(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 489**

(51) Int. CI.:

G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.10.2016 PCT/US2016/055974**

(87) Fecha y número de publicación internacional: **30.11.2017 WO17204846**

(96) Fecha de presentación y número de la solicitud europea: **07.10.2016 E 16785299 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3465524**

(54) Título: **Transmisión segura de datos sensibles**

(30) Prioridad:

27.05.2016 US 201662342491 P
27.05.2016 US 201662342490 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2021

(73) Titular/es:

CHARTER COMMUNICATIONS OPERATING LLC (100.0%)
12405 Powerscourt Drive
St. Louis, Missouri 63131, US

(72) Inventor/es:

CARLSON, JAY, ERIC;
COPELAND, RODNEY, ALLEN;
HANRAHAN, MICHAEL, DAVID y
ALCOTT, CHRISTOPHER, SCOTT

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Transmisión segura de datos sensibles

Referencia cruzada a solicitudes relacionadas

El presente documento reivindica el beneficio de la solicitud de patente estadounidense provisional n.º 62/342.490, presentada el 27 de mayo de 2016 y titulado “Secure Collection of Sensitive Data”, y de la solicitud de patente estadounidense provisional n.º 62/342.491, presentada el 27 de mayo de 2016 y titulado “Secure Transmission of Sensitive Data”.

Campo técnico

La presente divulgación se refiere a la seguridad de datos. En particular, la divulgación se refiere a sistemas y métodos para recopilar, enviar y/o almacenar de manera segura datos sensibles (por ejemplo, confidenciales) o potencialmente sensibles.

Antecedentes

Actualmente, muchas técnicas de codificación diferentes están diseñadas para impedir el acceso no autorizado a datos comunicados y/o almacenados. Sin embargo, estas técnicas están asociadas con diversos inconvenientes. Por ejemplo, estas técnicas no protegen, en general, ni ofuscan los datos sensibles de una manera de extremo a extremo (por ejemplo, comenzando en el momento en que un individuo introduce manualmente la información usando un teclado). Además, algunos usan un enfoque generalizado en el que, si el código se “rompe” con respecto a una transmisión, el código también puede verse comprometido para transmisiones futuras y/o con respecto a transmisiones entre otras partes o dispositivos. Todavía más, algunos no proporcionan la flexibilidad para personalizar el nivel de seguridad a diferentes entidades (por ejemplo, diferentes empresas, personas, dispositivos, etc.), o la flexibilidad para responder a amenazas de seguridad (por ejemplo, violaciones de datos) de manera precisa o enfocada.

El documento WO 2016/064888 A1 aborda el problema de garantizar la funcionalidad y la seguridad de los datos sensibles en un entorno distribuido de modo que se garantice el acceso de las diferentes entidades a los datos mientras se mantiene la seguridad de los datos sensibles.

Sumario

La presente invención se define mediante las reivindicaciones independientes adjuntas. En una realización, se implementa un método para proporcionar una comunicación segura de una cadena de datos a lo largo de un trayecto de comunicación que incluye una pluralidad de dispositivos, en un servidor que incluye uno o más procesadores y una memoria que almacena una base de datos de registro. El método incluye añadir a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad, añadir a la base de datos de registro una segunda entidad y un segundo identificador asociado con la segunda entidad, y proporcionar a un primer dispositivo de la pluralidad de dispositivos, a través de un primer canal de comunicación seguro, un primer valor actual del primer identificador para permitir una primera codificación de la cadena de datos. El primer dispositivo está asociado con la primera entidad, y la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas. El método también incluye proporcionar a un segundo dispositivo de la pluralidad de dispositivos, a través de un segundo canal de comunicación seguro, un primer valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos. El segundo dispositivo está asociado con la segunda entidad y aguas abajo del primer dispositivo en el trayecto de comunicación, y la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas. El método también incluye proporcionar a un tercer dispositivo de la pluralidad de dispositivos, a través de un tercer canal de comunicación seguro, el primer valor actual del primer identificador y el primer valor actual del segundo identificador para permitir la decodificación de la cadena de datos. El tercer dispositivo está aguas abajo del segundo dispositivo en el trayecto de comunicación.

En otra realización, se implementa un método para proporcionar comunicación segura de una cadena de datos en un servidor que incluye uno o más procesadores y una memoria que almacena una base de datos de registro. El método incluye añadir a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad, añadir a la base de datos de registro una segunda entidad y un segundo identificador asociado con la segunda entidad, proporcionar a un dispositivo de origen asociado con la primera entidad y la segunda entidad, a través de un primer canal de comunicación seguro, tanto (i) un primer valor actual del primer identificador para permitir una primera codificación de la cadena de datos, en el que la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas, como (ii) un primer valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos, en el que la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas. El método también incluye proporcionar a un dispositivo de destino, a través de un segundo canal de comunicación seguro, el primer

valor actual del primer identificador y el primer valor actual del segundo identificador para permitir la decodificación de la cadena de datos.

En otra realización, un método, implementado en un dispositivo electrónico que tiene uno o más procesadores, una interfaz de comunicación y una memoria, incluye obtener, por el uno o más procesadores, una cadena de datos codificada y recibir, por el uno o más procesadores a través de la interfaz de comunicación y un canal de comunicación seguro, los valores actuales de *N* identificadores desde un servidor remoto. Cada uno de los *N* identificadores (i) está asociado con una entidad respectiva de una pluralidad de entidades, estando asociada cada una de la pluralidad de entidades con la comunicación de la cadena de datos codificada, y (ii) corresponde a una operación respectiva de *N* operaciones de decodificación Cada una de las *N* operaciones de decodificación funciona en bloques de bits que tienen un tamaño de bloque respectivo, y *N* es un número entero mayor de 1. El método también incluye determinar, por el uno o más procesadores, una secuencia en la que las *N* operaciones de decodificación van a aplicarse a la cadena de datos codificada y generar, por el uno o más procesadores, una cadena de datos decodificada realizando las *N* operaciones de decodificación en la cadena de datos codificada según la secuencia determinada. Realizar las *N* operaciones de decodificación incluye, para cada operación de decodificación de las *N* operaciones de decodificación, (i) analizar al menos una parte de la cadena de datos codificada, o al menos una parte de una cadena de datos parcialmente decodificada resultante de una operación previa de las *N* operaciones de decodificación, en bloques que tienen el tamaño de bloque respectivo, (ii) decodificar por separado cada uno de los bloques que tienen el tamaño de bloque respectivo, y (iii) para las primeras *N* - 1 operaciones de decodificación, hacer pasar una cadena de los bloques decodificados por separado a la siguiente operación de las *N* operaciones de decodificación El método también incluye hacer, por el uno o más procesadores, que la cadena de datos decodificada uno o ambos de (i) se almacena en la memoria y (ii) se transmite a otro dispositivo.

En otra realización, un servidor incluye una primera memoria que almacena una base de datos de registro, una segunda memoria que almacena instrucciones, y uno o más procesadores. El uno o más procesadores están configurados para ejecutar las instrucciones para añadir a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad, añadir a la base de datos de registro una segunda entidad y un segundo identificador asociado con la segunda entidad, y proporcionar a un primer dispositivo de una pluralidad de dispositivos en un trayecto de comunicación para una cadena de datos, a través de un primer canal de comunicación seguro, un primer valor actual del primer identificador para permitir una primera codificación de la cadena de datos. El primer dispositivo está asociado con la primera entidad, y la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas. El uno o más procesadores también están configurados para proporcionar a un segundo dispositivo de la pluralidad de dispositivos, a través de un segundo canal de comunicación seguro, un primer valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos. El segundo dispositivo está asociado con la segunda entidad y aguas abajo del primer dispositivo en el trayecto de comunicación, y la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas. El uno o más procesadores también están configurados para proporcionar a un tercer dispositivo de la pluralidad de dispositivos, a través de un tercer canal de comunicación seguro, el primer valor actual del primer identificador y el primer valor actual del segundo identificador para permitir la decodificación de la cadena de datos. El tercer dispositivo está aguas abajo del segundo dispositivo en el trayecto de comunicación.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques de un sistema de ejemplo en el que pueden implementarse aspectos de la presente divulgación, según una realización.

La figura 2 es un diagrama de bloques de un dispositivo de origen de ejemplo, según una realización.

La figura 3 muestra un mapeo de ejemplo que puede usarse para ofuscar información de entrada por teclado, según una realización y situación.

La figura 4 muestra un conjunto de ejemplos de capas de mapeo que pueden usarse para ofuscar información de entrada por teclado, según una realización y situación.

La figura 5 representa un trayecto de comunicación de ejemplo para una cadena de datos en el que la cadena de datos puede codificarse, según una realización.

La figura 6 muestra un ejemplo de interfaz de usuario que puede presentarse a un usuario para seleccionar un código de autorización, según una realización y situación.

La figura 7 representa un entorno de ejemplo en el que pueden implementarse aspectos de la presente divulgación mientras se lleva a cabo una transacción de tarjeta de compra de crédito o débito, según una realización y situación.

La figura 8 es un diagrama de flujo de un método de ejemplo para recopilar de manera segura información sensible, según una realización.

La figura 9 es un diagrama de flujo de un método de ejemplo, método de ejemplo para proporcionar una comunicación segura de una cadena de datos a lo largo de un trayecto de comunicación que incluye una pluralidad de dispositivos, según una realización.

La figura 10 es un diagrama de flujo de un método de ejemplo para decodificar una cadena de datos transmitida de manera segura, según una realización.

Descripción detallada

Diversos aspectos de la presente divulgación proporcionan sistemas y métodos para ofuscar datos sensibles o potencialmente sensibles (por ejemplo, tarjeta de crédito u otra información financiera, información sanitaria, contraseñas, números de la seguridad social, etc.) durante el transcurso de una transacción. Tal como se usa en el presente documento, una “transacción” puede referirse a cualquier interacción u operación que implique introducir, recopilar y/o comunicar información. Así, por ejemplo, una transacción puede involucrar a un empleado de un minorista que introduce el número de tarjeta de crédito de un cliente en un teclado (por ejemplo, una pantalla táctil de un teléfono inteligente o una tableta, o un teclado de hardware, etc.) y transmitir información codificada correspondiente al número de tarjeta de crédito a un proveedor de pago (o almacenar la información codificada en una base de datos local, etc.). Como otro ejemplo, una transacción puede implicar que un paciente introduzca las respuestas a una encuesta o un cuestionario médico en un teclado y se transmita información codificada correspondiente a las respuestas del paciente a un servidor remoto. Como aún otro ejemplo, una transacción puede involucrar a un empleado administrativo de una empresa que envía registros contables confidenciales a otro empleado o departamento dentro de la empresa. Por supuesto, también son posibles otros tipos innumerables de transacciones que involucran información sensible o potencialmente sensible.

Algunos aspectos de la presente divulgación pueden requerir el registro previo de diversas entidades con un organismo coordinador. Tal como se usa en el presente documento, una “entidad” puede ser cualquier objeto físico o virtual que puede estar involucrado directa o tangencialmente en una transacción, tal como una empresa o institución (por ejemplo, minorista, hospital, banco, empresa de tarjetas de crédito, agencia gubernamental, etc.), un departamento, una persona (por ejemplo, un cliente particular, un empleado o agente particular, etc.), una tarjeta de crédito o débito específica, una aplicación de software, un encaminador (*router*), un conmutador de red, un cortafuegos (*firewall*), etc. Una vez que se registra una entidad particular, un servidor central puede mantener un identificador, o varios identificadores, asociado con esa entidad en un registro. Tal como se comentará con mayor detalle a continuación, el valor de cada identificador puede corresponder a un esquema de codificación/decodificación particular. Por ejemplo, un esquema de codificación puede codificar cadenas de datos analizando la cadena de datos en bloques de 32 bits, y usando un mapeo predeterminado para codificar cada bloque de 32 bits en un nuevo bloque de 32 bits. Un esquema de codificación diferente puede codificar cadenas de datos analizando la cadena de datos en bloques de 8 bits, y usando un mapeo predeterminado para codificar cada bloque de 8 bits en un nuevo bloque de 16 bits, y así sucesivamente. Cada esquema de codificación puede realizar un mapeo completamente predeterminado de secuencias de bits, o puede ser más complejo (por ejemplo, usando el tiempo actual para aleatorizar adicionalmente la secuencia de bits codificada, etc.). Para disminuir el riesgo de que un identificador lo descubra una parte no autorizada, el servidor central puede cambiar los valores de los identificadores almacenados en el registro de vez en cuando (por ejemplo, periódicamente y/o previa petición).

Algunos aspectos de la presente divulgación permiten que se ofusquen datos sensibles en el momento en que los datos se introducen manualmente usando una interfaz de teclado físico o virtual de un dispositivo electrónico. En general, esto puede lograrse mapeando cada entrada por teclado a una coordenada en un espacio virtual. Las coordenadas de espacio virtual, en lugar de otras representaciones más fáciles de determinar de las entradas por teclado (por ejemplo, símbolos ASCII), pueden almacenarse, procesarse adicionalmente, transmitirse, etc. El mapeo de cada entrada por teclado a una coordenada de espacio virtual puede estar dictado, en cualquier tiempo dado, por el valor actual de un identificador de una entidad registrada que está asociada con la transacción de alguna manera (por ejemplo, una empresa, un agente/empleado, un dispositivo de teclado, etc.). En algunas realizaciones y situaciones, pueden usarse múltiples identificadores (por ejemplo, 2, 5, 10, 100, etc.), correspondientes a múltiples capas de mapeo, para ofuscar adicionalmente la información de entrada por teclado de un usuario. Los identificadores pueden incluir identificadores de múltiples entidades (por ejemplo, uno para una empresa, uno para un agente que introduce la información, etc.) y/o múltiples identificadores de una única entidad. El dispositivo electrónico puede solicitar el/los identificador(es) apropiado(s) del servidor central según sea necesario a través de un canal de comunicación seguro (por ejemplo, usando técnicas de cifrado y autenticación del estado de la técnica), por ejemplo. Tal como se indicó anteriormente, el servidor central puede cambiar/actualizar cada identificador de la manera deseada. Si se usan múltiples identificadores, por ejemplo, uno o más de esos identificadores pueden cambiarse con la frecuencia suficiente para que el/los mapeo(s) correspondiente(s) cambien de una entrada por teclado a la siguiente.

Más generalmente, pueden aplicarse secuencialmente varias etapas de codificador para codificar una cadena de datos que se comunica durante una transacción. En la descripción anterior relacionada con la ofuscación de información de entrada por teclado, por ejemplo, cada “capa” (es decir, cada mapeo a un conjunto diferente de coordenadas virtuales) puede corresponder a una etapa de codificación particular. Sin embargo, en algunas realizaciones y situaciones, al menos algunas etapas de codificación las aplican otros dispositivos en el trayecto de

comunicación. Por ejemplo, puede aplicarse un primer conjunto de cuatro etapas de codificación secuencialmente por un dispositivo electrónico que se usó inicialmente para introducir información, puede aplicarse una quinta etapa de codificación por un encaminador en el trayecto de comunicación (por ejemplo, usando un identificador para el encaminador) y puede aplicarse una sexta etapa de codificación por un servidor de red aguas abajo del encaminador en el trayecto de comunicación (por ejemplo, usando un identificador para un cortafuegos implementado por el servidor), etc.

Cada etapa de codificación en la secuencia puede corresponder a un tamaño de bloque de salida específico. Por ejemplo, una etapa de codificación con un tamaño de bloque de salida de 16 puede analizar una cadena de datos de entrada en bloques de entrada de 16 bits cada uno, y luego codificar esos bloques de entrada para generar bloques de salida de 16 bits. Generalmente, diferentes etapas de codificación pueden tener diferentes tamaños de bloque de salida, y los tamaños de bloque de entrada no tienen que (pero pueden) coincidir con los tamaños de bloque de salida. Preferiblemente, sin embargo, el tamaño de bloque de salida es al menos tan grande como el tamaño de bloque de entrada para evitar posibles colisiones (es decir, situaciones en las que dos secuencias de bits diferentes se mapean a la misma secuencia de bits de salida).

Para decodificar la cadena de datos (por ejemplo, en un dispositivo electrónico de una entidad que recibe la comunicación), se aplica la operación inversa de cada etapa de codificación. Además, para decodificar apropiadamente la cadena de datos, las etapas de decodificación se aplican en el orden inverso en relación con las etapas de codificación correspondientes. Por ejemplo, la operación inversa de la última etapa de codificación se usa como la primera etapa de decodificación, y la operación inversa de la primera etapa de codificación se usa como la última etapa de decodificación. Si el proceso de codificación incluye el mapeo de entradas por teclado a la coordenada de espacio virtual como una etapa inicial, el de recepción de la cadena de datos codificada puede revertir ese proceso de codificación en la etapa de decodificación final para llegar a los datos introducidos/tecleados originariamente.

Para determinar las operaciones de decodificación apropiadas, el dispositivo electrónico que recibe la cadena de datos codificada puede solicitar, u obtener de otro modo, los valores de identificador apropiados del servidor central a través de un canal de comunicación seguro (por ejemplo, usando técnicas de cifrado y autenticación del estado de la técnica). El servidor central también puede enviar al dispositivo de recepción información relacionada con la secuencia en la que se producirán las diferentes operaciones de decodificación. En otras realizaciones, el dispositivo de recepción conoce la secuencia *a priori*, y sólo obtiene los valores de identificador actuales del servidor central.

Estos y otros aspectos de la presente divulgación resultarán evidentes a partir de la descripción que sigue.

I. SISTEMA A MODO DE EJEMPLO

Los componentes a modo de ejemplo que pueden implementar diversos aspectos de la invención se describirán en primer lugar en relación con las figuras 1 y 2. Haciendo referencia en primer lugar a la figura 1, un sistema 100 de ejemplo corresponde a una situación en la que se transmite información sensible o potencialmente sensible desde un dispositivo de origen 102 a un dispositivo de destino 104 a través de una red 106. En general, el dispositivo de origen 102 puede ser cualquier tipo de dispositivo electrónico adecuado que permita la entrada de datos y pueda transmitir datos (por ejemplo, un dispositivo de teclado dedicado, un teléfono inteligente (*smartphone*), una tableta, un ordenador portátil, un ordenador de escritorio, etc.), el dispositivo de destino 104 puede ser cualquier tipo de dispositivo electrónico adecuado que pueda recibir datos y permita el almacenamiento, procesamiento y/o reenvío/transmisión de datos (por ejemplo, un servidor), y la red 106 puede ser cualquier red de comunicación o combinación adecuada de redes de comunicación, tal como una o más redes de área local (LAN), una o más redes de área amplia (WAN), etc. El entorno 100 también incluye un servidor central 110 que mantiene un registro 112 de diversas entidades. El registro 112 puede incluir una base de datos almacenada en una o más memorias persistentes del servidor central 110, por ejemplo.

