



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0102065
(43) 공개일자 2021년08월19일

- (51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) H04W 4/70 (2018.01)
H04W 80/12 (2019.01)
(52) CPC특허분류
H04L 67/12 (2013.01)
H04L 67/306 (2013.01)
(21) 출원번호 10-2021-0009124
(22) 출원일자 2021년01월22일
심사청구일자 없음
(30) 우선권주장
62/972,723 2020년02월11일 미국(US)
63/084,130 2020년09월28일 미국(US)

- (71) 출원인
현대자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
기아 주식회사
서울특별시 서초구 헌릉로 12 (양재동)
(72) 발명자
송재승
서울특별시 광진구 능동로 209
(74) 대리인
성병기

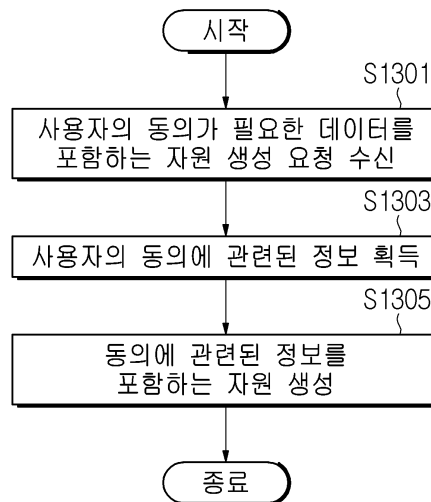
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 M2M 시스템에서 개인 데이터를 취급하기 위한 방법 및 장치

(57) 요약

본 발명은 M2M(Machine-to-Machine) 시스템에서 개인 데이터(personal data)를 취급하기 위한 방법 및 장치에 대한 것으로, M2M 장치의 동작 방법은, IoT(Internet of things) 장치로부터 제공되는 개인 데이터(personal data)에 대한 사용자의 동의에 관련된 정보를 획득하는 단계, 상기 정보에 기반하여 동의에 관련된 자원을 생성하는 단계를 포함한다. 상기 자원은, 상기 동의에 관련된 적어도 하나의 어트리뷰트를 포함한다.

대표도 - 도13



(52) CPC특허분류

H04L 67/32 (2013.01)

H04W 4/70 (2018.02)

H04W 80/12 (2019.01)

명세서

청구범위

청구항 1

M2M(Machine-to-Machine) 시스템에서 M2M 장치의 동작 방법에 있어서,
IoT(Internet of things) 장치로부터 제공되는 개인 데이터(personal data)에 대한 사용자의 동의에 관련된 정보를 획득하는 단계; 및
상기 정보에 기반하여 동의에 관련된 자원을 생성하는 단계를 포함하며,
상기 자원은, 상기 동의에 관련된 적어도 하나의 어트리뷰트를 포함하는 방법.

청구항 2

제1항에 있어서,
상기 정보는, 상기 IoT 장치를 위한 등록 절차를 통해 상기 M2M 장치에게 수신되는 방법.

청구항 3

제1항에 있어서,
상기 정보는, 상기 IoT 장치를 위한 등록 절차 후, 상기 사용자의 장치로부터 상기 M2M 장치에게 수신되는 방법.

청구항 4

제1항에 있어서,
상기 정보는, 상기 IoT 장치를 위한 등록 절차 중 상기 M2M 장치에게 수신되는 방법.

청구항 5

제1항에 있어서,
상기 동의에 관련된 자원은, 동의 관리 전용 자원을 포함하며,
상기 동의 관리 전용 자원은, 상기 개인 데이터를 포함하는 자원에 의해 참조되는 방법.

청구항 6

제1항에 있어서,
상기 동의에 관련된 자원은, 동의 관리 전용 자원을 포함하며,
상기 동의 관리 전용 자원은, 동의의 소유자(Owner of the consent), 동의가 생성된 시기(When this consent is created), 동의의 이름(Name of consent), 허용되는 처리의 종류(What kinds of processing is allowed), 동의의 유효성(Validity of the consent), 동의의 식별자(Identifier of the consent), 동의의 만료시점(Expiration of the consent), 소유자가 언제든 동의를 철회할 권리를 가지는지 여부(whether the owner has a right to withdraw the consent at anytime) 중 적어도 하나의 어트리뷰트를 포함하는 방법.

청구항 7

제1항에 있어서,

상기 동의에 관련된 자원은, 상기 동의에 관련된 ACP(access control policy)를 정의하기 위한 적어도 하나의 어트리뷰트를 포함하는 ACP 자원을 포함하며,

상기 ACP 자원은, 상기 개인 데이터를 포함하는 자원에 의해 참조되는 방법.

청구항 8

제1항에 있어서,

상기 동의에 관련된 자원은, 상기 동의에 관련된 ACP(access control policy)를 정의하기 위한 적어도 하나의 어트리뷰트를 포함하는 ACP 자원을 포함하며,

상기 ACP 자원은, 상기 ACP 자원을 참조하는 자원에 적용되는 ACP, ACP 자원 자체에 적용되는 ACP, 상기 ACP 자원을 참조하는 자원에 적용되는 동의 관리 규칙 중 적어도 하나의 어트리뷰트를 포함하는 방법.

청구항 9

M2M(Machine-to-Machine) 시스템에서 M2M 장치에 있어서,

신호를 송수신하는 송수신부; 및

상기 송수신부를 제어하는 프로세서를 포함하며,

상기 프로세서는,

IoT(Internet of things) 장치로부터 제공되는 개인 데이터(personal data)에 대한 사용자의 동의에 관련된 정보를 획득하고,

상기 정보에 기반하여 동의에 관련된 자원을 생성하며,

상기 자원은, 상기 동의에 관련된 적어도 하나의 어트리뷰트를 포함하는 M2M 장치.

청구항 10

제9항에 있어서,

상기 정보는, 상기 IoT 장치를 위한 등록 절차를 통해 상기 M2M 장치에게 수신되는 M2M 장치.

청구항 11

제9항에 있어서,

상기 정보는, 상기 IoT 장치를 위한 등록 절차 후, 상기 사용자의 장치로부터 상기 M2M 장치에게 수신되는 M2M 장치.

청구항 12

제9항에 있어서,

상기 정보는, 상기 IoT 장치를 위한 등록 절차 중 상기 M2M 장치에게 수신되는 M2M 장치.

청구항 13

제9항에 있어서,

상기 동의에 관련된 자원은, 동의 관리 전용 자원을 포함하며,

상기 동의 관리 전용 자원은, 상기 개인 데이터를 포함하는 자원에 의해 참조되며,

상기 동의 관리 전용 자원은, 동의의 소유자(Owner of the consent), 동의가 생성된 시기(When this consent is created), 동의의 이름(Name of consent), 허용되는 처리의 종류(What kinds of processing is allowed), 동의의 유효성(Validity of the consent), 동의의 식별자(Identifier of the consent), 동의의 만료시점(Expiration of the consent), 소유자가 언제든지 동의를 철회할 권리를 가지는지 여부(whether the owner has a right to withdraw the consent at anytime) 중 적어도 하나의 어트리뷰트를 포함하는 M2M 장치.

청구항 14

제9항에 있어서,

상기 동의에 관련된 자원은, 상기 동의에 관련된 ACP(access control policy)를 정의하기 위한 적어도 하나의 어트리뷰트를 포함하는 ACP 자원을 포함하며,

상기 ACP 자원은, 상기 개인 데이터를 포함하는 자원에 의해 참조되는 M2M 장치.

청구항 15

제9항에 있어서,

상기 동의에 관련된 자원은, 상기 동의에 관련된 ACP(access control policy)를 정의하기 위한 적어도 하나의 어트리뷰트를 포함하는 ACP 자원을 포함하며,

상기 ACP 자원은, 상기 ACP 자원을 참조하는 자원에 적용되는 ACP, ACP 자원 자체에 적용되는 ACP, 상기 ACP 자원을 참조하는 자원에 적용되는 동의 관리 규칙 중 적어도 하나의 어트리뷰트를 포함하는 M2M 장치.

발명의 설명

기술 분야

[0001] 본 발명은 M2M(Machine-to-Machine) 시스템에서 개인 데이터(personal data)를 취급하기 위한 방법 및 장치에 대한 것이다. 보다 구체적으로, 본 발명은 M2M 시스템에서 개인 데이터의 취급에 대한 동의(consent)를 확인하기 위한 방법 및 장치에 대한 것이다.

배경 기술

[0002] 최근 M2M(Machine-to-Machine) 시스템에 대한 도입이 활발해지고 있다. M2M 통신은 사람의 개입 없이 기계(machine)와 기계 사이에 수행되는 통신을 의미할 수 있다. M2M은 MTC(Machine Type Communication), IoT(Internet of Things) 또는 D2D(Device-to-Device)를 지칭할 수 있다. 다만, 하기에서는 설명의 편의를 위해 M2M로 통일하게 지칭하지만, 이에 한정되지 않는다. M2M 통신에 사용되는 단말은 M2M 단말(M2M device)일 수 있다. M2M 단말은 일반적으로 적은 데이터를 전송하면서 낮은 이동성을 갖는 디바이스일 수 있다. 이때, M2M 단말은 기계 간 통신 정보를 중앙에서 저장하고 관리하는 M2M 서버와 연결되어 사용될 수 있다. 또한, M2M 단말은 사물 추적, 자동차 연동, 전력 계량 등과 같이 다양한 시스템에서 적용될 수 있다.

[0003] 한편, M2M 단말과 관련하여, oneM2M 표준화 기구는 M2M 통신, 사물통신, IoT 기술을 위한 요구사항, 아키텍처, API(Application Program Interface) 사양, 보안 솔루션, 상호 운용성에 대한 기술을 제공하고 있다. oneM2M

표준화 기구의 사양은 스마트 시티, 스마트 그리드, 커넥티드 카, 홈 오토메이션, 치안, 건강과 같은 다양한 어플리케이션과 서비스를 지원하는 프레임워크를 제공하고 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 M2M(Machine-to-Machine) 시스템에서 개인 데이터(personal data)를 안전하게 취급하기 위한 방법 및 장치를 제공하는데 목적이 있다.

[0005] 본 발명은 M2M 시스템에서 개인 데이터의 사용에 대한 사용자의 동의(consent)를 효과적으로 확인하기 위한 방법 및 장치를 제공하는데 목적이 있다.

과제의 해결 수단

[0006] 본 발명의 일 실시 예에 따르면, M2M(Machine-to-Machine) 시스템에서 M2M 장치의 동작 방법은, IoT(Internet of things) 장치로부터 제공되는 개인 데이터(personal data)에 대한 사용자의 동의에 관련된 정보를 획득하는 단계, 상기 정보에 기반하여 동의에 관련된 자원을 생성하는 단계를 포함한다. 상기 자원은, 상기 동의에 관련된 적어도 하나의 어트리뷰트를 포함한다.

[0007] 본 발명의 일 실시 예에 따르면, M2M(Machine-to-Machine) 시스템에서 M2M 장치는, 신호를 송수신하는 송수신부, 및 상기 송수신부를 제어하는 프로세서를 포함한다. 상기 프로세서는, IoT(Internet of things) 장치로부터 제공되는 개인 데이터(personal data)에 대한 사용자의 동의에 관련된 정보를 획득하고, 상기 정보에 기반하여 동의에 관련된 자원을 생성한다. 상기 자원은, 상기 동의에 관련된 적어도 하나의 어트리뷰트를 포함한다.

발명의 효과

[0008] 본 개시에 따르면, M2M(Machine-to-Machine) 시스템에서 개인 데이터(personal data)가 안전하게 처리될 수 있다.

[0009] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0010] 도 1은 본 개시에 따른 M2M(Machine-to-Machine) 시스템의 계층 구조를 나타낸 도면이다.

도 2는 본 개시에 따른 M2M 시스템에서 기준점(reference point)을 나타낸 도면이다.

도 3은 본 개시에 따른 M2M 시스템에서 각각의 노드를 나타낸 도면이다.

도 4는 본 개시에 따른 M2M 시스템에서 공통 서비스 평선을 나타낸 도면이다.

도 5는 본 개시에 따른 M2M 시스템에서 송신자 및 수신자가 메시지를 교환하는 방법을 나타낸 도면이다.

도 6a는 본 개시에 따른 M2M 시스템에서 사후 제공(post-provisioning) 방식에 따라 사용자의 동의를 획득하기 위한 절차의 예를 나타낸 도면이다.

도 6b는 본 개시에 따른 M2M 시스템에서 사전 제공(pre-provisioning) 방식에 따라 사용자의 동의를 획득하기 위한 절차의 예를 나타낸 도면이다.

도 6c는 본 개시에 따른 M2M 시스템에서 상호작용 제공(interactive-provisioning) 방식에 따라 사용자의 동의를 획득하기 위한 절차의 예를 나타낸 도면이다.

도 7은 본 개시에 따른 M2M 시스템에서 어트리뷰트-기반(attribute-based) 동의 관리의 개념을 나타낸 도면이다.

도 8은 본 개시에 따른 M2M 시스템에서 자원-기반(resource-based) 동의 관리의 개념을 나타낸 도면이다.

도 9a는 본 개시에 따른 M2M 시스템에서 ACP(access control policy) 기반 동의 관리를 위한 ACP 규칙의 구조

를 나타낸 도면이다.

도 9b는 본 개시에 따른 M2M 시스템에서 ACP 기반 동의 관리를 위한 ACP 규칙 및 동의 규칙의 구조를 나타낸 도면이다.

도 9c는 본 개시에 따른 M2M 시스템에서 ACP 기반 동의 관리의 개념을 나타낸 도면이다.

도 10은 본 개시에 따른 M2M 시스템에서 사후 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 보다 구체적인 예를 나타낸 도면이다.

도 11은 본 개시에 따른 M2M 시스템에서 상호작용 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 보다 구체적인 예를 나타낸 도면이다.

도 12는 본 개시에 따른 M2M 시스템에서 사전 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 보다 구체적인 예를 나타낸 도면이다.

도 13은 본 개시에 따른 M2M 시스템에서 사용자의 동의에 관련된 정보를 관리하기 위한 절차의 예를 나타낸 도면이다.

도 14는 본 개시에 따른 M2M 시스템에서 사용자의 동의에 관련된 정보를 제공하기 위한 절차의 예를 나타낸 도면이다.

