(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0080296
(43) 공개일자 2023년06월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G16Y 10/75* (2020.01)
G16Y 30/10 (2020.01) *H04L 67/12* (2022.01)
(52) CPC특허분류
H04L 63/0876 (2013.01)
G16Y 10/75 (2020.01)
(21) 출원번호 10-2022-0118400
(22) 출원일자 2022년09월20일
심사청구일자 없음
(30) 우선권주장
63/283,586 2021년11월29일 미국(US)

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

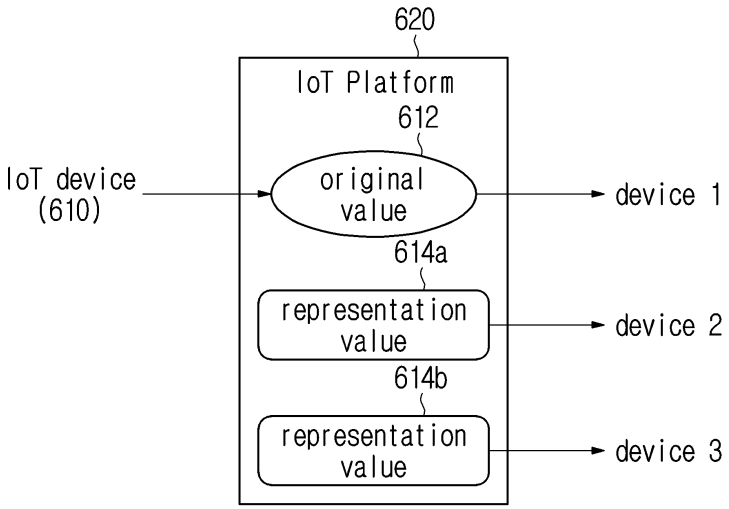
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **M2M 시스템에서 데이터를 보호하기 위한 방법 및 장치**

(57) 요 약

본 개시는 M2M(Machine-to-Machine) 시스템에서 데이터를 보호하기 위한 것으로, M2M(Machine-to-Machine) 시스템에서 제1 장치의 동작 방법은, 제2 장치로부터 상기 제2 장치에 의해 생성된 원본(original) 값을 포함하는 데이터를 수신하는 단계, 상기 원본 값에 대응하는 적어도 하나의 표현(representation) 값을 획득하는 단계, 및 상기 원본 값 및 상기 적어도 하나의 표현 값을 상기 제2 장치에 의해 생성되는 데이터를 저장하기 위한 자원에 저장하는 단계를 포함할 수 있다.

대 표 도 - 도6



(52) CPC특허분류
G16Y 30/10 (2020.01)
H04L 63/0428 (2013.01)
H04L 67/12 (2022.05)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711152795
과제번호 2019-0-00426
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보보호핵심원천기술개발사업[정보통신 · 방송연구개발사업]
연구과제명 IoT 기반 이식-침습형 고위험 의료장치를 위한 능동형 킬 스위치 및 바이오 마커 활용 방어 시스템 개발
기 여 율 1/1
과제수행기관명 국민대학교 산학협력단 (세종대학교 산학협력단)
연구기간 2019.04.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

M2M(Machine-to-Machine) 시스템에서 제1 장치의 동작 방법에 있어서,

제2 장치로부터 상기 제2 장치에 의해 생성된 원본(original) 값을 포함하는 데이터를 수신하는 단계;

상기 원본 값에 대응하는 적어도 하나의 표현(representation) 값을 획득하는 단계; 및

상기 원본 값 및 상기 적어도 하나의 표현 값을 상기 제2 장치에 의해 생성되는 데이터를 저장하기 위한 자원에 저장하는 단계를 포함하는 방법.

청구항 2

청구항 1에 있어서,

상기 자원을 생성하는 단계를 더 포함하며,

상기 자원은, 표현 값의 생성 및 저장에 대한 제1 정보, 상기 표현 값의 제공에 대한 제2 정보 중 적어도 하나를 포함하는 방법.

청구항 3

청구항 2에 있어서,

상기 자원은, 상기 제2 장치에 대한 등록 절차 중 생성되는 방법.

청구항 4

청구항 2에 있어서,

상기 제2 정보는, 상기 적어도 하나의 표현 값으로 응답할 데이터 요청을 식별하기 위한 정보로서, 접근 타입을 지시하는 방법.

청구항 5

청구항 1에 있어서,

제3 장치로부터 상기 자원에 저장된 데이터에 대한 검색 요청을 수신하는 단계;

상기 제3 장치가 상기 원본 값을 열람할 권한을 가지지 아니함을 확인하는 단계; 및

상기 검색 요청에 응하여, 상기 제3 장치에게 상기 적어도 하나의 표현 값 중 하나의 표현 값을 송신하는 단계를 더 포함하는 방법.

청구항 6

청구항 5에 있어서,

상기 제3 장치가 상기 원본 값을 열람할 권한을 가지지 아니함을 확인하는 단계는,

상기 제3 장치의 접근 타입(access type)에 기반하여 상기 제3 장치가 상기 제2 장치의 소유자(owner)와 무관한 장치임을 확인하는 단계를 포함하는 방법.

청구항 7

청구항 1에 있어서,

제4 장치로부터 상기 자원에 저장된 데이터에 대한 검색 요청을 수신하는 단계;

상기 제4 장치가 상기 원본 값을 열람할 권한을 가짐을 확인하는 단계; 및

상기 검색 요청에 응하여, 상기 제4 장치에게 상기 원본 값을 송신하는 단계를 더 포함하는 방법.

청구항 8

청구항 7에 있어서,

상기 제4 장치가 상기 원본 값을 열람할 권한을 가짐을 확인하는 단계는,

상기 제4 장치의 접근 타입(access type)에 기반하여 상기 제4 장치가 상기 제2 장치의 소유자(owner)와 관련된 장치임을 확인하는 단계를 포함하는 방법.

청구항 9

청구항 1에 있어서,

상기 자원은, 상기 원본 값을 저장하기 위한 하위 자원을 포함하며,

상기 하위 자원은, 상기 원본 값을 저장하기 위한 어트리뷰트 및 상기 적어도 하나의 표현 값을 저장하기 위한 어트리뷰트를 포함하는 방법.

청구항 10

청구항 1에 있어서,

상기 자원은, 상기 원본 값을 저장하기 위한 하위 자원 및 상기 적어도 하나의 표현 값을 저장하기 위한 하위 자원를 포함하는 방법.

청구항 11

M2M(Machine-to-Machine) 시스템에서 제1 장치에 있어서,

송수신기; 및

상기 송수신기와 연결된 프로세서를 포함하며,

상기 프로세서는,

제2 장치로부터 상기 제2 장치에 의해 생성된 원본(original) 값을 포함하는 데이터를 수신하고,

상기 원본 값에 대응하는 적어도 하나의 표현(representation) 값을 획득하고,

상기 원본 값 및 상기 적어도 하나의 표현 값을 상기 제2 장치에 의해 생성되는 데이터를 저장하기 위한 자원에 저장하도록 제어하는 제1 장치.

청구항 12

청구항 11에 있어서,

상기 프로세서는, 상기 자원을 생성하도록 제어하며,

상기 자원은, 표현 값의 생성 및 저장에 대한 제1 정보, 상기 표현 값의 제공에 대한 제2 정보 중 적어도 하나를 포함하는 제1 장치.

청구항 13

청구항 12에 있어서,

상기 자원은, 상기 제2 장치에 대한 등록 절차 중 생성되는 제1 장치.

청구항 14

청구항 12에 있어서,

상기 제2 정보는, 상기 적어도 하나의 표현 값으로 응답할 데이터 요청을 식별하기 위한 정보로서, 접근 타입을 지시하는 제1 장치.

청구항 15

청구항 11에 있어서,

상기 프로세서는,

제3 장치로부터 상기 자원에 저장된 데이터에 대한 검색 요청을 수신하고,

상기 제3 장치가 상기 원본 값을 열람할 권한을 가지지 아니함을 확인하고,

상기 검색 요청에 응하여, 상기 제3 장치에게 상기 적어도 하나의 표현 값 중 하나의 표현 값을 송신하도록 제어하는 제1 장치.

청구항 16

청구항 15에 있어서,

상기 프로세서는,

상기 제3 장치의 접근 타입(access type)에 기반하여 상기 제3 장치가 상기 제2 장치의 소유자(owner)와 무관한 장치임을 확인하는 제1 장치.

청구항 17

청구항 11에 있어서,

상기 프로세서는,

제4 장치로부터 상기 자원에 저장된 데이터에 대한 검색 요청을 수신하고,

상기 제4 장치가 상기 원본 값을 열람할 권한을 가짐을 확인하고,

상기 검색 요청에 응하여, 상기 제4 장치에게 상기 원본 값을 송신하도록 제어하는 제1 장치.

