(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 616 920**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/85 (2013.01)
G06F 17/30 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.12.2013 PCT/US2013/073736**

(87) Fecha y número de publicación internacional: **03.07.2014 WO2014105395**

(96) Fecha de presentación y número de la solicitud europea: **06.12.2013 E 13856061 (0)**

(97) Fecha y número de publicación de la concesión europea: **23.11.2016 EP 2929481**

(54) Título: **Plataforma de base de datos de nube segura**

(30) Prioridad:

07.12.2012 US 201213708396

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.06.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

RAMAMURTHY, RAVISHANKAR;
EGURO, KENNETH H. y
VENKATESAN, RAMARATHNAM

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Plataforma de base de datos de nube segura

Antecedentes

En muchas aplicaciones de computación resulta deseable mantener los datos seguros. Por ejemplo, en un entorno médico, las regulaciones requieren que se tomen medidas de seguridad para impedir que puedan acceder a los datos del paciente terceros no autorizados. Si datos financieros, tal como los números de tarjetas de crédito o los números de la seguridad social de los clientes de una empresa, fueran obtenidos por terceros malintencionados, podrían ocurrir grandes pérdidas financieras.

Para proteger los datos, las empresas pueden mantener sus propios sistemas de ordenador usando diversas técnicas de seguridad para impedir el acceso no autorizado a los datos. La empresa puede usar técnicas físicas y electrónicas para controlar el acceso a datos seguros. Una aproximación alternativa para proteger datos, incluso aunque no se pueda excluir el acceso a los datos en todos los casos, consiste en encriptar los datos cuando se almacenan en el sistema de ordenador.

Los datos que han sido encriptados (o procesados de otra manera de tal modo que, incluso aunque un tercero no autorizado acceda a los datos, el tercero no puede determinar el significado de los datos), se denomina a veces “texto cifrado”. En una red corporativa, los datos confidenciales pueden ser almacenados como texto cifrado, excepto cuando están siendo realmente procesados. Controlando la información de seguridad, tal como las claves de cifrado, que pueden convertir texto cifrado en “texto sin cifrar”, la seguridad de los datos puede ser mantenida limitando la existencia de datos en texto sin cifrar salvo en configuraciones altamente restrictivas que sean seguras.

Más recientemente, los datos están siendo almacenados o procesados en “la nube”. Los proveedores del servicio de nube (en vez de las empresas que tienen datos para procesar), proporcionan recursos de computación, incluyendo el procesamiento y el almacenaje de base de datos. Los proveedores del servicio de nube hacen que los recursos de computación estén disponibles para los clientes, cada uno de los cuales establece un acuerdo de nivel de servicio (SLA) con el proveedor del servicio de nube, para tener acceso a un determinado nivel de recursos de computación. Las empresas acceden a esos recursos presentando trabajos a través de Internet para su procesamiento en los recursos de computación “alquilados” en el proveedor del servicio de nube.

Las técnicas tradicionales para mantener la seguridad de los datos en el entorno de la nube, no se aplican. Aunque los datos puedan ser transmitidos a través de Internet como texto cifrado, una vez que son recibidos por el proveedor del servicio de nube, es decir, para muchas operaciones, son convertidos a texto sin cifrar. Como resultado, los empleados del proveedor del servicio de nube, quienes están inherentemente fuera de la empresa, tienen acceso a los datos de texto sin cifrar y posiblemente a la información de seguridad para convertir el texto cifrado a texto sin cifrar.

El documento US 2007/174271 A1 divulga un sistema de base de datos con un procesador frontal que recibe consultas desde una aplicación del cliente a través de una conexión de SSL encriptada, un expedidor que divide una consulta recibida en sub-consultas, y procesadores finales que reciben las sub-consultas expedidas y llevan a cabo operaciones criptográficas sobre los datos almacenados en la base de datos en respuesta a dichas sub-consultas.

Compendio

Las operaciones de base de datos seguras pueden ser proporcionadas en un entorno de computación de nube mediante la provisión de un componente de hardware que realiza funciones de seguridad sobre datos en base a información de seguridad única para un abonado. Como resultado, las posiciones físicas en las que resultan accesibles los datos de texto sin cifrar, pueden ser limitadas. Los datos pueden estar disponibles solamente de modo interno en un nodo de base de datos del entorno de nube o, en algunas realizaciones, pueden estar solamente disponibles en el interior del dispositivo de seguridad. En algunas realizaciones, el dispositivo de seguridad tiene un factor de forma que está adaptado para su inserción en una ranura estándar en un servidor de base de datos de tal modo que la comunicación de datos de texto sin cifrar está limitada a los buses internos del servidor.

Un dispositivo de seguridad de este tipo puede recibir comandos de base de datos que estén encriptados a través de Internet o de otra red pública. El dispositivo de seguridad puede desencriptar los comandos y suministrarlos a un servidor de base de datos para su procesamiento. Cuando la operación es una consulta, los resultados de la consulta pueden ser devueltos al dispositivo de seguridad donde son encriptados para su transmisión a través de la red pública.

En otras realizaciones, el servidor de base de datos puede recibir comandos que estén en un formato encriptado diferente del usado para la comunicación a través de la red pública. En una realización de ese tipo, el dispositivo de seguridad puede traducir consultas desde el formato encriptado usado para la comunicación a través de la red pública, hasta el usado por el servidor de base de datos. Los resultados generados por el servidor de base de datos pueden ser traducidos a la inversa.

En algunas realizaciones, la traducción a la inversa puede incluir realizar porciones del procesamiento de un comando. Esa porción del procesamiento puede incluir una operación de agregación o cualquier otro tipo adecuado de operación. En algunas realizaciones, la traducción del comando puede incluir dividir el comando en subcomandos. Diferentes subcomandos pueden tener diferentes formatos de encriptación. Un subcomando puede ser formateado para su aplicación a una base de datos de texto sin formato, mientras que otra subporción puede ser formateada para su aplicación a una base de datos encriptada.

Lo que antecede es un sumario no limitativo de la invención, la cual se define mediante las reivindicaciones anexas.

Breve descripción de los dibujos

No se pretende que los dibujos que se acompañan estén dibujados a escala. En los dibujos, cada componente idéntico o aproximadamente idéntico que se ilustra en las diversas Figuras, está representado por un mismo número. Por motivos de claridad, puede que no todos los componentes hayan sido etiquetados en cada dibujo. En los dibujos:

La Figura 1 es un croquis de un ejemplo de realización de una plataforma de computación en nube que utiliza un dispositivo de computación segura;

La Figura 2 es un diagrama de bloques funcional de un ejemplo de realización de un nodo de base de datos de nube que incorpora un dispositivo de seguridad;

La Figura 3 es un diagrama de bloques funcional de un segundo ejemplo de realización de un nodo de base de datos de nube que incorpora un dispositivo de seguridad;

La Figura 4 es un diagrama de bloques funcional de un tercer ejemplo de realización de un nodo de base de datos de nube que incorpora un dispositivo de seguridad;

Las Figuras 5A – 5D son ilustraciones esquemáticas de comandos de base de datos que son procesados por medio de un dispositivo de seguridad según se describe en la presente memoria, y

La Figura 6 es un diagrama de bloques funcional de un ejemplo de dispositivo de computación que puede ser usado para implementar algunas realizaciones de la invención.

Descripción detallada

Los inventores han reconocido y apreciado que la utilidad de una plataforma de base de datos de nube puede ser ampliada equipando a la plataforma de base de datos de nube con un dispositivo de seguridad. El dispositivo de seguridad puede servir como interfaz entre una red, a través de la cual un abonado accede a la plataforma de base de datos de nube, y uno o más dispositivos de computación que proporcionan almacenaje de datos y recursos de recuperación dentro de la plataforma de base de datos de nube para ese abonado.

El dispositivo de seguridad puede estar dotado de información criptográfica única para un abonado, tal como una clave privada. Este aprovisionamiento puede ser llevado a cabo, al menos en parte, por el abonado o por algún tercero de confianza. Como resultado, incluso el operador de la plataforma de base de datos de la nube puede no tener acceso a la información criptográfica. La información criptográfica puede ser usada para desencriptar consultas planteadas por el abonado y/o para encriptar datos a devolver al abonado en respuesta a una consulta.

El dispositivo de seguridad puede estar configurado para actuar a modo de interfaz entre una red insegura a través de la cual se intercambiarán las preguntas y las respuestas con un abonado. El dispositivo de seguridad puede interconectar con dispositivos de computación dentro de la plataforma de base de datos de la nube en la que puede ser ejecutada una consulta.

La seguridad puede ser mantenida a pesar del hecho de que el dispositivo de computación segura esté en posesión y/o bajo el control, de un operador de la plataforma de base de datos de la nube. Se puede usar una o más técnicas para mantener la seguridad. En algunas realizaciones, se puede mantener la seguridad ubicando el dispositivo de seguridad en el interior de un área segura en proximidad cercana a un procesador que ejecute consultas dentro de la plataforma de base de datos de la nube. Aunque las versiones de texto sin cifrar de la consulta y los datos generados en respuesta a la consulta pueden ser intercambiados entre el dispositivo de seguridad y el procesador, el hecho de tener esos dispositivos una proximidad cercana en un área segura puede hacer que resulte difícil acceder a esa información. En algunas realizaciones, el dispositivo de seguridad puede estar instalado en la misma envolvente física que aloja el procesador, y puede estar acoplado al procesador a través de un bus interno, tal como un bus de PCI, del dispositivo de computación. Las dificultades que se presentan a un individuo no autorizado para acceder a la información interna a un dispositivo de computación del interior de una plataforma de base de datos de la nube, incrementan adicionalmente la seguridad.

En algunas realizaciones, la plataforma de base de datos de la nube puede almacenar datos en un formato encriptado. De ese modo, incluso aunque un individuo no autorizado acceda a información que pasa entre el

dispositivo de seguridad y el procesador que procesa una consulta, la información puede estar encriptada. Esta información puede estar encriptada de una manera diferente a la usada para transmitir información a través de una red insegura. Por esta razón, incluso aunque un individuo no autorizado acceda a la información de esta manera, la seguridad no necesita verse comprometida.

En una realización de ese tipo, el dispositivo de seguridad puede recibir una consulta encriptada a través de una red pública. El dispositivo de seguridad puede desencriptar la información y traducirla a una segunda forma para su aplicación a un dispositivo de computación en el interior de la plataforma de base de datos de la nube que está configurada para ejecutar la consulta en una base de datos encriptada. Los resultados de tal consulta pueden ser devueltos al dispositivo de seguridad para su procesamiento y transmisión al abonado a través de una red pública.

En algunas realizaciones, el procesamiento en el interior del dispositivo de seguridad puede entrañar descifrar los resultados encriptados. Alternativamente o adicionalmente, el procesamiento en el interior del dispositivo de seguridad puede incluir operaciones sobre los resultados desencriptados. Como resultado, los resultados de la consulta procesada pueden ser retornados a un abonado, reduciendo la cantidad de información comunicada a través de la red pública y/o una cantidad de procesamiento requerida en un dispositivo de computación del cliente usado por el abonado a efectos de tener acceso a los resultados de la consulta.

Como ejemplo específico de procesamiento que puede ser llevado a cabo dentro de un dispositivo de seguridad, el dispositivo de seguridad puede realizar una función de agregación. Ejemplos de funciones de agregación incluyen sumar valores y registros en una base de datos que se emparejen con la consulta o contar el número de registros de la base de datos que se emparejan con la consulta.

En algunas realizaciones, una plataforma de base de datos de nube puede almacenar datos parcialmente como texto sin cifrar y parcialmente como datos encriptados. El procesamiento en el dispositivo de seguridad puede entrañar seccionar la consulta de tal modo que se puedan aplicar porciones a un procesador que tendrá acceso a datos de texto sin cifrar mientras que otras porciones se aplican a un proceso que podrá acceder a los datos protegidos. El procesamiento de los resultados con el dispositivo de seguridad puede entrañar combinar los resultados generados a partir de los datos de texto sin cifrar con los generados a partir de las páginas encriptadas. Tal procesamiento puede incluir desencriptar las páginas encriptadas de tal modo que puedan ser combinadas con otras páginas de texto sin cifrar.

