(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0093941
(43) 공개일자 2022년07월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *A61B 5/053* (2021.01)
G16Y 40/50 (2020.01) *H04L 65/40* (2022.01)
H04L 9/06 (2006.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
A61B 5/053 (2013.01)
(21) 출원번호 10-2020-0185129
(22) 출원일자 2020년12월28일
심사청구일자 2020년12월28일

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
송재승
서울특별시 강서구 강서로 348, 110동 902호
(74) 대리인
특허법인이상

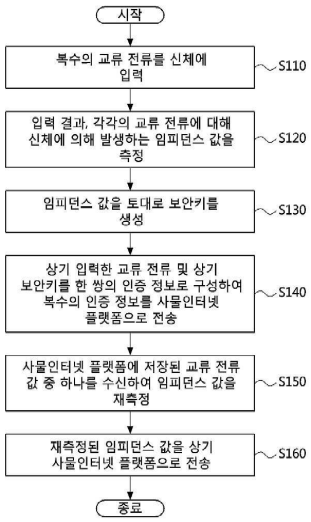
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **사물인터넷 기기 인증 방법 및 장치**

(57) 요 약

본 발명은 사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치를 통해 사물인터넷 기기를 인증하는 방법으로서, 복수의 교류 전류를 신체에 입력하는 단계; 상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하는 단계; 상기 임피던스 값을 토대로 보안키를 생성하는 단계; 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계; 상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하는 단계; 및 상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하는 단계를 포함하는, 사물인터넷 기기 인증 방법을 개시한다.

대 표 도 - 도1



(52) CPC특허분류
G16Y 40/50 (2020.01)
H04L 63/0861 (2013.01)
H04L 67/12 (2022.05)
H04L 9/0643 (2013.01)
H04L 9/083 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711102862
과제번호 2019-0-00426-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보보호핵심원천기술개발(R&D)
연구과제명 IoT 기반 이식-침습형 고위험 의료장치를 위한 능동형 킬 스위치 및 바이오 마커 활용 방어 시스템 개발
기 여 율 1/1
과제수행기관명 국민대학교산학협력단
연구기간 2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치를 통해 사물인터넷 기기를 인증하는 방법으로서,

복수의 교류 전류를 신체에 입력하는 단계;

상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하는 단계;

상기 임피던스 값을 토대로 보안키를 생성하는 단계;

상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계;

상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하는 단계; 및

상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하는 단계를 포함하는, 사물인터넷 기기 인증 방법.

청구항 2

청구항 1에 있어서,

상기 교류 전류는,

교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정된, 사물인터넷 기기 인증 방법.

청구항 3

청구항 1에 있어서,

상기 임피던스 값을 토대로 보안키를 생성하는 단계는,

해시 함수에 기반하여 상기 임피던스 값을 토대로 보안키를 생성하는 단계를 포함하는, 사물인터넷 기기 인증 방법.

청구항 4

청구항 1에 있어서,

상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하는 단계를 더 포함하는, 사물인터넷 기기 인증 방법.

청구항 5

청구항 1에 있어서,

상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계는,

상기 인증 정보를 미리 설정된 주기에 따라 최신화하여 사물인터넷 플랫폼으로 전송하는 단계를 포함하는, 사물인터넷 기기 인증 방법.

청구항 6

사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치로서,

프로세서; 및

상기 프로세서를 통해 실현되는 적어도 하나의 명령을 저장하는 메모리를 포함하고,

상기 적어도 하나의 명령은,

복수의 교류 전류를 신체에 입력하도록 하는 명령;

상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하도록 하는 명령;

상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령;

상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하도록 하는 명령;

상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하도록 하는 명령; 및

상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하도록 하는 명령을 포함하는, 사물인터넷 기기 인증 장치.

청구항 7

청구항 6에 있어서,

상기 교류 전류는,

교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정된, 사물인터넷 기기 인증 장치.

청구항 8

청구항 6에 있어서,

상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령은,

해시 함수에 기반하여 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령을 포함하는, 사물인터넷 기기 인증 장치.

청구항 9

청구항 6에 있어서,

상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하도록 하는 명령을 더 포함하는, 사물인터넷 기기 인증 장치.

