(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 737 273**

(51) Int. CI.:

G06F 17/30 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
G06F 21/32 (2013.01)
G06Q 30/02 (2012.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.05.2015 PCT/US2015/033214**

(87) Fecha y número de publicación internacional: **03.12.2015 WO15184278**

(96) Fecha de presentación y número de la solicitud europea: **29.05.2015 E 15799795 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2019 EP 3149626**

(54) Título: **Red de área personal**

(30) Prioridad:

30.05.2014 US 201462005504 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.01.2020

(73) Titular/es:

VISA INTERNATIONAL SERVICE ASSOCIATION (100.0%)
900 Metro Center Boulevard
Foster City, CA 94404-2172, US

(72) Inventor/es:

FAITH, PATRICK y
HARRIS, THEODORE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Red de área personal

Antecedentes

En el pasado, las entidades que deseaban realizar pagos utilizaban un dispositivo de pago tal como una tarjeta de crédito o una tarjeta de débito. El dispositivo de pago tendría números de cuenta en este y este número de cuenta sería leído por un proveedor y verificado por una parte de confianza tal como un emisor de tarjeta. Sin embargo, garantizar la seguridad de los dispositivos de pago se ha vuelto cada vez más complejo especialmente con más transacciones realizadas a través de una red y un proveedor que no pueden examinar físicamente una tarjeta y un titular de la tarjeta para determinar el fraude. Además, las personas que cometen fraude se han vuelto más expertas técnicamente.

Además, cuando las personas usan más las redes, la capacidad de controlar los datos relacionados con ellos ha disminuido. Los sitios de red recogen los datos relevantes sobre los usuarios y usan esos datos para dirigirse a las comunicaciones al usuario sin compensar al usuario por permitir que se usen sus datos. Finalmente, algunos usuarios pueden sentirse bien compartiendo datos con ciertos sitios de red y no con otras personas y la decisión de compartir los datos puede verse influenciada por la cantidad que alguien está dispuesto a pagar para obtener los datos.

El documento US2010185871 describe un sistema de información personal que permite a los usuarios recolectar, almacenar y transferir información personal de manera segura. El sistema de información personal proporciona una ubicación central para que los usuarios almacenen información, y permite que terceros accedan de manera segura a la información de acuerdo con las reglas de acceso definidas por el usuario. Al proporcionar un área de almacenamiento central a la que terceros puede acceder electrónicamente, el sistema de información personal facilita la transferencia de información del usuario a estos terceros. Para controlar el acceso a la información personal almacenada de un usuario, las reglas de acceso definidas por el usuario definen las condiciones bajo las cuales terceros pueden acceder a la información almacenada. El sistema también proporciona dispositivos de autenticación de usuario que incluyen componentes de reconocimiento biométricos y una pantalla táctil. Los dispositivos de autenticación de usuario pueden instalarse en ubicaciones externas para permitir que un usuario autorice la transferencia de información personal a terceros.

Sumario de la invención

Los aspectos de la presente invención se enumeran por las reivindicaciones adjuntas.

Se describe un nuevo sistema, proceso y método para controlar los datos relacionados con una entidad. Una entidad puede almacenar varios niveles de datos sensibles y personales en un entorno informático seguro. La entidad puede crear reglas de permiso que permitan compartir o no los datos en dependencia de las circunstancias y la situación. A medida que una entidad tal como un humano se mueve por la vida, la entidad puede estar en contacto con numerosos dispositivos electrónicos que actúan como sensores tales como redes inalámbricas, redes fotónicas, redes Bluetooth, grabadores de sonido, grabadores de aroma, grabadores de video, etc. La entidad puede compartir un token que puede permitir que un sensor u operador del sensor acceda a varios niveles de los datos sensibles almacenados en el entorno informático seguro.

Breve descripción de los dibujos

La Figura 1 ilustra una ilustración de muestra de los sensores que una entidad puede encontrar;
La Figura 2 ilustra una entidad con una interacción de red de computadoras personal con sensores;
La Figura 3 ilustra un método para controlar el acceso a datos sobre una entidad;
La Figura 4 ilustra algunos atributos de muestra de una entidad;
La Figura 5a ilustra una pantalla de entrada para añadir datos personales al sistema informático confiable;
La Figura 5b ilustra una pantalla de entrada para crear permisos para una pluralidad de entidades;
La Figura 6 ilustra una ilustración de muestra de una nube de red personal que interactúa con un sistema de pago;
La Figura 7 ilustra una entidad con un dispositivo informático portátil que interactúa con un dispositivo informático de tipo servidor;
La Figura 8 ilustra un dispositivo informático portátil; y
La Figura 9 ilustra un dispositivo informático de tipo servidor.

Descripción

A un alto nivel, se describe un nuevo sistema, proceso y método para controlar los datos relacionados con una entidad. Como se ilustra en la Figura 1, a medida que una entidad 100 tal como un humano se mueve por la vida, la entidad 100 puede estar en contacto con numerosos dispositivos electrónicos que actúan como sensores 110 tales como redes inalámbricas, redes fotónicas, redes Bluetooth, grabadores de sonido, receptores de aroma, grabadores de video, etc. Además, cada uno de estos sensores 110 está tomando los datos e intenta coincidir con los datos

adicionales de la entidad 100 para crear un perfil en la entidad 100 que puede usarse para fines de marketing, todos sin el permiso explícito de la entidad 100.

Red personal

Una red personal 120 intenta abordar el problema de controlar el acceso a los datos sensibles sobre una entidad 100. Una entidad 100 puede crear una lista de sensores 110, redes u operadores de redes de los que la entidad 100 está dispuesta a comunicar información adicional. Además, una entidad 100 también puede establecer umbrales para recibir ofertas de sensores 110 para intercambiar información adicional. Como se ilustra en la Figura 1, mientras se mueve por la vida, pueden encontrarse muchos sensores 110, desde cámaras de luz roja hasta redes Bluetooth para redes inalámbricas 802.11. Para las redes que la entidad 100 ha admitido, un token de la entidad 100 puede comunicarse a una fuente de confianza donde la información deseada puede comunicarse a la red y la comunicación puede tener nuevamente la forma de un token. El token puede contener suficientes datos para permitir una transacción de compra.

La Figura 2 puede ser una ilustración de alto nivel de una modalidad del sistema propuesto 200. Una entidad 100 puede moverse en el rango de un sensor 110 donde pueden recopilarse los atributos 210 de la entidad. Los atributos 210 pueden comunicarse en forma de tokens 220 desde la entidad a los sensores 110. En otras modalidades, los atributos detectados 210 pueden traducirse en un token 220. El token 220 puede entonces comunicarse a un servicio informático central 230 el cual puede considerarse un sistema informático confiable. El token 220 puede revisarse para determinar el fraude u otras características no deseadas mediante una aplicación de análisis de riesgos 240. Si el token 220 no es fraudulento, el sistema informático central 230 puede revisar el token 220 para determinar si la entidad 100 ha otorgado permiso 250 al sensor 110 (u operador del sensor 110) para obtener información adicional 260 sobre la entidad 100. Si no se ha concedido el permiso 250, el sistema informático central 230 puede quedar en silencio o puede enviar un mensaje de rechazo.

Más específicamente, con referencia a la Figura 3, puede ilustrarse un método, proceso y sistema basado en computadora para controlar el acceso a los datos sobre una entidad 100. En el bloque 100, los datos de atributo 210 pueden detectarse desde la entidad 100 en un dispositivo sensorial 110.

Dispositivos sensoriales

Los sensores 110 pueden ser muchos y variados. Aunque no se trata de ser exhaustivo o limitante, algunos ejemplos pueden incluir dispositivos de comunicación inalámbrica 802.11, dispositivos de comunicación inalámbrica en diferentes bandas de frecuencia tales como comunicación infrarroja o de 60 Mhz, cámaras, cámaras de video, sensores fotónicos, dispositivos de comunicación Bluetooth, sensores de sonido (micrófonos), sensores de olor, sensores de calor y cualquier otro sensor 110 que pueda ser no intrusivo pero que sea capaz de recopilar datos en una entidad 100. Los sensores 110 pueden diseñarse o destinarse para un propósito diferente pero pueden adaptarse para comunicarse con el sistema 200. Por ejemplo, una cámara de seguridad puede instalarse inicialmente con fines de seguridad pero puede adaptarse para ser un sensor 110 en el sistema descrito 200.

Cabe señalar que los dispositivos de comunicación inalámbrica tales como los enrutadores Wifi no se consideran a menudo sensores 110. Sin embargo, la comunicación con los dispositivos inalámbricos es a menudo de dos maneras y la entidad 100 puede tener que proporcionar información para comunicarse con el dispositivo inalámbrico, incluso si la comunicación es simplemente recopilar el nombre del dispositivo inalámbrico o una identidad del dispositivo informático en comunicación con el dispositivo inalámbrico. El nombre de un dispositivo, tal como una dirección MAC, puede ser suficiente para que una red identifique una entidad 100 y comience a comunicar los anuncios resultantes, incluso cuando la entidad 100 está en comunicación con una red nueva desconocida ya que la dirección MAC puede coincidir con búsquedas anteriores que pueden usarse para guiar los anuncios resultantes. Por lo tanto, controlando los datos compartidos con fuentes inalámbricas, la entidad 100 puede tomar el control de sus datos 260 y asegurar que los datos 260 se compartan solo cuando se desee.

Lógicamente, una entidad 100 puede pasar a través de una variedad y una pluralidad de sensores 110 en un día y cada uno de estos sensores 110 puede desear comunicarse con el dispositivo informático central 230 para determinar si más información 260 está disponible sobre la entidad 100.

En relación con esto, los atributos de la entidad 210 cambian a medida que la entidad 100 cambia de ubicación y los diferentes sensores 110 están en el rango relevante. Por ejemplo, una entidad 100 puede encontrarse en un coche y puede pasar a través de un aparato de recolección de peajes y puede pasar por numerosas conexiones Bluetooth y conexiones inalámbricas. El carro puede proporcionar atributos únicos ya que tiene una placa con licencia, una apariencia distintiva y puede transmitir un identificador único. Además, la entidad 100 puede no llevar una camisa en el carro ya que el clima puede controlarse dentro del carro. Más tarde, en el día, la entidad 100 puede salir del carro y ponerse una camisa. Por lo tanto, los atributos 210 del carro (placa con licencia, color, número de identificación) ya no están disponibles. Sin embargo, ahora se pueden añadir los atributos 210 de la camisa. Además, los atributos 210 pueden cambiar en el año y a través de la vida útil de una entidad 100.

Datos de atributo

Los atributos 210 pueden detectarse para ayudar a identificar entidades 100 o a diferenciar entre entidades 100. Los atributos 210 son amplios y variados y pueden ser virtualmente cualquier elemento o característica que pueda detectarse por el sensor 110 y usarse para diferenciar entre entidades 100. Ejemplos de atributos obvios 210 pueden ser una cara de una entidad 100, una dirección MAC de un dispositivo informático portátil asignado a una entidad 100 o un ID de RF de una mascota. Sin embargo, los atributos 210 pueden ser menos evidentes y estar más ocultos ya que los usuarios no desean que se haya creado una red de área personal 120 de atributos 210. Por ejemplo, un atributo 210 puede incluir una mano, una pieza de joyería, una tela, un aroma, un sonido, etc. Algunos atributos 210 pueden ser activos como un teléfono inteligente que pasa por una dirección MAC, una configuración del navegador, un tamaño de la memoria, aplicaciones en el dispositivo, etc. mientras que otros atributos 210 pueden ser pasivos tal como las características ópticas de una cara o de una mano.

