(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년07월30일
(11) 등록번호 10-2139589
(24) 등록일자 2020년07월24일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *G06K 19/06* (2006.01)
*H04L 29/06* (2006.01)
(52) CPC특허분류
*H04L 9/3242* (2013.01)
*G06K 19/06009* (2013.01)
(21) 출원번호 10-2018-0111994
(22) 출원일자 2018년09월19일
심사청구일자 2018년09월19일
(65) 공개번호 10-2020-0032856
(43) 공개일자 2020년03월27일
(56) 선행기술조사문헌
KR101740179 B1*
KR1020150112361 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**인하대학교 산학협력단**
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
**양대헌**
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
**정창훈**
서울특별시 강서구 방화동로1길 14, 공항타워팰리스오피스텔3 606호(방화동)
*(뒷면에 계속)*
(74) 대리인
**양성보**

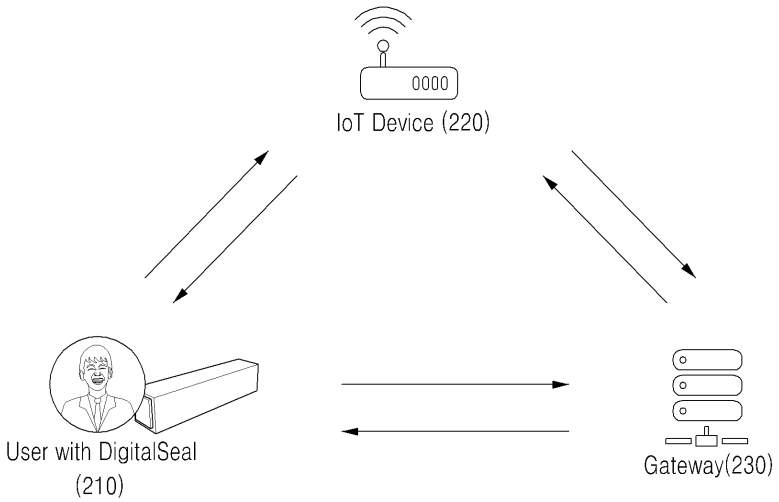
전체 청구항 수 : 총 4 항 심사관 : 한지혜

(54) 발명의 명칭 **사물 인터넷 환경에서 디지털 인감을 이용한 인증 및 키 설정 프로토콜**

## (57) 요 약

사물인터넷 환경에서 디지털 인감을 이용한 인증 및 키 설정 프로토콜 기술이 개신된다. 일 실시예에 따른 디지털 인감을 이용한 인증 방법은, 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 단계; 및 상기 게이트웨이에서 키를 생성함에 따라 상기 게이트웨이에서 생성된 키와 상기 등록된 디바이스에서 생성된 키를 비교한 결과에 기초하여 세션키를 설정하고, 상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 단계를 포함할 수 있다.

*대 표 도* - 도5



(52) CPC특허분류
*H04L 12/66* (2013.01)
*H04L 63/10* (2013.01)
*H04L 9/0825* (2013.01)
*H04L 9/321* (2013.01)

(72) 발명자
**최진춘**
경기도 광명시 안현로 36, 405동 502호(하안동, 하안4단지고층주공아파트)

**민대홍**
인천광역시 미추홀구 인하로 135, 금희,403호(용현동)

이 발명을 지원한 국가연구개발사업
과제고유번호 2018055881
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 글로벌연구실(GRL)사업
연구과제명 [Ezbaro] 빅데이터 기반의 DDoS공격의 분석, 모델링, 방어 기술 연구
기 여 율 1/1
주관기관 인하대학교
연구기간 2018.05.01 ~ 2019.02.28

# 명 세 서

## 청구범위

### 청구항 1

디지털 인감을 이용한 인증 방법에 있어서,

게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 단계; 및

상기 게이트웨이에서 키를 생성함에 따라 상기 게이트웨이에서 생성된 키와 상기 등록된 디바이스에서 생성된 키를 비교한 결과에 기초하여 세션키를 설정하고, 상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 단계

를 포함하고,

상기 게이트웨이에 특정 상황이 발생하였을 경우, 상기 디지털 인감을 통하여 상기 디바이스의 관리를 위한 상기 디바이스의 접근을 허용하는 단계

를 더 포함하고,

상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 단계는,

상기 게이트웨이에서 상기 게이트웨이의 개인키와 상기 등록된 디바이스의 공개키를 이용하여 ECDH 키를 생성하고, 상기 게이트웨이의 공개키, 상기 게이트웨이에서 생성된 디바이스의 해시 기반 메시지 인증 코드를 상기 등록된 디바이스에게 전달하고, 상기 등록된 디바이스에서 상기 게이트웨이로부터 전달받은 공개키와 디바이스의 개인키를 이용하여 ECDH 키를 생성하고, 상기 게이트웨이에서 생성된 ECDH 키와 상기 디바이스에서 생성된 ECDH 키가 동일할 경우, 상기 ECDH 키를 세션키로 사용하는 단계

를 포함하고,

상기 게이트웨이에 특정 상황이 발생하였을 경우, 상기 디지털 인감을 통하여 상기 디바이스의 관리를 위한 상기 디바이스의 접근을 허용하는 단계는,

상기 디바이스에 포함된 바코드가 디지털 인감으로 스캔됨에 따라 획득된 디바이스에 대한 해시 기반 메시지 인증 코드가 무선 통신을 통하여 상기 디바이스로 전송되고, 상기 디바이스에서 상기 전송받은 디바이스에 대한 해시 기반 메시지 인증 코드와 상기 디바이스의 비밀키를 공유함에 따라 저장된 해시 기반 메시지 인증 코드를 비교한 비교 결과 각각의 해시 기반 메시지 인증 코드가 동일한 경우, 상기 디바이스의 옵션 설정, 리셋을 포함하는 디바이스의 관리를 위한 디바이스의 접근을 허용하는 단계

를 포함하는 인증 방법.