Una plataforma de base de datos de nube de ese tipo puede ser usada para almacenar, y acceder a, cualquier tipo adecuado de datos. Por ejemplo, se puede usar una plataforma de base de datos de nube segura para habilitar el procesamiento de información médica sensible acerca de personas. En este ejemplo, la información médica, en caso de que forme parte de una consulta o forme parte de un resultado retornado como respuesta para ejecutar la consulta, puede ser transmitida como texto cifrado. Incluso aunque esta transmisión ocurra a través de una red pública, la seguridad de los datos en tránsito puede ser mantenida mediante la encriptación de los datos.

Tras la recepción de una consulta en la plataforma de base de datos de la nube, esta consulta puede ser desencriptada dentro del dispositivo de seguridad. Se puede mantener la seguridad de los datos usando una o más de las técnicas descritas en la presente memoria. Se debe apreciar que procesar información sanitaria es solamente un ejemplo del procesamiento que puede ser llevado a cabo en una plataforma de computación en la nube mientras se mantiene la seguridad de los datos. Una plataforma, según se describe en la presente memoria, puede ser usada para cualquier procesamiento de datos adecuado. En algunas realizaciones, el dispositivo de seguridad puede ser configurable para realizar operaciones según sean especificadas por un abonado al que haya sido asignado el dispositivo de seguridad, y esas operaciones pueden generar datos para un procesamiento adicional en la nube o para encriptación y transmisión al abonado.

En algunas realizaciones, el dispositivo de seguridad puede ser implementado con medios de seguridad físicos que impidan el acceso a los datos de texto sin cifrar que sean procesados en el interior del dispositivo como parte del funcionamiento normal del dispositivo de computación segura. La construcción física del dispositivo de seguridad puede frustrar, o al menos obstaculizar significativamente, la actividad maliciosa con la que se pretenda tener acceso a los datos de texto sin cifrar restringiendo el acceso a los datos de texto sin cifrar y/o a la información de seguridad usada para el procesamiento seguro en el interior del dispositivo sin modificaciones físicas en el dispositivo. Si se solicita la modificación física del dispositivo para el acceso no autorizado, ese acceso no autorizado puede ser fácilmente detectado y se pueden tomar medidas correctoras para mantener la seguridad.

Por consiguiente, en algunas realizaciones, el dispositivo de seguridad puede tener una arquitectura tal que los datos de texto sin cifrar solamente estén disponibles en el interior de un dispositivo semiconductor dentro del dispositivo de seguridad. Se pueden emplear técnicas conocidas para la construcción de esos dispositivos semiconductores para asegurar que los datos de texto sin cifrar no puedan ser detectados usando tecnología de detección electromagnética, térmica y/u otra tecnología no destructiva. Por ejemplo, una placa metálica de apantallamiento en el empaquetamiento del dispositivo semiconductor y/o una arquitectura que asegure que los conductores que transportan los datos de texto sin cifrar que están encerrados en el interior del dispositivo pueden ser empleados para asegurar que las señales presentes en esos conductores no pueden ser detectadas fácilmente desde fuera del dispositivo semiconductor. Se pueden emplear técnicas conocidas, alternativamente o

adicionalmente, para dificultar la alteración de una operación del dispositivo de seguridad que pudiera conducir a que el dispositivo de seguridad revele la información secreta que éste usa para el procesamiento seguro de datos sensibles. Según otro ejemplo, cualesquiera cables sobre los que puedan aparecer datos de texto sin cifrar fuera del empaquetamiento del dispositivo semiconductor pueden ser encapsulados en epoxi u otro material que tendría que ser físicamente alterado para conseguir el acceso a los datos de texto sin cifrar.

Un dispositivo semiconductor adecuado para implementar un dispositivo de seguridad puede ser un dispositivo lógico programable, tal como una matriz de puerta programable en campo (FPGA). Algunos dispositivos FPGA conocidos incluyen características que facilitan la carga de programación segura, solamente por terceros autorizados. Tales características pueden ser usadas en este caso para permitir que un abonado a una plataforma de base de datos de nube controle los programas ejecutados por el dispositivo de seguridad, incluso aunque el dispositivo de seguridad esté ubicado en las instalaciones de un operador de una plataforma de base de datos de nube. En consecuencia, se puede usar una FPGA sin modificación o, en algunas realizaciones, puede incorporar características adicionalmente a las de un dispositivo de FPGA convencional para soportar funciones adicionales del dispositivo de computación segura.

El dispositivo de seguridad puede emplear una o más técnicas para mantener la seguridad. Tales técnicas pueden entrañar la realización de procesamiento sobre datos de texto sin cifrar sensibles solamente en el interior de los componentes internos del dispositivo de seguridad de tal modo que, incluso un administrador de la plataforma de la base de datos de la nube no tenga acceso a los datos sensibles, de texto sin cifrar.

En realizaciones en las que el dispositivo de seguridad es programable, la seguridad puede ser mantenida mediante la verificación de instrucciones para programar el dispositivo con anterioridad a configurar el dispositivo con esas instrucciones. Se puede usar cualquier técnica adecuada para verificar un conjunto de instrucciones. En algunas realizaciones, se puede cargar un conjunto de instrucciones en el dispositivo de seguridad en un formato que esté encriptado, firmado criptográficamente o procesado de otro modo con información segura. El dispositivo de seguridad puede realizar procesamiento criptográfico sobre el conjunto de instrucciones para asegurar que éstas fueron procesadas con información de seguridad correspondiente a una fuente de confianza.

En algunas realizaciones, se pueden procesar diferentes tipos de información de forma diferente para mantener la seguridad. En algunas realizaciones, el dispositivo de seguridad puede usar un proceso de arranque para cargar información que se sepa que es segura. El proceso de arranque, por ejemplo, puede estar basado en información de seguridad, tal como una clave, asociada a la fuente de confianza cargada en el dispositivo de computación segura con anterioridad a la operación del dispositivo.

Esta información de seguridad previamente cargada, asociada a una fuente de confianza, puede ser usada por el dispositivo de seguridad para verificar la información proporcionada durante la operación del dispositivo. En algunas realizaciones, la información de seguridad puede ser usada por el dispositivo de seguridad para verificar la información de configuración que configura el dispositivo para realizar operaciones seguras para un abonado específico. Esa información de configuración puede incluir información de seguridad adicional asociada al cliente específico que puede desencriptar y/o encriptar consultas y/o datos asociados a operaciones realizadas para el cliente específico. Alternativamente o adicionalmente, la información de configuración puede incluir un programa de carga, el cual puede cargar un conjunto de instrucciones proporcionadas por el cliente para realizar una operación segura. El programa de carga puede estar adaptado para operar con la información de seguridad asociada al abonado específico de tal modo que la programación del dispositivo de seguridad esté limitada a ese cliente específico.

Una alternativa de ese tipo proporciona una importante flexibilidad en cuanto a la configuración del dispositivo de seguridad, sin acceso a ninguna información segura por el operador de la plataforma de base de datos de la nube. Para permitir que la plataforma de la nube sea usada para un procesamiento seguro para un abonado específico, el operador de la plataforma de base de datos de la nube puede asignar un dispositivo de seguridad para su uso por el abonado específico. A continuación, el dispositivo de seguridad puede interactuar automáticamente con una autoridad de confianza y/o con el abonado específico al que ha sido asignado.

Volviendo a la Figura 1, se ha ilustrado un ejemplo de entorno 100 de computación. El entorno 100 incluye una plataforma 130 de base de datos de nube. Al igual que en un entorno de base de datos de nube convencional, la plataforma 130 de base de datos de la nube incluye recursos de procesamiento y de almacenaje de datos. En este ejemplo, esos recursos de procesamiento han sido ilustrados mediante dispositivos de computación 140 y 150. Los recursos de almacenaje han sido ilustrados mediante bases de datos 142 y 152.

En este ejemplo la base de datos 142 puede ser una base de datos de texto sin cifrar. El dispositivo de computación 140 puede estar configurado con un motor de consulta para realizar consultas de texto sin cifrar respecto a la base de datos 142. La base de datos 152 puede ser una base de datos encriptada, estando algunos de, o todos, los datos almacenados en la base de datos almacenados en forma encriptada. El dispositivo de computación 150 puede estar configurado con un motor de consulta para realizar consultas encriptadas respecto a la base de datos 152.

Como ejemplo específico, la base de datos 152 puede almacenar información sanitaria. Cualquier información

personalmente identificable asociada a información sanitaria puede estar almacenada en la base de datos 152 en forma encriptada. De ese modo, si la base de datos 152 contiene información acerca de un paciente, cuyo nombre es John Smith, el nombre “John Smith” no aparecerá en la base de datos 152. En cambio, aparecerá una forma encriptada del nombre “John Smith”. Como ejemplo la forma encriptada del nombre “John Smith” podría aparecer como “AGF$#º%”. Por consiguiente, un motor de consulta que busque información sobre John Smith, investigaría los registros en la base de datos 152 que contengan el nombre encriptado “AGF$#º%”.

Aunque la Figura 1 muestra solamente dos dispositivos de computación y dos bases de datos en el interior de la plataforma 130 de base de datos de la nube, se apreciará que una plataforma de base de datos de una nube puede tener numerosos dispositivos de computación y numerosas bases de datos que, en operación, estén asignados a suscriptores que solicitan servicios de base de datos de un operador de plataforma 130 de base de datos de nube. Por consiguiente, se apreciará que muchos de los detalles de una plataforma 130 de base de datos de una nube han sido omitidos en la Figura 1 por motivos de simplicidad.

La Figura 1 muestra múltiples abonados 110A, 110B y 110C que pueden acceder a la plataforma 130 de base de datos de la nube a través de dispositivos de computación 112A, 112B y 112C de cliente respectivos. Del mismo modo que en una plataforma de base de datos de nube convencional, los dispositivos de computación del cliente están conectados a la plataforma 130 de base de datos de la nube a través de una red 120, la cual puede ser Internet.

Puesto que la red 120 puede ser una red pública u otra red insegura, los suscriptores pueden usar encriptación para la información intercambiada con la plataforma 130 de base de datos de la nube. De esta manera, puede existir información de texto sin cifrar solamente dentro de las instalaciones 108 del abonado y dentro de la instalación que contiene los componentes de la plataforma 130 de base de datos de la nube. Las comunicaciones que viajan entre esas instalaciones, pueden ser encriptadas de tal modo que, incluso aunque la comunicación sea interceptada por un tercero no autorizado, ese tercero no pueda estar capacitado para usar la información contenida en la comunicación.

Para soportar esta función de encriptación, un suscriptor, tal como el abonado 110B, puede disponer de una clave 114. Cuando el abonado 110B introduce una consulta en el dispositivo 112B de computación de cliente, un programa de encriptación que se ejecuta en el dispositivo de computación 112B del cliente puede usar la clave 114 en una computación criptográfica para generar una consulta 116 encriptada. La consulta 116 encriptada, en vez de la versión de texto sin cifrar de la consulta generada por el abonado 110B, puede ser comunicada a través de la red 120.

En la plataforma de computación 130 de la nube, se puede aplicar una clave correspondiente para desencriptar la consulta 116 encriptada. En este ejemplo, la clave 146A puede ser complementaria con la clave 114 de tal modo que un dispositivo de computación del interior de la plataforma de computación 130 de la nube puede usar la clave 146A para desencriptar la consulta. Esta consulta, una vez desencriptada, puede ser aplicada por un motor de consulta a la búsqueda de una base de datos 142 y/o 152. En realizaciones en las que se debe aplicar la consulta para buscar la base de datos 152 encriptada, se puede necesitar alguna traducción de la consulta de modo que la consulta, aunque inicialmente en texto sin cifrar, especifique valores según aparezcan en la base de datos 152 encriptada.

