(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 867 751**

(51) Int. CI.:

G06F 17/00	(2009.01)
G06F 21/31	(2013.01)
G06Q 20/40	(2012.01)
H04L 9/32	(2006.01)
H04L 29/06	(2006.01)
G06Q 30/06	(2012.01)
H04L 29/08	(2006.01)
G06Q 20/20	(2012.01)
G06Q 50/00	(2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.10.2015 PCT/US2015/055120**

(87) Fecha y número de publicación internacional: **16.06.2016 WO16093945**

(96) Fecha de presentación y número de la solicitud europea: **12.10.2015 E 15866753 (5)**

(97) Fecha y número de publicación de la concesión europea: **07.04.2021 EP 3207464**

(54) Título: **Método, dispositivo, terminal y servidor para verificar la seguridad de operación de servicio**

(30) Prioridad:

13.10.2014 CN 201410539483

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

LU, KUN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método, dispositivo, terminal y servidor para verificar la seguridad de operación de servicio

Referencia cruzada a aplicación relacionada

Esta solicitud se basa y reivindica la prioridad de la Solicitud de Patente China Número 201410539483.2, presentada el 13 de octubre de 2014.

Campo técnico

La presente solicitud se refiere al campo técnico de las comunicaciones y, más particularmente, a un método, dispositivo, terminal, y servidor para verificar una seguridad de una operación de servicio.

Antecedentes

Con el desarrollo de terminales inteligentes y la popularización de aplicaciones de red, un usuario puede realizar diversas operaciones de servicio utilizando diversos clientes de aplicación instalados en un terminal, tales como servicios de mensajería instantánea, servicios de pago, y similares. Para utilizar los servicios anteriores, un usuario de un terminal a menudo necesita registrar una cuenta de servicio en un servidor, y realizar una determinada operación de servicio con base en esta cuenta de servicio.

Convencionalmente, el patrón de comportamiento de la red de un usuario puede obtenerse con base en tecnologías de extracción de datos. Por ejemplo, cuando se realiza una operación de servicio en conexión con la cuenta de servicio, un servidor de servicio puede verificar la seguridad del servicio de acuerdo con el patrón de comportamiento de la red del usuario para impedir riesgos de servicio. Sin embargo, la extracción del patrón de comportamiento de la red del usuario en general está limitada a los datos históricos del servicio del usuario, los datos históricos de navegación del usuario y similares, donde el contenido de los datos es relativamente similar, lo que resulta en una verificación inexacta de la seguridad de la operación de servicio.

El documento WO 2014/145395 A2 se refiere a un sistema y método para autorizar una transacción financiera utilizando datos de terceros.

El documento US 2014/0137191 A1 se refiere a características de seguridad para dispositivos de comunicaciones móviles y métodos relacionados.

Resumen

La invención está definida por las reivindicaciones adjuntas. De acuerdo con la invención, se proporciona: un método implementado por ordenador para verificar la seguridad de una operación de servicio, como se indica en la reivindicación 1; un terminal, como se indica en la reivindicación 8; y medios de almacenamiento legibles por ordenador, como se indica en la reivindicación 9.

La presente divulgación proporciona un método para verificar la seguridad de una operación de servicio. De acuerdo con algunas realizaciones, el método incluye recibir, a través un terminal de servicio, una instrucción de análisis de credibilidad de la operación de servicio, siendo enviada la instrucción de análisis de credibilidad por un servidor de servicio. El método puede incluir además obtener, por el terminal de servicio, un resultado del análisis de credibilidad de la operación de servicio con base en la instrucción de análisis de credibilidad y uno o más modelos de control de riesgo almacenados previamente en el terminal de servicio, y enviar, a través del terminal de servicio, el resultado del análisis de credibilidad al servidor de servicio para determinar la seguridad de la operación de servicio.

De acuerdo con algunas realizaciones, esta divulgación proporciona otro método para verificar la seguridad de una operación de servicio. El método incluye enviar una instrucción de análisis de credibilidad de la operación de servicio a un terminal de servicio y recibir un resultado del análisis de credibilidad enviado por el terminal de servicio. El resultado del análisis de credibilidad puede ser obtenido por el terminal de servicio con base en la instrucción de análisis de credibilidad de la operación de servicio y uno o más modelos de control de riesgo almacenados previamente en el terminal de servicio. El método puede incluir además determinar la seguridad de la operación de servicio con base en el resultado del análisis de credibilidad.

De acuerdo con algunas realizaciones, esta divulgación proporciona un dispositivo para verificar la seguridad de una operación de servicio. El dispositivo incluye una unidad receptora configurada para recibir una instrucción de análisis de credibilidad de la operación de servicio enviada por un servidor de servicio, una unidad de análisis configurada para obtener un resultado del análisis de credibilidad de la operación de servicio con base en la instrucción de análisis de credibilidad y uno o más modelos de control de riesgo almacenados previamente en un terminal de servicio, y una unidad emisora configurada para enviar el resultado del análisis de credibilidad al servidor de servicio para determinar la seguridad de la operación de servicio.

De acuerdo con algunas realizaciones, esta divulgación proporciona otro dispositivo para verificar la seguridad de una operación de servicio. El dispositivo incluye una unidad emisora configurada para enviar una instrucción de análisis

de credibilidad de la operación de servicio a un terminal de servicio y una unidad receptora configurada para recibir un resultado del análisis de credibilidad enviado por el terminal de servicio. El resultado del análisis de credibilidad puede ser obtenido por el terminal de servicio con base en la instrucción de análisis de credibilidad de la operación de servicio y uno o más modelos de control de riesgo almacenados previamente en el terminal de servicio. El dispositivo puede incluir además una unidad de verificación configurada para determinar la seguridad de la operación de servicio con base en el resultado del análisis de credibilidad.

De acuerdo con algunas realizaciones, esta divulgación proporciona un terminal. El terminal incluye un procesador y una memoria configurados para almacenar instrucciones ejecutables por el procesador. El procesador puede estar configurado para recibir una instrucción de análisis de credibilidad de una operación de servicio enviada por un servidor de servicio, obtener un resultado del análisis de credibilidad de la operación de servicio con base en la instrucción de análisis de credibilidad y uno o más modelos de control de riesgo almacenados previamente en el terminal y enviar el resultado del análisis de credibilidad al servidor de servicio para determinar la seguridad de la operación de servicio.

De acuerdo con algunas realizaciones, esta divulgación proporciona un servidor de servicio. El servidor de servicio incluye un procesador y una memoria configurados para almacenar instrucciones ejecutables por el procesador. El procesador puede estar configurado para enviar una instrucción de análisis de credibilidad de una operación de servicio a un terminal de servicio y recibir un resultado del análisis de credibilidad enviado por el terminal de servicio. El resultado del análisis de credibilidad puede ser obtenido por el terminal de servicio con base en la instrucción de análisis de credibilidad de la operación de servicio y uno o más modelos de control de riesgo almacenados previamente en el terminal de servicio. El procesador puede configurarse además para determinar la seguridad de la operación de servicio con base en el resultado del análisis de credibilidad.

Los objetos y ventajas adicionales de las realizaciones divulgadas se expondrán en parte en la siguiente descripción, y en parte serán evidentes a partir de la descripción, o pueden aprenderse mediante la práctica de las realizaciones. Los objetos y ventajas de las realizaciones descritas pueden realizarse y lograrse mediante los elementos y combinaciones establecidos en las reivindicaciones.

