록 구성도이다.

[0074] 도 6을 참조하면, 본 발명의 일 실시예에 따른 상호 인증 장치(100)는 프로세서(110) 및 프로세서를 통해 실행되는 적어도 하나의 명령 및 명령 수행의 결과를 저장하는 메모리(120) 및 네트워크와 연결되어 통신을 수행하는 송수신 장치(130)를 포함할 수 있다.

[0075] 상호 인증 장치(100)는 또한, 입력 인터페이스 장치(140), 출력 인터페이스 장치(150), 저장 장치(160) 등을 더 포함할 수 있다. 상호 인증 장치(100)에 포함된 각각의 구성 요소들은 버스(Bus)(170)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0076] 프로세서(110)는 메모리(120) 및 저장 장치(160) 중에서 적어도 하나에 저장된 프로그램 명령(program command)을 실행할 수 있다. 프로세서(110)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU), 또는 본 발명의 실시예에 따른 방법들이 수행되는 전용의 프로세서를 의미할 수 있다. 메모리(120) 및 저장 장치(160) 각각은 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(120)는 읽기 전용 메모리(read only memory, ROM) 및 랜덤 액세스 메모리(random access memory, RAM) 중에서 적어도 하나로 구성될 수 있다.

[0077] 저장 장치(160)는 기존 비밀번호에 기반하여 암호화된 사물인터넷 디바이스의 암호화된 식별자, 새로운 비밀번호에 기반하여 암호화된 사물인터넷 디바이스의 암호화된 식별자, 사물인터넷 디바이스의 챌린지, 사물인터넷 디바이스의 최종 챌린지, 신뢰 서버에서 생성한 사물인터넷 디바이스의 새로운 식별자, 신뢰 서버의 챌린지, 신뢰 서버의 챌린지를 추출하는데 필요한 정보 및 신뢰 서버에서 생성한 세션 쿠키를 저장할 수 있다.

[0078] 여기서, 적어도 하나의 명령은, 기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자(ID)를 해시 함수로 암호화하여 신뢰 서버로 송신하도록 하는 명령; 상기 제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신하도록 하는 명령; 상기 세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신하도록 하는 명령; 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신하도록 하는 명령; 및 상기 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신하도록 하는 명령을 포함할 수 있다.

[0079] 또한, 적어도 하나의 명령은, 사물인터넷 디바이스에서 새로운 비밀번호를 선택하도록 하는 명령; 상기 새로운 비밀번호에 기반한 사물인터넷 디바이스의 제 3 식별자를 해시 함수로 암호화하도록 하는 명령; 세션키(session key)를 활용하여 상기 제 3 식별자를 상기 신뢰 서버로 송신하도록 하는 명령; 및 상기 제 3 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 4 식별자 및 세션 쿠키를 상기 신뢰 서버로부터 수신하도록 하는 명령을 더 포함할 수 있다.

[0081] 본 발명의 실시예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 정보가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0082] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

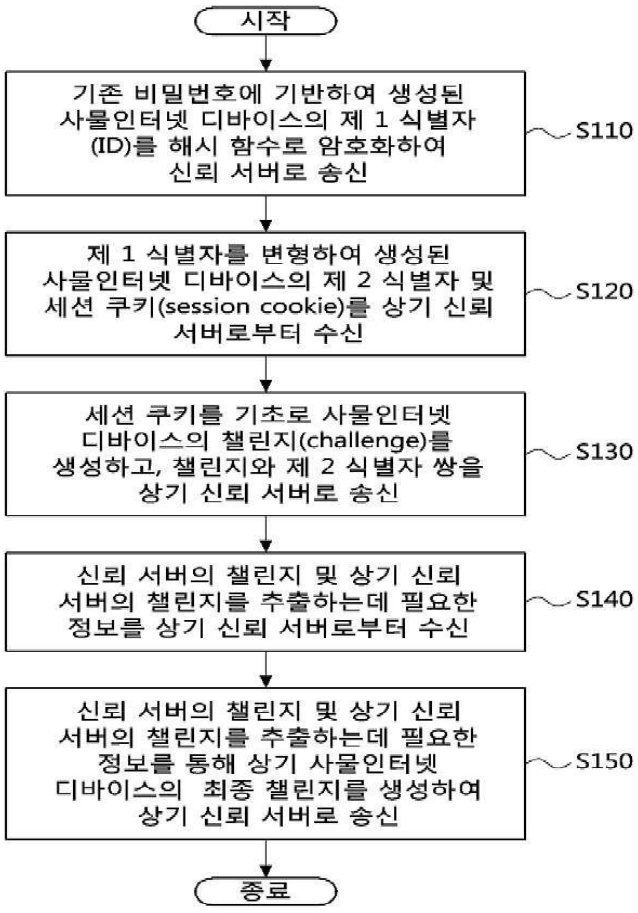
[0083] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0084] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그래머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

