(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 870 509**

(51) Int. CI.:

H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.06.2016 PCT/US2016/038772**

(87) Fecha y número de publicación internacional: **29.12.2016 WO16209967**

(96) Fecha de presentación y número de la solicitud europea: **22.06.2016 E 16744947 (9)**

(97) Fecha y número de publicación de la concesión europea: **24.02.2021 EP 3314825**

(54) Título: **Método y sistema de mensajería e intercambio de contenido controlado por el emisor**

(30) Prioridad:

24.06.2015 US 201562183855 P
02.10.2015 US 201514874346

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.10.2021

(73) Titular/es:

PRIVATE GIANT (100.0%)
12472 Lake Underhill Road 113
Orlando, Florida 32828, US

(72) Inventor/es:

MURPHY, SHAUN;
MURPHY, CHARLES y
JOHNSON, RICHARD

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Método y sistema de mensajería e intercambio de contenido controlado por el emisor

Antecedentes

Campo

Esta divulgación se refiere en general a mensajería e intercambio de contenido. Más específicamente, esta divulgación se refiere a una plataforma de mensajería e intercambio de contenido con seguridad controlada por el emisor y otras características.

Técnica relacionada

Dado que un número creciente de usuarios se conectan en línea, descubren las satisfacciones y dificultades de la comunicación a través de Internet. Los usuarios encuentran que les gusta compartir contenido y comunicarse entre sí a través de Internet. Sin embargo, como muchos usuarios se ha dado cuenta demasiado tarde, una vez que su correo electrónico se ha enviado, ya no tienen control sobre cómo se está usando su correo electrónico. Sus correos electrónicos y otras comunicaciones pueden reenviarse a otros y difundirse rápidamente más allá de su audiencia prevista. Esto puede tener un efecto perjudicial o incluso devastador en el emisor original, que no tenía intención de que la audiencia lectora se expandiera más allá del destinatario original. Por lo tanto, se necesita una mejor forma para que los usuarios controlen sus comunicaciones.

El documento US 2015/149774 A1 en su resumen indica "Un sistema y método de gestión de derechos permite que los usuarios asocien políticas de gestión de derechos con documentos enviados a través de correo electrónico desde un cliente (por ejemplo, un ordenador o escáner). El cliente transmite información de destinatario de correo electrónico, incluyendo el tipo de atención ("para", "cc" o "cco") para cada destinatario, a un servidor de gestión de derechos".

Sumario

La invención se define por las reivindicaciones independientes adjuntas, con características ventajosas incluidas en las reivindicaciones dependientes.

La invención proporciona un sistema para enviar un objeto. Durante la operación, un dispositivo de envío recibe el objeto, en donde el objeto es un mensaje u otro contenido. El dispositivo de envío puede recibir una entrada de usuario para establecer permisos y/o reglas para el objeto. Un respectivo permiso indica una respectiva operación que un dispositivo de recepción puede realizar en el objeto, y una respectiva regla indica una operación que el dispositivo de recepción realiza cuando se produce una condición especificada en conexión con el objeto. El dispositivo de envío puede adjuntar los permisos y reglas al objeto. El dispositivo de envío envía, a continuación, una porción del objeto al dispositivo de recepción.

El dispositivo de envío puede generar un identificador único para una porción del objeto. El dispositivo de envío puede enviar, a continuación, la porción del objeto con el identificador único a un servidor. El identificador único se almacena opcionalmente a través de una tabla de consulta distribuida que incluye, pero sin limitación a, una tabla de troceo distribuida. El dispositivo de envío puede enviar, a continuación, el identificador único al dispositivo de recepción.

En algunas realizaciones, en una sesión de mensajería que implica una pluralidad de usuarios, el dispositivo de envío puede visualizar respuestas a cada usuario de acuerdo con una estructura jerárquica de modo que una respuesta a un mensaje en un hilo de mensajes se representa ramificándose del mensaje.

En algunas realizaciones, una regla es una de: denegar que el dispositivo de recepción reenvíe el mensaje; denegar que el dispositivo de recepción haga una captura de pantalla del objeto; denegar que el dispositivo de recepción imprima el objeto; denegar que el dispositivo de recepción descargue el objeto; requerir que el dispositivo de recepción borre un objeto después de hacer una captura de pantalla; y requerir que el dispositivo de recepción borre un objeto después de que el usuario vea el objeto.

En algunas realizaciones, el dispositivo de envío permite que el usuario envíe de forma anónima un mensaje y/u otro contenido a un servicio externo. El dispositivo de envío puede verificar la identidad del usuario, y permitir que el usuario reciba mensajes de otros y continúe la mensajería con otros usando la identidad verificada del usuario.

En algunas realizaciones, el dispositivo de envío visualiza una pluralidad de mensajes en vista de adjuntos de modo que el usuario puede ver únicamente los adjuntos, en los que un adjunto incluye una miniatura generada para cada archivo que es menor que el tamaño original del archivo.

En algunas realizaciones, un permiso indica si se permite que el dispositivo de recepción realice uno de lo siguiente: reenviar el mensaje y/o contenido; ocultar el mensaje y/o contenido; añadir un participante a un encabezamiento de mensaje que indica las partes que reciben el mensaje y respuestas asociadas; eliminar un participante del encabezamiento de mensaje que indica las partes que reciben el mensaje y respuestas asociadas; hacer una captura de pantalla que incluye el mensaje y/o contenido; seleccionar texto del mensaje y/o contenido; imprimir el mensaje y/o contenido; y descargar el mensaje y/o contenido a un almacenamiento externo.

En algunas realizaciones, el objeto se encripta con una clave simétrica y la clave simétrica se encripta con una clave pública del dispositivo de recepción. Adicionalmente, enviar la porción del objeto incluye adicionalmente encriptar el objeto y enviar una porción del objeto encriptado al dispositivo de recepción.

En algunas realizaciones, el dispositivo de envío puede recibir una entrada de usuario para especificar permisos para que otros accedan a y retrocedan un artículo en una ocultación.

En algunas realizaciones, el dispositivo de envío puede realizar reconocimiento óptico de caracteres en los adjuntos. El dispositivo de envío puede recibir, a continuación, una entrada de usuario que especifica un artículo de búsqueda, y buscar el artículo de búsqueda a través de los adjuntos y metadatos asociados.

Otra realización proporciona un sistema para recibir un objeto. Durante la operación, un dispositivo de recepción recibe el objeto, en donde el objeto es un mensaje u otro contenido. El dispositivo de recepción puede extraer permisos y/o reglas del objeto. Un respectivo permiso indica una respectiva operación que el dispositivo de recepción puede realizar en el objeto, y una respectiva regla indica una operación que el dispositivo de recepción realiza cuando se produce una condición especificada en conexión con el objeto. El dispositivo de recepción puede proporcionar, a continuación, el objeto a un usuario.

En algunas realizaciones, el objeto se encripta, y el desencriptado del objeto implica obtener una porción encriptada del objeto desde un servidor.

En algunas realizaciones, el dispositivo de recepción recibe entrada de usuario que especifica una operación a realizar en el objeto. El dispositivo de recepción puede determinar, a continuación, si se autoriza la operación basándose en las reglas y/o permisos del objeto. En respuesta a determinar que se autoriza la operación, el dispositivo de recepción puede realizar la operación en el objeto.

En algunas realizaciones, el objeto se encripta y la extracción de permisos incluye adicionalmente: el dispositivo de recepción desencripta y extrae una clave simétrica del mensaje usando una clave privada del dispositivo de recepción. El dispositivo de recepción desencripta, a continuación, el objeto con la clave simétrica.

Breve descripción de las figuras

La Figura 1 ilustra un entorno de red ilustrativo que facilita una plataforma de mensajería e intercambio de contenido con seguridad controlada por el emisor de acuerdo con una realización.
La Figura 2 presenta un diagrama de flujo que ilustra un método para enviar un mensaje y/o contenido a un destinatario de acuerdo con una realización.
La Figura 3 presenta un diagrama de flujo que ilustra un método para recibir un mensaje y/o contenido de acuerdo con una realización.
La Figura 4 presenta un diagrama de flujo que ilustra un método para acceder de forma anónima a un servicio externo de acuerdo con una realización.
La Figura 5 presenta una ilustración de una pantalla que permite que un usuario establezca reglas para un mensaje nuevo de acuerdo con una realización.
La Figura 6 presenta una ilustración de una pantalla que permite que un usuario cambie permisos en todos los destinatarios de un mensaje nuevo de acuerdo con una realización.
La Figura 7 presenta una ilustración de una pantalla que muestra una visualización jerárquica ilustrativa de mensajes de grupo de acuerdo con una realización.
La Figura 8 ilustra un sistema informático ilustrativo que facilita una plataforma de mensajería e intercambio de contenido con seguridad controlada por el emisor de acuerdo con una realización. En las figuras, los números de referencia similares se refieren a los mismos elementos de figura.

Descripción detallada

La siguiente descripción se presenta para permitir que cualquier experto en la técnica haga y use las realizaciones, y se proporciona en el contexto de una aplicación particular y sus requisitos. Diversas modificaciones a las realizaciones divulgadas serán fácilmente evidentes para los expertos en la materia, y los principios generales definidos en este documento pueden aplicarse a otras realizaciones y aplicaciones sin apartarse del espíritu y el alcance de la presente divulgación. Por lo tanto, la presente invención no está limitada a las realizaciones mostradas, sino que se le otorgará el alcance más amplio consistente con los principios y características divulgados en este documento.

Visión general

Realizaciones de la presente invención resuelven el problema de provisión de seguridad de mensajería e intercambio de contenido controlada por el usuario permitiendo que un usuario establezca reglas y permisos para controlar el uso y ciclo de vida de mensajes y/u otro contenido. Una plataforma y sistema de mensajería e intercambio de contenido incluye un cliente instalado en cada dispositivo móvil que permite que un emisor establezca permisos y reglas para un mensaje o contenido. Estos permisos y reglas otorgan al emisor un control completo sobre cómo una parte de recepción puede usar el mensaje y/o contenido. Por ejemplo, un emisor puede denegar que la parte de recepción reenvíe, haga una captura de pantalla, imprima o descargue el mensaje. El emisor también puede requerir que el dispositivo de recepción borre el mensaje después de hacer una captura de pantalla o después de que el usuario vea el mensaje. Obsérvese que realizaciones de la presente invención no se limitan a los ejemplos divulgados.

La plataforma de mensajería e intercambio de contenido también puede presentar una visualización jerárquica para mensajería de grupo que utiliza una estructura de árbol para ilustrar los hilos de una conversación cuando múltiples usuarios se están comunicando entre sí. Esto permite que el usuario siga fácilmente la conversación de grupo y ver quién está mensajeándose con quién en la conversación.

La plataforma de mensajería e intercambio de contenido también puede incluir una vista de solo adjuntos de modo que un usuario puede desplazarse verticalmente a través de la lista de archivos adjuntos y filtrar adjuntos para encontrar lo que necesitan. La vista de solo adjuntos puede aplicarse a todo el sistema (por ejemplo, en el buzón de entrada, vista de contactos y vista de mensaje). La vista de solo adjuntos puede estar disponible en cualquier sitio en el que un archivo puede asociarse con un objeto o acción de sistema. El sistema puede permitir archivos adjuntos grandes (por ejemplo, un terabyte o más). La gestión de archivos adjuntos grandes es transparente para el usuario y los propios usuarios no necesitan cargar de forma separada grandes archivos en otro servidor.