Debe entenderse que tanto la descripción general anterior como la descripción detallada siguiente son únicamente de ejemplo y explicativas y no son restrictivas de las realizaciones divulgadas, como se reivindica.

Breve descripción de los dibujos

Los dibujos adjuntos, los cuales se incorporan en y constituyen una parte de esta especificación, ilustran realizaciones consistentes con la invención y, junto con la descripción, sirven para explicar los principios de la invención.

La Figura 1 ilustra un entorno de sistema de ejemplo para implementar métodos y dispositivos consistentes con la presente divulgación.

La Figura 2 es un diagrama de flujo de un método de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

La Figura 3 es un diagrama de flujo de otro método de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

La Figura 4 es un diagrama de flujo de un método de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

La Figura 5 es un diagrama de bloques de un servidor de servicio de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

La Figura 6 es un diagrama de bloques de un dispositivo de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

La Figura 7 es un diagrama de bloques de otro dispositivo de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

La Figura 8 es un diagrama de bloques de otro dispositivo de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación.

Descripción de las realizaciones

Ahora se hará referencia en detalle a realizaciones de ejemplo, ejemplos de los cuales se ilustran en los dibujos adjuntos. La siguiente descripción se refiere a los dibujos adjuntos en los cuales los mismos números en dibujos diferentes representan elementos iguales o similares a menos que se indique lo contrario. Las implementaciones expuestas en la siguiente descripción de realizaciones de ejemplo no representan todas las implementaciones consistentes con la invención. En cambio, son simplemente ejemplos de dispositivos y métodos consistentes con aspectos relacionados con la invención como se enumeran en las reivindicaciones adjuntas.

La Figura 1 ilustra un entorno de sistema 100 de ejemplo para implementar métodos y dispositivos consistentes con la presente divulgación. Como se muestra en la Figura 1, el entorno 100 del sistema incluye un servidor de servicio y teléfonos móviles de un usuario que ha registrado una cuenta de servicio en el servidor de servicio. Los teléfonos móviles que se muestran en la Figura 1 incluyen un teléfono móvil “A” que sirve como terminal de servicio y un teléfono móvil “B” que sirve como terminal de terceros.

En algunas realizaciones, el teléfono móvil A está provisto localmente con una base de datos de control de seguridad, la cual incluye una pluralidad de modelos de control de riesgo definidos de acuerdo con los datos del usuario en el teléfono móvil A. Después de que el servidor de servicio recibe una solicitud de operación de servicio, una instrucción de análisis de credibilidad de la operación de servicio puede enviarse al teléfono móvil A. El teléfono móvil A puede entonces obtener un resultado del análisis de credibilidad llamando a los modelos de control de riesgo y devolver el resultado del análisis de credibilidad al servidor de servicio. El servidor de servicio puede determinar la seguridad de la operación de servicio de acuerdo con el resultado del análisis de credibilidad. Dado que los datos del usuario incluyen datos privados del usuario almacenados en el teléfono móvil, los datos del usuario pueden reflejar una relación social, una rutina diaria, y similares del usuario. Por tanto, al verificar la credibilidad de la operación de servicio del usuario utilizando los modelos de control de riesgo, se puede mejorar la precisión para verificar la seguridad de la operación de servicio.

La Figura 2 es un diagrama de flujo de un método 200 de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación. El método 200 de ejemplo puede ser realizado por un terminal de servicio, tal como un teléfono inteligente, una tableta, un Ordenador Personal (PC) o similares. Con referencia a la Figura 2, el método 200 incluye las siguientes etapas.

En la etapa 201, el terminal de servicio recibe una instrucción de análisis de credibilidad de una operación de servicio enviada por un servidor de servicio. Por ejemplo, un usuario de un terminal de servicio puede registrar una cuenta de servicio en el servidor de servicio por adelantado para que el usuario pueda completar diversas operaciones de servicio con base en el servidor de servicio después de iniciar sesión en el servidor de servicio de acuerdo con la cuenta de servicio. En algunas implementaciones, el servidor de servicio puede ser un servidor mantenido por un tercero para soportar implementaciones de un servicio específico, tal como un servidor de sistema de pago de un tercero para facilitar las transacciones de compra de bienes.

En algunas realizaciones, el usuario del terminal de servicio puede enviar una solicitud de operación de una operación de servicio al servidor de servicio a través del terminal de servicio. Por ejemplo, el usuario puede realizar una operación de transferencia a través del terminal de servicio, y el terminal de servicio puede enviar una solicitud de operación de esta operación de transferencia al servidor de servicio. En otras realizaciones, otro terminal, tal como un terminal de terceros, puede enviar una solicitud de operación de la operación de servicio al servidor de servicio con respecto al usuario del terminal de servicio. Por ejemplo, el usuario del otro terminal puede enviar una solicitud de operación al servidor de servicio después de comprar algunos bienes, solicitando al usuario del terminal de servicio que realice una operación de pago. El servidor de servicio puede enviar una instrucción de análisis de credibilidad de esta operación de servicio al terminal de servicio después de recibir la solicitud de operación de la operación de servicio a partir del otro terminal.

En la etapa 202, el terminal de servicio obtiene un resultado del análisis de credibilidad de la operación de servicio con base en la instrucción de análisis de credibilidad y uno o más modelos de control de riesgo almacenados previamente. Por ejemplo, el terminal de servicio puede llamar a los modelos de control de riesgo almacenados previamente para obtener el resultado del análisis de credibilidad cuando recibe la instrucción de análisis de credibilidad del servidor de servicio. En algunas realizaciones, después de obtener un permiso de autorización del usuario, el terminal de servicio puede obtener datos del usuario del terminal de servicio con base en el permiso de autorización. Los datos del usuario pueden incluir datos sociales del usuario, datos de interés, datos de hábitos, y similares. El terminal de servicio puede generar una pluralidad de modelos de control de riesgo analizando los datos del usuario anteriores, donde cada modelo de control de riesgo puede contener una relación correspondiente entre la información de servicio y los valores del análisis de credibilidad del servicio. Por ejemplo, los modelos de control de riesgo pueden incluir un modelo de control de relación social generado de acuerdo con los datos sociales del usuario, un modelo de control de intereses generado de acuerdo con los datos de interés, un modelo de control de hábitos generado de acuerdo con los datos de hábitos, y similares. El terminal de servicio puede entonces almacenar estos modelos de control de riesgo en una base de datos de control de seguridad local después de cifrar los modelos de control de riesgo.

En algunas realizaciones, el terminal de servicio puede obtener información de servicio de la operación de servicio de acuerdo con la instrucción de análisis de credibilidad. Por ejemplo, cuando el terminal de servicio envía una solicitud de operación al servidor de servicio, el terminal de servicio puede obtener información de servicio de la operación de servicio de acuerdo con la solicitud de operación enviada por el terminal de servicio cuando se recibe la instrucción de análisis de credibilidad. La información de servicio puede comprender información del destinatario del servicio, tipo de operación de servicio, contenido de la operación de servicio, y similares. Por ejemplo, cuando la operación de servicio es una operación de transferencia, la información del destinatario del servicio puede incluir el nombre de una parte de la operación de transferencia, el tipo de operación de servicio puede ser una transacción de transferencia, y la información de contenido de la operación de servicio puede incluir una cantidad de transferencia.