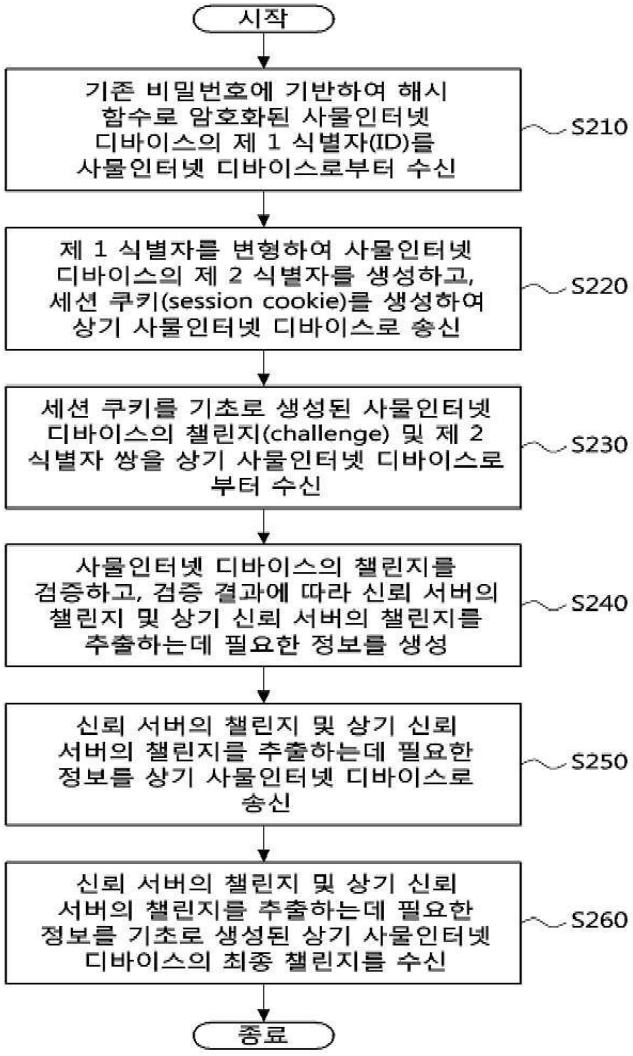
[0085] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