Algunas realizaciones también pueden incluir una característica de sin inicio de sesión que permite que un usuario use un servicio externo, tal como un servicio de redes sociales, sin inicio de sesión. El usuario puede usar el servicio de redes sociales de forma anónima para contactar a otros hasta que el usuario quiera autentificar su identidad con el servicio externo.

Entorno de red ilustrativo

La Figura 1 ilustra un entorno de red 100 ilustrativo que facilita una plataforma de mensajería e intercambio de contenido con seguridad controlada por el emisor de acuerdo con una realización. El entorno de red 100 puede incluir una red informática 102, que puede incluir cualquier red por cable o inalámbrica que interconecta diversos dispositivos informáticos entre sí, tales como una red informática implementada a través de una o más tecnologías (por ejemplo, Bluetooth, Wi-Fi, celular, Ethernet, fibra óptica, etc.). En algunas realizaciones, la red 102 incluye la Internet.

El entorno de red 100 también puede incluir un dispositivo informático 104, que un usuario 106 usa para comunicar un mensaje o contenido a otro dispositivo informático, tal como el dispositivo informático 110 o el dispositivo informático 112. El usuario 114 opera el dispositivo informático 110 y el usuario 116 opera el dispositivo informático 112. El usuario 106 puede usar un cliente de mensajería e intercambio de contenido 118 instalado en el dispositivo informático 104 para enviar mensajes u otro contenido a los otros usuarios. El mensaje o contenido puede ser texto, voz y/o vídeo. El software de cliente 118 permite que un usuario envíe mensajes, mensajes adjuntos, archivos y otro contenido. El dispositivo informático 110 y el dispositivo informático 112 también han instalado los clientes de mensajería e intercambio de contenido 120, 122 respectivamente. El usuario 106 también puede acceder de forma anónima a servicios externos, tales como el servicio de redes sociales 123. Aunque la Figura 1 representa dispositivo informático 104 como un teléfono inteligente, el dispositivo informático 104 puede ser también un ordenador personal o cualquier dispositivo que puede usar el usuario 106 para enviar mensajes o compartir un archivo/contenido con el usuario 112.

Un servidor de mensajería e intercambio de contenido 124 puede almacenar y ejecutar software de servidor, y puede almacenar contenido tal como archivos o adjuntos de mensajes que un usuario comparte con otros. El sistema puede dividir un archivo de modo que atacantes maliciosos tienen una mayor dificultad para encontrar y reensamblar las partes separadas del archivo encriptado. El servidor 124 puede almacenar pequeñas porciones de archivos encriptados y/o grandes porciones de los archivos encriptados. El sistema también puede enviar una gran porción de un archivo encriptado a un dispositivo de hardware de empresa, tal como un servidor de empresa 126, para el almacenamiento. Además, el sistema puede almacenar una gran porción del archivo encriptado usando servicios de almacenamiento en la nube, tal como el servidor de almacenamiento en la nube 128. Obsérvese que generalmente el sistema puede dividir objetos (encriptados o no), y almacenar una porción del objeto en una ubicación y el resto del objeto en cualquier número de otras ubicaciones.

Los objetos pueden incluir, pero sin limitación, imágenes, vídeos, documentos, mensajes de texto, correos

electrónicos y otros artículos digitales.

Permisos y reglas

Un usuario puede controlar el uso de mensajes u otro contenido usando permisos y reglas. Un permiso asociado con un objeto, tal como un mensaje y/o contenido, indica una operación que puede realizar un dispositivo de recepción en el objeto. El usuario puede establecer uno o más permisos para controlar las operaciones que pueden realizar los destinatarios con los mensajes/contenido. Por ejemplo, el usuario puede establecer permisos para permitir o impedir el reenvío de un mensaje, descargar localmente un adjunto y añadir/eliminar un participante en un mensaje de grupo. El usuario también puede establecer permisos para permitir o impedir que se haga una captura de pantalla, se imprima y/o archive un mensaje o contenido. El usuario puede establecer permisos por defecto que se aplican globalmente o por contacto. El usuario también puede establecer permisos detallados, tales como permisos que se aplican por usuario y/o por adjunto. Adicionalmente, el usuario puede cambiar los permisos en cualquier momento.

Una regla asociada con un objeto, tal como un mensaje y/o contenido, indica una operación que el dispositivo de recepción realiza cuando se produce una condición o evento especificado. Por ejemplo, una regla puede especificar que un dispositivo de recepción borre un mensaje y/o contenido después de que se ha leído. Otra regla puede especificar que un dispositivo de recepción borre un mensaje y/o contenido después de un cierto periodo de tiempo. Otro ejemplo de una regla es que se requiere que un dispositivo de recepción borre todos los mensajes y/o contenido enviado a un usuario si el usuario intenta hacer una captura de pantalla del mensaje y/o contenido. Como otro ejemplo, el usuario puede establecer una regla para controlar la duración de tiempo que el mensaje y/o contenido está disponible para los destinatarios. El usuario puede establecer reglas por defecto que se aplican globalmente o por nuevo mensaje y/o contenido enviado, y el usuario puede cambiar las reglas en cualquier momento.

Obsérvese que todos los objetos en el sistema se asocian con permisos y reglas, y las realizaciones de la presente invención no se limitan a los permisos y reglas de ejemplo. Cuando un dispositivo obtiene o genera un objeto, el dispositivo puede determinar los permisos y reglas asociados con el objeto y realizar operaciones en el objeto o gestionar el objeto de acuerdo con los permisos y reglas del objeto. Por ejemplo, objetos de mensaje, objetos de contenido almacenados y objetos de archivo adjunto se asocian todos con permisos y reglas y un dispositivo que obtiene o genera un objeto cumplirá con los permisos y reglas asociados con el objeto. Además, todo el sistema de mensajería e intercambio de contenido cumple con los permisos y reglas establecidos para objetos, y las realizaciones de la presente invención no se limitan a los objetos de ejemplo.

Además de permisos y reglas, el usuario también puede borrar un mensaje en todos los dispositivos. El usuario puede enviar un mensaje y, a continuación, retirar el mensaje. Si el destinatario reenvía un mensaje el usuario puede elegir borrar en todos los dispositivos, incluyendo cualquier mensaje reenviado, para retirar el mensaje reenviado. Retirando el mensaje de un dispositivo de recepción, el dispositivo de recepción ya no tiene acceso al mensaje. Adicionalmente, cuando un usuario reenvía un mensaje, el sistema puede garantizar que el usuario no ha modificado la información reenviada de ninguna forma. El sistema puede asegurar un mensaje de modo que el usuario puede no alterar el mensaje cuando se reenvía el mensaje a otro usuario. Un usuario puede no manipular o de otra manera alterar un mensaje y, a continuación, reenviar el mismo a otro usuario sin que los otros (por ejemplo, el usuario que recibe el mensaje reenviado y/o el usuario de envío) sepan de los cambios.

Envío de archivos grandes

El sistema también puede permitir enviar archivos adjuntos grandes, tales como adjuntos con tamaño de un terabyte, combinando almacenamiento en la nube con mensajería. Los sistemas de mensajería actuales se diseñan generalmente para almacenar y enviar mensajes de texto, archivos/objetos no binarios o archivos/objetos muy grandes. Un usuario puede enviar un archivo grande a través del sistema de mensajería sin que el usuario necesite descargar el archivo grande en un servicio de almacenamiento que puede tratar archivos grandes. El sistema puede dividir archivo encriptado grande en una pequeña porción que el sistema puede enviar con el mensaje y una gran porción que el sistema envía a un servidor remoto para almacenamiento y acceso por otros.

El sistema puede generar un enlace o referencia al archivo grande o una porción significativa del archivo grande e incluir el enlace con el mensaje. El sistema también puede generar un identificador único universal para el archivo grande. En general, el sistema puede asignar un identificador único universal a cada objeto. El identificador único universal no está vinculado con ningún usuario específico. Esto facilita enlaces de almacenamiento a contenido a través de una tabla de troceo distribuida de modo que el contenido no se almacena en un punto de almacenamiento central.

El sistema puede enviar el identificador único universal y el enlace al dispositivo de recepción y, en algunas realizaciones, también puede incluir una pequeña porción del archivo grande con el mensaje. El sistema puede enviar el archivo grande a un servidor con el identificador único universal.

El servidor puede almacenar datos que asocian el archivo adjunto con el identificador único. El sistema puede incluir

una tabla de troceo distribuida implementada a través de múltiples servidores para almacenar las asociaciones entre el identificador único y datos almacenados (por ejemplo, el archivo adjunto). Un servidor puede enviar el archivo adjunto a cualquier dispositivo que consulta datos usando el identificador único. Por ejemplo, cuando un dispositivo recibe un mensaje, el dispositivo obtiene el identificador único para recuperar el archivo adjunto grande. El usuario en el dispositivo de recepción no necesita saber que el archivo adjunto grande se recuperó de un servidor remoto (por ejemplo, un servicio de almacenamiento de archivos).

En algunas realizaciones, el sistema también puede proporcionan una vista de solo adjuntos. Cuando el usuario selecciona esta vista, el sistema oculta la porción de conversación y visualiza únicamente los adjuntos. El sistema puede visualizar múltiples imágenes de tamaños variables que indican al usuario los contenidos de los adjuntos. El sistema puede realizar reconocimiento óptico de caracteres en los adjuntos para permitir que el usuario busque a través de los adjuntos. El usuario puede desplazarse verticalmente a través de una lista de adjuntos para encontrar lo que está buscando el usuario. El usuario puede filtrar o clasificar los adjuntos de diferentes formas, tales como por fecha, nombre de archivo y/o nombre de emisor. El usuario puede buscar a través de metadatos en los adjuntos y también usar lógica booleana para combinar diferentes condiciones de clasificación y filtro. Por ejemplo, el usuario puede especificar clasificar de acuerdo con nombre y fecha. Además, cada archivo/adjunto puede tener una miniatura generada por cliente para cada archivo que es muy pequeña en tamaño y rápida de transferir. Esta miniatura puede generarse por un dispositivo de envío. Esto proporciona al destinatario una forma de ver una vista previa de resolución inferior de cada imagen, vídeo (por ejemplo, vista previa animada), documento de Word, etc. sin tener que descargar el documento original. Las características de vista de adjuntos también pueden incluir la capacidad o inteligencia para buscar contenido dentro y alrededor de los archivos (por ejemplo, reconocimiento óptico de caracteres, búsqueda de metadatos, etc.) para búsqueda y clasificación avanzada. Obsérvese que el software de correo electrónico actual requiere que el usuario vaya a través de mensajes de correo electrónico antiguos para encontrar adjuntos y esto puede ser muy incómodo y lento para un usuario ya que el usuario debe clicar en cada adjunto para ver los contenidos.

Obsérvese que el sistema de mensajería e informático descrito en este documento puede implementarse con un modelo de licencia y distribución de software como un servicio, y los clientes pueden licenciar el software para el sistema de mensajería e informático sobre una base de suscripción.

