(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 680 660**

(51) Int. CI.:

G06F 21/62 (2013.01)
G06F 21/60 (2013.01)
G06F 9/455 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.03.2013 PCT/US2013/031597**

(87) Fecha y número de publicación internacional: **10.10.2013 WO13151732**

(96) Fecha de presentación y número de la solicitud europea: **14.03.2013 E 13713640 (4)**

(97) Fecha y número de publicación de la concesión europea: **09.05.2018 EP 2834768**

(54) Título: **Sistemas y métodos para asegurar y restaurar máquinas virtuales**

(30) Prioridad:

06.04.2012 US 201261621268 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.09.2018

(73) Titular/es:

SECURITY FIRST CORP. (100.0%)
29811 Santa Margarita Parkway, Suite 600
Rancho Santa Margarita, CA 92688, US

(72) Inventor/es:

O'HARE, MARK, S. y
ORSINI, RICK, L.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistemas y métodos para asegurar y restaurar máquinas virtuales

Referencia cruzada a solicitud relacionada

Esta solicitud reivindica prioridad a la Solicitud Provisional de Estados Unidos N. º 61/621.268, presentada el 6 de abril de 2012.

Campo técnico

Esta divulgación se refiere en general a sistemas y métodos para asegurar entornos informáticos de máquina virtual

Los documentos WO 2006/047694 A1 y US 2011/0271279 proporcionan la técnica anterior pertinente en el mismo campo técnico.

Sumario

En algunos aspectos, se proporcionan métodos para asegurar una máquina virtual. Una máquina virtual se ejecuta en un dispositivo de anfitrión. La máquina virtual incluye ficheros de máquina virtual. Se genera información de análisis de datos que es usable para determinar en cuál de una pluralidad de compartimentos se colocará una unidad de datos de los ficheros de máquina virtual y cómo la unidad de datos se encriptará. Los ficheros de máquina virtual pueden restaurarse accediendo a un número umbral de la pluralidad de compartimentos. En respuesta a recibir un comando para detener la máquina virtual, se genera la pluralidad de compartimentos basándose en la información de análisis de datos, y se provoca que cada una de la pluralidad de compartimentos se almacene en respectivas localizaciones de almacenamiento separadas.

En algunas implementaciones, el dispositivo anfitrión puede ser un dispositivo informático portátil. Los ficheros de máquina virtual pueden incluir al menos uno de un fichero de registro, un fichero de estado de BIOS de máquina virtual, un fichero de disco virtual, un fichero de paginación, un fichero de estado de instantánea, un fichero de estado suspendido, y un fichero de configuración. El comando para detener la máquina virtual puede incluir al menos uno de un comando de grabación, un comando de apagado, un comando de suspensión y un comando de pausa. El comando para detener la máquina virtual puede emitirse por un usuario del dispositivo anfitrión. En algunas implementaciones, el comando para detener la máquina virtual se emite por un procesador del dispositivo anfitrión sin un comando sustancialmente síncrono de un usuario del dispositivo anfitrión.

En algunas implementaciones, generar la pluralidad de compartimentos basándose en la información de análisis de datos puede implicar identificar una pluralidad de porciones de los ficheros de máquina virtual y encriptar cada una de la pluralidad de porciones para formar la pluralidad de compartimentos. En algunas implementaciones, generar la pluralidad de compartimentos basándose en la información de análisis de datos puede implicar encriptar los ficheros de máquina virtual e identificar una pluralidad de porciones de los ficheros de máquina virtual encriptados para formar la pluralidad de compartimentos.

En algunas implementaciones, la información de análisis de datos especifica una técnica determinística para determinar en cuál de la pluralidad de compartimentos se colocará la porción de los ficheros de máquina virtual. En algunas implementaciones, la información de análisis de datos especifica una técnica determinística para determinar en qué posición en cada una de la pluralidad de compartimentos se colocará la porción de los ficheros de máquina virtual. En algunas implementaciones, la información de análisis de datos especifica una técnica sustancialmente aleatoria para determinar en cuál de la pluralidad de compartimentos se colocará la porción de los ficheros de máquina virtual. En algunas implementaciones, la información de análisis de datos especifica una técnica sustancialmente aleatoria para determinar en qué posición en cada una de la pluralidad de compartimentos se colocará la porción de los ficheros de máquina virtual.

En algunas implementaciones, las localizaciones de almacenamiento separadas incluyen una pluralidad de localizaciones de almacenamiento separadas en el dispositivo anfitrión. En algunas implementaciones, las localizaciones de almacenamiento separadas incluyen una pluralidad de localizaciones de almacenamiento separadas en uno o más dispositivos remotos del dispositivo anfitrión. En algunas implementaciones, las localizaciones de almacenamiento separadas incluyen al menos una localización de almacenamiento en el dispositivo anfitrión y al menos una localización de almacenamiento en un dispositivo remoto del dispositivo anfitrión.

En algunas implementaciones, antes de ejecutar la máquina virtual en el dispositivo anfitrión, puede recibirse una segunda pluralidad de compartimentos, y los ficheros de máquina virtual desde la segunda pluralidad de compartimentos pueden restaurarse usando los datos que restaura la información que determina cómo desencriptar y disponer porciones desde la pluralidad de compartimentos para formar los ficheros de máquina virtual. La segunda pluralidad de compartimentos puede recibirse desde uno o más dispositivos remotos del dispositivo anfitrión. El uno o más dispositivos remotos del dispositivo anfitrión pueden incluir uno o más servidores de datos. Las localizaciones

de almacenamiento separadas en las que se almacena la pluralidad de comparticiones respectivamente pueden estar localizadas en el uno o más dispositivos remotos del dispositivo anfitrión desde el que se recibe la segunda pluralidad de comparticiones.

En algunas implementaciones, antes de generar la información de análisis de datos, puede recibirse una tercera pluralidad de comparticiones, y puede restaurarse una aplicación de análisis ejecutable desde la tercera pluralidad de comparticiones. La información de análisis de datos puede generarse por la aplicación de análisis ejecutable. La tercera pluralidad de comparticiones puede recibirse desde uno o más dispositivos remotos del dispositivo anfitrión. El uno o más dispositivos remotos del dispositivo anfitrión incluyen uno o más servidores de datos. En algunas implementaciones, restaurar la aplicación de análisis ejecutable desde la tercera pluralidad de comparticiones pueden implicar ensamblar la tercera pluralidad de comparticiones de acuerdo con una técnica almacenada en y ejecutable por el dispositivo anfitrión. En algunas implementaciones, restaurar la aplicación de análisis ejecutable desde la tercera pluralidad de comparticiones implica ensamblar la tercera pluralidad de comparticiones de acuerdo con una técnica especificada en la tercera pluralidad de comparticiones y ejecutable por el dispositivo anfitrión.

En algunas implementaciones, el número umbral es menor que un número total de la pluralidad de comparticiones. La información de análisis de datos puede determinar el tamaño de cada una de las comparticiones, en la que el tamaño de al menos una compartición es diferente del tamaño de al menos otra compartición. El dispositivo anfitrión puede incluir uno o más ordenadores en una arquitectura distribuida y/o uno o más ordenadores en un entorno informático en la nube.

En otros aspectos, se proporcionan métodos para restaurar un conjunto de datos en respuesta a recibir una secuencia predeterminada de entradas de usuario. Un sistema informático genera una pluralidad de elementos seleccionables por el usuario para visualizar por una pantalla de un dispositivo informático del sistema informático, cada elemento asociado con una aplicación ejecutable diferente. Se recibe una secuencia predeterminada de entradas de usuario en el dispositivo informático mientras se visualiza la pluralidad de elementos seleccionables por el usuario, y en respuesta a recibir la secuencia predeterminada de entradas de usuario, se ejecuta una aplicación de restauración criptográfica no asociada con ningún elemento seleccionable por el usuario visualizado para restaurar un conjunto de datos desde una pluralidad de comparticiones de conjunto de datos (cada compartición de conjunto de datos representativa de una porción encriptada del conjunto de datos).

En algunas implementaciones, el dispositivo informático es un dispositivo informático portátil. Los elementos seleccionables por el usuario pueden incluir al menos un icono y/o al menos una lista de menú desplegable. En algunas implementaciones, la secuencia predeterminada de entradas de usuario incluye una entrada gestual, una entrada de reconocimiento biométrico, una orientación del dispositivo informático, una entrada de teclado numérico, y/o una aceleración del dispositivo informático. En respuesta a restaurar el conjunto de datos desde la pluralidad de comparticiones de conjunto de datos, un elemento gráfico asociado con el conjunto de datos puede visualizarse en la pantalla.

En algunas implementaciones, el conjunto de datos puede estar asociado con una aplicación ejecutable por el dispositivo informático, y en respuesta a restaurar el conjunto de datos desde la pluralidad de comparticiones de conjunto de datos, puede ejecutarse la aplicación asociada con el conjunto de datos. La aplicación puede ser una aplicación de comunicación telefónica.

En algunas implementaciones, la aplicación es una aplicación de máquina virtual. En implementaciones de este tipo, el conjunto de datos puede ser representativo de ficheros de máquina virtual, y ejecutar la aplicación asociada con el conjunto de datos puede implicar iniciar una máquina virtual usando los ficheros de máquina virtual. Además, los ficheros de máquina virtual pueden incluir al menos uno de un fichero de registro, un fichero de estado de BIOS de máquina virtual, un fichero de disco virtual, un fichero de paginación, un fichero de estado de instantánea, un fichero de estado suspendido, y un fichero de configuración.

En algunas implementaciones, dos o más comparticiones de conjunto de datos de la pluralidad de comparticiones de conjunto de datos se almacenan en respectivas localizaciones de almacenamiento separadas en el dispositivo informático. En algunas implementaciones, al menos una compartición de conjunto de datos de la pluralidad de comparticiones de conjunto de datos puede almacenarse en el dispositivo informático, y al menos una compartición de conjunto de datos de la pluralidad de comparticiones de conjunto de datos puede almacenarse en un dispositivo remoto del dispositivo informático. En algunas implementaciones, dos o más comparticiones de conjunto de datos de la pluralidad de comparticiones de conjunto de datos se almacenan en localizaciones de almacenamiento separadas en uno o más dispositivos remotos del dispositivo informático.

En algunas implementaciones, cada compartición de conjunto de datos puede representar una porción de datos del conjunto de datos seleccionado y/o dispuesta de acuerdo con una técnica determinística. En algunas implementaciones, cada compartición de conjunto de datos puede representar una porción de datos del conjunto de datos seleccionado y/o dispuesta de acuerdo con una técnica sustancialmente aleatoria. El sistema informático puede incluir uno o más ordenadores en una arquitectura distribuida y/o uno o más ordenadores en un entorno informático en la nube.

En otros aspectos, se proporcionan métodos para restaurar un conjunto de datos desde comparticiones de conjunto de datos desde una pluralidad de dispositivos informáticos. Se identifican primeras comparticiones de conjunto de datos almacenadas en un primer dispositivo informático de un sistema informático programado. Cada primera compartición de datos es representativa de una porción de datos del conjunto de datos, en el que el conjunto de datos no puede restaurarse desde las primeras comparticiones de conjunto de datos identificadas sino que puede restaurarse por un número umbral de comparticiones de conjunto de datos. Se detecta un enlace de comunicación entre el primer dispositivo informático y un segundo dispositivo informático diferente del primer dispositivo informático, y en respuesta a la detección, se reciben segundas comparticiones de conjunto de datos desde el segundo dispositivo informático en el primer dispositivo informático. Cuando la primera y segunda comparticiones de conjunto de datos se determina que incluyen al menos el número umbral de comparticiones de conjunto de datos, el conjunto de datos se restaura usando la primera y segunda comparticiones de conjunto de datos.

En algunas implementaciones, detectar un enlace de comunicación implica determinar que el segundo dispositivo informático está en un alcance de comunicación de un dispositivo de comunicación de frecuencia de radio del primer dispositivo informático. El dispositivo de comunicación de frecuencia de radio puede ser un dispositivo de Bluetooth o un dispositivo de comunicación de campo cercano. En otras implementaciones, detectar un enlace de comunicación implica determinar que el segundo dispositivo informático está conectado a una red de comunicaciones informáticas a la que también está conectado el primer dispositivo informático.

En algunas implementaciones, detectar un enlace de comunicación implica determinar que el segundo dispositivo informático está a una distancia geográfica predeterminada del primer dispositivo informático. En implementaciones de este tipo, determinar que el segundo dispositivo informático está dentro de una distancia geográfica predeterminada del primer dispositivo informático puede implicar recibir, en el primer dispositivo informático, un mensaje desde un servidor que indica proximidad del segundo dispositivo informático.

En algunas implementaciones, detectar un enlace de comunicación implica detectar una ruta de comunicación eléctrica entre el primer dispositivo informático y el segundo dispositivo informático mediante un cuerpo de un usuario del primer dispositivo informático y un cuerpo de un usuario del segundo dispositivo informático, los cuerpos de los usuarios en contacto físico entre sí y con sus respectivos dispositivos informáticos.

En algunas implementaciones, antes de identificar las primeras comparticiones de conjunto de datos, pueden recibirse al menos algunas de las primeras comparticiones de conjunto de datos desde un tercer dispositivo informático en respuesta a detectar un enlace de comunicación entre el primer dispositivo informático y el tercer dispositivo informático.

El primer dispositivo informático y/o el segundo dispositivo informático pueden ser un dispositivo informático portátil. En algunas implementaciones, el segundo dispositivo informático incluye un servidor.

En algunas implementaciones, en respuesta a restaurar el conjunto de datos desde la primera y segunda comparticiones de conjunto de datos, un elemento gráfico asociado con el conjunto de datos puede visualizarse en una pantalla del primer dispositivo informático. En algunas implementaciones, el conjunto de datos está asociado con una aplicación ejecutable por el dispositivo informático, y en respuesta a restaurar el conjunto de datos desde la pluralidad de comparticiones de conjunto de datos, se ejecuta la aplicación asociada con el conjunto de datos. La aplicación puede ser una aplicación de juegos.

En algunas implementaciones, en respuesta a detectar el enlace de comunicación, las primeras comparticiones de conjunto de datos pueden transmitirse desde el primer dispositivo informático al segundo dispositivo informático. En algunas implementaciones, se reciben las segundas comparticiones de conjunto de datos mediante el enlace de comunicación. En algunas implementaciones, cada compartición de conjunto de datos puede representar una porción de datos del conjunto de datos seleccionado y/o dispuesta de acuerdo con una técnica determinística. En algunas implementaciones, cada compartición de conjunto de datos puede representar una porción de datos del conjunto de datos seleccionado y/o dispuesta de acuerdo con una técnica sustancialmente aleatoria. El primer dispositivo informático y el segundo dispositivo informático pueden estar dispuestos en una arquitectura distribuida y/o pueden estar en un entorno informático en la nube.

De acuerdo con otros aspectos, se proporcionan sistemas para llevar a cabo las funcionalidades anteriormente descritas.

Breve descripción de los dibujos

La presente divulgación se describe en más detalle a continuación en relación con los dibujos adjuntos, que se pretenden para ilustrar y no para limitar la divulgación, y en los que:

La Figura 1 ilustra un proceso para asegurar datos que incluye características ilustrativas que pueden usarse en combinación con cualquiera de los procesos analizados en el presente documento, de acuerdo con una implementación.

La Figura 2 ilustra un proceso para analizar datos con encriptación y almacenamiento de la clave maestra de encriptación con los datos de acuerdo con una implementación.
La Figura 3 ilustra un proceso para analizar datos con encriptación y almacenamiento de la clave maestra de encriptación de manera separada de los datos de acuerdo con una implementación.
La Figura 4 ilustra el proceso de clave intermediaria para analizar datos con encriptación y almacenamiento de la clave maestra de encriptación con los datos de acuerdo con una implementación.
Las Figuras 5 y 6 son diagramas de bloques de un sistema ilustrativo que tiene el analizador de datos seguro integrado de acuerdo con una implementación.
La Figura 7 es un diagrama de flujo de proceso de etapas y características ilustrativas que pueden usarse en cualquier combinación adecuada, con cualesquiera adiciones, borrados o modificaciones adecuadas de acuerdo con una implementación.
La Figura 8 es un diagrama de bloques simplificado del almacenamiento de la clave y componentes de datos en comparticiones, usando opcionalmente una clave de grupo de trabajo, que puede usarse en cualquier combinación adecuada, con cualesquiera adiciones, borrados o modificaciones adecuadas de acuerdo con una implementación.
Las Figuras 9A y 9B son diagramas de flujo de proceso simplificados e ilustrativos para generación de encabezamiento y división de datos para datos en movimiento que pueden usarse en cualquier combinación adecuada, con cualesquiera adiciones, borrados o modificaciones de acuerdo con una implementación.
La Figura 10 es un diagrama de bloques simplificado de un formato de compartición ilustrativo, que puede usarse en cualquier combinación adecuada, con cualesquiera adiciones, borrados o modificaciones adecuadas de acuerdo con una implementación.
La Figura 11 es un diagrama de bloques que muestra varias disposiciones ejemplares para implementar una solución de seguridad de datos de informática en la nube de acuerdo con una implementación.
La Figura 12 es un diagrama de bloques de un dispositivo informático para realizar cualquiera de los procesos descritos en el presente documento.
La Figura 13 es un diagrama de flujo de un proceso para asegurar una máquina virtual (VM) de acuerdo con una implementación.
Las Figuras 14A-14G son diagramas de bloques de un entorno de VM seguro configurado para ejecutar el proceso de la Figura 13 de acuerdo con una implementación.
Las Figuras 15A-15B son diagramas de bloques de otro entorno de VM seguro configurado para ejecutar el proceso de la Figura 13 de acuerdo con una implementación.
La Figura 16 representa un ejemplo de una pantalla que incluye una estructura de directorio en la que las comparticiones de VM están “ocultas” de acuerdo con una implementación.
La Figura 17 representa un ejemplo de un sistema de medio de almacenamiento particionado usado para oscurecer la presencia de comparticiones de VM de acuerdo con una implementación.
La Figura 18 es un diagrama 1800 de flujo de un proceso para restaurar un conjunto de datos de acuerdo con implementaciones de este tipo.
Las Figuras 19A y 19B representan pantallas en un dispositivo portátil que pueden presentarse antes y después de que se identifica la secuencia predeterminada de entradas de usuario en el proceso de la Figura 18 de acuerdo con una implementación.
La Figura 20 es un diagrama de flujo de un proceso para restaurar un conjunto de datos de acuerdo con una implementación.
Las Figuras 21A y 21B ilustran una implementación de algunas de las etapas de la Figura 20.
Las Figuras 22A y 22B ilustran otra implementación de algunas de las etapas de la Figura 20.
Las Figuras 23A-23C ilustran otra implementación de algunas de las etapas de la Figura 20.
Las Figuras 24A y 24B ilustran otra implementación de algunas de las etapas de la Figura 20.
Las Figuras 25A-25C ilustran otra implementación de algunas de las etapas de la Figura 20.
Las Figuras 26A y 26B ilustran otra implementación de algunas de las etapas de la Figura 20.

Descripción detallada

De acuerdo con un aspecto, se describe en el presente documento un sistema criptográfico donde uno o más servidores seguros, implementados como un motor de confianza, almacenan claves criptográficas y datos de autenticación de usuario. Los usuarios acceden a la funcionalidad de sistemas criptográficos convencionales a través de la red de acceso al motor de confianza. Sin embargo, el motor de confianza no libera las claves reales y otros datos de autenticación y por lo tanto, las claves y los datos permanecen seguros. Este almacenamiento céntrico en el servidor de las claves y datos de autenticación proporciona seguridad independiente del usuario, portabilidad, disponibilidad y facilidad.

Puesto que los usuarios pueden estar seguros y confiar en el sistema criptográfico para realizar autenticación de usuario y de documentos y otras funciones criptográficas, puede incorporarse una amplia gama de funcionalidades en el sistema. Por ejemplo, el proveedor de motor de confianza puede asegurarse contra repudiación de acuerdo, por ejemplo, autenticando los participantes del acuerdo, firmando digitalmente el acuerdo en nombre de o para los participantes, y almacenando un registro del acuerdo firmado digitalmente por cada participante. Además, el sistema criptográfico puede monitorizar acuerdos y determinar aplicar grados variables de autenticación, basándose en, por ejemplo, precio, usuario, proveedor, localización geográfica, lugar de uso o similares.

El sistema criptográfico puede incluir un analizador de datos seguro ya sea en solitario o en combinación con otros componentes de sistema. Como se usa en el presente documento, un analizador de datos seguro incluye software y/o hardware configurado para realizar varias funciones relacionadas con uno o más del análisis, aseguración y almacenamiento de datos. Por ejemplo, las funciones del analizador de datos seguro pueden incluir cualquier combinación de encriptar datos, analizar datos en una o más comparticiones , encriptar comparticiones, dispersar comparticiones, almacenar de manera segura comparticiones en múltiples localizaciones, recuperar comparticiones de datos, desencriptar comparticiones de datos, re-ensamblar datos, desencriptar datos o cualquier otra función descrita en el presente documento. Analizar incluye generar una o más comparticiones distintas a partir de un conjunto de datos original donde cada una de las comparticiones incluye al menos una porción del conjunto de datos original. Analizar puede implementarse por cualquiera de un número de técnicas. Por ejemplo, analizar puede incluir distribuir unidades de datos a partir del conjunto de datos original en una o más comparticiones de manera aleatoria, pseudo-aleatoria, determinística o usando alguna combinación adecuada de técnicas aleatorias, pseudo-aleatorias y deterministicas. Una operación de análisis puede actuar en cualquier tamaño de datos, incluyendo un único bit, un grupo de bits, un grupo de bytes, un grupo de kilobytes, un grupo de megabytes, o mayores grupos de datos, así como cualquier patrón o combinación de tamaños de unidades de datos. Por lo tanto, los datos originales pueden verse como una secuencia de estas unidades de datos. En algunas implementaciones, la operación de análisis está basada en información de análisis generada por el analizador de datos seguro o por otro componente en el sistema criptográfico. La información de análisis puede estar en cualquier forma adecuada (por ejemplo, una o más claves que incluyen una clave predeterminada, determinística, pseudo-aleatoria o aleatoria). La información de análisis puede determinar uno o más aspectos de la operación de análisis, que incluye cualquier combinación del número de comparticiones, el tamaño de una o más comparticiones, el tamaño de las unidades de datos, el orden de las unidades de datos en las comparticiones, y el orden de los datos del conjunto de datos original en las comparticiones. En algunas realizaciones, la información de análisis puede indicar también o puede usarse (entre otros factores) para determinar cómo se encriptarán una o más comparticiones de datos. Aunque ciertas técnicas de análisis pueden presentar los datos más seguros (por ejemplo, en algunas implementaciones, el tamaño de las mismas unidades de datos pueden hacer a las comparticiones de datos resultantes más seguras, o el análisis puede implicar reorganizar datos de datos), este no es necesariamente el caso con cada técnica de análisis. Las comparticiones resultantes pueden ser de cualquier tamaño de datos, y dos o más comparticiones resultantes pueden contener diferentes cantidades del conjunto de datos original.

En algunas implementaciones, el análisis puede incluir realizar una operación criptográfica en el conjunto de datos original antes, durante o después de generar la una o más comparticiones. Por ejemplo, el análisis puede implicar mezclar el orden de las unidades de datos en la compartición, por ejemplo, reorganizando las unidades de datos en la compartición o comparticiones resultantes. En algunas implementaciones, el análisis puede implicar mezclar el orden de los bits en cada unidad de datos, por ejemplo, reorganizando subunidades en una o más unidades de datos que están distribuidas en la compartición o comparticiones resultantes, donde una sub-unidad incluye al menos una porción distinta de una unidad de datos. Cuando el análisis implica mezclar datos en el conjunto de datos original, la operación de mezclado puede realizarse en cualquier tamaño del conjunto de datos original, incluyendo el conjunto de datos original completo, la una o más comparticiones, las unidades de datos, un único bit, un grupo de bits, un grupo de bytes, un grupo de kilobytes, un grupo de megabytes, o mayores grupos de datos, así como cualquier patrón o combinación de tamaños de unidad de datos. Mezclar datos puede implicar distribuir los datos originales en una o más comparticiones de una manera que mezcla los datos, distribuye los datos originales en una o más comparticiones y a continuación mezcla los datos en la compartición o comparticiones resultantes, mezcla los datos originales y a continuación distribuye los datos mezclados en una o más comparticiones, o cualquier combinación de las mismas.

Por lo tanto, las comparticiones resultantes pueden incluir una distribución sustancialmente aleatoria del conjunto de datos original. Como se usa en el presente documento, una distribución de datos sustancialmente aleatoria hace referencia a generar una o más comparticiones distintas de un conjunto de datos original donde al menos una de las comparticiones se genera usando una o más técnicas aleatorias o pseudo-aleatorias, información aleatoria o pseudo-aleatoria (por ejemplo, una clave aleatoria o pseudo-aleatoria), o cualquier combinación de las mismas. Se entenderá que puesto que generar un número verdaderamente aleatorio en un ordenador puede no ser práctico, el uso de un número sustancialmente aleatorio será suficiente. Las referencias a aleatorización en el presente documento se entiende que incluyen aleatorización sustancial como cuando, por ejemplo, se implementan usando un dispositivo informático que tiene limitaciones con respecto a generar la aleatorización verdadera. Como un ejemplo de análisis de datos que da como resultado distribución sustancialmente aleatoria de los datos originales en comparticiones, considérese un conjunto de datos original de 23 bytes en tamaño, con el tamaño de la unidad de datos elegido para que sea un byte, y con el número de comparticiones seleccionado para que sean 4. Cada byte se distribuiría en una de las 4 comparticiones. Suponiendo una distribución sustancialmente aleatoria, se obtendría una clave para crear una secuencia de 23 números aleatorios (r_1, r_2, r_3 a r_{23}), cada uno con un valor entre 1 y 4 que corresponde a las cuatro comparticiones. Cada una de las unidades de datos (en este ejemplo, 23 bytes individuales de datos) está asociada con uno de los 23 números aleatorios que corresponden a una de las cuatro comparticiones. La distribución de los bytes de datos en las cuatro comparticiones tendría lugar colocando el primer byte de los datos en el número de compartición r_1, el byte dos en la compartición r_2, el byte tres en la compartición r_3, hasta el byte de orden 23 de datos en la compartición r_{23}. Puede usarse una amplia gama de otras posibles etapas o

combinación o secuencia de etapas, incluyendo ajustar el tamaño de las unidades de datos, en el proceso de análisis. Para recrear los datos originales, se realizaría la operación inversa.

Una operación de análisis puede añadir tolerancia a fallos a las comparticiones generadas de modo que sean necesarias menos de todas las comparticiones para restaurar los datos originales. Por ejemplo, la operación de análisis puede proporcionar suficiente redundancia en las comparticiones de manera que únicamente sea necesario un subconjunto de las comparticiones para re-ensamblar o restaurar los datos a su forma original o usable. Por ejemplo, el análisis puede hacerse como un análisis “3 de 4”, de manera que únicamente son necesarias tres de las cuatro comparticiones para re-ensamblar o restaurar los datos a su forma original o usable. Esto también se denomina como “análisis M de N” en el que N es el número total de comparticiones, y M es al menos uno menos N.

La Figura 1 muestra un sistema 100 de análisis de datos seguro ilustrativo (también denominado en el presente documento como un analizador de datos seguro). El sistema 100 de análisis de datos seguro puede implementarse usando hardware y/o software tal como un programa de análisis o conjunto de software. El analizador de datos seguro puede incluir adicionalmente o interactuar con una o más instalaciones de almacenamiento de datos y otros módulos de hardware o software a partir de los que puede recibirse o transmitirse datos y que pueden realizar diversas funciones en los datos. El sistema 100 puede incluir uno o más de pre-procesadores 104, uno o más analizadores 106 de datos, y uno o más post-procesadores 108. Todas las características descritas con respecto al sistema 100 son opcionales y las operaciones realizadas por el pre-procesador 104, el analizador 106 de datos y el post-procesador 108 pueden realizarse en cualquier combinación u orden posible. El analizador 100 de datos seguro recibe datos a asegurarse 102 y analiza los datos en un pre-procesador 104 que puede realizar cualquier combinación de pre-operaciones de procesamiento en los datos 102 recibidos, tal como encriptar los datos, añadir información de integridad (por ejemplo, una función de troceo) a los datos, y añadir información de autenticación a los datos. El pre-procesamiento puede implicar como alternativa o adicionalmente acceder y/o generar una o más claves u otra información usada por el analizador 100 de datos seguro. La una o más claves pueden ser cualquier clave o claves adecuadas para generar distintas porciones de datos desde un conjunto de datos original y/o cualquier clave adecuada para otras operaciones descritas en el presente documento que se realizan por el analizador 100 de datos seguro. La clave o claves pueden generarse de manera aleatoria, pseudo-aleatoria o determinística. Estas y otras operaciones de pre-procesamiento se describen adicionalmente en el presente documento.

