(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0013209
(43) 공개일자 2017년02월06일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/08 (2013.01)
H04L 63/0807 (2013.01)
(21) 출원번호 10-2016-7029180
(22) 출원일자(국제) 2015년05월29일
심사청구일자 없음
(85) 번역문제출일자 2016년10월19일
(86) 국제출원번호 PCT/US2015/033214
(87) 국제공개번호 WO 2015/184278
국제공개일자 2015년12월03일
(30) 우선권주장
62/005,504 2014년05월30일 미국(US)

(71) 출원인
비자 인터내셔날 써비스 어쏘시에이션
미합중국 94404 캘리포니아주 포스터시티 메트로 센터 보우리바드 900
(72) 발명자
페이스, 패트릭
미국, 94404-2172 캘리포니아, 포스터 시티, 메트로 센터 불러버드 900
해리스, 테오도어
미국, 94404-2172 캘리포니아, 포스터 시티, 메트로 센터 불러버드 900
(74) 대리인
강명구

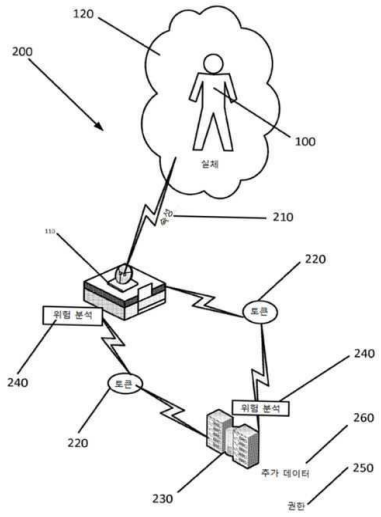
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **개인 영역 네트워크**

(57) 요 약

일 실체가 안전한 컴퓨팅 환경에 다양한 레벨의 민감한 개인 데이터를 저장할 수 있다. 실체는 환경 및 상황에 따라 데이터를 공유하거나 공유불허할 수 있는 권한 규정을 생성할 수 있다. 사람과 같은 실체가 이동함에 따라, 실체는 센서와 같이 작용하는 수많은 전자 장치들과 접할 수 있다. 실체는 안전한 컴퓨팅 환경에 저장되는 다양한 레벨의 민감한 데이터에 센서 또는 센서 운영자가 액세스할 수 있게 하는 토큰을 공유할 수 있다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/10 (2013.01)
H04L 63/105 (2013.01)

명 세 서

청구범위

청구항 1

실체에 관한 데이터의 액세스를 제어하기 위한 컴퓨터 기반 시스템에 있어서,

센서 장치(110)에서 실체(110)로부터 속성 데이터(210)를 검출하고,

추가 데이터(260)를 전송하기 위해, 사용자에 의해 생성되는 권한 규정(250)을 속성 데이터가 충족시키는 지를 검증할 수 있도록, 컴퓨터 네트워크를 통해 중앙 컴퓨터(230) 상의 신뢰 검증 서비스(240)에 속성 데이터(210)를 전송하며,

속성 데이터(210)가 검증됨에 응답하여, 실체(100)에 관한 추가 데이터(260)를 얻기 위한 권한을 포함하는 토큰(250)을 센서 장치(110)에 제공하는

컴퓨터 기반 시스템.

청구항 2

제 1 항에 있어서,

상기 속성 데이터(210)는 사기 특성에 대해 분석되는

컴퓨터 기반 시스템.

청구항 3

제 1 항에 있어서,

상기 속성 데이터(210)는 이동 컴퓨팅 장치 관련 데이터, 스마트 물질, 얼굴, 손, 보석, 홍채 스캔, 및 심장 신호를 포함하는 그룹으로부터 선택되는 적어도 하나를 포함하는

컴퓨터 기반 시스템.

청구항 4

제 1 항에 있어서,

상기 센서 장치(100)는 무선 신호 속성, 광학 속성, 사운드 속성, 냄새 속성, 및 광 속성(photonic attribute)을 포함하는 그룹 중 적어도 하나를 감지하는

컴퓨터 기반 시스템.

청구항 5

제 4 항에 있어서,

상기 광학 속성은 1차원, 2차원 또는 3차원적인 속성인

컴퓨터 기반 시스템.

청구항 6

제 5 항에 있어서,

상기 광학 속성은 센서에 의해 검출가능한 신호를 방출하도록 설계된 직물의 감지를 포함하는

컴퓨터 기반 시스템.

청구항 7

제 1 항에 있어서,

상기 권한 규정(250)은 네트워크-특이적인

컴퓨터 기반 시스템.

청구항 8

제 1 항에 있어서,

상기 컴퓨터 네트워크는 소유자를 갖고, 상기 권한 규정은 상기 소유자에 따라 설정되는

컴퓨터 기반 시스템.

청구항 9

제 1 항에 있어서,

상기 권한 규정(250)은 금전적 가치를 최소값으로 설정하고, 센서(110) 소유자가 최소의 금전적 가치를 지불하고자할 경우, 추가 데이터에 대한 토큰이 제공되는

컴퓨터 기반 시스템.

청구항 10

제 1 항에 있어서,

상기 실체(100)는 복수의 센서(110)와 통신하고, 다양한 센서(110)를 거쳐 이동하는

컴퓨터 기반 시스템.

청구항 11

제 1 항에 있어서,

상기 통신은 신뢰 도메인을 향하는

컴퓨터 기반 시스템.

청구항 12

제 1 항에 있어서,

상기 통신은 적어도 하나의 토큰(220)을 포함하고, 상기 토큰(220)은 사기행위 또는 이상여부 확인을 위해 리뷰되는

컴퓨터 기반 시스템.

청구항 13

제 1 항에 있어서,

승인된 거래는 종래의 지불 네트워크를 통해 이루어지는

컴퓨터 기반 시스템.

청구항 14

제 1 항에 있어서,

상기 토큰(220)의 통신은 가치(value)에 대한 거래를 실현하는

컴퓨터 기반 시스템.

청구항 15

제 1 항에 있어서,

상기 실체는 센서(110)를 통해 실체 승인 메시지를 전송하는

컴퓨터 기반 시스템.

발명의 설명

배 경 기 술

[0001] 과거에, 결제하길 원하던 실체들은 신용 카드 또는 데빗 카드와 같은 지불 장치를 이용했을 것이다. 이러한 지불 장치는 계정 번호를 가질 것이며, 이러한 계정 번호는 판매자(vendor)에 의해 판독될 것이고, 카드 발급자와 같은 신뢰 기관에 의해 검증될 것이다. 그러나, 지불 장치의 보안성 보장은 점점 더 복잡해지고 있고, 특히, 네트워크를 통해 더 많은 거래가 이루어지고 있고, 판매자는 사기 행위 결정을 위해 카드 및 카드 소지자를 물리적으로 검사할 수가 없다. 추가적으로, 사기 행위를 하는 사람들은 점점 더 기술적인 요령이 늘고 있다.

[0002] 추가적으로, 사람들이 네트워크를 더 이용함에 따라, 이들에 관련된 데이터를 제어하는 능력이 감소하고 있다. 네트워크 사이트는 사용자들에 대한 관련 데이터를 수집하고, 상기 데이터를 이용하여 자신의 데이터를 사용할 사용자에게 보상없이 사용자에게 통신을 목표로 한다. 마지막으로, 일부 사용자들은 소정의 네트워크 사이트와 데이터를 훌륭히 공유할 수 있고, 데이터 공유 여부에 관한 결정은 얼마나 많은 사람들이 데이터 획득을 위해 기꺼이 비용을 지불할지에 의해 영향받을 수 있다.

발명의 내용

과제의 해결 수단

[0003] 실체와 관련된 데이터의 제어를 위한 신규한 시스템, 프로세스, 및 방법이 개시된다. 실체는 안전한 컴퓨팅 환경에 다양한 레벨의 민감하고 사적인 데이터를 저장할 수 있다. 실체는 환경 및 상황에 따라 데이터를 공유 또는 공유하지 않는 권한 규칙(permission rules)을 생성할 수 있다. 사람과 같은 실체가 이동할 때, 실체는 무선 네트워크, 광 네트워크, 블루투스 네트워크, 사운드 레코더, 냄새 레코더, 비디오 레코더, 등과 같은 센서들과 같이 작용하는 수많은 전자 장치들과 접할 수 있다. 실체는 안전한 컴퓨팅 환경에 저장되는 다양한 레벨의 민감한 데이터에 센서 또는 센서의 조작자가 액세스할 수 있도록 토큰을 공유할 수 있다.

도면의 간단한 설명

[0004] 도 1은 실체가 만날 수 있는 센서들의 샘플 예시를 도시하고,

도 2는 센서들과 개인 컴퓨팅 네트워크 상호작용하는 실체를 도시하며,

도 3은 실체에 관한 데이터에 대한 액세스를 제어하는 방법을 도시하고,

도 4는 실체의 소정의 샘플 속성을 도시하며,

도 5a는 신뢰 컴퓨팅 시스템에 개인 데이터를 추가하기 위한 입력 디스플레이를 도시하고,

도 5b는 복수의 실체에 대한 권한을 생성하기 위한 입력 디스플레이를 도시하며,

도 6은 지불 시스템과 상호작용하는 개인 네트워크 클라우드의 샘플 도해를 도시하며,

도 7은 서버형 컴퓨팅 디바이스와 인터페이싱하는 휴대형 컴퓨팅 장치를 갖는 실체를 도시하고,

도 8은 휴대형 컴퓨팅 장치를 도시하며,

도 9는 서버형 컴퓨팅 장치를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0005] 실체에 관련된 데이터를 제어하는 신규한 시스템, 프로세스, 및 방법이 하이-레벨도로 개시된다. 도 1에 도시되는 바와 같이, 사람과 같은 실체(100)가 생활하다보면, 실체(100)는 무선 네트워크, 광 네트워크, 블루투스 네트워크, 사운드 레코더, 냄새 수신기, 비디오 레코더, 등과 같은 센서(110)처럼 작용하는 수많은 전자 장치들과 연결될 수 있다. 더욱이, 이러한 센서(110)들 각각은 데이터를 취하여, 실체(100)로부터 명백한 권한없이 판촉용으로 사용될 수 있는 실체(100)에 대한 프로파일을 생성하기 위해 상기 데이터를 실체(100)에 대한 추가 데이

터와 짝지으려 시도한다.

[0006] **개인 네트워크**

[0007] 개인 네트워크(120)는 실체(100)에 관한 민감한 데이터에 대한 액세스를 제어하는 문제를 해결하려 시도한다. 실체(100)는 실체(100)가 기꺼이 추가적인 정보를 통신하고자 하는 센서(110), 네트워크, 또는 네트워크 운영자들의 리스트를 생성할 수 있다. 추가적으로, 실체(100)는 추가적인 정보를 교환하기 위해, 센서(110)들로부터 오퍼를 수신하기 위한 임계치를 또한 설정할 수 있다. 도 1에 도시되는 바와 같이, 삶을 살아가면서, 적색등 카메라로부터 블루투스 네트워크, 무선 802.11 타입 네트워크까지, 많은 센서(100)들을 만날 수 있다. 실체(100)가 허락한 네트워크의 경우에, 실체(100)로부터의 토큰이 신뢰 소스에 전송될 수 있고, 여기서 요망 정보가 네트워크에 전송될 수 있으며, 이러한 통신이 다시 토큰 형태일 수 있다. 토큰은 구매 거래를 가능하게 할 수 있는 충분한 데이터를 지닐 수 있다.

