(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 808 209**

(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/US2016/055971**

(87) Fecha y número de publicación internacional: **30.11.2017 WO17204845**

(96) Fecha de presentación y número de la solicitud europea: **07.10.2016 E 16785298 (7)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3465523**

(54) Título: **Recopilación 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:
25.02.2021

(73) Titular/es:

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

(72) Inventor/es:

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

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Recopilación segura de datos sensibles

Referencia cruzada a solicitudes relacionadas

La presente reivindica el beneficio de la solicitud provisional de patente estadounidense n° 62/342.490, presentada el 27 de mayo de 2016 y titulada “Secure Collection of Sensitive Data”, y de la solicitud provisional de patente estadounidense n° 62/342,491, presentada el 27 de mayo de 2016 y titulada “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 forma segura datos sensibles (por ejemplo, confidenciales) o posiblemente sensibles.

Antecedentes

Actualmente, se diseñan muchas técnicas de codificación diferentes para impedir un acceso no autorizado a los datos almacenados y/o comunicados. Sin embargo, estas técnicas están asociadas con diversos inconvenientes. Por ejemplo, generalmente, estas técnicas no protegen ni ofuscan datos sensibles de una manera que sea de extremo a extremo (por ejemplo, comenzando en el momento en que la información se introduce manualmente por un individuo que usa un teclado). Además, algunos usan un enfoque generalizado en el que, si el código se “descifra” con respecto a una transmisión, el código también puede verse comprometido para futuras transmisiones y/o con respecto a las transmisiones entre otras partes o dispositivos. Todavía adicionalmente, algunos no proporcionan la flexibilidad para adaptar el nivel de seguridad a diferentes entidades (por ejemplo, diferentes empresas, personas, dispositivos, etc.), ni la flexibilidad para responder a amenazas a la seguridad (por ejemplo, filtraciones de datos) de forma precisa o específica. El documento US2015007265 aborda el problema de generar entropía de alta calidad en entornos de software asistido por hardware o software, tales como entornos virtualizados.

Sumario

La presente invención se define por las reivindicaciones independientes adjuntas. En una realización, 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 incluye la detección, por el uno o más procesadores, de una primera entrada de tecla realizada a través de la interfaz de usuario. El método también incluye la recepción, por parte del uno o más procesadores a través de la interfaz de comunicación y un canal de comunicación seguro, de primera información procedente de un servidor remoto. La primera información incluye al menos un primer valor actual de un primer identificador de capa. El método también incluye determinar, por el uno o más procesadores y usar el primer valor actual del primer identificador de capa, una primera cadena de bits correspondiente a la primera entrada de tecla, 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 provocar, por el uno o más procesadores, que la cadena de datos sea una o ambas de (i) almacenada en la memoria y (ii) transmitida a otro dispositivo a través de una red.

En otra realización, un dispositivo electrónico comprende una interfaz de usuario que incluye una pluralidad de teclas. El dispositivo electrónico también incluye una interfaz de comunicación, una memoria y uno o más procesadores. El uno o más procesadores se configuran para detectar una primera entrada de tecla realizada a través de la interfaz de usuario, y recibir la primera información procedente de un servidor remoto a través de la interfaz de comunicación y un canal de comunicación seguro. La primera información incluye al menos un primer valor actual de un primer identificador de capa. El uno o más procesadores también están configurados para determinar, usando el primer valor actual del primer identificador de capa, una primera cadena de bits correspondiente a la primera entrada de tecla, generar al menos una primera parte de una cadena de datos que usa la primera cadena de bits, y provocar que la cadena de datos sea uno o más de (i) almacenada en la memoria y (ii) transmitida a otro dispositivo a través de una red.

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 fuente de ejemplo, según una realización.

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

La figura 4 representa un conjunto de ejemplo de capas de mapeo que puede usarse para ofuscar información de

entrada de tecla, según una realización y situación.

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

La figura 6 representa una interfaz de usuario de ejemplo 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 al llevar a cabo una transacción con tarjeta de crédito o débito al por menor, 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 para proporcionar una comunicación segura de una cadena de datos a lo largo de una ruta 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, información de tarjetas de crédito u otra información financiera, información sanitaria, contraseñas, números de seguridad social, etc.) durante una transacción. Tal como se utiliza en el presente documento, una “transacción” puede referirse a cualquier interacción u operación que implique introducir, recopilar y/o comunicar información. Por tanto, por ejemplo, una transacción puede implicar que un empleado de un minorista introduzca el número de tarjeta de crédito de un cliente en un teclado (por ejemplo, una pantalla táctil de teléfono inteligente o tableta, o un teclado de hardware, etc.) y transmita la información codificada correspondiente al número de tarjeta de crédito a un proveedor de pago (o almacene la información codificada en una base de datos local, etc.). Como otro ejemplo, una transacción puede implicar que un paciente introduzca respuestas a una encuesta o cuestionario médico en un teclado, y transmitir la información codificada correspondiente a las respuestas del paciente a un servidor remoto. Como otro ejemplo adicional, una transacción puede implicar que un empleado administrativo de una empresa envíe registros contables confidenciales a otro empleado o departamento dentro de la empresa. Por supuesto, también son posibles otra infinidad de tipos de transacciones que implican información sensible o posiblemente sensible.

Algunos aspectos de la presente divulgación pueden requerir el registro previo de diversas entidades en un órgano coordinador. Tal como se utiliza en el presente documento, una “entidad” puede ser cualquier cosa física o virtual que pueda estar directa o tangencialmente implicada en una transacción, tal como una empresa o institución (por ejemplo, minorista, hospital, banco, compañía 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 enrutador, un conmutador de red, un cortafuegos, y así sucesivamente. Una vez registrada una entidad particular, un servidor central puede mantener un identificador, o diversos identificadores, asociados 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 mediante el análisis sintáctico de 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 mediante el análisis sintáctico de la cadena de datos en bloques de 8 bits, 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, además, aleatorizar la secuencia de bits codificada, etc.). Para disminuir el riesgo de que un identificador sea descubierto por 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 bajo solicitud).

Algunos aspectos de la presente divulgación permiten que los datos sensibles se ofusquen en el momento en que los datos se introducen manualmente usando una interfaz de teclado físico o virtual de un dispositivo electrónico. Generalmente, esto puede lograrse mapeando cada entrada de tecla con respecto a una coordenada en un espacio virtual. Las coordenadas del espacio virtual, en lugar de otras, representaciones comprobadas más fácilmente de las entradas de tecla (por ejemplo, símbolos ASCII), pueden entonces almacenarse, procesarse adicionalmente, transmitirse, etc. El mapeo de cada entrada de tecla con respecto a una coordenada de espacio virtual puede dictarse, en cualquier momento dado, por el valor actual de un identificador de una entidad registrada que está asociada con la transacción de alguna forma (por ejemplo, una empresa, un agente/empleado, un dispositivo de teclado, etc.). En algunas realizaciones y situaciones, múltiples identificadores (por ejemplo, 2, 5, 10, 100, etc.), correspondientes a

múltiples capas de mapeo, pueden usarse para ofuscar adicionalmente la información de entrada de tecla de un usuario. Los identificadores pueden incluir identificadores de múltiples entidades (por ejemplo, uno para una empresa, otro para un agente que introduce la información, etc.), y/o múltiples identificadores de una única entidad. El dispositivo electrónico podrá solicitar el/los identificador(es) apropiado(s) al servidor central, según sea necesario, a través de un canal de comunicación seguro (por ejemplo, usando las técnicas de cifrado y autenticación de la técnica anterior), por ejemplo. Tal como se señaló anteriormente, el servidor central puede cambiar/actualizar cada identificador según se desee. Si se usan múltiples identificadores, por ejemplo, pueden cambiarse uno o más de esos identificadores con la frecuencia suficiente para que el/los mapeo(s) correspondiente(s) cambie(n) de una entrada de tecla a la siguiente.

Más generalmente, pueden aplicarse varias etapas de codificación secuencialmente para codificar una cadena de datos que se comunica durante una transacción. En la descripción anterior relativa al ofuscamiento de la información de entrada de tecla, por ejemplo, cada “capa” (es decir, cada mapeo para un conjunto diferente de coordenadas virtuales) puede corresponder a una etapa de codificación particular. En algunas realizaciones y situaciones, sin embargo, al menos algunas etapas de codificación se aplican mediante otros dispositivos en la ruta de comunicación. Por ejemplo, un primer conjunto de cuatro etapas de codificación puede aplicarse secuencialmente por un dispositivo electrónico que se usó inicialmente para introducir información, una quinta etapa de codificación puede aplicarse por un enrutador en la ruta de comunicación (por ejemplo, usando un identificador para el enrutador) y una sexta etapa de codificación puede aplicarse por un servidor de red aguas abajo del enrutador en la ruta de comunicación (por ejemplo, usando un identificador para un cortafuegos implementado por el servidor), etc.

Cada etapa de codificación de 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 sintácticamente una cadena de datos de entrada en bloques de entrada de 16 bits cada uno, y entonces codificar esos bloques de entrada para generar bloques de salida de 16 bits. Generalmente, las diferentes etapas de codificación pueden tener diferentes tamaños de bloque de salida, y los tamaños de bloque de entrada no necesitan (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 se mapean dos secuencias de bits diferentes 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 correctamente la cadena de datos, las etapas de decodificación se aplican en el orden inverso con respecto a 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 incluía el mapeo de entradas de tecla a una coordenada de espacio virtual como etapa inicial, el receptor de la cadena de datos codificada puede revertir ese proceso de codificación en la etapa de decodificación final para llegar a los datos introducidos/escritos originalmente.

Para determinar las operaciones de decodificación adecuadas, el dispositivo electrónico que recibe la cadena de datos codificada puede solicitar, o de otro modo, obtener, los valores de identificador apropiados desde el servidor central a través de un canal de comunicación seguro (por ejemplo, usando técnicas de cifrado y autenticación de la técnica anterior). El servidor central también puede enviar la información de dispositivo de recepción relativa a la secuencia en la que van a producirse las diferentes operaciones de decodificación. En otras realizaciones, el dispositivo de recepción conoce la secuencia *a priori*, y solo obtiene los valores de identificador actuales desde el servidor central.

Estos y otros aspectos de la presente divulgación serán evidentes a partir de la siguiente descripción.

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 primero a la figura 1, un sistema 100 de ejemplo corresponde a una situación en la que información sensible o posiblemente sensible se transmite desde un dispositivo fuente 102 hasta un dispositivo de destino 104 a través de una red 106. Por lo general, el dispositivo fuente 102 puede ser cualquier tipo adecuado de dispositivo electrónico que permita la entrada de datos y pueda transmitir datos (por ejemplo, un dispositivo de teclado dedicado, un teléfono inteligente, una tableta, un ordenador portátil, un ordenador de escritorio, etc.), el dispositivo de destino 104 puede ser cualquier tipo adecuado de dispositivo electrónico que pueda recibir datos y que permita el almacenamiento, el procesamiento y/o el reenvío/transmisión (por ejemplo, un servidor) de datos, y la red 106 puede ser cualquier red de comunicación adecuada o combinación 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 simplificado, del dispositivo fuente 102 de la figura 1, según una realización. El dispositivo fuente 102 puede ser un dispositivo dedicado (por ejemplo, un dispositivo de teclado de hardware o tableta dedicados) o un dispositivo con fines generales (por ejemplo, un ordenador portátil, un ordenador de escritorio, un teléfono inteligente, una tableta, etc.). Tal como se observa en la figura 2, el dispositivo

fuente 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 de la única casilla etiquetada con 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 fuente 102 descritas 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 solo 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 diversas teclas físicas, así como cualquier firmware y/o hardware subyacente (por ejemplo, contactos, conmutadores, etc.) necesario para detectar las entradas de tecla. Alternativamente, la interfaz de usuario 124 puede incluir una pantalla táctil, junto con cualquier firmware y/o hardware de soporte (por ejemplo, un circuito integrado con 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, signo et, 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 adicionales (por ejemplo, audio). El/los componente(s) de salida puede(n) o no estar integrado(s) 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 deba enviarse al usuario (por ejemplo, instrucciones para introducir información usando el teclado 130, confirmaciones de que los mensajes se han enviado satisfactoriamente, etc.). En general, el procesador 120 puede detectar y actuar sobre entradas del 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 puertos de comunicación adicionales). En algunas realizaciones, la interfaz de comunicación 126 incluye una o más interfaces específicamente configuradas para soportar protocolos de comunicación altamente seguros (por ejemplo, establecimiento de comunicación, 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, seguro, y un segundo puerto para comunicarse con el dispositivo de destino 104 en un canal menos seguro, con fines generales. Alternativamente, puede usarse un único puerto para ambos tipos de comunicación, pero usando un protocolo de autenticación y/o de cifrado más seguro para el primero que para el segundo.