Los atributos adicionales 210 pueden resultar de los elementos creados a propósito. A modo de ejemplo, una tela puede proporcionar una respuesta dada cuando se expone a cierta radiofrecuencia. Como otro ejemplo, la pieza de joyería puede proporcionar una respuesta conocida cuando recibe ondas de radio en una frecuencia predeterminada. En otro ejemplo, un empaste dental puede incluir un dispositivo que puede proporcionar una respuesta conocida cuando recibe ondas de radio en una frecuencia conocida. La Figura 4 puede ilustrar algunos atributos de muestra 120 de una entidad 100.

Los atributos 210 relacionados con las imágenes pueden asumir una variedad de dimensiones de manera que el reconocimiento puede ocurrir de varias maneras. Una primera dimensión puede ser un mapeo de la separación de las características faciales. Una segunda dimensión puede añadirse para determinar aún más la profundidad de las características faciales. Una tercera dimensión puede añadirse mediante el uso de múltiples sensores o un sensor sofisticado. El uso de múltiples dimensiones puede permitir además que las entidades se reconozcan aún más con mayor precisión.

Lógicamente, los sensores 110 pueden estar en comunicación con una red de computadoras de manera que la imagen puede comunicarse a la autoridad central 230 para verificarse. Como se mencionó anteriormente, los datos del atributo sensado 210 pueden comunicarse a una autoridad central 230. En algunas modalidades, los datos del atributo 210 pueden convertirse a una forma comprimida. En algunas modalidades, la forma comprimida puede convertirse en un token 220 que se comunica con la autoridad informática central 230. En algunas modalidades, la conversión ocurre en el dispositivo sensor 110. En otras modalidades, la conversión ocurre cuando la imagen del atributo 210 se comunica a la autoridad central 230.

La conversión a un token 220 puede producirse de varias maneras. A un nivel alto, la tokenización puede producirse de tal manera que oculte la fuente del mensaje y el mensaje tal como a través de encriptación pero que permita que el mensaje y la fuente sean desencriptados por el sistema informático central confiable 230. Además, el token 220 puede ser revisado por aplicaciones de software de seguridad o análisis de riesgos 240 para asegurar que el contenido malicioso no se administre al sistema informático central 230.

Entidades

Las entidades 100 pueden ser cualquier persona, organización u otra cosa que pueda tener información 260 que pueda considerarse sensible o personal. Lógicamente, una persona puede considerarse una entidad 100. Además, una corporación o cualquier otra organización legal puede considerarse una entidad 100 dado que la información sensible 260 sobre la organización puede estar disponible. Además, los grupos libremente organizados también pueden considerarse una entidad 100. A modo de ejemplo, un grupo de amigos puede jugar póker cada semana y el grupo puede considerarse una entidad 100. Lógicamente, una entidad más grande 100 puede estar formada por un grupo de entidades 100. A un nivel incluso menor, cada dispositivo informático puede contener información que puede considerarse sensible y cada dispositivo informático puede considerarse una entidad 100. Por ejemplo, un usuario puede tener un teléfono inteligente únicamente con fines de trabajo y ese teléfono puede ser una primera entidad 100 y el usuario puede tener un segundo teléfono para usos personales que pueden tener datos sensibles muy diferentes 260 y el segundo teléfono puede considerarse una entidad separada 100.

Información sensible

Los datos sensibles 260 que merece la pena proteger pueden depender de la entidad 100. Puede necesitarse que determinados datos 260 lleven a cabo transacciones fraudulentas, tal como un nombre y un número de cuenta. Al mismo tiempo, algunas entidades 100 pueden considerar incluso más información para ser sensibles 260 y ser dignas de protección. Por ejemplo, puede considerarse que una dirección o número de teléfono es información sensible 260 para un actor famoso mientras que otras entidades 100, como un proveedor, pueden promover activamente la diseminación de un número telefónico y una dirección. Por lo tanto, el actor famoso puede marcar la dirección y el número de teléfono como sensibles 260 y solo puede comunicarse con la dirección del actor. En el sentido opuesto, un proveedor puede compartir un número de teléfono y una dirección con tantas personas como sea posible. Una interfaz de usuario puede usarse para permitir que una entidad 100 especifique que determinados datos son sensibles

260 y solo deben compartirse con permiso mientras que otros datos pueden compartirse prácticamente a cualquier persona.

La Figura 5a puede ser una ilustración de una pantalla para introducir datos sensibles 260. Las entidades 100 pueden tener la opción de ingresar la mayor cantidad de información que deseen. Por ejemplo, un proveedor puede ingresar o desear ingresar mucha información que pueda compartirse con clientes potenciales mientras que un actor famoso que desee privacidad puede ingresar la información mínima necesaria para trabajar de manera productiva en la vida moderna.

Sistema informático confiable

El sistema informático 230 puede ilustrarse en la Figura 7 y puede incluir un sistema informático confiable que está en comunicación con una variedad de sensores 110. El sistema informático confiable 230 puede proporcionar además un análisis de los tokens 220 para abordar cualquier preocupación sobre el fraude. El sistema informático confiable 230 puede considerarse el guardián de la información de la entidad 260 y a menos que la entidad 100 haya autorizado la liberación de información 260 a un sensor 110 (o al propietario del sensor), el sensor 110 solo se queda con la información que puede reunir por sí mismo. El sistema informático 230 puede tener una única ubicación o puede extenderse entre una variedad de ubicaciones. Para los usuarios del sistema 230, el sistema 230 puede parecer que es una única computadora pero el sistema 230 puede propagarse entre una pluralidad de sistemas informáticos 230 que pueden propagarse por todo el mundo como un tipo de diseño de computación en la nube.

La Figura 7 puede ser una ilustración de alto nivel de algunos de los elementos en un sistema informático de muestra 230 que puede configurarse físicamente para ejecutar las diversas modalidades del método. El sistema informático 230 puede ser un dispositivo informático dedicado 141, un dispositivo informático portátil dedicado 101, una aplicación en el dispositivo informático 141, una aplicación en el dispositivo informático portátil 101 o una combinación de todos estos. La Figura 8 puede ser una ilustración de alto nivel de un dispositivo informático portátil 101 que se comunica con un dispositivo informático remoto 141 a través de un sensor 110 pero la aplicación puede almacenarse y accederse en una variedad de maneras. Adicionalmente, la aplicación puede obtenerse en una variedad de maneras tal como desde una tienda de aplicaciones, desde un sitio web, desde un sistema Wifi de almacenamiento, etc. Puede haber varias versiones de la aplicación para aprovechar los beneficios de diferentes dispositivos informáticos, diferentes lenguajes informáticos y diferentes plataformas de API.

En una modalidad, un dispositivo informático portátil 101 puede ser un dispositivo que funciona mediante el uso de una fuente de energía portátil 155 tal como una batería (Figura 8). Con referencia a la Figura 7, el dispositivo informático portátil 101 puede tener además una pantalla 102 que puede o no ser una pantalla sensible al tacto. Más específicamente, la pantalla 102 puede tener un sensor de capacitancia, por ejemplo, que puede usarse para proporcionar datos de entrada al dispositivo informático portátil 101. En otras modalidades, un panel de entrada 104 tal como flechas, ruedas de desplazamiento, teclados, etc., pueden usarse para proporcionar información al dispositivo informático portátil 101. Además, el dispositivo informático portátil 101 puede tener un micrófono 106 que puede aceptar y almacenar datos verbales, una cámara 108 para aceptar imágenes y un altavoz 110 para comunicar sonidos.

El dispositivo informático portátil 101 puede ser capaz de comunicarse con un dispositivo informático 141 o una pluralidad de dispositivos informáticos 141 que conforman una nube de dispositivos informáticos 111. El dispositivo informático portátil 101 puede ser capaz de comunicarse de diversas maneras. En algunas modalidades, la comunicación puede cablearse tal como a través de un cable Ethernet, un cable USB o un cable RJ6. En otras modalidades, la comunicación puede ser inalámbrica tal como a través de dispositivos Wi-Fi (estándar 802.11), Bluetooth, comunicación celular o de comunicación de campo cercano. La comunicación puede dirigirse al dispositivo informático 141 o puede ser a través de un dispositivo de comunicaciones o red de dispositivos tal como servicio celular, a través de Internet, a través de una red privada, a través de Bluetooth, a través de comunicaciones de campo cercano, etc. La Figura 8 puede ser una ilustración simplificada de los elementos físicos que conforman un dispositivo informático portátil 101 y la Figura 9 puede ser una ilustración simplificada de los elementos físicos que conforman un dispositivo informático de tipo servidor 141.

Con referencia a la Figura 8, un dispositivo informático portátil de muestra 101 puede configurarse físicamente de acuerdo con un método para formar parte del sistema. El dispositivo informático portátil 101 puede tener un procesador 150 que se configura físicamente de acuerdo con instrucciones ejecutables por computadora. Este puede tener un suministro de energía portátil 155 tal como una batería que puede ser recargable. Este también puede tener un módulo de video y sonido 160 que ayuda en la visualización del video y el sonido y puede apagarse cuando no se utiliza para conservar la energía y la vida útil de la batería. El dispositivo informático portátil 101 puede tener además una memoria volátil 165 y una memoria no volátil 170. También puede haber un bus de entrada/salida 175 que transmite datos hacia y desde los diversos dispositivos de entrada de usuario tales como el micrófono 106, la cámara 108 y otras entradas 102, etc. Este también puede controlar la comunicación con las redes, ya sea a través de dispositivos inalámbricos o cableados. Por supuesto, esta es solo una modalidad del dispositivo informático portátil 101 y el número y tipos de dispositivos informáticos portátiles 101 se limitan solamente por la imaginación. El dispositivo informático portátil 101 puede actuar como la pantalla 102 o puede ser una parte de la pantalla 102.

Los elementos físicos que constituyen el dispositivo informático remoto 141 pueden ilustrarse además en la Figura 9. A un nivel alto, el dispositivo informático 141 puede incluir un almacenamiento digital tal como un disco magnético, un disco óptico, almacenamiento flash, almacenamiento no volátil, etc. Los datos estructurados pueden almacenarse en el almacenamiento digital tal como en una base de datos. El servidor 141 puede tener un procesador 300 configurado físicamente de acuerdo con las instrucciones ejecutables por computadora. Este también puede tener un módulo de video y sonido 305 que ayuda en la visualización del video y el sonido y puede apagarse cuando no se utiliza para conservar la energía y la vida útil de la batería. El servidor 141 también puede tener una memoria volátil 310 y una memoria no volátil 315.