[0008] 도 2는 제안된 시스템(200)의 일 실시예의 하이 레벨도일 수 있다. 일 실체(100)가 센서(110) 범위 내에서 움직일 수 있고, 실체의 속성(210)이 수집될 수 있다. 속성(210)은 실체로부터 센서(110)로 토큰(220) 형태로 전송될 수 있다. 다른 실시예에서, 감지된 속성(210)이 토큰(220)으로 변환될 수 있다. 그 후 토큰(220)은 중앙 컴퓨팅 서비스(230)로 전송될 수 있고, 이는 신뢰 컴퓨팅 시스템으로 간주될 수 있다. 토큰(220)은 위험 분석 애플리케이션(240)에 의해 사기 또는 다른 바람직하지 않은 특성을 위해 리뷰될 수 있다. 토큰(220)이 사기가 아니라고 가정하면, 중앙 컴퓨팅 시스템(230)은 토큰(220)을 리뷰하여, 실체(100)에 관한 추가 정보(260)를 얻기 위해, 실체(100)가 센서(110)를 위한 권한(250)을 허가하였는지 여부를 결정할 수 있다. 권한(250)이 허락되지 않은 경우, 중앙 컴퓨팅 시스템(230)은 침묵하거나 거절 메시지를 전송할 수 있다.

[0009] 더 구체적으로, 도 3을 참조하면, 실체(100)에 관한 데이터에 대한 액세스의 제어를 위한 컴퓨터 기반 방법, 프로세스, 및 시스템이 도시된다. 블록(100)에서, 속성 데이터(210)가 센서 디바이스(110)에서 실체(100)로부터 검출될 수 있다.

[0010] **센서 디바이스**

[0011] 센서(110)는 많을 수 있고 변경될 수 있다. 소모적이거나 제한적인 의도없이, 일부 예들은 802.11 무선 통신 장치, 적외선 통신 또는 60MHz와 같이 서로 다른 주파수 대역에서의 무선 통신 장치, 정지 영상 카메라, 비디오 카메라, 광 센서, 블루투스 통신 장치, 사운드 센서(마이크로폰), 냄새 센서, 열 센서, 및 비침습적이지만 실체(100)에 대한 데이터를 수집할 수 있는 기타 다른 센서(110)를 포함할 수 있다. 센서(110)는 서로 다른 용도로 설계 또는 구성될 수 있으나, 시스템(200)과 통신하도록 적응될 수 있다. 예를 들어, 보안 카메라가 보안 용도로 초기에 설치될 수 있으나, 설명되는 시스템(200) 내의 센서(110)가 되도록 적응될 수 있다.

[0012] 중요사항으로서, 와이파이 라우터와 같은 무선 통신 장치는 종종 센서(110)로 간주되지 않는다. 그러나, 무선 장치와의 통신은 종종 양방향이고, 실체(100)는 통신이 무선 장치와 통신하는 컴퓨팅 장치의 신원 또는 무선 장치의 명칭을 단지 수집하는 것임에도 불구하고, 무선 장치와 통신하기 위해 정보를 제공해야 할 수 있다. MAC 어드레스와 같은 장치의 명칭은, MAC 어드레스가 목표로하는 광고의 안내에 사용될 수 있는 과거 검색에 매칭될 수 있기 때문에, 실체(100)가 새로운 알려지지 않은 네트워크와 통신할 때에도, 네트워크가 실체(100)를 식별하여 목표로하는 광고 통신을 시작하기에 충분할 수 있다. 따라서, 무선 소스와 공유되는 데이터를 제어함으로써, 실체(100)는 그 데이터(260)를 제어할 수 있고, 요망될 때만 데이터(260)가 공유됨을 보장할 수 있다.

[0013] 논리적으로, 일 실체(100)는 하루에 다양한 복수의 센서(110)를 거칠 수 있고, 이러한 센서(110)들 각각은 실체(100)에 관한 더 많은 정보가 가용한지 여부를 결정하기 위해, 중앙 컴퓨팅 장치(230)와 통신하고자할 수 있다.

[0014] 관련된 실체 속성(210)은, 실체(100)가 위치를 변경하고 서로 다른 센서(110)들이 관련 범위 내에 있음에 따라 변화할 수 있다. 예를 들어, 실체(100)가 차량 내에 있을 수 있고, 톨 수집 장치를 통과할 수 있으며, 수많은 블루투스 연결 및 무선 연결을 거칠 수 있다. 차량은 번호판, 고유 외관을 갖기 때문에 고유 속성을 제공할 수 있고, 고유 식별자를 송출할 수 있다. 더욱이, 실체(100)는 차량 내의 온도가 제어될 수 있기 때문에 차량 내에서 재킷을 입고있지 않을 수 있다. 하루 중 나중에, 실체(100)가 차량에서 나와서 재킷을 입을 수 있다. 따라서, 차량의 속성(210)(가령, 번호판, 색상, id 번호)이 더이상 가용하지 않을 수 있다. 그러나, 재킷의 속성(210)이 이제 추가될 수 있다. 더욱이, 속성(210)은 내내 변할 수 있고, 실체(100)의 수명 전체를 통해 변화할 수 있다.

[0015] **속성 데이터**

[0016] 속성(210)은 신원(100) 식별을 돕도록 또는 실체(100)들 간에 차별화를 돕도록 검출될 수 있다. 속성(210)은 폭넓고, 변경될 수 있으며, 센서(110)에 의해 감지될 수 있는, 그리고, 실체(100)들 간의 차별화에 사용될 수 있는, 실질적으로 임의의 품목 또는 특성일 수 있다. 명백한 속성(210) 예는 실체(100)의 얼굴, 실체(100)에게 할당된 휴대용 컴퓨팅 장치의 MAC 어드레스, 또는 애완동물의 RF id일 수 있다. 그러나, 속성(210)을 개인 영역 네트워크(120)의 중앙에 가짐을 사용자가 요망하지 않을 수 있기 때문에 속성(210)이 덜 명확하고 더 흐려질 수 있다. 예를 들어, 일 속성(210)이 손, 하나의 보석, 직물, 향, 소리, 등을 포함할 수 있다. 일부 속성(210)은 MAC 어드레스를 거치는 스마트폰, 브라우저 구조, 메모리 크기, 장치 상의 앱, 등과 같이 액티브한 것일 수 있고, 반면 다른 속성(210)은 얼굴 또는 손의 광학적 특성과 같이 패시브한 것일 수 있다.

[0017] 추가적인 속성(210)은 의도적으로 생성된 품목으로부터 나타날 수 있다. 한 예로서, 직물은 소정의 RF 주파수에 노출될 때 주어진 응답을 제공할 수 있다. 다른 예로서, 보석은 지정된 주파수의 전파를 수신할 때 알려진 응답을 제공할 수 있다. 다른 예로서, 치과 충전재는 알려진 주파수의 전파를 수신할 때 알려진 응답을 제공할 수 있는 장치를 포함할 수 있다. 도 4는 실체(100)의 일부 샘플 속성(120)을 도시할 수 있다. 도 4는 실체(100)의 소정의 샘플 속성(120)을 도시할 수 있다.

[0018] 이미지에 관련된 속성(210)은 인지가 다양한 방식으로 이루어지도록 다양한 치수를 취할 수 있다. 제 1 치수는 얼굴 특징부의 간격의 매핑일 수 있다. 제 2 치수는 얼굴 특징부의 깊이를 추가로 결정하도록 추가될 수 있다. 제 3 치수는 복수의 센서 또는 하나의 정교한 센서를 이용함으로써 추가될 수 있다. 복수의 치수를 이용함으로써, 더 높은 정확도로 실체를 더욱 인지할 수 있다.

[0019] 논리적으로, 센서(110)는 이미지의 검증을 위해 이미지를 중앙 기관(2230)에 전송하도록 컴퓨터 네트워크와 통신할 수 있다. 앞서 언급한 바와 같이, 감지된 속성(210) 데이터는 중앙 기관(230)에 전송될 수 있다. 일부 실시예에서, 속성(210) 데이터는 압축 형태로 변환될 수 있다. 일부 실시예에서, 압축 형태는 중앙 컴퓨팅 기관(230)에 전송되는 토큰(220)으로 변환될 수 있다. 일부 실시예에서, 변환은 센서 장치(110)에서 이루어진다. 다른 실시예에서, 변환은 속성(210) 이미지가 중앙 기관(230)에 전송될 때 일어난다.

[0020] 토큰(220)으로의 변환은 다양한 방식으로 나타날 수 있다. 하이 레벨도에서, 토큰화는 암호화를 통해서와 같이 메시지 및 메시지의 소스를 알려지지 않게 하는 방식으로, 그러나 신뢰 중앙 컴퓨팅 시스템(230)에 의해서 메시지 및 소스를 해역할 수 있도록, 이루어질 수 있다. 더욱이, 토큰(220)은 악의적 콘텐트가 중앙 컴퓨팅 시스템(230)에 전달되지 않음을 보장하기 위해 보안 소프트웨어 또는 위험 분석 애플리케이션(240)에 의해 리뷰될 수 있다.

[0021] **실체**

[0022] 실체(100)는 민감하다거나 개인적인 것으로 여겨질 수 있는 정보(260)를 가질 수 있는 임의의 개인, 조직, 또는 것일 수 있다. 논리적으로, 사람이 실체(100)로 여겨질 수 있다. 추가적으로, 법인 또는 그외 다른 법적 조직이 조직에 관한 민감한 정보(260)가 가용할 수 있기 때문에 실체(100)로 또한 여겨질 수 있다. 더욱이, 느슨하게 조직된 그룹이 또한 실체(100)로 여겨질 수 있다. 한 예로서, 일 그룹의 친구들이 매주 포커 게임을 할 수 있고, 이 그룹이 실체(100)로 여겨질 수 있다. 논리적으로, 하나의 큰 실체(100)가 일 그룹의 실체(100)들로 구성될 수 있다. 훨씬 더 작은 레벨에서, 각각의 컴퓨팅 장치는 민감하다고 여겨질 수 있는 정보를 지닐 수 있고, 각각의 컴퓨팅 장치는 실체(100)로 여겨질 수 있다. 예를 들어, 사용자는 단지 업무용으로 스마트폰을 가질 수 있고 이 폰이 제 1 실체(100)일 수 있으며, 사용자는 매우 다른 민감한 데이터(260)를 가질 수 있는 개인 용도의 제 2 폰을 가질 수 있고, 제 2 폰이 별도의 실체(100)로 여겨질 수 있다.

[0023] **민감한 정보**

[0024] 보호할만한 민감한 데이터(260)가 무엇인지는 실체(100)에 달려있을 수 있다. 성명 및 계정 번호와 같이 사기 거래 수행에 소정의 데이터(260)가 필요할 수 있다. 이와 동시에, 일부 실체(100)는 더 많은 정보를 민감한(260)한 것, 보호할 가치가 있는 것으로 간주할 수 있다. 예를 들어, 어드레스 또는 전화 번호가 유명 배우에게 민감한 데이터(260)로 여겨질 수 있고, 반면 판매자와 같은 다른 실체(100)는 전화 번호 및 어드레스의 전파를 적극적으로 권장할 수 있다. 따라서, 유명 배우는 어드레스 및 전화 번호를 민감한 것(260)으로 표시할 수 있고, 배우의 지시 하에만 전송될 수 있다. 반대편 극단에서, 판매자는 전화 번호 및 어드레스를 가능한 많은 사람들과 공유할 수 있다. 사용자 인터페이스를 이용하여, 소정의 데이터가 민감한 것(260)이고 허락을 얻어서만 공유되어야하고, 반면 다른 데이터는 실질적으로 누구와도 공유될 수 있음을 실체(100)가 명시할 수 있게 한다.

