(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 010 128**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04L 67/1097 (2012.01)
H04L 67/12 (2012.01)
H04W 12/61 (2011.01)
H04W 12/084 (2011.01)
H04W 12/04 (2011.01)
H04W 12/03 (2011.01)
H04W 12/00 (2011.01)
H04W 4/38 (2008.01)
H04W 84/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.02.2022 PCT/EP2022/054149**

(87) Fecha y número de publicación internacional: **25.08.2022 WO22175490**

(96) Fecha de presentación y número de la solicitud europea: **18.02.2022 E 22711173 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2024 EP 4295537**

(54) Título: **Métodos y sistemas para controlar el acceso a datos de sensor**

(30) Prioridad:

19.02.2021 EP 21158265

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.04.2025

(73) Titular/es:

NAGRAVISION SÀRL (100.00%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

GREMAUD, FABIEN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Métodos y sistemas para controlar el acceso a datos de sensor

Campo técnico de la invención

La presente invención se refiere a controlar el acceso a datos de sensor. Más específicamente, se refiere a métodos y sistemas que se basan en el cifrado basado en una clave local en un sensor y el uso de un testigo de autorización para garantizar que un dispositivo únicamente puede acceder a los datos a los que tiene permitido acceder. Diversos aspectos de la invención se refieren a diferentes partes del sistema y los métodos realizados por esas partes diferentes.

Antecedentes de la invención

Los sensores están presentes en todas partes en la vida cotidiana y son esenciales para el funcionamiento y el mantenimiento de casi todos los dispositivos que vemos y usamos. Es necesario garantizar que los datos obtenidos por un sensor determinado no puedan ser accedidos ni modificados por ningún otro dispositivo. Por ejemplo, puede ser deseable que los datos recopilados por un sensor que detecta el desgaste de la maquinaria industrial únicamente sean accesibles para los dispositivos pertenecientes a ingenieros encargados del mantenimiento de esas máquinas. Del mismo modo, también es importante garantizar que los datos de sensor no puedan ser manipulados, excepto por partes autorizadas. Tradicionalmente, los permisos de acceso a un dispositivo estaban controlados por una plataforma de seguridad. Sin embargo, con la llegada de la computación perimetral, en la que el procesamiento de datos se lleva a cabo en dispositivos en los nodos de una red, en lugar de realizarse de forma central, los dispositivos perimetrales pueden estar significativamente separados de la plataforma de seguridad, por un llamado "hueco de aire". En estos casos, es posible que no haya una conexión segura o una red segura entre el dispositivo perimetral y la plataforma de seguridad. Por lo tanto, existe la necesidad de un sistema en el que el acceso a los datos de sensor por un dispositivo pueda controlarse de forma segura, incluso cuando el dispositivo y el sensor estén alejados de la plataforma de seguridad que controla los permisos de acceso. Esta necesidad es abordada por la invención a la que se refiere la presente solicitud.

El documento US 2017/103216 A1 describe métodos y sistemas para la seguridad y privacidad de datos de redes sensoriales de iluminación. "Security Patterns for Capturing Encryption-Based Access Control to Sensor Data" por Cuevas *et al.* (2008) describe una solución genérica para garantizar el control de acceso de extremo a extremo a los datos generados por sensores inalámbricos y consumidos por aplicaciones comerciales, basándose en un nuevo enfoque para el control de acceso basado en cifrado.

Sumario de la invención

En términos generales, la presente invención proporciona un sistema en el que los datos de control de acceso, incluidos, por ejemplo, en un testigo de autorización que puede generarse por una plataforma de seguridad remota, se despliegan en un dispositivo tal como un dispositivo perimetral, definiendo los datos de control de acceso, por ejemplo, en el testigo de autorización, los datos de sensor a los que el dispositivo tiene acceso y las operaciones que el dispositivo está autorizado a ejecutar en esos datos de sensor. Un sensor genera datos de sensor, los protege y, a continuación, los transmite al dispositivo para su almacenamiento. Por lo tanto, aunque los datos de sensor están almacenados en el dispositivo - es posible que el dispositivo no pueda utilizarlos debido a que están protegidos. Si el dispositivo desea acceder a los datos de sensor, puede enviar una solicitud al sensor, junto con los datos de control de acceso, por ejemplo, el testigo de autorización. El sensor permite a continuación que el dispositivo ejecute únicamente ciertas operaciones permitidas, por ejemplo, devolviendo al dispositivo claves que únicamente se pueden usar para ejecutar las operaciones permitidas. Desplegando el testigo de autorización en el dispositivo, no es necesario que el dispositivo tenga una conexión física con la plataforma de seguridad. Y, debido a que los datos almacenados en el dispositivo están protegidos y únicamente se puede acceder a ellos con los permisos correctos, la seguridad de los datos no se ve comprometida. Se observará que esta invención tiene numerosos componentes, cada uno de los cuales contribuye a las ventajas técnicas logradas. En consecuencia, existen numerosos aspectos de la presente invención.

Un aspecto de la invención proporciona un método para controlar el acceso a datos de sensor, como se expone en la reivindicación 1.

En el presente documento, los datos de sensor pueden protegerse usando una clave secreta, tal como, por ejemplo, una clave de cifrado.

Específicamente, permitir que el dispositivo ejecute la operación permitida puede comprender transmitir, al dispositivo, una señal que comprende una o más claves, o datos que codifican una o más claves, siendo la una o más claves utilizables por el dispositivo para ejecutar la operación permitida en los datos de sensor protegidos. Otro aspecto de la invención proporciona un sensor como se expone en la reivindicación 15.

Hay dos formas importantes en las que se puede controlar el acceso a los datos de sensor: en primer lugar, dependiendo de la operación permitida, se pueden proporcionar diferentes claves al dispositivo. Como alternativa, o adicionalmente, los datos de sensor pueden incluir una pluralidad de subconjuntos (que pueden ser distintos) de datos de sensor, cada uno protegido individualmente. En ese caso, el sensor puede proporcionar al dispositivo únicamente claves que puedan usarse para acceder a subconjuntos permitidos de los datos de sensor.

Otro aspecto complementario de la invención es un método que se realiza por el dispositivo, en lugar del sensor, específicamente un método de acceso a datos de sensor protegidos por un dispositivo, como se expone en la reivindicación 10.

Un aspecto adicional de la invención proporciona un dispositivo como se expone en la reivindicación 16.

Las implementaciones de la presente invención permiten realizar mayores cantidades de procesamiento y computación en "el perímetro" con un riesgo reducido de interferencia por actores maliciosos. Como resultado, la invención puede aplicarse ventajosamente a diversos casos de uso, tales como vehículos inteligentes y edificios inteligentes. En el contexto de la presente invención, el término "inteligente" puede usarse en general para referirse a áreas de tecnología en las que los datos se recopilan mediante sensores a través de todo, por ejemplo, el vehículo o el edificio, y los datos se usan para informar los procesos de control relacionados con el vehículo o el edificio. Con la llegada del llamado "Internet de las cosas", cada vez se realizan más cálculos y procesamientos también en los propios sensores. De acuerdo con un aspecto adicional de la invención, se proporciona un edificio que comprende una pluralidad de sensores interconectados por una red, en donde al menos un sensor de la pluralidad de sensores es un sensor de acuerdo con un aspecto anterior de la presente invención. Preferentemente, cada sensor de la pluralidad de sensores es un sensor de acuerdo con un aspecto anterior de la invención. Los aspectos equivalentes de la invención proporcionan un vehículo en lugar de un edificio.

Los sensores de acuerdo con todos los aspectos de la invención pueden incluir cualquiera o todos los siguientes: cámaras, sensores de proximidad, sensores de CO_2, sensores de humo, sensores de presión, sensores de humedad, acelerómetros, sensores de posición, sensores de movimiento, sensores basados en LiDAR, sensores de temperatura, sensores de fuerza, sensores de vibración, sensores piezoeléctricos, sensores de propiedades de fluidos, sensores fotoópticos, sensores de intensidad de luz. Sin embargo, se apreciará que ésta no es una lista exhaustiva y la invención no está de ninguna manera limitada a este tipo de sensores.

En el contexto de los vehículos, los "sensores" de la invención pueden estar configurados para detectar condiciones específicas dentro del vehículo.

A continuación, los datos pueden protegerse para garantizar que únicamente el personal de mantenimiento autorizado pueda acceder a los datos de sensor para informar decisiones de mantenimiento. Los tipos específicos de datos de sensor u otra información que podrían obtenerse en el contexto de vehículos inteligentes o de vehículos más en general incluyen los siguientes:

- Información acerca de la identidad del vehículo (que podría estar codificada u obtenerse de un código u otro identificador tal como un código QR, donde el sensor puede ser el dispositivo que se usa para obtener la información de identidad del código u otro identificador). Esto podría aplicarse, por ejemplo, a los sistemas de reconocimiento automático de matrículas. De manera similar, también podría haber información acerca de la identidad del pasajero o del conductor del vehículo que podría obtenerse, por ejemplo, a partir de sensores de imagen o explorando un código, como en el caso de la identidad del vehículo.

- Información que puede ser útil para la navegación, por ejemplo, la posición del vehículo, un vector que indica el movimiento del vehículo, así como un cambio en el vector que puede ser indicativo de un cambio de dirección del vehículo o una aceleración o desaceleración del vehículo. Esto puede detectarse mediante un rastreador de GPS (u otro sistema de navegación por satélite) ubicado en el coche. En este caso, puede ser particularmente importante proteger los datos de sensor, por el bien de la privacidad del propietario del vehículo. Dado que tal información a menudo se usa por compañías de seguros y las autoridades policiales, también es muy importante que cualquier intento de manipulación de los datos obtenidos sea prevenible o detectable. De manera similar, los datos de sensor pueden incluir el kilometraje del vehículo o la cantidad de tiempo durante la que se ha usado el vehículo.

- Los sensores pueden configurarse para detectar cuándo varios componentes del vehículo requieren mantenimiento o están dañados. Esta información es de particular relevancia para el personal de mantenimiento. De manera similar, los sensores pueden detectar el consumo de, por ejemplo, aceite, combustible o energía de la batería dentro del vehículo. La detección de la carga de la batería es particularmente importante en el contexto de vehículos eléctricos.

- Puede haber sensores del entorno dentro del vehículo, del tipo enumerado anteriormente.

Los contextos comerciales en los que los sensores que obtienen este tipo de información podrían ser particularmente

útiles incluyen: seguros, gestión de flotas, comercio/transacciones, estado/mantenimiento de vehículos, comunicaciones de vehículo a vehículo, vehículos autónomos, estacionamiento inteligente y gestión de tráfico.

Consideraciones similares se aplican a los edificios que incluyen sensores: es importante garantizar que únicamente el personal de mantenimiento autorizado pueda acceder a los datos de sensor.

La invención incluye la combinación de los aspectos y características preferidas descritas excepto cuando una combinación de este tipo sea claramente inadmisible o se evite expresamente.

Breve descripción de los dibujos

Las realizaciones de la presente invención se describirán ahora con referencia a las siguientes figuras, en las que:

- La Figura 1 muestra un sistema que incluye un sensor 10 y un dispositivo 20.
- La figura 2 muestra un ejemplo de un método que puede realizarse por el sensor 10.
- La figura 3 muestra un ejemplo de un método que puede realizarse por el dispositivo 20.
- La Figura 4 muestra un ejemplo alternativo de un sensor 100.
- La Figura 5 muestra un ejemplo alternativo de un dispositivo 200.
- La Figura 6 ilustra cómo los datos de sensor pueden dividirse en subconjuntos.
- La Figura 7 ilustra un proceso para recuperar o generar una clave de cifrado para una pieza de datos dada.
- Las Figuras 8A y 8B ilustran las distribuciones de dos tablas de datos de claves de cifrado ilustrativas.
- La Figura 9 ilustra un método de generación de clave de cifrado.
- La Figura 10 ilustra un método de autenticación.
- La Figura 11 ilustra un sistema que incluye sensores, dispositivos y un componente operativo.

Descripción detallada de los dibujos

A continuación, se analizarán aspectos y realizaciones de la presente invención con referencia a las figuras adjuntas. Para los expertos en la materia serán evidentes aspectos y realizaciones adicionales. Todos los documentos mencionados en este texto se incorporan como referencia en el presente documento.

La presente invención se refiere a diversos métodos y dispositivos. En particular, la invención se refiere a un método realizado por un sensor, un método realizado por un dispositivo tal como un dispositivo perimetral o un servidor, y un método realizado por un sistema que incluye los dos. La invención se refiere también al sensor, al dispositivo y al sistema en sí. La Figura 1 muestra un sistema 1 que incluye un sensor 10 y un dispositivo 20. Las Figuras 2 y 3 muestran, respectivamente, un ejemplo específico de un método según la presente invención que puede realizarse por el sensor 10 y el dispositivo 20.

Como se ha analizado, el sistema 1 de la Figura 1 incluye un sensor 10 y un dispositivo 20. El sensor 10 y el dispositivo 20 están conectados a través de una conexión C. La conexión C puede ser cualquier forma de conexión que pueda transportar datos y/o información entre los dos. Preferentemente, la conexión C es una conexión eléctrica, y puede ser una conexión alámbrica o una conexión inalámbrica, tal como una conexión a través de una red inalámbrica, tal como una red Wi-Fi o celular. Como alternativa, la conexión inalámbrica puede ser en forma de una conexión de Bluetooth o una conexión de comunicación de campo cercano. Se entenderá que, la conexión C podría tomar un número de formas diferentes que no es necesario exponer explícitamente en el presente documento.

El sensor 10 incluye un procesador 11, que incluye un módulo de cifrado 12 y un módulo de determinación de acceso 13. Tanto con referencia a la Figura 1, como al resto de la solicitud, debe observarse que, el término "módulo" se refiere a cualquier unidad funcional configurada para realizar una función dada. El módulo puede implementarse ya sea con hardware especializado, adaptado o modificado, o, como alternativa, puede implementarse en forma de un módulo de software, por ejemplo, en forma de una sección de código.

El eNB 10 incluye además un transmisor 14 y un receptor 15. En el presente documento, el término "transmisor" se utiliza de forma amplia para cubrir cualquier componente que pueda transmitir datos o efectuar la transmisión de datos. Por ejemplo, el transmisor 14 puede estar configurado para generar y enviar una señal inalámbrica, codificando la señal inalámbrica los datos. Como alternativa, el transmisor 14 puede estar configurado para efectuar la transmisión

de datos a través de una conexión alámbrica, tal como la conexión C. El término "receptor" debe tratarse de manera similar y amplia como cualquier componente que pueda recibir datos. Por ejemplo, el receptor 15 puede estar configurado para recibir una señal inalámbrica, o puede estar configurado para recibir datos a través de una conexión alámbrica, tal como la conexión C. Las funciones del sensor 10, el procesador 11, el módulo de cifrado 12, el módulo de determinación de acceso 13, el transmisor 14 y el receptor 15 se describen con más detalle más adelante en esta solicitud, con referencia a las Figuras 2 y 3.

El dispositivo 20 incluye un receptor 21, una memoria 22, un procesador 25 y un transmisor 26. Los términos "transmisor" y "receptor" deberán interpretarse como se expone en el párrafo anterior. La memoria 22 del dispositivo 20 incluye o tiene almacenados en la misma un testigo de autorización 23 y datos de sensor cifrados 24. La naturaleza de éstos se describirá más adelante.

Antes de describir realizaciones específicas de la invención, exponemos en primer lugar características opcionales del primer aspecto de la invención y del segundo aspecto de la invención en términos generales. Aunque en la siguiente divulgación se usan números de referencia, debe observarse que se prevé explícitamente que el método pueda implementarse usando un sistema distinto del sistema mostrado en la Figura 1.

Como se analizó anteriormente, el primer aspecto de la invención proporciona un método para controlar el acceso a datos de sensor, incluyendo el método las etapas de generar datos de sensor y proteger los datos de sensor usando una o más claves secretas, para generar datos de sensor protegidos 24; y transmitir los datos de sensor protegidos 24 a un dispositivo 20 para su almacenamiento; recibir, por el sensor 10: un testigo de autorización 23 que incluye datos de control de acceso que definen una o más operaciones que el dispositivo 20 está autorizado a ejecutar en los datos de sensor protegidos 24; determinar por el sensor 10, basándose en los datos de control de acceso, una operación que el dispositivo 20 está autorizado a ejecutar en los datos de sensor protegidos 24; proporcionar al dispositivo 20 una o más claves utilizables por el dispositivo 20 para ejecutar la operación permitida en los datos de sensor protegidos 24. En casos preferidos, para reducir los requisitos de almacenamiento del sensor 10 (específicamente, una memoria del mismo), el método puede incluir además una etapa de borrado de los datos de sensor después de la etapa de transmisión de los mismos al dispositivo 20. En el corazón de la invención está la idea de que el sensor 10 proporcionará al dispositivo 20 únicamente la clave o claves que el dispositivo 10 puede utilizar para ejecutar operaciones que está autorizado a ejecutar, basándose en los datos de control de acceso en el testigo de autorización 23. Las operaciones permitidas y la naturaleza de las claves asociadas a las mismas se analizarán con más detalle más adelante, pero antes de eso, describiremos un caso general en el que se pueden aplicar diversas claves durante la generación de los datos de sensor protegidos, y se pueden utilizar combinaciones de esas claves para ejecutar diversas operaciones en los datos de sensor protegidos. Debe observarse que las diversas claves se pueden aplicar una después de otra, de manera "apilada".

En algunos casos, proteger los datos de sensor incluye aplicar una primera clave secreta a los datos de sensor, para generar los primeros datos de sensor protegidos. A continuación, si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar una primera operación en los primeros datos de sensor protegidos, la etapa de proporcionar puede incluir proporcionar, al dispositivo, una primera clave complementaria, utilizable por el dispositivo para ejecutar la primera operación. En el presente documento, la primera operación puede ser complementaria a la aplicación de la primera clave secreta a los datos de sensor, por ejemplo, cifrado/descifrado (este ejemplo específico se analiza con cierto detalle más adelante en la solicitud). En el presente documento, el término "complementario" debe entenderse en el sentido de que la clave puede realizar la acción complementaria a la clave secreta. Por ejemplo, si la clave secreta es una clave de cifrado, la clave complementaria puede ser la clave de descifrado correspondiente. Si la clave secreta se usa para generar un código de autenticación, a continuación, la clave complementaria puede ser la misma que la clave secreta, permitiendo de esta manera que el dispositivo genere el mismo código de autenticación para autenticar los datos de sensor protegidos. Es importante observar que, la clave complementaria puede ser la misma que la clave secreta.

En un caso preferido, la primera clave secreta es una clave de cifrado y los primeros datos de sensor protegidos son datos de sensor cifrados. A continuación, la primera operación puede ser una operación de descifrado o de lectura. En ese caso, la etapa de proporcionar puede incluir proporcionar una clave complementaria en forma de clave de descifrado al dispositivo. En algunas realizaciones, la clave de cifrado puede ser una clave de cifrado simétrico, en cuyo caso la clave de cifrado y la clave de descifrado pueden ser la misma. En este ejemplo, el sensor cifra los datos de sensor y el dispositivo únicamente puede recibir la clave para descifrarlos si los datos de control de acceso especifican que está permitido.

En otros casos, proteger los datos de sensor puede incluir aplicar una segunda clave secreta a los primeros datos de sensor protegidos, para generar segundos datos de sensor protegidos. A continuación, son posibles dos resultados posibles:

1. Si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar una segunda acción en los segundos datos protegidos, la etapa de proporcionar puede incluir proporcionar, al dispositivo, una segunda clave complementaria, utilizable por el dispositivo para ejecutar la segunda operación en los segundos datos de sensor protegidos. En el presente documento, la segunda operación puede ser complementaria a la aplicación de

la segunda clave secreta a los primeros datos de sensor protegidos, como se ha descrito anteriormente.