### 청구항 2

삭제

### 청구항 3

삭제

### 청구항 4

제1항에 있어서,

상기 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 단계는,

사용자가 디지털 인감을 발급받음에 따라 상기 사용자에 의하여 상기 디지털 인감으로 상기 디바이스의 바코드가 스캔되어 디바이스에 대한 해시 기반 메시지 인증 코드가 획득되고, 상기 게이트웨이로 상기 획득된 디바이

스에 대한 해시 기반 메시지 인증 코드가 입력되는 단계

를 포함하는 인증 방법.

**청구항 5**

제1항에 있어서,

상기 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 단계는,

상기 게이트웨이에서, 상기 디바이스로부터 전달받은 디바이스의 공개키, 맥(MAC) 주소, 시리얼 번호를 포함하는 디바이스의 정보에 기초하여 상기 디바이스의 해시 기반 메시지 인증 코드를 생성하고, 상기 생성된 디바이스의 해시 기반 메시지 인증 코드와 사용자로부터 입력받은 디바이스에 대한 해시 기반 메시지 인증 코드를 비교한 비교 결과에 기초하여 상기 디바이스를 등록하는 단계

를 포함하는 인증 방법.

**청구항 6**

디지털 인감을 이용한 인증 방법을 위한 인증 시스템에 있어서,

컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로세서는,

게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 과정; 및

상기 게이트웨이에서 키를 생성함에 따라 상기 게이트웨이에서 생성된 키와 상기 등록된 디바이스에서 생성된 키를 비교한 결과에 기초하여 세션키를 설정하고, 상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 과정을 포함하고,

상기 게이트웨이에 특정 상황이 발생하였을 경우, 상기 디지털 인감을 통하여 상기 디바이스의 관리를 위한 상기 디바이스의 접근을 허용하는 과정

을 더 포함하고,

상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 과정은,

상기 게이트웨이에서 상기 게이트웨이의 개인키와 상기 등록된 디바이스의 공개키를 이용하여 ECDH 키를 생성하고, 상기 게이트웨이의 공개키, 상기 게이트웨이에서 생성된 디바이스의 해시 기반 메시지 인증 코드를 상기 등록된 디바이스에게 전달하고, 상기 등록된 디바이스에서 상기 게이트웨이로부터 전달받은 공개키와 디바이스의 개인키를 이용하여 ECDH 키를 생성하고, 상기 게이트웨이에서 생성된 ECDH 키와 상기 디바이스에서 생성된 ECDH 키가 동일할 경우, 상기 ECDH 키를 세션키로 사용하는 과정을 포함하고,

상기 게이트웨이에 특정 상황이 발생하였을 경우, 상기 디지털 인감을 통하여 상기 디바이스의 관리를 위한 상기 디바이스의 접근을 허용하는 과정은,

상기 디바이스에 포함된 바코드가 디지털 인감으로 스캔됨에 따라 획득된 디바이스에 대한 해시 기반 메시지 인증 코드가 무선 통신을 통하여 상기 디바이스로 전송되고, 상기 디바이스에서 상기 전송받은 디바이스에 대한 해시 기반 메시지 인증 코드와 상기 디바이스의 비밀키를 공유함에 따라 저장된 해시 기반 메시지 인증 코드를 비교한 비교 결과 각각의 해시 기반 메시지 인증 코드가 동일한 경우, 상기 디바이스의 옵션 설정, 리셋을 포함하는 디바이스의 관리를 위한 디바이스의 접근을 허용하는 과정을 포함하는,

인증 시스템.

## *발명의 설명*

## 기 술 분 야

[0001] 아래의 설명은 온라인상에 존재하는 사물인터넷 디바이스를 안전하게 관리해주는 프로토콜에 관한 기술이다.

## 배 경 기 술

[0003] 사물인터넷이란, 기존에 컴퓨터나 스마트 폰에서만 가능했던 인터넷을 책상, 자동차, 냉장고, 수온 조절기, 가스레인지, 침대, 실내등 등의 여러 사물에서도 사용 가능한 것을 의미한다. 사물인터넷의 범위는 앞에서 언급한 유형의 사물에만 국한되지 않으며, 교실, 커피숍, 버스정류장 등 공간은 물론 결제 프로세스 등 무형의 사물까지도 그 대상에 포함된다. 이렇게 인터넷에 연결된 유·무형의 사물인터넷은 사용자에게 다양한 서비스를 제공할 수 있다. 예를 들면, 침대가 사람이 수면 중인지를 스스로 인지하여 실내등을 자동으로 ON/OFF하는 기능, 냉장고가 보관중인 물품을 확인하여 거의 소진된 물품을 자동으로 주문하는 기능 등의 서비스를 제공할 수 있다. 그런데 이러한 사물인터넷은 다양한 네트워크 취약점이 존재하며 따라서 악성 해커로부터 스니핑, 스푸핑, DDoS 등의 공격을 받을 수 있다. 게다가 사물인터넷은 사용자의 삶의 물리적으로 영향을 줄 수도 있으므로, 사용자에게 물리적인 피해를 발생시킬 수도 있다. 예를 들어, 사물인터넷 홈 캠을 이용하여 사용자의 사생활을 파악할 수도 있고, 사용자가 집에 없는 동안 사물인터넷 스마트 가스레인지를 켜서 화재를 발생시킬 수도 있다. 이에 따라 사물인터넷 분야에서는 안전한 세션키 관리, 통신, 접근제어 프로토콜 등이 필요한 상황이다.