[0025] 도 5a는 민감한 데이터(260)를 입력하기 위한 디스플레이의 도해일 수 있다. 실체(100)는 요망하는 것보다 많은 또는 적은 정보를 입력하기 위한 옵션을 가질 수 있다. 예를 들어, 판매자는 유망 고객들과 공유할 수 있는 다량의 정보를 입력하고자 하는 소망을 입력할 수 있고, 프라이버시를 지키길 원하는 유명 배우는 현대의 삶에서 작업 생산성에 필요한 순수 최소치를 입력할 수 있다.

[0026] **신뢰 컴퓨팅 시스템**

[0027] 컴퓨터 시스템(230)이 도 7에 도시될 수 있고, 다양한 센서(110)와 통신하는 신뢰 컴퓨팅 시스템을 포함할 수 있다. 신뢰 컴퓨팅 시스템(230)은 사기에 관한 우려를 취급하기 위한 토큰(220) 분석을 또한 제공할 수 있다. 신뢰 컴퓨팅 시스템(230)은 실체 정보(260)의 문지기(게이트키퍼)로 여겨질 수 있고, 실체(100)가 센서(110)(또는 센서 소유자)에게 정보(260)의 배포를 승인하지 않은 경우, 센서(110)는 자체적으로 수집할 수 있는 정보만으로 남게 된다. 컴퓨팅 시스템(230)은 단일 위치에 놓일 수도 있고, 다양한 위치들 간에 확산될 수도 있다. 시스템(230) 사용자에게, 시스템(230)은 단일 컴퓨터로 나타날 수 있으나, 시스템(230)은 복수의 컴퓨팅 시스템(230) 간에 확산될 수 있고, 이는 일 유형의 클라우드 컴퓨팅 설계로 세계에 확산될 수 있는

[0028] 도 7은 방법의 다양한 실시예를 실행하도록 물리적으로 구성될 수 있는 샘플 컴퓨팅 시스템(230) 내 요소들 중 일부의 하이 레벨도일 수 있다. 컴퓨팅 시스템(230)은 전용 컴퓨팅 장치(141), 전용 휴대형 컴퓨팅 장치(101), 컴퓨팅 장치(141) 상의 애플리케이션, 휴대형 컴퓨팅 장치(101) 상의 애플리케이션, 또는 이들 모두의 조합일 수 있다. 도 8은 센서(110)를 통해 원격 컴퓨팅 장치(141)와 통신하는 휴대형 컴퓨팅 장치(101)의 하이 레벨도일 수 있으나, 애플리케이션은 다양한 방식으로 저장 및 액세스될 수 있다. 추가적으로, 애플리케이션은 앱 스토어로부터, 웹 사이트로부터, 매장 와이파이 시스템으로부터, 등과 같이 다양한 방식으로 획득될 수 있다. 여기서, 서로 다른 컴퓨팅 장치, 서로 다른 컴퓨터 언어, 및 서로 다른 API 플랫폼들의 장점을 이용하기 위해 다양한 버전의 애플리케이션이 존재할 수 있다.

[0029] 일 실시예에서, 휴대형 컴퓨팅 장치(101)는 배터리와 같은 휴대형 전력원(155)(도 8)을 이용하여 작동하는 장치일 수 있다. 도 7을 참조하면, 휴대형 컴퓨팅 장치(101)는 터치 감지식 디스플레이일 수도 있고 아닐 수도 있는 디스플레이(102)를 또한 가질 수 있다. 더 구체적으로, 디스플레이(102)는, 예를 들어, 휴대형 컴퓨팅 장치(101)에 입력 데이터 제공에 사용될 수 있는, 용량성 센서를 가질 수 있다. 다른 실시예에서, 화살표, 스크롤 휠, 키보드, 등과 같은 입력 패드(104)를 이용하여, 휴대용 컴퓨팅 장치(101)에 입력을 제공할 수 있다. 추가적으로, 휴대형 컴퓨팅 장치(101)는 언어적 데이터(verbal data)를 수용 및 저장할 수 있는 마이크로폰(106), 이미지를 수용하기 위한 카메라(108), 및 소리를 통신하기 위한 스피커(110)를 가질 수 있다.

[0030] 휴대형 컴퓨팅 장치(101)는 일 컴퓨팅 장치와 통신할 수 있고, 또는, 컴퓨팅 장치(111)들의 클라우드를 구성하는 복수의 컴퓨팅 장치(141)와 통신할 수 있다. 휴대형 컴퓨팅 장치(101)는 다양한 방식으로 통신할 수 있다. 일부 실시예에서, 통신은 이더넷 케이블, USB 케이블, 또는 RJ6 케이블을 통해서와 같이 유선으로 이루어질 수 있다. 다른 실시예에서, 통신은 와이파이(802.11 표준), 블루투스, 셀룰러 통신, 또는 근거리 통신(NFC) 장치를 통해서와 같이, 무선으로 이루어질 수 있다. 통신은 컴퓨팅 장치(141)에 직접적으로 이루어질 수도 있고, 셀룰러 서비스와 같은 통신 장치 또는 장치들의 네트워크를 통해, 인터넷을 통해, 개인 네트워크를 통해, 블루투스를 통해, 근거리 통신을 통해, 등과 같이 이루어질 수도 있다. 도 8은 휴대형 컴퓨팅 장치(101)를 구성하는 물리적 요소들의 단순화된 도해일 수 있고, 도 9는 서버형 컴퓨팅 장치(141)를 구성하는 물리적 요소들의 단순화된 도해일 수 있다.

[0031] 도 8을 참조하면, 샘플 휴대형 컴퓨팅 장치(101)가 시스템의 일부분인 방법에 따라 물리적으로 구성될 수 있다. 휴대형 컴퓨팅 장치(101)는 컴퓨터 실행가능 명령어에 따라 물리적으로 구성되는 프로세서(150)를 가질 수 있다. 이는 충전가능한 배터리와 같은 휴대형 전력 공급원(155)을 가질 수 있다. 또한, 비디오 및 사운드의 디스플레이를 돕는 사운드 및 비디오 모듈(160)을 또한 가질 수 있고, 전력 및 배터리 수명 보존을 위해 사용하지 않을 때 전원을 끌 수 있다. 휴대형 컴퓨팅 장치(101)는 휘발성 메모리(165) 및 비휘발성 메모리(170)를 또한 가질 수 있다. 여기서, 마이크로폰(106), 카메라(108), 및 기타 입력부(102), 등과 같이, 다양한 사용자 입력 장치 내외로 데이터를 실어나르는 입력/출력 버스(175)가 또한 존재할 수 있다. 장치는 무선 또는 유선 장치를 통한 네트워크와의 통신을 또한 제어할 수 있다. 물론, 이는 휴대형 컴퓨팅 장치(101)의 일 실시예에 지나지 않으며, 휴대형 컴퓨팅 장치(101)의 개수 및 유형은 상상에 의해서만 제한된다. 휴대형 컴퓨팅 장치(101)는 디스플레이(102)로 작용할 수 있고, 또는, 디스플레이(102)의 일부분일 수 있다.

[0032] 원격 컴퓨팅 장치(141)를 구성하는 물리적 요소들은 도 9에 추가로 도시될 수 있다. 하이 레벨도에서, 컴퓨팅 장치(141)는 자기 디스크, 광학 디스크, 플래시 스토리지, 비휘발성 스토리지, 등과 같은 디지털 스토리지를 포

함할 수 있다. 구조화된 데이터가 데이터베이스와 같은 디지털 스토리지에 저장될 수 있다. 서버(141)는 컴퓨터 실행가능 명령어에 따라 물리적으로 구성되는 프로세서(300)를 가질 수 있다. 서버는 비디오 및 사운드 디스플레이를 돕는 사운드 및 비디오 모듈(305)을 또한 가질 수 있고, 전력 및 배터리 수명 보존을 위해 사용하지 않을 때 전원을 끌 수 있다. 서버(141)는 휘발성 메모리(310) 및 비휘발성 메모리(315)를 또한 가질 수 있다.

[0033] 데이터베이스(325)는 메모리(310 또는 315)에 저장될 수 있고, 또는 별도의 것일 수 있다. 데이터베이스(325)는 컴퓨팅 장치(141)의 클라우드의 일부분일 수도 있고, 복수의 컴퓨팅 장치(141) 간에 분배되는 방식으로 저장될 수 있다. 마이크로폰(106), 카메라(108), 입력부(102), 등과 같이, 다양한 사용자 입력 장치로 내외로 데이터를 실어나르는 입력/출력 버스(320)가 또한 존재할 수 있다. 입력/출력 버스(320)는 무선 또는 유선 장치를 통한 네트워크와의 통신을 또한 제어할 수 있다. 일부 실시예에서, 애플리케이션은 로컬 컴퓨팅 장치(101) 상에 존재할 수 있고, 다른 실시예에서, 애플리케이션이 원격(141)으로 위치할 수 있다. 물론, 이는 서버(141)의 일 실시예에 불과하고, 컴퓨팅 장치(141)의 개수 및 유형은 상상에 의해서만 제한된다.

[0034] 도 3을 다시 참조하면, 블록(110)에서, 속성 데이터(210)가 컴퓨터 네트워크를 통해 신뢰 컴퓨팅 시스템(230)으로 전송되어, 추가 데이터(260) 전송을 허가하기 위해 사용자에 의해 생성된 권한 규칙(250)을 속성 데이터가 충족시키는지를 검증할 수 있다. 앞서 언급한 바와 같이, 속성 데이터(210)는 네트워크를 통해 전송될 수 있는 토큰(220)으로 변환될 수 있다. 이러한 변환은 컴퓨터 네트워크에 해킹 시도할 수 있는 범죄 실체들이 쉽게 이해하는 방식으로 전송되지 않는다는 편안함을 실체(100)에게 제공할 수 있다. 이러한 변환은 추가 데이터를 신뢰 컴퓨팅 시스템(230)이 이해할 수 있도록, 그러나, 컴퓨터 네트워크에 액세스할 수 있는 기타에 의해서는 이해할 수 없도록, 암호화 형태 기법으로 또는 다른 방식을 통해 이루어질 수 있다.

[0035] **사기행위 분석**

[0036] 더욱이, 간단히 언급된 바와 같이, 컴퓨터 네트워크를 통해 전송되는 토큰(220)은 보안을 이유로 리뷰될 수 있다. 이러한 방식으로, 안전한 컴퓨팅 서비스(230) 내로 파고들려는 시도가 최소화될 수 있다. 예를 들어, 속성 데이터(210)는 사기 특성을 위해 분석될 수 있다. 더욱이, 시스템(230)을 이용하는 실체(100)가 네트워크 상의 메시지가 보안용도로 리뷰되고 있음을 알 때 더욱 편안함을 가질 수 있다.

[0037] 사기 분석(240)은 위험 측면에서 거래를 살필 수 있다. 토큰(220) 및 토큰(220)에 의해 표현되는 데이터를 분석하여, 데이터가 사기일 가능성이 높은지 여부를 결정할 수 있다. 추가적으로, 사기 분석(240)은 신경망 또는 인공 지능을 이용하여 분석을 계속적으로 개선시킬 수 있다. 예를 들어, 분석은 단일 사용자가 동시에 서로 다른 장소에 놓이는 것이 불가능함을 시간에 걸쳐 결정할 수 있다. 마찬가지로, 글루텐(gluten)에 앨러지 반응이 있는 자는 글루텐을 함유한 제품을 사고 있을 수 있고 분석이 시간에 걸쳐 이를 학습할 수 있을 가능성이 매우 높을 것이다.

