(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 954 314**

(51) Int. CI.:

H04L 9/40 (2012.01)
G06Q 20/14 (2012.01)
G06Q 20/36 (2012.01)
H04L 9/32 (2006.01)
H04W 12/02 (2009.01)
H04L 9/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.01.2018 E 18150999 (3)**

(97) Fecha y número de publicación de la concesión europea: **19.07.2023 EP 3512228**

(54) Título: **Procedimiento para proporcionar de forma segura resultados analíticos y dispositivo sensor para determinar los datos auténticos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2023

(73) Titular/es:

E.ON DIGITAL TECHNOLOGY GMBH (100.0%)
Tresckowstraße 5
30457 Hannover, DE

(72) Inventor/es:

KÜHNEL, THORSTEN;
SOMMERKAMP, KATHARINA;
KELLERER, ELISABETH DR.;
ORD, NICHOLAS y
DE DURFORT, FLORE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para proporcionar de forma segura resultados analíticos y dispositivo sensor para determinar los datos auténticos

La presente invención se refiere a un procedimiento para proporcionar de forma segura resultados analíticos basados en datos, preferiblemente autentificados, de una fuente a un único receptor, así como a un dispositivo sensor para determinar los datos auténticos que se utilizarán en el citado procedimiento.

Con el avance de varios dispositivos de uso diario, así como elementos sensores dedicados que se conectan a Internet y transmiten varios tipos de información sobre su uso y/o su entorno a los proveedores de servicios de Internet para su posterior procesamiento y para ofrecer servicios tales como el control remoto de un hogar dispositivo inteligente, el comportamiento de un usuario que posee estos dispositivos y elementos sensores se puede rastrear con una precisión cada vez mayor.

Aunque los usuarios pueden imaginar los beneficios inmediatos proporcionados por los dispositivos del llamado Internet de las cosas (I-o-T), por lo general no se desea una transparencia concomitante potencialmente ilimitada de su comportamiento. En el pasado, la citada transparencia se aceptaba a cambio de, por ejemplo, servicios gratuitos o se intentó evitar confiando en que los diversos proveedores de servicios de Internet no compartirían los datos recibidos de una parte de los dispositivos del usuario, de modo que no se recopilara un conjunto completo de datos del usuario en un único lugar.

Sin embargo, en los últimos tiempos ha despertado el interés de empresas y usuarios el proporcionar una información predeterminada a los proveedores de servicios sobre el comportamiento de un usuario basada en datos recopilados por dispositivos I-o-T a cambio de beneficios acordados. Por ejemplo, las primas de un seguro pueden reducirse si los datos recopilados pueden verificar suficientemente un estilo de vida saludable, pero reajustarse si se detecta una desviación del citado estilo de vida.

Con el fin de hacer esto, actualmente, el usuario tiene que configurar sus dispositivos para enviar los datos requeridos al proveedor de servicios que ofrece a su vez, por ejemplo, un descuento. Aunque el usuario puede asumir que el citado proveedor de servicios está utilizando los datos solo para el propósito previsto, no hay garantía de que los datos no se transfieran a otra parte. En otras palabras, el usuario no puede definir de manera concluyente quién tiene acceso a sus datos.

Al mismo tiempo, el proveedor de servicios no puede estar seguro de que el usuario le proporcione los citados datos únicamente a él, por ejemplo a cambio de un descuento, pero no a otra parte, nivelando potencialmente de esta manera cualquier ventaja competitiva que el proveedor de servicios espera de ciertos datos del usuario, por lo que otorga un beneficio al usuario.

Por último, pero no menos importante, en el estado de la técnica conocida se requiere que cada proveedor de servicios mantenga su propio centro de datos y emplee expertos en datos para desarrollar rutinas de evaluación adecuadas para analizar los datos recibidos para cualquier fin previsto.

El documento WO 2017/190795 A1 propone utilizar una red entre iguales para evaluar datos de telemetría, requiriendo que los usuarios confíen en la seguridad y buen comportamiento no solo de una instancia central, sino de todos los nodos de la red que manejan y evalúan sus datos. Sin embargo, como característica común en las redes entre iguales, los datos del usuario se distribuyen y comparten entre varios nodos que, a menudo, no le conocen individualmente, lo que da como resultado un nivel de confianza reducido.

Un objeto de la presente invención es proporcionar un procedimiento para proporcionar de forma segura resultados analíticos basados en datos, preferiblemente autentificados, de una fuente a un único receptor, en el que las desventajas del estado de la técnica son al menos reducidas. La invención también se refiere a un dispositivo sensor para proporcionar datos autentificados que se utilizarán preferentemente en el procedimiento de acuerdo con la presente invención.

Este objeto se soluciona mediante el procedimiento de acuerdo con la reivindicación independiente 1. Las realizaciones preferidas son el objeto de las reivindicaciones dependientes.