청구항 18

청구항 17에 있어서,

상기 프로세서는,

상기 제4 장치의 접근 타입(access type)에 기반하여 상기 제4 장치가 상기 제2 장치의 소유자(owner)와 관련된 장치임을 확인하는 제1 장치.

청구항 19

청구항 11에 있어서,

상기 자원은, 상기 원본 값을 저장하기 위한 하위 자원을 포함하며,

상기 하위 자원은, 상기 원본 값을 저장하기 위한 어트리뷰트 및 상기 적어도 하나의 표현 값을 저장하기 위한 어트리뷰트를 포함하는 제1 장치.

청구항 20

청구항 11에 있어서,

상기 자원은, 상기 원본 값을 저장하기 위한 하위 자원 및 상기 적어도 하나의 표현 값을 저장하기 위한 하위 자원를 포함하는 제1 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 M2M(Machine-to-Machine) 시스템에 관한 것으로, 보다 구체적으로, M2M 시스템에서 데이터를 보호하기 위한 방법 및 장치에 대한 것이다.

배 경 기 술

[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 개시는 M2M(Machine-to-Machine) 시스템에서 데이터를 효과적으로 보호하기 위한 방법 및 장치를 제공하는데 목적이 있다.

[0005] 본 개시는 M2M 시스템에서 데이터를 다중 값(multiple values)을 가지도록 저장하기 위한 방법 및 장치를 제공하는데 목적이 있다.

[0006] 본 개시는 M2M 시스템에서 다중 값의 데이터를 관리하기 위한 방법 및 장치를 제공하는데 목적이 있다.

[0007] 본 개시는 M2M 시스템에서 다중 값의 데이터에 대한 정보를 포함하는 자원을 관리하기 위한 방법 및 장치를 제공하는데 목적이 있다.

과제의 해결 수단

[0008] 본 개시의 일 실시예에 따르면, M2M(Machine-to-Machine) 시스템에서 제1 장치의 동작 방법은, 제2 장치로부터 상기 제2 장치에 의해 생성된 원본(original) 값을 포함하는 데이터를 수신하는 단계, 상기 원본 값에 대응하는 적어도 하나의 표현(representation) 값을 획득하는 단계, 및 상기 원본 값 및 상기 적어도 하나의 표현 값을 상기 제2 장치에 의해 생성되는 데이터를 저장하기 위한 자원에 저장하는 단계를 포함할 수 있다.

[0009] 본 개시의 일 실시예에 따르면, M2M(Machine-to-Machine) 시스템에서 제1 장치는, 송수신기, 및 상기 송수신기와 연결된 프로세서를 포함하며, 상기 프로세서는, 제2 장치로부터 상기 제2 장치에 의해 생성된 원본(original) 값을 포함하는 데이터를 수신하고, 상기 원본 값에 대응하는 적어도 하나의 표현(representation) 값을 획득하고, 상기 원본 값 및 상기 적어도 하나의 표현 값을 상기 제2 장치에 의해 생성되는 데이터를 저장하기 위한 자원에 저장하도록 제어할 수 있다.

발명의 효과

[0010] 본 개시에 따르면, M2M(Machine-to-Machine) 시스템에서 데이터가 효과적으로 보호될 수 있다.

[0011] 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

[0012] 도 1은 본 개시에 따른 M2M(Machine-to-Machine) 시스템의 계층 구조를 도시한다.

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

도 3은 본 개시에 따른 M2M 시스템에서 각각의 노드를 도시한다.

도 4는 본 개시에 따른 M2M 시스템에서 공통 서비스 펑션을 도시한다.

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

도 6은 본 개시에 따른 M2M 시스템에서 다중 값(multiple values)을 가지는 데이터의 개념을 도시한다.

도 7a 및 도 7b은 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터에 관련된 자원의 예들을 도시한다.

도 8은 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터를 처리하는 절차의 예를 도시한다.

도 9는 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터를 생성 및 발견하는 절차의 예를 도시한다.

도 10은 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터를 생성 및 발견하는 절차의 다른 예를 도시한다.

도 11은 본 개시에 따른 M2M 시스템에서 M2M 장치의 구성을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하에서는 첨부한 도면을 참고로 하여 본 개시의 실시예에 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 실시예에 한정되지 않는다.

[0014] 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 실시예에서의 제1 구성요소는 다른 실시예에서 제2 구성요소라고 칭할 수도 있고, 마찬가지로 일 실시예에서의 제2 구성요소를 다른 실시예에서 제1 구성요소라고 칭할 수도 있다.

[0015] 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.

[0016] 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 실시예도 본 개시의 범위에 포함된다.

[0017] 본 개시에 있어서, 다양한 실시예에서 설명하는 구성요소들이 반드시 필수적인 구성요소들은 의미하는 것은 아니며, 일부는 선택적인 구성요소일 수 있다. 따라서, 일 실시예에서 설명하는 구성요소들의 부분집합으로 구성되는 실시예도 본 개시의 범위에 포함된다. 또한, 다양한 실시예에서 설명하는 구성요소들에 추가적으로 다른 구성요소를 포함하는 실시예도 본 개시의 범위에 포함된다.

[0018] 본 개시의 실시예를 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.

[0019] 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.

[0020] 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 실시예로 한정되지 않는다.

[0021] 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.

[0022] 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 실시예로 한정되지 않는다.

[0023] 또한, 일 예로, 본 개시는 M2M 시스템을 중심으로 설명되지만 본 개시는 M2M 시스템에만 제한적으로 적용되는 것은 아니다.

[0024] 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 실시예로 한정되지 않는다.

[0026] 본 개시는 M2M(Machine-to-Machine) 시스템에서 데이터를 보호하기 위한 방법 및 장치에 대한 것이다. 보다 구체적으로, 본 개시는 M2M 시스템에서 데이터를 복수의 값들을 가지도록 저장하는 기술에 대해 설명한다.

[0028] oneM2M은 에너지, 교통, 국방, 공공서비스 등 산업별로 종속적이고 폐쇄적으로 운영되는, 파편 화된 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.

[0030] 도 1은 본 개시에 따른 M2M(Machine-to-Machine) 시스템의 계층 구조(layered structure)를 도시한다.

[0031] 도 1를 참조하면, M2M 시스템의 계층 구조는 어플리케이션 계층(110), 공통 서비스 계층(120), 네트워크 서비스 계층(120)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), 원거리 혈당 모니터링 어플리케이션(remote blood sugar monitoring application), 전략 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.

[0032] 공통 서비스 계층(120)은 공통 서비스 평션(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.

[0033] 공통 서비스 계층(120)은 기능에 의해 CSF로 그룹화되는 서비스들의 집합을 제공할 수 있다. 다수의 인스턴스화된 CSF들은 CSE들을 형성한다. CSE들은 어플리케이션들(예: oneM2M 명명법에서 어플리케이션 엔티티들 또는 AE들), 다른 CSE들 및 기저 네트워크들(예: oneM2M 명명법에서 네트워크 서비스 엔티티 또는 NSE)과 인터페이스할 수 있다.

[0034] 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.

[0036] 도 2는 본 개시에 따른 M2M 시스템에서 기준점(reference point)을 도시한다.

[0037] 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.

[0039] 도 3은 본 개시에 따른 M2M 시스템에서 각각의 노드를 도시한다.

[0040] 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.

[0041] 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 연

결되는 노드일 수 있다. 일 예로, ASN은 하드웨어적으로 M2M 단말에 설정되는 노드일 수 있다.

[0042] 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.

[0043] 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.

[0045] 도 4는 본 개시에 따른 M2M 시스템에서 공통 서비스 펑션을 도시한다.

[0046] 도 4를 참조하면, 공통 서비스 펑션들이 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 CSF을 제공할 수 있다. 이때, 공통 서비스 펑션에 기초하여 M2M 단말들이 동작할 수 있다. 또한, 공통 서비스 펑션은 다른 실시예도 가능할 수 있으며, 상술한 실시예로 한정되지 않는다.

[0047] 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.

[0048] 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.

[0049] 데이터 관리 및 저장(406) CSF는 데이터 저장 및 중재 기능들(예: 집결을 위한 데이터 수집, 데이터 리포맷팅, 및 분석 및 시멘틱 처리를 위한 데이터 저장)을 제공한다.

[0050] 장치 관리(408) CSF는 M2M 게이트웨이들 및 M2M 디바이스들 상에서 디바이스 능력들의 관리를 제공한다.

[0051] 발견(410) CSF는 필터 기준들에 기초하여 어플리케이션들 및 서비스들에 대한 정보를 검색하는 기능을 제공한다.

[0052] 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.

[0053] 위치(414) CSF는 AE들이 지리적 장소 정보를 획득하는 것을 가능하게 하는 기능을 제공한다.

[0054] 네트워크 서비스 노출/서비스 실행 및 트리거링(416) CSF는 네트워크 서비스 기능들에 액세스하기 위한 기저 네트워크들과의 통신들을 관리한다.

[0055] 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.