청구항 10

청구항 6에 있어서,

상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하도록 하는 명령은,

상기 인증 정보를 미리 설정된 주기에 따라 최신화하여 사물인터넷 플랫폼으로 전송하도록 하는 명령을 포함하는, 사물인터넷 기기 인증 장치.

청구항 11

사물인터넷 기기 인증 장치와 연동하는 사물인터넷 플랫폼을 통해 사물인터넷 기기를 인증하는 방법으로서,

교류 전류 및 보안키를 한 쌍으로 하는 인증 정보 복수개를 사물인터넷 기기 인증 장치로부터 수신하여 등록하는 단계;

저장된 교류 전류 값 중 하나를 사물인터넷 기기 인증 장치로 송신하는 단계;

상기 저장된 교류 전류 값을 토대로 재측정된 임피던스 값을 상기 사물인터넷 기기 인증 장치로부터 수신하는 단계; 및

상기 재측정된 임피던스 값에 기반하여 인증을 수행하는 단계를 포함하는, 사물인터넷 기기 인증 방법.

청구항 12

청구항 11에 있어서,

상기 교류 전류는,

교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정된, 사물인터넷 기기 인증 방법.

청구항 13

청구항 11에 있어서,

상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하는 단계를 더 포함하는, 사물인터넷 기기 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 사물인터넷 기기를 인증하는 방법 및 장치에 관한 것으로, 더욱 상세하게는 사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치를 통해 사물인터넷 기기를 인증하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 사물인터넷 기기들은 다양한 물리적인 능력을 가지고 있다. 예를 들어, 일부 사물인터넷 기기들은 충분한 계산 능력(computing power) 및 메모리를 가지고 있고, 일부 사물인터넷 기기들은 메모리 등에 상당한 제약을 가지고 있다.

[0003] 물리적인 제약이 있는 사물인터넷 기기의 경우 인증을 위한 보안키를 저장하거나, 보안키를 생성해내기 위한 알고리즘 등을 저장하는 것에도 제약을 받는다. 따라서, 반도체 분야에서는 기계가 가지는 전기적 특성을 활용하여 해당 기계만이 가질 수 있는 유일한 키를 생성해낼 수 있는 연구가 진행되고 있다.

[0004] 물리적인 제약이 있는 사물인터넷 기기의 예는 몸에 임플란트(implant)하는 웨어러블 센서 등이 메모리의 제약을 가지고 있다. 따라서, 웨어러블 센서 등의 메모리 제약을 극복하여 보안키를 저장하고, 보안키를 생성하는 방법이 필요하다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 사람마다 특징적으로 가지고 있는 생체 임피던스 신호를 활용하여 보안키를 생성하는 방법을 제공하는 데 있다.

[0006] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 사물인터넷 플랫폼을 통해 사물인터넷 기기의 인증을 지원하는 방법을 제공하는 데 있다.

과제의 해결 수단

[0007] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 사물인터넷 기기 인증 방법은, 사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치를 통해 사물인터넷 기기를 인증하는 방법으로서, 복수의 교류 전류를 신체에 입력하는 단계; 상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하는 단계; 상기 임피던스 값을 토대로 보안키를 생성하는 단계; 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계; 상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하는 단계; 및 상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하는 단계를 포함할 수 있다.

[0008] 여기서, 상기 교류 전류는, 교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정될 수 있다.

[0009] 또한, 상기 임피던스 값을 토대로 보안키를 생성하는 단계는, 해시 함수에 기반하여 상기 임피던스 값을 토대로 보안키를 생성하는 단계를 포함할 수 있다.

[0010] 한편, 사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치를 통해 사물인터넷 기기 인증 방법은 상기 사

물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하는 단계를 더 포함할 수 있다.

[0011] 또한, 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계는, 상기 인증 정보를 미리 설정된 주기에 따라 최신화하여 사물인터넷 플랫폼으로 전송하는 단계를 포함할 수 있다.

[0013] 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 실시예에 따른 사물인터넷 기기 인증 장치는, 사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치로서, 프로세서; 및 상기 프로세서를 통해 실현되는 적어도 하나의 명령을 저장하는 메모리를 포함하고, 상기 적어도 하나의 명령은, 복수의 교류 전류를 신체에 입력하도록 하는 명령; 상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하도록 하는 명령; 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령; 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하도록 하는 명령; 상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하도록 하는 명령; 및 상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하도록 하는 명령을 포함할 수 있다.