Por tanto, la invención se refiere a un procedimiento para proporcionar de forma segura resultados analíticos basados en datos de una fuente a un único receptor previsto, en el que el propietario de la fuente y el receptor están vinculados por un contrato con una tercera parte de confianza que supervisa el cumplimiento del contrato, que comprende la ejecución de los pasos:

- transmitir datos sin procesar de forma segura desde la fuente a un servidor de la tercera parte de confianza;

- cifrar todos los datos sin procesar recibidos por el servidor con una primera clave de cifrado proporcionada por el propietario de la fuente;

y comprende, además, la ejecución de los siguientes pasos, en caso de que se haya concluido un contrato entre el titular de la fuente y el receptor:

- el propietario de la fuente proporciona al servidor una primera clave de descifrado que le permite descifrar los datos sin procesar necesarios para los análisis necesarios para que el servidor controle el cumplimiento del contrato;

- el servidor evalúa el cumplimiento del contrato en función de criterios predeterminados y cifra el resultado de esta evaluación con una segunda clave de cifrado proporcionada por el propietario de la fuente antes de colocar el resultado como un recurso móvil en una cadena de bloques; y

- el propietario de la fuente proporciona al receptor una segunda clave de descifrado para descifrar el resultado de la evaluación y, por lo tanto, permitir que el receptor previsto recupere los resultados de la evaluación de la cadena de bloques como único receptor.

Además, la invención se refiere a un dispositivo sensor que comprende al menos un módulo sensor para capturar al menos una característica del entorno del sensor como datos sin procesar, un módulo de comunicaciones para transmitir los datos sin procesar adquiridos a un servidor y un procesador para recibir los datos sin procesar del al menos un módulo sensor y reenviar los datos sin procesar al servidor por medio del módulo de comunicaciones, en el que al menos un módulo sensor comprende un sensor de presión con una precisión de determinación de una caída vertical de 20 cm.

Antes de explicar la invención en detalle, se define alguna terminología utilizada junto con la misma.

El término "fuente" abarca todos los dispositivos que se pueden asignar a un propietario específico y que envían activamente datos de detección, medición o introducidos por el usuario, es decir, datos sin procesar, al servidor de la tercera parte de confianza. Los dispositivos pueden enviar repetidamente, en intervalos predefinidos o desencadenados por cambios en los datos, sus datos sin procesar al servidor.

El término "clave" se refiere a claves asimétricas o simétricas para descifrar y/o cifrar, así como para la firma digital de datos. El término también comprende conjuntos de claves diferentes pero interrelacionadas, por ejemplo cada clave del citado paquete se usa para cifrar o descifrar diferentes partes de los datos, por ejemplo datos sin procesar asignados a un único propietario.

El término "contrato inteligente" designa un protocolo electrónico para facilitar y verificar la celebración y ejecución de un contrato entre dos partes. Los contratos inteligentes pueden ser autorizador por una tercera parte.

La presente invención proporciona un procedimiento en el que un propietario y un receptor pueden celebrar un contrato con condiciones y criterios predefinidos que se derivan de los datos producidos por la fuente de datos del propietario, en el que el cumplimiento de las condiciones del contrato es supervisado continuamente por una tercera parte de confianza, tanto por el propietario como por el receptor.

Para lograr esto, la fuente del propietario en todo momento transmite de forma segura sus datos sin procesar a un servidor. En otras palabras, todos los dispositivos que se pueden asignar a un propietario específico y que por lo tanto, forman colectivamente la fuente del propietario, transmiten los datos que han recogido, por ejemplo por medio de sensores, detectores u otros medios de entrada, como datos sin procesar al servidor administrado por la tercera parte de confianza.

Si los citados dispositivos de la fuente están conectados a Internet, los dispositivos pueden transmitir sus datos utilizando un protocolo de transmisión seguro, por ejemplo Protocolo de Transferencia de Hipertexto Seguro (HTTPS), Protocolo de Transferencia de archivos seguro (FTPS), Protocolo de Transferencia de Archivos SSH (SFTP), Seguridad de la Capa de Transporte (TLS) o similar.

Los datos transmitidos también pueden incluir un identificador único y una marca de tiempo. El citado identificador puede ser único para cada dispositivo como parte de una fuente ("identificador único de dispositivo", por ejemplo, una dirección de control de acceso a medios (MAC)) o un identificador común compartido por todos los dispositivos de una fuente ("identificador único de fuente"), permitiendo ambos el mapeo de los datos a un propietario específico. La marca de tiempo es adecuada preferiblemente para determinar el momento de la adquisición real de los datos y para convertirla en un esquema de tiempo predefinido común, por ejemplo, Tiempo Universal Coordinado (UTC).

Con el fin asignar los datos recibidos por el servidor a un propietario específico, se prefiere que el propietario use una clave privada para firmar digitalmente el identificador de dispositivo único de un dispositivo de su propiedad y transmita este identificador de dispositivo único firmado al servidor. Entonces, el servidor puede verificar la firma digital en el identificador único de dispositivo firmado por medio de la clave pública correspondiente a dicha clave privada y, en consecuencia, asigna todos los datos recibidos con el citado identificador único al citado propietario. La firma digital puede haber sido validada y/o renovada periódicamente.

Para que el propietario firme el identificador único del dispositivo, puede usar, por ejemplo, una aplicación en un dispositivo móvil, por ejemplo un teléfono inteligente Para firmar digitalmente un identificador único, la aplicación en

primer lugar importa o crea la clave pública y privada del propietario. Posteriormente, el usuario puede introducir manualmente, escanear usando la cámara del dispositivo móvil o seleccionar de una lista proporcionada por la aplicación o el servidor en función de todos los dispositivos potenciales en las cercanías (por ejemplo, estando conectado a la misma red Wi-Fi que el dispositivo móvil) el identificador único del dispositivo que se va a firmar. El identificador de dispositivo único firmado, así como la clave pública, pueden transmitirse entonces al servidor para ser procesado adicionalmente como se describe.

