(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017 년 1 월 26 일 (26.01.2017)

WIPO | PCT

(10) 국제공개번호
WO 2017/014614 A1

(51) 국제특허분류:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) 국제출원번호: PCT/KR2016/008115

(22) 국제출원일: 2016 년 7 월 25 일 (25.07.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0104318 2015 년 7 월 23 일 (23.07.2015) KR
10-2016-0094254 2016 년 7 월 25 일 (25.07.2016) KR

(71) 출원인: **주식회사 투아이피 (2IP CO., LTD.)** [KR/KR]; 04418 서울시 용산구 한남대로 80, 3 층(한남동), Seoul (KR).

(72) 발명자: **조광현 (CHO, Kwang Hyun)**; 08254 서울시 구로구 고척로 3 가길 12 (오류동), Seoul (KR). **원재선 (WON, Jae Son)**; 14255 경기도 광명시 가림일로 79, 102 동 206 호 (철산동, 도덕파크타운), Gyeonggi-do (KR). **김태정 (KIM, Tae Jung)**; 04798 서울시 성동구 아차산로 153 (성수동 2 가), Seoul (KR).

(74) 대리인: **특허법인 무한 (MUHANN PATENT & LAW FIRM)**; 06044 서울시 강남구 학동로 3 길 9, 5 층 (논현동, 명림빌딩), Seoul (KR).

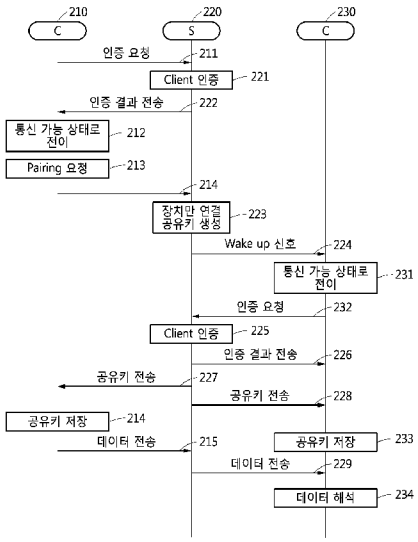
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[다음 쪽 계속]

(54) **Title**: METHOD FOR OPERATING COMMUNICATION CLIENT OF IOT DEVICE, AND IOT DEVICE INCLUDING COMMUNICATION CLIENT

(54) **발명의 명칭** : IOT 디바이스의 통신 클라이언트의 동작 방법 및 상기 통신 클라이언트를 포함하는 IOT 디바이스



211, 232 ... Request authentication
212, 231 ... Shift to communicable state
213 ... Request pairing
214, 233 ... Store sharing key
215, 229 ... Send data
221, 225 ... Authenticate client
222, 226 ... Send authentication result
223 ... Connect only device, generate sharing key
224 ... Wake up signal
227, 228 ... Send sharing key
234 ... Interpret data

(57) **Abstract**: An IoT device using a peer-to-peer communication is disclosed. A method for operating a client of the IoT device, which is a method for operating a client of the IoT device using a peer-to-peer communication, comprises the steps of: generating a personal key on the basis of a public key stored in a memory; sending the personal key to a server, and receiving a key-pair generation message for the public key and the personal key from the server; sending, to the server, an identifier generation request including at least one item of unique information; receiving, from the server, an identifier corresponding to the identifier generation request and a security key corresponding to the unique information; sending an authentication request including the identifier and the security key to the server, and receiving an authentication result corresponding the authentication request from the server; in response to the authentication result, shifting to a state in which the client is capable of communication; and sending data to a counterpart client via the server by using a sharing key sent from the server according to a request for pairing with the counterpart client.

(57) **요약서**: 피어투피어 통신을 이용한 IoT 디바이스가 개시된다. 이러한 IoT 디바이스의 클라이언트의 동작 방법은, 피어투피어 통신을 이용한 IoT 디바이스의 클라이언트의 동작 방법은, 메모리에 저장된 공개키를 기초로 개인키를 생성하는 단계; 상기 개인키를 서버로 전송하고, 상기 서버로부터 공개키 및 개인키에

[다음 쪽 계속]

WO 2017/014614 A1

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

대한 키-페어 생성 메시지를 수신하는 단계; 상기 서버로 하나 이상의 고유 정보를 포함하는 식별자 생성 요청을 전송하는 단계; 상기 서버로부터 상기 식별자 생성 요청에 대응하는 식별자 및 고유 정보에 대응하는 보안키를 수신하는 단계; 및 상기 서버로 상기 식별자 및 상기 보안키를 포함하는 인증 요청을 전송하고, 상기 서버로부터 상기 인증 요청에 대응하는 인증 결과를 수신하는 단계; 상기 인증 결과에 대응하여, 상기 클라이언트가 통신 가능한 상태로 천이하는 단계; 및 상대 클라이언트와의 페이링 요청에 따라 상기 서버로부터 전송된 공유키를 이용하여 데이터를 서버를 통해 상기 상대 클라이언트로 전송하는 단계를 포함한다.

명세서

발명의 명칭: IOT 디바이스의 통신 클라이언트의 동작 방법 및 상기 통신 클라이언트를 포함하는 IOT 디바이스

기술분야

[1] 아래 실시예들은 IoT 디바이스의 통신 클라이언트의 동작 방법 및 상기 통신 클라이언트를 포함하는 IoT 디바이스에 관한 것이다.

배경기술

[2] 최근 들어 사물 인터넷이라고 불리는 IoT(Internet of Things)가 화두가 되고 있다.

[3] 이러한 IoT를 통해 가전제품, 전자기기뿐만 아니라 헬스케어, 원격검침, 스마트홈, 스마트카 등 다양한 분야에서 사물을 네트워크로 연결해 정보를 공유할 수 있다.

[4] 이러한 IoT로의 기술 진화에 따라 다양한 회사 또는 연구소에서 IoT에 대한 기술 개발이 가속화 되고 있으나, 실제 생활에서 활용되기는 쉽지 않다. 이는 IoT의 기반이 되는 객체(entity)들에게 통신 기능을 부여하기가 어려울 뿐 아니라. 통신 기능을 부여한다고 해도 어떻게 통신을 할 것인지에 대한 표준 기술이 정의되어 있지 않기 때문이다. 따라서, 현재로서는 개별 통신 회사 별로 독자적인 기술에 기반하여 IoT 서비스를 준비하고 있으나, 범용성이 결여된다.

발명의 상세한 설명

기술적 과제

[5] 실시예들은 사용자의 개인 정보를 입력하지 않고 통신 가능한 식별자를 부여할 수 있는 보안 통신 플랫폼을 기반으로 한 IoT 네트워크를 제공한다. 또한, 실시예들은 IoT 네트워크에서 동작하는 IoT 디바이스 및 IoT 디바이스를 IoT 네트워크를 통해 통신 가능하도록 하는 클라이언트를 제공한다.