Después de cualquier pre-procesamiento deseado, los (opcionalmente transformados) datos 102 y cualquier información adicional, tal como cualesquiera claves adecuadas, se pasan a un analizador 106 de datos. El analizador 106 de datos puede analizar los datos recibidos para generar una o más comparticiones desde los datos 102 usando cualquiera de las técnicas de análisis descritas en el presente documento. El analizador 106 de datos puede usar cualquier clave adecuada para análisis de datos.

En algunas implementaciones, el analizador 106 de datos implica analizar una o más claves usadas en la encriptación o análisis de los datos. Cualquiera de las técnicas de análisis anteriormente descritas puede usarse para analizar cualquier clave. En algunas realizaciones, analizar una clave provoca que la clave se almacene en una o más comparticiones de los datos 102 analizados. En otras realizaciones, las comparticiones de clave resultantes de una operación de análisis de clave se almacenan de manera separada de las comparticiones de datos resultantes de la operación de análisis de datos. Estas y otras características y funciones que pueden realizarse por el analizador 106 de datos se describen adicionalmente en el presente documento.

Después de analizar los datos y/o cualesquiera claves, los datos y claves analizados pueden post-procesarse por uno o más post-procesadores 108. El post-procesador 108 puede realizar cualesquiera una o más operaciones en las comparticiones de datos recibidas individuales, tales como encriptar una o más comparticiones de datos, añadir información de integridad (por ejemplo, una función de troceo) a una o más comparticiones, y añadir información de autenticación a una o más comparticiones. El post-procesador 108 puede también realizar cualesquiera una o más operaciones en las claves o comparticiones de clave recibidas, tales como encriptar una o más claves o comparticiones de clave, añadir información de integridad (por ejemplo, una función de troceo) a una o más claves o comparticiones de claves, y añadir información de autenticación a una o más claves o comparticiones de clave. El post-proceso puede dirigir también las comparticiones de datos, claves y/o comparticiones de clave para que se transmitan o almacenen. Estas y otras características y funciones que pueden realizarse por el post-procesador 108 se describen adicionalmente en el presente documento.

La combinación y orden de procesos usados por el analizador 100 de datos seguro pueden depender de la aplicación o uso particular, el nivel de seguridad deseado, ya se desee pre-encriptación opcional, post-encriptación, o ambas, la redundancia deseada, las capacidades o rendimiento de un sistema integrado o subyacente, o cualquier otro factor adecuado o combinación de factores.

En una implementación, el analizador 106 de datos analiza los datos para generar cuatro o más comparticiones de datos o claves, y el post-procesador 108 encripta todas las comparticiones, a continuación almacena estas comparticiones encriptadas en diferentes localizaciones en la base de datos desde las que se recibieron. Como alternativa o adicionalmente, el post-procesador 108 puede re-localizar las comparticiones encriptadas a cualquiera

de uno o más dispositivos de almacenamiento adecuados, que pueden ser fijos o extraíbles, dependiendo de la necesidad del solicitante de privacidad y seguridad. En particular, las comparticiones encriptadas pueden almacenarse virtualmente en cualquier lugar, incluyendo, pero sin limitación, un único servidor o dispositivo de almacenamiento de datos, o entre instalaciones de almacenamiento de datos o dispositivos separados. La gestión de cualesquiera claves usadas por el analizador 100 de datos seguro puede manejarse por el analizador 100 de datos seguro, o puede integrarse en una infraestructura existente o cualquier otra localización deseada. La recuperación, recombinación, reensamblaje o reconstitución de las comparticiones de datos encriptados puede utilizar también cualquier número de técnicas de autenticación, incluyendo, pero sin limitación, biométricas, tales como reconocimiento de huellas digitales, exploración facial, exploración de mano, exploración de iris, exploración retinal, exploración de oreja, reconocimiento de patrón bascular o análisis de ADN.

Las tecnologías de encriptación tradicionales se basan en una o más claves usadas para encriptar los datos y presentarlos inutilizables sin la una o más claves. Sin embargo, los datos permanecen en su totalidad e intactos y sometidos a ataque. En algunas realizaciones, el analizador de datos seguro trata este problema analizando el fichero encriptado en dos o más comparticiones, añadiendo otra capa de encriptación a cada compartición de los datos, y a continuación almacenando las comparticiones en diferentes localizaciones físicas y/o lógicas. Cuando una o más comparticiones de datos se eliminan físicamente del sistema, usando un dispositivo extraíble, tal como un dispositivo de almacenamiento de datos, o colocando la compartición bajo el control de otra parte, cualquier posibilidad de compromiso de datos asegurados se elimina de manera eficaz. En algunas realizaciones, el fichero encriptado se analiza en cuatro o más porciones o comparticiones.

Un ejemplo de un analizador de datos seguro se muestra en la Figura 2, que muestra las siguientes etapas de un proceso realizado por el analizador de datos seguro en los datos a analizarse, dando como resultado almacenar una clave maestra de sesión con los datos analizados:

1. Generar una clave maestra de sesión y encriptar los datos usando, por ejemplo, el cifrado de flujo de RS1 o RC4.
2. Analizar los datos encriptados resultantes en cuatro comparticiones de datos de acuerdo con el patrón de la clave maestra de sesión.
3. Analizar la clave maestra de sesión de acuerdo con el patrón de una clave maestra del analizador y anexar las comparticiones de clave resultantes a las comparticiones de datos. Las cuatro comparticiones de datos resultantes contendrán porciones de los datos originales encriptados y porciones de la clave maestra de sesión. En otras realizaciones, la clave maestra de sesión no se almacena con las comparticiones de datos (véase, por ejemplo, la Figura 3 y análisis adjuntos).
4. Generar una clave de cifrado de flujo para cada una de las cuatro comparticiones.
5. Encriptar cada compartición con su respectiva clave de cifrado de flujo, a continuación almacenar las claves de encriptación en diferentes localizaciones desde las comparticiones encriptadas. Como se muestra en la Figura 2, la compartición 1 se almacena con la clave 4, la compartición 2 se almacena con la clave 1, la compartición 3 se almacena con la clave 2, y la compartición 4 se almacena con la clave 3. Sin embargo, puede usarse cualquier otro emparejamiento de claves con comparticiones, incluyendo, por ejemplo, disposiciones en las que se almacena más de una clave con una compartición particular, o en las que la misma clave se analiza y almacena a través de múltiples comparticiones.

Para restaurar el formato de los datos originales, las etapas anteriores se invierten. Por ejemplo, para restaurar los datos originales en el ejemplo de la Figura 2, se recupera un número suficiente de las comparticiones. En implementaciones donde la operación de análisis incluye redundancia, los datos originales pueden restaurarse desde un número mínimo del número total de comparticiones, que es menor que el número total de comparticiones. Por lo tanto, los datos originales pueden restaurarse desde cualquier número adecuado de comparticiones que, en este ejemplo, puede variar de uno o a cuatro, dependiendo de la operación de análisis usada. Las claves de cifrado para cada una de las comparticiones recuperadas se reciben también. Cada compartición puede desencriptarse con la clave de cifrado de flujo que se usó para encriptar la respectiva compartición. La clave maestra de sesión puede recuperarse, o las comparticiones de clave de la clave maestra de sesión analizada se recuperan también desde las comparticiones. Como con las comparticiones de datos, la clave maestra de sesión puede restaurarse desde un número mínimo (que puede ser menor que o igual a todas) las comparticiones de clave totales, dependiendo de la operación de análisis usada. La sesión maestra se restaura desde las comparticiones de clave invirtiendo la operación de análisis de clave. Las comparticiones de datos recuperadas desde las comparticiones pueden restaurarse también invirtiendo la operación de análisis de datos, que puede implicar el uso de la clave maestra de sesión recuperada o restaurada. Si los datos restaurados invirtiendo la operación de análisis se hubieran encriptado antes del análisis, los datos originales pueden revelarse desencriptando los datos restaurados. Puede realizarse procesamiento adicional en los datos según sea necesario.

En el ejemplo anterior, el analizador de datos seguro puede implementarse con la gestión de clave de sesión externa o almacenamiento interno seguro de claves de sesión. Tras la implementación, se genera la clave maestra de analizador para asegurar la aplicación y para fines de encriptación. La incorporación de la clave maestra de analizador en las comparticiones resultantes permite una flexibilidad de compartición de datos asegurados por individuos en un grupo de trabajo, empresa o público aumentado.

La Figura 3 representa otro ejemplo del analizador de datos seguro, que incluye otro proceso que puede realizarse por el analizador de datos seguro, dando como resultado almacenar los datos de clave maestra de sesión en una o más tablas de gestión de clave separadas. Las etapas de generar una clave maestra de sesión, encriptar los datos a analizarse con la clave maestra de sesión, y analizar los datos encriptados resultantes en cuatro comparticiones o porciones de datos analizados de acuerdo con el patrón de la clave maestra de sesión son similares a las etapas correspondientes anteriormente descritas en relación a la Figura 2.

En este ejemplo, la clave maestra de sesión se analizará en una tabla de gestión de clave separada en un depositario de datos. Se genera un ID de transacción único para esta transacción. El ID de transacción y la clave maestra de sesión se almacenan en la tabla de gestión de clave separada. El ID de transacción se analiza de acuerdo con el patrón de la clave maestra de analizador, y las comparticiones del ID de transacción se anexan a los datos analizados encriptados. Las cuatro comparticiones resultantes contendrán porciones encriptadas de los datos originales y porciones del ID de transacción.

Como en la Figura 2, se genera una clave de cifrado de flujo para cada una de las cuatro comparticiones de datos, cada compartición se encripta con su respectiva clave de cifrado de flujo, y las claves de encriptación usadas para encriptar las comparticiones de datos se almacenan de manera separada de las comparticiones de datos (por ejemplo, en diferentes localizaciones desde las comparticiones de datos encriptados). Para restaurar los datos originales, se invierten las etapas.

La Figura 4 representa otro ejemplo del analizador de datos seguro, que incluye otro proceso que puede realizarse por un analizador de datos seguro en los datos a analizarse. Este ejemplo implica el uso de una clave intermediaria. El proceso incluye las siguientes etapas:

1. Acceder a una clave maestra del analizador con el usuario autenticado.
2. Generar una clave maestra de sesión única.
3. Derivar una clave intermediaria, por ejemplo, usando una función OR exclusiva (XOR) de la clave maestra de analizador y clave maestra de sesión.
4. Encriptar opcionalmente los datos usando un algoritmo de encriptación con clave con la clave intermediaria.
5. Analizar los datos encriptados opcionalmente en cuatro comparticiones de datos analizadas de acuerdo con el patrón de la clave intermediaria.
6. Generar un ID de transacción único y almacenar el ID de transacción y la clave maestra de sesión en una tabla de gestión de clave separada.
7. Analizar el ID de transacción de acuerdo con el patrón de la clave maestra de analizador.
8. Anexar comparticiones del ID de transacción a las comparticiones de datos analizadas. Las comparticiones combinadas resultantes contendrán opcionalmente porciones encriptadas de los datos originales y porciones de la clave maestra de sesión.
9. Generar opcionalmente una clave de encriptación para cada una de las cuatro comparticiones de datos.
10. Encriptar opcionalmente cada compartición con un algoritmo de encriptación existente o nuevo, almacenar a continuación las claves de encriptación en diferentes localizaciones desde las comparticiones combinadas. Como se muestra en la Figura 4, la compartición 1 se almacena con la clave 4, la compartición 2 se almacena con la clave 1, la compartición 3 se almacena con la clave 2, y la compartición 4 se almacena con la clave 3.

Para restaurar el formato de datos original, se invierten las etapas.

En algunas realizaciones, las etapas 6-8 anteriores, anteriores, pueden sustituirse por las siguientes etapas:

6. Almacenar la clave maestra de sesión junto con las comparticiones de datos aseguradas en un depositario de datos.
7. Analizar la clave maestra de sesión de acuerdo con el patrón de la clave maestra de analizador.
8. Anexar los datos de clave a las comparticiones opcionalmente encriptadas.

Ciertas etapas de los métodos descritos en el presente documento (por ejemplo, las etapas descritas para cualquiera de los métodos representados en las Figuras 2-4) pueden realizarse en orden diferente, o repetirse múltiples veces, según se desee. También es fácilmente evidente para los expertos en la materia que las porciones de los datos pueden manejarse de manera diferente unas de las otras. Por ejemplo, múltiples etapas de análisis pueden realizarse en únicamente una porción de los datos analizados. Cada porción de datos analizados puede asegurarse de manera única de cualquier manera deseable con la condición de que únicamente los datos puedan reensamblarse, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original u otra usable. Se entiende que uno o más de estos métodos puede combinarse en la misma implementación sin alejarse del alcance de la divulgación.

Los datos asegurados de acuerdo con los métodos descritos en el presente documento pueden recuperarse, restaurarse, reconstituirse, reensamblarse, desencriptarse o retornarse de otra manera fácilmente a su forma original u otra adecuada para su uso. Para restaurar los datos originales, pueden utilizarse los siguientes elementos:

1. Algunas o todas las compartición es o porciones del conjunto de datos.
2. El conocimiento de y capacidad para reproducir el flujo de proceso del método usado para asegurar los datos.
3. El acceso a la clave maestra de sesión.
4. El acceso a la clave maestra de analizador.

En algunas realizaciones, no todos estos elementos pueden requerirse para recuperar y restaurar, reconstituir, re-ensamblar, desencriptar o retornar de otra manera en la forma original u otra adecuada para su uso, cada unidad de datos asegurados de acuerdo con uno o más de los métodos anteriormente descritos. En algunas realizaciones, pueden requerirse elementos adicionales no expresamente enumerados anteriormente para restaurar una unidad particular de datos. Por ejemplo, en algunas implementaciones, los métodos anteriormente descritos usan tres tipos de claves para encriptación. Cada tipo de clave puede tener opciones de almacenamiento, recuperación, seguridad y recuperación de clave individuales, basándose en la instalación. Las claves que pueden usarse incluyen, pero sin limitación:

1. La clave maestra de analizador puede ser una clave individual asociada con la instalación del analizador de datos seguro. Está instalada en el servidor en el que se ha desplegado el analizador de datos seguro. Hay una diversidad de opciones adecuadas para almacenar esta clave incluyendo, pero sin limitación, una tarjeta inteligente, almacén de clave de hardware separado, almacenes de clave convencionales, almacenes de clave personalizados o en una tabla de base de datos asegurada, por ejemplo.
2. La clave maestra de sesión puede generarse cada vez que se analizan datos. La clave maestra de sesión se usa para encriptar los datos antes de las operaciones de análisis. Puede usarse también (si la clave maestra de sesión no está integrada en los datos analizados) para analizar los datos encriptados. La clave maestra de sesión puede almacenarse de una diversidad de maneras, incluyendo, pero sin limitación, un almacén de clave convencional, almacén de clave personalizado, tabla de base de datos separada, o asegurarse en las compartición es encriptadas, por ejemplo.
3. Las claves de encriptación de compartición: para cada compartición o porciones de un conjunto de datos que se crean, puede generarse una clave de encriptación de compartición individual para encriptar adicionalmente las compartición es. Las claves de encriptación de compartición pueden almacenarse en diferentes compartición es a las que se encriptó la compartición.

Como se muestra en la Figura 4, puede utilizarse también una clave intermediaria. La clave intermediaria puede generarse cada vez que se analizan datos. La clave intermediaria se usa para encriptar los datos antes de las operaciones de análisis. Puede incorporarse también como un medio de análisis de los datos encriptados.

La Figura 5 muestra una implementación alternativa del analizador de datos seguro como el analizador 500 de datos seguro. El analizador 500 de datos seguro puede incluir capacidades integradas para analizar datos en compartición es usando el módulo 502. El analizador 500 de datos seguro puede incluir también capacidades integradas en el módulo 504 para realizar redundancia para que pueda implementar, por ejemplo, el análisis de M de N anteriormente descrito. El analizador 500 de datos seguro puede incluir también capacidades de distribución de compartición usando el módulo 506 para colocar las compartición es en memorias intermedias desde las que se envían para comunicación a una localización remota, para almacenamiento, etc. Se entenderá que cualesquiera otras capacidades adecuadas pueden integrarse en el analizador 500 de datos seguro.

La memoria 508 intermedia de datos ensamblada puede ser cualquier memoria adecuada usada para almacenar los datos originales (aunque no necesariamente en su forma original) que se analizará por analizador 500 de datos seguro. En una operación de análisis, la memoria 508 intermedia de datos ensamblada proporciona entrada al analizador 500 de datos seguro. En una operación de restauración, la memoria 508 intermedia de datos ensamblada puede usarse para almacenar la salida de analizador 500 de datos seguro.

Las memorias 510 intermedias de compartición pueden ser uno o más módulos de memoria que pueden usarse para almacenar las múltiples compartición es de datos que resultaron del análisis de datos original. En una operación de análisis, las memorias 510 intermedias de compartición mantienen la salida del analizador de datos seguro. En una operación de restauración, las memorias intermedias de compartición mantienen la entrada al analizador 500 de datos seguro.

Se entenderá que cualquier otra disposición adecuada de capacidades puede integrarse para el analizador 500 de datos seguro. Cualesquiera características adicionales pueden estar integradas y cualquiera de las características ilustradas pueden eliminarse, hacerse más robustas, hacerse menos robustas, o pueden modificarse de otra manera de cualquier manera adecuada. Las memorias intermedias 508 y 510 son análogamente meramente ilustrativas y pueden modificarse, eliminarse o añadirse de cualquier manera adecuada.

Cualesquiera módulos adecuados implementados en software, hardware o ambos, pueden ser llamados por o pueden llamar al analizador 500 de datos seguro. Como se ilustra, algunos módulos externos incluyen el generador 512 de números aleatorio, generador 514 de clave de realimentación de cifrado, algoritmo 516 de función de troceo, uno cualquiera o más tipos de encriptación 518, y gestión 520 de clave. Se entenderá que estos son meramente módulos externos ilustrativos. Cualesquiera otros módulos adecuados pueden usarse además de o en lugar de aquellos ilustrados. Si se desea, uno o más módulos externos pueden sustituir las capacidades que se crean en el analizador 500 de datos seguro.

El generador 514 de clave de realimentación de cifrado puede generar, para cada operación del analizador de datos seguro, una clave única o número aleatorio (usando, por ejemplo, el generador 512 de número aleatorio), para usarse como un valor de semilla para una operación que amplía un tamaño de clave de sesión original (por ejemplo, un valor de 128, 256, 512 o 1024 bits) en un valor igual a la longitud de los datos a analizarse. Cualquier algoritmo adecuado puede usarse para la generación de clave de realimentación de cifrado, tal como el algoritmo de generación de clave de realimentación de cifrado de AES.

Para facilitar la integración del analizador 500 de datos seguro y sus módulos externos (es decir, la capa 526 de analizador de datos seguro) en una capa 524 de aplicación (por ejemplo, una aplicación de correo electrónico o aplicación de base de datos), puede usarse una capa de envoltura que puede usar, por ejemplo, llamadas de función de API. Puede usarse cualquier otra disposición adecuada para integrar la capa 526 de analizador de datos seguro en la capa 524 de aplicación.

La Figura 5 también muestra cómo el analizador 500 de datos seguro y los módulos externos pueden usarse cuando se emite un comando de escritura (por ejemplo, a un dispositivo de almacenamiento), de inserción (por ejemplo, en un campo de base de datos), o de transmisión (por ejemplo, a través de una red) en la capa 524 de aplicación. En la etapa 550 se identifican los datos a analizarse y se hace una llamada al analizador de datos seguro. La llamada se pasa a través de la capa 522 de envoltura donde en la etapa 552, la capa 522 de envoltura envía por flujo continuo los datos de entrada identificados en la etapa 550 en la memoria 508 intermedia de datos ensamblada. También en la etapa 552, cualquier información de compartición adecuada, nombres de ficheros, cualquier otra información adecuada, o cualquier combinación de las mismas puede almacenarse (por ejemplo, como información 556 en la capa 522 de envoltura). El procesador 500 de datos seguro a continuación analiza los datos que toma como entrada desde la memoria 508 intermedia de datos ensamblada. Emite las comparticiones de datos en las memorias 510 intermedias de compartición. En la etapa 554, la capa 522 de envoltura obtiene a partir de información 556 almacenada cualquier información de compartición adecuada (es decir, almacenada por el dispositivo 522 de envoltura en la etapa 552) y la localización o localizaciones de compartición (por ejemplo, desde uno o más ficheros de configuración). La capa 522 de envoltura a continuación escribe las comparticiones de salida (obtenidas desde las memorias 510 intermedias de compartición) de manera apropiada (por ejemplo, escritas en uno o más dispositivos de almacenamiento, comunicados en una red, etc.).

La Figura 6 muestra cómo el analizador 500 de datos seguro y los módulos externos pueden usarse cuando tiene lugar una lectura (por ejemplo, desde un dispositivo de almacenamiento), selección (por ejemplo, desde un campo de base de datos), o recepción (por ejemplo, desde una red). En la etapa 600, los datos a restaurarse se identifican y se hace una llamada al analizador 500 de datos seguro desde la capa 524 de aplicación. En la etapa 602, desde la capa 522 de envoltura, se obtiene cualquier información de compartición adecuada y se determina la localización de la compartición. La capa 522 de envoltura carga las porciones de datos identificados en la etapa 600 en las memorias 510 intermedias de compartición. El analizador 500 de datos seguro a continuación procesa estas comparticiones como se describe en el presente documento (por ejemplo, si únicamente están disponibles tres o cuatro comparticiones, entonces pueden usarse las capacidades de redundancia del analizador 500 de datos seguro para restaurar los datos originales usando únicamente las tres comparticiones). Los datos restaurados se almacenan a continuación en la memoria 508 intermedia de datos ensamblada. En la etapa 504, la capa 522 de aplicación convierte los datos almacenados en memoria 508 intermedia de datos ensamblada en su formato de datos original (si fuera necesario) y proporciona los datos originales en su formato original a la capa 524 de aplicación.

La Figura 7 representa opciones 700 de ejemplo para usar los componentes del analizador de datos seguro. Se señalan varias combinaciones de opciones ejemplares a continuación con referencia a la Figura 7. Como se describe en relación a las Figuras 5 y 6, el analizador de datos seguro puede ser modular en su naturaleza, permitiendo que se use cualquier algoritmo conocido en cada uno de los bloques de función mostrados en la Figura 7. Las etiquetas mostradas en el ejemplo de la Figura 7 representan meramente una posible combinación de algoritmos. Puede usarse cualquier algoritmo adecuado o combinación de algoritmos en lugar de los algoritmos etiquetados. Por ejemplo, pueden usarse otros algoritmos de análisis de clave (por ejemplo, compartición secreta) tal como Blakely en lugar de Shamir, o sustituirse la encriptación de AES por otros algoritmos de encriptación conocidos tales como Triple DES.

1) 710, 716, 717, 718, 719, 720, 721, 722

Si se reciben datos previamente encriptados en la etapa 710, los datos pueden analizarse en un número predefinido de comparticiones. Si el algoritmo de análisis requiere una clave, puede generarse una clave de sesión en la etapa

716 usando un pseudo-generador de número aleatorio criptográficamente seguro. La clave de sesión puede transformarse opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de sesión de transformación en la etapa 717 antes de analizarse en el número predefinido de compartimentos con tolerancia a fallos en la etapa 718. Los datos pueden a continuación analizarse en el número predefinido de compartimentos en la etapa 719. Puede usarse un esquema tolerante a fallos en la etapa 720 para permitir la regeneración de los datos de menos del número total de compartimentos. Una vez que se crean las compartimentos, la información de autenticación/integridad puede embeberse en las compartimentos en la etapa 721. Cada compartición puede opcionalmente post-encriptarse en la etapa 722.

2) 711, 716, 717, 718, 719, 720, 721, 722

En algunas realizaciones, los datos de entrada pueden encriptarse en primer lugar usando una clave de pre-encriptación proporcionada por un usuario o un sistema externo antes de que se analicen los datos. Se proporciona una clave de pre-encriptación externa en la etapa 711. Por ejemplo, la clave puede proporcionarse desde un almacén de clave externa. Si el algoritmo de análisis requiere una clave, la clave de sesión puede generarse usando un pseudo-generador de número aleatorio criptográficamente seguro en la etapa 716. La clave de sesión puede transformarse opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de sesión de transformación en la etapa 717 antes de analizarse en el número predefinido de compartimentos con tolerancia a fallos en la etapa 718. Los datos a continuación se analizan a un número predefinido de compartimentos en la etapa 719. Puede usarse un esquema tolerante a fallos en la etapa 720 para permitir la regeneración de los datos de menos del número total de compartimentos. Una vez que se crean las compartimentos, la información de autenticación/integridad puede embeberse en las compartimentos en la etapa 721. Cada compartición puede opcionalmente post-encriptarse en la etapa 722.

3) 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722

En algunas realizaciones, se requiere encriptación pero no se usa una clave externa para la pre-encriptación. En tales realizaciones, puede generarse una clave de encriptación usando un pseudo-generador de número aleatorio criptográficamente seguro en la etapa 712 para transformar los datos. La encriptación de los datos usando la clave de encriptación generada puede tener lugar en la etapa 713. La clave de encriptación puede transformarse opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de encriptación de transformación en la etapa 714. La clave de encriptación de transformación y/o la clave de encriptación generada pueden a continuación analizarse en el número predefinido de compartimentos con tolerancia a fallos en la etapa 715. Si el algoritmo de análisis requiere una clave, puede tener lugar la generación de la clave de sesión usando un pseudo-generador de número aleatorio criptográficamente seguro en la etapa 716. La clave de sesión puede transformarse opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de sesión de sesión de transformación en la etapa 717 antes de analizarse en el número predefinido de compartimentos con tolerancia a fallos en la etapa 718. Los datos pueden a continuación analizarse en un número predefinido de compartimentos en la etapa 719. Un esquema tolerante a fallos puede usarse en la etapa 720 para permitir la regeneración de los datos de menos del número total de compartimentos. Una vez que se crean las compartimentos, la información de autenticación/integridad se embeberá en las compartimentos en la etapa 721. Cada compartición puede a continuación opcionalmente post-encriptarse en la etapa 722.

El analizador de datos seguro puede ofrecer protección de datos flexible para facilitar la separación física. Los datos pueden encriptarse en primer lugar, a continuación analizarse en compartimentos con tolerancia a fallos “m de n”. Esto permite la regeneración de la información inicial cuando hay disponible menos del número total de compartimentos. Por ejemplo, algunas compartimentos pueden perderse o corromperse en la transmisión. Las compartimentos perdidas o corruptas pueden recrearse a partir de tolerancia a fallos o información de integridad anexada a las compartimentos, como se analiza en más detalle a continuación.

Para crear las compartimentos, se utiliza opcionalmente un número de claves utilizado por el analizador de datos seguro anteriormente descrito. Estas claves pueden incluir uno o más de lo siguiente:

Clave de pre-encriptación: cuando se selecciona la pre-encriptación de las compartimentos, una clave de encriptación externa puede analizarse en el analizador de datos seguro. Esta clave puede generarse y almacenarse externamente en un almacén de claves (u otra localización) y puede usarse para encriptar opcionalmente datos antes de analizar los datos.

Clave de encriptación interna: esta clave puede generarse internamente y usarse por el analizador de datos seguro para encriptar los datos antes del análisis. Esta clave puede a continuación almacenarse de manera segura en las compartimentos usando un algoritmo de análisis de clave.

Clave de sesión: esta clave no se usa con un algoritmo de encriptación; en su lugar, puede usarse para codificar los algoritmos de particionamiento de datos cuando se selecciona análisis aleatorio. Cuando se usa un análisis aleatorio, puede generarse una clave de sesión internamente y usarse por el analizador de datos seguro para

particionar los datos en comparticiones. Esta clave puede almacenarse de manera segura en las comparticiones usando un algoritmo de análisis de clave.

Clave de post encriptación: cuando se selecciona la post encriptación de las comparticiones, puede pasarse una clave externa al analizador de datos seguro y usarse para post encriptar las comparticiones individuales. Esta clave puede generarse y almacenarse externamente en un almacén de claves u otra localización adecuada.

En algunas realizaciones, cuando se aseguran datos usando el analizador de datos seguro de esta manera, la información puede únicamente reensamblarse con la condición de que todas las comparticiones requeridas y claves de encriptación externas estén presentes.