[0038] 토큰(220)이 사기성인지 여부를 결정하기 위해 복수의 속성(210)이 검사될 수 있다. 예를 들어, 제 1 센서(110)는 실체(100)의 제 1 속성(210)을 관찰할 수 있고, 제 2 센서(110)는 실체(100)의 제 2 속성(210)을 관찰할 수 있다. 실체(100)를 관찰하는 두 속성(210)들 모두 리뷰 및 교차-매칭되어, 적절하고 신뢰가능한 실체(100) 식별을 보장할 수 있다. 한 예로서, 제한없이, 제 1 속성(210)(얼굴 특징부)이 제 1 실체(100)에 속한다고 결정되지만 제 2 속성(210)(전화 MAC 어드레스)이 제 2 실체(100)에 속한다고 결정되면, 사기가 일어나고 있을 가능성이 높다는 결정이 이루어질 수 있다. 마찬가지로, 제 1 속성(210)(머리카락 색상)이 제 1 실체(100)에 속한다고 결정되고 제 2 속성(210)(링 RFID 시그너처)이 제 1 속성(100)에 속한다고 결정되면, 사기가 아닐 가능성이 높다는 결정이 이루어질 수 있다. 논리적으로, 실체(100)에 대한 속성 데이터(210)의 축적이 소정 시간 주기 동안 이루어질 수 있고, 가까운 시간 근접도 내에서 관찰된 속성(210)들을 비교하여 동일한 실체(100)가 관찰되고 있음을 보장할 수 있다.

[0039] 위험 서비스(240)는 관찰되는 관련 속성(210) 데이터를 축적할 수 있고, 하나 이상의 분석 알고리즘을 수행하여 사기 가능성이 높은지 여부를 결정할 수 있다. 위험 서비스(240)는 중앙 신뢰 컴퓨팅 장치(230)의 일부분일 수 있으나, 네트워크를 통해 나타나는 토큰(220)과 같은 통신을 또한 검사할 수 있다. 신뢰 네트워크에 도달하기 전에 통신을 리뷰함으로써, 범죄 통신이 결정될 수 있고, 신뢰 서버(230)에 도달하기 전임에도 불구하고 위치결정될 수 있다.

[0040] 위험 분석 서비스(240)는 다양한 물리적 형태를 취할 수 있다. 일 실시예에서, 컴퓨팅 시스템은 위험 서비스(240)로 작동하도록 물리적으로 구성된다. 컴퓨팅 칩은 위험 서비스(240)의 일부분으로 물리적으로 구성 및 설치될 수 있다. 또 다른 실시예에서, 컴퓨팅 칩은 컴퓨터 실행가능 명령어에 따라 물리적으로 구성될 수 있고,

명령어는 시간에 따라 변화하거나 업데이트될 수 있다. 그 결과, 프로세서 또는 메모리와 같은 컴퓨팅 칩이, 업데이트된 컴퓨터 실행가능 명령어의 결과로, 그 물리적 구조를 변경할 수 있다.

[0041] 또 다른 실시예에서, 위험 서비스(240)는 네트워크에 걸쳐 확산될 수 있다. 예를 들어, 센서(110)가 속성(210) 데이터를 중앙 컴퓨팅 시스템(230)에 전송하고자 할 경우, 속성 데이터(210)는 먼저, 센서(110) 위치에서 또는 그 근처에서 컴퓨팅 장치(230) 상에 위치할 수 있는 위험 서비스(240)에 의해 분석되어야 한다. 이러한 방식으로, 사기성 또는 범죄 통신이 네트워크 내로 침입하기 전에 중단될 수 있다.

[0042] **권한(PERMISSIONS)**

[0043] 도 3을 다시 참조하면, 블록(120)에서, 중앙 컴퓨팅 장치(230)에서, 속성(210)을 분석하여, 실체(100)에 관한 추가 데이터의 전송을 허용하기 위해 실체(100)가 기설정된 권한을 갖고 있는지 여부를 결정할 수 있다. 실체(100)는 사용자 인터페이스를 갖는 애플리케이션을 이용하여, 실체(100)에 관한 추가 데이터가 네트워크를 이용하는 다른 사람들에게 언제 어떻게 전송되는지를 결정할 수 있다. 권한(250)은 다양한 방식으로 세부화될 수 있다. 한 예에서, 권한(250)은 센서(110)-특이적일 수 있다. 한 예로서, 일 실체가 미국, Anytown의 Maple Avenue and River Road의 코너의 Coffee House에서 커피를 계속하여 구매할 경우, 실체(100)는 지불 정보와 같은 추가의 정보를 비디오 카메라(센서)(110) 및 Coffee House에서 지불 시스템을 작동시키기 위한 관련 컴퓨팅 장비와 공유할 수 있다.

[0044] 또 다른 실시예에서, 권한은 더 폭넓을 수 있고 위치-특이적일 수 있다. Coffee House 예를 다시 참조하면, 와이파이 시스템, 비디오 카메라, 정지화상 카메라, 냄새 센서, 등과 같이, Maple & River의 Coffee House에서 모든 센서(110)들은, 지불 정보와 같이, 실체(100)에 관한 추가 정보(260)를 얻기 위한 권한을 허가받을 수 있다.

[0045] 다른 실시예에서, 권한(250)은 소유자-특이적 센서(110)일 수 있다. 실체(100)는 미국 내 모든 Coffee Houses를 신뢰할 수 있고, 미국 내 모든 Coffee Houses와 추가 정보 공유를 바랄 수 있다. 이러한 방식으로, 실체(100)는 미국 내 임의의 Coffee House 내로 걸어들어갈 수 있고, Coffee House는 지불 정보를 포함한, 실체(100)에 관한 추가 정보를 얻을 수 있다.

[0046] 추가의 실시예에서, 실체(100)는 커피를 서빙하는 네트워크의 모든 사용자들이, 실체(100)에 관한 추가 정보를 얻기 위한 권한을 갖게할 수 있다. 이러한 배열에서, 실체(100)는 임의의 커피 서빙 위치에 데이터를 전송할 수 있고, 실체(100)는 이러한 위치들 중 임의의 위치에서 커피를 얻을 수 있다.

[0047] **권한 생성**

[0048] 도 6은 샘플 권한(250) 생성 디스플레이(600)의 도해일 수 있다. 권한 디스플레이(600)는 네트워크 액세스를 갖는, 그리고, 휴대형 컴퓨팅 장치를 포함한 입력 정보를 디스플레이 및 수신할 수 있는, 임의의 컴퓨팅 장치 상에 생성될 수 있다. 센서 소유자 명칭(610), 추가 데이터 획득에 요구되는 요금(620), 데이터를 허가받을 위치(630), 및 권한 레벨(640)(하이 레벨에서 시작하여 실체(100)로 하여금 권한(250)을 점점 더 구체화함)과 같은 복수의 입력 필드가 존재할 수 있다. 더욱이, 판매자/센서(110) 위치에 있으면서도 생성된 권한(250)들이 또한 나열되고 수정될 수 있다.

[0049] 마찬가지로, 실체(100)는 진행 중에 권한(250)을 설정할 수 있다. 예를 들어, 사용자가 공항에 있을 경우, 사용자가 택시 운전자가 아닌 리무진 운전자와 통신하기 위한 권한(250)을 설정할 수 있다. 다른 예로서, 사용자가 중국 음식을 원할 경우, 사용자는 피자를 서빙하는 식당이 아닌 중국 음식을 서빙하는 식당과 통신하기 위한 권한을 설정할 수 있다.

[0050] **비딩(BIDDING)**

[0051] 또 다른 실시예에서, 권한(250) 규정은 금전적 가치를 최소값으로 설정할 수 있고, 센서(110) 소유자가 최소의 금전적 가치를 지불하고자 할 경우, 추가 데이터(260)의 토큰(220)이 제공될 수 있다. 이러한 방식으로, 실체(100)는 추가 정보(260)의 공유를 보상받을 수 있다. 논리적으로, 권한(250) 규정은 다양한 제한사항과 함께 여러가지 방식으로 생성될 수 있다.

[0052] 한 예로서, 실체(100)는 일부 개인 정보를 배포하기 위한 댓가로 판매자로부터 할인 오퍼 수신을 선택할 수 있다. 실체(100)에 의해 할인 퍼센티지가 또한 설정될 수 있고, 정보(260)는 더 높은 할인 퍼센티지로 입찰하고자 하는 판매자와만 공유될 수 있다. 또 다른 예로서, 실체(100)는 소정 시간 주기 동안 단일 판매자 또는 판매자 라인에서 단지 광고 수신(또는 지불 설정)의 댓가로 이익(할인, 보상, 특별 오퍼) 수령을 선택할 수 있다. 판매자로부터의 오퍼가 임계치를 충족하지 못할 경우, 오퍼는 거절될 수 있고, 실체(100)에 대한 데이터가 계속 사

적인 상태로 유지될 수 있다.

[0053] **추가 데이터**

[0054] 도 3을 다시 참조하면, 블록(130)에서, 권한이 허가되면, 추가 정보(260)가 전송될 수 있다. 추가 데이터(260)는 다양한 형태 또는 레벨을 취할 수 있고, 그 형태 및 레벨은 실체(100)에 의해 설정될 수 있다. 앞서 언급한 바와 같이, 일 실체(100)가 사적인 또는 민감한 데이터(260)로 여기는 것이 무엇인지는 실체(100)에 따라 달라질 수 있고, 이러한 요인들은 공유하고자 하는 데이터(260) 및 설정된 권한(250)에 반영될 수 있다. 더욱이, 일부 실체(100)는 다른 실체(100)들보다 제공할 더 많은 추가 데이터(260)를 가질 수 있다.

[0055] 한 예로서, 추가 데이터(260)는, 실체(100)가 고객일 가능성을 결정하기 위해, 판매자가 이용할 수 있는 실체(100)의 수입 레벨에 관한 데이터를 포함할 수 있다. 다른 예에서, 추가 데이터(260)는 실체(100)가 유효 계정을 갖고 있는지 여부, 또는, 계정이 추가 구매를 위한 공간을 갖고 있는지 여부와 같이, 지불 정보 데이터를 포함할 수 있다. 실체(100)는 미리 추가 데이터의 레벨을 설정할 수 있다. 예를 들어, 실체(100)는 $5 지불을 원하는 판매자가 실체(100)에 관한 우편번호를 볼 수 있고, $50 지불을 원하는 판매자가 실체(100)에 관한 수입 레벨 정보를 살필 수 있다.

[0056] 일부 실시예에서, 정보(260)의 레벨은 판매자 위치에서도 실체(100)에 의해 설정될 수 있다. 한 예로서, 실체(100)는 실체(100)가 아직 권한 레벨을 설정하지 않은 새 점포를 돌아다닐 수 있고, 실체(100)가 판매자에게서 구매를 원할 수 있다. 실체(100)는 보안 카메라(센서(110))를 살펴볼 수 있고, 보안 카메라(110)가 중앙 서버(230)에서 인증 데이터로 이미지를 전송할 수 있다. 이미지 및 와이파이 획득 데이터를 포함할 수 있는 인증 데이터는, 사기성이 없는 것으로 비준될 수 있다. 실체(100)는, 센서(110)들 중 하나를 통해, 판매자에게 전송될 데이터의 구매를 위해 실체(100)가 권한(250)을 허가함을 중앙 기관(230)에 표시할 수 있다.