[0004] 기존의 사물인터넷 디바이스 접근제어 프로토콜에 따르면, 사용자가 새로운 사물인터넷 디바이스(또는 서비스)를 사용하기 위해서는 WIFI 또는 Bluetooth를 통해 비밀번호를 입력한 후, 자신의 홈 네트워크에 디바이스를 등록하여야 한다. 그런데 사용자들은 여러 사물인터넷 디바이스를 쉽게 관리하기 위하여 다음과 같은 취약점을 무시하고 사용하는 경우가 있다. (1)사용자들은 "0000", "1234", "asdf"처럼 초기 비밀번호를 사용한다. (2)사용자들은 "apple", "Room302"처럼 간단한 비밀번호를 사용한다. (3)사용자들은 여러 디바이스에 대하여 하나의 비밀번호를 사용한다. (4)비밀번호가 스티커 형식으로 사물인터넷 디바이스 외부에 붙여져 있는 경우가 있는데, 이 비밀번호를 그대로 사용한다. 이러한 취약점뿐만 아니라 사회공학적 기법 등의 공격 기법을 이용하여, 공격자는 WIFI 또는 Bluetooth를 통해 사용자의 집 외부에서 사용자의 사물인터넷 디바이스 또는 홈 네트워크에 접속을 할 수 있으며, 이를 통해 다양한 네트워크 공격을 시도할 수 있게 된다.

[0005] 메시지 인증 코드를 위한 디지털인감(특허 등록번호 1017401790000)이란 온라인 또는 오프라인 상에서 어떠한 데이터를 포함하고 있는 2차원의 바코드를 스캔하여 바코드 데이터를 읽어 들이고, 그 바코드 데이터와 내장되어 있는 비밀키를 이용하여 해시 기반의 메시지 인증 코드를 생성하는 도구이다. 디지털인감은 바코드를 스캔하기 위해서 복수 개의 센서를 가지고 있으며, 비밀키를 저장하기 위하여 그리고 해시 기반의 메시지 인증 코드를 생성하기 위하여 소형 컴퓨터가 내장되어 있다. 디지털인감은 온라인 또는 오프라인에서 메시지의 대한 인증과 메시지의 무결성을 보장할 수 있다. 예를 들어 온라인 뱅킹에 적용하면, MitM, MitB 공격으로부터 안전한 트랜잭션을 제공할 수 있으며 비밀키 관리에 대하여 보안성을 향상시킬 수 있고, 차용증 같은 오프라인 문서에 적용하면, 차용 사실을 증명할 수 있는 인감처럼 사용될 수 있다.

[0006] 한편, 미국의 IT 분야 리서치 기업인 가트너에 따르면, 2020년이 되면 거의 200억 대에 가까운 사물인터넷 디바이스가 인터넷에 연결이 될 것이고, 사물인터넷 제품 및 서비스 공급 업체는 약 3000억 달러가 넘는 매출을 올리게 될 것이라고 전망하였다. Shodan은 세계 최초 사물인터넷 검색엔진이며, 검색 필터에 따라서 사물인터넷 디바이스의 헤더 정보를 검색할 수 있다. 그런데 이 헤더 정보에는 관리자 아이디와 기본 비밀번호가 노출되어 있는 경우가 많으며, 이에 따라 공격자는 공격 가능한 사물인터넷 디바이스를 쉽게 검색할 수 있다. 이에 따라 다양한 보안 솔루션, 안전한 사물인터넷 비밀키 관리 프로토콜, 접근제어 프로토콜 등이 필요한 상황이다.

## 발명의 내용

### 해결하려는 과제

[0008] 본 발명이 해결하고자 하는 과제는 사용자가 사물인터넷 디바이스를 자신의 게이트웨이(홈 네트워크)에 안전하게 등록해주는 것을 보장하는 기술을 제안한다.

### 과제의 해결 수단

[0010] 디지털 인감을 이용한 인증 방법은, 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지

인증 코드에 기초하여 상기 디바이스를 등록하는 단계; 및 상기 게이트웨이에서 키를 생성함에 따라 상기 게이트웨이에서 생성된 키와 상기 등록된 디바이스에서 생성된 키를 비교한 결과에 기초하여 세션키를 설정하고, 상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 단계를 포함할 수 있다.

[0011] 상기 인증 방법은, 상기 게이트웨이에 특정 상황이 발생하였을 경우, 사용자에게 상기 디바이스에 접근을 허용하는 단계를 더 포함하고, 상기 게이트웨이에 특정 상황이 발생하였을 경우, 사용자에게 상기 디바이스에 접근을 허용하는 단계는, 상기 사용자에 의하여 상기 디바이스에 포함된 바코드가 디지털 인감으로 스캔되어 상기 디바이스에 대한 해시 기반 인증 코드가 획득되고, 무선 통신을 통하여 상기 디바이스에 상기 획득된 디바이스에 대한 해시 기반 인증 코드가 상기 디바이스로 전송되는 단계; 및 상기 디바이스에서 상기 사용자로부터 전송받은 디바이스에 대한 해시 기반 인증 코드와 상기 디바이스의 비밀키를 공유함에 따라 저장된 해시 기반 인증 코드를 비교함에 따른 비교 결과 각각의 해시 기반 인증 코드가 동일한 경우, 사용자의 접근을 허용하는 단계를 포함할 수 있다.

[0012] 상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 단계는, 상기 게이트웨이에서 상기 게이트웨이의 개인키와 상기 등록된 디바이스의 공개키를 이용하여 ECDH 키를 생성하고, 상기 게이트웨이의 공개키, 상기 게이트웨이에서 생성된 디바이스의 해시 기반 메시지 인증 코드를 상기 등록된 디바이스에게 전달하고, 상기 등록된 디바이스에서 상기 게이트웨이로부터 전달받은 공개키와 디바이스의 개인키를 이용하여 ECDH 키를 생성하고, 상기 게이트웨이에서 생성된 ECDH 키와 상기 디바이스에서 생성된 ECDH 키가 동일할 경우, 상기 ECDH 키를 세션키로 사용하는 단계를 포함할 수 있다.

[0013] 상기 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 단계는, 사용자가 디지털 인감을 발급받음에 따라 상기 사용자에 의하여 상기 디지털 인감으로 상기 디바이스의 바코드가 스캔되어 디바이스에 대한 해시 기반 메시지 인증 코드가 획득되고, 상기 게이트웨이로 상기 획득된 디바이스에 대한 해시 기반 메시지 인증 코드가 입력되는 단계를 포함할 수 있다.