La figura 2 es un diagrama de bloques más detallado, aunque todavía simplificado, del dispositivo de origen 102 de la figura 1, según una realización. El dispositivo de origen 102 puede ser un dispositivo dedicado (por ejemplo, una tableta dedicada o un dispositivo de teclado de hardware), o un dispositivo de uso general (por ejemplo, un ordenador portátil, ordenador de escritorio, teléfono inteligente, tableta, etc.). Tal como se observa en la figura 2, el dispositivo de origen 102 incluye un procesador 120, una memoria 122, una interfaz de usuario 124 y una interfaz de comunicación 126. Aunque la figura 2 muestra cada uno de estos componentes dentro del recuadro individual marcado como 102, se entiende que los componentes pueden distribuirse entre múltiples alojamientos y/o dispositivos.

El procesador 120 puede ser un único procesador o incluir múltiples procesadores (por ejemplo, una CPU y una GPU), y puede ejecutar instrucciones (por ejemplo, almacenadas en la memoria 122) para realizar las diversas operaciones del dispositivo de origen 102 descrito a continuación. Por ejemplo, el procesador 120 puede ejecutar un módulo de codificación 128 para realizar las diversas operaciones de codificación descritas a continuación. La memoria 122 puede incluir una o más memorias persistentes, tales como una memoria de sólo lectura (ROM), y una o más memorias no persistentes, tales como una memoria de acceso aleatorio (RAM).

La interfaz de usuario 124 presenta un teclado físico o virtual 130. Por ejemplo, la interfaz de usuario 124 puede incluir un teclado de hardware con varias teclas físicas, así como cualquier hardware y/o firmware subyacente (por ejemplo, contactos, conmutadores, etc.) necesario para detectar entradas por teclado. Alternativamente, la interfaz de usuario 124 puede incluir una pantalla de visualización táctil, junto con cualquier hardware y/o firmware de soporte (por ejemplo, un circuito integrado de sensor táctil), y el teclado 130 puede ser un teclado virtual visualizado en la pantalla táctil. Las teclas pueden corresponder a números, letras, caracteres especiales (por ejemplo, un punto, coma, y comercial, etc.) y/u otros símbolos. El teclado 130 puede incluir teclas similares a un teclado QWERTY, por ejemplo.

En algunas realizaciones, la interfaz de usuario 124 también incluye una pantalla de visualización y/o uno o más componentes de salida (por ejemplo, audio). El/los componente(s) de salida puede(n) estar integrado(s) o no con el teclado 130. Si la interfaz de usuario 124 incluye una pantalla táctil, por ejemplo, la pantalla táctil puede presentar tanto el teclado 130 como cualquier información que se emita al usuario (por ejemplo, instrucciones para introducir información usando el teclado 130, confirmaciones de que los mensajes se han enviado con éxito, etc. En general, el procesador 120 puede detectar y actuar sobre las entradas de usuario realizadas a través del teclado 130, y puede generar información (si la hubiera) emitida al usuario a través de la interfaz de usuario 124.

La interfaz de comunicación 126 incluye hardware y/o firmware para soportar uno o más protocolos de comunicación (por ejemplo, un puerto Ethernet, una tarjeta de red de área local inalámbrica y/o uno o más de otros puertos de comunicación). En algunas realizaciones, la interfaz de comunicación 126 incluye una o más interfaces configuradas específicamente para soportar protocolos de comunicación altamente seguros (por ejemplo, protocolo de enlace, autenticación, cifrado/descifrado, etc.) así como protocolos menos seguros. Por ejemplo, la interfaz de comunicación 126 puede incluir un primer puerto para comunicarse con el servidor central 110 en un canal dedicado y seguro, y un segundo puerto para comunicarse con el dispositivo de destino 104 en un canal de uso general, menos seguro. Alternativamente, puede usarse un único puerto para ambos tipos de comunicación, pero usando un protocolo de cifrado y/o autenticación más seguro para el primero que para el segundo.

El funcionamiento del sistema 100 y el dispositivo de origen 102 se comentará con más detalle en las secciones a continuación, según diversas realizaciones. Aunque el comentario a continuación se refiere a veces a los componentes del sistema 100 y el dispositivo de origen 102, se entiende que los diversos aspectos de la invención descritos en el presente documento pueden implementarse en otros tipos de sistemas, dispositivos y/o componentes.

II. REGISTRO

En algunas realizaciones, varias entidades diferentes pueden registrarse previamente con un servicio de seguridad de datos. Tal como se indicó anteriormente, una “entidad” puede ser cualquier objeto físico o virtual que puede estar involucrado directa o tangencialmente en una transacción (por ejemplo, una empresa, institución, departamento u otra organización, una persona, una tarjeta de crédito o débito, una aplicación de software, un encaminador, un conmutador de red u otro dispositivo de red, un cortafuegos, etc.). El servicio de seguridad de datos puede proporcionarlo una empresa particular, y el proceso para registrar una entidad en particular puede incluir verificar o certificar que la entidad es lo que se supone que es, y asignar un identificador a la entidad. El identificador puede almacenarse entonces en el registro 112 del servidor central 110 en la figura 1, por ejemplo.

En algunas realizaciones y situaciones, se asignan completamente identificadores por el servicio de seguridad de datos (por ejemplo, por el servidor central 110). Alternativamente, para algunos identificadores que no cambian en una frecuencia muy alta (por ejemplo, una vez al año, ante la sospecha de robo de identidad, etc.), los identificadores pueden seleccionarse manualmente por una persona que pasa por el proceso de registro. Por ejemplo, una persona puede seleccionar un identificador (o un conjunto de identificadores) para sí mismo, y/o para una tarjeta de crédito o débito que posee, etc. En algunas realizaciones, la persona puede seleccionar más bien una secuencia de imágenes, y el servidor central 110 puede asociar la secuencia de imágenes al/a los identificador(es). La secuencia de imágenes puede ser más fácil de recordar que el/los identificador(es) completo(s) y, por tanto, puede ser útil con propósitos de autorización (tal como se comenta más adelante).

La seguridad puede aumentarse cambiando automáticamente (y/o previa petición) los valores de los identificadores almacenados en el registro de vez en cuando. De esta manera, los niveles de seguridad pueden personalizarse a la sensibilidad o al nivel de riesgo de los datos que se protegen. Por ejemplo, un identificador asociado con una institución financiera o un conmutador de red de “alta seguridad” puede cambiarse cada dos minutos (o cada vez que un dispositivo de codificación solicita el identificador, etc.), aunque un identificador asociado con una persona particular o un encaminador de uso general puede cambiarse mensual o anualmente (o sólo previa petición, etc.). Los identificadores también pueden actualizarse basándose en otros desencadenantes (por ejemplo, violaciones de seguridad), lo que permite de ese modo que las respuestas a las amenazas de seguridad se personalicen estrechamente basándose en la naturaleza de la amenaza de seguridad. Por ejemplo, el servidor central puede actualizar un identificador asociado con un cliente particular de un minorista en línea si se produjese una transacción fraudulenta con ese minorista a nombre del cliente, y actualizar el identificador asociado con el propio minorista si el minorista sospecha de una violación más amplia de sus registros confidenciales. En realizaciones y situaciones en las que los identificadores se cambian manualmente, pueden cambiarse usando una interfaz administrativa segura

(por ejemplo, proporcionada por un terminal informático acoplado al servidor central 110, o puesto a disposición de otros a través de un canal de comunicación seguro, etc.), por ejemplo.

En algunas realizaciones y situaciones, la frecuencia con la que cambia un identificador, y/o la cantidad de variación y/o aleatorización asociada con cada cambio, puede estar dictada por un nivel de seguridad actual asociado con la entidad correspondiente (por ejemplo, una empresa particular). Por ejemplo, el identificador de una entidad puede actualizarse mensualmente si un nivel de seguridad "amarillo" está asociado con la entidad, diariamente si el nivel de seguridad cambia a "naranja" (por ejemplo, en respuesta a informes generales de aumento de la actividad de piratería informática), y cada cinco minutos si el nivel de seguridad cambia a "rojo" (por ejemplo, en respuesta a un informe confirmado de una violación de seguridad específica que involucra a la entidad).

III. ENTRADA SEGURA DE DATOS

Tal como se indicó anteriormente, en un aspecto de la presente invención, no se recopila, almacena ni transmite información introducida en un teclado, ni datos correspondientes a representaciones convencionales de dicha información (por ejemplo, códigos ASCII). Con referencia a las figuras 1 y 2, por ejemplo, el usuario puede introducir números y/o letras realizando una serie de entradas por teclado en el teclado 130, y el dispositivo de origen 102 puede codificar directamente las entradas por teclado de tal manera que no puede seguirse la pista de ninguna información almacenada y/o transmitida o mapearse de vuelta a las entradas por teclado originales sin el conocimiento de las operaciones de decodificación adecuadas y dependientes del tiempo y su secuencia apropiada.

La figura 3 representa un mapeo 140 de ejemplo que el dispositivo de origen 102 puede usar para ofuscar información de entrada por teclado, según una realización y situación. En la mapeo 140, las entradas de usuario realizadas con las teclas 142 se mapean a coordenadas espaciales virtuales 144. Las teclas 142 pueden ser teclas del teclado 130 en la figura 2, por ejemplo. El mapeo 140 corresponde a un valor específico de un identificador particular. El identificador puede ser uno que esté asociado (en el registro 112) con el dispositivo de origen 102, un agente u otro usuario que introduzca información en el teclado 130, una empresa asociada con el dispositivo de origen 102, o cualquier otra entidad adecuada, y el valor de identificador puede haberse proporcionado al dispositivo de origen 102 por el servidor central 110. Al recibir el valor de identificador (por ejemplo, a través de la interfaz de comunicación 126 y un canal de comunicación seguro), el procesador 120 del dispositivo de origen 102 puede usar el módulo de codificación 128 para determinar el mapeo 140.

Tal como se observa en la figura 3, en el mapeo 140 de ejemplo, una entrada de usuario (por ejemplo, presionar, tocar, etc.) de "0" se mapea a las coordenadas [2,0], una entrada de usuario de "1" se mapea a las coordenadas [2,3], una entrada de usuario de la tecla "Introducir" ("*Enter*") se mapea a las coordenadas [2,1], y así sucesivamente. Tras detectar una entrada por teclado particular, el módulo de codificación 128 puede generar una cadena de bits que representa las coordenadas correspondientes que resultan del mapeo 140. Si un usuario introduce "421" seguido de la tecla "Introducir", por ejemplo, y si se usan cuatro bits para representar cada par de coordenadas, el módulo de codificación 128 puede generar la cadena de bits 0001 0011 1000 1001 para representar la secuencia de coordenadas de espacio virtual [0,1], [0,3], [2,0], [2,1]. Sin embargo, tal como se indicó anteriormente, el servidor central 110 puede cambiar, en algunas situaciones, el identificador en una frecuencia muy alta. Por ejemplo, el dispositivo de origen 102 puede solicitar un identificador del servidor central 110 inmediatamente después de cada entrada por teclado, y el mapeo 140 puede cambiar a un nuevo mapeo para cada entrada por teclado en la secuencia de ejemplo anterior. Así, por ejemplo, una entrada de "4" puede mapearse a [0,1] bajo el mapeo 140, mapearse a [1,2] (u otra coordenada) bajo un mapeo aplicado a una pulsación de tecla posterior, etc.

Aunque la figura 3 ilustra un ejemplo en el que el tamaño del espacio virtual coincide aproximadamente 1:1 con el tamaño del teclado (en términos de valores discretos numéricos), en otras realizaciones el espacio virtual puede ser mucho mayor. Por ejemplo, cada una de las teclas 142 puede mapearse a una coordenada diferente de una cuadrícula virtual que es 256x256, cambiando el mapeo para cada valor de identificador. Por ejemplo, una entrada por teclado de "0" puede mapearse a la coordenada de espacio virtual [163,24] para un primer identificador/mapeo, mapearse a la coordenada de espacio virtual [212,148] para el siguiente identificador/mapeo, etc. Generalmente, los espacios virtuales más grandes requieren representaciones de bits más largas de las coordenadas resultantes, pero pueden proporcionar una aleatorización mejorada desde la perspectiva de un observador no autorizado.

Además, el dispositivo de origen 102 puede implementar capas de mapeo adicionales para ofuscar y proteger adicionalmente la información introducida. La figura 4 representa uno de tales conjuntos 200 de capas de mapeo, según una realización y situación. En esta realización de ejemplo, el conjunto 200 incluye tres capas de mapeo 202-1, 202-2 y 202-3, aplicando la primera capa de mapeo 202-1 el mapeo 140 de la figura 3 y aplicando las capas de mapeo 202-2 y 202-3 posteriores diferentes mapeos. Tal como se indicó anteriormente, la capa de mapeo 202-1 puede mapear más bien entradas por teclado a un espacio virtual más grande (por ejemplo, 8x8, 16x16, 256x256, etc.). De manera similar, la capa de mapeo 202-2 puede mapear más bien las coordenadas de la capa 202-1 a un espacio virtual más grande, y/o 202-3 puede mapear las coordenadas de la capa 202-2 a un espacio virtual más grande.

Aunque la figura 4 muestra tres capas 202-1 a 202-3, otras realizaciones pueden usar cualquier otro número

adecuado de capas (por ejemplo, dos, cinco, 10, 100, etc.). En general, pueden usarse más capas cuando se desean mayores niveles de seguridad. Por ejemplo, las transacciones que involucran a una institución financiera pueden usar 50 capas similares a las capas 202, aunque las transacciones que involucran normalmente información menos sensible pueden involucrar sólo tres capas, etc. En algunas realizaciones, el dispositivo de origen 102 conoce *a priori* cuántas capas de mapeo/codificación se aplicarán. Alternativamente, el servidor central 110 puede informar al dispositivo de origen 102 del número de capas (por ejemplo, de manera explícita a través de una indicación enviada en el mismo canal de comunicación seguro usado para enviar el/los identificador(es), o de manera implícita enviando sólo el número requerido de identificadores, etc.) En esta última realización, el número de capas puede cambiar de vez en cuando (por ejemplo, incluso entre entradas por teclado posteriores).

IV. CADENA DE DATOS CODIFICADA EN EL TRAYECTO DE COMUNICACIÓN

La sección anterior describe una o múltiples capas o etapas de mapeo/codificación dentro de un único dispositivo de origen. Sin embargo, de manera más general, pueden implementarse diferentes etapas de codificación por diferentes dispositivos en un trayecto de comunicación. Por ejemplo, una cadena de datos puede codificarse mediante una o más etapas de codificación en el dispositivo de origen 102 (por ejemplo, etapas correspondientes a las capas 202-1 a 202-3 de la figura 4), y posteriormente mediante una o más etapas de codificación en cada uno de uno o más dispositivos de red en la red 106 (por ejemplo, un encaminador, un conmutador de red, un servidor, etc.). Además, aunque la sección anterior describe la codificación de información correspondiente a entradas de usuario en un teclado (por ejemplo, el teclado 130), una cadena de datos puede corresponder o basarse prácticamente en cualquier otro tipo de información. Por ejemplo, una cadena de datos que va a codificarse y transmitirse puede incluir datos que se generaron automáticamente por una aplicación de software que se ejecuta en un dispositivo de origen, o recuperados de una memoria local del dispositivo de origen, etc.

La figura 5 representa un trayecto de comunicación 250 de ejemplo para una cadena de datos en el que la cadena de datos puede codificarse usando las técnicas descritas en el presente documento, según una realización y situación. El trayecto de comunicación 250 incluye un dispositivo de origen 252, un primer dispositivo de red 254, un segundo dispositivo de red 256 y un dispositivo de destino 260. El dispositivo de origen 252 puede ser similar al dispositivo de origen 102 de la figura 1, los dispositivos de red 254 y 256 pueden ser dispositivos dentro de la red 106 de la figura 1, y el dispositivo de destino 250 puede ser similar al dispositivo de destino 104 de la figura 1, por ejemplo. En un caso, el dispositivo de origen 252 puede ser una tableta con un teclado virtual, el dispositivo de red 254 puede ser un encaminador, el dispositivo de red 256 puede ser un conmutador de red y el dispositivo de destino 260 puede ser un servidor empresarial.

Tal como se observa en la figura 5, el dispositivo de origen 252 incluye cinco etapas de codificación 262-1 a 262-5, el dispositivo de red 254 incluye dos etapas de codificación 264-1 y 264-2, y el segundo dispositivo de red 256 incluye una etapa de codificación 266. Cada etapa de codificación puede implementarse por el uno o más procesadores del dispositivo respectivo cuando se ejecutan las instrucciones del módulo de codificación almacenadas en una memoria del dispositivo respectivo. En otras realizaciones, el trayecto de comunicación 250 puede incluir más o menos dispositivos de los que se muestran en la figura 5, y/o algunos o todos de los diversos dispositivos pueden incluir más o menos etapas de codificación. Por ejemplo, el dispositivo de origen 252 puede incluir decenas o cientos de etapas de codificación 262, y/o el trayecto de comunicación 250 puede incluir varios dispositivos de red adicionales que no incluyen ninguna etapa de codificación, etc.

En realizaciones y situaciones en las que la cadena de datos que se codifica se basa en entradas de teclado, la primera etapa de codificación 262-1 puede mapear las entradas por teclado a secuencias de bits de la manera descrita en la sección anterior (es decir, secuencias de bits que representan coordenadas de espacio virtual en una primera capa, tal como la capa 202-1 de la figura 4). El número de bits usados para representar cada coordenada de espacio virtual puede considerarse el tamaño de bloque de salida para la etapa de codificación 262-1. A partir de lo anterior y de la siguiente descripción, un experto en la técnica apreciará que las capas 202-1 a 202-3 de la figura 4 pueden considerarse una realización específica del funcionamiento de las etapas de codificación 262-1 a 262-3 de la figura 5. En realizaciones o situaciones en las que la cadena de datos no se basa en entradas de teclado (por ejemplo, datos recuperados de una memoria, etc.), la etapa de codificación 262-1 puede funcionar de manera similar a las etapas de codificación posteriores (por ejemplo, 262-2, 262-3, etc.).

Cada una de las etapas de codificación 262-2 a 262-5, 264-1, 264-2 y 266 funciona con la salida de la etapa de codificación anterior, y puede estar asociada con un tamaño de bloque de entrada (X_l para la etapa de codificación de orden *l* en el trayecto de comunicación 250) y un algoritmo de codificación o mapeo particular que dicta el tamaño de bloque de salida (Y_l Para la etapa de codificación de orden *l* en el trayecto de comunicación 250). En particular, cada etapa de codificación puede analizar su entrada en bloques de X_l bits, y aplicar el algoritmo de codificación apropiado para generar los bloques correspondientes de Y_l bits. En general, el tamaño de bloque de salida para una etapa de codificación particular puede ser igual a o mayor que el tamaño de bloque de entrada para esa etapa (aunque preferiblemente no más pequeño, para impedir colisiones).