[0057] 실체(100)는 실체(100)에 의해 기설정될 수 있는 표시를 다양한 방식으로 행할 수 있다. 예를 들어, 실체(100)는 의도적인 엄지를 위로 향하는 제스처가 지불 데이터(260)를 이러한 판매자에게 전송함에 관한 권한을 허가받았음을 의미함을 기설정할 수 있다. 다른 예로서, 사용자는 사운드 기능을 또한 가질 수 있는 카메라(110)에 기설정 어구를 말할 수 있고, 사운드 및 이미지는 속성(210)으로 검증될 수 있으며, 지불 데이터(260)가 그 후 판매자에게 전송될 수 있다. 또 다른 예로서, 실체(100)는 지불 데이터가 특정 판매자에게 전송될 수 있음을 중앙 기관(230)에 전송하기 위해 스마트 폰과 같은 휴대형 컴퓨팅 장치를 이용할 수 있다.

[0058] **통신/토큰**

[0059] 앞서 언급한 바와 같이, 통신은 신뢰 도메인에게로 이루어질 수 있다. 통신은 토큰(220) 형태를 취할 수 있다. 일부 실시예에서, 토큰(220)은 실체(100)로부터 센서(110)로 전달되며, 토큰(220)은 그 후 신뢰 기관(230)에 전송된다.

[0060] 또 다른 실시예에서, 토큰(220)은 실체 명칭.도메인 형태로 전송되며, 도메인은 신뢰 네트워크 제공자의 명칭일 수 있다. 또 다른 실시예에서, 토큰(220)은 토큰.도메인의 형태로 전송될 수 있고, 도메인은 신뢰 네트워크 제공자의 명칭일 수 있다. 일부 버전의 인터넷 프로토콜에서, 토큰(220) 자체는 어드레스의 일부분일 수 있고, 토큰(220)은 동적인 것일 수 있다.

[0061] 토큰(220)이 받아들여지고 추가 통신에 관한 권한이 허가되면, 그 후 차후의 통신들이 암호화된 방식으로, 또는 다른 안전하고 효율적인 포맷으로 진행될 수 있다. 권한이 허가되었는지에 관한 결정의 결과와 함께, 중앙 컴퓨팅 시스템(230)으로부터 센서(110)로의 통신은, 토큰(220)의 형태를 취할 수 있다. 토큰(220)은 판매자 또는 센서(110) 소유자가 볼 수 있도록 실체(100)가 허가한 데이터의 레벨을 표시할 수 있다. 토큰(220)은 권한이 허가되었을 경우 실체(100)에 관한 소정의 예비 정보를 또한 지닐 수 있고, 판매자/센서 소유자(110)가 그 후 추가 데이터(260)가 유용한지 여부를 결정할 수 있다. 관련하여, 추가 정보(260)를 얻기 위해 비딩 또는 지불이 요구되는 상황에서, 정보(260) 관련 비용 또는 현재 입찰 상태가 토큰(220)의 일부분으로 전송될 수 있다.

[0062] 일부 실시예에서, 모든 통신이 토큰(220)을 이용하여 이루어진다. 사기 행위를 감소시키기 위해, 다양한 토큰(220)들이 동적인 것일 수 있다. 예를 들어, 실체(100)는 제 1 토큰(220)을 제 1 센서(110)로 전송할 수 있고, 다른 토큰(220)을 다른 센서(110)에 전송할 수 있다. 이러한 방식으로, 판매자는 실체(110)와의 통신을 시도하기 위해 이전 토큰(220)을 이용할 수 없다. 토큰(220)이 신뢰 컴퓨팅 시스템(100)에 의해 이해될 수 있는 한, 토큰(220)은 변화하거나 동적인 것일 수 있다. 예를 들어, 토큰(220)은 중앙 컴퓨터(230) 및 센서(110)를 동기화시키는 클럭에 따라 변할 수 있다. 추가적으로, 앞서 언급한 바와 같이, 신뢰 컴퓨팅 시스템(230)을 향한 모

든 통신은 위기 분석 시스템(240)에 의해 사기 또는 이상여부를 위해 리뷰될 수 있다.

[0063] 또 다른 실시예에서, 도 6에 도시되는 바와 같이, 토큰(220)은 종래의 지불 네트워크를 통해 거래를 구현할 수 있다. 실체(100)가 센서(110) 또는 판매자와 신뢰를 구축할 수 있다. 실체(100)가 지불 정보(260)에 대한 액세스를 허가하였다고 가정할 때, 신뢰 컴퓨팅 스토어(230)에 저장된 지불 정보(260)가 획득자(700)를 통해서와 같이, 종래의 지불 네트워크를 통해 발급자 프로세서(710)에게로 그리고 그 후 발급자(720)에게로 전송될 수 있다. 또 다른 실시예에서, 지불 정보는 신뢰 컴퓨팅 스토어(230)에 머무를 수 있고, 지불 정보를 나타내는 토큰(220)이 종래의 지불 시스템(700-720)을 거칠 수 있으며, 여기서 인지 및 이용되어, 관련 지불 정보(260)에 액세스할 수 있다. 본 실시예에서, 지불 정보(260)는 안전한 시스템 내에서 유지될 수 있고, 따라서 위험을 감소시킨다.

[0064] 토큰(220)은 다양한 용도로 교환될 수 있다. 한 예에서, 토큰(220)은 추가 정보를 전달할 수 있다. 또 다른 실시예에서, 토큰(220)은 추가 정보(260)를 거부할 수 있다. 더욱이, 토큰(220)은 사기 행위가 발생하고 있음을, 그리고 현재의 문의가 사기성이 있음을 표시할 수 있다.

[0065] **요금 분리**

[0066] 또 다른 형태에서, 제 1 판매자/센서 소유자(110)는 특정 위치로 실체(100)를 안내할 책임이 있다. 한 예로서, 아이스크림 매장은 더운 날 동안 많은 군중들의 안내를 책임진다. 군중은 아이스크림 구매 후 추가의 판매자(110)에서 또한 쇼핑할 수 있다. 추가 판매자(110)에 의한 판매분의 소정 퍼센티지가 첫번째 판매자(110)에게 공유될 수 있다. 판매자/센서 소유자(110)가 또한 신뢰 컴퓨팅 시스템(230)의 멤버일 수 있기 때문에, 대금 전송이 신뢰 컴퓨팅 네트워크(230)를 또한 이용할 수 있다. 일부 실시예에서, 공유되는 퍼센티지는 당사자들 간에 협상될 수 있다. 다른 실시예에서, 추가의 판매자에 의한 판매량 증가가 결정될 수 있고, 자동적으로 배분될 수 있다.

[0067] 다른 실시예에서, 센서(110) 소유자는 주 센서(110) 소유자일 수 있고, 주 센서(110) 소유자는 거래가 발생할 경우 주 센서(110) 소유자에게 논리적으로 가까운 보조 센서(110) 소유자로부터 보상을 수신할 수 있다. 다양한 판매자(110)의 센서(110)들은 고객의 움직임을 추적할 수 있고, 고객이 제 1 판매자/센서 소유자에게로 안내되어 그 후 추가 매장에서 구매를 할 경우, 추가 매장들은 주 판매자와 수입의 일부분을 공유할 수 있다.

[0068] **거래 리뷰**

[0069] 시스템은 사기성 과금에 대항하기 위한 추가의 기능을 또한 제공할 수 있다. 실체(100)가 거래 개시 이전에 대게 수많은 센서(110)를 만나기 때문에, 실체(100)가 추가 정보 제공에 동의하였는지 여부에 관해 중앙 컴퓨팅 위치에서 수많은 질의가 있을 수 있다. 구매가 이루어지고 추가 질의가 이루어지지 않은 경우, 사기 행위가 발생했을 확률이 높다. 마찬가지로, 사기 행위가 나타난 경우, 사기 행위를 한 사람이 네트워크 상에서 수많은 센서(110)들에 의해 감지되었을 가능성이 높다. 사기 행위 가해자의 감지된 속성(210)은 사기 행위를 추적하는데 사용될 수 있다. 더욱이, 감지된 데이터를 이용하여, 실체(110)가 구매가 이루어졌을 때와 다른 위치에 있음을 나타낼 수 있다. 개인 클라우드(120)가 많은 고유 속성들을 가질 것이기 때문에, 복제하는 것이 특히나 어려울 것이다. 마찬가지로, 사기꾼이 개인 네트워크(120)의 속성(210)을 복제하려 시도할 경우, 사기꾼의 속성(210)들 중 일부를 얻을 수 있고, 이를 이용하여 사기꾼을 추적할 수 있다.

[0070] **신뢰 네트워크를 통한 통신(이메일)**

[0071] 다른 형태에서는 실체(100)가 네트워크를 이용하여 구매 외에 기타 행위를 할 수 있다. 실체(100)는, 실체(100)가 인지되어 네트워크의 추가 기능에 액세스할 수 있도록, 권한(250)을 설정할 수 있다. 한 예로서, 실체(100)는 개인 데이터(260)에 액세스할 수 있는 권한을 소정의 판매자에게 부여할 수 있다. 실체(100)가 검증되면, 실체(100)는 임의의 컴퓨팅 시스템처럼 작업을 수행하기 위해 안전한 컴퓨팅 네트워크(230)에 일 종류의 입력 장치로 센서(110)를 이용할 수 있다. 실체(100)는 보안 카메라(110)를 들여다볼 수 있고, 기차가 늦는다는 이메일을 조수에게 전송할 것을 요청할 수 있다. 마찬가지로, 실체(100)는 컴퓨팅 장치 내로의 입력과 같이, 카메라 또는 다른 센서(110)를 이용할 수 있고, 컴퓨터를 이용하여 가용한 실질적으로 모든 옵션들이 가용할 수 있다.

[0072] 또 다른 형태에서, 실체(100)는 작업 생성을 위해 휴대형 컴퓨팅 장치(101) 내 카메라와 같은 센서(110)를 이용할 수 있고, 상기 작업은 적절한 컴퓨터 네트워크 액세스가 가용할 때 차후의 시간에 실행될 수 있다. 예를 들어, 실체(100)는 대중 교통을 이용 중일 수 있고, 매장에 대한 새로운 레벨의 권한을 생성하고자할 수 있다. 사용자는 휴대형 컴퓨팅 장치(101) 상에서 이미지 센서(108)를 이용하여 메시지를 생성 및 저장할 수 있고, 사용

자가 대중 교통 및 인근의 만족스런 컴퓨팅 액세스 네트워크에서 빠져나오면, 메시지가 전송될 수 있다.

[0073] 또 다른 예로서, 판매자가 전화 부스와 유사한 통신 스팟을 설정할 수 있다. 통신 스팟에서, 고객과 같은 실체(100)는 프라이버시를 가질 수 있고, 시스템에 의해 인지된 후 사적 정보에 액세스할 수 있다. 예를 들어, 실체(100)가 적절한 속성(210)에 의해 인지될 수 있고, 통신 스팟에서 이메일에 액세스할 수 있다. 마찬가지로, 실체(100)는 추가 매장에 맵을 요청할 수 있고, 이러한 맵이 통신 스팟에 디스플레이될 수 있다. 더욱이, 맵(또는 다른 컴퓨터 기반 객체)가 휴대형 컴퓨팅 장치(101)와 같은, 실체(100)와 관련된 다른 컴퓨팅 장치로 다운로드될 수 있다. 다른 예로서, 실체는 카메라를 볼 수 있고, 판매자를 지불 데이터에 접근할 수 있게 하는 것과 같이, 문제의 특정 판매자에 대한 액세스 변화를 요청할 수 있다.