[0056] 보안(420) CSF는 식별, 인증, 및 허가를 포함하는 액세스 제어와 같은 서비스 레이어에 대한 보안 기능들을 제공한다.

[0057] 서비스 과금 및 계산(422) CSF는 서비스 레이어에 대한 과금 기능들을 제공한다.

[0058] 구독/통지(424) CSF는 이벤트에 가입하는 것을 허용하고, 해당 이벤트가 발생할 때 통지되는 기능을 제공한다.

[0060] 도 5는 본 개시에 따른 M2M 시스템에서 송신자 및 수신자가 메시지를 교환하는 방법을 도시한다.

[0061] 도 5를 참조하면, 발생자(originator, 510)는 요청 메시지를 수신자(receiver, 520)로 전송할 수 있다. 이때, 발생자(510)와 수신자(520)는 상술한 M2M 단말일 수 있다. 다만, M2M 단말에 한정되지 않고, 발생자(510)와 수신자(520)는 다른 단말일 수 있으며, 상술한 실시예로 한정되지 않는다. 또한, 일 예로, 발생자(510) 및 수신자(520)는 상술한 노드, 엔티티, 서버 또는 게이트웨이일 수 있다. 즉, 발생자(510) 및 수신자(520)는 하드웨어적인 구성 또는 소프트웨어적인 구성일 수 있으며, 상술한 실시예로 한정되지 않는다.

[0062] 이때, 일 예로, 발생자(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 발생자(510)에 대한 파라미터일 수 있다. 또한, 수신단 관련 파라미터는 수신자(520)에 대한 파라미터일 수 있다. 또한, 식별 파라미터는 상호 간의 식별을 위해 요구되는 파라미터일 수 있다.

[0063] 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.

[0064] 이때, 수신자(520)는 발생자(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.

[0065] 일 예로, 이벤트가 발생하는 경우, 발생자(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 발생자(510)로 다시 전송할 수 있다.

[0066] 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, 발생자(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.

[0068] 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

[0069]

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

[0070] 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

[0071]

Condition tag	Multiplicity	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

[0072]

Condition tag	Multip-licity	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.

[0073] 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

[0074]

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

[0075] 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 자원

으로 이해될 수 있다.

[0076] 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.

[0077] 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 자원으로의 링크(link)를 포함한다.

[0078] 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.

[0079] 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.

[0081] 데이터 유출(data leakage)은 IoT 시스템에서 중요한 이슈이다. 익명화(anonymization) 및 가명화(pseudonymization)는 개인 정보를 은닉하기 위한 기술들이다. 그러나, 데이터 보호를 지원하기 위한 다른 방법들이 존재할 수 있다. 단일 자원(예: <contantInstance>)에 대해 다중 값들(multiple values)를 가지는 것을 허용하는 것이 대안이 될 수 있다.

[0082] 다양한 실시예들에 따른 데이터 보호 기술의 기본적 개념은 단일 측정에 대하여 다중 값들을 생성하는 것을 사용자들에게 허용하는 것이다. 데이터의 소유자는 어플리케이션 측정에서 다중 데이터 포인트들을 생성할 수 있다. 각 컨텐트 값은, 서로 다른 접근 타입(access type)을 가지고, 이로 인해 어플리케이션이 특정 접근 타입에 따라 다른 값을 볼 수 있다.

[0084] 도 6은 본 개시에 따른 M2M 시스템에서 다중 값(multiple values)을 가지는 데이터의 개념을 도시한다. 도 6을 참고하면, IoT 플랫폼(620)은 IoT 장치(610)에의해 생성된 원본 값(612)을 가지는 데이터를 수신하고, 저장한다. 이때, IoT 플랫폼(620)은 원본 값(612)을 보호하기 위해, 표현 값(representation value)들(614a, 614b)를 생성하고, 함께 저장한다. 도 6은 2개의 표현 값들(614a, 614b)을 예로 보여주고 있으나, 하나의 원본 값(612)에 대하여 하나 또는 셋 이상의 표현 값들이 저장될 수 있다. 이에 따라, 해당 데이터에 대한 검색 요청이 발생하는 경우, IoT 플랫폼(620)은 정해진 기준에 따라 어느 장치(예: 장치1)에게 원본 값(612)을, 다른 장치들(예: 장치2, 장치3)에게 표현 값들(614a, 614b) 중 하나를 제공할 수 있다. 이에 따라, 다른 장치들로부터 원본 값(612)이 보호될 수 있다.

[0086] 다양한 실시예들에 따라, 다중 값들을 가지는 데이터의 생성에 대한 2가지 옵션들이 적용될 수 있다. 제1 옵션은 표현 값을 생성하는 것이다. 제1 옵션에 따르면, 특정 멤버들을 제외한 모든 요청은 표현 값을 볼 것이고, 표현 값은 컨테이너 내에 정의될 수 있다. 제2 옵션은 자원(예: <contentInstance>) 내에서 다중 값들을 지원하는 것이다. 제2 옵션에 따르면, 원본 값(original value)는 제1 어트리뷰트(예: 'content')에 저장되고, 표현 값은 제2 어트리뷰트(예: 'representationContent')에 저장될 수 있다. 그리고, 표현 값을 저장하는 제2 어트리뷰트는 하나 또는 그 이상 생성될 수 있고, 이 경우, 소유자는 누가 어느 어트리뷰트 내의 컨텐트를 볼 수 있는지 정의할 수 있다. 예를 들어, 소유자는 실제 컨텐트(actual content)를 볼 수 있는 반면, 패밀리 멤버는 표현 값을 저장하는 어트리뷰트(예: 'representationContent1')에 저장된 값을 보고, 다른이들은 다른 표현 값을 저장하는 어트리뷰트(예: 'representationContent2')에 저장된 값을 볼 수 있다.

[0088] 도 7a 및 도 7b은 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터에 관련된 자원의 예들을 도시한다. 도 7a는 제1 옵션에 따른 자원 구조를, 도 7b은 제2 옵션에 따른 자원 구조를 예시한다.

[0089] 도 7a를 참고하면, 어플리케이션의 소유자는 자원 <representationInstance>(713)를 포함하는 자원 <container>(710)를 생성한다. 자원 <container>(710)은 어트리뷰트 <accessTypeRepresentation>(711)을 더 포함할 수 있다. 어트리뷰트 <accessTypeRepresentation>(711)는 어느 접근(access)이 <representationInstance>(713)를 볼 것인지를 정의한다. 즉, 어트리뷰트 <accessTypeRepresentation>(711)는 표현 값을 보여주도록 지정된 접근 타입을 지시할 수 있다. 다른 실시 예에 따라, 어트리뷰트 <accessTypeRepresentation>(711)는 원본 값을 보여주도록 지정된 접근 타입을 지시할 수 있다.

[0090] 도 7b를 참고하면, 어플리케이션의 소유자는 어트리뷰트 'representationContent'(726)를 포함하는 자원 <contentInstance>(724)을 생성한다. 자원 <contentInstance>(724)은 원본 값을 포함하는 어트리뷰트 'content'(725)를 더 포함한다. 자원 <contentInstance>(724)은 자원 <Container>(720)에 포함되며, 자원 <Container>(720)는 어트리뷰트 'accessTypeRpresentation'(721)를 포함한다. 어트리뷰트 'accessTypeRpresentation'(721)은, 어느 접근(access)이 어트리뷰트 'content'(725)가 아닌 어트리뷰트 'representationContent'(726) 내의 값을 누가 볼 것인지를 정의한다.

[0092] 도 8은 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터를 처리하는 절차의 예를 도시한다. 도 8의 동작 주체는 자원을 관리하는(예: CSE)일 수 있다. 이하 설명에서, 도 8의 동작 주체는 '장치'라 지칭된다.

[0093] 도 8을 참고하면, S801 단계에서, 장치는 IoT 장치로부터 원본 값을 가지는 데이터를 수신한다. IoT 장치는 동작 중 데이터를 생성하는 장치(예: 센서)이며, 생성된 데이터를 자원에 저장하기 위해 송신한다. 이때, 장치는 IoT 장치의 데이터를 저장하기 위한 자원을 가지고 있다. 일 실시예에 따라, 자원은 다중 값 저장에 관련된 정보를 포함할 수 있다.

[0094] S803 단계에서, 장치는 원본 값 및 적어도 하나의 표현 값을 저장한다. 즉, 장치는 IoT 장치로부터 수신된 원본 값은 물론, 원본 값을 보호하기 위한 적어도 하나의 표현 값을 저장할 수 있다. 이를 위해, 일 실시예에 따라, 장치는 원본 값에 대응하는 적어도 하나의 표현 값을 생성할 수 있다. 다른 실시예에 따라, 적어도 하나의 표현 값은 다른 장치에 의해 생성될 수 있다. 이 경우, 장치는 다른 장치에게 적어도 하나의 표현 값을 생성할 것을 요청하고, 적어도 하나의 표현 값을 수신할 수 있다. 이때, 장치는 다른 장치에게 원본 값에 관련된 정보를 제공할 수 있다. 다양한 실시예들에 따라, 적어도 하나의 표현 값은 원본 값, 랜덤 변수 중 적어도 하나에 기반하여 생성될 수 있다.