En algunas realizaciones, alguna o todas de entre estas desencriptación y traducción, podrían ocurrir dentro de los dispositivos de computación 140 y/o 150. Sin embargo, en la realización ilustrada en la Figura 1, la plataforma de computación de la nube está equipada con un dispositivo 144 de seguridad. Algo de, o todo, el procesamiento realizado con relación a la encriptación/desencriptación y traducción de consultas por motivos de seguridad que se lleva a cabo en la plataforma 130 de computación de la nube, puede ser realizado en el interior del dispositivo 144 de seguridad. El dispositivo 144 de seguridad puede ser un dispositivo de computación según se describe en la presente memoria, que sea propiedad del operador de la plataforma de computación en la nube y que esté asignado a un abonado. Aunque la Figura 1 muestra solamente un único dispositivo 144 de seguridad que, en este ejemplo, ha sido asignado al abonado 110B, una plataforma de computación de la nube que soporte múltiples abonados puede contener múltiples dispositivos de seguridad (que no han sido ilustrados explícitamente por motivos de simplicidad).

Se puede llevar a cabo cualquier procesamiento adecuado dentro del dispositivo 144 de seguridad. En algunas realizaciones, el procesamiento específico realizado puede ser especificado por un programa cargado bajo el control del abonado 110B. Ese procesamiento puede usar claves que sean también cargadas bajo el control del abonado 110B. Además, el dispositivo 144 de seguridad puede estar configurado, y empaquetado, de tal modo que no se pueda tener acceso a los datos del interior del dispositivo 144 de seguridad usando herramientas fácilmente disponibles. De esta manera, ninguna persona incluso aunque sea del operador de la plataforma de computación 130 de la nube, puede tener un acceso fácil a la programación y a las claves u otra información de seguridad dentro del dispositivo 144 de seguridad.

En el ejemplo de la Figura 1, se han ilustrado las claves 146A y 146B. Estas claves ilustran que se pueden usar diferentes claves para diferentes funciones de seguridad. Por ejemplo, la clave 146A puede ser usada para

desencriptar consultas encriptadas enviadas por el abonado 110B y/o para encriptar los resultados de la ejecución de esas consultas retornados al abonado 110B. La clave 146B puede ser usada para funciones de seguridad asociadas al acceso a datos en la base de datos 152 encriptada. Por ejemplo, la clave 146B puede ser usada en la traducción de una consulta desencriptada para su aplicación a la base de datos 152 encriptada. Alternativamente o adicionalmente, la clave 146B puede ser usada en la desencriptación de resultados encriptados retornados por la base de datos 152 encriptada consultante. Tener una clave para la desencriptación de los resultados procedentes de una base de datos 152 encriptada, puede permitir un procesamiento seguro dentro del dispositivo 144 de seguridad para incluir operaciones sobre datos de texto sin cifrar derivados de información encriptada en la base de datos 152 encriptada.

El procesamiento de seguridad proporcionado por el dispositivo 144 de seguridad puede ser usado en cualquiera de un número de formas. El procesamiento especifico realizado puede depender de un nivel de seguridad deseado. La Figura 2 es un ejemplo de la realización que proporciona un primer nivel de seguridad. La Figura 2 muestra un dispositivo de computación 240, tal como un servidor de base de datos, configurado con un motor de consulta 264 que trabaja dentro de un entorno 260 de sistema operativo. También trabajando con un entorno 260 de sistema operativo está el módulo 262 de confianza. El módulo 262 de confianza puede asegurar que el dispositivo de computación 240 arranca en un estado conocido, el cual, por ejemplo, puede ser un estado que no esté contaminado por un virus. Adicionalmente, el módulo 262 de confianza puede permitir que un dispositivo de computación 240 mantenga información en el almacenamiento masivo en forma encriptada.

Por consiguiente, el ejemplo de la Figura 2 incluye páginas 242B encriptadas. Para procesar la consulta, alguna porción de las páginas 242B encriptadas puede ser traducida por el módulo 262 de confianza en páginas 242A de texto sin cifrar. El entorno 260 de sistema operativo puede controlar cuáles de las páginas encriptadas han de ser traducidas a páginas 242B de texto sin cifrar, y cuándo las páginas 242A de texto sin cifrar han de ser borradas. Este procesamiento por parte del sistema operativo puede acceder a la RAM 266.

En este ejemplo, el motor de consulta 264 está configurado para ejecutar una consulta de texto sin formato. Cuando se aplica una consulta al motor de consulta 264, éste puede aplicar esa consulta sobre páginas 242A de texto sin cifrar. Los resultados de una consulta de ese tipo se devuelven en forma de texto sin cifrar. Este procesamiento puede ser llevado a cabo usando componentes como los conocidos en el estado de la técnica. No obstante, dicho procesamiento dentro del dispositivo de computación 240 puede ser llevado a cabo de cualquier forma adecuada.

Para proporcionar seguridad, incluso aunque las consultas y los resultados puedan ser transmitidos a través de una red pública según sean intercambiados con el cliente 212, un dispositivo de seguridad puede estar incorporado en las instalaciones de la plataforma de computación de la nube. En este ejemplo, ese dispositivo de seguridad puede estar implementado como parte de un componente 244 de interfaz de red.

El dispositivo de seguridad puede incluir una interfaz 270 de red física, que permita que el dispositivo de seguridad sea conectado directamente a una red a través de la cual se pueden intercambiar comunicaciones con el cliente 212. En este ejemplo, una comunicación recibida puede estar en forma de consulta 214 que esté encriptada y/o firmada mediante procesamiento criptográfico en el cliente 212. De igual modo, los resultados pueden ser encriptados y/o firmados antes de ser transmitidos a través de la interfaz 270 de red física hasta el cliente 212.

Para soportar el procesamiento criptográfico necesario para encriptar y/o firmar, así como para desencriptar y/o verificar una comunicación firmada, el dispositivo de seguridad puede estar configurado con una clave 246A. Esa clave puede ser una clave privada encriptada o puede estar almacenada de cualquier forma adecuada. Se pueden usar técnicas como las descritas en lo que antecede, u otras técnicas adecuadas cualesquiera, para configurar el dispositivo de seguridad con la clave 246A de una manera segura.

En el ejemplo de la Figura 2, la clave 246A se usa en el componente 274 para desencriptar y autenticar consultas recibidas desde el cliente 212. Las consultas de texto sin cifrar resultantes pueden ser aplicadas al motor de consulta 264. Los resultados de texto sin cifrar devueltos como resultado del motor de consulta 264 que ejecuta la consulta, pueden ser procesados en el componente 272. El procesamiento en el componente 272 puede encriptar los resultados de texto sin cifrar de la ejecución de la consulta para su transmisión a través de la interfaz 270 de red física de nuevo al cliente 212.

En este ejemplo, los componentes 272 y 274 pueden ser implementados mediante programación de una FPGA que sea parte del dispositivo de seguridad. Dicha programación puede ser realizada de tal modo que no se pueda acceder a una versión sin encriptar de la clave 246A privada sin medidas extremas para irrumpir en el procesamiento interno de esa FPGA. No obstante, debe apreciarse que las técnicas específicas y el hardware usado para realizar el procesamiento criptográfico dentro del dispositivo de seguridad no son críticos para la invención y que se pueden usar cualesquiera técnicas y hardware adecuados.

La Figura 3 ilustra una realización alternativa en la que se puede proporcionar seguridad adicional. La Figura 3 muestra un dispositivo de computación 340 configurado con un motor de consulta 364. Al igual que con la realización mostrada en la Figura 2, las páginas 342B encriptadas pueden ser almacenadas en forma masiva. De manera similar, puede estar disponible RAM 366 para su uso por parte de los componentes del entorno 360 de

sistema operativo.

Sin embargo, en esta realización, en vez de desencriptar las páginas, se pueden seleccionar páginas 342A encriptadas a partir de las páginas 342B encriptadas en forma masiva y copiadas en memoria más rápida. El motor de búsquedas 364 puede ejecutar consultas respecto a las páginas 342A encriptadas. Puesto que las páginas están encriptadas, el motor de consulta 364 puede procesar una consulta formateada para su aplicación a páginas encriptadas.

Por consiguiente, un dispositivo de seguridad puede recibir una consulta y traducir la consulta a un formato para su aplicación por el motor de consulta 364 a páginas encriptadas. Al igual que en la realización de la Figura 2, el dispositivo de seguridad puede estar implementado como parte de un componente de interfaz de red. En el ejemplo específico de la Figura 3, ese componente de interfaz de red puede ser una tarjeta de interfaz de red conectada a componentes de procesamiento del dispositivo de computación 340 a través de un bus PCI para otro bus interno de un dispositivo de computación.

En consecuencia, la Figura 3 muestra que el componente 344 de interfaz de red está en la misma envoltura 330 que los componentes que realizan el procesamiento para el dispositivo de computación 340. La envoltura 330, por ejemplo, puede ser una envoltura para un rack de servidores. No obstante, se debe apreciar que se puede usar cualquier envoltura adecuada para encerrar tanto el dispositivo de seguridad como los componentes de procesamiento de un dispositivo de computación 340. En algunas realizaciones, la envoltura puede ser un alojamiento para un servidor. Con independencia de la construcción específica de la envoltura que encierra el dispositivo de seguridad, los componentes de procesamiento y un bus que los interconecta, una disposición de ese tipo puede proporcionar seguridad física que reduce las oportunidades para que terceros no autorizados accedan a los datos. En consecuencia, se puede usar una envoltura de ese tipo en cualquiera de las realizaciones descritas en la presente memoria.

En el ejemplo ilustrado, un cliente 312 genera una consulta 314 encriptada/firmada. La consulta 314 puede ser transmitida a través de una red pública tal como Internet. Esa consulta puede ser recibida en la interfaz física 370, la cual puede formar parte de una tarjeta 344 de interfaz de red. También implementados en la tarjeta 344 de interfaz de red pueden estar componentes para realizar funciones de seguridad. Adicionalmente, la clave 346A privada encriptada puede estar almacenada en la tarjeta 344 de interfaz de red. Al igual que en la realización ilustrada en la Figura 2, la clave encriptada puede estar almacenada de una forma tal que no sea usada fuera de los componentes que realizan un procesamiento seguro dentro del dispositivo de seguridad.

En la realización ilustrada, esos componentes pueden incluir un componente 374 que desencripta y autentica la consulta 314. La consulta desencriptada, la cual puede estar en texto sin formato, puede ser proporcionada al componente 378 que traduce la consulta.

La traducción dentro del componente 378 puede entrañar el formateo de la consulta para su aplicación al motor de consulta 364. En este ejemplo, el motor de consulta 364 aplica consultas a una base de datos encriptada. En consecuencia, la traducción dentro del componente 378 puede entrañar el formateo de términos en la consulta de tal modo que los mismos se emparejen con términos correspondientes en las páginas 342A encriptadas. Un procesamiento de ese tipo puede ser llevado a cabo usando una clave, tal como la clave 146B (Figura 1), o cualquier otra clave adecuada para la técnica de procesamiento. De esta manera, los datos sensibles contenidos dentro de la consulta pueden estar disponibles solamente dentro del dispositivo de seguridad.

El procesamiento realizado dentro del componente 378 de traducción, y de otros componentes dentro del dispositivo de seguridad, puede ser especificado por un abonado en base a la forma de encriptación usada para datos almacenados en páginas 342A encriptadas. Por ejemplo, el componente 378 puede estar programado para identificar valores correspondientes a campos de una base de datos para los que se use la encriptación. Esta información puede ser conocida a priori en el momento de la programación o el componente 378 puede ser programado para que reconozca dinámicamente campos para los que se usa la encriptación.

Se puede usar una alternativa similar para los resultados retornados a partir de la consulta. El motor de consulta 364 puede, en respuesta a una consulta, devolver datos extraídos de páginas 342A encriptadas. Tales datos pueden contener valores sensibles solamente en forma encriptada. Estos datos pueden ser asimismo desencriptados para traducirlos al formato usado para las páginas 342A encriptadas.