과제 해결 수단

[6] 이러한 IoT 디바이스의 클라이언트의 동작 방법은, 피어투피어 통신을 이용한 IoT 디바이스의 클라이언트의 동작 방법은, 메모리에 저장된 공개키를 기초로 개인키를 생성하는 단계; 상기 개인키를 서버로 전송하고, 상기 서버로부터 공개키 및 개인키에 대한 키-페어 생성 메시지를 수신하는 단계; 상기 서버로 하나 이상의 고유 정보를 포함하는 식별자 생성 요청을 전송하는 단계; 상기 서버로부터 상기 식별자 생성 요청에 대응하는 식별자 및 고유 정보에 대응하는 보안키를 수신하는 단계; 및 상기 서버로 상기 식별자 및 상기 보안키를 포함하는 인증 요청을 전송하고, 상기 서버로부터 상기 인증 요청에 대응하는 인증 결과를 수신하는 단계; 상기 인증 결과에 대응하여, 상기 클라이언트가 통신 가능한 상태로 천이하는 단계; 및 상대 클라이언트와의 페이링 요청에 따라 상기 서버로부터 전송된 공유키를 이용하여 데이터를 서버를 통해 상기 상대

클라이언트로 전송하는 단계를 포함한다.

[7] 피어투피어 통신을 이용한 IoT 디바이스는, 피어투피어 통신을 위한 통신 인터페이스; 피어투피어 통신을 수행하는 클라이언트가 저장된 메모리; 및 상기 클라이언트의 실행을 제어하는 중앙처리장치를 포함하고, 상기 클라이언트는, 상기 메모리에 저장된 공개키를 기초로 개인키를 생성하는 단계; 상기 개인키를 서버로 전송하고, 상기 서버로부터 공개키 및 개인키에 대한 키-페어 생성 메시지를 수신하는 단계; 상기 서버로 하나 이상의 고유 정보를 포함하는 식별자 생성 요청을 전송하는 단계; 상기 서버로부터 상기 식별자 생성 요청에 대응하는 식별자 및 고유 정보에 대응하는 보안키를 수신하는 단계; 및 상기 서버로 상기 식별자 및 상기 보안키를 포함하는 인증 요청을 전송하고, 상기 서버로부터 상기 인증 요청에 대응하는 인증 결과를 수신하는 단계; 상기 인증 결과에 대응하여, 상기 클라이언트가 통신 가능한 상태로 천이하는 단계; 및 상대 클라이언트와의 페이링 요청에 따라 상기 서버로부터 전송된 공유키를 이용하여 데이터를 서버를 통해 상기 상대 클라이언트로 전송하는 단계를 수행한다.

발명의 효과

[8] 실시예들은 사용자의 개인 정보를 입력하지 않고 통신 가능한 식별자를 부여할 수 있는 보안 통신 플랫폼을 기반으로 한 IoT 네트워크를 제공할 수 있다. 또한, 실시예들은 IoT 네트워크에서 동작하는 IoT 디바이스 및 IoT 디바이스를 IoT 네트워크를 통해 통신 가능하도록 하는 클라이언트를 제공할 수 있다. 이를 통해 통신사 위주의 IoT 네트워크가 아니라, 무선 통신망을 통해 쉽게 IoT 네트워크를 구현할 수 있도록 한다.

도면의 간단한 설명

[9] 도 1은 일실시예에 따른 클라이언트 인증 방법을 설명하기 위한 흐름도이다.

[10] 도 2는 일실시예에 따른 IoT 디바이스의 클라이언트의 페어링(paring) 동작 방법을 설명하기 위한 흐름도이다.

[11] 도 3은 일실시예에 따른 IoT 디바이스를 설명하기 위한 블록도이다.

발명의 실시를 위한 형태

[12] 이하, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[13] 아래 설명하는 실시예들에는 다양한 변경이 가해질 수 있다. 아래 설명하는 실시예들은 실시 형태에 대해 한정하려는 것이 아니며, 이들에 대한 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[14] 실시예에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 실시예를 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 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.

[15] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 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 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[16] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조 부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[17] <u><IoT 디바이스 간 통신을 위한 보안 통신 플랫폼(Secure Communication Platform(SCP)></u>

[18] 도 1은 일실시예에 따른 IoT 디바이스에 설치되는 클라이언트 인증 방법을 설명하기 위한 흐름도이다.

[19] 도 1을 참조하면, 클라이언트(110)는 서버로 공개키(public key) 요청을 전송한다(111). 서버(120)는 클라이언트(110)로부터 수신된 공개키 요청에 대응하여 공개키를 발급한다(121). 공개키의 사이즈는, 예를 들어, 64 바이트, 즉, 512 비트일 수 있다. 서버(120)는 클라이언트(110)로 공개키를 전송한다(122). 서버(120)와 클라이언트(110)는 암호화되지 않은 통신을 수행할 수 있다.

[20] 클라이언트(110)는 공개키를 저장하고, 개인키(private key)를 생성한다(112). 개인키의 사이즈는, 예를 들어, 64 바이트일 수 있다. 클라이언트(110)는 개인키를 서버(120)로 전송한다(113). 클라이언트(110)는 공개키를 이용하여 개인키를 암호화할 수 있고, 암호화된 개인키를 서버(120)로 전송할 수 있다. 서버(120)는 클라이언트(110)로부터 개인키를 수신한다. 서버(120)는 공개키를 가지고 있으므로, 공개키를 이용하여 암호화된 개인키를 복호화(decryption)할 수 있다.

[21] 서버(120)는 공개키 및 개인키를 키-페어(key pair)로 매핑한다(123). 서버(120)는 매핑된 키-페어를 서버(120)에 저장할 수 있다(124). 서버(120)는 키-페어 생성 메시지를 클라이언트(110)에게 전송한다(125). 서버(120)는 개인키를 이용하여 키-페어 생성 메시지를 암호화할 수 있다.

[22] 클라이언트(110)는 키-페어 생성 메시지를 이용하여 키-페어의 생성을 확인한다. 클라이언트(110)는 키-페어를 저장한다(114). 예를 들어, 키-페어의 생성이 확인된 경우, 클라이언트(110)는 개인키 및 공개키를 키-페어로 매핑할 수 있고, 매핑된 키-페어를 클라이언트(110)에 저장할 수 있다.

[23] 도 1에 도시된 예의 경우, 키-페어는 클라이언트(110) 및 서버(120)에 저장될 수

있다. 전술한 키-페어의 저장 위치는 일실시예에 따른 예시적인 사항일 뿐, 키-페어의 저장 위치는 전술한 사항으로 한정되지 않는다. 예를 들어, 키-페어는 클라이언트(110) 및 서버(120) 중 어느 하나에 저장될 수 있다.

[24] 클라이언트(110)는 고유 정보를 포함하는 식별자 생성 요청을 서버(120)로 전송한다(115). 식별자 생성 요청은 개인키를 이용하여 암호화될 수 있다. 고유 정보는, 예를 들어, 클라이언트(110)가 설치되는 물리적 장치 또는 운영체제(Operating System, OS)에 대응하는 장치 고유키 및 클라이언트(110)에서 실행되는 통신 소프트웨어에 대응하는 제조키 중 적어도 하나를 포함할 수 있다.