Cuando otro terminal envía una solicitud de operación al servidor de servicio, el servidor de servicio puede obtener información de servicio a partir de esta solicitud de operación, incluir esta información de servicio en la instrucción de análisis de credibilidad, y enviar la información de servicio al terminal de servicio, de tal manera que el terminal de servicio puede obtener la información de servicio a partir de la instrucción de análisis de credibilidad. La información de servicio puede comprender información del destinatario del servicio, tipo de operación de servicio, contenido de la operación de servicio, y similares. Por ejemplo, cuando la operación de servicio es una operación de pago, la información del destinatario del servicio puede incluir el nombre de un iniciador de la transacción de pago, el tipo de operación de servicio puede ser una transacción de pago, y la información del contenido de la operación de servicio puede incluir una cantidad de pago.

Después de obtener la información de servicio de la operación de servicio, el terminal de servicio puede llamar a un modelo de control de riesgo objetivo a partir de modelos de control de riesgo almacenados previamente con base en el tipo de operación de servicio. Por ejemplo, el terminal de servicio puede buscar el modelo de control de riesgo objetivo utilizando la información de servicio como palabra clave para obtener un valor de análisis de credibilidad del servicio como resultado del análisis de credibilidad.

En la etapa 203, el terminal de servicio envía el resultado del análisis de credibilidad al servidor de servicio. El servidor de servicio puede determinar la seguridad de la operación de servicio de acuerdo con el resultado del análisis de credibilidad.

En el método 200, cuando se verifica la seguridad de la operación de servicio, el resultado del análisis de credibilidad de la operación de servicio puede obtenerse utilizando los modelos de control de riesgo del terminal de servicio. Dado que los modelos de control de riesgo pueden generarse de acuerdo con los datos del usuario almacenados en el terminal de servicio, los cuales pueden reflejar una relación social, un hábito y similares del usuario, se puede mejorar la precisión para verificar la seguridad de la operación de servicio.

La Figura 3 es un diagrama de flujo de otro método 300 de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación. El método 300 de ejemplo puede ser realizado por un servidor de servicio. Con referencia a la Figura 3, el método 300 incluye las siguientes etapas.

En la etapa 301, el servidor de servicio envía una instrucción de análisis de credibilidad de la operación de servicio a un terminal de servicio. El proceso de enviar la instrucción de análisis de credibilidad a un terminal de servicio puede implementarse de una manera consistente con la descripción del método 200 en relación con la Figura 2, la cual se omitirá en este documento.

En la etapa 302, el servidor de servicio recibe un resultado del análisis de credibilidad enviado por el terminal de servicio, donde el resultado del análisis de credibilidad es obtenido por el terminal de servicio con base en la instrucción de análisis de credibilidad de la operación de servicio y uno o más modelos de control de riesgo almacenados previamente en el terminal de servicio. El proceso de recibir el resultado del análisis de credibilidad por parte del servidor de servicio puede implementarse de una manera consistente con la descripción del método 200 en relación con la Figura 2, la cual se omitirá en este documento.

En la etapa 303, el servidor de servicio determina la seguridad de la operación de servicio de acuerdo con el resultado del análisis de credibilidad.

En algunas realizaciones, se puede almacenar un modelo de control de riesgo local en el servidor de servicio, y el modelo de control de riesgo local se puede crear de acuerdo con los datos de comportamiento de la red del usuario del terminal. Cuando se verifica la seguridad de la operación de servicio, el servidor de servicio puede obtener un primer valor de análisis de credibilidad de la operación de servicio de acuerdo con el modelo de control de riesgo local, y utilizar el resultado del análisis de credibilidad enviado por el terminal de servicio como un segundo valor de análisis de credibilidad. El servidor de servicio puede obtener valores de ponderación para el primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad respectivamente, multiplicar el primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad por los respectivos valores de ponderación, y sumar el primer valor de análisis de credibilidad ponderado y el segundo valor de análisis de credibilidad ponderado para obtener un valor de análisis de credibilidad combinado. A continuación, el servidor de servicio puede comparar el valor de análisis de credibilidad combinado con un umbral de credibilidad predefinido. El servidor de servicio puede determinar que la operación de servicio es segura si el valor de análisis de credibilidad combinado es mayor que el umbral de credibilidad y determinar que la operación de servicio es insegura si el valor de análisis de credibilidad combinado no es mayor que el umbral de credibilidad.

En el método 300, cuando se verifica la seguridad de la operación de servicio, el resultado del análisis de credibilidad de la operación de servicio puede obtenerse utilizando los modelos de control de riesgo dentro del terminal de servicio. Dado que los modelos de control de riesgo pueden generarse de acuerdo con los datos del usuario almacenados en el terminal de servicio, los cuales pueden reflejar una relación social, un hábito y similares del usuario, se puede mejorar la precisión para verificar la seguridad de la operación de servicio.

La Figura 4 es un diagrama de flujo de un método de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación. El método 400 de ejemplo puede implementarse entre un

terminal de servicio y un servidor de servicio para verificar la seguridad de una operación de servicio. Con referencia a la Figura 4, el método 400 incluye las siguientes etapas.

En la etapa 401, el terminal de servicio obtiene datos del usuario a partir del terminal de servicio de acuerdo con un permiso de autorización de un usuario del terminal de servicio. Los datos del usuario en el terminal de servicio pueden incluir información privada del usuario.

En algunas implementaciones, el permiso de autorización del usuario puede obtenerse por adelantado. Por ejemplo, se puede instalar una Aplicación ("APP") en el terminal de servicio para obtener los datos del usuario. El usuario puede otorgar el permiso de autorización instalando esta APP y, como resultado, el terminal de servicio puede acceder a los datos del usuario.

Los datos del usuario pueden comprender datos sociales del usuario, datos de interés, datos de hábitos, o similares. Por ejemplo, los datos sociales del usuario pueden incluir información de comunicación convencional en el terminal de servicio, tal como grupos, contactos, y notas en una libreta de direcciones, participantes de llamadas pasadas, duración de la llamada, e información sobre el número de llamadas en los registros de llamadas, remitente y destinatario de mensajes de texto anteriores y cantidad de mensajes de texto en registros de mensajes de texto, y similares. Los datos del usuario pueden comprender además información de comunicación asociada con una aplicación de mensajería instantánea instalada en el terminal de servicio, tal como contactos de mensajería instantánea, duración de la conexión de cada contacto, y similares. Los datos de interés pueden comprender el historial de navegación del usuario obtenido por un navegador en el terminal de servicio, tales como bienes, eventos buscados por un usuario, o similares. Los datos de interés pueden comprender además información de ubicación geográfica del usuario obtenida por un dispositivo de posicionamiento en el terminal de servicio, tal como restaurantes, centros comerciales donde el usuario visita con frecuencia, y similares. Los datos de hábitos pueden comprender información registrada por una libreta de notas en el terminal de servicio, tales como itinerarios de usuario, recordatorios, y similares. Los datos de hábitos pueden comprender además configuraciones de aplicaciones en el terminal de servicio, tales como configuración de alarmas, recordatorios de calendario y similares. El usuario del terminal de servicio puede autorizar al terminal de servicio a obtener una parte o la totalidad de los datos del usuario descritos anteriormente sin apartarse del alcance de la presente divulgación.

En la etapa 402, el terminal de servicio genera uno o más modelos de control de riesgo analizando los datos del usuario. Después de obtener los datos del usuario en la etapa 401, se pueden analizar diferentes tipos de datos del usuario de tal modo que se pueda obtener un modelo de control de relaciones sociales, un modelo de control de intereses, y/o un modelo de control de hábitos, donde cada modelo de control de riesgo incluye una relación correspondiente entre la información de servicio y los valores del análisis de credibilidad del servicio.