La base de datos 325 puede almacenarse en la memoria 310 o 315 o puede estar separada. La base de datos 325 puede además ser parte de una nube del dispositivo informático 141 y puede almacenarse de una manera distribuida a través de una pluralidad de dispositivos informáticos 141. También puede haber un bus de entrada/salida 320 que transmite datos hacia y desde los diversos dispositivos de entrada del usuario tales como el micrófono 106, la cámara 108, las entradas 102, etc. El bus de entrada/salida 320 también puede controlar la comunicación con las redes, ya sea a través de dispositivos inalámbricos o por cable. En algunas modalidades, la aplicación puede estar en el dispositivo informático local 101 y en otras modalidades, la aplicación puede ser remota 141. Por supuesto, esta es solo una modalidad del servidor 141 y el número y tipos de dispositivos informáticos 141 se limitan solamente por la imaginación.

Con referencia de nuevo a la Figura 3, en el bloque 110, los datos de atributo 210 pueden comunicarse a través de una red de computadoras a un sistema informático confiable 230 para verificar que los datos de atributo 210 cumplen con las reglas del permiso 250 creadas por el usuario para permitir que se comunique información adicional 260. Como se mencionó anteriormente, los datos de atributo 210 pueden convertirse en un token 220 que puede comunicarse a través de la red. La conversión puede proporcionar comodidad a las entidades 100 que sus datos personales 260 pueden no comunicarse de manera que se entienda fácilmente por entidades nefariosas que pueden intentar adherirse a la red de computadoras. La conversión puede producirse a través de un esquema de tipo de encriptación o a través de otra manera tal que los datos adicionales 260 pueden entenderse por el sistema informático confiable 230 pero no por otros que pueden tener acceso a la red de computadoras.

Análisis del fraude

Además, como se mencionó brevemente, los tokens 220 que se comunican a través de la red de computadoras pueden revisarse por razones de seguridad. De esta manera, pueden minimizarse intentos de ruptura en el servicio informático seguro 230. Por ejemplo, los datos de atributo 210 pueden analizarse para determinar las características fraudulentas. Además, las entidades 100 que usan el sistema 230 pueden tener más comodidad al saber que los mensajes en la red son revisados por seguridad.

El análisis de fraude 240 puede ver la transacción en términos de riesgo. Los tokens 220 y los datos representados por el token 220 pueden analizarse para determinar si es más probable que los datos sean fraudulentos. Además, el análisis de fraude 240 puede usar la red pura o la inteligencia artificial para mejorar continuamente el análisis. Por ejemplo, el análisis puede determinar con el tiempo que es imposible para un único usuario estar en lugares diferentes al mismo tiempo. De manera similar, sería muy probable que alguien que sea alérgico al gluten compre productos que contengan gluten y el análisis puede aprender esto con el tiempo.

Se puede examinar múltiples atributos 210 para determinar si un token 220 es fraudulento. Por ejemplo, un primer sensor 110 puede observar un primer atributo 210 de la entidad 100 y un segundo sensor 110 puede observar un segundo atributo 210 de la entidad 100. Ambos atributos 210 observados de la entidad 100 pueden revisarse y probarse su compatibilidad cruzada para garantizar una identificación adecuada y confiable de la entidad 100. Como un ejemplo y sin limitación, si se determina que un primer atributo 210 (características faciales) pertenece a una primera entidad 100 pero se determina que un segundo atributo 210 (dirección MAC del teléfono) pertenece a una segunda entidad 100, puede determinarse que es probable que ocurra el fraude. De manera similar, si se determina que un primer atributo 210 (color del pelo) pertenece a una primera entidad 100 y se determina que un segundo atributo 210 (firma RFID anular) pertenece a la primera entidad 100, puede determinarse que es probable que el fraude no ocurra. Lógicamente, la acumulación de datos de atributo 210 para una entidad 100 puede producirse durante un período de tiempo y los atributos 210 observados en proximidad de tiempo cercano pueden compararse para asegurar que se observe la misma entidad 100.

El servicio de riesgo 240 puede acumular el atributo relevante 210 observado y puede realizar uno o más algoritmos de análisis para determinar si es probable el fraude. El servicio de riesgo 240 puede ser parte del dispositivo informático de confianza central 230 pero puede examinar además las comunicaciones tales como los tokens 220 que se producen sobre la red. Al revisar las comunicaciones antes de alcanzar la red confiable, las comunicaciones nefariosas pueden determinarse y ubicarse incluso antes de llegar al servidor de confianza 230.

El servicio de análisis de riesgos 240 puede asumir una variedad de formas físicas. En una modalidad, un sistema informático está físicamente configurado para funcionar como el servicio de riesgo 240. Los chips de computadora pueden estar físicamente configurados e instalados como parte del servicio de riesgo 240. En aún otra modalidad, los

chips de computadora pueden configurarse físicamente de acuerdo con instrucciones ejecutables por computadora y las instrucciones pueden cambiar o actualizarse con el tiempo. Como resultado, los chips de computadora tales como un procesador o memoria pueden cambiar su estructura física como resultado de las instrucciones ejecutables por computadora actualizadas.

En aun otra modalidad, el servicio de riesgo 240 puede propagarse a través de la red. Por ejemplo, si un sensor 110 desea comunicar los datos de atributo 210 al sistema informático central 230, los datos de atributo 210 pueden primero analizarse en cuanto al servicio de riesgo 240 el cual puede residir en un dispositivo informático 230 en o cerca de la ubicación del sensor 110. De esta manera, las comunicaciones fraudulentas o nefariosas pueden detenerse antes de avanzar mucho por la red.

Permisos

Con referencia de nuevo a la Figura 3, en el bloque 120 en el dispositivo informático central 230, los atributos 210 pueden analizarse para determinar si la entidad 100 tiene permisos predeterminados para permitir que se comunicen datos adicionales sobre la entidad 100. La entidad 100 puede usar una aplicación con una interfaz de usuario para determinar cómo y cuándo se comunican los datos adicionales con respecto a la entidad 100 a otras personas que usan la red. Los permisos 250 pueden especificarse de varias maneras. En un ejemplo, los permisos 250 pueden ser específicos del sensor 110. A modo de ejemplo, si una entidad compra constantemente café en la Casa de Café en la esquina de Maple Avenue y River Road en una ciudad de Anytown, Estados Unidos, la entidad 100 puede permitir información adicional tal como información de pago que se comparta con la cámara de video (sensor) 110 y equipos informáticos relacionados para hacer funcionar el sistema de pago en la Casa de Café.

Aún en otra modalidad, el permiso puede ser más amplio y puede ser específico de la ubicación. Con referencia nuevamente al ejemplo de la Casa de Café, a todos los sensores 110 en la Casa de Café en Maple & River tal como el sistema Wifi, las cámaras de video, las cámaras fijas, los sensores de aroma, etc., se le puede otorgar permiso para obtener información adicional 260 sobre la entidad 100 tal como información de pago.

En otra modalidad, el permiso 250 puede ser específico del sensor 110. La entidad 100 puede confiar en todas las Casas de Café en los Estados Unidos y puede desear compartir información adicional con todas las Casas de Café en los Estados Unidos. De esta manera, la entidad 100 puede ser capaz de caminar hacia cualquier Casas de Café en los Estados Unidos y la Casa de Café puede ser capaz de obtener información adicional sobre la entidad 100, incluyendo la información de pago.

Aún como otra modalidad, la entidad 100 puede permitir a TODOS los usuarios de la red que sirven café tener permiso para obtener información adicional sobre la entidad 100. En esta disposición, la entidad 100 puede entonces permitir que los datos se comunicen a cualquier lugar de servicio del café y la entidad 100 puede obtener café en cualquiera de estas ubicaciones.

Creación de permisos

La Figura 6 puede ser una ilustración de una pantalla de creación 600 de permisos de muestra 250. La pantalla de permisos 600 puede crearse en cualquier dispositivo informático que tenga acceso a la red y sea capaz de visualizar y recibir información de entrada que incluya dispositivos informáticos portátiles. Puede haber múltiples campos de entrada tales como un nombre del propietario del sensor 610, un honorario requerido para obtener información adicional 620, una ubicación que se le conceda 630 y un nivel de permisos 640 que puede comenzar en un alto nivel y puede permitir que una entidad 100 haga los permisos 250 progresivamente más específicos. Además, los permisos 250 que se hayan creado mientras están en ubicaciones del proveedor/sensor 110 también pueden enumerarse y pueden modificarse.

De manera similar, la entidad 100 puede configurar los permisos 250 mientras esté en marcha. Por ejemplo, si un usuario está en el aeropuerto, el usuario puede establecer los permisos 250 para comunicarse con los conductores de limusinas pero no con los conductores de taxis. Como otro ejemplo, si el usuario desea comida china, el usuario puede configurar los permisos para comunicarse con los restaurantes que sirven comida china pero no con los restaurantes que sirven pizza.

Oferta

En aun otra modalidad, las reglas del permiso 250 pueden establecer un valor monetario mínimo y si el propietario del sensor 110 está dispuesto a pagar el valor mínimo del valor monetario, puede proporcionarse un token 220 para los datos adicionales 260. De esta manera, la entidad 100 puede compensarse por compartir información adicional 260. Lógicamente, las reglas del permiso 250 pueden crearse de muchas maneras diferentes con una variedad de limitaciones.

A modo de ejemplo, una entidad 100 puede seleccionar recibir ofertas de descuentos de proveedores a cambio de la liberación de información personal 260. El porcentaje de descuento también puede establecerse por la entidad 100 y

la información 260 solo puede compartirse con proveedores dispuestos a ofertar más que el porcentaje de descuento. Como aun otro ejemplo, una entidad 100 puede seleccionar recibir un beneficio (descuento, compensación, ofertas especiales) a cambio de recibir solamente anuncios (o realizar pagos) con un único proveedor o línea de proveedor por un período de tiempo. Si la oferta del proveedor no cumple con un umbral, la oferta puede rechazarse y la información 260 sobre la entidad 100 puede continuar siendo privada.

Datos adicionales

Con referencia nuevamente a la Figura 3, en el bloque 130, si se otorga el permiso, puede comunicarse información adicional 260. La información adicional 260 puede asumir una variedad de formas o niveles y la forma y el nivel pueden ser establecidos por la entidad 100. Como se mencionó previamente, lo que una entidad 100 considera que es información privada o sensible 260 puede variar dependiendo de la entidad 100 y estos factores pueden reflejarse en los permisos 250 establecidos y en la información 260 que está dispuesta a compartirse. Además, algunas entidades 100 pueden tener más información adicional 260 para proporcionar que otras entidades 100.

Como un ejemplo, la información adicional 260 puede incluir datos relacionados con el nivel de ingresos de la entidad 100 que el proveedor puede usar para determinar si es probable que la entidad 100 sea un cliente. En otro ejemplo, la información adicional 260 puede incluir datos de información de pago, tal como si la entidad 100 tuviera una cuenta válida o si la cuenta tuviera espacio para compras adicionales. La entidad 100 puede establecer el nivel de datos adicionales con antelación. Por ejemplo, la entidad 100 puede determinar que un proveedor dispuesto a pagar $5 puede ver un código postal relacionado con una entidad 100 y un proveedor dispuesto a pagar $50 puede ver información sobre el nivel de ingresos de la entidad 100.