2. Si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar **cualquiera de** tanto la primera como la segunda operación, **o** una tercera operación (que puede ser, opcionalmente, una combinación de la primera y la segunda operación, o requerir que ambas se ejecuten para ejecutarla), a continuación, la etapa de proporcionar puede incluir: proporcionar, al dispositivo, la primera clave complementaria y la segunda clave complementaria, siendo la primera clave complementaria y la segunda clave complementaria utilizables en combinación para ejecutar la tercera operación en los segundos datos de sensor protegidos. O, la etapa de proporcionar puede incluir: proporcionar, al dispositivo, la primera clave complementaria y la segunda clave complementaria, utilizable la segunda clave complementaria por el dispositivo para ejecutar la segunda operación en los segundos datos de sensor protegidos para recuperar los primeros datos de sensor protegidos, y, a continuación, utilizable la primera clave complementaria por el dispositivo para ejecutar la primera operación en los primeros datos de sensor protegidos.

A continuación, describimos dos situaciones ilustrativas en las que se pueden usar dos claves.

La primera es cuando a los datos de sensor se les aplica en primer lugar una clave de autenticación para generar un código de autenticación. A continuación, se aplica una clave de cifrado a la combinación de los datos de sensor y el código de autenticación, para generar datos de sensor cifrados. En este caso, la primera clave secreta es la clave de autenticación; los primeros datos protegidos son la combinación de los datos de sensor y el código de autenticación; la segunda clave secreta es la clave de cifrado; y los segundos datos de sensor protegidos son los datos de sensor cifrados. A continuación, consideramos los casos 1 y 2 mencionados anteriormente:

1. La segunda operación puede ser el descifrado. En otras palabras, si los datos de control de acceso definen que el dispositivo está autorizado a descifrar los datos de sensor cifrados, la etapa de proporcionar puede incluir proporcionar al dispositivo una clave de descifrado (complementaria a la clave de cifrado) utilizable por el dispositivo para descifrar los datos de sensor cifrados. En el caso de que se use una clave de cifrado simétrica, la clave de cifrado y la clave de descifrado pueden ser idénticas.

2. La primera operación puede ser la autenticación y la segunda operación puede ser (aún) el descifrado. En otras palabras, la tercera operación puede comprender, por ejemplo, modificar los datos de sensor, específicamente la modificación de los datos de sensor de una manera que puedan ser autenticados. Para que el dispositivo modifique los datos de sensor, en primer lugar, debe poder descifrarlos, punto en el cual podrá modificarlos. Si un dispositivo no autorizado hace esto, a continuación, será detectable porque (sin la clave de autenticación), un dispositivo de este tipo no podrá generar un código de autenticación correspondiente a los datos de sensor modificados. Así, los dispositivos autorizados deben poder tanto descifrar los datos de sensor (es decir, leerlos), como también, después de modificarlos, volver a autenticarlos para que los datos de sensor modificados puedan autenticarse. **En consecuencia,** si los datos de control de acceso definen que el dispositivo está autorizado a descifrar y volver a autenticar los datos de sensor cifrados, o para modificar los datos de sensor, la etapa de proporcionar puede incluir:

a. proporcionar al dispositivo la primera clave de autenticación y la clave de descifrado, utilizables la primera clave de autenticación y la clave de cifrado en combinación para modificar los datos de sensor; o

b. proporcionar al dispositivo la primera clave de autenticación y la clave de descifrado, utilizable la clave de descifrado por el dispositivo para descifrar los datos de sensor cifrados, para recuperar la combinación de los datos de sensor y el código de autenticación, permitiendo de esta manera que el dispositivo modifique los datos de sensor, genere datos de sensor modificados, y utilizable la primera clave de autenticación por el dispositivo en los datos de sensor modificados para generar un segundo código de autenticación. En algunos casos, como se ha analizado, la clave de cifrado es simétrica y, por tanto, idéntica a la clave de descifrado. En tales casos, a continuación, el dispositivo puede usar la clave para volver a cifrar la combinación de los datos de sensor modificados y el segundo código de autenticación para generar datos de sensor cifrados modificados para su almacenamiento en, por ejemplo, una memoria del dispositivo.

En un segundo ejemplo, la primera clave secreta puede ser una clave de cifrado y los primeros datos de sensor protegidos pueden ser datos de sensor cifrados. A continuación, la segunda clave secreta puede ser una segunda clave de autenticación (no relacionada con la primera clave de autenticación que formaba parte del ejemplo anterior), y los segundos datos de sensor protegidos pueden tomar la forma de un código de autenticación o, preferentemente, una combinación de los datos de sensor cifrados y el código de autenticación. La primera operación puede ser una operación de descifrado y la segunda operación puede ser una operación de autenticación. Obsérvese que, esto es opuesto al ejemplo anterior.

A continuación:

1. La segunda operación puede ser la autenticación. En ese caso, si los datos de control de acceso definen que el dispositivo está autorizado a autenticar los datos de sensor cifrados, la etapa de proporcionar puede incluir proporcionar, al dispositivo, una clave de autenticación utilizable por el dispositivo para autenticar los datos de

sensor cifrados. La etapa de autenticación en el presente documento puede incluir usar la clave de autenticación en los datos de sensor cifrados, para generar un código de autenticación y comparar el código de autenticación generado con el código de autenticación incluido en los segundos datos de sensor protegidos. Si los dos son iguales, se puede concluir que los datos de sensor cifrados no han sido manipulados. Si los dos no coinciden, a continuación, es posible que los datos sensor cifrados hayan sido manipulados de manera no autorizada.

2. La primera operación puede ser el cifrado. En ese caso, si los datos de control de acceso definen que el dispositivo está autorizado a descifrar los datos de sensor cifrados, la etapa de proporcionar al dispositivo una clave de descifrado utilizable por el dispositivo para descifrar los datos de sensor cifrados, recuperando de esta manera los datos de sensor. Cabe señalar que, en este caso, el descifrado podría tener lugar sin autenticación. Sin embargo, es conveniente confirmar en primer lugar que los datos de sensor cifrados son auténticos. En consecuencia, si los datos de control de acceso definen que el dispositivo está autorizado tanto autenticar como descifrar los datos de sensor cifrados, se prefiere que el dispositivo ejecute la etapa de autenticación antes de la etapa de descifrado.

Los ejemplos anteriores únicamente requieren (explícitamente) la aplicación de una primera clave secreta y una segunda clave secreta. Sin embargo, se apreciará que el método puede generalizarse a la aplicación de una pluralidad general de claves secretas. En tales casos, proteger los datos de sensor puede incluir aplicar una pluralidad de claves secretas a los datos de sensor para generar los datos de sensor protegidos. A continuación, la etapa de proporcionar puede incluir proporcionar, al dispositivo, una pluralidad de claves complementarias, cada una complementaria a una clave secreta respectiva de la pluralidad de claves secretas, una combinación de la pluralidad de claves complementarias utilizables por el dispositivo para ejecutar la operación permitida.

En un caso que es una extensión del ejemplo específico analizado anteriormente, se usan tres claves:

1. La primera clave secreta es una primera clave de autenticación.

2. La segunda clave secreta es una clave de cifrado.

3. La tercera clave secreta es una segunda clave de autenticación.

En este caso, proteger los datos de sensor incluye las siguientes etapas: aplicar la primera clave de autenticación para generar primeros datos de sensor protegidos, incluyendo los datos de sensor y un primer código de autenticación; aplicar la clave de cifrado a los primeros datos de sensor protegidos para generar segundos datos de sensor protegidos en forma de datos de sensor cifrados (que es un cifrado tanto de los datos de sensor como del primer código de autenticación); y aplicar la segunda clave de autenticación de los segundos datos de sensor protegidos para generar terceros datos de sensor protegidos que incluyen los datos de sensor cifrados y un segundo código de autenticación.

Este ejemplo combina eficazmente los dos ejemplos expuestos anteriormente. En este caso:

1. La primera operación es la autenticación de los datos de sensor.

2. La segunda operación es una operación de descifrado.

3. La tercera operación es la autenticación de los datos de sensor cifrados.

Si los datos de control de acceso definen que el dispositivo está autorizado a autenticar los datos de sensor cifrados, la etapa de proporcionar puede incluir proporcionar, al dispositivo, la segunda clave de autenticación utilizable por el dispositivo para autenticar los datos de sensor cifrados.

Si los datos de control de acceso definen que el dispositivo está autorizado a descifrar los datos de sensor cifrados, la etapa de proporcionar puede incluir proporcionar al dispositivo una clave de descifrado (complementaria a la clave de cifrado) utilizable por el dispositivo para descifrar los datos de sensor cifrados. En el caso de que se use una clave de cifrado simétrica, la clave de cifrado y la clave de descifrado pueden ser idénticas. En el caso de que los datos de control de acceso definan que el dispositivo está autorizado a autenticar y descifrar los datos de sensor cifrados, a continuación, se pueden proporcionar ambas claves para permitir que el dispositivo ejecute ambas operaciones.

Si los datos de control de acceso definen que el dispositivo está autorizado a descifrar y volver a autenticar los datos de sensor cifrados, o para modificar los datos de sensor, la etapa de proporcionar puede incluir:

proporcionar al dispositivo la primera clave de autenticación y la clave de descifrado, utilizables la primera clave de autenticación y la clave de cifrado en combinación para modificar los datos de sensor; o

proporcionar al dispositivo la primera clave de autenticación y la clave de descifrado, utilizable la clave de descifrado por el dispositivo para descifrar los datos de sensor cifrados, para recuperar la combinación de los datos de sensor y el primer código de autenticación, permitiendo de esta manera que el dispositivo modifique los datos

de sensor, genere datos de sensor modificados, y la primera clave de autenticación utilizable por el dispositivo en los datos de sensor modificados para generar un tercer código de autenticación. En algunos casos, como se ha analizado, la clave de cifrado es simétrica y, por tanto, idéntica a la clave de descifrado. En tales casos, a continuación, el dispositivo puede usar la clave para volver a cifrar la combinación de los datos de sensor modificados y el tercer código de autenticación para generar datos de sensor cifrados modificados para su almacenamiento en, por ejemplo, una memoria del dispositivo.

Puede darse el caso de que el orden en el que se aplica la pluralidad de claves secretas sea importante y, en correspondencia, el orden en el que se aplica la pluralidad de claves complementarias también sea importante. En estos casos (que pueden o no formar un subconjunto de los casos anteriores señalados anteriormente), proteger los datos de sensor puede incluir: aplicar, en sucesión, N claves secretas a los datos de sensor, para generar datos de sensor protegidos de orden *N*, en donde la aplicación de la primera clave a los datos de sensor genera primeros datos de sensor protegidos y, para $k > 1$, aplicar la clave de orden *k* para los datos de sensor protegidos de orden (*k*-1) genera datos de sensor protegidos de orden *k*, en donde $1 < k \leq N$. A continuación, si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar una operación de orden *M* en los datos de sensor protegidos de orden *N*, donde $1 \leq M \leq N$, la etapa de proporcionar incluye proporcionar, al dispositivo ($N + 1 - M$) claves complementarias al subconjunto de claves de la pluralidad de claves secretas para las que $M \leq k \leq N$, siendo utilizables las *M* claves en sucesión desde la clave complementaria de orden *N* a la clave complementaria de orden *M*, para ejecutar o facilitar la ejecución de la operación de orden *M*. En concreto, el dispositivo puede aplicar a continuación la pluralidad de claves complementarias en el sensor protegido de orden *N* en sucesión desde *N* hasta *M*, en donde la aplicación de la clave complementaria de orden *k* a los datos de sensor protegidos de orden *k* recupera los datos de sensor protegidos de orden $(k - 1)$ para $k > 1$, y en donde la aplicación de la primera clave complementaria a los primeros datos de sensor protegidos recupera los datos de sensor.

De acuerdo con ciertas implementaciones, el método puede incluir además una etapa de generación de una clave secreta para cada pieza individual de datos que se genera por el sensor. La generación y el almacenamiento de las claves secretas de esta manera se explica con más detalle más adelante en esta solicitud, en el contexto de las claves de cifrado. Sin embargo, debe observarse que dicha divulgación se aplica igualmente al caso de una clave secreta genérica usada para proteger los datos de sensor.

En algunos casos, se puede permitir que el dispositivo ejecute diferentes operaciones en diferentes subconjuntos de los datos. Por ejemplo, un dispositivo dado puede modificar y volver a autenticar un subconjunto de los datos, pero únicamente para descifrar otro subconjunto. Tales permisos se definen preferentemente en los datos de control de acceso incluidos en el testigo de autorización. Específicamente, los datos de sensor pueden incluir un primer subconjunto de datos de sensor y un segundo subconjunto de datos de sensor. En consecuencia, generar los datos de sensor protegidos puede incluir: proteger el primer subconjunto de datos de sensor para generar un primer subconjunto de datos de sensor protegidos, y proteger el segundo subconjunto de datos de sensor para generar un segundo subconjunto de datos de sensor protegidos. La forma en que los datos de sensor pueden dividirse en subconjuntos se explica en detalle más adelante en esta solicitud. Como antes, generar el primer subconjunto de datos de sensor protegidos puede incluir aplicar una primera clave secreta al primer subconjunto de datos de sensor, y generar el segundo subconjunto de datos de sensor protegidos puede incluir aplicar una segunda clave secreta al segundo subconjunto de datos de sensor.

En estos casos, los datos de control de acceso pueden definir: una primera operación que el dispositivo está autorizado a ejecutar en el primer subconjunto de datos de sensor protegidos; y/o una segunda operación que el dispositivo está autorizado a ejecutar en el segundo subconjunto de datos de sensor protegidos.

A continuación, la etapa de determinación puede incluir determinar, basándose en los datos de control de acceso: una primera operación que el dispositivo está autorizado a ejecutar en el primer subconjunto de datos de sensor protegidos; y/o una segunda operación que el dispositivo está autorizado a ejecutar en el segundo subconjunto de datos de sensor protegidos. Es posible que no se permita que el dispositivo ejecute una operación tanto en el primer subconjunto como en el segundo subconjunto. En consecuencia, la etapa de proporcionar puede incluir: únicamente si se determina que el dispositivo está autorizado para ejecutar la primera operación, proporcionar una o más claves utilizables por el dispositivo para ejecutar la primera operación en el primer subconjunto de los datos de sensor protegidos; y únicamente si se determina que el dispositivo está autorizado a ejecutar la segunda operación, proporcionar una o más claves utilizables por el dispositivo para ejecutar la segunda operación en el segundo subconjunto de datos de sensor protegidos. En otras palabras, la primera y la segunda operación no se pueden ejecutar a menos que los datos de control de acceso indiquen que el dispositivo puede hacerlo.

En un caso más general, los datos de sensor pueden incluir una pluralidad de subconjuntos de datos de sensor. La etapa de cifrar los datos de sensor puede incluir a continuación proteger cada uno de la pluralidad de subconjuntos de datos de sensor con una clave respectiva para generar una pluralidad respectiva de subconjuntos de datos de sensor protegidos. En consecuencia, los datos de control de acceso pueden definir una o más operaciones que el dispositivo está autorizado a ejecutar en un subconjunto respectivo de datos de sensor protegidos. Por ejemplo, se puede definir una operación para cada uno de los subconjuntos de datos, únicamente para uno de ellos o para algunos de ellos. La etapa de determinación puede incluir a continuación la determinación de una o más operaciones que el dispositivo

está autorizado a ejecutar en un subconjunto respectivo de datos de sensor protegidos. Una vez que ha tenido lugar esta determinación, el método puede incluir una etapa de proporcionar, al dispositivo, una o más claves, siendo cada clave utilizable por el dispositivo para ejecutar una operación permitida en un subconjunto respectivo de los datos de sensor protegidos.

En los ejemplos anteriores, únicamente se especifica que el sensor recibe el testigo de autorización. Debe entenderse que la etapa de determinación tiene lugar en respuesta a la recepción del testigo de autorización. En los casos anteriores, debe entenderse que, en respuesta a la etapa de determinación, el sensor proporciona, al dispositivo, la clave o claves que son utilizables por el dispositivo para ejecutar todas las operaciones que están permitidas, basándose en los datos de control de acceso. Sin embargo, en algunos casos, el dispositivo puede no desear ejecutar todas las operaciones posibles. En tales casos, el método puede incluir además una etapa de recibir una solicitud de acceso desde el dispositivo, especificando la solicitud de acceso una o más de: la primera operación a ejecutar en el primer subconjunto de datos de sensor protegidos, y la segunda operación a ejecutar en el segundo subconjunto de datos de sensor protegidos. A continuación, la etapa de determinación puede incluir: determinar si se permite que el dispositivo ejecute la primera operación en el primer subconjunto de datos de sensor protegidos; y/o determinar si se permite que el dispositivo ejecute la segunda operación en el segundo subconjunto de datos de sensor protegidos. A continuación, como ya se ha analizado, las claves pertinentes únicamente se proporcionarán en el caso de que haya tenido lugar una determinación positiva.

Anteriormente, hemos expuesto implementaciones en las que se puede ejecutar más de una operación en los datos de sensor protegidos, dependiendo de los permisos de un dispositivo dado. También hemos expuesto implementaciones en las que un dispositivo puede realizar diferentes operaciones en diferentes subconjuntos de datos de sensor. Cabe señalar que, la invención también abarca implementaciones en las que cada uno de la pluralidad de subconjuntos de datos de sensor protegidos está protegido por una pluralidad de claves secretas, y los datos de control de acceso definen operaciones separadas que pueden ejecutarse para cada subconjunto de datos de sensor protegidos. Una implementación de este tipo se puede obtener combinando las características opcionales establecidas anteriormente y debe considerarse como explícitamente divulgada en esta solicitud.

Cuando el sensor 10 recibe el testigo de autorización 23, puede realizar una etapa de autenticación del testigo de autorización 23. Por ejemplo, cuando se genera, el testigo de autorización 23 puede haber sido firmado usando, por ejemplo, un algoritmo de firma digital de curva elíptica y una clave privada. La clave privada puede estar incorporada en una PKI, por lo que está firmada por una autoridad de certificación (CA) en forma de certificados. La clave pública de la CA raíz puede estar codificada de forma permanente en el sensor 10, por ejemplo, en un elemento seguro del mismo, y, a continuación, puede usarse para autenticar el testigo de autorización 23. Cuando el dispositivo 20 solicita acceso a datos, se puede establecer un canal seguro entre el sensor 10 y el dispositivo 20. En este caso, el sensor 10 y/o el dispositivo 20 pueden realizar un proceso de autenticación mutua, usando, por ejemplo, una clave simétrica previamente compartida o una PKI asimétrica.

En una implementación preferida de la presente invención, el método se usa para proteger los datos de sensor al menos cifrándolos, generando de esta manera datos de sensor cifrados. En tales casos, el método incluye las etapas de generar datos de sensor y cifrar los datos de sensor usando una clave de cifrado, para generar datos de sensor cifrados 24; y transmitir los datos de sensor cifrados 24 a un dispositivo 20 para su almacenamiento; recibir, por el sensor 10: un testigo de autorización 23 que incluye datos de control de acceso que definen una o más operaciones que el dispositivo 20 está autorizado a ejecutar en los datos de sensor cifrados 24; determinar por el sensor 10, basándose en los datos de control de acceso, una operación que el dispositivo 20 está autorizado a ejecutar en los datos de sensor protegidos 24; proporcionar, al dispositivo 20, una o más claves utilizables por el dispositivo 20 para ejecutar la operación permitida en los datos de sensor cifrados 24. A continuación, se exponen características opcionales adicionales de la invención. Debe tenerse en cuenta que las características que se exponen a continuación pueden representar una nueva redacción de los ejemplos descritos anteriormente. Cuando sea compatible, cualquier característica opcional de la invención divulgada en esta solicitud puede combinarse con cualquier otra característica, sin extenderse más allá del alcance pretendido de esta divulgación. En particular, debe tenerse en cuenta que cualquier característica opcional expuesta a continuación relacionada con el cifrado o las claves de cifrado puede aplicarse igualmente para la protección general usando claves secretas o las propias claves secretas mismas y sus complementos.