[0095] S805 단계에서, 장치는 데이터 검색에 대한 요청을 수신한다. 다시 말해, 장치는 S803 단계에서 저장된 데이터의 검색을 요청하는 메시지를 송신할 수 있다. 데이터 검색에 대한 요청은 원본 값을 송신한 IoT 장치와 다른 장치로부터 수신될 수 있다.

[0096] S807 단계에서, 장치는 원본에 대한 열람이 허용되는지 판단한다. 다시 말해, 장치는 데이터 검색을 요청한 다른 장치가 데이터의 원본 값을 열람할 권한을 가지는지 여부를 판단할 수 있다. 원본 값을 열람할 권한을 가지는지 여부는 IoT 장치에 관련된 자원에 포함되는 접근 타입에 관련된 정보에 기반하여 판단될 수 있다. 즉, 장치는 IoT 장치에 관련된 자원에 포함되는 정보에 기반하여 데이터 검색을 요청한 다른 장치에게 원본 값을 송신할지 여부를 판단한다.

[0097] 만일, 원본에 대한 열람이 허용되면, S809 단계에서, 장치는 원본 값을 송신한다. 즉, 데이터 검색을 요청한 다른 장치가 원본에 대한 열람 권한을 가지는 경우, 장치는 원본 값을 포함하는 데이터를 송신할 수 있다. 다시 말해, 장치는 S805 단계에서의 요청에 응하여 원본 값을 송신한다.

[0098] 반면, 원본에 대한 열람이 허용되지 아니하면, S811 단계에서, 장치는 표현 값을 송신한다. 여기서, 복수의 표현 값들이 저장된 경우, 장치는 복수의 표현 값들을 하나를 선택하고, 선택된 표현 값을 송신할 수 있다. 또는, 장치는 복수의 표현 값들에 기반하여 새로운 표현 값을 생성하고, 생성된 표현 값을 송신할 수 있다.

[0099] 도 8을 참고하여 설명한 실시예와 같이, 표현 값을 이용하여 원본 값이 보호될 수 있다. 이를 위해, 도 8의 절차에 앞서, 원본 값 및 적어도 하나의 표현 값을 포함하는 다중 값을 가지도록 데이터를 저장하는 동작(이하 '다중 값 저장')에 대한 설정이 수행될 수 있다. 일 실시예에 따라, 다중 값 저장에 대한 설정은 IoT 장치의 등록 절차 중 수행될 수 있다. 구체적으로, IoT 장치에 의해 생성되는 데이터를 저장하기 위한 자원 내에 다중 값 저장에 대한 설정 정보가 부가될 수 있다.

[0100] 일 실시예에 따라, 설정 정보는 표현 값의 생성 및 저장에 대한 정보, 표현 값의 제공에 대한 정보 중 적어도

하나를 포함할 수 있다. 예를 들어, 표현 값의 생성 및 저장에 대한 정보는 표현 값의 생성 시점, 하나의 원본 값에 대응하는 표현 값들의 개수, 표현 값들의 생성 알고리즘 중 적어도 하나를 지시할 수 있다. 또한, 표현 값의 제공에 대한 정보는 표현 값으로 응답할 데이터 요청을 식별하기 위한 정보(예: 장치, 장치 타입, 접근 타입 등)를 지시할 수 있다.

[0102] 도 9는 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터를 생성 및 발견하는 절차의 예를 도시한다. 도 9는 데이터를 생성하는 센서(910), 센서(910)에 의해 생성된 데이터를 자원에 저장하는 서버 IN-CSE(920), 데이터 검색을 요청하는 어플리케이션(930) 간 신호 교환을 예시한다.

[0103] 도 9를 참고하면, S901 단계에서, 센서(910) 및 서버 IN-CSE(920) 등록 절차를 수행한다. 이를 위해, 센서(910)는 서버 IN-CSE(920)에게 등록에 관련된 적어도 하나의 메시지를 송신하고, 서버 IN-CSE(920)로부터 등록에 관련된 적어도 하나의 메시지를 수신할 수 있다. 이때, 센서(910) 및 서버 IN-CSE(920) 간 데이터를 다중 값들로 저장하는 것에 대한 설정이 부가된다. 즉, 서버 IN-CSE(920)는 센서(910)에 의해 생성된 데이터를 저장 시 원본 값은 물론 적어도 하나의 표현 값을 함께 저장할 것을 설정한다. 또한, 설정은 원본 값에 대한 열람이 허용되는 장치들을 식별하기 위한 정보를 포함할 수 있다.

[0104] S903 단계에서, 센서(910) 및 서버 IN-CSE(920)는 표현 값을 저장하기 위한 자원(예: <representationInstance>)을 생성하기 위한 절차를 수행한다. 여기서, 표현 값을 저장하기 위한 자원(이하 '표현 값 자원')은 다양한 원본 값들에 대하여 공동적으로 사용될 수 있다. 따라서, 표현 값 자원은 원본 값을 포함하는 자원을 생성하기에 앞서 생성될 수 있다. 즉, 원본 값이 아직 존재하지 아니하더라도, 서버 IN-CSE(920)는 표현 값 자원을 생성할 수 있다. 나아가, 서버 IN-CSE(920)는 적어도 하나의 표현 값을 생성하고, 표현 값 자원에 저장할 수 있다.

[0105] S905 단계에서, 센서(910) 및 서버 IN-CSE(920)는 원본 값을 포함하는 데이터를 저장하기 위한 자원(예: <contentInstance>)을 생성하기 위한 절차를 수행한다. 다시 말해, 서버 IN-CSE(920)는 표현 값 자원과 관련되는 원본 값을 포함하는 데이터를 저장하기 위한 자원(이하 '원본 값 자원')을 생성한다. 예를 들어, 센서(910)는 서버 IN-CSE(920)에게 원본 값을 포함하는 데이터를 송신하고, 서버 IN-CSE(920)는 원본 값 자원을 생성하고, 원본 값 자원에 원본 값을 저장할 수 있다. 원본 값은 센서(910)의 동작 중 발생하는 데이터로서, 센서(910)의 종류에 따라 지시 대상이 달라질 수 있다. 원본 값은 본 개시에서 제안하는 기술에 의한 보호 대상이며, 표현 값들과 같은 종류의 정보를 가진다. 이때, 도 9에 도시되지 아니하였으나, 서버 IN-CSE(920)는 원본 값에 대응하는 적어도 하나의 표현 값을 생성하고, 생성된 적어도 하나의 표현 값을 표현 값 자원에 저장할 수 있다. 도 9에서, 원본 값 자원의 생성은 1회로 예시되었으나, 시간의 흐름에 따라 복수의 원본 값들이 생성될 수 있고, 이때마다 S905 단계가 반복적으로 수행될 수 있다.

[0106] S907 단계에서, 어플리케이션(930)은 서버 IN-CSE(920)에게 원본 값 자원(예: <contentInstance>)에 대한 검색 요청을 송신한다. 검색 요청과 함께, 어플리케이션(930)은 S905 단계에서 생성된 원본 값 자원에 포함되는 데이터를 특정하는 정보를 송신할 수 있다. 그리고, 어플리케이션(930)은 어플리케이션(930)의 접근 타입에 관련된 정보를 송신할 수 있다.

[0107] S909 단계에서, 서버 IN-CSE(920)는 센서(910)에 의해 생성된 원본 값에 대한 열람 권한을 가지는 장치를 식별하기 위한 정보(예: 어트리뷰트 'accessTypeRepresentation')를 검사한다. 원본 값에 대한 열람 권한을 가지는 장치를 식별하기 위한 정보(이하 '열람 권한 정보')는 S901 단계에서 생성된 자원에 포함된다. 열람 권한 정보는 원본 값에 대한 열람 권한을 가지는 장치 또는 장치의 종류 또는 특성을 지시하거나, 또는 원본 값을 대신하여 표현 값을 열람하는 장치 또는 장치의 종류 또는 특성을 지시할 수 있다. 여기서, 특성은 접근 타입을 포함할 수 있다. 이 경우, 서버 IN-CSE(920)는 어플리케이션(930)의 접근 타입이 열람 권한 정보에 의해 표현 값을 보여주도록 지정된 접근 타입인지를 판단할 수 있다. 본 실시예에서, 어플리케이션(930)의 접근 타입이 열람 권한 정보에 의해 표현 값을 보여주도록 지정된 접근 타입에 속한다. 즉, 서버 IN-CSE(920)는 접근 타입에 대한 검사를 통해 어플리케이션(930)이 센서(910)의 소유자와 무관함을 확인한다.