En general, los datos recibidos por el servidor desde la fuente de un propietario se cifran instantáneamente con una primera clave de cifrado proporcionada por el propietario de la fuente. La clave de cifrado puede ser idéntica a la clave pública utilizada para verificar la firma digital de un identificador de dispositivo único (ver más arriba) o puede comprender un conjunto de claves, cada una de las cuales se utiliza para cifrar diferentes partes de los datos recibidos. Como resultado, los datos adquiridos por los dispositivos de la fuente en primer lugar se transmiten de forma segura y a continuación se almacenan de forma segura, es decir, encriptada en el servidor.

El cifrado inmediato de los datos puede suspenderse, si el propietario lo acepta, durante un tiempo determinado para que el servidor pueda analizar inicialmente los datos sin procesar para identificar potencialmente ciertos patrones en los datos que podrían reflejar ciertos aspectos del comportamiento habitual del propietario que podría ser la base de una condición de un contrato y, por lo tanto, un criterio para ser validado posteriormente por el servidor. El tiempo para que se suspenda el cifrado inmediato puede ser una cantidad fija de tiempo establecida por el propietario o ejecutarse siempre que uno o más patrones encontrados en los datos estén suficientemente consolidados. Una vez concluido el citado análisis de patrón inicial, los datos sin procesar se cifran con la primera clave de cifrado proporcionada por el propietario de la fuente inmediatamente después de la recepción.

En caso de que los datos sin procesar se analicen inicialmente, la tercera parte de confianza puede informar a los receptores potenciales qué resultados analíticos están disponibles para evaluar el cumplimiento de un contrato con un propietario específico. En otras palabras, los potenciales receptores aprenden del tercera parte qué aspectos del comportamiento de un titular pueden ser deducibles de los datos recibidos, especialmente en función de los patrones encontrados en ellos, para formar la base de cualquier condición que va a ser pactada en un contrato que puede ser validado por el servidor. Sin embargo, el receptor no recibe más información sobre el propietario y su comportamiento. Explícitamente, la tercera parte de confianza no proporciona datos sin procesar o información de patrones, en ningún momento, a un receptor potencial o real.

Sobre la base de la recopilación de datos descrita, el propietario puede celebrar un contrato con un receptor elegido, en el que el contrato comprende ciertas condiciones que se derivan de los datos proporcionados por la fuente del propietario por el servidor de la tercera parte de confianza. Con la ayuda de la tercera parte de confianza se puede asegurar al receptor que el titular cumple con las condiciones pactadas.

Con el fin de permitir que el servidor de la tercera parte de confianza evalúe los datos sin procesar proporcionados por la fuente del propietario para verificar el cumplimiento del contrato por parte del propietario, el propietario de la fuente proporciona al servidor una primera clave de descifrado que le permite descifrar al menos esas partes de la fuente del propietario requeridas para los análisis necesarios para monitorizar el cumplimiento del contrato. Preferiblemente, los datos que no se requieren para estos análisis pueden no ser descifrados con éxito por la primera clave de descifrado y, por lo tanto, permanecen confidenciales. Esto se puede lograr fácilmente si varias partes de los datos sin procesar se cifran con diferentes claves, de modo que el propietario solo pueda proporcionar claves a la tercera parte de confianza adecuadas para descifrar la parte de los datos sin procesar realmente requerida.

Una vez descifrados los datos, se puede evaluar el cumplimiento real del contrato mediante criterios predefinidos, por ejemplo determinando las desviaciones de un patrón descubierto durante el análisis inicial o cualquier patrón perpetuado basado en el mismo. El resultado puede comprender, por ejemplo, una simple declaración positiva o negativa, una calificación o cualquier otro esquema de codificación, ya sea que el propietario se haya mantenido dentro de los límites prescritos por una desviación de un patrón dado encontrado en sus datos sin procesar. Únicamente el resultado de esta evaluación, pero no los resultados provisionales o incluso los datos de origen, se cifra con una segunda clave de cifrado proporcionada por el propietario de la fuente antes de que el servidor coloque el resultado como un activo móvil en una cadena de bloques a la que puede acceder el receptor.

El receptor único elegido por el propietario mediante la celebración del contrato puede recuperar el resultado de la evaluación encriptada de la cadena de bloques y descifrar el resultado de la evaluación con la ayuda de una segunda clave de descifrado que le proporcionó el propietario de la fuente, verificando el cumplimiento del propietario con el contrato.

El procedimiento inventivo tiene varias ventajas técnicas sobre el estado conocido de la técnica.

Además de una posible fase de análisis inicial, cualquier dato sin procesar después de ser transmitido de forma segura desde la fuente real al servidor de la tercera parte de confianza se cifra inmediatamente mediante una clave de cifrado proporcionada por el propietario. Como resultado, incluso la tercera parte de confianza no puede acceder a la información proporcionada en el mismo sin el consentimiento del propietario, que es transmitido por el propietario proporcionando una primera clave de descifrado que permite al servidor de tercera parte descifrar al menos partes de

los datos sin procesar almacenados. En caso de que el propietario desee retirar el permiso para descifrar partes de los citados datos, puede retirar la primera clave de descifrado (tecnologías seguras que se conocen en el estado de la técnica) o cambiar la primera clave de cifrado, haciendo de esta manera que la primera clave de descifrado proporcionada anteriormente sea inútil. Siempre que el propietario confíe en que el tercera parte cifre inmediatamente los datos sin procesar recibidos con la clave de cifrado proporcionada por él, el propietario mantiene el control total de los datos a los que puede acceder técnicamente incluso por el propio tercera parte de confianza.