Envío de mensaje y/o contenido

La Figura 2 presenta un diagrama de flujo que ilustra un método para enviar un mensaje y/o contenido a un destinatario de acuerdo con una realización. Obsérvese que diferentes realizaciones pueden variar de acuerdo con el detalle y el orden de operaciones, y las realizaciones no se limitan a las operaciones específicas representadas en la figura. Durante la operación, el dispositivo de envío puede recibir inicialmente un mensaje tal y como se introduce por el usuario. El sistema también puede recibir contenido cargado por el usuario o seleccionado por el usuario (operación 202). El sistema también puede recibir reglas y permisos desde el usuario para el mensaje y/o contenido (operación 204). El sistema también puede usar reglas y permisos por defecto para el mensaje y/o contenido.

El dispositivo de envío puede encriptar, a continuación, el mensaje y/o contenido, que puede incluir reglas, permisos, un objeto de seguridad que incluye datos de permiso y de regla, un identificador único y/o cualquier otro dato (operación 206). El dispositivo de envío puede encriptar datos usando una clave simétrica, y encriptar, a continuación, la clave simétrica de forma separada para cada destinatario previsto usando una clave pública específica de destinatario. El sistema de dispositivo de envío envía las claves simétricas encriptadas a múltiples dispositivos. Los destinatarios de las claves simétricas encriptadas pueden usar su propia clave privada para desencriptar y extraer la clave simétrica, y usar la clave simétrica para desencriptar datos enviados desde el dispositivo de envío.

En general, el sistema puede encriptar todos los objetos usando una clave de encriptación simétrica por objeto, y el sistema encripta la clave para un objeto encriptado con clave simétrica usando encriptación asimétrica. Es decir, el dispositivo de envío necesita encriptar únicamente un objeto una vez usando una clave simétrica y, a continuación, encripta la clave simétrica específicamente para cada destinatario. El dispositivo de envío no necesita encriptar un objeto múltiples veces para diferentes destinatarios. Esto ahorra tiempo y es más eficiente porque algunos de los objetos pueden ser archivos adjuntos o contenido grandes (por ejemplo, 1 terabyte o más).

El sistema puede usar una clave simétrica diferente para encriptar cada objeto y no reutiliza una clave simétrica para encriptar un objeto diferente. Por ejemplo, el sistema usa una clave simétrica diferente para encriptar cada uno del mensaje, el adjunto de mensaje, un adjunto de miniatura y todos los demás objetos asociados con el mensaje. Por lo tanto, incluso si una parte maliciosa puede atacar y comprometer una clave simétrica (por ejemplo, para un adjunto), las otras claves simétricas permanecen intactas (por ejemplo, para otros objetos asociados con el mensaje).

El sistema puede generar un identificador único universal para identificar datos o porciones de los datos. Por ejemplo, el sistema (por ejemplo, dispositivo de envío) puede dividir un archivo grande en dos porciones y generar un identificador único para la porción más grande. El sistema puede enviar el identificador único a un dispositivo de recepción y al servidor. El identificador único funciona como una clave para una tabla de troceo distribuida. Esta

tabla de troceo distribuida puede implementarse a través de múltiples servidores. La tabla de troceo distribuida almacena la asociación entre los datos almacenados y el identificador único. El dispositivo de recepción puede enviar una consulta con el identificador único a cualquier servidor que implementa la tabla de troceo distribuida y/o almacena una copia de los datos. Obsérvese que el identificador único se almacena opcionalmente a través de una tabla de consulta distribuida que incluye, pero sin limitación a, una tabla de troceo distribuida. El dispositivo de recepción puede recuperar los datos de cualquier número de servidores ya que los datos pueden replicarse y almacenarse en múltiples servidores.

A continuación, el dispositivo de envío puede enviar una porción encriptada (o no encriptada) grande del mensaje y/o contenido de un tamaño predeterminado a un servidor de empresa o un servidor en la nube para su almacenamiento (operación 208). Por ejemplo, si el mensaje incluye un adjunto de archivo grande, el dispositivo de envío puede encriptar el archivo adjunto grande, y dividir el archivo (encriptado o no encriptado) en dos porciones (por ejemplo, los primeros 100 bytes del archivo para una porción pequeña y el resto del archivo para la porción grande). El dispositivo de envío puede enviar, a continuación, la porción más grande del archivo adjunto a un servidor desde el que puede recuperar el dispositivo de recepción. El sistema puede retener la porción pequeña de los datos y almacenar la misma localmente dentro de un almacenamiento seguro del sistema y, en algunas realizaciones, también puede incluir una copia de la porción pequeña cuando se envía un mensaje. Sin la porción pequeña de los datos, el dispositivo de recepción (y atacantes maliciosos) puede no ser capaz de juntar el conjunto de datos completo. En algunas realizaciones, el dispositivo de envío puede dividir el archivo encriptado (o un archivo no encriptado) en múltiples porciones que incluyen más de dos porciones, y las porciones pueden variar en tamaño. Por ejemplo, puede haber muchas piezas pequeñas, una grande y una pequeña, una grande y varias pequeñas, etc. Adicionalmente, el servidor también puede enviar todo el archivo adjunto grande encriptado o contenido a un servidor.

El sistema puede enviar una gran porción del archivo encriptado (o no encriptado) a un servidor que es uno de muchos dispositivos de hardware de empresa dentro de un entorno informático de empresa, o el servidor puede ser parte del sistema de mensajería e informático. En algunas realizaciones, el sistema también puede acceder a un servidor de un servicio en la nube (por ejemplo, almacenamiento en la nube de Dropbox o Google) en la Internet para enviar y almacenar datos.

El dispositivo de envío puede enviar, a continuación, el mensaje y/o contenido, que puede incluir reglas, permisos, el identificador único, el objeto de seguridad, la porción pequeña del archivo encriptado (o no encriptado) (o un enlace a la porción pequeña) y/o cualquier otro dato al dispositivo de recepción (operación 210). En algunas realizaciones, el dispositivo de envío puede enviar información de contacto, contraseñas, listas y borradores de mensajes a otros usuarios, encriptados o no encriptados, y puede revocar la información en un momento posterior o basándose en una condición establecida por el usuario del dispositivo de envío.

Si el dispositivo de envío recibe un comando de usuario para realizar una operación en el mensaje y/o contenido (operación 212), el dispositivo de envío puede enviar el comando al dispositivo de recepción para ejecutar el comando (operación 214). En algunas realizaciones, el dispositivo de recepción también puede reenviar el comando a otros dispositivos a los que se ha reenviado el mensaje.

En algunas implementaciones, el dispositivo de envío puede recibir datos desde un dispositivo informático que indica que recibieron una copia del mensaje reenviado. El dispositivo de envío puede enviar directamente el comando a cualquier dispositivo que ha recibido una copia del mensaje reenviado. Los dispositivos que reciben el comando pueden cumplir, a continuación, con el comando.

Recepción de mensaje y/o contenido

La Figura 3 presenta un diagrama de flujo que ilustra un método para recibir un mensaje y/o contenido de acuerdo con una realización. Obsérvese que diferentes realizaciones pueden variar de acuerdo con el orden de operaciones, y las realizaciones no se limitan a las operaciones específicas representadas en la figura.

Un dispositivo de recepción puede recibir inicialmente el mensaje y/o contenido (operación 302). El dispositivo de recepción puede recibir el mensaje y/o contenido desde un dispositivo que envió originalmente el mensaje y/o contenido, o desde un dispositivo que reenvió el mensaje y/o contenido. El dispositivo de recepción puede recibir el mensaje a través de un servidor de mensajería. El mensaje y/o contenido puede encriptarse (o no encriptarse) y el dispositivo de recepción puede desencriptar y/o extraer diversos datos del mensaje y/o contenido recibido. Estos datos pueden incluir uno o más de reglas, permisos, un identificador único universal, un enlace a una porción significativa de un archivo adjunto grande encriptado (y no encriptado) o contenido almacenado en un servidor remoto, una pequeña porción del archivo adjunto grande encriptado (y no encriptado) o contenido (por ejemplo, un archivo de tipo .zip pequeño), un objeto de seguridad y/o cualquier otro dato incluido con el mensaje (operación 304). En algunas realizaciones, el dispositivo de recepción puede recibir un enlace a una pequeña porción de un archivo adjunto grande u otro contenido, y consultar un servidor para la porción pequeña en lugar de recibir la porción pequeña con el mensaje.

El dispositivo de recepción puede obtener datos adicionales de un servidor si el mensaje y/o contenido indica que una porción de un archivo encriptado (o no encriptado) grande se almacena en otro sitio (operación 306). Por ejemplo, si el mensaje incluye un archivo adjunto grande, entonces el dispositivo de recepción puede recuperar una porción encriptada (o no encriptada) grande del archivo adjunto desde un servidor remoto. El dispositivo de recepción envía el identificador único a uno o más servidores a través de la red y, a continuación, recibe los correspondientes datos de vuelta desde un servidor. El dispositivo de recepción puede recuperar los datos almacenados (por ejemplo, archivo adjunto grande u otro contenido) desde uno cualquiera de múltiples servidores que replican los datos adicionales. El dispositivo de recepción puede combinar juntos, a continuación, las porciones divididas del archivo adjunto grande o contenido. Si el dispositivo de recepción puede desencriptar satisfactoriamente todo un archivo encriptado, entonces el dispositivo de recepción ha obtenido los datos correctos. Por ejemplo, si las porciones se encriptan, entonces el archivo encriptado completo es una combinación de una pieza encriptada y un resto encriptado. El archivo encriptado completo puede desencriptarse, a continuación, usando la clave simétrica mientras que la pieza encriptada o resto encriptado no se desencriptarían independientes el uno del otro. La porción grande (por ejemplo, archivo restante) puede estar disponible públicamente en Dropbox, un servidor web, etc. Un archivo diferenciado (por ejemplo, una porción mucho más pequeña) puede transmitirse o almacenarse de forma segura en algún otro sitio. El dispositivo de recepción puede aplicar el archivo diferenciado al resto del archivo para generar un archivo igual al archivo original (encriptado o no). Obsérvese que, en algunos escenarios, un dispositivo puede combinar juntas las porciones de un archivo no encriptado.

Obsérvese que múltiples servidores pueden implementar una tabla de troceo distribuida que almacena asociaciones entre el identificador único universal y objetos tales como archivos adjuntos o contenido. El identificador único puede funcionar como una clave de consulta para la tabla de troceo distribuida. Los servidores pueden consultar la tabla de troceo distribuida para identificar el objeto correcto para volver a un dispositivo que envía una consulta usando un correspondiente identificador único.

La tabla de troceo distribuida también puede almacenar claves públicas para usuarios o dispositivos de recepción, de modo que un dispositivo de envío puede solicitar una clave pública para cualquier destinatario potencial. El dispositivo de envío puede obtener claves públicas para múltiples destinatarios, y puede enviar a cada destinatario la misma clave simétrica, aunque la clave simétrica se encripta usando la clave pública de cada destinatario. Cada destinatario puede desencriptar y extraer la clave simétrica usando su propia calve privada específica.