도 15는 본 개시에 따른 M2M 시스템에서 M2M 장치의 구성을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0011] 이하에서는 첨부한 도면을 참고로 하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나, 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.
- [0012] 본 개시에 있어서, 제1, 제2 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용되며, 특별히 언급되지 않는 한 구성요소들간의 순서 또는 중요도 등을 한정하지 않는다. 따라서, 본 개시의 범위 내에서 일 실시 예에서의 제1 구성요소는 다른 실시 예에서 제2 구성요소라고 칭할 수도 있고, 마찬가지로 일 실시 예에서의 제2 구성요소를 다른 실시 예에서 제1 구성요소라고 칭할 수도 있다.
- [0013] 본 개시에 있어서, 어떤 구성요소가 다른 구성요소와 "연결", "결합" 또는 "접속"되어 있다고 할 때, 이는 직접적인 연결관계뿐만 아니라, 그 중간에 또 다른 구성요소가 존재하는 간접적인 연결관계도 포함할 수 있다. 또한 어떤 구성요소가 다른 구성요소를 "포함한다" 또는 "가진다"고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 배제하는 것이 아니라 또 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0014] 본 개시에 있어서, 서로 구별되는 구성요소들은 각각의 특징을 명확하게 설명하기 위함이며, 구성요소들이 반드시 분리되는 것을 의미하지는 않는다. 즉, 복수의 구성요소가 통합되어 하나의 하드웨어 또는 소프트웨어 단위로 이루어질 수도 있고, 하나의 구성요소가 분산되어 복수의 하드웨어 또는 소프트웨어 단위로 이루어질 수도 있다. 따라서, 별도로 언급하지 않더라도 이와 같이 통합된 또는 분산된 실시 예도 본 개시의 범위에 포함된다.
- [0015] 본 개시에 있어서, 다양한 실시 예에서 설명하는 구성요소들이 반드시 필수적인 구성요소들은 의미하는 것은 아니며, 일부는 선택적인 구성요소일 수 있다. 따라서, 일 실시 예에서 설명하는 구성요소들의 부분집합으로 구성되는 실시 예도 본 개시의 범위에 포함된다. 또한, 다양한 실시 예에서 설명하는 구성요소들에 추가적으로 다른 구성요소를 포함하는 실시 예도 본 개시의 범위에 포함된다.
- [0016] 본 개시의 실시 예를 설명함에 있어서 공지 구성 또는 기능에 대한 구체적인 설명이 본 개시의 요지를 흐릴 수 있다고 판단되는 경우에는 그에 대한 상세한 설명은 생략한다. 그리고, 도면에서 본 개시에 대한 설명과 관계없는 부분은 생략하였으며, 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0017] 또한 본 명세서는 M2M(Machine-to-Machine) 통신에 기초한 네트워크에 대해 설명하며, M2M 통신 네트워크에서 이루어지는 작업은 해당 통신 네트워크를 관할하는 시스템에서 네트워크를 제어하고 데이터를 송신하는 과정에서 이루어질 수 있다.
- [0018] 또한, 본 명세서에서 M2M 단말은 M2M 통신을 수행하는 단말일 수 있으나, 호환성(Backward Compatibility)을 고려하여 무선 통신 시스템에서 동작하는 단말일 수 있다. 즉, M2M 단말은 M2M 통신 네트워크에 기초하여 동작될

수 있는 단말을 의미할 수 있으나, M2M 통신 네트워크로 한정되는 것은 아니다. M2M 단말은 다른 무선 통신 네트워크에 기초하여 동작하는 것도 가능할 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0019] 또한, M2M 단말은 고정되거나 이동성을 가질 수 있다. 또한, M2M 서버는 M2M 통신을 위한 서버를 지칭하며 고정국(fixed station) 또는 이동국(mobile station)일 수 있다.

[0020] 또한, 본 명세서에서 엔티티는 M2M 디바이스, M2M 게이트웨이, M2M 서버와 같은 하드웨어를 지칭할 수 있다. 또한, 일 예로, 엔티티는 M2M 시스템의 계층 구조에서 소프트웨어적인 구성을 지칭하는데 사용할 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0021] 또한, 일 예로, 본 발명은 M2M 시스템을 중심으로 설명되지만 본 발명은 M2M 시스템에만 제한적으로 적용되는 것은 아니다.

[0022] 또한, M2M 서버는 M2M 단말 또는 다른 M2M 서버와 통신을 수행하는 서버일 수 있다. 또한, M2M 게이트웨이는 M2M 단말과 M2M 서버를 연결하는 연결점 역할을 수행할 수 있다. 일 예로, M2M 단말과 M2M 서버의 네트워크가 상이한 경우, M2M 게이트웨이를 통해 서로 연결될 수 있다. 이때, 일 예로, M2M 게이트웨이, M2M 서버 모두 M2M 단말일 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0024] 본 발명은 M2M(Machine-to-Machine) 시스템에서 개인 데이터(personal data)를 취급하기 위한 방법 및 장치에 대한 것이다. 보다 구체적으로, 본 발명은 M2M 시스템에서 개인 데이터의 취급에 대한 동의(consent)를 확인하기 위한 기술에 대해 설명한다.

[0026] oneM2M은 에너지, 교통, 국방, 공공서비스 등 산업별로 종속적이고 폐쇄적으로 운영되는, 파편화된 서비스 플랫폼 개발 구조를 벗어나 응용서비스 인프라(플랫폼) 환경을 통합하고 공유하기 위한 사물인터넷 공동서비스 플랫폼 개발을 위해 발족된 사실상 표준화 단체이다. oneM2M은 사물통신, IoT(Internet of Things) 기술을 위한 요구사항, 아키텍처, API(Application Program Interface) 사양, 보안 솔루션, 상호 운용성을 제공하고자 한다. 예를 들어, oneM2M의 사양은 스마트 시티, 스마트 그리드, 커넥티드 카, 홈 오토메이션, 치안, 건강과 같은 다양한 어플리케이션과 서비스를 지원하는 프레임워크를 제공한다. 이를 위해, oneM2M은 모든 어플리케이션들 사이에 데이터의 교환 및 공유를 위한 단일 수평 플랫폼을 정의하는 표준들의 집합을 개발해왔다. oneM2M에서 고려하는 어플리케이션들은 상이한 산업 부문들에 걸친 어플리케이션들도 포함할 수 있다. oneM2M은, 운영 체제처럼, 상이한 기술들과 연동하기 위한 프레임워크를 제공함으로써, 단일화를 촉진하는 분산된 소프트웨어 레이어를 생성하고 있다. 분산된 소프트웨어 레이어는 M2M 어플리케이션들과 데이터 전송을 제공하는 통신 HW(Hardware)/SW(Software) 사이에 위치하는 공통 서비스 계층에서 구현된다. 예를 들어, 공통 서비스 계층은 도 1과 같은 계층 구조의 일부를 차지할 수 있다.

[0028] 도 1은 본 개시에 따른 M2M(Machine-to-Machine) 시스템의 계층 구조(layered structure)를 나타낸 도면이다.

[0029] 도 1를 참조하면, M2M 시스템의 계층 구조는 어플리케이션 계층(110), 공통 서비스 계층(120), 네트워크 서비스 계층(130)으로 구성될 수 있다. 이때, 어플리케이션 계층(110)은 구체적인 어플리케이션에 기초하여 동작하는 계층일 수 있다. 일 예로, 어플리케이션은 차량 추적 어플리케이션(fleet tracking application), 원격거리 혈당 모니터링 어플리케이션(remote blood sugar monitoring application), 전력 계량 어플리케이션(power metering application) 또는 제어 어플리케이션(controlling application) 등일 수 있다. 즉, 어플리케이션 계층은 구체적인 어플리케이션에 대한 계층일 수 있다. 이때, 어플리케이션 계층에 기초하여 동작하는 엔티티는 어플리케이션 엔티티(Application Entity, AE)일 수 있다.

[0030] 공통 서비스 계층(120)은 공통 서비스 평면(Common Service Function, CSF)에 대한 계층일 수 있다. 일 예로, 공통 서비스 계층(120)은 데이터 관리(data management), 단말 관리(device management), M2M 서비스 구독 관리(M2M service subscription management), 위치 서비스(location Services) 등과 같이 공통 서비스 제공에 대한 계층일 수 있다. 일 예로, 공통 서비스 계층(120)에 기초하여 동작하는 엔티티는 공통 서비스 엔티티(Common Service Entity, CSE)일 수 있다.

[0031] 공통 서비스 계층(120)은 기능에 의해 CSF로 그룹화되는 서비스들의 집합을 제공할 수 있다. 다수의 인스턴스화

된 CSF들은 CSE들을 형성한다. CSE들은 어플리케이션들(예: oneM2M 명명법에서 어플리케이션 엔티티들 또는 AE 들), 다른 CSE들 및 기저 네트워크들(예: oneM2M 명명법에서 네트워크 서비스 엔티티 또는 NSE)과 인터페이스할 수 있다.

[0032] 네트워크 서비스 계층(120)은 장치 관리(device management), 위치 서비스(location service) 및 장치 트리거링(device triggering)과 같은 서비스들을 공통 서비스 계층(120)에 제공할 수 있다. 이때, 네트워크 계층(120)에 기초하여 동작하는 엔티티는 네트워크 서비스 엔티티(Network Service Entity, NSE)일 수 있다.

[0034] 도 2는 본 개시에 따른 M2M 시스템에서 기준점(reference point)을 나타낸 도면이다.

[0035] 도 2를 참조하면, M2M 시스템 구조는 필드 도메인(Field Domain) 및 인프라스트럭처 도메인(Infrastructure Domain)으로 구별될 수 있다. 이때, 각각의 도메인에서 각각의 엔티티들은 기준점(예: Mca 또는 Mcc)을 통해 통신을 수행할 수 있다. 일 예로, 기준점(reference point)은 각각의 엔티티들 간의 통신 흐름을 나타낼 수 있다. 이때, 도 2를 참조하면, AE(210 또는 240)와 CSE(220 또는 250) 사이의 기준점인 Mca 기준점, 서로 다른 CSE 사이의 기준점인 Mcc 기준점 및 CSE(220 또는 250)와 NSE(230 또는 260) 사이의 기준점인 Mcn 기준점이 설정될 수 있다.

[0037] 도 3은 본 개시에 따른 M2M 시스템에서 각각의 노드를 나타낸 도면이다.

[0038] 도 3을 참조하면, 특정 M2M 서비스 제공자의 인프라스트럭처 도메인은 특정 인프라스트럭처 노드(310, Infrastructure Node, IN)를 제공할 수 있다. 이때, IN의 CSE는 다른 인프라스트럭처 노드의 AE와 Mca 기준점에 기초하여 통신을 수행할 수 있다. 이때, 하나의 M2M 서비스 제공자마다 하나의 IN이 설정될 수 있다. 즉, IN은 인프라스트럭처 구조에 기초하여 다른 인프라스트럭처의 M2M 단말과 통신을 수행하는 노드일 수 있다. 또한, 일 예로, 노드의 개념은 논리적 엔티티일 수 있으며, 소프트웨어적인 구성일 수 있다.

[0039] 다음으로, 어플리케이션 지정 노드(320, Application Dedicated Node, ADN)는 적어도 하나의 AE를 포함하고, CSE를 포함하지 않는 노드일 수 있다. 이때, ADN은 필드 도메인에서 설정될 수 있다. 즉, ADN은 AE에 대한 전용 노드일 수 있다. 일 예로, ADN은 하드웨어적으로 M2M 단말에 설정되는 노드일 수 있다. 또한, 어플리케이션 서비스 노드(330, Application Service Node, ASN)는 하나의 CSE와 적어도 하나의 AE를 포함하는 노드일 수 있다. ASN은 필드 도메인에서 설정될 수 있다. 즉, AE 및 CSE를 포함하는 노드일 수 있다. 이때, ASN은 IN과 연결되는 노드일 수 있다. 일 예로, ASN은 하드웨어적으로 M2M 단말에 설정되는 노드일 수 있다.

[0040] 또한, 미들 노드(340, Middle Node, MN)은 CSE를 포함하고, 0개 또는 그 이상의 AE를 포함하는 노드일 수 있다. 이때, MN은 필드 도메인에서 설정될 수 있다. MN은 다른 MN 또는 IN과 기준점에 기초하여 연결될 수 있다. 또한 일 예로, MN은 하드웨어적으로 M2M 게이트웨이에 설정될 수 있다.

[0041] 또한, 일 예로, 논-M2M 단말 노드(350, Non-M2M device node, NoDN)은 M2M 엔티티들을 포함하지 않은 노드로서 M2M 시스템과 관리나 협업 등을 수행하는 노드일 수 있다.

[0043] 도 4는 본 개시에 따른 M2M 시스템에서 공통 서비스 평선을 나타낸 도면이다.

[0044] 도 4를 참조하면, 공통 서비스 평선들이 제공될 수 있다. 일 예로, 공통 서비스 엔티티는 어플리케이션 및 서비스 계층 관리(402, Application and Service Layer Management), 통신 관리 및 전달 처리(404, Communication Management and Delivery Handling), 데이터 관리 및 저장(406, Data Management and Repository), 장치 관리(408, Device Management), 발견(410, Discovery), 그룹 관리(412, Group Management), 위치(414, Location), 네트워크 서비스 노출/서비스 실행 및 트리거링(416, Network Service Exposure/ Service Execution and Triggering), 등록(418, Registration), 보안(420, Security), 서비스 과금 및 계산(422, Service Charging and Accounting), 서비스 세션 관리 기능(Service Session Management) 및 구독/통지(424, Subscription/Notification) 중 적어도 어느 하나 이상의 CSF를 제공할 수 있다. 이때, 공통 서비스 평선에 기초하여 M2M 단말들이 동작할 수 있다. 또한, 공통 서비스 평선은 다른 실시 예도 가능할 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0045] 어플리케이션 및 서비스 계층 관리(402) CSF는 AE들 및 CSE들의 관리를 제공한다. 어플리케이션 및 서비스 계층

관리(402) CSF는 CSE의 기능들을 구성하고, 문제 해결하고, 및 업그레이드하는 것뿐만 아니라, AE들을 업그레이드하는 능력들을 포함한다.

