(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 696 751**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.09.2015 E 15187286 (8)**

(97) Fecha y número de publicación de la concesión europea: **15.08.2018 EP 3151502**

(54) Título: **Transmisión de datos de un objeto, encriptada de diferentes modos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.01.2019

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

VERMA, AMIT

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Transmisión de datos de un objeto, encriptada de diferentes modos

La presente invención hace referencia a un sistema y a un procedimiento para la transmisión de datos de objetos de un operador del sistema mediante recolectores de datos y mediante un módulo de clasificación para la clasificación de los datos.

La presente invención se sitúa en el área de las recolecciones de datos basadas en agentes para así llamados sistemas basados en la nube y para la prestación de servicios. La invención hace referencia además al área de la así llamada "Internet of Things (IoT) (Internet de las cosas) o bien de la así llamada "Web of Systems" (WoS) (Red de sistemas). En los recolectores de datos basados en agentes, los agentes representan la interfaz entre una fuente de datos y un sistema basado en la nube. Los mismos recolectan los datos, eventualmente efectúan evaluaciones previas y envían los datos al sistema. El envío de los datos puede tener lugar de forma directa, mediante operadoras (así llamados proxys) o mediante pasarelas. Las fuentes de datos son unidades de automatización o unidades de ordenador en un entorno industrial, en particular en un sistema de automatización. Dichas unidades pueden ser controladores programables de almacenamiento, dispositivos de campo con controladores como motores, convertidores, sensores o sin embargo pueden ser también controladores en autos, instalaciones de señales luminosas, cámaras o similares. Los agentes pueden ser meros agentes de software que en ese caso están integrados directamente en los así llamados mandos o bien controladores, los cuales aprovechan su capacidad de cálculo y actúan allí como recolectores de datos. De manera alternativa, el agente puede ejecutarse también en un hardware propio que conecta entonces la fuente de datos de forma indirecta, mediante protocolos de comunicaciones (Siemens S7, Profibus, Modbus, OPC DA/UA, SOAP/XML, etc.) En cuanto a las exigencias durante el acoplamiento de la fuente de datos mediante agentes, pueden subdividirse en los siguientes tipos.

En un caso, el agente debe recolectar datos desde la fuente de datos, enviarlos al sistema basado en la nube y/o debe ser capaz de recibir señales de control desde el sistema basado en la nube, en la fuente de datos. Un ejemplo de un agente de recolección de datos y de control de esa clase podría ser un agente en un motor que en un caso de aplicación simple lee datos, por ejemplo datos de aceleración, desde sensores en el motor y envía esos datos al sistema basado en la nube con un fin analítico. Si se trata de un motor que para el sistema de automatización industrial se encuentra expuesto debido a su función y, con ello, debe ser monitoreado, el sistema basado en la nube, después de la evaluación de los datos, podría determinar una anomalía y enviar una orden de detención al agente, el cual a su vez emite una señal correspondiente para la detención del motor al controlador del motor. En otro caso, el agente se trata de un recolector de datos pasivo que solamente recolecta datos y los envía el sistema basado en la nube, el cual, con esos datos, realiza otras funciones analíticas. Esa forma de agentes no debe recibir órdenes desde el sistema basado en la nube. Usualmente, la comunicación entre agentes y un sistema de ordenador externo basado en la nube está encriptada por razones de seguridad. Un ejemplo de esa tecnología es conocido por el documento US2015/200919-A1.