El funcionamiento del sistema 100 y el dispositivo fuente 102 se comentará con más detalle en las siguientes secciones, según diversas realizaciones. Aunque la siguiente discusión se refiere en ocasiones a los componentes del sistema 100 y del dispositivo fuente 102, se entiende que los diversos aspectos de la invención descritos en el presente documento pueden implementarse, en su lugar, 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 señaló anteriormente, una “entidad” puede ser cualquier cosa física o virtual que pueda estar directa o tangencialmente implicada 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 enrutador, un conmutador de red u otro dispositivo de red, un cortafuegos, etc.). El servicio de seguridad de datos puede proporcionarse por una empresa particular, y el proceso de registro de una entidad particular puede incluir la verificación o certificación de que la entidad es lo que pretende ser, y la asignación de un identificador a la entidad. El identificador puede almacenarse entonces en el registro 112 del servidor central 110 de la figura 1, por ejemplo.

En algunas realizaciones y situaciones, los identificadores se asignan en su totalidad por el servicio de seguridad de datos (por ejemplo, por el servidor central 110). Alternativamente, para algunos identificadores que no cambian con una frecuencia muy alta (por ejemplo, una vez al año, bajo sospecha de usurpación de identidad, etc.), los identificadores pueden seleccionarse manualmente por una persona que esté realizando el proceso de registro. Por ejemplo, una persona puede seleccionar un identificador (o un conjunto de identificadores) para sí misma, y/o para una tarjeta de crédito o débito que posea, etc. En algunas realizaciones, la persona puede seleccionar, en su lugar, 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 la totalidad del/de los identificador(es), y por lo tanto puede resultar útil para fines de autorización (tal como se comenta adicionalmente a continuación).

La seguridad puede aumentar automáticamente (y/o bajo solicitud) cambiando los valores de los identificadores almacenados en el registro de vez en cuando. De esta manera, los niveles de seguridad pueden adaptarse a la

sensibilidad o el nivel de riesgo de los datos protegidos. Por ejemplo, un identificador asociado a una institución financiera o un conmutador de red de “alta seguridad” puede cambiarse cada dos minutos (o cada vez que un dispositivo de codificación solicite el identificador, etc.), mientras que un identificador asociado con una persona particular o con un enrutador con fines generales puede cambiarse mensual o anualmente (o solo bajo solicitud, etc.). Los identificadores también pueden actualizarse basándose en otros desencadenantes (por ejemplo, infracciones de seguridad), permitiendo de ese modo que las respuestas a las amenazas de seguridad se adapten de manera estricta 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 ha producido una transacción fraudulenta con ese minorista en representación del cliente, y actualizar el identificador asociado con el propio minorista si el minorista sospecha una infracción más amplia de sus registros confidenciales. En realizaciones y situaciones en donde 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 puesta 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 varianza y/o aleatorización asociadas con cada cambio, pueden dictarse por un nivel de seguridad actual asociado con la entidad correspondiente (por ejemplo, una empresa particular). Por ejemplo, un identificador de una entidad puede actualizarse mensualmente si se asocia un nivel de seguridad “amarillo” 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), y cada cinco minutos si el nivel de seguridad cambia a “rojo” (por ejemplo, en respuesta a un informe confirmado de una infracción de seguridad específica que afecta a la entidad).

III. Entrada de datos segura

Tal como se señaló anteriormente, en un aspecto de la presente invención, no se recopila, almacena ni transmite información introducida en un teclado, ni datos correspondientes a representaciones habituales 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 de tecla en el teclado 130, y el dispositivo fuente 102 puede codificar directamente las entradas de tecla de manera que cualquier información transmitida y/o almacenada no pueda ser rastreada o mapeada de vuelta a las entradas de tecla originales sin conocimiento de las operaciones de decodificación adecuadas y dependientes del tiempo y su secuencia adecuada.

La figura 3 representa un mapeo 140 de ejemplo que el dispositivo fuente 102 puede usar para ofuscar información de entrada de tecla, según una realización y situación. En el mapeo 140, las entradas de usuario realizadas con teclas 142 se mapean a las coordenadas de espacio virtual 144. Las teclas 142 pueden ser teclas de un teclado 130 de la figura 2, por ejemplo. El mapeo 140 corresponde a un valor específico de un identificador particular. El identificador puede ser uno asociado (en el registro 112) con el dispositivo fuente 102, un agente u otro usuario que introduce información en el teclado 130, una empresa asociada con el dispositivo fuente 102, o cualquier otra entidad adecuada, y el valor de identificador puede haberse proporcionado al dispositivo fuente 102 por el servidor central 110. Tras 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 fuente 102 puede utilizar un 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” se mapea a las coordenadas [2,1], y así sucesivamente. Tras detectar una entrada de tecla en 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 por 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 señaló anteriormente, el servidor central 110 puede, en algunos casos, cambiar el identificador a una frecuencia muy alta. Por ejemplo, el dispositivo fuente 102 puede solicitar un identificador desde el servidor central 110 inmediatamente después de cada entrada de tecla, y el mapeo 140 puede cambiar a un nuevo mapeo para cada entrada de tecla en la secuencia de ejemplo anterior. Por tanto, 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 cuanto a valores discretos numéricos), en otras realizaciones el espacio virtual puede ser mucho mayor. Por ejemplo, cada una de las claves 142 puede mapearse a una coordenada diferente de una red de distribución virtual que es 256x256, cambiando el mapeo para cada valor de identificador. Por ejemplo, una entrada de tecla de “0” puede mapearse a la coordenada del espacio virtual [163,24] para un primer identificador/mapeo, mapearse a la coordenada del 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 fuente 102 puede implementar capas de mapeo adicionales para ofuscar y proteger adicionalmente información introducida. La figura 4 representa un conjunto 200 de este tipo 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 señaló anteriormente, la capa de mapeo 202-1 puede, en su lugar, mapear entradas de tecla a un espacio virtual más grande (por ejemplo, 8x8, 16x16, 256x256, etc.). Del mismo modo, la capa de mapeo 202-2 puede asignar, en su lugar, 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.). Generalmente, pueden usarse más capas cuando se desean mayores niveles de seguridad. Por ejemplo, las transacciones que implican una institución financiera pueden utilizar 50 capas similares a las capas 202, mientras que las transacciones que normalmente implican información menos sensible pueden solo incluir tres capas, etc. En algunas realizaciones, el dispositivo fuente 102 conoce *a priori* cuántas capas de mapeo/codificación se aplicarán. Alternativamente, el servidor central 110 puede informar al dispositivo fuente 102 del número de capas (por ejemplo, explícitamente a través de una indicación enviada en el mismo canal de comunicación seguro usado para enviar el/los identificador(es), o implícitamente enviando solo 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 de tecla posteriores).

IV. Codificación de cadena de datos en la ruta de comunicación

La sección anterior describe una o múltiples capas o etapas de mapeo/codificación dentro de un único dispositivo fuente. Más generalmente, sin embargo, pueden implementarse diferentes etapas de codificación por diferentes dispositivos en una ruta de comunicación. Por ejemplo, una cadena de datos puede codificarse mediante una o más etapas de codificación en un dispositivo fuente 102 (por ejemplo, etapas correspondientes a capas 202-1 a 202-3 de la figura 4), y posteriormente mediante una o más etapas de codificación en cada uno de uno más dispositivos de red en la red 106 (por ejemplo, un enrutador, 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, teclado 130), una cadena de datos puede corresponder o estar basada, en su lugar, en prácticamente cualquier otro tipo de información. Por ejemplo, una cadena de datos que va a codificarse y transmitirse puede incluir datos generados automáticamente por una aplicación de software que se ejecuta en un dispositivo fuente, o recuperarse a partir de una memoria local del dispositivo fuente, etc.

La figura 5 representa una ruta de comunicación 250 de ejemplo para una cadena de datos en donde la cadena de datos puede codificarse usando las técnicas descritas en el presente documento, según una realización y situación. La ruta de comunicación 250 incluye un dispositivo fuente 252, un primer dispositivo de red 254, un segundo dispositivo de red 256 y un dispositivo de destino 260. El dispositivo fuente 252 puede ser similar al dispositivo fuente 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. Por ejemplo, el dispositivo fuente 252 puede ser un dispositivo tableta con teclado virtual, el dispositivo de red 254 puede ser un enrutador, el dispositivo de red 256 puede ser un conmutador de red y el dispositivo de destino 260 puede ser un servidor de empresa.

Tal como se observa en la figura 5, el dispositivo fuente 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 uno o más procesadores del dispositivo respectivo al ejecutar instrucciones del módulo de codificación almacenadas en una memoria del dispositivo respectivo. En otras realizaciones, la ruta de comunicación 250 puede incluir más o menos dispositivos de los mostrados en la figura 5, y/o algunos o todos los diversos dispositivos pueden incluir más o menos etapas de codificación. Por ejemplo, el dispositivo fuente 252 puede incluir decenas o cientos de etapas de codificación 262, y/o una ruta de comunicación 250 puede incluir varios dispositivos de red adicionales que no incluyen ninguna etapa de codificación, etc.

En realizaciones y situaciones en donde la cadena de datos que se codifica se basa en entradas de tecla, la primera etapa de codificación 262-1 puede mapear las entradas de tecla 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 observarse como 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 observarse como una realización específica del funcionamiento de las etapas de codificación 262-1 a 262-3 de la figura 5. En realizaciones o situaciones en donde la cadena de datos no se basa en entradas de tecla (por ejemplo, datos recuperados a partir de una memoria, etc.), la etapa de codificación 262-1 puede funcionar de una 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 en la salida de la etapa de

codificación anterior, y puede asociarse con un tamaño de bloque de entrada (X_l para la l-ésima etapa de codificación en la ruta de comunicación 250) y un algoritmo o mapeo de codificación particular que dicta el tamaño de bloque de salida (Y_l para la l-ésima etapa de codificación en la ruta de comunicación 250). En particular, cada etapa de codificación puede analizar sintácticamente su entrada en bloques de X_l bits, y aplicar el algoritmo de codificación apropiado para generar bloques correspondientes de Y_l bits. Generalmente, el tamaño de bloque de salida para una etapa de codificación particular puede ser igual o mayor que el tamaño del bloque de entrada para esa etapa (aunque preferiblemente no más pequeño, para evitar 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 dictarse por el valor actual de un identificador respectivo, donde 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 asociarse con el dispositivo fuente 252, el identificador para la etapa de codificación 262-2 puede asociarse con una empresa particular (por ejemplo, una que posea, mantenga y/o use el dispositivo fuente 252, o que esté de otro modo implicada en la transacción que requiere la transmisión de la cadena de datos), el identificador para la etapa de codificación 262-3 puede asociarse con un departamento particular de la empresa, el identificador para la etapa de codificación 262-4 puede asociarse con un agente/empleado particular usando el dispositivo fuente 252, y el identificador para la etapa de codificación 262-5 puede asociarse con una aplicación de software particular que se ejecuta en el dispositivo fuente 252. Continuando con este ejemplo, el identificador para la etapa de codificación 264-1 puede asociarse con el dispositivo de red (por ejemplo, enrutador) 254, el identificador para la etapa de codificación 264-2 puede asociarse con un cortafuegos implementado por el dispositivo de red 254, y el identificador para la etapa de codificación 266 puede asociarse 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 solicitud a un servidor central (por ejemplo, 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 enviar valores actuales de los identificadores apropiados a algunos o todos los dispositivos 252, 254 y 256 (por ejemplo, de forma periódica) a través de canales de comunicación seguros. Los canales de comunicación seguros entre el servidor central y cada dispositivo pueden usar fuertes técnicas de autenticación/verificación y cifrado conocidas en la técnica, por ejemplo. En algunas realizaciones, uno o más de los dispositivos 252, 254, 256 añade información de marca de tiempo a la cadena de datos transmitida a uno o más intervalos, para informar al dispositivo de destino 260 del/de los tiempo(s) en el/los que los distintos valores de identificador eran “actuales”. Esta información puede permitir que el dispositivo de destino 260 decodifique apropiadamente la cadena de datos recibida, tal como se comentará adicionalmente a continuación. Además, en algunas realizaciones, el tiempo actual u otra información puede usarse por uno o más de los dispositivos 252, 254 y 256 para codificar o aleatorizar adicionalmente la cadena de datos.