[25] 클라이언트(110)의 물리적 장치는, 예를 들어, CPU 및 MPU(Micro Processor Unit) 중 적어도 하나를 포함할 수 있다. 장치 고유키는 CPU의 식별 정보 또는 MPU의 식별 정보로부터 획득될 수 있다. 클라이언트(110)에 저장된 운영체제는 다른 운영체제와 구별되게 하는 고유 정보를 가질 수 있다. 이로 인해, 클라이언트(110)는 운영체제의 고유 정보로부터 장치 고유키를 획득할 수 있다.

[26] 제조키는 사이트키, 제조사키, 및 제품키를 포함할 수 있다. 사이트키는 사이트 정보에 대응한다. 사이트 정보는, 예를 들어, 사이트 IP 주소를 기초로 하는 정보를 나타낼 수 있다. 제조사키는 제조사 정보에 대응한다. 제조사 정보는, 예를 들어, 통신 소프트웨어를 제조하는 제조사의 식별 정보를 나타낼 수 있다. 제품키는 통신 소프트웨어의 버전 정보에 대응한다.

[27] 장치 고유키 및 제조키는 미리 정해진 사이즈를 가질 수 있다. 예를 들어, 장치 고유키의 사이즈는 128 비트이고, 제조키의 사이즈는 208 비트일 수 있다. 마찬가지로, 사이트키, 제조사키, 및 제품키는 미리 정해진 사이즈를 가질 수 있다. 예를 들어, 사이트키의 사이즈는 80비트일 수 있고, 제조사키의 사이즈는 64비트일 수 있으며, 제품키의 사이즈는 64비트일 수 있다.

[28] 제조키는 사이트키, 제조사키, 및 제품키의 순서대로 구성될 수 있다. 사이트키, 제조사키, 및 제품키의 순서는 예시적인 사항일 뿐, 사이트키, 제조사키, 및 제품키의 순서는 전술한 사항으로 한정되지 않는다.

[29] 서버(120)는 보안키를 생성한다. 일실시예에 있어서, 서버(120)는 클라이언트(110)의 고유 정보에 대응하는 보안키를 생성할 수 있다. 예를 들어, 서버(120)가 클라이언트(110)로부터 장치 고유키 및 제조키를 수신한 경우, 서버(120)는 장치 고유키 및 제조키를 변형하여 보안키를 생성할 수 있다. 서버(120)는 128 비트의 장치 고유키 및 208 비트의 제조키를 기초로 256 비트의 보안키를 생성할 수 있다. 후술하겠지만, 보안키는 클라이언트와 다른 클라이언트 사이에 교환되는 패킷을 암호화하는데 사용될 수 있다.

[30] 서버(120)는 식별자를 생성한다. 식별자의 사이즈는, 예를 들어, 64 바이트일 수 있다. 이하, 식별자에 대해서 설명한다.

[31] 서버(120)는 클라이언트(110)의 식별자 생성 요청이 있는 경우, 식별자를 랜덤하게 생성할 수 있고, 식별자를 클라이언트(110)에 할당할 수 있다. 식별자는

n개의 구별 정보를 기초로 한 n자리의 랜덤 값(n^n) 중 어느 하나일 수 있다. 예를 들어, 1 바이트의 구별 정보가 64개인 경우, 식별자는 64자리를 갖는 64^64개의 랜덤 값 중에서 어느 하나일 수 있다. 서버(120)는 64개의 구별 정보를 랜덤하게 배열하여 식별자를 생성할 수 있다. 서버(120)는 식별자가 다른 식별자와 중복되는지 확인할 수 있고, 중복되지 않는 경우, 식별자를 클라이언트(110)에 할당할 수 있다. 이로 인해, 식별자는 클라이언트(110)마다 유니크(unique)할 수 있다. 서버는 식별자를 이용하여 클라이언트(110)와 다른 클라이언트를 구별할 수 있다.

[32] 식별자에는 해시 인덱스(Hash index)가 임베디드(embedded)될 수 있다. 해시 인덱스의 사이즈는, 예를 들어, 64 비트일 수 있다. 서버(120)는 변환 로직을 이용하여 식별자에 해시 인덱스를 임베디드할 수 있다. 예를 들어, 식별자의 사이즈가 64 바이트라 하자. 서버(120)는 첫 번째 바이트 내에 포함된 특정 비트에 변환 로직을 적용할 수 있다. 특정 비트에 변환 로직이 적용되는 경우, 특정 비트는 다른 비트로 변경되거나 변경되지 않을 수 있다. 특정 비트가 제1 논리값을 갖는 경우, 특정 비트는 변환 로직에 의해 제2 논리값으로 변경되거나 제1 논리값을 유지할 수 있다. 특정 비트는, 예를 들어, 1개일 수 있다. 서버는 나머지 바이트 내에 포함된 특정 비트에 변환 로직을 적용할 수 있다. 이로 인해, 식별자의 스트링(string) 중 일부는 변경될 수 있고, 해시 인덱스가 식별자에 임베디드될 수 있다. 예를 들어, 식별자가 ABCD의 스트링인 경우, ABCD는 변환 로직에 의해 AZDD가 될 수 있고, AZDD에 해시 인덱스가 임베디드될 수 있다.

[33] 서버(120)는 클라이언트(110)의 식별자 대신에 식별자로부터 획득되는 해시 인덱스를 이용하여 데이터베이스에 접근(access)할 수 있다. 서버(120)는 클라이언트(110)의 식별자에 기초하는 쿼리(query)를 데이터베이스로 전송하지 않고, 해시 인덱스에 기초하는 쿼리를 데이터베이스로 전송할 수 있다. 데이터베이스는 클라이언트(110)의 식별자의 스트링과 데이터베이스에 저장된 복수의 식별자의 스트링을 비교하지 않고, 해시 인덱스와 DB 인덱스를 비교할 수 있다. 이로 인해, 데이터베이스의 응답 속도 또는 데이터베이스를 검색하는 속도가 증가할 수 있다.

[34] 서버(120)는 클라이언트(110)에게 UDP 세션 유지를 위한 질문(question)을 생성한다. 서버(120)는 질문에 헤시 인덱스를 임베디드할 수 있다. 서버(120)는 질문을 클라이언트(110)로 전송한다.

[35] 클라이언트(110)가 질문을 수신하는 경우, 클라이언트(110)는 답(answer)을 생성할 수 있다. 여기서, 답이 질문에 대응하는 경우, UDP 세션은 유지될 수 있고, 답이 질문에 대응하지 못한 경우, UDP 세션은 유지되지 못하고 해제(release)된다.

[36] 생성된 답에는 해시 인덱스가 임베디드된다. 클라이언트(110)는 해시 인덱스가 임베디드된 답을 서버(120)로 전송할 수 있다.