[0108] S911 단계에서, 서버 IN-CSE(920)는 어플리케이션(930)에게 표현 값 자원에 포함된 표현 값을 반환한다. 즉, 서버 IN-CSE(920)는 어플리케이션(930)에게 표현 값 자원에 포함된 적어도 하나의 표현 값 중 하나를 송신한다. 이에 따라, 서버 IN-CSE(920)는 어플리케이션(930)으로부터 원본 값을 보호할 수 있다.

[0110] 도 10은 본 개시에 따른 M2M 시스템에서 다중 값을 가지는 데이터를 생성 및 발견하는 절차의 다른 예를 도시한다. 도 10은 데이터를 생성하는 센서(1010), 센서(1010)에 의해 생성된 데이터를 자원에 저장하는 서버 IN-CSE(1020), 데이터 검색을 요청하는 어플리케이션(1030) 간 신호 교환을 예시한다.

[0111] 도 10을 참고하면, S1001 단계에서, 센서(1010) 및 서버 IN-CSE(1020) 등록 절차를 수행한다. 이를 위해, 센서(1010)는 서버 IN-CSE(1020)에게 등록에 관련된 적어도 하나의 메시지를 송신하고, 서버 IN-CSE(1020)로부터 등록에 관련된 적어도 하나의 메시지를 수신할 수 있다. 이때, 센서(1010) 및 서버 IN-CSE(1020) 간 데이터를 다중 값들로 저장하는 것에 대한 설정이 부가된다. 즉, 서버 IN-CSE(1020)는 센서(1010)에 의해 생성된 데이터를 저장 시 원본 값은 물론 적어도 하나의 표현 값을 함께 저장할 것을 설정한다. 또한, 설정은 원본 값에 대한 열람이 허용되는 장치들을 식별하기 위한 정보를 포함할 수 있다.

[0112] S1003 단계에서, 센서(1010) 및 서버 IN-CSE(1020)는 표현 값을 저장하기 위한 어트리뷰트(예: 'representationContent')을 포함하는 원본 값을 포함하는 데이터를 저장하기 위한 자원(예: <contentInstance>)을 생성하기 위한 절차를 수행한다. 다시 말해, 서버 IN-CSE(1020)는 원본 값을 저장하기 위한 어트리뷰트(예: 'content')(이하, '원본 값 어트리뷰트') 및 표현 값을 저장하기 위한 어트리뷰트(이하, '표현 값 어트리뷰트')를 포함하는 자원(이하 '컨텐트 자원')을 생성한다. 예를 들어, 센서(1010)는 서버 IN-CSE(1020)에게 원본 값을 포함하는 데이터를 송신하고, 서버 IN-CSE(1020)는 컨텐트 자원을 생성하고, 원본 값 어트리뷰트에 원본 값을, 표현 값 어트리뷰트에 표현 값을 저장할 수 있다. 원본 값은 센서(1010)의 동작 중 발생하는 데이터로서, 센서(1010)의 종류에 따라 지시 대상이 달라질 수 있다. 원본 값은 본 개시에서 제안하는 기술에 의한 보호 대상이며, 표현 값들과 같은 종류의 정보를 가진다.

[0113] S1005 단계에서, 어플리케이션(1030)은 서버 IN-CSE(1020)에게 컨텐트 자원(예: <contentInstance>)에 대한 검색 요청을 송신한다. 검색 요청과 함께, 어플리케이션(1030)은 S1003 단계에서 생성된 컨텐트 자원에 포함되는 데이터를 특정하는 정보를 송신할 수 있다. 그리고, 어플리케이션(1030)은 어플리케이션(1030)의 접근 타입에 관련된 정보를 송신할 수 있다.

[0114] S1007 단계에서, 서버 IN-CSE(1020)는 센서(1010)에 의해 생성된 원본 값에 대한 열람 권한을 가지는 장치를 식별하기 위한 정보(예: 어트리뷰트 'accessTypeRepresentation')를 검사한다. 원본 값에 대한 열람 권한을 가지는 장치를 식별하기 위한 정보(이하 '열람 권한 정보')는 S1001 단계에서 생성된 자원에 포함된다. 열람 권한 정보는 원본 값에 대한 열람 권한을 가지는 장치 또는 장치의 종류 또는 특성을 지시하거나, 또는 원본 값을 대신하여 표현 값을 열람하는 장치 또는 장치의 종류 또는 특성을 지시할 수 있다. 여기서, 특성은 접근 타입을 포함할 수 있다. 이 경우, 서버 IN-CSE(1020)는 어플리케이션(1030)의 접근 타입이 열람 권한 정보에 의해 표현 값을 보여주도록 지정된 접근 타입인지를 판단할 수 있다. 본 실시예에서, 어플리케이션(1030)의 접근 타입이 열람 권한 정보에 의해 표현 값을 보여주도록 지정된 접근 타입에 속한다.

[0115] S1009 단계에서, 서버 IN-CSE(1020)는 어플리케이션(1030)에게 표현 값 어트리뷰트에 포함된 표현 값을 반환한다. 즉, 서버 IN-CSE(1020)는 어플리케이션(1030)에게 표현 값 어트리뷰트에 포함된 적어도 하나의 표현 값 중 하나를 송신한다. 이에 따라, 서버 IN-CSE(1020)는 어플리케이션(1030)으로부터 원본 값을 보호할 수 있다.

[0116] S1011 단계에서, 어플리케이션(1040)은 서버 IN-CSE(1020)에게 컨텐트 자원(예: <contentInstance>)에 대한 검색 요청을 송신한다. 검색 요청과 함께, 어플리케이션(1040)은 S1003 단계에서 생성된 컨텐트 자원에 포함되는 데이터를 특정하는 정보를 송신할 수 있다. 그리고, 어플리케이션(1040)은 어플리케이션(1040)의 접근 타입에 관련된 정보를 송신할 수 있다.

[0117] S1013 단계에서, 서버 IN-CSE(1020)는 센서(1010)에 의해 생성된 원본 값에 대한 열람 권한을 가지는 장치를 식별하기 위한 정보(예: 어트리뷰트 'accessTypeRepresentation')를 검사한다. 원본 값에 대한 열람 권한을 가지는 장치를 식별하기 위한 정보(이하 '열람 권한 정보')는 S1001 단계에서 생성된 자원에 포함된다. 열람 권한 정보는 원본 값에 대한 열람 권한을 가지는 장치 또는 장치의 종류 또는 특성을 지시하거나, 또는 원본 값을 대신하여 표현 값을 열람하는 장치 또는 장치의 종류 또는 특성을 지시할 수 있다. 여기서, 특성은 접근 타입을 포함할 수 있다. 이 경우, 서버 IN-CSE(1020)는 어플리케이션(1040)의 접근 타입이 열람 권한 정보에 의해 표현 값을 보여주도록 지정된 접근 타입인지를 판단할 수 있다. 본 실시예에서, 어플리케이션(1040)의 접근 타입이 열람 권한 정보에 의해 원본 값을 보여주도록 지정된 접근 타입에 속한다. 즉, 서버 IN-CSE(1020)는 접근 타입에 대한 검사를 통해 어플리케이션(1040)이 센서(1010)의 소유자과 관련됨을 확인한다.

[0118] S1015 단계에서, 서버 IN-CSE(1020)는 어플리케이션(1040)에게 원본 값 어트리뷰트에 포함된 원본 값을 반환한

다. 즉, 서버 IN-CSE(1020)는 어플리케이션(1040)에게 원본 값을 송신한다.

[0120] 도 11은 본 개시에 따른 M2M 시스템에서 M2M 장치의 구성을 도시한다. 도 11에 도시된 M2M 장치(1110) 또는 M2M 장치(1120)는 전술한 AE, CSE, 서버 중 적어도 하나의 기능을 수행하는 하드웨어로 이해될 수 있다.

[0121] 도 11을 참고하면, M2M 장치(1110)는 장치를 제어하는 프로세서(1111) 및 신호를 송수신하는 송수신부(1114)를 포함할 수 있다. 이때, 프로세서(1111)는 송수신부(1114)를 제어할 수 있다. 또한, M2M 장치(1110)는 다른 M2M 장치(1120)와 통신을 수행할 수 있다. 다른 M2M 장치(1120)도 프로세서(1122) 및 송수신부(1124)를 포함할 수 있으며, 프로세서(1122) 및 송수신부(1124)는 프로세서(1111) 및 송수신부(1114)와 동일한 기능을 수행할 수 있다.

[0122] 일 예로, 상술한 송신자, 수신자, AE, CSE는 각각 도 11의 M2M 장치들(1110 및 1120) 중 하나일 수 있다. 또한, 도 11의 장치들(1110 및 1120)은 다른 장치일 수 있다. 일 예로, 도 11의 장치들(1110 및 1120)은 통신을 수행하는 장치, 자동차 또는 기지국 등과 같은 장치일 수 있다. 즉, 도 11의 장치들(1110 및 1120)은 통신을 수행할 수 있는 장치를 지칭하는 것으로 상술한 실시 예로 한정되지 않는다.

[0124] 상술한 본 개시의 실시예들은 다양한 수단을 통해 구현될 수 있다. 일 예로, 본 개시의 실시예들은 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다.