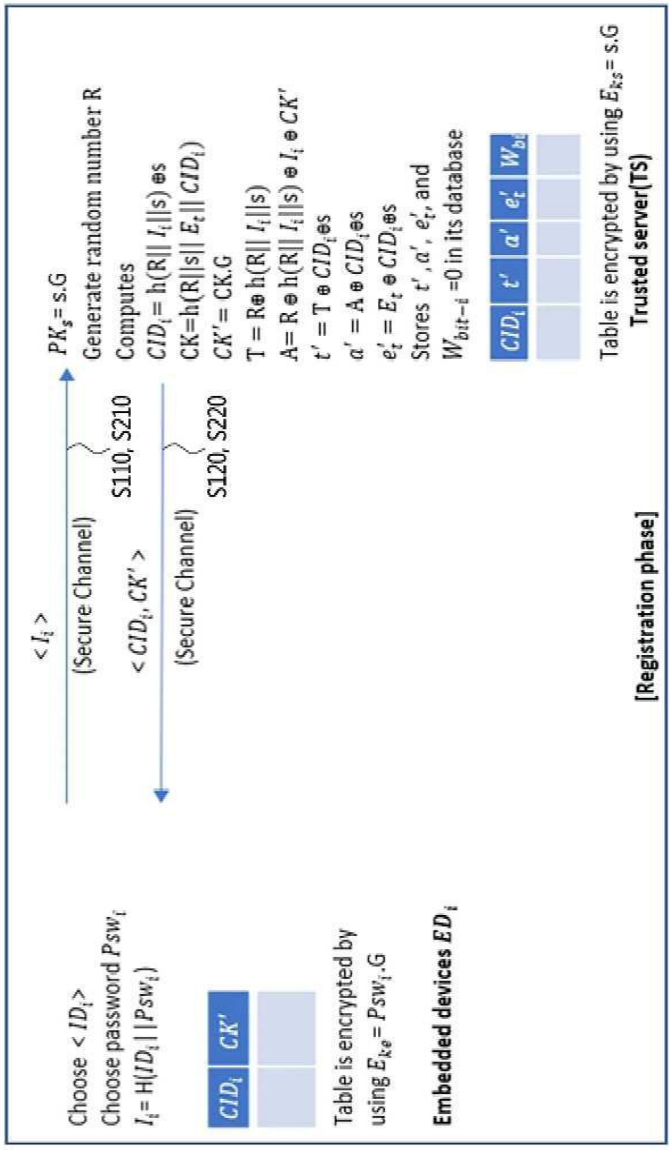
도면1


시작
기존 비밀번호에 기반하여 생성된 사물인터넷 디바이스의 제 1 식별자 (ID)를 해시 함수로 암호화하여 신뢰 서버로 송신
S110
제 1 식별자를 변형하여 생성된 사물인터넷 디바이스의 제 2 식별자 및 세션 쿠키(session cookie)를 상기 신뢰 서버로부터 수신
S120
세션 쿠키를 기초로 사물인터넷 디바이스의 챌린지(challenge)를 생성하고, 챌린지와 제 2 식별자 쌍을 상기 신뢰 서버로 송신
S130
신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 신뢰 서버로부터 수신
S140
신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 통해 상기 사물인터넷 디바이스의 최종 챌린지를 생성하여 상기 신뢰 서버로 송신
S150
종료