En algunas modalidades, el nivel de información 260 puede establecerse por la entidad 100 mientras está en el proveedor. A modo de ejemplo, una entidad 100 puede desviarse hacia un nuevo almacén para el cual la entidad 100 no haya establecido un nivel de permiso y la entidad 100 puede desear realizar una compra al proveedor. La entidad 100 puede mirar una cámara de seguridad (sensor 110) donde la cámara de seguridad 110 puede comunicar la imagen como datos de autenticación en el servidor central 230. Los datos de autenticación, que pueden incluir la imagen y los datos obtenidos por Wifi, pueden validarse como no fraudulentos. La entidad 100, a través de uno de los sensores 110, puede indicar a la autoridad central 230, la entidad 100 otorga permiso al proveedor 250 para comunicarse con el proveedor.

La entidad 100 puede hacer la indicación de una variedad de maneras que pueden predeterminarse por la entidad 100. Por ejemplo, la entidad 100 puede predeterminar que un gesto deliberado de pulgar hacia arriba puede significar que se le otorga permiso para que la información de pago 260 se comunique a este proveedor. A modo de otro ejemplo, el usuario puede hablar una frase predeterminada en la cámara 110 que también puede tener capacidades de sonido, el sonido y la imagen pueden verificarse como atributos 210 y los datos de pago 260 pueden entonces comunicarse al proveedor. A modo de incluso otro ejemplo, la entidad 100 puede usar un dispositivo informático portátil tal como un teléfono inteligente para comunicarse con la autoridad central 230, cuyos datos de pago pueden comunicarse a un proveedor específico.

Comunicación/tokens

Como se mencionó anteriormente, la comunicación puede ser a un dominio confiable. La comunicación puede ser en forma de tokens 220. En algunas modalidades, los tokens 220 se pasan de la entidad 100 al sensor 110 donde los tokens 220 se comunican luego a la autoridad de confianza 230.

Aún en otra modalidad, el token 220 se comunica en forma de nombre de entidad.dominio donde el dominio puede ser el nombre del proveedor de red confiable. En aun otra modalidad, el token 220 puede comunicarse en forma de token.dominio donde el dominio puede ser el nombre del proveedor de red confiable. En algunas versiones del protocolo de Internet, el propio token 220 puede ser parte de la dirección y el token 220 puede ser dinámico.

Si se acepta el token 220 y se otorga permiso para una comunicación adicional, entonces las comunicaciones futuras pueden proceder de manera encriptada o en otro formato seguro y eficiente. La comunicación desde el sistema informático central 230 al sensor 110 con los resultados de la determinación si se otorga el permiso puede tener la forma de un token 220. El token 220 puede indicar el nivel de datos que la entidad 100 ha permitido ver al proveedor o al propietario 110. El token 220 también puede contener cierta información preliminar sobre la entidad 100 si se otorgó el permiso y el proveedor/propietario del sensor 110 puede decidir si los datos adicionales 260 serían útiles. En relación con lo anterior, en las situaciones en las que se requiera la oferta o un pago para obtener información adicional 260, el costo relevante para la información 260 o el estado actual de la oferta puede comunicarse como parte del token 220.

En algunas modalidades, toda la comunicación tiene lugar mediante el uso de tokens 220. Para reducir el fraude, los diversos tokens 220 pueden ser dinámicos. Por ejemplo, la entidad 100 puede comunicar un primer token 220 a un primer sensor 110 y puede comunicar un token diferente 220 a un sensor diferente 110. De esta manera, un proveedor no puede usar un token anterior 220 para intentar comunicarse con una entidad 100. Siempre que el token 220 pueda

ser entendido por el sistema informático confiable 230, el token 220 puede cambiar o ser dinámico. Por ejemplo, el token 220 puede cambiar de acuerdo con un reloj que sincroniza la computadora central 230 y los sensores 110. Adicionalmente, como se mencionó anteriormente, toda la comunicación al sistema informático de confianza 230 puede revisarse para el fraude o anomalías por el sistema de análisis de riesgos 240.

En aún otra modalidad como se ilustra en la Figura 6, los tokens 220 pueden permitir una transacción sobre una red de pago tradicional. Una entidad 100 puede establecer confianza con un sensor 110 o proveedor. Asumiendo que la entidad 100 ha concedido acceso a la información de pago 260, la información de pago 260 almacenada en la tienda de computadoras de confianza 230 puede comunicarse a través de la red de pago tradicional tal como a través del adquiriente 700 al procesador emisor 710 y luego al emisor 720. Aún en otra modalidad, la información de pago puede permanecer en la tienda de computadoras de confianza 230 y un token 220 que representa la información de pago puede hacerse pasar a través del sistema de pago tradicional 700-720 donde puede reconocerse y usarse para acceder a la información de pago relevante 260. En esta modalidad, la información de pago 260 puede mantenerse dentro del sistema seguro, reduciendo así el riesgo.

Los tokens 220 pueden intercambiarse por una variedad de propósitos. En un ejemplo, un token 220 puede permitir que ocurra una transacción. En otro ejemplo, el token 220 puede permitir que se suministre información adicional. En aun otra modalidad, el token 220 puede denegar información adicional 260. Además, el token 220 puede indicar que el fraude puede ocurrir y que la presente solicitud es probablemente fraudulenta.

División de tarifas

En aún otro aspecto, un primer proveedor/propietario del sensor 110 puede ser responsable de atraer entidades 100 hacia una ubicación geográfica particular. A modo de ejemplo, una tienda de helados puede ser responsable de atraer grandes grupos durante días cálidos. Los grupos también pueden comprar en otros proveedores adicionales 110 después de comprar el helado. Un porcentaje de las ventas de los proveedores adicionales 110 puede compartirse al primer proveedor 110. La transferencia de fondos puede usar además la red de computadoras confiable 230 ya que los proveedores/propietarios del sensor 110 pueden ser también miembros del sistema informático confiable 230. En algunas modalidades, el porcentaje compartido puede negociarse entre las partes. En otra modalidad, puede determinarse el aumento de las ventas por los proveedores adicionales y pueden distribuirse automáticamente.

En otra modalidad, un propietario del sensor 110 puede ser un propietario del sensor primario 110 y el propietario del sensor primario 110 puede recibir compensación de los propietarios del sensor secundario 110 en una proximidad lógica al propietario del sensor primario 110 si se produce una transacción. Los sensores 110 de los diversos proveedores 110 pueden controlar los movimientos de los clientes y si los clientes se acercaron a un primer proveedor/propietario del sensor y luego realizaron compras en tiendas adicionales, las tiendas adicionales pueden compartir una parte de los ingresos con el proveedor principal.

Revisión de la transacción

El sistema también puede proporcionar capacidades adicionales para que las entidades 100 desafíen cargos fraudulentos. A medida que la entidad 100 encuentre probablemente numerosos sensores 110 antes de activar una transacción, puede haber numerosas consultas en la ubicación central de computación si una entidad 100 ha acordado proporcionar información adicional. Si se realiza una compra y no se realizaron las consultas adicionales, la probabilidad de que haya ocurrido un fraude es mayor. De manera similar, si ocurrió un fraude, es probable que la persona que cometió el fraude fuera detectada por numerosos sensores 110 en la red. Los atributos detectados 210 del perpetrador del fraude pueden usarse para perseguir el fraude. Además, los datos detectados pueden usarse para ilustrar que la entidad 110 puede haber estado en una ubicación diferente cuando se realizó la compra. Dado que la nube personal 120 tendrá muchos atributos únicos, esta será especialmente difícil de replicar. De manera similar, si un estafador intenta duplicar los atributos 210 de una red personal 120, algunos de los atributos 210 del estafador pueden obtenerse y pueden usarse para rastrear el estafador.

Comunicación a través de la red de confianza (correo electrónico)

Otro aspecto es que la entidad 100 puede usar la red para hacer más que realizar compras. Una entidad 100 puede establecer permisos 250 de manera que la entidad 100 puede reconocerse y puede acceder a funcionalidades adicionales de la red. A modo de ejemplo, una entidad 100 puede otorgar permiso para que determinados proveedores tengan acceso a datos personales 260. Una vez que la entidad 100 se verifica, la entidad 100 puede usar el sensor 110 como un ordenamiento del dispositivo de entrada a la red de computadoras segura 230 para realizar tareas como cualquier sistema informático. La entidad 100 puede mirar a una cámara de seguridad 110 y solicitar que se envíe un correo electrónico a su asistente de que su tren está demorado. De manera similar, la entidad 100 puede usar la cámara u otro sensor 110 como una entrada en un dispositivo informático y virtualmente todas las opciones disponibles mediante el uso de una computadora pueden estar disponibles.

En aún otro aspecto, la entidad 100 puede usar un sensor 110 tal como una cámara en un dispositivo informático portátil 101 para crear una tarea y la tarea puede ejecutarse en un momento dado en el futuro cuando está disponible

un acceso a la red de computadoras adecuado. Por ejemplo, la entidad 100 puede estar en el transporte público y puede desear crear un nuevo nivel de permisos a una tienda. El usuario puede crear y almacenar un mensaje mediante el uso del sensor de imagen 108 en el dispositivo informático portátil 101 y una vez que el usuario no está en el transporte público y está cerca de un acceso satisfactorio a la red de computadoras, el mensaje puede enviarse.

Como aun otro ejemplo, un proveedor puede configurar un punto de comunicaciones similar a una cabina telefónica. En el punto de comunicaciones, una entidad 100 como un cliente puede tener privacidad y puede acceder a la información privada después de ser reconocida por el sistema. Por ejemplo, una entidad 100 puede ser reconocida por los atributos apropiados 210 y puede acceder a su correo electrónico en el punto de comunicaciones. De manera similar, una entidad 100 puede solicitar un mapa a un almacenamiento adicional y el mapa puede visualizarse en el punto de comunicaciones. Además, el mapa (u otro objeto basado en computadora) puede descargarse a otro dispositivo informático asociado con la entidad 100 tal como un dispositivo informático portátil 101. A modo de otro ejemplo, una entidad puede mirar a una cámara y solicitar un cambio en el acceso a un proveedor específico en cuestión, tal como permitir que el proveedor tenga acceso a los datos de pago.

La red confiable puede ser una red pública tal como Internet con salvaguardas suficientes o puede ser una red privada o una combinación de redes públicas y privadas con seguridad adecuada aplicada. Si la red es una red privada tal como una red de procesamiento de pagos, las entidades pueden tener más fe de que su información personal y sensible se almacena y mantiene de una manera segura y por lo tanto las entidades pueden ser más propensas a aprovechar más aspectos del sistema.

Conclusión

La red, proceso y sistema descritos pueden permitir que las entidades 100 controlen mejor el acceso a los datos sensibles 260 sobre la entidad 100. En lugar de que múltiples partes recopilen datos 260 y los utilicen a medida que las partes vean el ajuste, la entidad 100 tendrá control de dichos datos. La entidad 100 puede usar entonces la información 260 a medida que la entidad 100 considere adecuado, a partir del autorizo de los pagos, a aceptar ofertas para obtener información adicional para denegar el acceso a dicha información 260.

De acuerdo con las disposiciones de los estatutos de patentes y la jurisprudencia, las configuraciones ilustrativas descritas anteriormente se consideran que representan una modalidad preferida de la invención. Sin embargo, debe notarse que la invención puede llevarse a la práctica de cualquier otra manera que como se ilustra y se describe específicamente sin apartarse de su alcance.