[0014] 여기서, 상기 교류 전류는, 교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정될 수 있다.

[0015] 또한, 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령은, 해시 함수에 기반하여 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령을 포함할 수 있다.

[0016] 한편, 상기 적어도 하나의 명령은, 상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하도록 하는 명령을 더 포함할 수 있다.

[0017] 또한, 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하도록 하는 명령은, 상기 인증 정보를 미리 설정된 주기에 따라 최신화하여 사물인터넷 플랫폼으로 전송하도록 하는 명령을 포함할 수 있다.

[0019] 상기와 같은 문제점을 해결하기 위한 본 발명의 또 다른 실시예에 따른 사물인터넷 기기 인증 방법은, 사물인터넷 기기 인증 장치와 연동하는 사물인터넷 플랫폼을 통해 사물인터넷 기기를 인증하는 방법으로서, 교류 전류 및 보안키를 한 쌍으로 하는 인증 정보 복수개를 사물인터넷 기기 인증 장치로부터 수신하여 등록하는 단계; 저장된 교류 전류 값 중 하나를 사물인터넷 기기 인증 장치로 송신하는 단계; 상기 저장된 교류 전류 값을 토대로 재측정된 임피던스 값을 상기 사물인터넷 기기 인증 장치로부터 수신하는 단계; 및 상기 재측정된 임피던스 값에 기반하여 인증을 수행하는 단계를 포함할 수 있다.

[0020] 여기서, 상기 교류 전류는, 교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정될 수 있다.

[0021] 또한, 사물인터넷 기기 인증 장치와 연동하는 사물인터넷 플랫폼을 통해 사물인터넷 기기를 인증하는 방법은 상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하는 단계를 더 포함할 수 있다.

발명의 효과

[0022] 본 발명의 일 실시예에 따르면 생체 신호에 기반하여 보안키를 생성할 수 있다.

[0023] 본 발명의 다른 실시예에 따르면 사물인터넷 플랫폼을 활용하여 보안키를 관리할 수 있다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 일 실시예에 따른 사물인터넷 기기 장치를 통한 사물인터넷 기기 인증 방법의 동작 순서도이다.

도 2는 본 발명의 일 실시예에 따른 사물인터넷 플랫폼을 통한 사물인터넷 기기 인증 방법의 동작 순서도이다.

도 3은 본 발명의 사물인터넷 기기 인증 방법의 예시도이다.

도 4는 보안키를 생성하는 방법을 설명하기 위한 도면이다.

도 5는 사물인터넷 플랫폼을 설명하기 위한 도면이다.

도 6은 사물인터넷 플랫폼과 연동하는 엔티티를 설명하기 위한 제 1 예시도이다.

도 7은 사물인터넷 플랫폼과 연동하는 엔티티를 설명하기 위한 제 2 예시도이다.

도 8은 본 발명의 다른 실시예에 따른 사물인터넷 기기 인증 장치의 블록 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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.

[0031] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0032] 도 1은 본 발명의 일 실시예에 따른 사물인터넷 기기 장치를 통한 사물인터넷 기기 인증 방법의 동작 순서도이다.

[0033] 도 1을 참고하면, 본 발명의 일 실시예에 따른 사물인터넷 기기 장치를 통한 사물인터넷 기기 인증 방법은, 사물인터넷 플랫폼과 연동하는 사물인터넷 기기 인증 장치를 통해 사물인터넷 기기를 인증하는 방법으로서, 복수의 교류 전류를 신체에 입력하는 단계(S110)를 포함할 수 있다.

[0034] 여기서, 상기 교류 전류는, 교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정될 수 있다.

[0035] 또한, 본 발명은 상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하는 단계; 상기 임피던스 값을 토대로 보안키를 생성하는 단계(S120)를 포함할 수 있다.

[0036] 여기서, 상기 임피던스 값을 토대로 보안키를 생성하는 단계는, 해시 함수에 기반하여 상기 임피던스 값을 토대로 보안키를 생성하는 단계를 포함할 수 있다.