Ya que los datos almacenados se replican y distribuyen en diferentes servidores, existen múltiples formas en las que el dispositivo de recepción puede obtener los datos almacenados. En algunas realizaciones, el dispositivo de recepción puede intentar recuperar los datos almacenados enviando una consulta con la clave de identificador único a un dispositivo de hardware local o un dispositivo informático de empresa. El dispositivo de hardware local puede devolver los datos o puede proporcionar al dispositivo de recepción información sobre servidores que almacenan los datos y sus respectivas velocidades de descarga, incluyendo qué servidores proporcionan una velocidad de descarga más rápida. El dispositivo de recepción puede intentar recuperar los datos almacenados enviando una consulta a servidores con acceso a la tabla de troceo distribuida y/o copias almacenadas de los datos, y recibir datos desde un servidor que se conoce como confiable. El dispositivo de recepción también puede recuperar datos enviando la consulta con la clave de identificador único a un servidor que es parte del sistema de mensajería y comunicación (por ejemplo, el software como un servicio). En algunos casos puede ser más rápido que el dispositivo de recepción acceda a un dispositivo de hardware de empresa para recuperar datos a través de una red de área local, pero si el dispositivo de recepción no tiene acceso al dispositivo de hardware de empresa, entonces el dispositivo de recepción puede acceder a los datos desde el software como un servicio.

El dispositivo de recepción puede visualizar, a continuación, el mensaje o de otra manera facilitar el contenido al usuario del dispositivo de recepción (operación 308).

Si el dispositivo de recepción recibe una entrada de usuario que indica una operación en el mensaje y/o contenido (operación 310), el dispositivo de recepción puede determinar si se autoriza la operación basándose en las reglas y permisos (operación 312). Si se autoriza la operación, entonces el dispositivo de recepción puede ejecutar la operación en el mensaje y/o contenido (operación 314). El dispositivo de recepción continúa gestionando el mensaje y/o contenido mientras cumple con las reglas y permisos (operación 316). Por ejemplo, el dispositivo de recepción puede determinar cuándo borrar un objeto basándose en una regla asociada con el objeto. Como otro ejemplo, el dispositivo de recepción puede recibir peticiones posteriores para realizar operaciones en el mensaje y/o contenido y el dispositivo de recepción puede realizar únicamente tales operaciones cuando se autorizan por los permisos y reglas.

Acceso de forma anónima al servicio externo

La Figura 4 presenta un diagrama de flujo que ilustra un método para acceder de forma anónima a un servicio externo de acuerdo con una realización. Obsérvese que diferentes realizaciones pueden variar de acuerdo con el orden de operaciones, y las realizaciones no se limitan a las operaciones específicas representadas en la figura. Además, algunas realizaciones pueden ejecutar el proceso de la Figura 4 en su totalidad en un dispositivo móvil, mientras en otras realizaciones, un dispositivo móvil puede usar un servidor para acceder de forma anónima a

servicios externos.

El sistema puede incluir una característica de sin inicio de sesión que permite que un usuario añada y use un servicio externo, tal como un servicio de redes sociales, sin iniciar sesión en el servicio externo. El servicio externo puede ser un proveedor de servicio, tal como Twitter o un proveedor de servicio de mensajería de texto SMS. El sistema actúa como un intermediario que permite que el usuario acceda de forma anónima a los servicios externos. Por ejemplo, el usuario puede usar de forma anónima el servicio de redes sociales para contactar (por ejemplo, correo electrónico o mensaje de texto) o enviar datos a otros hasta que el usuario quiera autenticar esta identidad con el servicio de redes sociales. El sistema proporciona al usuario un ID de usuario anónimo y el usuario únicamente necesita indicar la identidad de la otra parte con la que quiere comunicarse el usuario. La otra parte ve que el mensaje procede de un ID de usuario anónimo. En una realización, la parte de recepción recibe un mensaje con un enlace, y el mensaje informa a la parte de recepción que un usuario anónimo está intentando comunicarse con la parte de recepción o enviar un archivo a la parte de recepción. La parte de recepción puede clicar, a continuación, en el enlace para ver el mensaje u obtener el archivo.

En algunas realizaciones, el usuario puede autenticarse a sí mismo en el sistema usando un inicio de sesión asociado con un servicio externo, tal como una dirección de correo electrónico, una cuenta de Twitter o una cuenta de Facebook. El sistema puede verificar que el usuario es propietario de la cuenta de inicio de sesión en el servicio externo. El sistema también puede verificar cómo otros usuarios pueden enviar un mensaje al usuario a través del servicio externo usando el inicio de sesión (por ejemplo, dirección de correo electrónico, número de SMS, nombre de usuario social, etc.). Después de que el usuario se autentica a sí mismo para un servicio externo particular, el sistema puede revelar la identidad verdadera del usuario en el servicio externo a los destinatarios de comunicaciones anónimas y/u otros datos del usuario. Después de que se revela la identidad del usuario, el usuario recibiría directamente datos de mensajes y de contenido de otros usuarios en el servicio externo.

Durante un proceso sin inicio de sesión, el sistema puede recibir inicialmente una selección de usuario de un servicio externo y una entrada de usuario de un mensaje y/o contenido (operación 402). El usuario también puede seleccionar contenido de su dispositivo local o en una red. El sistema puede enviar, a continuación, la comunicación de usuario y/o contenido como un usuario anónimo al servicio externo (operación 404). Por ejemplo, el sistema puede enviar el mensaje "¿Cómo estás?" a otro usuario en un servicio de redes sociales. El otro usuario recibirá el mensaje, pero sin ninguna información que identifica quién era el emisor.

El sistema puede recibir, a continuación, una entrada de usuario que verifica la identidad del usuario para un servicio externo particular (operación 406). El sistema puede verificar la identidad de usuario con el servicio externo. El sistema puede usar, a continuación, la identidad de usuario verificada para el servicio externo (operación 408).

Establecimiento de reglas para un mensaje nuevo

La Figura 5 presenta una ilustración de una pantalla que permite que un usuario establezca reglas para un mensaje nuevo de acuerdo con una realización. Como se ilustra en la Figura 5, una pantalla 500 visualiza un área de entrada de texto de mensaje nuevo 502. El mensaje se dirige a un destinatario Lisa. El usuario puede establecer cuándo el sistema borrará el mensaje. En la pantalla representada el usuario ha ajustado el ajuste "borrar después" 504 de modo que el sistema (por ejemplo, un dispositivo de recepción) borrará el mensaje después de que una parte de recepción vea por primera vez el mensaje. También, el usuario puede ajustar un botón de "borrar después de una captura de pantalla" 506 (por ejemplo, habilitado en la actualidad) de modo que el sistema borrará el mensaje después de que el dispositivo de recepción haga una captura de pantalla del mensaje. El usuario también puede ajustar un botón de "notificar después de una captura de pantalla" 508 de modo que se notifica a la parte de envío de cualquier captura de pantalla hecha por las partes de recepción. En la pantalla representada, el botón 508 se establece a una posición deshabilitada, de forma que no se notifica a la parte de envío las capturas de pantallas hechas por las partes receptoras. El sistema incluye un ajuste 510 que permite que el usuario seleccione si las reglas se aplican a todos los destinatarios o una selección de destinatarios.

Cambio de permisos en destinatarios de mensaje nuevo

La Figura 6 presenta una ilustración de una pantalla que permite que un usuario cambie permisos en todos los destinatarios de un mensaje nuevo de acuerdo con una realización. Como se ilustra en la Figura 6, una pantalla 600 visualiza un área de entrada de texto de mensaje 602. El mensaje se dirige a un destinatario Lisa. El usuario puede ajustar un botón de reenvío 604 (por ejemplo, habilitado en la actualidad) para permitir que otros usuarios reenvíen el mensaje, y puede ajustar un botón de ocultación 606 (por ejemplo, habilitado en la actualidad) para permitir que otros usuarios oculten (por ejemplo, archive o mueva a una carpeta para su almacenamiento y/o clasificación) el mensaje.

Una ocultación es también una ubicación sincronizada a través de todos los dispositivos de usuario para borradores de mensaje, archivos cargados, notas, contraseñas, objetos etc. que pueden enviarse o compartirse, a continuación, a través de la plataforma. La ocultación puede funcionar como un disco duro virtual. La ocultación permite que el usuario guarde objetos versionados de todos los tipos al sistema distribuido para una vista posterior, intercambio,

colaboración y edición en grupo y envío. Un usuario puede poner sus artículos en ocultación para hacer que aparezca en todos los demás dispositivos del usuario. Todo lo almacenado con ocultación puede encriptarse. Únicamente el usuario y las personas que especifica el usuario pueden ver/editar, etc. tener el poder de retroceder a versiones antiguas, ver miniaturas (por ejemplo, similares a la vista de adjuntos), y buscar/clasificar de una manera similar a mensajes y adjuntos. Algunos ejemplos de características de ocultación incluyen, pero sin limitación, borradores de mensaje, archivos y notas.

Borradores de mensaje - estos son mensajes que un usuario comenzó a redactar y desea continuar editando en un dispositivo diferente o pasar a un usuario diferente para su edición. El borrador de mensaje puede o no encriptarse, y pueden darse diversos niveles de permisos al emisor y cualquier visualizador/editor para acceder al borrador de mensaje. Pueden guardarse y retrocederse múltiples versiones, y el usuario puede ver las diferencias entre versiones, etc. Algunas realizaciones también pueden soportar archivos que se han cargado al sistema y adjuntado, pero no enviados.

Archivos - este es un servicio de alojamiento de archivos seguro y protegido. Un usuario puede cargar uno a muchos archivos y carpetas, asignar permisos sobre quién puede ver/acceder/editar, asignar etiquetas para clasificar un archivo y establecer recordatorios para realizar alguna acción en el archivo. Algunas realizaciones también pueden soportar todas las características de creación de versiones, diferencias visibles de retroceso, etc.

Notas - incluye, pero sin limitación, texto de formato libre, imágenes, vídeo, ubicación de Sistema de Posicionamiento Global (GPS), mapas, voz, etc. con la capacidad de tomar notas. Los usuarios pueden etiquetar, adjuntar archivos, asignar permisos, establecer recordatorios y usar capacidades de creación de versiones.

El usuario también puede ajustar un botón 608 para permitir que otros usuarios añadan participantes (por ejemplo, deshabilitado en la actualidad), y puede ajustar un botón de "eliminar participantes" 610 (por ejemplo, habilitado en la actualidad) para permitir que otros usuarios eliminen participantes. Obsérvese que el usuario también puede cambiar permisos para un único destinatario o cualquier conjunto de destinatarios. Otros ejemplos de permisos incluyen, pero sin limitación, impresión, selección de texto y descarga externa.

Visualización jerárquica de mensajes de grupo

La Figura 7 presenta una ilustración de una pantalla que muestra una visualización jerárquica ilustrativa de mensajes de grupo de acuerdo con una realización. El sistema también puede incluir una estructura jerárquica y visualización jerárquica para mensajería de grupo. El sistema gestiona y almacena datos de mensajería de grupo usando una estructura jerárquica. Esta visualización jerárquica utiliza una estructura de árbol para ilustrar los hilos de una conversación cuando múltiples usuarios se están comunicando entre sí. El usuario puede seguir fácilmente, a continuación, los hilos de la conversación de grupo y ver quién está respondiendo a quién en la conversación. El software de mensajería de grupo existente habitualmente únicamente visualiza una interfaz con desplazamiento vertical que visualiza cada mensaje a medida que un usuario envía el mensaje. Es difícil que un usuario siga los diferentes hilos de una conversación de grupo con el software de mensajería de grupo existente.