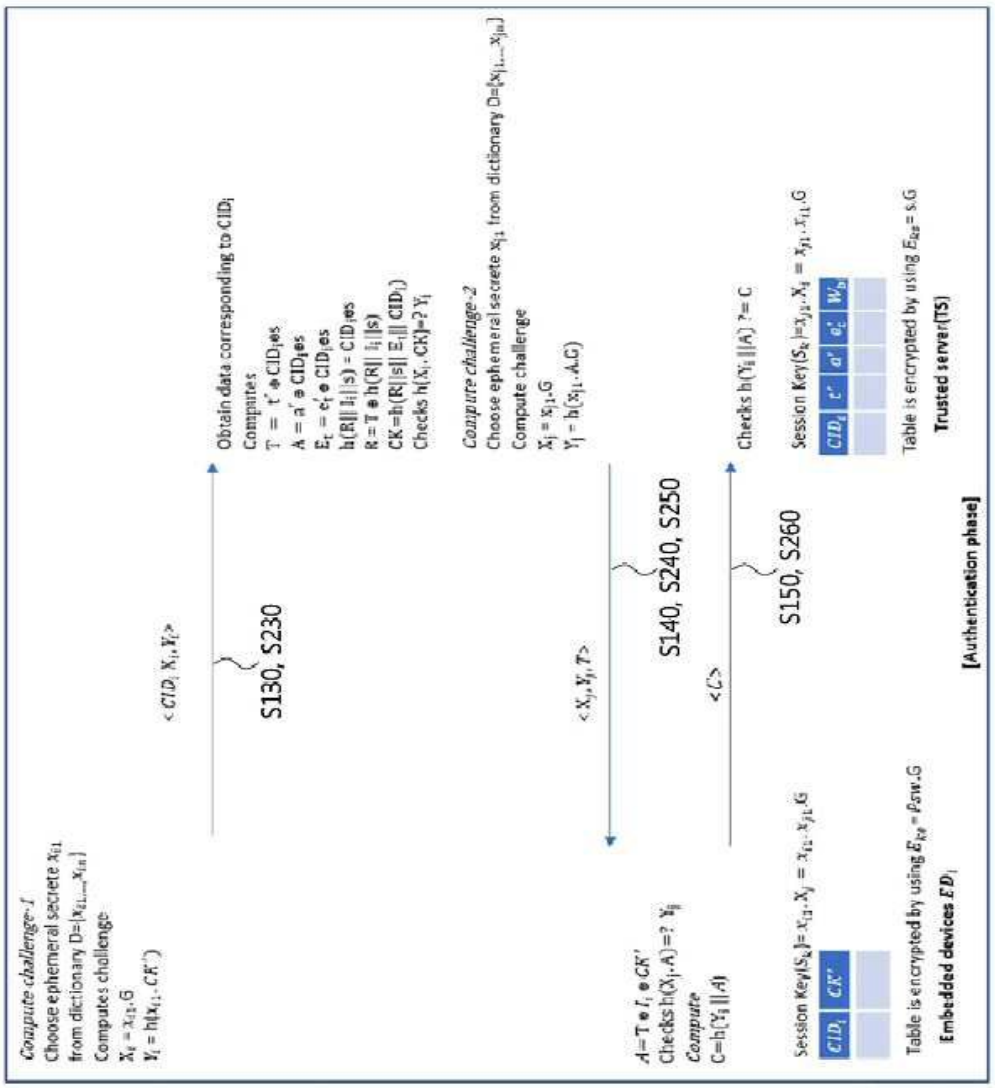
도면2


시작
기존 비밀번호에 기반하여 해시 함수로 암호화된 사물인터넷 디바이스의 제 1 식별자(ID)를 사물인터넷 디바이스로부터 수신
S210
제 1 식별자를 변형하여 사물인터넷 디바이스의 제 2 식별자를 생성하고, 세션 쿠키(session cookie)를 생성하여 상기 사물인터넷 디바이스로 송신
S220
세션 쿠키를 기초로 생성된 사물인터넷 디바이스의 챌린지(challenge) 및 제 2 식별자 쌍을 상기 사물인터넷 디바이스로부터 수신
S230
사물인터넷 디바이스의 챌린지를 검증하고, 검증 결과에 따라 신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 생성
S240
신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 상기 사물인터넷 디바이스로 송신
S250
신뢰 서버의 챌린지 및 상기 신뢰 서버의 챌린지를 추출하는데 필요한 정보를 기초로 생성된 상기 사물인터넷 디바이스의 최종 챌린지를 수신
S260
종료