[0037] 한편, 본 발명은 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계(S130)를 포함할 수 있다.

[0038] 여기서, 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하는 단계는, 상기 인증 정보를 미리 설정된 주기에 따라 최신화하여 사물인터넷 플랫폼으로

전송하는 단계를 포함할 수 있다.

[0039] 또한, 본 발명은 상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하는 단계(S140)를 포함할 수 있다.

[0040] 한편, 본 발명은 상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하는 단계(S150)를 포함할 수 있다.

[0041] 또한, 본 발명은 상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하는 단계를 더 포함할 수 있다.

[0043] 도 2는 본 발명의 일 실시예에 따른 사물인터넷 플랫폼을 통한 사물인터넷 기기 인증 방법의 동작 순서도이다.

[0044] 도 2를 참고하면, 본 발명의 일 실시예에 따른 사물인터넷 플랫폼을 통한 사물인터넷 기기 인증 방법은, 사물인터넷 기기 인증 장치와 연동하는 사물인터넷 플랫폼을 통해 사물인터넷 기기를 인증하는 방법으로서, 교류 전류 및 보안키를 한 쌍으로 하는 인증 정보 복수개를 사물인터넷 기기 인증 장치로부터 수신하여 등록하는 단계(S210)를 포함할 수 있다.

[0045] 여기서, 상기 교류 전류는, 교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정될 수 있다.

[0046] 또한, 본 발명은 저장된 교류 전류 값 중 하나를 사물인터넷 기기 인증 장치로 송신하는 단계(S220)를 포함할 수 있다.

[0047] 한편, 본 발명은 상기 저장된 교류 전류 값을 토대로 재측정된 임피던스 값을 상기 사물인터넷 기기 인증 장치로부터 수신하는 단계(S230)를 포함할 수 있다.

[0048] 한편, 본 발명은 상기 재측정된 임피던스 값에 기반하여 인증을 수행하는 단계(S240)를 포함할 수 있다.

[0049] 또한, 본 발명은 상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하는 단계를 더 포함할 수 있다.

[0051] 도 3은 본 발명의 사물인터넷 기기 인증 방법의 예시도이다.

[0052] 도 3을 참고하면, 어플리케이션 엔티티(Application Entity; AE)는 사물인터넷 기기 인증 장치를 의미할 수 있고, 공통 서비스 엔티티(Commom Service Entity; CSE)는 사물인터넷 플랫폼과 연동하는 엔티티를 의미할 수 있고, 제 3 서버는 사물인터넷 플랫폼과 연동하는 외부 서버를 의미할 수 있다.

[0053] 먼저, 어플리케이션 엔티티는 생체 신호(bio seed) 및 임피던스 값(또는 보안키)를 한 쌍으로 구성하여 인증 정보를 복수개 생성할 수 있다(S130). 이어서, 어플리케이션 엔티티는 공통 서비스 엔티티에 생성된 복수개의 인증 정보를 송신하여 어플리케이션 엔티티의 등록을 요청할 수 있다(S140).

[0054] 한편, 공통 서비스 엔티티는 인증 정보를 수신하여 저장할 수 있다(S210). 이 때, 공통 서비스 엔티티와 연동하는 제 3 서버가 있는 경우 제 3 서버에 상기 인증 정보를 송신할 수 있다.

[0055] 이어서, 공통 서비스 엔티티는 인증 정보의 신뢰성을 확인하기 위해 어플리케이션 엔티티에 저장된 생체 신호 중 하나를 송신할 수 있다(S220). 이 때, 어플리케이션 엔티티는 공통 서비스 엔티티로부터 주어진 생체 신호를 활용하여 임피던스 값(또는 보안키)를 생성할 수 있다(S150). 이어서, 어플리케이션 엔티티는 주어진 생체 신호를 활용하여 생성한 임피던스 값(또는 보안키)를 공통 서비스 엔티티에 송신하고(S160), 공통 서비스 엔티티는 이를 수신할 수 있다(S230).

[0056] 마지막으로, 공통 서비스 엔티티는 어플리케이션 엔티티로부터 수신한 임피던스 값(또는 보안키)와 인증 정보를 비교하여 어플리케이션 엔티티에 대한 인증을 수행할 수 있다(S240).