El modelo de control de relación social puede generarse con base en los datos sociales del usuario y puede incluir una relación correspondiente entre los contactos del usuario y los valores de análisis de credibilidad de estos contactos. Por ejemplo, si el miembro de contacto "A" es un pariente del usuario del terminal, el miembro de contacto A puede obtener un valor de análisis de credibilidad elevado. Como otro ejemplo, si el período de tiempo en donde el miembro de contacto "B" se ha agregado en una libreta de direcciones de usuario es largo y la frecuencia de comunicación del miembro de contacto B con el usuario es elevada, el miembro de contacto B puede ser un colega o amigo del usuario y, por lo tanto, puede obtener un valor de análisis de credibilidad elevado. Como otro ejemplo, si el período de tiempo en donde el miembro de contacto "C" se ha agregado en la libreta de direcciones del usuario es corto y el miembro de contacto C solo interactúa con el usuario con pocos mensajes de texto, el miembro de contacto C puede ser un extraño y, por lo tanto, puede obtener un valor de análisis de credibilidad bajo.

El modelo de control de intereses puede generarse de acuerdo con los datos de interés y puede indicar una relación correspondiente entre los objetos de interés del usuario y los valores del análisis de credibilidad de los objetos de interés. Por ejemplo, si el objeto de interés del usuario es un ordenador portátil y un historial de navegación del usuario indica que el usuario busca con frecuencia información relevante del ordenador portátil dentro de un cierto período de tiempo, se puede establecer un valor de análisis de credibilidad elevado para el ordenador portátil. Como otro ejemplo, si el objeto de interés del usuario es un centro comercial pero la información de ubicación geográfica indica que el usuario rara vez visita este centro comercial, se puede establecer un valor de análisis de credibilidad bajo para este centro comercial.

El modelo de control de hábitos puede generarse de acuerdo con los datos de hábitos y puede indicar una relación correspondiente entre las actividades habituales del usuario y los valores del análisis de credibilidad de las actividades habituales. Por ejemplo, la actividad habitual del usuario es correr durante una hora en un parque a las 8 P.M. todas las noches, se puede establecer un valor de análisis de credibilidad elevado para correr en el parque de 8 P.M. a 9 P.M. todas las noches.

En algunas realizaciones, la información de servicio puede excluirse de los modelos de control de riesgo anteriores, y un valor de análisis de credibilidad correspondiente a la información de servicio puede establecerse como cero por defecto.

En la etapa 403, el terminal de servicio almacena los modelos de control de riesgo en una base de datos de control de seguridad local del terminal de servicio.

En algunas realizaciones, los modelos de control de riesgo obtenidos en la etapa 402 pueden cifrarse con el fin de garantizar la seguridad de los modelos de control de riesgo en el terminal de servicio, y los modelos de control de riesgo cifrados pueden almacenarse en la base de datos de control de seguridad local. Cuando el terminal de servicio utiliza los modelos de control de riesgo, los modelos de control de riesgo cifrados pueden descifrarse realizando un algoritmo de descifrado correspondiente al algoritmo de cifrado.

En la etapa 404, cuando el usuario del terminal de servicio inicia una operación de servicio, el terminal de servicio envía una solicitud de operación de la operación de servicio al servidor de servicio. Por ejemplo, el usuario puede registrar una cuenta de servicio en el servidor de servicio de antemano, de tal modo que se puedan completar diversas operaciones de servicio cuando el usuario del terminal inicie sesión en el servidor de servicio de acuerdo con la cuenta de servicio. Cuando el usuario inicia una determinada operación de servicio, el terminal de servicio puede enviar una solicitud de operación de la operación de servicio al servidor de servicio. La solicitud de operación puede contener información del destinatario del servicio, el tipo de operación de servicio, el contenido de la operación de servicio y similares. Por ejemplo, cuando la operación de servicio es que el usuario transfiere 10,000 RMB a un amigo, la información del destinatario del servicio puede comprender un nombre de usuario, un nombre, un número de teléfono móvil, una dirección de correo electrónico y similares del amigo, el tipo de la operación de servicio puede ser una transacción de transferencia, y la información del contenido de la operación de servicio puede incluir una cantidad de transferencia de 10,000 RMB.

En la etapa 405, el servidor de servicio envía la instrucción de análisis de credibilidad de la operación de servicio al terminal de servicio de acuerdo con la solicitud de operación. Por ejemplo, después de recibir la solicitud de operación de la operación de servicio, el servidor de servicio puede solicitar al terminal de servicio que analice la credibilidad de la operación de servicio enviando la instrucción de análisis de credibilidad de la operación de servicio al terminal de servicio.

En la etapa 406, el terminal de servicio obtiene información de servicio de la operación de servicio de acuerdo con la solicitud de operación enviada previamente en la etapa 404. Como se describió anteriormente en la etapa 404, la solicitud de operación de la operación de servicio puede contener información del destinatario del servicio, tipo de operación de servicio, contenido de la operación de servicio, y similares. El terminal de servicio puede utilizar la información descrita anteriormente como información de servicio de la operación de servicio.

En la etapa 407, el terminal de servicio llama a un modelo de control de riesgo objetivo a partir de los modelos de control de riesgo de acuerdo con el tipo de operación de servicio. Dado que los modelos de control de riesgo se almacenan en la base de datos de control de seguridad local del terminal de servicio y cada modelo de control de riesgo puede corresponder a un tipo diferente de operación de servicio, el terminal de servicio puede llamar al modelo de control de riesgo objetivo correspondiente al tipo de operación de servicio de los modelos de control de riesgo. Por ejemplo, cuando el tipo de operación de servicio es transferencia o pago, la operación de servicio involucra a una parte de la transferencia o un usuario del servicio que inicia el pago, y puede existir una cierta relación social entre el usuario y la parte de la transferencia o el usuario del servicio, y por lo tanto, el modelo de control de relación social puede llamarse a partir de los modelos de control de riesgo.

En la etapa 408, el terminal de servicio busca el modelo de control de riesgo objetivo utilizando la información de servicio como palabra clave para obtener un valor de análisis de credibilidad del servicio correspondiente a la información de servicio, donde el valor de análisis de credibilidad del servicio corresponde a un segundo valor de análisis de credibilidad. Continuando con el ejemplo de que la operación de servicio es que el usuario transfiere 10,000 RMB al amigo, donde la información de servicio obtenida correspondiente en la etapa 406 puede comprender el nombre de usuario, el nombre, el número de teléfono móvil, la dirección de correo electrónico y similares del amigo como la información del destinatario del servicio, el tipo de operación de servicio puede ser una transacción de transferencia, y el modelo de control de riesgo objetivo denominado correspondientemente de acuerdo con el tipo de servicio “transferencia” en la etapa 407 es el modelo de control de relación social. El terminal de servicio puede buscar en el modelo de control de relación social utilizando el nombre y el número de teléfono móvil del amigo como palabras clave para obtener los valores de análisis de credibilidad del servicio correspondientes. Se asume que existe una relación cercana entre el amigo y el usuario, cuando se genera el modelo de control de la relación social, el valor de análisis de credibilidad del servicio sería relativamente elevado.

En la etapa 409, el terminal de servicio envía el segundo valor de análisis de credibilidad al servidor de servicio.

En la etapa 410, el servidor de servicio obtiene el primer valor de análisis de credibilidad de la operación de servicio de acuerdo con el modelo de control de riesgo local.