[0014] 상기 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 단계는, 상기 게이트웨이에서, 상기 디바이스로부터 전달받은 디바이스의 공개키, 맥(MAC) 주소, 시리얼 번호를 포함하는 디바이스의 정보에 기초하여 상기 디바이스의 해시 기반 메시지 인증 코드를 생성하고, 상기 생성된 디바이스의 해시 기반 메시지 인증 코드와 사용자로부터 입력받은 디바이스에 대한 해시 기반 메시지 인증 코드를 비교한 비교 결과에 기초하여 상기 디바이스를 등록하는 단계를 포함할 수 있다.

[0015] 디지털 인감을 이용한 인증 방법을 위한 인증 시스템은, 컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 게이트웨이에서 디지털 인감을 통하여 획득된 디바이스의 해시 기반 메시지 인증 코드에 기초하여 상기 디바이스를 등록하는 과정; 및 상기 게이트웨이에서 키를 생성함에 따라 상기 게이트웨이에서 생성된 키와 상기 등록된 디바이스에서 생성된 키를 비교한 결과에 기초하여 세션키를 설정하고, 상기 등록된 디바이스와 상기 게이트웨이 간 상기 설정된 세션키를 공유하는 과정을 처리할 수 있다.

## 발명의 효과

[0017] 디지털 인감을 이용하여 디바이스를 홈 네트워크에 등록시킴에 따라 통신을 위한 세션키를 디바이스와 게이트웨이가 공유함으로써 안전하게 통신을 수행할 수 있도록 제공할 수 있다.

[0018] 악성 해커가 사용자의 가정 내부 또는 외부에서 사용자의 디바이스에 접근하거나 홈 네트워크에 접근하는 것을 방어할 수 있다.

## 도면의 간단한 설명

[0020] 도 1은 바코드를 나타낸 예이다.

도 2는 일 실시예에 있어서, 디바이스를 게이트웨이에 등록하는 과정을 설명하기 위한 흐름도이다.

도 3은 일 실시예에 있어서, 다바이스와 게이트웨이가 세션키를 공유하는 과정을 설명하기 위한 흐름도이다.

도 4는 일 실시예에 있어서, 사용자가 디바이스에 접근하는 과정을 설명하기 위한 흐름도이다.

도 5는 일 실시예에 따른 인증 시스템의 구성을 설명하기 위한 블록도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0021] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0023] 도 2는 일 실시예에 있어서, 디바이스를 게이트웨이에 등록하는 과정을 설명하기 위한 흐름도이다.

[0024] 실시예에서는 디지털 인감을 발급하고, 디지털 인감과 네트워크의 비밀키를 공유하여 디바이스를 등록할 수 있다. 사용자는 정부, 은행, 제3 신뢰 기관(Trusted Third Party) 등의 공신력이 있는 기관으로부터 2차원의 바코드를 스캔할 수 있고, 비밀키와 해시 기반 메시지 인증 코드 알고리즘을 내장하고 있는 디지털 인감을 발급받는다. 이때, 사용자는 비밀키가 명시되어 있는 문서도 같이 받는다. 디지털 인감의 비밀키는 사용자마다 다르며, 발급받은 기관의 대면 인증을 통해 변경할 수 있다.

[0025] 사용자는 디지털 인감의 비밀키가 명시되어 있는 문서를 참조하여 게이트웨이에 비밀키를 직접 입력할 수 있다. 게이트웨이는 비밀키를 안전하게 보관함으로써 사용자의 디지털 인감과 네트워크의 비밀키 공유를 완료할 수 있다.

[0026] 사용자는 새로운 디바이스를 구입할 수 있다. 패키지 내에는 디바이스의 공개키, 맥(MAC) 주소, 시리얼번호로 이루어진 2차원의 바코드가 스티커 또는 종이 형식으로 포함될 수 있다.

[0027] 도 1을 참고하면, 바코드(10)를 나타낸 예이다. 예를 들면, 대한민국 등록특허번호 제10-1740179호에 제시된 바와 같이, 디지털 인감은 2차원 바코드를 스캔하기 위하여 구성된 복수 개의 센서를 통하여 2차원 바코드를 스캔함에 따른 바코드 데이터로부터 해시 기반의 메시지 인증 코드를 생성하는 처리하고, 바코드 데이터로부터 생성된 해시 기반의 메시지 인증 코드의 일부를 디스플레이하는 구성을 포함할 수 있다. 이때, 디지털 인감은 내부에 소형 컴퓨터가 내장되고, 해시 기반의 메시지 인증 코드를 생성하기 위한 키를 포함할 수 있다. 일례로, 바코드는 2차원의 검은색과 흰색으로 구성될 수 있으며, 흰색과 검은색의 구별이 가능한 광센서를 이용하여 2차원 바코드가 스캔될 수 있다.

[0028] 사용자(210)는 사용자의 디지털 인감을 이용하여 2차원의 바코드를 스캔하여 해시 기반 메시지 인증 코드를 획득할 수 있다(241, 242). 예를 들면, 사용자는 디지털 인감으로 디바이스(220)의 2차원 바코드를 스캔할 수 있다.

[0029] 사용자(210)는 디지털 인감으로 바코드를 스캔함에 따라 획득된 인증 코드를 게이트웨이에 입력할 수 있다(243). 이때, 인증 코드는 디바이스(예를 들면, 사물인터넷 디바이스) 등록을 위한 비밀번호 역할을 수행할 수 있다. 그리고, 사용자는 디바이스의 전원을 온(On)할 수 있다. 디바이스(220)는 자동으로 게이트웨이(230)에 공개키, 맥 주소 또는 시리얼 번호를 전송할 수 있다(244).