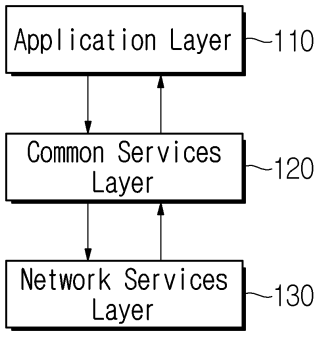
[0125] 상술한 바와 같이 개시된 본 개시의 바람직한 실시형태에 대한 상세한 설명은 당업자가 본 개시를 구현하고 실시할 수 있도록 제공되었다. 상기에서는 본 개시의 바람직한 실시 형태를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 개시의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 개시를 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다. 따라서, 본 개시는 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다. 또한, 이상에서는 본 명세서의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 명세서는 상술한 특정의 실시예에 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.

[0126] 그리고 당해 명세서에서는 물건 발명과 방법 발명이 모두 설명되고 있으며, 필요에 따라 양 발명의 설명은 보충적으로 적용될 수 있다.

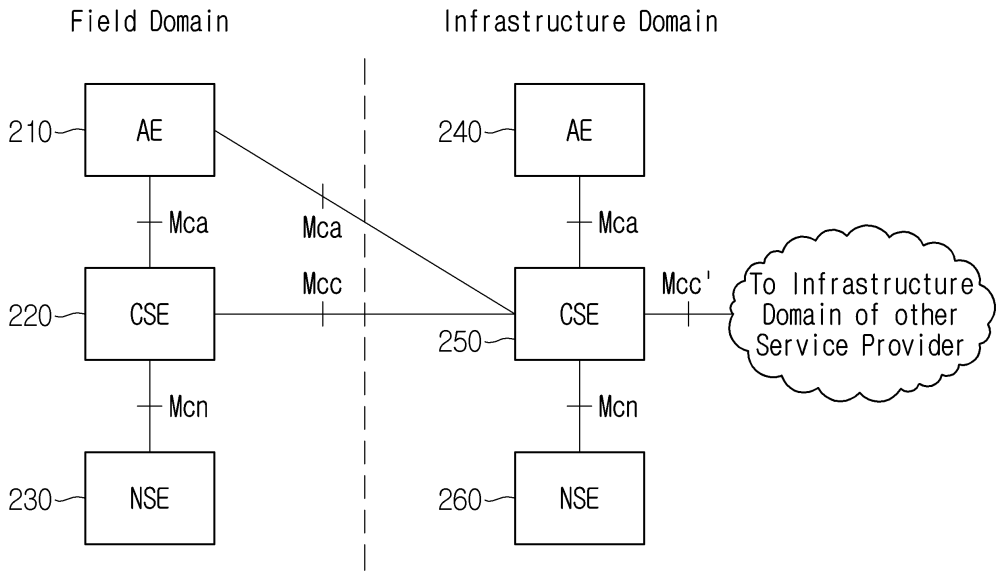
[0127] 또한, 본 개시에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 개시이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 개시이 본 개시의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 개시의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 개시에 포함된 것으로 해석되어야 할 것이다.