La encriptación se realiza mediante protocolos de comunicaciones seguros, como por ejemplo TLS, SSL, HTTPS, etc. Eso conduce a los siguientes problemas. Por una parte, el software del agente en la mayoría de los casos se ejecuta en un hardware que posee una capacidad de rendimiento comparativamente reducida (los así llamados Pico- Controller u ordenadores de placa reducida, como Ardinao, Raspberry Pi, etc.). Las tecnologías de encriptación para todo el tráfico de datos desde el agente hacia la unidad de cálculo basada en la nube, sin embargo, implican un cálculo intensivo. Esto significa que se dispone de menos capacidad informática para otras actividades necesarias, como por ejemplo la recolección de datos y el preprocesamiento de los datos. Cuando el software de agente se ejecuta en el hardware de los dispositivos de campo, por ejemplo en un convertidor, utilizando con ello los recursos del dispositivo de campo, con frecuencia tampoco se dispone de capacidad informática suficiente, ya que el hardware de los dispositivos de campo, en cuanto a la capacidad informática, usualmente está adaptado a sus tareas originales y sólo quedan pocas reservas de potencia para esas tareas. Si los agentes están instalados en aparatos que funcionan con baterías, la capacidad informática adicional de los agentes conduce a una descarga más rápida de las baterías. Por otra parte, canales de transmisión más seguros entre el agente y la unidad de cálculo basada en la nube, en el caso de la misma velocidad de transmisión, requieren también anchos de banda comparativamente más elevados, ya que los protocolos de encriptación inician sesiones de red seguras, lo cual aumenta marcadamente el volumen de los datos que deben intercambiarse en total, a través del así llamado encabezado (por ejemplo a través de certificados). Ese balance empeora otra vez cuando la sesión de comunicación segura debe establecerse muchas veces una y otra vez, ya que precisamente el establecimiento de la comunicación produce encabezados elevados. Otros aparatos IoT pueden poseer agentes que usan canales de comunicaciones móviles (por ejemplo GSM, GPRS, EDGE, UMTS) para el intercambio de datos. En este caso, los costes pueden depender de la cantidad de los datos efectivamente transmitidos, lo cual puede conducir a que la utilización de canales de comunicaciones seguros para todos los datos que deben transmitirse sea comparativamente costosa y/o pueda ser lenta.

Usualmente, el problema se remedia de modo que se utiliza un hardware de alto rendimiento y se ponen a disposición los anchos de banda necesarios. El problema de los encabezados para una comunicación segura en aparatos IoT reducidos ya es conocido, pero no está realmente direccionado.

Partiendo de la problemática antes descrita, conforme a ello, el objeto de la invención consiste en indicar un procedimiento que garantice la seguridad requerida en la transmisión de datos, con una inversión reducida en la encriptación.

Dicho objeto se soluciona a través de un sistema con las características de la reivindicación 1 y de un procedimiento con las características de la reivindicación 7.

El sistema según la invención está configurado para la transmisión de datos de al menos un objeto y comprende una unidad de cálculo asociada al objeto. El término objeto se entiende en este contexto como componentes de campo que, mediante interfaces de entrada/salida, están conectados con un proceso industrial. Los componentes de campo reciben datos desde sensores y usualmente mediante conexiones activas pueden actuar en el proceso en cuanto al control. Sin embargo, un objeto puede ser también un dispositivo que comprende en sí mismo componentes de sensor y/o de control y que, a ese respecto, trabaja de forma autárquica. A ese objeto se encuentra asociada una unidad de cálculo local. Usualmente, la unidad de cálculo está integrada en el objeto y cada objeto presenta su propia unidad de cálculo. En otros casos, una unidad de cálculo puede estar asociada también a varios objetos. La unidad de cálculo local presenta memoria de datos, unidad de evaluación y al menos una aplicación, donde la aplicación dispone a la unidad de evaluación almacenar los datos del objeto en la memoria de datos. Los datos del objeto comprenden de este modo los así llamados datos brutos del objeto, por ejemplo datos del sensor del proceso o de la periferia del sensor. Sin embargo, los datos del objeto también pueden contener datos que pueden ser obtenidos por la aplicación desde los datos del sensor, por ejemplo variables intermedias derivadas u órdenes de control. Además, el sistema comprende un agente de software que recolecta los datos de la memoria de datos y, mediante una conexión de datos (en particular en base al protocolo de Internet), los transmite a una unidad de cálculo externa. El agente de software presenta un módulo de clasificación que clasifica los datos en datos sensibles y datos no sensibles. Los datos de la clase sensible se transmiten a la unidad de cálculo externa empleando un algoritmo de encriptación, y los datos de la clase no sensible se transmiten a la unidad de cálculo externa de forma no encriptada. La subdivisión en datos sensibles y no sensibles tiene lugar basada en reglas, donde se define una serie de reglas diferentes y éstas pueden almacenarse como instrucciones en el agente de software. Por ejemplo, un caso de monitoreo para el objeto de una máquina industrial comprende así llamada information asset (o un activo de información) como tipo de máquina, denominación de la máquina, lugar de la máquina, información de la red (direcciones) y/o datos de configuración de la máquina, etc. Además, el caso de monitoreo comprende naturalmente también datos de monitoreo, como series temporales de datos de temperatura o datos de vibración. En un caso de esa clase, la information asset podría clasificarse como datos sensibles, mientras que los datos de monitoreo se clasifican como datos no sensibles. Se excluiría entonces una asociación de los datos de monitoreo sobre el objeto aun a través de terceros y, con ello, se garantizaría el grado de seguridad necesario en la transmisión. En una instalación de producción, a su vez, datos sobre el volumen de producción (unidades producidas por unidad de tiempo) podrían ser datos sensibles, mientras que los tiempos de ciclo de la máquina en sí mismos podrían representar datos no sensibles. En una división aún más general, errores o mensajes de alerta podrían ser datos sensibles, mientras que la información normal son datos no sensibles. En otros casos de aplicación, a su vez, metadatos podrían ser datos sensibles, mientras que el resto de los datos representan ya datos no sensibles. En el monitoreo de vehículos los datos relativos al lugar pueden representar datos sensibles, mientras que los datos de velocidad correspondientes son datos no sensibles. O en el monitoreo de objetos en el ámbito de la domótica los datos relativos a identificaciones de un sensor o el tipo del sensor pueden clasificarse como datos sensibles, a diferencia de las temperaturas o los caudales medidos por el sensor.