Además de la protección individual de elementos de información, en ocasiones hay un requisito de compartición de información entre diferentes grupos de usuarios o comunidades de interés. Puede ser necesario a continuación controlar el acceso a las comparticiones individuales en ese grupo de usuarios o compartir las credenciales entre aquellos usuarios que permitiera únicamente a miembros del grupo re-ensamblar las comparticiones. Para este fin, puede implementarse una clave de grupo de trabajo a miembros de grupo. La clave de grupo de trabajo debería protegerse y mantenerse confidencial, como el compromiso de la clave de grupo de trabajo puede permitir potencialmente a aquellos fuera del grupo acceder a información. El concepto de clave de grupo de trabajo permite protección mejorada de elementos de información encriptando información de clave almacenada en las comparticiones. Una vez que se realiza esta operación, incluso si se descubrieran todas las comparticiones y otras claves externas requeridas, un atacante no tiene posibilidad de recrear la información sin acceder a la clave de grupo de trabajo.

La Figura 8 muestra el diagrama 800 de bloques ilustrativo para almacenar claves y componentes de datos en las comparticiones. En el ejemplo del diagrama 800, las etapas de pre-encriptación y post-encriptación opcionales se omiten, aunque estas etapas pueden incluirse en otras realizaciones.

El proceso simplificado para analizar los datos incluye en primer lugar encriptar los datos usando una clave de encriptación en la etapa 802 de encriptación. La clave de encriptación puede a continuación opcionalmente encriptarse con una clave de grupo de trabajo en la etapa 804. La clave de encriptación, opcionalmente encriptada por la clave de grupo de trabajo, puede a continuación analizarse en comparticiones y almacenarse en comparticiones 812 de datos. La clave 808 de sesión puede analizarse también y almacenarse en las comparticiones 812. Usando la clave de sesión, los datos 810 encriptados se analizan y almacenan en comparticiones 812.

Para restaurar los datos, las porciones de clave de sesión pueden recuperarse de las comparticiones 812 y restaurarse. La operación de análisis de los datos puede a continuación invertirse para restaurar los datos encriptados. Las comparticiones de la clave de encriptación (que se encriptaron con la clave de grupo de trabajo) pueden recuperarse y la clave de encriptación encriptada restaurarse. La clave de encriptación encriptada puede a continuación desencriptarse usando la clave de grupo de trabajo. Finalmente, los datos encriptados pueden a continuación desencriptarse usando la clave de encriptación para revelar los datos originales.

Hay varios métodos seguros para desplegar y proteger claves de grupo de trabajo. La selección de qué método usar para una aplicación particular depende de un número de factores. Estos factores pueden incluir nivel de seguridad requerido, coste, conveniencia y el número de usuarios en el grupo de trabajo. Técnicas ejemplares incluyen almacenamiento de clave basado en hardware y almacenamiento de clave basado en software.

Las soluciones basadas en hardware en general proporcionan las garantías más fuertes para la seguridad de claves de encriptación/desencriptación en un sistema de encriptación. Ejemplos de soluciones de almacenamiento basadas en hardware incluyen dispositivos de testigo de clave resistentes a manipulación que almacenan claves en un dispositivo portátil (por ejemplo, tarjeta inteligente/mochila), o periféricos de almacenamiento de clave no portátiles. Estos dispositivos están diseñados para evitar la fácil duplicación de material de clave por partes no autorizadas. Pueden generarse claves por una autoridad confiable y distribuirse a usuarios, o generarse en el hardware. Adicionalmente, los sistemas de almacenamiento de claves pueden proporcionar autenticación de múltiples factores, donde el uso de las claves requiere acceso tanto a un objeto físico (testigo) como una frase de paso o biométrica. Mientras que el almacenamiento basado en hardware especializado puede ser deseable para implementaciones o aplicaciones de alta seguridad, otros despliegues pueden elegir almacenar claves directamente en hardware local (por ejemplo, almacenes de discos, RAM o RAM no volátil tal como unidades USB). Esto proporciona un nivel inferior de protección contra atacantes internos, o en casos donde un atacante pueda acceder directamente a la máquina de encriptación.

Para asegurar las claves en un disco, la gestión de clave basada en software a menudo protege las claves almacenándolas en forma encriptada bajo una clave derivada de una combinación de otras métricas de autenticación, incluyendo: contraseñas y frases de paso, presencia de otras claves (por ejemplo, desde una solución basada en hardware), biométricas o cualquier combinación adecuada. El nivel de seguridad proporcionado por tales técnicas puede variar de los mecanismos de protección de clave relativamente débiles proporcionados por algunos

sistemas operativos (por ejemplo, MS Windows y Linux) a soluciones más robustas implementadas usando autenticación de múltiples factores.

El analizador de datos seguro descrito en el presente documento puede usarse ventajosamente en un número de aplicaciones y tecnologías. Por ejemplo, el sistema de correo electrónico, sistemas RAID, sistemas de difusión de vídeo, sistemas de base de datos, sistemas de copia de respaldo de cinta o cualquier otro sistema adecuado que pueda tener el analizador de datos seguro integrado a cualquier nivel adecuado. Como se ha analizado anteriormente, se entenderá que el analizador de datos seguro puede estar también integrado para protección y tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, medios de transporte alámbricos, inalámbricos o físicos. Como un ejemplo, las aplicaciones de voz sobre el protocolo de internet (VoIP) pueden hacer uso del analizador de datos seguro para resolver los problemas relacionados con ecos y retardos que se encuentran comúnmente en VoIP. La necesidad de reintento de red en paquetes descartados puede eliminarse usando tolerancia frente a fallos, que garantiza la entrega de paquetes incluso con la pérdida de un número predeterminado de comparticiones. Los paquetes de datos (por ejemplo, paquetes de red) pueden también analizarse eficazmente y restaurarse “al vuelo” con retardo y almacenamiento en memoria intermedia mínimos, dando como resultado una solución completa para diversos tipos de datos en movimiento. El analizador de datos seguro puede actuar en paquetes de datos de red, paquetes de voz de red, sistema de ficheros bloques de datos, o cualquier otra unidad de información adecuada. Además de estar integrado con una aplicación de VoIP, el analizador de datos seguro puede estar integrado con una aplicación de compartición de ficheros (por ejemplo, una aplicación de compartición de ficheros entre iguales), una aplicación de difusión de vídeo, una aplicación de voto o encuestas electrónica (que puede implementar un protocolo de voto electrónico y firmas ciegas, tal como el protocolo Sensus), una aplicación de correo electrónico, o cualquier otra aplicación de red que pueda requerir o desear comunicación segura.

En algunas realizaciones, el soporte de datos de red en movimiento puede proporcionarse por el analizador de datos seguro en dos fases distintas -- una fase de generación de encabezamiento y una fase de análisis de datos. El proceso 900 de generación de encabezamiento simplificado y el proceso 910 de análisis de datos simplificado se muestran en las Figuras 9A y 9B, respectivamente. Uno o ambos de estos procesos pueden realizarse en paquetes de red, bloques de sistema de ficheros, o cualquier otra información adecuada.

En algunas realizaciones, el proceso 900 de generación de encabezamiento puede realizarse una vez en la iniciación de un flujo de paquete de red. En la etapa 902, puede generarse una clave de encriptación, K, aleatoria (o pseudoaleatoria). La clave de encriptación, K, puede a continuación encriptarse opcionalmente (por ejemplo, usando la clave de grupo de trabajo anteriormente descrita) en la etapa 904 de envoltura de clave de AES. Aunque puede usarse una envoltura de clave de AES en algunas realizaciones, puede usarse cualquier encriptación de clave adecuada o algoritmo de envoltura de clave en otras realizaciones. La etapa 904 de envoltura de clave de AES puede operar en toda la clave de encriptación, K, o la clave de encriptación puede analizarse en varios bloques (por ejemplo, bloques de 64 bits). La etapa 904 de envoltura de clave de AES puede a continuación operar en bloques de la clave de encriptación, si se desea.

En la etapa 906, un algoritmo de compartición secreto (por ejemplo, Shamir) puede usarse para analizar la clave de encriptación, K, en comparticiones de clave. Cada compartición de clave puede a continuación embeberse en una de las comparticiones de salida (por ejemplo, en los encabezamientos de compartición). Finalmente, puede anexarse un bloque de integridad de compartición y (opcionalmente) una etiqueta de post-autenticación (por ejemplo, MAC) al bloque de encabezamiento de cada compartición. Cada bloque de encabezamiento puede diseñarse para ajustarse en un único paquete de datos.

Después de que la generación de encabezamiento está completa (por ejemplo, usando el proceso 900 de generación de encabezamiento simplificado), el analizador de datos seguro puede entrar en la fase de particionamiento de datos usando proceso 910 de análisis de datos simplificado. Cada paquete de datos o bloque de datos entrante en el flujo se encripta usando la clave de encriptación, K, en la etapa 912. En la etapa 914, la información de integridad de compartición (por ejemplo, una función de troceo H) puede calcularse en el texto cifrado resultante de la etapa 912. Por ejemplo, puede calcularse una función de troceo SHA-256. En la etapa 916, el paquete de datos o bloque de datos puede a continuación particionarse en dos o más comparticiones de datos usando uno de los algoritmos de análisis de datos anteriormente descritos. En algunas realizaciones, el paquete de datos o bloque de datos puede analizarse de modo que cada compartición de datos contenga una distribución sustancialmente aleatoria de los paquetes de datos o bloque de datos encriptados. La información de integridad (por ejemplo, función de troceo H) puede a continuación anexarse a cada compartición de datos. Puede calcularse también una etiqueta de post-autenticación opcional (por ejemplo, MAC) y anexarse a cada compartición de datos en algunas realizaciones.

Cada compartición de datos puede incluir metadatos, que pueden ser necesarios para permitir la reconstrucción correcta de los bloques de datos o paquetes de datos. Esta información puede incluirse en el encabezamiento de compartición. Los metadatos pueden incluir tal información tal como comparticiones de clave criptográfica, identidades de clave, números aleatorios utilizados solo una vez de compartición, valores de firmas/MAC, y bloques

de integridad. Para maximizar la eficacia de ancho de banda, los metadatos pueden almacenarse en un formato binario compacto.

Por ejemplo, en algunas realizaciones, el encabezamiento de compartición incluye un fragmento de encabezamiento de texto sin formato, que no está encriptado y puede incluir tales elementos como la compartición de clave Shamir, número aleatorio utilizado solo una vez por sesión, número aleatorio utilizado solo una vez por compartición, identificadores de clave (por ejemplo, un identificador de clave de grupo de trabajo y un identificador de clave de post-autenticación). El encabezamiento de compartición puede incluir también un fragmento de encabezamiento encriptado, que se encripta con la clave de encriptación. Un fragmento de encabezamiento de integridad, que puede incluir comprobaciones de integridad para cualquier número de los bloques anteriores (por ejemplo, los dos bloques anteriores), puede incluirse también en el encabezamiento. Cualesquiera otros valores adecuados o información pueden incluirse también en el encabezamiento de compartición.

Como se muestra en el formato 1000 de compartición ilustrativo de la Figura 10, el bloque 1002 de encabezamiento puede estar asociado con dos o más bloques 1004 de salida. Cada bloque de encabezamiento, tal como el bloque 1002 de encabezamiento, puede estar diseñado para adaptarse en un único paquete de datos de red. En algunas realizaciones, después de que se transmite el bloque 1002 de encabezamiento desde una primera localización a una segunda posición, los bloques de salida pueden transmitirse a continuación. Como alternativa, el bloque 1002 de encabezamiento y los bloques 1004 de salida pueden transmitirse al mismo tiempo en paralelo. La transmisión puede tener lugar a través de una o más rutas de comunicaciones similares o no similares.

Cada bloque de salida puede incluir la porción 1006 de datos y la porción 1008 de integridad/autenticidad. Como se ha descrito anteriormente, cada compartición de datos puede asegurarse usando una porción de integridad de compartición que incluye la información de integridad de compartición (por ejemplo, una función de troceo SHA-256) de los datos encriptados, pre-particionados. Para verificar la integridad de los bloques de salida en tiempo de recuperación, el analizador de datos seguro puede comparar los bloques de integridad de compartición de cada compartición y a continuación invertir el algoritmo de análisis. La función de troceo de los datos recuperados puede a continuación verificarse contra la función de troceo de compartición.

En algunas realizaciones, puede emplearse una rutina de compartición de secreto con clave usando dispersión de información con clave (por ejemplo, a través del uso de un algoritmo de dispersión de información con clave o “IDA”). La clave para el IDA con clave puede protegerse también por una o más claves de grupo de trabajo externas, una o más claves compartidas, o cualquier combinación de claves de grupo de trabajo y claves compartidas. De esta manera, puede emplearse un esquema de compartición de secreto de múltiples factores. Para reconstruir los datos, pueden requerirse al menos “M” comparticiones más la clave o claves de grupo de trabajo (y/o clave o claves compartidas) en algunas realizaciones. El IDA (o la clave para el IDA) puede controlarse también en el proceso de encriptación. Por ejemplo, la transformación puede controlarse en texto sin formato (por ejemplo, durante la capa de pre-procesamiento antes de la encriptación) y puede proteger adicionalmente el texto sin formato antes de que se encripte.

En algunas realizaciones, la clave de sesión puede encriptarse usando una clave compartida (por ejemplo, una clave de grupo de trabajo) antes de que se analice para generar unas comparticiones de clave de sesión. A continuación pueden formarse dos o más comparticiones de usuario combinado al menos una compartición de conjunto de datos encriptados y al menos una compartición de clave de sesión. Al formar una compartición de usuario, en algunas realizaciones, la al menos una compartición de clave de sesión puede intercalarse en una compartición de conjunto de datos encriptados. En otras realizaciones, la al menos una compartición de clave de sesión puede insertarse en una compartición de conjunto de datos encriptados en una localización basándose al menos en parte en la clave de grupo de trabajo compartida. Por ejemplo, la dispersión de información con clave puede usarse para distribuir cada compartición de clave de sesión en una única compartición de conjunto de datos encriptados para formar una compartición de usuario. Intercalar o insertar una compartición de clave de sesión en una compartición de conjunto de datos encriptados en una localización basándose al menos en parte en el grupo de trabajo compartido puede proporcionar seguridad aumentada frente a ataques criptográficos. En otras realizaciones, puede anexarse una o más comparticiones de clave de sesión al comienzo o al final de una compartición de conjunto de datos encriptados para formar una compartición de usuario. La colección de comparticiones de usuario puede a continuación almacenarse de manera separada en al menos un depositario de datos. El depositario o depositarios de datos pueden estar localizados en la misma localización física (por ejemplo, en el mismo dispositivo de almacenamiento magnético o de cinta) o geográficamente separados (por ejemplo, en servidores físicamente separados en diferentes localizaciones geográficas). Para reconstruir el conjunto de datos original, puede requerirse un conjunto de comparticiones de usuario autorizadas y la clave de grupo de trabajo compartida.

El analizador de datos seguro puede usarse para implementar una solución de seguridad de datos de informática en la nube. La informática en la nube es informática basada en la red, almacenamiento, o ambos, donde los recursos informáticos y de almacenamiento pueden proporcionarse a sistemas informáticos y otros dispositivos a través de una red. Los recursos de la informática en la nube se acceden en general a través de la Internet, aunque la informática en la nube puede realizarse a través de cualquier red pública o privada adecuada. La informática en la nube puede proporcionar un nivel de abstracción entre recursos informáticos y sus componentes de hardware

subyacentes (por ejemplo, servidores, dispositivos de almacenamiento, redes), que posibilitan el acceso remoto a un grupo de recursos informáticos. Estos recursos de la informática en la nube pueden denominarse de manera colectiva como la “nube”. La informática en la nube puede usarse para proporcionar dinámicamente recursos escalables y a menudo virtualizados como un servicio a través de la Internet o cualquier otra red adecuada o combinación de redes.

Una red 1100 que muestra varias disposiciones para usar un analizador de datos seguro para implementar una solución de seguridad de datos de informática en la nube se muestra en la Figura 11. La red 1100 incluye dos nubes, 1102 y 1112, para procesamiento y/o almacenamiento de datos y claves, un sistema 1120 de usuario que tiene un analizador 1122 de datos seguro local, un dispositivo 1130 de usuario que no tiene un analizador de datos seguro local y un receptor 1140 de datos.

Los sistemas 1120 y 1130 de usuario están acoplados a la nube 1102 que incluye un número de recursos en la nube para almacenar comparticiones de datos entre otras funciones. Los sistemas 1120 y 1130 de usuario pueden incluir cualquier hardware adecuado, tal como un terminal informático, ordenador personal, dispositivo portátil (por ejemplo, PDA, Blackberry, teléfono inteligente, dispositivo de tableta), teléfono celular, red informática, cualquier otro hardware adecuado o cualquier combinación de los mismos. El sistema 1120 de usuario puede estar configurado para ejecutar un analizador 1122 de datos seguro que puede ser similar a las diversas realizaciones de analizadores de datos seguros anteriormente descritos. El analizador 1122 de datos seguro puede estar integrado a cualquier nivel adecuado del sistema 1120 de usuario. Por ejemplo, el analizador 1122 de datos seguro puede estar integrado en el hardware y/o software del sistema 1120 de usuario a un nivel de extremo trasero suficiente de manera que la presencia del analizador 1122 de datos seguro puede ser sustancialmente transparente para un usuario final del sistema 1120 de usuario. Un receptor 1140 puede estar acoplado de manera similar a la nube 1102 para acceder a datos almacenados por otro usuario.

En algunas realizaciones un sistema de usuario, tal como el dispositivo 1130 de usuario, puede no estar configurado para ejecutar un analizador de datos seguro, tal como el analizador 1122 de datos, sino que en su lugar puede acceder a un analizador de datos externo que puede residir en una red, por ejemplo, en el servicio 1106 de seguridad de datos en la nube 1102. La nube 1102 puede incluir múltiples recursos en la nube ilustrativos, tales como el servicio 1106 de seguridad de datos, servidor 1107 de registro/autenticación, y almacenamiento 1108 de clave. El servicio 1106 de seguridad de datos puede usarse para realizar operaciones en datos recibidos tal como analizar, encriptar y almacenar datos, y puede interconectar con otros recursos en la nube. El servidor 1107 de registro/autenticación puede usarse para registrar y autenticar usuarios de un sistema de almacenamiento seguro. Se describen diversas funciones del servidor 1107 de reg/aut en mayor detalle a continuación. El almacén 1108 de claves puede comprender uno o más servidores u otros dispositivos de almacenamiento usados para almacenar claves tales como claves compartidas o claves de grupo de trabajo externas al sistema de usuario y en una localización física diferente de donde se almacenan los datos. Un dispositivo de usuario o sistema de usuario puede acceder a estas claves comunicando directamente con el almacén 1108 de claves o a través del servicio 1106 de seguridad de datos. La nube 1102 también tiene dispositivos 1104a a 1104n de almacenamiento en red. Los recursos en la nube pueden proporcionarse por una pluralidad de proveedores de recursos en la nube, por ejemplo, Amazon, Google o Dropbox. Estos recursos de informática en la nube son meramente ilustrativos, y cualquier número y tipo adecuado de recursos de informática en la nube puede ser accesible desde los sistemas 1120 y 1130 de usuarios.

El servidor 1107 de registro/autenticación puede incluir uno o más procesadores configurados para registrar usuarios de un sistema de almacenamiento seguro tal como el usuario del analizador 1122 de datos seguro, usuarios del servicio 1106 de seguridad de datos, y usuarios 1140 receptores (que pueden ser también usuarios del servicio 1106 de seguridad de datos). Los usuarios pueden incluir usuarios individuales, dispositivos de usuario, y grupos de usuarios o dispositivos. El servidor 1107 de reg/aut puede estar configurado adicionalmente para almacenar credenciales de usuario tales como direcciones de correo electrónico o nombres de usuarios, autenticar usuarios (por ejemplo, basándose en las credenciales almacenadas), buscar usuarios por su dirección de correo electrónico u otras credenciales, transmitir una clave pública a un cliente de compartición criptográfica, des-autorizar a uno o más usuarios que accedan al servidor 1107 de registro/autenticación. El servidor 1107 de registro/autenticación puede dirigir también a los usuarios o dispositivos de usuario a una o más de las localizaciones 1104 de almacenamiento para escribir datos o para recuperar datos. En particular, si los datos que un dispositivo de usuario solicita recuperar han sido analizados de acuerdo con una técnica de M de N (una en la que M comparticiones de N comparticiones son necesarias para re-ensamblar o restaurar un conjunto de datos a su forma original o usable, con M menor que N), el servidor 1107 de registro/autenticación puede identificar y devolver al usuario información de dispositivo acerca de M localizaciones de almacenamiento recomendadas de entre las localizaciones 1104a-1104n de almacenamiento. El dispositivo de usuario puede a continuación usar esta información para acceder de manera selectiva a localizaciones de almacenamiento para recuperar los datos deseados.

La nube 1102 y uno o más dispositivos de usuario o sistemas, tales como el sistema 1120 de usuario, pueden estar en comunicación con una segunda nube 1112. La nube 1112 incluye una pluralidad de dispositivos 1114a-1114n de almacenamiento y puede incluir cualesquiera otros recursos en la nube, tales como los recursos en la nube descritos en relación con la nube 1102. En algunas realizaciones, la nube 1102 puede ser una nube pública (tal como

Amazon, Google, o Dropbox), y la nube 1112 puede ser una nube privada o viceversa. En otras realizaciones, la nube 1102 y la nube 1112 pueden ser diferentes nubes públicas (por ejemplo, la nube 1102 puede proporcionarse por Amazon y la nube 1112 puede proporcionarse por Google). Almacenar comparticiones de datos y/o comparticiones de clave a través de diferentes nubes puede proporcionar seguridad de datos mejorada. Además de almacenar datos en la nube, una o más comparticiones de datos, comparticiones de clave, o claves pueden almacenarse en almacenamiento local, tal como memoria 1124 local del sistema 1120 de usuario o una memoria local del dispositivo 1130 de usuario, y una o más comparticiones de datos, comparticiones de clave o claves pueden almacenarse en almacenamiento extraíble (por ejemplo, una memoria USB), tal como puede ser, por ejemplo, el almacenamiento 1126 extraíble o el almacenamiento 1136 extraíble. Puede usarse cualquier número adecuado de nubes. Por ejemplo, en algunas realizaciones, la nube 1102 y la nube 1112 pueden formar una única nube, o únicamente puede usarse una de las nubes 1102 y 1112. En algunas realizaciones, pueden usarse tres o más nubes.

El almacenamiento 1126 o 1136 extraíble puede ser, por ejemplo, una unida flash USB compacta, un disco flexible, un disco óptico, o una tarjeta inteligente. En algunas realizaciones, el almacenamiento 1126 o 1136 extraíble puede usarse para autenticar la identidad de un usuario remoto que desea ver, encriptar o desencriptar datos que gestiona por el servicio 1106 de seguridad de datos. En algunas realizaciones, el almacenamiento 1126 o 1136 extraíble puede requerirse que inicie la encriptación, desencriptación o análisis de datos por el servicio 1106 de seguridad de datos. En tales realizaciones, el almacenamiento 1126 o 1136 extraíble puede considerarse un testigo físico. Un receptor 1140 autorizado puede también acceder al almacenamiento extraíble configurado para autenticar al usuario receptor de modo que el receptor 1140 puede recuperar y desencriptar datos que está autorizado a acceder.

Una ventaja de la informática en la nube es que un usuario (por ejemplo, un usuario del dispositivo 1130 de usuario o sistema 1120 de usuario) puede acceder a múltiples recursos de informática en la nube sin tener que invertir en hardware de almacenamiento especializado. El usuario puede tener la capacidad de controlar dinámicamente el número y tipo de recursos de informática en la nube accesibles para él. Por ejemplo, el dispositivo 1130 de usuario o el sistema 1120 de usuario pueden proporcionarse con recursos de almacenamiento bajo demanda en la nube que tienen capacidades que son ajustables dinámicamente basándose en las necesidades actuales. En algunas realizaciones, una o más aplicaciones de software, tales como el analizador 1122 de datos seguro ejecutadas en el sistema 1120 de usuario o un explorador web de Internet en el dispositivo 1130 de usuario, pueden acoplar a un usuario a los recursos en la nube 1102. El acoplamiento de recursos en la nube 1102 al dispositivo 1130 de usuario o sistema 1120 de usuario puede ser transparente para los usuarios de manera que los recursos en la nube 1102 aparecen a los usuarios como recursos de hardware locales y/o recursos de hardware especializados.

La Figura 12 es un diagrama de bloques de un dispositivo informático para realizar cualquiera de los procesos descritos en el presente documento. Cada uno de los componentes de estos sistemas puede implementarse en uno o más dispositivos 1200 informáticos. En ciertos aspectos, una pluralidad de los componentes de estos sistemas puede incluirse en un dispositivo 1200 informático. En ciertas implementaciones, un componente y un dispositivo de almacenamiento pueden implementarse a través de varios dispositivos 1200 informáticos.

El dispositivo 1200 informático comprende al menos una unidad de interfaz de comunicaciones, un controlador 1210 de entrada/salida, memoria de sistema, y uno o más dispositivos de almacenamiento de datos. La memoria de sistema incluye al menos una memoria de acceso aleatorio (RAM 1202) y al menos una memoria de solo lectura (ROM 1204). Todos estos elementos están en comunicación con una unidad de procesamiento central (CPU 1206) para facilitar la operación del dispositivo 1200 informático. El dispositivo 1200 informático puede estar configurado de muchas maneras diferentes. Por ejemplo, el dispositivo 1200 informático puede ser un ordenador independiente convencional o como alternativa, las funciones del dispositivo 1200 informático pueden distribuirse a través de múltiples sistemas informáticos y arquitecturas. En la Figura 12, el dispositivo 1200 informático está vinculado, mediante red o red local, a otros servidores o sistemas.

El dispositivo 1200 informático puede estar configurado en una arquitectura distribuida, en la que bases de datos y procesadores se alojan en unidades o localizaciones separadas. Algunas unidades realizan funciones de procesamiento primario y contienen como mínimo un controlador general o un procesador y una memoria de sistema. En implementaciones de arquitectura distribuida, cada una de estas unidades puede conectarse mediante la unidad 1208 de interfaz de comunicaciones a un concentrador o puerto de comunicaciones (no mostrado) que sirve como un enlace de comunicación primario con otros servidores, ordenadores de cliente o de usuario y otros dispositivos relacionados. El concentrador o puerto de comunicaciones puede tener por sí mismo mínima capacidad de procesamiento, sirviendo principalmente como un encaminador de comunicaciones. Una diversidad de protocolos de comunicaciones pueden ser parte del sistema, incluyendo, pero sin limitación: Ethernet, SAP, SAS™, ATP, BLUETOOTH™, GSM y TCP/IP.

La CPU 1206 comprende un procesador, tal como uno o más microprocesadores convencionales y uno o más co-procesadores complementarios tales como co-procesadores matemáticos para descargar la carga de trabajo de la CPU 1206. La CPU 1206 está en comunicación con la unidad 1208 de interfaz de comunicaciones y el controlador 1210 de entrada/salida, a través del cual la CPU 1206 comunica con otros dispositivos tales como otros servidores, terminales de usuario, o dispositivos. La unidad 1208 de interfaz de comunicaciones y el controlador 1210 de

entrada/salida pueden incluir múltiples canales de comunicación para comunicación simultánea con, por ejemplo, otros procesadores, servidores o terminales de cliente.

La CPU 1206 también está en comunicación con el dispositivo de almacenamiento de datos. El dispositivo de almacenamiento de datos puede comprender una combinación apropiada de memoria magnética, óptica o de semiconductores, y puede incluir, por ejemplo, RAM 1202, ROM 1204, unidad flash, un disco óptico tal como un disco compacto o un disco duro o unidad. La CPU 1206 y el dispositivo de almacenamiento de datos cada uno pueden estar localizados, por ejemplo, completamente en un único ordenador u otro dispositivo informático; o conectados entre sí mediante un medio de comunicación, tal como un puerto USB, cable de puerto serie, un cable coaxial, un cable de Ethernet, una línea de teléfono, un transceptor de frecuencia de radio u otro medio o combinación inalámbrica o alámbrica similar o combinación de los anteriores. Por ejemplo, la CPU 1206 puede estar conectada al dispositivo de almacenamiento de datos mediante la unidad 1208 de interfaz de comunicaciones. La CPU 1206 puede estar configurada para realizar una o más funciones de procesamiento particulares.

El dispositivo de almacenamiento de datos puede almacenar, por ejemplo, (i) un sistema operativo 1212 para el dispositivo 1200 informático; (ii) una o más aplicaciones 1214 (por ejemplo, código de programa informático o un producto de programa informático) adaptadas para dirigir la CPU 1206 de acuerdo con los sistemas y métodos descritos en este punto, y particularmente de acuerdo con los procesos descritos en detalle con respecto a la CPU 1206; o (iii) base o bases de datos 1216 adaptadas para almacenar información que puede utilizarse para almacenar información requerida por el programa.