REIVINDICACIONES

1. Un método basado en computadora para controlar el acceso a los datos sobre una persona (100), el método comprende:
recoger de manera no intrusiva, mediante un dispositivo sensorial (110), datos de atributo (210) que diferencia a la persona (100) de otra persona en un primer de una pluralidad de dispositivos sensoriales (110) en diferentes ubicaciones visitadas por la persona detectando los atributos de la persona (100) en cualquiera de la pluralidad de ubicaciones, la primera de la pluralidad de dispositivos sensoriales se asocia con un propietario del sensor;
comunicar los datos de atributo (210) del dispositivo sensorial (110) a través de una red de computadoras a un servicio de verificación confiable (240) en una computadora central (230) para verificar que los datos de atributo cumplen con las reglas del permiso (250) creadas por la persona (100) para permitir que los datos adicionales (260) incluyan la información de pago para la persona que se comunica;
generar, en la computadora central (230), un token (250) en respuesta a los datos de atributo (210) que se verifican, el token (250) comprende permiso para el dispositivo sensorial (110) para obtener información adicional (260); y
en respuesta a que se verifican los datos de atributo (210), proporcionar el token (250) al dispositivo sensorial (110), en donde el token (250) incluye los datos adicionales (260) usados para realizar una compra por parte de la persona con el propietario del sensor.

2. El método de acuerdo con la reivindicación 1, en donde los datos de atributo (210) se analizan para determinar características fraudulentas.

3. El método de acuerdo con la reivindicación 1, en donde los datos de atributo (210) comprenden al menos uno seleccionado del grupo que comprende un dato relacionado con el dispositivo informático móvil, un material inteligente, una cara, una mano, joyas, escaneo del iris, y una señal cardíaca.

4. El método de acuerdo con la reivindicación 1, que comprende además usar el dispositivo sensor (100) para detectar al menos uno del grupo que comprende atributos de señales inalámbricas, atributos ópticos, atributos de sonido, atributos de olor, y atributos fotónicos.

5. El método de acuerdo con la reivindicación 4, en donde los atributos ópticos tienen una dimensión, dos dimensiones o tres dimensiones.

6. El método de acuerdo con la reivindicación 5, en donde la detección de atributos ópticos comprende detectar una tela diseñada para emitir una señal que es detectable por el sensor.

7. El método de acuerdo con la reivindicación 1, en donde las reglas del permiso (250) son específicas de la red.

8. El método de acuerdo con la reivindicación 1, en donde la red de computadoras tiene un propietario y las normas del permiso se establecen de acuerdo con el propietario.

9. El método de acuerdo con la reivindicación 1, en donde las reglas del permiso (250) establecen un valor monetario mínimo y si el propietario del sensor (110) está dispuesto a pagar el valor monetario mínimo a la persona (100), se proporciona un token para los datos adicionales.

10. El sistema de acuerdo con la reivindicación 1, en donde la persona (100) está en comunicación con una pluralidad de sensores (110) y se mueve a través de una variedad de sensores (110).

11. El método de acuerdo con la reivindicación 1, en donde:
la comunicación es hacia un dominio de confianza; O
la comunicación comprende al menos un token (220) y el token (220) se revisa con respecto al fraude o anomalías

12. El método de acuerdo con la reivindicación 1, en donde las transacciones aprobadas fluyen a través de una red de pago tradicional.

13. El método de acuerdo con la reivindicación 1, en donde la comunicación de los tokens (220) permite una transacción para el valor.

14. El método de acuerdo con la reivindicación 1, en donde la persona (100) comunica un mensaje aprobado por la persona a través de los sensores (110).

15. Un sistema basado en computadora para controlar el acceso a los datos sobre una persona (100), el sistema comprende:
una computadora central (230) que tiene un servicio de verificación confiable (240);

una primera de una pluralidad de dispositivos sensoriales configurados para detectar de manera no invasiva los datos de atributo (210) en diferentes ubicaciones visitadas por la persona que diferencia la persona (100) de otra persona al sensar los atributos de la persona (100) en cualquiera de la pluralidad de ubicaciones, el primero de la pluralidad de dispositivos sensoriales está asociado con un propietario del sensor,

en donde el dispositivo sensorial se configura además para comunicar los datos de atributo (210) a través de una red de computadoras al servicio de verificación confiable (240) en la computadora central (230) para verificar que los datos de atributo cumplen con las reglas del permiso (250) creadas por la persona (100) para permitir que se comuniquen los datos adicionales (260), en donde los datos adicionales incluyen información de pago;

en donde la computadora central (230) se configura además para generar un token (250) en respuesta a que se verifican los datos de atributo (210), el token (250) comprende permiso para que el dispositivo sensorial (110) obtenga información adicional (260); y

en donde la computadora central (230) está configurada además, en respuesta a que los datos de atributo (210) se verifican, para proporcionar el token (250) al dispositivo sensorial (110), en donde el token (250) incluye los datos adicionales (260) usados por el propietario del sensor para que la persona realice una compra.

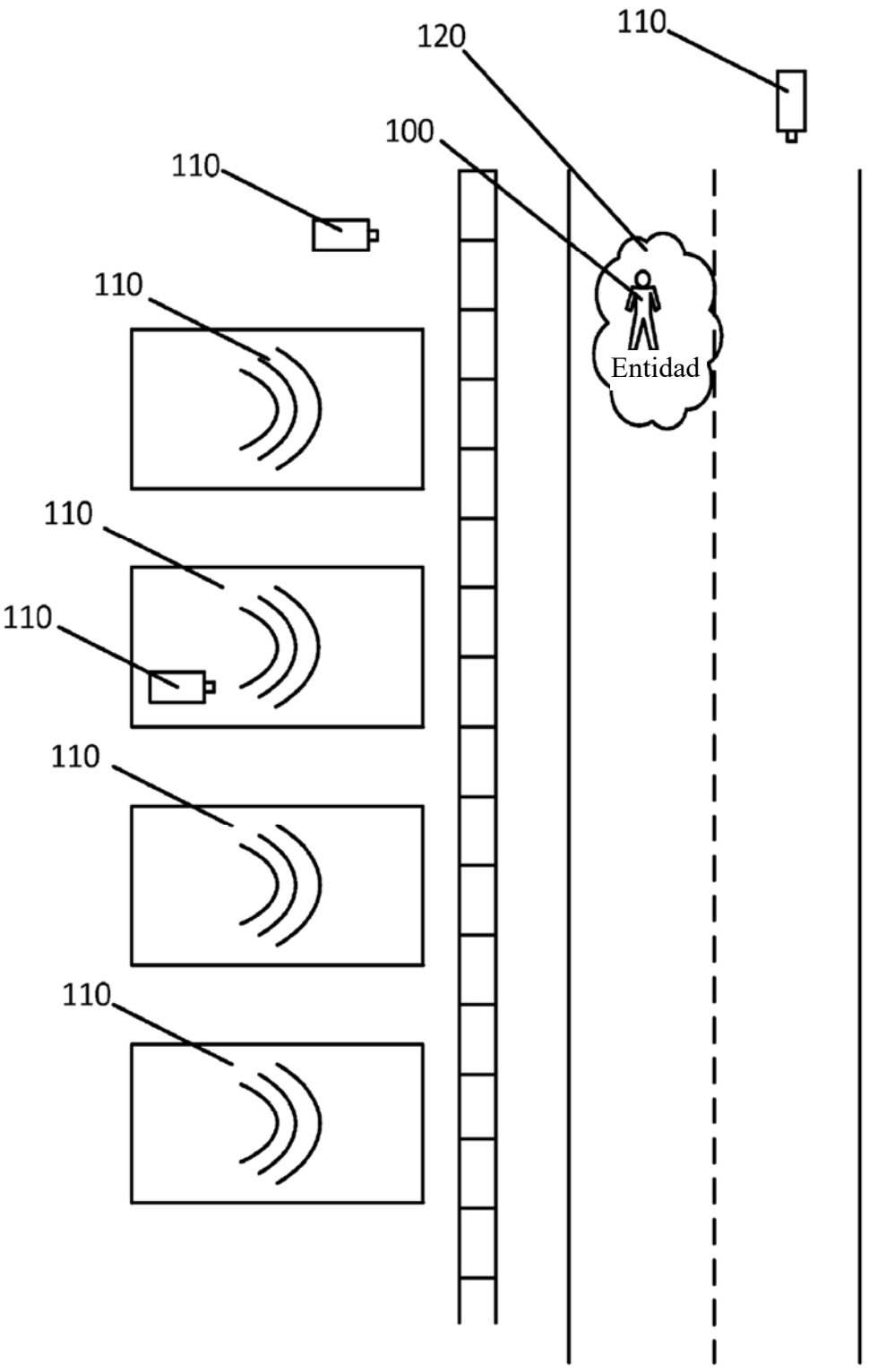

Figura 1

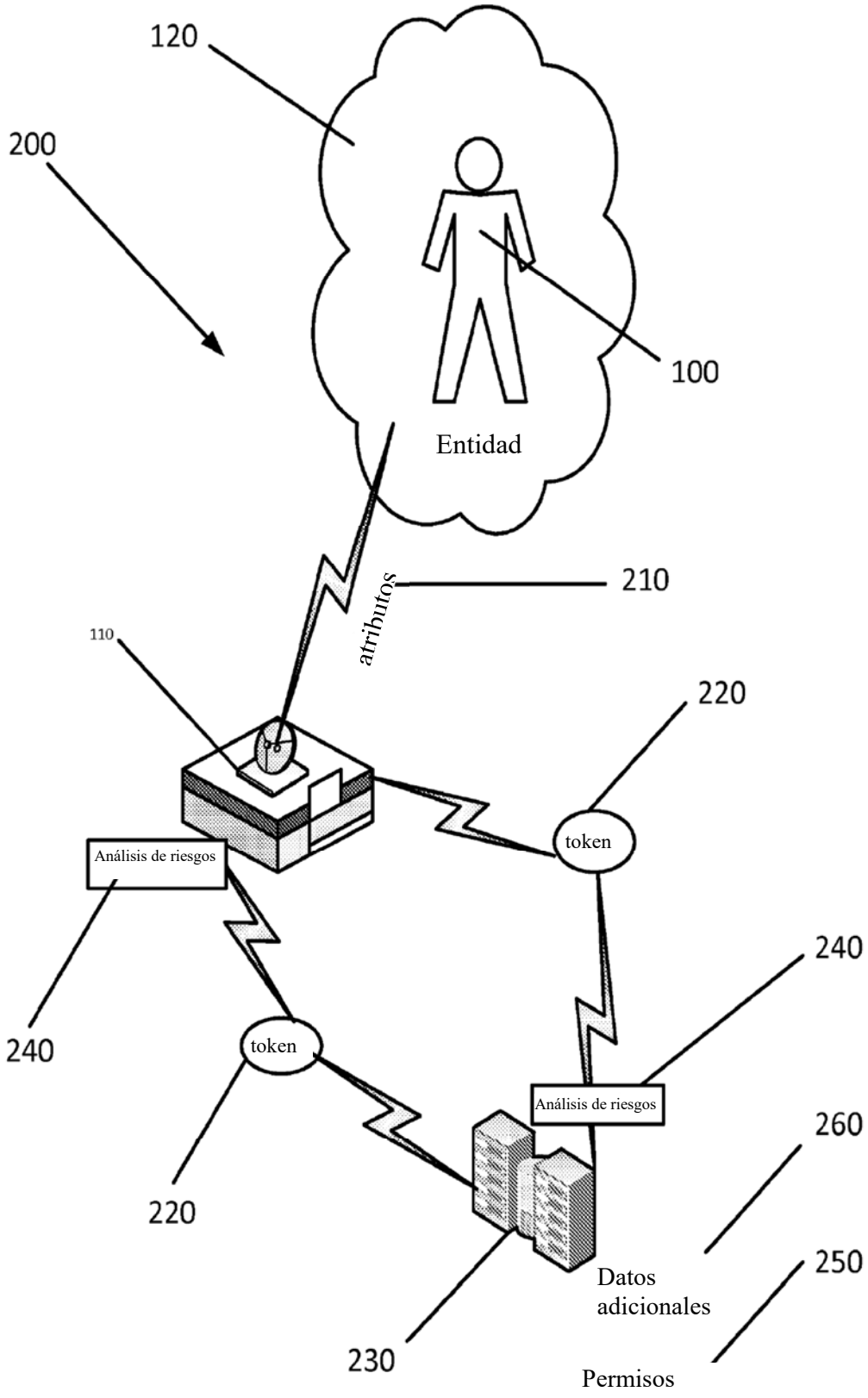
120
200
100
Entidad
210
atributos
110
220
token
Análisis de riesgos
240
240
token
Análisis de riesgos
260
220
Datos
adicionales
250
230
Permisos