Como se ilustra en la Figura 7, una pantalla 700 visualiza una sesión de mensajería de grupo entre los usuarios Rey, Henry y Brian. Los tres usuarios se representan en el visualizador de panel de usuarios 702. Los mensajes en la sesión de mensajería de grupo pueden organizarse en una visualización jerárquica. Esta visualización jerárquica se asemeja a una estructura de árbol que permite que el usuario siga fácilmente los hilos de conversación, ya que las respuestas a un mensaje se visualizan como anidadas dentro de (por ejemplo, ramificándose de) el mensaje.

Una imagen u otro icono de usuario (por ejemplo, las imágenes 704a, 704b, 704c, 704d) que representa a cada usuario y un correspondiente mensaje pueden sangrarse dentro de área de pantalla 706 para mostrar respuestas a la pregunta de Henry. Por ejemplo, el usuario puede seguir más fácilmente las respuestas a la pregunta de Henry (por ejemplo, "¿Chipotle?") ya que las respuestas en el área de pantalla 706 están sangradas para mostrar que las respuestas se aniden dentro de la pregunta original. En algunas implementaciones, el área de pantalla 706 puede sombrearse con un destacado en gris claro o algún otro sombreado o color para indicar respuestas a la pregunta de Henry. Una caja de entrada de mensaje 708 permite que un usuario introduzca una pregunta a enviar a participantes en el grupo de mensajería (por ejemplo, "¿Qué tal unas alitas?").

En algunas implementaciones, un usuario puede clicar en un mensaje de respuesta en un hilo de conversación para provocar que el sistema visualice el mensaje original al que se dirige el mensaje de respuesta. Por ejemplo, un usuario puede clicar en una caja de visualización de mensaje 710 que visualiza "Suena bien" y, a continuación, el sistema hará emerger y visualizará el mensaje original que comenzó el hilo (por ejemplo, "¿Chipotle?"). El sistema puede visualizar el indicador visual emergente que indica el contenido y emisor para el mensaje "¿Chipotle?" que inició el hilo. El sistema también puede responder al usuario que clica en el indicador visual emergente navegando al mensaje original "¿Chipotle?" y poner en gris los mensajes de respuesta en el hilo. Esto hace más fácil navegar hilos orientados a empresa con un gran número de mensajes. Algunas realizaciones también pueden visualizar una horquilla en un hilo cuando un usuario reenvía un mensaje.

La Figura 8 ilustra un sistema informático ilustrativo que facilita una plataforma de mensajería e intercambio de contenido con seguridad controlada por el emisor de acuerdo con una realización. En este ejemplo, un sistema 800 para mensajería e intercambio de contenido puede incluir, pero sin limitación, un procesador 802, un dispositivo de memoria 804 y un dispositivo de almacenamiento 806. El sistema 800 puede incluir opcionalmente un módulo de visualización 808, un módulo de entrada 810 y un módulo de comunicación 812. En algunas realizaciones, el sistema 800 puede implementarse en un dispositivo móvil, y en otras realizaciones, también pueden implementarse uno o más componentes del sistema 800 en otro dispositivo informático, tal como un servidor.

El dispositivo de almacenamiento 806 puede almacenar instrucciones que cuando se cargan en la memoria 804 y ejecutan por el procesador 802 provocan que el procesador 802 realice las operaciones anteriormente mencionadas (por ejemplo, para un dispositivo de envío o un dispositivo de recepción). Más específicamente, las instrucciones almacenadas en dispositivo de almacenamiento 806 puede incluir un módulo de encriptado/desencriptado 814, un módulo de seguridad 816 y un módulo de gestión de identidad 818.

El módulo de encriptado/desencriptado 814 encripta y desencripta objetos tales como mensajes, adjuntos y otros objetos de contenido. El módulo de seguridad 816 gestiona las reglas y permisos asociados con objetos. El módulo de gestión de identidad 818 verifica la identidad del usuario. Puede verificar la identidad del usuario con servicios externos tales como Twitter, correo electrónico y Facebook. El módulo de gestión de identidad 818 también puede actuar como un intermediario para el usuario cuando el usuario busca usar servicios externos de forma anónima. En algunas realizaciones, el módulo de gestión de identidad 818 puede implementarse en un servidor, y un dispositivo móvil puede interactuar con un servidor que ejecuta el módulo de gestión de identidad 818 para acceder a servicios externos de forma anónima.

Las estructuras de datos y código descritos en esta descripción detallada se almacenan habitualmente en un medio de almacenamiento legible por ordenador, que puede ser cualquier dispositivo o medio que puede almacenar código y/o datos para su uso por un sistema informático. El medio de almacenamiento legible por ordenador incluye, pero sin limitación, memoria volátil, memoria no volátil, dispositivos de almacenamiento magnético y óptico tal como unidades de disco, cinta magnética, CD (discos compactos), DVD (discos versátiles digitales o discos de vídeo digital), u otros medios que pueden almacenar medios legibles por ordenador conocidos ahora o desarrollados más adelante.

Los métodos y procesos descritos en la sección de descripción detallada pueden incorporarse como código y/o datos, que pueden almacenarse en un medio de almacenamiento legible por ordenador como se describe anteriormente. Cuando un sistema informático lee y ejecuta el código y/o los datos almacenados en el medio de almacenamiento legible por ordenador, el sistema informático realiza los métodos y procesos incorporados como estructuras de datos y código y almacenados dentro del medio de almacenamiento legible por ordenador.

Adicionalmente, los métodos y procesos descritos anteriormente pueden incluirse en módulos de hardware. Por ejemplo, los módulos de hardware pueden incluir, pero sin limitación, chips de circuito integrado específico de aplicación (ASIC), campos de matriz de puertas programables (FPGA) y otros dispositivos de lógica programable conocidos actualmente o desarrollados más adelante. Cuando los módulos de hardware se activan, los módulos de hardware realizan los métodos y procesos incluidos dentro de los módulos de hardware.

Las descripciones anteriores de realizaciones de la presente invención se han presentado únicamente para propósitos de ilustración y descripción. No pretenden ser exhaustivas o limitar la presente invención a las formas divulgadas. En consecuencia, para los expertos en la técnica serán evidentes muchas modificaciones y variaciones. Además, la divulgación anterior no pretende limitar la presente invención. El alcance de la presente invención se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para enviar un objeto que comprende:

recibir (202) el objeto en un servidor de mensajería y contenido (124), en donde el objeto es un mensaje y/o contenido;
recibir (204) por el servidor de mensajería y contenido (124) una entrada de usuario, a través de un medio de entrada, para establecer permisos y reglas para el objeto, en donde un respectivo permiso indica una respectiva operación que un dispositivo de recepción puede realizar en el objeto, y en donde una respectiva regla indica una operación que se requiere que realice el dispositivo de recepción cuando se produce una condición especificada en conexión con el objeto;
encriptar (206) por el servidor de mensajería y contenido (124) el objeto;
adjuntar por el servidor de mensajería y contenido (124) los permisos y reglas al objeto;
generar un identificador único para una porción del objeto, para identificar una porción del objeto;
enviar la porción del objeto con el identificador único a un servidor; y
enviar (210) por el servidor de mensajería y contenido (124) al menos una porción restante del y el identificador único al dispositivo de recepción.

2. El método de la reivindicación 1, en donde el identificador único se almacena opcionalmente a través de una tabla de consulta distribuida que incluye, pero sin limitación a, una tabla de troceo distribuida.

3. El método de la reivindicación 1, que comprende adicionalmente en una sesión de mensajería que implica una pluralidad de usuarios visualizar respuestas a cada usuario de acuerdo con una estructura jerárquica de modo que una respuesta a un mensaje en un hilo de mensajes se representa ramificándose del mensaje.

4. El método de la reivindicación 1, en donde una regla es una de:

denegar que el dispositivo de recepción haga una captura de pantalla del objeto;
denegar que el dispositivo de recepción imprima el objeto;
denegar que el dispositivo de recepción descargue el objeto;
requerir que el dispositivo de recepción borre un objeto después de hacer una captura de pantalla; y
requerir que el dispositivo de recepción borre un objeto después de que el usuario vea el objeto.

5. El método de la reivindicación 1, que comprende adicionalmente:

permitir que el usuario envíe de forma anónima un mensaje y/o contenido a un servicio externo;
verificar la identidad del usuario; y
permitir que el usuario reciba mensajes de otros y continúe la mensajería con otros usando la identidad verificada del usuario.

6. El método de la reivindicación 1, que comprende adicionalmente:
visualizar una pluralidad de mensajes en vista de adjuntos de modo que el usuario puede ver únicamente los adjuntos, en donde un adjunto incluye una miniatura generada para cada archivo que es menor que el tamaño original del archivo.

7. El método de la reivindicación 1, en donde un permiso indica si se permite que el dispositivo de recepción realice uno de lo siguiente:

ocultar el mensaje y/o contenido;
eliminar un participante del encabezamiento de mensaje que indica las partes que reciben el mensaje y respuestas asociadas;
hacer una captura de pantalla que incluye el mensaje y/o contenido; seleccionar texto del mensaje y/o contenido;
imprimir el mensaje y/o contenido; y
descargar el mensaje y/o contenido a un almacenamiento externo.

8. El método de la reivindicación 1, en donde el objeto se encripta con una clave simétrica y la clave simétrica se encripta con una clave pública del dispositivo de recepción; y en donde enviar la porción del objeto comprende además:
enviar una porción del objeto encriptado al dispositivo de recepción.

9. El método de la reivindicación 1, que comprende adicionalmente recibir una entrada de usuario para especificar permisos para que otros accedan a y retrocedan un artículo en una ocultación.

10. El método de la reivindicación 1, que comprende adicionalmente:

realizar reconocimiento óptico de caracteres en los adjuntos;

recibir una entrada de usuario que especifica un artículo de búsqueda, y buscar el artículo de búsqueda a través de los adjuntos y metadatos asociados.

11. Un medio de almacenamiento legible por ordenador no transitorio que almacena instrucciones que cuando se ejecutan por un ordenador provocan que el ordenador realice un método para enviar un objeto, comprendiendo el método:

recibir (202) el objeto por un servidor de mensajería y contenido (124), en donde el objeto es un mensaje y/o contenido;
encriptar (206) el objeto por el servidor de mensajería y contenido;
recibir (204) una entrada de usuario en el servidor de mensajería y contenido para establecer permisos y reglas para el objeto, en donde un respectivo permiso indica una respectiva operación que un dispositivo de recepción puede realizar en el objeto, y en donde una respectiva regla indica una operación que el dispositivo de recepción realiza cuando se produce una condición especificada en conexión con el objeto;
adjuntar, por el servidor de mensajería y contenido, los permisos y reglas al objeto;
generar un identificador único para una porción del objeto, para identificar una porción del objeto;
enviar la porción del objeto con el identificador único a un servidor; y
enviar (210) por el servidor de mensajería y contenido (124) al menos una porción restante del objeto y el identificador único al dispositivo de recepción.