Un objetivo importante de la presente invención es garantizar que los datos de sensor permanezcan seguros y únicamente puedan ser leídos y/o modificados por partes particulares especificadas. En consecuencia, las operaciones pueden incluir descifrar los datos de sensor cifrados 24 y modificar y volver a autenticar los datos de sensor. En el último caso, se apreciará que los datos de sensor cifrados 24 deben descifrarse en primer lugar antes de que puedan modificarse los datos de sensor correspondientes (es decir, no cifrados).

En primer lugar, consideramos el caso donde los datos de control de acceso definen que al dispositivo 20 se le permite descifrar los datos de sensor cifrados 24. En este caso, el método puede incluir proporcionar, al dispositivo 20, una clave de descifrado que es utilizable por el dispositivo 20 para descifrar los datos de sensor cifrados. En otras palabras, debido a que los datos de control de acceso definen que el dispositivo está autorizado a descifrar los datos de sensor cifrados 24, se determinará (basándose en ello) que el dispositivo está autorizado a descifrar los datos de sensor

cifrados 24. En algunos casos, la clave de cifrado puede ser una clave simétrica, en cuyo caso la clave de descifrado puede ser la misma que la clave de cifrado que se usó para cifrar los datos de sensor en primer lugar.

En otros casos, se puede permitir que el dispositivo 20 vaya una etapa adicional y modifique los datos de sensor. Se observará que cualquier parte que posea la clave de descifrado podrá descifrar y modificar los datos. Sin embargo, es de vital importancia que las modificaciones no autorizadas de los datos sean identificables para poder ignorarlas. Para garantizar que este sea el caso, la etapa de cifrado puede incluir aplicar una primera clave de autenticación a los datos antes de usar la clave de cifrado. De esta manera, si una parte no autorizada modificara los datos de sensor y, a continuación, los volviera a cifrar, sin la primera clave de autenticación, no podría autenticar los datos y sería fácil detectar que se ha tenido lugar una manipulación no autorizada. Consideremos ahora el caso donde un dispositivo 20 está autorizado a modificar los datos. Si los datos de control de acceso permiten que el dispositivo 20 modifique los datos de sensor, el método puede incluir: proporcionar al dispositivo 20 una clave de descifrado que es utilizable para descifrar los datos de sensor cifrados, emitiendo de esta manera los datos de sensor; y proporcionar al dispositivo 20 la primera clave de autenticación, utilizable por el dispositivo 20 para volver a autenticar los datos de sensor modificados. Por lo tanto, el dispositivo 20 puede configurarse para descifrar los datos, modificarlos y volver a aplicar la clave de autenticación para autenticar los datos de sensor modificados. A continuación, el dispositivo 20 puede volver a cifrar los datos.

En algunos otros casos, las operaciones pueden incluir únicamente la autenticación de los datos de sensor cifrados. En otras palabras, en algunos casos, el dispositivo 20 puede desear confirmar que los datos de sensor cifrados 24 no han sido modificados entre su generación y transmisión y almacenamiento en el dispositivo. Para lograr esto, la etapa de cifrado puede incluir aplicar una segunda clave de autenticación después de los datos de sensor cifrados 24. A continuación, la etapa de proporcionar puede incluir proporcionar, al dispositivo 20, la segunda clave de autenticación, utilizable por el dispositivo 20 para autenticar los datos de sensor cifrados. Se debe tener en cuenta que, en los casos en los que se permite al dispositivo 20 descifrar y/o modificar los datos de sensor, como se ha descrito anteriormente, la segunda clave de autenticación también puede proporcionarse al dispositivo 20.

Cabe señalar que, en el contexto de la presente solicitud, una clave de autenticación es una clave que puede aplicarse a algunos datos (cifrados o no cifrados) que emiten un código de autenticación de mensaje (MAC). A continuación, el MAC puede etiquetarse con los datos originales (es decir, el "mensaje"). Específicamente, aplicar una clave de autenticación a los datos puede comprender aplicar un algoritmo basado en clave a los datos, que es un algoritmo cuya salida depende de los datos de entrada y de la clave. En otras palabras, el mismo resultado únicamente se obtiene si tanto los datos de entrada como la clave son iguales. Una clave diferente producirá un resultado diferente. En ejemplos preferidos, aplicar una clave de autenticación a los datos de sensor (o datos de sensor cifrados) puede comprender usar un algoritmo de función de troceo con clave o un esquema de HMAC que implica una clave de autenticación, en los datos de sensor (o datos de sensor cifrados) para generar un HMAC. También se prevén otros esquemas de autenticación con clave.

Debe tenerse en cuenta que, cualquier acción descrita a lo largo de toda esta solicitud con respecto a la clave de cifrado también puede realizarse con respecto a la primera y/o segunda claves de autenticación (particularmente aquellas acciones relacionadas con la generación y/o recuperación de aquellas claves).

En algunos casos, se pueden permitir diferentes operaciones para diferentes subconjuntos de los datos de sensor. Por ejemplo, un sensor 10 puede obtener dos tipos diferentes de datos, y a un dispositivo dado 20 se le puede permitir leer únicamente un tipo de datos, pero modificar el otro tipo. Como alternativa, al dispositivo 20 únicamente se le puede permitir ver datos que se registraron dentro de un marco de tiempo específico. Algunas implementaciones de la presente invención permiten aplicar diferentes reglas para diferentes subconjuntos de los datos de sensor. Específicamente, los datos de sensor pueden incluir un primer subconjunto de datos de sensor y un segundo subconjunto de datos de sensor. Por supuesto, los datos de sensor pueden dividirse en una pluralidad general de subconjuntos de datos de sensor. En el presente documento, la división en un primer subconjunto y un segundo subconjunto es para propósitos ilustrativos. El caso general se describirá más adelante.

Existen numerosas maneras en las que los datos de sensor pueden dividirse en subconjuntos. Por ejemplo, el método puede incluir generar y anexar una cabecera a cada pieza de datos de sensor generado, incluyendo la cabecera metadatos que contienen información acerca de esa pieza de datos de sensor, incluyendo los metadatos uno o más de: una indicación de tiempo que indica una hora y/o fecha en la que se recopiló/generó la pieza de datos de sensor; un ID de sensor que identifica el sensor que recopiló los datos; un tipo de datos que indica el tipo de datos; y uno o más ID de dispositivo que identifican los dispositivos 20 que están permitidos a acceder a los datos. En tales casos, el subconjunto al que pertenece cada pieza respectiva de datos de sensor se basa en los metadatos de la cabecera de esa pieza de datos de sensor.

La etapa de cifrado puede incluir el cifrado del primer subconjunto de datos de sensor con una primera clave de cifrado para generar un primer subconjunto de datos de sensor cifrados 24; y cifrar el segundo subconjunto de datos de sensor con una segunda clave de cifrado, diferente de la primera clave de cifrado, para generar un segundo subconjunto de datos de sensor cifrados 24. En tales casos, los datos de control de acceso pueden definir: una primera operación que el dispositivo está 20 permitido a ejecutar en el primer subconjunto de datos de sensor cifrados 24; y/o una segunda

operación que el dispositivo 20 está autorizado a ejecutar en el segundo subconjunto de datos de sensor cifrados 24. En consecuencia, la etapa de determinación puede incluir determinar, basándose en los datos de control de acceso: una primera operación que el dispositivo 20 está autorizado a ejecutar en el primer subconjunto de datos de sensor cifrados 24; y/o una segunda operación que el dispositivo 20 está autorizado a ejecutar en el segundo subconjunto de datos de sensor cifrados 24. Es posible que no se permita que el dispositivo 20 ejecute una operación tanto en el primer subconjunto como en el segundo subconjunto. En consecuencia, la etapa de proporcionar puede incluir: únicamente si se determina que el dispositivo 20 está autorizado para ejecutar la primera operación, proporcionar una o más claves utilizables por el dispositivo 20 para ejecutar la primera operación en el primer subconjunto de los datos de sensor cifrados 24; y únicamente si se determina que el dispositivo 20 está autorizado a ejecutar la segunda operación, proporcionar una o más claves utilizables por el dispositivo 20 para ejecutar la segunda operación en el segundo subconjunto de datos de sensor cifrados 24. En otras palabras, la primera y la segunda operación no se pueden ejecutar a menos que los datos de control de acceso indiquen que el dispositivo 20 puede hacerlo.

En un caso más general, los datos de sensor pueden incluir una pluralidad de subconjuntos de datos de sensor. La etapa de cifrar los datos de sensor 24 puede incluir a continuación cifrar cada uno de la pluralidad de subconjuntos de datos de sensor con una clave respectiva para generar una pluralidad respectiva de subconjuntos de datos de sensor cifrados 24. En consecuencia, los datos de control de acceso pueden definir una o más operaciones que el dispositivo 20 está autorizado a ejecutar en un subconjunto respectivo de datos de sensor cifrados 24. Por ejemplo, se puede definir una operación para cada uno de los subconjuntos de datos, únicamente para uno de ellos o para algunos de ellos. La etapa de determinación puede incluir a continuación la determinación de una o más operaciones que el dispositivo 20 está autorizado a ejecutar en un subconjunto respectivo de datos de sensor cifrados 24. Una vez que ha tenido lugar esta determinación, el método puede incluir una etapa de proporcionar, al dispositivo 20, una o más claves, siendo cada clave utilizable por el dispositivo 20 para ejecutar una operación permitida en un subconjunto respectivo de los datos de sensor cifrados 24.

En los ejemplos anteriores, únicamente se especifica que el sensor 10 recibe el testigo de autorización 23. Debe entenderse que la etapa de determinación tiene lugar en respuesta a la recepción del testigo de autorización 23. En los casos anteriores, debe entenderse que, en respuesta a la etapa de determinación, el sensor 10 proporciona, al dispositivo 20, la clave o claves que son utilizables por el dispositivo 20 para ejecutar todas las operaciones que están permitidas, basándose en los datos de control de acceso. Sin embargo, en algunos casos, el dispositivo 20 puede no desear ejecutar todas las operaciones posibles. En tales casos, el método puede incluir además una etapa de recibir una solicitud de acceso desde el dispositivo 20, especificando la solicitud de acceso una o más de: la primera operación a ejecutar en el primer subconjunto de datos de sensor cifrados 24, y la segunda operación a ejecutar en el segundo subconjunto de datos de sensor cifrados 24. A continuación, la etapa de determinación puede incluir: determinar si se permite que el dispositivo 20 ejecute la primera operación en el primer subconjunto de datos de sensor cifrados 24; y/o determinar si se permite que el dispositivo 20 ejecute la segunda operación en el segundo subconjunto de datos de sensor cifrados 24. A continuación, como ya se ha analizado, las claves pertinentes únicamente se proporcionarán en el caso de que haya tenido lugar una determinación positiva.

Como antes, esto puede generalizarse al caso donde hay una pluralidad de subconjuntos de datos de sensor. En este caso, la solicitud de acceso puede especificar una o más operaciones a ejecutar en un subconjunto respectivo de datos de sensor, y la etapa de determinación incluye determinar si al dispositivo 20 se le permite ejecutar cada operación especificada en el subconjunto especificado respectivo de datos de sensor cifrados 24.

Las características opcionales presentadas anteriormente se refieren principalmente al primer aspecto de la invención, en concreto, el método ejecutado por el sensor 10. Sin embargo, se apreciará que, cuando sean compatibles, estas características se aplicarán igualmente bien al segundo aspecto de la invención, es decir, el método ejecutado por el dispositivo 20. A continuación, se exponen, en términos generales, algunas características opcionales adicionales que pueden aplicarse al segundo aspecto de la invención. El segundo aspecto de la invención proporciona un método para acceder a datos de sensor protegidos mediante un dispositivo 20, teniendo almacenado el dispositivo 20 en el mismo un testigo de autorización 23 que incluye datos de control de acceso que definen una o más operaciones que el dispositivo 20 está autorizado a ejecutar en datos de sensor cifrados 24, incluyendo el método las etapas de: recibir datos de sensor cifrados 24 desde un sensor, estando los datos de sensor cifrados, cifrados usando una clave de cifrado; almacenar los datos de sensor recibidos; enviar el testigo de autorización 23 al sensor; y recibir una clave utilizable por el dispositivo 20 para ejecutar una operación permitida en los datos de sensor cifrados 24. Como se analizó anteriormente, las operaciones pueden incluir descifrar los datos de sensor cifrados 24; y modificar y volver a autenticar los datos de sensor.

Cuando la invención se define en términos amplios, como anteriormente, el dispositivo 20 envía únicamente el testigo de autorización 23 al sensor 10. En estos casos, el dispositivo 20 puede recibir claves son utilizables para ejecutar todas las operaciones permitidas por los datos de control de acceso del testigo de autorización 23. Sin embargo, en algunos casos donde esto no es deseable, el dispositivo 20 puede enviar una solicitud de acceso al sensor 10, especificando la solicitud de acceso una operación solicitada a ejecutarse en los datos de sensor cifrados 24.

Como explicamos anteriormente con referencia al primer aspecto de la invención, los datos de sensor pueden incluir un primer subconjunto y un segundo subconjunto, y se puede permitir que el dispositivo 20 ejecute diferentes

operaciones en los diferentes subconjuntos. Como antes, los datos de sensor cifrados 24 pueden incluir un primer subconjunto de datos de sensor cifrados 24 y un segundo subconjunto de datos de sensor cifrados 24. A continuación, los datos de control de acceso pueden definir una primera operación que el dispositivo puede ejecutar en el primer subconjunto de datos de sensor cifrados 24, y/o una segunda operación que el dispositivo está autorizado a ejecutar en el segundo subconjunto de datos de sensor cifrados 24. En tales casos, como resultado de la etapa de determinación que tiene lugar en el sensor 10, la etapa de recepción puede incluir: únicamente si está definido en los datos de control de acceso que el dispositivo está autorizado a ejecutar la primera operación, recibir una o más claves utilizables por el dispositivo 20 para ejecutar la primera operación en el primer subconjunto de los datos de sensor cifrados 24; y únicamente si está definido en los datos de control de acceso que el dispositivo 20 está autorizado a ejecutar la segunda operación, recibir una o más claves utilizables por el dispositivo 20 para ejecutar la segunda operación en el segundo subconjunto de datos de sensor cifrados 24. Por supuesto, los datos de sensor pueden incluir más que únicamente el primer y el segundo subconjunto. Las características opcionales descritas en este párrafo pueden generalizarse a una pluralidad general de subconjuntos de datos de sensor. Específicamente, el dispositivo 20 puede recibir una pluralidad de subconjuntos de datos de sensor cifrados 24, y los datos de control de acceso pueden definir una o más operaciones que el dispositivo 20 está autorizado a ejecutar en un subconjunto respectivo de datos de sensor cifrados 24. Por ejemplo, se puede definir una operación para cada uno de los subconjuntos de datos, únicamente para uno de ellos o para algunos de ellos. A continuación, el método incluye una etapa de recibir desde el sensor 10, una o más claves, cada clave utilizable por el dispositivo 20 para ejecutar una operación permitida en un subconjunto respectivo de los datos de sensor cifrados 24.

En casos donde el dispositivo 20 envía una solicitud de acceso, la solicitud de acceso puede especificar una o más de: la primera operación a ejecutar en el primer subconjunto de datos de sensor cifrados 24, y la segunda operación a ejecutar en el segundo subconjunto de datos de sensor cifrados 24.

Para seguridad añadida, el sensor 10 puede cifrar la clave o claves antes de proporcionarlas al dispositivo. En implementaciones preferidas, el sensor 10 puede estar precargado con una clave pública, y el dispositivo 20 puede estar precargado con una clave privada, y el método puede incluir una etapa de cifrado de la clave o claves usando la clave pública. Debido a que únicamente el dispositivo 20 al que se envían la clave o las claves tiene la clave privada que puede descifrar las claves cifradas, se impide que otras partes externas accedan a la clave o claves y, en consecuencia, a los datos de sensor. El método del segundo aspecto de la invención puede incluir una etapa correspondiente de descifrado de la clave o claves, preferentemente usando una clave privada.

El método del segundo aspecto de la invención puede incluir además una etapa de usar la clave o claves recibidas desde el sensor para ejecutar las operaciones permitidas, por ejemplo, la primera operación y/o la segunda operación.

Las Figuras 2 y 3 presentan un ejemplo específico del método del primer y segundo aspecto de la invención, en forma de una serie de etapas S1 a S12 que pueden realizarse por el sistema 1 de la Figura 1. En casos preferidos, las etapas S1 a S12 se realizan en ese orden, aunque el experto apreciará que puede ser posible variar el orden de algunas de las etapas. La Figura 2 muestra las etapas que realiza el sensor 10, y la Figura 3 muestra las etapas que realiza el dispositivo 20.

En la etapa S1, el sensor 10 genera datos de sensor. En este punto, conviene especificar algunos de los usos previstos de la presente invención. Por ejemplo, el dispositivo 20 puede ser una puerta de enlace perimetral o una unidad de control que gestiona varios sensores, para lo cual necesita accesos diferentes y específicos. Un ejemplo puede ser una unidad de control de seguimiento conectada a un contenedor que usa datos de acelerómetro generados para guiar operaciones específicas (por ejemplo, detección de aterrizaje de avión) y que también almacena datos cifrados generados por sensores de temperatura o sensores de estado de la puerta a informar en una nube para garantizar la calidad del transporte y la no manipulación. La integridad y privacidad de los datos de seguimiento de la temperatura y el estado de la puerta están protegidas de extremo a extremo entre el sensor y el sistema. En otro ejemplo: un vehículo (tal como un coche, un barco, un tren, etc.) con varios sensores todos conectados a una red local en la que hay diferentes unidades de control que necesitan un acceso diferente y específico a los datos generados por los sensores. Un sensor puede proporcionar diferentes tipos de datos a diferentes unidades de control, todas gestionadas y autorizadas por un sistema configurado en producción, en fase de mantenimiento o en campo bajo solicitud cuando se conecta.

Una vez que se han generado los datos de sensor por el sensor 10, en la etapa S2, los datos de sensor se cifran por el módulo de cifrado 12 del procesador 11. A continuación, en la etapa S3, el transmisor 14 envía los datos de sensor cifrados 24 al dispositivo 20, que se reciben por el receptor 21 del dispositivo 20 en la etapa S4 de la Figura 3. En casos preferidos, el método incluye además una etapa de borrado de los datos de sensor después de transmitirlos al dispositivo 20 para su almacenamiento en la memoria 22. Como alternativa, el sensor 10 puede estar configurado para borrar los datos de sensor después de transmitirlos al dispositivo 20 en almacenamiento en la memoria 22.

A continuación, en la etapa S5, los datos de sensor cifrados 24 se almacenan en la memoria 22 del dispositivo 20. En este punto, cuando un usuario del dispositivo 20 desea acceder a algunos o todos los datos de sensor cifrados 24, en la etapa S6, el procesador 25 del dispositivo 20 puede generar una solicitud de acceso, que puede especificar, opcionalmente, un subconjunto de los datos de sensor cifrados 24 a los que el usuario del dispositivo 20 desea

acceder. La solicitud de acceso es una solicitud del dispositivo 20 para ejecutar algún tipo de operación en los datos de sensor cifrados, y se analizará en detalle más adelante en esta solicitud. En la etapa S7, el transmisor 26 del dispositivo 20 transmite la solicitud al sensor 10, junto con el testigo de autorización 23, o una copia del mismo. Cabe señalar que, en algunos casos, el transmisor 26 puede transmitir únicamente el testigo de autorización 23. En tales casos, el sensor 10 puede enviar al dispositivo 10 las claves que permiten ejecutar todas las acciones permitidas.

El testigo de autorización 23 incluye datos de control de acceso que definen datos de sensor 24 a los que el dispositivo 20 está autorizado a acceder. Por ejemplo, los datos de control de acceso pueden definir uno o más subconjuntos de los datos de sensor 24 que el dispositivo 20 está autorizado a acceder. Además, los datos de control de acceso pueden definir operaciones que el dispositivo 20 puede ejecutar en los datos de sensor cifrados.