Para reducir la cantidad de datos transmitidos al cliente 312, el dispositivo de seguridad puede ejecutar una función de agregación sobre los datos. La función de agregación puede, de alguna manera, agregar valores retornados desde múltiples piezas de datos que se emparejan con la consulta específica. Como ejemplo específico, la función de agregación puede sumar valores a partir de múltiples registros que se emparejan con una consulta. Como ejemplo específico, las páginas 342A encriptadas pueden contener información sobre compras realizadas. Una consulta aplicada puede necesitar información sobre todas las compras realizadas por un individuo concreto. La agregación puede entrañar sumar las cantidades de esas compras.

En la realización ilustrada, sin embargo, la función de agregación no podría devolver un resultado apropiado donde

actuó sobre valores encriptados tomados directamente desde las páginas 342A encriptadas. En consecuencia, los resultados de la consulta pasaron desde el motor de consulta 364 hasta el componente 380 de desencriptación dentro del dispositivo de seguridad. El componente 380 de desencriptación puede desencriptar cualesquiera valores encriptados en el resultado de la consulta. El procesamiento en el componente 380 de desencriptación puede usar la misma clave u otra información de seguridad según se usa en el componente 378 de traducción. No obstante, se puede usar cualquier procesamiento adecuado para desencriptar valores en el resultado encriptado.

Los resultados desencriptados pueden ser pasados al componente 376 de agregación. El componente 376 de agregación puede estar programado para realizar cualquier función de agregación deseada. La función específica puede depender del uso específico de los datos y de la naturaleza de las consultas que son planteadas por el cliente 312. Al igual que con otros componentes del interior del dispositivo, la programación del componente 376 de agregación puede ser especificada por el abonado al que ha sido asignado el dispositivo de seguridad.

Con independencia de la función de agregación específica ejecutada dentro del componente 376, los resultados de esa función pueden ser pasados al componente 372. En el componente 372, los datos resultantes pueden ser encriptados. Los datos encriptados pueden ser pasados a continuación a través de la interfaz 370 de red física para su transmisión a través de Internet de nuevo al cliente 312.

En esta realización, se debe reconocer que se usan formatos diferentes de encriptación para las comunicaciones a través de Internet y para el almacenaje de datos encriptados dentro de la plataforma de base de datos de la nube. Una arquitectura de ese tipo permite una encriptación fuerte de la información transmitida a través de la red pública y un procesamiento más rápido para los datos mantenidos dentro de un entorno de base de datos de nube privada. Sin embargo, se debe apreciar que se puede usar cualesquiera técnicas de encriptación adecuadas, con independencia de su fortaleza, tanto para una cualquiera como para ambas de esas funciones.

Volviendo a la Figura 4, se muestra una realización adicional que proporciona una mayor flexibilidad en los tipos de operaciones de procesamiento que pueden ser llevadas a cabo sobre los resultados recuperados en respuesta a una consulta. En esta realización, al igual que con las realizaciones de las Figuras 2 y 3, se implementa un dispositivo de seguridad como parte de una interfaz de red 444. La interfaz de red 444 tiene una interfaz 270 de red física que puede conectar con una red pública, tal como Internet. Aunque no se ha representado en la Figura 4, uno o más dispositivos de cliente pueden enviar consultas recibidas a través de la interfaz 470 de red pública.

Las consultas recibidas pueden estar encriptadas por seguridad. En consecuencia, el dispositivo de seguridad de la Figura 4 incluye un componente 474 de desencriptación/autenticación, el cual puede realizar funciones similares a los componentes 374 o 274, según se ha descrito con anterioridad. De igual modo, el dispositivo de seguridad de la Figura 4 puede incluir un componente 472 de encriptación, el cual puede realizar funciones similares a los componentes 272 y 372 de encriptación, según se ha descrito con anterioridad. Para soportar estas funciones, el dispositivo de seguridad puede estar configurado con una clave privada 446A dañada, la cual puede ser también similar a las claves privadas descritas en relación con las Figuras 2 y 3 anteriores.

También según se ha descrito con anterioridad en relación con la Figura 3, los datos pueden ser almacenados en páginas 442B masivas encriptadas. Alguna porción de esas páginas puede ser seleccionada y copiada en páginas 442A encriptadas, las cuales pueden ser almacenadas temporalmente en la memoria más rápida para la aplicación más rápida de consultas a esas páginas por el motor de consulta 464B.

También según se ha descrito con anterioridad en relación con la Figura 2, alguna de las páginas de entre las páginas 442B masivas encriptadas pueden ser seleccionadas, desencriptadas y almacenadas temporalmente como páginas 442C de texto sin cifrar. Las consultas de texto sin cifrar pueden ser aplicadas a páginas 442C de texto sin cifrar.

En consecuencia, la Figura 4 ilustra una realización en la que las consultas de texto tanto encriptado como sin cifrar pueden ser procesadas en el mismo nodo de base de datos. En este ejemplo, para soportar el procesamiento de ambas consultas de texto encriptado y sin cifrar, se han ilustrado dos dispositivos de computación, cada uno de ellos con un motor de consulta. El dispositivo de computación 440 ha sido mostrado de modo que contiene el motor de consulta 464A. En este ejemplo, el motor de consulta 464A ejecuta consultas de texto sin cifrar en relación con páginas 442C de texto sin cifrar. El dispositivo de computación 450 ha sido mostrado conteniendo el motor de consulta 464B. El motor de consulta 464B ejecuta consultas encriptas en relación con páginas 442A encriptadas.

Se debe apreciar que se han mostrado dos dispositivos de computación con dos motores de consultas, por motivos de simplicidad. En algunas realizaciones se pueden usar más dispositivos de computación y/o más motores de consultas. Alternativamente, en algunas realizaciones, un motor de consulta puede estar configurado para ejecutar consultas tanto de texto encriptado como sin cifrar. Alternativamente, se pueden ejecutar múltiples motores de consultas en un dispositivo de computación.

Con independencia de la manera en que esté estructurado el nodo de base de datos para soportar la ejecución de consultas encriptadas y de texto sin cifrar, el dispositivo de seguridad puede estar configurado para generar esas consultas en base a consultas recibidas desde un cliente. En el ejemplo ilustrado en la Figura 4, el dispositivo de

seguridad incluye un componente 478 de división de consulta. Una vez que una consulta ha sido recibida y desencriptada y autenticada, el componente 474A pasa esa consulta al componente 478 de división de consulta.

El componente 4788 de división de consulta procesa la consulta para generar una consulta de texto sin cifrar y una consulta desencriptada. La consulta de texto sin cifrar puede ser proporcionada al motor de consulta 4648. La consulta encriptada puede ser proporcionada al motor de consulta 464B.

El dispositivo de seguridad puede contener también un componente para combinar los resultados del procesamiento de las porciones de la consulta dividida. Para este fin, el dispositivo de seguridad puede incluir un componente 476 de combinación. El componente 476 de combinación recibe resultados de texto sin cifrar desde el motor de consulta 464A. Los resultados encriptados son recibidos desde el motor de consulta 464B.

Se puede realizar cualquier procesamiento adecuado para combinar los resultados de la consulta. En la realización ilustrada, los resultados encriptados procedentes del motor de consulta 464B pueden ser traducidos, dentro del componente 476 de combinación, a un formato de texto sin cifrar. Como resultado, dentro del dispositivo de seguridad pueden existir todos los resultados en formato de texto sin cifrar y pueden ser combinados fácilmente.

Una vez combinados, los resultados pueden ser suministrados al componente 4724 de encriptación para su transmisión a un cliente que generó la consulta.

Las Figuras 5A, 5B, 5C y 5D ilustran varios formatos de consulta. La Figura 5A ilustra una consulta 510 de texto sin cifrar. La consulta 510 incluye una función de agregación, mostrada en este caso como función suma: sum(1_extendprice * (1.0 – 1_discount). Esta función indica campos dentro de los registros de base de datos que han de ser combinados numéricamente y proporciona una fórmula para esa combinación. Otras porciones de la consulta especifican qué registros han de ser seleccionados desde la base de datos para su procesamiento en la función suma.

En este ejemplo, la consulta es texto sin cifrar de tal modo que cualquier información sensible sea discernible en la consulta. Por ejemplo, el valor 512 puede ser un nombre. La entidad que mantiene una base de datos a la que puede ser aplicada esta consulta puede no querer revelar que está almacenando información acerca de un individuo nombrado. Por esta razón, la consulta 510 puede ser comunicada a través de una red pública en forma encriptada.

La Figura 5B ilustra una consulta 520 completamente encriptada. En la consulta 520 completamente encriptada, ni la función de la consulta ni nombres específicos u otros valores son identificables. Sin embargo, en este formato, sería difícil o imposible emparejar criterios especificados en la consulta con datos almacenados en una base de datos.

La Figura 5C Ilustra una consulta encriptada que puede ser aplicada fácilmente a una base de datos. En la consulta 530, los valores que representan información sensible pueden estar encriptados. Sin embargo, otras porciones de la consulta se mantienen como texto sin cifrar. Por consiguiente, comparando la Figurea 5C con la Figura 5A, se puede apreciar que el valor 512 de texto sin cifrar ha sido sustituido por el valor 532 encriptado. No obstante, ambos valores pueden ser vistos en el contexto de las consultas como un valor para el campo “o_clerk” en una base de datos. Si todos los valores correspondientes del campo “o_clerk” en una base de datos están también encriptados con el mismo esquema de daños, el valor encriptado 532 se emparejará con registros apropiados en la base de datos. De esta manera, la consulta puede ser aplicada en forma encriptada a la base de datos.

La Figura 5D ilustra un ejemplo de división de consulta. Una consulta 540 ha sido dividida en las porciones 550 y 560. La porción 550 es una consulta de texto sin cifrar, que especifica información a recuperar desde una base de datos de texto sin cifrar. Por el contrario, la porción 560 contiene un valor 562 encriptado, que especifica criterios para recuperar información desde una base de datos encriptada.

En un sistema como el ilustrado en la Figura 4, la consulta recibida puede estar dividida en porciones, tal como las porciones 550 y 560. Esas porciones pueden ser aplicadas a motores de consultas 464A y 464B, respectivamente. En un sistema como el ilustrado en la Figura 3, una consulta traducida en forma de consulta 530 puede ser aplicada al motor de consulta 364. En un sistema como el ilustrado en la Figura 2, se puede aplicar una consulta de texto sin cifrar, como la ilustrada en la Figura 5A, al motor de consulta 264. De esta manera, se pueden aplicar consultas de diferentes formas a sistemas con diferentes arquitecturas para proporcionar un nivel de seguridad deseado.

La Figura 6 ilustra un ejemplo de entorno 600 de sistema de computación adecuado en el que puede ser implementada la invención. El entorno 600 de sistema de computación es solamente un ejemplo de un entorno de computación adecuado y no se pretende sugerir ninguna limitación respecto al ambito de uso o funcionalidad de la invención. En ningún caso se debe interpretar que el entorno 600 de computación tiene alguna dependencia o necesidad en relación con uno cualquiera o con una combinación de componentes ilustrados en el ejemplo de entorno 600 operativo.

La invención es operativa con otros numerosos entornos o configuraciones de sistema de computación de propósito general o de propósito especial. Ejemplos de sistemas de computación, entornos y/o configuraciones bien conocidos que pueden ser adecuados para su uso con la invención incluyen, aunque sin limitación, ordenadores personales, ordenadores servidores, dispositivos de mano o portátiles, sistemas multiprocesadores, sistemas a base de

microprocesador, descodificadores, electrónica de consumo programable, PCs en red, minicomputadores, ordenadores centrales, entornos de computación distribuida que incluyen cualquiera de los sistemas o dispositivos anteriores, y similares.