El algoritmo de codificación específico usado por cada una de las etapas de codificación 262-1 a 262-5, 264-1, 264-2 y 266 puede estar dictado por el valor actual de un identificador respectivo, en el que el identificador está asociado con una entidad registrada particular tal como se comentó anteriormente. Por ejemplo, el identificador para la etapa

de codificación 262-1 puede estar asociado con el dispositivo de origen 252, el identificador para la etapa de codificación 262-2 puede estar asociado con una empresa particular (por ejemplo, una que posee, mantiene y/o usa el dispositivo de origen 252, o está involucrada de otro modo con la transacción que requiere la transmisión de la cadena de datos), el identificador para la etapa de codificación 262-3 puede estar asociado con un departamento particular de la empresa, el identificador para la etapa de codificación 262-4 puede estar asociado con un agente/empleado particular que usa el dispositivo de origen 252, y el identificador para la etapa de codificación 262-5 puede estar asociado con una aplicación de software particular que se ejecuta en el dispositivo de origen 252. Continuando con este ejemplo, el identificador para la etapa de codificación 264-1 puede estar asociado con el dispositivo de red (por ejemplo, encaminador) 254, el identificador para la etapa de codificación 264-2 puede estar asociado con un cortafuegos implementado por el dispositivo de red 254, y el identificador para la etapa de codificación 266 puede estar asociado con el dispositivo de red (por ejemplo, un conmutador de red) 256.

Cada uno de los dispositivos 252, 254 y 256 puede obtener los valores actuales de su(s) identificador(es) de etapa de codificación respectivo(s) enviando una petición a un servidor central (por ejemplo, el servidor central 110 de la figura 1) a través de un canal de comunicación seguro justo antes de la codificación. Alternativamente, los valores de identificador pueden solicitarse periódicamente, o el servidor central puede introducir los valores actuales de los identificadores apropiados en algunos o todos los dispositivos 252, 254 y 256 (por ejemplo, de manera periódica) a través de canales de comunicación seguros. Los canales de comunicación seguros entre el servidor central y cada dispositivo pueden usar técnicas fuertes de autenticación/verificación y cifrado conocidas en la técnica, por ejemplo. En algunas realizaciones, uno o más de los dispositivos 252, 254, 256 añaden información de sello de tiempo a la cadena de datos transmitida en uno o más intervalos, para informar al dispositivo de destino 260 del/de los tiempo(s) en que los diversos valores de identificación eran “actuales”. Esta información puede permitir que el dispositivo de destino 260 decodifique adecuadamente la cadena de datos recibida, tal como se comentará más adelante. Además, en algunas realizaciones, uno o más de los dispositivos 252, 254 y 256 pueden usar el tiempo actual u otra información para codificar o aleatorizar adicionalmente la cadena de datos.

Cada uno de los dispositivos 252, 254 y 256 puede almacenar un conjunto de reglas que permite que el dispositivo determine el algoritmo de codificación apropiado a usar, en cada etapa de codificación implementada por el dispositivo, basándose en el valor de identificador actual. En algunas realizaciones, el tamaño de bloque de entrada X_I y el tamaño de bloque de salida Y_I pueden cambiar para una etapa de codificación particular basándose en el valor de identificador actual. En otras realizaciones, los tamaños de bloque de entrada y/o salida son constantes, y los valores de identificador sólo dictan el algoritmo actual (por ejemplo, mapeo) a usar en cada etapa de codificación. Sin embargo, preferiblemente, los tamaños de bloque de entrada y/o salida pueden cambiar con el valor de identificador para aumentar la aleatorización desde la perspectiva de un observador no autorizado. Además, al menos algunos de los tamaños de bloque de salida Y_I de las etapas de codificación dentro del trayecto de comunicación 250 difieren preferiblemente para aumentar la dificultad de la decodificación no autorizada. Como un ejemplo específico, en una transmisión (o para una parte de la misma), $Y_1 = 8$ (es decir, la etapa de codificación 262-1 tiene un tamaño de bloque de salida de ocho bits), $Y_2 = 16$, $Y_3 = 4$, $Y_4 = 4$, $Y_5 = 32$, y así sucesivamente.

Para cada etapa de codificación, el identificador correspondiente puede ser constante en la totalidad de la transmisión de una cadena de datos particular, o puede cambiar durante la transmisión. Por ejemplo, la etapa de codificación 262-3 puede configurarse basándose en el valor de un identificador asociado con una empresa de servicios financieros u otra empresa que requiera niveles de seguridad muy altos, y el valor de identificador (y, por tanto, la operación de codificación) puede cambiar incluso a lo largo del transcurso de la transmisión de una única cadena de datos.

V. DECODIFICACIÓN DE LA CADENA DE DATOS

En una realización, un dispositivo que recibe una cadena de datos codificada usando cualquiera de las técnicas anteriores (por ejemplo, el dispositivo de destino 104 de la figura 1 o el dispositivo de destino 260 de la figura 5) decodifica la cadena de datos implementando una etapa de decodificación diferente correspondiente a cada etapa de codificación. En particular, para decodificar apropiadamente la cadena de datos, el dispositivo de recepción implementa las etapas de decodificación a la inversa del orden en que se aplicaron las etapas de codificación correspondientes. Con referencia a la figura 5, por ejemplo, el dispositivo de destino 260 (por ejemplo, uno o más procesadores dentro del dispositivo 260, que ejecutar instrucciones de un módulo de decodificación almacenado en una memoria del dispositivo 260) puede implementar en primer lugar una etapa de decodificación que es la inversa de la etapa de codificación 266, implementar en segundo lugar una etapa de decodificación que es la inversa de la etapa de codificación 264-2, implementar en tercer lugar una etapa de decodificación que es la inversa de la etapa de codificación 264-1, implementar en cuarto lugar una etapa de decodificación que es la inversa de la etapa de codificación 262-5, y así sucesivamente, hasta que finalmente se implemente una etapa de decodificación que es la inversa de la etapa de codificación 262-1 (por ejemplo, para determinar las entradas por teclado realizadas por un usuario o la cadena de datos original).

Para determinar los algoritmos apropiados a aplicar en cada etapa de decodificación, en una realización, el dispositivo de destino 260 puede obtener los valores de identificador que se usaron para las etapas de codificación correspondientes desde un servidor central a través de un canal de comunicación seguro (por ejemplo, desde el servidor central 110, usando técnicas de autenticación y/o cifrado similares a las usadas por los dispositivos 252,

254 y/o 256 cuando esos dispositivos obtuvieron los valores de identificador con propósitos de codificación). Los valores de identificador puede solicitarlos el dispositivo de destino 260 tras recibir la cadena de datos, por ejemplo, o solicitarlos (o introducirse en) el dispositivo de destino 260 de manera periódica u otra.

En algunas realizaciones, los valores de identificador obtenidos por el dispositivo de destino 260 pueden ser simplemente los valores más recientes, con la suposición de que los valores probablemente no han cambiado desde que se codificó la cadena de datos. En otras realizaciones, y particularmente aquellas en las que los valores de identificador pueden cambiar con alta frecuencia (por ejemplo, entre cada entrada por teclado de usuario), uno o más de los dispositivos 252, 254 y 256 pueden incluir uno o más sellos de tiempo dentro, o junto con, la transmisión de la cadena de datos. El dispositivo de destino 260 puede reenviar entonces la información de sello de tiempo al servidor central, de modo que el servidor central puede enviar al dispositivo de destino 260 los valores de identificador correspondientes a los tiempos en que los valores de identificador se enviaron a las etapas de codificación. Para ello, el servidor central puede almacenar un historial para cada valor de identificador (por ejemplo, una lista de valores pasados, junto con los tiempos en que esos valores eran actuales).

El dispositivo de destino 260 puede almacenar un conjunto de reglas que permite que el dispositivo 260 determine los algoritmos de decodificación apropiados a usar basándose en los valores de identificador recibidos. Para deshacer la codificación realizada por la etapa de codificación de orden *I*, por ejemplo, la etapa de decodificación correspondiente del dispositivo de destino 260 puede analizar la cadena de datos (o la cadena de datos parcialmente decodificada de la etapa de decodificación previa) en bloques de tamaño Y_I (es decir, el tamaño de bloque de salida para la etapa de codificación /) y decodificar cada bloque en un bloque de salida de tamaño X_I (es decir, el tamaño de bloque de entrada para la etapa de codificación de orden *I* usando el mapeo apropiado).

En una realización, para que el dispositivo de destino 260 decodifique de manera apropiada y completa la cadena de datos recibida, el dispositivo 260 debe conocer, o aprender, la secuencia en la que realizar las etapas de decodificación correspondientes a las etapas de codificación (es decir, la inversa del orden en el que se aplicaron las etapas de codificación correspondientes). En una realización, el servidor central envía información indicativa de la secuencia correcta al dispositivo de destino 260. En otras realizaciones, el dispositivo de destino 260 conoce *a priori* cuál es la secuencia correcta, y sólo es necesario obtener los valores de identificador apropiados desde el servidor central. En una de tales realizaciones, el trayecto de comunicación (por ejemplo, el trayecto de comunicación 250) puede considerarse un “sistema de confianza”, y la secuencia correcta de etapas de decodificación puede actuar como un tipo de autenticación. Es decir, si el dispositivo de destino 260 implementa las etapas de decodificación en el orden correcto y usa los valores de identificador apropiados del servidor central, entonces un fallo al decodificar la cadena de datos puede indicar que la cadena de datos no se transmitió a lo largo de un trayecto de comunicación “aprobado”.

En algunas situaciones, el dispositivo de destino 260 puede no decodificar totalmente la cadena de datos y, por tanto, puede no realizar etapas de decodificación correspondientes a algunas o todas las etapas de codificación. Por ejemplo, una parte de recepción asociada con el dispositivo de destino 260 puede desear almacenar versiones al menos parcialmente codificadas de los números de tarjeta de crédito del cliente, en lugar de almacenar los números de tarjeta en un formato fácil de determinar (por ejemplo, representaciones ASCII), para evitar activar obligaciones de cumplimiento Estándar de seguridad de datos para la industria de tarjetas de pago (PCI DSS, por sus siglas en inglés).

VI. AUTORIZACIÓN

Puede proporcionarse una capa adicional de seguridad al requerir autorización para una transacción dada. Por ejemplo, las compras con una tarjeta de crédito o débito sólo pueden ser aprobadas por un procesador de pago después de que el usuario de la tarjeta haya autorizado la compra. Para facilitar la explicación, el comentario a continuación se refiere principalmente a realizaciones o situaciones en las que el titular de una tarjeta de crédito o débito se registra previamente para proporcionar la autorización. Sin embargo, en otras realizaciones y/o situaciones, el proceso puede usarse para otros individuos y/o en otros tipos de transacciones. Por ejemplo, un agente de una empresa puede registrarse previamente para proporcionar autorización/confirmación para transacciones llevadas a cabo en nombre de los consumidores, o para transacciones meramente internas (por ejemplo, para autorizar una petición particular para recuperar o modificar información en una base de datos empresarial), etc.

Para proporcionar la autorización del usuario, una persona puede registrarse previamente a sí misma, y/o su tarjeta, con un servidor central (por ejemplo, el servidor central 110 de la figura 1). El proceso de registro puede ser similar al descrito anteriormente en la Sección II, por ejemplo, asignándose un identificador a cada persona y/o tarjeta que se registra.

En una realización, la persona puede seleccionar su identificador personal (o tarjeta). Debido a que el identificador puede ser una larga cadena de números y/u otros caracteres difíciles de memorizar, se le puede dar a la persona la opción de seleccionar una secuencia específica de imágenes entre un conjunto limitado de imágenes. Para proporcionar sólo un par de ejemplos, el solicitante puede seleccionar cualquier secuencia específica de cuatro colores/palos de naipes (por ejemplo, diamante negro, pica roja, corazón rojo, diamante rojo), o cualquier secuencia

específica de tres colores/palos/categorías de naipes (por ejemplo, el tres rojo de tréboles, el rey negro de corazones, la jota negra de diamantes), etc.

Se proporciona otro ejemplo en la figura 6, que muestra una interfaz de usuario 300 de ejemplo con varias imágenes esencialmente aleatorias/no relacionadas 302. Aunque la figura 6 muestra la interfaz de usuario 300 que se presenta en la pantalla de visualización de un teléfono inteligente, en otras realizaciones o situaciones, pueden usarse otros dispositivos. Además, aunque la figura 6 muestra un total de 12 imágenes de las cuales puede realizarse una selección, son posibles otros números de imágenes (por ejemplo, 10, 20, 100, etc.). Cada una de las imágenes 302 puede corresponder a una cadena de caracteres particular, de tal manera que la secuencia de imágenes seleccionada corresponde a un identificador que consiste en varias cadenas de caracteres en un orden particular. En la figura 6, por ejemplo, si la imagen del mundo corresponde a “3a7e16”, la imagen del automóvil corresponde a “4b4a22”, y la imagen de la casa corresponde a “9u3c59”, entonces la secuencia “mundo, automóvil, casa” puede corresponder al identificador “3a7e164b4a229u3c59”.

En algunas realizaciones, la secuencia de imágenes seleccionada corresponde a múltiples identificadores. Por ejemplo, la secuencia puede corresponder a una concatenación de un primer identificador para el/la propio/propia solicitante de registro, y un segundo identificador para una tarjeta de crédito o débito del solicitante de registro. Como otro ejemplo, una única secuencia de imágenes puede corresponder a una secuencia predeterminada de valores de identificador, haciendo cada actualización del identificador por el servidor central que el valor de identificador avance al siguiente valor en la secuencia. La secuencia de valores de identificador puede almacenarse en una tabla del servidor central, por ejemplo, o puede basarse en una función matemática, etc. De esta manera, pueden mantenerse al menos algunos de los beneficios de seguridad de cambiar el identificador de vez en cuando, sin requerir que el individuo memorice una nueva secuencia de imágenes cada vez que se actualiza el identificador.

La secuencia de imágenes puede seleccionarse accediendo a una interfaz de usuario proporcionada por el servidor central. En una realización, el solicitante de registro puede llamar a un agente de una empresa que proporciona el servicio de seguridad de datos, y el agente puede acceder a una interfaz administrativa segura para realizar las selecciones. Por ejemplo, el agente puede informar al solicitante de registro de las opciones de imagen y luego introducir las selecciones a medida que el solicitante de registro les indica a los agentes esas selecciones. En otra realización, el solicitante de registro puede acceder de manera remota al servidor central a través de un canal de comunicación seguro para realizar sus selecciones. En esta realización, el servidor central puede enviar al solicitante de registro la colección de imágenes que pueden seleccionarse (por ejemplo, para su visualización a través de una interfaz de usuario de un navegador web o una aplicación de software dedicada que se ejecuta en el teléfono inteligente, la tableta, el ordenador portátil u ordenador de escritorio del solicitante de registro, etc.), y las selecciones del solicitante de registro pueden transmitirse de vuelta al servidor central. El solicitante de registro puede hacer las selecciones a través de una interfaz de usuario similar a la interfaz de usuario 300 de la figura 6, por ejemplo. En otras realizaciones, el solicitante de registro no selecciona una secuencia de imágenes en absoluto, sino que más bien se le informa de una secuencia de imágenes que corresponde a su identificador asignado aleatoriamente.

En algunas realizaciones, un solicitante de registro también puede seleccionar la(s) manera(s) en que se realizan las peticiones de autorización. Por ejemplo, pueden proporcionársele al solicitante de registro opciones de autorización telefónica, autorización por correo electrónico, autorización por mensaje de texto SMS y/u otros tipos de autorización.

Una vez que se ha establecido una secuencia de imágenes para un solicitante de registro particular (o su tarjeta), y se ha(n) establecido el/los método(s) de autorización apropiado(s) para el solicitante de registro, la secuencia de imágenes puede usarse para autorizar transacciones futuras. Con referencia a el trayecto de comunicación 250 de la figura 5, por ejemplo, el dispositivo de destino 260 puede recibir la cadena de datos codificada (por ejemplo, tal como se describió anteriormente en la Sección III o IV), decodificar la cadena de datos (por ejemplo, tal como se describió anteriormente en la Sección V), y determine a partir de los datos decodificados que una persona en particular, o la tarjeta de crédito o débito de esa persona, está asociada con la transacción que se realiza. El dispositivo de destino 260, o un agente asociado con el dispositivo 260, puede solicitar entonces la secuencia de imágenes de la persona a través del/de los mecanismo(s) apropiado(s) (por ejemplo, llamada telefónica, mensaje de texto SMS, etc.). Alternativamente, el dispositivo de destino 260 puede usar el canal de comunicación seguro para informar al servidor central que es necesario autorización, y el servidor central puede solicitar la secuencia de imágenes a través del/de los mecanismo(s) apropiado(s) e informar al dispositivo de destino 260 en cuanto a si se recibió una respuesta correcta.

En algunas realizaciones y situaciones (por ejemplo, si se solicita autorización por teléfono), un usuario puede autorizar una transacción describiendo la secuencia de imágenes a un agente (por ejemplo, diciendo “mundo, automóvil, casa”), y el agente o bien puede introducir esa información, o bien simplemente aprobar la transacción directamente si el agente conoce la secuencia apropiada. En otras realizaciones y situaciones (por ejemplo, si se solicita autorización a través de un navegador web o una aplicación de software dedicada que se ejecuta en el dispositivo electrónico del usuario), el usuario puede autorizar una transacción o bien tecleando descriptores de la secuencia de imágenes correcta o bien seleccionando la secuencia correcta entre una pluralidad de imágenes (por ejemplo, a través de una interfaz de usuario similar a la interfaz de usuario 300 de la figura 6). Una vez que se ha

proporcionado la secuencia de imágenes correcta, puede aprobarse la transacción. En algunas realizaciones, si se proporciona una secuencia de imágenes incorrecta (o se proporciona un número umbral de intentos), el servidor central trata la entrada o entradas incorrectas como una sospecha de violación de seguridad. Por ejemplo, el servidor central puede actualizar un identificador asociado con la persona que supuestamente realiza la transacción, y/o actualizar un identificador asociado con la tarjeta de crédito o débito de esa persona.

En algunas realizaciones, el/los identificador(es) correspondiente(s) a la secuencia de imágenes también se usa(n) en el proceso de codificación comentado anteriormente en la Sección III o IV. Por ejemplo, una de las etapas de codificación 262-1 a 262-5 en la figura 5 puede seleccionar un algoritmo de codificación basándose en un valor de un identificador correspondiente a la secuencia de imágenes. En algunas de tales realizaciones, esto puede requerir que el servidor central aprenda quién está realizando la transacción, o qué tarjeta está usándose para realizar la transacción, de modo que el identificador apropiado pueda recuperarse y enviarse al dispositivo de origen 252. Un ejemplo de tal realización se describe a continuación en la Sección VII, en relación con un caso/situación de uso particular.