Cada uno de los dispositivos 252, 254 y 256 puede almacenar un conjunto de normas que permiten que el dispositivo determine el algoritmo de codificación apropiado para usar, en cada etapa de codificación implementada por el dispositivo, basándose en el valor de identificador actual. En algunas realizaciones, el tamaño del bloque de entrada X_l y el tamaño del bloque de salida Y_l puede cambiar para una etapa de codificación particular basándose en el valor de identificador actual. En otras realizaciones, los tamaños de bloque de salida y/o de entrada son constantes, y los valores de identificador solo dictan el algoritmo actual (por ejemplo, mapeo) que va a usarse en cada etapa de codificación. Sin embargo, preferiblemente, los tamaños de bloque de salida y/o de entrada 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_l de las etapas de codificación dentro de la ruta de comunicación 250 difieren, preferiblemente, con el fin de aumentar la dificultad de decodificación no autorizada. Como 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 durante la transmisión de una única cadena de datos.

V. Decodificación de cadenas 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 en el orden inverso en el 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 ejecutan instrucciones de un módulo de decodificación almacenado en una memoria del dispositivo 260) puede implementar, en primer lugar, una etapa de decodificación que es inversa a la etapa de codificación 266, en segundo lugar, implementar una etapa de decodificación que es inversa a la etapa de

codificación 264-2, en tercer lugar, implementar una etapa de decodificación que es inversa a la etapa de codificación 264-1, en cuarto lugar implementar una etapa de decodificación que es inversa a la etapa de codificación 262-5,y así sucesivamente, hasta que finalmente se implementa una etapa de decodificación que es inversa a la etapa de codificación 262-1 (por ejemplo, para determinar las entradas de tecla realizadas por un usuario, o la cadena de datos original).

Para determinar los algoritmos apropiados que van a aplicarse 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 fines de codificación). Los valores de identificador pueden solicitarse por el dispositivo de destino 260 tras recibir la cadena de datos, por ejemplo, o solicitarse por (o enviarse) el dispositivo de destino 260 de forma periódica o de otra forma.

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

El dispositivo de destino 260 puede almacenar un conjunto de normas que permiten que el dispositivo 260 determine los algoritmos de decodificación apropiados para usar basándose en los valores de identificador recibidos. Para deshacer la codificación realizada por la l-ésima etapa de codificación, por ejemplo, la etapa de decodificación correspondiente del dispositivo de destino 260 puede analizar sintácticamente la cadena de datos (o la cadena de datos parcialmente decodificada de la etapa de decodificación anterior) en bloques de tamaño Y_l (es decir, el tamaño de bloque de salida para la l-ésima codificación), y decodificar cada bloque a un bloque de salida de tamaño X_l (es decir, el tamaño de bloque de entrada para la l-ésima etapa de codificación usando el mapeo apropiado).

En una realización, para que el dispositivo de destino 260 decodifique de forma apropiada y por completo 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, el orden inverso en 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 solo necesita obtener los valores de identificador apropiados del servidor central. En una realización de este tipo, la ruta de comunicación (por ejemplo, ruta de comunicación 250) puede observarse como 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 apropiado y usa los valores de identificador apropiados del servidor central, entonces un fallo para decodificar la cadena de datos puede indicar que la cadena de datos no se transmitió a lo largo de una ruta de comunicación “aprobada”.

En algunas situaciones, el dispositivo de destino 260 puede no decodificar completamente la cadena de datos y, por lo tanto, puede no realizar las 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 números de tarjetas de crédito del cliente, en lugar de almacenar los números de tarjeta en un formato fácilmente determinado (por ejemplo, representaciones ASCII), con el fin de evitar la activación de las obligaciones de conformidad de la norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS).

VI. Autorización

Una capa de seguridad adicional puede proporcionarse al requerir autorización para una transacción dada. Por ejemplo, las compras que usan una tarjeta de crédito o débito pueden solo aprobarse por un procesador de pagos después de que el usuario de la tarjeta haya autorizado la compra. Para facilitar la explicación, la siguiente discusión se refiere, principalmente, a realizaciones o situaciones en los que un titular de tarjeta de crédito o débito se registra previamente con el fin de proporcionar autorización. En otras situaciones y/o realizaciones, sin embargo, el proceso puede usarse para otros individuos y/o en otros tipos de transacciones. Por ejemplo, un agente de una empresa puede registrarse previamente con el fin de proporcionar autorización/confirmación para transacciones llevadas a cabo en representación de consumidores, o para transacciones puramente internas (por ejemplo, para autorizar una solicitud particular de recuperación o modificación de información en una base de datos empresarial), etc.

Para permitir una autorización de usuario, una persona puede registrarse previamente, y/o su tarjeta, en 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 tarjeta y/o persona que se registra.

En una realización, la persona puede seleccionar su identificador personal (o tarjeta). Dado que el identificador puede ser una cadena de números larga y/u otros caracteres que es difícil de memorizar, puede proporcionarse a la persona la opción de seleccionar una secuencia específica de imágenes de entre un conjunto limitado de imágenes. Para proporcionar solo un par de ejemplos, el inscrito debe poder seleccionar cualquier secuencia específica de cuatro colores/palos de cartas de juego (por ejemplo, diamante negro, espada roja, corazón rojo, diamante rojo), o cualquier secuencia específica de tres colores/palos/grupos de cartas de juego (por ejemplo, tres de tréboles rojo, rey de corazones negro, sota de diamantes negra), etc.

Otro ejemplo se proporciona 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 presentada en una pantalla de visualización de teléfono inteligente, en otras realizaciones o situaciones pueden usarse otros dispositivos. Además, aunque la figura 6 muestra un total de 12 imágenes de las que 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 manera que la secuencia de imagen 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 globo corresponde a “3a7e16”, la imagen del coche corresponde a “4b4a22” y la imagen de la casa corresponde a “9u3c59”, entonces la secuencia “globo, coche, casa” puede corresponder al identificador “3a7e164b4a229u3c59”.

En algunas realizaciones, la secuencia de imagen seleccionada corresponde a múltiples identificadores. Por ejemplo, la secuencia puede corresponder a una concatenación de un primer identificador para el propio/propia inscrito/inscrita, y un segundo identificador para una tarjeta de crédito o débito del inscrito. Como otro ejemplo, una secuencia de imagen única puede corresponder a una secuencia predeterminada de valores de identificador, provocando cada actualización del identificador por el servidor central el avance del valor de identificador 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 del cambio del 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 inscrito 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 inscrito de las opciones de imagen, y entonces introducir las selecciones a medida que el inscrito indica a los agentes esas selecciones. En otra realización, el inscrito 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 inscrito la colección de imágenes que pueden seleccionarse (por ejemplo, para su visualización a través de una interfaz de usuario de un navegador web o de una aplicación de software dedicada que se ejecuta en el teléfono inteligente, tableta, ordenador portátil o de escritorio del inscrito, etc.), y las selecciones del inscrito pueden transmitirse de nuevo al servidor central. El inscrito puede realizar 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 inscrito no selecciona una secuencia de imagen, sino que, en su lugar, se le informa de una secuencia de imágenes que corresponde a su identificador asignado aleatoriamente.

En algunas realizaciones, un inscrito también puede seleccionar el/los modo(s) en el/los que se realizan las solicitudes de autorización. Por ejemplo, pueden proporcionarse al inscrito opciones de autorización telefónica, autorización de correo electrónico, autorización de mensajes de texto SMS, y/u otros tipos de autorización.

Una vez establecida una secuencia de imágenes para un inscrito particular (o su tarjeta), y se han establecido el/los método(s) apropiado(s) de autorización para el inscrito, puede usarse la secuencia de imágenes para autorizar futuras transacciones. Con referencia a la ruta 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 determinar a partir de los datos decodificados que una persona particular, o la tarjeta de crédito o débito de esa persona, se asocia con la transacción que se está realizando. El dispositivo de destino 260, o un agente asociado con el dispositivo 260, puede entonces solicitar 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 de que se necesita 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 sobre si se recibió una respuesta correcta.

En algunas realizaciones y situaciones (por ejemplo, si se solicita la autorización por teléfono), un usuario puede autorizar una transacción describiendo la secuencia de imágenes a un agente (por ejemplo, diciendo “globo, coche, casa”), y el agente puede o bien introducir esa información, o bien simplemente aprobar la transacción directamente si se informa al agente de la secuencia apropiada. En otras realizaciones y situaciones (por ejemplo, si la autorización

se solicita a través de un navegador web o de una aplicación de software dedicada que se ejecuta en el dispositivo electrónico del usuario), el usuario puede autorizar una transacción o bien escribiendo descriptores de la secuencia de imágenes correcta, o bien seleccionando la secuencia correcta de 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 presunta infracción de seguridad. Por ejemplo, el servidor central puede actualizar un identificador asociado con la persona que, presuntamente, 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 usan en el proceso de codificación descrito anteriormente en las secciones III o IV. Por ejemplo, una de las etapas de codificación 262-1 a 262-5 de la figura 5 puede seleccionar un algoritmo de codificación basado en un valor de un identificador correspondiente a la secuencia de imágenes. En algunas de estas realizaciones, esto puede requerir que el servidor central sepa quién está realizando la transacción, o qué tarjeta se está usando para realizar la transacción, de modo que el identificador apropiado pueda recuperarse y enviarse al dispositivo fuente 252. Un ejemplo de una realización de este tipo se describe a continuación en la sección VII, en relación con un caso/situación de uso particular.

VII. Caso de uso de ejemplo

La figura 7 representa un entorno 400 de ejemplo en el que pueden implementarse aspectos de la presente divulgación al llevar a cabo una transacción con tarjeta de crédito o débito de venta al por menor, según una realización y situación. Se entiende que esto representa solo un caso de uso de ejemplo, y que los casos de uso relacionados con otros tipos de transacciones, y en otros entornos/sistemas, también son posibles.

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 se sitúa 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 de consumidor) cuando se realizan transacciones/compras. Alternativamente, el dispositivo 404 puede ser un dispositivo dedicado o con fines generales con un teclado de hardware. La información de pago para las transacciones, que incluye números de tarjeta de crédito o débito, importes de pago, etc., puede enviarse a un proveedor de pagos 406 (por ejemplo, uno o más servidores del proveedor de pagos 406), que reenvía información de pago a una red de pagos 410 (por ejemplo, uno o más servidores de la red de pagos 410) para añadir la cantidad apropiada a un saldo de tarjeta de crédito o restar la cantidad apropiada de un saldo de cuenta asociado a una tarjeta de débito, etc. La red de pagos 410 puede ser un banco, por ejemplo.

Para ofuscar al menos parte de la información de pago para la transacción, pueden usarse una o más de las técnicas descritas anteriormente. Para ello, el entorno de ejemplo 400 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 pagos 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 su lugar, estar registradas previamente, tal como la propia tienda minorista, un empleado/agente de la tienda, uno o más dispositivos de red (por ejemplo, enrutadores) y/o aplicaciones o nodos (por ejemplo, cortafuegos) en la ruta de comunicación entre el dispositivo de tableta 404 y el proveedor de pagos 406, y así sucesivamente.

En la situación de ejemplo descrita en este caso, la tarjeta 402 también se registra 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 de “tarjeta presente”) de modo 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 de “tarjeta no presente”). Alternativamente, el titular de la tarjeta puede introducir el número de tarjeta usando la tableta 404.

En una realización, solo una versión codificada de manera segura del número de tarjeta está presente, en formato digital, en cualquier punto de la transacción. Por ejemplo, las técnicas descritas anteriormente en relación con las figuras 3 y 4 pueden usarse para mapear las entradas de tecla a las coordenadas de espacio virtual, siendo cada mapeo dependiente 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 adicionales (no mostrados en la figura 7) dentro de la ruta de comunicación entre el dispositivo de tableta 404 y el proveedor de pagos 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. Entonces, 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 posteriormente enviar el valor actual del identificador correspondiente a la tarjeta 402 al dispositivo de tableta 404. El dispositivo de tableta 404 puede entonces usar el valor del 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 sobre la identidad de la tarjeta 402.

Después de que el dispositivo de tableta 404, y cualquier otro dispositivo de codificación en la ruta de comunicación, codifica una cadena de datos correspondiente a la información de pago, la cadena de datos codificados se recibe en el proveedor de pago 406. Tal como se comentó anteriormente en la sección V, el proveedor de pagos 406 puede obtener los valores de identificador apropiados desde el 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 pagos 406 o el servidor central 412 puede usar el método de autorización preferido por el titular de la tarjeta para solicitar la secuencia de imágenes correspondiente al identificador de la tarjeta 402 (por ejemplo, según cualquiera de las técnicas mencionadas anteriormente en la sección VI). Si el titular de la tarjeta proporciona la secuencia apropiada, el proveedor de pagos 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. Dado que la información de pago nunca se almacena en el dispositivo de tableta 402 (o en cualquier otro dispositivo del minorista), puede 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 de ejemplo 500 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 fuente 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, memoria 122 de la figura 2), por ejemplo.