Las características del testigo de autorización 23 se describirán con más detalle más adelante en esta solicitud. Volviendo a la Figura 2, en la etapa S8, el receptor 15 del sensor 10 recibe la solicitud de acceso y el testigo de autorización 23 del transmisor 26 del dispositivo 20. A continuación, en la etapa S9, el módulo de determinación de acceso 13 del procesador 11 del sensor 10 determina, basándose en los datos de control de acceso en el testigo de autorización 23, si al dispositivo 20 se le permite acceder a los datos de sensor cifrados 24. En algunos casos, el módulo de determinación de acceso 13 determina a qué datos de sensor cifrados 24 está autorizado a acceder el dispositivo 20, o qué operaciones está autorizado a ejecutar el dispositivo 20. Este proceso de determinación de acceso es central para la invención y se describirá con más detalle más adelante. En la etapa S10, el sensor 10, específicamente el transmisor 14 del mismo, envía una o más claves de acceso al dispositivo 10, siendo la clave o claves utilizables para ejecutar las operaciones permitidas. Volviendo finalmente a la Figura 3, el receptor 21 del dispositivo 20 recibe la clave de acceso en la etapa S11, y el procesador 25 del dispositivo 20 usa la clave o claves de acceso para ejecutar la operación permitida en los datos de sensor cifrados 24.

La Figura 4 muestra un ejemplo alternativo de un módulo de sensor 100 que puede formar parte de un sistema de la presente invención o puede realizar un método de la presente invención (por ejemplo, las etapas S1, S2, S3, S8, S9 y S10 como se muestra en la Figura 2). La estructura fundamental del módulo de sensor 100 de la Figura 4 es similar a la estructura del sensor 10 de la Figura 1, pero muestra numerosas características opcionales.

Aunque las características opcionales de la Figura 4 se muestran en un único dibujo, se debe enfatizar que, por su propia naturaleza como características opcionales, no es necesario que todas estas características estén presentes en combinación exactamente como se muestra en la Figura 4. Se muestran en un único sensor 100 para propósitos ilustrativos, y, debe entenderse que, cualquiera, algunas o todas las características mostradas en el sensor alternativo 100 de la Figura 4 pueden excluirse del ejemplo sin que la disposición resultante quede fuera del alcance de esta divulgación.

Como con la Figura 1, describiremos en primer lugar la estructura del sensor 100 y, a continuación, explicaremos la función de los diversos módulos opcionales. El sensor 100 incluye un entorno seguro de sensor (SSE) 101, que puede definirse como un subsistema del sensor 100 que implementa el almacenamiento y uso controlados de los datos de sensor. Uno de los propósitos de los entornos seguros tales como SSE 101 es proteger datos seguros/confidenciales en caso de pérdida de datos. El SSE 101 puede usar medios criptográficos, tales como función de troceo, como una manera de proteger la información. En la Figura 4, el SSE 101 incluye el procesador 102, la memoria 104, un módulo de recopilación de datos 103 y un módulo de interfaz de dispositivo 106. Es preferible que el procesador 102 y la memoria 104 estén ubicados dentro del SSE 101, sin embargo, el módulo de interfaz de dispositivo 106 puede estar ubicado dentro del sensor 100 pero fuera del SSE 101. El módulo de interfaz de dispositivo 106 actúa como una interfaz entre señales externas y dispositivos (por ejemplo, el dispositivo 20 o el dispositivo 200) y el sensor 100. El módulo de interfaz de dispositivo 106 en la Figura 4 incluye el transmisor 124 y el receptor 126. Como alternativa, en otros casos, el módulo de interfaz de dispositivo 106 puede actuar como una interfaz únicamente y estar configurado para transportar señales a un transmisor 124 y para recibir señales de un receptor 126; tales ejemplos aún caen dentro del alcance de la invención.

El procesador 102 de la Figura 4 puede incluir uno o más de: un módulo de cifrado 108, un módulo de determinación de acceso 110 y un módulo de autorización 112. Análogamente, la memoria 104 puede incluir una memoria persistente 114 y un búfer 116. El búfer puede tener una capacidad de 100 KB a 10 MB. En el presente documento, la expresión "memoria persistente" debe entenderse que hace referencia a memoria a largo plazo o memoria permanente. Únicamente los datos que requieren almacenamiento a largo plazo deben almacenarse en la memoria persistente 114, tales como los metadatos 118 y los datos de clave de cifrado 120 en el presente ejemplo. La naturaleza de estos datos se describirá con más detalle más adelante. El búfer 116 es una memoria a corto plazo y puede usarse para almacenar datos de sensor 122 después de que se hayan generado y antes de que se hayan transmitido, por ejemplo, por el transmisor 124 al dispositivo (por ejemplo, 20 o 200).

A continuación. se describirá con más detalle la función de los componentes mostrados en la Figura 4, en el contexto del método de alto nivel de las Figuras 2 y 3, estableciendo cualquier característica opcional adicional.

El módulo de recopilación de datos 103 es el módulo del sensor 100 que realiza la detección en sí y, como tal, puede incluir un elemento de detección 105 que está configurado para percibir, detectar y/o medir algún parámetro externo.

El elemento de sensor 105 puede incluir uno o más de los siguientes: un sensor de temperatura, un sensor de luz, un sensor de sonido, un sensor de humedad, un sensor de CO_2, un sensor de humo, un sensor de presión, un sensor de humedad, un detector de proximidad o una cámara. También puede incluir un dispositivo o dispositivos configurados para medir uno o más de los siguientes: tensión, corriente, resistencia, intensidad de campo magnético, densidad de flujo magnético, capacitancia, inductancia, frecuencia y longitud de onda. El elemento de sensor 105 también puede incluir un acelerómetro. Se apreciará que, el elemento de detección 105 puede incluir un dispositivo que está configurado para percibir, detectar o medir cualquier forma de estímulo físico o ambiental externo. Además de detectar un estímulo físico o ambiental, el elemento de detección 105 puede implementarse en forma de un módulo de software, que está configurado para detectar la ocurrencia de un proceso predeterminado en un dispositivo informático (tal como un ordenador, una tableta o un teléfono inteligente). Por ejemplo, el elemento de detección 105 puede estar configurado para detectar una operación de procesamiento de datos predeterminada, o para detectar un resultado particular de una operación de procesamiento de datos. El elemento de detección 105 puede incluir un contador configurado para contar el número de veces que tiene lugar un evento particular. El módulo de recopilación de datos 103 puede incluir opcionalmente su propio procesador, configurado para convertir los datos sin procesar recopilados por el dispositivo de detección 105 en un formato que puede procesarse por el procesador 102. Como alternativa, los datos sin procesar pueden enviarse directamente al procesador 102, tras lo cual, se convierten a un formato más adecuado. Debe apreciarse que, el sensor 100 puede incluir más de un módulo de recopilación de datos 103. Cada módulo de recopilación de datos 103 puede incluir también uno o más elementos de detección 105, del tipo descrito en este párrafo.

En la etapa S2 de la Figura 2, se cifran los datos de sensor. Antes de analizar el proceso de cifrado, es útil describir con más detalle la posible naturaleza de los datos de sensor que se obtienen y los procesos opcionales que se pueden llevar a cabo antes de que se cifren.

Cuando se recopila en primer lugar una pieza de datos de sensor, el procesador 102 puede estar configurado para generar una cabecera y anexar esa cabecera a la pieza de datos. Entre la recopilación de datos y la anexión de la cabecera, la pieza de datos de sensor puede almacenarse en el búfer 116 de la memoria 104 del sensor 100 para su procesamiento. El búfer 116 es adecuado para este almacenamiento, ya que es únicamente almacenamiento a corto plazo. La cabecera contiene preferentemente metadatos que contienen información acerca de esa pieza de datos de sensor, incluyendo preferiblemente los metadatos uno o más de: una indicación de tiempo que indica una hora y/o fecha en la que se recopilaron los datos, un ID de sensor que indica la identidad del sensor 100 o elemento de detección 105 que recopiló los datos, un tipo de datos que indica el tipo de datos (por ejemplo, el parámetro físico al que pertenecen los datos o el tipo de actividad detectada), material de valor único (nonce) y datos de generación de claves que pueden usarse para generar las claves requeridas, información de sensor, tal como referencias de hardware y firmware (por ejemplo, ID y versión). Estos se denominan "tipos de metadatos". Los datos de sensor pueden dividirse en una pluralidad de subconjuntos. Estos pueden ser subconjuntos exclusivos, es decir, cada pieza de datos de sensor pertenece a un único subconjunto. Como alternativa, cada pieza de datos de sensor puede pertenecer a uno o más subconjuntos. Un subconjunto puede incluir únicamente una única pieza de datos de sensor.

Los datos de sensor pueden subdividirse en subconjuntos basándose en un primer tipo de metadatos. En otras palabras, los datos de sensor pueden dividirse en una pluralidad de subconjuntos, registrándose cada subconjunto dentro de un marco de tiempo diferente, o siendo cada uno un tipo de datos diferente, o registrándose cada uno por un sensor diferente. Los datos de sensor pueden dividirse además en una pluralidad de subconjuntos basándose en un segundo tipo de metadatos.

En el presente documento, el término "dividido" no significa necesariamente que los datos de sensor estén particionados o que los diferentes subconjuntos se almacenen por separado unos de otros, aunque este puede ser el caso opcionalmente. Preferentemente, sin embargo, la pluralidad de subconjuntos se puede asignar basándose en los metadatos, pero (al menos en este punto) no están separados entre sí. En este punto, hemos establecido una pluralidad de subconjuntos de datos, incluyendo cada pieza de datos opcionalmente una cabecera que contiene metadatos que proporcionan información acerca de esos datos, y basándose los subconjuntos en los metadatos. En este punto, las piezas de datos con las cabeceras adjuntas se pueden almacenar temporalmente en el búfer 116 de la memoria 104 del sensor 100.

A continuación, el módulo de cifrado 108 del procesador 102 está configurado para cifrar los datos de sensor, para generar datos de sensor cifrados. El módulo de cifrado 108 puede configurarse para cifrar tanto los datos de sensor como de la cabecera, pero preferentemente cifra únicamente los datos de sensor. Específicamente, el módulo de cifrado 108 está configurado para cifrar cada uno de la pluralidad de subconjuntos de datos con una clave de cifrado respectiva diferente.

En el caso en que cada pieza de datos de sensor pertenezca a un único subconjunto de la pluralidad de subconjuntos, esto es sencillo.

Sin embargo, en el caso de que una pieza de datos pueda pertenecer o asignarse a más de un subconjunto (por ejemplo, un subconjunto establecido basándose en el tiempo en el que se registraron los datos y un subconjunto basándose en el elemento de detección 105 que registró los datos), la situación es más compleja y puede abordarse

de cualquiera de las siguientes maneras:

(i) El módulo de cifrado 108 puede configurarse para cifrar cada pieza de datos de sensor con una clave respectiva diferente, para generar un único conjunto de datos de sensor cifrados, correspondiendo cada pieza de datos de sensor cifrados a una pieza respectiva de datos de sensor (en bruto, no cifrados). A continuación, el procesador 102 (opcionalmente el módulo de cifrado 108 del mismo) puede anexar una cabecera a cada pieza de datos de sensor cifrados, incluyendo la cabecera metadatos que identifican el subconjunto o subconjuntos de datos a los que pertenece esa pieza de datos de sensor cifrados (o, más específicamente, el subconjunto o subconjuntos a los que pertenecen los datos de sensor no cifrados correspondientes). Esto se ilustra en la Figura 6, en la que se usan las claves K_1 a K_4 para cifrar, respectivamente, las piezas A a D de datos de sensor. En el presente documento, se genera una pieza de datos de sensor por cifrado y se identifican dos subconjuntos en cada cabecera.

(ii) El módulo de cifrado 108 puede configurarse para cifrar cada pieza de datos en cada subconjunto respectivo con la misma clave de cifrado, para generar una pluralidad de piezas de datos cifrados correspondientes a un subconjunto de los datos de sensor sin procesar, no cifrados. El módulo de cifrado 108 puede configurarse para hacer esto para todos los subconjuntos de datos (teniendo en cuenta que estos subconjuntos pueden superponerse). En el caso de que la pluralidad de subconjuntos de datos de sensor se superpongan (es decir, en donde cada pieza de datos de sensor pertenece a más de un subconjunto), para una pieza dada de datos de sensor no cifrados, se puede generar de esta manera una pluralidad de piezas de datos de sensor cifrados, cifrándose cada pieza de datos de sensor cifrados con una clave de cifrado respectiva diferente, cada clave de cifrado asociada con un respectivo subconjunto de los que pertenece esa pieza de datos de sensor no cifrados, o al que está asignada. De nuevo, el procesador 102 (opcionalmente el módulo de cifrado 108 del mismo) puede anexar una cabecera a cada pieza de datos de sensor cifrados, incluyendo la cabecera metadatos que identifican el subconjunto de datos a los que pertenece esa pieza de datos de sensor cifrados (o, más específicamente, el subconjunto o subconjuntos a los que pertenecen los datos de sensor no cifrados correspondientes). Esto se ilustra en la Figura 6, en la que puede observarse que cada pieza de datos de sensor se cifra dos veces: una vez con la clave correspondiente a su "subconjunto de tiempo" y otra vez con la clave correspondiente a su subconjunto de "tipo de datos". K_1 se usa para datos del subconjunto T1, K_2 se usa para datos en el subconjunto de temperatura, K_3 se usa para datos en el subconjunto actual y K_4 Se usa para datos del subconjunto T2. Puede observarse que, de acuerdo con el caso (ii), se genera el doble de datos cifrados.

Ahora analizamos cómo tiene lugar el cifrado. En un caso sencillo, el módulo de cifrado 108 puede configurarse para cifrar una pieza dada de datos de sensor (a través de toda esta solicitud, a menos que se especifique de otra manera, la expresión "datos de sensor" puede entenderse como una referencia a datos de sensor no cifrados) usando una clave de cifrado para generar una pieza correspondiente de datos de sensor cifrados. La clave de cifrado puede ser una clave simétrica o una clave asimétrica. Cada uno de estos tipos de claves tiene ventajas asociadas, dependiendo de las prioridades del sistema. Por ejemplo, las claves simétricas son mucho más sencillas de generar, por lo que, si la clave de cifrado es una clave simétrica, se reducen los requisitos de procesamiento del procesador 102, lo que permite que el sensor 100 sea más sencillo, más pequeño y más económico de fabricar. Por otro lado, una clave asimétrica es más segura, pero requiere una mayor capacidad de procesamiento para generarla y aplicarla.

Para poder identificar y transmitir la clave de acceso apropiada al dispositivo 20 o 200 en respuesta a una solicitud y una determinación de que se permite el acceso, el sensor 100 debe poder almacenar las claves en asociación con los metadatos que identifican los datos de sensor o datos cifrados en la memoria 104. Como alternativa, para reducir los requisitos de memoria de la memoria 104 del sensor 104, el procesador 102 del sensor 100 puede regenerar de manera fiable las claves de acceso basándose en alguna entrada. Ambas de etas posibilidades se describen a continuación.

El método del primer caso se ilustra en la Figura 7, que ilustra el proceso que se realiza en una única pieza de datos de sensor. En la etapa S108A, la pieza de datos de sensor se recibe en el módulo de cifrado 108, incluyendo la pieza de datos de sensor metadatos, identificando los metadatos un subconjunto al que pertenece esa pieza de datos de sensor. A continuación, en la etapa S108B, el módulo de cifrado 108 (o, como alternativa, el procesador 102) está configurado para realizar una búsqueda en la tabla de datos de clave de cifrado 120 para determinar si existe una clave de cifrado correspondiente al subconjunto. Opcionalmente, antes de realizar esta etapa, el módulo de cifrado 108 o el procesador 102 pueden eliminar la cabecera de a pieza de datos de sensor y extraer los metadatos que contienen o indican el ID de subconjunto de la pieza de datos de sensor (no mostrado). En el caso de que exista una clave de cifrado, en la etapa S108C, la clave se recupera de la tabla de datos de clave de cifrado 120 y se usa para cifrar la pieza de datos de sensor en la etapa S108E. En el caso de que se determine que no existe ninguna clave correspondiente al subconjunto, se genera una nueva clave en la etapa S108D, por ejemplo, mediante el módulo de generación de claves 109, y se almacena en la tabla de datos de clave de cifrado 120, antes de que se use esa clave para cifrar la pieza de datos de sensor en la etapa S108E. El método puede detenerse en este punto, pero, como alternativa, puede continuar a la etapa S108F en la que se determina si la pieza de datos de sensor pertenece a algún subconjunto adicional. En caso contrario, el procesamiento de esa pieza de datos se completa y el método puede opcionalmente volver a la etapa S108A, recibiendo una pieza de datos de sensor adicional. De lo contrario, si se determina que la pieza de datos de sensor pertenece a otro subconjunto de datos de sensor, a continuación, el método

vuelve a la etapa S108B. Usando este método, a medida que se reciben más datos de sensor, crece la tabla de datos de clave de cifrado 120. En las Figuras 8A a 8B se muestran dos ejemplos de distribuciones de ejemplo de las tablas de datos de clave de cifrado. En la Figura 8A, las claves de cifrado se almacenan en asociación con los ID de subconjunto que indican un subconjunto particular, mientras que en la Figura 8B, las claves de cifrado se almacenan en asociación con una pieza particular de metadatos correspondiente a un subconjunto y un ID de subconjunto. En un caso ligeramente diferente, es posible que el ID de subconjunto no esté incluido en la tabla de datos de clave de cifrado 120.

Se debe observar que, cuando el módulo de cifrado 108 usa claves asimétricas para cifrar la pieza de datos de sensor, en la etapa S108D, se deben generar tanto la clave de cifrado como la clave de descifrado complementaria, y, a continuación, ambas se almacenan en la tabla de datos de clave de cifrado 120. Como alternativa, una vez que se haya generado y usado la clave de cifrado, se puede borrar y almacenar únicamente la clave de descifrado.

En los ejemplos dados anteriormente, se genera una tabla de datos de clave de cifrado 120 y se hace crecer con la recepción de cada vez más datos de sensor. En algunos casos, por ejemplo, cuando la capacidad de la memoria 104 es limitada, esto puede ser indeseable. Por lo tanto, en un ejemplo alternativo, el módulo de generación de claves 109 puede estar configurado para generar una clave de cifrado que se basa en uno o más de los metadatos o ID de subconjunto y datos de generación de clave local 118, que son únicos para del sensor 100 y secretos. De esta manera, una vez que se ha generado la clave de cifrado, no es necesario almacenarla en la memoria del sensor 100, ni en cualquier otro sitio, debido a que la misma puede regenerarse de forma fiable basándose en los metadatos relacionados con los datos de sensor que protege. Todo lo que necesita almacenarse en la memoria son los datos de generación de clave local 118. La Figura 9 muestra un ejemplo de este método. En la etapa S109A, se recibe una pieza de datos de sensor en el módulo de cifrado. A continuación, en la etapa S109B, el módulo de generación de claves 109 puede generar una clave de cifrado basándose en los metadatos en la cabecera de la pieza de datos de sensor y los datos de generación de clave local 118. Es importante que los datos de generación de clave local 118 se usen y permanezcan secretos, de lo contrario sería posible que cualquier otro actor vuelva a generar la clave con únicamente el conocimiento de los metadatos, lo que presenta un riesgo de seguridad claro y no insignificante. En la etapa S109C, la clave de cifrado generada se usa para cifrar la pieza de datos de sensor. A continuación, la clave de cifrado generada se puede borrar en la etapa S109D. Como alternativa, la clave de cifrado generada se puede almacenar en el búfer 116 en la tabla de datos de clave temporal 123. De esta manera, cuando se encuentra otra pieza de datos de sensor del mismo subconjunto, el módulo de cifrado 108 puede realizar una búsqueda en la tabla de datos de clave temporal 123, para determinar si ya se ha generado una clave de cifrado correspondiente a ese subconjunto, en cuyo caso, esa clave de cifrado se recupera de la tabla de datos de clave temporal 123, y se usa para cifrar la pieza de datos de sensor posterior. Esto puede ser especialmente útil en escenarios en los que los subconjuntos se basan en el tiempo en el que se recopilan los datos, de modo que se puede usar la misma clave de cifrado para cifrar una serie de datos de sensor, todos los cuales se recopilaron dentro de un intervalo de tiempo predeterminado. En consecuencia, las claves de cifrado generadas que se almacenan en la tabla de datos de claves temporales 123 pueden tener una vida útil o un tiempo de expiración asociado, después del cual se eliminan de la tabla 123. Después de que la pieza de datos de sensor se ha cifrado en la etapa S109C y se ha borrado en la etapa S109D, el método vuelve a la etapa S109A, con la llegada de una nueva pieza de datos de sensor. En los casos donde se generan claves asimétricas, en la etapa S109B, tanto la clave de cifrado como la clave de descifrado complementaria se generan por el módulo de generación de claves 109. A continuación, la clave de cifrado (preferentemente una clave privada) se usa para cifrar la pieza de datos de sensor en la etapa S109C. La clave de descifrado es preferentemente una clave pública.