[37] 서버(120)는 클라이언트(110)의 답을 확인한다. 서버(120)는 답으로부터 해시

인덱스를 획득할 수 있다. 예를 들어, 서버(120)는 답에 포함된 바이트를 XOR 연산하여 해시 인덱스를 획득할 수 있다. UDP 세션 유지를 위해 서버(120)는 클라이언트(110)의 식별자를 확인할 수 있다. 서버(120)는 해시 인덱스를 획득하였으므로, 해시 인덱스를 이용하여 식별자가 저장된 데이터베이스에 접근할 수 있다. 데이터베이스는 해시 인덱스에 대응하는 식별자를 서버(120)로 전송할 수 있다. 이로 인해, 서버(120)는 클라이언트(110)로부터 식별자를 수신하지 않고, 해시 인덱스에 기초하는 쿼리에 대한 응답을 통해 클라이언트(110)를 식별할 수 있어, 보다 빠르게 클라이언트(110)를 식별할 수 있다. 이로 인해, UDP 세션의 validation이 보다 빠르게 확인될 수 있고, UDP 세션이 유지될 수 있다. 또한, 클라이언트(110)의 IP 주소가 변경되어도 서버(120)는 해시 인덱스를 이용하여 클라이언트(110)를 빠르게 식별할 수 있다. 이로 인해, 피투피 통신과 같이 IP가 변화하는 환경에서도 UDP 세션의 validation이 확인될 수 있고, UDP 세션이 유지될 수 있다.

[38] 서버(120)가 식별자 및 보안키를 생성한 경우(126), 서버(120)는 식별자 및 보안키를 클라이언트(110)로 전송한다(127). 식별자 및 보안키는 개인키를 이용하여 암호화될 수 있다.

[39] 클라이언트(110)는 식별자 및 보안키를 저장한다(116). 클라이언트(110)는 식별자 및 보안키를 포함하는 인증 요청을 서버(120)로 전송할 수 있다(116). 인증 요청은 개인키를 이용하여 암호화될 수 있다.

[40] 서버(120)는 클라이언트(110)로부터 수신된 식별자 및 보안키를 확인할 수 있다. 보다 구체적으로, 서버(120)는 클라이언트(110)로부터 수신된 식별자 및 보안키가 단계(125)에서 생성된 식별자 및 보안키와 동일한지 여부를 확인할 수 있다.

[41] 서버(120)는 클라이언트(110)로부터 수신된 식별자 및 보안키를 기초로 클라이언트(110)를 인증하고(128), 인증 결과를 클라이언트(110)로 전송한다(129). 인증 결과는 개인키를 이용하여 암호화될 수 있다.

[42] 클라이언트(110)는 인증 결과에 따라 다른 클라이언트와 통신 가능한 상태로 천이할 수 있다. 서버는 다른 클라이언트를 인증할 수 있고, 다른 클라이언트는 통신 가능한 상태로 천이할 수 있다. 이로 인해, 클라이언트(110)에서 구동되는 통신 소프트웨어에는 다른 클라이언트의 목록이 표시될 수 있다.
클라이언트(110)와 다른 클라이언트는 피투피 통신 또는 다이렉트 통신이 가능한 동작 모드로 진입할 수 있다. 클라이언트(110)가 다른 클라이언트와 피투피 통신하는 경우, 클라이언트(110)는 보안키를 이용하여 패킷을 암호화할 수 있고, 암호화된 패킷을 다른 클라이언트에게 전송할 수 있다.

[43] <보안 통신 플랫폼(Secure Communication Platform(SCP) 상에서 클라이언트 간의 페어링>

[44] 도 2는 일실시예에 따른 IoT 디바이스의 클라이언트의 페어링(paring) 동작 방법을 설명하기 위한 흐름도이다.

[45] 도 2를 참조하면, 클라이언트(210)는 서버(220)로 인증 요청을 전송한다.

[46] 서버(220)는 클라이언트(210)를 인증한다(221). 서버(220)는 위에서 설명한 인증 방법으로 클라이언트(210)를 인증할 수 있다. 인증 결과는 개인키를 이용하여 암호화된다. 서버(220)는 인증 결과를 클라이언트(210)에게 전송한다(222).

[47] 클라이언트(210)는 개인키를 이용하여 인증 결과를 복호화한다. 클라이언트(210)가 인증된 경우, 클라이언트(210)는 통신 가능한 상태로 천이된다(212). 클라이언트(210)는 피투피 통신 가능한 상태로 천이될 수 있다.

[48] 클라이언트(210)는 서버(220)로 클라이언트(230)와의 페이링 요청을 생성하여(213), 서버(220)로 페어링 요청을 전송한다(214).

[49] 서버(220)는 클라이언트(210, 230) 간 연결 고유키를 생성한다(223).

[50] 서버(220)는 클라이언트(210)이 페이링을 요청한 클라이언트(230)로 웨이크업 신호를 전송한다(224).

[51] 클라이언트(230)는 서버(220)로부터 전송된 웨이크업 신호에 대응하여 통신 가능 상태로 천이한다(231). 클라이언트(230)는 도 1에 도시된 방법에 따라 보안 통신 플랫폼에서 피투피 통신을 할 수 있는 보안키 및 식별자를 미리 부여 받은 것이다.

[52] 클라이언트(230)는 서버(220)로 인증 요청을 전송한다(232).

[53] 서버(220)는 클라이언트(230)를 인증하고(225), 인증 결과를 클라이언트(230)로 전송한다(226).

[54] 서버(220)는 클라이언트(210)로 공유키를 전송한다(227).

[55] 서버(220)는 클라이언트(230)로 공유키를 전송한다(228).

[56] 클라이언트(210)는 서버(220)로부터 전송된 공유키를 저장하고(214), 클라이언트(230)로 전송하고자 하는 데이터를 서버(220)로 전송한다(215). 상기 데이터는 공유키로 암호화된 것일 수 있다.

[57] 클라이언트(230)는 서버(220)로부터 전송된 공유키를 저장하고(233), 서버(220)로부터 클라이언트(210)가 전송한 데이터를 수신한다(229).

[58] 클라이언트(230)는 데이터를 해석한다(234). 클라이언트(230)는 상기 데이터를 공유키로 복호화할 수 있다.

[59] 위 도 2는 클라이언트(210에서 클라이언트(230)으로의 데이터 전송의 일례를 도시하고 있으나, 클라이언트(230)에서 클라이언트(210)로의 데이터 전송도 동일한 방식으로 수행될 수 있다. 도 2에 도시된 클라이언트(210)는 IoT 센서, 클라이언트(230)은 IoT 센서에서 수집된 센싱 데이터를 수집하는 수집기일 수 있다. 이하 도 3을 참조하여, 일실시예에 따른 IoT 디바이스 및 IoT 센서와 수집기의 일례를 상세히 설명한다.

[60] <u><네트워크 기반의 IoT 디바이스의 통신></u>

[61] 일실시예에 따른 네트워크 기반의 IoT 디바이스들은 도 1 및 도 2에서 설명한 보안 통신 플랫폼에서 동작한다.

[62] 도 3은 일실시예에 따른 IoT 디바이스의 구조를 도시한 도면이다. IoT 디바이스는 아래의 구성 파트들을 포함할 수 있고, 보안 통신 플랫폼에서 피투피 통신이 가능하도록 하는 클라이언트는 IoT 디바이스의 메모리에 설치될 수 있다. IoT 다비아스는 온도/빛/압력/습도 등 다양한 물리량을 센싱하는 센서부(도시되지 않음)를 더 포함할 수 있다.