El procesamiento real de los datos sin procesar publicados para evaluar el cumplimiento de un contrato específico lo realiza únicamente el servidor de terceras partes, por lo que no es necesario transmitir datos de origen o resultados intermedios, por ejemplo el receptor. En consecuencia, el receptor posterior no necesita proporcionar ninguna instalación para analizar los datos sin procesar provenientes de las fuentes de los propietarios. El receptor se libera así de tener que mantener amplias capacidades de procesamiento.

La combinación del cifrado de los resultados de la evaluación mediante una segunda clave de cifrado proporcionada por el propietario de la fuente y el uso de una cadena de bloques entre el servidor de la tercera parte de confianza y el receptor tiene dos ventajas principales. Mediante el uso de la tecnología de cadena de bloques, tanto el propietario como el receptor tienen la seguridad de que el resultado de la evaluación acordado como parte de un contrato no puede ser multiplicado y utilizado libremente por varias entidades autorizadas o no autorizadas, sino que solo se transfiere una vez desde la tercera parte de confianza. al receptor único previsto. Además, debido a que el propietario debe proporcionar la segunda clave de descifrado al receptor, todavía tiene el control total de los resultados de la evaluación. Al retirar la citada segunda clave de descifrado, por ejemplo de acuerdo con las tecnologías establecidas o cambiando la segunda clave de cifrado, el propietario puede deshabilitar, en cualquier momento, la capacidad del receptor para acceder al menos a los resultados de evaluación futuros proporcionados por la tercera parte de confianza.

Como se puede deducir fácilmente, el propietario de la fuente tiene al menos dos posibilidades para interrumpir el flujo de información desde su fuente hasta el receptor único por medios técnicos rastreables. El receptor único puede interrumpir el flujo de información al dejar de aceptar transacciones de cadena de bloques de activos de la tercera parte de confianza con respecto a un propietario específico, que es, como la omisión de un paso técnico, también totalmente rastreable.

En todos los casos de interrupción intencional del flujo de información, la tercera parte de confianza podrá informar a las partes involucradas, ya que esto puede afectar la validez del contrato entre el titular y el receptor y requerir un ajuste. En caso de que el contrato sea un contrato inteligente, cuya compensación haya sido proporcionada por la tercera parte de confianza, la tercera parte de confianza también podrá retractarse de cualquier compensación electrónica proporcionada anteriormente, en caso de que la evaluación resulte en un incumplimiento del contrato por parte del propietario. En este caso, el contrato entre el propietario y el receptor se extingue automáticamente o se aplican las disposiciones específicas previstas en el mismo para el caso de que se aplique una compensación retraída.

Aunque el procedimiento, como se ha explicado hasta ahora, proporciona una transmisión y un procesamiento seguros de los datos desde la fuente de datos sin procesar de un propietario hasta que solo los resultados analíticos estén disponibles para un receptor previsto, aún no se ha desarrollado un procedimiento potencialmente deseable para garantizar la autenticidad de los datos sin procesar. El procedimiento para garantizar la autenticidad de los datos sin procesar recopilados por un dispositivo sensor, como se explica a continuación, puede merecer una patente por sí mismo, es decir, separada del procesamiento de datos sin procesar de la fuente de un propietario.

Con el fin de autenticar al menos parte de los datos sin procesar proporcionados por la fuente de un propietario, se prefiere que los datos sin procesar de la fuente sean proporcionados al menos parcialmente por un dispositivo sensor conectado a Internet con al menos un sensor para capturar el entorno del sensor, en el que el dispositivo sensor comprende medios para determinar su altitud, preferiblemente con una precisión suficiente para detectar una caída vertical de 20 cm. El citado dispositivo sensor está diseñado para colocarse permanentemente en una ubicación predeterminada y no para ser movido por el propietario, por ejemplo a un lugar en el que se esperan resultados de medición más favorables. Además, el dispositivo sensor está conectado preferentemente a Internet por medio de Wi-Fi, lo que permite determinar su ubicación aproximada por medio de servicios de geolocalización Wi-Fi conocidos.

Los medios para determinar la altitud del dispositivo sensor pueden comprender un sensor de presión para medir con precisión la presión ambiental. Incluso si no está calibrado, el sensor de presión ya es capaz de detectar que cambios repentinos en la presión que, por encima de ciertos umbrales no pueden deberse a causas naturales habituales (es decir, cambios en el clima), sino que se debe asumir que son causados por el reposicionamiento del dispositivo sensor. La precisión del sensor de presión permite detectar preferentemente caídas verticales de 20 cm.