[0074] 신뢰 네트워크는 충분한 안전장치를 갖춘 인터넷과 같은 공공 네트워크일 수 있고, 또는, 사적 네트워크일 수 있으며, 또는, 적절한 보안성을 갖춘 공공 및 사적 네트워크의 조합일 수 있다. 네트워크가 지불 처리 네트워크와 같은 사적 네트워크일 경우, 실체는 그 개인적이고 민감한 정보가 안전한 위치에 저장되어 유지되고 있다는 믿음을 굳건히 할 수 있고, 따라서 실체가 더 많은 형태의 시스템을 활용할 가능성이 높다.

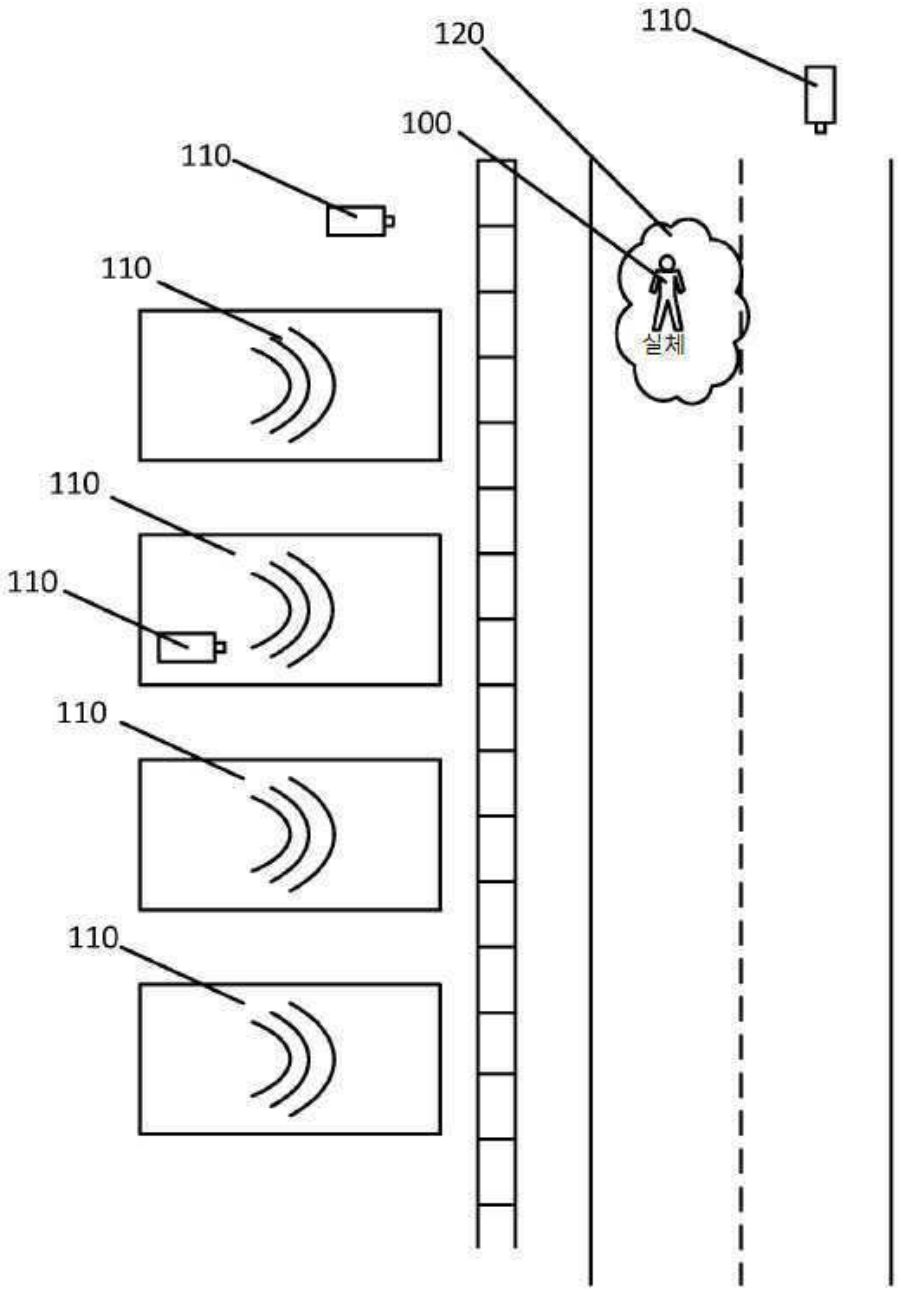
[0075] **결론**

[0076] 상술한 네트워크, 프로세서, 및 시스템은 실체(100)에 관한 민감한 데이터(260)에 대한 액세스를 실체(100)로 하여금 더 잘 제어할 수 있게 한다. 복수의 당사자가 데이터(260)를 수집하여 당사자들이 적합성 확인에 따라 이를 이용하는 대신에, 실체(100)는 이러한 데이터의 제어를 가질 것이다. 실체(100)는 그 후 실체(100)가 적합성을 확인함에 따라 데이터(260)를 이용하여, 지불 인가로부터, 추가 정보에 대한 비드 수용까지, 그리고 이러한 정보(260)에 대한 액세스 거부까지 실현할 수 있다.

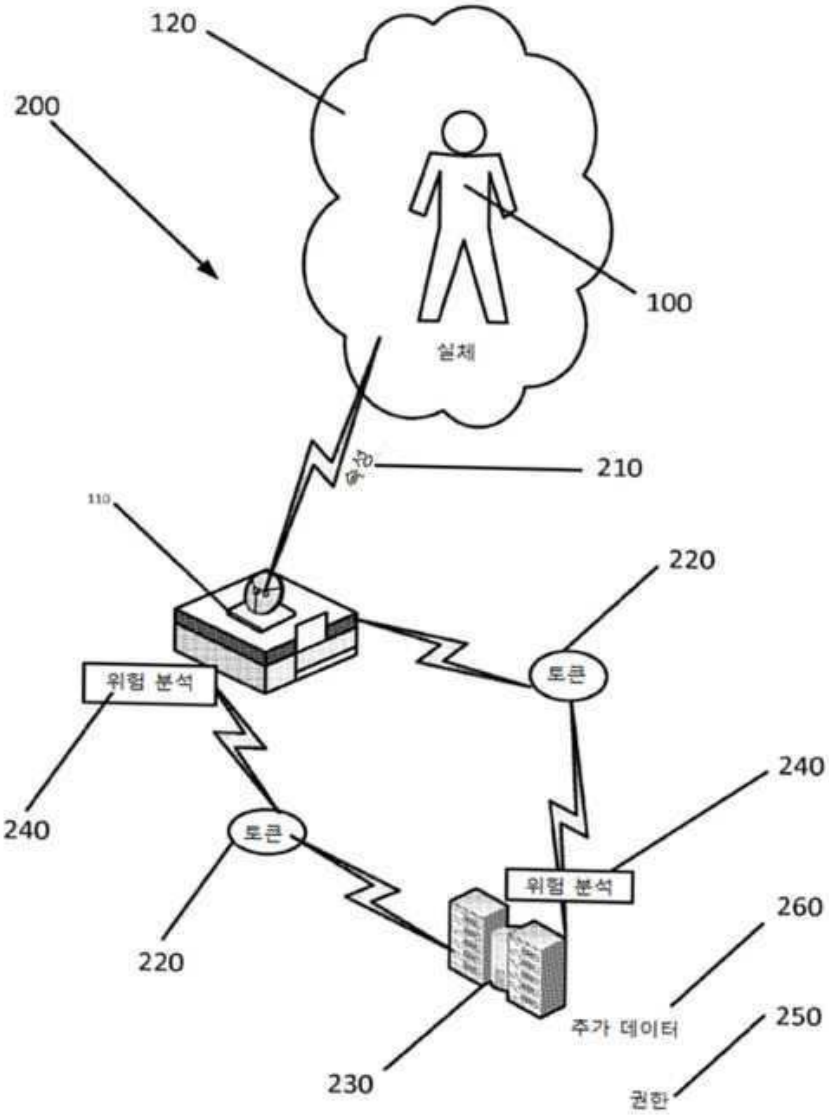
[0077] 특허 법령 및 법학의 규정에 따라, 앞서 설명된 예시적 구조들은 발명의 선호 실시예를 나타내는 것으로 여겨진다. 그러나, 발명은 그 사상 또는 범위로부터 벗어나지 않으면서 구체적으로 예시 및 설명되는 것과는 다르게 실시될 수 있음에 주목하여야 한다.