En el método 500, se detecta una primera entrada de tecla (bloque 502). La entrada de tecla 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 de tecla puede realizarse durante el proceso de introducción manual de información sensible, tal como el número de tarjeta de crédito o débito, otra información financiera, información personal de salud, número de seguridad social, etc. En algunas realizaciones, la interfaz de usuario (por ejemplo, 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 la detección de cuál de la pluralidad de teclas se tocó o 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 táctil del dispositivo electrónico, cada tecla de la pluralidad de teclas es una tecla diferente en el teclado virtual, y el bloque 502 incluye la detección de qué área de la pantalla táctil se tocó. El dispositivo electrónico puede ser un teléfono inteligente, tableta, ordenador portátil u ordenador de escritorio, por ejemplo.

Asimismo, en el método 500, la información se recibe 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, 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 solicitud realizada por el dispositivo electrónico). El servidor remoto puede ser un servidor similar al servidor central 110 de la figura 1 o el servidor central 412 de la figura 7, por ejemplo. El bloque 504 puede producirse antes, simultáneamente con, y/o después del bloque 502.

La información recibida en el bloque 504 incluye al menos un 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, empresa, 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 a través de múltiples transmisiones.

Una cadena de bits correspondiente a la primera entrada de tecla 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 apropiados que van a usarse cuando se codifica la entrada de tecla detectada en el bloque 502. Bajo una codificación/mapeo, por ejemplo, puede mapearse una entrada de tecla de “5” a la cadena de bits 01 11 (por ejemplo, las coordenadas del espacio virtual [1,3]), una entrada de tecla de “g” puede mapearse a la cadena de bits 100 001 (por ejemplo, las coordenadas del espacio virtual [4,1]), etc.

Puede generarse al menos una primera parte de una cadena de datos usando la cadena de bits determinada en el bloque 506 (bloque 508). Toda la cadena de datos puede corresponder a un número de tarjeta completo, contraseña, mensaje o cualquier otro tipo de información introducida en el teclado. Si el dispositivo electrónico solo utiliza una única capa de mapeo (por ejemplo, tal como se representa en la figura 3), el bloque 506 puede incluir la generación de 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 incluía un 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 un valor actual de un segundo identificador de capa incluido en la información recibida. Si existen más capas de codificación, la salida de cadena de bits 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 cadena de datos, puede entonces 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 explícita o implícitamente el número de capas (por ejemplo, implícitamente enviando solo 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*.

La cadena de datos que se genera al menos parcialmente en el bloque 508 puede hacerse almacenar en una memoria local del dispositivo electrónico (por ejemplo, memoria 122 de la figura 2), y/o transmitirse 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 mensaje de control que provoca que otro dispositivo o unidad realice la transmisión y/o almacenamiento, por ejemplo.

Los bloques 502 a 508 pueden repetirse para una o más entradas de tecla posteriores. En algunas realizaciones en las que los valores de identificador no cambian con frecuencia, puede omitirse el bloque 504 para estas repeticiones posteriores. En otras realizaciones, sin embargo, el bloque 504 se repite en cada una (o al menos algunas de) de las repeticiones posteriores con el fin de obtener valores de identificador actualizados entre algunas o todas las entradas de tecla. 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 fuera necesario) para cada entrada de tecla. En cualquier caso, la cadena de datos que se hace almacenar y/o transmitirse en el bloque 510 puede incluir múltiples segmentos/partes de cadena, correspondiendo cada uno a una diferente de las entradas de tecla detectadas.

La figura 9 es un diagrama de flujo de un método de ejemplo 520 para proporcionar una comunicación segura de una cadena de datos a lo largo de una ruta de comunicación que incluye una pluralidad de dispositivos, según una realización. La cadena de datos puede ser en sí misma una versión codificada de una o más entradas de tecla manuales, o puede ser algún otro tipo de dato no codificado o parcialmente codificado (por ejemplo, una representación ASCII de un número de seguridad social, informe de salud 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 ejecuta las instrucciones almacenadas en una memoria del servidor, por ejemplo.

En el método 520, una primera entidad (por ejemplo, una persona, empresa, 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, un 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 como el que se describió anteriormente en la sección II, por ejemplo.

Se proporciona un valor actual del primer identificador a un primer dispositivo, de los dispositivos en la ruta de comunicación, a través de un primer canal de comunicación seguro con el fin de habilitar una primera codificación de la cadena de datos (bloque 526). El valor puede proporcionarse en respuesta a una solicitud recibida desde el primer dispositivo, por ejemplo. El primer dispositivo puede asociarse con la primera entidad de alguna manera. Por ejemplo, la primera entidad puede ser el propio primer dispositivo, o puede ser una persona u organización (por ejemplo, empresa, departamento, etc.) que posea, controle y/o use el primer dispositivo, etc. La primera codificación de la cadena de datos codifica una pluralidad de secuencias de bits en la cadena de datos tal como una primera pluralidad de secuencias de bits codificadas, teniendo cada una un primer tamaño de bloque (por ejemplo, número de bits).

Se proporciona un valor actual del segundo identificador a un segundo dispositivo de los dispositivos en la ruta de comunicación, a través de un segundo canal de comunicación seguro, con el fin de habilitar una segunda codificación de la cadena de datos (bloque 528). El valor puede proporcionarse en respuesta a una solicitud recibida desde el segundo dispositivo, por ejemplo. El segundo dispositivo se encuentra aguas abajo del primer dispositivo en la ruta de comunicación, y puede asociarse con la segunda entidad de alguna manera. Por ejemplo, la segunda entidad puede

ser el propio segundo dispositivo (por ejemplo, un dispositivo de red tal como un enrutador o un 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 la ruta de comunicación, a través de un tercer canal de comunicación seguro, con el fin de permitir la decodificación de la cadena de datos (bloque 530). El tercer dispositivo se encuentra aguas abajo del segundo dispositivo en la ruta 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 momento posterior cuando se codifica y transmite la cadena de datos posterior. Dependiendo del tiempo que haya pasado desde la transmisión de la cadena de datos inicial, 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 situaciones y/o realizaciones, el método 520 se modifica de manera que el servidor proporciona los valores actuales tanto del primer identificador como del segundo identificador al primer dispositivo (por ejemplo, un dispositivo fuente), 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 aún otras situaciones y/o realizaciones, los dispositivos primero y segundo (y posiblemente otros) implementan 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 de ejemplo 540 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 recibiendo la cadena de datos codificada desde un dispositivo fuente (por ejemplo, después de que la cadena de datos se codifique usando el método 500). En otra situación, la cadena de datos codificada se obtiene recuperando la cadena de datos codificada a partir de una memoria local del dispositivo electrónico. La cadena de datos codificada puede representar información sensible o posiblemente sensible (por ejemplo, un número de tarjeta de crédito o débito u otra información financiera, información de salud personal, un número de seguridad social, etc.).

Los valores actuales de los N identificadores ($N \geq 1$) se reciben 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, simultáneamente con, y/o después del bloque 542. Cada uno de los N identificadores está asociado con una 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 información correspondiente a la cadena de datos, una puede ser una persona u organización implicada en una transacción relacionada con la cadena de datos, una puede ser un dispositivo de red o cortafuegos en la ruta de comunicación de la cadena de datos, etc. Además, cada una de las entidades corresponde a una respectiva de N operaciones de decodificación, en 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.

Se determina una secuencia en la que las N operaciones de decodificación deben aplicarse a la cadena de datos codificada (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 normas 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, el análisis sintáctico de al menos de una parte de la cadena de datos codificada (o de una cadena de datos parcialmente decodificada que resulta de una operación anterior 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), decodificando por separado cada uno de los bloques que tienen el tamaño de bloque respectivo, y, para las primeras N - 1 operaciones de decodificación, 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 mensaje de control a otro dispositivo o unidad que realice la transmisión y/o almacenamiento, por ejemplo.

IX. Aspectos de la invención

Aunque el texto anterior expone una descripción detallada de numerosos aspectos y realizaciones diferentes de la invención, debe entenderse que el alcance de la patente se define por las palabras de las reivindicaciones expuestas al final de esta patente. La descripción detallada debe interpretarse únicamente a modo de ejemplo y no describe todas las realizaciones posibles, ya que describir todas las realizaciones posibles sería poco práctico, si no imposible. Podrían implementarse numerosas realizaciones alternativas, usando o bien tecnología actual o bien tecnología desarrollada después de la fecha de presentación de esta patente, que seguirían encontrándose 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, una primera entrada de tecla 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, la primera información procedente de 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 de tecla; (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) provocar, por el uno o más procesadores, que la cadena de datos sea una o ambas de (a) almacenada en la memoria y (b) transmitida a otro dispositivo a través de una red.

Aspecto 2. El método según el 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 de tecla incluye la detección de cuál de la pluralidad de teclas se tocó o presionó.

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

Aspecto 4. El método según cualquiera de los aspectos 1 a 3, que comprende, además, solicitar la primera información procedente del servidor remoto, en el que la recepción de la primera información es en respuesta a la solicitud de la primera información.

Aspecto 5. El método según el aspecto 4, en el que la solicitud de la primera información es o bien (i) en respuesta a la detección de la primera entrada de tecla, o bien (ii) antes de la detección de la primera entrada de tecla.

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

Aspecto 7. El método según el 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 según 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 la generación de al menos una primera parte de una cadena de datos que usa 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 según el aspecto 8, que comprende, además, recibir, a través de la interfaz de comunicación y un canal de comunicación seguro, datos que indican varias capas de codificación que van a aplicarse por el dispositivo electrónico.

Aspecto 10. El método según cualquiera de los aspectos 1 a 9, que comprende, además: (i) detectar, por el uno o más procesadores, una segunda entrada de tecla 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, la segunda información procedente del 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 de tecla; 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 según el aspecto 10, en el que no se realiza ninguna entrada de tecla a través de la interfaz de usuario entre la primera entrada de tecla y la segunda entrada de tecla.

Aspecto 12. El método según el 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 momento; y (ii) el segundo valor actual del primer identificador de capa se asocia con la entidad del registro en un segundo momento después del primer momento.

Aspecto 13. El método según el 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 según el aspecto 10, en el que: (i) la primera información incluye, además, el 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 según el aspecto 14, que comprende, además: (i) solicitar la primera información procedente del servidor remoto; y (ii) solicitar la segunda información procedente del servidor remoto, en el que la recepción de la primera información es en respuesta a la solicitud de la primera información, y en el que la recepción de la segunda información es en respuesta a la solicitud de 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 de tecla realizada a través de la interfaz de usuario, (b) recibir la primera información procedente de 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 de tecla, (d) generar al menos una primera parte de una cadena de datos usando la primera cadena de bits, y (e) provocar 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 según el 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 se configuran para detectar la primera entrada de tecla al menos detectando cuál de la pluralidad de teclas se tocó o presionó.

Aspecto 18. El dispositivo electrónico según el aspecto 16, en el que: (i) la interfaz de usuario incluye un teclado virtual presentado en una pantalla 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 se configuran para detectar la primera entrada de tecla al menos detectando qué área de la pantalla táctil se tocó.

Aspecto 19. El dispositivo electrónico según 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 se configuran para generar al menos la primera parte de la cadena de datos usando la primera cadena de bits al menos mediante: (i) codificando, 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) generando al menos la primera parte de la cadena de datos usando la segunda cadena de bits.

Aspecto 20. El dispositivo electrónico según cualquiera de los aspectos 16 a 18, en el que el uno o más procesadores están configurados, además, para: (i) detectar una segunda entrada de tecla realizada a través de la interfaz de usuario; (ii) recibir, a través de la interfaz de comunicación y el canal de comunicación seguro, la segunda información procedente del 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 de tecla; 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 una ruta 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 la ruta 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 dispositivo se encuentra aguas abajo del segundo dispositivo en la ruta de comunicación.

Aspecto 22. El método según el 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 según el 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 según cualquiera de los aspectos 21 a 23, en el que el segundo dispositivo es un dispositivo de red, y la segunda entidad es una de: (i) el dispositivo de red; o (ii) un cortafuegos implementado por el segundo dispositivo.