El entorno de computación puede ejecutar instrucciones ejecutables con ordenador, tal como módulos de programa. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas particulares o que implementan tipos de datos abstractos particulares. La invención puede ser también puesta en práctica en entornos de computación distribuida donde las tareas son realizadas por dispositivos de procesamiento remotos que están enlazados a través de una red de comunicaciones. En un entorno de computación distribuida, los módulos de programa pueden estar ubicados en medios de almacenaje de ordenador tanto locales como remotos, incluyendo los dispositivos de almacenaje en memoria.

Con referencia a la Figura 6, un ejemplo de sistema para implementar la invención incluye un dispositivo de computación de propósito general en forma de ordenador 610. Los componentes del ordenador 610 pueden incluir, aunque sin limitación, una unidad 620 de procesamiento, una memoria de sistema 630, y un bus de sistema 621 que acopla varios componentes del sistema incluyendo la memoria del sistema a la unidad 620 de procesamiento. El bus de sistema 621 puede ser cualquiera de entre varios tipos de estructuras de bus incluyendo un controlador de memoria o de bus de memoria, un bus periférico, y un bus local que usa cualquiera de una diversidad de arquitecturas de bus. A título de ejemplo, y sin limitación, tales arquitecturas incluyen el bus de Arquitectura Estándar Industrial (ISA), el bus de Arquitectura de Micro Canal (MCA), el bus ISA Potenciado (EISA), el bus local de la Asociación de Estándares Electrónicos de Video (VESA), y el bus de Interconexión de Componente Periférico (PCI) conocido también como bus Mezzanine.

El ordenador 610 incluye típicamente una diversidad de medios legibles con ordenador. Los medios legibles con ordenador pueden ser cualquier medio disponible al que se pueda acceder mediante el ordenador 610 e incluye tanto medios volátiles como no volátiles, medios extraíbles y no extraíbles. A título de ejemplo, y sin limitación, los medios legibles con ordenador pueden comprender medios de almacenaje con ordenador y medios de comunicación. Los medios de almacenaje con ordenador incluyen tanto medios volátiles como no volátiles, medios extraíbles y no extraíbles implementados en cualquier método o tecnología para almacenaje de información tal como instrucciones legibles con ordenador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenaje con ordenador incluyen, aunque sin limitación, memoria RAM, ROM, EEPROM, flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otros dispositivos de almacenaje en disco óptico, casetes magnéticos, cinta magnética, almacenaje en disco magnético u otros dispositivos de almacenaje magnético, o cualquier otro medio que pueda ser usado para almacenar la información deseada y al que se pueda acceder mediante el ordenador 610. El medio de comunicación materializa típicamente instrucciones legibles con ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada tal como una onda portadora u otro mecanismo de transporte, e incluye cualquier medio de suministro de información. El término “señal de datos modulada” significa una señal que tiene una o más de sus características establecida o cambiada de tal manera que codifique información en la señal. A título de ejemplo, y sin limitación, el medio de comunicación incluye medios cableados tal como una red cableada o conexión cableada directa, y medios inalámbricos tal como medios acústicos, RF, infrarrojos y otros medios inalámbricos. Las combinaciones de cualesquiera de los medios anteriores deberán estar también incluidas dentro del ámbito de los medios legibles con ordenador.

La memoria de sistema 630 incluye medios de almacenaje en ordenador en forma de memoria volátil y/o no volátil tal como la memoria de sólo lectura (ROM) 631 y la memoria de acceso aleatorio (RAM) 632. Un sistema 633 básico de entrada/salida (BIOS), que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del ordenador 610, tal como durante el arranque, está típicamente almacenado en la ROM 631. La RAM 632 contiene típicamente datos y/o módulos de programa que son inmediatamente accesibles para, y/o que están actualmente operados por, la unidad 620 de procesamiento. A título de ejemplo, y sin limitación, la Figura 6 ilustra el sistema operativo 634, programas de aplicación 635, otros módulos de programa 636, y datos de programa 637.

El ordenador 610 puede incluir también otros medios de almacenaje en ordenador extraíbles/no extraíbles, volátiles/no volátiles. A título de ejemplo solamente, la Figura 6 ilustra una unidad 641 de disco duro que lee desde, o escribe en, medios magnéticos no extraíbles, no volátiles, una unidad 651 de disco magnético que lee desde, o escribe en, un disco magnético 652 extraíble, no volátil, y una unidad 655 de disco óptico que lee desde, o escribe en, un disco óptico 656 extraíble, no volátil tal como un CD ROM u otro medio óptico. Otros medios de almacenaje en ordenador extraíbles/no extraíbles, volátiles/no volátiles que pueden ser usados en el entorno operativo del ejemplo pueden incluir, aunque sin limitación, casetes de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cinta de video digital, RAM de estado sólido, ROM de estado sólido, y similares. La unidad 641 de disco duro está conectado típicamente al bus de sistema 621 a través de una interfaz de memoria no extraíble tal como la interfaz 640, y la unidad 651 de disco magnético y la unidad 655 de disco óptico están conectadas típicamente al bus de sistema 621 mediante una interfaz de memoria extraíble, tal como la interfaz 650.

Las unidades y sus medios de almacenaje en ordenador asociados que se han discutido con anterioridad e ilustrado en la Figura 6, proporcionan el almacenaje de instrucciones legibles con ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador 610. En la Figura 6, por ejemplo, la unidad 641 de disco duro ha sido ilustrada como sistema 644 operativo de almacenamiento, programas de aplicación 645, otros módulos de programa

646, y datos de programa 647. Obsérvese que estos componentes pueden ser iguales o bien ser diferentes que los del sistema operativo 634, los programas de aplicación 635, otros módulos de programa 636, y datos de programa 637. El sistema operativo 644, los programas de aplicación 645, otros módulos de programa 646 y los datos de programa 647 han sido identificados en este caso con números diferentes para ilustrar que, como mínimo, son copias diferentes. Un usuario puede introducir comandos e información en el ordenador 610 a través de dispositivos de entrada tal como un teclado 662 y un dispositivo de puntero 661, mencionado habitualmente como ratón, rueda de desplazamiento o panel táctil. Otros dispositivos de entrada (no representados) pueden incluir un micrófono, joystick, control para juegos, escáner o similar. Estos y otros dispositivos de entrada están con frecuencia conectados a la unidad 620 de procesamiento a través de una interfaz 660 de entrada de usuario que está acoplada al bus del sistema, pero que pueden estar conectados por medio de otra interfaz y estructuras de bus, tal como un puerto paralelo, puerto para juegos, o un bus serie universal (USB). Un monitor 691 u otro tipo de dispositivo de reproducción está también conectado al bus de sistema 621 a través de una interfaz, tal como una interfaz de video 690. Adicionalmente al monitor, los ordenadores pueden incluir también otros dispositivos periféricos de salida tal como altavoces 697 e impresora 696, los cuales pueden estar conectados a través de una interfaz 695 periférica de salida.

El ordenador 610 puede operar en un entorno de red usando conexiones lógicas a uno o más ordenadores remotos, tal como un ordenador 680 remoto. El ordenador 680 remoto puede ser un ordenador personal, un servidor, un enrutador, un PC de red, un dispositivo homólogo u otro nodo de red común, y típicamente incluye muchos de, o todos, los elementos descritos con anterioridad en relación con el ordenador 610, aunque solamente se ha ilustrado un dispositivo 681 de almacenaje en memoria en la Figura 6. Las conexiones lógicas representadas en la Figura 6 incluyen una red de área local (LAN) 671 y una red de área extensa (WAN) 673, pero también pueden incluir otras redes. Tales entornos de red son lugares comunes en oficinas, redes de ordenador amplias de empresa, intranets e Internet.

Cuando se usa en un entorno de red LAN, el ordenador 610 está conectado a la LAN 671 a través de una interfaz de red o adaptador 670. Cuando se usa en un entorno de red WAN, el ordenador 610 incluye típicamente un módem 672 u otros medios para establecer comunicaciones a través de la WAN 673, tal como Internet. El módem 672, el cual puede ser interno o externo, puede estar conectado al bus de sistema 621 por medio de la interfaz 660 de entrada de usuario, o de otro mecanismo apropiado. En un entorno equipado con red, los módulos de programa representados en relación con el ordenador 610, o con porciones del mismo, pueden estar almacenados en el dispositivo de almacenaje en memoria remoto. A título de ejemplo, y sin limitación, la Figura 6 ilustra programas 685 de aplicación remota como residentes en el dispositivo de memoria 681. Se apreciará que las conexiones de red mostradas son ejemplos y que se pueden usar otros medios de establecimiento de un enlace de comunicaciones entre los ordenadores.

Habiendo descrito de ese modo diversos aspectos de al menos una realización de la presente invención, se debe apreciar que diversas alteraciones, modificaciones, y mejoras serán fácilmente imaginables para los expertos en la materia.

Aunque se han indicado las ventajas de la presente invención, se debe apreciar que cada realización de la invención no tendrá que incluir cada una de las ventajas descritas. Algunas realizaciones pueden no implementar cualquiera de las características descritas como ventajosas. En consecuencia, la descripción que antecede y los dibujos se proporcionan únicamente a título de ejemplo.

Las realizaciones de la presente invención descritas en lo que antecede pueden ser implementadas en una cualquiera de numerosas formas. Por ejemplo, las realizaciones pueden ser implementadas usando hardware, software o una combinación de ambos. Cuando se implementa en software, el código de software puede ser ejecutado en cualquier procesador adecuado o recopilación de procesadores, si se proporcionan en un único ordenador o distribuidos entre múltiples ordenadores. Tales procesadores pueden ser implementados como circuitos integrados, con uno o más procesadores en un componente de circuito integrado. No obstante, un procesador puede ser implementado usando circuitería en cualquier formato adecuado.

Además, se debe apreciar que un ordenador puede estar materializado en una cualquiera de un número de formas, tal como un ordenador montado en un rack, un ordenador de sobremesa, un ordenador portátil, o un ordenador de tableta. Adicionalmente, un ordenador puede estar incluido en un dispositivo no mencionado generalmente como ordenador, pero con capacidades de procesamiento adecuadas, incluyendo un Asistente Digital Personal (PDA), un teléfono inteligente o cualquier otro dispositivo electrónico portátil o fijo adecuado.

También, un ordenador puede tener uno o más dispositivos de entrada y salida. Estos dispositivos pueden ser usados, entre otras cosas, para presentar una interfaz de usuario. Ejemplos de dispositivos de salida que pueden ser usados para proporcionar una interfaz de usuario incluyen impresoras o pantallas de visualización para la presentación visual de señales de salida y altavoces u otros dispositivos de generación de sonido para la presentación audible de señales de salida. Ejemplos de dispositivos de entrada que pueden ser usados para una interfaz de usuario incluyen teclados y dispositivos de puntero, tal como ratones, paneles táctiles, y tabletas de digitalización. Según otro ejemplo, un ordenador puede recibir información de entrada a través de reconocimiento de habla o en otro formato audible.

Tales ordenadores pueden estar interconectados mediante una o más redes de cualquier forma adecuada, incluyendo una red de área local o una red de área extensa, tal como una red de empresa o Internet. Tales redes pueden estar basadas en cualquier tecnología adecuada y pueden operar según cualquier protocolo adecuado y pueden incluir redes inalámbricas, redes cableadas o redes de fibra óptica.

También, los diversos métodos o procesos expuestos en la presente memoria pueden estar codificados como software que sea ejecutable en uno o más procesadores que empleen uno cualquiera de una diversidad de sistemas operativos o plataformas. Adicionalmente, ese software puede estar escrito usando uno cualquiera de un número de lenguajes de programación adecuados y/o herramientas de programación o escritura, y también puede estar compilado como código de lenguaje máquina ejecutable o código intermedio que sea ejecutado en un ordenador central o una máquina virtual.