12. El medio de almacenamiento de la reivindicación 11, en donde el identificador único se almacena opcionalmente a través de una tabla de consulta distribuida que incluye, pero sin limitación a, una tabla de troceo distribuida.

13. El medio de almacenamiento de la reivindicación 11, en donde el método comprende adicionalmente:
en una sesión de mensajería que implica una pluralidad de usuarios visualizar respuestas a cada usuario de acuerdo con una estructura jerárquica de modo que una respuesta a un mensaje en un hilo de mensajes se representa ramificándose del mensaje.

14. El medio de almacenamiento de la reivindicación 11, en donde una regla es una de:

denegar que el dispositivo de recepción haga una captura de pantalla del objeto;
denegar que el dispositivo de recepción imprima el objeto; denegar que el dispositivo de recepción descargue el objeto; requerir que el dispositivo de recepción borre un objeto después de hacer una captura de pantalla; y
requerir que el dispositivo de recepción borre un objeto después de que el usuario vea el objeto.

15. El medio de almacenamiento de la reivindicación 11, en donde el método comprende adicionalmente:

permitir que el usuario envíe de forma anónima un mensaje y/o contenido a un servicio externo; verificar la identidad del usuario; y
permitir que el usuario reciba mensajes de otros y continúe la mensajería con otros usando la identidad verificada del usuario.

16. El medio de almacenamiento de la reivindicación 11, en donde un permiso indica si se permite que el dispositivo de recepción realice uno de lo siguiente:

ocultar el mensaje y/o contenido;
eliminar un participante del encabezamiento de mensaje que indica las partes que reciben el mensaje y respuestas asociadas;
hacer una captura de pantalla que incluye el mensaje y/o contenido
seleccionar texto del mensaje y/o contenido; imprimir el mensaje y/o contenido; y
descargar el mensaje y/o contenido a un almacenamiento externo.

17. Un sistema que comprende:

un procesador (802);
una memoria (804); y
un medio de almacenamiento legible por ordenador no transitorio (806) que almacena instrucciones que cuando se ejecutan por un ordenador provocan que el ordenador realice un método para enviar un objeto, comprendiendo el método:

recibir (202) el objeto por un servidor de mensajería y contenido (124), en donde el objeto es un mensaje y/o contenido;
encriptar (206) el objeto por el servidor de mensajería y contenido (124);
recibir (204) una entrada de usuario en el servidor de mensajería y contenido (124) para establecer permisos y reglas para el objeto, en donde un respectivo permiso indica una respectiva operación que un dispositivo de recepción puede realizar en el objeto, y en donde una respectiva regla indica una operación que se requiere

que realice el dispositivo de recepción cuando se produce una condición especificada en conexión con el objeto;

adjuntar, por el servidor de mensajería y contenido (124), los permisos y reglas al objeto;
generar un identificador único para una porción del objeto, para identificar una porción del objeto;
enviar la porción del objeto con el identificador único a un servidor; y
enviar (210) por el servidor de mensajería y contenido (124) al menos una porción restante del objeto y el identificador único al dispositivo de recepción.

18. El sistema de la reivindicación 17, en donde el identificador único se almacena opcionalmente a través de una tabla de consulta distribuida que incluye, pero sin limitación a, una tabla de troceo distribuida.

19. El sistema de la reivindicación 17, en donde el método comprende adicionalmente:

permitir que el usuario envíe de forma anónima un mensaje y/o contenido a un servicio externo;
verificar la identidad del usuario; y
permitir que el usuario reciba mensajes de otros y continúe la mensajería con otros usando la identidad verificada del usuario.

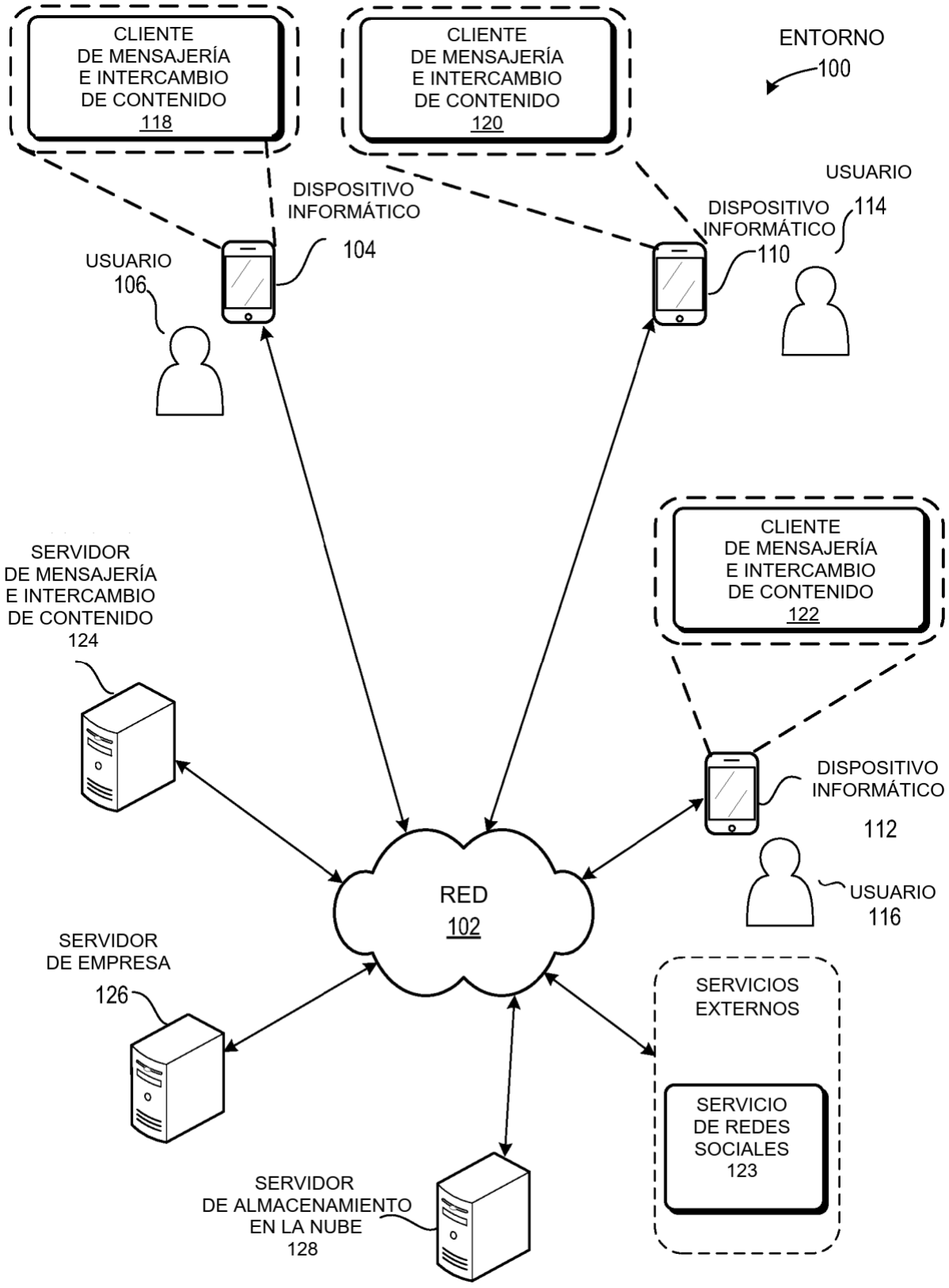
CLIENTE
DE MENSAJERÍA
E INTERCAMBIO
DE CONTENIDO
118
CLIENTE
DE MENSAJERÍA
E INTERCAMBIO
DE CONTENIDO
120
ENTORNO
100
USUARIO
DISPOSITIVO
INFORMÁTICO
104
USUARIO
106
DISPOSITIVO
INFORMÁTICO
110
USUARIO
114
CLIENTE
DE MENSAJERÍA
E INTERCAMBIO
DE CONTENIDO
122
SERVIDOR
DE MENSAJERÍA
E INTERCAMBIO
DE CONTENIDO
124
DISPOSITIVO
INFORMÁTICO
112
USUARIO
116
RED
102
SERVIDOR
DE EMPRESA
126
SERVICIOS
EXTERNOS
SERVICIO
DE REDES
SOCIALES
123
SERVIDOR
DE ALMACENAMIENTO
EN LA NUBE
128