[0030] 게이트웨이(230)는 해시 기반 메시지 인증 코드 알고리즘에 기반하여 디바이스(220)로부터 전송받은 공개키, 맥 주소 또는 시리얼 번호를 이용하여 해시 기반 메시지 인증 코드를 생성할 수 있다(245). 게이트웨이(230)는 생성된 디바이스의 해시 기반 메시지 인증 코드와 사용자로부터 입력받은 디바이스에 대한 메시지 인증 코드를 비교할 수 있다(246). 이때, 게이트웨이(230)는 각각의 메시지 인증 코드를 비교하여 디바이스의 등록 여부를 결정할 수 있다.

[0031] 게이트웨이(230)는 생성된 디바이스의 해시 기반 메시지 인증 코드와 사용자로부터 입력받은 디바이스에 대한 메시지 인증 코드를 비교한 결과 동일할 경우, 게이트웨이(230)에 디바이스(220)를 등록할 수 있고, 동일하지 않을 경우, 게이트웨이(230)에 디바이스(220)를 등록하지 않는다. 이러한 과정을 통하여 안전하게 디바이스(220)를 게이트웨이(230)에 등록시킬 수 있다.

[0032] 도 3은 일 실시예에 있어서, 다바이스와 게이트웨이의 세션키를 공유하는 과정을 설명하기 위한 흐름도이다.

[0033] 게이트웨이(230)와 게이트웨이(230)에 등록된 디바이스(220)는 통신을 위한 세션키를 공유하여 안전하게 통신을 수행할 수 있다. 게이트웨이(230)는 게이트웨이의 개인키(230)와 디바이스(220)로부터 전달받은 공개키를 이용하여 ECDH(Elliptic Curve Diffie Hellman) 키를 생성할 수 있다(310). 게이트웨이(230)는 게이트웨이의 공개키, 해시 기반 메시지 인증 코드를 디바이스(220)로 전송할 수 있다(311). 여기서, 해시 기반 메시지 인증 코드는 도 2에서 설명한 바와 같이, 디바이스(220)로부터 전달받은 공개키, 맥 주소 또는 시리얼 번호를 이용하여 생성된 코드일 수 있다.

[0034] 디바이스(220)는 게이트웨이(230)로부터 전달받은 공개키와 디바이스(220)의 개인키를 이용하여 ECDH 키를 생성할 수 있다(312). ECDH 알고리즘에 따라 게이트웨이(230)에서 생성한 ECDH 키와 디바이스(220)에서 생성한

ECDH 키는 동일하다. 이와 같이 생성된 ECDH 키를 통신을 위한 세션키로 사용할 수 있다. 디바이스(220)는 전송받은 해시 기반 메시지 인증 코드를 디바이스 내에 저장할 수 있다(313). 이를 통해 안전하게 게이트웨이(230)와 디바이스(220)가 세션키를 공유할 수 있고, 상기 세션키를 이용하여 안전하게 통신을 수행할 수 있다. 다시 말해서, 게이트웨이(230)에 등록된 디바이스들 간에 세션키를 이용하여 통신을 수행할 수 있다. 여기서, 세션키 공유에 사용된 ECDH는 RSA 등과 같은 공개키 알고리즘으로 대체될 수 있으며, 공개키 알고리즘뿐만 아니라 세션키 공유에 사용할 수 있는 다른 알고리즘으로 대체될 수 있다.

[0035] 도 4는 일 실시예에 있어서, 사용자가 디바이스에 접근하는 과정을 설명하기 위한 흐름도이다.

[0036] 게이트웨이(230)에 특정 상황이 발생하였을 경우, 사용자(210)가 디바이스(220)에 직접 접근해야 하는 경우가 발생할 수 있다. 예를 들면, 게이트웨이(230)가 오류로 인해 작동을 멈추거나 접근할 수 없을 때, 사용자(210)가 디바이스(220)의 옵션 설정, 리셋 등을 위해 디바이스(220)에 직접 접근해야 하는 경우가 발생할 수 있다. 이때. 사용자(210)는 디바이스(220)의 패키지에 포함되어 있던 바코드를 사용자의 디지털 인감으로 스캔하여 디바이스(220)에 대한 해시 기반 메시지 인증 코드를 획득할 수 있다(410, 411). 그리고 사용자(210)는 디지털 인감을 통하여 무선 통신(예를 들면, WIFI, Bluetooth 등)을 통해 디바이스(220)에 대한 해시 기반 메시지 인증 코드를 전송할 수 있다(412).

[0037] 디바이스(220)는 전송받은 디바이스(220)에 대한 해시 기반 메시지 인증 코드와 기 저장된 해시 기반 메시지 인증 코드를 비교할 수 있다(413). 디바이스(220)는 사용자(210)로부터 전달받은 디바이스(220)에 대한 해시 기반 메시지 인증 코드와 비밀키를 공유할 때 저장했었던 해시 기반 메시지 인증 코드를 비교할 수 있다. 디바이스(220)는 사용자(210)로부터 전달받은 해시 기반 메시지 인증 코드와 비밀키를 공유함에 따라 저장해놓았던 해시 기반 메시지 인증 코드가 일치할 경우, 사용자(210)의 접근을 허락할 수 있다. 또한, 디바이스(220)는 사용자(210)로부터 전달받은 해시 기반 메시지 인증 코드와 비밀키를 공유함에 따라 저장해놓았던 해시 기반 메시지 인증 코드가 일치하지 않는다면, 사용자(210)의 접근을 불허할 수 있다. 사용자(210)는 해시 기반 메시지 인증 코드를 통해 디바이스(220)와 직접적으로 통신을 수행할 수 있게 된다.

[0038] 도 5는 일 실시예에 따른 인증 시스템의 구성을 설명하기 위한 블록도이다.