A este respecto, la invención puede estar materializada como medio de almacenaje legible con ordenador (o múltiples medios legibles con ordenador) (por ejemplo, una memoria de ordenador, uno o más discos flotantes, discos compactos (CD), discos ópticos, discos de video digital (DVD), cintas magnéticas, memorias flash, configuraciones de circuito en Matrices de Puerta Programable en Campo u otros dispositivos semiconductores, u otro medio tangible de almacenaje en ordenador) codificado con uno o más programas que, cuando se ejecutan en uno o más ordenadores u otros procesadores, ejecutan métodos que implementan las diversas realizaciones de la invención discutida en lo que antecede. Según resulta evidente a partir de los ejemplos anteriores, un medio de almacenaje legible con ordenador puede mantener información durante un tiempo suficiente para proporcionar instrucciones ejecutables con ordenador de una forma no transitoria. Tal medio (o medios) de almacenaje legible(s) con ordenador puede(n) ser transportable(s), de tal modo que el programa o programas almacenados en el (los) mismo(s) pueden ser cargados en uno o más ordenadores diferentes u otros procesadores para implementar diversos aspectos de la presente invención según se ha expuesto en lo que antecede. Según se usa en la presente memoria, el término “medio de almacenaje legible con ordenador” abarca solamente un medio legible con ordenador que puede ser considerado que es un fabricado (es decir, un artículo de fabricación) o una máquina. Alternativa o adicionalmente, la invención puede ser materializada como un medio legible con ordenador distinto de un medio de almacenaje legible con ordenador, tal como una señal de propagación.

Los términos “programa” o “software” se usan en la presente memoria en un sentido genérico para referirse a cualquier tipo de código informático o conjunto de instrucciones ejecutables con ordenador que puede ser empleado para programar un ordenador u otro procesador para implementar diversos aspectos de la presente invención según se ha discutido con anterioridad. Adicionalmente, se apreciará que, según un aspecto de la presente realización, uno o más programas informáticos que cuando se ejecutan realizan métodos de la presente invención no necesitan residir en un único ordenador o procesador, sino que pueden estar distribuidos de una forma modular entre un número de ordenadores o procesadores diferentes para implementar diversos aspectos de la presente invención.

Las instrucciones ejecutables con ordenador pueden estar de muchas formas, tal como módulos de programa, ejecutados por uno o más ordenadores u otros dispositivos. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares. Típicamente, la funcionalidad de los módulos de programa puede estar combinada o distribuida según se desee en varias realizaciones.

También, las estructuras de datos pueden ser almacenadas en medios legibles con ordenador de cualquier forma adecuada. Por simplicidad de la ilustración, las estructuras de datos pueden ser mostradas de modo que tengan campos que se relacionen mediante su ubicación en la estructura de datos. Tales relaciones pueden ser logradas asimismo asignando almacenaje para los campos con localizaciones en un medio legible con ordenador que transporta la relación entre los campos. Sin embargo, se puede usar cualquier mecanismo adecuado para establecer una relación entre la información en los campos de una estructura de datos, incluyendo el uso de punteros, etiquetas u otros mecanismos que establezcan la relación entre elementos de datos.

Los diversos aspectos de la presente invención pueden ser usados solos, en combinación, o en una diversidad de disposiciones no discutidas específicamente en las realizaciones descritas en lo que antecede, y por lo tanto no se limita en su aplicación a los detalles y a la disposición de componentes establecida en la descripción que antecede o ilustrada en los dibujos. Por ejemplo, los aspectos descritos en una realización pueden ser combinados de cualquier manera con los aspectos descritos en otras realizaciones.

También, la invención puede ser materializada como método, del que se ha proporcionado un ejemplo. Las acciones realizadas como parte del método pueden estar ordenadas de cualquier forma adecuada. Por consiguiente, se puede construir realizaciones en las que las acciones se lleven a cabo en un orden diferente al ilustrado, lo que puede incluir realizar algunas acciones simultáneamente, incluso aunque se muestren como acciones secuenciales en realizaciones ilustrativas.

El uso de términos ordinales tales como “primero”, “segundo”, “tercero”, etc., en las reivindicaciones para modificar un elemento de reivindicación, no indica en sí mismo ninguna prioridad, precedencia u orden de un elemento de la reivindicación sobre otro, o el orden temporal en el que se llevan a cabo las acciones de un método, sino que se usan simplemente como etiquetas para distinguir un elemento de reivindicación que tenga un cierto nombre de otro

elemento que tenga un mismo nombre (pero para uso del término ordinal) para distinguir los elementos reivindicados.

También, la fraseología y la terminología usadas en la presente memoria se entienden a efectos de descripción y no deben ser entendidas como limitación. El uso de “incluyendo”, “comprendiendo” o “teniendo”, “conteniendo”, “envolviendo” y las variaciones de los mismos en la presente memoria, se entiende que abarcan los elementos relacionados a continuación y los equivalentes de los mismos, así como elementos adicionales.

REIVINDICACIONES

1.- Un dispositivo de computación (140, 150, 112, 240, 340, 440, 450, 610) de una plataforma (130) de base de datos en la nube, comprendiendo el dispositivo de computación:

una envoltura física (330)

al menos un procesador dispuesto en el interior de la envoltura (330), estando el al menos un procesador adaptado para ejecutar consultas en una base de datos (142, 152) de la nube, en donde la base de datos (142, 152) de la nube almacena datos parcialmente como datos de texto sin cifrar y parcialmente como datos encriptados;

una interfaz de red (270, 344, 370, 444, 470, 670) dispuesta en el interior de la envoltura (330), estando la interfaz de red (270, 344, 370, 444, 470, 670) adaptada para proporcionar una interfaz para una red (120, 671, 673) y que comprende circuitería de seguridad, comprendiendo la circuitería de seguridad:

un componente (274, 374, 380, 474) de desencriptación y un componente de división de consulta adaptado para:

recibir una consulta encriptada a través de la red (120, 671, 673), siendo la consulta encriptada recibida desde un dispositivo de un abonado al servicio de computación de la nube;

procesar la consulta encriptada para generar una consulta procesada, comprendiendo el procesamiento desencriptar la consulta con una clave (114, 46, 246, 346, 446) que es complementaria de una clave (114, 46, 246, 346, 446) en el dispositivo del abonado y dividir la consulta de tal modo que porciones de consulta desencriptada sean procesadas sobre datos de texto sin cifrar mientras que otras porciones son aplicadas a los datos encriptados, estando un componente de combinación adaptado para:

combinar los resultados de procesar porciones de la consulta dividida, y

un componente de encriptación adaptado para:

encriptar los resultados combinados, y

transmitir los resultados encriptados a través de la red (120, 671, 673) dirigidos al dispositivo del abonado en donde:

la circuitería de seguridad comprende además un componente de traducción de consulta adaptado para generar una consulta traducida mediante la realización de una traducción sobre la consulta desencriptada, y

la consulta traducida se proporciona como consulta desencriptada para su ejecución por el al menos un procesador;

comprendiendo además la circuitería de seguridad un componente de agregación adaptado para:

desencriptar un resultado de la consulta, y

llevar a cabo una función de agregación sobre el resultado desencriptado para producir un resultado agregado, y

el resultado agregado se suministra al componente de encriptación como resultado de la consulta desencriptada.

2.- El dispositivo de computación (140, 150, 112, 240, 340, 440, 450, 610) de la reivindicación 1, en donde:

la interfaz de red (270, 344, 370, 444, 470, 670) comprende una tarjeta (344) de interfaz de red, conectada a un bus del dispositivo de computación.

3.- El dispositivo de computación (140, 150, 112, 240, 340, 440, 450, 610) de la reivindicación 2, en donde la red (120, 671, 673) es Internet y el bus es un bus de PCI.

4.- El dispositivo de computación (140, 150, 112, 240, 340, 440, 450, 610) de la reivindicación 1, en donde:

la circuitería de seguridad comprende además un almacén de hardware configurado con al menos una clave de encriptación (114, 46, 246, 346, 446) para desencriptar la consulta y encriptar el resultado.

5.- El dispositivo de computación (140, 150, 112, 240, 340, 440, 450, 610) de la reivindicación 1, con un factor de

forma adaptado para su inserción en una ranura en un servidor de base de datos de la plataforma (130) de computación en la nube.

6.- Un método de operación de un servicio de base de datos en la nube, comprendiendo el método:

en el interior de un componente de hardware en una plataforma (130) de base de datos de la nube, proporcionar con el componente de hardware una interfaz (270, 344, 370, 444, 470, 670) entre una red insegura (120, 671, 673) y un servicio de base de datos configurado para proporcionar un servicio de base de datos en la nube desde una base de datos (142, 152) en la nube que almacena datos parcialmente como datos de texto sin cifrar y parcialmente como datos encriptados:

intercambiar con un dispositivo de computación (140, 150, 112, 240, 340, 440, 450, 610) de un abonado del servicio de base de datos de la nube, una consulta y un resultado de la consulta, siendo la consulta y el resultado de la consulta intercambiados en un primer formato de encriptación, y

procesar la consulta (11, 314, 510, 520, 530) y el resultado de la consulta para desencriptar la consulta (11, 314, 510, 520, 530) con una clave (114, 46, 246, 346, 446) que es complementaria con una clave (114, 46, 246, 346, 446) en el dispositivo del abonado, y dividir la consulta (11, 314, 510, 520, 530) de tal modo que porciones de la consulta desencriptada sean procesadas sobre los datos de texto sin cifrar mientras que otras porciones son aplicadas a los datos encriptados;

combinar los resultados del procesamiento de porciones de la consulta dividida;

y encriptar los resultados de la consulta combinados; e,

intercambiar con al menos un motor de consulta (264, 364, 464) la consulta procesada y un resultado de ejecución de la consulta por el motor de consulta (264, 364, 464), siendo la consulta procesada y el resultado de la ejecución intercambiados en al menos un segundo formato de encriptación.

7.- El método de la reivindicación 6, que comprende además:

identificar a partir de la consulta (11, 314, 510, 520, 530) la porción para ejecución en la base de datos encriptada y una porción restante de la consulta.

8.- El método de la reivindicación 7, que comprende además:

generar la base de datos de texto sin cifrar desencriptando al menos una poción de la base de datos encriptada.

9.- El método de la reivindicación 8, que comprende además:

eliminar la base de datos de texto sin cifrar a continuación de la ejecución de la consulta (11, 314, 510, 520, 530).

10.- El método de la reivindicación 6, en donde:

el resultado de la ejecución de la consulta consiste en datos encriptados, y

el método comprende además, dentro del componente de hardware, ejecutar una función de agregación sobre los datos encriptados.