En esta realización, el modelo de control de riesgo local se almacena en el servidor de servicio, y el modelo de control de riesgo local se puede crear de acuerdo con los datos de comportamiento de la red del usuario del terminal. En algunas implementaciones, cuando se verifica la seguridad de la operación de servicio, el servidor de servicio puede

obtener el primer valor de análisis de credibilidad de la operación de servicio de acuerdo con el modelo de control de riesgo local.

En la etapa 411, el servidor de servicio obtiene valores ponderados del primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad.

Por ejemplo, el servidor de servicio puede establecer los valores de ponderación para el primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad, y almacenar los valores de ponderación localmente. Cabe señalar que los valores de ponderación anteriores pueden ajustarse de acuerdo con las necesidades de la aplicación práctica, las cuales no se limitarán en la presente divulgación.

En la etapa 412, el servidor de servicio calcula un valor de análisis de credibilidad combinado con base en el primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad de acuerdo con los valores de ponderación.

En esta etapa, el servidor de servicio puede configurarse para multiplicar el primer valor de análisis de credibilidad por su valor de ponderación, y multiplicar el segundo valor de análisis de credibilidad por su valor de ponderación, y sumar los dos productos anteriores para obtener el valor de análisis de credibilidad combinado.

En la etapa 413, el servidor de servicio compara el valor de análisis de credibilidad combinado con un umbral de credibilidad predefinido. En algunas realizaciones, el servidor de servicio puede definir un umbral de credibilidad por adelantado para determinar la seguridad de la operación de servicio.

Continuando con el ejemplo de que la operación de servicio es que el usuario transfiere 10,000 RMB al amigo, se asume que el umbral de credibilidad definido en el servidor de servicio de antemano es 60, valores de ponderación definidos para el primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad son respectivamente 80% y 20%, el primer valor de análisis de credibilidad obtenido por el servidor de servicio es 50, el segundo valor de análisis de credibilidad obtenido del terminal de servicio por el servidor de servicio es 90, y el valor de análisis de credibilidad combinado obtenido al realizar la etapa 412 es 80% x 55 + 20% x 90 = 62.

En la etapa 414, el servidor de servicio determina la seguridad de la operación de servicio de acuerdo con un resultado de comparación.

De acuerdo con un resultado de comparación en la etapa 413, si el valor de análisis de credibilidad global es mayor que el umbral de credibilidad, el servidor de servicio puede determinar que la operación de servicio es segura. Si el valor de análisis de credibilidad integral no es mayor que el umbral de credibilidad, el servidor de servicio puede determinar que la operación de servicio es insegura. Por ejemplo, si el usuario del terminal desea transferir 10,000 RMB al amigo, porque el monto de la transferencia es mayor, el servidor del servicio puede determinar que este servicio de transferencia no es creíble de acuerdo con el primer valor 55 de análisis de credibilidad (menor que el umbral 60 de credibilidad) obtenido de acuerdo con el cálculo, lo cual daría lugar a un resultado de verificación inexacto. Sin embargo, al combinarlo con el segundo valor de análisis de credibilidad obtenido por el terminal de servicio, el valor de análisis de credibilidad combinado obtenido es 62, y se puede determinar que el servicio de transferencia es seguro. Por tanto, al combinarlo con el segundo valor de análisis de credibilidad obtenido por el terminal de servicio, se puede mejorar la precisión para verificar la seguridad de la operación de servicio.

La Figura 5 es un diagrama de bloques de un servidor 500 de servicio de ejemplo para verificar la seguridad de una operación de servicio, de acuerdo con algunas realizaciones de esta divulgación. Como se muestra en la Figura 5, el servidor 500 de servicio de ejemplo incluye una CPU, una memoria, una interfaz de red, y un almacenamiento no volátil. La CPU puede configurarse para realizar diversas funciones y procesamiento de datos mediante programas operativos y módulos almacenados en la memoria. Por ejemplo, la CPU puede configurarse para ejecutar instrucciones a fin de realizar todas o parte de las etapas de los métodos descritos anteriormente. En realizaciones de ejemplo, las instrucciones pueden ser rojas a partir del almacenamiento no volátil a la memoria, tales como instrucciones para verificar la seguridad de las operaciones de servicio, las cuales son ejecutables por la CPU en el servidor 500 de servicio para realizar los métodos descritos anteriormente. Se pueden implementar estructuras similares en un terminal de servicio para realizar métodos para verificar la seguridad de las operaciones de servicio descritas anteriormente. El servidor de servicio y el terminal de servicio también pueden incluir otros componentes que no se muestran en la Figura 5.

La Figura 6 es un diagrama de bloques de un dispositivo 600 de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación. El dispositivo 600 de ejemplo puede implementarse en un terminal de servicio. Con referencia a la Figura 6, el dispositivo 600 comprende una unidad 610 receptora, una unidad 620 de análisis y una unidad 630 emisora.

La unidad 610 receptora está configurada para recibir una instrucción de análisis de credibilidad de una operación de servicio, enviada por un servidor de servicio.

La unidad 620 de análisis está configurada para obtener un resultado del análisis de credibilidad de la operación de servicio con base en la instrucción de análisis de credibilidad y uno o más modelos de control de riesgo almacenados previamente.

La unidad 630 emisora está configurada para enviar el resultado del análisis de credibilidad al servidor de servicio, de tal manera que el servidor de servicio puede determinar la seguridad de la operación de servicio con base en el resultado del análisis de credibilidad. En algunas implementaciones, la unidad 630 emisora puede configurarse además para enviar una solicitud de operación de la operación de servicio al servidor de servicio cuando un usuario del terminal de servicio inicia la operación de servicio.

La Figura 7 es un diagrama de bloques de otro dispositivo 700 de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación. El dispositivo 700 de ejemplo puede implementarse en un terminal de servicio. Con referencia a la Figura 7, el dispositivo 700 comprende además una unidad 640 de obtención, una unidad 650 de generación, una unidad 660 de cifrado y una unidad 670 de almacenamiento, además de una unidad 610 receptora, una unidad 620 de análisis y una unidad 630 emisora.

La unidad 640 de obtención está configurada para obtener datos del usuario a partir de un terminal de servicio de acuerdo con un permiso de autorización de un usuario del terminal.

La unidad 650 de generación está configurada para generar uno o más modelos de control de riesgo analizando los datos del usuario.

La unidad 660 de cifrado está configurada para cifrar los modelos de control de riesgo generados por la unidad de generación.

La unidad 670 de almacenamiento está configurada para almacenar los modelos de control de riesgo cifrados en una base de datos de control de seguridad local del terminal de servicio.

En algunas realizaciones, la unidad 620 de análisis puede comprender una subunidad de obtención de información de servicio, una subunidad de llamada de modelo de control de riesgo objetivo, y una subunidad de obtención del valor de análisis de credibilidad del servicio.

La subunidad de obtención de información de servicio está configurada para obtener información de servicio de la operación de servicio de acuerdo con la instrucción de análisis de credibilidad. En algunas implementaciones, la subunidad de obtención de información de servicio puede configurarse para obtener información de servicio de la operación de servicio a partir de la instrucción de análisis de credibilidad, donde la información de servicio de la operación de servicio es obtenida por el servidor de servicio de acuerdo con una solicitud de operación enviada por otro terminal, como un terminal de terceros. En algunas implementaciones, la subunidad de obtención de información de servicio puede configurarse para obtener la información de servicio de la operación de servicio de acuerdo con la solicitud de operación enviada al servidor de servicio, cuando se recibe la instrucción de análisis de credibilidad.