VII. EJEMPLO DE CASO DE USO

La figura 7 representa un entorno 400 de ejemplo en el que pueden implementarse aspectos de la presente divulgación cuando se realiza una transacción de tarjeta de compra de crédito o débito, según una realización y situación. Se entiende que esto representa sólo un caso de uso de ejemplo, y que también son posibles casos de uso relacionados con otros tipos de transacciones y en otros entornos/sistemas.

En la situación de ejemplo de la figura 7, un consumidor posee una tarjeta de crédito o débito 402 que se usa para comprar productos en una tienda minorista. En la tienda minorista está ubicado un dispositivo de tableta 404, que presenta una interfaz de usuario que incluye un teclado virtual para introducir información de compra (por ejemplo, números de tarjeta del consumidor) cuando se realizan transacciones/compras. Alternativamente, el dispositivo 404 puede ser un dispositivo dedicado o de uso general con un teclado de hardware. La información de pago para las transacciones, incluidos los números de tarjeta de crédito o débito, los importes de pago, etc., puede enviarse a un proveedor de pago 406 (por ejemplo, uno o más servidores del proveedor de pago 406), que reenvía la información de pago a una red de pago 410 (por ejemplo, uno o más servidores de la red de pago 410) para añadir la cantidad apropiada al saldo de una tarjeta de crédito o deducir la cantidad apropiada del saldo de una cuenta asociada con una tarjeta de débito, etc. La red de pago 410 puede ser un banco, por ejemplo.

Para ofuscar al menos parte de la información de pago de la transacción, pueden usarse una o más de las técnicas descritas anteriormente. Para ello, el entorno 400 de ejemplo incluye un servidor central 412 (por ejemplo, similar al servidor central 110 de la figura 1), que puede estar en comunicación con el dispositivo de tableta 404 y el proveedor de pago 406 a través de canales de comunicación seguros respectivos. Además, el dispositivo de tableta 404 puede haberse registrado previamente con el servidor central 412 de la manera descrita anteriormente en la Sección II. Otras entidades asociadas con las transacciones minoristas también pueden, o en cambio, estar registradas previamente, como la propia tienda minorista, un empleado/agente de la tienda, uno o más dispositivos de red (por ejemplo, encaminadores) y/o aplicaciones o nodos (por ejemplo, cortafuegos) en el trayecto de comunicación entre el dispositivo de tableta 404 y el proveedor de pago 406, y así sucesivamente.

En la situación de ejemplo descrita en el presente documento, la tarjeta 402 también está registrada previamente con el servidor central 412. Por ejemplo, el titular de la tarjeta 402 puede haber registrado la tarjeta 402 en parte seleccionando una secuencia de imágenes específica, tal como se comentó anteriormente en la Sección VI.

En funcionamiento, el titular de la tarjeta 402 puede o bien presentar su tarjeta a un empleado de la tienda (una transacción con “tarjeta presente”) para que el empleado pueda introducir el número de tarjeta en el teclado virtual de la tableta 404, o bien proporcionar su número de tarjeta al empleado por teléfono (una transacción con “tarjeta no presente”). Alternativamente, el titular de la tarjeta puede introducir el número de la tarjeta usando la tableta 404.

En una realización, sólo una versión codificada de manera segura del número de tarjeta está presente, en forma digital, en cualquier punto dentro de la transacción. Por ejemplo, las técnicas descritas anteriormente en relación con las figuras 3 y 4 pueden usarse para mapear las entradas por teclado a las coordenadas de espacio virtual, dependiendo cada mapeo del valor de un valor de identificador respectivo recibido desde el servidor central 412 a través del canal de comunicación seguro. Además, uno o más dispositivos (no mostrados en la figura 7) dentro del trayecto de comunicación entre el dispositivo de tableta 404 y el proveedor de pago 406 pueden añadir, cada uno, una o más etapas de codificación, tal como se describió anteriormente en relación con la figura 5.

En algunas realizaciones, el valor actual del identificador asociado con la tarjeta 402 se usa para una etapa de codificación. Por ejemplo, el titular de la tarjeta 402 puede proporcionar su nombre al empleado de la tienda, y el empleado puede usar el dispositivo de tableta 404 u otro dispositivo para transmitir el nombre del titular de la tarjeta al servidor central 412. El servidor central 412 puede responder con una pregunta de seguridad que se acordó en el momento del registro del titular de la tarjeta. Luego, el empleado puede obtener la respuesta a la pregunta de seguridad del titular de la tarjeta y proporcionar la respuesta al servidor central 412. El servidor central 412 puede usar la respuesta del titular de la tarjeta para identificar la tarjeta 402, y después de eso enviar el valor actual del

identificador correspondiente a la tarjeta 402 al dispositivo de tableta 404. El dispositivo de tableta 404 puede usar entonces el valor de identificador para determinar la codificación apropiada en una de las etapas de codificación, tal como se comentó anteriormente. En otras realizaciones, pueden usarse otras técnicas para informar al servidor central 412 de la identidad de la tarjeta 402.

Después de que el dispositivo de tableta 404, y cualquier otro dispositivo de codificación en el trayecto de comunicación, codifica una cadena de datos correspondiente a la información de pago, la cadena de datos codificada se recibe en el proveedor de pago 406. Tal como se comentó anteriormente en la Sección V, el proveedor de pago 406 puede obtener los valores de identificador apropiados del servidor central 412 a través de un canal de comunicación seguro, y usar esos valores para decodificar la cadena de datos invirtiendo cada una de las etapas de codificación en el orden correcto. Para autorizar la transacción, el proveedor de pago 406 o el servidor central 412 pueden usar el método de autorización preferido del titular de la tarjeta para solicitar la secuencia de imágenes correspondiente al identificador para la tarjeta 402 (por ejemplo, según cualquiera de las técnicas comentadas anteriormente en la Sección VI). Si el titular de la tarjeta proporciona la secuencia apropiada, el proveedor de pago 406 puede aprobar la transacción y reenviar la información de pago a la red de pago 410 a través de otro canal de comunicación seguro. Debido a que la información de pago nunca se almacena en el dispositivo de tableta 402 (ni en ningún otro dispositivo del minorista), es posible que el minorista no tenga que cumplir con las obligaciones de PCI DSS.

VIII. MÉTODOS DE EJEMPLO

La figura 8 es un diagrama de flujo de un método 500 de ejemplo para recopilar de manera segura información sensible, según una realización. El método 500 puede implementarse por uno o más procesadores de un dispositivo electrónico (por ejemplo, el procesador 120 de la figura 2, o uno o más procesadores del dispositivo de origen 252 de la figura 5 o el dispositivo de tableta 404 de la figura 7), cuando ejecuta instrucciones almacenadas en una memoria del dispositivo electrónico (por ejemplo, la memoria 122 de la figura 2), por ejemplo.

En el método 500, se detecta una primera entrada por teclado (bloque 502). La entrada por teclado es aquella que se realiza a través de una interfaz de usuario del dispositivo electrónico, incluyendo la interfaz de usuario una pluralidad de teclas. La entrada por teclado puede realizarse durante el proceso de introducir manualmente información sensible, tal como un número de tarjeta de crédito o débito, otra información financiera, información sanitaria personal, un número de la seguridad social, etc. En algunas realizaciones, la interfaz de usuario (por ejemplo, la interfaz de usuario 124 de la figura 2) incluye un teclado de hardware, cada tecla de la pluralidad de teclas es una tecla diferente en el teclado de hardware, y el bloque 502 incluye detectar cuál de la pluralidad de teclas se tocó o se presionó. El dispositivo electrónico puede ser un dispositivo de teclado de hardware dedicado, por ejemplo. En otras realizaciones, la interfaz de usuario incluye un teclado virtual presentado en una pantalla de visualización táctil del dispositivo electrónico, cada tecla de la pluralidad de teclas es una tecla diferente en el teclado virtual, y el bloque 502 incluye detectar qué área de la pantalla de visualización táctil se tocó. El dispositivo electrónico puede ser un teléfono inteligente, una tableta, un ordenador portátil u ordenador de escritorio, por ejemplo.

También en el método 500, se recibe información desde un servidor remoto (bloque 504). La información se recibe desde el servidor remoto a través de una interfaz de comunicación del dispositivo electrónico (por ejemplo, la interfaz de comunicación 126 de la figura 2), y a través de un canal de comunicación seguro al servidor remoto (por ejemplo, en respuesta a una petición realizada por el dispositivo electrónico). El servidor remoto puede ser un servidor similar al servidor central 110 de la figura 1 o al servidor central 412 de la figura 7, por ejemplo. El bloque 504 puede producirse antes de, simultáneamente a, y/o después del bloque 502.

La información recibida en el bloque 504 incluye al menos el valor actual de un primer identificador de capa. El primer identificador de capa puede ser un identificador asociado con una entidad en un registro mantenido por el servidor remoto, por ejemplo. Por ejemplo, la entidad puede ser el dispositivo electrónico que implementa el método 500, una organización (por ejemplo, una empresa, un departamento, fabricante, etc.) asociada con el dispositivo electrónico, una persona asociada con una transacción que se realiza a través del dispositivo electrónico, etc. En algunas realizaciones, la información recibida en el bloque 504 también incluye valores actuales de uno o más identificadores de capa adicionales. La información puede recibirse en una única transmisión desde el servidor remoto, o en múltiples transmisiones.

Una cadena de bits correspondiente a la primera entrada por teclado puede determinarse usando el valor actual del primer identificador de capa (bloque 506). Por ejemplo, el dispositivo electrónico puede usar el valor actual para determinar la codificación/mapeo apropiado a usar cuando se codifica la entrada por teclado detectada en el bloque 502. En una codificación/mapeo, por ejemplo, una entrada por teclado de “5” puede mapearse a la cadena de bits 01 11 (por ejemplo, las coordenadas de espacio virtual [1,3]), una entrada por teclado de “g” puede mapearse a la cadena de bits 100 001 (por ejemplo, las coordenadas de espacio virtual [4,1]), etc.

Al menos una primera parte de una cadena de datos puede generarse usando la cadena de bits determinada en el bloque 506 (bloque 508). La cadena de datos completa puede corresponder a un número de tarjeta total, contraseña, mensaje o cualquier otro tipo de información introducida en el teclado. Si el dispositivo electrónico utiliza

sólo una única capa de mapeo (por ejemplo, tal como se muestra en la figura 3), el bloque 506 puede incluir generar la cadena de datos o la parte de cadena de datos directamente a partir de la cadena de bits determinada en el bloque 506. Por el contrario, si el dispositivo electrónico utiliza múltiples capas de mapeo (por ejemplo, tal como se representa en la figura 4), y si la información recibida en el bloque 504 incluye el valor actual para al menos un identificador de capa adicional, el bloque 506 puede incluir operaciones adicionales. Por ejemplo, al menos una parte de la cadena de bits determinada en el bloque 506 puede codificarse según el valor actual de un segundo identificador de capa incluido en la información recibida. Si existen más capas de codificación, la cadena de bits emitida por cada capa puede codificarse en la capa posterior, usando el algoritmo de codificación correspondiente al valor actual del identificador para esa capa posterior. La cadena de datos, o parte de la cadena de datos, puede ser igual a la salida de la capa de codificación final.

En algunas realizaciones, el dispositivo electrónico recibe datos que indican el número de capas de codificación que van a aplicarse desde el servidor remoto a través de un canal de comunicación seguro (por ejemplo, junto con la otra información recibida en el bloque 504). Los datos pueden indicar de manera explícita o implícita el número de capas (por ejemplo, enviando de manera implícita sólo el número requerido de valores de identificador, en el orden correcto). En otras realizaciones, el dispositivo electrónico conoce el número correcto de capas *a priori*.

Puede hacerse que la cadena de datos que se genera al menos parcialmente en el bloque 508 se almacene en una memoria local del dispositivo electrónico (por ejemplo, la memoria 122 de la figura 2) y/o se transmita a otro dispositivo a través de una red (bloque 510). Si se transmite, el dispositivo de destino puede ser similar al dispositivo de destino 104 o al dispositivo de destino 260, por ejemplo, y la red puede ser similar a la red 106. El bloque 510 puede realizarse almacenando y/o transmitiendo directamente la cadena de datos, o enviando una señal o un mensaje de control que hace que otro dispositivo o unidad realice el almacenamiento y/o transmisión, por ejemplo.

Los bloques 502 a 508 pueden repetirse para una o más entradas por teclado posteriores. En algunas realizaciones cuando los valores de identificador no cambian con frecuencia, el bloque 504 puede omitirse para estas iteraciones posteriores. Sin embargo, en otras realizaciones, el bloque 504 se repite en cada una (o al menos algunas) de las iteraciones posteriores para obtener valores de identificador actualizados entre algunas o todas las entradas por teclado. Por ejemplo, el servidor remoto puede proporcionar un nuevo valor del primer identificador de capa (o para cada uno de los múltiples identificadores de capa, si es necesario) para cada entrada por teclado. En cualquier caso, la cadena de datos que se hace que se almacene y/o transmita en el bloque 510 puede incluir múltiples segmentos/partes de cadena, cada uno correspondiente a una entrada diferente de las entradas por teclado detectadas.

La figura 9 es un diagrama de flujo de un método 520 de ejemplo para proporcionar una comunicación segura de una cadena de datos a lo largo de un trayecto de comunicación que incluye una pluralidad de dispositivos, según una realización. La propia cadena de datos puede ser una versión codificada de una o más entradas por teclado manuales, o puede ser algún otro tipo de datos no codificados o parcialmente codificados (por ejemplo, una representación ASCII de un número de la seguridad social, informe sanitario personal, etc.), por ejemplo. El método 520 puede implementarse por uno o más procesadores de un servidor (por ejemplo, el servidor central 110 de la figura 1, o el servidor central 412 de la figura 7), cuando se ejecutan instrucciones almacenadas en una memoria del servidor, por ejemplo.

En el método 520, una primera entidad (por ejemplo, una persona, empresa, un departamento, dispositivo de entrada de datos, etc.) y un primer identificador asociado con la primera entidad, se añaden a una base de datos de registro almacenada en una memoria persistente del servidor (bloque 522). Una segunda entidad (por ejemplo, una empresa, un departamento, dispositivo de red, etc.) y un segundo identificador asociado con la segunda entidad, también se añaden a la base de datos de registro (bloque 524). Las entidades pueden añadirse después de un proceso de registro tal como el descrito anteriormente en la Sección II, por ejemplo.

Se proporciona el valor actual del primer identificador a un primer dispositivo, de los dispositivos en el trayecto de comunicación, a través de un primer canal de comunicación seguro para permitir una primera codificación de la cadena de datos (bloque 526). El valor puede proporcionarse en respuesta a una petición recibida desde el primer dispositivo, por ejemplo. El primer dispositivo puede estar asociado con la primera entidad de alguna manera. Por ejemplo, la primera entidad puede ser el primer dispositivo en sí mismo, o puede ser una persona u organización (por ejemplo, una empresa, un departamento, etc.) que posee, controla y/o usa el primer dispositivo, etc. La primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas, teniendo cada una un primer tamaño de bloque (por ejemplo, número de bits).

Se proporciona el valor actual del segundo identificador a un segundo dispositivo de los dispositivos en el trayecto de comunicación, a través de un segundo canal de comunicación seguro, para permitir una segunda codificación de la cadena de datos (bloque 528). El valor puede proporcionarse en respuesta a una petición recibida desde el segundo dispositivo, por ejemplo. El segundo dispositivo está aguas abajo del primer dispositivo en el trayecto de comunicación, y puede estar asociado con la segunda entidad de alguna manera. Por ejemplo, la segunda entidad puede ser el segundo dispositivo en sí mismo (por ejemplo, un dispositivo de red tal como un encaminador o conmutador de red), o puede ser un cortafuegos implementado por el segundo dispositivo, etc. La segunda

codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas. Cada una de la segunda pluralidad de secuencias de bits codificadas tiene un segundo tamaño de bloque, que puede ser diferente del primer tamaño de bloque para la primera pluralidad de secuencias de bits codificadas.

El valor actual del primer identificador y el valor actual del segundo identificador se proporcionan a un tercer dispositivo de los dispositivos en el trayecto de comunicación, a través de un tercer canal de comunicación seguro, para permitir la decodificación de la cadena de datos (bloque 530). El tercer dispositivo está aguas abajo del segundo dispositivo en el trayecto de comunicación. Por ejemplo, el tercer dispositivo puede ser un destino temporal o final para la cadena de datos.

En algunas situaciones, el método 520 también incluye bloques asociados con la codificación y decodificación de una cadena de datos posterior. Por ejemplo, el método 520 puede incluir bloques en los que se proporcionan nuevos valores para los identificadores primero y segundo en un tiempo posterior cuando la cadena de datos posterior se codifica y transmite. Según el tiempo transcurrido desde la transmisión inicial de la cadena de datos y la frecuencia con la que el servidor actualiza cada valor de identificador, uno o ambos de los nuevos valores pueden diferir de los valores que se habían proporcionado para la cadena de datos anterior (en los bloques 256 y 258).

En algunas realizaciones y/o situaciones, el método 520 se modifica de tal manera que el servidor proporcione los valores actuales tanto del primer identificador como del segundo identificador al primer dispositivo (por ejemplo, un dispositivo de origen), para permitir que el primer dispositivo realice las etapas de codificación dictadas por ambos de esos valores de identificador, en lugar de distribuir la codificación a través de dos dispositivos. En todavía otras realizaciones y/o situaciones, los dispositivos primero y segundo (y posiblemente otros) implementan ambos etapas de codificación, y al menos uno de esos dispositivos implementa múltiples etapas de codificación.

La figura 10 es un diagrama de flujo de un método 540 de ejemplo de decodificación de una cadena de datos transmitida de manera segura, según una realización. El método 540 puede implementarse por uno o más procesadores de un dispositivo electrónico (por ejemplo, uno o más procesadores del dispositivo de destino 104 de la figura 1 o el dispositivo de destino 260 de la figura 5), cuando se ejecutan instrucciones almacenadas en una memoria del dispositivo electrónico, por ejemplo.

En el método 540, se obtiene una cadena de datos codificada (bloque 542). En una situación, la cadena de datos codificada se obtiene al recibir la cadena de datos codificada desde un dispositivo de origen (por ejemplo, después de que la cadena de datos se codifica usando el método 500). En esta situación, la cadena de datos codificada se obtiene recuperando la cadena de datos codificada desde una memoria local del dispositivo electrónico. La cadena de datos codificada puede representar información sensible o potencialmente sensible (por ejemplo, un número de tarjeta de crédito o débito u otra información financiera, información sanitaria personal, un número de la seguridad social, etc.).