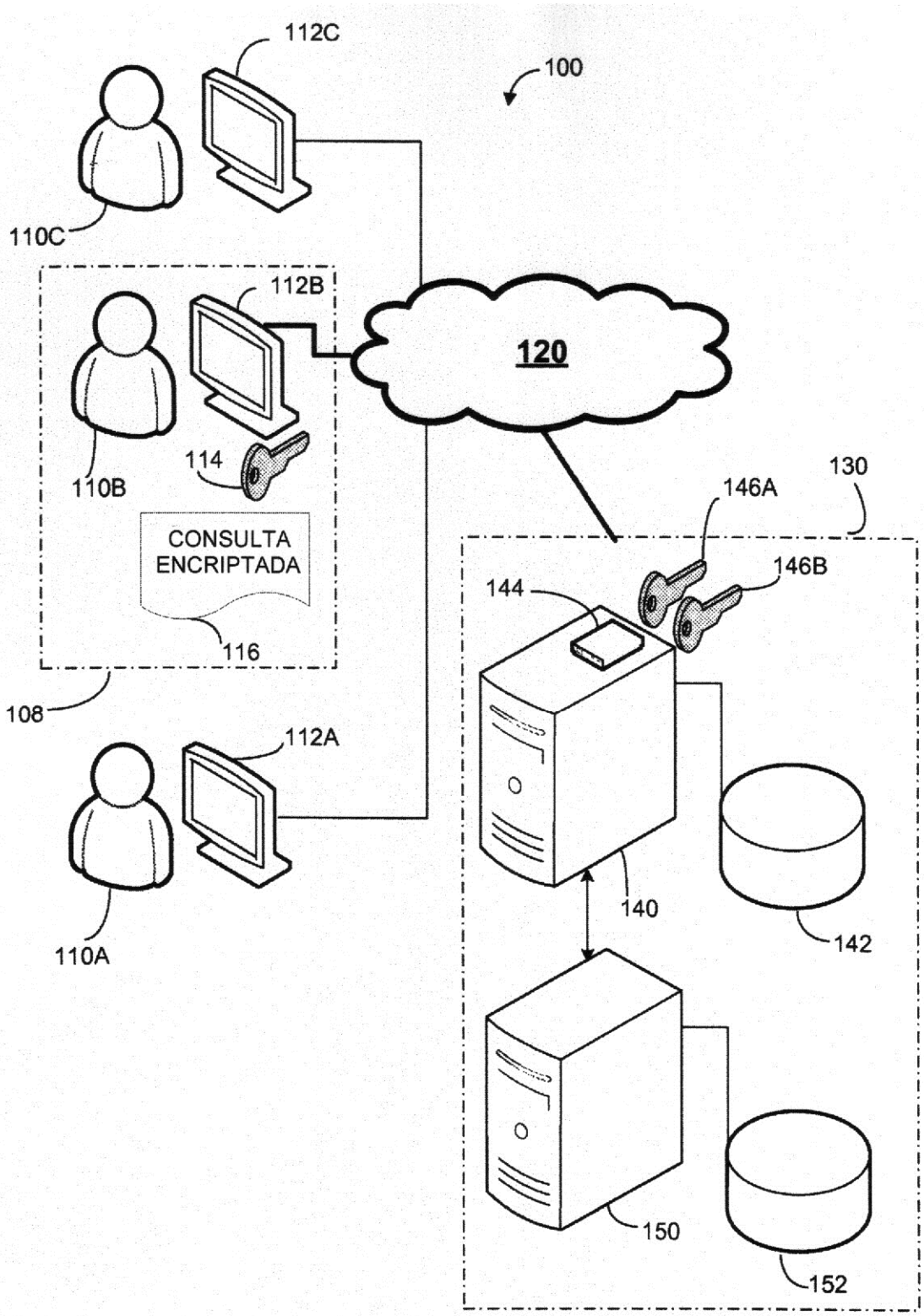
112C
100
110C
112B
120
114
110B
130
146A
CONSULTA
ENCRIPTADA
146B
144
116
108
112A
140
142
110A
150
152

FIG. 1

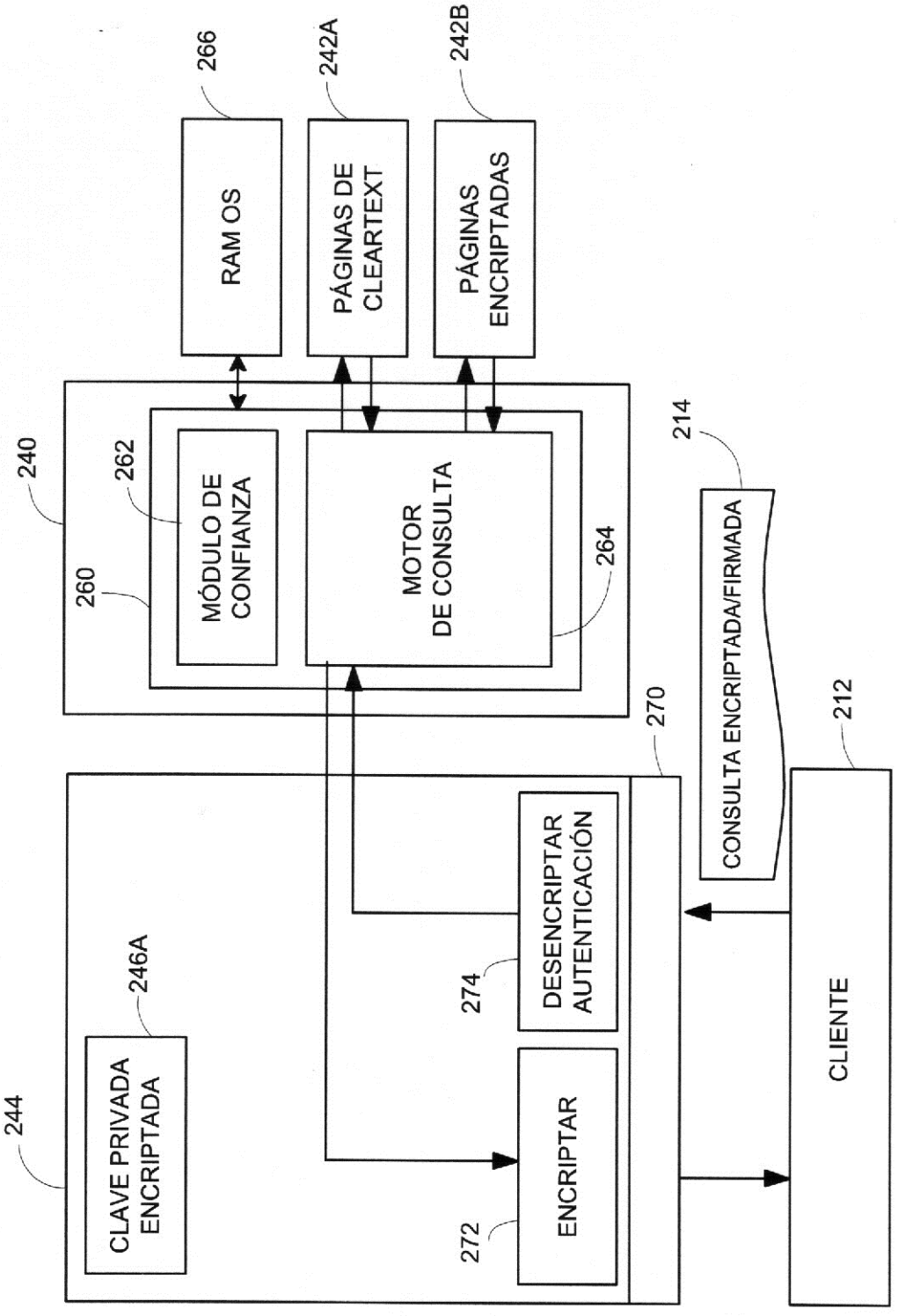
266
242A
242B
RAM OS
PÁGINAS DE CLEARTEXT
PÁGINAS ENCRIPTADAS
240
262
MÓDULO DE CONFIANZA
MOTOR DE CONSULTA
260
264
214
CONSULTA ENCRIPTADA/FIRMADA
270
212
DESENCRIPTAR AUTENTICACIÓN
274
246A
CLAVE PRIVADA ENCRIPTADA
244
ENCRIPTAR
272
CLIENTE

FIG. 2

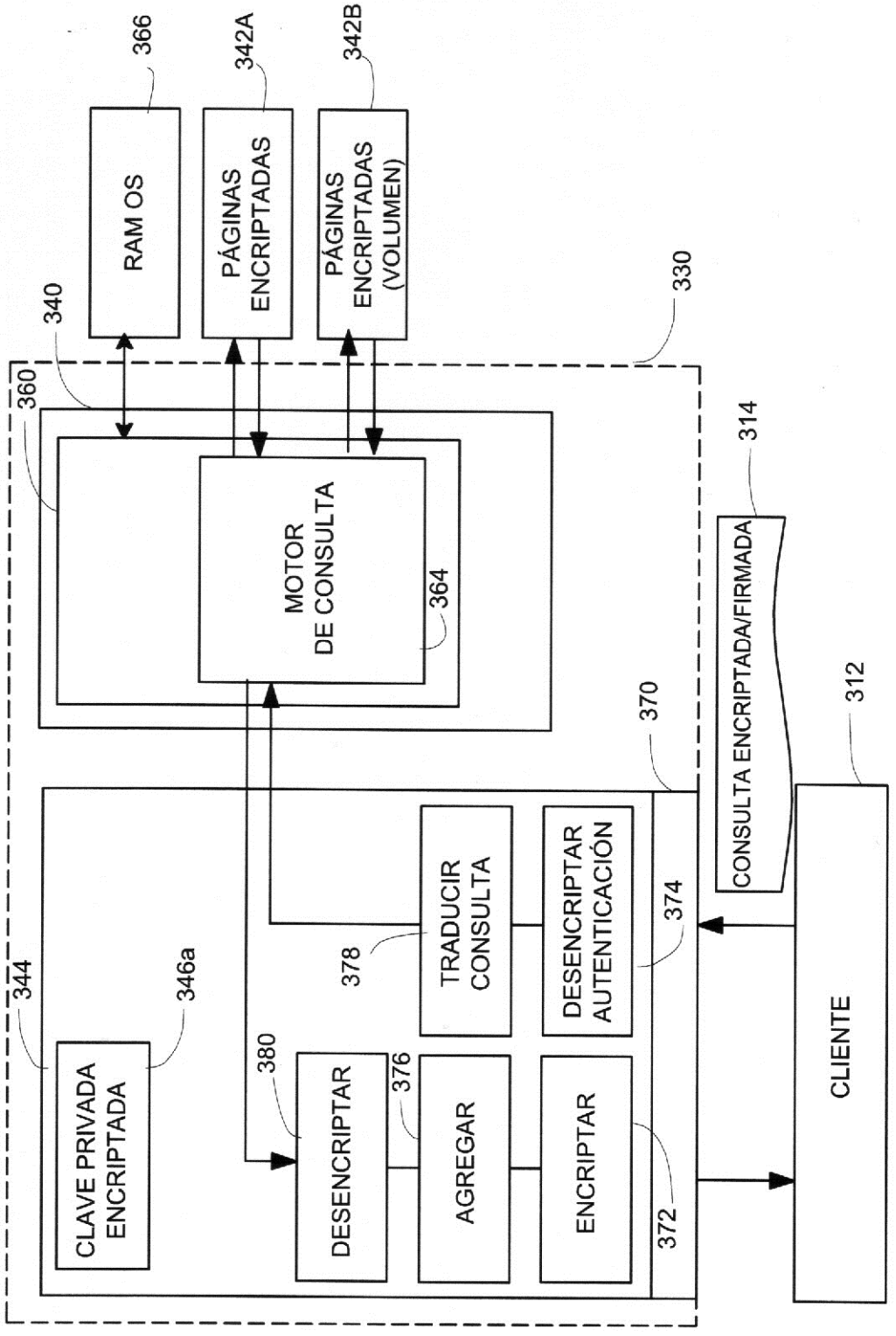
366
342A
342B
RAM OS
PÁGINAS ENCRIPTADAS
PÁGINAS ENCRIPTADAS (VOLUMEN)
340
330
360
MOTOR DE CONSULTA
364
314
CONSULTA ENCRIPTADA/FIRMADA
370
312
344
346a
CLAVE PRIVADA ENCRIPTADA
378
TRADUCIR CONSULTA
DESENCRIPTAR AUTENTICACIÓN
374
380
DESENCRIPTAR
376
AGREGAR
ENCRIPTAR
372
CLIENTE