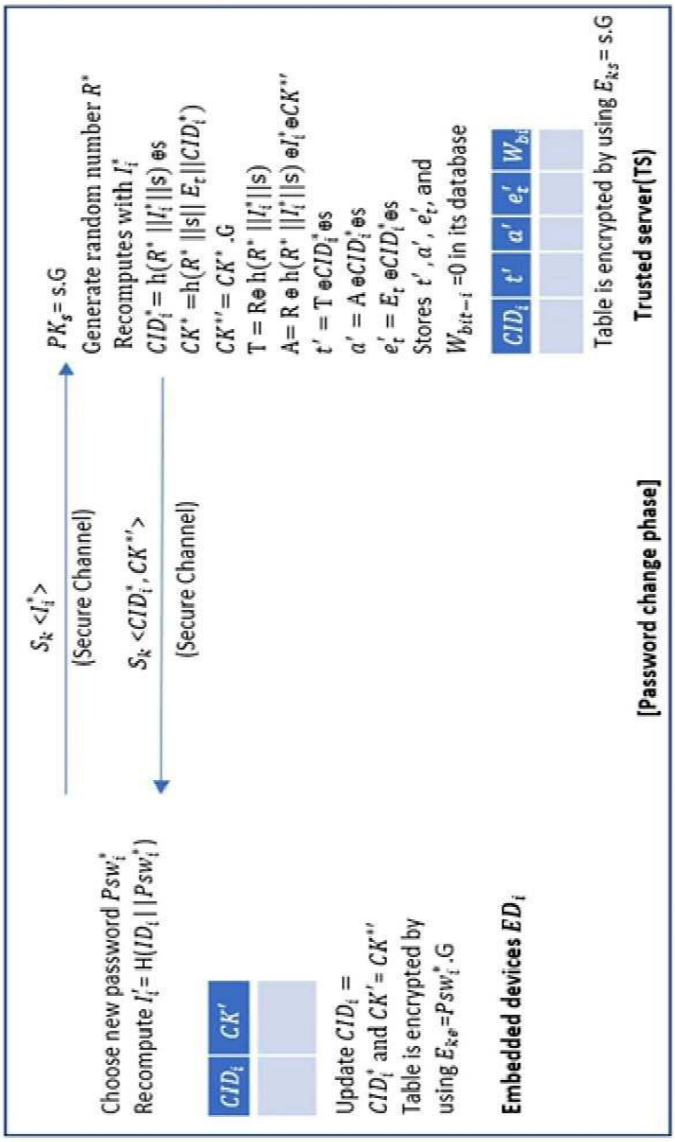
도면3


Choose < ID_i >
Choose password Psw_i
$I_i = H(ID_i || Psw_i)$
CID_i | CK'
Table is encrypted by using $E_{ke} = Psw_i.G$
Embedded devices ED_i
< I_i >
(Secure Channel)
S110, S210
< CID_i, CK' >
(Secure Channel)
S120, S220
$PK_s = s.G$
Generate random number R
Computes
$CID_i = h(R||I_i||s) \oplus s$
$CK = h(R||s||E_t||CID_i)$
$CK' = CK.G$
$T = R \oplus h(R||I_i||s)$
$A = R \oplus h(R||I_i||s) \oplus I_i \oplus CK'$
$t' = T \oplus CID_i \oplus s$
$a' = A \oplus CID_i \oplus s$
$e'_t = E_t \oplus CID_i \oplus s$
Stores t', a', e'_t, and
$W_{bit-i} = 0$ in its database
CID_i | t' | a' | e'_t | W_{bit}
Table is encrypted by using $E_{ks} = s.G$
Trusted server(TS)
[Registration phase]