Sin embargo, se prefiere calibrar el citado sensor de presión para reflejar una altitud absoluta. Esto se puede lograr en un proceso de inicialización que potencialmente se lleva a cabo simultáneamente para registrar el identificador único de los dispositivos sensores con la tercera parte de confianza (ver más arriba). Los teléfonos inteligentes modernos, como un ejemplo de los dispositivos móviles de un propietario que se utilizan para registrar el dispositivo sensor, normalmente comprenden un sensor de presión preciso para proporcionar información de altitud precisa al usuario incluso cuando está en interiores, es decir, sin recepción de señales de navegación por satélite. El sensor de

presión de un teléfono inteligente que es medido constantemente por medio de señales de navegación por satélite, si está disponible, se puede usar para calibrar a su vez el sensor de presión del dispositivo sensor, si se puede suponer que el dispositivo móvil está cerca del dispositivo sensor durante la inicialización, por ejemplo por estar conectado a la misma red Wi-Fi o porque el identificador único del dispositivo sensor se transfiere ópticamente a la cámara integrada del dispositivo móvil. Esto ayuda a asegurar que el dispositivo sensor está instalado, por ejemplo, en el piso del propietario del edificio de apartamentos en lugar de en el piso de un vecino de abajo o de arriba con un estilo de vida más saludable. Los datos de calibración pueden almacenarse directamente en el dispositivo sensor o en el servidor de la tercera parte de confianza para traducir los datos brutos proporcionados por el sensor de presión del dispositivo sensor en una altitud absoluta.

Es preferible que el dispositivo sensor proporcione una advertencia al servidor o que el servidor genere una advertencia basada en las mediciones de altitud recibidas en caso de que la altitud del dispositivo sensor cambie de una manera que no se pueda explicar, por ejemplo por fenómenos meteorológicos. En este caso, se puede dudar de la autenticidad de los datos brutos recibidos, al menos procedentes del citado dispositivo sensor.

Es preferible que cada vez que el dispositivo móvil conectado a Internet de un propietario entre en una ubicación geográfica predeterminada, la información de identificación de su punto de acceso a Internet se transmita de forma segura al servidor para compararla con la información de identificación del punto de acceso a Internet de los dispositivos sensores que se supone que están en la ubicación geográfica predeterminada transmitida regularmente al servidor por los dispositivos sensores y creando una advertencia en caso de que un dispositivo sensor no se encuentre en la ubicación geográfica esperada. En otras palabras, la tecnología conocida de geo-perimetraje para dispositivos móviles basada en señales de navegación por satélite, localización GSM y/o conectividad a una red Wi-Fi se utiliza para determinar que la ubicación general de los dispositivos sensores en esa ubicación no ha sido alterada, al menos no significativamente. El punto de acceso a Internet es preferiblemente un punto de acceso Wi-Fi, lo que permite que la comparación del dispositivo móvil y los dispositivos sensores se base en el SSID o cualquier otro identificador de la red Wi-Fi a la que están conectados los dispositivos. Como alternativa o además, la dirección IP pública de un punto de acceso a Internet, por ejemplo se puede facilitar un enrutador para tener en cuenta los dispositivos cableados. De cualquier manera, se puede revisar si un dispositivo sensor está realmente instalado en la ubicación prevista, por ejemplo la casa del propietario. Solo si el dispositivo sensor está realmente ubicado en la casa del propietario, el dispositivo móvil del propietario se registrará regularmente a través de la misma red Wi-Fi y/o punto de acceso a Internet que los dispositivos sensores, especialmente durante la noche.

La invención se describe ahora con más detalle junto con el dibujo adjunto. Se muestra:

Figura 1: un dibujo esquemático de una disposición que comprende un dispositivo sensor y que ejecuta un procedimiento, ambos de acuerdo con la invención.

La Figura 1 representa una disposición 1 que comprende una fuente del propietario 100 con un dispositivo sensor 110 de acuerdo con la presente invención, un servidor 200 de una tercera parte de confianza y un receptor 300, en el que se ejecuta el procedimiento de acuerdo con la invención.

En este ejemplo, para facilitar la concisión, se muestra que la fuente 100 asignada a un propietario específico 101 está compuesta por un solo dispositivo sensor 110, aunque típicamente se usa una pluralidad de dispositivos sensores 110. Además, otros dispositivos conectados a Internet, tales como dispositivos portátiles, televisores inteligentes, etc., pueden aportar datos sobre el uso u otros aspectos a la fuente 100 del propietario.

En la fuente 100 del propietario se proporciona un punto de acceso a Internet 120 que establece una red inalámbrica local, en este caso de acuerdo con los estándares Wi-Fi o IEEE 802.11, cuyo alcance se indica mediante la línea de puntos y trazos 121.

Dentro del rango 121 del punto de acceso a Internet 120, se coloca el dispositivo sensor 110. Comprende un módulo sensor 111 con un sensor de presión de alta precisión 112, un procesador 113 para procesar los datos adquiridos por el módulo sensor 111 y un módulo de comunicación 114 adecuado para establecer una conexión con el punto de acceso a Internet 120 y transferir de esta manera datos a través del internet 2 al servidor 200, lo que se explicará más adelante.

Además del sensor de presión 112, el módulo sensor 111 comprende una pluralidad de sensores adicionales para detectar características del entorno del sensor, tales como sensores de temperatura y de luz, etc. Todos los datos adquiridos por el módulo sensor 111 tienen una marca de tiempo y se complementan con el identificador único de los dispositivos sensores 110 por el procesador 113, antes de ser enviado al servidor 200. El procesador 113 también envía el identificador de red determinado por el módulo de comunicación 114 (por ejemplo, el SSID de una red Wi-Fi) junto con el identificador único al servidor 200 ya sea periódicamente o siempre que cambie el identificador de red.

La transmisión real de datos desde la fuente 100 del propietario al servidor está asegurada, por ejemplo por la transmisión de datos cifrados con SSL o TLS.