Se reciben valores actuales de N identificadores ($N \geq 1$) desde un servidor remoto a través de una interfaz de comunicación del dispositivo electrónico y un canal de comunicación seguro (bloque 544). El bloque 544 puede producirse antes de, simultáneamente a y/o después del bloque 542. Cada uno de los N identificadores está asociado con una entidad respectiva de una pluralidad de entidades, y cada una de esas entidades está asociada con la comunicación de la cadena de datos codificada. Por ejemplo, una entidad puede ser un dispositivo de teclado que se usó para introducir manualmente la información correspondiente a la cadena de datos, una puede ser una persona u organización involucrada en una transacción relacionada con la cadena de datos, una puede ser un dispositivo de red o cortafuegos en el trayecto de comunicación de la cadena de datos, etc. Además, cada una de las entidades corresponde a una operación respectiva de N operaciones de decodificación, donde cada una de las N operaciones de decodificación funciona en bloques de bits que tienen un tamaño de bloque respectivo (por ejemplo, número de bits). Algunas o todas de las N operaciones de decodificación pueden usar diferentes tamaños de bloque.

Una secuencia en la que van a aplicarse las N operaciones de decodificación a la cadena de datos codificada se determina (bloque 546). En una realización, el servidor remoto proporciona datos que indican la secuencia correcta. En otra realización, el dispositivo electrónico que implementa el método 540 conoce la secuencia correcta *a priori*, y determina la secuencia correcta accediendo a las reglas o instrucciones almacenadas en una memoria local.

Se genera una cadena de datos decodificada realizando las N operaciones de decodificación en la cadena de datos codificada según la secuencia determinada en el bloque 546 (bloque 548). El bloque 548 puede incluir, para cada una de las N operaciones de decodificación, analizar al menos una parte de la cadena de datos codificada (o de una cadena de datos parcialmente decodificada resultante de una operación previa de las N operaciones de decodificación) en bloques que tienen el tamaño de bloque respectivo (es decir, el tamaño correspondiente a esa operación de decodificación particular), decodificar por separado cada uno de los bloques que tienen el tamaño de bloque respectivo y, para las primeras $N - 1$ operaciones de decodificación, hacer pasar una cadena de los bloques decodificados por separado a la siguiente de las N operaciones de decodificación.

Se hace que la cadena de datos decodificada se almacene en una memoria local del dispositivo electrónico y/o se transmita a otro dispositivo (bloque 550). El bloque 550 puede realizarse almacenando y/o transmitiendo

directamente la cadena de datos decodificada, o enviando una señal o un mensaje de control a otro dispositivo o unidad que realiza el almacenamiento y/o transmisión, por ejemplo.

IX. ASPECTOS DE LA INVENCIÓN

Aunque el texto anterior establece una descripción detallada de numerosos aspectos y realizaciones diferentes de la invención, debe entenderse que el alcance de la patente está definido por la redacción de las reivindicaciones expuestas al final de esta patente. La descripción detallada debe interpretarse sólo como a modo de ejemplo y no describe todas las realizaciones posibles porque describir cada realización posible sería poco práctico, si no imposible. Pueden implementarse numerosas realizaciones alternativas, usando o bien tecnología actual o bien tecnología desarrollada después de la fecha de presentación de esta patente, que todavía estaría dentro del alcance de las reivindicaciones. A modo de ejemplo, y no de limitación, la divulgación en el presente documento contempla al menos los siguientes aspectos:

Aspecto 1: Un método implementado en un dispositivo electrónico que tiene una interfaz de usuario con una pluralidad de teclas, una interfaz de comunicación, una memoria y uno o más procesadores, comprendiendo el método: (i) detectar, por el uno o más procesadores, un primera entrada por teclado realizada a través de la interfaz de usuario; (ii) recibir, por el uno o más procesadores a través de la interfaz de comunicación y un canal de comunicación seguro, una primera información desde un servidor remoto, incluyendo la primera información al menos un primer valor actual de un primer identificador de capa; (iii) determinar, por el uno o más procesadores y usando el primer valor actual del primer identificador de capa, una primera cadena de bits correspondiente a la primera entrada por teclado; (iv) generar, por el uno o más procesadores y usando la primera cadena de bits, al menos una primera parte de una cadena de datos; y (v) hacer, por el uno o más procesadores, que la cadena de datos uno o ambos de (a) almacene en la memoria y (b) transmita a otro dispositivo a través de una red.

Aspecto 2. El método del aspecto 1, en el que la interfaz de usuario incluye un teclado de hardware, cada tecla de la pluralidad de teclas es una tecla diferente en el teclado de hardware, y la detección de la primera entrada por teclado incluye detectar cuál de la pluralidad de teclas se tocó o presionó.

Aspecto 3. El método del aspecto 1, en el que la interfaz de usuario incluye un teclado virtual presentado en una pantalla de visualización táctil del dispositivo electrónico, cada tecla de la pluralidad de teclas es una tecla diferente en el teclado virtual, y detectar la primera entrada por teclado incluye detectar qué área de la pantalla de visualización táctil se tocó.

Aspecto 4. El método de uno cualquiera de los aspectos 1 a 3, que comprende además solicitar la primera información desde el servidor remoto, en el que recibir la primera información es en respuesta a solicitar la primera información.

Aspecto 5. El método del aspecto 4, en el que solicitar la primera información es o bien (i) en respuesta a detectar la primera entrada por teclado, o bien (ii) antes de detectar la primera entrada por teclado.

Aspecto 6. El método de uno cualquiera de los aspectos 1 a 5, en el que el primer identificador de capa está asociado con una entidad en un registro mantenido por el servidor remoto.

Aspecto 7. El método del aspecto 6, en el que la entidad es uno de (i) el dispositivo electrónico; (ii) una organización asociada con el dispositivo electrónico; o (iii) una persona asociada con una transacción que se realiza a través del dispositivo electrónico.

Aspecto 8. El método de uno cualquiera de los aspectos 1 a 7, en el que la primera información incluye además un primer valor actual de un segundo identificador de capa, y en el que generar al menos una primera parte de una cadena de datos usando la primera cadena de bits incluye: (i) codificar, usando el primer valor actual del segundo identificador de capa, al menos una parte de la primera cadena de bits para generar una segunda cadena de bits; y (ii) generar al menos la primera parte de la cadena de datos usando la segunda cadena de bits.

Aspecto 9. El método del aspecto 8, que comprende además recibir, a través de la interfaz de comunicación y un canal de comunicación seguro, datos que indican un número de capas de codificación que van a aplicarse por el dispositivo electrónico.

Aspecto 10. El método de uno cualquiera de los aspectos 1 a 9, que comprende además: (i) detectar, por el uno o más procesadores, una segunda entrada por teclado realizada a través de la interfaz de usuario; (ii) recibir, por el uno o más procesadores a través de la interfaz de comunicación y el canal de comunicación seguro, una segunda información desde el servidor remoto, incluyendo la segunda información al menos un segundo valor actual del primer identificador de capa; (iii) determinar, por el uno o más procesadores y usando el segundo valor actual del primer identificador de capa, una segunda cadena de bits correspondiente a la segunda entrada por teclado; y (iv) generar, por el uno o más procesadores y usando la segunda cadena de bits, al menos una segunda parte de la cadena de datos.

Aspecto 11. El método del aspecto 10, en el que no se realiza ninguna entrada por teclado a través de la interfaz de

usuario entre la primera entrada por teclado y la segunda entrada por teclado.

Aspecto 12. El método del aspecto 10, en el que: (i) el primer valor actual del primer identificador de capa está asociado con una entidad en un registro mantenido por el servidor remoto en un primer tiempo; y (ii) el segundo valor actual del primer identificador de capa está asociado con la entidad en el registro en un segundo tiempo más tarde que el primer tiempo.

Aspecto 13. El método del aspecto 12, en el que la entidad es uno de: (i) el dispositivo electrónico; (ii) una organización asociada con el dispositivo electrónico; o (iii) una persona asociada con una transacción que se realiza a través del dispositivo electrónico.

Aspecto 14. El método del aspecto 10, en el que: (i) la primera información incluye además un primer valor actual de un segundo identificador de capa; (ii) la segunda información incluye además un segundo valor actual del segundo identificador de capa; (iii) generar al menos la primera parte de la cadena de datos usando la primera cadena de bits incluye (a) codificar, usando el primer valor actual del segundo identificador de capa, al menos una parte de la primera cadena de bits para generar una tercera cadena de bits y (b) generar al menos la primera parte de la cadena de datos usando la tercera cadena de bits; y (iv) generar al menos la segunda parte de la cadena de datos usando la segunda cadena de bits incluye (a) codificar, usando el segundo valor actual del segundo identificador de capa, al menos una parte de la segunda cadena de bits para generar una cuarta cadena de bits, y (b) generar al menos la segunda parte de la cadena de datos usando la cuarta cadena de bits.

Aspecto 15. El método del aspecto 14, que comprende además: (i) solicitar la primera información desde el servidor remoto; y (ii) solicitar la segunda información desde el servidor remoto, en el que recibir la primera información es en respuesta a solicitar la primera información, y en el que recibir la segunda información es en respuesta a solicitar la segunda información.

Aspecto 16. Un dispositivo electrónico que comprende: (i) una interfaz de usuario que incluye una pluralidad de teclas; (ii) una interfaz de comunicación; (iii) una memoria; y (iv) uno o más procesadores configurados para (a) detectar una primera entrada por teclado realizada a través de la interfaz de usuario, (b) recibir la primera información desde un servidor remoto a través de la interfaz de comunicación y un canal de comunicación seguro, incluyendo la primera información al menos un primer valor actual de un primer identificador de capa, (c) determinar, usando el primer valor actual del primer identificador de capa, una primera cadena de bits correspondiente a la primera entrada por teclado, (d) generar al menos una primera parte de una cadena de datos usando la primera cadena de bits, y (e) hacer que la cadena de datos se almacene en la memoria y/o se transmita a otro dispositivo a través de una red.

Aspecto 17. El dispositivo electrónico del aspecto 16, en el que: (i) la interfaz de usuario incluye un teclado físico; (ii) cada tecla de la pluralidad de teclas es una tecla diferente en el teclado de hardware; y (iii) el uno o más procesadores están configurados para detectar la primera entrada por teclado detectando al menos cuál de la pluralidad de teclas se tocó o presionó.

Aspecto 18. El dispositivo electrónico del aspecto 16, en el que: (i) la interfaz de usuario incluye un teclado virtual presentado en una pantalla de visualización táctil del dispositivo electrónico; (ii) cada tecla de la pluralidad de teclas es una tecla diferente en el teclado virtual; y (iii) el uno o más procesadores están configurados para detectar la primera entrada por teclado detectando al menos qué área de la pantalla de visualización táctil se tocó.

Aspecto 19. El dispositivo electrónico de uno cualquiera de los aspectos 16 a 18, en el que la primera información incluye además un primer valor actual de un segundo identificador de capa, y en el que el uno o más procesadores están configurados para generar al menos la primera parte de la cadena de datos usando la primera cadena de bits al menos mediante: (i) codificar, usando el primer valor actual del segundo identificador de capa, al menos una parte de la primera cadena de bits para generar una segunda cadena de bits; y (ii) generar al menos la primera parte de la cadena de datos usando la segunda cadena de bits.

Aspecto 20. El dispositivo electrónico de uno cualquiera de los aspectos 16 a 18, en el que el uno o más procesadores están configurados además para: (i) detectar una segunda entrada por teclado realizada a través de la interfaz de usuario; (ii) recibir, a través de la interfaz de comunicación y el canal de comunicación seguro, una segunda información desde el servidor remoto, incluyendo la segunda información al menos un segundo valor actual del primer identificador de capa; (iii) determinar, usando el segundo valor actual del primer identificador de capa, una segunda cadena de bits correspondiente a la segunda entrada por teclado; y (iv) generar, usando la segunda cadena de bits, al menos una segunda parte de la cadena de datos.

Aspecto 21. Un método, implementado en un servidor que incluye uno o más procesadores y una memoria que almacena una base de datos de registro, para proporcionar una comunicación segura de una cadena de datos a lo largo de un trayecto de comunicación que incluye una pluralidad de dispositivos, comprendiendo el método: (i) añadir a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad; (ii) añadir a la base de datos de registro una segunda entidad y un segundo identificador asociado con la segunda entidad; (iii) proporcionar a un primer dispositivo de la pluralidad de dispositivos, a través de un primer canal de comunicación seguro, un primer valor actual del primer identificador para permitir una primera codificación de la

cadena de datos, en el que el primer dispositivo está asociado con la primera entidad, y en el que la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas; (iv) proporcionar a un segundo dispositivo de la pluralidad de dispositivos, a través de un segundo canal de comunicación seguro, un primer valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos, en el que el segundo dispositivo está asociado con la segunda entidad y aguas abajo del primer dispositivo en el trayecto de comunicación, y en el que la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas; y (v) proporcionar a un tercer dispositivo de la pluralidad de dispositivos, a través de un tercer canal de comunicación seguro, el primer valor actual del primer identificador y el primer valor actual del segundo identificador para permitir la decodificación de la cadena de datos, en el que el tercer el dispositivo está aguas abajo del segundo dispositivo en el trayecto de comunicación.

Aspecto 22. El método del aspecto 21, en el que cada una de la primera pluralidad de secuencias de bits codificadas tiene un primer tamaño de bloque, y cada una de la segunda pluralidad de secuencias de bits codificadas tiene un segundo tamaño de bloque diferente del primer tamaño de bloque.

Aspecto 23. El método del aspecto 21 o 22, en el que la primera entidad es uno de: (i) el primer dispositivo; (ii) una persona; o (iii) una organización.

Aspecto 24. El método de uno cualquiera de los aspectos 21 a 23, en el que el segundo dispositivo es un dispositivo de red, y la segunda entidad es uno de: (i) el dispositivo de red; o (ii) un cortafuegos implementado por el segundo dispositivo.

Aspecto 25. El método de uno cualquiera de los aspectos 21 a 24, que comprende además: (i) proporcionar al primer dispositivo, a través del primer canal de comunicación seguro, un segundo valor actual del primer identificador para permitir una primera codificación de una cadena de datos posterior, en el que la primera codificación de la cadena de datos posterior codifica una pluralidad de secuencias de bits en la cadena de datos posterior como una tercera pluralidad de secuencias de bits codificadas; (ii) proporcionar al segundo dispositivo, a través del segundo canal de comunicación seguro, un segundo valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos posterior, en el que la segunda codificación de la cadena de datos posterior codifica la tercera pluralidad de secuencias de bits codificadas como una cuarta pluralidad de secuencias de bits codificadas; y (iii) proporcionar al tercer dispositivo, a través del tercer canal de comunicación seguro, el segundo valor actual del primer identificador y el segundo valor actual del segundo identificador para permitir la decodificación de la cadena de datos posterior, en el que uno o ambos de (i) el segundo valor actual del primer identificador es diferente del primer valor actual del primer identificador, o (ii) el segundo valor actual del segundo identificador es diferente del primer valor actual del segundo identificador.

Aspecto 26. El método de uno cualquiera de los aspectos 21 a 25, en el que uno o ambos de: (i) proporcionar al primer dispositivo el primer valor actual del primer identificador es en respuesta a recibir una petición desde el primer dispositivo; y (ii) proporcionar al segundo dispositivo el primer valor actual del segundo identificador es en respuesta a recibir una petición desde el segundo dispositivo.

Aspecto 27. Un método, implementado en un servidor que incluye uno o más procesadores y una memoria que almacena una base de datos de registro, para proporcionar una comunicación segura de una cadena de datos, comprendiendo el método: (i) añadir a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad; (ii) añadir a la base de datos de registro una segunda entidad y un segundo identificador asociado con la segunda entidad; (iii) proporcionar a un dispositivo de origen asociado con la primera entidad y la segunda entidad, a través de un primer canal de comunicación seguro, tanto (a) un primer valor actual del primer identificador para permitir una primera codificación de la cadena de datos, en el que la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas, como (b) un primer valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos, en el que la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas; y (iv) proporcionar a un dispositivo de destino, a través de un segundo canal de comunicación seguro, el primer valor actual del primer identificador y el primer valor actual del segundo identificador para permitir la decodificación de la cadena de datos.

Aspecto 28. El método del aspecto 27, en el que cada una de la primera pluralidad de secuencias de bits codificadas tiene un primer tamaño de bloque, y cada una de la segunda pluralidad de secuencias de bits codificadas tiene un segundo tamaño de bloque diferente del primer tamaño de bloque.

Aspecto 29. El método del aspecto 27 o 28, en el que la primera entidad y la segunda entidad son entidades diferentes de: (i) el dispositivo de origen; (ii) una persona; o (iii) una organización.

Aspecto 30. El método de uno cualquiera de los aspectos 27 a 29, que comprende además: (i) proporcionar al dispositivo de origen, a través del primer canal de comunicación seguro, tanto (a) un segundo valor actual del primer identificador para permitir una primera codificación de una cadena de datos posterior, en el que la primera

codificación de la cadena de datos posterior codifica una pluralidad de secuencias de bits en la cadena de datos posterior como una tercera pluralidad de secuencias de bits codificadas, como (b) un segundo valor actual del segundo identificador para permitir un segunda codificación de la cadena de datos posterior, en el que la segunda codificación de la cadena de datos posterior codifica la tercera pluralidad de secuencias de bits codificadas como una cuarta pluralidad de secuencias de bits codificadas; y (ii) proporcionar al tercer dispositivo, a través del tercer canal de comunicación seguro, el segundo valor actual del primer identificador y el segundo valor actual del segundo identificador para permitir la decodificación de la cadena de datos posterior, en el que el segundo valor actual del primer identificador es diferente del primer valor actual del primer identificador y/o el segundo valor actual del segundo identificador es diferente del primer valor actual del segundo identificador.

Aspecto 31. El método de uno cualquiera de los aspectos 27 a 30, en el que proporcionar al primer dispositivo uno o ambos de (i) el primer valor actual del primer identificador, y (ii) el primer valor actual del segundo identificador es en respuesta a recibir una petición desde el primer dispositivo.

Aspecto 32. Un método, implementado en un dispositivo electrónico que tiene uno o más procesadores, una interfaz de comunicación y una memoria, comprendiendo el método: (i) obtener, por el uno o más procesadores, una cadena de datos codificada; (ii) recibir, por el uno o más procesadores a través de la interfaz de comunicación y un canal de comunicación seguro, valores actuales de *N* identificadores desde un servidor remoto, en el que cada uno de los *N* identificadores (a) está asociado con una entidad respectiva de una pluralidad de entidades, estando asociada cada una de la pluralidad de entidades con la comunicación de la cadena de datos codificada, y (b) corresponde a una operación respectiva de *N* operaciones de decodificación, funcionando cada una de las *N* operaciones de decodificación en bloques de bits que tienen un tamaño de bloque respectivo, y siendo *N* un número entero mayor de 1; (iii) determinar, por el uno o más procesadores, una secuencia en la que *N* operaciones de decodificación van a aplicarse a la cadena de datos codificada; (iv) generar, por el uno o más procesadores, una cadena de datos decodificada realizando las *N* operaciones de decodificación en la cadena de datos codificada según la secuencia determinada, en el que realizar las *N* operaciones de decodificación incluye, para cada operación de decodificación de las *N* operaciones de decodificación, (a) analizar al menos una parte de la cadena de datos codificada, o al menos una parte de una cadena de datos parcialmente decodificada resultante de una operación previa de las *N* operaciones de decodificación, en bloques que tienen el tamaño de bloque respectivo, (b) decodificar por separado cada uno de los bloques que tienen el tamaño de bloque respectivo, y (c) para las primeras *N* - 1 operaciones de decodificación, hacer pasar una cadena de los bloques decodificados por separado a la siguiente operación de las *N* operaciones de decodificación; y (v) hacer, por el uno o más procesadores, que la cadena de datos decodificada uno o ambos de (i) se almacene en la memoria y (ii) se transmita a otro dispositivo.