La subunidad de llamada del modelo de control de riesgo objetivo está configurada para llamar a un modelo de control de riesgo objetivo de los modelos de control de riesgo almacenados previamente de acuerdo con un tipo de operación de servicio, donde el modelo de control de riesgo objetivo indica una relación correspondiente entre la información de servicio y los valores de análisis de credibilidad del servicio.

La subunidad de obtención del valor de análisis de credibilidad del servicio está configurada para buscar el modelo de control de riesgo objetivo utilizando la información de servicio como palabra clave para obtener un valor de análisis de credibilidad del servicio.

La Figura 8 es un diagrama de bloques de otro dispositivo 800 de ejemplo para verificar la seguridad de una operación de servicio, consistente con algunas realizaciones de esta divulgación. El dispositivo 800 de ejemplo puede implementarse en un servidor de servicio. Con referencia a la Figura 8, el dispositivo 800 comprende una unidad 810 emisora, una unidad 820 receptora, y una unidad 830 de verificación.

La unidad 810 emisora está configurada para enviar una instrucción de análisis de credibilidad de una operación de servicio a un terminal de servicio.

La unidad 820 receptora está configurada para recibir un resultado del análisis de credibilidad enviado por el terminal de servicio, donde el resultado del análisis de credibilidad es obtenido por el terminal de servicio con base en la instrucción de análisis de credibilidad de la operación de servicio y uno o más modelos de control de riesgo almacenados previamente en el terminal de servicio.

La unidad 830 de verificación está configurada para determinar la seguridad de la operación de servicio de acuerdo con el resultado del análisis de credibilidad.

En algunas implementaciones, la unidad 820 receptora puede configurarse además para recibir una solicitud de operación de la operación de servicio enviada por otro terminal, tal como un terminal de terceros. En algunas realizaciones, el dispositivo 800 puede comprender además una unidad de obtención (no se muestra en la Figura 8)

configurada para obtener información de servicio de la operación de servicio de acuerdo con la solicitud de operación enviada por el otro terminal. La unidad 810 emisora puede configurarse para enviar una solicitud de operación que incluye la información de servicio de la operación de servicio al terminal de servicio.

En algunas implementaciones, la unidad 820 receptora puede configurarse además para recibir una solicitud de operación de la operación de servicio enviada por el terminal de servicio, cuando un usuario del terminal de servicio inicia la operación de servicio. La unidad 810 emisora puede configurarse para, utilizando la solicitud de operación como una instrucción de activación, enviar una instrucción de análisis de credibilidad de la operación de servicio al terminal de servicio.

En algunas realizaciones, la unidad 830 de verificación puede comprender una subunidad de obtención del valor de análisis de credibilidad, una subunidad de obtención del valor de ponderación, una subunidad de cálculo del valor de análisis de credibilidad combinada, una subunidad de comparación del valor de análisis de credibilidad, y una subunidad de determinación de seguridad de servicio (no se muestra en la Figura 8).

La subunidad de obtención del valor de análisis de credibilidad se configura para obtener un primer valor de análisis de credibilidad de la operación de servicio de acuerdo con un modelo de control de riesgo local.

La subunidad de obtención del valor de ponderación está configurada para, utilizando un resultado del análisis de credibilidad enviado por el terminal de servicio como un segundo valor de análisis de credibilidad, obtener valores de ponderación del primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad.

La subunidad de cálculo del valor de análisis de credibilidad combinado está configurada para calcular un valor de análisis de credibilidad combinado del primer valor de análisis de credibilidad y el segundo valor de análisis de credibilidad de acuerdo con los valores de ponderación.

El valor de análisis de credibilidad que compara la subunidad está configurado para comparar el valor de análisis de credibilidad combinado con un umbral de credibilidad predefinido.

La subunidad de determinación de la seguridad del servicio está configurada para, si el valor de análisis de credibilidad combinado es mayor que el umbral de credibilidad, determinar que la operación de servicio es segura, y si el valor de análisis de credibilidad combinado no es mayor que el umbral de credibilidad, determinar que la operación de servicio es insegura.

En realizaciones de ejemplo, también se proporciona un medio de almacenamiento legible por ordenador no transitorio que incluye instrucciones, y las instrucciones pueden ser ejecutadas por un dispositivo (tal como un terminal, un servidor, un ordenador personal, o similares), para realizar los métodos descritos anteriormente. El dispositivo puede incluir uno o más procesadores (CPUs), una interfaz de entrada/salida, una interfaz de red, y/o una memoria.

Cabe señalar que los términos relacionales en este documento, como “primero” y “segundo”, se utilizan solo para diferenciar una entidad u operación de otra entidad u operación, y no requieren ni implican ninguna relación o secuencia real entre estas entidades u operaciones. Además, las palabras “que comprende”, “que tiene”, “que contiene” y “que incluye” y otras formas similares pretenden ser equivalentes en significado y tener un final abierto en el sentido de que un elemento o elementos que siguen a cualquiera de estas palabras no pretenden ser una lista exhaustiva de dicho artículo o artículos, o debe limitarse únicamente al artículo o artículos enumerados.

Un experto en la técnica comprenderá que las realizaciones descritas anteriormente pueden implementarse mediante hardware, o software (códigos de programa) o una combinación de hardware y software. Si se implementa mediante software, puede almacenarse en los medios legibles por ordenador descritos anteriormente. El software, cuando lo ejecuta el procesador, puede realizar los métodos divulgados. Las unidades informáticas y las otras unidades funcionales descritas en esta descripción pueden implementarse mediante hardware o software, o una combinación de hardware y software. Un experto en la técnica también entenderá que múltiples módulos/unidades descritos anteriormente pueden combinarse como un módulo/unidad, y cada uno de los módulos/unidades descritos anteriormente puede dividirse adicionalmente en una pluralidad de submódulos/subunidades.

Otras realizaciones de la invención resultarán evidentes para los expertos en la técnica a partir de la consideración de la especificación y la práctica de la invención divulgada en el presente documento. Esta solicitud está destinada a cubrir cualquier variación, uso, o adaptación de la invención siguiendo los principios generales de la misma y que incluye las desviaciones de la presente divulgación que se encuentran dentro de la práctica conocida o habitual en la técnica. Se pretende que la memoria descriptiva y los ejemplos se consideren únicamente a modo de ejemplo, indicándose el verdadero alcance de la invención mediante las siguientes reivindicaciones.

Se apreciará que la presente invención no se limita a la construcción exacta que se ha descrito anteriormente y que se ilustra en los dibujos adjuntos, y que se pueden realizar diversas modificaciones y cambios sin apartarse del alcance de la misma. Se pretende que el alcance de la invención solo esté limitado por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método (200, 400) implementado por ordenador para verificar la seguridad de una operación de servicio, que comprende:

recibir (201, 405), por un terminal (600, 700), una instrucción de análisis de credibilidad de la operación de servicio, siendo enviada la instrucción de análisis por un servidor (500, 800) de servicio;
obtener (202, 405), por el terminal (600, 700), un resultado del análisis de credibilidad de la operación de servicio con base en la instrucción de análisis de credibilidad y uno o más modelos de control de riesgo almacenados previamente en el terminal (600, 700); y
enviar (203, 409), por el terminal (600, 700), el resultado del análisis de credibilidad al servidor (500, 800) de servicio para determinar la seguridad de la operación de servicio.