El cifrado de los datos usando las claves de cifrado generadas o recuperadas garantiza que los datos queden, de manera efectiva, aleatorizados hasta quedar irreconocibles, para garantizar su confidencialidad, es decir, garantizar que un usuario que intercepte su transmisión no pueda derivar ningún significado de ellos. Además de cifrar los datos de sensor, también es importante que el sensor 100 y el dispositivo 20 o 200 puedan garantizar que los datos que han recibido se reciben desde la entidad de la que creen que los han recibido - esto es conocido como "autenticación". Hay un número de esquemas disponibles para este proceso, tales como cifrar y a continuación aplicar MAC, aplicar MAC y a continuación cifrar y cifrar y aplicar MAC. Se prefiere que, en la presente invención, se use el proceso de cifrar y a continuación aplicar MAC. Esto se explicará para una primera pieza de datos de sensor, pero se entenderá que el método se puede aplicar a cada pieza de datos de sensor entrante.

En la Figura 10, se muestra un ejemplo de esto. En primer lugar, en la etapa S108M, la pieza de datos de sensor se puede cifrar como se ha explicado en los párrafos anteriores, para generar una pieza de datos de sensor cifrados. A continuación, en la etapa S108N, el módulo de cifrado 108 puede configurarse para aplicar una clave de autenticación a la pieza de datos de sensor cifrados, para generar un código de autenticación de mensaje (en el presente documento, "MAC"). Es importante destacar que la pieza de datos de sensor cifrados no se borra; el MAC se genera junto con la pieza de datos de sensor cifrados. A continuación, en la etapa S108O, la pieza de datos de sensor cifrados y el MAC se pueden concatenar para generar un mensaje. El destino de un mensaje de este tipo se analizará más adelante. En algunos casos, se puede aplicar una clave de autenticación a los datos de sensor antes de cifrarlos usando la clave de cifrado. Esto se describe en cualquier otro sitio de esta solicitud.

En este punto, en la etapa S3, de la Figura 2, los datos de sensor cifrados se transmiten, por el transmisor 124 al

dispositivo 20 o 200. Específicamente, se podrá transmitir la pieza de datos de sensor cifrados o bien generar el mensaje tal y como se ha explicado en el párrafo anterior. En algunos casos, en lugar de transmitir los datos de sensor cifrados tan pronto como se generan, el módulo de cifrado 108 puede transmitir la pieza de datos de sensor cifrados al búfer 116 para su almacenamiento temporal. A continuación, el transmisor 124 puede enviar todos los datos de sensor cifrados en el búfer 116 cuando supera un volumen umbral predeterminado. Como alternativa, el transmisor 124 puede configurarse para enviar todos los datos de sensor cifrados en el búfer 116 a intervalos de tiempo regulares. Antes de analizar con más detalle las etapas que realiza el dispositivo 20 o 200, es útil considerar con más detalle la estructura del dispositivo.

En consecuencia, de forma muy similar a la Figura 4, la figura 5 muestra un ejemplo alternativo de un dispositivo 200 que puede formar parte de un sistema de la presente invención o puede realizar un método de la presente invención (por ejemplo, las etapas S4, S5, S6, S7, S11 y S12). La estructura fundamental del dispositivo 200 de la Figura 5 es similar a la estructura del dispositivo 20 de la Figura 1, pero muestra numerosas características opcionales. Aunque las características opcionales de la Figura 5 se muestran en un único dibujo, se debe enfatizar que, por su propia naturaleza como características opcionales, no es necesario que todas estas características estén presentes en combinación exactamente como se muestra en la Figura 5. Se muestran en un único dispositivo 200 para propósitos ilustrativos, y, debe entenderse que, cualquiera, algunas o todas las características mostradas en el dispositivo alternativo 200 de la Figura 5 pueden excluirse del ejemplo sin que la disposición resultante quede fuera del alcance de esta divulgación.

Antes de analizar los componentes que lo componen, es importante considerar qué es realmente el dispositivo 200. En casos preferidos, el dispositivo 200 es un dispositivo perimetral. En el contexto de la presente invención, la expresión "dispositivo perimetral" debe entenderse como una referencia a un dispositivo que proporciona un punto de entrada a una red de dispositivos, teniendo el dispositivo cierta capacidad de procesamiento propia, para permitir que el procesamiento tenga lugar de manera no centralizada, mejorando por lo tanto la eficiencia de la red global. En algunos casos, el dispositivo puede ser un servidor. El dispositivo también puede ser una unidad de control electrónico de un vehículo u otro sistema, o un sistema integrado básico con una unidad de control multipunto (MCU) que usa uno o más tipos de datos de sensor como entrada.

El dispositivo 200 de la Figura 5 está conectado a través de una conexión C2 a una plataforma de seguridad 300. La plataforma de seguridad 300 incluye un módulo de generación de testigo de autorización 302, cuya función se describirá más adelante. Al igual que, por ejemplo, el sensor 100, el dispositivo 200 incluye un entorno seguro, en este caso un entorno seguro de dispositivo (DSE) 201. En el ejemplo mostrado en la Figura 5, el DSE 201 incluye: un procesador 202 y una memoria 204. Además, el DSE 201 también puede incluir: un módulo de interfaz de usuario 206, un módulo de interfaz de sensor 208 y un módulo de interfaz de plataforma de seguridad 209. Si bien en la Figura 5 se muestra que los cinco componentes antes mencionados forman parte del DSE 201, debe apreciarse que uno o más, o todos los componentes, podrían estar ubicados fuera del DSE 201. El procesador 202 puede incluir uno o más de: un módulo de descifrado 210, un módulo de generación de solicitud de acceso 212 y un módulo de autorización 214. La memoria 204 puede incluir una memoria persistente 216 (que tiene el mismo significado que en la Figura 4), que, a su vez, puede almacenar un testigo de autorización 216 y datos de sensor cifrados 220. El módulo de interfaz de usuario 206 puede incluir una pantalla 222 y un receptor de entrada de usuario 224. El módulo de interfaz de sensor 208 puede incluir un transmisor 226 y un receptor 228. Finalmente, el módulo de interfaz de la plataforma de seguridad 209 también puede incluir un transmisor 230 y un receptor 232 (que pueden, opcionalmente, ser el mismo, respectivamente, el transmisor 226 y el receptor 228). A continuación, se describirá la operación de los diversos componentes de la Figura 5 en el contexto del método mostrado en la Figura 3, así como la divulgación de características opcionales.

En la etapa S4, el receptor 228 del módulo de interfaz de sensor 206 recibe los datos de sensor cifrados que fueron transmitidos por el transmisor 124 del sensor 100. Tras lo cual, en la etapa S5, los datos de sensor cifrados recibidos 220 se almacenan en la memoria persistente 216.

En este punto, puede ser necesario que un usuario del dispositivo 200 acceda a un subconjunto de los datos recopilados por el elemento de detección 105 del dispositivo de recopilación de datos 103 del sensor 100. El usuario típicamente es un usuario de mantenimiento que necesita acceder a datos del subsistema (es decir, unos datos de sensor almacenados en el dispositivo 20). El usuario puede conectarse al dispositivo con, por ejemplo, un teléfono inteligente, una memoria USB, un dispositivo de mantenimiento o una UI del dispositivo, y proporcionar sus credenciales para obtener el testigo de autorización para solicitar la clave secreta para procesar los datos de sensor.

Para ello, en la etapa S6, el módulo de generación de solicitudes de acceso 212 genera una solicitud de acceso. Los datos a los que se permite el acceso al usuario están regidos por el testigo de autorización 218, por lo que antes de analizar la generación de la solicitud por el módulo de generación de solicitud de acceso 212, se describe la naturaleza del testigo de autorización 218.

En términos generales, el testigo de autorización 218 es un testigo electrónico que se implementa en la memoria persistente 216 de la memoria 204 del dispositivo 200, que incluye datos de control de acceso que definen uno o más subconjuntos de datos de sensor a los que el dispositivo 200 está autorizado a acceder. Como se ilustra en la Figura

5, el testigo de autorización 218 puede generarse por un módulo de generación de testigo de autorización 302 de una plataforma de seguridad 300.

El testigo de autorización 218 puede definir los subconjuntos usando, por ejemplo, un ID de subconjunto, o preferiblemente en términos de los metadatos asociados con el subconjunto. Específicamente, el testigo de autorización 218 puede definir uno o más de los siguientes:

- El tipo de datos a los que el dispositivo 200 está autorizado a acceder. Por ejemplo, la autorización puede especificar que al dispositivo 200 únicamente está autorizado a acceder a datos de temperatura.

- La indicación de tiempo o el intervalo de indicaciones de tiempo de los datos a los que el dispositivo 200 está autorizado acceder. Por ejemplo, el testigo de autorización 218 puede especificar que al dispositivo 200 está autorizado a acceder a los datos registrados en octubre de 2020 únicamente.

- En sistemas en los que hay más de un sensor 100, el testigo de autorización puede especificar que el dispositivo 200 está autorizado a acceder únicamente desde un sensor 100 específico. Como alternativa, en sistemas en los que un sistema 100 incluye una pluralidad de elementos de detección 105, el testigo de autorización 218 puede especificar que el dispositivo 200 está autorizado a acceder a los datos recopilados únicamente por un elemento de detección específico 115.

Además de especificar metadatos relacionados con los datos de sensor recopilados, el testigo de autorización 218 también puede incluir otras restricciones. Por ejemplo, en algunos casos, el testigo de autorización 218 puede definir una o más condiciones de validez. En el presente documento, una "condición de validez" se refiere a una regla que define cuándo el testigo de autorización 218 puede ser válido, puede usarse o puede ser efectivo. Si no se cumple la condición de validez, el testigo de autorización 218 se considera no válido. Las condiciones de validez podrán incluir una o más de las siguientes:

- Una restricción en el período o períodos de tiempo durante los que el testigo de autorización 218 es válido. Por ejemplo, el testigo de autorización 218 puede ser válido únicamente el primer día de cada mes o puede ser válido únicamente durante un año. [1] Después de este punto, el testigo de autorización 218 puede expirar.

- Una restricción sobre el número de veces que puede usarse el testigo de autorización 218. El testigo de autorización 218 puede incluir un contador de uso que se incrementa en uno cada vez que se usa, y el testigo de autorización 218 puede expirar después de que el contador de uso alcance un valor predeterminado.

- Una restricción sobre quién puede usar el testigo de autorización 218. Para este fin, el testigo de autorización 218 puede especificar una credencial de usuario o un conjunto de credenciales de usuario para las que es válido. En este caso, el procesador 102 del sensor 100 o el procesador 202 del dispositivo 200 pueden estar configurados para comparar una credencial de usuario en el testigo de autorización 218 con, por ejemplo, una credencial de usuario incluida en la solicitud o una credencial de usuario recibida en la interfaz de entrada de usuario 206 del dispositivo 200. A continuación, si las credenciales del usuario no coinciden, el testigo de autorización 218 puede considerarse no válido.

- En un sistema que incluye una pluralidad de dispositivos 200, el testigo de autorización 218 también puede especificar un dispositivo 200 (o dispositivos) específicos que están permitidos acceder a los datos de sensor solicitados. En el caso de que la solicitud provenga de un dispositivo diferente, a continuación, el testigo de autorización 218 puede considerarse no válido y la solicitud puede denegarse.

[1] Esto no debe confundirse con la restricción del período de tiempo durante el que se registran los datos de sensor. Las condiciones de validez son una propiedad del propio testigo de autorización y se aplican independientemente de la naturaleza de los datos de sensor en cuestión.

El testigo de autorización 218 puede especificar tipos específicos de acceso a los datos:

- El testigo de autorización 218 puede especificar que el dispositivo 200 únicamente está autorizado a descifrar y leer los datos de sensor cifrados 220 en cuestión. En otras palabras, el dispositivo 200 no podría modificar los datos.

- El testigo de autorización 218 puede especificar que el dispositivo 200 está autorizado a descifrar y autenticar los datos de sensor cifrados 220 en cuestión.

- El testigo de autorización 218 puede especificar que el dispositivo 200 únicamente está autorizado a autenticar los datos de sensor cifrados 220 en su forma cifrada, es decir, no descifrarlos.

A continuación, se explicarán las características opcionales de este proceso, con referencia a la Figura 5. En la etapa S6, se genera una solicitud de acceso. En algunos ejemplos del método, la solicitud de acceso incluye una indicación

de un subconjunto o subconjuntos de datos de sensor cifrados. Sin embargo, en otros casos, la solicitud no incluye una indicación de este tipo. En estos últimos casos, la etapa S7 implica simplemente transmitir la solicitud para acceder a algunos datos y el testigo de autorización 218 al sensor 100.

Es deseable, sin embargo, que la solicitud incluya alguna indicación de los datos de sensor cifrados 220 almacenados en la memoria 204 del dispositivo a los que el dispositivo 200 desea acceder (es decir, descifrar). Antes de que se genere la solicitud de acceso, el receptor de entrada inferior 224 del módulo de interfaz de usuario 206 puede recibir una entrada de usuario de un usuario. La entrada de usuario puede tener la forma de una solicitud para acceder a un subconjunto específico de los datos obtenidos por el sensor 100. La solicitud puede incluir información que identifica el subconjunto de datos de sensor al que el usuario desea acceder, por ejemplo, puede incluir el tipo de datos, el período de tiempo durante el que se recopilaron los datos y/o el sensor o elemento de detección específico que recopiló los datos. Cabe recordar que, cuando se recopilaron los datos por primera vez, es posible que se les haya anexado una cabecera que contenga metadatos, incluyendo los metadatos información acerca de la pieza específica de datos de sensor. En algunos casos, la solicitud del usuario puede incluir metadatos en el mismo formato.

Después de que se haya recibido la solicitud de datos a través del módulo de interfaz de usuario 208, el módulo de generación de solicitud de acceso 212 genera una solicitud basándose en lo que se recibe del usuario. Hay un número de maneras en que esto puede tener lugar, y todas tienen, en términos generales, el mismo resultado. En términos generales, se pueden dividir en dos categorías: (i) casos en los que la solicitud identifica el ID de subconjunto, y (ii) casos en los que la solicitud no identifica el ID de subconjunto.

(i) En algunos casos, la solicitud recibida por el receptor de entrada de usuario 224 puede incluir los metadatos en una forma que sea compatible con o equivalente a la forma en que los metadatos están almacenados en la memoria, a continuación, la solicitud puede enviarse directamente al módulo de generación de solicitud de acceso 212. A continuación, el módulo de generación de solicitud de acceso 212 puede configurarse para realizar una búsqueda en los datos de sensor cifrados 220 para determinar el subconjunto o subconjuntos de datos correspondientes a los metadatos en cuestión. Por ejemplo, para usar el ejemplo de los datos de la tabla central de la Figura 6, si la solicitud de acceso fuera para todos los datos de temperatura, a continuación, se devolvería el subconjunto de "temperatura". Como es evidente a partir del resto de la solicitud, el subconjunto puede tener asociado un ID de subconjunto, por ejemplo, numérico o alfanumérico. A continuación, el módulo de generación de solicitud de acceso 212 genera una solicitud que contiene los ID de subconjunto correspondientes a todos los metadatos recibidos a través de la interfaz de usuario. Opcionalmente, la solicitud también puede incluir los metadatos. En una versión ligeramente modificada de este enfoque, si la solicitud recibida por el receptor de entrada de usuario 224 incluye datos en un formato no adecuado para su procesamiento por el módulo de generación de solicitud de acceso 212, a continuación, el método puede incluir una etapa adicional de conversión de la solicitud recibida en la interfaz de usuario 206 en metadatos en una forma adecuada para su procesamiento por el módulo de generación de solicitud de acceso 212. En consecuencia, el procesador 202 puede incluir además un módulo de conversión de metadatos 211 como se muestra en la Figura 5.

(ii) Como alternativa, una vez que se ha recibido la solicitud en la interfaz de usuario 206, el módulo de generación de solicitud de acceso 212 puede configurarse para generar una solicitud que incluye los metadatos, sin búsqueda ni identificación del ID de subconjunto.

En este punto, el módulo de generación de solicitud de acceso 212 ha generado la solicitud, incluyendo opcionalmente la solicitud una indicación de los subconjuntos de los datos de sensor cifrados 220 que le gustaría poder descifrar. La indicación de los subconjuntos puede ser en forma de metadatos relacionados con los datos o en forma de un ID de subconjunto.

A continuación, en la etapa S8, el transmisor 226 del módulo de interfaz de sensor 208 envía la solicitud y el testigo de autorización 218 al sensor 100. En este punto, volvemos a la Figura 2, etapa S8, en la que el receptor 126 del módulo de interfaz del dispositivo 106 recibe la solicitud y el testigo de autorización 218.

Antes de determinar, mediante el módulo de determinación de acceso 110, a qué datos de sensor está autorizado acceder el dispositivo 200, el procesador 102 o el sensor 100, o el módulo de determinación de acceso 110 pueden determinar opcionalmente en primer lugar si se cumple la condición de validez, si el testigo de autorización 218 incluye una.

A continuación, en la etapa S9, el procesador 102 (específicamente, el módulo de determinación de acceso 110 del mismo) determina, usando el testigo de autorización 218, si al dispositivo 200 está autorizado a acceder a los datos de sensor que ha solicitado. Hay varias situaciones en este punto: situaciones en las que la solicitud no incluye una indicación de los datos solicitados, situaciones en las que la solicitud incluye los metadatos, pero no el ID del subconjunto y situaciones en las que la solicitud incluye el ID de subconjunto. Estas se analizan a continuación.

(i) En los casos donde la solicitud no incluye una indicación de los datos solicitados, la única información que el sensor 100, específicamente el módulo de determinación de acceso 110 del mismo, tiene que consultar es la información almacenada en el testigo de autorización 218 que recibe junto con la solicitud de datos. De manera

efectiva, se trata de una solicitud de clave de descifrado para todas las piezas de datos de sensor cifrados a los que el dispositivo 200 tiene permiso de acceder. Como se ha analizado anteriormente, el testigo de autorización puede incluir metadatos que identifican los subconjuntos de datos a los que el dispositivo 200 tiene acceso, o puede incluir el ID de subconjunto específico. En cualquier caso, el módulo de determinación de acceso 110 puede realizar, a continuación, una búsqueda de los metadatos y/o los ID de subconjuntos en la tabla de datos de claves de cifrado 120, y recuperar las claves de descifrado asociadas con cada una de las piezas de metadatos o ID de subconjuntos. Se entenderá que, en el caso de que la clave de cifrado sea simétrica, la clave de descifrado es la misma que la clave de cifrado.