Aspecto 33. El método del aspecto 32, en el que obtener la cadena de datos codificada incluye recibir la cadena de datos codificada desde otro dispositivo electrónico a través de una red.

Aspecto 34. El método del aspecto 32, en el que obtener la cadena de datos codificada incluye recuperar la cadena de datos codificada de la memoria del dispositivo electrónico.

Aspecto 35. El método de un aspecto cualquiera de los aspectos 32 a 34, en el que determinar la secuencia en la que van a aplicarse las *N* operaciones de decodificación a la cadena de datos codificada incluye recibir, a través de la interfaz de comunicación y el canal de comunicación seguro, una indicación de la secuencia.

Aspecto 36. El método de uno cualquiera de los aspectos 32 a 35, en el que la pluralidad de entidades incluye dos o más de: (i) otro dispositivo electrónico en el que se introdujo manualmente información correspondiente a la cadena de datos codificada; (ii) una persona; (iii) una organización; (iv) un dispositivo de red; o (v) un cortafuegos.

Aspecto 37. Un servidor que comprende: (i) una primera memoria que almacena una base de datos de registro; (ii) una segunda memoria que almacena instrucciones; y (iii) uno o más procesadores están configurados para ejecutar las instrucciones para (a) añadir a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad, (b) añadir a la base de datos de registro una segunda entidad y una segunda identificador asociado con la segunda entidad, (c) proporcionar a un primer dispositivo de una pluralidad de dispositivos en un trayecto de comunicación para una cadena de datos, a través de un primer canal de comunicación seguro, un primer valor actual del primer identificador para permitir una primera codificación de la cadena de datos, en el que el primer dispositivo está asociado con la primera entidad, y en el que la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas, (d) proporcionar a un segundo dispositivo de la pluralidad de dispositivos, a través de un segundo canal de comunicación seguro, un primer valor actual del segundo identificador para permitir una segunda codificación de la cadena de datos, en el que el segundo dispositivo está asociado con la segundo entidad y aguas abajo del primer dispositivo en el trayecto de comunicación, y en el que la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas, y (e) proporcionar a un tercer dispositivo de la pluralidad de dispositivos, a través de un tercer canal de comunicación seguro, el primer valor actual del primer identificador y el primer valor actual del segundo identificador para permitir la decodificación de la cadena de datos, en el que el tercer dispositivo está aguas abajo del segundo dispositivo en el trayecto de comunicación.

Aspecto 38. El servidor del aspecto 37, en el que cada una de la primera pluralidad de secuencias de bits codificadas tiene un primer tamaño de bloque, y cada una de la segunda pluralidad de secuencias de bits codificadas tiene un segundo tamaño de bloque diferente del primer tamaño de bloque.

Aspecto 39. El servidor del aspecto 37 o 38, en el que la primera entidad es uno de: (i) el primer dispositivo; (ii) una persona; o (iii) una organización.

Aspecto 40. El servidor de uno cualquiera de los aspectos 37 a 40, en el que el segundo dispositivo es un dispositivo de red, y la segunda entidad es uno de: (i) el dispositivo de red; o (ii) un cortafuegos implementado por el segundo dispositivo.

X. OTRAS CONSIDERACIONES

Las diversas operaciones de los métodos de ejemplo descritos en el presente documento pueden realizarse, al menos parcialmente, por uno o más procesadores que están configurados temporalmente por ejemplo, por software) o configurados permanentemente para realizar las operaciones relevantes. Ya estén configurados temporal o permanentemente, tales procesadores pueden constituir módulos implementados por procesador que funcionan para realizar una o más operaciones o funciones. Los módulos a los que se hace referencia en el presente documento pueden comprender, en alguna realización de ejemplo, módulos implementados por procesador.

De manera similar, los métodos o las rutinas descritos en el presente documento pueden implementarse al menos parcialmente por procesador. Por ejemplo, al menos algunas de las operaciones de un método pueden realizarse por uno o más procesadores o módulos de hardware implementados por procesador. El rendimiento de ciertas operaciones puede distribuirse entre uno o más procesadores, no sólo residiendo dentro de una única máquina, sino desplegarse a través de varias máquinas. En una realización, el procesador o procesadores pueden estar ubicados en una única ubicación (por ejemplo, dentro de un entorno doméstico, un entorno de oficina o como una granja de servidores), aunque en otras realizaciones los procesadores pueden distribuirse a través de varias ubicaciones.

El rendimiento de ciertas operaciones puede distribuirse entre el uno o más procesadores, no sólo residiendo dentro de una única máquina, sino desplegarse a través de varias máquinas. En algunas realizaciones de ejemplo, el uno o más procesadores o módulos implementados por procesador pueden estar ubicados en una única ubicación geográfica (por ejemplo, dentro de un entorno doméstico, un entorno de oficina o una granja de servidores). En otras realizaciones de ejemplo, el uno o más procesadores o módulos implementados por procesador pueden distribuirse a través de varias ubicaciones geográficas.

A menos que se indique específicamente lo contrario, los comentarios en el presente documento que usan términos tales como “procesamiento”, “informática”, “cálculo”, “determinación”, “presentación”, “visualización” o similares pueden referirse a acciones o procesos de una máquina (por ejemplo, un ordenador) que manipula o transforma datos representados como cantidades físicas (por ejemplo, electrónicas, magnéticas u ópticas) en una o más memorias (por ejemplo, memoria volátil, memoria no volátil, o una combinación de las mismas), registros u otros componentes de máquina que reciben, almacenan, transmiten o visualizan información.

Tal como se usa en el presente documento, cualquier referencia a “una realización” o “una única realización” significa que un elemento, rasgo, una estructura o característica particular descritos en relación con la realización se incluye en al menos una realización. Las apariciones de la expresión “en una realización” en varios lugares de la memoria descriptiva no se refieren necesariamente a la misma realización.

Tal como se usa en el presente documento, los términos “comprende”, “que comprende”, “incluye”, “que incluye”, “tiene”, “que tiene” o cualquier otra variación de los mismos, están destinados a cubrir una inclusión no exclusiva. Por ejemplo, un proceso, método, artículo o aparato que comprende una lista de elementos no se limita necesariamente sólo a esos elementos sino que puede incluir otros elementos que no se enumeran expresamente o son inherentes a dicho proceso, método, artículo o aparato. Además, a menos que se indique expresamente lo contrario, “o” se refiere a un o inclusivo y no a un o exclusivo. Por ejemplo, una condición A o B es satisfecha por cualquiera de los siguientes: A es verdadero (o presente) y B es falso (o no presente), A es falso (o no presente) y B es verdadero (o presente), y tanto A como B son verdaderos (o presentes).

Además, el uso de “un(o)” o “una” se emplean para describir elementos y componentes de las realizaciones en el presente documento. Esto se realiza simplemente por conveniencia y para dar una idea general de la descripción. Esta descripción, y las siguientes reivindicaciones, deben leerse como que incluyen uno o al menos uno y el singular también incluye el plural a menos que sea obvio que quiere decirse lo contrario. Esta descripción detallada debe interpretarse como ejemplos y no describe todas las realizaciones posibles, ya que describir todas las realizaciones posibles sería poco práctico, si no imposible. Pueden implementarse numerosas realizaciones alternativas, usando o bien tecnología actual o bien tecnología desarrollada después de la fecha de presentación de esta solicitud.

REIVINDICACIONES

1. Un método, implementado en un servidor (110) que incluye uno o más procesadores y una memoria que almacena una base de datos de registro (112), para proporcionar una comunicación segura de una cadena de datos a lo largo de un trayecto de comunicación (250) que incluye una pluralidad de dispositivos, comprendiendo el método:

añadir a la base de datos de registro (112) una primera entidad y un primer identificador asociado con la primera entidad;

añadir (524) a la base de datos de registro una segunda entidad y un segundo identificador asociado con la segunda entidad, en el que la segunda entidad es diferente de la primera entidad;

proporcionar a un primer dispositivo (404) de la pluralidad de dispositivos, a través de un primer canal de comunicación seguro, un primer valor actual del primer identificador asociado con la primera entidad para permitir una primera codificación de la cadena de datos, en el que el primer dispositivo está asociado con la primera entidad, y en el que la primera codificación de la cadena de datos (526) codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas;

proporcionar (528) a un segundo dispositivo de la pluralidad de dispositivos, a través de un segundo canal de comunicación seguro, un primer valor actual del segundo identificador asociado con la segunda entidad para permitir una segunda codificación de la cadena de datos, en el que el segundo dispositivo es diferente del primer dispositivo, está asociado con la segunda entidad, y está aguas abajo del primer dispositivo en el trayecto de comunicación, y en el que la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas; y

proporcionar (530) a un tercer dispositivo de la pluralidad de dispositivos, a través de un tercer canal de comunicación seguro, el primer valor actual del primer identificador asociado con la primera entidad y el primer valor actual del segundo identificador asociado con la segunda entidad para permitir la decodificación de la cadena de datos, en el que el tercer dispositivo es diferente del primer dispositivo y el segundo dispositivo, y está aguas abajo del segundo dispositivo en el trayecto de comunicación (250),

en el que el primer identificador cambia su valor en una primera frecuencia dictada por un nivel de seguridad asociado con la primera entidad, y

en el que el segundo identificador cambia su valor en una segunda frecuencia dictada por un nivel de seguridad asociado con la segunda entidad, siendo la segunda frecuencia diferente de la primera frecuencia.

2. El método según la reivindicación 1, en el que cada una de la primera pluralidad de secuencias de bits codificadas tiene un primer tamaño de bloque, y cada una de la segunda pluralidad de secuencias de bits codificadas tiene un segundo tamaño de bloque diferente del primer tamaño de bloque.

3. El método según la reivindicación 1, en el que la primera entidad es uno de:

el primer dispositivo

una persona; o

una organización.

4. El método según la reivindicación 1, en el que el segundo dispositivo es un dispositivo de red, y la segunda entidad es uno de:

el dispositivo de red; o

un cortafuegos implementado por el segundo dispositivo.

5. El método según la reivindicación 1, que comprende además:

proporcionar al primer dispositivo, a través del primer canal de comunicación seguro, un segundo valor actual del primer identificador asociado con la primera entidad para permitir una primera codificación de una cadena de datos posterior, en el que la primera codificación de la cadena de datos posterior codifica una pluralidad de secuencias de bits en la cadena de datos posterior como una tercera pluralidad de secuencias de bits codificadas;

proporcionar al segundo dispositivo, a través del segundo canal de comunicación seguro, un segundo valor actual del segundo identificador asociado con la segunda entidad para permitir una segunda codificación de

la cadena de datos posterior, en el que la segunda codificación de la cadena de datos posterior codifica la tercera pluralidad de secuencias de bits codificadas como una cuarta pluralidad de secuencias de bits codificadas; y

proporcionar al tercer dispositivo, a través del tercer canal de comunicación seguro, el segundo valor actual del primer identificador asociado con la primera entidad y el segundo valor actual del segundo identificador asociado con la segunda entidad para permitir la decodificación de la cadena de datos posterior,

en el que uno o ambos de (i) el segundo valor actual del primer identificador asociado con la primera entidad es diferente del primer valor actual del primer identificador asociado con la primera entidad, o (ii) el segundo valor actual del segundo identificador asociado con la segunda entidad es diferente del primer valor actual del segundo identificador asociado con la segunda entidad.

6. El método según la reivindicación 1, en el que uno o ambos de:

proporcionar al primer dispositivo el primer valor actual del primer identificador asociado con la primera entidad es en respuesta a recibir una petición del primer dispositivo; y

proporcionar al segundo dispositivo el primer valor actual del segundo identificador asociado con la segunda entidad es en respuesta a recibir una petición del segundo dispositivo.

7. Un servidor (110) que comprende:

una primera memoria que almacena una base de datos de registro (112);

una segunda memoria que almacena instrucciones; y

uno o más procesadores están configurados para ejecutar las instrucciones para

añadir (522) a la base de datos de registro una primera entidad y un primer identificador asociado con la primera entidad,

añadir a la base de datos de registro una segunda entidad y un segundo identificador (524) asociado con la segunda entidad, en el que la segunda entidad es diferente de la primera entidad,

proporcionar (526) a un primer dispositivo de una pluralidad de dispositivos en un trayecto de comunicación para una cadena de datos, a través de un primer canal de comunicación seguro, un primer valor actual del primer identificador asociado con la primera entidad para permitir una primera codificación de la cadena de datos,

en el que el primer dispositivo está asociado con la primera entidad, y en el que la primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos como una primera pluralidad de secuencias de bits codificadas,

proporcionar (528) a un segundo dispositivo de la pluralidad de dispositivos, a través de un segundo canal de comunicación seguro, un primer valor actual del segundo identificador asociado con la segunda entidad para permitir una segunda codificación de la cadena de datos, en el que el segundo dispositivo es diferente del primer dispositivo, está asociado con la segunda entidad y está aguas abajo del primer dispositivo en el trayecto de comunicación, y en el que la segunda codificación de la cadena de datos codifica la primera pluralidad de secuencias de bits codificadas como una segunda pluralidad de secuencias de bits codificadas, y

proporcionar (530) a un tercer dispositivo de la pluralidad de dispositivos, a través de un tercer canal de comunicación seguro, el primer valor actual del primer identificador asociado con la primera entidad y el primer valor actual del segundo identificador asociado con la segunda entidad para permitir la decodificación de la cadena de datos, en el que el tercer dispositivo es diferente del primer dispositivo y el segundo dispositivo, y está aguas abajo del segundo dispositivo en el trayecto de comunicación,

en el que el primer identificador cambia su valor en una primera frecuencia dictada por un nivel de seguridad asociado con la primera entidad, y

en el que el segundo identificador cambia su valor en una segunda frecuencia dictada por un nivel de seguridad asociado con la segunda entidad, siendo la segunda frecuencia diferente de la primera frecuencia.

8. El servidor según la reivindicación 7, en el que cada una de la primera pluralidad de secuencias de bits codificadas tiene un primer tamaño de bloque, y cada una de la segunda pluralidad de secuencias de bits codificadas tiene un segundo tamaño de bloque diferente del primer tamaño de bloque.

9. El servidor según la reivindicación 7, en el que la primera entidad es uno de:

el primer dispositivo

una persona; o

una organización.

10. El servidor según la reivindicación 7, en el que el segundo dispositivo es un dispositivo de red, y la segunda entidad es uno de:

el dispositivo de red; o

un cortafuegos implementado por el segundo dispositivo.

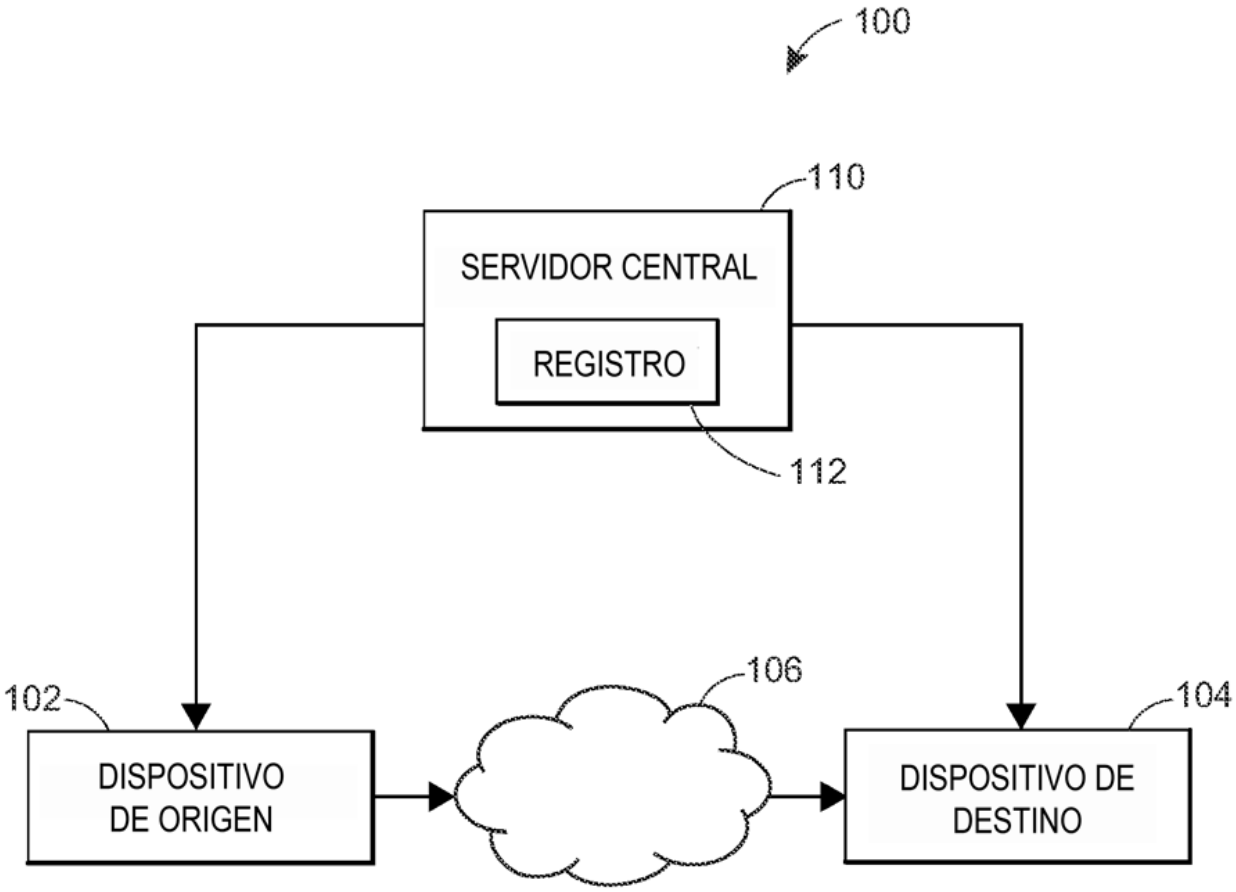
100
110
SERVIDOR CENTRAL
REGISTRO
112
102
106
104
DISPOSITIVO DE ORIGEN
DISPOSITIVO DE DESTINO