El sistema operativo 1212 y las aplicaciones 1214 pueden almacenarse, por ejemplo, en un formato comprimido, uno no compilado y uno encriptado, y pueden incluir código de programa informático. Las instrucciones del programa pueden leerse en una memoria principal del procesador a partir de un medio legible por ordenador distinto del dispositivo de almacenamiento de datos, tal como desde la ROM 1204 o desde la RAM 1202. Aunque la ejecución de secuencias de instrucciones en el programa provoca que la CPU 1206 realice las etapas de proceso descritas en el presente documento, puede usarse circuitería de cableado permanente en lugar de, o en combinación con, instrucciones de software para implementación de los procesos de la presente divulgación. Por lo tanto, los sistemas y métodos descritos no están limitados a ninguna combinación específica de hardware y software.

Puede proporcionarse código de programa informático adecuado para realizar una o más funciones en relación con el encaminamiento de vehículos y planificación de movimiento como se describe en el presente documento. El programa puede incluir también elementos de programa tales como un sistema operativo 1212, un sistema de gestión de base de datos y “controladores de dispositivo” que permiten que el procesador interconecte con dispositivos periféricos informáticos (por ejemplo, una pantalla de vídeo, un teclado, un ordenador ratón, etc.) mediante el controlador 1210 de entrada/salida.

La expresión “medio legible por ordenador” como se usa en el presente documento hace referencia a cualquier medio no transitorio que proporcione o participe en proporcionar instrucciones al procesador del dispositivo 1200 informático (o cualquier otro procesador de un dispositivo descrito en el presente documento) para su ejecución. Un medio de este tipo puede tomar muchas formas, incluyendo pero sin limitación, medios no volátiles y medios volátiles. Medios no volátiles incluyen, por ejemplo, discos óptico, magnéticos u opto-magnéticos, o memoria de circuito integrado, tal como memoria flash. Medios volátiles incluyen memoria de acceso aleatorio dinámica (DRAM), que típicamente constituye la memoria principal. Formas comunes de medio legible por ordenador incluyen, por ejemplo, un disquete, un disco flexible, disco duro, cinta magnética, cualquier otro medio magnético, un CD-ROM, DVD, cualquier otro medio óptico, tarjetas de perforación, cinta de papel, cualquier otro medio físico con patrones de orificios, una RAM, una PROM, una EPROM o EEPROM (memoria de solo lectura electrónicamente borrable programable), una FLASH-EEPROM, cualquier otro chip o cartucho de memoria o cualquier otro medio no transitorio desde el que pueda leer un ordenador.

Diversas formas de medio legible por ordenador pueden verse implicadas en llevar una o más secuencias de una o más instrucciones a la CPU 1206 (o cualquier otro procesador de un dispositivo descrito en el presente documento) para su ejecución. Por ejemplo, las instrucciones pueden inicialmente llevarse en un disco magnético de un ordenador remoto (no mostrado). El ordenador remoto puede cargar las instrucciones en su memoria dinámica y enviar las instrucciones a través de una conexión de Ethernet, línea de cable, o incluso línea de teléfono usando un módem. Un dispositivo de comunicaciones local a un dispositivo 1200 informático (por ejemplo, un servidor) puede recibir los datos en la respectiva línea de comunicaciones y colocar los datos en un bus de sistema para el procesador. El bus de sistema lleva los datos a la memoria principal, a partir de la cual el procesador recupera y ejecuta las instrucciones. Las instrucciones recibidas por la memoria principal pueden almacenarse opcionalmente en memoria ya sea antes o después de la ejecución por el procesador. Además, pueden recibirse instrucciones mediante un puerto de comunicación tal como señales eléctricas, electromagnéticas u ópticas, que son formas ejemplares de comunicaciones inalámbricas o flujos de datos que llevan diversos tipos de información.

Las técnicas de análisis de datos seguras descritas en el presente documento pueden aplicarse a acceso de datos usando máquinas virtuales, y en particular, a comunicación entre una máquina virtual y uno o más servidores o usuarios finales. Se describen en detalle sistemas y métodos para proporcionar características de seguridad

adicionales en entornos informáticos de máquina virtual que integran operaciones de seguridad de máquina virtual y máquina de anfitrión en la Solicitud de Patente de Estados Unidos N. º 13/212.360, presentada el 18 de agosto de 2011.

Los procesos de análisis, encriptación, almacenamiento y restauración anteriormente descritos pueden emplearse, en algunas implementaciones, en entornos de máquina virtual para asegurar la operación y almacenamiento de instancias de máquina virtual. En particular, estos procesos pueden usarse para asegurar una máquina virtual en reposo, asegurando que la máquina virtual no se manipule antes del reinicio. Se describe un número de sistemas y técnicas para asegurar máquinas virtuales en el presente documento, cualquiera de las cuales puede usarse en combinación con cualquiera de las técnicas de seguridad adicionales descritas en el presente documento.

La Figura 13 es un diagrama 1300 de flujo de un proceso para asegurar una máquina virtual. Las etapas del diagrama 1300 de flujo pueden implementarse por un sistema informático programado, que puede incluir uno o más procesadores, dispositivos de almacenamiento y dispositivos de comunicación, dispuestos local y/o remotamente entre sí, programados con instrucciones legibles por máquina (tal como código en cualquiera de un número de lenguajes de programación) con instancias en un medio legible por ordenador o un dispositivo de lógica configurado personalizado. Para facilidad de ilustración, las etapas del diagrama 1300 de flujo se describen en el presente documento realizadas por un dispositivo de anfitrión de un sistema informático programado, pero se entenderá que uno cualquiera o más dispositivos de procesamiento pueden estar configurados para llevar a cabo estas etapas según sea apropiado. En algunas implementaciones, el dispositivo anfitrión es un ordenador personal, un servidor, o un ordenador principal, por ejemplo. En algunas implementaciones, el dispositivo anfitrión es un dispositivo informático portátil, tal como un dispositivo de tableta, portable, portátil, teléfono móvil, teléfono inteligente, o cualquier otro dispositivo de este tipo. En algunas implementaciones, el dispositivo anfitrión incluye múltiples dispositivos informáticos, tales como cualquiera de los anteriormente descritos. Los múltiples dispositivos informáticos pueden estar configurados para ejecutar cada uno una o más etapas u operaciones del proceso de la Figura 13 (por ejemplo, en una manera en serie o paralelo). El dispositivo anfitrión puede ejecutarse en un sistema operativo tal como Windows (Microsoft), Linux, MacOS (Apple), Android (Google), iOS (Cisco Systems), Blackberry OS (Research In Motion), Symbian (Nokia) o Windows Phone (Microsoft), por ejemplo.

En la etapa 1302, el dispositivo anfitrión recibe una pluralidad de compartimentos de datos de módulo de seguridad criptográfica (CSM). Cada una de estas comparticiones es representativa de una porción de los datos necesarios para proporcionar un CSM ejecutable configurado para realizar una cualquiera o más de las operaciones de seguridad descritas en el presente documento (tales como el análisis y restauración de compartimentos de datos analizadas). En particular, el CSM está configurado para generar información de análisis de datos que es usable para determinar en cuál de una pluralidad de compartimentos se colocará una unidad de datos de un conjunto de datos especificados y cómo se encriptará la unidad de datos. Ejemplos de información de análisis de datos se analizan a continuación. En algunas implementaciones, la pluralidad de compartimentos de datos de CSM se reciben desde uno o más dispositivos remotos del dispositivo anfitrión mediante una red de comunicación (por ejemplo, uno o más servidores de datos en comunicación con el dispositivo anfitrión mediante la Internet o una intranet). Como se usa en el presente documento, el término “red” incluye redes ad-hoc, redes entre iguales y redes de campo cercano. Las compartimentos de datos de CSM pueden transmitirse al dispositivo anfitrión en una planificación (por ejemplo, cada veinticuatro horas) o en respuesta a una solicitud del dispositivo anfitrión (como se analiza en detalle a continuación).

Las compartimentos de datos de CSM pueden generarse usando cualquiera de las técnicas descritas en el presente documento para generar compartimentos de datos, tales como técnicas determinística y aleatoria. La técnica de generación de compartición particular seleccionada debería ser complementaria a las técnicas de restauración disponibles para el dispositivo anfitrión para asegurar que el CSM pueda restaurarse apropiadamente a partir de las compartimentos de datos de CSM. En algunas implementaciones, la técnica usada para restaurar el CSM a partir de las compartimentos de datos de CSM se almacena en y es ejecutable por el dispositivo anfitrión. Esta técnica puede ser una técnica de restauración más sencilla que la que puede realizarse por el CSM, tal como una técnica determinística sencilla en la que las compartimentos de CSM se combinan en un orden predeterminado para formar un CSM ejecutable o un instalador para un CSM ejecutable. En algunas implementaciones, la técnica usada para restaurar el CSM a partir de las compartimentos de datos de CSM se especifica por las compartimentos de datos de CSM o en un fichero de datos que acompaña las compartimentos de datos de CSM, y es ejecutable por el dispositivo anfitrión. En implementaciones de este tipo, se proporciona una medida de seguridad separando las compartimentos de datos de CSM entre sí, incluso aunque pueda obtenerse la técnica para restaurar el CSM a partir de las compartimentos de datos de CSM. Encriptar las instrucciones de técnica de restauración puede proporcionar un nivel de seguridad adicional.

En la etapa 1304, el dispositivo anfitrión restaura el CSM a partir de las compartimentos de datos de CSM, de acuerdo con la técnica de restauración apropiada como se describe en el presente documento. Si la restauración de las compartimentos de datos de CSM proporciona un instalador de CSM, el dispositivo anfitrión puede ejecutar el instalador después de la restauración para obtener el CSM ejecutable. En algunas implementaciones, únicamente se recibe una única compartición de datos de CSM en la etapa 1302; los datos restantes necesarios para la restauración del CSM ya están disponibles para el dispositivo anfitrión (por ejemplo, almacenados localmente). En

algunas implementaciones, el dispositivo anfitrión recibe el CSM o instalador de CSM “en su totalidad” en la etapa 1302, caso en el que la restauración del CSM a partir de comparticiones de CSM de datos de la etapa 1304 puede realizarse almacenando el CSM o instalando el CSM, por ejemplo. En algunas implementaciones, el dispositivo anfitrión no realiza las etapas 1302 y 1304; en su lugar, el CSM ejecutable está disponible para el dispositivo anfitrión (por ejemplo, almacenado en almacenamiento local o remotamente accesible), y por lo tanto el CSM no necesita restaurarse a partir de las comparticiones de datos.

En la etapa 1306, el dispositivo anfitrión recibe una pluralidad de primeras comparticiones de máquina virtual (VM). Estas comparticiones pueden recibirse desde uno o más dispositivos remotos del dispositivo anfitrión (por ejemplo, servidores remotos), uno o más dispositivos locales o una combinación de los mismos. Cada una de estas comparticiones representa una porción de uno o más ficheros de VM que se usan para generar instancias y ejecutar una VM en el dispositivo anfitrión. Por ejemplo, las primeras comparticiones de VM recibidas en la etapa 1305 pueden representar uno o más de un fichero de registro, un fichero de estado de BIOS de máquina virtual, un fichero de disco virtual, un fichero de paginación, un fichero de estado de instantánea, un fichero de estado suspendido, y un fichero de configuración. Los ficheros de VM representados por las primeras comparticiones de VM recibidos en la etapa 1306 pueden depender de la aplicación de VM a través de la cual operará la VM. Ejemplos de aplicaciones de VM comercialmente disponibles incluyen VMware (VMWare, Inc.), Xen, e Hyper-V (Microsoft), aunque puede usarse cualquier otra aplicación de VM de nivel de aplicación, de nivel de sistema operativo o de nivel de hardware. Estos ficheros de VM pueden procesarse de cualquier manera descrita en el presente documento con referencia a cualquier conjunto de datos, y en particular, las primeras comparticiones de VM pueden generarse usando cualquiera de las técnicas descritas en el presente documento para generar comparticiones de datos, tales como técnicas determinísticas y aleatorias, siempre que el CSM en el dispositivo anfitrión pueda restaurar la VM de las primeras comparticiones de VM.

En la etapa 1308, el dispositivo anfitrión restaura los ficheros de VM de las primeras comparticiones de VM usando información de restauración de datos generada por el CSM. Por ejemplo, la información de restauración de datos puede ordenar que el CSM restaure los ficheros de VM de las primeras comparticiones de VM desencriptando en primer lugar cada primera compartición de VM y a continuación combinando las primeras comparticiones de VM. Puede almacenarse una o más claves de encriptación/desencriptación con o de manera separada de las primeras comparticiones de VM y pueden analizarse ellas mismas en comparticiones (por ejemplo, aplicando una técnica Shamir). En algunas implementaciones, la información de restauración de datos ordena al CSM que combine en primer lugar las comparticiones de VM y a continuación que desencripte la combinación para restaurar la VM. La información de restauración de datos puede especificar cualquiera de un número de etapas de desencriptación y combinación, o cualesquiera otras técnicas de restauración de datos descritas en el presente documento. En algunas implementaciones, únicamente se recibe una única primera compartición de VM en la etapa 1306; los datos restantes necesarios para la restauración de los ficheros de VM ya están disponibles para el dispositivo anfitrión (por ejemplo, localmente almacenados). En algunas implementaciones, el dispositivo anfitrión recibe los ficheros de VM “en su totalidad” en la etapa 1306, caso en el que la restauración de los ficheros de VM en la etapa 1308 puede realizarse almacenando los ficheros de VM o extrayendo los ficheros de VM de un formato de fichero comprimido (por ejemplo, un fichero ZIP), por ejemplo. En algunas implementaciones, el dispositivo anfitrión no realiza las etapas 1306 y 1308; en su lugar, una aplicación de VM que reside en los dispositivos anfitriones genera una nueva instancia de VM sin necesitar acceder a comparticiones de VM existentes.

En la etapa 1310, el dispositivo anfitrión ejecuta la VM usando los ficheros de VM restaurados en la etapa 1308. La VM puede ser cualquier VM configurada para realizar cualquier función, tal como funciones de comunicación, funciones de procesamiento de datos y funciones de juegos. Por ejemplo, la VM puede ser un sistema operativo de invitado (SO) soportado por un empleado del usuario. El empleado puede controlar la configuración de la VM para asegurar que ninguno de los procesos y aplicaciones nativos para el dispositivo anfitrión pueda infectar o contaminar la operación del SO de invitado. El uso de una VM en este contexto permite que un usuario interactúe con un único dispositivo para realizar tanto tareas informáticas personales (a través del SO nativo) como tareas informáticas relacionadas con el trabajo (a través del SO de invitado), aunque son conocidos muchos otros usos para las VM y pueden usarse en relación con esta y otras implementaciones adecuadas.

En la etapa 1312, el dispositivo anfitrión determina si se ha recibido un comando para detener la VM. Como se usa en el presente documento, un “comando de detención” hace referencia a cualquier comando que active el almacenamiento de uno o más ficheros de VM asociados con la VM, tal como un comando de grabación, un comando de apagado, un comando de suspensión y un comando de pausa. El uno o más ficheros de VM a almacenarse en respuesta a un comando de detención pueden haber cambiado desde que se restauraron los ficheros en la etapa 1308 debido a cualquier cambio a la VM o información adicional generada desde que se ejecutó la VM en la etapa 1310. En algunas implementaciones, el comando de detención se emite por un usuario del dispositivo anfitrión (por ejemplo, cuando el usuario desea conmutar de un SO de invitado ejecutado por la VM al SO nativo). En algunas implementaciones, el comando de detención se emite por el dispositivo anfitrión u otro dispositivo sin un comando sustancialmente síncrono de un usuario (por ejemplo, en un tiempo de “auto-grabación” predeterminado, en respuesta a un evento de interrupción, etc.). Si no se recibe comando de detención en la etapa 1312, el dispositivo anfitrión continúa monitorizando un comando de detención.

Si se identifica un comando de detención en la etapa 1312, el dispositivo anfitrión continúa para invocar el CSM para que genere información de análisis de datos para generar comparticiones de los ficheros de VM en la etapa 1314. La actividad de la VM puede detenerse durante alguno o todo el tiempo durante el cual los ficheros de VM se están almacenando de manera segura (por ejemplo, etapas 1314-1318). La información de análisis de datos generada en la etapa 1314 es usable para determinar en cuál de una pluralidad de comparticiones se colocará una unidad de datos de los ficheros de máquina virtual y cómo se encriptará la unidad de datos, como se describe en detalle a través de toda esta divulgación. En algunas implementaciones, la información de análisis de datos especifica una técnica determinística para determinar en cuál de la pluralidad de comparticiones se colocará la unidad de datos de los ficheros de máquina virtual. En algunas implementaciones, la información de análisis de datos especifica una técnica sustancialmente aleatoria para determinar en cuál de la pluralidad de comparticiones se colocará la unidad de datos de los ficheros de máquina virtual. Puede usarse cualquiera de un número de técnicas de análisis, y múltiples técnicas de análisis pueden estar en capas.

En la etapa 1316, el dispositivo anfitrión invoca el CSM para generar una pluralidad de segundas comparticiones de VM de los ficheros de VM basándose en la información de análisis de datos generada en la etapa 1314. Como se ha descrito con referencia a la etapa 1302 y la etapa 1306, las segundas comparticiones de VM pueden generarse analizando los ficheros de VM en cualquiera de un número de maneras. En algunas implementaciones, el CSM identifica una pluralidad de porciones de los ficheros de VM y encripta cada una de la pluralidad de porciones para formar las segundas comparticiones de VM. En algunas implementaciones, el CSM encripta los ficheros de máquina virtual e identifica una pluralidad de porciones de los ficheros de VM encriptados para formar las segundas comparticiones de VM. Como se analiza en detalle a través de toda esta divulgación, los ficheros de VM pueden restaurarse accediendo a un número umbral de las segundas comparticiones de VM. En algunas implementaciones, el número umbral es menor que un número total de las segundas comparticiones de VM.

En la etapa 1318, el dispositivo anfitrión provoca que cada una de las segundas comparticiones de VM se almacene en respectivas localizaciones de almacenamiento separadas. En algunas implementaciones, las localizaciones de almacenamiento separadas incluyen una pluralidad de localizaciones de almacenamiento separadas en el mismo dispositivo anfitrión, una pluralidad de localizaciones de almacenamiento separadas en uno o más dispositivos remotos del dispositivo anfitrión, o una combinación de al menos una localización de almacenamiento en el dispositivo anfitrión y al menos una localización de almacenamiento en un dispositivo remoto del dispositivo anfitrión. En algunas implementaciones, las localizaciones de almacenamiento en las que se almacenan las segundas comparticiones de VM son las mismas localizaciones que las primeras comparticiones de VM que se almacenaron antes de que las primeras comparticiones de VM se recibieran por el dispositivo anfitrión en la etapa 1306.

En la etapa 1320, el dispositivo anfitrión determina si se ha recibido un comando de inicio de VM. Como se usa en el presente documento, un “comando de inicio” incluye cualquier comando en respuesta a cuál de los ficheros de VM debería restaurarse desde las segundas comparticiones de VM para ejecutar la VM. Si no se identifica comando de inicio en la etapa 1320, el dispositivo anfitrión continúa monitorizando un comando de este tipo. Si se identifica un comando de inicio en la etapa 1320, el dispositivo anfitrión vuelve a la etapa 1308 para restaurar los ficheros de VM de las segundas comparticiones de VM. De esta manera, una VM detenida puede almacenarse de manera segura analizando los ficheros de VM, y restaurarse de manera segura en respuesta a un comando de inicio, reduciendo la probabilidad de que la VM se corrompiera o manipulara mientras está detenida.

El proceso de la Figura 13 se ilustra por los diagramas de bloques de un entorno 1400 de VM seguro en las Figuras 14A-14G. En la Figura 14A, el dispositivo 1402 anfitrión recibe una o más comparticiones 1404 de módulo de seguridad criptográfica (CSM) desde un dispositivo 1406 y una o más comparticiones de CSM 1408 desde un dispositivo 1410 (etapa 1302 de la Figura 13). El dispositivo 1402 anfitrión también recibe una o más primeras comparticiones 1412, 1414 y 1416 de máquina virtual (VM) desde los dispositivos 1418, 1420 y 1422, respectivamente (etapa 1306 de la Figura 13). En algunas implementaciones, los dispositivos 1406, 1410, 1418, 1420 y 1422 cada uno comprenden servidores en comunicación inalámbrica o alámbrica con el dispositivo 1402 anfitrión. La Figura 14B ilustra las comparticiones 1406 y 1410 de CSM y las primeras comparticiones 1412, 1414 y 1416 de VM localmente almacenadas en el dispositivo 1402 anfitrión.

La Figura 14C ilustra un CSM 1424 restaurado generado desde las comparticiones 1406 y 1410 de CSM (etapa 1304 de la Figura 13), que se usa para restaurar la VM 1432 (Figura 14D) de las primeras comparticiones 1412, 1414 y 1416 de VM (etapa 1308 de la Figura 13). La VM 1432 se ejecuta a continuación (etapa 1310 de la Figura 13), durante periodo el cual se cambian los ficheros subyacentes a la VM. En respuesta a un comando de detención (etapa 1312 de la Figura 13), el dispositivo anfitrión 1404 usa el CSM 1424 para generar información de análisis (etapa 1314 de la Figura 13) para generar un conjunto de segundas comparticiones 1426, 1428 y 1430 de VM como se muestra en la figura 14E (etapa 1316 de la Figura 13). Las segundas comparticiones 1426, 1428 y 1420 de VM se almacenan a continuación en los dispositivos 1418, 1420 y 1422 como se muestra en la Figura 14F (etapa 1318 de la Figura 13). El dispositivo 1402 anfitrión puede borrar el CSM 1424, como se muestra en la Figura 14G, y esperar un comando para iniciar la VM (etapa 1320 de la Figura 13), punto en el cual la máquina 1402 de anfitrión puede recuperar las segundas comparticiones 1426, 1428 y 1430 de VM desde los dispositivos 1418, 1420 y 1422.

Como se indica en el presente documento, en algunas implementaciones, el módulo de seguridad criptográfica (CSM) y la máquina virtual (VM) ya están disponibles para un dispositivo de anfitrión, y por lo tanto no necesitan realizarse las etapas 1302 y 1304 y las etapas 1306 y 1308. Se presentan diagramas de bloques de un entorno 1500 de VM seguro de acuerdo con una implementación de este tipo en las Figuras 15A-15B. En la Figura 15A, el CSM 1524 y la VM 1532 están disponibles para el dispositivo anfitrión 1504, y por lo tanto el proceso de la Figura 13 puede comenzar en la etapa 1310, con la ejecución de la VM 1532. En respuesta a un comando de detención (etapa 1312 de la Figura 13), el dispositivo anfitrión 1504 usa el CSM 1524 para generar información de análisis (etapa 1314 de la Figura 13) para generar un conjunto de segundas compartimentaciones 1526, 1528 y 1530 de VM como se muestra en la Figura 15B (etapa 1316 de la Figura 13). Las segundas compartimentaciones 1526, 1528 y 1520 de VM pueden a continuación almacenarse remotamente (como se ha ilustrado anteriormente en la Figura 14) o localmente.

En algunas implementaciones, se almacenan compartimentaciones de VM juntas o se organizan de otra manera en directorios reconocibles para el acceso fácil. En algunas implementaciones de las técnicas de aseguración de la VM descritas en el presente documento, las compartimentaciones de VM se almacenan localmente en un dispositivo de anfitrión en una o más localizaciones de almacenamiento separadas que se seleccionan para hacer difícil detectar la presencia de compartimentaciones de VM en el dispositivo anfitrión. Esto puede conseguirse almacenando las compartimentaciones en directorios asociados con aplicaciones no de VM o ficheros de sistema, y nombrando las compartimentaciones de VM con nombres de fichero y extensiones que oscurecen su origen. Adicionalmente, la compartición de VM puede oscurecerse adicionalmente cambiando la información de fichero (tal como hora/fecha creada, hora/fecha modificada y la hora/fecha accedida) usando un programa de gestión de ficheros comercialmente disponible u otra utilidad, por ejemplo.

La Figura 16 representa un ejemplo de una pantalla 1602 que incluye una estructura de directorio en la que las compartimentaciones de VM están “ocultas”. En este ejemplo, se almacena una primera compartición 1604 de VM en un directorio “Módulos de extensión” para la aplicación “Internet Explorer” y se etiqueta como “x2qd.dll”. Se almacena una segunda compartición 1606 de VM en un directorio de sistema “Ayuda” como “g9ggy.H1T”. Se almacena una tercera compartición 1608 de VM en un directorio “Archivos de programa” como “autoc.dat”. En implementaciones de este tipo, la localización de las compartimentaciones de VM es conocida para el CSM de modo que las compartimentaciones pueden recuperarse y la VM restaurarse tras la recepción de un comando de inicio. Un observador casual, sin embargo, no detectará fácilmente la presencia de una VM inspeccionando la estructura de directorio de la pantalla 1602.

En algunas implementaciones, las compartimentaciones de VM se almacenan en la partición de un medio de almacenamiento (tal como un disco duro) que está separado de una partición gestionada por el sistema operativo (SO). Como resultado, las compartimentaciones de VM no están disponibles para que no se reconozcan por el SO, y por lo tanto no son visibles para un observador del sistema de ficheros del SO. El CSM puede almacenar las compartimentaciones de VM en esta partición separada escribiendo los datos de compartición de VM directamente a bloques de datos en la partición separada, analizando el sistema de ficheros del SO. El CSM puede almacenar las compartimentaciones de VM en esta partición separada escribiendo los datos de compartición de VM directamente a bloques de datos en la partición separada, pasando el sistema de ficheros del SO.

La Figura 17 representa un ejemplo de un sistema 1700 de medio de almacenamiento particionado usado para oscurecer la presencia de compartimentaciones de VM. El sistema 1700 de medio de almacenamiento incluye un medio 1714 de almacenamiento que está particionado en una primera partición 1702 y una segunda partición 1704. La primera partición 1702 es una partición de los bloques de datos del medio 1714 de almacenamiento (por ejemplo, 196 GB de un disco duro de 200 GB) que está asignada al sistema operativo (SO) 1706 para gestión por el sistema 1708 de ficheros. La segunda partición 1704 puede incluir los bloques de datos restantes del medio 1714 de almacenamiento (por ejemplo, 4 GB del disco duro de 200 GB). El sistema 1700 de medio de almacenamiento está configurado de manera que el CSM 1710 (que opera bajo el SO 1706) escribe las compartimentaciones 1712 de VM directamente a localizaciones de almacenamiento en la segunda partición 1704. El CSM 1710 puede recuperar estas compartimentaciones leyendo directamente desde la segunda partición 1704. Aunque las compartimentaciones 1712 de VM son accesibles al CSM 1710, las compartimentaciones no se gestionan por el sistema 1708 de ficheros y por lo tanto no son visibles para el SO 1706.

La presencia de una máquina virtual u otro conjunto de datos puede oscurecerse adicionalmente para un observador casual requiriendo una secuencia predeterminada de entradas de usuario antes de que se visualice una indicación del conjunto de datos en el dispositivo. Por ejemplo, después de que una VM detenida se asegura almacenando compartimentaciones de los ficheros de VM en localizaciones de almacenamiento separadas, el dispositivo anfitrión puede no proporcionar icono o entrada de menú desplegable con la que un usuario pueda emitir un comando para iniciar la VM; en su lugar, el dispositivo anfitrión puede esperar que el usuario realice una serie de entradas gestuales antes de que se inicie la VM. Estas entradas gestuales pueden seleccionarse por su similitud a gestos comunes, por ejemplo, tocar el dispositivo anfitrión en una superficie o frotar una pantalla táctil como si fuera borrar una huella dactilar. No teniendo indicación visual de la presencia de un conjunto de datos, y requiriendo una entrada gestual “camuflada” u otra para restaurar el conjunto de datos, el conjunto de datos se oscurece adicionalmente de un observador.

La Figura 18 es un diagrama 1800 de flujo de un proceso para restaurar un conjunto de datos de acuerdo con tales implementaciones. Como se ha descrito con referencia a la Figura 13, las etapas del diagrama 1800 de flujo pueden implementarse por un sistema informático programado, que puede incluir uno o más procesadores, dispositivos de almacenamiento y dispositivos de comunicación, dispuestos localmente y/o de manera remota entre sí, programarse con instrucciones legibles por máquina (tal como código en cualquiera de un número de lenguajes de programación) instanciados en un medio legible por ordenador o en un dispositivo lógico configurado personalizado. Para facilidad de ilustración, las etapas del diagrama 1800 de flujo se describen en el presente documento según se realizan por un dispositivo de procesamiento de un sistema informático programado, pero se entenderá que uno cualquiera o más dispositivos de procesamiento pueden configurarse para llevar a cabo estas etapas según sea apropiado. En algunas implementaciones, el dispositivo de procesamiento es un ordenador personal, un servidor, o un ordenador principal, por ejemplo. En algunas implementaciones, el dispositivo de procesamiento es un dispositivo informático portátil, tal como un dispositivo de tableta, portable, portátil, teléfono móvil, teléfono inteligente, o cualquier otro dispositivo de este tipo. En algunas implementaciones, el dispositivo de procesamiento incluye múltiples dispositivos informáticos, tal como cualquiera de aquellos descritos en el presente documento. Los múltiples dispositivos informáticos pueden configurarse para ejecutar cada uno una o más etapas u operaciones del proceso de la Figura 18 (por ejemplo, de manera en serie o paralela). El dispositivo de procesamiento puede estar ejecutando un sistema operativo tal como Windows (Microsoft), Linux, MacOS (Apple), Android (Google), iOS (Cisco Systems), Blackberry OS (Research In Motion), Symbian (Nokia), o Windows Phone (Microsoft), por ejemplo.