FIG. 1

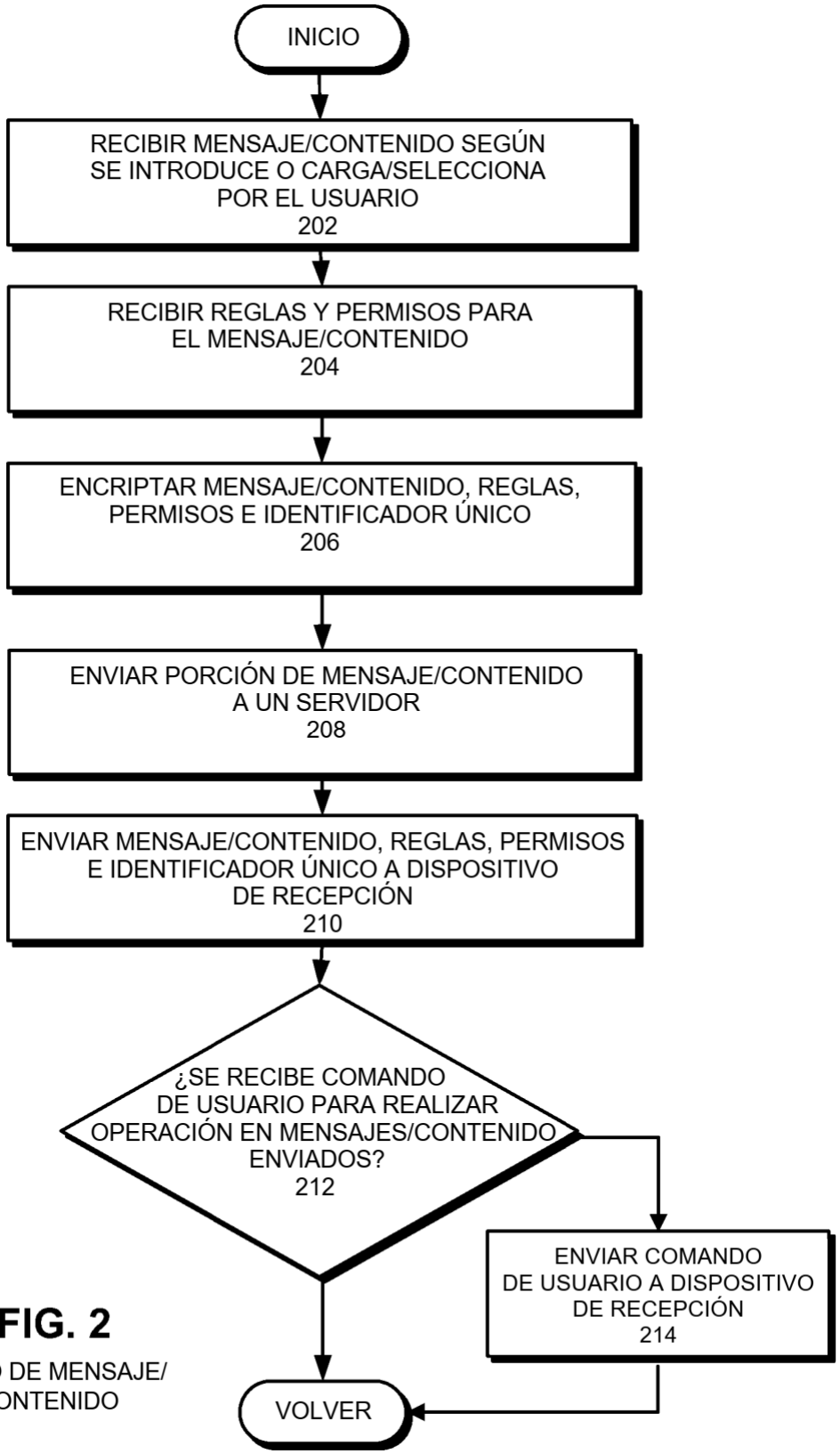

FIG. 2

ENVÍO DE MENSAJE/ CONTENIDO

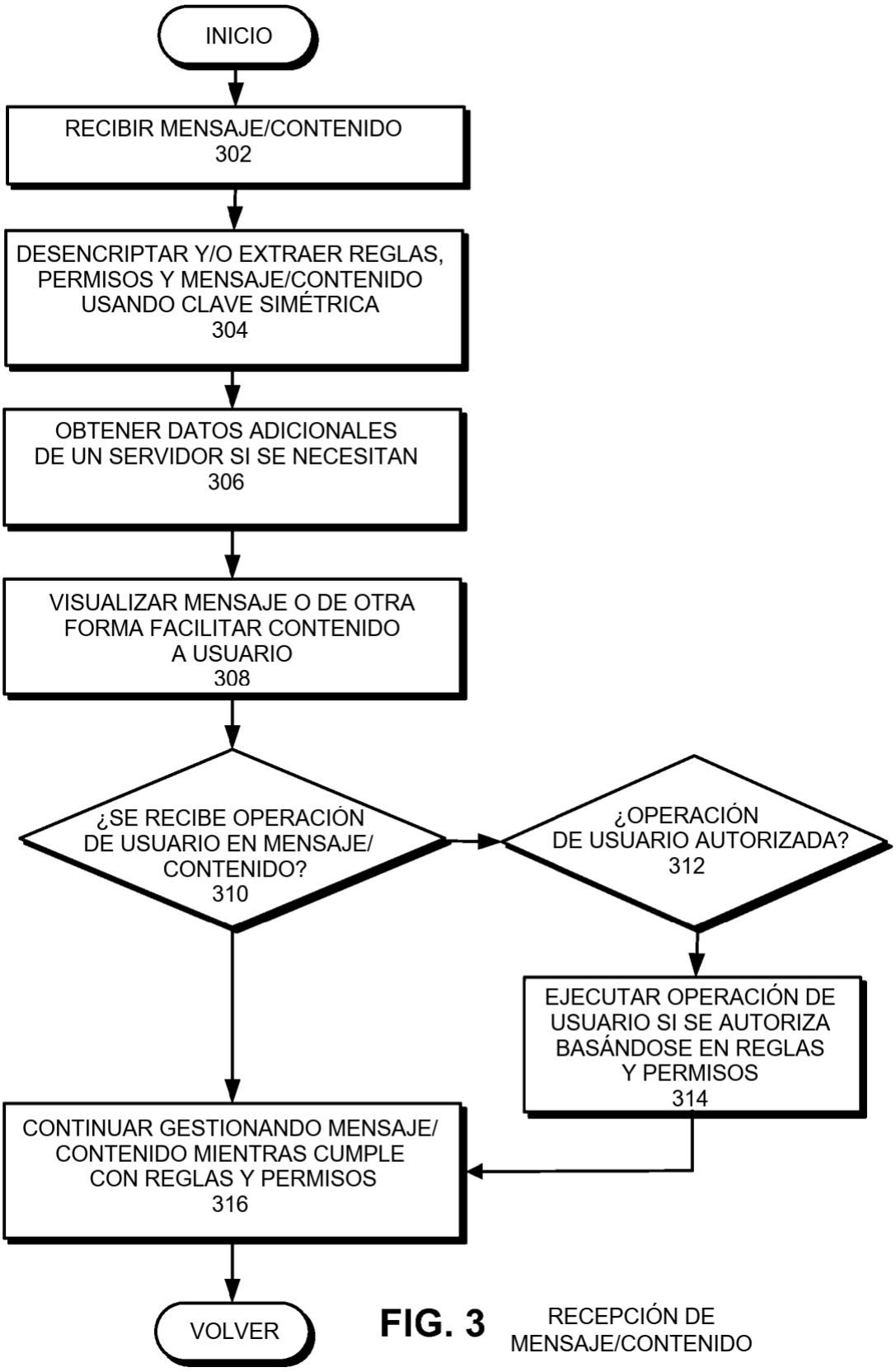

FIG. 3 RECEPCIÓN DE MENSAJE/CONTENIDO

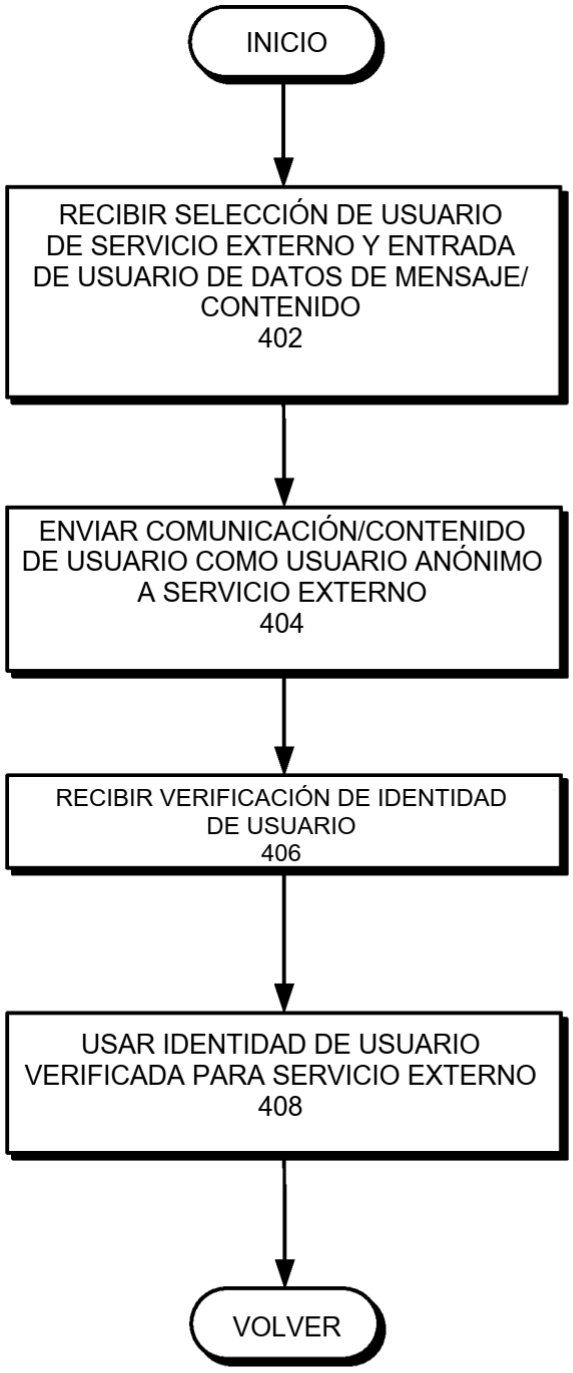

FIG. 4 ACCESO A SERVICIOS EXTERNOS

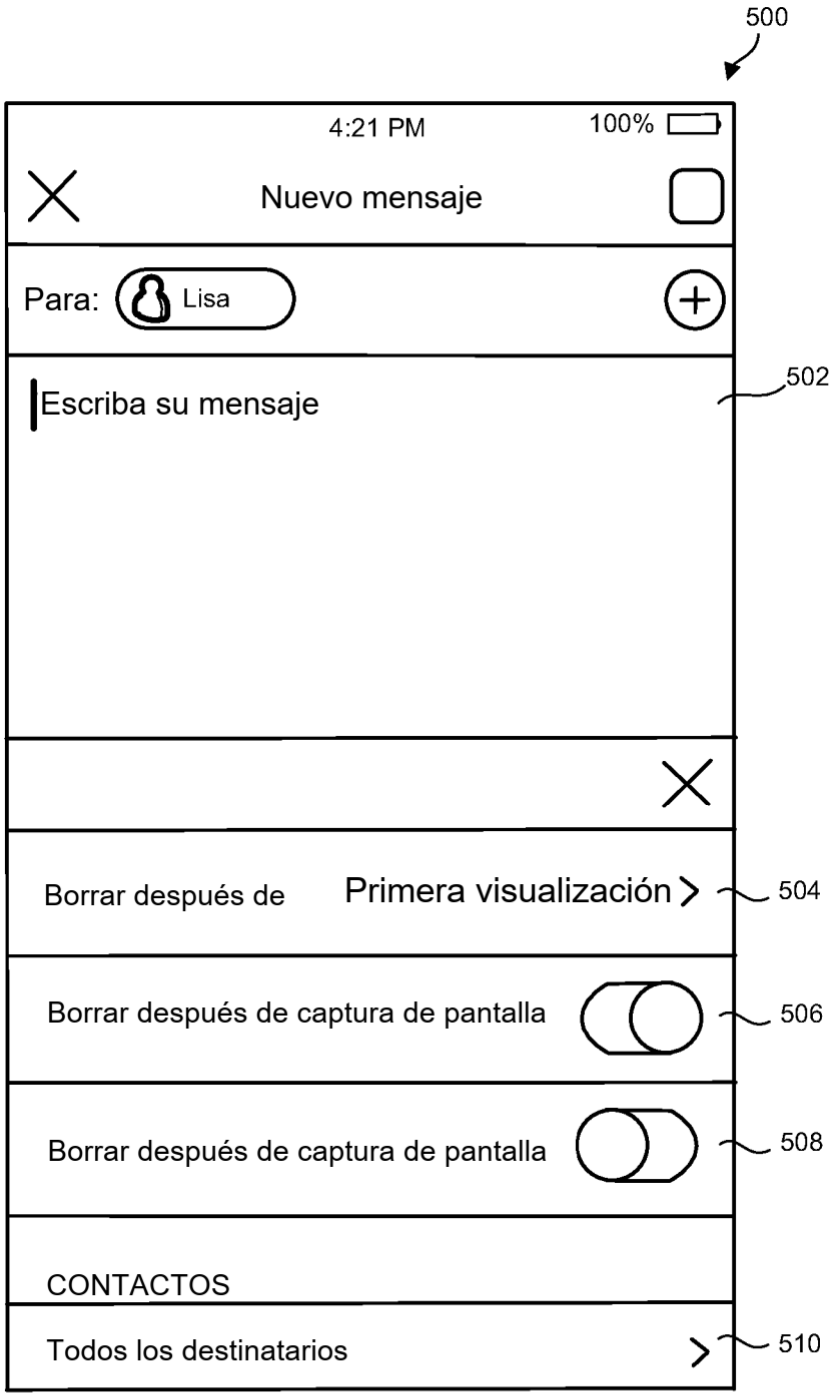

FIG. 5 ESTABLECIMIENTO DE REGLAS PARA UN NUEVO MENSAJE