[0039] 인증 시스템은 사용자(210), 디바이스(220) 및 게이트웨이(230)간 데이터의 송수신을 통하여 네트워크 환경에서 디지털 인감을 이용한 인증 및 키 설정 프로토콜을 제공할 수 있다. 이때, 인증 시스템은 네트워크 환경으로 사물 인터넷 환경에서 사물 인터넷 디바이스(예를 들면, 사물 인터넷 디바이스)(220)를 안전하게 관리하는 프로토콜을 제공하여 디바이스(220)가 게이트웨이(230)에 안전하게 접속될 수 있다.

[0040] 사용자(210)는 디지털 인감을 이용하여 자신의 디바이스(220)만 게이트웨이(예를 들면, 홈 네트워크, 사물 인터넷 네트워크 등)(230)에 안전하게 등록시킬 수 있다. 다시 말해서, 공격자의 디바이스는 게이트웨이(230)에 등록시킬 수 없다. 이와 같이 등록된 적어도 하나 이상의 디바이스(220)는 안전하게 세션키를 공유하여 통신을 수행할 수 있다. 또한 사용자(210)가 직접 디바이스(220)에 안전하게 접근을 할 수 있다. 결과적으로, 사물인터넷 분야에서 안전한 통신 프로토콜을 제공할 수 있다.

[0041] 인증 시스템은 사용자(210)가 디바이스(220)를 자신의 게이트웨이(홈 네트워크)(230)에 안전하게 등록해주는 것을 보장한다. 사용자(210)는 디지털 인감을 이용하여 엔트로피(무질서도)가 높은 비밀번호를 생성할 수 있고, 상기 생성된 비밀번호를 이용하여 안전하게 디바이스(220)를 홈 네트워크에 등록시킬 수 있다. 등록 후에는 통신을 위한 세션키를 디바이스(220)와 게이트웨이(230)가 안전하게 공유함에 따라 안전한 통신이 가능하다.

[0042] 또한, 사용자(210)가 원한다면 직접 디바이스(220)에 접근할 수도 있다. 이를 통해 악성 해커가 사용자의 집 내부 또는 외부에서 사용자의 디바이스(220)에 접근하거나 게이트웨이에 접근하는 것을 방어할 수 있다. 이에 따라, DDoS 또는 멀웨어 확산, 개인 사생활 침해, 물리적 피해 등을 방어할 수 있다.

[0043] 실시예에 따른 기술을 통하여 다음과 같은 보안적 측면의 기술적 효과가 도출될 수 있다.

[0044] (1)사용자는 복수의 사물인터넷 디바이스의 비밀번호를 기억할 필요가 없다. 필요할 때마다 디지털 인감으로 사물인터넷 디바이스의 바코드를 스캔하면 비밀번호를 알 수 있기 때문에 복수의 디바이스의 비밀번호를 쉽게 관리할 수 있다.

[0045] (2)디지털 인감을 통해 생성되는 해시 기반 메시지 인증 코드는 비밀번호 역할을 하는데, 엔트로피가 높기 때문에, 공격자가 쉽게 공격할 수 없으므로 공격자가 사용자의 집 내부뿐만 아니라 외부에서 사용자의 사물인터넷 디바이스 또는 홈 네트워크에 접근하는 것을 차단할 수 있다.

[0046] (3)또한, 안전하게 통신을 위한 비밀키를 공유할 수 있으므로, 디바이스 간에 또는 디바이스와 게이트웨이(홈 네트워크)간에 안전한 통신을 보장한다. 따라서, 사용자의 사물인터넷 디바이스가 DDoS 또는 멀웨어 확산 등에 사용되거나, 개인의 사생활이 침해되거나, 스마트 온수기 또는 스마트 가스레인지를 통해 발생할 수 있는 화상 및 화재 사고를 방지할 수 있다.

[0047] (4)디바이스를 게이트웨이에 등록할 때, 디지털 인감을 이용하므로 MitM 공격에 강하다.

[0048] 일 실시예에 따르면, 스마트 냉장고, 스마트 가스레인지, 스마트 교실, 스마트 아파트 등의 모든 사물인터넷 디바이스 및 서비스 분야에서 사물인터넷 시스템을 구축 및 등록할 때 사용될 수 있다. 특히, 보안이 더욱 중요한 국방, 국가기관, 국/공립 연구소 등에서 사용되는 사물인터넷 디바이스에 적용 및 응용될 수 있다.

[0049] 일 실시예에 따른 인증 시스템은 모든 사물인터넷을 사용하는 분야에서 사용될 수 있으며, 사물인터넷은 국내에서 한정적으로 사용되는 것이 아니라 국제적으로도 많이 사용되고 있고, 그에 따라 전 세계 사용자들이 안전하게 사물인터넷을 사용할 수 있도록 제공할 수 있다. 또한, 디지털 인감 생산에 있어서 대량 생산 시스템을 도입하여 적은 비용으로 생산할 수 있다면, 디지털 인감 구입에 따라 소요되는 경비가 감소될 수 있다.

[0050] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0051] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0052] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

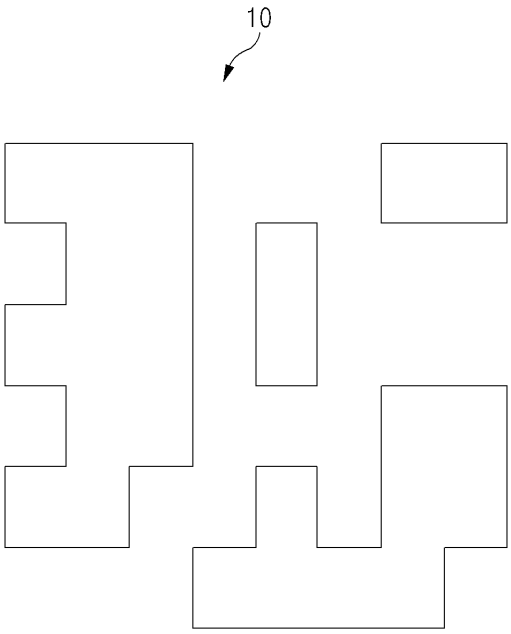
[0053] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0054] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한