[0058] 도 4는 보안키를 생성하는 방법을 설명하기 위한 도면이다.

[0059] 도 4를 참고하면, 본 발명에 따라 보안키를 생성하는 방법을 알 수 있다. 예를 들어, 본 발명의 사물인터넷 기기 인증 장치에서 복수의 교류 전류를 신체에 입력하고, 입력 결과에 따라 발생하는 임피던스 값을 측정하여 보

안키를 생성할 수 있다. 구체적으로는, 해시 함수에 기반하여 측정된 임피던스 값을 보안키로 생성할 수 있다. 다만, 임피던스 값을 보안키로 생성할 때 암호화하는 방법은 해시함수에 한정되지 않는다.

[0060] 또한, 사물인터넷 기기 인증 장치는 신체에 입력하는 교류 전류의 크기, 시간 등을 다르게 하여, 다르게 측정되는 임피던스 값을 저장하여 교류 전류 및 보안키를 한 쌍의 인증 정보로 구성할 수 있다.

[0062] 도 5는 사물인터넷 플랫폼을 설명하기 위한 도면이다.

[0063] 도 5를 참고하면, 사물인터넷 플랫폼에 바이오 생체 신호 기반 사물인터넷 기기 인증 방법을 추가하기 위한 정보를 알 수 있다. 예를 들어, 국제 표준에 기반한 사물인터넷 플랫폼인 oneM2M에 바이오 인증을 위한 추가 자원(resource) 및 속성(attributes)에 대한 정보를 알 수 있다.

[0064] 여기서, 'bioKeyPair' 속성 정보는 입력 신호 및 인증키로 구성된 한 쌍의 인증 정보를 포함할 수 있고, 'thirdPartyAuthServer'속성 정보는 사물인터넷 플랫폼과 연동하는 제 3 서버의 주소를 포함할 수 있고, 'keyIdentifier'속성 정보는 제 3 서버에 입력 신호 및 인증키로 구성된 인증 정보가 저장된 경우 상기 제 3 서버에 저장된 인증 정보를 식별하기 위한 식별자(identifier)를 포함할 수 있고, 'bioKeyIncation' 속성 정보는 사물인터넷 기기가 인증을 수행하기 위해 바이오 신호를 사용한다는 정보를 포함할 수 있다.

[0065] 도 6은 사물인터넷 플랫폼과 연동하는 엔티티를 설명하기 위한 제 1 예시도이고, 도 7은 사물인터넷 플랫폼과 연동하는 엔티티를 설명하기 위한 제 2 예시도이다.

[0066] 도 6을 참고하면, 사물인터넷 플랫폼과 연동하는 어플리케이션 엔티티(AE)는 어플리케이션 엔티티와 연결된 공통 서비스 엔티티(CSE)의 식별자(ID), 복수의 바이오 신호(bio seed) 값 및 복수의 바이오 신호에 따라 측정된 임피던스 값을 기반으로 암호키(PSK)를 생성할 수 있는 해시 함수에 대한 정보를 저장할 수 있다.

[0067] 한편, 도 7을 참고하면, 사물인터넷 플랫폼과 연동하는 공통 서비스 엔티티(CSE)는 공통 서비스 엔티티와 연결된 어플리케이션 엔티티(AE)의 식별자(ID), 어플리케이션 엔티티에 대한 바이오 시드와 인증키로 구성된 한 쌍의 인증 정보를 저장하는 데이터베이스, 복수의 어플리케이션 엔티티를 관리하는 경우 각각의 어플리케이션 엔티티에 대한 정보를 포함할 수 있다.

[0069] 도 8은 본 발명의 다른 실시예에 따른 사물인터넷 기기 인증 장치의 블록 구성도이다.

[0070] 도 8를 참조하면, 본 발명의 일 실시예에 따른 사물인터넷 기기 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.

[0071] 사물인터넷 기기 인증 장치(100)는 또한, 입력 인터페이스 장치(140), 출력 인터페이스 장치(150), 저장 장치(160) 등을 더 포함할 수 있다. 사물인터넷 기기 인증 장치(100)에 포함된 각각의 구성 요소들은 버스(Bus)(170)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0072] 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.