Cuando el agente de software puede ejecutarse como otra aplicación en la unidad de cálculo local, puede accederse a los datos de la memoria de datos sin una inversión adicional con respecto al hardware. Pueden utilizarse interfaces de comunicaciones de la unidad de cálculo local.

En una variante ventajosa, el módulo de clasificación puede subdividir además los datos de la clase sensible, a saber, en clases de diferentes niveles de encriptación. De ese modo, puede producirse por ejemplo una clase que trabaja con una encriptación de 256 Bits, y otra clase que trabaja con una encriptación de 128 Bits. De este modo, los datos pueden transmitirse encriptados, donde el grado de la encriptación está adaptado al contenido y al carácter confidencial de los datos.

En otra variante, el módulo de clasificación soporta tecnologías de aprendizaje automáticas. Es decir que la clasificación automática se basa en tecnología de aprendizaje automática de esa clase. De este modo, el módulo de clasificación aprende en la evaluación si los datos se tratan de datos sensibles o no sensibles debido a ejemplos o bien a objetos de entrenamiento, y después de una fase de aprendizaje puede efectuar generalizaciones extrayendo regularidades determinadas desde los datos de aprendizaje, las cuales entonces, aplicadas en futuros datos, permiten una clasificación de los datos. Las tecnologías de aprendizaje de esa clase se conocen en otras áreas con denominaciones como árboles de decisión (decision tree), método de vector soporte SVM, máquina de vector de

soporte) o redes neuronales. Las mismas pueden estar implementadas como aprendizaje monitoreado o como aprendizaje no monitoreado.

El objeto se soluciona además a través de un procedimiento para la transmisión de datos de un objeto hacia una unidad de cálculo externa desde una unidad de cálculo local asociada al objeto, mediante un agente de software que recolecta los datos del objeto dentro de la unidad de cálculo local y los transmite a la unidad de cálculo externa mediante Internet. El agente de software divide los datos del objeto según datos sensitivos y datos no sensitivos, y transmite los datos sensibles de forma encriptada a la unidad de cálculo externa. Los datos no sensibles se transmiten de forma no encriptada desde el agente de software hacia la unidad de cálculo externa.

En otro paso del procedimiento, el agente de software subdivide los datos sensitivos del objeto. Además, transmite los datos sensitivos con diferentes niveles de encriptación.

Las propiedades, características y ventajas descritas de la invención, así como el modo en que se alcanzan, se explican en detalle con relación a las figuras. En una representación esquemática, las figuras muestran:

Figura 1: un sistema compuesto por varias unidades de ordenador para el análisis de objetos en una unidad de ordenador basada en la nube;

Figura 2: el funcionamiento de agentes y del módulo de clasificación.