- [0046] 통신 관리 및 전달 처리(404) CSF는 다른 CSE들, AE들, 및 NSE들과의 통신들을 제공한다. 통신 관리 및 전달 처리(404) CSF는 어떤 시간 및 어느 통신 연결로 통신들을 전달할지를 결정하고, 필요하고 허용되는 경우 그것들이 나중에 전달될 수 있도록 통신들 요청을 버퍼링하기로 결정한다.
- [0047] 데이터 관리 및 저장(406) CSF는 데이터 저장 및 중재 기능들(예: 집결을 위한 데이터 수집, 데이터 리포매팅, 및 분석 및 시멘틱 처리를 위한 데이터 저장)을 제공한다.
- [0048] 장치 관리(408) CSF는 M2M 게이트웨이들 및 M2M 디바이스들 상에서 디바이스 능력들의 관리를 제공한다.
- [0049] 발견(410) CSF는 필터 기준들에 기초하여 어플리케이션들 및 서비스들에 대한 정보를 검색하는 기능을 제공한다.
- [0050] 그룹 관리(412) CSF는 그룹 관련 요청들의 처리를 제공한다. 그룹 관리(412) CSF는 M2M 시스템이 여러 디바이스들, 어플리케이션들 등에 대한 대량 작업들(bulk operations)을 지원하는 것을 가능하게 한다.
- [0051] 위치(414) CSF는 AE들이 지리적 장소 정보를 획득하는 것을 가능하게 하는 기능을 제공한다.
- [0052] 네트워크 서비스 노출/서비스 실행 및 트리거링(416) CSF는 네트워크 서비스 기능들에 액세스하기 위한 기저 네트워크들과의 통신들을 관리한다.
- [0053] 등록(418) CSF는 AE들(또는 다른 원격 CSE들)이 CSE에 등록하기 위한 기능을 제공한다. 등록(418) CSF는 AE들(또는 원격 CSE)이 CSE의 서비스들을 사용하는 것을 허용한다.
- [0054] 보안(420) CSF는 식별, 인증, 및 허가를 포함하는 액세스 제어와 같은 서비스 레이어에 대한 보안 기능들을 제공한다.
- [0055] 서비스 과금 및 계산(422) CSF는 서비스 레이어에 대한 과금 기능들을 제공한다.
- [0056] 구독/통지(424) CSF는 이벤트에 가입하는 것을 허용하고, 해당 이벤트가 발생할 때 통지되는 기능을 제공한다.
- [0058] 도 5는 본 개시에 따른 M2M 시스템에서 송신자 및 수신자가 메시지를 교환하는 방법을 나타낸 도면이다.
- [0059] 도 5를 참조하면, 송신자(originator, 510)는 요청 메시지를 수신자(receiver, 520)로 전송할 수 있다. 이때, 송신자(510)와 수신자(520)는 상술한 M2M 단말일 수 있다. 다만, M2M 단말에 한정되지 않고, 송신자(510)와 수신자(520)는 다른 단말일 수 있으며, 상술한 실시 예로 한정되지 않는다. 또한, 일 예로, 송신자(510) 및 수신자(520)는 상술한 노드, 엔티티, 서버 또는 게이트웨이일 수 있다. 즉, 송신자(510) 및 수신자(520)는 하드웨어적인 구성 또는 소프트웨어적인 구성일 수 있으며, 상술한 실시 예로 한정되지 않는다.
- [0060] 이때, 일 예로, 송신자(510)가 전송하는 요청 메시지에는 적어도 하나의 파라미터가 포함될 수 있다. 이때, 일 예로, 파라미터는 필수 파라미터 또는 선택 파라미터가 있을 수 있다. 일 예로, 송신단과 관련된 파라미터, 수신단과 관련된 파라미터, 식별 파라미터 및 동작 파라미터 등은 필수적인 파라미터일 수 있다. 또한, 그 밖에 다른 정보에 대해서는 선택 파라미터일 수 있다. 이때, 송신단 관련 파라미터는 송신자(510)에 대한 파라미터일 수 있다. 또한, 수신단 관련 파라미터는 수신자(520)에 대한 파라미터일 수 있다. 또한, 식별 파라미터는 상호간의 식별을 위해 요구되는 파라미터일 수 있다.
- [0061] 또한, 동작 파라미터는 동작을 구분하기 위한 파라미터일 수 있다. 일 예로, 동작 파라미터는 생성(Create), 조회(Retrieve), 갱신(Update), 삭제>Delete) 및 통지(Notify) 중 적어도 어느 하나로 설정될 수 있다. 즉, 동작을 구별하기 위한 파라미터일 수 있다.
- [0062] 이때, 수신자(520)는 송신자(510)로부터 요청 메시지를 수신하면 해당 요청 메시지를 처리할 수 있다. 일 예로, 수신자(520)는 요청 메시지에 포함된 동작을 수행할 수 있으며, 이를 위해 파라미터가 유효한지 여부 및 권한이 있는지 여부 등을 판단할 수 있다. 이때, 수신자(520)는 파라미터가 유효하고, 권한이 있다면 요청 대상이 되는 자원 존재하는지 여부를 확인하고, 이에 기초하여 프로세싱을 수행할 수 있다.
- [0063] 일 예로, 이벤트가 발생하는 경우, 송신자(510)는 수신자(520)에게 통지에 대한 파라미터를 포함하는 요청 메시지를 전송할 수 있다. 수신자(520)는 요청 메시지에 포함된 통지에 대한 파라미터를 확인하고, 이에 기초하여

동작을 수행할 수 있으며, 응답 메시지를 송신자(510)로 다시 전송할 수 있다.

[0064] 도 5와 같은 요청 메시지 및 응답 메시지를 이용한 메시지 교환 절차는 Mca 기준점에 기반하여 AE 및 CSE 간 또는 Mcc 기준점에 기반하여 CSE들 간 수행될 수 있다. 즉, 송신자(510)는 AE 또는 CSE이고, 수신자(520)는 AE 또는 CSE일 수 있다. 요청 메시지 내의 동작에 따라, 도 5와 같은 메시지 교환 절차는 AE 또는 CSE에 의해 시작될 (initiated) 수 있다.

[0066] 기준점 Mca 및 Mcc를 통한 요청자로부터 수신자로의 요청은 적어도 하나의 필수적인(mandatory) 파라미터를 포함하고, 적어도 하나의 선택적인(optional) 파라미터를 포함할 수 있다. 즉, 정의된 각 파라미터는 요청되는 동작(operation)에 따라 필수적이거나 선택적일 수 있다. 예를 들어, 응답 메시지는 이하 [표 1]에 나열된 파라미터들 중 적어도 하나를 포함할 수 있다.

표 1

Response message parameter/success or not
Response Status Code - successful, unsuccessful, ack
Request Identifier - uniquely identifies a Request message
Content - to be transferred
To - the identifier of the Originator or the Transit CSE that sent the corresponding non-blocking request
From - the identifier of the Receiver
Originating Timestamp - when the message was built
Result Expiration Timestamp - when the message expires
Event Category - what event category shall be used for the response message
Content Status
Content Offset
Token Request Information
Assigned Token Identifiers
Authorization Signature Request Information
Release Version Indicator - the oneM2M release version that this response message conforms to

[0068] 요청 메시지 또는 응답 메시지에서 사용될 수 있는 필터 기준 조건(filter criteria condition)은 이하 [표 2] 및 [표 3]과 같이 정의될 수 있다.

표 2

Condition tag	Multipl city	Description
Matching Conditions		
createdBefore	0..1	The creationTime attribute of the matched resource is chronologically before the specified value.
createdAfter	0..1	The creationTime attribute of the matched resource is chronologically after the specified value.
modifiedSince	0..1	The lastModifiedTime attribute of the matched resource is chronologically after the specified value.
unmodifiedSince	0..1	The lastModifiedTime attribute of the matched resource is chronologically before the specified value.
stateTagSmaller	0..1	The stateTag attribute of the matched resource is smaller than the specified value.
stateTagBigger	0..1	The stateTag attribute of the matched resource is bigger than the specified value.
expireBefore	0..1	The expirationTime attribute of the matched resource is chronologically before the specified value.
expireAfter	0..1	The expirationTime attribute of the matched resource is chronologically after the specified value.
labels	0..1	The labels attribute of the matched resource matches the specified value.

labelsQuery	0..1	The value is an expression for the filtering of labels attribute of resource when it is of key-value pair format. The expression is about the relationship between label-key and label-value which may include equal to or not equal to, within or not within a specified set etc. For example, label-key equals to label value, or label-key within {label-value1, label-value2}. Details are defined in [3]
childLabels	0..1	A child of the matched resource has labels attributes matching the specified value. The evaluation is the same as for the labels attribute above. Details are defined in [3].
parentLabels	0..1	The parent of the matched resource has labels attributes matching the specified value. The evaluation is the same as for the labels attribute above. Details are defined in [3].
resourceType	0..n	The resourceType attribute of the matched resource is the same as the specified value. It also allows differentiating between normal and announced resources.
childResourceType	0..n	A child of the matched resource has the resourceType attribute the same as the specified value.
parentResourceType	0..1	The parent of the matched resource has the resourceType attribute the same as the specified value.
sizeAbove	0..1	The contentSize attribute of the <contentInstance> matched resource is equal to or greater than the specified value.
sizeBelow	0..1	The contentSize attribute of the <contentInstance> matched resource is smaller than the specified value.
contentType	0..n	The contentInfo attribute of the <contentInstance> matched resource matches the specified value.
attribute	0..n	This is an attribute of resource types (clause 9.6). Therefore, a real tag name is variable and depends on its usage and the value of the attribute can have wild card *. E.g. creator of container resource type can be used as a filter criteria tag as "creator=Sam", "creator=Sam*", "creator=*Sam".
childAttribute	0..n	A child of the matched resource meets the condition provided. The evaluation of this condition is similar to the attribute matching condition above.
parentAttribute	0..n	The parent of the matched resource meets the condition provided. The evaluation of this condition is similar to the attribute matching condition above.
semanticsFilter	0..n	Both semantic resource discovery and semantic query use semanticsFilter to specify a query statement that shall be specified in the SPARQL query language [5]. When a CSE receives a RETRIEVE request including a semanticsFilter, and the Semantic Query Indicator parameter is also present in the request, the request shall be processed as a semantic query; otherwise, the request shall be processed as a semantic resource discovery. In the case of semantic resource discovery targeting a specific resource, if the semantic description contained in the <semanticDescriptor> of a child resource matches the semanticFilter, the URI of this child resource will be included in the semantic resource discovery result. In the case of semantic query, given a received semantic query request and its query scope, the SPARQL query statement shall be executed over aggregated semantic information collected from the semantic resource(s) in the query scope and the produced output will be the result of this semantic query. Examples for matching semantic filters in SPARQL to semantic descriptions can be found in [i.28].
filterOperation	0..1	Indicates the logical operation (AND/OR) to be used for different condition tags. The default value is logical AND.
contentFilterSyntax	0..1	Indicates the Identifier for syntax to be applied for content-based discovery.
contentFilterQuery	0..1	The query string shall be specified when contentFilterSyntax parameter is present.

표 3

Condition tag	Multiplicity	Description
Filter Handling Conditions		
filterUsage	0..1	Indicates how the filter criteria is used. If provided, possible values are 'discovery' and 'IPEOnDemandDiscovery'. If this parameter is not provided, the Retrieve operation is a generic retrieve operation and the content of the child resources fitting the filter criteria is returned. If filterUsage is 'discovery', the Retrieve operation is for resource discovery (clause 10.2.6), i.e. only the addresses of the child resources are returned. If filterUsage is 'IPEOnDemandDiscovery', the other filter conditions are sent to the IPE as well as the discovery Originator ID. When the IPE successfully generates new resources matching with the conditions, then the resource address(es) shall be returned. This value shall only be valid for the Retrieve request targeting an <AE> resource that represents the IPE.
limit	0..1	The maximum number of resources to be included in the filtering result. This may be modified by the Hosting CSE. When it is modified, then the new value shall be smaller than the suggested value by the Originator.
level	0..1	The maximum level of resource tree that the Hosting CSE shall perform the operation starting from the target resource (i.e. To parameter). This shall only be applied for Retrieve operation. The level of the target resource itself is zero and the level of the direct children of the target is one.
offset	0..1	The number of direct child and descendant resources that a Hosting CSE shall skip over and not include within a Retrieve response when processing a Retrieve request to a targeted resource.
applyRelativePath	0..1	This attribute contains a resource tree relative path (e.g. ../tempContainer/LATEST). This condition applies after all the matching conditions have been used (i.e. a matching result has been obtained). The attribute determines the set of resource(s) in the final filtering result. The filtering result is computed by appending the relative path to the path(s) in the matching result. All resources whose Resource-IDs match that combined path(s) shall be returned in the filtering result. If the relative path does not represent a valid resource, the outcome is the same as if no match was found, i.e. there is no corresponding entry in the filtering result.

[0071] 기준점 Mca 및 Mcc를 통한 자원으로의 접근(accessing)에 대한 요청에 대응한 응답은 적어도 하나의 필수적인 (mandatory) 파라미터를 포함하고, 적어도 하나의 선택적인(optional) 파라미터를 포함할 수 있다. 즉, 정의된 각 파라미터는 요청되는 동작(operation) 또는 필수 응답 코드(mandatory response code)에 따라 필수적이거나 선택적일 수 있다. 예를 들어, 요청 메시지는 이하 [표 4]에 나열된 파라미터들 중 적어도 하나를 포함할 수 있다.