Aspecto 25. El método según cualquiera de los aspectos 21 a 24, que comprende, además: (i) proporcionar al primer dispositivo, a través del primer canal de comunicación segura, 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 según 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 la recepción de una solicitud procedente del primer dispositivo; y (ii) proporcionar al segundo dispositivo el primer valor actual del segundo identificador es en respuesta a la recepción de una solicitud procedente del 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 fuente 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 según el 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 según el aspecto 27 o 28, en el que la primera entidad y la segunda entidad son entidades

diferentes de: (i) el dispositivo fuente; (ii) una persona; o (iii) una organización.

Aspecto 30. El método según cualquiera de los aspectos 27 a 29, que comprende, además: (i) proporcionar al dispositivo fuente, 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 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 (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 según cualquiera de los aspectos 27 a 30, en el 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 la recepción de una solicitud procedente del 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) se asocia con una respectiva de una pluralidad de entidades, estando cada una de la pluralidad de entidades asociada con la comunicación de la cadena de datos codificados, y (b) corresponde a una 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 que 1; (iii) determinar, mediante el uno o más procesadores, una secuencia en la que las *N* operaciones de decodificación deben 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 la realización de las *N* operaciones de decodificación incluye, para cada operación de decodificación de las *N* operaciones de decodificación, (a) analizar sintácticamente al menos una parte de la cadena de datos codificada, o al menos una parte de una cadena de datos parcialmente decodificada que resulta de una anterior 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 de las *N* operaciones de decodificación; y (v) provocar, por el uno o más procesadores, que la cadena de datos decodificada sea una o ambas de (i) almacenada en la memoria y (ii) transmitida a otro dispositivo.

Aspecto 33. El método según el 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 según el 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 según cualquiera de los aspectos 32 a 34, en el que determinar la secuencia en la que las *N* operaciones de decodificación deben aplicarse 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 según 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 haya introducido 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 se configuran para ejecutar las instrucciones de (a) añadir a la base de datos del 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 un segundo identificador asociado con la segunda entidad, (c) proporcionar a un primer dispositivo de una pluralidad de dispositivos en una ruta 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 segunda entidad y aguas abajo del primer dispositivo en la ruta 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 se encuentra aguas abajo del segundo dispositivo en la ruta de comunicación.

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

Aspecto 40. El servidor según 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, mediante software) o configurados permanentemente para realizar las operaciones relevantes. Independientemente de que 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 algún ejemplo de una realización, módulos implementados por procesador.

De manera similar, los métodos o rutinas descritos en el presente documento pueden ser al menos parcialmente implementados 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 algunas de las operaciones puede distribuirse entre el uno o más procesadores, que no solo se encuentran dentro de una única máquina, sino que se despliegan en varias máquinas. En una realización, el procesador o los procesadores pueden ubicarse en una única ubicación (por ejemplo, dentro de un entorno doméstico, un entorno de oficina o como una granja de servidores), mientras que en otras realizaciones los procesadores pueden distribuirse en varias ubicaciones.

El rendimiento de algunas de las operaciones puede distribuirse entre el uno o más procesadores, que no solo residen dentro de una única máquina, sino que se despliegan en varias máquinas. En algunas realizaciones de ejemplo, el uno o más procesadores o módulos implementados por procesador pueden ubicarse 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 el procesador pueden distribuirse a través de varias ubicaciones geográficas.

A menos que se indique expresamente lo contrario, las discusiones en el presente documento que usan palabras como “procesamiento”, “computación”, “cálculo”, “determinación”, “presentación”, “visualización” o similares pueden hacer referencia 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) dentro de una o más memorias (por ejemplo, memoria volátil, memoria no volátil, o una combinación de las mismas), registros u otros componentes de máquina que reciban, almacenen, transmitan o visualicen información.

Tal como se usa en el presente documento, cualquier referencia a “una realización” significa que un elemento, rasgo, estructura o característica particular descrito en relación con la realización se incluye en al menos una realización. Las apariciones de la frase “en una realización” en diversos lugares de la memoria descriptiva no se refieren todas 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 abarcar una inclusión no exclusiva. Por ejemplo, un proceso, método, artículo o aparato que comprende una lista de elementos no se limita necesariamente a solo esos elementos, sino que puede incluir otros elementos no enumerados expresamente o inherentes a tal 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 se cumple por cualquiera de las siguientes: A es verdadero (o está presente) y B es falso (o no está presente), A es falso (o no está presente) y B es verdadero (o está presente), y A y B son verdaderos (o están presentes).

Además, el uso de “un” o “una” se emplea para describir elementos y componentes de las realizaciones en el presente documento. Esto se realiza simplemente por motivos de conveniencia y para proporcionar un sentido general de la descripción. Esta descripción, y las siguientes reivindicaciones, deben leerse para incluir uno o al menos uno y el

singular también incluye el plural a menos que sea obvio que implique lo contrario. Esta descripción detallada debe interpretarse como ejemplo y no describe cada posible realización, ya que la descripción de toda realización posible sería poco práctica, si no imposible. Pueden implementarse numerosas realizaciones alternativas, usando o bien tecnología actual o bien tecnología desarrollada después de la fecha de presentación de la presente solicitud.

REIVINDICACIONES

1. Un método implementado en un dispositivo electrónico (260, 404) que tiene una interfaz de usuario (124, 300) con una pluralidad de teclas, una interfaz de comunicación (126), una memoria (122), y uno o más procesadores, comprendiendo el método:

recibir, por el uno o más procesadores a través de la interfaz de comunicación (126) y un canal de comunicación seguro, primera información desde un servidor remoto (110) que cambia valores de un primer identificador de capa periódicamente y/o bajo solicitud, incluyendo la primera información al menos un primer valor actual del primer identificador de capa;

detectar, por el uno o más procesadores, una primera entrada de tecla (502) realizada a través de la interfaz de usuario, siendo la primera entrada de tecla una entrada de una primera tecla de la pluralidad de teclas;

determinar, por el uno o más procesadores y usando el primer valor actual del primer identificador de capa, una primera cadena de bits ofuscada correspondiente a la primera entrada de tecla, en el que la determinación de la primera cadena de bits ofuscada correspondiente a la primera entrada de tecla incluye

(i) usar el primer valor actual del primer identificador de capa para determinar un primer mapeo (140) que mapea cada una de la pluralidad de teclas con respecto a un conjunto diferente de coordenadas dentro de un primer espacio virtual, correspondiendo cada conjunto de coordenadas dentro del primer espacio virtual a una cadena de bits diferente, y

(ii) usar el primer mapeo para mapear la primera tecla con respecto a la primera cadena de bits ofuscada;

generar, por el uno o más procesadores y usando la primera cadena de bits ofuscada, al menos una primera parte de una primera cadena de datos ofuscada;

provocar, por el uno o más procesadores, que la primera cadena de datos ofuscada se transmita a otro dispositivo (260) a través de una red (106);

recibir, por el uno o más procesadores a través de la interfaz de comunicación (126) y el canal de comunicación seguro, la segunda información desde el servidor remoto, incluyendo la segunda información al menos un segundo valor actual del primer identificador de capa, y siendo el segundo valor actual del primer identificador de capa un nuevo valor resultante de un cambio, realizado por el servidor remoto, al primer valor actual del primer identificador de capa;

detectar, por el uno o más procesadores, una segunda entrada de tecla realizada a través de la interfaz de usuario, siendo la segunda entrada de tecla una entrada de una segunda tecla de la pluralidad de teclas;

determinar, por el uno o más procesadores y usando el segundo valor actual del primer identificador de capa, una segunda cadena de bits ofuscada correspondiente a la segunda entrada de tecla, en el que la determinación de la segunda cadena de bits ofuscada correspondiente a la segunda entrada de tecla incluye

(i) usar el segundo valor actual del primer identificador de capa para determinar un segundo mapeo que mapea cada una de la pluralidad de teclas con respecto a un conjunto diferente de coordenadas dentro de un segundo espacio virtual, correspondiendo cada conjunto de coordenadas dentro del segundo espacio virtual a una cadena de bits diferente, y siendo el segundo mapeo diferente del primer mapeo, y

(ii) usar el segundo mapeo para mapear la segunda tecla con respecto a la segunda cadena de bits ofuscada;

generar, por el uno o más procesadores y usando la segunda cadena de bits ofuscada, al menos una primera parte de una segunda cadena de datos ofuscada; y

provocar, por el uno o más procesadores, que la segunda cadena de datos ofuscada se transmita a otro dispositivo (260) a través de la red (106).

2. El método según la reivindicación 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 de tecla incluye la detección de cuál de la pluralidad de teclas se tocó o presionó.

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

4. El método según la reivindicación 1, que comprende, además, solicitar la primera información del servidor remoto, en el que la recepción de la primera información es en respuesta a la solicitud de la primera información.

5. El método según la reivindicación 1, en el que el primer identificador de capa está asociado con una entidad en un registro mantenido por el servidor remoto.

6. El método según la reivindicación 5, en el que la entidad es uno de:

el dispositivo electrónico;

una organización asociada con el dispositivo electrónico; o

una persona asociada a una transacción que se realiza a través del dispositivo electrónico.

7. El método según la reivindicación 1, en el que:

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 momento; y

el segundo valor actual del primer identificador de capa está asociado con la entidad en el registro en un segundo momento después del primer momento.

8. El método según la reivindicación 7, en el que la entidad es uno de:

el dispositivo electrónico;

una organización asociada con el dispositivo electrónico; o

una persona asociada a una transacción que se realiza a través del dispositivo electrónico.

9. El método según la reivindicación 1, en el que:

la primera información incluye, además, un primer valor actual de un segundo identificador de capa;

la segunda información incluye, además, un segundo valor actual del segundo identificador de capa;

generar la primera cadena de datos ofuscada usando la primera cadena de bits ofuscada incluye

codificar, usando el primer valor actual del segundo identificador de capa, al menos una parte de la primera cadena de bits ofuscada para generar una tercera cadena de bits ofuscada, y

generar la primera cadena de datos ofuscada usando la tercera cadena de bits ofuscada; y

generar la segunda cadena de datos ofuscada usando la segunda cadena de bits ofuscada incluye

codificar, usando el segundo valor actual del segundo identificador de capa, al menos una parte de la segunda cadena de bits ofuscada para generar una cuarta cadena de bits ofuscada, y

generar la segunda cadena de datos ofuscada usando la cuarta cadena de bits ofuscada.

10. El método según la reivindicación 9, que comprende, además:

solicitar la primera información desde el servidor remoto; y

solicitar la segunda información desde el servidor remoto,

en el que recibir la primera información es en respuesta a la solicitud de la primera información, y

en el que recibir la segunda información es en respuesta a la solicitud de la segunda información.

11. Un dispositivo electrónico que comprende:

una interfaz de usuario (124, 300) que incluye una pluralidad de teclas;

una interfaz de comunicación (126);

una memoria (122); y

uno o más procesadores configurados para

recibir, a través de la interfaz de comunicación (126) y un canal de comunicación seguro, primera información desde un servidor remoto que cambia los valores de un primer identificador de capa periódicamente y/o bajo solicitud, incluyendo la primera información al menos un primer valor actual del primer identificador de capa,

detectar una primera entrada de tecla (502) realizada a través de la interfaz de usuario, siendo la primera entrada de tecla una entrada de una primera tecla de la pluralidad de teclas,

determinar, usando el primer valor actual del primer identificador de capa, una primera cadena de bits ofuscada correspondiente a la primera entrada de tecla, en el que la determinación de la primera cadena de bits ofuscada correspondiente a la primera entrada de tecla incluye

(i) usar el primer valor actual del primer identificador de capa para determinar un primer mapeo (140) que mapea cada una de la pluralidad de teclas con respecto a un conjunto diferente de coordenadas dentro de un primer espacio virtual, correspondiendo cada conjunto de coordenadas dentro del primer espacio virtual a una cadena de bits diferente, y

(ii) usar el primer mapeo (140) para mapear la primera tecla con respecto a la primera cadena de bits ofuscada,

generar al menos una primera parte de una primera cadena de datos ofuscada usando la primera cadena de bits ofuscada,

provocar que la primera cadena de datos ofuscada se transmita a otro dispositivo a través de una red,

recibir, a través de la interfaz de comunicación (126) y el canal de comunicación seguro, segunda información desde el servidor remoto, incluyendo la segunda información al menos un segundo valor actual del primer identificador de capa, y siendo el segundo valor actual del primer identificador de capa un nuevo valor resultante de un cambio, realizado por el servidor remoto, al primer valor actual del primer identificador de capa,

detectar una segunda entrada de tecla realizada a través de la interfaz de usuario, siendo la segunda entrada de tecla una entrada de una segunda tecla de la pluralidad de teclas,

determinar, usando el segundo valor actual del primer identificador de capa, una segunda cadena de bits ofuscada correspondiente a la segunda entrada de tecla, en el que la determinación de la segunda cadena de bits ofuscada correspondiente a la segunda entrada de tecla incluye

(i) usar el segundo valor actual del primer identificador de capa para determinar un segundo mapeo que mapea cada una de la pluralidad de teclas con respecto a un conjunto diferente de coordenadas dentro de un segundo espacio virtual, correspondiendo cada conjunto de coordenadas dentro del segundo espacio virtual a una cadena de bits diferente, y siendo el segundo mapeo diferente del primer mapeo, y

(ii) usar el segundo mapeo para mapear la segunda tecla con respecto a la segunda cadena de bits ofuscada,

generar al menos una primera parte de una segunda cadena de datos ofuscada usando la segunda cadena de bits ofuscada, y

provocar que la segunda cadena de datos ofuscada se transmita a otro dispositivo (260) a través de la red (106).