도면

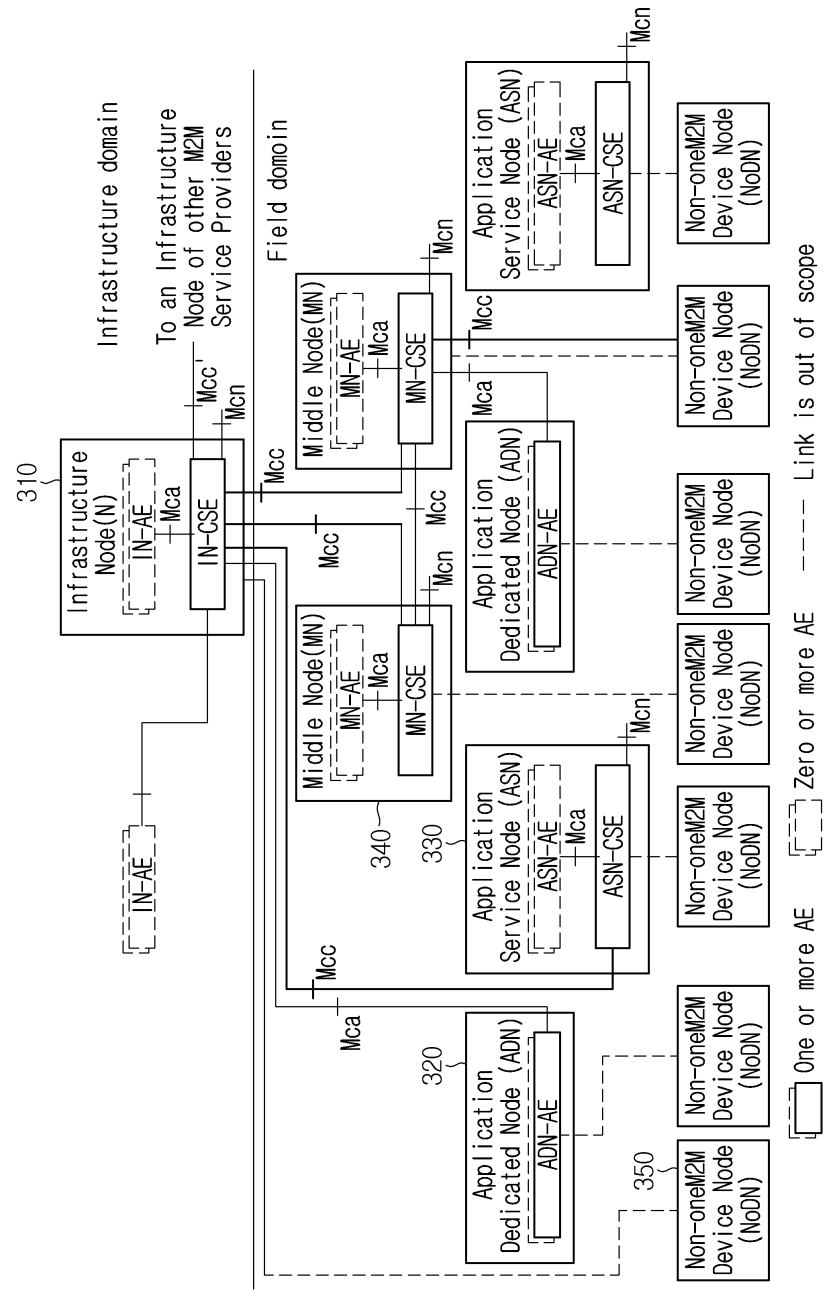
도면1



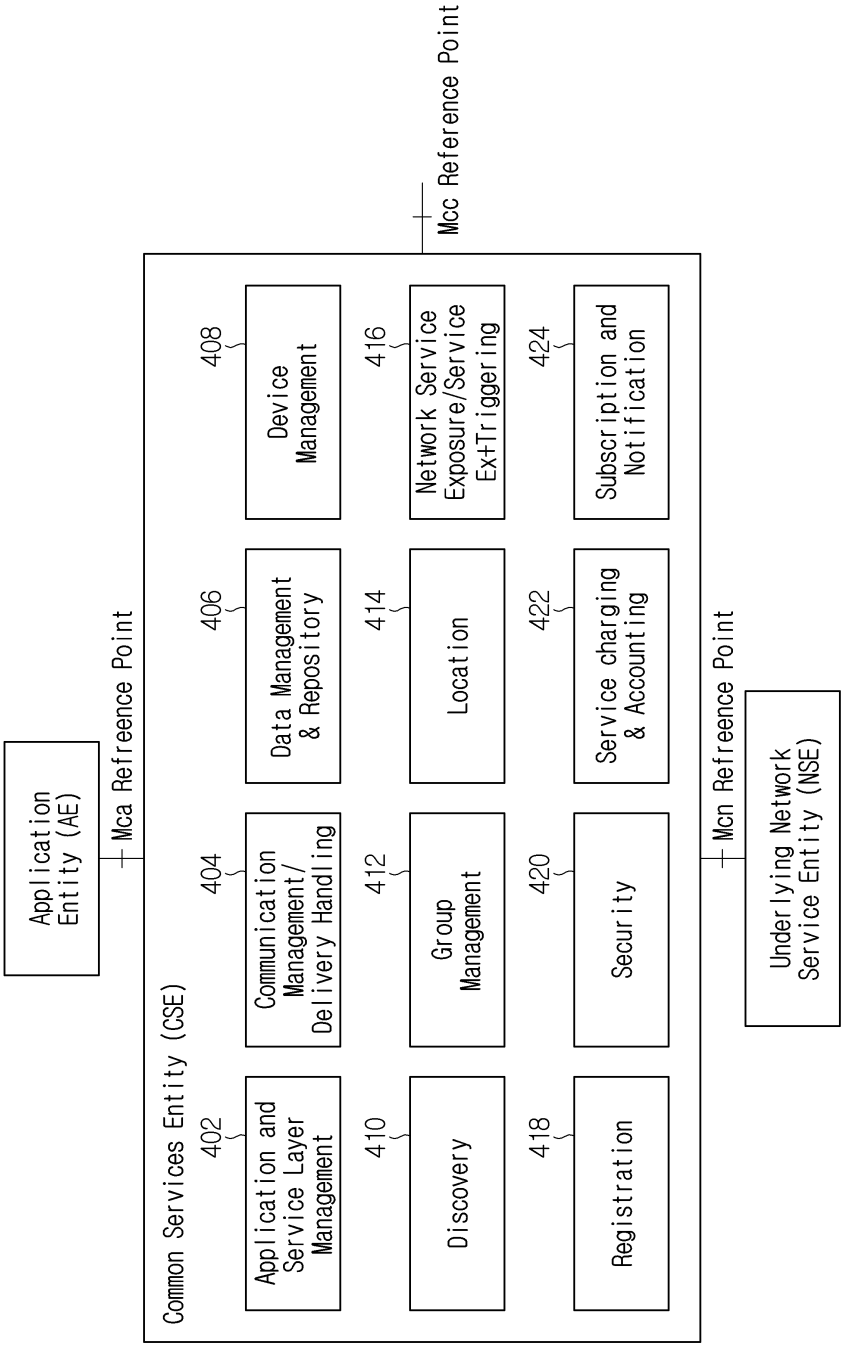
도면2


Field Domain
Infrastructure Domain
210
AE
240
AE
Mca
Mca
Mca
220
CSE
Mcc
250
CSE
Mcc'
To Infrastructure Domain of other Service Provider
Mcn
Mcn
230
NSE
260
NSE

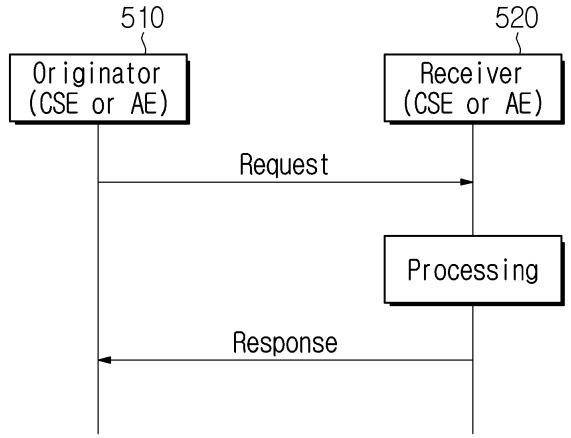
도면3


Infrastructure domain
To an Infrastructure Node of other M2M Service Providers
Field domoin
310
Infrastructure Node(N)
IN-AE
IN-CSE
Mca
Mcc
Mcc'
Mcn
320
Application Dedicated Node (ADN)
ADN-AE
330
Application Service Node (ASN)
ASN-AE
ASN-CSE
340
Middle Node(MN)
MN-AE
MN-CSE
350
Non-oneM2M Device Node (NoDN)
One or more AE
Zero or more AE
Link is out of scope

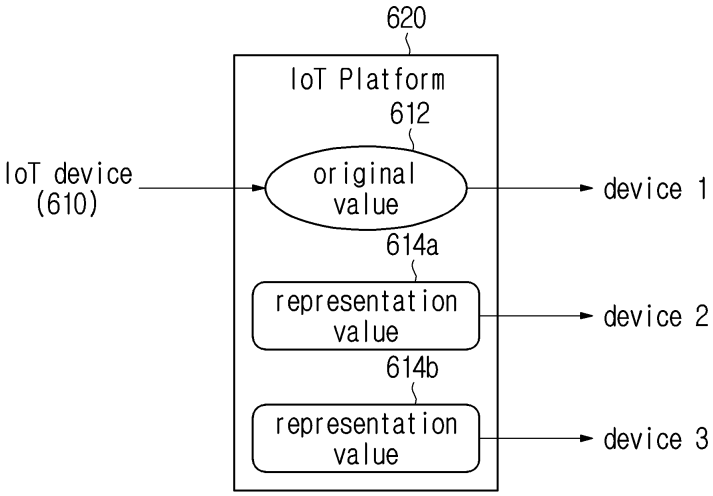
도면4


Application Entity (AE)
Mca Refreence Point
Common Services Entity (CSE)
402
Application and Service Layer Management
404
Communication Management/ Delivery Handling
406
Data Management & Repository
408
Device Management
410
Discovery
412
Group Management
414
Location
416
Network Service Exposure/Service Ex+Triggering
418
Registration
420
Security
422
Service charging & Accounting
424
Subscription and Notification
Mcc Reference Point
Mcn Refreence Point
Underlying Network Service Entity (NSE)

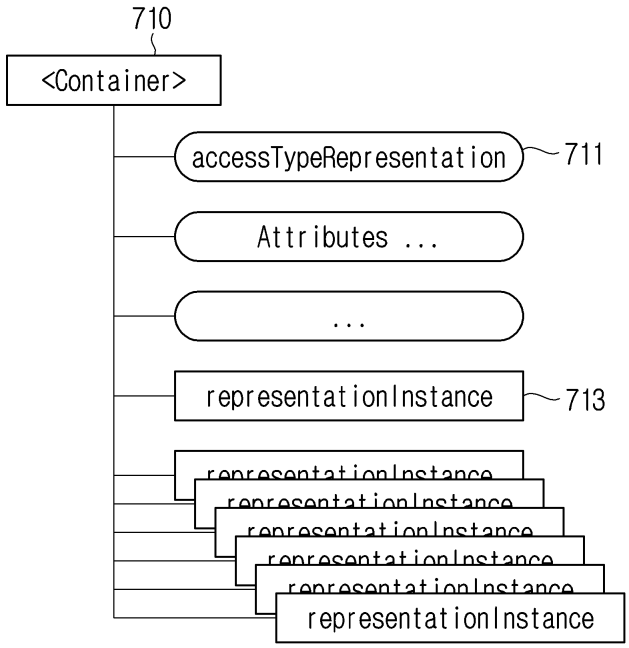
도면5


510
520
Originator
(CSE or AE)
Receiver
(CSE or AE)
Request
Processing
Response

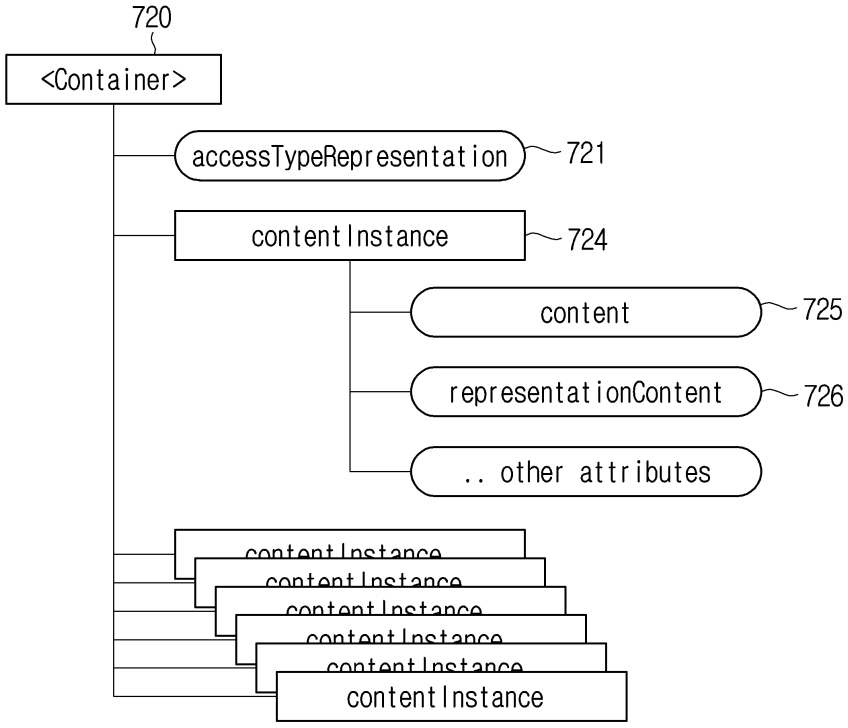
도면6


620
IoT Platform
612
IoT device
(610)
original
value
device 1
614a
representation
value
device 2
614b
representation
value
device 3