Figura 2

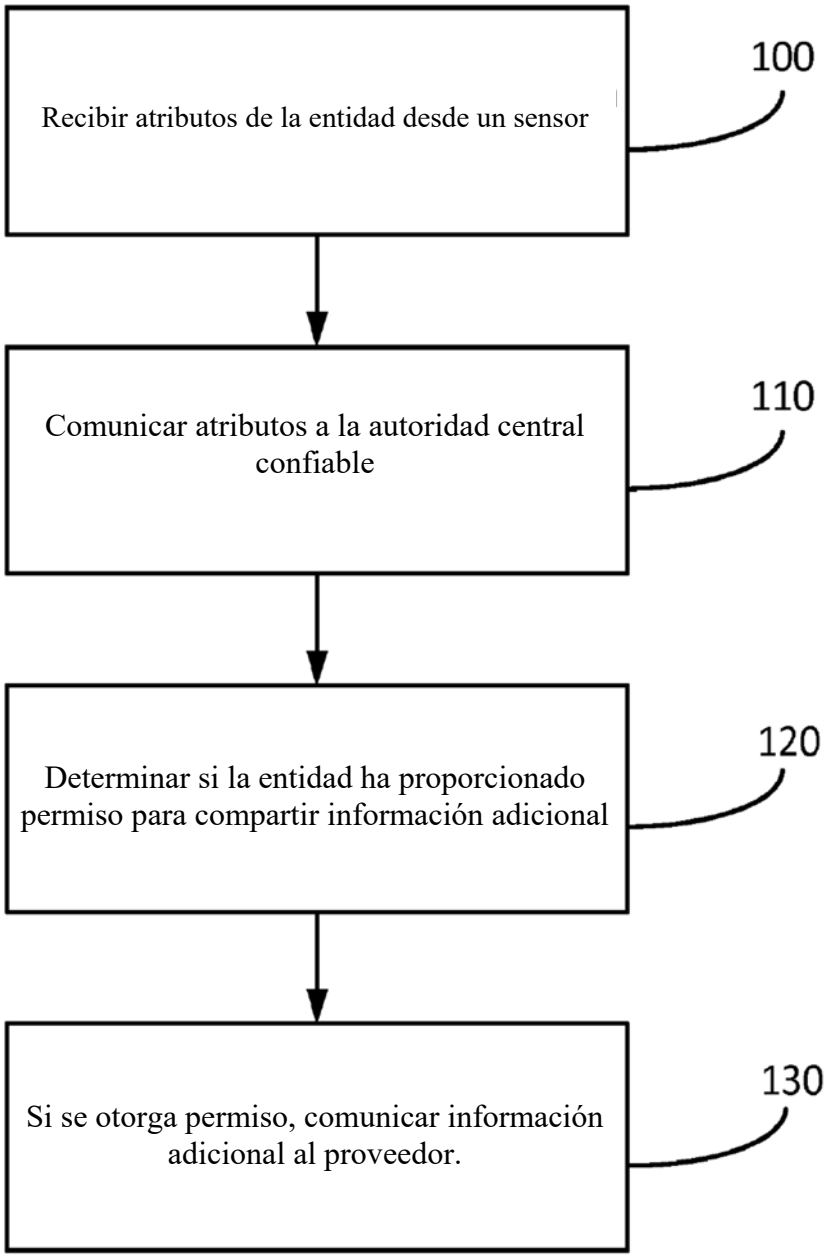
Recibir atributos de la entidad desde un sensor
100
Comunicar atributos a la autoridad central confiable
110
Determinar si la entidad ha proporcionado permiso para compartir información adicional
120
Si se otorga permiso, comunicar información adicional al proveedor.
130

Figura 3

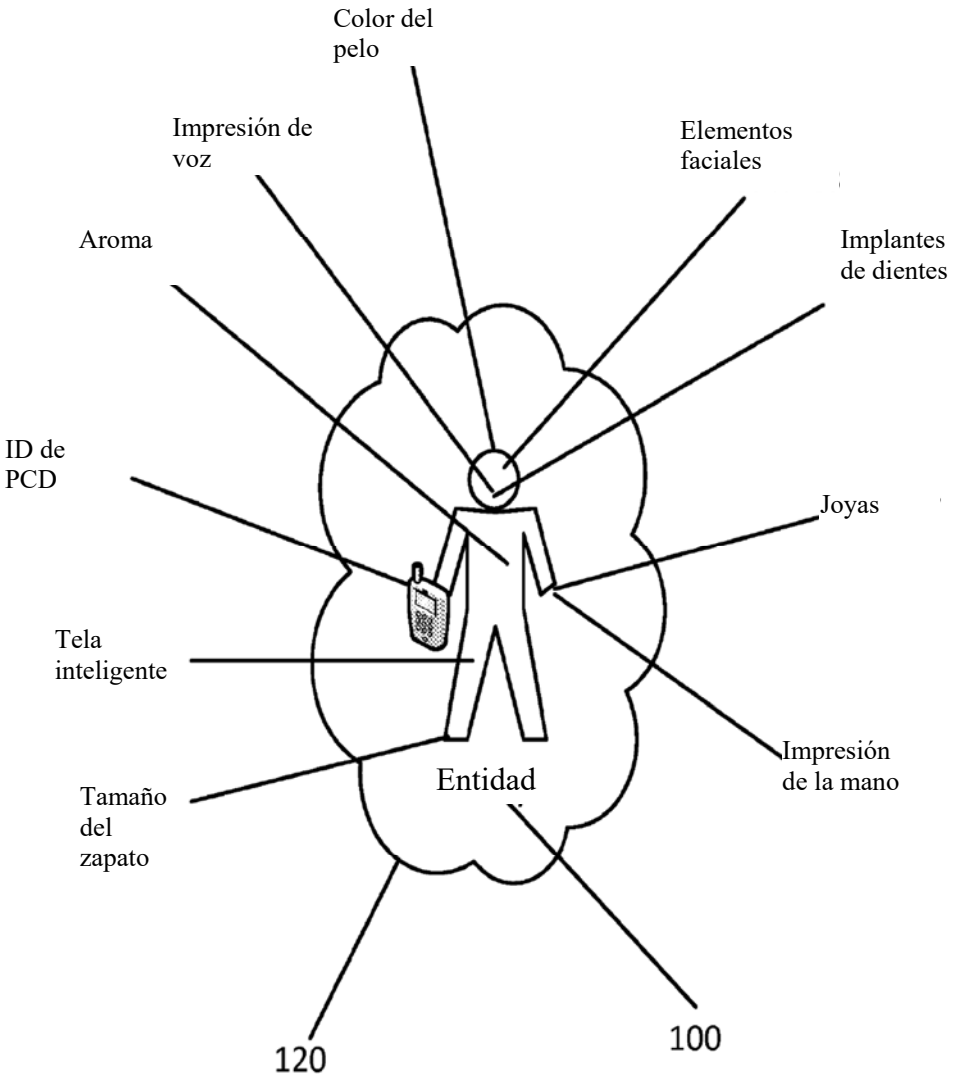
Color del pelo
Impresión de voz
Elementos faciales
Aroma
Implantes de dientes
ID de PCD
Joyas
Tela inteligente
Impresión de la mano
Tamaño del zapato
Entidad
120
100

Figura 4

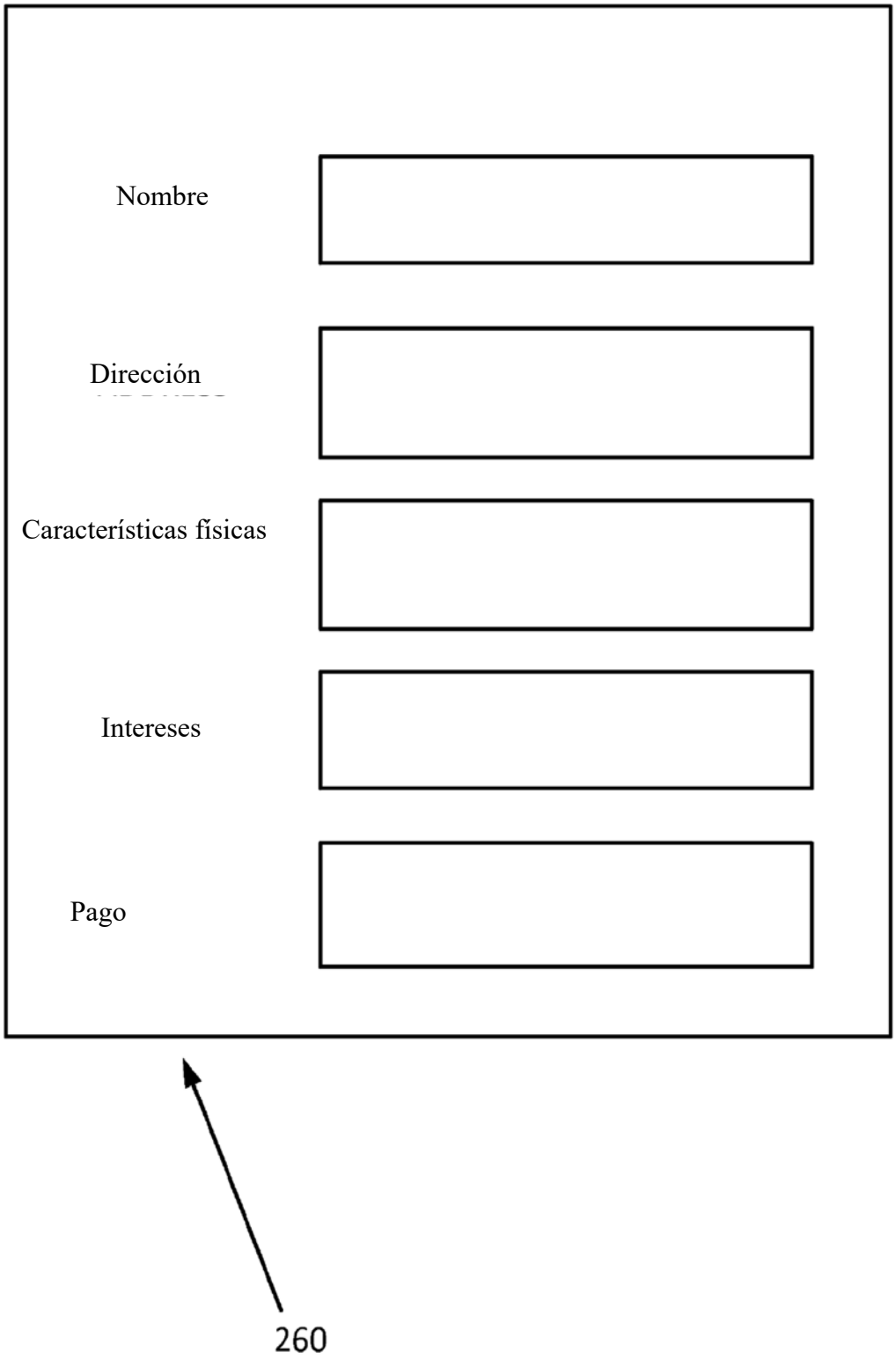
Nombre
Dirección
Características físicas
Intereses
Pago
260