En la etapa 1802, el dispositivo de procesamiento visualiza una pluralidad de elementos seleccionables por el usuario en un dispositivo de visualización. Cada elemento seleccionable por el usuario está asociado con una aplicación ejecutable diferente, tal como una aplicación de explorador o una aplicación de procesamiento de textos. Los elementos seleccionables por el usuario pueden incluir uno o más iconos, uno o más listados de menús desplegables o cualquier otro elemento de visualización seleccionable.

En la etapa 1804, mientras se visualiza la pluralidad de elementos seleccionables por el usuario, el dispositivo de procesamiento determina si se ha recibido una secuencia predeterminada de entradas de usuario. La secuencia predeterminada de entradas de usuario puede incluir una cualquiera o más de una entrada gestual (por ejemplo, una forma particular dibujada en un panel táctil con un lápiz óptico o el dedo), una entrada de reconocimiento biométrica (por ejemplo, una entrada de reconocimiento facial, una entrada de reconocimiento de huella dactilar, una entrada de exploración retinal), una orientación del dispositivo de procesamiento (por ejemplo, mantener el dispositivo al revés durante un periodo de tiempo predeterminado), y una aceleración del dispositivo de procesamiento (por ejemplo, tocar el dispositivo en una superficie un número predeterminado de veces, o a una velocidad predeterminada, u ondear el dispositivo en una manera predeterminada), una entrada de teclado numérico (por ejemplo, un código de paso u otra secuencia de presiones de tecla). Si el dispositivo de procesamiento no identifica la secuencia predeterminada de entradas de usuario, los dispositivos de procesamiento continúan monitorizando las entradas.

Si el dispositivo de procesamiento no identifica la secuencia predeterminada de entradas de usuario en la etapa 1804, el dispositivo de procesamiento ejecuta un módulo de seguridad criptográfica (CSM) en la etapa 1806. El CSM está configurado para restaurar conjuntos de datos de compartimentos de conjunto de datos, y no está asociado con ninguno de los elementos seleccionables por el usuario visualizados en la etapa 1802 (antes de recibir la secuencia predeterminada de entradas de usuario). En otras palabras, la presencia del CSM no era evidente para un observador por inspección visual del dispositivo de visualización en la etapa 1802.

En la etapa 1808, el dispositivo de procesamiento usa la funcionalidad de restauración criptográfica del CSM para restaurar un conjunto de datos asociado con la secuencia predeterminada de entradas de usuario desde una pluralidad de compartimentos de conjunto de datos, cada compartición de conjunto de datos representativa de una porción encriptada del conjunto de datos. Se describen en detalle técnicas para generar compartimentos de datos y restaurar estas compartimentos de datos a través de toda esta divulgación. Las compartimentos de conjunto de datos pueden almacenarse en respectivas localizaciones de almacenamiento separadas locales al dispositivo de procesamiento, remotas al dispositivo de procesamiento, o una combinación de las mismas.

En la etapa 1810, el dispositivo de procesamiento visualiza un elemento gráfico asociado con el conjunto de datos en el dispositivo de visualización. El elemento gráfico puede ser un icono u otro indicador que señaliza al usuario del dispositivo de procesamiento que el conjunto de datos se ha restaurado. En algunas implementaciones, este elemento gráfico es una representación visual del mismo conjunto de datos. Esta etapa de visualización es opcional; en algunas implementaciones, no se presenta indicación visual de los conjuntos de datos restaurados. Sin embargo, el dispositivo de procesamiento puede utilizar cualquier funcionalidad adicional proporcionada por el conjunto de datos restaurados, o hacer cualquier funcionalidad adicional de este tipo para el usuario. Por ejemplo, el conjunto de datos restaurado en la etapa 1808 puede ser una aplicación de teléfono móvil ejecutada (o máquina virtual que ejecuta una aplicación de este tipo) que permite que un usuario haga llamadas desde el teléfono “oculto” en un teléfono inteligente con una aplicación de teléfono “aparente” existente. La presencia del teléfono oculto puede indicarse visualmente para proporcionar seguridad adicional.

En algunas implementaciones, el conjunto de datos está asociado con una aplicación ejecutable por el dispositivo de procesamiento. En implementaciones de este tipo, el dispositivo de procesamiento puede realizar opcionalmente la etapa 1812 y ejecutar la aplicación asociada. Por ejemplo, el conjunto de datos puede ser un instalador para una aplicación de comunicación telefónica o puede proporcionar datos de configuración para una aplicación de este tipo. En otro ejemplo, el conjunto de datos puede ser representativo de ficheros de máquina virtual, tales como un fichero de registro, un fichero de estado de BIOS de máquina virtual, un fichero de disco virtual, un fichero de paginación, un fichero de estado de instantánea, un fichero de estado suspendido, y un fichero de configuración. Cuando el conjunto de datos es representativo de ficheros de máquina virtual, ejecutar la aplicación asociada puede incluir iniciar una máquina virtual usando los ficheros de máquina virtual.

En la etapa 1814, el dispositivo de procesamiento determina si se ha recibido un comando de ocultación. Como se usa en el presente documento, un “comando de ocultación” es cualquier comando que indica que la presencia del conjunto de datos debería oscurecerse de un observador. Un comando de ocultación puede incluir cualquiera de los comandos de etapa anteriormente descritos con referencia a la Figura 13, por ejemplo, o puede incluir comandos para hibernar, entrar en inactividad, bloquear o suspender el dispositivo de procesamiento. Si no se recibe comando de ocultación en la etapa 1814, el dispositivo de procesamiento continúa monitorizando un comando de este tipo. Un usuario puede emitir un comando de ocultación usando una secuencia predeterminada de entradas de usuario (incluyendo cualquiera de las entradas de usuario anteriormente analizadas con referencia a la etapa 1804) o una única entrada designada. Un comando de ocultación también puede generarse automáticamente cuando los dispositivos de procesamiento detectan ciertas condiciones, tales como la firma eléctrica de una nave enemiga en un escenario de conflicto.

Si se recibe un comando de ocultación en la etapa 1814, el dispositivo de procesamiento oscurece el conjunto de datos generando información de análisis de datos usando el CSM (etapa 1816), generando comparticiones del conjunto de datos basándose en la información de análisis de datos (etapa 1818) y provocando el almacenamiento de las comparticiones en respectivas localizaciones separadas (etapa 1820). Estas etapas pueden realizarse en cualquiera de las maneras descritas en el presente documento (por ejemplo, aquellas anteriormente descritas con referencia a la Figura 13).

Las Figuras 19A y 19B representan pantallas en un dispositivo portátil que pueden presentarse antes y después de que se identifique la secuencia predeterminada de entradas de usuario en la etapa 1804 de la Figura 18. La Figura 19A representa una pantalla 1902 con los iconos 1904, 1906 y 1908 seleccionables por el usuario, que pueden estar asociados con aplicaciones de música, exploración y chat, respectivamente. Ninguno de los iconos 1904, 1906 y 1908 seleccionables por el usuario están asociados con un módulo de seguridad criptográfica (CSM) o un conjunto de datos almacenado en comparticiones y oscurecido en el dispositivo portátil. Después de que se identifica la secuencia predeterminada de entradas de usuario en la etapa 1804 de la Figura 18, se visualiza el elemento 1910 gráfico adicional, indicando que el conjunto de datos se ha restaurado. El elemento 1910 gráfico puede ser seleccionable por el usuario para activar la visualización del conjunto de datos o el lanzamiento de una aplicación asociada con el conjunto de datos.

En algunas de las técnicas de seguridad y restauración de datos de la máquina virtual anteriormente descritas, un dispositivo recibe una o más comparticiones desde uno o más otros dispositivos antes de que se restaure un módulo de seguridad criptográfica (CSM), una máquina virtual (VM) o un conjunto de datos La capacidad de recuperar comparticiones únicamente cuando dos dispositivos están en “proximidad” puede tener un número de ventajas para ciertas aplicaciones. Por ejemplo, una compañía puede desear únicamente permitir a sus empleados acceder al sitio de datos sensibles cuando los empleados están dentro de las instalaciones de la compañía. En otro ejemplo, un informador de noticias puede desear intercambiar datos con un periodista cuando los dos están en proximidad, pero no hasta entonces. En otro ejemplo, un desarrollador de un juego multijugador para dispositivos portátiles puede desear permitir únicamente a usuarios acceso a nuevos niveles de juego cuando un número suficiente de ellos han entrado en proximidad geográfica. En cualquiera de estos ajustes, el acceso a recursos puede controlarse proporcionando únicamente suficientes comparticiones de datos para restaurar un recurso deseado (o acceso a un recurso deseado) cuando se cumplen las condiciones de proximidad.

La Figura 20 es un diagrama 2000 de flujo de un proceso de este tipo para restaurar un conjunto de datos. Como se ha descrito con referencia a las Figuras 13 y 18, las etapas del diagrama 2000 de flujo pueden implementarse por un sistema informático programado, puede incluir uno o más procesadores, dispositivos de almacenamiento y dispositivos de comunicación, dispuestos local y/o remotamente entre sí, programados con instrucciones legibles por máquina (tal como código en cualquiera de un número de lenguajes de programación) instanciadas en un medio legible por ordenador o un dispositivo lógico configurado personalizado. Para facilidad de ilustración, las etapas del diagrama 1800 de flujo se describen en el presente documento realizadas por un primer dispositivo informático de un sistema informático programado, pero se entenderá que uno cualquiera o más dispositivos de procesamiento pueden configurarse para llevar a cabo estas etapas según sea apropiado. En algunas implementaciones, el primer dispositivo informático es un ordenador personal, un servidor, o un ordenador principal, por ejemplo. En algunas implementaciones, el primer dispositivo informático es un dispositivo informático portátil, tal como un dispositivo de tableta, portable, portátil, teléfono móvil, teléfono inteligente, o cualquier otro dispositivo de este tipo. En algunas implementaciones, el primer dispositivo informático incluye múltiples dispositivos informáticos, tales como cualquiera

de aquellos anteriormente descritos. Los múltiples dispositivos informáticos pueden configurarse para ejecutar cada uno una o más etapas u operaciones del proceso de la Figura 13 (por ejemplo, de una manera en serie o paralela). El primer dispositivo informático puede estar ejecutando un sistema operativo tal como Windows (Microsoft), Linux, MacOS (Apple), Android (Google), iOS (Cisco Systems), Blackberry OS (Research In Motion), Symbian (Nokia), o Windows Phone (Microsoft), por ejemplo.

En la etapa 2002, el primer dispositivo informático identifica primeras comparticiones de conjunto de datos disponibles para el dispositivo de procesamiento. Cada primera compartición de datos es representativa de una porción de datos desde un conjunto de datos deseado. El conjunto de datos no puede restaurarse desde las primeras comparticiones de conjunto de datos identificadas sino que puede restaurarse por un número umbral de comparticiones de conjunto de datos. En algunas implementaciones, las primeras comparticiones de conjunto de datos se almacenan localmente al primer dispositivo informático.

En la etapa 2004, el primer dispositivo informático determina si se detecta un enlace de comunicación entre el primer dispositivo informático y un segundo dispositivo informático diferente del primer dispositivo informático. El segundo dispositivo informático puede ser un dispositivo informático portátil, un servidor, un portátil, o cualquier otro dispositivo informático. En algunas implementaciones, detectar un enlace de comunicación en la etapa 2004 incluye determinar que el segundo dispositivo informático está en un alcance de comunicación de un dispositivo de comunicación de frecuencia de radio (tal como un dispositivo de Bluetooth) del primer dispositivo informático. En algunas implementaciones, detectar un enlace de comunicación en la etapa 2004 incluye determinar que el segundo dispositivo informático está conectado a una red de comunicaciones informáticas a la que el primer dispositivo informático también está conectado. Esta conexión puede ser alámbrica o inalámbrica. En algunas implementaciones, detectar un enlace de comunicación en la etapa 2004 incluye determinar que el segundo dispositivo informático está en una distancia geográfica predeterminada del primer dispositivo informático. Esta determinación geográfica puede realizarse, por ejemplo, recibiendo información en el primer dispositivo informático desde un servidor configurado para almacenar información acerca de la localización geográfica del segundo dispositivo informático (por ejemplo, seguimiento GPS). La información desde el servidor puede ser un mensaje que indica una proximidad del segundo dispositivo informático al primer dispositivo informático. En algunas realizaciones, detectar un enlace de comunicación en la etapa 2004 incluye detectar una ruta de comunicación eléctrica entre el primer dispositivo informático y el segundo dispositivo informático mediante un cuerpo de un usuario del primer dispositivo informático y un cuerpo de un usuario del segundo dispositivo informático, los cuerpos de los usuarios en contacto físico entre sí y con sus respectivos dispositivos informáticos. Ejemplos de estas diversas implementaciones de la etapa 2004 se describen a continuación con referencia a las Figuras 21-69.

Si no se detecta enlace de comunicación en la etapa 2004, el primer dispositivo informático continúa monitorizando un enlace de comunicación. Si se detecta un enlace de comunicación en la etapa 2004, el primer dispositivo informático recibe segundas comparticiones de conjunto de datos desde el segundo dispositivo informático en la etapa 2006 El primer dispositivo informático puede transmitir también las primeras comparticiones de conjunto de datos al segundo dispositivo informático en la etapa 2008. En algunas implementaciones, la recepción de la etapa 2006 y la transmisión de la etapa 2008 tienen lugar mediante el enlace de comunicación detectado. En algunas implementaciones, la recepción de la etapa 2006 y la transmisión de la etapa 2008 tienen lugar mediante un dispositivo intermediario, tal como un servidor en comunicación con tanto el primer dispositivo informático como el segundo dispositivo informático.

En la etapa 2010, el primer dispositivo informático determina si el número umbral de comparticiones se ha recibido para restaurar el conjunto de datos deseado. Si no, el primer dispositivo informático vuelve a la etapa 2004 para monitorizar un enlace de comunicación con otro dispositivo informático. Si el número umbral de comparticiones se ha recibido en la etapa 2010, el primer dispositivo informático restaura el conjunto de datos deseado desde las comparticiones en la etapa 2012 (usando, por ejemplo, un módulo de seguridad criptográfica configurado para realizar cualquiera de las técnicas de restauración descritas en el presente documento) o combinación de las mismas.

En la etapa 2014, el dispositivo de procesamiento visualiza un elemento gráfico asociado con el conjunto de datos en el dispositivo de visualización. El elemento gráfico puede ser un icono u otro indicador que señaliza al usuario del dispositivo de procesamiento que el conjunto de datos se ha restaurado. En algunas implementaciones, este elemento gráfico es una representación visual del mismo conjunto de datos. Esta etapa de visualización es opcional; en algunas implementaciones, no se presenta indicación visual del conjunto de datos restaurados. Sin embargo, el primer dispositivo informático puede utilizar cualquier funcionalidad adicional proporcionada por el conjunto de datos restaurado, o hacer cualquier funcionalidad adicional de este tipo disponible para un usuario, como se ha analizado anteriormente con referencia a la etapa 1810 de la Figura 18.

En algunas implementaciones, el conjunto de datos está asociado con una aplicación ejecutable por el dispositivo de procesamiento. En implementaciones de este tipo, el dispositivo de procesamiento puede realizar opcionalmente la etapa 2016 y ejecutar la aplicación asociada. Por ejemplo, el conjunto de datos puede ser un instalador para una aplicación de comunicación telefónica o puede proporcionar datos de configuración para una aplicación de este tipo. En otro ejemplo, el conjunto de datos puede estar asociado con una aplicación de juegos. En otro ejemplo, el

conjunto de datos puede ser representativo de ficheros de máquina virtual, tal como un fichero de registro, un fichero de estado de BIOS de máquina virtual, un fichero de disco virtual, un fichero de paginación, un fichero de estado de instantánea, un fichero de estado suspendido, y un fichero de configuración. Cuando el conjunto de datos es representativo de ficheros de máquina virtual, ejecutar la aplicación asociada puede incluir iniciar una máquina virtual usando los ficheros de máquina virtual.

Las Figuras 21A y 21B ilustran una implementación de las etapas 2002-2006 de la Figura 20. La Figura 21A representa un primer dispositivo 2102 informático que tiene acceso a primeras comparticiones de conjunto de datos S1 2104 y un servidor 2106 que tiene acceso a segundas comparticiones de conjunto de datos S2 2108. En la Figura 21B, cuando el primer dispositivo 2102 informático conecta al servidor 2106 mediante una conexión cableada (por ejemplo, acoplando el primer dispositivo 2102 informático en una estación de acoplamiento cableada a una red de comunicación común con el servidor 2106), el primer dispositivo 2102 informático recibe las segundas comparticiones de conjunto de datos S2 2108 desde el servidor 2106.

Las Figuras 22A y 22B ilustran otra implementación de las etapas 2002-2006 de la Figura 20. La Figura 22A representa un primer dispositivo 2202 informático que tiene acceso a primeras comparticiones de conjunto de datos S1 2204 y un servidor 2206 que tiene acceso a segundas comparticiones de conjunto de datos S2 2208. En la Figura 22B, cuando el primer dispositivo 2202 informático entra en alcance de una conexión 2210 inalámbrica del servidor 2206 y conecta al servidor 2206 mediante una conexión inalámbrica (por ejemplo, una conexión 802.11b o Bluetooth), el primer dispositivo 2202 informático recibe las segundas comparticiones de conjunto de datos S2 2208 desde el servidor 2206.

Las Figuras 23A-23C ilustran otra implementación de varias de las etapas de la Figura 20. La Figura 23A representa un primer dispositivo 2302 informático que tiene acceso a primeras comparticiones de conjunto de datos S1 2304, un segundo dispositivo 2306 informático que tiene acceso a segundas comparticiones de conjunto de datos S2 2308, y un tercer dispositivo 2310 informático que tiene acceso a terceras comparticiones de conjunto de datos S3 2312. En la Figura 23B, cuando el primer dispositivo 2302 informático entra en un alcance de conexión 2314 inalámbrica del segundo dispositivo 2306 informático y conecta al segundo dispositivo 2306 informático mediante una conexión inalámbrica, el primer dispositivo 2302 informático recibe las segundas comparticiones de conjunto de datos S2 2308 desde el segundo dispositivo 2306 informático. En la Figura 23C, cuando el primer dispositivo 2302 informático entra en un alcance de conexión 2316 inalámbrica del tercer dispositivo 2310 informático y conecta al tercer dispositivo 2310 informático mediante una conexión inalámbrica, el primer dispositivo 2302 informático recibe las terceras comparticiones de conjunto de datos S3 2312 desde el tercer dispositivo 2310 informático.

Las Figuras 24A y 24B ilustran otra implementación de varias de las etapas de la Figura 20. La Figura 24A representa un primer dispositivo 2402 informático que tiene acceso a primeras comparticiones de conjunto de datos S1 2404, un segundo dispositivo 2406 informático que tiene acceso a segundas comparticiones de conjunto de datos S2 2408, y un tercer dispositivo 2410 informático que tiene acceso a terceras comparticiones de conjunto de datos S3 2412. En la Figura 24B, cuando el primer dispositivo 2402 informático está en un alcance de conexión 2414 inalámbrica del segundo dispositivo 2406 informático y conecta al segundo dispositivo 2406 informático mediante una conexión inalámbrica, y también está en un alcance de conexión 2416 inalámbrica del tercer dispositivo 2410 informático y conecta al tercer dispositivo 2410 informático mediante una conexión inalámbrica, el primer dispositivo 2402 informático recibe las segundas comparticiones de conjunto de datos S2 2408 desde el segundo dispositivo 2406 informático y las terceras comparticiones de conjunto de datos S3 2412 desde el tercer dispositivo 2410 informático.

Las Figuras 25A-25C ilustran otra implementación de varias de las etapas de la Figura 20. La Figura 25A representa un primer dispositivo 2502 informático que tiene acceso a primeras comparticiones de conjunto de datos S1 2504, un segundo dispositivo 2506 informático que tiene acceso a segundas comparticiones de conjunto de datos S2 2508, y un tercer dispositivo 2510 informático que tiene acceso a terceras comparticiones de conjunto de datos S3 2512. En la Figura 25B, cuando el primer dispositivo 2502 informático entra en un alcance de conexión 2514 inalámbrica del segundo dispositivo 2506 informático y conecta al segundo dispositivo 2506 informático mediante una conexión inalámbrica, el primer dispositivo 2502 informático recibe las segundas comparticiones de conjunto de datos S2 2508 desde el segundo dispositivo 2506 informático, y también transmite las primeras comparticiones de conjunto de datos S1 2504 al segundo dispositivo 2506 informático. En la Figura 25C, cuando el primer dispositivo 2502 informático entra en un alcance de conexión 2516 inalámbrica del tercer dispositivo 2510 informático y conecta al tercer dispositivo 2510 informático mediante una conexión inalámbrica, el primer dispositivo 2502 informático recibe las terceras comparticiones de conjunto de datos S3 2512 desde el tercer dispositivo 2510 informático, y también transmite las primeras comparticiones de conjunto de datos S1 2504 al tercer dispositivo 2510 informático. En algunas implementaciones, el primer dispositivo 2502 informático puede transmitir tanto las primeras comparticiones de conjunto de datos S1 2504 como las segundas comparticiones de conjunto de datos S2 2508 al tercer dispositivo 2510 informático.

Las Figuras 26A y 26B ilustran otra implementación de algunas de las etapas de la Figura 20. La Figura 26A representa un primer dispositivo 2602 informático, mantenido por un primer usuario 2610, que tiene acceso a primeras comparticiones de conjunto de datos S1 2604 y un segundo dispositivo 2606 informático, mantenido por un segundo usuario 2612, que tiene acceso a segundas comparticiones de conjunto de datos S2 2608. En la Figura 26B, cuando el primer usuario 2610 entra en contacto físico con el segundo usuario 2612, el primer y segundo dispositivos 2602 y 2606 informáticos pueden detectar una impedancia relativamente baja entre electrodos montados en sus respectivas superficies, y en respuesta, transferir sus respectivas comparticiones de conjunto de datos al otro dispositivo.

Otras combinaciones, adiciones, sustituciones y modificaciones serán evidentes para el experto en la materia en vista de la divulgación del presente documento.

REIVINDICACIONES

1. Un método para asegurar una máquina virtual, que comprende:

ejecutar una máquina virtual en un dispositivo de anfitrión, comprendiendo la máquina virtual ficheros de máquina virtual;
generar información de análisis de datos, en el que la información de análisis de datos es usable para determinar en cuál de una pluralidad de comparticiones se colocará una porción de los ficheros de máquina virtual y cómo se encriptará la porción;
en respuesta a recibir un comando para detener la máquina virtual:

generar la pluralidad de comparticiones basándose en la información de análisis de datos;
provocar que cada una de la pluralidad de comparticiones se almacene en respectivas localizaciones de almacenamiento separadas, en el que las respectivas localizaciones de almacenamiento separadas incluyen uno o más directorios asociados con una aplicación no de máquina virtual;

en el que los ficheros de máquina virtual pueden restaurarse accediendo a un número umbral de la pluralidad de comparticiones.

2. El método de la reivindicación 1, en el que el comando para detener la máquina virtual se emite por un procesador del dispositivo anfitrión sin un comando sustancialmente síncrono de un usuario del dispositivo anfitrión.

3. El método de cualquiera de las reivindicaciones anteriores, en el que generar la pluralidad de comparticiones basándose en la información de análisis de datos comprende:

identificar una pluralidad de porciones de los ficheros de máquina virtual; y
encriptar cada una de la pluralidad de porciones para formar la pluralidad de comparticiones.

4. El método de cualquiera de las reivindicaciones anteriores, en el que generar la pluralidad de comparticiones basándose en la información de análisis de datos comprende:

encriptar los ficheros de máquina virtual; e
identificar una pluralidad de porciones de los ficheros de máquina virtual encriptados para formar la pluralidad de comparticiones.

5. El método de cualquiera de las reivindicaciones anteriores, en el que la información de análisis de datos especifica una técnica determinística para determinar en cuál de la pluralidad de comparticiones se colocará la porción de los ficheros de máquina virtual.

6. El método de cualquiera de las reivindicaciones anteriores, en el que la información de análisis de datos especifica una técnica determinística para determinar en cuál posición en cada una de la pluralidad de comparticiones se colocará la porción de los ficheros de máquina virtual.

7. El método de cualquiera de las reivindicaciones anteriores, en el que la información de análisis de datos especifica una técnica sustancialmente aleatoria para determinar en cuál de la pluralidad de comparticiones se colocará la porción de los ficheros de máquina virtual.

8. El método de cualquiera de las reivindicaciones anteriores, en el que la información de análisis de datos especifica una técnica sustancialmente aleatoria para determinar en cuál posición en cada una de la pluralidad de comparticiones se colocará la porción de los ficheros de máquina virtual.

9. El método de cualquiera de las reivindicaciones anteriores, en el que las localizaciones de almacenamiento separadas incluyen una pluralidad de localizaciones de almacenamiento separadas en el dispositivo anfitrión.

10. El método de cualquiera de las reivindicaciones anteriores, en el que las localizaciones de almacenamiento separadas incluyen una pluralidad de localizaciones de almacenamiento separadas en uno o más dispositivos remotos del dispositivo anfitrión.

11. El método de cualquiera de las reivindicaciones anteriores, en el que las localizaciones de almacenamiento separadas incluyen al menos una localización de almacenamiento en el dispositivo anfitrión y al menos una localización de almacenamiento en un dispositivo remoto del dispositivo anfitrión.

12. El método de cualquiera de las reivindicaciones anteriores, que comprende adicionalmente:
antes de ejecutar la máquina virtual en el dispositivo anfitrión:

recibir una segunda pluralidad de compartimentos; y
restaurar los ficheros de máquina virtual de la segunda pluralidad de compartimentos usando información de restauración de datos que determina cómo desencriptar y disponer porciones de la pluralidad de compartimentos para formar los ficheros de máquina virtual.

13. El método de cualquiera de las reivindicaciones anteriores, que comprende adicionalmente:

antes de generar la información de análisis de datos:

recibir una tercera pluralidad de compartimentos desde uno o más dispositivos remotos del dispositivo anfitrión; y
restaurar una aplicación de análisis ejecutable desde la tercera pluralidad de compartimentos;

en el que la información de análisis de datos se genera por la aplicación de análisis ejecutable.

14. El método de cualquiera de las reivindicaciones anteriores, en el que la información de análisis de datos determina el tamaño de cada una de las compartimentos, en el que el tamaño de al menos una compartición es diferente del tamaño de al menos otra compartición.

15. Un sistema informático que comprende:

al menos un procesador; y
un medio legible por ordenador no transitorio que almacena instrucciones ejecutables por ordenador que, cuando se ejecutan por el al menos un procesador, provocan que el sistema informático lleve a cabo el método de cualquiera de las reivindicaciones anteriores.