La figura 1 muestra un sistema 100 para el análisis de objetos 1a a 1d. Los objetos se tratan de componentes de automatización en el plano de control y de campo, tal como se conocen por ejemplo en la automatización industrial. El objeto 1a muestra un motor 4 activado por un convertidor 2 mediante las líneas de control 3. El objeto 1b se trata de un controlador programable de almacenamiento 5, el cual, del modo convencional, está conectado mediante entradas/salidas digitales/analógicas 6, con una periferia del proceso 7. En otra variante, el objeto 1c muestra un dispositivo de campo inteligente 8, y el objeto 1d muestra un motor 9 inteligente, controlado de forma directa. Los objetos, mediante una red de comunicaciones local 10, están conectados en este ejemplo con un controlador 11 de orden superior que ejecuta funciones de control y de monitoreo. Los objetos 1a a 1d proporcionan datos del objeto 22 que se tratan tanto de datos del objeto internos (formados, calculados dentro del objeto), así como de datos del objeto externos (datos de estado provenientes del nivel del proceso 101). A los objetos se encuentran asociadas unidades de ordenador 12 que efectúan el procesamiento de los datos de objetos, las cuales monitorean, controlan o regulan los objetos. Para ello, las unidades de ordenador 12 están provistas de al menos una unidad de evaluación 13, de memorias de datos 14 y de aplicaciones 15. Mediante la conexión de datos 16, unidades de cálculo 12 de los objetos están conectadas a una unidad de ordenador 17, externa con respecto a la instalación, e intercambian datos con la misma. La conexión de datos 16, preferentemente, se realiza mediante Internet. Los objetos, como se muestra en la figura 1, son del mismo operador del sistema, pero también diferentes operadores del sistema, mediante Internet, pueden estar conectados a la unidad de ordenador 17, y enviar datos del objeto a la misma. La unidad de ordenador 17 presenta una unidad de evaluación 18 y memorias de datos 19. Las aplicaciones 10 desarrollan el procesamiento de los datos del objeto con la ayuda del dispositivo de evaluación 18 y de las memorias de datos 19. Las aplicaciones 10 pueden mostrar funciones de control y de regulación más complejas (por ejemplo en simulaciones), o análisis, revisión del historial, monitoreo de condición, etc. Un agente de software 25 - cuya función se describe en detalle en la figura 2, se utiliza como recolector de datos, y recolecta y transmite los datos del objeto 22 a la unidad de ordenador 17.

La figura 2 muestra esquemáticamente el manejo de los datos en las unidades de ordenador 12 y 17. De este modo, a la memoria de datos 14 se transfieren datos del objeto 22, desde el objeto 1 (1a, 1b, 1c o 1d), como fuente de datos. Dichos datos pueden ser todos datos del objeto internos, como por ejemplo corrientes o tensiones de un motor conectado o tensiones o corrientes del circuito intermedio del convertidor que opera el motor; variables del valor objetivo calculadas internamente para los objetos (a este respecto, también resultados 24). Dichos datos, sin embargo, pueden ser también datos de sensor, de sensores o actuadores externos, con respecto al objeto y/o al proceso controlado y/o monitoreado por el objeto. Dependiendo de la forma de ejecución, los datos del objeto pueden transmitirse a la memoria de datos 14 de forma continua, periódica, controlada temporalmente o controlada por eventos. La memoria de datos 14 interactúa con la unidad de evaluación 13. La unidad de evaluación 13 tiene acceso a la memoria de datos 14 y puede requerir o solicitar datos desde la misma. La unidad de evaluación 13 puede estar realizada como combinación de hardware y software. En la variante aquí descrita, la unidad de evaluación está diseñada como unidad de ordenador independiente, separada de las memorias de datos 14. Mediante la unidad de evaluación 13 se procesan solicitudes desde distintas aplicaciones 15. Las aplicaciones 15 representan un programa instalado en la unidad de ordenador 12. Una aplicación 15 dispone a la unidad de evaluación 13 procesar datos 22 de la memoria de datos 14 según las instrucciones 23 almacenadas en la aplicación 15, y transmitir los resultados 24 de ese procesamiento a la memoria de datos 14 para la transmisión hacia el objeto 1. El objeto 1 puede ser controlado o bien influenciado mediante esos resultados. Un agente de software 25 de un operador de servicio que, según la figura 2, se desarrolla como aplicación ejecutable dentro de la unidad de ordenador 2, mediante instrucciones 26, dispone a la unidad de evaluación 13 pasar los datos del objeto