Con el fin de registrar el dispositivo sensor 110 como perteneciente al propietario 101 y autenticar periódicamente los datos adquiridos por el dispositivo 110, el propietario 101 registra inicialmente el dispositivo sensor 110 como suyo en

el servidor 200. Para ello, el propietario 101 utiliza su dispositivo móvil 102, es decir, su teléfono inteligente, para ejecutar una aplicación que toma una fotografía de una representación gráfica del identificador único del dispositivo, por ejemplo un código de barras o QR, determina el identificador único de dicha fotografía, firma el identificador único con una clave privada creada por la aplicación y transmite el identificador único firmado digitalmente junto con la clave pública apropiada 130 al servidor 200. En consecuencia, el servidor 200 puede asignar cualquier dato recibido de la fuente 100 a su propietario 101.

Debido a que el dispositivo móvil 102 del propietario se encuentra muy cerca del dispositivo sensor 110 para el registro inicial debido a la foto requerida que se debe tomar, la medición de altitud generalmente proporcionada por el dispositivo móvil 102 puede usarse para la calibración del sensor de presión 112 del dispositivo sensor 110. Para ello, la altitud determinada por el dispositivo móvil 102 cuando se toma la citada foto se transfiere al servidor 200 para ser contextualizada con la lectura de presión recibida del dispositivo sensor 110 al mismo tiempo. Después de esto, las lecturas de presión del dispositivo sensor 110 pueden transferirse a la altitud real del dispositivo sensor 110, al menos teniendo en cuenta los efectos del clima y/o la temperatura.

Sin perjuicio de una posible calibración del sensor de presión 112 del dispositivo sensor 110, el sensor 112 es capaz de detectar caídas verticales de 20 cm. En caso de que el procesador 113 detecte una caída vertical de este tipo, se genera una advertencia de que el dispositivo sensor 110 probablemente se ha movido y se transmite al servidor 200 para su posterior consideración, por ejemplo señalar que los datos recibidos desde el respectivo dispositivo sensor 110 ya no son fiables.

De manera similar, el servidor 200 puede verificar que el propietario 101 esté regularmente cerca del dispositivo sensor 110, asegurando de esta manera que los datos generados por el dispositivo sensor 110 realmente reflejen al propietario 101. Para esto, el dispositivo móvil del propietario 102 está equipado con una aplicación de geo-perimetraje. que transmite al servidor 200 la identificación de red de la red inalámbrica a la que el dispositivo móvil 102 está conectado momentáneamente, siempre que la ubicación geográfica del dispositivo móvil 102 corresponda, por ejemplo, al domicilio del propietario. El servidor 200 puede comparar el identificador de red recibido del dispositivo móvil 102 con el identificador de red recibido del dispositivo sensor 110. Si ambos identificadores coinciden, se puede suponer que el dispositivo sensor 110 está instalado, por ejemplo en el domicilio del propietario.

Además de una posible fase de inicialización, en la que los datos sin procesar se transmiten de forma segura desde la fuente 100 al servidor 200 para ejecutar el análisis inicial, por ejemplo determinar patrones en los datos, después de recibir los datos sin procesar por parte del servidor 200, se cifran inmediatamente con una primera clave de cifrado 130 proporcionada al servidor 200 por el propietario 101 (o por el dispositivo móvil del propietario 102 para ser precisos) por un primer módulo de cifrado 201. En el presente ejemplo, la primera clave de cifrado 130 es idéntica a la clave pública utilizada para firmar digitalmente el identificador de dispositivo único del dispositivo sensor 110 (ver más arriba).

Solo los datos sin procesar cifrados se almacenan en el depósito de datos 202 del servidor 200 y, por lo tanto, en principio, ni siquiera son accesibles para la tercera parte de confianza que opera el servidor 200.

En el presente ejemplo, el propietario de la fuente 101 ha suscrito un contrato 400, por ejemplo un contrato de seguro médico, con un receptor 300, por ejemplo una compañía de seguros, que le ofrece un descuento siempre que observe ciertas disposiciones de comportamiento cuyo cumplimiento puede ser verificado por los datos adquiridos por el dispositivo sensor 110, por ejemplo tener regularmente un descanso nocturno suficiente.

El servidor 200, precisamente su procesador 204, cuenta con criterios para evaluar suficientemente el cumplimiento del propietario 101 con el contrato 400. Por ejemplo, un criterio podría ser el requisito para que el dispositivo sensor 110 determine la oscuridad en su entorno durante una duración del tiempo específico en al menos el 90% de las noches, que el propietario 101 pasa en casa de acuerdo con la aplicación de geoperimetraje explicada más arriba. Esto, cuando se correlaciona con cambios en CO_2 en el mismo lugar (por ejemplo, el dormitorio) junto con la detección microsísmica de los movimientos del sueño, también puede indicar, además, cuánto tiempo y con qué calidad duerme el ocupante en ese lugar.

Con el fin de que el servidor 200 pueda evaluar el cumplimiento del propietario 101 con los criterios proporcionados, el propietario 101 proporciona al servidor 200 una primera clave de descifrado 131 para ser utilizada por el módulo de descifrado 203 para descifrar los datos sin procesar inicialmente proporcionados por el dispositivo sensor 110 y almacenados en el depósito de datos 202 que realmente se necesita para la verificación de los criterios proporcionados. Los datos sin procesar restantes proporcionados por el dispositivo sensor 110 permanecen encriptados. Preferiblemente, los citados datos sin procesar restantes ni siquiera pueden descifrarse mediante el uso de la primera clave de descifrado proporcionada, sino que requieren una clave de descifrado diferente.