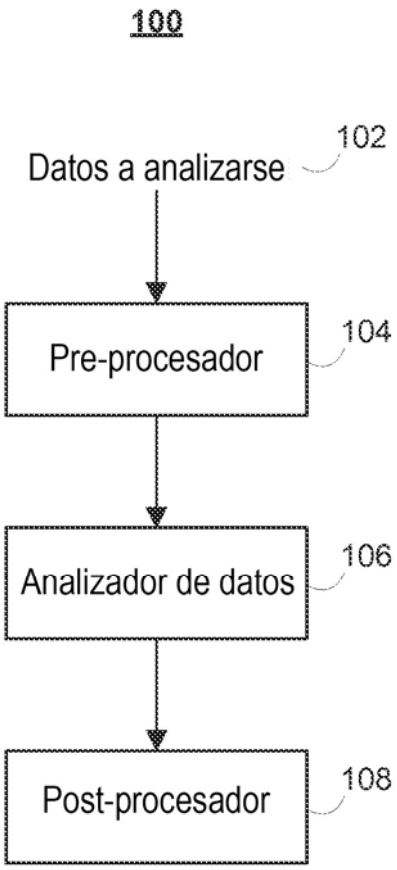

100
Datos a analizarse
102
Pre-procesador
104
Analizador de datos
106
Post-procesador
108

FIG. 1

FIG. 2

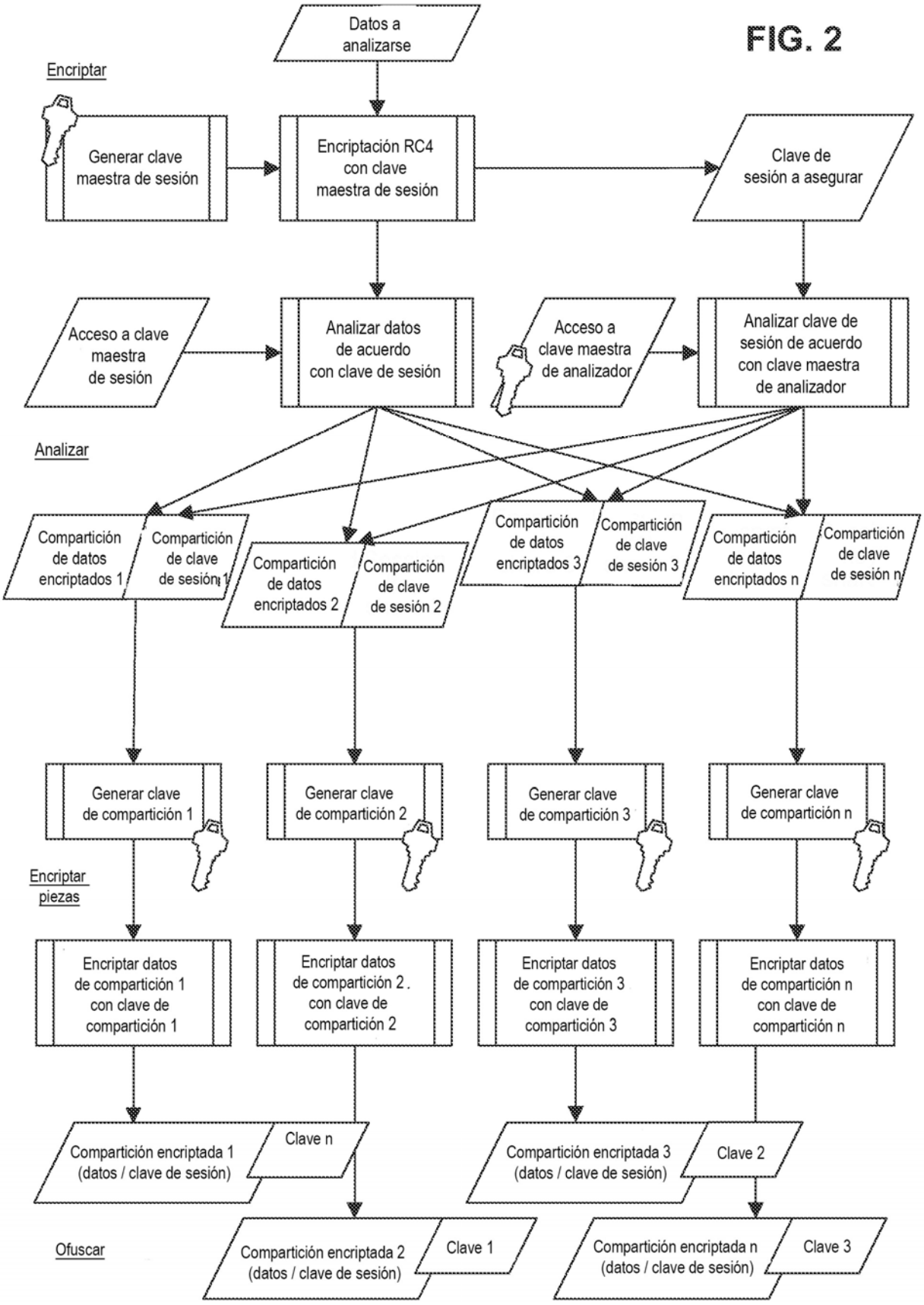

Datos a analizarse
Encriptar
Generar clave maestra de sesión
Encriptación RC4 con clave maestra de sesión
Clave de sesión a asegurar
Acceso a clave maestra de sesión
Analizar datos de acuerdo con clave de sesión
Acceso a clave maestra de analizador
Analizar clave de sesión de acuerdo con clave maestra de analizador
Analizar
Compartición de datos encriptados 1
Compartición de clave de sesión 1
Compartición de datos encriptados 2
Compartición de clave de sesión 2
Compartición de datos encriptados 3
Compartición de clave de sesión 3
Compartición de datos encriptados n
Compartición de clave de sesión n
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar piezas
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / clave de sesión)
Clave n
Compartición encriptada 3 (datos / clave de sesión)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / clave de sesión)
Clave 1
Compartición encriptada n (datos / clave de sesión)
Clave 3

FIG. 3

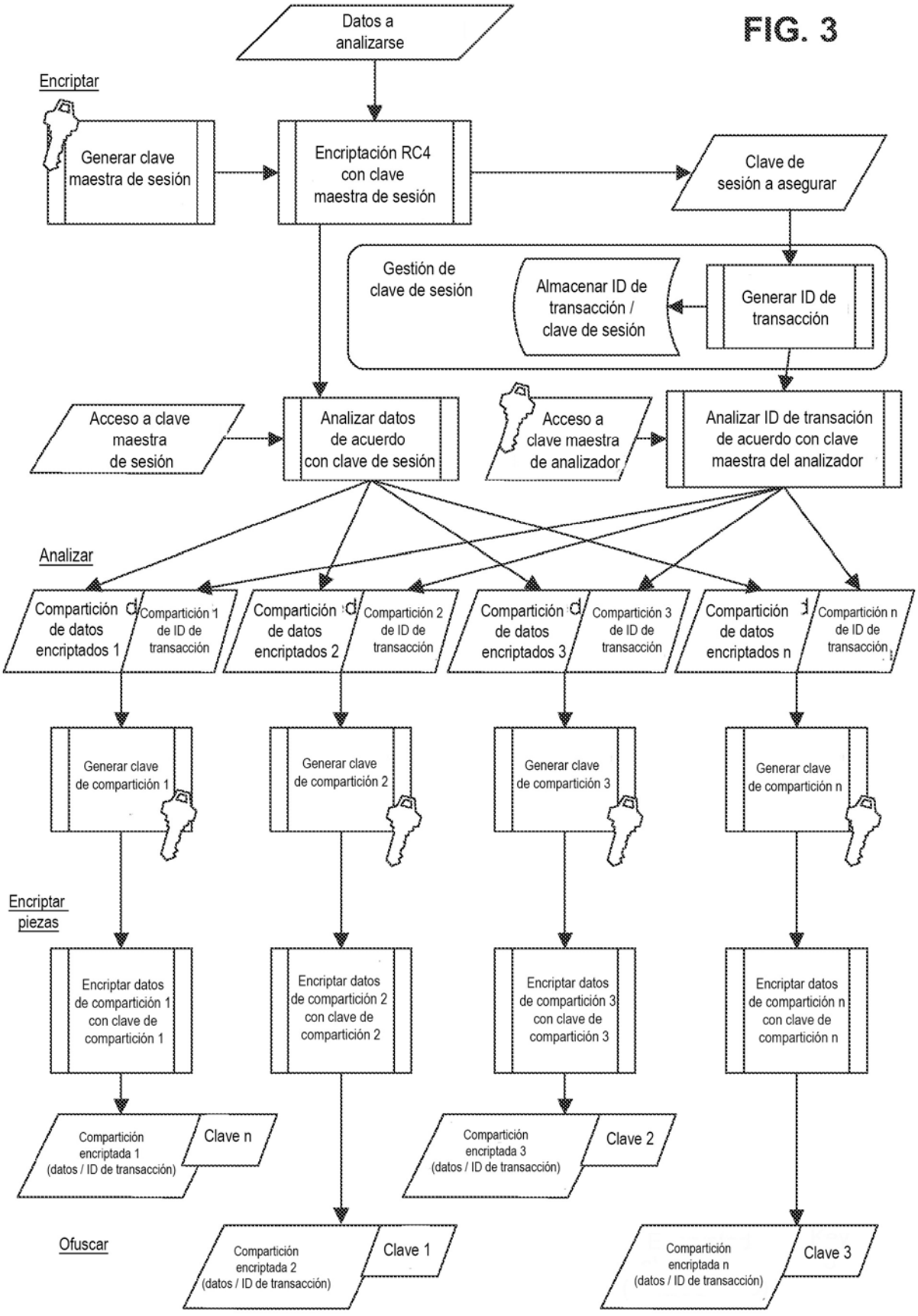
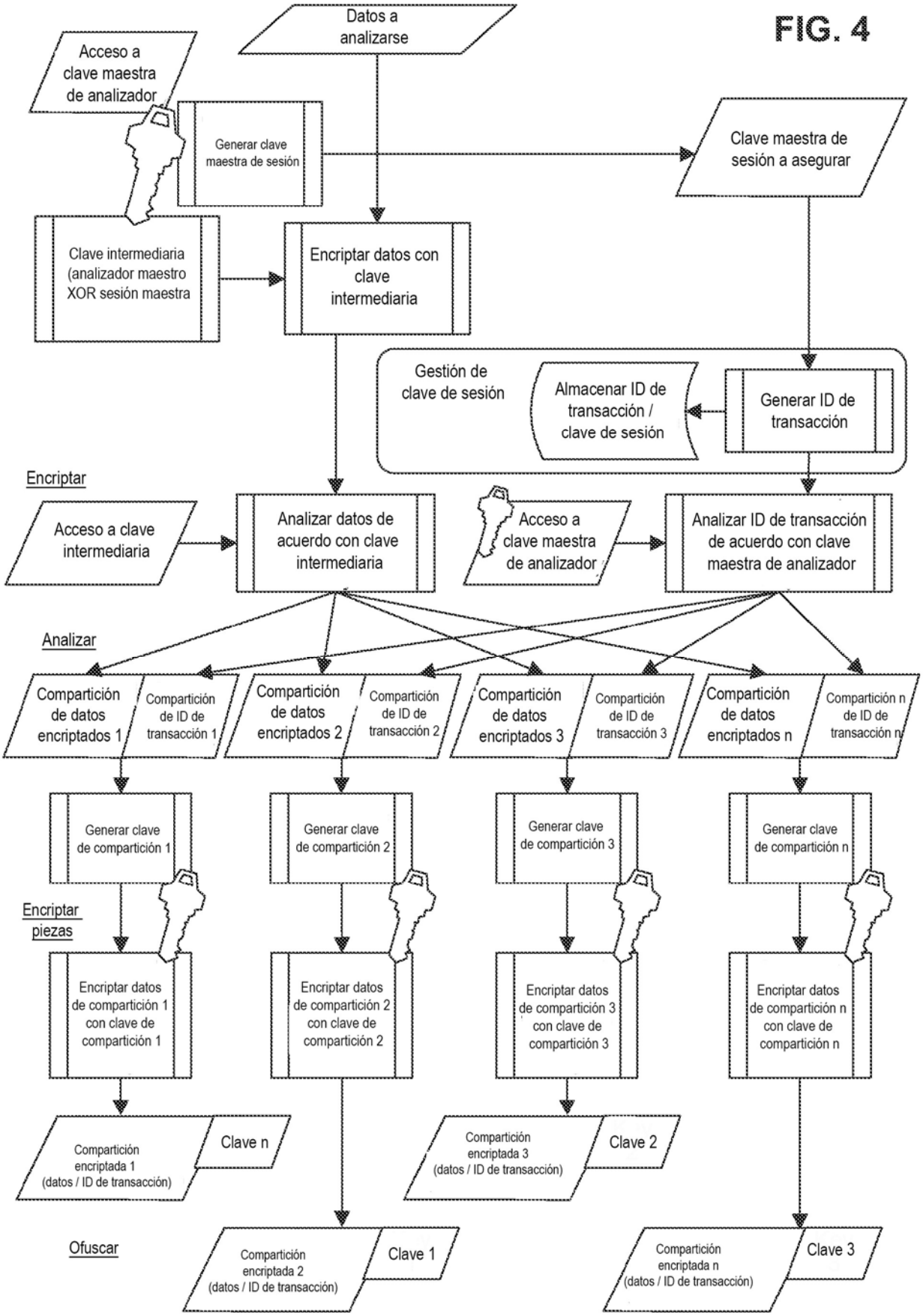

Datos a analizarse
Encriptar
Generar clave maestra de sesión
Encriptación RC4 con clave maestra de sesión
Clave de sesión a asegurar
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar ID de transacción
Acceso a clave maestra de sesión
Analizar datos de acuerdo con clave de sesión
Acceso a clave maestra de analizador
Analizar ID de transación de acuerdo con clave maestra del analizador
Analizar
Compartición de datos encriptados 1
Compartición 1 de ID de transacción
Compartición de datos encriptados 2
Compartición 2 de ID de transacción
Compartición de datos encriptados 3
Compartición 3 de ID de transacción
Compartición de datos encriptados n
Compartición n de ID de transacción
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar piezas
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / ID de transacción)
Clave n
Compartición encriptada 3 (datos / ID de transacción)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / ID de transacción)
Clave 1
Compartición encriptada n (datos / ID de transacción)
Clave 3

FIG. 4


Datos a analizarse
Acceso a clave maestra de analizador
Generar clave maestra de sesión
Clave maestra de sesión a asegurar
Clave intermediaria (analizador maestro XOR sesión maestra
Encriptar datos con clave intermediaria
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar ID de transacción
Encriptar
Acceso a clave intermediaria
Analizar datos de acuerdo con clave intermediaria
Acceso a clave maestra de analizador
Analizar ID de transacción de acuerdo con clave maestra de analizador
Analizar
Compartición de datos encriptados 1
Compartición de ID de transacción 1
Compartición de datos encriptados 2
Compartición de ID de transacción 2
Compartición de datos encriptados 3
Compartición de ID de transacción 3
Compartición de datos encriptados n
Compartición n de ID de transacción n
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar piezas
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / ID de transacción)
Clave n
Compartición encriptada 3 (datos / ID de transacción)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / ID de transacción)
Clave 1
Compartición encriptada n (datos / ID de transacción)
Clave 3

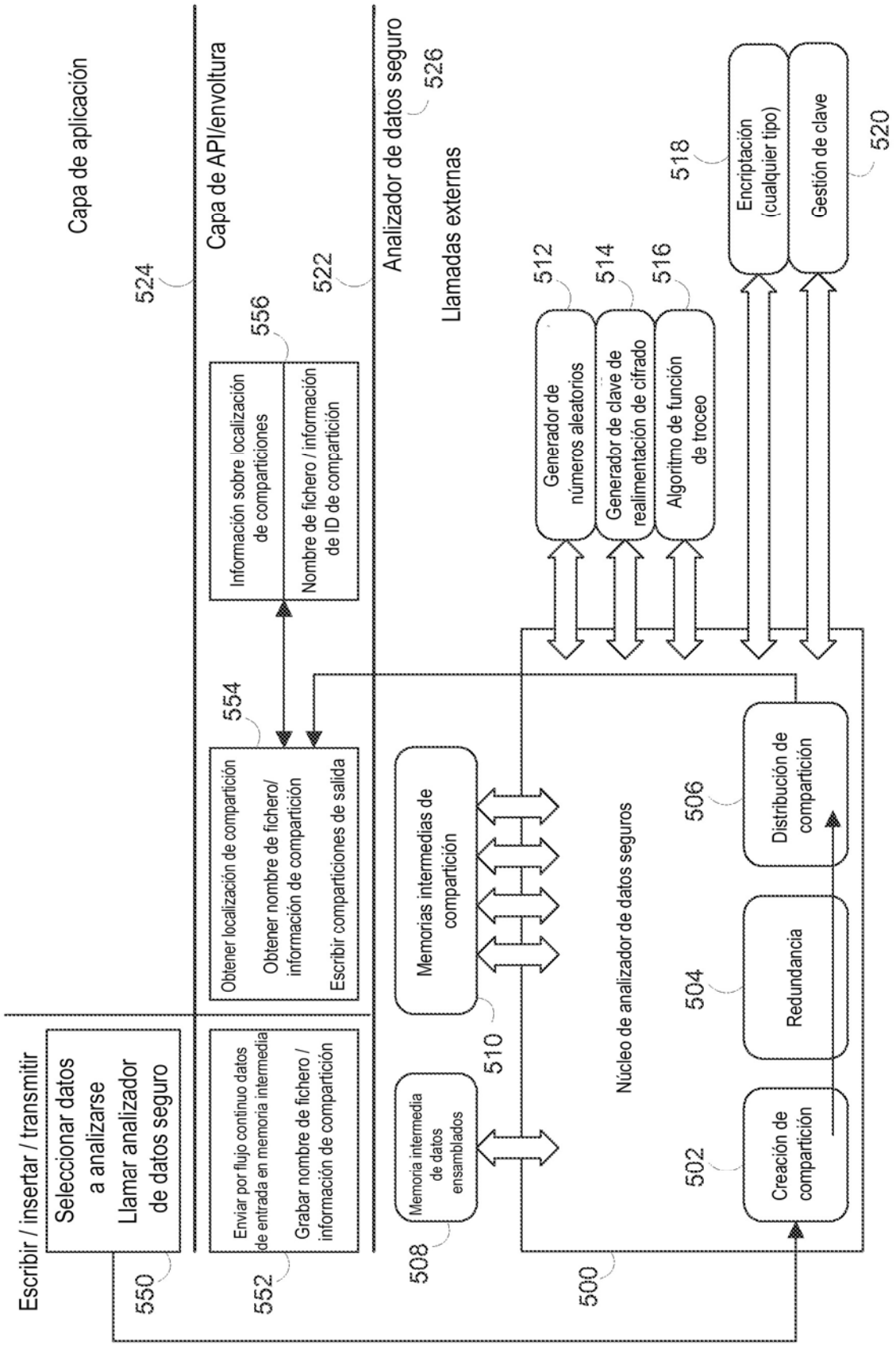

Escribir / insertar / transmitir
Capa de aplicación
Capa de API/envoltura
Analizador de datos seguro
526
Llamadas externas
524
522
556
554
550
552
500
508
510
502
504
506
512
514
516
518
520
Seleccionar datos a analizarse
Llamar analizador de datos seguro
Enviar por flujo continuo datos de entrada en memoria intermedia
Grabar nombre de fichero / información de compartición
Información sobre localización de compartición
Nombre de fichero / información de ID de compartición
Obtener localización de compartición
Obtener nombre de fichero/ información de compartición
Escribir compartición de salida
Memoria intermedia de datos ensamblados
Memorias intermedias de compartición
Núcleo de analizador de datos seguros
Creación de compartición
Redundancia
Distribución de compartición
Generador de números aleatorios
Generador de clave de realimentación de cifrado
Algoritmo de función de troceo
Encriptación (cualquier tipo)
Gestión de clave

FIG. 5

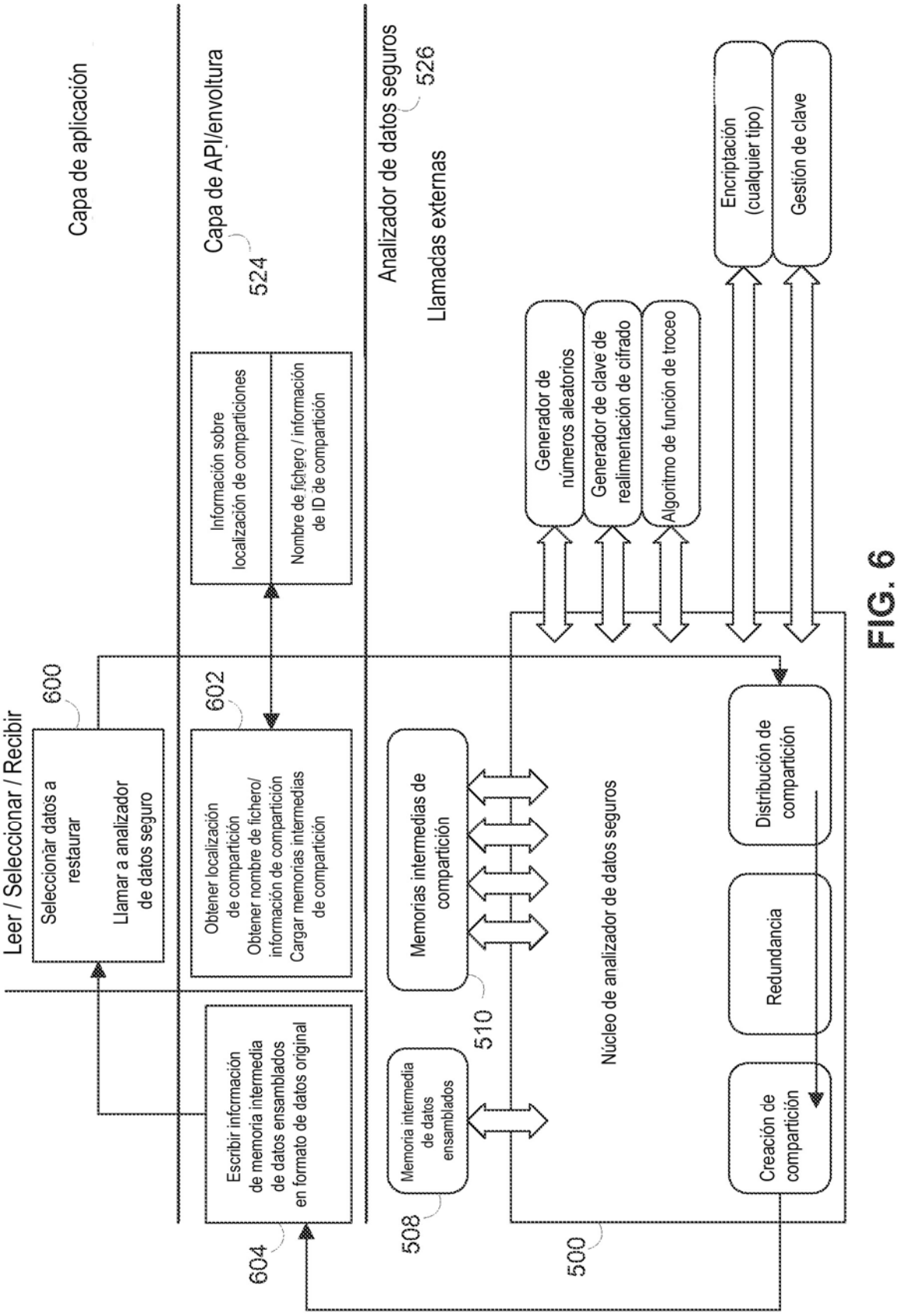

Capa de aplicación
Capa de API/envoltura
524
Analizador de datos seguros
526
Llamadas externas
Leer / Seleccionar / Recibir
600
Seleccionar datos a restaurar
Llamar a analizador de datos seguro
602
Obtener localización de compartición
Obtener nombre de fichero/ información de compartición
Cargar memorias intermedias de compartición
Información sobre localización de compartición
Nombre de fichero / información de ID de compartición
Generador de números aleatorios
Generador de clave de realimentación de cifrado
Algoritmo de función de troceo
Encriptación (cualquier tipo)
Gestión de clave
Memorias intermedias de compartición
510
Memoria intermedia de datos ensamblados
508
Escribir información de memoria intermedia de datos ensamblados en formato de datos original
604
Núcleo de analizador de datos seguros
500
Distribución de compartición
Redundancia
Creación de compartición

FIG. 6

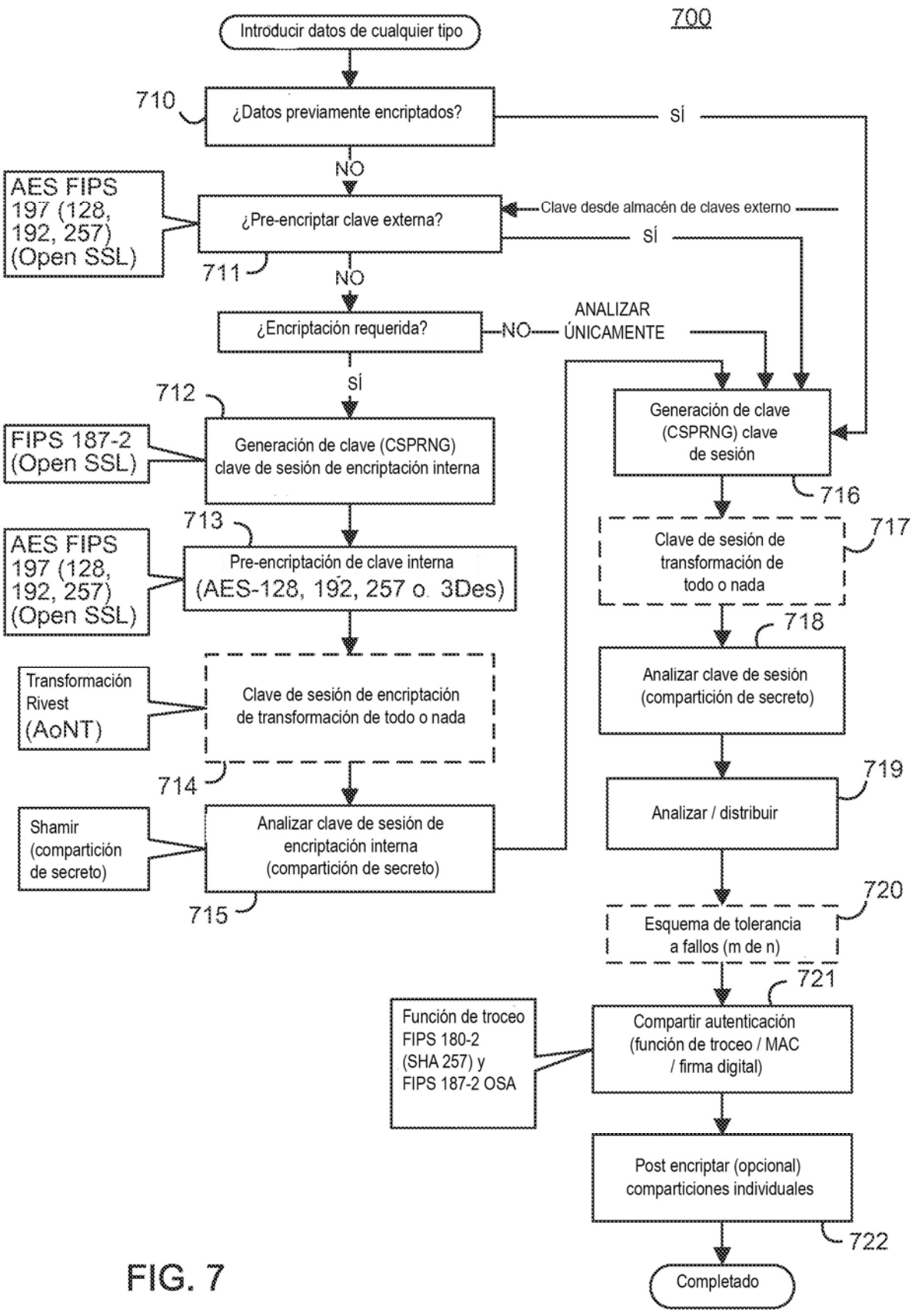

700
Introducir datos de cualquier tipo
710
¿Datos previamente encriptados?
SÍ
NO
AES FIPS 197 (128, 192, 257) (Open SSL)
¿Pre-encriptar clave externa?
Clave desde almacén de claves externo
SÍ
711
NO
¿Encriptación requerida?
NO
ANALIZAR ÚNICAMENTE
SÍ
712
FIPS 187-2 (Open SSL)
Generación de clave (CSPRNG) clave de sesión de encriptación interna
713
AES FIPS 197 (128, 192, 257) (Open SSL)
Pre-encriptación de clave interna (AES-128, 192, 257 o 3Des)
Transformación Rivest (AoNT)
Clave de sesión de encriptación de transformación de todo o nada
714
Shamir (compartición de secreto)
Analizar clave de sesión de encriptación interna (compartición de secreto)
715
Generación de clave (CSPRNG) clave de sesión
716
Clave de sesión de transformación de todo o nada
717
718
Analizar clave de sesión (compartición de secreto)
719
Analizar / distribuir
720
Esquema de tolerancia a fallos (m de n)
721
Función de troceo FIPS 180-2 (SHA 257) y FIPS 187-2 OSA
Compartir autenticación (función de troceo / MAC / firma digital)
Post encriptar (opcional) comparticiones individuales
722
Completado