12. El dispositivo electrónico según la reivindicación 11, en el que:

la interfaz de usuario incluye un teclado físico;

cada tecla de la pluralidad de teclas es una tecla diferente en el teclado físico; y

el uno o más procesadores están configurados para detectar la primera entrada de tecla al menos detectando cuál de la pluralidad de teclas se tocó o presionó.

13. El dispositivo electrónico según la reivindicación 11, en el que:

la interfaz de usuario incluye un teclado virtual presentado en una pantalla táctil del dispositivo electrónico;

cada tecla de la pluralidad de teclas es una tecla diferente en el teclado virtual; y

el uno o más procesadores están configurados para detectar la primera entrada de tecla al menos detectando qué área de la pantalla táctil se tocó.

14. El dispositivo electrónico según la reivindicación 11, 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 la primera cadena de datos ofuscada usando la primera cadena de bits ofuscada al menos mediante:

codificación, usando el primer valor actual del segundo identificador de capa, de al menos una parte de la primera cadena de bits ofuscada para generar una tercera cadena de bits ofuscada; y

generación de la primera cadena de datos ofuscada que usa la tercera cadena de bits ofuscada.

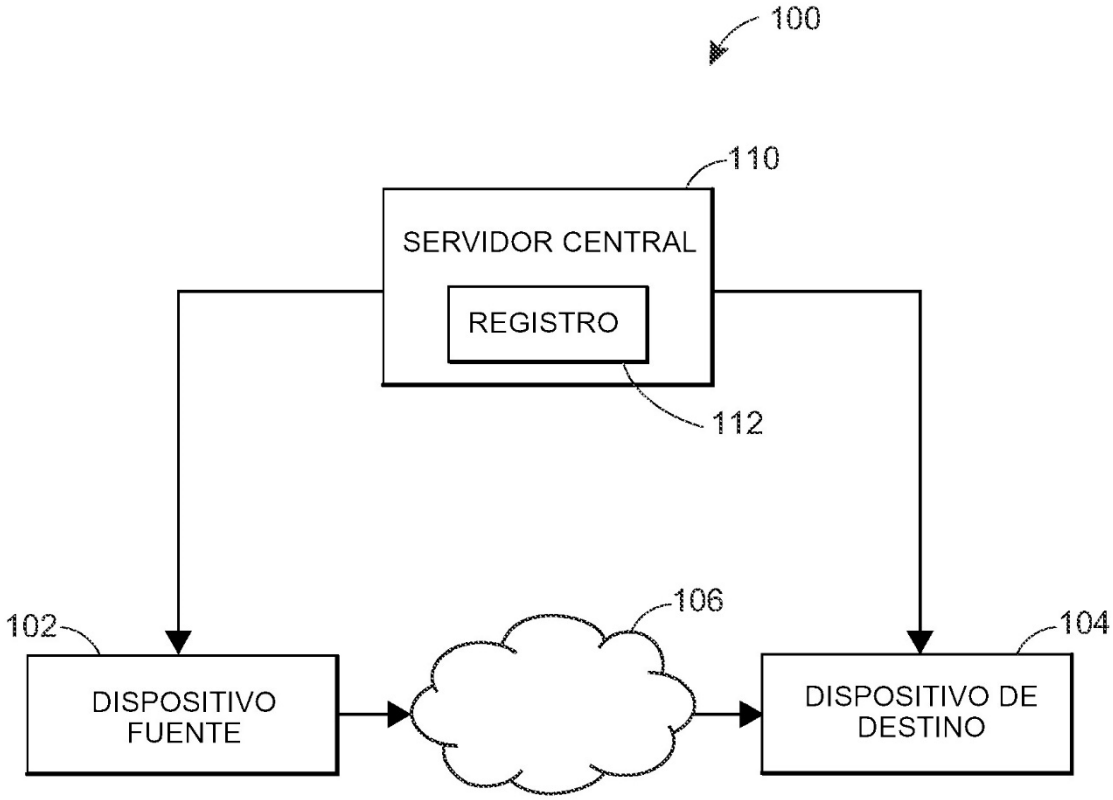
100
110
SERVIDOR CENTRAL
REGISTRO
112
102
106
104
DISPOSITIVO FUENTE
DISPOSITIVO DE DESTINO

FIG. 1

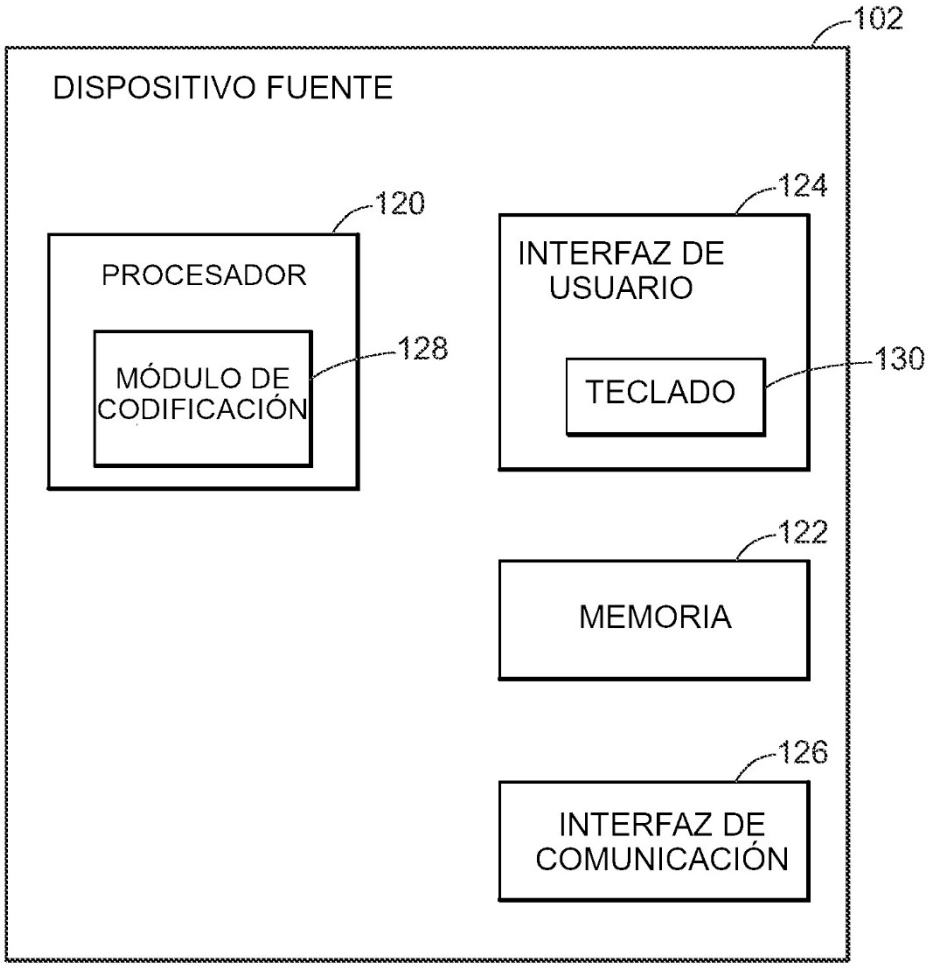
102
DISPOSITIVO FUENTE
120
PROCESADOR
128
MÓDULO DE CODIFICACIÓN
124
INTERFAZ DE USUARIO
130
TECLADO
122
MEMORIA
126
INTERFAZ DE COMUNICACIÓN

FIG. 2

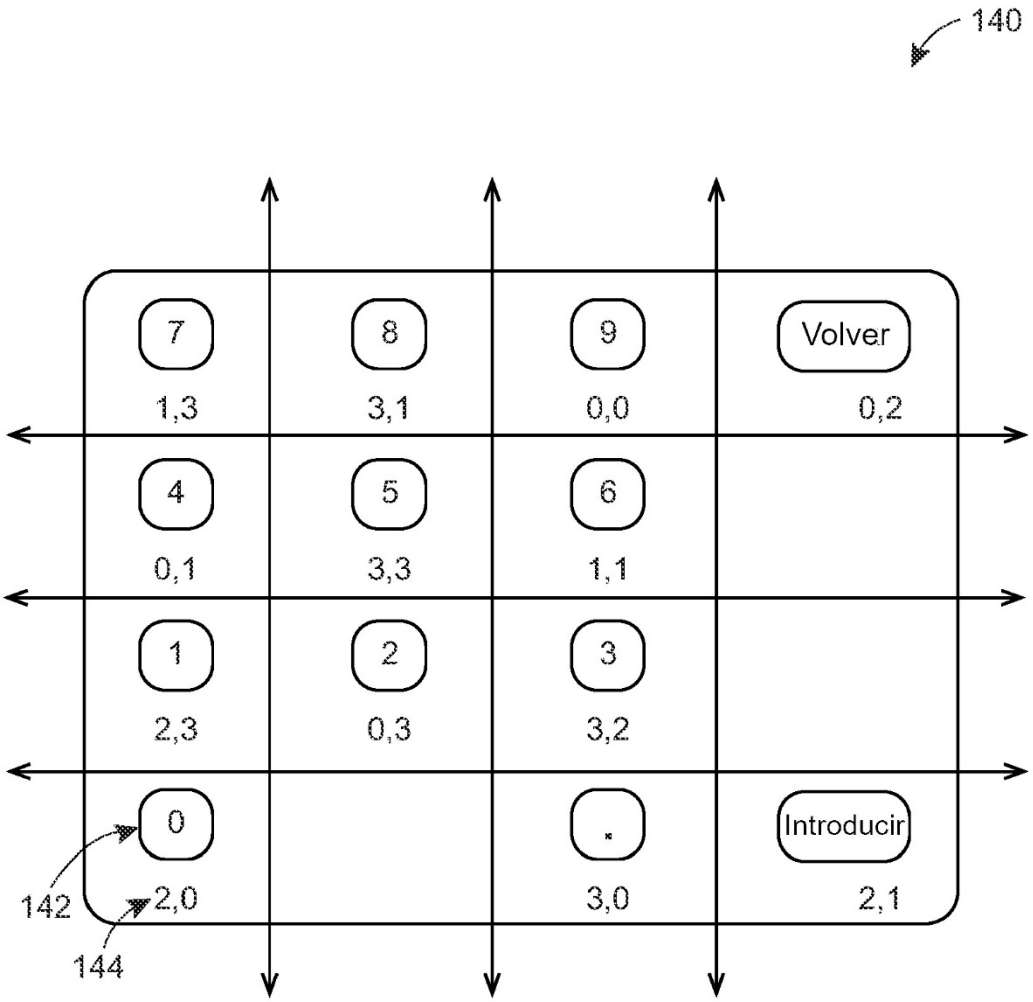
140
7
8
9
Volver
1,3
3,1
0,0
0,2
4
5
6
0,1
3,3
1,1
1
2
3
2,3
0,3
3,2
0
.
Introducir
142
2,0
3,0
2,1
144