도면

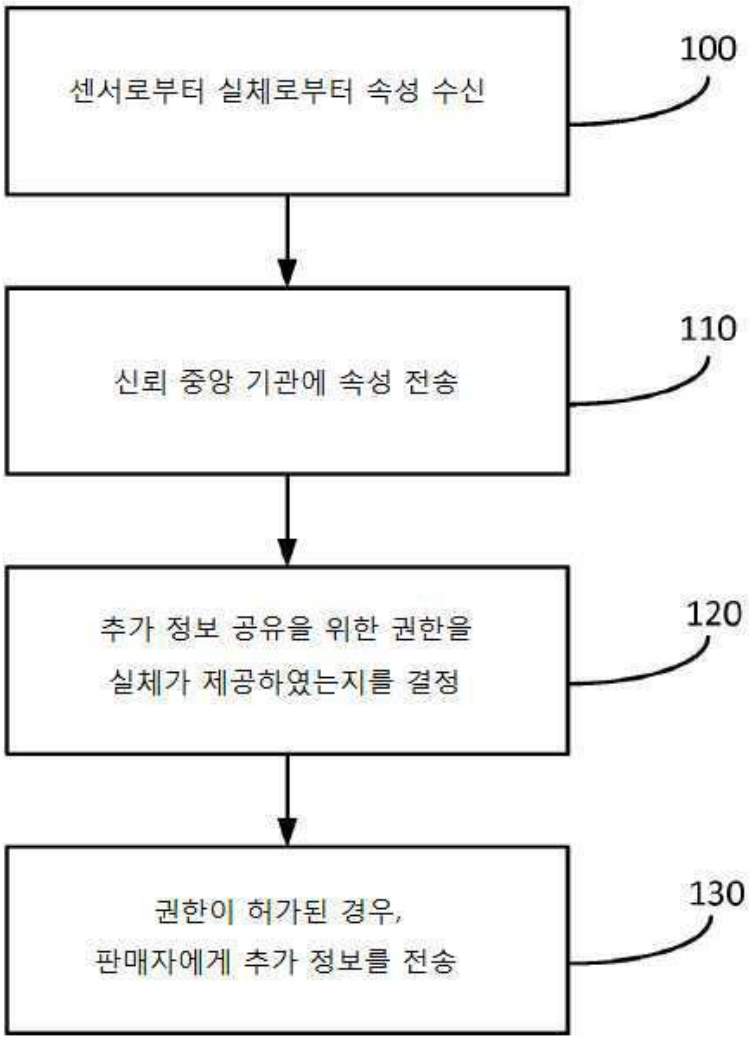
도면1



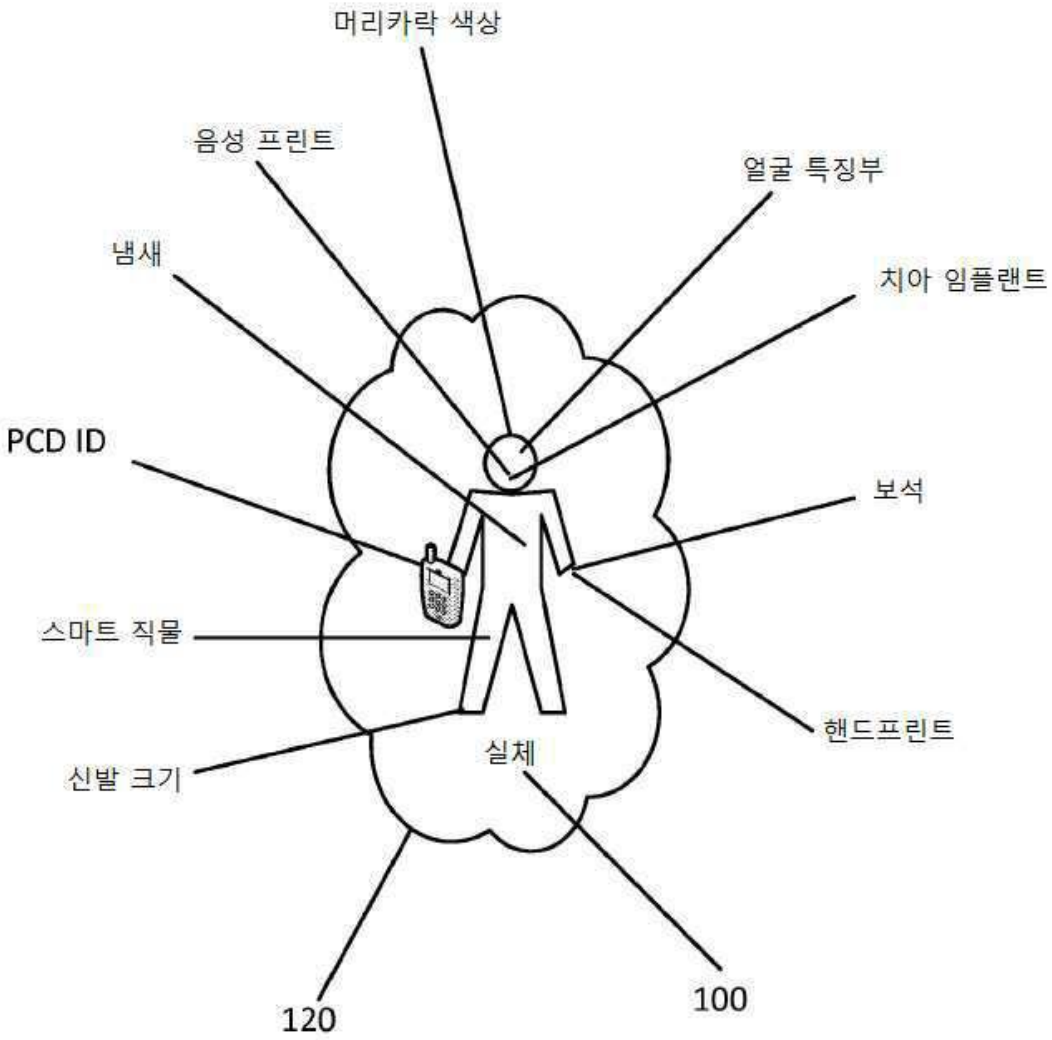
도면2


120
200
100
실체
210
110
220
위험 분석
토큰
240
240
토큰
위험 분석
220
260
주가 데이터
250
230
권한

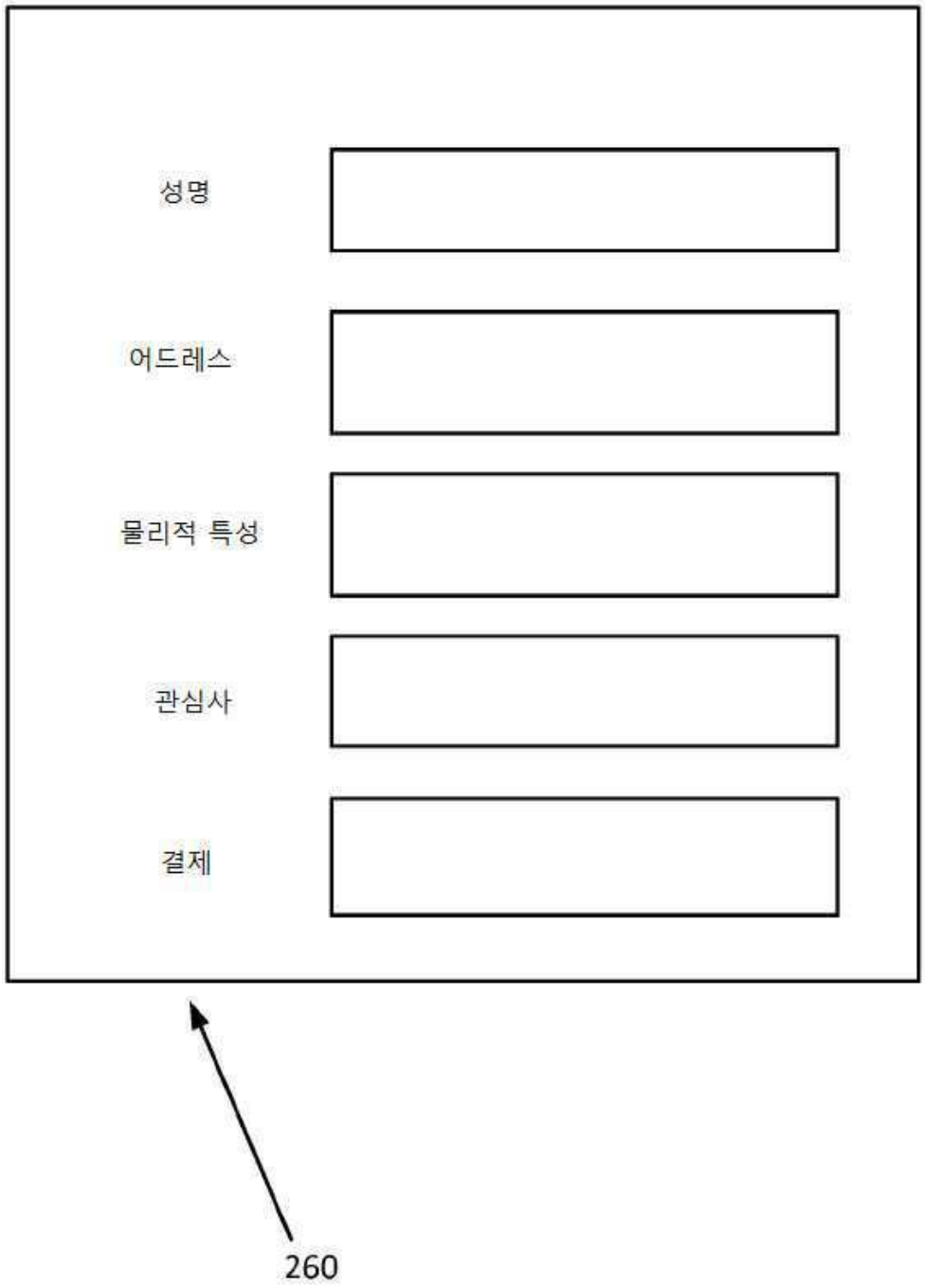
도면3


센서로부터 실체로부터 속성 수신
100
신뢰 중앙 기관에 속성 전송
110
추가 정보 공유을 위한 권한을
실체가 제공하였는지를 결정
120
권한이 허가된 경우,
판매자에게 추가 정보를 전송
130