표 4

Request message parameter	
Mandatory	Operation - operation to be executed / CREAT, Retrieve, Update, Delete, Notify
	To - the address of the target resource on the target CSE
	From - the identifier of the message Originator
	Request Identifier - uniquely identifies a Request message
Operation dependent	Content - to be transferred
	Resource Type - of resource to be created

Optional	Originating Timestamp - when the message was built
	Request Expiration Timestamp - when the request message expires
	Result Expiration Timestamp - when the result message expires
	Operational Execution Time - the time when the specified operation is to be executed by the target CSE
	Response Type - type of response that shall be sent to the Originator
	Result Persistence - the duration for which the reference containing the responses is to persist
	Result Content - the expected components of the result
	Event Category - indicates how and when the system should deliver the message
	Delivery Aggregation - aggregation of requests to the same target CSE is to be used
	Group Request Identifier - Identifier added to the group request that is to be fanned out to each member of the group
	Group Request Target Members-indicates subset of members of a group
	Filter Criteria - conditions for filtered retrieve operation
	Desired Identifier Result Type - format of resource identifiers returned
	Token Request Indicator - indicating that the Originator may attempt Token Request procedure (for Dynamic Authorization) if initiated by the Receiver
	Tokens - for use in dynamic authorization
	Token IDs - for use in dynamic authorization
	Role IDs - for use in role based access control
	Local Token IDs - for use in dynamic authorization
	Authorization Signature Indicator - for use in Authorization Relationship Mapping
	Authorization Signature - for use in Authorization Relationship Mapping
	Authorization Relationship Indicator - for use in Authorization Relationship Mapping
	Semantic Query Indicator - for use in semantic queries
	Release Version Indicator - the oneM2M release version that this request message conforms to.
	Vendor Information

- [0073] 일반 자원(normal resource)은 관리될 정보의 기저(base)를 구성하는 데이터의 표현(representation)의 완전한 집합을 포함한다. 가상(virtual) 또는 선언된(announced)이 아닌 한, 본 문서에서 자원 종류(type)는 일반 자원으로 이해될 수 있다.
- [0074] 가상 자원(virtual resource)은 처리(processing) 및/또는 검색 결과(retrieve result)를 트리거링하기 위해 사용된다. 하지만, 가상 자원은 CSE 내에서 영구적인(permanent) 표현을 가지지 아니한다.
- [0075] 선언된 자원(announced resource)은 오리지널(original) 자원의 어트리뷰트들(attributes)의 집합을 포함한다. 오리지널 자원이 변화할 때, 선언된 자원은 오리지널 자원의 호스팅(hosting) CSE에 의해 자동적으로 갱신된다. 선언된 자원은 오리지널 자원으로서의 링크(link)를 포함한다.
- [0076] 자원 선언(resource announcement)은 자원 발견(resource discovery)을 가능하게 한다. 원격(remote) CSE에서의 선언된 자원은 원격 CSE에서, 오리지널 자원의 자식(children)으로서 존재하지(present) 아니하거나 선언된 자식이 아닌, 자식 자원(child resource)을 생성하기 위해 사용될 수 있다.
- [0077] 자원의 선언을 지원하기 위해, 자원 템플릿(template) 내의 추가적인 열(column)이 관련된 선언된 자원 타입 내의 포함을 위해 선언될 속성을 특정할 수 있다. 각 선언된 <resourceType>에 대하여, 오리지널 <resourceType>으로의 접미사 'Annc'의 추가가 관련된 선언된 자원 종류를 지시하기 위해 사용될 수 있다. 예를 들어, 자원 <containerAnnc>는 <container> 자원을 위한 선언된 자원 종류를 지시할 수 있고, <groupAnnc>는 <group>을 위한 선언된 자원 종류를 지시할 수 있다.
- [0079] GDPR(general data protection regulation)는 유럽 연합(European Union, EU) 및 유럽 경제 지역(European economic area, EEA)의 개인(individual citizens)에 대한 프라이버시(privacy) 및 데이터 보호에 관련된 유럽 연합 법 내의 규정이다. 개인 데이터를 다루는 비즈니스 절차는 원칙의 고려와 함께 설계 및 구현되어야 하며, 데이터를 보호하기 위한 보호 장치를 제공한다. 그리고, 개인 데이터를 다루는 비즈니스 절차는, 데이터가 명백하게 알려진 허락없이 공개적으로 활용되지 아니하고, 분리되어 저장된 부가 정보 없이 대상을 식별하기 위해

사용될 수 없도록, 기본적으로 가장 높은 가능한 프라이버시 설정(highest-possible privacy setting)을 이용한다.

- [0080] GDPR에 따르면, 개인 데이터를 처리하는 것은 원칙적으로 금지되나, 법에 의해 특별히 허용되거나 또는 데이터 주체가 동의한 경우에 허용된다. 동의는 방해 없이, 특정적으로, 모호함 없이 이루어져야 한다. 자유로이 주어진 동의를 획득하기 위해, 동의는 자발성에 기반하여 주어져야 한다. 그러므로, IoT 플랫폼에서 동의를 어떻게 관리하는지는 매우 주요한 문제이다.
- [0081] IoT 데이터를 위한 동의를 제공하기 위한 방안은 다음과 같은 3가지 방식들로 도출될 수 있다. 첫째, 동의는 웹 인터페이스를 통해 제공될 수 있다. 이 경우, 동의는 어플리케이션이 IoT 플랫폼에 등록된 이후에 추가될 수 있다. 둘째, 동의는 등록 절차에서 동의 또는 비동의가 명시적으로 포함됨에 의해 제공될 수 있다. 셋째, 동의는 상호작용 등록(interactive registration)에 의해 제공될 수 있다. 이를 위해, 등록 절차는 IoT 어플리케이션의 사용자로부터의 동의를 획득하는 단계를 포함할 수 있다. 그러나, oneM2M 규격은 ACP(access control policy)를 가지지만, ACP는 IoT 데이터의 동의를 다루지 아니한다. 또한, 동의와 유사한 개념이 oneM2M 규격에 도입된 바 없다. oneM2M 규격에서, IoT 데이터를 처리(cover)하는 것을 허용하는지 여부를 지시할 방안이 없다.
- [0082] 개인 데이터 사용에 대한 사용자의 동의를 제공하는 3가지 방식들에 대해 보다 구체적으로 살펴보면 다음과 같다.
- [0083] □ 사후 제공(post-provisioning): IoT 어플리케이션은 동의 없이 IoT 플랫폼에 등록된다. 일단 IoT 어플리케이션의 데이터가 개인 데이터임이 확인되면, 사용자는 동의를 선택할 수 있다. 예를 들어, 사용자는 웹 인터페이스에 의해 동의를 선택할 수 있다. 사후 제공을 위한 절차의 일 예는 도 6a와 같다.
- [0084] 도 6a는 본 개시에 따른 M2M 시스템에서 사후 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 예를 나타낸 도면이다. 도 6a를 참고하면, S611 단계에서, IoT 어플리케이션(610)은 IoT 플랫폼(620)에게 등록 요청(registration request) 메시지를 송신한다. S613 단계에서, IoT 플랫폼(620)은 IoT 어플리케이션(610)에게 등록 응답(registration response) 메시지를 송신한다. 이후, S615 단계에서, 사용자(630)는 IoT 플랫폼(620)에게 동의 설정(consent setup) 메시지를 송신한다.
- [0085] □ 사전 제공(pre-provisioning): 사용자가 서비스 제공자로부터 IoT 장치를 구매하면, 동의가 주어지고, IoT 장치에 저장된다(embedded). 장치가 IoT 플랫폼에 등록되면, 사전 제공된 동의가 등록 절차에 포함될 수 있다. 사전 제공을 위한 절차의 일 예는 도 6b와 같다.
- [0086] 도 6b는 본 개시에 따른 M2M 시스템에서 사전 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 예를 나타낸 도면이다. 도 6b를 참고하면, S621 단계에서, 사용자(630)는 IoT 어플리케이션(610)에게 동의 설정 메시지를 송신한다. 이후, S623 단계에서, IoT 어플리케이션(610)은 IoT 플랫폼(620)에게 등록 요청 메시지를 송신한다. 여기서, 등록 요청 메시지는 동의에 대한 정보를 포함한다. S625 단계에서, IoT 플랫폼(620)은 IoT 어플리케이션(610)에게 등록 응답 메시지를 송신한다.
- [0087] □ 상호작용 제공(interactive-provisioning): IoT 어플리케이션이 IoT 플랫폼에 등록될 때, 사용자의 동의를 획득하기 위한 추가적인 절차가 존재한다. 사전 제공을 위한 절차의 일 예는 도 6c와 같다.
- [0088] 도 6c는 본 개시에 따른 M2M 시스템에서 상호작용 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 예를 나타낸 도면이다. 도 6c를 참고하면, S631 단계에서, IoT 어플리케이션(610)은 IoT 플랫폼(620)에게 등록 요청 메시지를 송신한다. S633 단계에서, 사용자(630)는 IoT 플랫폼(620)에게 동의 설정 메시지를 송신한다. 도 6c에 도시되지 아니하였으나, S633 단계에 앞서, IoT 플랫폼(620) 또는 IoT 어플리케이션(610)이 사용자(630)에게 동의 설정을 요청하는 동작이 수행될 수 있다. 여기서, 등록 요청 메시지는 동의에 대한 정보를 포함한다. S635 단계에서, IoT 플랫폼(620)은 IoT 어플리케이션(610)에게 등록 응답 메시지를 송신한다.
- [0089] 전술한 3가지 방안들을 비교하면 다음과 같다. 동의를 제공하기 위해, 사후 제공 방식의 경우, 사용자가 등록 이후에 UI(예: 웹 UI)를 이용한다. 사전 제공 방식의 경우, 사용자 또는 서비스 제공자가 IoT 장치의 구매 시점에 미리 설정된 메시지를 이용한다. 상호작용 제공 방식의 경우, 사용자가 등록 절차 동안 개선된(enhanced) 등록 절차를 이용한다. 3가지 방안들의 비교를 정리하면 이하 [표 5]와 같다.

표 5

[0090]	사후 제공 누가 사용자	사전 제공 사용자 또는 서비스제공자	상호작용 제공 사용자
--------	-----------------	------------------------	----------------

언제	등록 이후	IoT 장치 구매 시	등록 동안
어떻게	UI를 이용 (예: 웹 UI)	미리설정된 메시지를 이용	개선된 등록 절차를 이용

[0092] IoT 플랫폼에서 사용자의 동의를 관리하는 것은 높은 레벨의 요구사항을 필요로 한다. 구체적으로, IoT 시스템은 IoT 데이터에 대한 동의를 관리하는 것을 지원한다. IoT 데이터에 대한 동의는 방해없이(freely) 주어져야 한다. 개인 데이터로서 확인된 IoT 데이터는 명확한(unambiguous) 동의를 가져야 한다. IoT 시스템은 IoT 데이터의 수집(collection)에 대한 동의를 지원한다.

[0093] oneM2M 시스템의 경우, 사용자의 동의에 대한 관리는 다양한 형식으로 지원될 수 있다. 다양한 실시 예들에 따라, 어트리뷰트 기반(attributed-based) 동의 관리(consent management)에 의해, 자원 기반(resource-based) 동의 관리에 의해, 또는 ACP(access control policy) 기반 동의 관리에 의해, 사용자의 동의가 관리될 수 있다. 이하 각 형식의 개념이 설명된다.

[0095] 어트리뷰트 기반 동의 관리

[0096] 동의를 지시하는 어트리뷰트가 개인 데이터로서 확인된 IoT 데이터에 부가될 수 있다. 즉, 동의를 필요로 하는 개인 데이터를 포함하는 IoT 데이터를 포함하는 자원이 생성되면, 해당 자원에 동의에 관련된 어트리뷰트가 추가된다. 개별 콘텐츠 인스턴스(contentInstance), 컨테이너(container), 또는 그룹(group)은 동의에 관련된 새로운 어트리뷰트(예: 'consent')를 포함할 수 있다. 콘텐츠 인스턴스에 동의에 관련된 어트리뷰트가 포함된 경우, 동의가 개별적인 IoT 데이터 인스턴스에 주어지는 것으로 해석될 수 있다. 컨테이너에 해당 어트리뷰트가 포함된 경우, 동의가 대상 컨테이너 하의 모든 콘텐츠 인스턴스 자원들에 대해 주어지는 것으로 해석될 수 있다. 그룹에 해당 어트리뷰트가 포함된 경우, 동의가 해당 그룹 하의 모든 IoT 데이터에 대해 주어진 것으로 해석될 수 있다.

[0097] 도 7은 본 개시에 따른 M2M 시스템에서 어트리뷰트-기반 동의 관리의 개념을 나타낸 도면이다. 도 7을 참고하면, 어트리뷰트 내의 공통 어트리뷰트(common attribute)들 중 하나로서 'consent'(702)가 정의된다. 여기서, 어트리뷰트 'consent'(702)는 이하 [표 6]과 같이 정의될 수 있다.

표 6

어트리뷰트 이름	설명
consent	IoT 데이터의 소유자가 특정 목적을 위해 데이터를 더 처리하는 것을 허용하는지 여부를 지시하기 위해 사용됨(Used to indicate whether the owner of the IoT data gives a permission to further process data for specific purposes)

[0100] 자원-기반 동의 관리

[0101] 동의는 목적(purpose) 및 관련된 활동(activity)들을 명확히 하기 위한 다양한 정보를 포함할 수 있다. 일 실시 예에 따라, 다양한 정보를 관리하기 위해, 동의를 관리하는 새로운 자원(이하 '동의 자원'이라 칭함)이 정의된다. 동의 자원은 동일한 자원 하의 자원들의 목록을 포함할 수 있다. 예를 들어, 활동들 및 정보는 전용(dedicated) 자원(예: consentMgt)으로 모델링될 수 있으며, 개인 데이터로서 확인되는 각 자원은 관련된 적어도 하나의 동의 자원을 참조한다(refer to). 동의 자원은 동의의 목적 및 관련 정보(relevant information)를 저장하기 위해 사용될 수 있다. 동의 자원은 동의의 식별 정보를 포함하고, 서로 다른 처리 규칙들을 정의하는 복수의 동의들을 가질 수 있다. 또한, 동의 자원은 동일한 동의에 관련된 자원들의 목록을 포함할 수 있다.

[0102] 도 8은 본 개시에 따른 M2M 시스템에서 자원-기반 동의 관리의 개념을 나타낸 도면이다. 도 8을 참고하면, 어트리뷰트 내의 공통 어트리뷰트들 중 하나로서 'consentTypeIDs'(802)가 정의된다. 예를 들어, 동의를 관리하기 위한 자원은 이하 [표 7]에 나열된 어트리뷰트들 중 적어도 하나를 포함할 수 있다.