Posteriormente, los datos descifrados se examinan para ver si se cumplen los criterios proporcionados o, en caso contrario, lo grande que es la desviación. Este examen conduce al resultado de análisis 205, que contiene únicamente información sobre en qué medida se cumplen o no los criterios proporcionados, pero ningún resultado intermedio o incluso datos sin procesar que conduzcan al citado resultado.

Los resultados analíticos 205 son cifrados por el módulo de cifrado 206 con una segunda clave de cifrado 206 proporcionada por el propietario 101 o su dispositivo móvil 102 respectivamente, antes de colocarse en una cadena de bloques 207 como un activo móvil (pero no copiable) 208.

Puesto que los resultados analíticos 205 se almacenan como un activo 208 de una cadena de bloques 207, se pueden transferir solo una vez a un receptor 300 a través de Internet 2, pero no están disponibles libremente para numerosos receptores potenciales.

El receptor único previsto 300, que es parte del contrato 400, puede hacer que el activo 208 se mueva a su bolsillo 301 y, en consecuencia, se le asegura que ningún otro receptor tiene acceso al activo 208.

Con el fin de que el receptor 300 acceda a los resultados analíticos 205 dentro del activo móvil 208 después de que se haya movido a su bolsillo 301, el receptor 300 es requerido por el propietario 101 para le proporcionara una segunda clave de descifrado 133 para que el módulo de descifrado 302 pueda descifrar los resultados analíticos cifrados 205.

Como se puede ver en la figura 1, el propietario 101 puede estar asegurado únicamente por medios técnicos de que el receptor real 300 que es socio de un contrato mutuo recibe solo información seleccionada, es decir, los resultados analíticos 205, pero no cualquier dato adicional adquirido. por la fuente del propietario 100. Además, el propietario 101 dispone de diversos medios técnicos para evitar que cualquier información sea procesada por la tercera parte de confianza o transmitida al receptor 300 mediante el cambio de una o más claves. Por ejemplo, un cambio de las claves de cifrado 130 o 132 en un momento específico, por lo general hace que todos los datos cifrados posteriormente sean inutilizables por la tercera parte de confianza y/o el receptor 300, a menos que se les proporcione una clave de descifrado actualizada 131 y/o 133.

Aunque no se muestra en la Figura 1, el servidor 200 de la tercera parte de confianza puede trabajar, por supuesto, con una pluralidad de fuentes del propietario 100 y receptores 300, lo que permite que se celebren varios contratos entre los diferentes participantes. Proporcionar un servidor 200 por parte de una tercera parte de confianza que sea capaz de ejecutar los análisis requeridos y proporcionar a los receptores 300 los resultados analíticos deseados 205, publicados activamente por el propietario 101, permite ahorrar la potencia computacional requerida en cada receptor potencial 300.

REIVINDICACIONES

1. Procedimiento para proporcionar de forma segura un resultado analítico (205) basado en datos de una fuente (100) a un único receptor (300), en el que el propietario de la fuente (101) y el receptor (300) están vinculados por un contrato (400) con un tercera parte de confianza que supervisa el cumplimiento del contrato (400), que comprende la ejecución permanente de los pasos:

- transmitir datos sin procesar de forma segura desde la fuente (100) a un servidor (300) de la tercera parte de confianza;

- cifrar todos los datos sin procesar recibidos por el servidor (300) con una primera clave de cifrado (130) proporcionada por el propietario de la fuente (101);

y que comprende la ejecución de los siguientes pasos, en caso de que se celebre un contrato (400):

- el propietario de la fuente (101) proporciona al servidor (200) una primera clave de descifrado (131) que permite al servidor (200) descifrar los datos sin procesar requeridos para los análisis necesarios para monitorizar el cumplimiento del contrato (400);

- el servidor (200) evalúa el cumplimiento del contrato (400) en base a criterios predeterminados y cifra el resultado de esta evaluación (205) con una segunda clave de cifrado (132) proporcionada por el propietario de la fuente (101) antes de poner el resultado como activo movible (208) en una cadena de bloques (207); y

- el propietario de la fuente (101) proporciona al receptor (300) una segunda clave de descifrado (133) para descifrar el resultado de la evaluación (205) y, por lo tanto, permitir que el receptor previsto (300) recupere los resultados de la evaluación (205) de la cadena de bloques (207) como único receptor (300).

2. Procedimiento de acuerdo con la reivindicación 1,

caracterizado por que

el servidor (200) analiza los datos sin procesar recibidos antes del cifrado para identificar patrones de datos durante un período de tiempo predeterminado o hasta que se consoliden uno o más patrones.

3. Procedimiento de acuerdo con la reivindicación 2,

caracterizado por que

la tercera parte de confianza que informa a los receptores potenciales (300) cuales resultados analíticos para el propietario de una fuente (101) están disponibles para evaluar el cumplimiento de un contrato (400).

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado por que

los datos sin procesar de la fuente (100) comprenden un identificador único que preferentemente se asigna a un propietario (101) mediante una copia del identificador único firmado con una clave privada del propietario de la fuente (101) y verificable por el servidor (200) con una clave pública del propietario de la fuente (101), preferentemente la primera clave de cifrado.

5. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado por que

la transmisión segura de datos sin procesar se realiza por medio de Internet (2) mediante el uso de un protocolo de transmisión seguro.

6. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado por que

los datos brutos de la fuente (100) son proporcionados al menos parcialmente por un dispositivo sensor (110) conectado a Internet que comprende medios para determinar su altitud.

7. Procedimiento de acuerdo con la reivindicación 6,

caracterizado por que

el dispositivo sensor (11) proporciona una advertencia al servidor (200) o el servidor (200) genera una advertencia basada en las mediciones de altitud recibidas en caso de que se cambie la altitud del dispositivo sensor (110).

8. Procedimiento de acuerdo con la reivindicación 6 o 7,

caracterizado por que

cada vez que el dispositivo móvil conectado a internet de un propietario (102) ingresa a una ubicación geográfica predeterminada, la información de identificación de su punto de acceso a internet (120) se transmite de forma segura al servidor (200) para compararla con la información de identificación del punto de acceso a internet (120) de esos dispositivos sensores (110) que se supone que están en la ubicación geográfica predeterminada transmitida regularmente al servidor (200) por el dispositivo sensor (110) y creando una advertencia en caso de que un dispositivo sensor (110) no se encuentre en el lugar esperado localización geográfica.

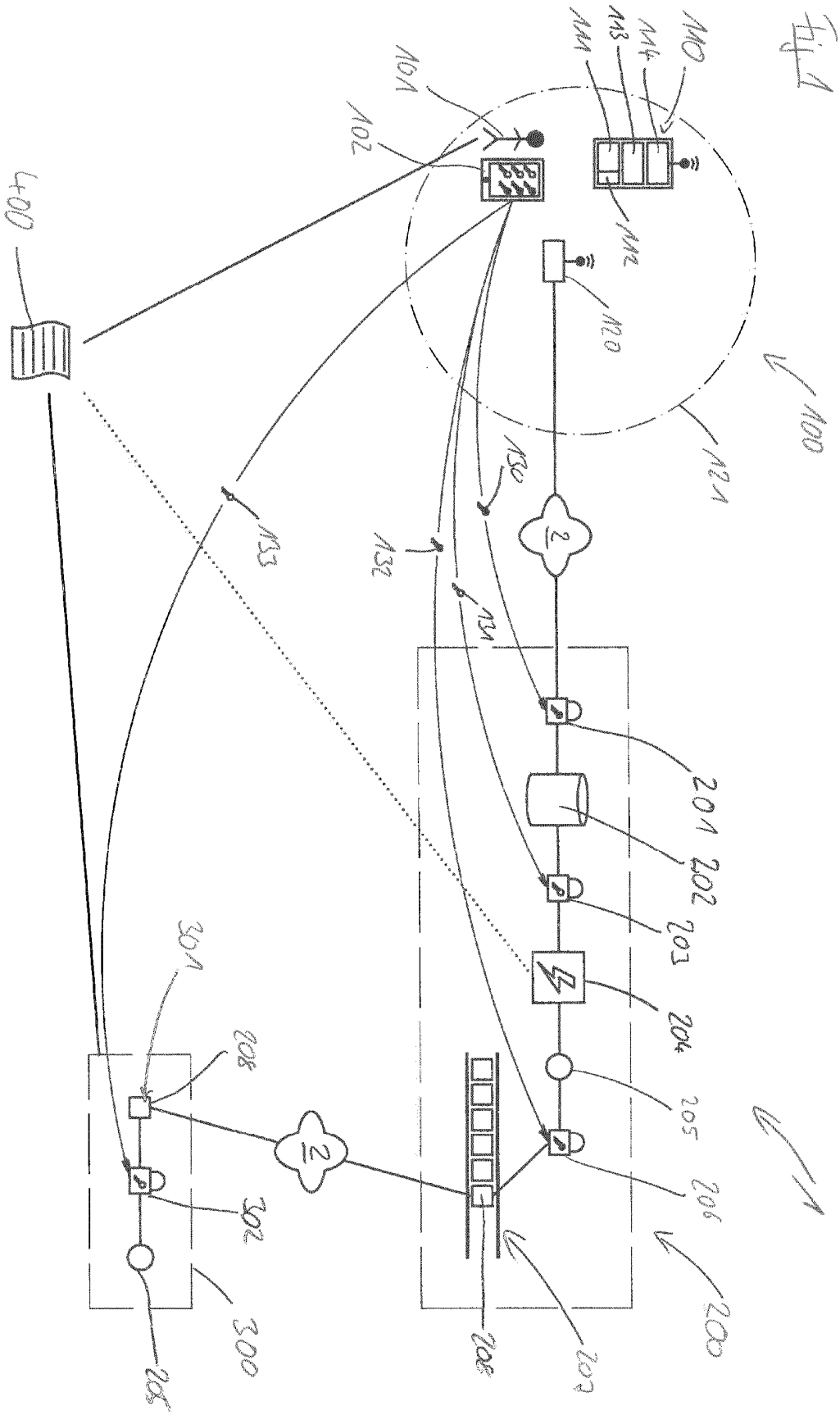
Fig. 1
100
110
111
112
113
114
101
102
120
121
130
131
132
133
200
201
202
203
204
205
206
207
208
300
301
302
303
400