[63] 도 3을 참조하면, 일실시예에 따른 IoT 디바이스(300)는 전원부(301), 메모리(302), 중앙처리장치(303), 및 통신 인터페이스(304)을 포함한다.

[64] 전원부(301)는 배터리 형식의 전원일 수 있고, 최대 5초 정도 IoT 디바이스를 구동할 수 있는 전력을 저장할 수 있도록 하는 캐패시턴스(capacitance)를 포함하는 축전부일 수 있다.

[65] 메모리(302)는 도 1 및 도 2를 참조하여 설명한 피투피 통신을 위한 클라이언트가 설치되는 ROM 또는 RAM과, IoT 디바이스의 고유키 또는 IoT 디바이스의 데이터를 암호화하여 저장하거나, 공개키/개인키를 저장하는 EEPROM을 포함할 수 있다. 클라이언트에 포함되는 통신 소프트웨어는 아래의 동작을 수행할 수 있다.

[66] (1) 서버로부터 공개키 요청에 대응하는 공개키를 통신 인터페이스를 통해 수신하고, 개인키를 생성한다.

[67] (2) 통신 소프트웨어는 개인키를 통신 인터페이스를 통해 서버로 전송하고, 서버로부터 공개키 및 개인키에 대한 키-페어 생성 메시지를 통신 인터페이스를 통해 수신한다.

[68] (3) 통신 소프트웨어는 서버로 클라이언트의 하나 이상의 고유 정보를 포함하는 식별자 생성 요청을 통신 인터페이스를 통해 전송한다.

[69] (4) 통신 소프트웨어는 서버로부터 식별자 생성 요청에 대응하는 식별자 및 고유 정보에 대응하는 보안키를 통신 인터페이스를 통해 수신한다.

[70] (5) 통신 소프트웨어는 서버로 식별자 및 보안키를 포함하는 인증 요청을 통신 인터페이스를 통해 전송한다.

[71] (6) 통신 소프트웨어는 서버로부터 인증 요청에 대응하는 인증 결과를 통신 인터페이스를 통해 수신한다.

[72] (7) 통신 소프트웨어는 인증 결과에 따라 클라이언트가 다른 클라이언트와 통신 가능한 상태로 천이하도록 클라이언트를 제어한다. 이로 인해, 클라이언트는 서버에 의해 인증된 다른 클라이언트와 피투피 통신 또는 직접 통신이 가능한 동작 모드로 진입할 수 있다.

[73] 위의 방식으로 보안 통신 플랫폼 상에서 인증된 다수의 IoT 디바이스들은 도 2에 도시된 방식으로 다른 IoT 디바이스들과 페어링될 수 있고, 서로의 데이터를 송수신할 수 있다.

[74] 중앙처리장치(303)는 메모리(302)에 기록된 IoT 디바이스의 펌웨어(Firmware) 및 기타 소프트웨어는 물론, 클라이언트의 실행 및 동작을 제어한다.

[75] 통신 인터페이스(304)는 IoT 디바이스(300)이 보안 통신 플랫폼 상에서 피투피

통신할 수 있도록 한다. 통신 인터페이스(304)는 WWAN(Wireless Wide Area Network) 또는 WLAN(Wireless Local Area Network)을 위한 인터페이스를 포함할 수 있다. WWAN은 CDMA(Code Division Multiple Access) 네트워크 TDMA(Time Division Multiple Access) 네트워크, FDMA(Frequency Division Multiple Access) 네트워크, OFDMA(Orthogonal Frequency Division Multiple Access) 네트워크, 및/또는 SC-FDMA(Single-Carrier Frequency Division Multiple Access) 네트워크 중 어느 하나 또는 이들의 조합을 포함할 수 있다. WLAN은 IEEE 802.11x 네트워크를 포함할 수 있다. 또한, 통신 인터페이스(304)는 블루투스(Bluetooth), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra-Wideband), ZigBee, NFC(Near Field Communication), 또는 Z-wave 등이 가능한 인터페이스를 포함할 수 있다.

[76] IoT 디바이스(300)에 센서부가 더 포함되는 경우, IoT 디바이스(300)는 센싱 데이터의 수집을 담당하는 수집기(도시되지 않음)와 페어링하여 도 1 및 도 2를 참조하여 설명한 피투피 통신을 통해 수집기로 센싱 데이터를 전송할 수 있다. 이 경우, 수집기는 IoT 디바이스(300)의 전원부(301)로 구동 전력을 전송하도록 구현될 수 있다.

[77] 다른 일실시예에 따른 보안 통신 플랫폼에서 동작하는 IoT 디바이스(300)는 아래와 같이 동작할 수 있다.

[78] (1) IoT 디바이스(300)는 도 1에서 설명한 공개키는 부여 받았지만 개인키는 저장하고 있지 않을 수 있다. 상기 공개키는 IoT 디바이스(300)의 제조 과정에서 미리 부여된 것일 수 있다.

[79] (2) 개인키는 보안 통신 플랫폼 또는 수집기와의 최초 접속 이후, 보안 통신 플랫폼의 서버 또는 수집기와 개인키 교환을 진행하여 부여 받을 수 있다. 부여 받은 개인키는 IoT 디바이스(300)의 메모리(302)에 포함된 EEPROM 내의 OTP(One Time Programmable) 영역에 저장될 수 있다.

[80] (3) 보안 통신 플랫폼의 서버 또는 수집기와 개인키를 교환한 이후, IoT 디바이스(300) 내의 모든 데이터는 공개키 또는/및 개인키로 암호화 되어 저장될 수 있다. 이러한 암호화 과정을 통해 데이터의 무결성(integrity) 및 보안성이 향상될 수 있다.

[81] (4) IoT 디바이스(300)에 센서가 포함되는 경우, IoT 디바이스(300)는 수집기와 지속적으로 통신을 하는 과정에서, RF를 활용하여 수집기로부터 passive RFID 방식으로 전원을 공급 받을 수 있다. IoT 디바이스(300)는 센서에서 센싱한 센싱 데이터를 메모리(302)의 EEPROM에 저장할 수 있다. IoT 디바이스(300)는 수집기로부터 센싱 데이터 요청을 수신하는 경우, EEPROM에 저장된 센싱 데이터를 개인키로 암호화하고, 다시 공개키로 암호화하여, RFID 고유키값과 함께 수집기로 센싱 데이터를 전송할 수 있다. 수집기는 공개키로 암호화된 센싱 데이터를 1차 복호화하고, 다시 RFID 고유키값으로 개인키를 찾아 센싱 데이터를 2차 복호화할 수 있다. 수집기는 RFID 고유키값 별 센싱 데이터를 저장

수단에 저장할 수 있다.