표 7

[0103]

어트리뷰트 이름	설명
Owner	동의의 소유자(Owner of the consent)
createdTime	동의가 생성된 시기(When this consent is created)
Name	동의의 이름(Name of consent)
allowedProcessing	허용되는 처리의 종류(What kinds of processing is allowed)(예: 처리(processing), 제삼자와의 공유(sharing with 3 rd party))
Validity	동의의 유효성(Validity of the consent)
Identifier	동의의 식별자(Identifier of the consent)
expirationTime	동의의 만료시점(Expiration of the consent)
rightToWithdraw	소유자가 언제든지 동의를 철회할 권리를 가지는지 여부를 지시(Indicate whether the owner has a right to withdraw the consent at anytime)

[0104]

추가적으로, 동의 자원은 [표 7]에 나열된 어트리뷰트들 외에, 해당 동의의 소유자가 속한 그룹의 목록(예: 사업, 소비자, 관리자, VIP 등), 해당 동의의 식별 정보, 해당 동의가 속한 동의 그룹의 목록(예: 특정 어플리케이션, 마케팅 캠페인, 쿠키(cookie) 타입 등) 중 적어도 하나를 더 포함할 수 있다.

[0106]

ACP-기반 동의 관리

[0107]

동의를 데이터의 사용에 대한 데이터 소유자의 의도를 다루기 때문에, 동의는 ACP의 일부로서 고려될 수 있다. 만일 데이터의 콘텐츠가 개인을 식별할 수 있는(personally identifiable) 정보에 관련된 경우, 오직 사용자의 동의가 있는 콘텐츠만이 공유되거나 데이터의 소유자 외 다른 이에 의해 사용될 수 있다. 그러므로, 동의는 ACP의 하나로서 취급될 수 있다. 따라서, 본 발명은 동의 관리를 처리하도록 ACP 매커니즘을 강화하는 방안을 제안한다

[0108]

oneM2M은 REST(representational state transfer)의 원리에 따르는(RESTful) 구조를 사용한다. API는 자원 상에서의 동작을 수행하는 것을 요구한다. 여기서, 동작은 생성(Create), 조회(Retrieve), 갱신(Update), 삭제>Delete)를 포함한다. CSE는 자원 접근에 대한 스스로의 판단(resource access judgement calls)을 만들 수 없다. 따라서, CSE는 각 자원에 대한 명확한 규칙 설명(clear rules dictating)을 필요로 하며, 그 규칙이 ACP이다. ACP는 누가(예: CSE, AE)가 접근을 허가받는지, 어떤 동작인지, 어떤 환경인지(예: 시간, 엔티티의 위치) 등에 대한 규칙을 정의한다.

[0109]

도 9a는 본 개시에 따른 M2M 시스템에서 ACP 기반 동의 관리를 위한 ACP 규칙의 구조를 나타낸 도면이다. 도 9a를 참고하면, 하나의 자원(912)은 하나의 ACP(914)와 연결되고(linked), ACP(914)는 ACP 규칙(916)을 포함한다. ACP 규칙(916)은 객체(entity)에 대한 사항(918a), 동작(operation)에 대한 사항(918b), 환경(circumstance)에 대한 사항(918c)에 관련된 조건들과 관련된다. 요청 객체, 요청된 동작 및 환경에 의해 조건들(예: WHO, WHIAT, WHICH)이 만족되면, ACP 규칙(916)이 만족된다.

[0110]

동의 관리를 처리하는(cover) ACP 매커니즘에 의해, 사용자의 동의가 관리될 수 있다. 이를 위해, 추가적인 어트리뷰트가 및 매커니즘이 ACP에 추가될 수 있다. 동의 관리에 있어서, 서비스 제공자에 의해 허용되는 처리의 종류가 무엇인지를 정의하는 것은 중요하다. 이에 따라 동의 관리 규칙(consent management rule)들을 정의하는 어트리뷰트(이하 '동의 규칙 어트리뷰트'라 칭함)가 정의될 수 있다. 동의 규칙 어트리뷰트는 ACP 자원을 참조하는 자원에 적용될 수 있다.

[0111]

도 9b는 본 개시에 따른 M2M 시스템에서 ACP 기반 동의 관리를 위한 ACP 규칙 및 동의 규칙의 구조를 나타낸 도면이다. 도 9b를 참고하면, 자원(922)는 ACP(924)와 연결된다. ACP(924)는 복수의 ACP 규칙들(926a-1 내지 926a-3) 및 동의 규칙들(926b-1 내지 926b-3)을 포함한다. 요청 객체, 요청된 동작 및 환경에 의해 조건들(예: WHO, WHIAT, WHICH)이 만족되면, 동의 규칙이 만족된다.

[0112]

ACP 자원은 <accessControlPolicy>이라 지칭될 수 있고, 이하 [표 8]에 나열된 어트리뷰트들 중 적어도 하나를 포함할 수 있다.

표 8

어트리뷰트	multiplicity	RW /RO /WO	설명	<accessControlPolicyAnn c> 어트리뷰 트
resourceType	1	RO	See clause 9.6.1.3.	NA
resourceID	1	RO	See clause 9.6.1.3.	NA
resourceName	1	WO	See clause 9.6.1.3.	NA
parentID	1	RO	See clause 9.6.1.3.	NA
expirationTime	1	RW	See clause 9.6.1.3.	MA
labels	0..1(L)	RW	See clause 9.6.1.3.	MA
creationTime	1	RO	See clause 9.6.1.3.	NA
lastModifiedTime	1	RO	See clause 9.6.1.3.	NA
announceTo	0..1(L)	RW	See clause 9.6.1.3.	NA
announcedAttribute	0..1(L)	RW	See clause 9.6.1.3.	NA
announceSyncType	0..1	RW	See clause 9.6.1.3.	MA
owner	0..1	RW	See clause 9.6.1.3.	NA
privileges	1	RW	A set of access control rules that applies to resources referencing this <accessControlPolicy> resource using the accessControlPolicyID attribute.	MA
selfPrivileges	1	RW	A set of access control rules that apply to the <accessControlPolicy> resource itself and accessControlPolicyIDs attribute of any other resource which is linked to this <accessControlPolicy> resource.	MA
consents	1	RW	A set of consent management rules that applies to resources referencing this <accessControlPolicy> resource	NA
authorizationDecisionResourceIDs	0..1(L)	RW	A list of addresses of <authorizationDecision> resources. See clause 9.6.41 for further details.	MA
authorizationPolicyResourceIDs	0..1(L)	RW	A list of addresses of <authorizationPolicy> resources. See clause 9.6.42 for further details.	MA
authorizationInformationResourceIDs	0..1(L)	RW	A list of addresses of <authorizationInformation> resources. See clause 9.6.43 for further details.	MA

[0114] [표 8]에서, 어트리뷰트 <consents>는 전술한 동의 규칙 어트리뷰트로 이해될 수 있다. 어트리뷰트 <consents>에 표현된 동의 관리 규칙들의 집합은 동의 관리 규칙 튜플들(consent-management-rule-tuples)(예: consentOwner, createdTime, consentName, allowedProcessing, consentValidity, expirationTime, rightToWithdraw)을 포함한다. 예를 들어, 튜플들은 이하 [표 9]에 나열된 항목들 중 적어도 하나를 포함할 수 있다.

표 9

이름	설명
consentOwner	동의의 소유자(Owner of the consent)
consentTimestamp	동의가 생성된 시기(When this consent is created)
consentName	동의의 이름(Name of consent)
consentAllowedProcessing	허용되는 처리의 종류(What kinds of processing is allowed)(예: 처리(processing), 제삼자와의 공유(sharing with 3 rd party))

consentCollectionMethod	동의를 획득하는 방법의 설명(Describe the method by which consent was obtained)
consentValidity	동의의 유효성(Validity of the consent)
consentIdentifier	동의의 식별자(Identifier of the consent)
consentExpirationTime	동의의 만료시점(Expiration of the consent)
consentRightToWithdraw	Indicate whether the owner has a right to withdraw the consent at anytime
consentPublicKey	제어자의 공개 키(Controller's public key)
ThirdPartyDisclosure	제어자가 개인 정보를 제삼자에게 공개하고 있는지 여부를 지시(Indicates if the controller is disclosing personal information to a third party.)
ThirdPartyName	프로세서가 개인 정보를 공개할 제삼자의 이름(The name of the third party to which the processor may disclose the personal information.)

[0117] 도 9c는 본 개시에 따른 M2M 시스템에서 ACP 기반 동의 관리의 개념을 나타낸 도면이다. 도 9c를 참고하면, 어트리뷰트 <consents>(932)가 자원 <ACP1>에 포함되며, 복수의 동의들(932a 내지 932c)에 관련될 수 있다. 복수의 동의들(932a 내지 932c)은 서로 다른 동의 관리 규칙 튜플들(consent management rule tuples)로 구성될 수 있다. 동의 관리 규칙 튜플들의 내용에 따라, 다양한 조건들을 가지는 동의가 정의될 수 있다. 예를 들어, 동의 관리 규칙 튜플들의 내용에 따라, 마케팅 용도에 대한(for marketing) 동의, 제삼자 사용에 대한(for third party processing) 동의가 정의될 수 있다.

[0119] 도 10은 본 개시에 따른 M2M 시스템에서 사후 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 보다 구체적인 예를 나타낸 도면이다. 도 10은 도 6a의 절차를 보다 상세히 나타낸 것으로서, AE#1(1010a), AE#2(1010b), IN(infrastructure node)-CSE(common service entity)(1020) 간 신호 교환을 예시한다. 도 10에서, AE#1(1010a)은 자원을 생성할 것을 요청하는 송신자(originator)이며, IN-CSE(1020)은 자원을 호스팅하는 CES이고, AE#2(1010b)는 사용자가 사용하는 장치이다. 예를 들어, AE#1(1010a)은 IoT 통신에 기반하여 서비스를 제공하는 장치이고, AE#2(1010b)는 사용자가 AE#1(1010a)를 제어하거나 AE#1(1010a)와 상호작용하기 위해 사용하는 장치(예: 스마트폰)일 수 있다.

[0120] 도 10을 참고하면, S1001 단계에서, AE#1(1010a)는 IN-CSE(1020)에게 개인 정보(privacy information)를 포함하는 자원 생성을 위한 요청 메시지를 송신한다. 도 10에 도시되지 아니하였으나, AE#1(1010a) 및 IN-CSE(1020)는 본 절차에 앞서 등록 절차를 수행할 수 있다. 등록 이후, AE#1(1010a)가 AE#2(1010b)에게 서비스를 제공하는 중, AE#1(1010a)는 AE#2(1010b)로부터 사용자의 개인 정보에 해당하는 데이터 또는 개인 정보를 유추할 수 있는 데이터를 획득할 수 있다. 이 경우, 본 단계와 같이, AE#1(1010a)는 개인 정보의 처리에 대한 동의를 관리하기 위한 자원을 생성하는 절차를 시작(initiate)한다.

[0121] S1003 단계에서, IN-CSE(1020)는 로컬 처리를 수행한다. 구체적으로, IN-CSE(1020)는 AE#1(1010a)로부터 요청된 자원을 생성한다. 즉, IN-CSE(1020)는 개인 정보를 포함하는 자원을 생성한다. 일 실시 예에 따라, 개인 정보를 포함하는 자원은 동의에 관련된 어트리뷰트를 포함할 수 있다. 다른 실시 예에 따라, IN-CSE(1020)는 동의에 관련된 자원을 더 생성할 수 있다. 또 다른 실시 예에 따라, IN-CSE(1020)는 동의에 관련된 ACP를 생성할 수 있다. 이때, 아직 사용자의 동의 여부가 확인되지 아니한 상태이므로, 동의에 관련된 어트리뷰트 또는 튜플들 중 적어도 하나는 동의가 없음 또는 알수 없음을 의미하는 값으로 초기화된다.

[0122] S1005 단계에서, IN-CSE(1020)는 AE#1(1010a)에게 응답 메시지를 송신한다. 다시 말해, IN-CSE(1020)는 AE#1(1010a)에 의해 요청된 자원이 생성되었음을 통지한다.

[0123] S1007 단계에서, AE#2(1010b)는 IN-CSE(1020)에게 생성된 자원의 동의 어트리뷰트의 갱신을 위한 갱신 메시지를 송신한다. 갱신 메시지는 개인 정보의 사용에 대한 동의에 관련된 정보를 포함한다. 동의에 관련된 정보는 동의의 여부에 대한 정보, 동의의 소유자에 대한 정보, 동의의 범위에 대한 정보, 동의의 만료 시점에 대한 정보, 동의의 가변성에 대한 정보 중 적어도 하나를 포함할 수 있다. 예를 들어, AE#2(1010b)는 사용자로부터 입력되는 동의 여부에 대한 정보를 확인하고, 확인된 정보에 기반하여 동의 여부에 대한 정보를 생성할 수 있다. 이때, 사용자의 동의 여부 의사는 웹 인터페이스를 통해 입력될 수 있다. 도 10에 도시되지 아니하였으나, 다른 실시 예

에 따라, S1007 단계에 앞서, IN-CSE(1020)는 AE#2(1010b) 또는 AE#1(1010a)에게 동의 여부에 대한 정보를 요청하는 메시지를 송신할 수 있다.

[0124] S1009 단계에서, IN-CSE(1020)는 로컬 처리를 수행한다. 구체적으로, IN-CSE(1020)는 AE#2(1010a)의 요청에 따라 동의 어트리뷰트의 값을 갱신한다. 예를 들어, IN-CSE(1020)는 AE#2(1010a)로부터 수신된 갱신 메시지에 포함된 동의에 관련된 정보에 기반하여 동의에 관련된 어트리뷰트들 또는 튜플들 중 적어도 하나의 값을 설정한다.

[0125] S1011 단계에서, IN-CSE(1020)는 AE#2(1010b)에게 응답 메시지를 송신한다. 다시 말해, IN-CSE(1020)는 AE#2(1010b)의 요청에 따라 동의에 관련된 어트리뷰트들 또는 튜플들 중 적어도 하나의 값이 갱신되었음을 통지한다.

[0127] 도 11은 본 개시에 따른 M2M 시스템에서 상호작용 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 보다 구체적인 예를 나타낸 도면이다. 도 11은 도 6c의 절차를 보다 상세히 나타낸 것으로서, AE#1(1110a), AE#2(1110b), IN-CSE(1120) 간 신호 교환을 예시한다. 도 11에서, AE#1(1110a)은 자원을 생성할 것을 요청하는 송신자(originator)이며, IN-CSE(1120)은 자원을 호스팅하는 CES이고, AE#2(1110b)는 사용자가 사용하는 장치이다. 예를 들어, AE#1(1110a)은 IoT 통신에 기반하여 서비스를 제공하는 장치이고, AE#2(1110b)는 사용자가 AE#1(1110a)를 제어하거나 AE#1(1110a)와 상호작용하기 위해 사용하는 장치(예: 스마트 폰)일 수 있다.