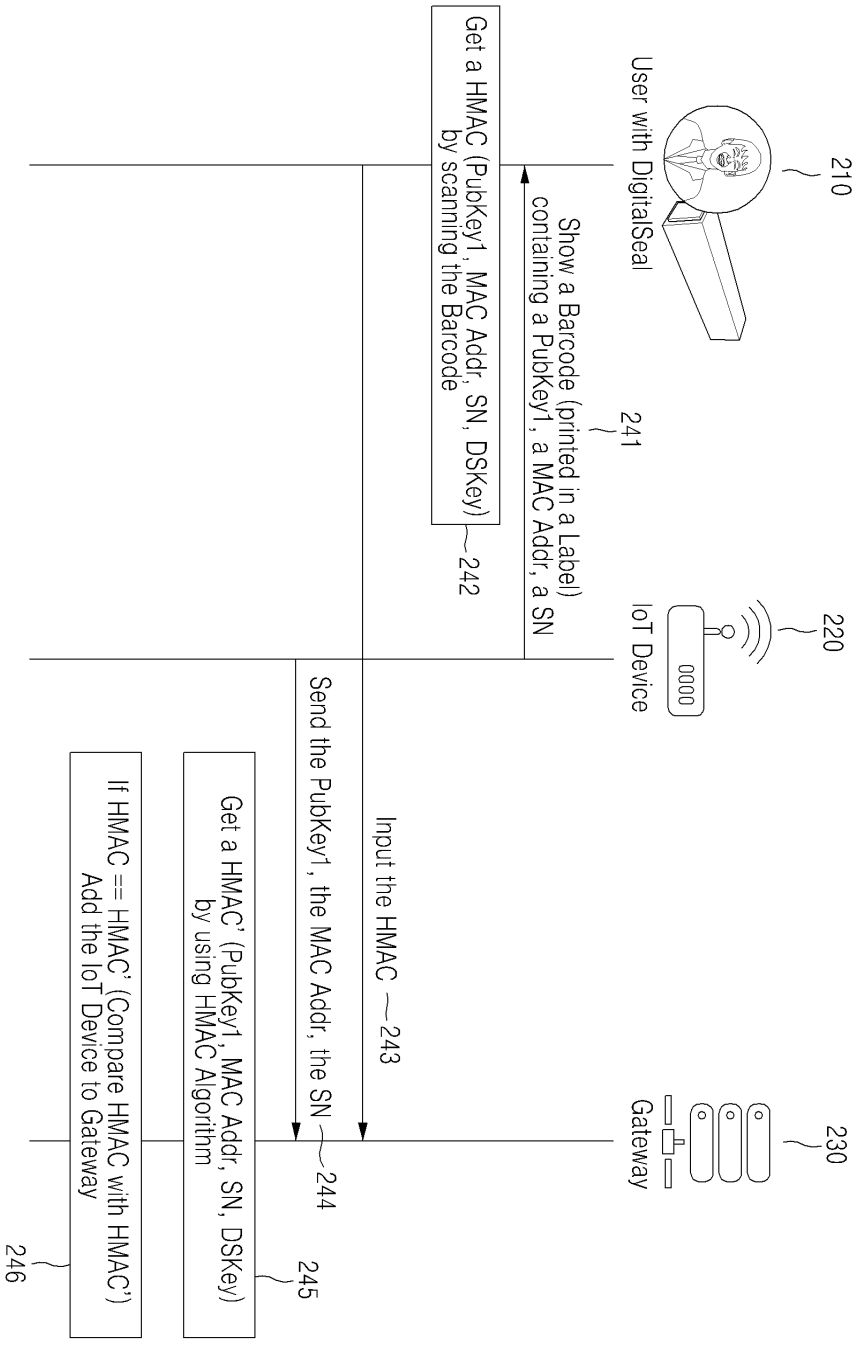
다.