(ii) En los casos donde la solicitud especifica los metadatos a los que el dispositivo 200 desea acceder, en primer lugar, es necesario verificar si el dispositivo 200 está autorizado a acceder a esos datos. En consecuencia, el módulo de determinación de acceso 110 valida los metadatos o los ID de subconjunto en la solicitud basándose en los datos de control de acceso del testigo de autorización 218. Específicamente, el módulo de determinación de acceso compara los metadatos o los ID de subconjuntos en la solicitud con los metadatos o los ID de subconjuntos enumerados en los datos de control de acceso. Puede un número de resultados:

- Si se determina que el dispositivo 200 está autorizado a para acceder a todos los metadatos o ID de subconjuntos solicitados, el módulo de determinación de acceso 110 puede realizar una búsqueda de todos los metadatos o ID de subconjuntos en la solicitud en la tabla de datos de clave de cifrado 120 y recuperar las claves de descifrado asociadas con cada una de las piezas de metadatos o ID de subconjuntos. Se entenderá que, en el caso de que la clave de cifrado sea simétrica, la clave de descifrado es la misma que la clave de cifrado.

- Si se determina que el dispositivo 200 únicamente está autorizado a acceder a algunos de los metadatos o ID de subconjuntos solicitados en la solicitud, ya sea:

    a. La solicitud se considerará nula y el procedimiento finaliza, o

    b. El módulo de determinación de acceso 110 determinará cuáles de los metadatos o ID de subconjunto en la solicitud del dispositivo 200 **están** permitidos a acceder y realizar una búsqueda únicamente de aquellos metadatos o ID de subconjuntos en la tabla de datos de clave de cifrado 120 y recuperar las claves de descifrado asociadas con cada una de esas piezas de metadatos o ID de subconjuntos. Se entenderá que, en el caso de que la clave de cifrado sea simétrica, la clave de descifrado es la misma que la clave de cifrado.

- Si se determina que el dispositivo 200 no está autorizado a acceder a ninguno de los metadatos o ID de subconjunto solicitados, la solicitud se considerará nula y el método finaliza.

Opcionalmente, puede haber una etapa adicional en el que el procesador 102 realiza una búsqueda para identificar los ID de subconjunto correspondientes a los metadatos en la solicitud o los metadatos a los que el dispositivo 200 tiene acceso, y, a continuación, realiza la búsqueda de la tabla de datos de clave de cifrado 120 usando los ID de subconjunto identificados como entrada.

Lo anterior se refiere a situaciones en las que las claves de cifrado/descifrado se almacenan en la tabla de datos de claves de cifrado 120. Sin embargo, también hemos analizado la posibilidad de que las claves de cifrado y/o descifrado se puedan generar basándose en los metadatos y/o ID de subconjuntos y en los datos de generación de claves almacenados localmente 118. En estos casos, si no hay datos especificados o indicados en la solicitud, a continuación, el módulo de determinación de acceso 110 puede enviar todos los metadatos y/o ID de subconjuntos definidos en los datos de control de acceso del testigo de autorización 218 al módulo de cifrado 108, al módulo de generación de claves 109 o a cualquier otro módulo apropiado del procesador 102 (no mostrado). Allí, el método puede incluir una etapa de generación de una clave de descifrado para cada pieza de datos de sensor cifrados correspondiente a los metadatos y/o los ID de subconjuntos definidos por los datos de control de acceso. La clave de descifrado se genera de forma determinista, de la misma manera que la clave de cifrado, como se explicó anteriormente en la solicitud.

El proceso para los casos en los que la solicitud incluye una indicación de los ID de subconjuntos/metadatos de solicitudes es análogo. En primer lugar, es necesario verificar si el dispositivo 200 tiene permitido el acceso a esos datos. En consecuencia, el módulo de determinación de acceso 110 valida los metadatos o los ID de subconjunto en la solicitud basándose en los datos de control de acceso del testigo de autorización 218. Específicamente, el módulo de determinación de acceso compara los metadatos o los ID de subconjuntos en la solicitud con los metadatos o los ID de subconjuntos enumerados en los datos de control de acceso. Entonces, como antes:

- Si se determina que al dispositivo 200 está autorizado a acceder a todos los metadatos o ID de subconjuntos solicitados, el módulo de determinación de acceso 110 puede enviar todos los metadatos y/o ID de subconjuntos definidos en la solicitud al módulo de cifrado 108, al módulo de generación de claves 109 o a cualquier otro módulo apropiado del procesador 102 (no mostrado). Allí, el método puede incluir una etapa de generación de una clave de descifrado para cada pieza de datos de sensor cifrados correspondiente a los metadatos y/o los ID de

subconjuntos definidos por los datos de control de acceso. La clave de descifrado se genera de forma determinista, de la misma manera que la clave de cifrado, como se explicó anteriormente en la solicitud.

- Si se determina que el dispositivo 200 únicamente está autorizado a acceder a **algunos** de los metadatos o ID de subconjuntos solicitados en la solicitud, ya sea:

  a. La solicitud se considerará nula y el procedimiento finaliza, o

  b. El módulo de determinación de acceso 110 identificará cuáles de los metadatos o ID de subconjuntos en la solicitud el dispositivo 200 **está autorizado a** acceder. A continuación, el módulo de determinación de acceso 110 puede enviar todos esos metadatos identificados y/o ID de subconjuntos definidos en los datos de control de acceso del testigo de autorización 218 al módulo de cifrado 108, al módulo de generación de claves 109 o a cualquier otro módulo apropiado del procesador 102 (no mostrado). Allí, el método puede incluir una etapa de generación de una clave de descifrado para cada pieza de datos de sensor cifrados correspondiente a los metadatos y/o los ID de subconjuntos definidos por los datos de control de acceso. La clave de descifrado se genera de forma determinista, de la misma manera que la clave de cifrado, como se explicó anteriormente en la solicitud.

- Si se determina que el dispositivo 200 no está autorizado a acceder a ninguno de los metadatos o ID de subconjunto solicitados, la solicitud se considerará nula y el método finaliza.

En este punto, las claves de descifrado correspondientes a las piezas de datos de sensor cifrados 220 definidas por los metadatos o los ID de subconjuntos se han generado o recuperado en el sensor 100, por ejemplo, mediante el módulo de generación de claves 109, el módulo de determinación de acceso 110 o cualquier otro módulo adecuado en el procesador 102. En algunos casos, se han recuperado o generado claves de descifrado correspondientes a todas las piezas de datos de sensor cifrados 220 definidas por los metadatos o los ID de subconjuntos a los que el dispositivo 200 está autorizado a acceder, como se define por los datos de control de acceso en el testigo de autorización. En otros casos, se han recuperado o generado claves de descifrado correspondientes a todas las piezas de datos de sensor cifrados 220 definidas por los metadatos o los ID de subconjuntos incluidos en la solicitud. Y, en otros casos, se han recuperado o generado claves de descifrado correspondientes a todas las piezas de datos de sensor cifrados 220 definidas por los metadatos o los ID de subconjuntos incluidos en la solicitud, y a los que el dispositivo 200 está autorizado a acceder, como se define por los datos de control de acceso en el testigo de autorización. A continuación, en la etapa 510, el transmisor 124 del módulo de interfaz de dispositivo 106 del sensor 100 transmite esas claves de descifrado al dispositivo 200.

Volviendo a la Figura 3, el receptor 228 del módulo de interfaz de sensor 208 del dispositivo 200 recibe las claves transmitidas, y el módulo de descifrado 210 del procesador 202, a continuación, puede usar las claves de descifrado recibidas para descifrar los datos requeridos, para su procesamiento adicional, completando el método.

La Figura 11 muestra un sistema 1000, que incluye diversos componentes. Como se apreciará a partir de la siguiente descripción, el sistema 1000 representa un entorno en el que se puede implementar la presente invención. A continuación, también se describen casos de uso específicos, con referencia en particular a los tipos de sensores y parámetros operativos en cuestión. Los detalles del método de la invención, que se ha descrito en detalle anteriormente en la descripción anterior, y las diversas opciones no se repiten en este punto, pero debe entenderse que, cuando sea compatible, cualquier característica descrita anteriormente puede combinarse con cualquiera de las características siguientes.

El sistema 1000 incluye una pluralidad de sensores 1002a, 1002b, 1002c, 1002d, 1002e (aunque se apreciará que el contenedor puede incluir cualquier número de sensores, incluyendo un único sensor 1002). Cada uno de los sensores 1002 puede configurarse para realizar el método del primer aspecto de la invención. Cada sensor 1002, puede incluir una memoria intermedia en la que se almacenan temporalmente datos de sensor, por ejemplo, una clave de protección generada y almacenada en el respectivo sensor 1002. Como alternativa, como se analizó anteriormente, el sensor 1002 puede generar las claves en una base *ad hoc*, y las claves pueden usarse únicamente para proteger los datos de sensor generados, y no pueden almacenarse en el sensor 1002. Los sensores 1002 pueden ser como se han descrito previamente en esta solicitud.

El sistema 1000 también incluye una pluralidad de dispositivos 1006a, 1006b, 1006c. En el ejemplo mostrado en la Figura 11, cada uno de los dispositivos 1006 puede corresponder a un respectivo sensor 1002. Sin embargo, esto no es siempre el caso. Por ejemplo, se prevé que cada uno de los sensores 1002 podría enviar sus datos de sensor protegidos generados a un único dispositivo 1006. Como alternativa, un solo sensor 1002 podría enviar diferentes tipos de datos de sensor protegidos a diferentes dispositivos 1002. En este ejemplo, los dispositivos 1006 pueden tener la forma de estaciones de monitorización en o cerca del sistema 1000, como alternativa, pueden ser dispositivos terminales (accesibles por un usuario) o unidades de control. En la Figura 11 se muestra un ejemplo de cada uno de ellos, con propósitos ilustrativos.

Cada uno de los dispositivos 1006 puede incluir una memoria 1008a, 1008b, 1008c, (donde se pueden almacenar los

datos de sensor protegidos), y un procesador respectivo 1010a, 1010b, 1010c. Un uso de los dispositivos 1006 es permitir que un usuario acceda a los datos permitidos, por ejemplo, para propósitos de mantenimiento de sistema, control o control de calidad. Algunos ejemplos (para reiterar, aunque estos ejemplos se divulgan en este punto en combinación con el ejemplo específico del sistema 1000, se pueden aplicar de forma general a cualquier implementación de la invención):

- El dispositivo 1006a puede ser un terminal que tiene una pantalla 1012a. La memoria del terminal 1008a puede incluir el testigo de autorización que incluye los datos de control de acceso. En tales casos, cuando un usuario desea acceder a los datos de sensor protegidos, puede activar el terminal e introducir instrucciones que hagan que el terminal 1006a envíe una solicitud de acceso y/o el testigo de autorización al sensor 1002a. A continuación, de acuerdo con una de las realizaciones de la invención, el sensor 1002a puede enviar las claves de acceso pertinentes al terminal 1006a, permitiendo al usuario el acceso pertinente, por ejemplo, para ver los datos en la pantalla, o para modificar y volver a cifrar los datos.

- El dispositivo 1006b también puede ser un terminal que tiene una pantalla 1012b. En este ejemplo, el terminal 1006b se diferencia del terminal 1006a en que el terminal 1006b no tiene un testigo de autorización. En este caso, un usuario que desee acceder a los datos de sensor protegidos puede tener su propio dispositivo portátil 1014b (tal como un ordenador portable, un ordenador portátil, una tableta, un teléfono inteligente o similar) que tenga el testigo de autorización implementado en el mismo. El dispositivo 1006b incluye una interfaz 1016b (que puede ser una interfaz física o inalámbrica) a través de la que el usuario puede conectar el dispositivo portátil 1014b. A continuación, el dispositivo portátil 1014b puede implementar el testigo de autorización en el dispositivo 1006b. En este punto, se puede considerar que el testigo de autorización está desplegado en el dispositivo 1006b. Como alternativa, el testigo de autorización puede permanecer en el dispositivo portátil 1014b. En esta situación, la combinación del dispositivo 1006b y el portátil 1014b puede considerarse que representa "un dispositivo que tiene el testigo de autorización desplegado en el mismo", o equivalente. En este punto se pueden realizar las etapas descritas anteriormente. El acceso de datos puede realizarse a través de la pantalla 1012b o de una pantalla 1018b del dispositivo portátil 1014b.

- El dispositivo 1006c puede ser una unidad de control, que está configurada para controlar uno o más parámetros operativos de un componente 1020 en el sistema 1000. La unidad de control 1006c del sistema 1000 puede estar configurada para ajustar uno o más parámetros operativos basándose en los datos de sensor. Para obtener los datos de sensor, la unidad de control 1006c debe acceder a los datos de sensor protegidos que están almacenados en su memoria 1008c. La unidad de control 1006c tiene almacenado en la misma el testigo de autorización, aunque éste puede desplegarse a través de un dispositivo portátil. A continuación, de acuerdo con una realización, la unidad de control 1006c puede recibir una clave apropiada para acceder a los datos deseados. A continuación, la unidad de control 1006c puede configurarse para variar, seleccionar o determinar de otra manera un valor de uno o más parámetros operativos basándose en los datos de sensor. Protegiendo los datos según la invención, es posible garantizar que dispositivos no autorizados no puedan controlar los parámetros operativos.

Algunos casos de uso específicos se describen a continuación.

En una situación, el sistema 1000 puede tener la forma de un contenedor (tal como un contenedor de envío) para transportar mercancías. Por ejemplo, el contenedor puede estar configurado para transportar alimentos a largas distancias. En este caso, el contenedor puede incluir una unidad de refrigeración, la unidad de refrigeración puede incluir un sensor de temperatura y el parámetro operativo puede ser la temperatura de un área de almacenamiento de la unidad de refrigeración.

De esta manera, el sistema 100 puede monitorizar de forma segura la temperatura de la unidad de refrigeración y ajustar la temperatura basándose en los datos de temperatura que se reciben. En el ejemplo del contenedor, otros sensores que pueden incluirse son otros tipos de sensores ambientales, tales como sensores de temperatura, sensores de humedad, sensores de presión, sensores de estado de puerta, sensores de movimiento y similares. Los usuarios, tales como el personal de mantenimiento o los ingenieros, pueden de esta manera monitorizar las condiciones del contenedor, sin riesgo de que los datos de sensor hayan sido modificados, ya que únicamente el personal autorizado podrá acceder a los datos y se puede garantizar que cualquier manipulación sea detectable.

En un caso alternativo, el sistema 1000 puede tener la forma de un vehículo, tal como un coche, un tren, un avión, un autobús, un helicóptero o cualquier otro vehículo. En casos preferidos, el sistema 1000 puede tener la forma de un vehículo "inteligente". La invención podría ser particularmente ventajosa en dos situaciones en un vehículo o un vehículo inteligente (que tenga varios tipos de sensores, tales como sensor de radar, sensor láser, incluyendo el sensor LiDAR 3D, o sensor ultrasónico):

- **Monitorización.** En este caso, los sensores pueden incluir sensores de desgaste, cada uno de los cuales está configurado para monitorizar el desgaste de un componente respectivo del vehículo, u otros sensores que están configurados para medir parámetros indicativos de el "estado" o el "desgaste" de los componentes del vehículo. En un caso particularmente ventajoso, cuando el sensor o dispositivo detecta que el valor del parámetro medido cumple o supera un umbral predeterminado, puede configurarse para generar una alerta. La alerta puede informar

al usuario o propietario del vehículo que debe llevarlo para su reparación. Los ingenieros registrados también pueden acceder a los datos de sensor (o a un subconjunto diferente de los datos de sensor) para ayudarlos con la reparación. Esto puede garantizar que únicamente los ingenieros registrados o autorizados puedan realizar reparaciones en el vehículo en cuestión.

- **Control.** La presente invención puede usarse para habilitar sistemas avanzados de asistencia al conductor (ADAS) o la funcionalidad autónoma del vehículo. En este punto, el término "piloto automático" debe entenderse que corresponde a cualquier control automático del vehículo, y no necesariamente sólo de un avión. Esta función se puede lograr de manera similar al control de refrigeración analizado con respecto al contenedor. Los sensores pueden configurarse para detectar diversos parámetros relevantes para el control del vehículo, por ejemplo, proximidad a otros vehículos u obstáculos, ubicación (por ejemplo, la posición de un coche en un mapa, la posición de un avión en relación con una pista, la posición del casco de un barco en relación con las características del fondo marino), altitud, profundidad, velocidad, orientación del vehículo. A continuación, la unidad de control puede, basándose en estos parámetros, configurarse para determinar o variar el valor de uno o más parámetros operativos. Esta funcionalidad podría usarse, por ejemplo, para el aterrizaje automático de un avión, el estacionamiento de un coche o un tren, o el amarre de un barco. La presente invención es ventajosa en este punto porque permite garantizar que dispositivos no autorizados no puedan acceder a los datos de sensor, lo que, claramente, podría tener consecuencias desastrosas.

De manera similar al caso de uso del vehículo inteligente, la presente invención también puede ser aplicable a sistemas de control industrial, tanto en contextos de monitorización como de control. En otras palabras, el sistema 1000 puede ser un sistema de control industrial. En el contexto de la monitorización, el sistema puede funcionar de forma muy similar al caso del vehículo inteligente. En el caso del control industrial, los parámetros que miden los sensores pueden ser diferentes. Por ejemplo, pueden configurarse para medir condiciones ambientales, tales como temperatura, presión, nivel de humedad/humectación, pH, concentraciones o presiones parciales de ciertas sustancias. Las condiciones adicionales pueden incluir diversas propiedades eléctricas (por ejemplo, corriente, tensión, potencia, intensidad del campo eléctrico/densidad de flujo, intensidad del campo magnético/densidad de flujo, carga, resistencia, inductancia, capacitancia, conductividad/conductancia, resistividad/resistencia), conductividad térmica y cualquier otro parámetro que pueda dar una indicación en cuanto al progreso de un proceso industrial. Además, también está previsto que se empleen sensores de "desgaste" para monitorizar el estado de los componentes industriales. Como antes, una unidad de control puede configurarse para variar uno o más parámetros operativos basándose en los datos de sensor.

Otra situación en la que se puede usar la presente invención es en un hospital.

Las características analizadas en la descripción anterior, o en las reivindicaciones siguientes, o en los dibujos adjuntos, expresadas en sus formas específicas o en términos de un medio para realizar la función divulgada, o un método o proceso para obtener los resultados divulgados, según sea apropiado, pueden utilizarse, por separado, o en cualquier combinación de tales características, para realizar la invención en diversas formas de la misma.

Mientras la invención se ha descrito en conjunto con las realizaciones ilustrativas descritas anteriormente, muchas modificaciones y variaciones equivalentes serán evidentes para expertos en la materia cuando se proporcione esta divulgación. Por consiguiente, las realizaciones ilustrativas de la invención expuestas anteriormente se consideran ilustrativas y no limitativas. Se pueden realizar diversos cambios a las realizaciones descritas sin alejarse del alcance de la invención.

Para evitar cualquier duda, las explicaciones teóricas proporcionadas en el presente documento se ofrecen con el propósito de mejorar la comprensión de un lector. Los inventores no desean quedar limitados por ninguna de estas explicaciones teóricas.

Cualesquiera títulos de sección usados en el presente documento tienen únicamente propósitos organizativos y no deben interpretarse como limitantes de la materia objeto.

A través de toda esta memoria descriptiva, incluyendo en las reivindicaciones que siguen, a menos que el contexto lo requiera de otra manera, las palabras "comprende" e "incluye" y variaciones tales como "comprende" y "que comprende" se entenderá que implican la inclusión de un elemento integrante o grupo de elementos integrantes o etapas establecidos, pero no la exclusión de cualquier otro elemento integrante o etapa o grupo de elementos integrantes o etapas.

Debe observarse que, como se usa en la memoria descriptiva y en las reivindicaciones adjuntas, las formas singulares "un", "una", "el", "la" incluyen referentes plurales a menos que el contexto dicte claramente el contexto de otra manera. Pueden expresarse intervalos en el presente documento como desde "aproximadamente" un valor particular, y/o hasta "aproximadamente" otro valor particular. Cuando se expresa un intervalo de este tipo, otra realización incluye desde el valor particular y/o hasta el otro valor particular. De manera similar, cuando se expresan valores como aproximaciones, mediante el uso del antecedente "aproximadamente", se entenderá que el valor particular forma otra realización. El término "aproximadamente" en relación con un valor numérico es opcional y significa, por ejemplo, +/- 10 %.