2. El método (200, 400) de acuerdo con la reivindicación 1, comprendiendo además:

obtener (401) datos del usuario del terminal (600, 700) con base en un permiso de autorización de un usuario del terminal (600, 700);
generar (402) el uno o más modelos de control de riesgo analizando los datos del usuario; y
almacenar (403) el uno o más modelos de control de riesgo en una base de datos del terminal (600, 700).

3. El método (200, 400) de acuerdo con la reivindicación 2, comprendiendo además:

cifrar el uno o más modelos de control de riesgo antes de almacenar el uno o más modelos de control de riesgo en una base de datos de control de seguridad local del terminal (600, 700); y
almacenar (403) el uno o más modelos de control de riesgo encriptados en la base de datos del terminal (600, 700).

4. El método (200, 400) de acuerdo con la reivindicación 2 o la reivindicación 3, en donde los datos del usuario comprenden al menos uno de: datos sociales del usuario, datos de interés y datos de hábitos, y en donde uno o más modelos de control de riesgo comprenden al menos uno de: un modelo de control de relación social generado con base en los datos sociales del usuario, un modelo de control de intereses generado con base en los datos de interés, y un modelo de control de hábitos generado con base en los datos de hábitos.

5. El método (200, 400) de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde obtener (405) un resultado del análisis de credibilidad de la operación de servicio comprende:

obtener (406) información de servicio de la operación de servicio con base en la instrucción de análisis de credibilidad;
obtener (407) un modelo de control de riesgo objetivo a partir del uno o más modelos de control de riesgo con base en un tipo de operación de servicio, en donde el modelo de control de uno o más riesgos incluye una relación correspondiente entre la información de servicio y los valores del análisis de credibilidad del servicio; y
buscar el modelo de control de riesgo objetivo utilizando la información de servicio como palabra clave para obtener un valor de análisis de credibilidad del servicio correspondiente a la información de servicio.

6. El método (200, 400) de acuerdo con la reivindicación 5, en donde obtener (406) información de servicio de la operación de servicio con base en la instrucción de análisis de credibilidad comprende:
obtener (405) la información de servicio a partir de la instrucción de análisis de credibilidad de la operación de servicio, en donde la información de servicio incluye información obtenida por el servidor (500, 800) de servicio con base en una solicitud de operación de la operación de servicio enviada por un terminal de terceros.

7. El método (200, 400) de acuerdo con la reivindicación 5, comprendiendo además:

cuando un usuario del terminal (600, 700) inicia la operación de servicio, enviar una solicitud de operación de la operación de servicio al servidor (500, 800) de servicio antes de recibir la instrucción de análisis de credibilidad; y
cuando recibe la instrucción de análisis de credibilidad, obtener la información de servicio de la operación de servicio con base en la solicitud de operación de la operación de servicio.

8. Un terminal (600, 700), que comprende:

un procesador; y
una memoria configurada para almacenar instrucciones ejecutables por el procesador;
en donde el procesador está configurado para realizar el método de una cualquiera de las reivindicaciones 1 a 7.

9. Un medio de almacenamiento legible por ordenador que almacena instrucciones las cuales, cuando son ejecutadas por un ordenador, hacen que el ordenador realice el método (200, 400) de cualquiera de las reivindicaciones 1 a 7.

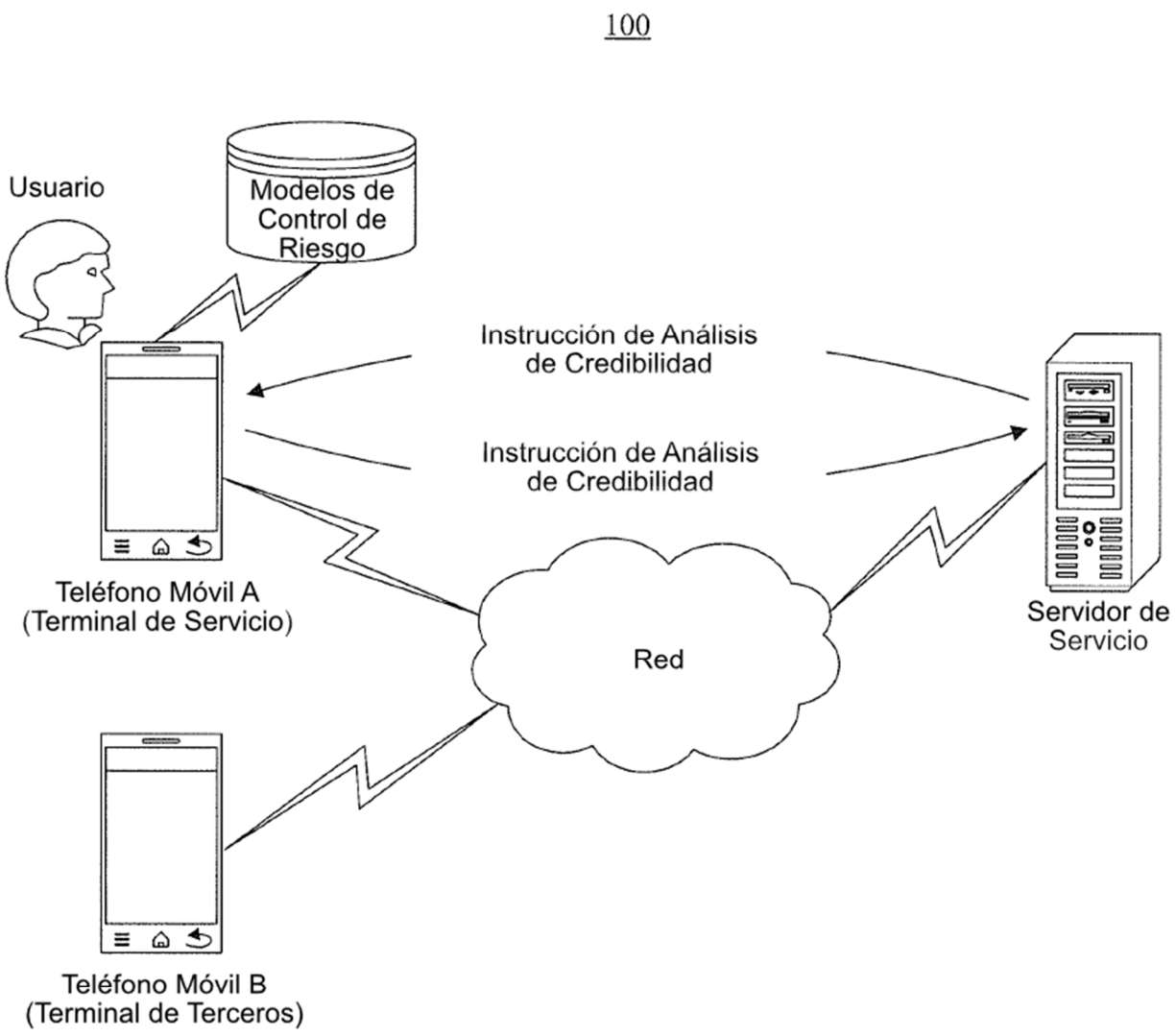
100
Usuario
Modelos de Control de Riesgo
Instrucción de Análisis de Credibilidad
Instrucción de Análisis de Credibilidad
Teléfono Móvil A (Terminal de Servicio)
Red
Servidor de Servicio
Teléfono Móvil B (Terminal de Terceros)