FIG. 3

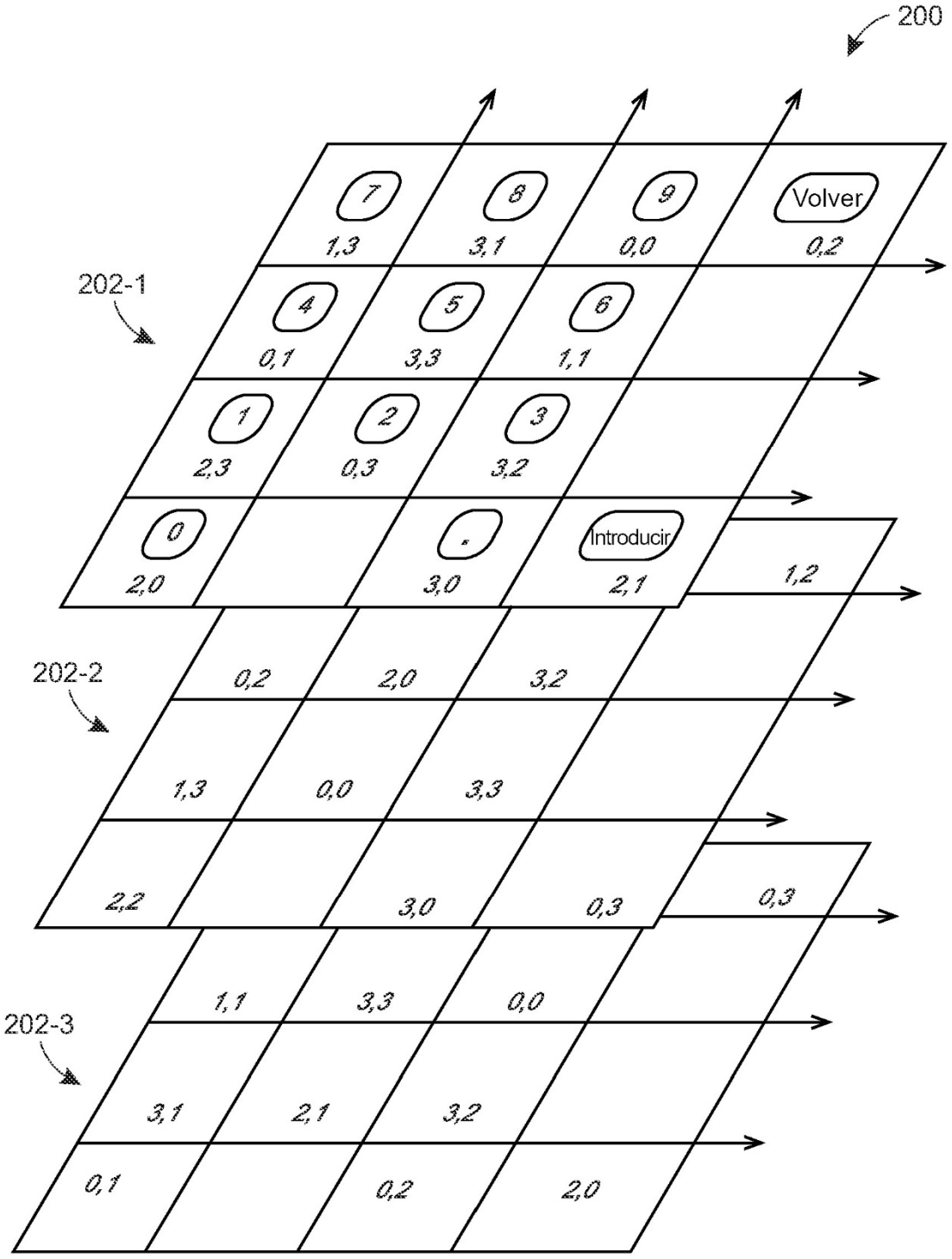
200
202-1
202-2
202-3
7
1,3
8
3,1
9
0,0
Volver
0,2
4
0,1
5
3,3
6
1,1
1
2,3
2
0,3
3
3,2
0
2,0
.
3,0
Introducir
2,1
1,2
0,2
2,0
3,2
1,3
0,0
3,3
2,2
3,0
0,3
0,3
1,1
3,3
0,0
3,1
2,1
3,2
0,1
0,2
2,0

FIG. 4

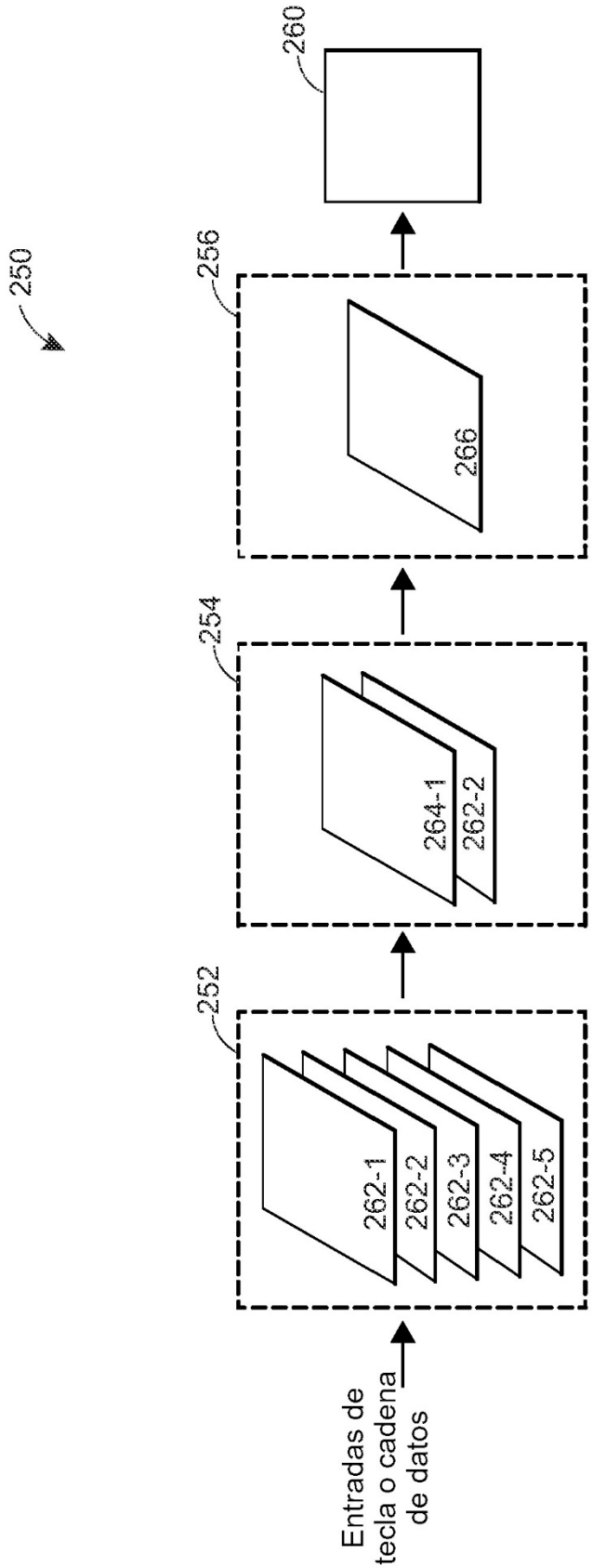
250
252
262-1
262-2
262-3
262-4
262-5
254
264-1
262-2
256
266
260
Entradas de tecla o cadena de datos