## 도면

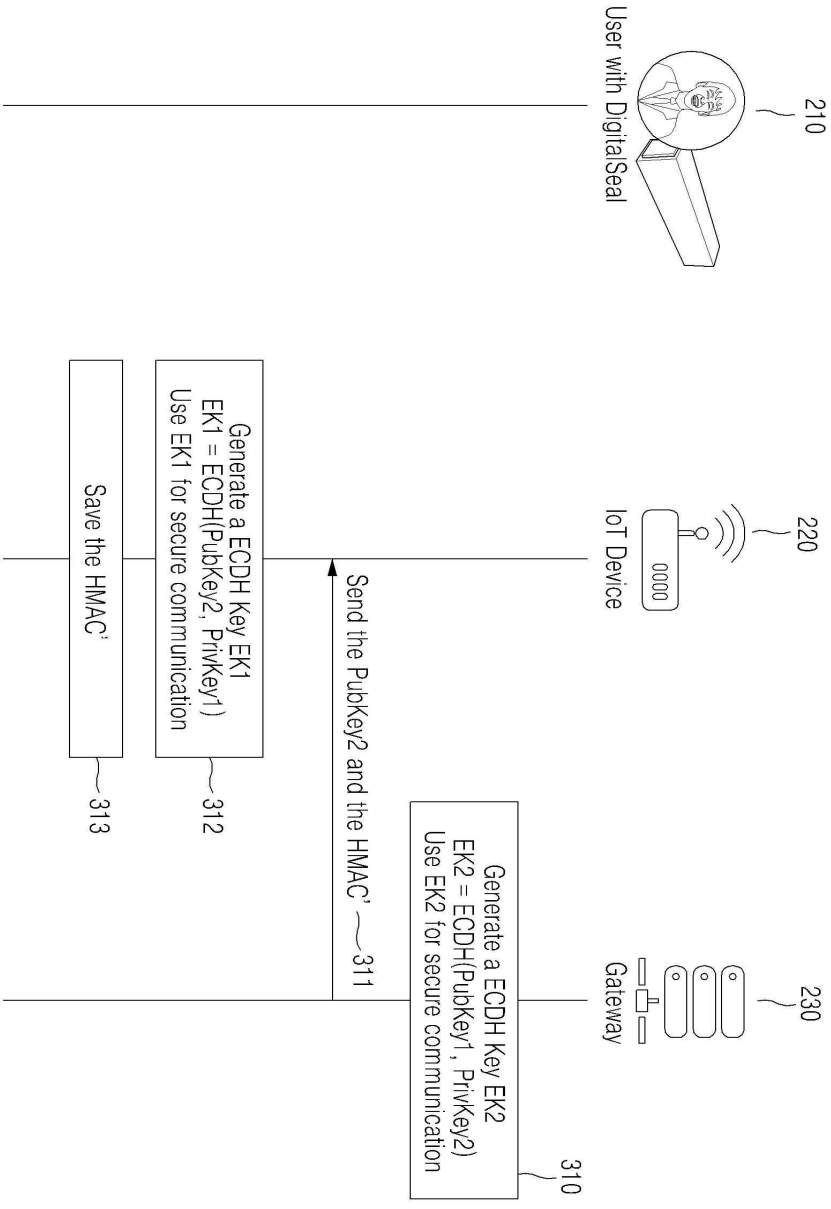
### 도면1



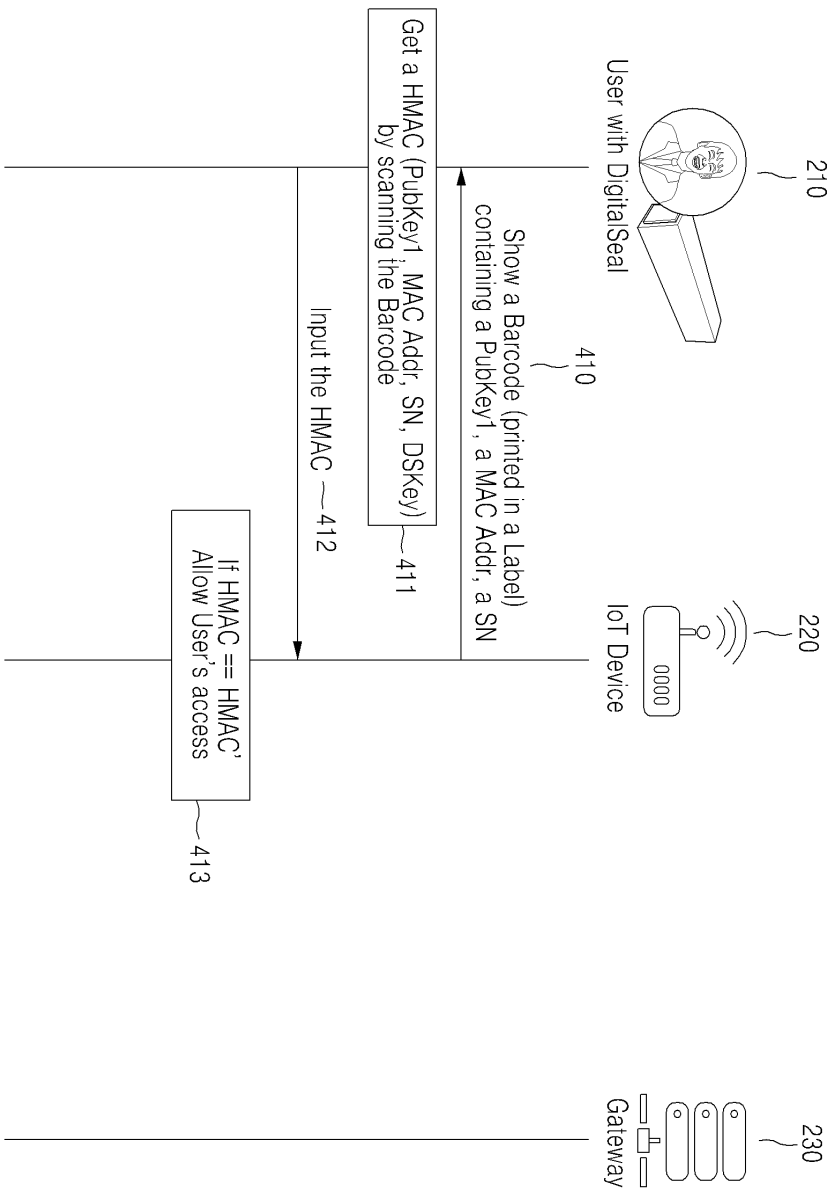
도면2


User with DigitalSeal
210
IoT Device
220
Gateway
230
Show a Barcode (printed in a Label) containing a PubKey1, a MAC Addr, a SN
241
Get a HMAC (PubKey1, MAC Addr, SN, DSKey) by scanning the Barcode
242
Input the HMAC
243
Send the PubKey1, the MAC Addr, the SN
244
Get a HMAC' (PubKey1, MAC Addr, SN, DSKey) by using HMAC Algorithm
245
If HMAC == HMAC' (Compare HMAC with HMAC') Add the IoT Device to Gateway
246

도면3


User with DigitalSeal
210
IoT Device
220
Gateway
230
Generate a ECDH Key EK2
EK2 = ECDH(PubKey1, PrivKey2)
Use EK2 for secure communication
310
Send the PubKey2 and the HMAC'
311
Generate a ECDH Key EK1
EK1 = ECDH(PubKey2, PrivKey1)
Use EK1 for secure communication
312
Save the HMAC'
313

도면4


User with DigitalSeal
210
IoT Device
220
Gateway
230
Show a Barcode (printed in a Label)
containing a PubKey1, a MAC Addr, a SN
410
Get a HMAC (PubKey1, MAC Addr, SN, DSKey)
by scanning the Barcode
411
Input the HMAC
412
If HMAC == HMAC'
Allow User's access
413

도면5