[0073] 저장 장치(160)는 사물인터넷 기기 인증 장치에서 입력하는 교류 신호의 크기 및 입력한 시간, 입력한 교류 신호에 따라 신체에서 발생하는 임피던스 값, 측정된 임피던스 값을 통해 생성된 보안키, 교류 신호 및 보안키로 구성된 인증 정보, 사물인터넷 플랫폼으로 수신한 임의의 교류 전류 값, 임의의 교류 전류 값을 통해 생성한 보안키를 저장할 수 있다.

[0074] 여기서, 적어도 하나의 명령은, 복수의 교류 전류를 신체에 입력하도록 하는 명령; 상기 입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정하도록 하는 명령; 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령; 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증

정보를 사물인터넷 플랫폼으로 전송하도록 하는 명령; 상기 사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정하도록 하는 명령; 및 상기 재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송하도록 하는 명령을 포함할 수 있다.

[0075] 여기서, 상기 교류 전류는, 교류 전류의 크기 및 신체에 입력되는 시간이 사용자에 의해 미리 설정될 수 있다.

[0076] 또한, 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령은, 해시 함수에 기반하여 상기 임피던스 값을 토대로 보안키를 생성하도록 하는 명령을 포함할 수 있다.

[0077] 한편, 상기 적어도 하나의 명령은, 상기 사물인터넷 플랫폼과 연동하는 제 3 서버에 상기 인증 정보를 전송하도록 하는 명령을 더 포함할 수 있다.

[0078] 또한, 상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송하도록 하는 명령은, 상기 인증 정보를 미리 설정된 주기에 따라 최신화하여 사물인터넷 플랫폼으로 전송하도록 하는 명령을 포함할 수 있다.

[0080] 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.

[0081] 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.

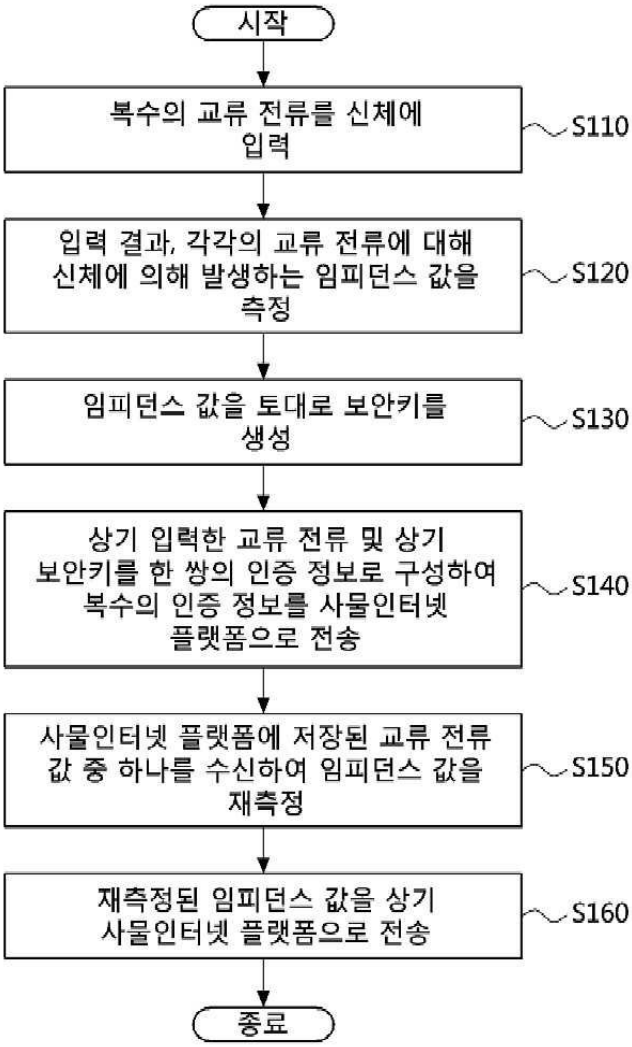
[0082] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0083] 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.