FIG. 5

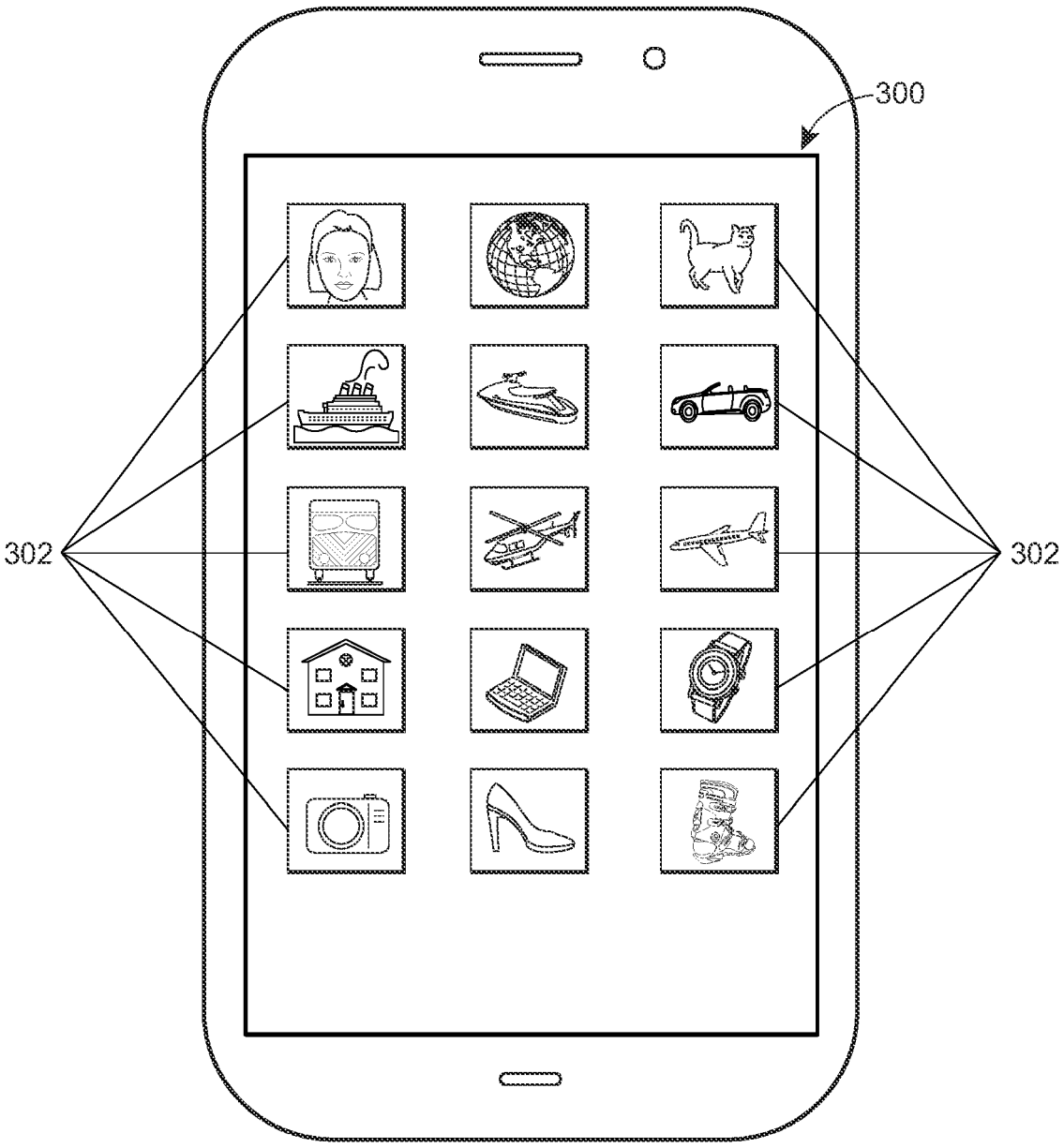

FIG. 6

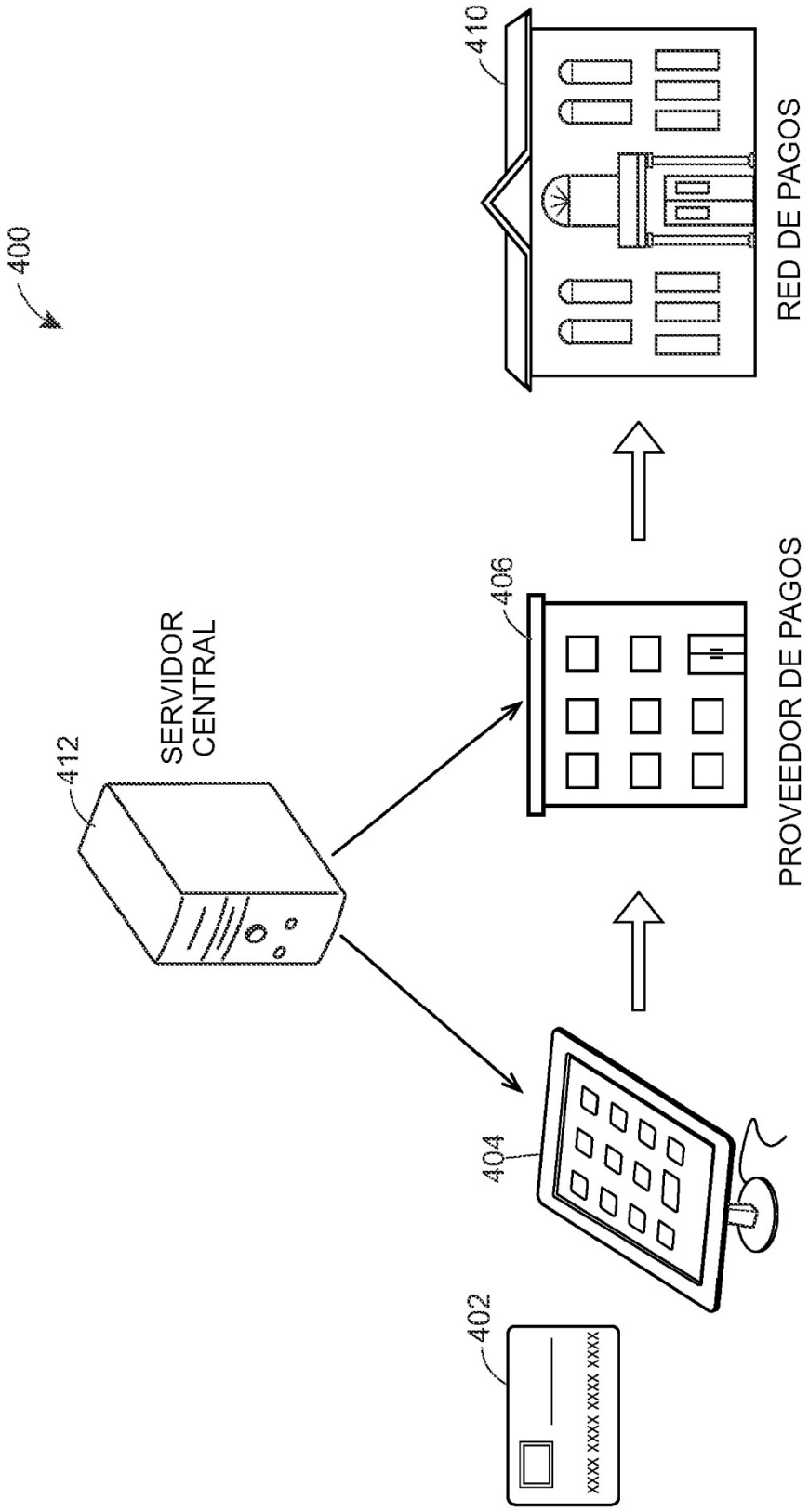
400
410
RED DE PAGOS
406
PROVEEDOR DE PAGOS
412
SERVIDOR CENTRAL
404
402
XXXX XXXX XXXX XXXX

FIG. 7

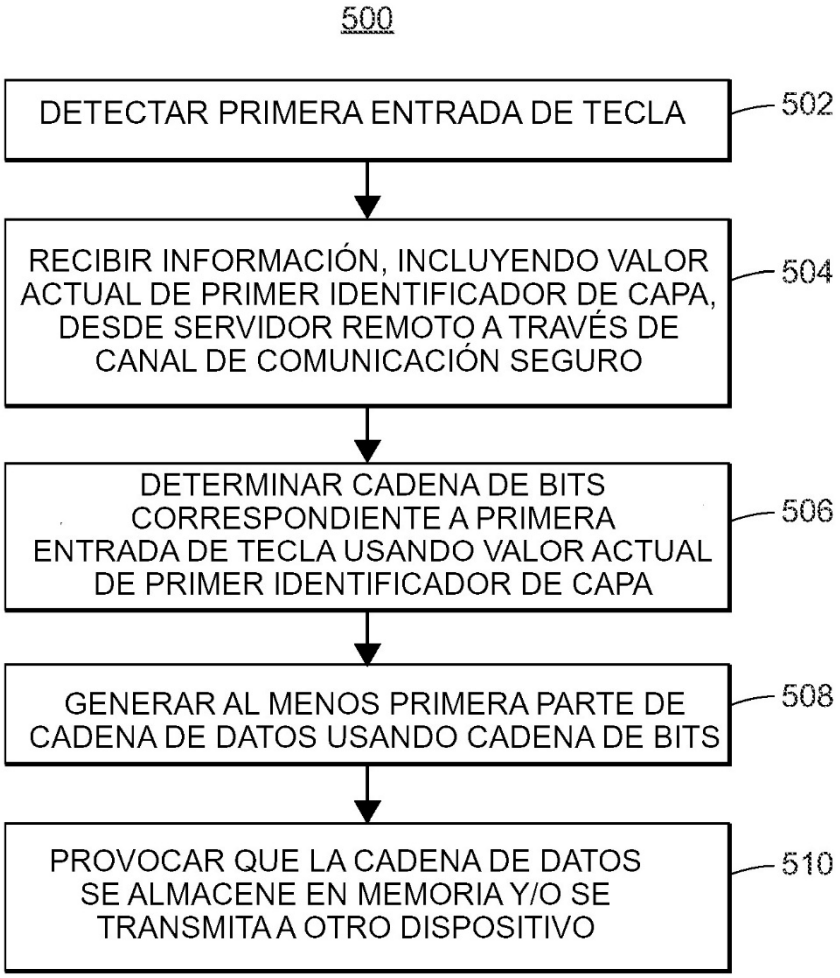
500
DETECTAR PRIMERA ENTRADA DE TECLA
502
RECIBIR INFORMACIÓN, INCLUYENDO VALOR ACTUAL DE PRIMER IDENTIFICADOR DE CAPA, DESDE SERVIDOR REMOTO A TRAVÉS DE CANAL DE COMUNICACIÓN SEGURO
504
DETERMINAR CADENA DE BITS CORRESPONDIENTE A PRIMERA ENTRADA DE TECLA USANDO VALOR ACTUAL DE PRIMER IDENTIFICADOR DE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

FIG. 8

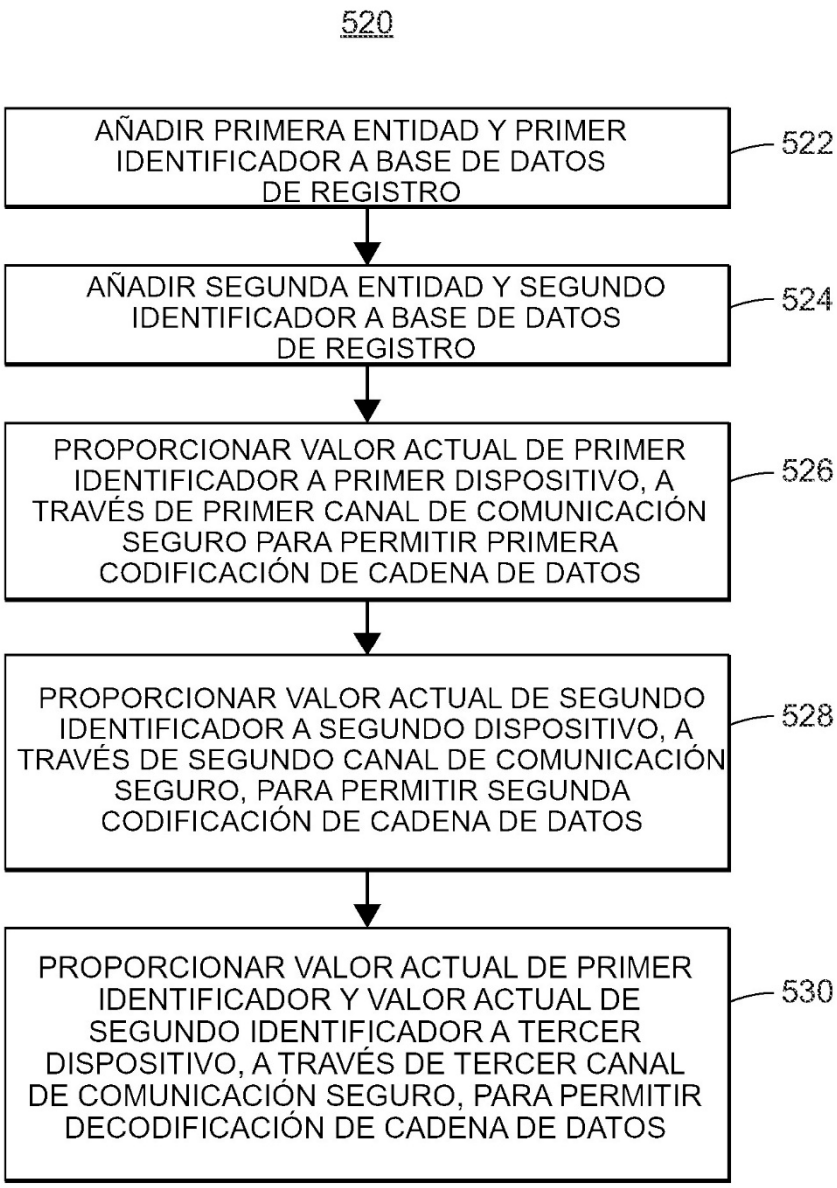
520
AÑADIR PRIMERA ENTIDAD Y PRIMER IDENTIFICADOR A BASE DE DATOS DE REGISTRO
522
AÑADIR SEGUNDA ENTIDAD Y SEGUNDO IDENTIFICADOR A BASE DE DATOS DE REGISTRO
524
PROPORCIONAR VALOR ACTUAL DE PRIMER IDENTIFICADOR A PRIMER DISPOSITIVO, A TRAVÉS DE PRIMER CANAL DE COMUNICACIÓN SEGURO PARA PERMITIR PRIMERA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

FIG. 9

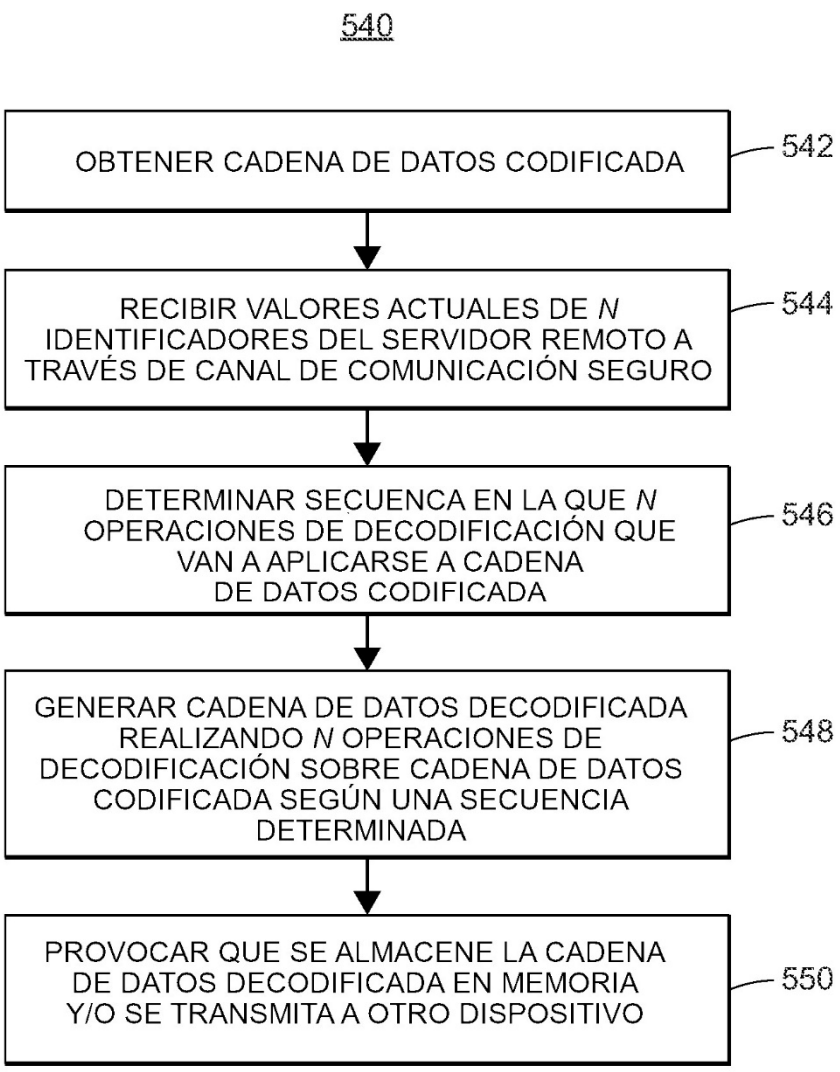
540
OBTENER CADENA DE DATOS CODIFICADA
542
RECIBIR VALORES ACTUALES DE N IDENTIFICADORES DEL SERVIDOR REMOTO A TRAVÉS DE CANAL DE COMUNICACIÓN SEGURO
544
DETERMINAR SECUENCA EN LA QUE N OPERACIONES DE DECODIFICACIÓN QUE VAN A APLICARSE A CADENA DE DATOS CODIFICADA
546
GENERAR CADENA DE DATOS DECODIFICADA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

FIG. 10