FIG. 1

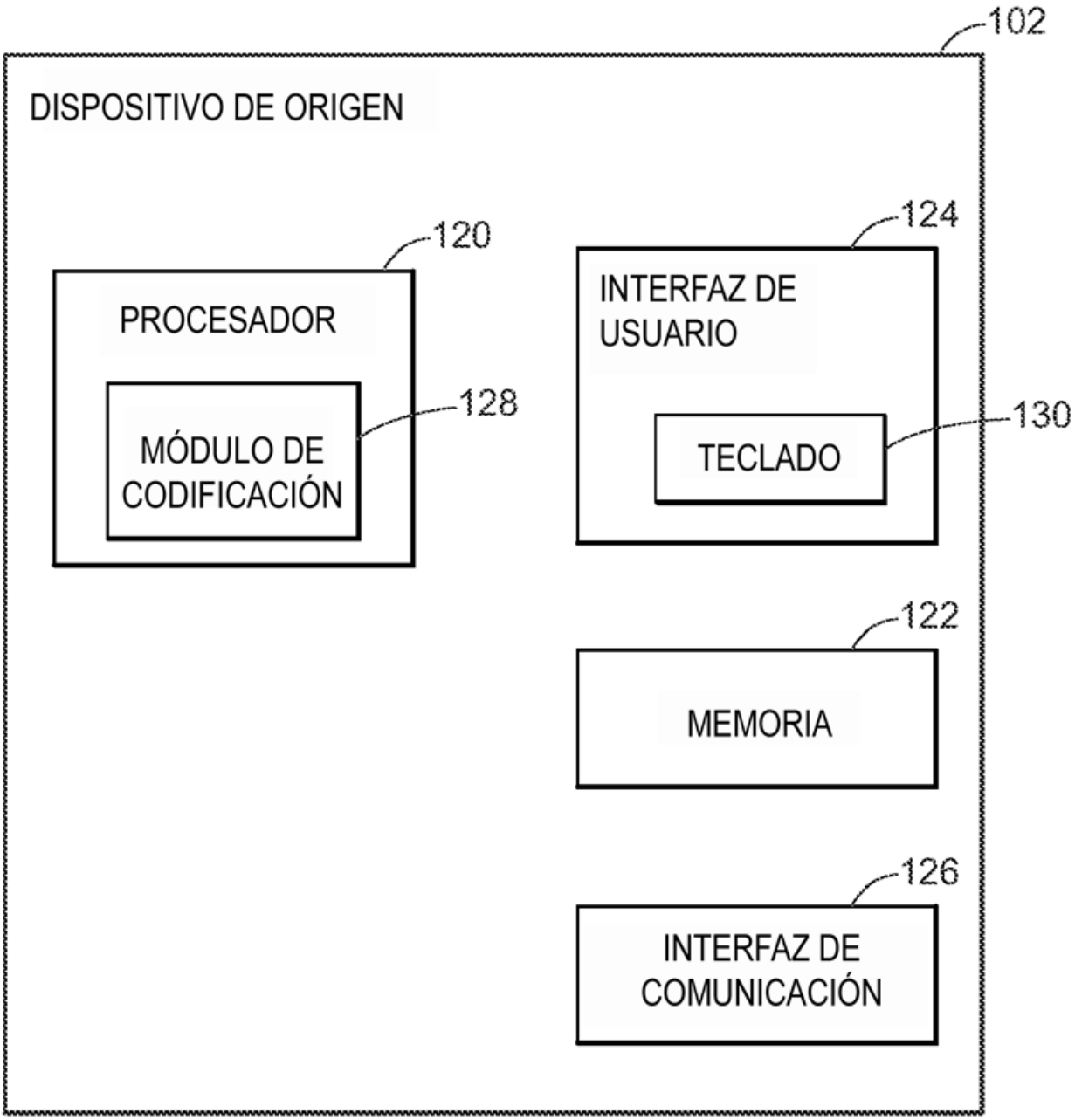
102
DISPOSITIVO DE ORIGEN
120
PROCESADOR
128
MÓDULO DE CODIFICACIÓN
124
INTERFAZ DE USUARIO
130
TECLADO
122
MEMORIA
126
INTERFAZ DE COMUNICACIÓN

FIG. 2

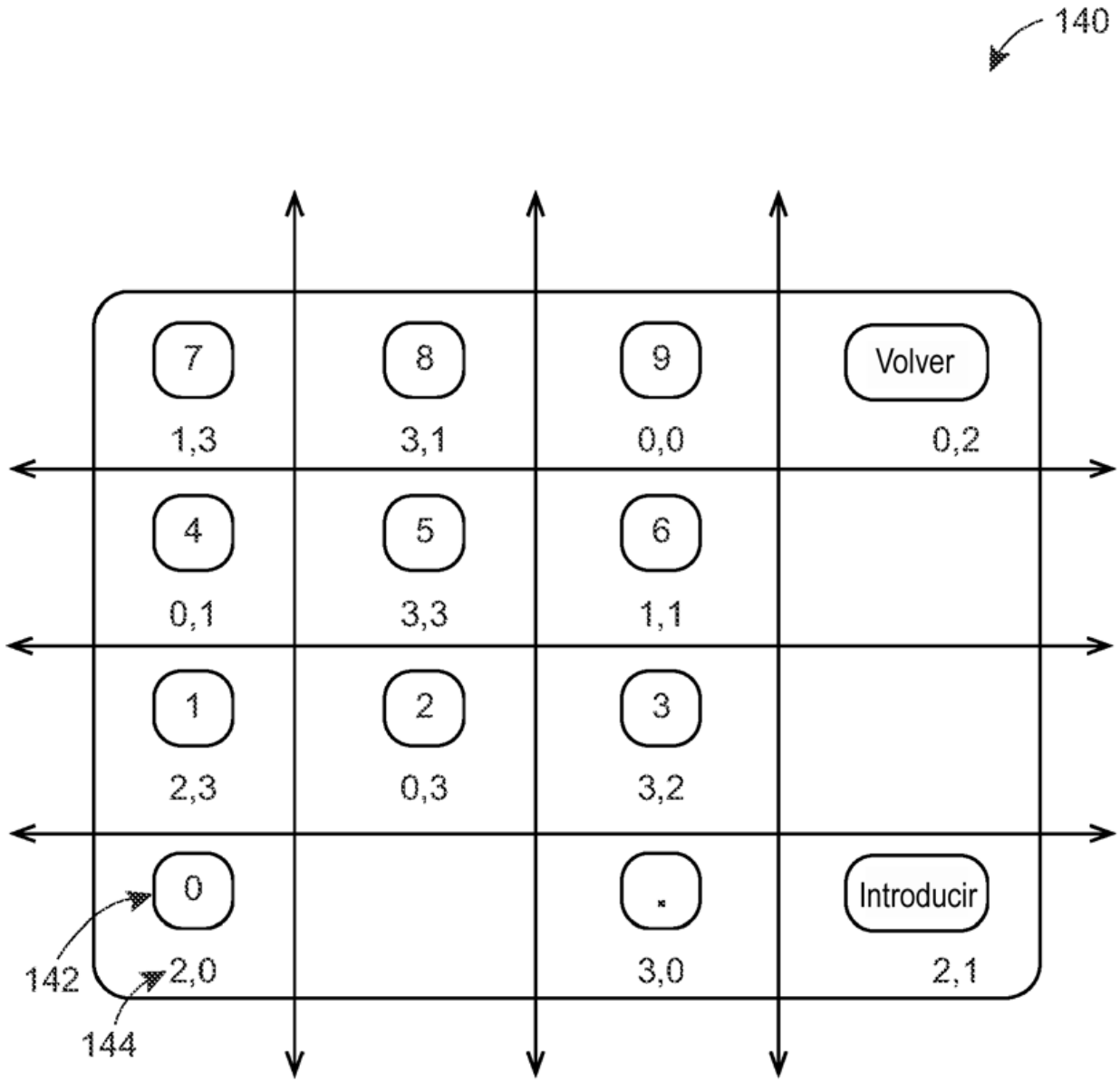
140
7
8
9
Volver
1,3
3,1
0,0
0,2
4
5
6
0,1
3,3
1,1
1
2
3
2,3
0,3
3,2
0
.
Introducir
142
2,0
3,0
2,1
144

FIG. 3

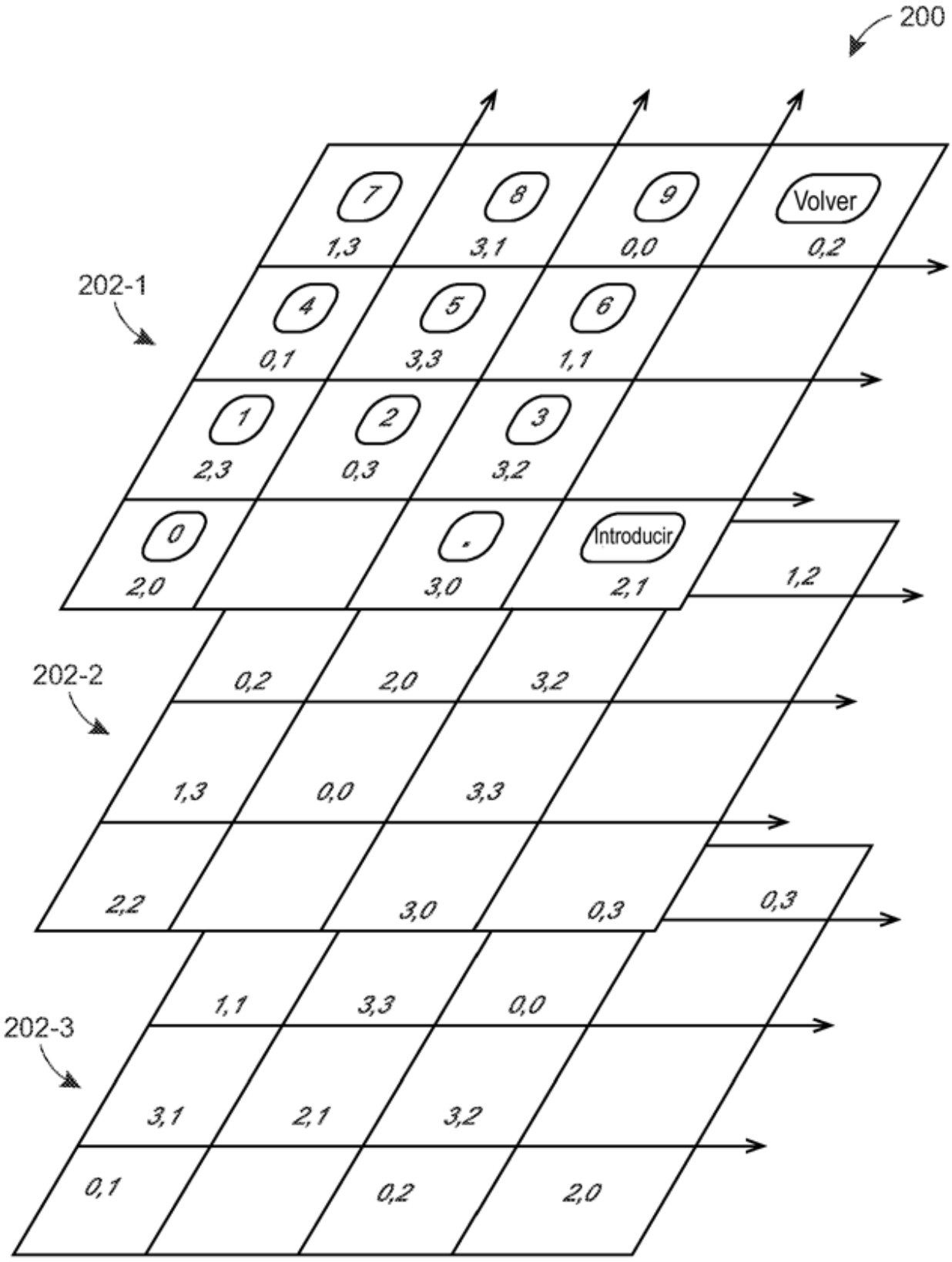
200
202-1
202-2
202-3
7
8
9
Volver
1,3
3,1
0,0
0,2
4
5
6
0,1
3,3
1,1
1
2
3
2,3
0,3
3,2
0
.
Introducir
2,0
3,0
2,1
1,2
0,2
2,0
3,2
1,3
0,0
3,3
2,2
3,0
0,3
0,3
1,1
3,3
0,0
3,1
2,1
3,2
0,1
0,2
2,0

FIG. 4

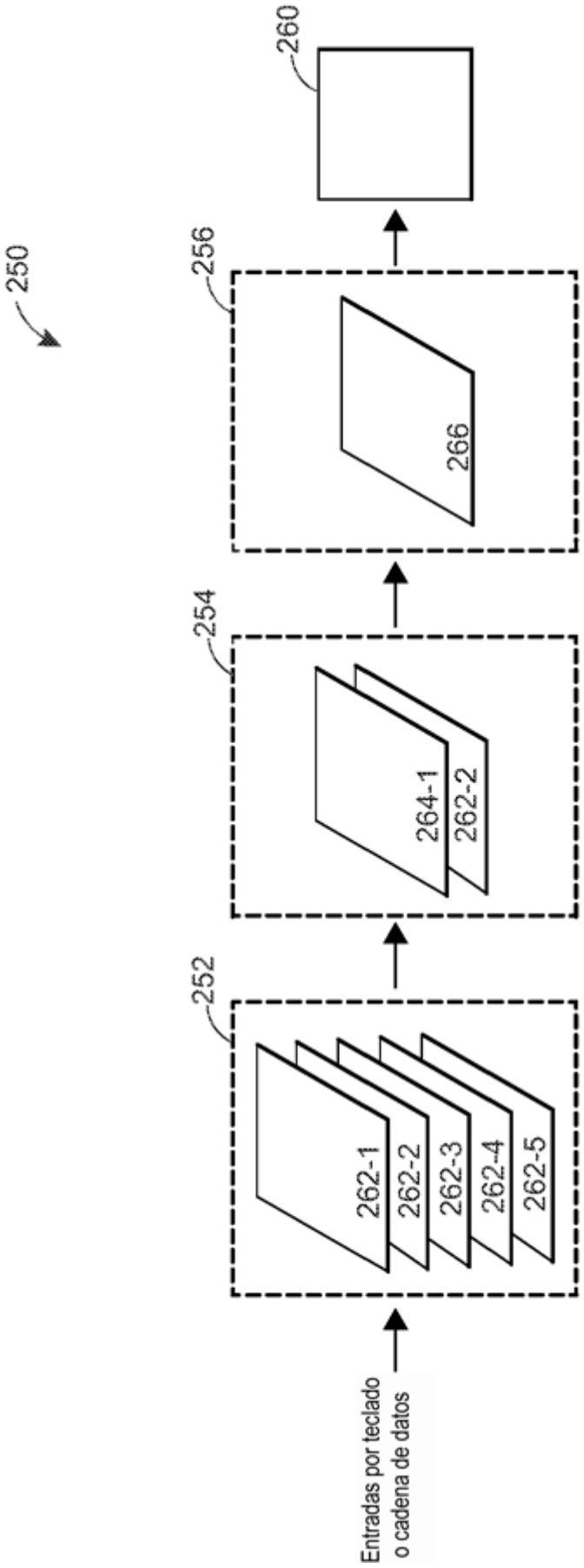
250
252
262-1
262-2
262-3
262-4
262-5
254
264-1
262-2
256
266
260
Entradas por teclado
o cadena de datos