REIVINDICACIONES

1. Un método, realizado por un sensor (10), para controlar el acceso a datos de sensor, incluyendo el método las etapas de:

generar (S1) datos de sensor y proteger (S2) los datos de sensor para generar datos de sensor protegidos; y
transmitir (S3) los datos de sensor protegidos a un dispositivo (20) para su almacenamiento;
caracterizado por que:
el método comprende, además:

recibir (S4), desde el dispositivo (20) un testigo de autorización (23) que incluye datos de control de acceso que definen una o más operaciones que el dispositivo está autorizado a ejecutar en los datos de sensor protegidos (24);
determinar (S9), basándose en los datos de control de acceso, una operación que el dispositivo (20) está autorizado a ejecutar en los datos de sensor protegidos (24);
proporcionar (S10), al dispositivo (20), una o más claves utilizables por el dispositivo para ejecutar la operación en los datos de sensor protegidos (24).

2. El método de la reivindicación 1, en donde:
proteger datos de sensor comprende proteger los datos de sensor mediante una clave secreta.

3. El método de la reivindicación 1 o reivindicación 2, en donde:
el método incluye además borrar los datos de sensor y/o los datos de sensor protegidos después de la etapa de transmitirlos al dispositivo.

4. El método de una cualquiera de las reivindicaciones 1 a 3, en donde:

proteger los datos de sensor incluye:
aplicar una primera clave secreta a los datos de sensor, para generar los datos de sensor protegidos; y
si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar una primera operación en los datos de sensor protegidos, la etapa de proporcionar incluye:
proporcionar, al dispositivo, una primera clave complementaria, utilizable por el dispositivo para ejecutar la primera operación, siendo complementaria la primera clave complementaria a la primera clave secreta.

5. El método de la reivindicación 4, en donde:

la primera clave secreta es una clave de cifrado;
los primeros datos de sensor protegidos son datos de sensor cifrados;
la primera operación es una operación de descifrado o de lectura;
la etapa de proporcionar incluye:
proporcionar una clave complementaria en forma de clave de descifrado al dispositivo.

6. El método de la reivindicación 5, en donde:
proteger los datos de sensor incluye:
aplicar una segunda clave secreta a los primeros datos de sensor protegidos, para generar segundos datos de sensor protegidos; y

(i) si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar una segunda operación en los segundos datos protegidos, la etapa de proporcionar incluye:
proporcionar, al dispositivo, una segunda clave complementaria, utilizable por el dispositivo para ejecutar la segunda operación en los segundos datos de sensor protegidos; o
(ii) si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar tanto la primera como la segunda operación, la etapa de proporcionar incluye:
proporcionar, al dispositivo, la primera clave complementaria y la segunda clave complementaria, utilizable la segunda clave complementaria por el dispositivo para ejecutar la segunda operación en los segundos datos de sensor protegidos para recuperar los primeros datos de sensor protegidos, y, a continuación, utilizable la primera clave complementaria por el dispositivo para ejecutar la primera operación en los primeros datos de sensor protegidos
(iii) si los datos de control de acceso definen que el dispositivo está autorizado a ejecutar una tercera operación en los segundos datos protegidos, la etapa de proporcionar incluye:
proporcionar, al dispositivo, la primera clave complementaria y la segunda clave complementaria, utilizables la primera clave complementaria y la segunda clave complementaria en combinación para ejecutar la tercera operación en los segundos datos de sensor protegidos.

7. Un método de acuerdo con la reivindicación 6, en donde:

la primera clave secreta es una primera clave de autenticación;
la segunda clave secreta es una clave de cifrado;
la etapa de proteger los datos de sensor incluye:

aplicar la primera clave de autenticación a los datos de sensor para generar un código de autenticación, siendo los primeros datos de sensor protegidos una combinación de los datos de sensor y el código de autenticación;
aplicar la clave de cifrado a los primeros datos de sensor protegidos, para generar datos de sensor cifrados.

8. Un método de acuerdo con la reivindicación 6, en donde:

si los datos de control de acceso definen que el dispositivo está autorizado a descifrar los datos de sensor cifrados, la etapa de proporcionar incluye proporcionar al dispositivo una clave de descifrado utilizable por el dispositivo para descifrar los datos de sensor cifrados; y
si los datos de control de acceso definen que el dispositivo está autorizado a descifrar y volver a autenticar los datos de sensor cifrados, o modificar los datos de sensor, la etapa de proporcionar incluye proporcionar, al dispositivo, la primera clave de autenticación y la clave de descifrado, utilizable la clave de descifrado por el dispositivo para descifrar los datos de sensor cifrados, para recuperar la combinación de los datos de sensor y el código de autenticación, permitiendo de esta manera que el dispositivo modifique los datos de sensor, genere datos de sensor modificados, y utilizable la primera clave de autenticación por el dispositivo en los datos de sensor modificados para generar un segundo código de autenticación.

9. El método de una cualquiera de las reivindicaciones 1 a 8, en donde:

los datos de sensor incluyen un primer subconjunto de datos de sensor y un segundo subconjunto de datos de sensor;
la etapa de proteger los datos de sensor incluye:

proteger el primer subconjunto de datos de sensor para generar un primer subconjunto de datos de sensor protegidos; y
proteger el segundo subconjunto de datos de sensor para generar un segundo subconjunto de datos de sensor protegidos;
los datos de control de acceso definen:

una primera operación que el dispositivo está autorizado a ejecutar en el primer subconjunto de datos de sensor protegidos; y/o
una segunda operación que el dispositivo está autorizado a ejecutar en el segundo subconjunto de datos de sensor protegidos;

la etapa de determinación incluye determinar, basándose en los datos de control de acceso:

una primera operación que el dispositivo está autorizado a ejecutar en el primer subconjunto de datos de sensor protegidos; y/o
una segunda operación que el dispositivo está autorizado a ejecutar en el segundo subconjunto de datos protegidos; y

la etapa de proporcionar incluye:

únicamente si se determina que el dispositivo está autorizado a ejecutar la primera operación, proporcionar una o más claves utilizables por el dispositivo para ejecutar la primera operación en el primer subconjunto de los datos de sensor protegidos; y
únicamente si se determina que el dispositivo está autorizado a ejecutar la segunda operación, proporcionar una o más claves utilizables por el dispositivo para ejecutar la segunda operación en el segundo subconjunto de datos de sensor protegidos.

10. Un método para acceder a datos de sensor protegidos mediante un dispositivo (20), incluyendo el método las etapas de:

recibir (S4) datos de sensor protegidos (24) de un sensor (10);
almacenar (S5) los datos de sensor protegidos recibidos (24);
caracterizado por que:
el dispositivo (20) tiene almacenado en el mismo un testigo de autorización (23) que incluye datos de control de acceso que definen una o más operaciones que el dispositivo (20) está autorizado a ejecutar en datos de sensor protegidos (24); y
el método comprende, además:
enviar (S7) el testigo de autorización al sensor (10); y
recibir (S11), desde el sensor (10), una o más claves utilizables por el dispositivo (20) para ejecutar una operación

permitida en los datos de sensor protegidos (24).

11. El método de la reivindicación 10, que incluye, además:
enviar una solicitud de acceso al sensor, especificando la solicitud de acceso una operación solicitada a ejecutar en los datos de sensor protegidos.

12. El método de la reivindicación 10 o reivindicación 11, en donde:

los datos de sensor protegidos incluyen un primer subconjunto de datos de sensor protegidos y un segundo subconjunto de datos de sensor protegidos;
los datos de control de acceso definen: una primera operación que el dispositivo está autorizado a ejecutar en el primer subconjunto de datos de sensor protegidos; y/o una segunda operación que el dispositivo está autorizado a ejecutar en el segundo subconjunto de datos de sensor protegidos;
la etapa de recepción incluye:

únicamente si se define en los datos de control de acceso que el dispositivo está autorizado a ejecutar la primera operación, recibir una o más claves utilizables por el dispositivo para ejecutar la primera operación en el primer subconjunto de los datos de sensor protegidos; y
únicamente si se define en los datos de control de acceso que el dispositivo está autorizado a ejecutar la segunda operación, recibir una o más claves utilizables por el dispositivo para ejecutar la segunda operación en el segundo subconjunto de los datos de sensor protegidos.

13. El método de la reivindicación 12, que incluye:
enviar una solicitud de acceso al sensor, especificando la solicitud de acceso uno o más de: la primera operación a ejecutar en el primer subconjunto de datos de sensor cifrados, y la segunda operación a ejecutar en el segundo subconjunto de datos de sensor cifrados.

14. El método de una cualquiera de las reivindicaciones 10 a 13, en donde:

el testigo de autorización define una o más condiciones de validez en forma de una condición que debe cumplirse para que el testigo de autorización sea válido, incluyendo las condiciones de validez uno o más de:
una restricción sobre el período de tiempo o períodos de tiempo durante los que el testigo de autorización es válido;
una restricción sobre el número de veces que se puede usar el testigo de autorización;
una restricción sobre una credencial de usuario o un conjunto de credenciales de usuario que pueden usarse en asociación con el testigo de autorización; y
una restricción en un dispositivo que envía el testigo de autorización.

15. Un sensor (10) configurado para generar datos de sensor y para controlar el acceso a los datos de sensor, el sensor (10) configurado para realizar el método de una cualquiera de las reivindicaciones 1 a 9.

16. Un dispositivo (20) para procesar datos de sensor protegidos (24), el dispositivo (20) configurado para realizar el método de una cualquiera de las reivindicaciones 10 a 14.

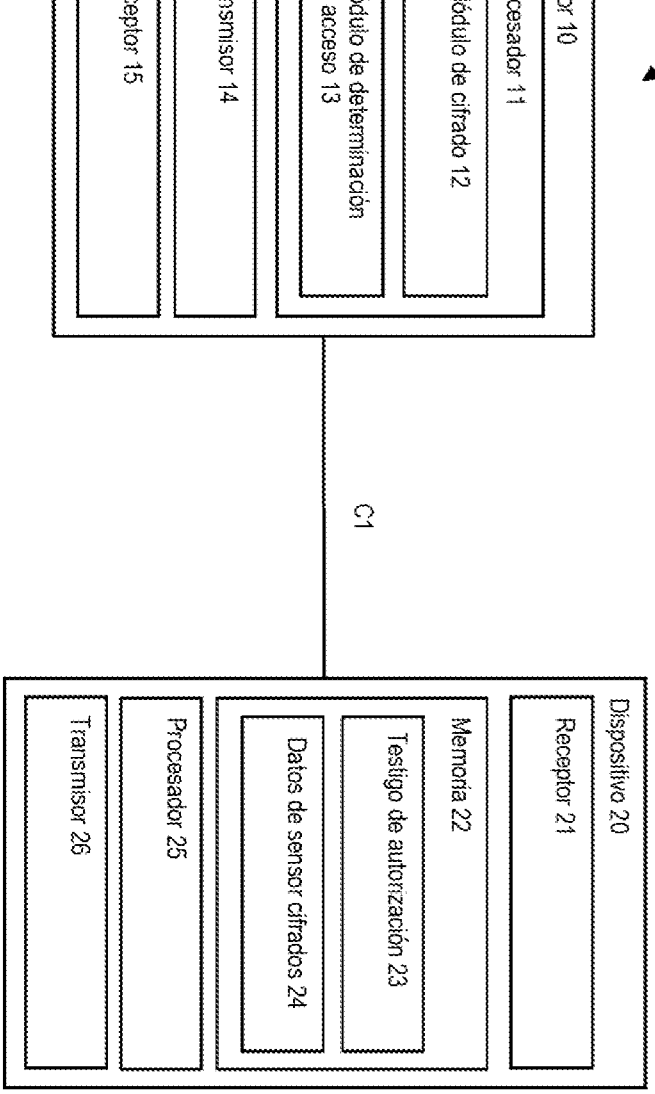
1
Sensor 10
Procesador 11
Módulo de cifrado 12
Módulo de determinación de acceso 13
Transmisor 14
Receptor 15
C1
Dispositivo 20
Receptor 21
Memoria 22
Testigo de autorización 23
Datos de sensor cifrados 24
Procesador 25
Transmisor 26

Fig. 1

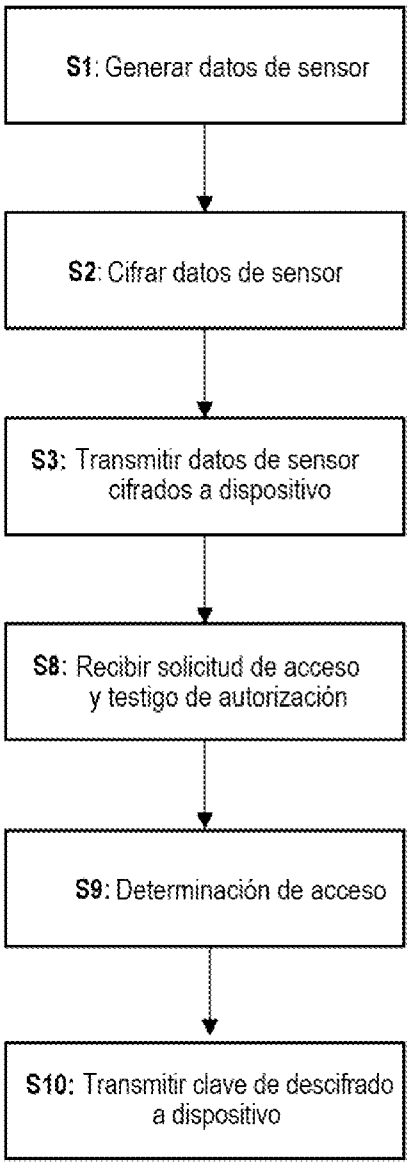
S1: Generar datos de sensor
S2: Cifrar datos de sensor
S3: Transmitir datos de sensor cifrados a dispositivo
S8: Recibir solicitud de acceso y testigo de autorización
S9: Determinación de acceso
S10: Transmitir clave de descifrado a dispositivo

Fig. 2

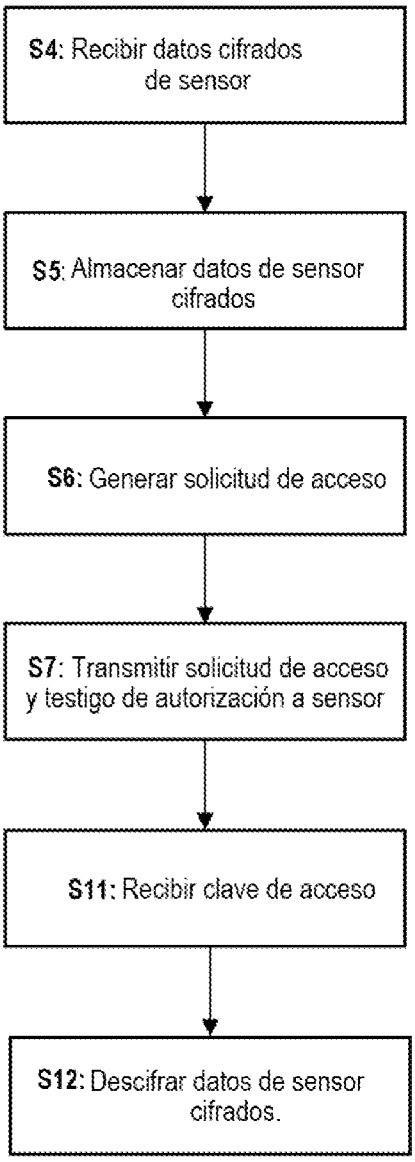
S4: Recibir datos cifrados de sensor
S5: Almacenar datos de sensor cifrados
S6: Generar solicitud de acceso
S7: Transmitir solicitud de acceso y testigo de autorización a sensor
S11: Recibir clave de acceso
S12: Descifrar datos de sensor cifrados.

Fig. 3

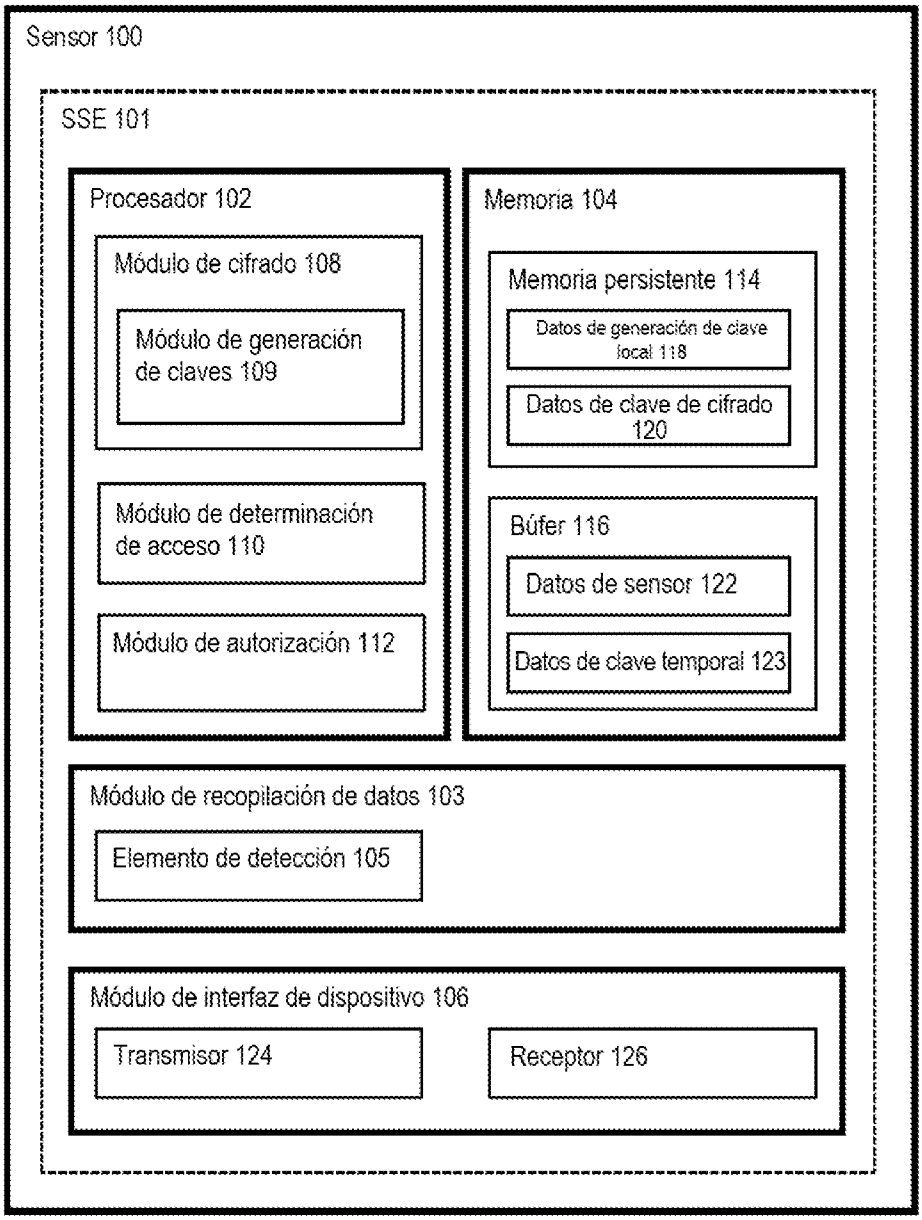
Sensor 100
SSE 101
Procesador 102
Módulo de cifrado 108
Módulo de generación de claves 109
Módulo de determinación de acceso 110
Módulo de autorización 112
Memoria 104
Memoria persistente 114
Datos de generación de clave local 118
Datos de clave de cifrado 120
Búfer 116
Datos de sensor 122
Datos de clave temporal 123
Módulo de recopilación de datos 103
Elemento de detección 105
Módulo de interfaz de dispositivo 106
Transmisor 124
Receptor 126