[0128] 도 11을 참고하면, S1101 단계에서, AE#1(1110a)는 IN-CSE(1120)에게 개인 정보 및 소유자 정보를 포함하는 자원 생성을 위한 요청 메시지를 송신한다. 여기서, 소유자 정보는 개인 정보의 소유자가 AE#1(1110b)임을 지시한다. 도 11에 도시되지 아니하였으나, AE#1(1110a) 및 IN-CSE(1120)는 본 절차에 앞서 등록 절차를 수행할 수 있다. 등록 이후, AE#1(1110a)가 AE#2(1110b)에게 서비스를 제공하는 중, AE#1(1110a)는 AE#2(1110b)로부터 사용자의 개인 정보에 해당하는 데이터 또는 개인 정보를 유추할 수 있는 데이터를 획득할 수 있다. 이 경우, 본 단계와 같이, AE#1(1110a)는 개인 정보의 처리에 대한 동의를 관리하기 위한 자원을 생성하는 절차를 시작(initiate)한다.

[0129] S1103 단계에서, IN-CSE(1120)는 로컬 처리를 수행한다. 구체적으로, IN-CSE(1120)는 AE#1(1110a)로부터 요청된 자원을 생성한다. 즉, IN-CSE(1120)는 개인 정보를 포함하는 자원을 생성한다. 일 실시 예에 따라, 개인 정보를 포함하는 자원은 동의에 관련된 어트리뷰트를 포함할 수 있다. 다른 실시 예에 따라, IN-CSE(1120)는 동의에 관련된 자원을 더 생성할 수 있다. 또 다른 실시 예에 따라, IN-CSE(1120)는 동의에 관련된 ACP를 생성할 수 있다. 이때, 아직 사용자의 동의 여부가 확인되지 아니한 상태이므로, 동의에 관련된 어트리뷰트 또는 튜플들 중 적어도 하나는 동의가 없음 또는 알수 없음을 의미하는 값으로 초기화된다.

[0130] S1105 단계에서, IN-CSE(1120)는 AE#2(1110b)에게 생성된 자원에 대한 동의를 요청하는 요청 메시지를 송신한다. 즉, 개인 정보를 포함하는 자원을 생성한 후, IN-CSE(1120)는 개인 정보를 사용하기 위해 필요한 동의를 요청한다. IN-CSE(1120)는 AE#1(1110a)로부터 제공된 소유자 정보에 기반하여 AE#2(1110b)를 확인할 수 있다.

[0131] S1107 단계에서, AE#2(1110b)는 IN-CSE(1120)에게 자원에 대한 동의를 지시하는 응답 메시지를 송신한다. 응답 메시지는 개인 정보의 사용에 대한 동의에 관련된 정보를 포함한다. 동의에 관련된 정보는 동의 여부에 대한 정보, 동의의 소유자에 대한 정보, 동의의 범위에 대한 정보, 동의의 만료 시점에 대한 정보, 동의의 가변성에 대한 정보 중 적어도 하나를 포함할 수 있다. 예를 들어, AE#2(1110b)는 사용자로부터 입력되는 동의 여부에 대한 정보를 확인하고, 확인된 정보에 기반하여 동의 여부에 대한 정보를 생성할 수 있다. 이때, 사용자의 동의 여부의사는 웹 인터페이스를 통해 입력될 수 있다.

[0132] S1109 단계에서, IN-CSE(1120)는 로컬 처리를 수행한다. 구체적으로, IN-CSE(1120)는 AE#2(1110a)의 응답에 따라 동의 어트리뷰트의 값을 갱신한다. 예를 들어, IN-CSE(1120)는 AE#2(1110a)로부터 수신된 갱신 메시지에 포함된 동의에 관련된 정보에 기반하여 동의에 관련된 어트리뷰트들 또는 튜플들 중 적어도 하나의 값을 설정한다.

[0133] S1111 단계에서, IN-CSE(1120)는 AE#1(1110a)에게 응답 메시지를 송신한다. 다시 말해, IN-CSE(1120)는 AE#1(1110a)에 의해 요청된 자원이 생성되었음을 통지한다.

- [0135] 도 12는 본 개시에 따른 M2M 시스템에서 사전 제공 방식에 따라 사용자의 동의를 획득하기 위한 절차의 보다 구체적인 예를 나타낸 도면이다. 도 12는 도 6b의 절차를 보다 상세히 나타낸 것으로서, AE#1(1210a), AE#2(1210b), IN-CSE(1220) 간 신호 교환을 예시한다. 도 12에서, AE#1(1210a)은 자원을 생성할 것을 요청하는 송신자(originator)이며, IN-CSE(1220)은 자원을 호스팅하는 CES이고, AE#2(1210b)는 사용자가 사용하는 장치이다. 예를 들어, AE#1(1210a)은 IoT 통신에 기반하여 서비스를 제공하는 장치이고, AE#2(1210b)는 사용자가 AE#1(1210a)를 제어하거나 AE#1(1210a)와 상호작용하기 위해 사용하는 장치(예: 스마트 폰)일 수 있다.
- [0136] 도 12를 참고하면, S1201 단계에서, AE#2(1212b)는 AE#1(1212a)에게 자원에 대한 동의를 제공하는 메시지를 송신한다. 메시지는 개인 정보의 사용에 대한 동의에 관련된 정보를 포함한다. 동의에 관련된 정보는 동의 여부에 대한 정보, 동의의 소유자에 대한 정보, 동의의 범위에 대한 정보, 동의의 만료 시점에 대한 정보, 동의의 가변성에 대한 정보 중 적어도 하나를 포함할 수 있다. 예를 들어, AE#2(1210b)는 사용자로부터 입력되는 동의 여부에 대한 정보를 확인하고, 확인된 정보에 기반하여 동의 여부에 대한 정보를 생성할 수 있다. 이때, 사용자의 동의 여부 의사는 웹 인터페이스를 통해 입력될 수 있다. 예를 들어, 본 단계는 AE#2(1212b)의 사용자가 AE#1(1212a)를 설치 및 설정하는 과정에서 수행될 수 있다.
- [0137] S1203 단계에서, AE#1(1212a)는 IN-CSE(1220)에게 개인 정보 및 동의를 포함하는 자원 생성을 위한 요청 메시지를 송신한다. 여기서, 소유자 정보는 개인 정보의 소유자가 AE#1(1210b)임을 지시한다. AE#1(1210a)가 AE#2(1210b)에게 서비스를 제공하는 중, AE#1(1210a)는 AE#2(1210b)로부터 사용자의 개인 정보에 해당하는 데이터 또는 개인 정보를 유추할 수 있는 데이터를 획득할 수 있다. 이 경우, 본 단계와 같이, AE#1(1210a)는 개인 정보의 처리에 대한 동의를 관리하기 위한 자원을 생성하는 절차를 시작한다.
- [0138] S1205 단계에서, IN-CSE(1220)는 로컬 처리를 수행한다. 구체적으로, IN-CSE(1220)는 AE#1(1212a)로부터 요청된 자원을 생성한다. 구체적으로, IN-CSE(1220)는 AE#1(1210a)로부터 요청된 자원을 생성한다. 즉, IN-CSE(1220)는 개인 정보를 포함하는 자원을 생성한다. 일 실시 예에 따라, 개인 정보를 포함하는 자원은 동의에 관련된 어트리뷰트를 포함할 수 있다. 다른 실시 예에 따라, IN-CSE(1220)는 동의에 관련된 자원을 더 생성할 수 있다. 또 다른 실시 예에 따라, IN-CSE(1220)는 동의에 관련된 ACP를 생성할 수 있다. 이때, 아직 사용자의 동의 여부가 확인되지 아니한 상태이므로, 동의에 관련된 어트리뷰트 또는 튜플들 중 적어도 하나는 동의가 없음 또는 알수 없음을 의미하는 값으로 초기화된다.
- [0139] S1207 단계에서, IN-CSE(1220)는 AE#1(1212a)에게 응답 메시지를 송신한다. 다시 말해, IN-CSE(1220)는 AE#1(1210a)에 의해 요청된 자원이 생성되었음을 통지한다.
- [0141] 도 13은 본 개시에 따른 M2M 시스템에서 사용자의 동의에 관련된 정보를 관리하기 위한 절차의 예를 나타낸 도면이다. 도 13은 동의에 관련된 정보를 관리하는 장치(예: IN-CSE)의 동작 방법을 예시한다. 도 13을 참고한 설명에서, 동작 주체는 '장치'라 지칭된다.
- [0142] 도 13을 참고하면, S1301 단계에서, 장치는 사용자의 동의가 필요한 개인 데이터를 포함하는 자원 생성에 대한 요청을 수신한다. 이때, 요청과 함께 개인 데이터, 사용자의 동의에 관련된 정보 중 적어도 하나가 수신될 수 있다.
- [0143] S1303 단계에서, 장치는 사용자의 동의에 관련된 정보를 획득한다. 동의에 관련된 정보는 서비스 과정에서 개인 데이터를 수집하는 제1 장치로부터 수신되거나, 또는 사용자가 사용하는 제2 장치로부터 수신될 수 있다. 또한, 동의에 관련된 정보는 자원 생성에 대한 요청이 수신된 후에 수신되거나, 또는 요청과 함께 수신될 수 있다. 동의에 관련된 정보는 동의 여부에 대한 정보, 동의의 소유자에 대한 정보, 동의의 범위에 대한 정보, 동의의 만료 시점에 대한 정보, 동의의 가변성에 대한 정보 중 적어도 하나를 포함할 수 있다.
- [0144] S1305 단계에서, 장치는 동의에 관련된 정보를 포함하는 자원을 생성한다. 여기서, 자원은 개인 데이터를 포함하는 자원과 동일하거나 또는 개인 데이터를 포함하는 자원과 별개의 자원일 수 있다. 동의에 관련된 정보를 포함하는 자원이 개인 데이터를 포함하는 자원과 별개인 경우, 개인 데이터를 포함하는 자원은 동의에 관련된 정보를 포함하는 자원을 참조한다.
- [0146] 도 14는 본 개시에 따른 M2M 시스템에서 사용자의 동의에 관련된 정보를 제공하기 위한 절차의 예를 나타낸 도면이다. 도 14는 동의에 관련된 정보를 제공하는 장치(예: AE#1 또는 AE#2)의 동작 방법을 예시한다. 도 14를

참고한 설명에서, 동작 주체는 '장치'라 지칭된다.

[0147] 도 14를 참고하면, S1401 단계에서, 장치는 사용자의 동의에 관련된 정보를 획득한다. 동의에 관련된 정보는 동의 여부에 대한 정보, 동의의 소유자에 대한 정보, 동의의 범위에 대한 정보, 동의의 만료 시점에 대한 정보, 동의의 가변성에 대한 정보 중 적어도 하나를 포함할 수 있다. 예를 들어, 장치가 사용자 장치(예: AE#2)인 경우, 장치는 장치에 구비된 입력 수단을 통해 동의에 관련된 정보를 획득할 수 있다. 이 경우, 장치는 사용자에게 동의 여부 및 관련된 항목들을 결정하기 위해 필요한 답변을 문의하는 화면을 표시하고, 화면에 응하는 사용자의 입력을 확인할 수 있다. 다른 예로, 장치가 IoT 서비스를 제공하는 장치(예: AE#1)인 경우, 장치는 다른 장치로부터 통신 연결을 통해 동의에 관련된 정보를 수신할 수 있다.

[0148] S1403 단계에서, 장치는 동의에 관련된 정보를 송신한다. 장치는 동의에 관련된 정보를 동의에 관련된 정보를 관리하는 장치(예: IN-CSE)로 송신한다. 송신된 동의에 관련된 정보는 동의에 관련된 자원, 어트리뷰트를 생성하기 위해 사용된다.

[0150] 도 15는 본 개시에 따른 M2M 시스템에서 M2M 장치의 구성을 나타낸 도면이다. 도 15에 도시된 M2M 장치(1510) 또는 M2M 장치(1520)는 전술한 AE, CSE, NSE 중 적어도 하나의 기능을 수행하는 하드웨어로 이해될 수 있다.

[0151] 도 15를 참고하면, M2M 장치(1510)는 장치를 제어하는 프로세서(1512) 및 신호를 송수신하는 송수신부(1514)를 포함할 수 있다. 이때, 프로세서(1512)는 송수신부(1514)를 제어할 수 있다. 또한, M2M 장치(1510)는 다른 M2M 장치(1520)와 통신을 수행할 수 있다. 다른 M2M 장치(1520)도 프로세서(1522) 및 송수신부(1524)를 포함할 수 있으며, 프로세서(1522) 및 송수신부(1524)는 프로세서(1512) 및 송수신부(1514)와 동일한 기능을 수행할 수 있다.

[0152] 일 예로, 상술한 송신자, 수신자, AE, CSE는 각각 도 15의 M2M 장치들(1510 및 1520) 중 하나일 수 있다. 또한, 도 15의 장치들(1510 및 1520)은 다른 장치일 수 있다. 일 예로, 도 15의 장치들(1510 및 1520)은 통신을 수행하는 장치, 자동차 또는 기지국 등과 같은 장치일 수 있다. 즉, 도 15의 장치들(1510 및 1520)은 통신을 수행할 수 있는 장치를 지칭하는 것으로 상술한 실시 예로 한정되지 않는다.

[0154] 상술한 본 발명의 실시 예들은 다양한 수단을 통해 구현될 수 있다. 일 예로, 본 발명의 실시 예들은 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다.

[0155] 상술한 바와 같이 개시된 본 발명의 바람직한 실시형태에 대한 상세한 설명은 당업자가 본 발명을 구현하고 실시할 수 있도록 제공되었다. 상기에서는 본 발명의 바람직한 실시 형태를 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. 따라서, 본 발명은 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다. 또한, 이상에서는 본 명세서의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 명세서는 상술한 특징의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 명세서의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형 실시들은 본 명세서의 기술적 사상이나 전망으로부터 개별적으로 이해되어서는 안될 것이다.