FIG. 5

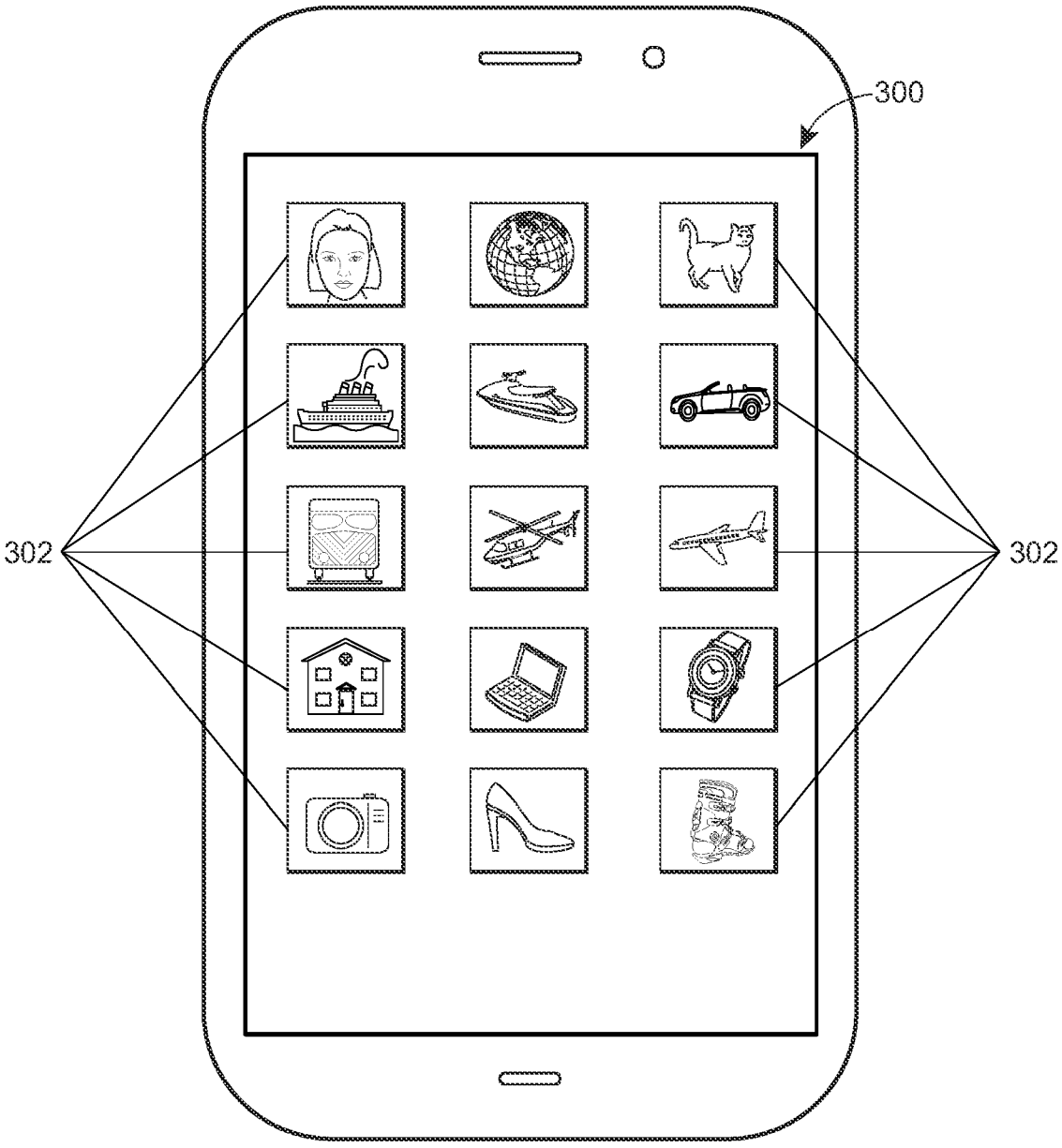

FIG. 6

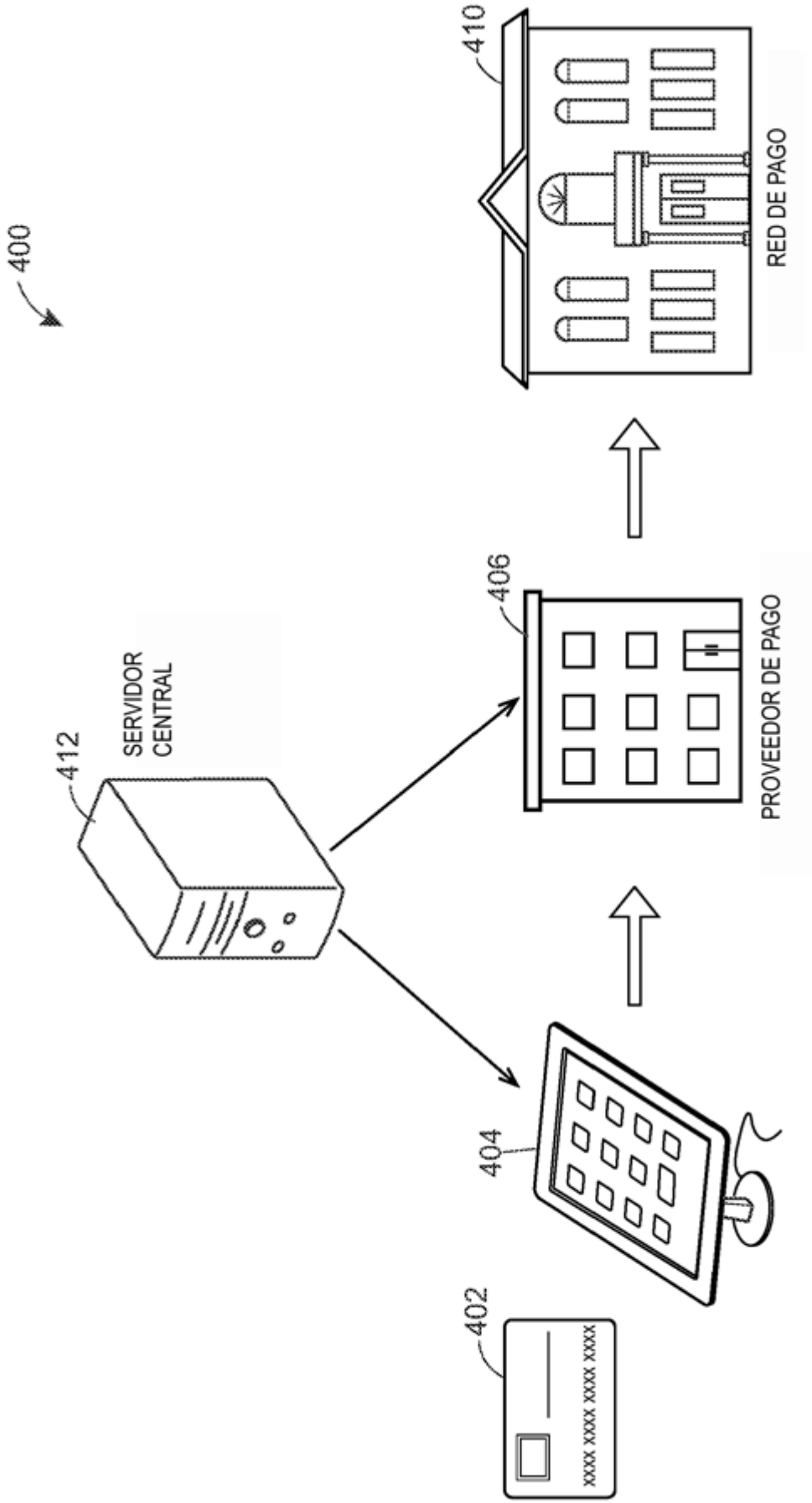
400
410
RED DE PAGO
406
PROVEEDOR DE PAGO
412
SERVIDOR CENTRAL
404
402
xxxx xxxx xxxx xxxx

FIG. 7

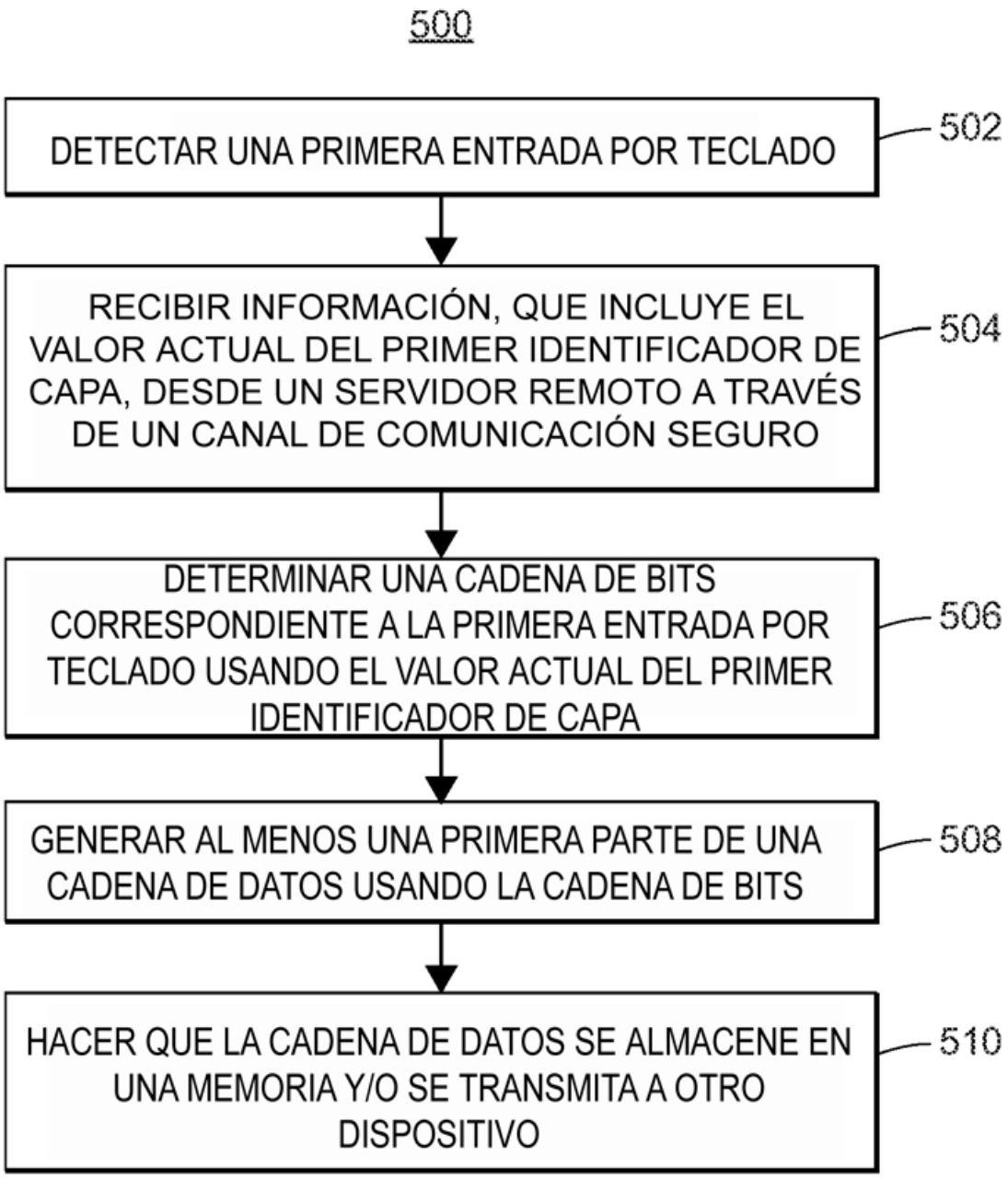
500
DETECTAR UNA PRIMERA ENTRADA POR TECLADO
502
RECIBIR INFORMACIÓN, QUE INCLUYE EL VALOR ACTUAL DEL PRIMER IDENTIFICADOR DE CAPA, DESDE UN SERVIDOR REMOTO A TRAVÉS DE UN CANAL DE COMUNICACIÓN SEGURO
504
DETERMINAR UNA CADENA DE BITS CORRESPONDIENTE A LA PRIMERA ENTRADA POR TECLADO USANDO EL VALOR ACTUAL DEL PRIMER IDENTIFICADOR DE CAPA
506
GENERAR AL MENOS UNA PRIMERA PARTE DE UNA CADENA DE DATOS USANDO LA CADENA DE BITS
508
HACER QUE LA CADENA DE DATOS SE ALMACENE EN UNA MEMORIA Y/O SE TRANSMITA A OTRO DISPOSITIVO
510

FIG. 8

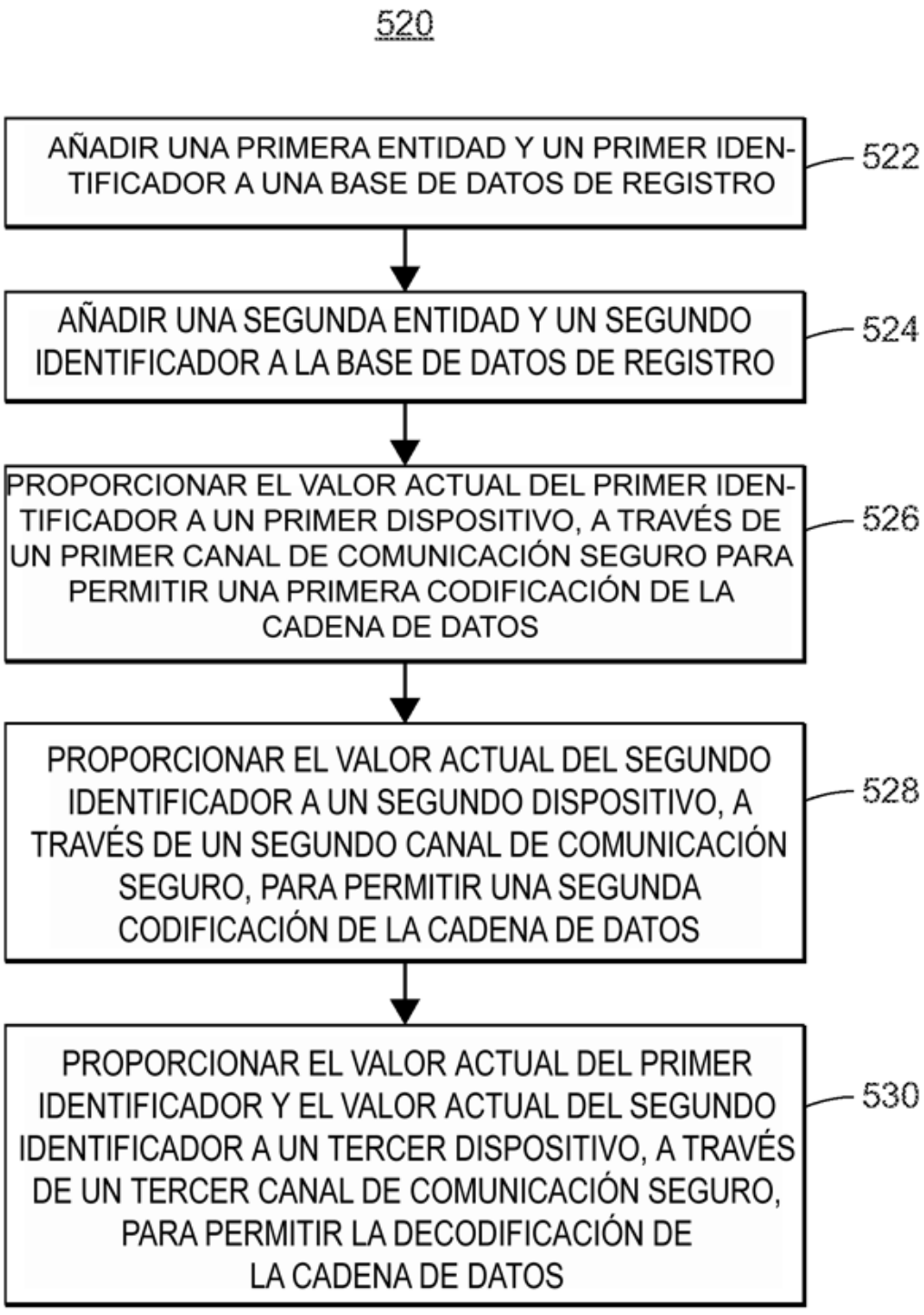
520
AÑADIR UNA PRIMERA ENTIDAD Y UN PRIMER IDENTIFICADOR A UNA BASE DE DATOS DE REGISTRO
522
AÑADIR UNA SEGUNDA ENTIDAD Y UN SEGUNDO IDENTIFICADOR A LA BASE DE DATOS DE REGISTRO
524
PROPORCIONAR EL VALOR ACTUAL DEL PRIMER IDENTIFICADOR A UN PRIMER DISPOSITIVO, A TRAVÉS DE UN PRIMER CANAL DE COMUNICACIÓN SEGURO PARA PERMITIR UNA PRIMERA CODIFICACIÓN DE LA CADENA DE DATOS
526
PROPORCIONAR EL VALOR ACTUAL DEL SEGUNDO IDENTIFICADOR A UN SEGUNDO DISPOSITIVO, A TRAVÉS DE UN SEGUNDO CANAL DE COMUNICACIÓN SEGURO, PARA PERMITIR UNA SEGUNDA CODIFICACIÓN DE LA CADENA DE DATOS
528
PROPORCIONAR EL VALOR ACTUAL DEL PRIMER IDENTIFICADOR Y EL VALOR ACTUAL DEL SEGUNDO IDENTIFICADOR A UN TERCER DISPOSITIVO, A TRAVÉS DE UN TERCER CANAL DE COMUNICACIÓN SEGURO, PARA PERMITIR LA DECODIFICACIÓN DE LA CADENA DE DATOS
530

FIG. 9

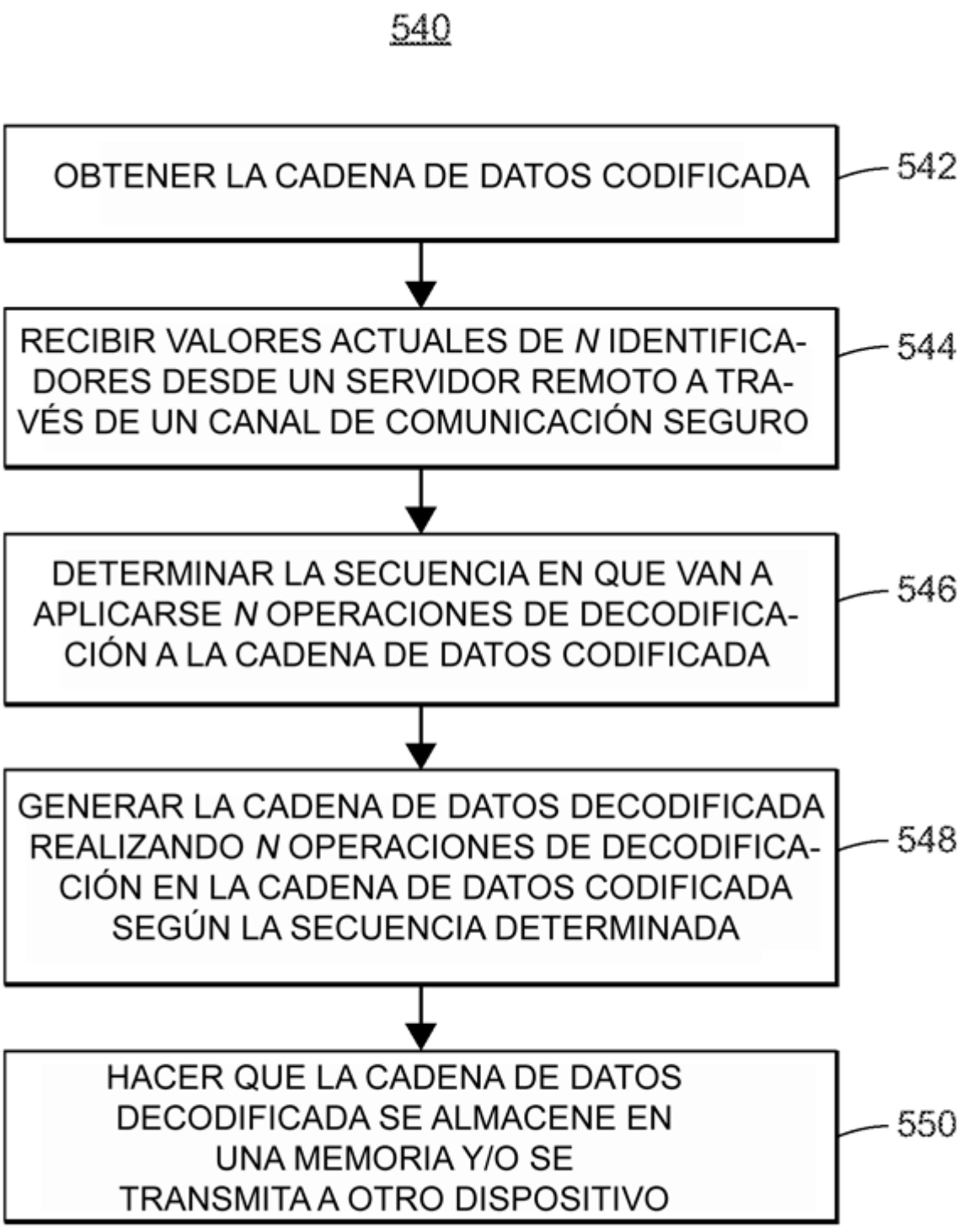
540
OBTENER LA CADENA DE DATOS CODIFICADA
542
RECIBIR VALORES ACTUALES DE N IDENTIFICADORES DESDE UN SERVIDOR REMOTO A TRAVÉS DE UN CANAL DE COMUNICACIÓN SEGURO
544
DETERMINAR LA SECUENCIA EN QUE VAN A APLICARSE N OPERACIONES DE DECODIFICACIÓN A LA CADENA DE DATOS CODIFICADA
546
GENERAR LA CADENA DE DATOS DECODIFICADA REALIZANDO N OPERACIONES DE DECODIFICACIÓN EN LA CADENA DE DATOS CODIFICADA SEGÚN LA SECUENCIA DETERMINADA
548
HACER QUE LA CADENA DE DATOS DECODIFICADA SE ALMACENE EN UNA MEMORIA Y/O SE TRANSMITA A OTRO DISPOSITIVO
550

FIG. 10