[82] (5) 수집기는 주기적으로 보안 통신 플랫폼으로부터 받은 공개키와 개인키를 활용하여 암호화된 센싱 데이터를 보안 통신 플랫폼으로 전송한다. 사용자는 수집기를 보안 통신 플랫폼에 접속시켜 등록을 해야 하고, 수집기가 보안 통신 플랫폼 상에 등록되면, 보안 통신 플랫폼의 서버는 해당 수집기로 RFID 고유키값을 발급한다. 사용자는 수집기에 발급된 RFID 고유키값을 활용하여 수집기로부터 전송된 센싱 데이터를 열람할 수 있다.

[83] (6) 센싱 데이터의 보안을 위해, SSL 3.0 / TLS 1.0+ 또는 AES128 / AES256 등의 암호화 기법이 이용될 수 있다.

[84] 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.

[85] 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 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 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.

[86] 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[87] 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.

[88] 그러므로, 다른 구현들, 다른 실시예들 및 청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

청구범위

[청구항 1] 피어투피어 통신을 이용한 IoT 디바이스의 클라이언트의 동작 방법에 있어서,
메모리에 저장된 공개키를 기초로 개인키를 생성하는 단계;
상기 개인키를 서버로 전송하고, 상기 서버로부터 공개키 및 개인키에 대한 키-페어 생성 메시지를 수신하는 단계;
상기 서버로 하나 이상의 고유 정보를 포함하는 식별자 생성 요청을 전송하는 단계;
상기 서버로부터 상기 식별자 생성 요청에 대응하는 식별자 및 고유 정보에 대응하는 보안키를 수신하는 단계; 및
상기 서버로 상기 식별자 및 상기 보안키를 포함하는 인증 요청을 전송하고, 상기 서버로부터 상기 인증 요청에 대응하는 인증 결과를 수신하는 단계;
상기 인증 결과에 대응하여, 상기 클라이언트가 통신 가능한 상태로 천이하는 단계; 및
상대 클라이언트와의 페이링 요청에 따라 상기 서버로부터 전송된 공유키를 이용하여 데이터를 서버를 통해 상기 상대 클라이언트로 전송하는 단계
를 포함하는,
IoT 디바이스의 클라이언트의 동작 방법.

[청구항 2] 제1항에 있어서,
상기 하나 이상의 고유 정보는,
상기 IoT 디바이스의 장치 고유키 및 상기 클라이언트에서 구동되는 통신 소프트웨어에 대응하는 제조키를 포함하는,
IoT 디바이스의 클라이언트의 동작 방법.

[청구항 3] 제1항에 있어서,
상기 개인키는 상기 메모리의 미리 정해진 영역에 저장되는,
IoT 디바이스의 클라이언트의 동작 방법.

[청구항 4] 제1항에 있어서,
상기 IoT 디바이스는 센서부를 포함하고,
상기 상대 클라이언트는 수집기인,
IoT 디바이스의 클라이언트의 동작 방법.

[청구항 5] 제1항에 있어서,
상기 데이터는 상기 공유키로 암호화되는,
IoT 디바이스의 클라이언트의 동작 방법.

[청구항 6] 제4항에 있어서,
상기 IoT 디바이스는 상기 수집기로부터 전력을 공급받는.

IoT 디바이스의 클라이언트의 동작 방법.

[청구항 7] 피어투피어 통신을 이용한 IoT 디바이스에 있어서,
피어투피어 통신을 위한 통신 인터페이스;
피어투피어 통신을 수행하는 클라이언트가 저장된 메모리; 및
상기 클라이언트의 실행을 제어하는 중앙처리장치
를 포함하고,
상기 클라이언트는,
상기 메모리에 저장된 공개키를 기초로 개인키를 생성하는 단계;
상기 개인키를 서버로 전송하고, 상기 서버로부터 공개키 및
개인키에 대한 키-페어 생성 메시지를 수신하는 단계;
상기 서버로 하나 이상의 고유 정보를 포함하는 식별자 생성
요청을 전송하는 단계;
상기 서버로부터 상기 식별자 생성 요청에 대응하는 식별자 및
고유 정보에 대응하는 보안키를 수신하는 단계; 및
상기 서버로 상기 식별자 및 상기 보안키를 포함하는 인증 요청을
전송하고, 상기 서버로부터 상기 인증 요청에 대응하는 인증
결과를 수신하는 단계;
상기 인증 결과에 대응하여, 상기 클라이언트가 통신 가능한
상태로 천이하는 단계; 및
상대 클라이언트와의 페이링 요청에 따라 상기 서버로부터 전송된
공유키를 이용하여 데이터를 서버를 통해 상기 상대 클라이언트로
전송하는 단계
를 수행하는,
IoT 디바이스.

[청구항 8] 제7항에 있어서,
상기 개인키는 상기 메모리의 미리 정해진 영역에 저장되는,
IoT 디바이스.

[청구항 9] 제7항에 있어서,
상기 IoT 디바이스는 센서부를 포함하고,
상기 상대 클라이언트는 수집기인,
IoT 디바이스.

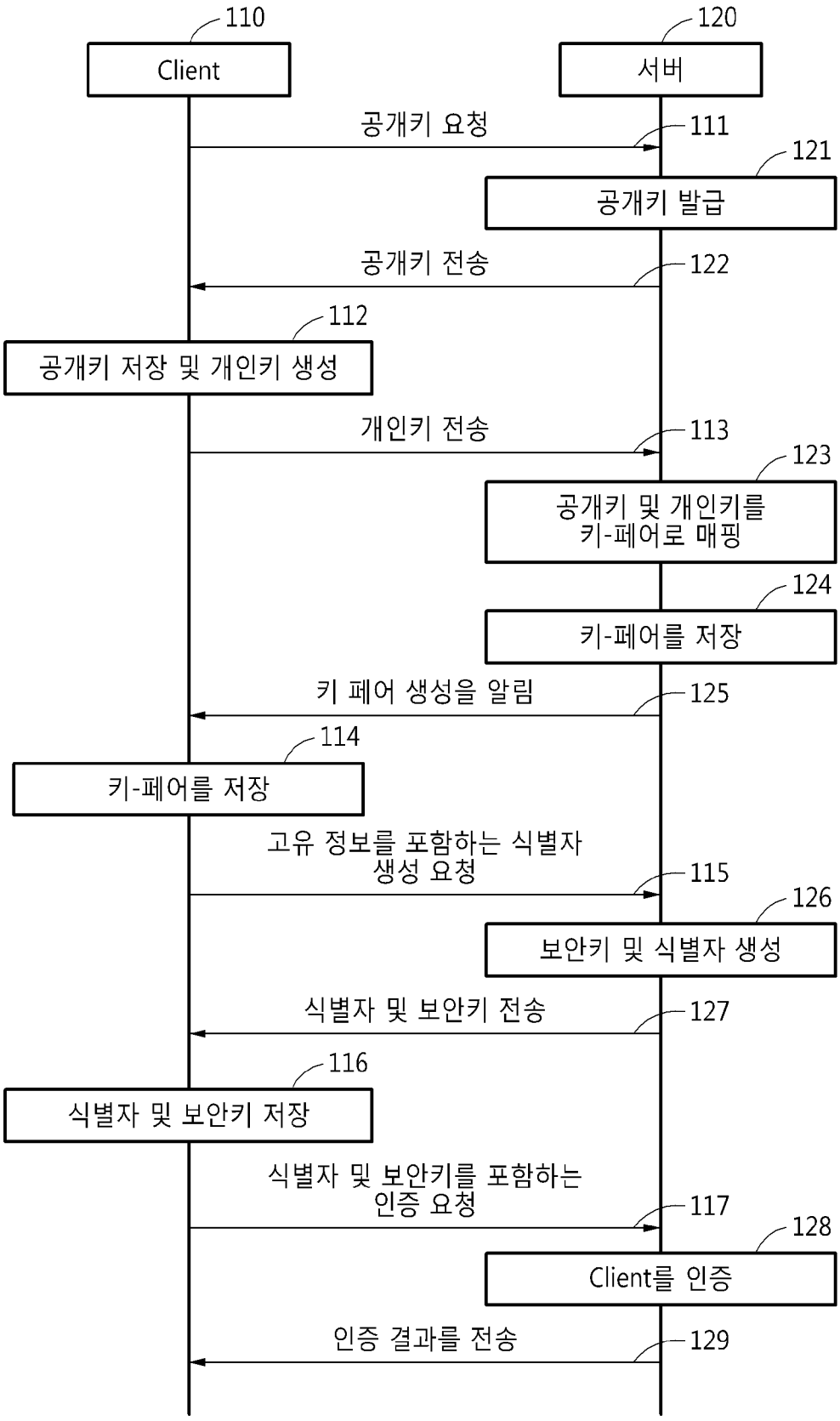
[청구항 10] 제7항에 있어서,
상기 데이터는 상기 공유키로 암호화되는,
IoT 디바이스.