Fig. 4

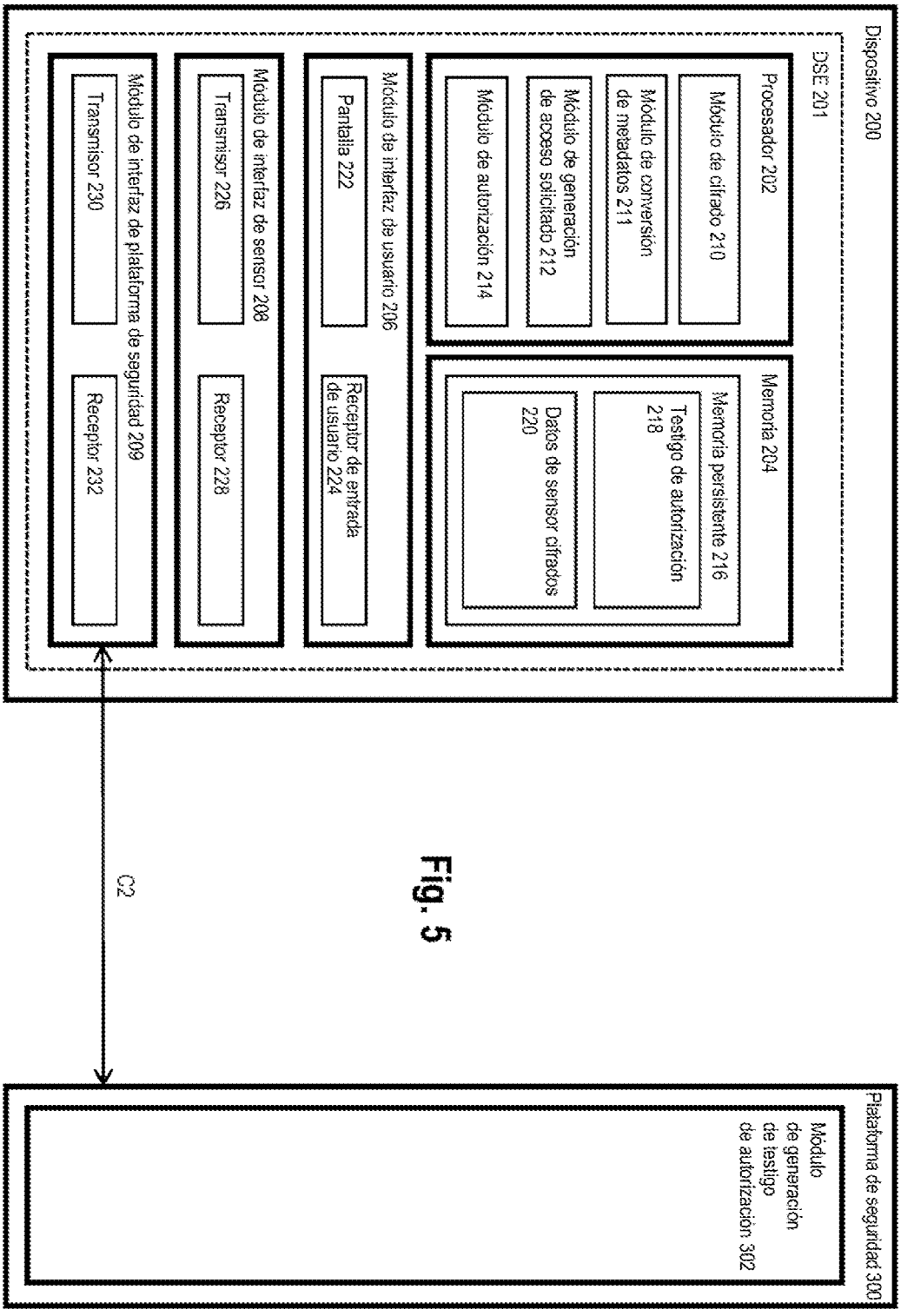
Dispositivo 200
DSE 201
Procesador 202
Módulo de cifrado 210
Módulo de conversión de metadatos 211
Módulo de generación de acceso solicitado 212
Módulo de autorización 214
Memoria 204
Memoria persistente 216
Testigo de autorización 218
Datos de sensor cifrados 220
Módulo de interfaz de usuario 206
Pantalla 222
Receptor de entrada de usuario 224
Módulo de interfaz de sensor 208
Transmisor 226
Receptor 228
Módulo de interfaz de plataforma de seguridad 209
Transmisor 230
Receptor 232
C2
Plataforma de seguridad 300
Módulo de generación de testigo de autorización 302

Fig. 5

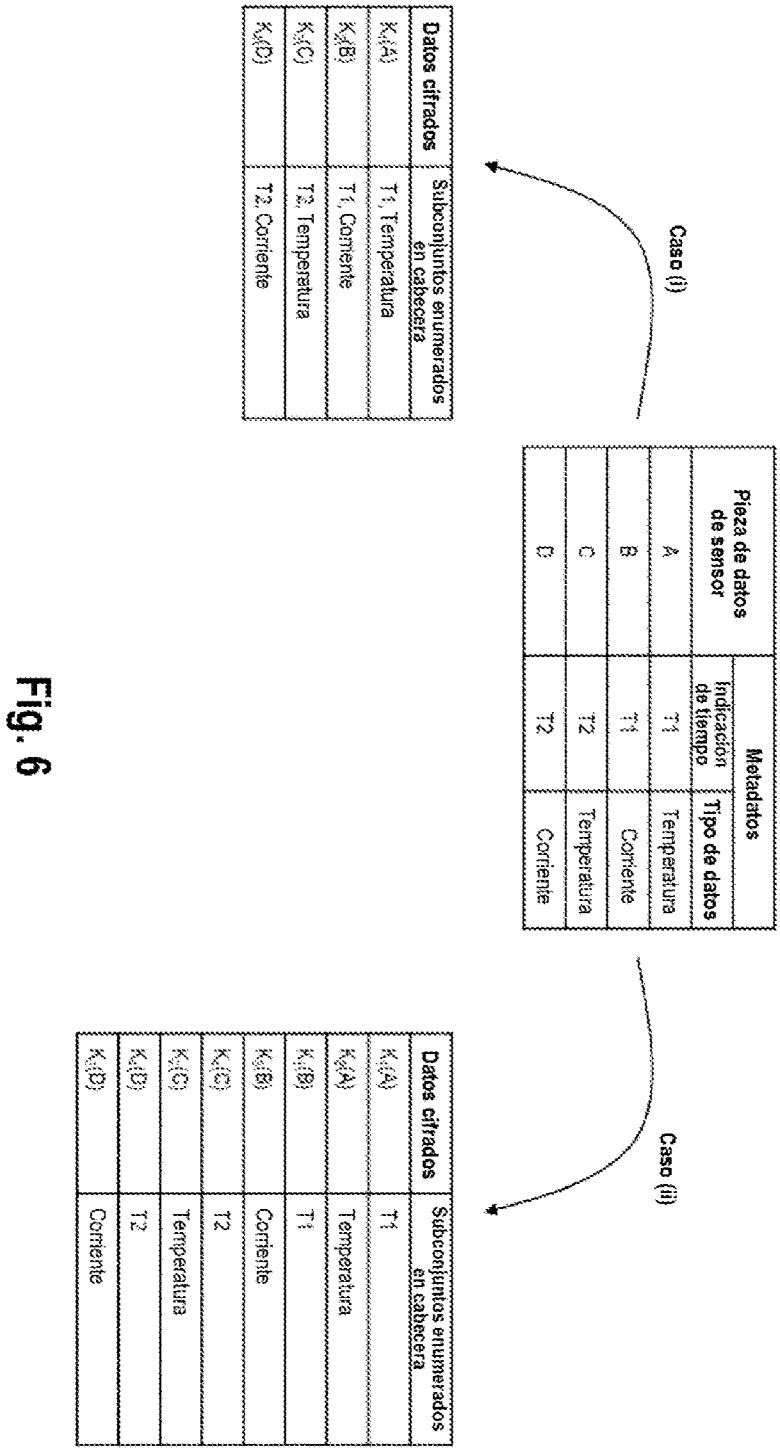
Caso (i)
Caso (ii)
Pieza de datos de sensor
Metadatos
Indicación de tiempo
Tipo de datos
A
T1
Temperatura
B
T1
Corriente
C
T2
Temperatura
D
T2
Corriente
Datos cifrados
Subconjuntos enumerados en cabecera
K1(A)
T1, Temperatura
K2(B)
T1, Corriente
K1(C)
T2, Temperatura
K2(D)
T2, Corriente
Datos cifrados
Subconjuntos enumerados en cabecera
K1(A)
T1
K2(A)
Temperatura
K1(B)
T1
K2(B)
Corriente
K1(C)
T2
K2(C)
Temperatura
K1(D)
T2
K2(D)
Corriente

Fig. 6

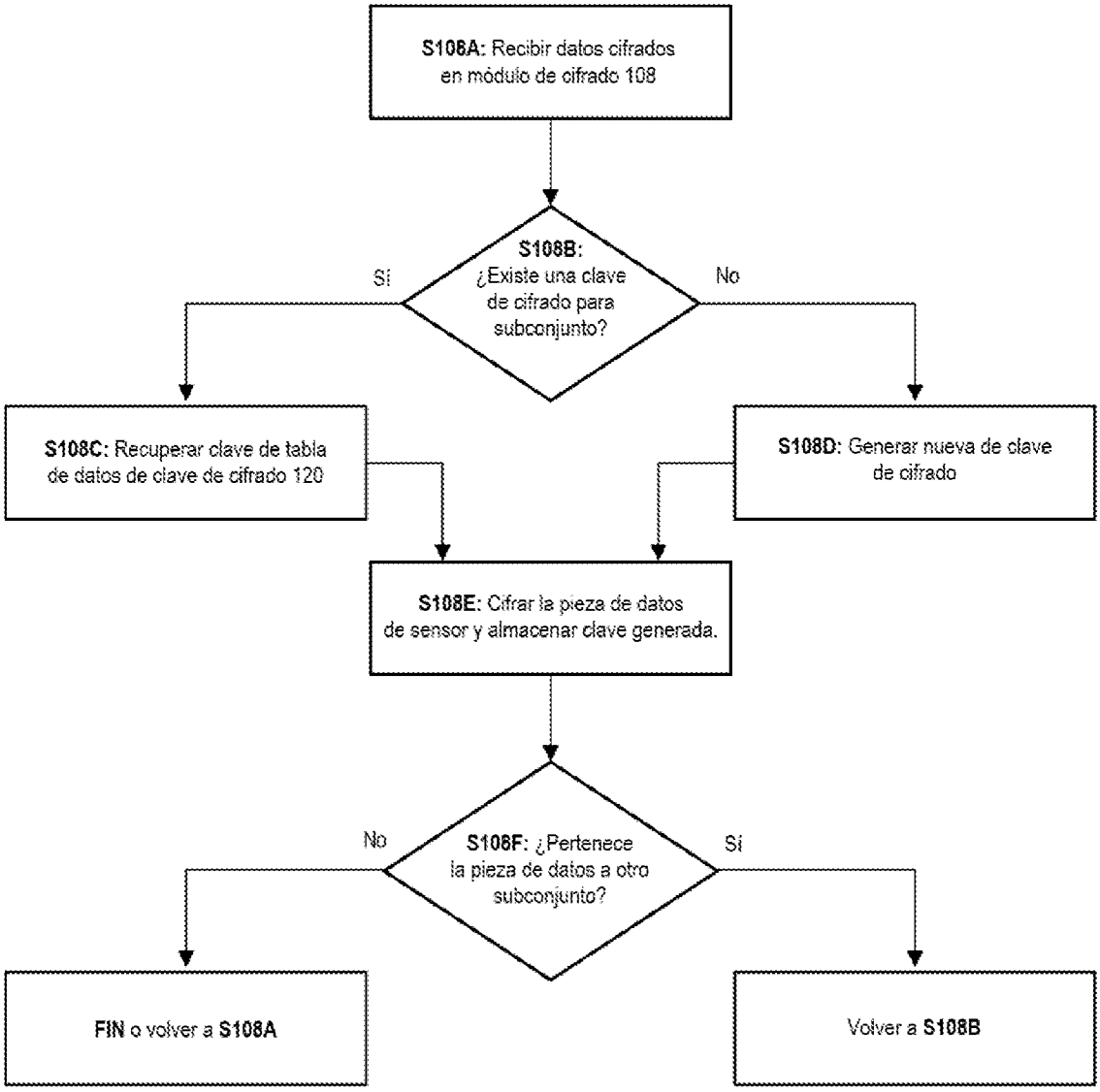
S108A: Recibir datos cifrados en módulo de cifrado 108
S108B: ¿Existe una clave de cifrado para subconjunto?
Sí
No
S108C: Recuperar clave de tabla de datos de clave de cifrado 120
S108D: Generar nueva de clave de cifrado
S108E: Cifrar la pieza de datos de sensor y almacenar clave generada.
S108F: ¿Pertenece la pieza de datos a otro subconjunto?
No
Sí
FIN o volver a S108A
Volver a S108B

Fig. 7

Clave de cifrado	ID de subconjunto
K_1	S_1
K_2	S_2
K_3	S_3
K_4	S_4

Fig. 8A

Clave de cifrado	Metadatos correspondientes	ID de subconjunto
K_1	T1	S_1
K_2	Temperatura	S_2
K_3	Corriente	S_3
K_4	T2	S_4

Fig. 8B

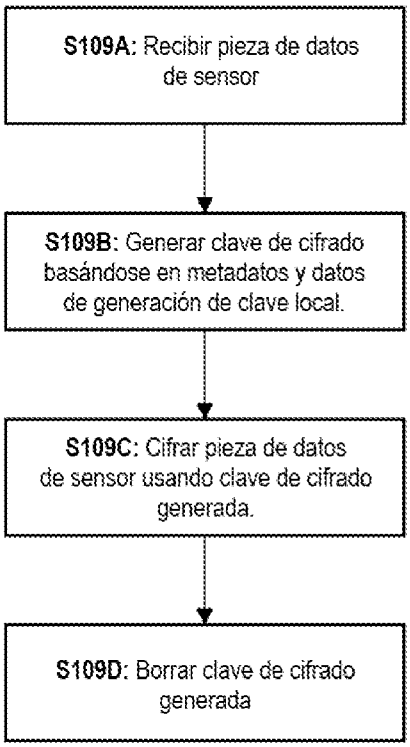
S109A: Recibir pieza de datos de sensor
S109B: Generar clave de cifrado basándose en metadatos y datos de generación de clave local.
S109C: Cifrar pieza de datos de sensor usando clave de cifrado generada.
S109D: Borrar clave de cifrado generada

Fig. 9

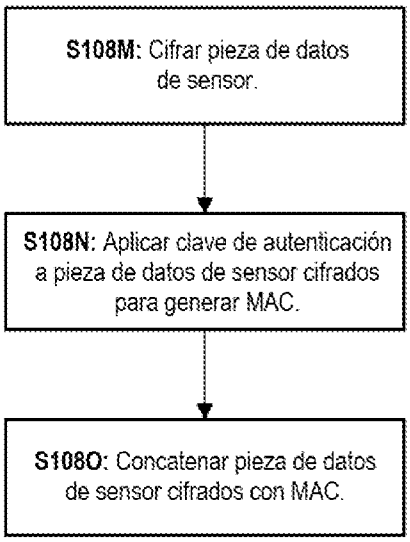
S108M: Cifrar pieza de datos de sensor.
S108N: Aplicar clave de autenticación a pieza de datos de sensor cifrados para generar MAC.
S108O: Concatenar pieza de datos de sensor cifrados con MAC.

Fig. 10

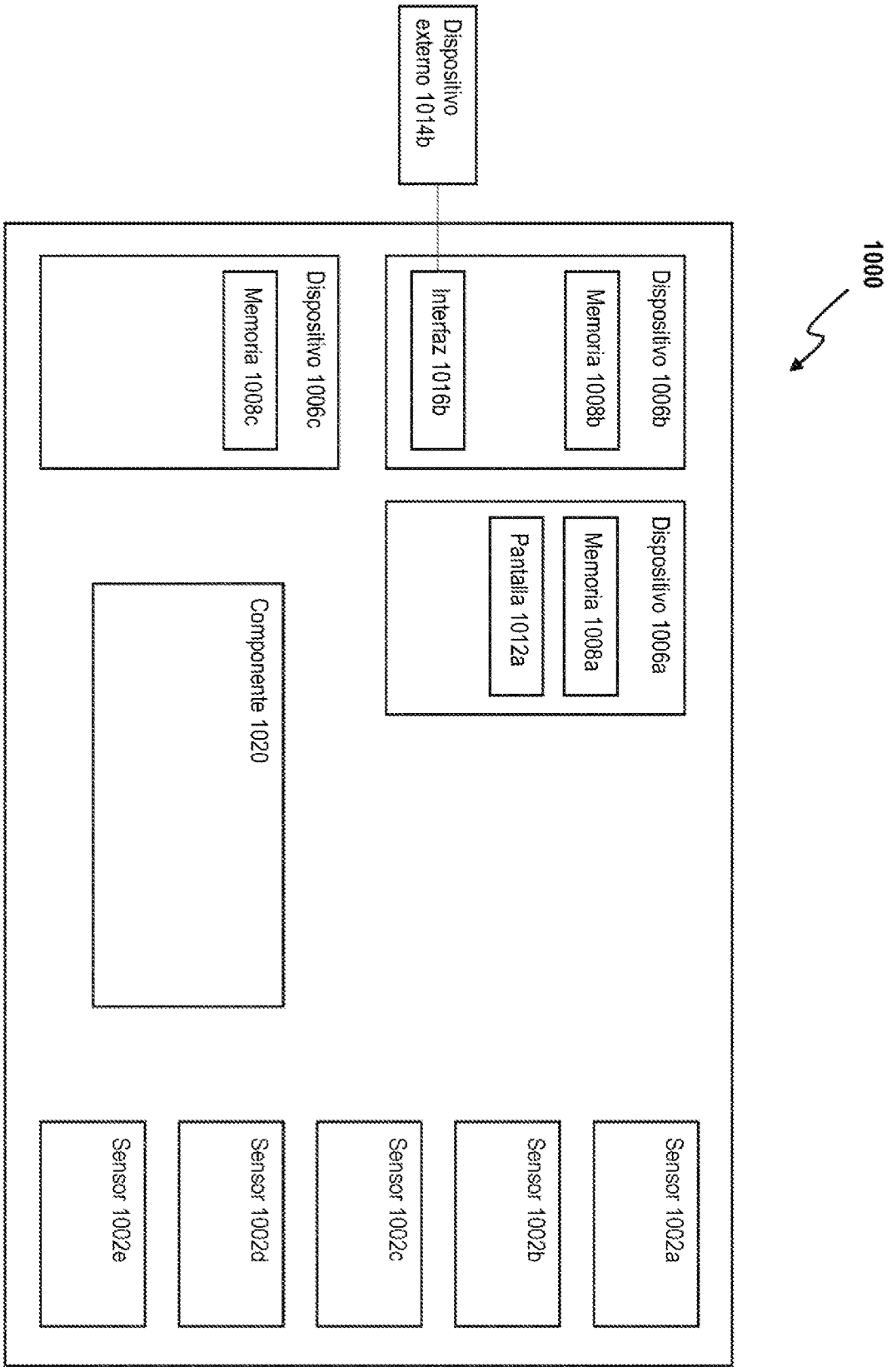
1000
Dispositivo externo 1014b
Dispositivo 1006b
Memoria 1008b
Interfaz 1016b
Dispositivo 1006a
Memoria 1008a
Pantalla 1012a
Dispositivo 1006c
Memoria 1008c
Componente 1020
Sensor 1002a
Sensor 1002b
Sensor 1002c
Sensor 1002d
Sensor 1002e

Fig. 11