22, 24 de la memoria de datos 14, mediante la conexión de datos 16, a la unidad de ordenador 17, externa con respecto a la instalación. La unidad de ordenador 17 presenta memorias de datos 19, una unidad de evaluación 18 y aplicaciones 20. La unidad de cálculo 17 puede comprender aplicaciones de distintos operadores de servicio. La aplicación 20 indica a la unidad de evaluación 18 procesar datos 22 de la memoria de datos 19 según las instrucciones 21 almacenadas en la aplicación 20, y almacenar los resultados 27 en la memoria de datos 19. Mediante el agente 25 y la conexión de datos 16, datos de la memoria de datos 19 pueden llegar a la unidad de cálculo 12. El agente 25 presenta un módulo de clasificación 28 que divide los datos del objeto 22, 24 en datos sensibles 29 y datos no sensibles 30. Los datos sensibles 29, antes de la transmisión de los datos mediante la conexión de datos 16, son guiados mediante un algoritmo de encriptación 31 y son transmitidos de forma encriptada, mientras que los datos no sensibles 30 se transmiten de forma no encriptada mediante la conexión de datos 16.

REIVINDICACIONES

1. Sistema (100) para transmitir datos (22, 24) de un objeto (1, 1a, 1b, 1c, 1d), el cual comprende

- una unidad de cálculo local (12) asociada al objeto, la cual presenta memoria de datos (14), unidad de evaluación (13) y al menos una aplicación (15), donde la aplicación dispone a la unidad de evaluación almacenar los datos del objeto en la memoria de datos, y

- un agente de software (25) que recolecta los datos de la memoria de datos y, mediante una conexión de datos (16), los transmite a una unidad de cálculo externa (17),

caracterizado porque el objeto se trata de un componente de automatización en el plano de control o de campo y el objeto proporciona datos del objeto internos, así como externos, donde los datos del objeto internos se calculan dentro del objeto y los datos del objeto externos son datos de estado provenientes del plano del proceso, y el agente de software (25) presenta un módulo de clasificación (28) que clasifica los datos (22, 24) en datos sensibles (29) y datos no sensibles (30), donde los datos de la clase sensible, empleando un algoritmo de encriptación (31), se transmiten a la unidad de cálculo externa y los datos de la clase no sensible se transmiten de forma no encriptada a la unidad de cálculo externa.

2. Sistema según la reivindicación 1, caracterizado porque el agente de software (25) se ejecuta como otra aplicación en la unidad de cálculo local.

3. Sistema según la reivindicación 1, caracterizado porque el agente de software (25) se ejecuta en un hardware propio, conectado mediante tecnología de comunicaciones a la unidad de cálculo local en una red de comunicaciones local.

4. Sistema según la reivindicación 2 ó 3, caracterizado porque el módulo de clasificación (28) subdivide además los datos sensibles (29) en clases de diferentes niveles de encriptación.

5. Sistema según la reivindicación 2 ó 3, caracterizado porque el módulo de clasificación (28) soporta tecnologías de aprendizaje automáticas.

6. Sistema según la reivindicación 5, caracterizado porque la tecnología de aprendizaje automática presenta un árbol de decisión, una máquina de vector de soporte o una red neuronal.

7. Procedimiento para transmitir datos (22, 24) de un objeto (1, 1a, 1b, 1c, 1d) a una unidad de cálculo externa (17) desde una unidad de cálculo local (12) asociada al objeto, mediante un agente de software (25) que recolecta los datos desde el objeto dentro de la unidad de cálculo local y, mediante una conexión de datos (16), los transmite a la unidad de cálculo externa, donde el objeto se trata de un componente de automatización en el plano de control y de campo, donde dicho objeto proporciona datos del objeto (22) internos, así como externos, donde los datos del objeto internos se calculan dentro del objeto y los datos del objeto externos son datos de estado provenientes del plano del proceso (101), en el cual:

a) el agente de software divide los datos del objeto según datos sensibles (29) y datos no sensibles (30),

b) el agente de software transmite los datos sensibles (29) de forma encriptada a la unidad de cálculo externa,

b) el agente de software transmite los datos no sensibles (30) de forma no encriptada a la unidad de cálculo externa.