FIG. 7

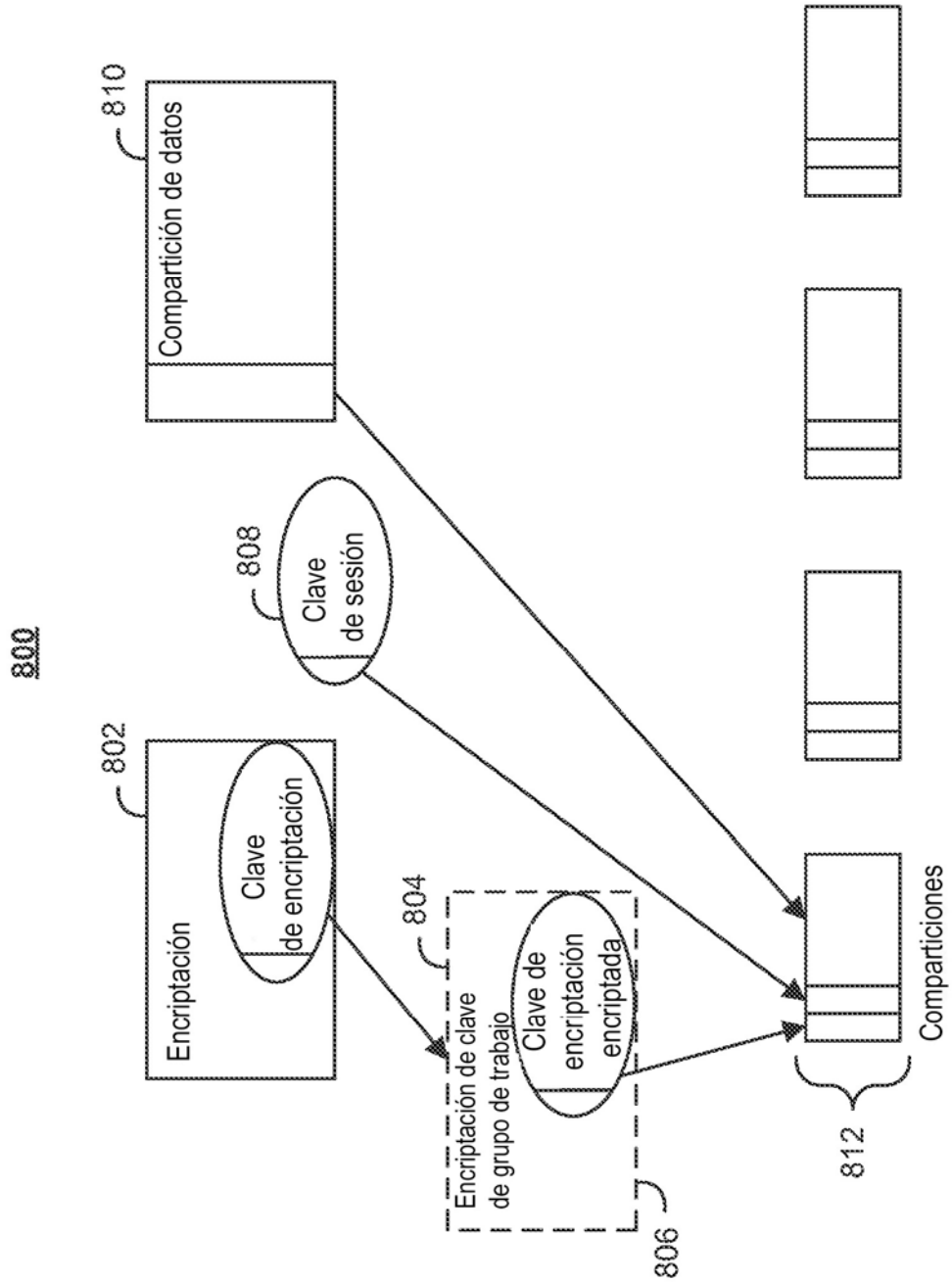

800
802
Encriptación
Clave de encriptación
804
Encriptación de clave de grupo de trabajo
Clave de encriptación encriptada
806
808
Clave de sesión
810
Compartición de datos
812
Compartición

FIG. 8

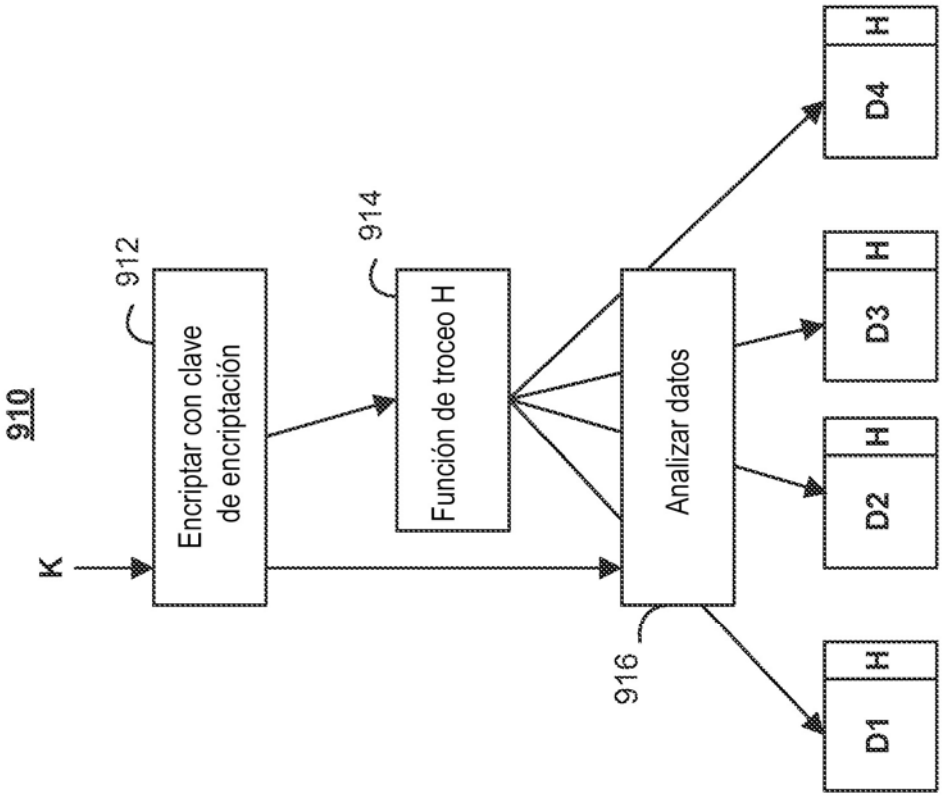

910
K
912
Encriptar con clave de encriptación
914
Función de troceo H
916
Analizar datos
D1
H
D2
H
D3
H
D4
H

FIG. 9B

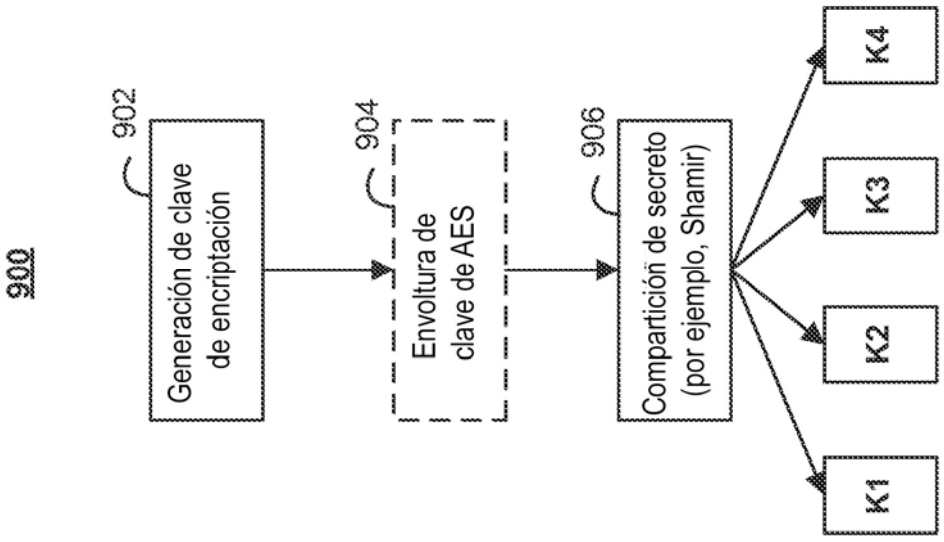

900
902
Generación de clave de encriptación
904
Envoltura de clave de AES
906
Compartición de secreto (por ejemplo, Shamir)
K1
K2
K3
K4

FIG. 9A

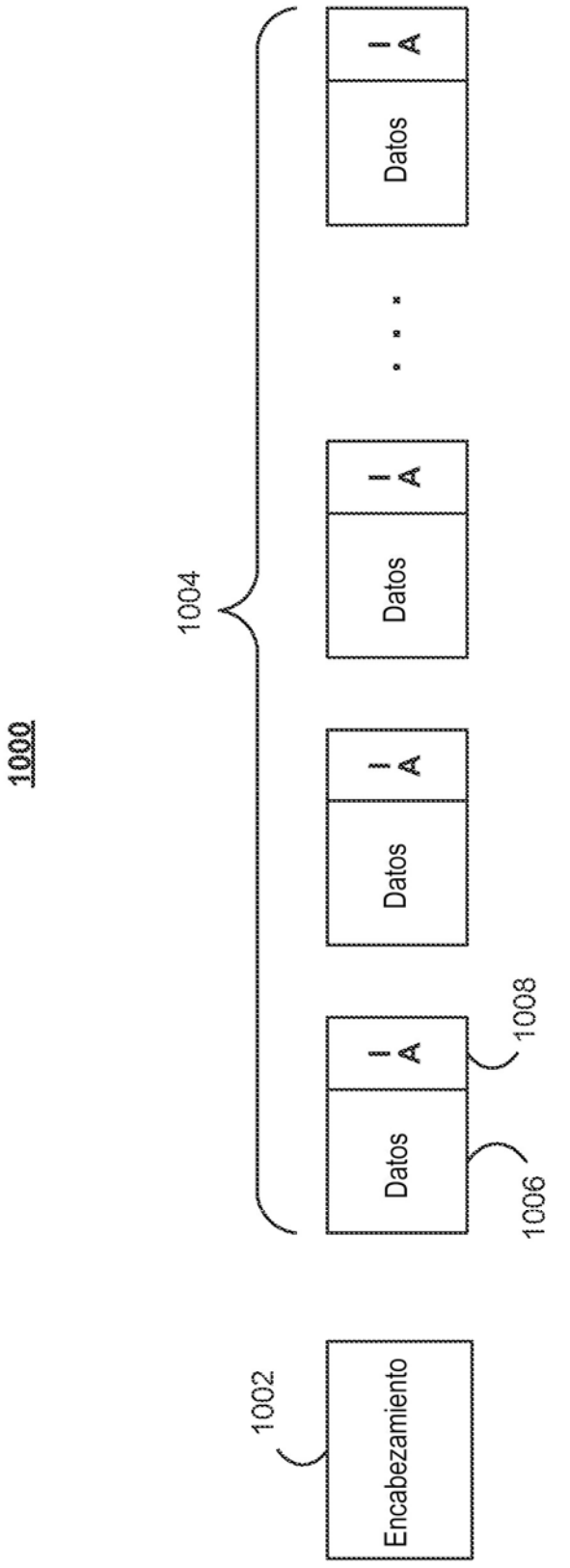


FIG. 10

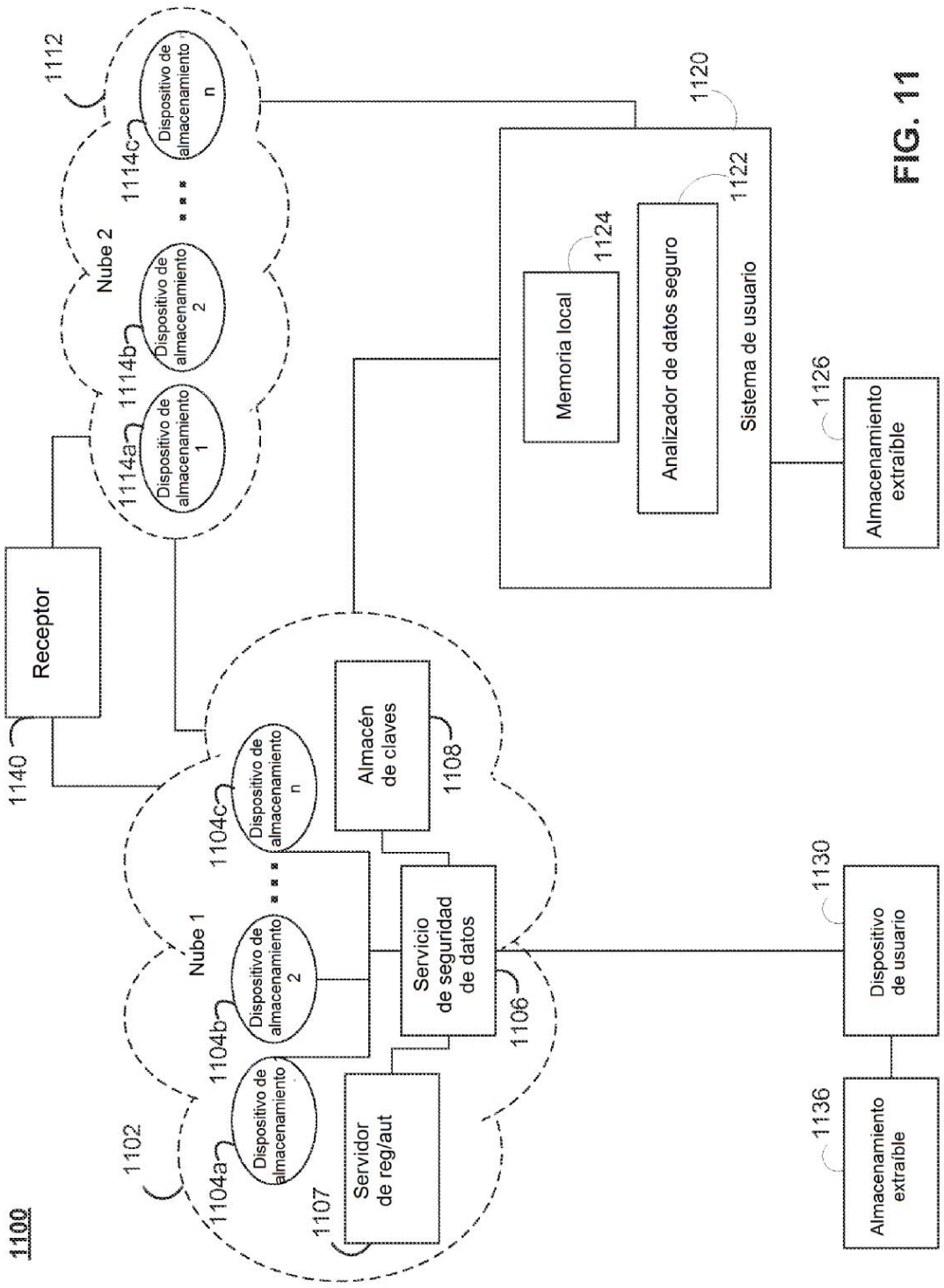

1100
1102
Nube 1
1104a
Dispositivo de almacenamiento 1
1104b
Dispositivo de almacenamiento 2
1104c
Dispositivo de almacenamiento n
1107
Servidor de reg/aut
1106
Servicio de seguridad de datos
1108
Almacén de claves
1140
Receptor
1112
Nube 2
1114a
Dispositivo de almacenamiento 1
1114b
Dispositivo de almacenamiento 2
1114c
Dispositivo de almacenamiento n
1120
Sistema de usuario
1122
Analizador de datos seguro
1124
Memoria local
1126
Almacenamiento extraíble
1130
Dispositivo de usuario
1136
Almacenamiento extraíble

FIG. 11

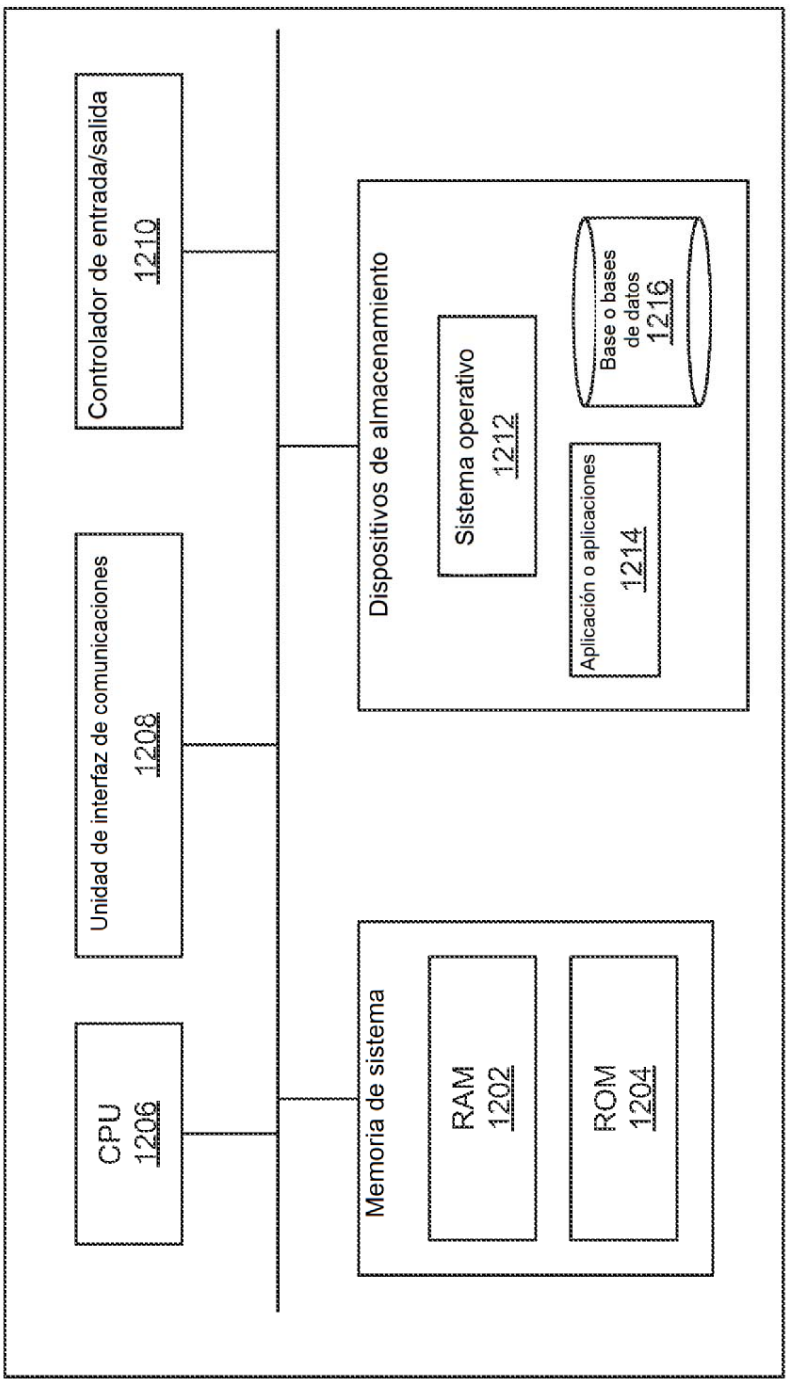

1200
CPU
1206
Unidad de interfaz de comunicaciones
1208
Controlador de entrada/salida
1210
Memoria de sistema
RAM
1202
ROM
1204
Dispositivos de almacenamiento
Sistema operativo
1212
Aplicación o aplicaciones
1214
Base o bases de datos
1216

FIG. 12

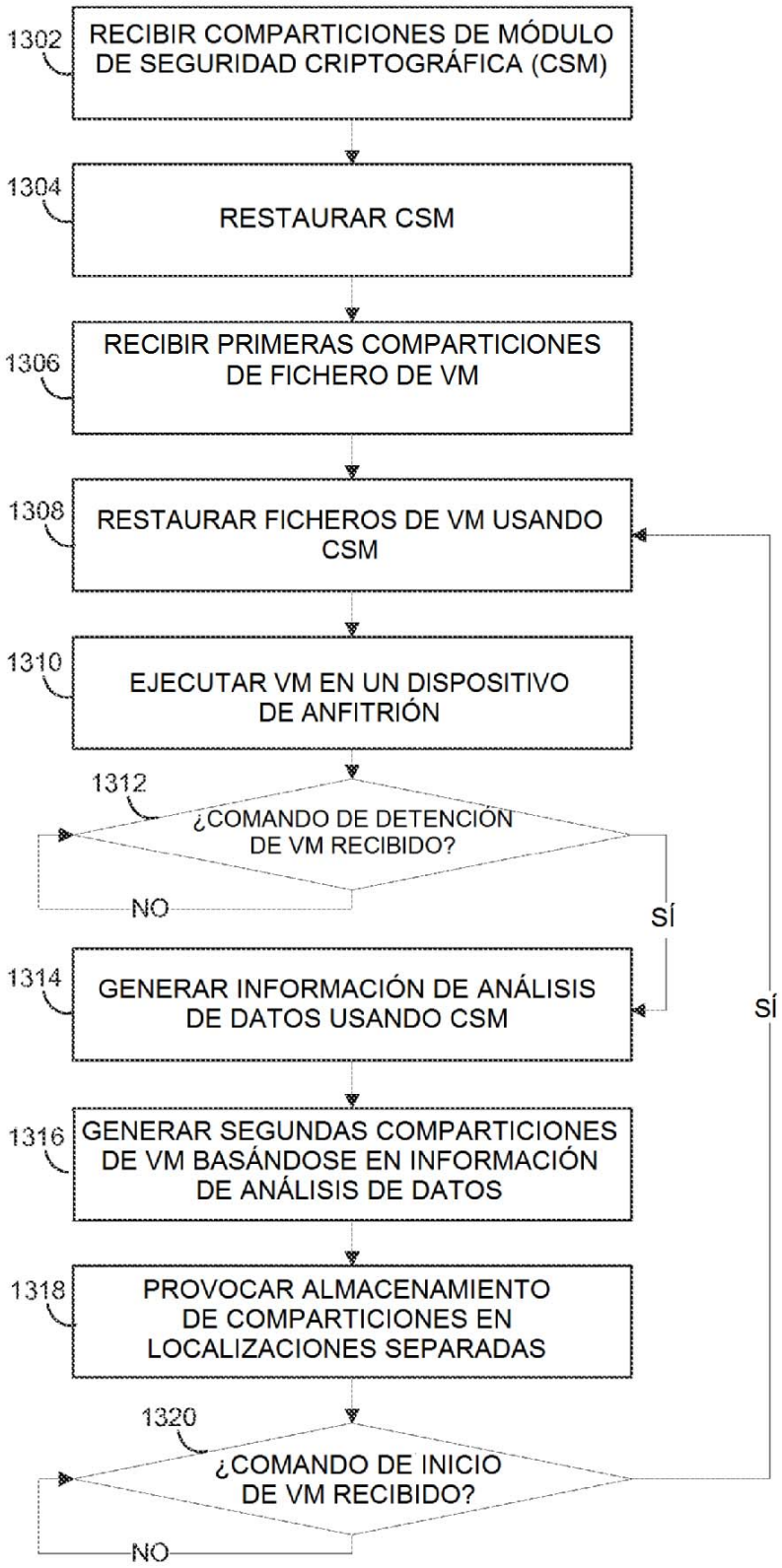

1302
RECIBIR COMPARTICIONES DE MÓDULO DE SEGURIDAD CRIPTOGRÁFICA (CSM)
1304
RESTAURAR CSM
1306
RECIBIR PRIMERAS COMPARTICIONES DE FICHERO DE VM
1308
RESTAURAR FICHEROS DE VM USANDO CSM
1310
EJECUTAR VM EN UN DISPOSITIVO DE ANFITRIÓN
1312
¿COMANDO DE DETENCIÓN DE VM RECIBIDO?
NO
SÍ
1314
GENERAR INFORMACIÓN DE ANÁLISIS DE DATOS USANDO CSM
1316
GENERAR SEGUNDAS COMPARTICIONES DE VM BASÁNDOSE EN INFORMACIÓN DE ANÁLISIS DE DATOS
1318
PROVOCAR ALMACENAMIENTO DE COMPARTICIONES EN LOCALIZACIONES SEPARADAS
1320
¿COMANDO DE INICIO DE VM RECIBIDO?
NO
SÍ

FIG. 13

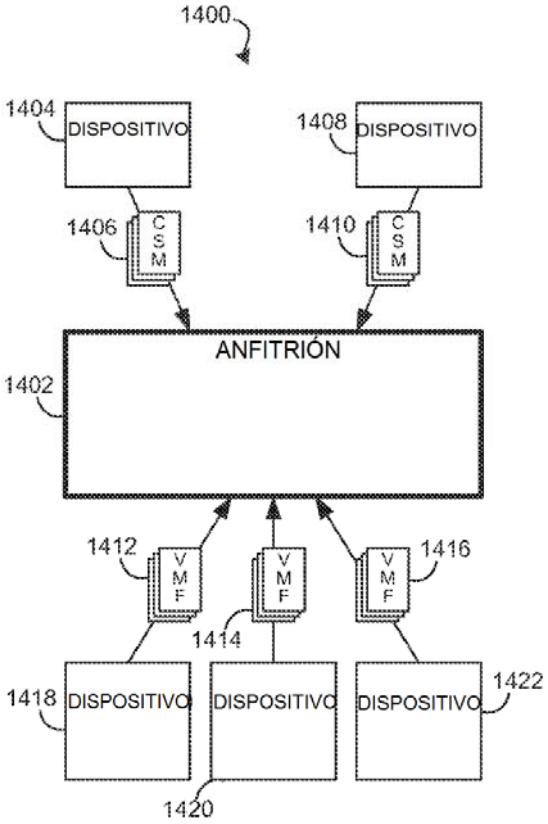


FIG. 14A

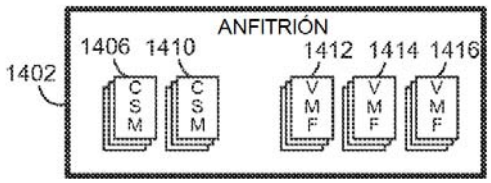


FIG. 14B

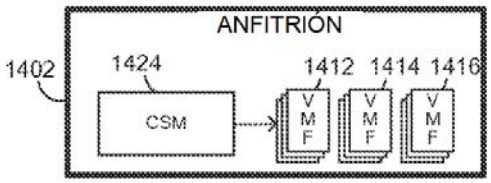


FIG. 14C

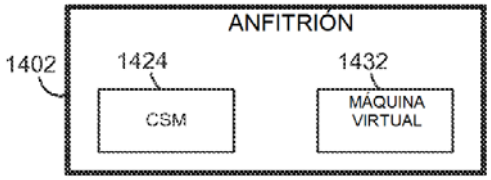


FIG. 14D

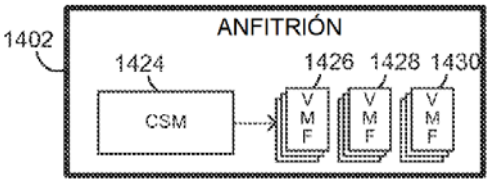


FIG. 14E

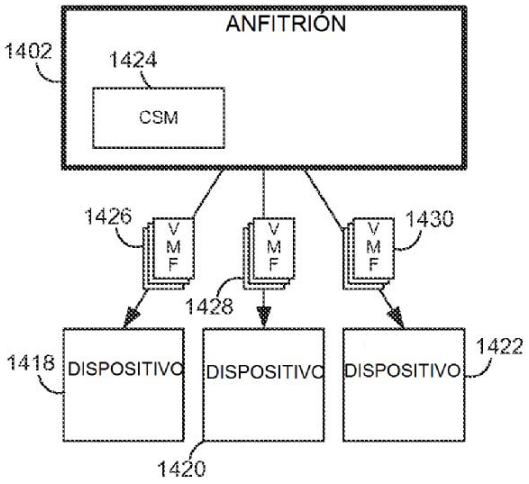


FIG. 14F

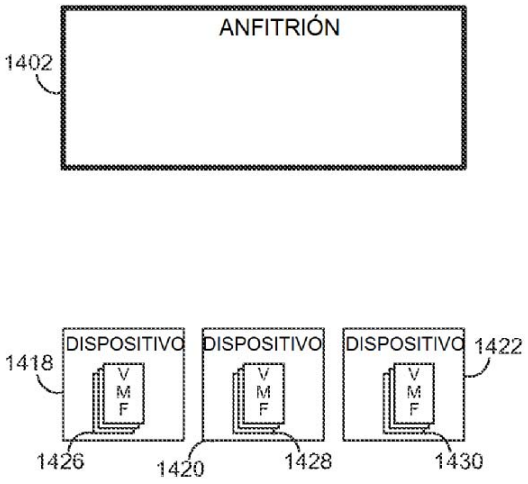


FIG. 14G

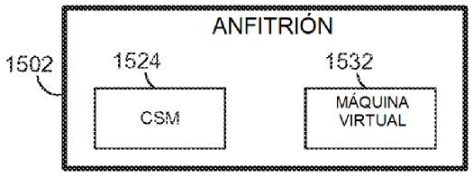


FIG. 15A

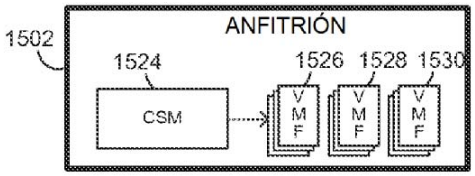


FIG. 15B

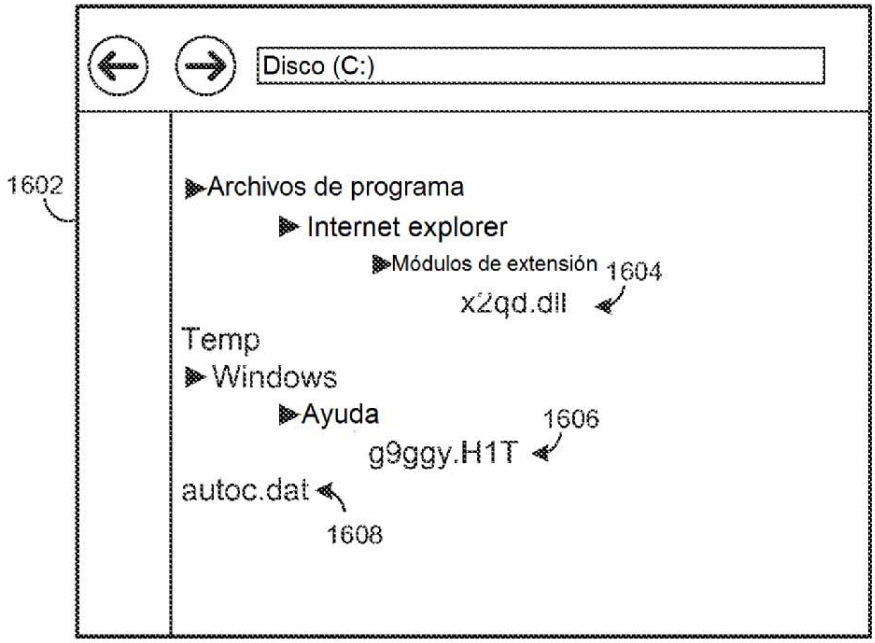

Disco (C:)
1602
Archivos de programa
Internet explorer
Módulos de extensión
1604
x2qd.dll
Temp
Windows
Ayuda
1606
g9ggy.H1T
autoc.dat
1608