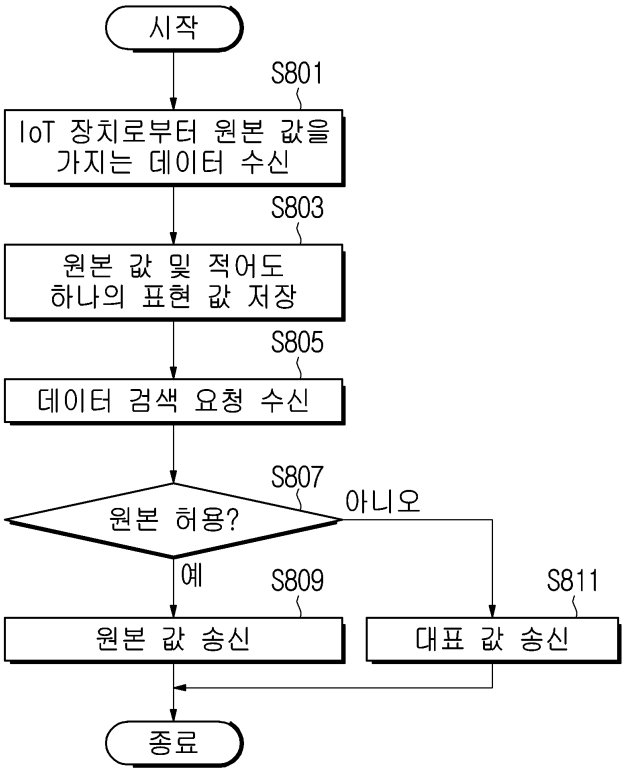
도면7a


710
<Container>
accessTypeRepresentation
711
Attributes ...
...
representationInstance
713
representationInstance
representationInstance
representationInstance
representationInstance
representationInstance
representationInstance

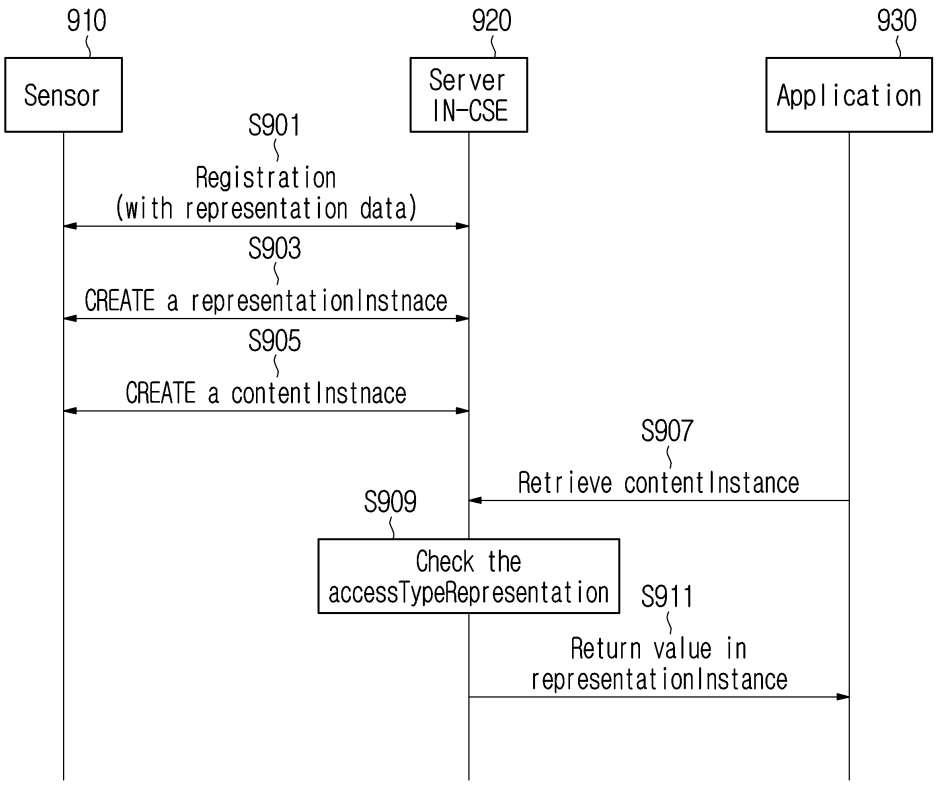
도면7b


720
<Container>
accessTypeRepresentation
721
contentInstance
724
content
725
representationContent
726
.. other attributes
contentInstance
contentInstance
contentInstance
contentInstance
contentInstance
contentInstance

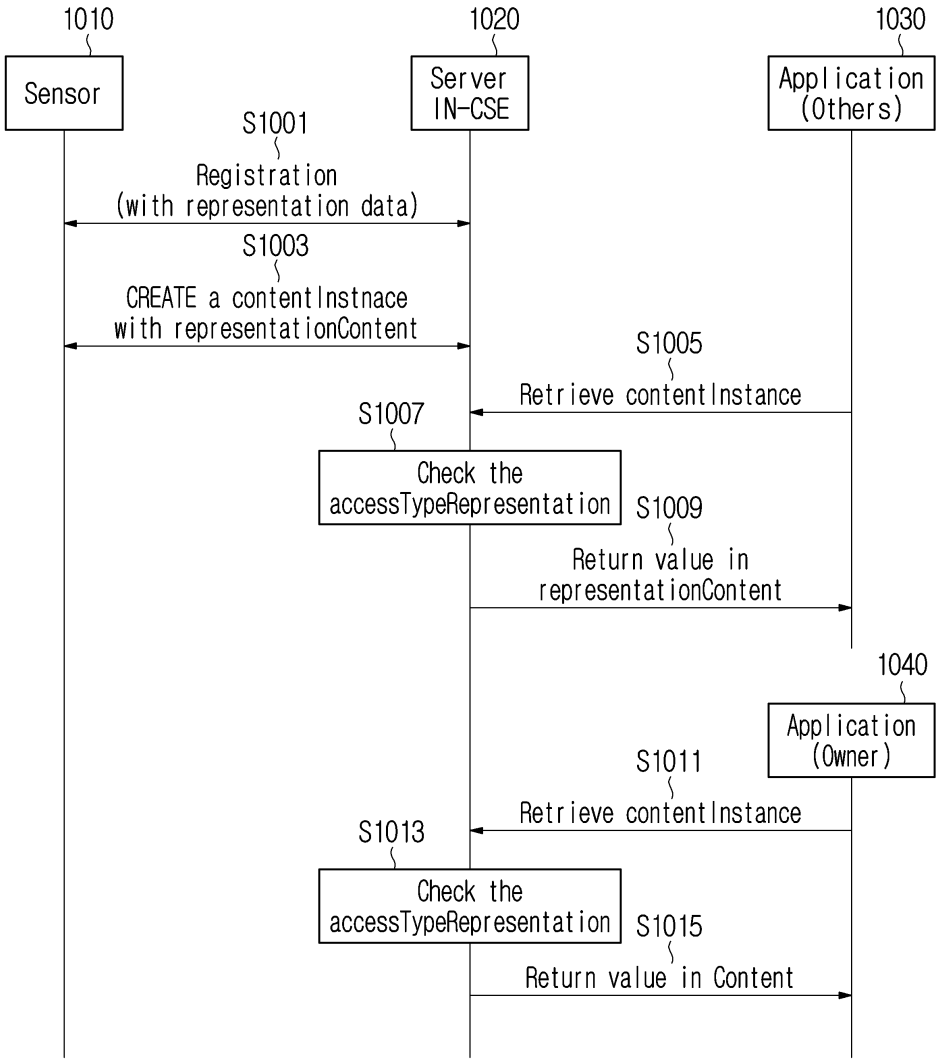
도면8


시작
S801
IoT 장치로부터 원본 값을 가지는 데이터 수신
S803
원본 값 및 적어도 하나의 표현 값 저장
S805
데이터 검색 요청 수신
S807
원본 허용?
아니오
예
S809
원본 값 송신
S811
대표 값 송신
종료

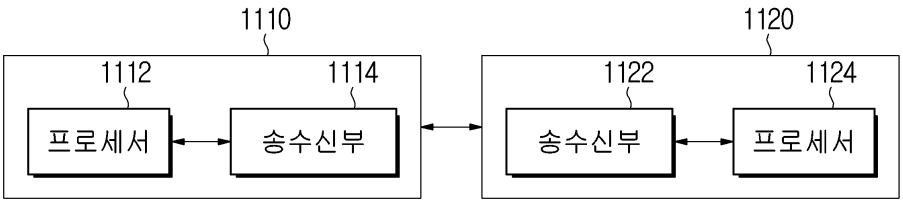
도면9


910
Sensor
920
Server IN-CSE
930
Application
S901
Registration (with representation data)
S903
CREATE a representationInstnace
S905
CREATE a contentInstnace
S907
Retrieve contentInstance
S909
Check the accessTypeRepresentation
S911
Return value in representationInstance

도면10


1010
Sensor
1020
Server
IN-CSE
1030
Application
(Others)
S1001
Registration
(with representation data)
S1003
CREATE a contentInstnace
with representationContent
S1005
Retrieve contentInstance
S1007
Check the
accessTypeRepresentation
S1009
Return value in
representationContent
1040
Application
(Owner)
S1011
Retrieve contentInstance
S1013
Check the
accessTypeRepresentation
S1015
Return value in Content

도면11


1110
1112
프로세서
1114
송수신부
1120
1122
송수신부
1124
프로세서