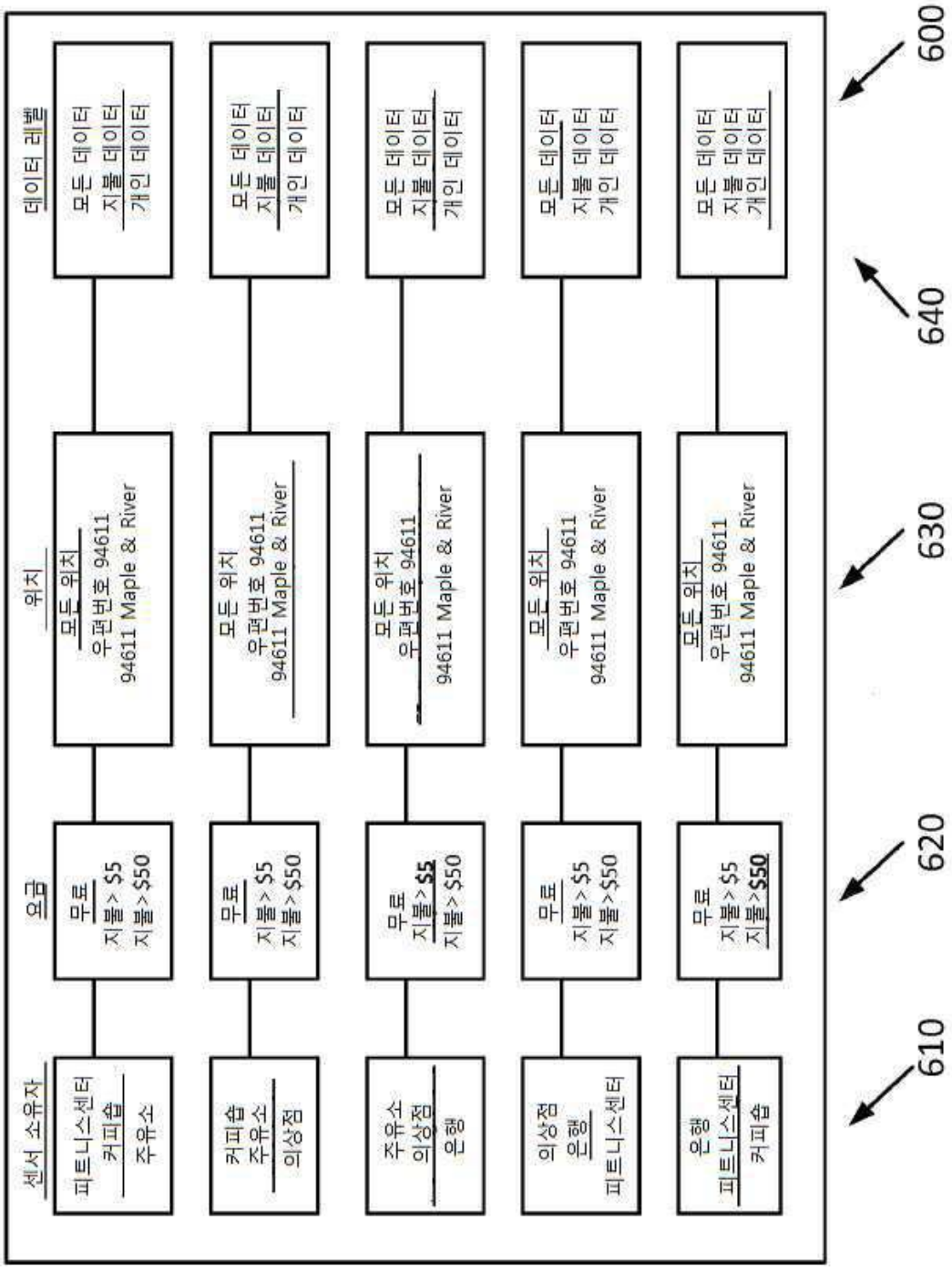
도면4


머리카락 색상
음성 프린트
얼굴 특징부
냄새
치아 임플랜트
PCD ID
보석
스마트 직물
핸드프린트
실체
신발 크기
120
100

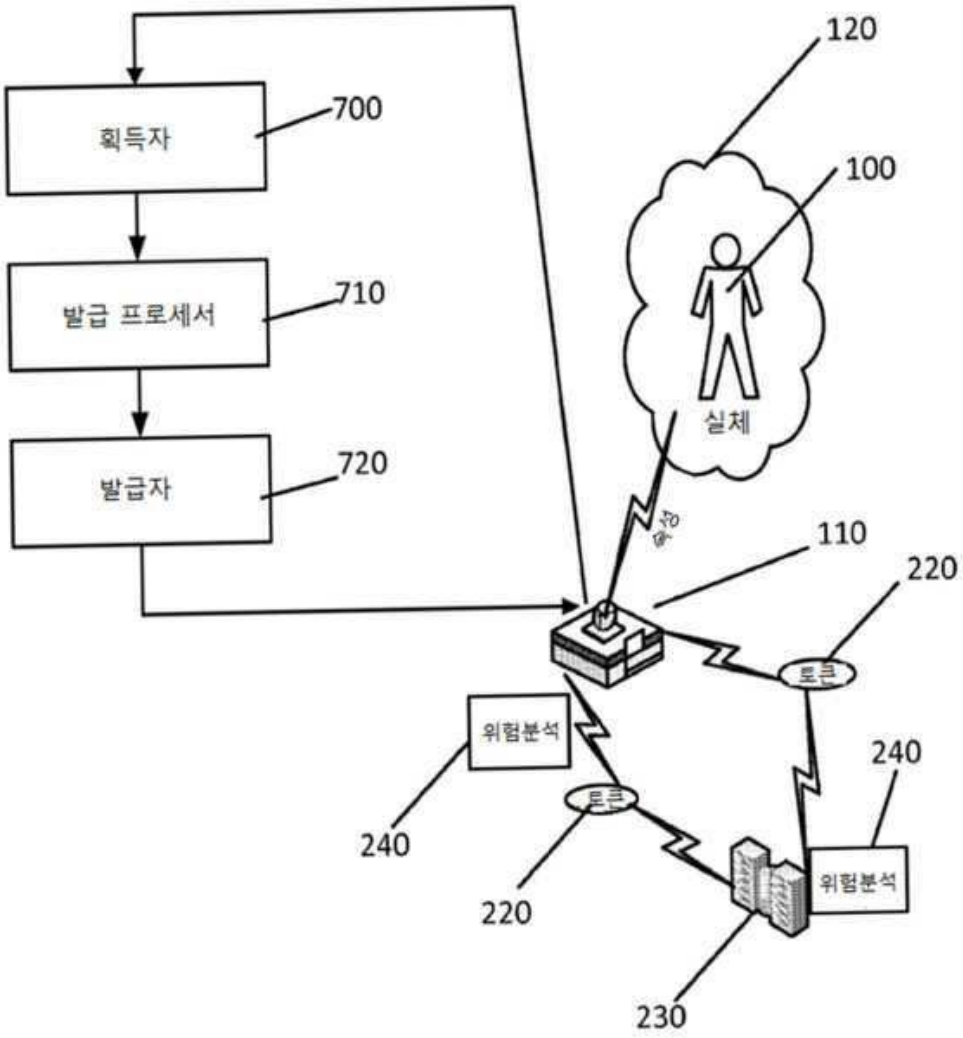
도면5a



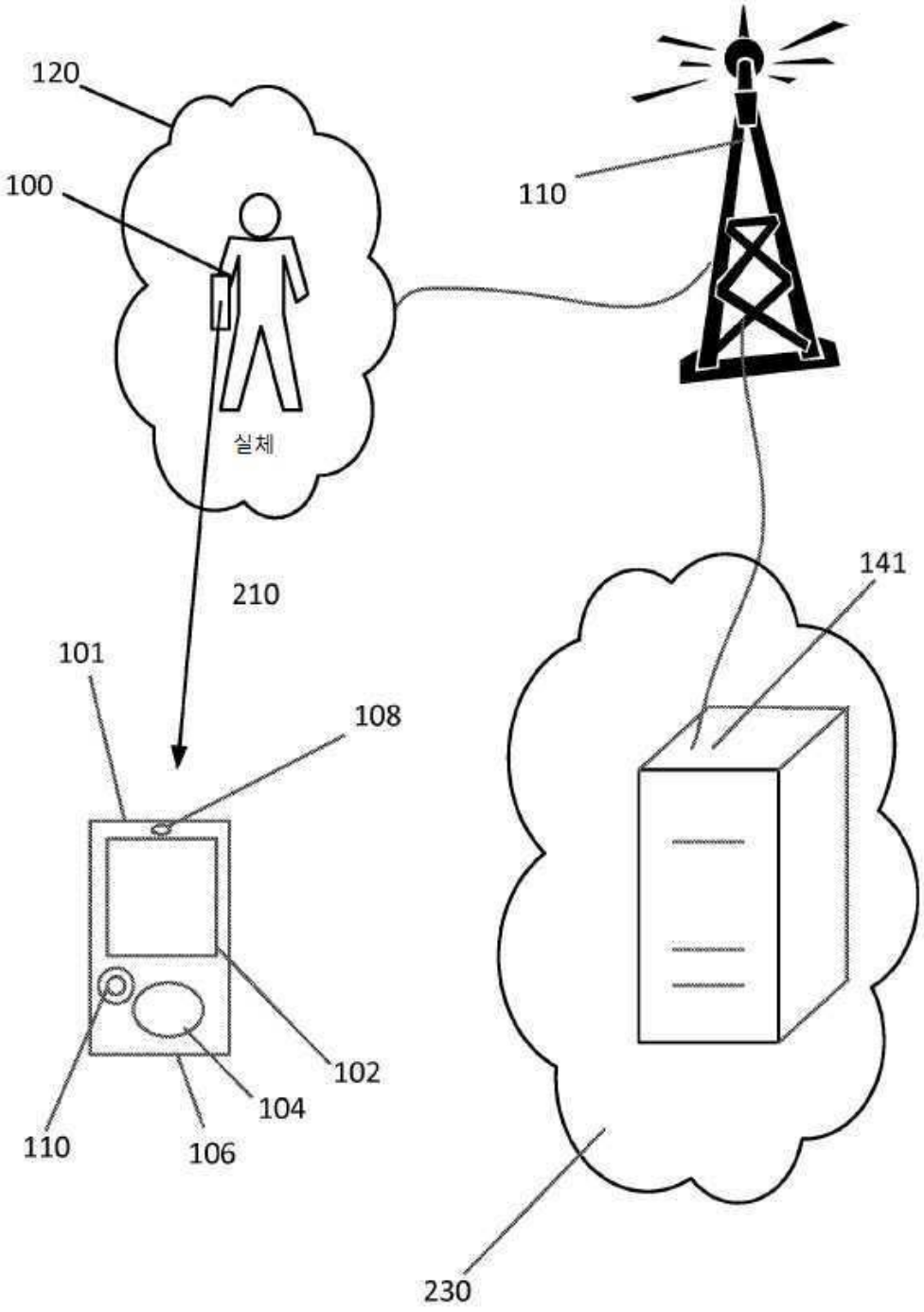
도면5b


600
640
630
620
610
데이터 레벨
위치
요금
센서 소유자
모든 데이터
지불 데이터
개인 데이터
모든 위치
우편번호 94611
94611 Maple & River
무료
지불> $5
지불> $50
피트니스센터
커피숍
주유소
커피숍
주유소
의상점
주유소
의상점
은행
의상점
은행
피트니스센터
은행
피트니스센터
커피숍

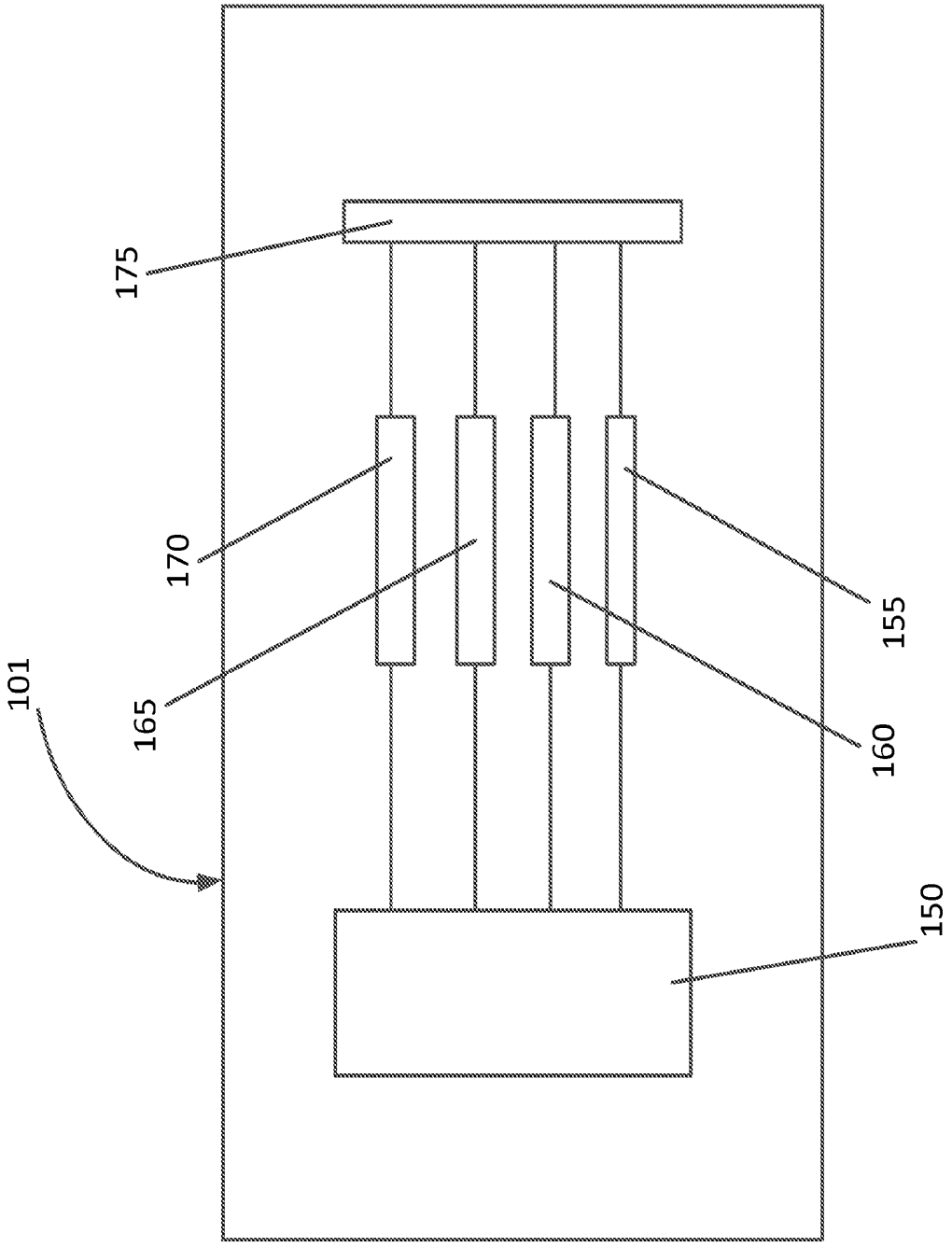
도면6


획득자
700
발급 프로세서
710
발급자
720
120
100
실체
110
220
토큰
위험분석
240
토큰
240
220
위험분석
230

도면7



도면8



도면9