[청구항 11] 제9항에 있어서,
전원부
를 더 포함하고,
상기 전원부는 상기 수집기로부터 전력을 공급받는.

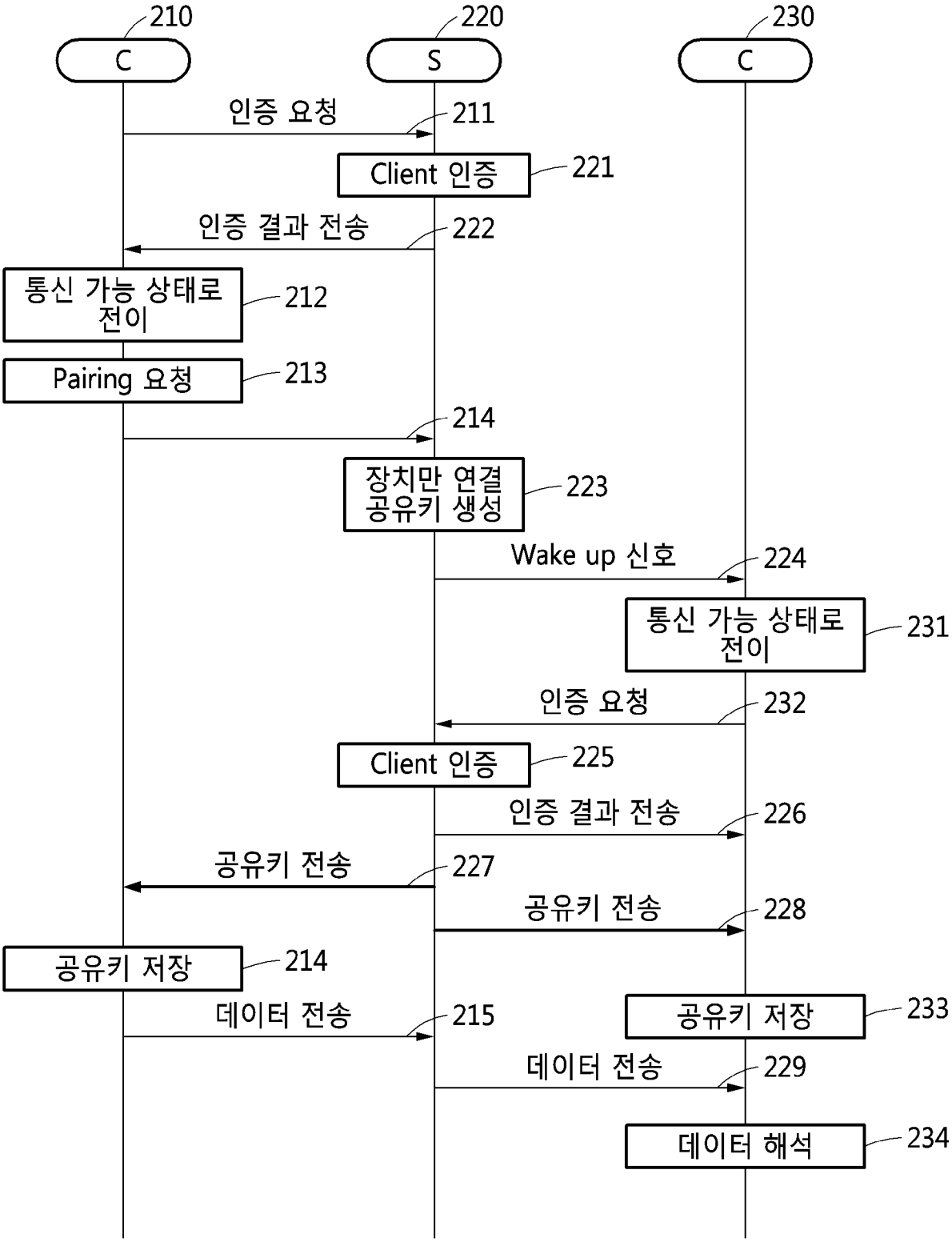
IoT 디바이스.

WO 2017/014614 PCT/KR2016/008115

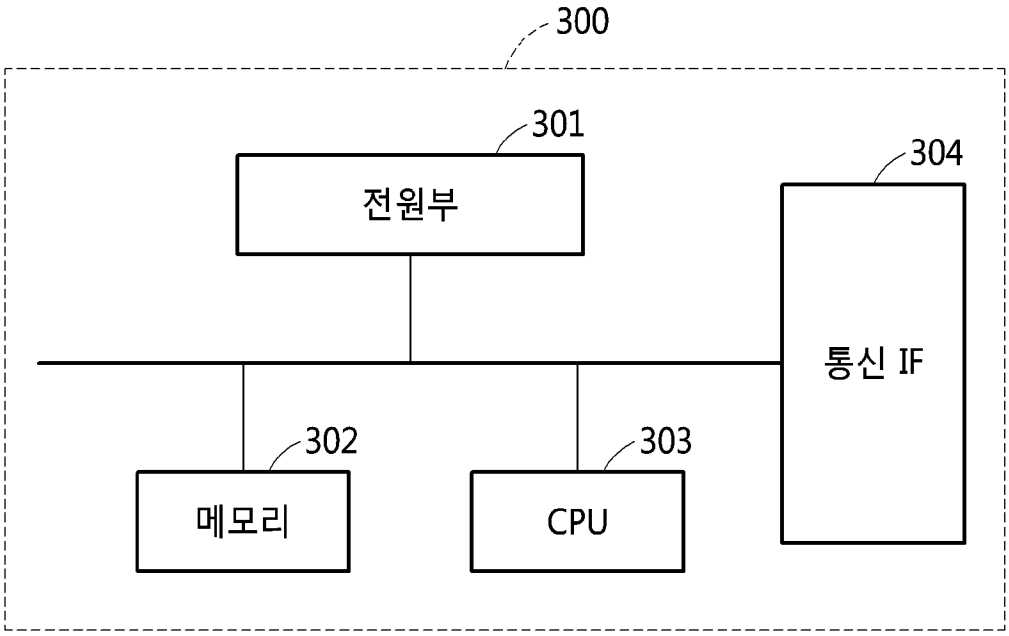
[Fig. 1]