8. Procedimiento según la reivindicación 7, caracterizado porque el agente de software (25) subdivide además los datos sensibles (29) del objeto (1, 1a, 1b, 1c, 1d) y transmite los datos sensibles (29) con diferentes niveles de encriptación.

9. Procedimiento según la reivindicación 6, caracterizado porque la división según el paso a) se basa en tecnologías de aprendizaje automáticas.

FIG 1

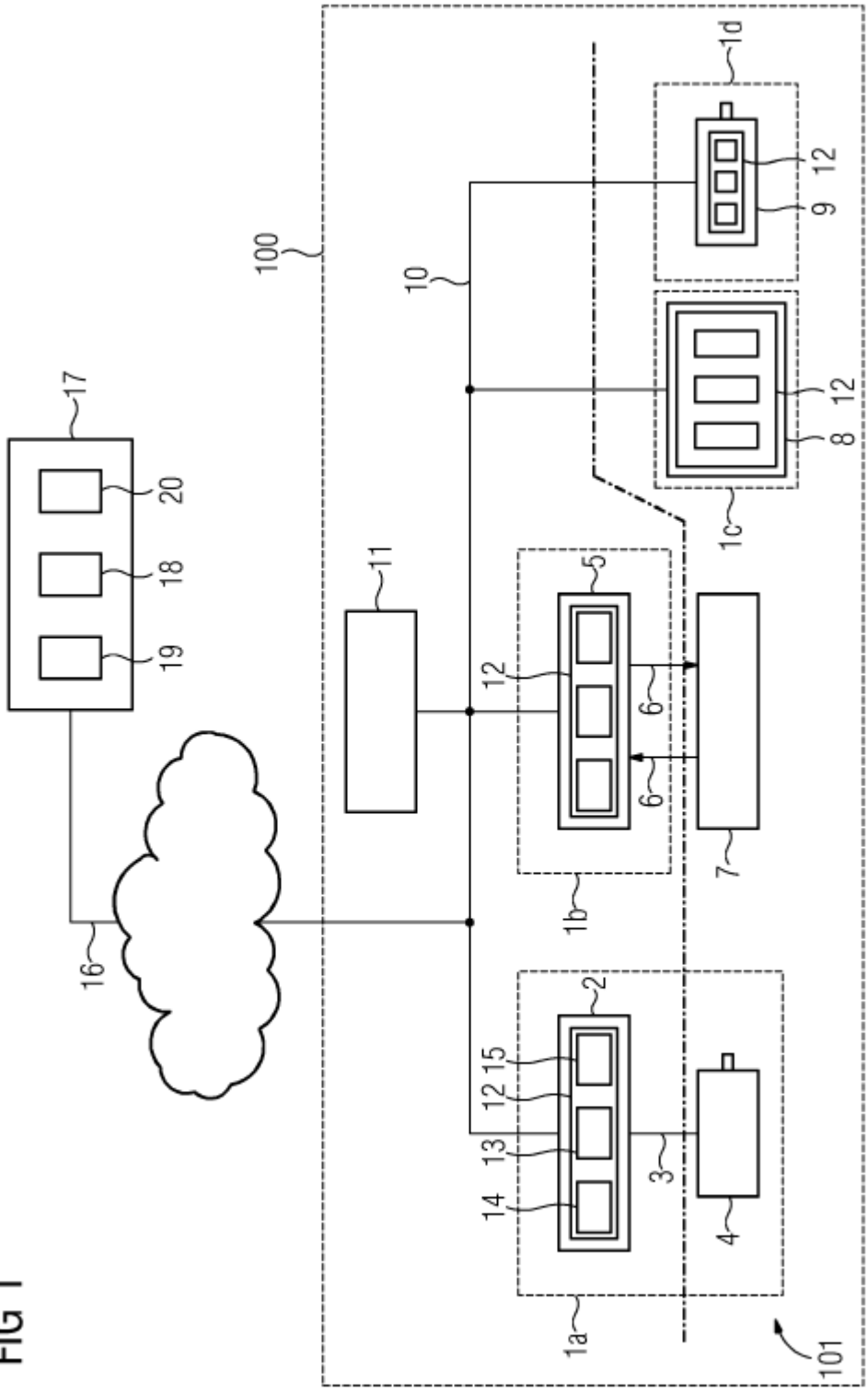
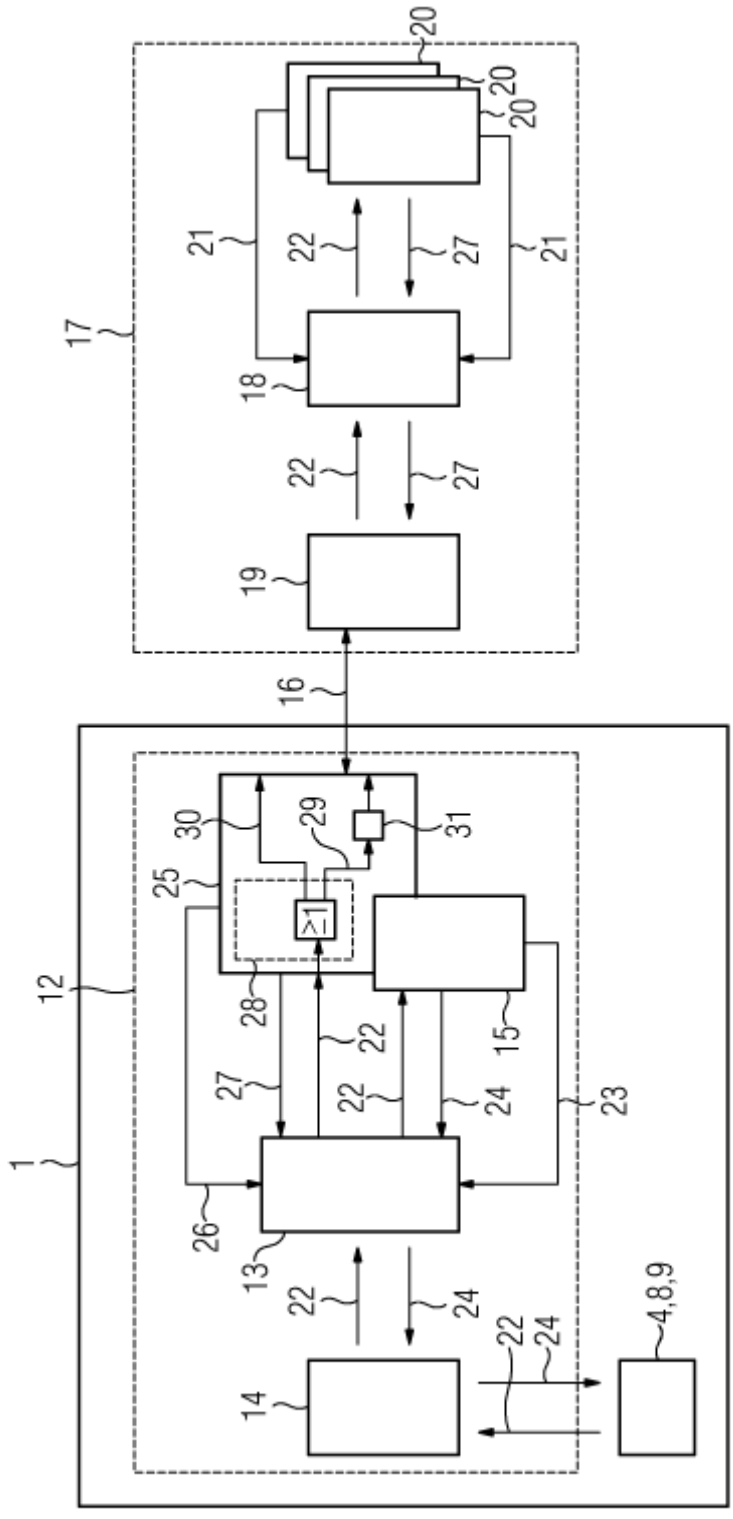


FIG 2


20
20
20
21
22
27
21
17
18
22
27
19
16
1
12
30
29
31
25
≥1
28
22
15
27
22
24
23
26
13
22
24
22
24
4,8,9
14