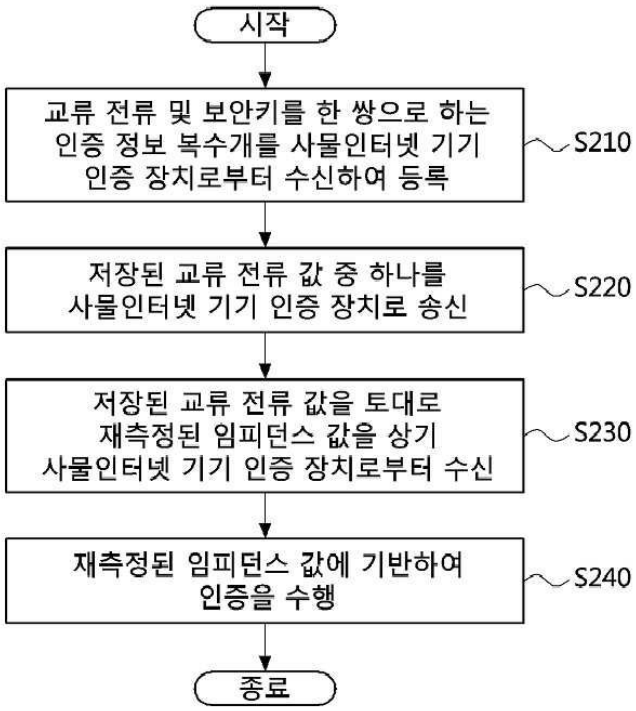
[0084] 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