Figura 5a

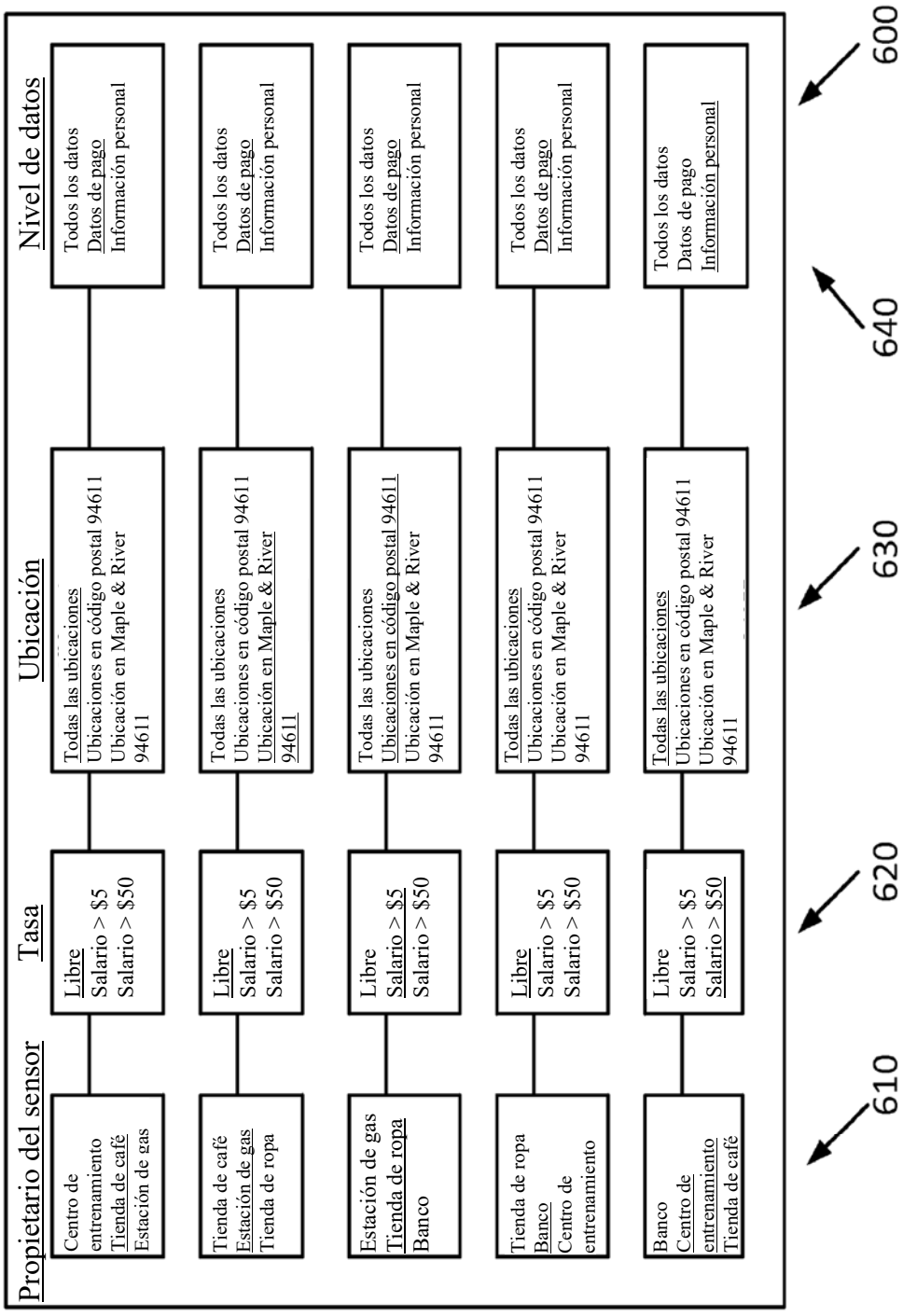
Propietario del sensor
Tasa
Ubicación
Nivel de datos
Centro de entrenamiento
Tienda de café
Estación de gas
Libre
Salario > $5
Salario > $50
Todas las ubicaciones
Ubicaciones en código postal 94611
Ubicación en Maple & River
94611
Todos los datos
Datos de pago
Información personal
Tienda de café
Estación de gas
Tienda de ropa
Libre
Salario > $5
Salario > $50
Todas las ubicaciones
Ubicaciones en código postal 94611
Ubicación en Maple & River
94611
Todos los datos
Datos de pago
Información personal
Estación de gas
Tienda de ropa
Banco
Libre
Salario > $5
Salario > $50
Todas las ubicaciones
Ubicaciones en código postal 94611
Ubicación en Maple & River
94611
Todos los datos
Datos de pago
Información personal
Tienda de ropa
Banco
Centro de entrenamiento
Libre
Salario > $5
Salario > $50
Todas las ubicaciones
Ubicaciones en código postal 94611
Ubicación en Maple & River
94611
Todos los datos
Datos de pago
Información personal
Banco
Centro de entrenamiento
Tienda de café
Libre
Salario > $5
Salario > $50
Todas las ubicaciones
Ubicaciones en código postal 94611
Ubicación en Maple & River
94611
Todos los datos
Datos de pago
Información personal
610
620
630
640
600

Figura 5b

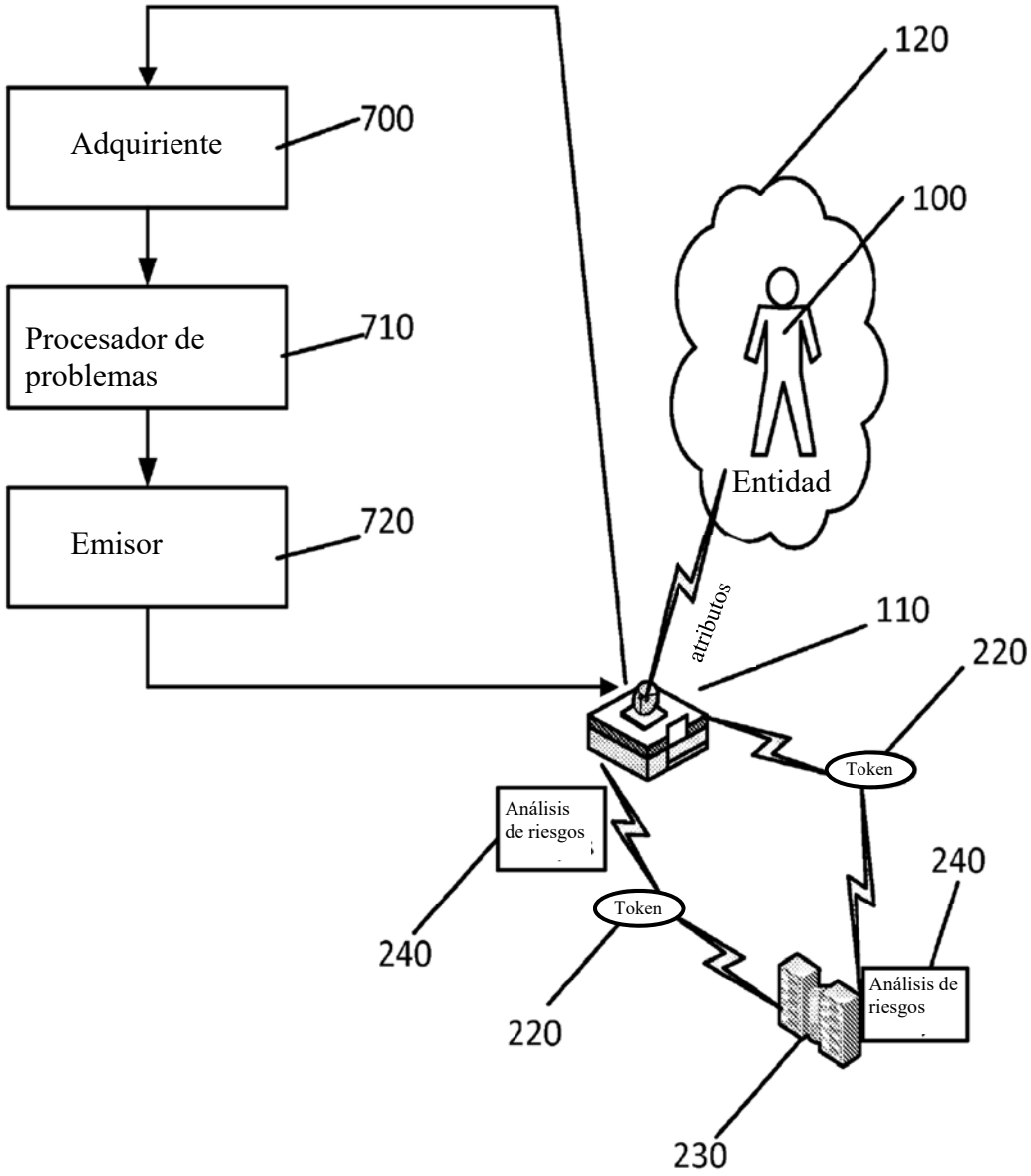
Adquiriente
700
Procesador de problemas
710
Emisor
720
120
100
Entidad
atributos
110
220
Token
Análisis de riesgos
240
Token
240
220
Análisis de riesgos
230