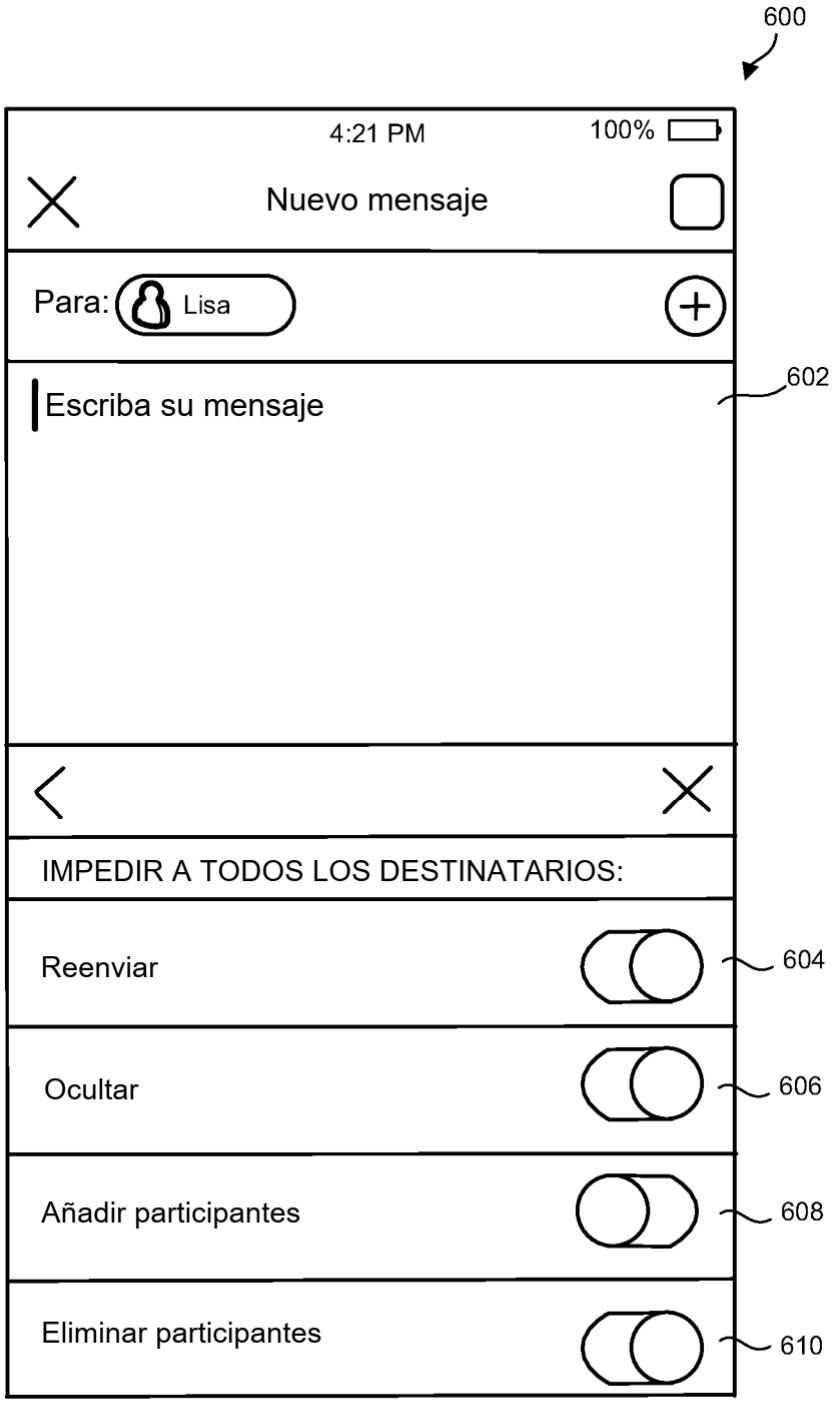

FIG. 6 CAMBIO DE PERMISOS A TODOS DESTINATARIOS DE UN MENSAJE NUEVO

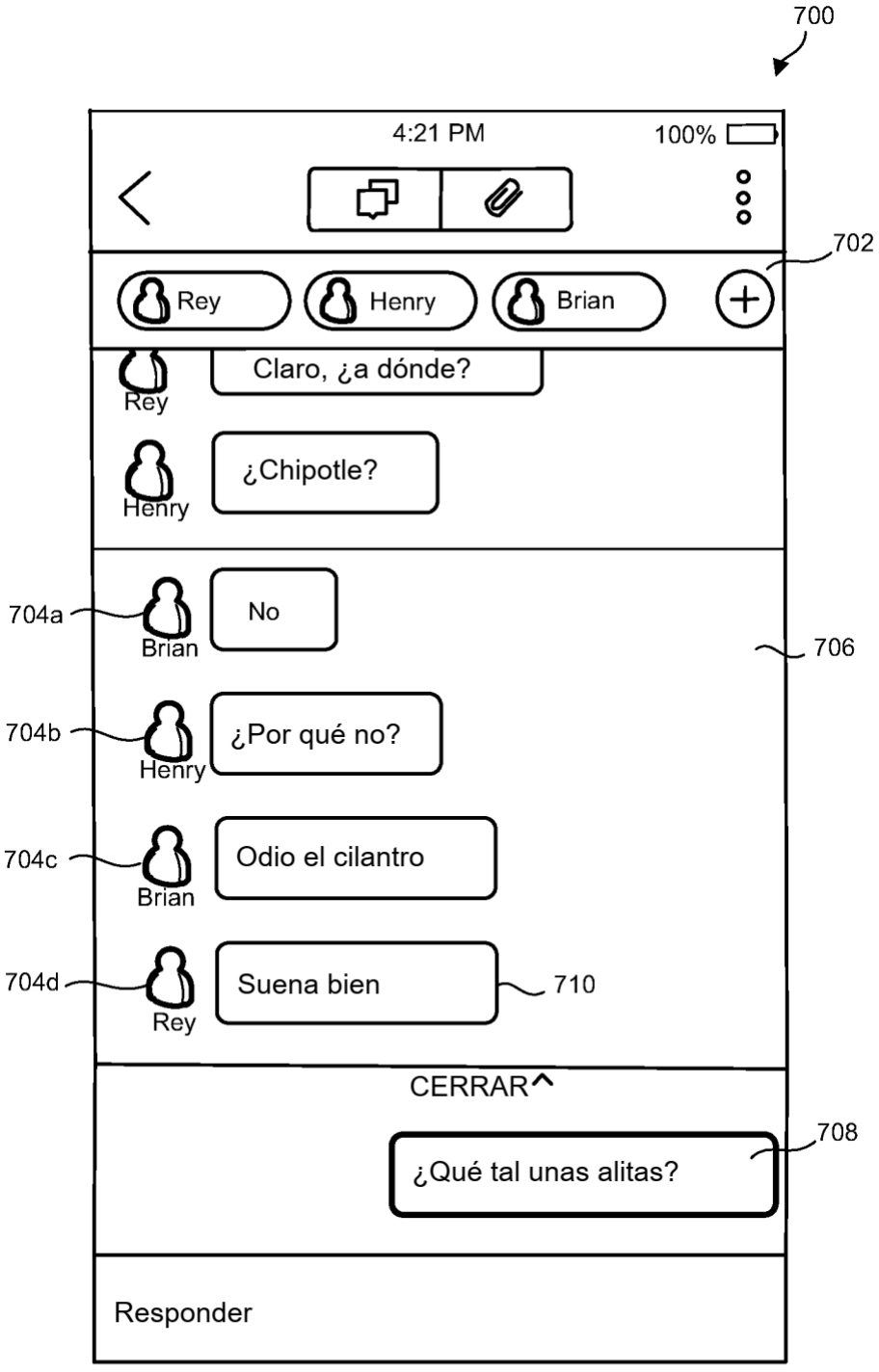

FIG. 7 VISUALIZACIÓN JERÁRQUICA DE MENSAJERÍA DE GRUPO

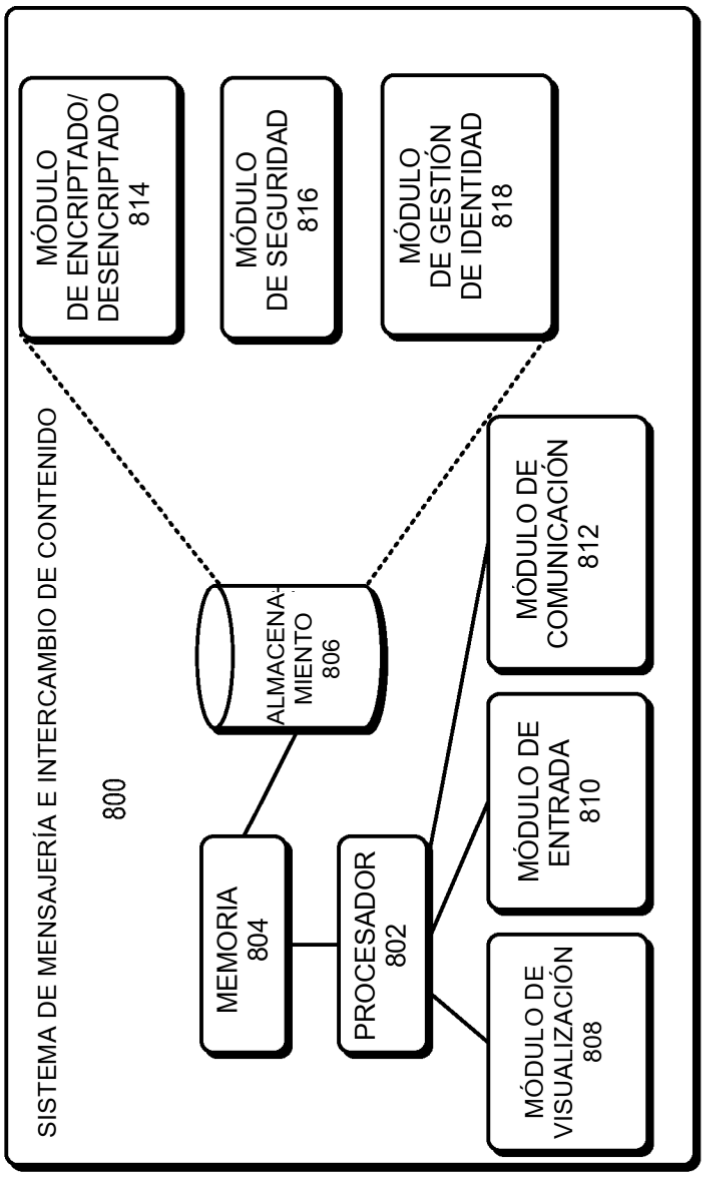

FIG. 8 SISTEMA DE MENSAJERÍA E INTERCAMBIO DE CONTENIDO