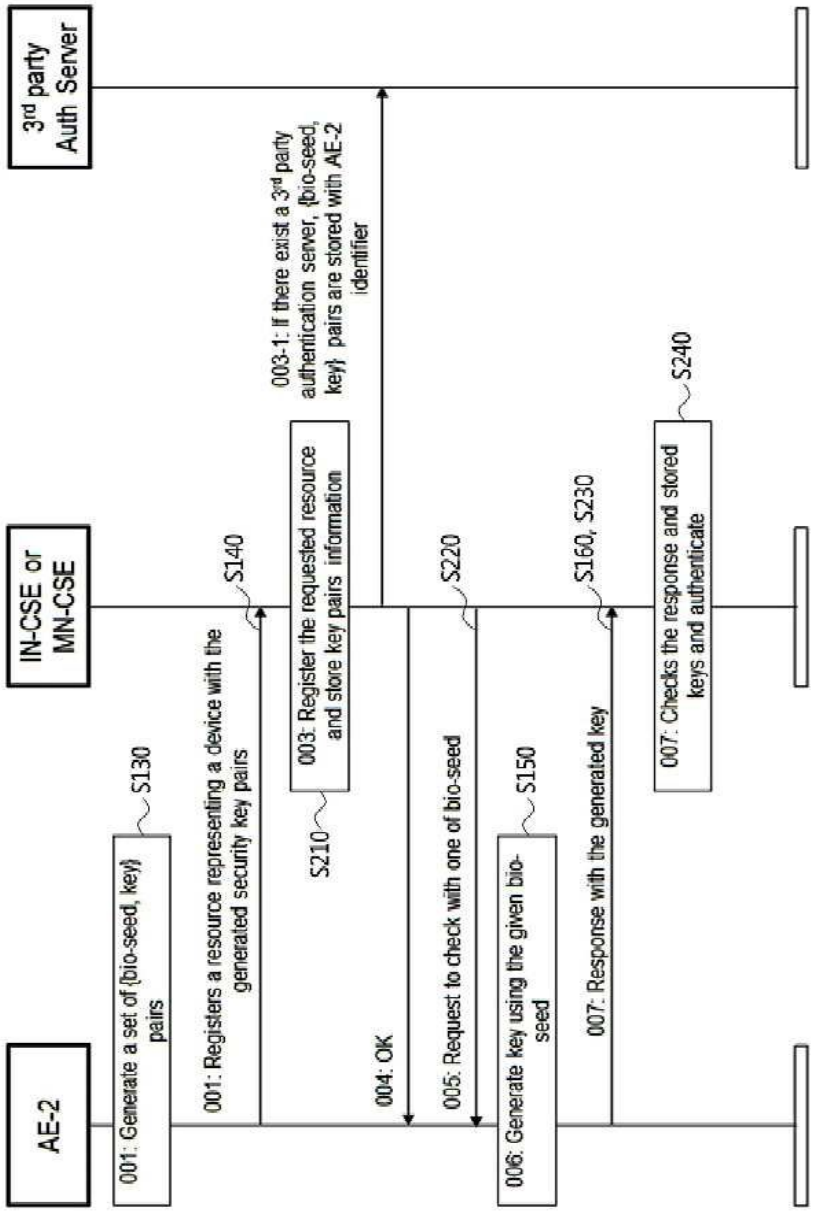
도면1


시작
복수의 교류 전류를 신체에 입력
S110
입력 결과, 각각의 교류 전류에 대해 신체에 의해 발생하는 임피던스 값을 측정
S120
임피던스 값을 토대로 보안키를 생성
S130
상기 입력한 교류 전류 및 상기 보안키를 한 쌍의 인증 정보로 구성하여 복수의 인증 정보를 사물인터넷 플랫폼으로 전송
S140
사물인터넷 플랫폼에 저장된 교류 전류 값 중 하나를 수신하여 임피던스 값을 재측정
S150
재측정된 임피던스 값을 상기 사물인터넷 플랫폼으로 전송
S160
종료

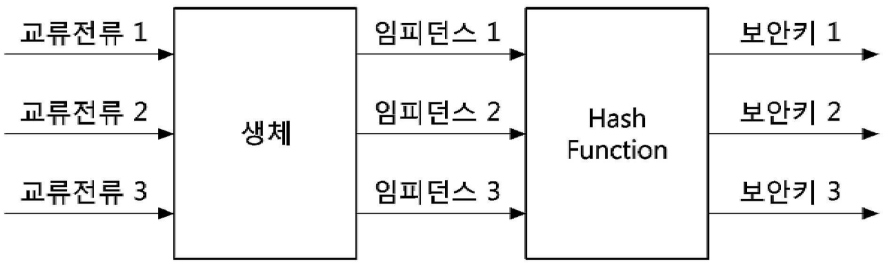
도면2


시작
교류 전류 및 보안키를 한 쌍으로 하는 인증 정보 복수개를 사물인터넷 기기 인증 장치로부터 수신하여 등록
S210
저장된 교류 전류 값 중 하나를 사물인터넷 기기 인증 장치로 송신
S220
저장된 교류 전류 값을 토대로 재측정된 임피던스 값을 상기 사물인터넷 기기 인증 장치로부터 수신
S230
재측정된 임피던스 값에 기반하여 인증을 수행
S240
종료

도면3


3rd party Auth Server
IN-CSE or MN-CSE
AE-2
001: Generate a set of {bio-seed, key} pairs
S130
001: Registers a resource representing a device with the generated security key pairs
S140
003: Register the requested resource and store key pairs information
S210
003-1: If there exist a 3rd party authentication server, {bio-seed, key} pairs are stored with AE-2 identifier
004: OK
005: Request to check with one of bio-seed
S220
006: Generate key using the given bio-seed
S150
007: Response with the generated key
S160, S230
007: Checks the response and stored keys and authenticate
S240

도면4


교류전류 1
교류전류 2
교류전류 3
생체
임피던스 1
임피던스 2
임피던스 3
Hash Function
보안키 1
보안키 2
보안키 3

도면5

Attribute Name	Description
bioKeyPair	This attribute contains a set of {input, key} pairs for the purpose of authentication
thirdPartyAuthServer	This attribute contains the address of 3rd party authentication server that holds a set of {input, key} pairs for a device representing this resource
keyIdentifier	If a set of {input, key} pairs is stored in a 3rd party authentication server, this identifier is a link to the stored authentication key pair.
bioKeyIndication	This attribute indicates that this IoT application uses bio key for its authentication

도면6

Entity	Bio-seeds	Key
ADN-AE1	10	1a2b3c4d5e6f7a8b
	12	3d7a2d4b8f6a9d7e
	14	1a2b3c4d8f9e7d7a

도면7

AE-ID	Bio-seeds	Key
C-Lock-ADN-AE1	10	1a2b3c4d5e6f7a8b
	12	3d7a2d4b8f6a9d7e
	14	1a2b3c4d8f9e7d7a
C-Door-ADN-AE2	19	2a1b4c4d5e6f7a8b
	17	1d3a3d4b8f6a9d7e
	15	3a8b3c4d8f9e7d7a

도면8