Figura 6

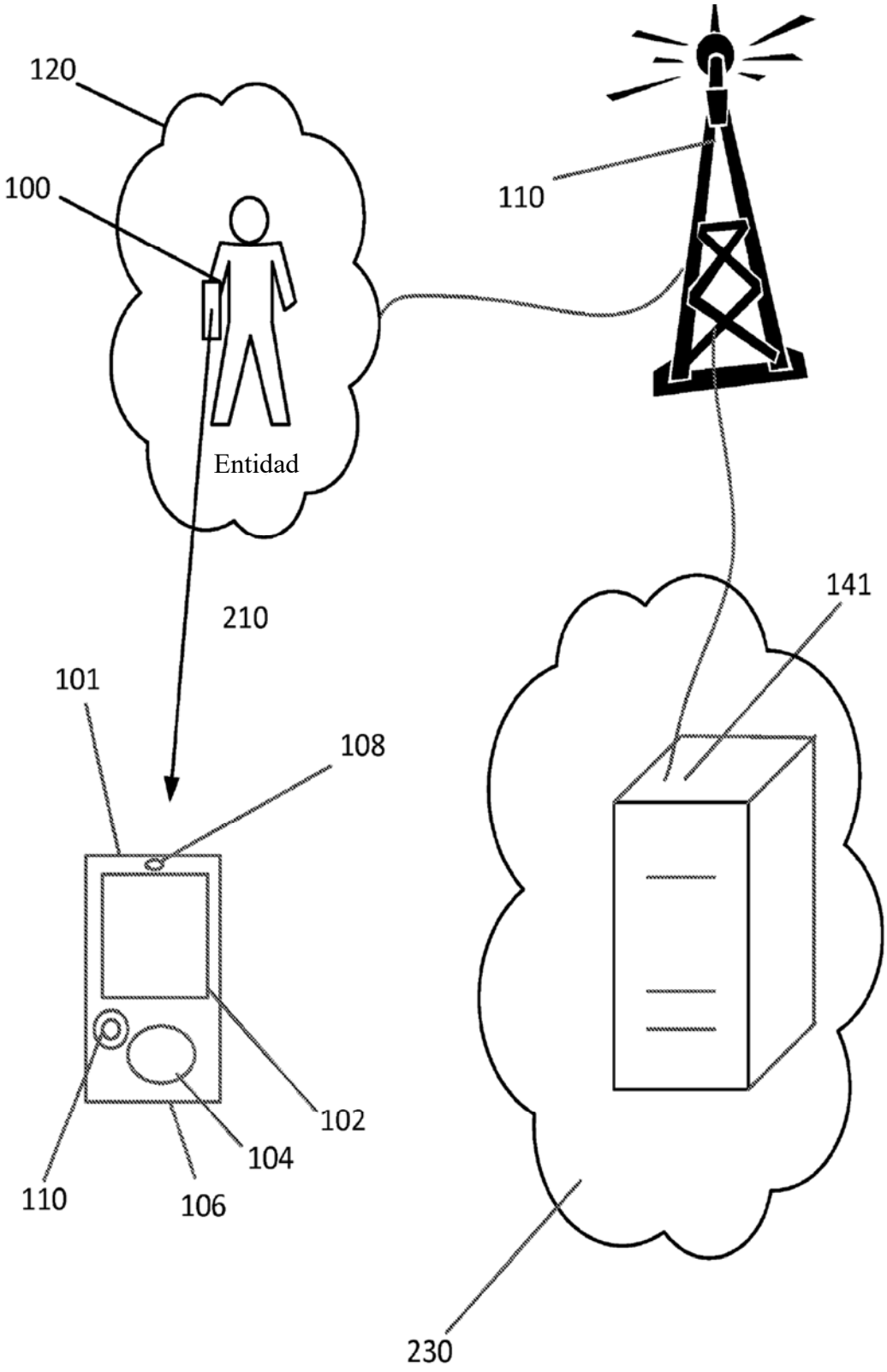

Figura 7

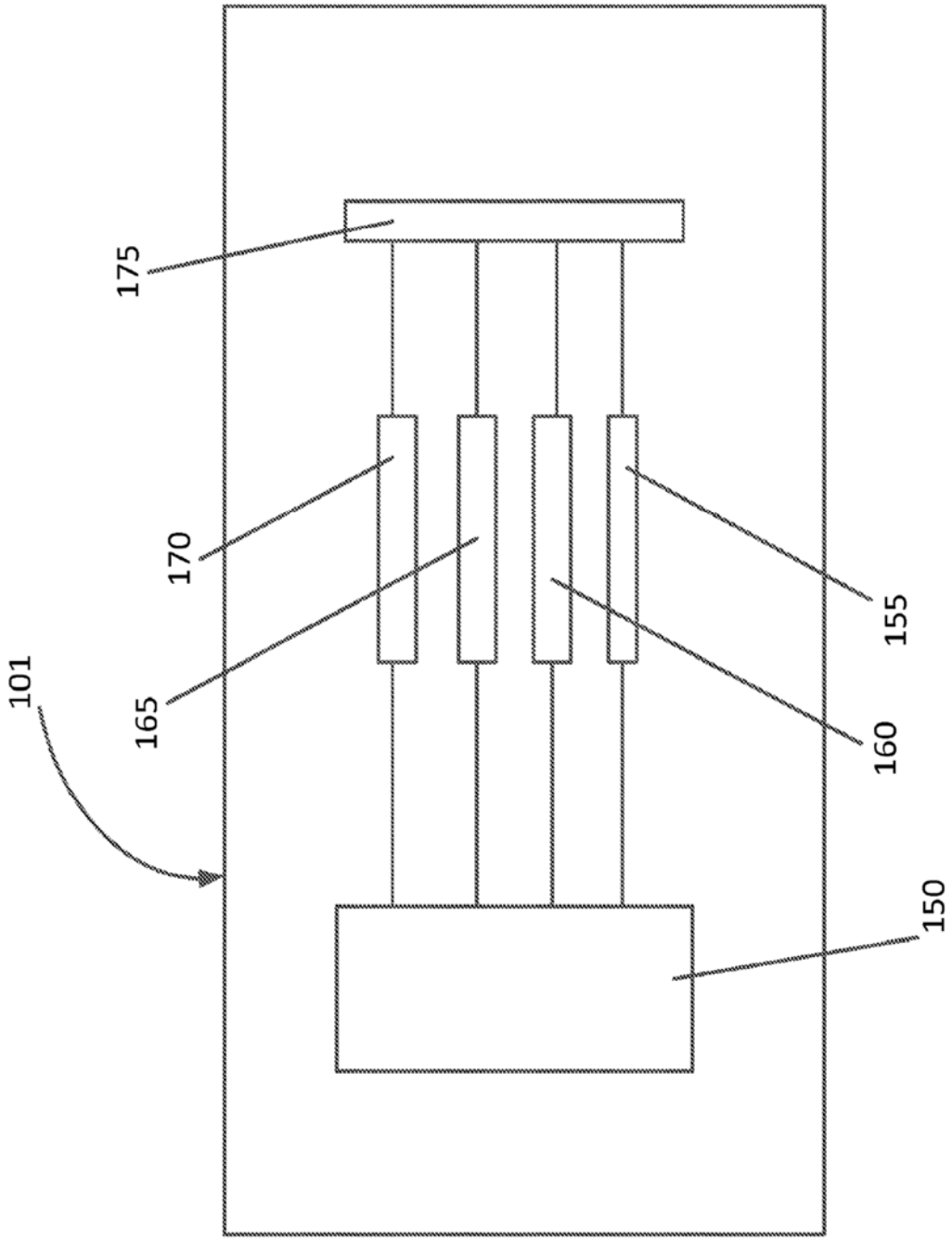

Figura 8

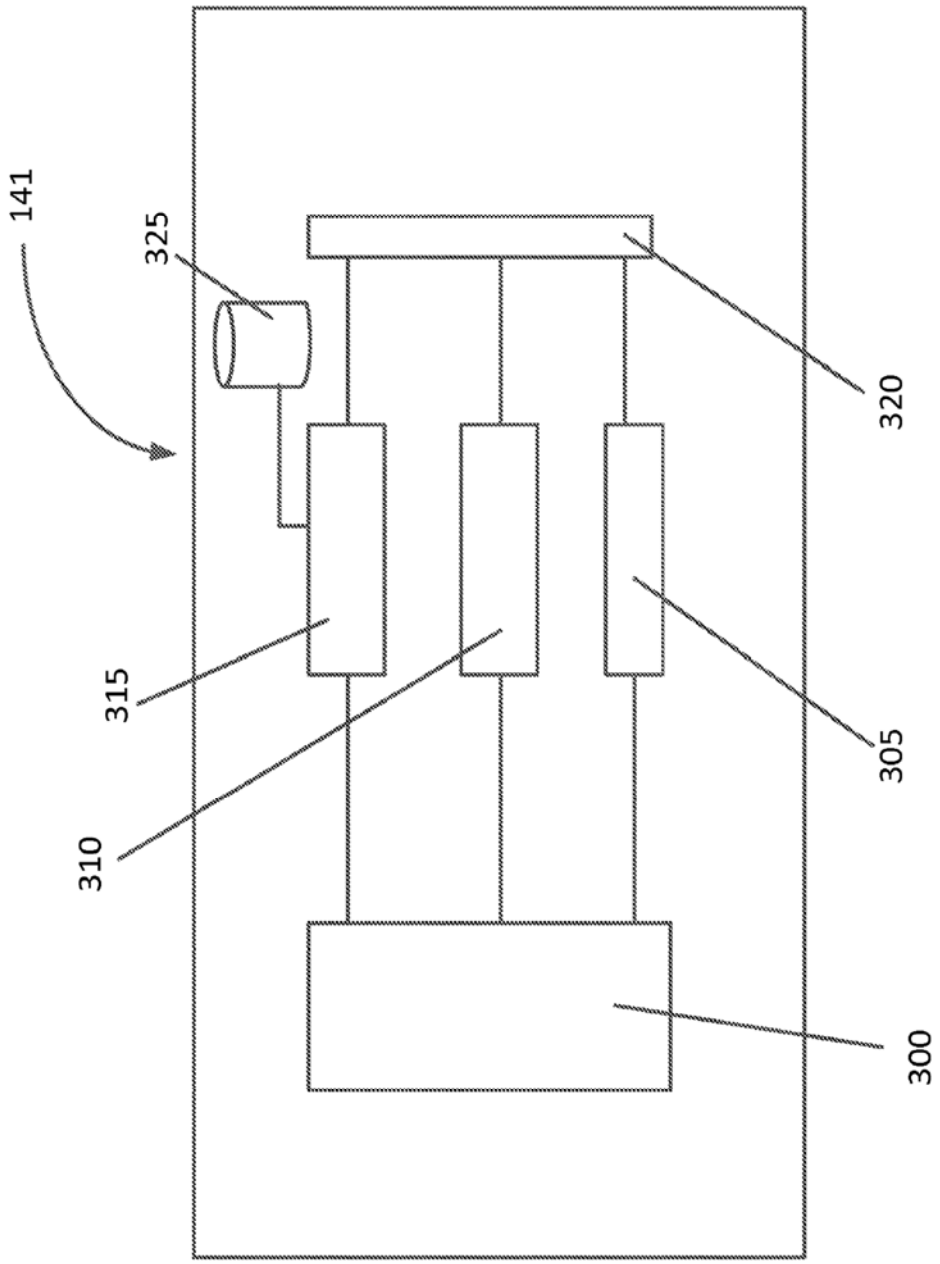

Figura 9