FIG. 3

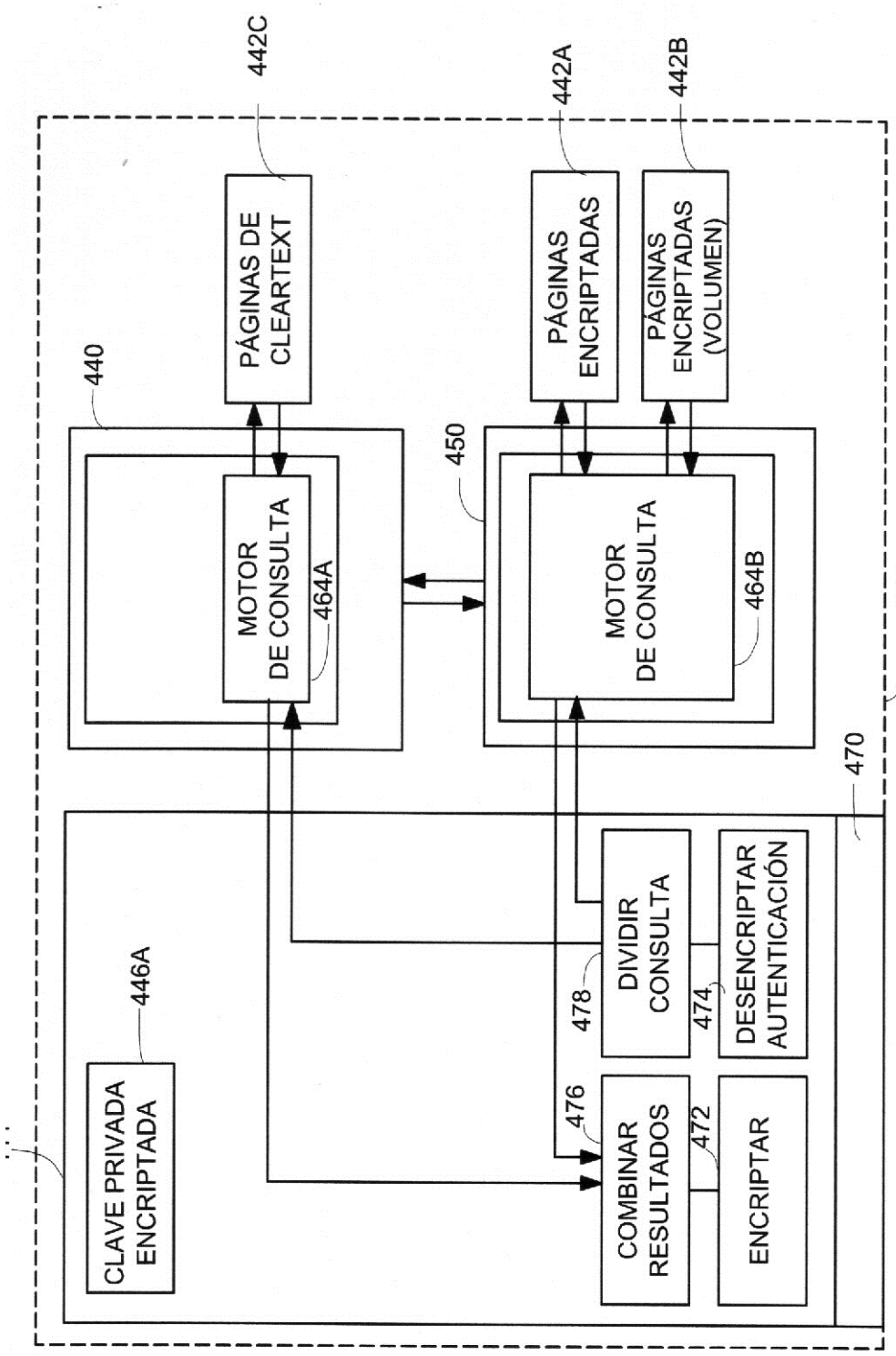
442C
442A
442B
PÁGINAS DE CLEARTEXT
PÁGINAS ENCRIPTADAS
PÁGINAS ENCRIPTADAS (VOLUMEN)
440
450
MOTOR DE CONSULTA
464A
MOTOR DE CONSULTA
464B
430
470
CLAVE PRIVADA ENCRIPTADA
446A
DIVIDIR CONSULTA
478
DESENCRIPTAR AUTENTICACIÓN
474
COMBINAR RESULTADOS
476
ENCRIPTAR
472

FIG. 4

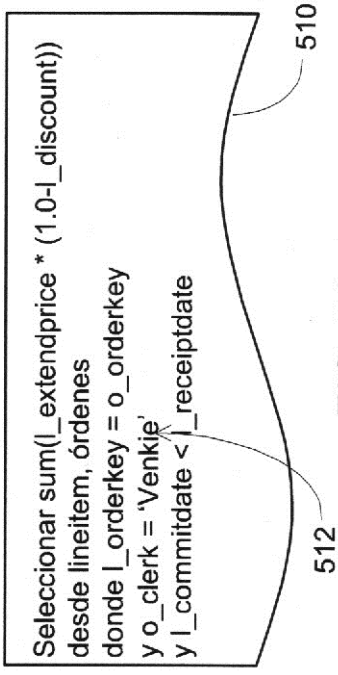

FIG. 5A

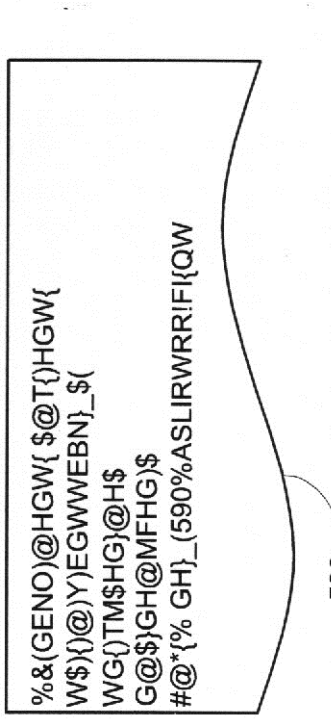

FIG. 5B

FIG. 5C

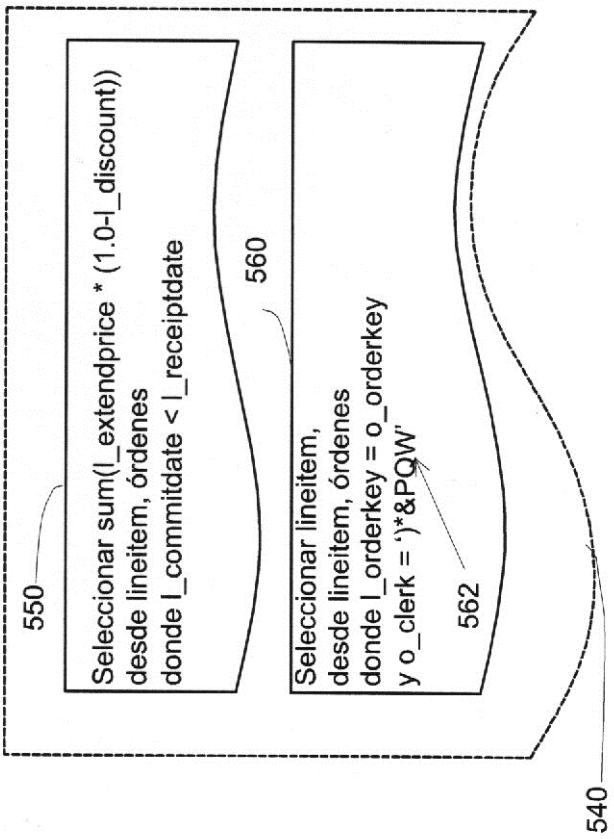

FIG. 5D

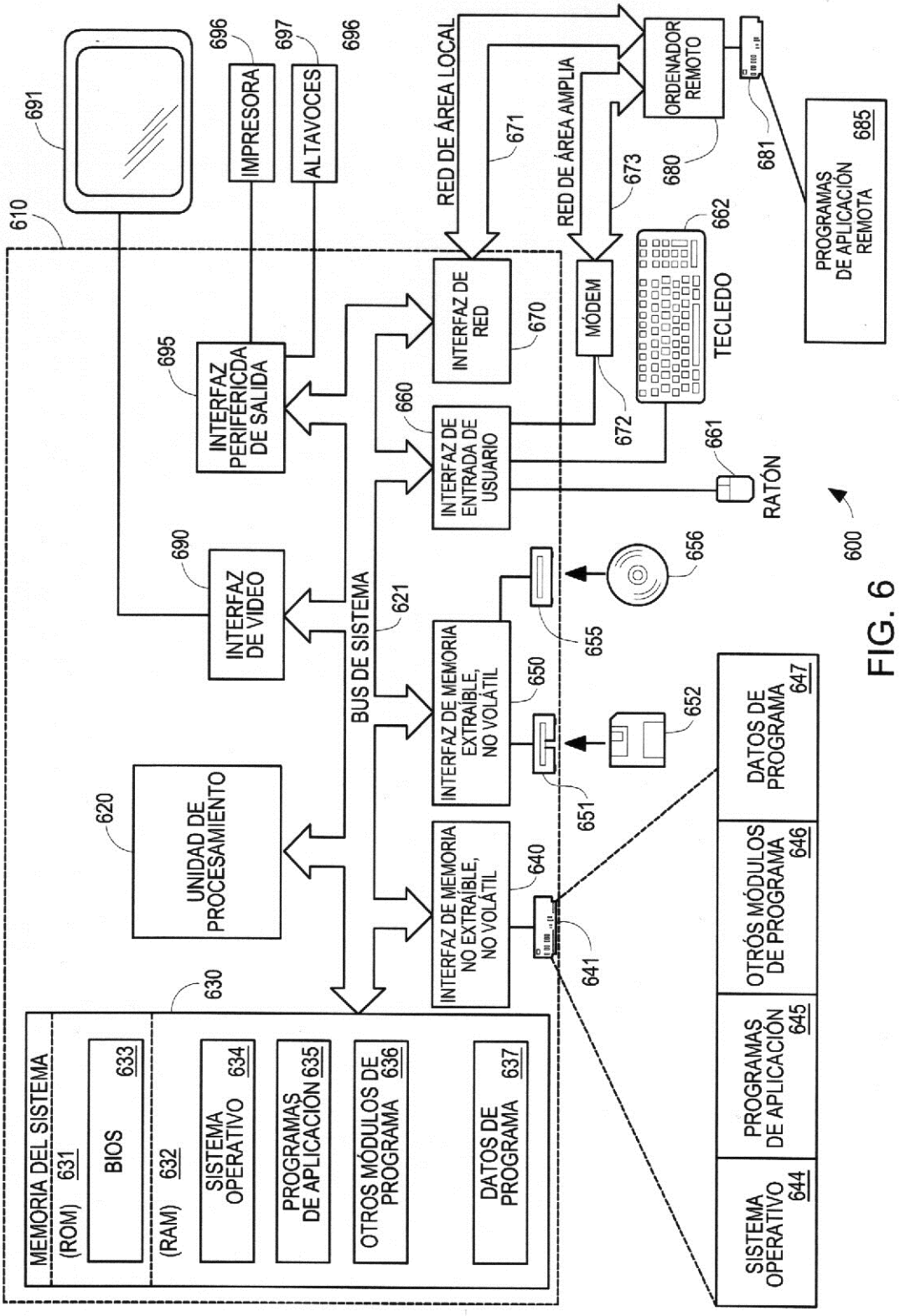
600
610
691
696
IMPRESORA
697
ALTAVOCES
696
RED DE ÁREA LOCAL
671
RED DE ÁREA AMPLIA
673
ORDENADOR REMOTO
680
681
PROGRAMAS DE APLICACIÓN REMOTA
685
662
TECLADO
672
661
RATÓN
695
INTERFAZ PERIFÉRICDA DE SALIDA
INTERFAZ DE RED
670
MÓDEM
660
INTERFAZ DE ENTRADA DE USUARIO
690
INTERFAZ DE VIDEO
BUS DE SISTEMA
621
656
655
650
INTERFAZ DE MEMORIA EXTRAÍBLE, NO VOLÁTIL
652
651
620
UNIDAD DE PROCESAMIENTO
640
INTERFAZ DE MEMORIA NO EXTRAÍBLE, NO VOLÁTIL
641
630
MEMORIA DEL SISTEMA
(ROM) 631
BIOS 633
(RAM) 632
SISTEMA OPERATIVO 634
PROGRAMAS DE APLICACIÓN 635
OTROS MÓDULOS DE PROGRAMA 636
DATOS DE PROGRAMA 637
DATOS DE PROGRAMA 647
OTROS MÓDULOS DE PROGRAMA 646
PROGRAMAS DE APLICACIÓN 645
SISTEMA OPERATIVO 644

FIG. 6