[0156] 그리고 당해 명세서에서는 물건 발명과 방법 발명이 모두 설명되고 있으며, 필요에 따라 양 발명의 설명은 보충적으로 적용될 수 있다.

[0157] 또한, 본 발명에 대하여 그 바람직한 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0158] 1510: M2M 장치

1512: 송수신부

1514: 프로세서

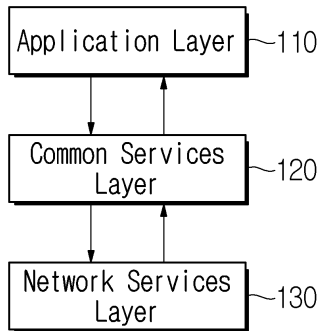
1520: M2M 장치

1222: 송수신부

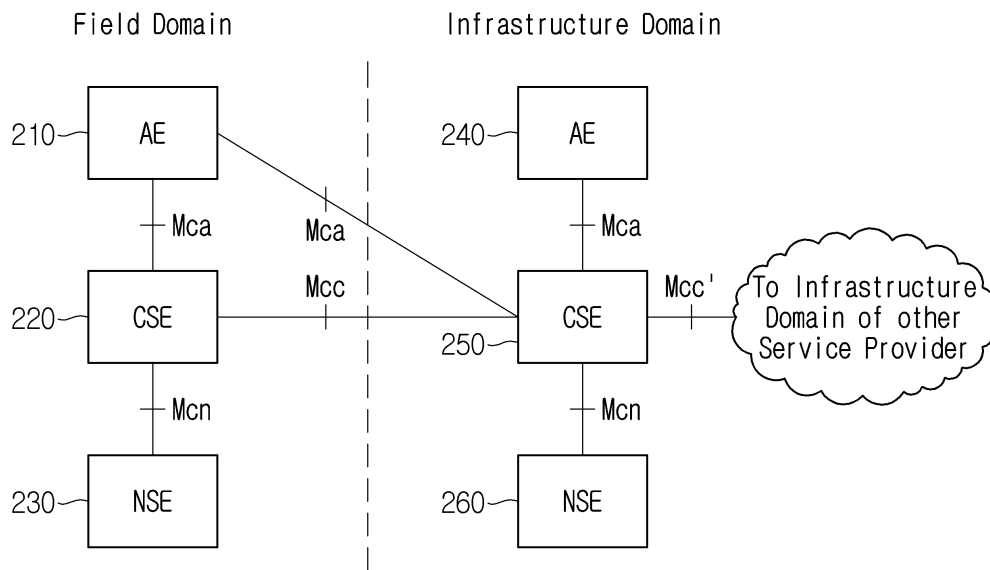
1224: 프로세서

도면

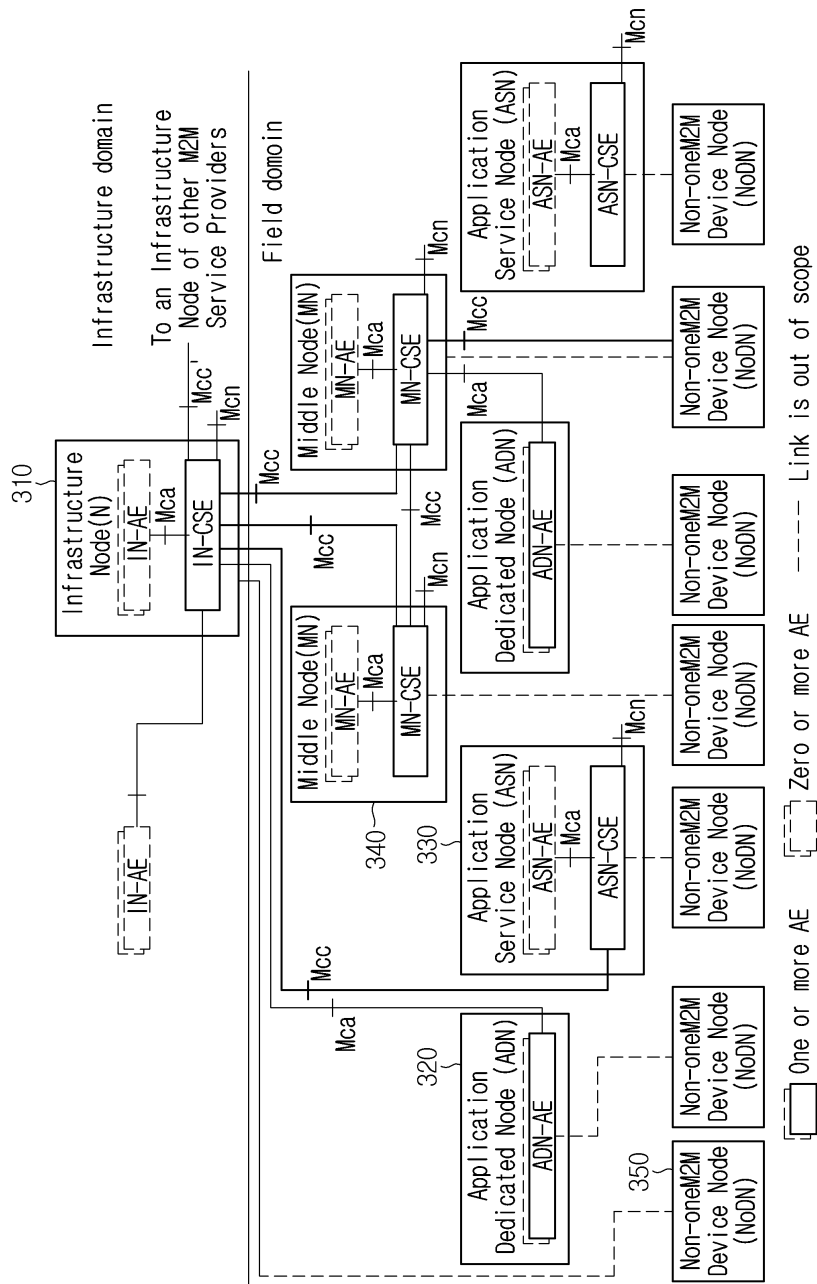
도면1



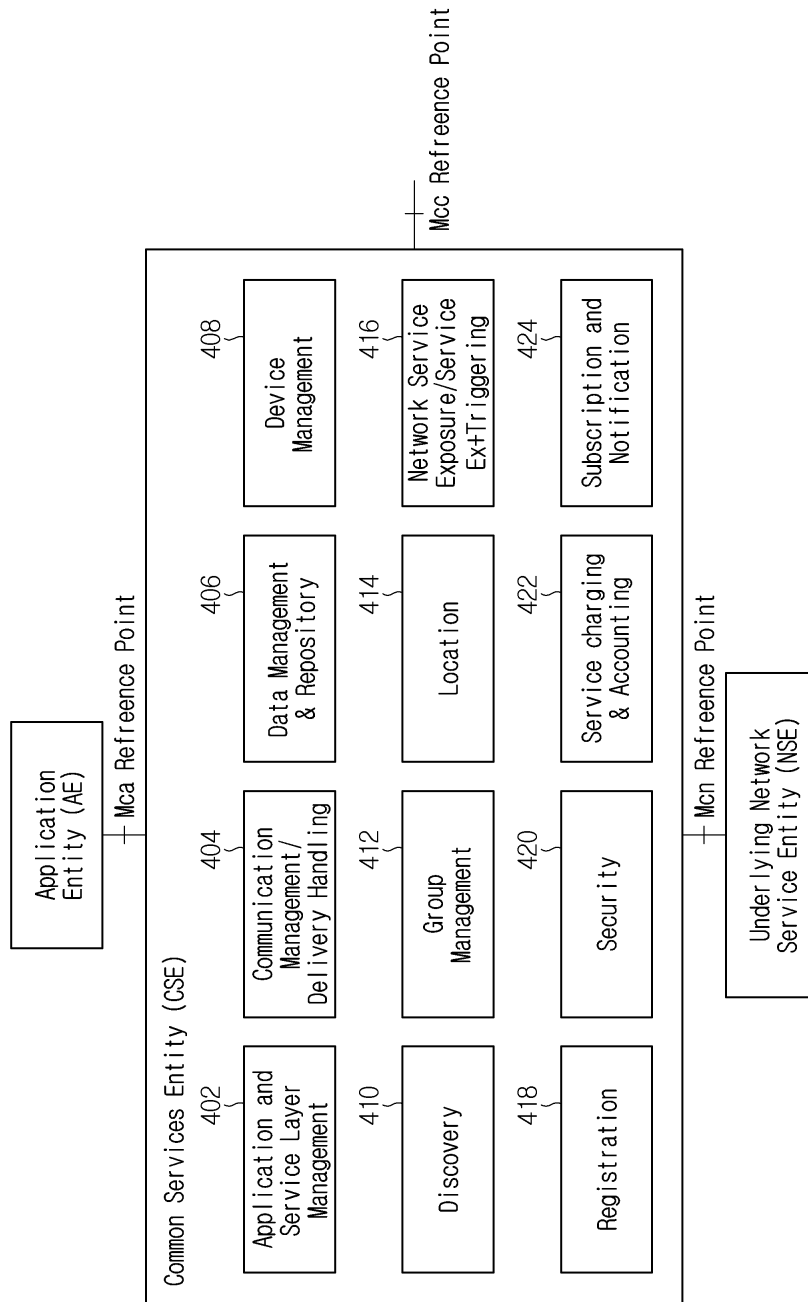
도면2



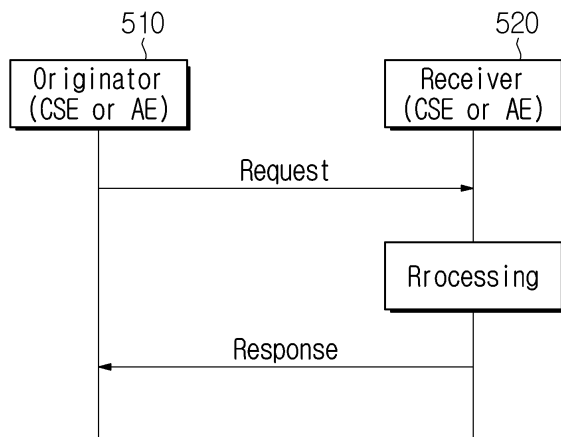
도면3



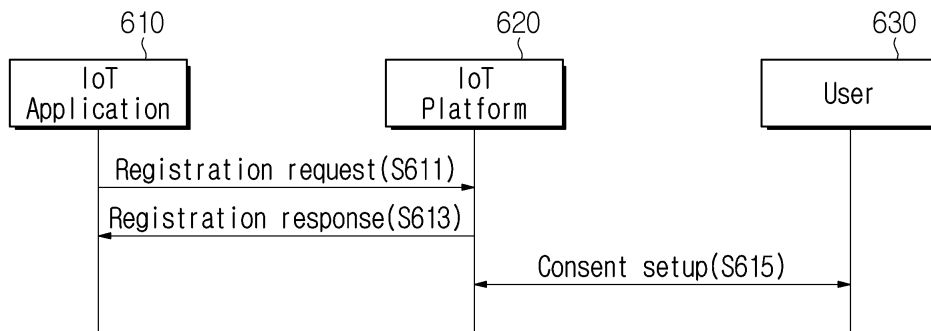
도면4



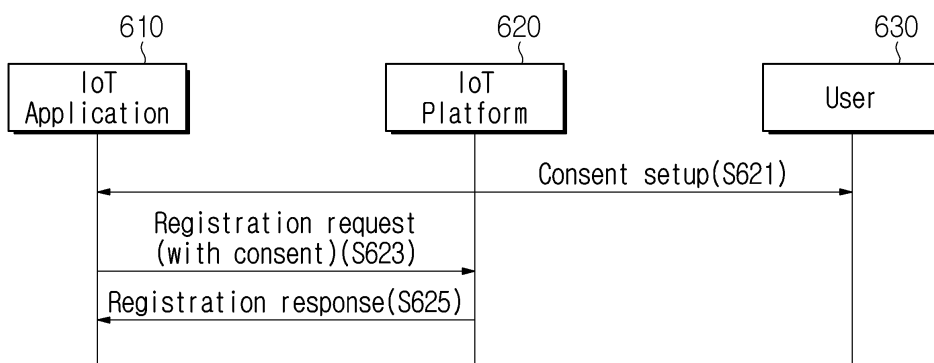