FIG. 16

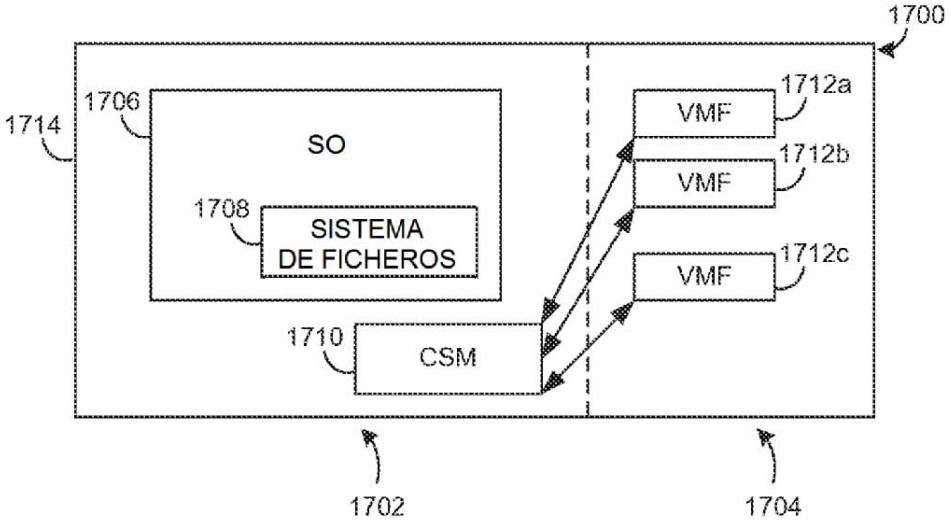

1700
1706
1714
SO
1708
SISTEMA
DE FICHEROS
1710
CSM
1712a
VMF
1712b
VMF
1712c
VMF
1702
1704

FIG. 17

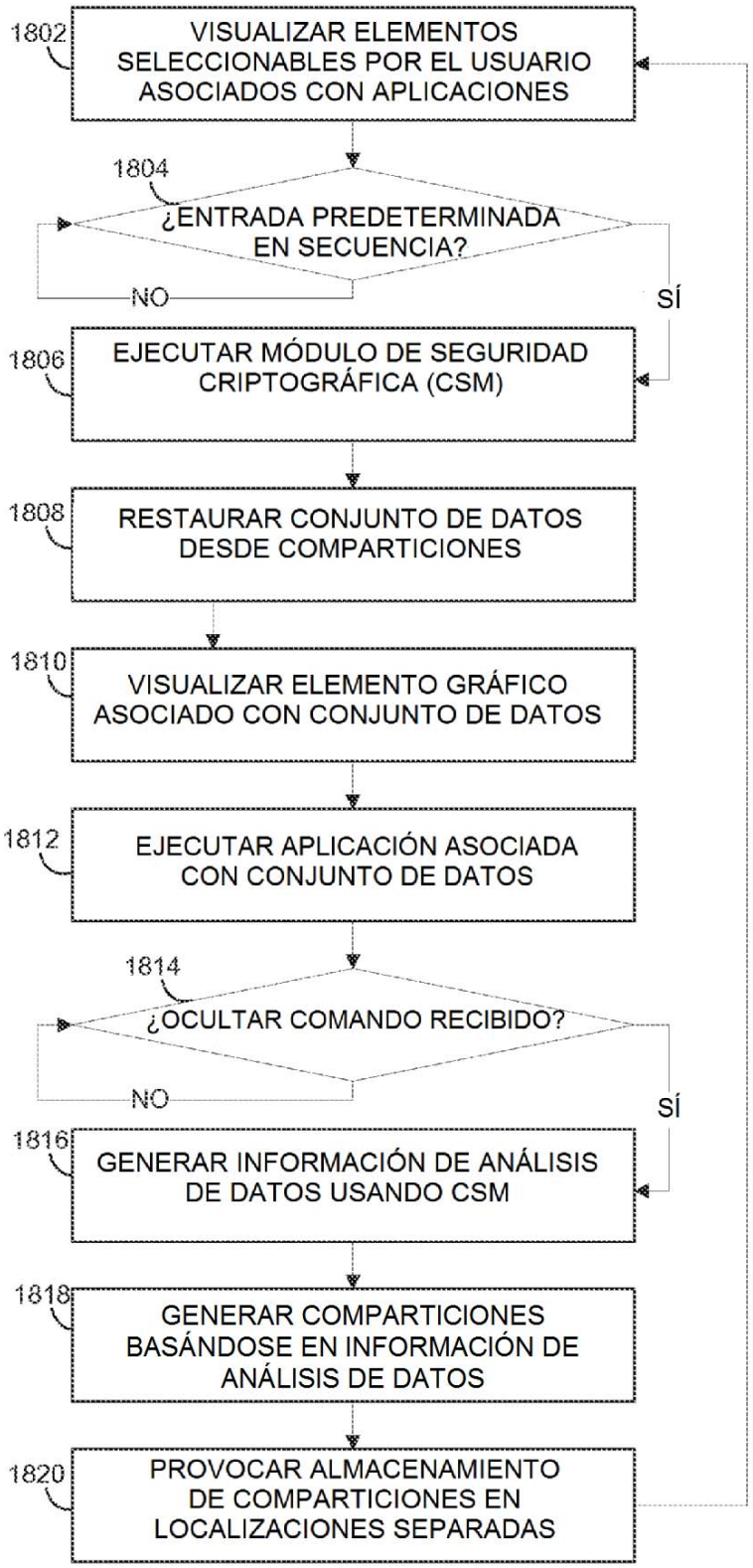

1802
VISUALIZAR ELEMENTOS SELECCIONABLES POR EL USUARIO ASOCIADOS CON APLICACIONES
1804
¿ENTRADA PREDETERMINADA EN SECUENCIA?
NO
SÍ
1806
EJECUTAR MÓDULO DE SEGURIDAD CRIPTOGRÁFICA (CSM)
1808
RESTAURAR CONJUNTO DE DATOS DESDE COMPARTICIONES
1810
VISUALIZAR ELEMENTO GRÁFICO ASOCIADO CON CONJUNTO DE DATOS
1812
EJECUTAR APLICACIÓN ASOCIADA CON CONJUNTO DE DATOS
1814
¿OCULTAR COMANDO RECIBIDO?
NO
SÍ
1816
GENERAR INFORMACIÓN DE ANÁLISIS DE DATOS USANDO CSM
1818
GENERAR COMPARTICIONES BASÁNDOSE EN INFORMACIÓN DE ANÁLISIS DE DATOS
1820
PROVOCAR ALMACENAMIENTO DE COMPARTICIONES EN LOCALIZACIONES SEPARADAS

FIG. 18

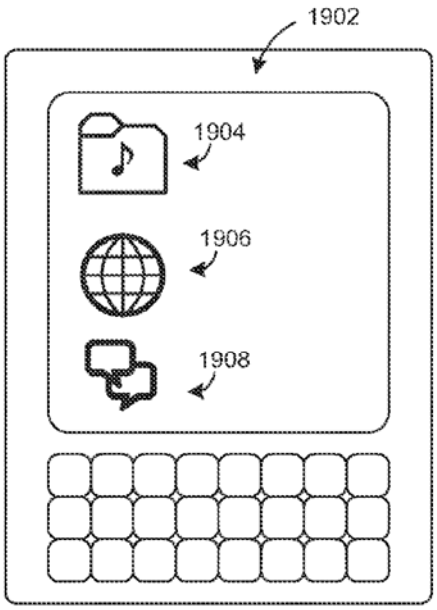


FIG. 19A

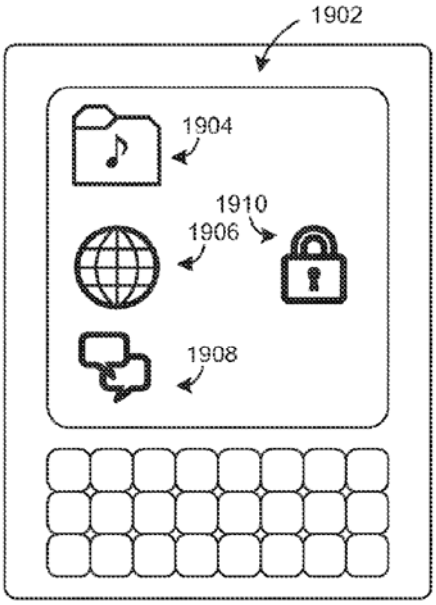


FIG. 19B

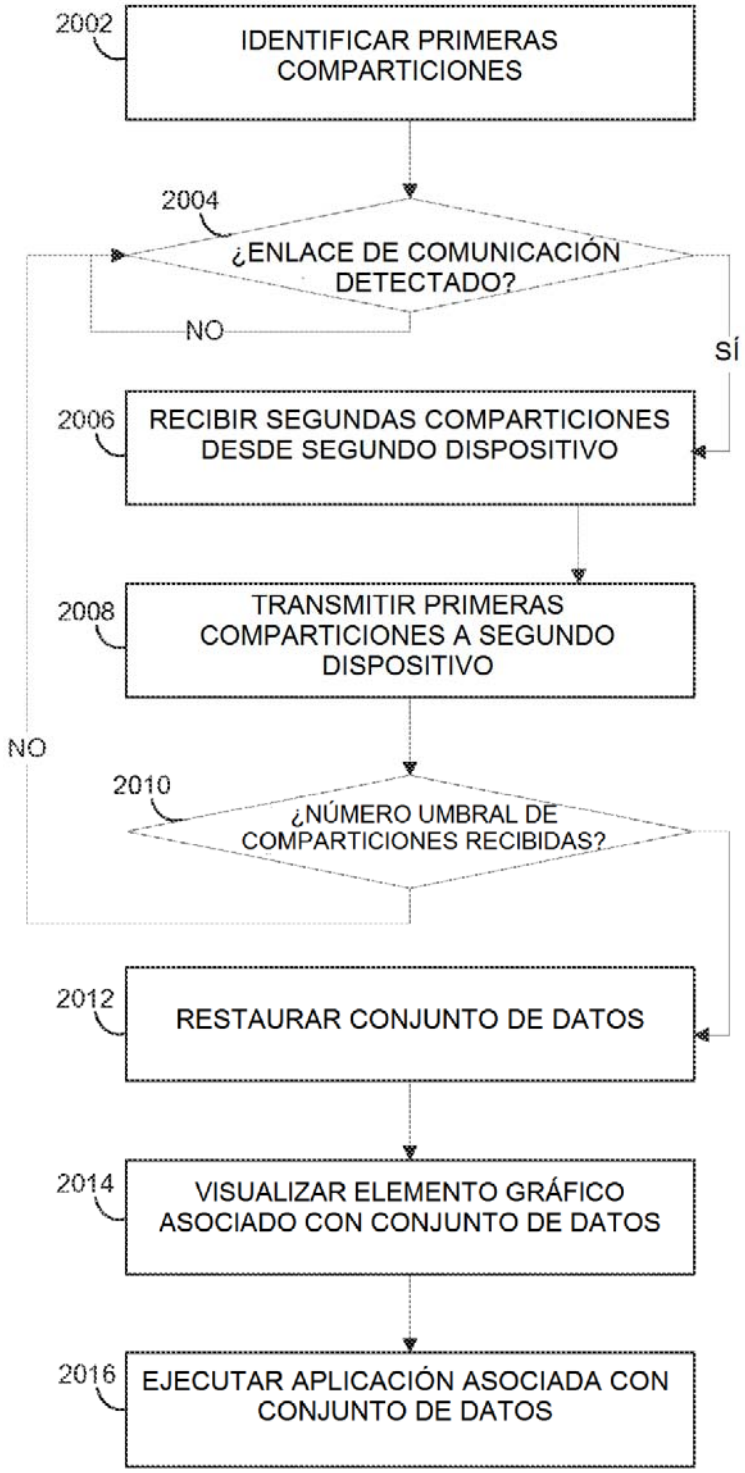

2002
IDENTIFICAR PRIMERAS COMPARTICIONES
2004
¿ENLACE DE COMUNICACIÓN DETECTADO?
NO
SÍ
2006
RECIBIR SEGUNDAS COMPARTICIONES DESDE SEGUNDO DISPOSITIVO
2008
TRANSMITIR PRIMERAS COMPARTICIONES A SEGUNDO DISPOSITIVO
NO
2010
¿NÚMERO UMBRAL DE COMPARTICIONES RECIBIDAS?
2012
RESTAURAR CONJUNTO DE DATOS
2014
VISUALIZAR ELEMENTO GRÁFICO ASOCIADO CON CONJUNTO DE DATOS
2016
EJECUTAR APLICACIÓN ASOCIADA CON CONJUNTO DE DATOS

FIG. 20

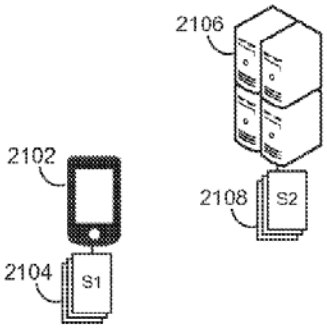


FIG. 21A

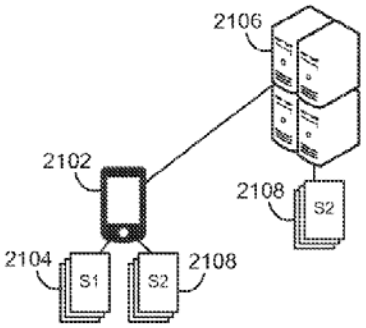


FIG. 21B

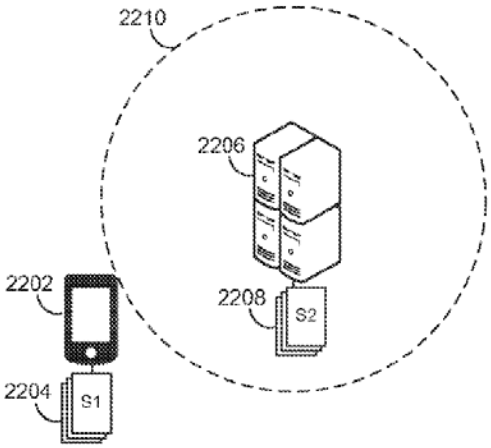


FIG. 22A

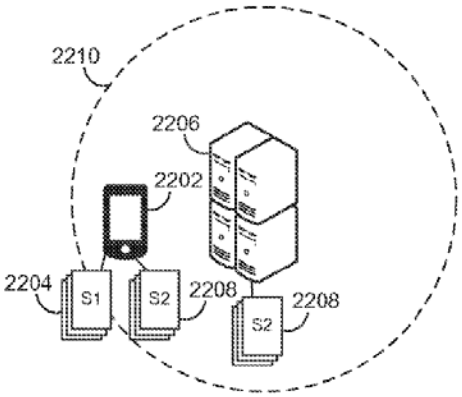


FIG. 22B

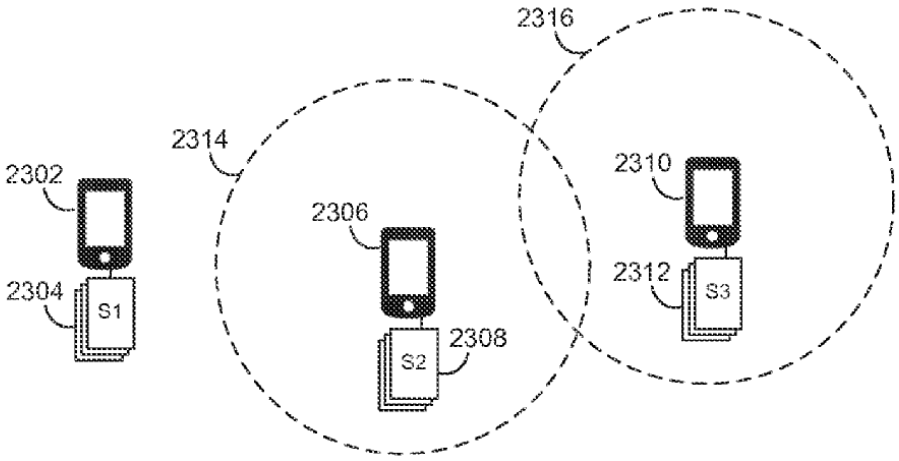


FIG. 23A

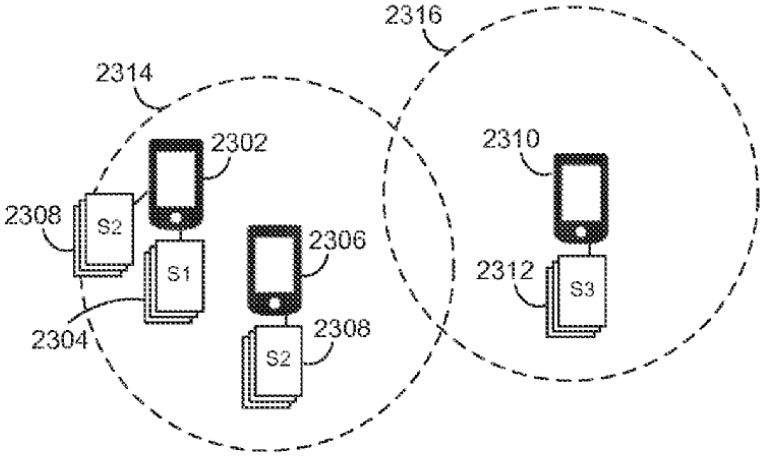


FIG. 23B

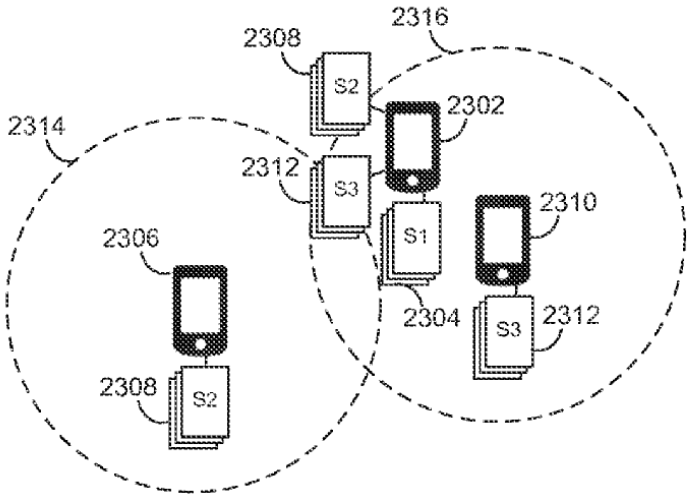


FIG. 23C

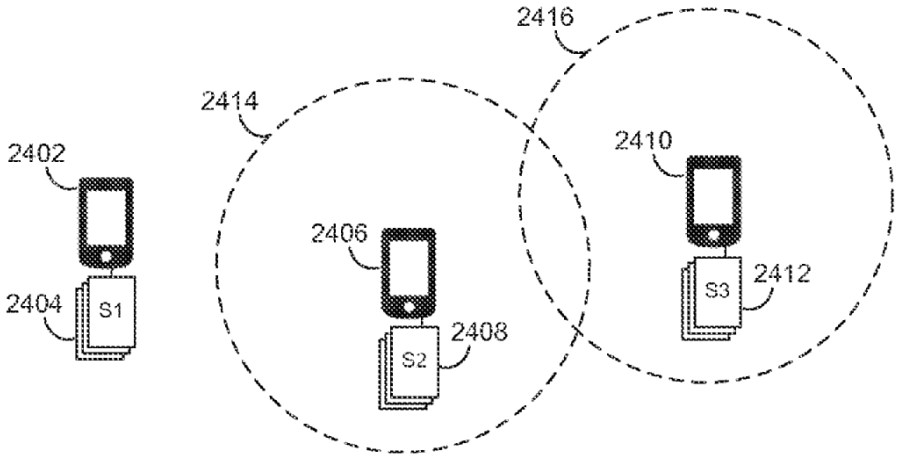


FIG. 24A

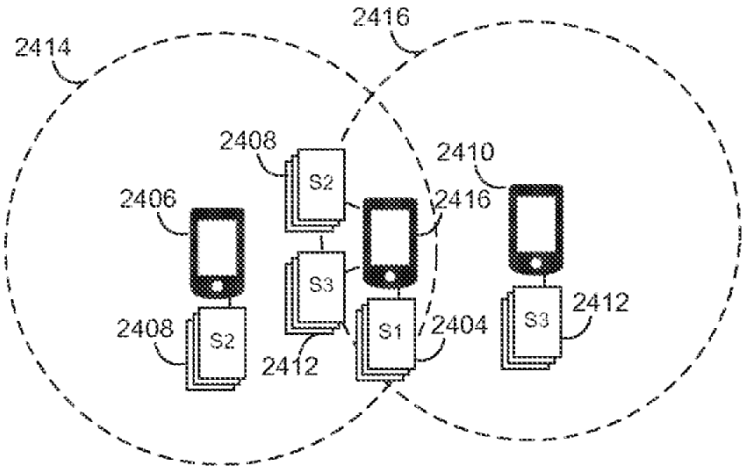


FIG. 24B

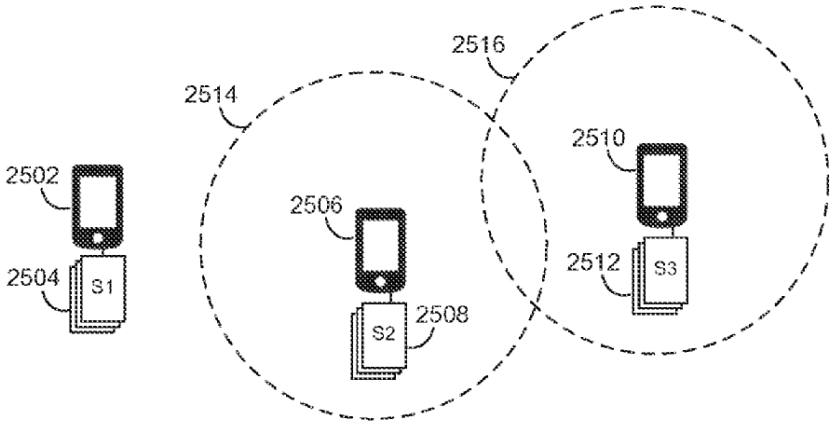


FIG. 25A

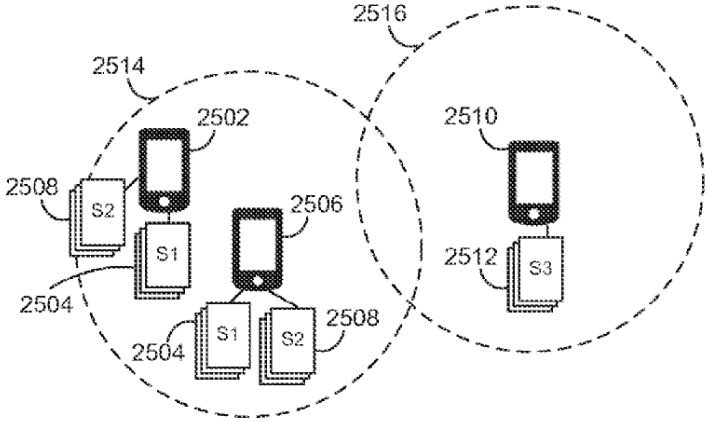


FIG. 25B

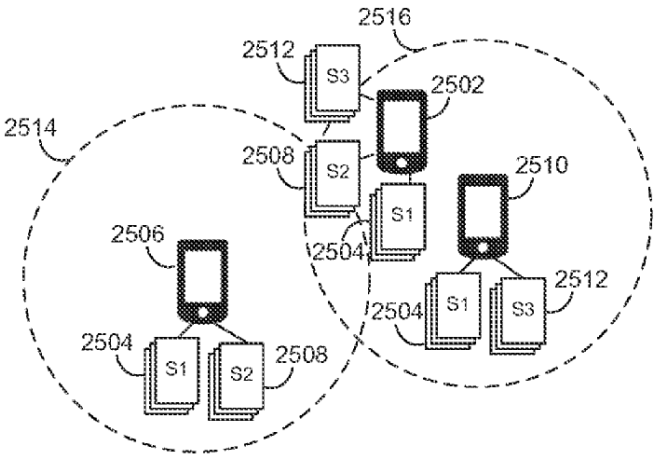


FIG. 25C

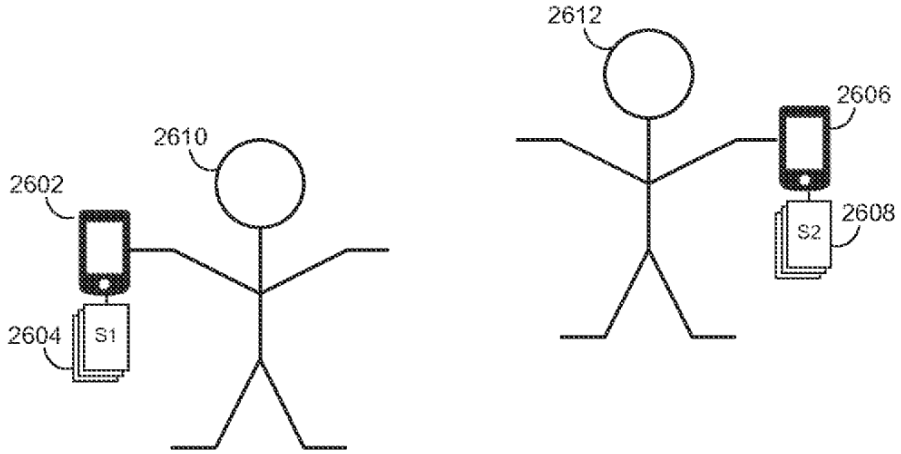


FIG. 26A

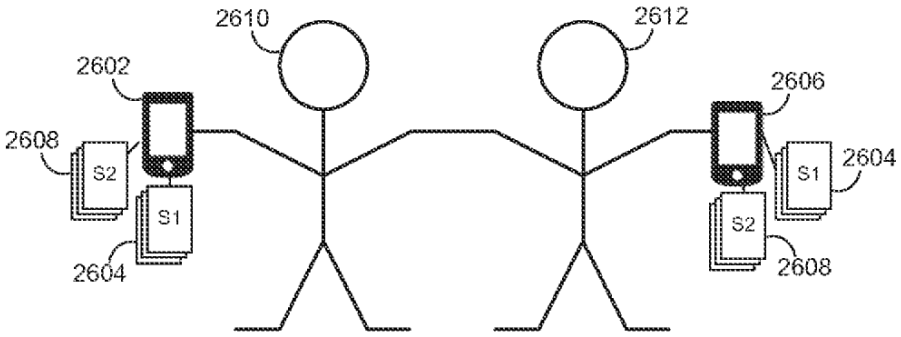


FIG. 26B