[Fig. 2]


210
C
220
S
230
C
인증 요청
211
Client 인증
221
인증 결과 전송
222
통신 가능 상태로 전이
212
Pairing 요청
213
214
장치만 연결 공유키 생성
223
Wake up 신호
224
통신 가능 상태로 전이
231
인증 요청
232
Client 인증
225
인증 결과 전송
226
공유키 전송
227
공유키 전송
228
공유키 저장
214
데이터 전송
215
공유키 저장
233
데이터 전송
229
데이터 해석
234

[Fig. 3]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/008115

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, H04L 29/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/06; H04L 9/14; H04L 9/08; H04W 88/16; H04L 9/30; H04L 9/32; H04W 12/06; H04L 9/00; H04L 29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: personal key, public key, server, pairing, identifying, identifier, pair, shared key, IoT device

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2014-0055509 A (SAMSUNG SDS CO., LTD. et al.) 09 May 2014 See paragraphs [0004]-[0007], [0015]-[0016]; and figure 1.	1-11
Y	KR 10-2014-0054970 A (BELLEPHOS CO., LTD.) 09 May 2014 See paragraphs [0011]-[0014], [0021]-[0023], [0034], [0038]-[0044]; and figure 3.	1-11
A	KR 10-2014-0045629 A (SAMSUNG SDS CO., LTD.) 17 April 2014 See paragraphs [0009]-[0010], [0031]-[0039]; and figure 3.	1-11
A	WO 2013-025060 A2 (ICTK CO., LTD.) 21 February 2013 See paragraphs [0021]-[0038]; and figure 8.	1-11
A	US 2012-0023336 A1 (NATARAJAN, Vijayarangan) 26 January 2012 See paragraphs [0031]-[0068]; and figure 1.	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 OCTOBER 2016 (12.10.2016)	**19 OCTOBER 2016 (19.10.2016)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/008115

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2014-0055509 A	09/05/2014	CN 103795533 A	14/05/2014
		KR 10-1493212 B1	23/02/2015
		US 2014-0192976 A1	10/07/2014
		US 9379891 B2	28/06/2016
		WO 2014-069778 A1	08/05/2014
KR 10-2014-0054970 A	09/05/2014	KR 10-1518489 B1	18/05/2015
KR 10-2014-0045629 A	17/04/2014	KR 10-1508360 B1	07/04/2015
		US 2014-0101444 A1	10/04/2014
		US 9137223 B2	15/09/2015
		WO 2014-058166 A1	17/04/2014
WO 2013-025060 A2	21/02/2013	CN 103748831 A	23/04/2014
		EP 2747335 A2	25/06/2014
		EP 2747335 A4	27/05/2015
		JP 2014-528195 A	23/10/2014
		KR 10-1372719 B1	19/03/2014
		KR 10-2013-0019358 A	26/02/2013
		KR 10-2013-0129334 A	28/11/2013
		TW 201342868 A	16/10/2013
		TW I479870 B	01/04/2015
		US 2014-0310515 A1	16/10/2014
		WO 2013-025060 A3	11/04/2013
US 2012-0023336 A1	26/01/2012	CN 102098157 A	15/06/2011
		CN 102098157 B	18/05/2016
		EP 2334008 A1	15/06/2011
		JP 2011-125020 A	23/06/2011
		JP 2016-036166 A	17/03/2016
		US 8670563 B2	11/03/2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/008115

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i, H04L 29/08(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; H04L 9/14; H04L 9/08; H04W 88/16; H04L 9/30; H04L 9/32; H04W 12/06; H04L 9/00; H04L 29/08

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 개인키, 공개키, 서버, 페어링, 인증, 식별자, 페어, 공유키, IoT 디바이스

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2014-0055509 A (삼성에스디에스 주식회사 등) 2014.05.09 단락 [0004]-[0007], [0015]-[0016]; 및 도면 1 참조.	1-11
Y	KR 10-2014-0054970 A (벨포스 주식회사) 2014.05.09 단락 [0011]-[0014], [0021]-[0023], [0034], [0038]-[0044]; 및 도면 3 참조.	1-11
A	KR 10-2014-0045629 A (삼성에스디에스 주식회사) 2014.04.17 단락 [0009]-[0010], [0031]-[0039]; 및 도면 3 참조.	1-11
A	WO 2013-025060 A2 ((주)아이씨티케이) 2013.02.21 단락 [0021]-[0038]; 및 도면 8 참조.	1-11
A	US 2012-0023336 A1 (VIJAYARANGAN NATARAJAN) 2012.01.26 단락 [0031]-[0068]; 및 도면 1 참조.	1-11

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2016년 10월 12일 (12.10.2016)	2016년 10월 19일 (19.10.2016)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
김성우
전화번호 +82-42-481-3348

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/008115

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2014-0055509 A	2014/05/09	CN 103795533 A	2014/05/14
		KR 10-1493212 B1	2015/02/23
		US 2014-0192976 A1	2014/07/10
		US 9379891 B2	2016/06/28
		WO 2014-069778 A1	2014/05/08
KR 10-2014-0054970 A	2014/05/09	KR 10-1518489 B1	2015/05/18
KR 10-2014-0045629 A	2014/04/17	KR 10-1508360 B1	2015/04/07
		US 2014-0101444 A1	2014/04/10
		US 9137223 B2	2015/09/15
		WO 2014-058166 A1	2014/04/17
WO 2013-025060 A2	2013/02/21	CN 103748831 A	2014/04/23
		EP 2747335 A2	2014/06/25
		EP 2747335 A4	2015/05/27
		JP 2014-528195 A	2014/10/23
		KR 10-1372719 B1	2014/03/19
		KR 10-2013-0019358 A	2013/02/26
		KR 10-2013-0129334 A	2013/11/28
		TW 201342868 A	2013/10/16
		TW I479870 B	2015/04/01
		US 2014-0310515 A1	2014/10/16
		WO 2013-025060 A3	2013/04/11
US 2012-0023336 A1	2012/01/26	CN 102098157 A	2011/06/15
		CN 102098157 B	2016/05/18
		EP 2334008 A1	2011/06/15
		JP 2011-125020 A	2011/06/23
		JP 2016-036166 A	2016/03/17
		US 8670563 B2	2014/03/11