도면5



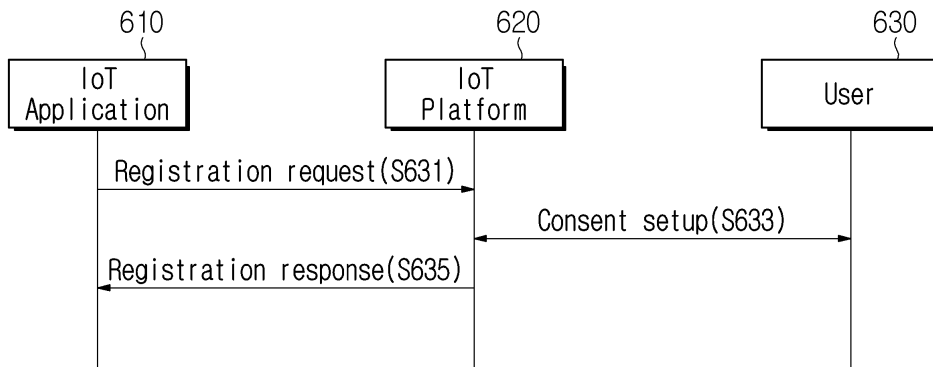
도면6a



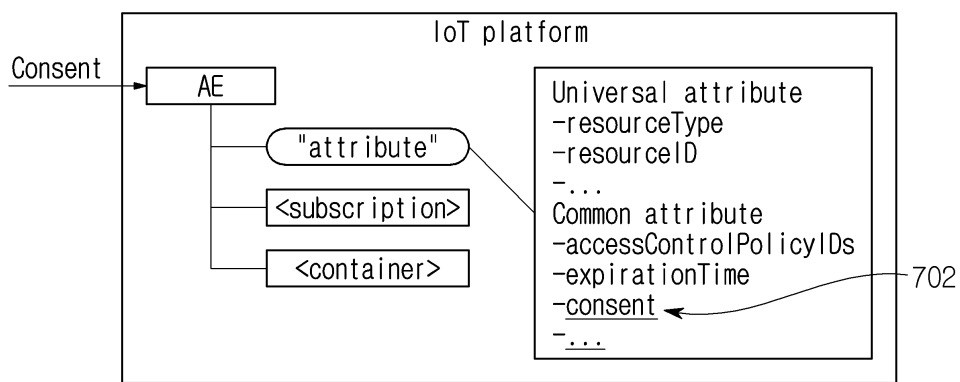
도면6b



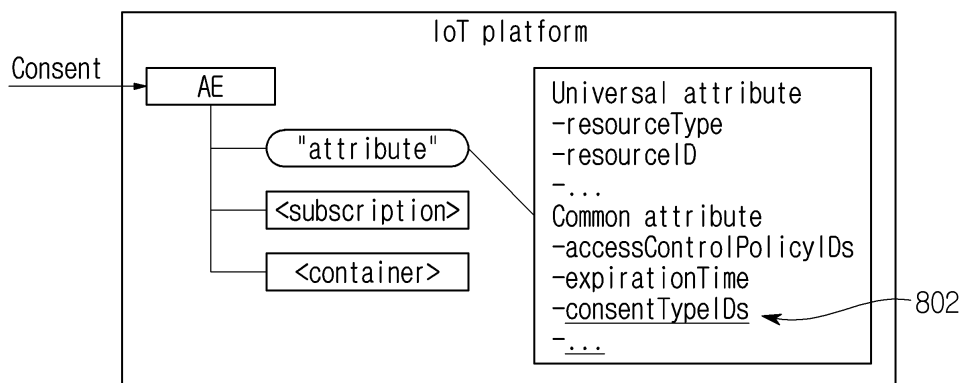
도면6c



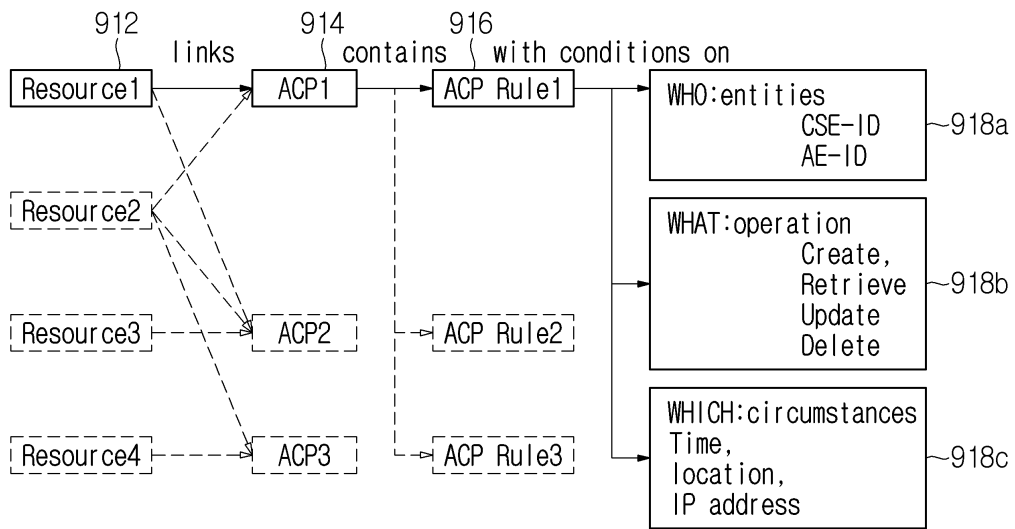
도면7



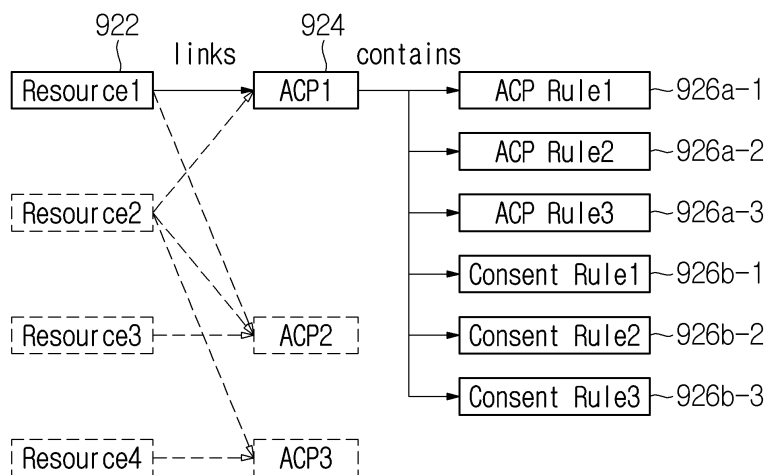
도면8



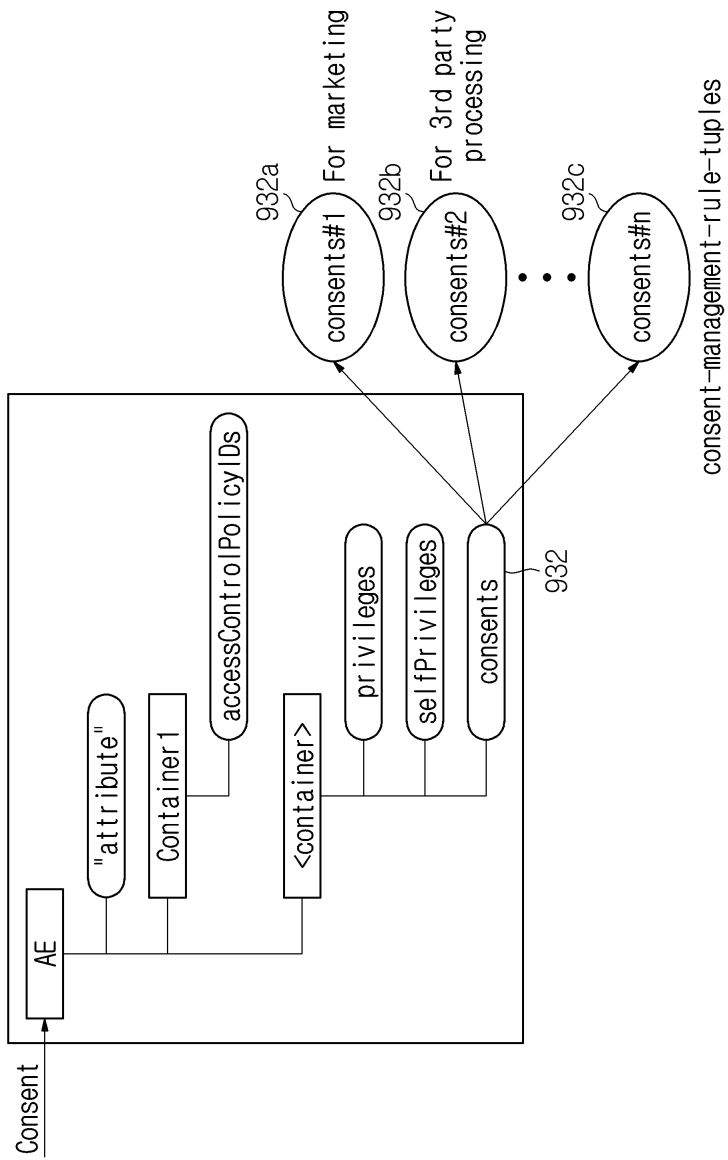
도면9a



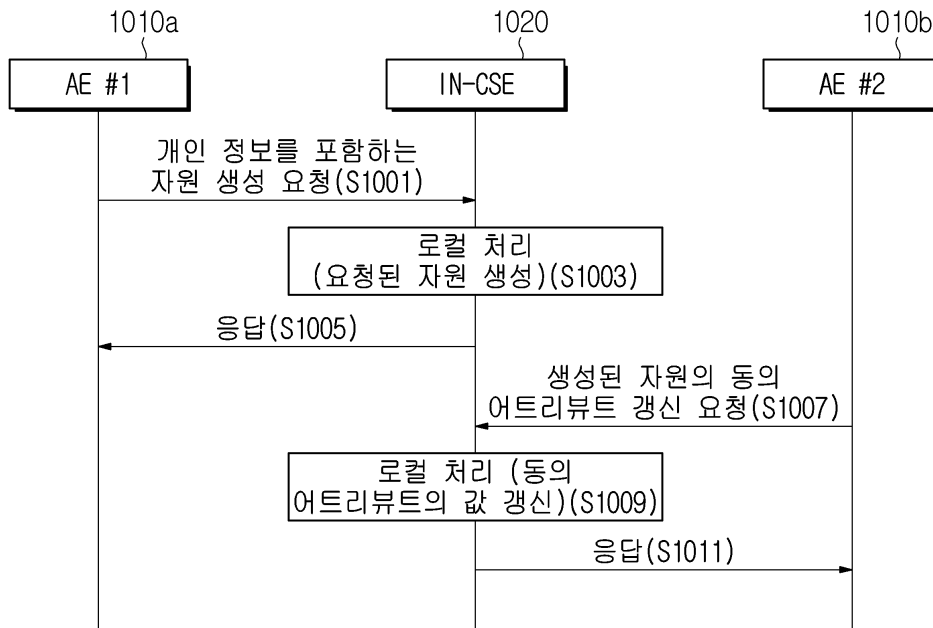
도면9b



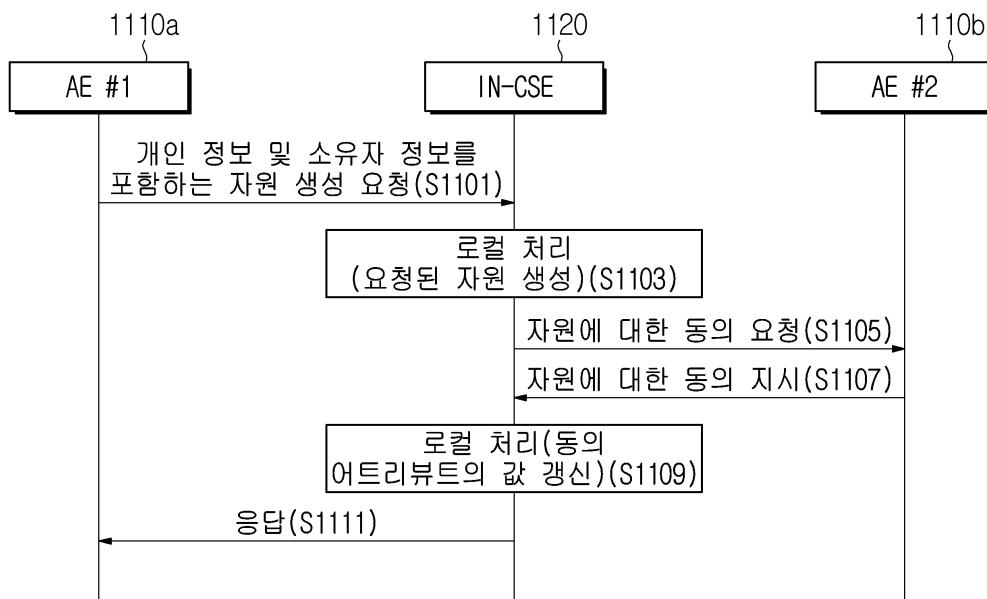
도면9c



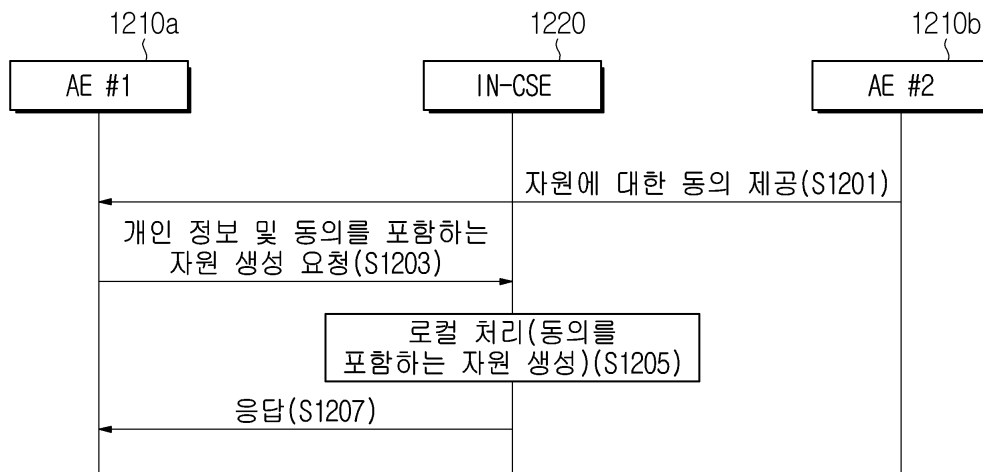
도면10



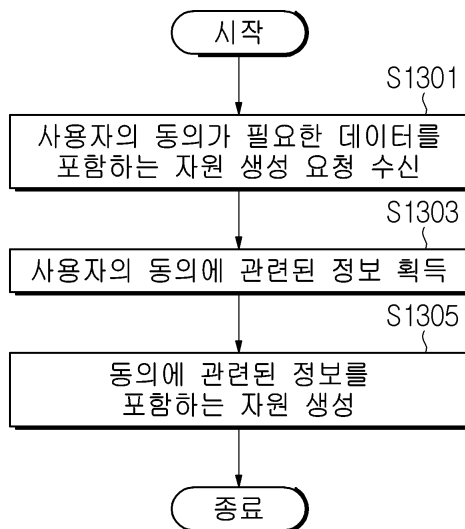
도면11



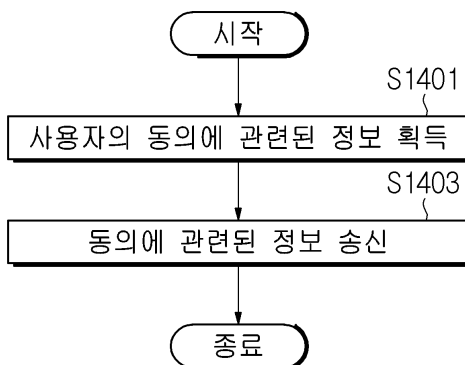
도면12



도면13



도면14



도면15