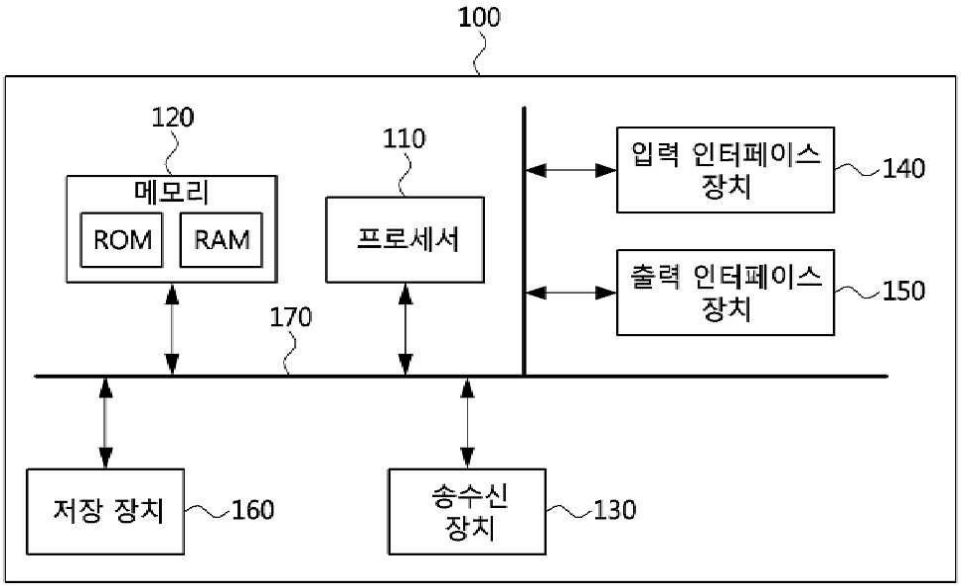
도면4


Computes challenge-1
Choose ephemeral secrete x_{i1}
from dictionary D={x_{i1},...,x_{in}}
Computes challenge
$X_i = x_{i1}.G$
$Y_i = h(x_{i1}.CK')$
<CID_i, X_i, Y_i>
S130, S230
Obtain data corresponding to CID_i
Computes
$T = t' \oplus CID_i$es
$A = a' \oplus CID_i$es
$E_t = e'_t \oplus CID_i$es
$h(R||I_i||s) = CID_i$es
$R = T \oplus h(R||I_i||s)$
$CK = h(R||s||E_t||CID_i)$
Checks $h(X_i.CK) = ?Y_i$
Computes challenge-2
Choose ephemeral secrete x_{ij} from dictionary D={x_{i1},...,x_{in}}
Compute challenge
$X_j = x_{ij}.G$
$Y_j = h(x_{ij}.A.G)$
<X_j, Y_j, T>
S140, S240, S250
$A = T \oplus I_i \oplus CK'$
Checks $h(X_j.A) = ?Y_j$
Computes
$C = h(Y_j||A)$
<C>
S150, S260
Checks $h(Y_j||A) ?= C$
Session $Key(S_k) = x_{ij}.X_j = x_{ij}.x_{ij}.G$
CID_i | CK'
Session $Key(S_k) = x_{ij}.X_j = x_{ij}.x_{ij}.G$
CID_i | t' | a' | e'_t | W_0
Table is encrypted by using $E_{Kp} = Psw.G$
Embedded devices ED_i
Table is encrypted by using $E_{Ks} = s.G$
Trusted server(TS)
[Authentication phase]

도면5


S_k <I_i^*>
(Secure Channel)
$PK_s = s.G$
Generate random number R^*
Recomputes with I_i^*
$CID_i^* = h(R^* || I_i^* || s) \oplus s$
$CK^* = h(R^* || s || E_t || CID_i^*)$
$CK''_i = CK^* . G$
$T = R \oplus h(R^* || I_i^* || s)$
$A = R \oplus h(R^* || I_i^* || s) \oplus I_i^* \oplus CK''$
$t' = T \oplus CID_i^* \oplus s$
$a' = A \oplus CID_i^* \oplus s$
$e_t' = E_t \oplus CID_i^* \oplus s$
Stores t', a', e_t', and
W_{bit-i} =0 in its database
S_k <CID_i^*, CK''>
(Secure Channel)
Choose new password Psw_i^*
Recompute $I_i' = H(ID_i || Psw_i^*)$
CID_i CK'
Update CID_i =
CID_i^* and $CK' = CK''$
Table is encrypted by
using $E_{k_e} = Psw_i^* . G$
Embedded devices ED_i
[Password change phase]
Table is encrypted by using $E_{k_s} = s.G$
Trusted server(TS)
CID_i t' a' e_t' W_{bit}

도면6


100
120
메모리
ROM
RAM
110
프로세서
입력 인터페이스 장치
140
출력 인터페이스 장치
150
170
저장 장치
160
송수신 장치
130