FIG. 1

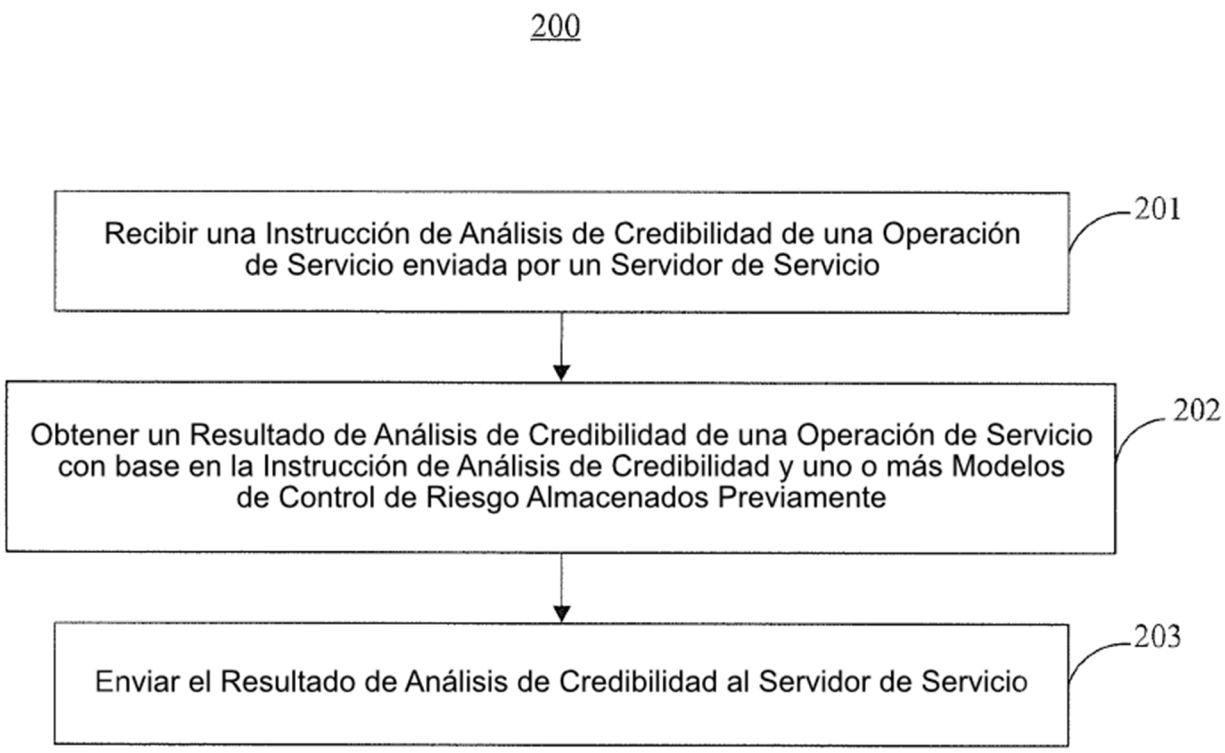
200
Recibir una Instrucción de Análisis de Credibilidad de una Operación de Servicio enviada por un Servidor de Servicio
201
Obtener un Resultado de Análisis de Credibilidad de una Operación de Servicio con base en la Instrucción de Análisis de Credibilidad y uno o más Modelos de Control de Riesgo Almacenados Previamente
202
Enviar el Resultado de Análisis de Credibilidad al Servidor de Servicio
203

FIG. 2

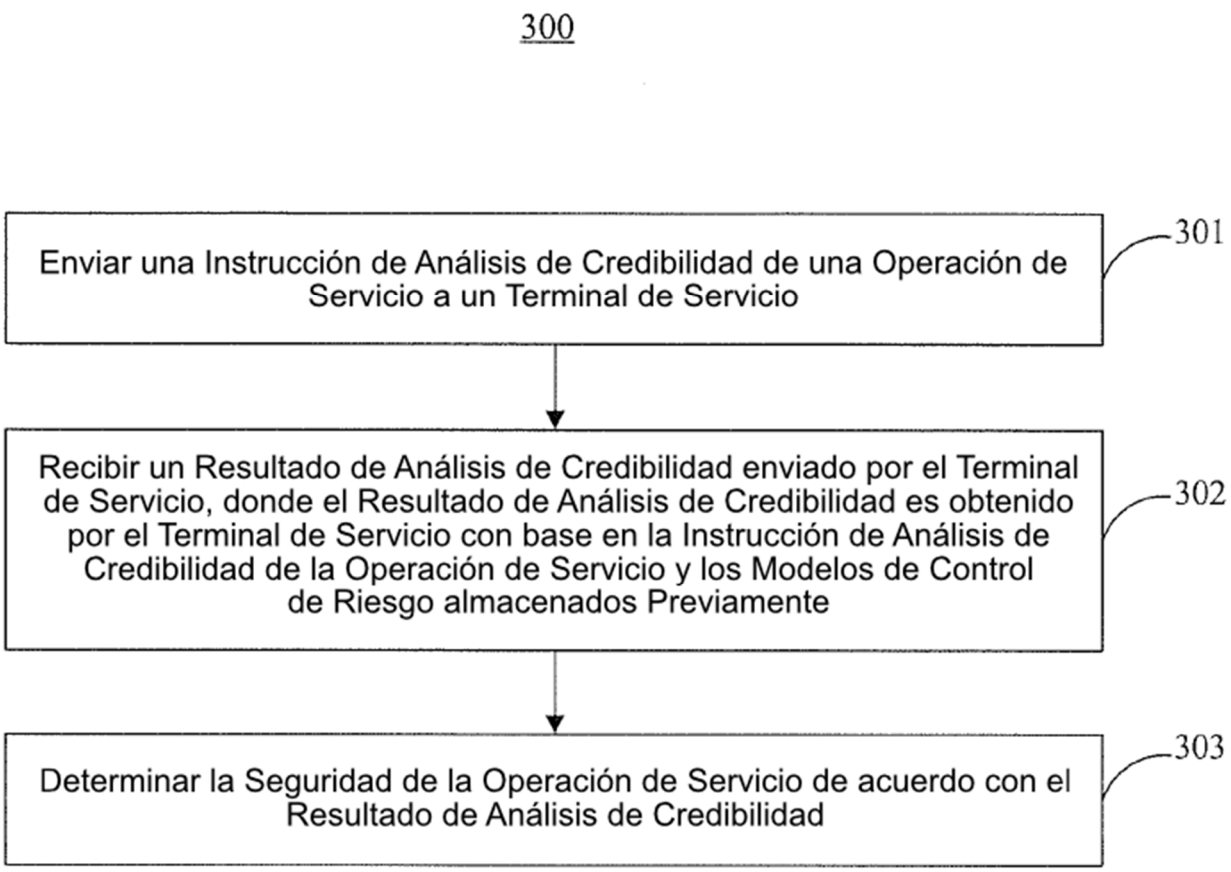
300
Enviar una Instrucción de Análisis de Credibilidad de una Operación de Servicio a un Terminal de Servicio
301
Recibir un Resultado de Análisis de Credibilidad enviado por el Terminal de Servicio, donde el Resultado de Análisis de Credibilidad es obtenido por el Terminal de Servicio con base en la Instrucción de Análisis de Credibilidad de la Operación de Servicio y los Modelos de Control de Riesgo almacenados Previamente
302
Determinar la Seguridad de la Operación de Servicio de acuerdo con el Resultado de Análisis de Credibilidad
303

FIG. 3

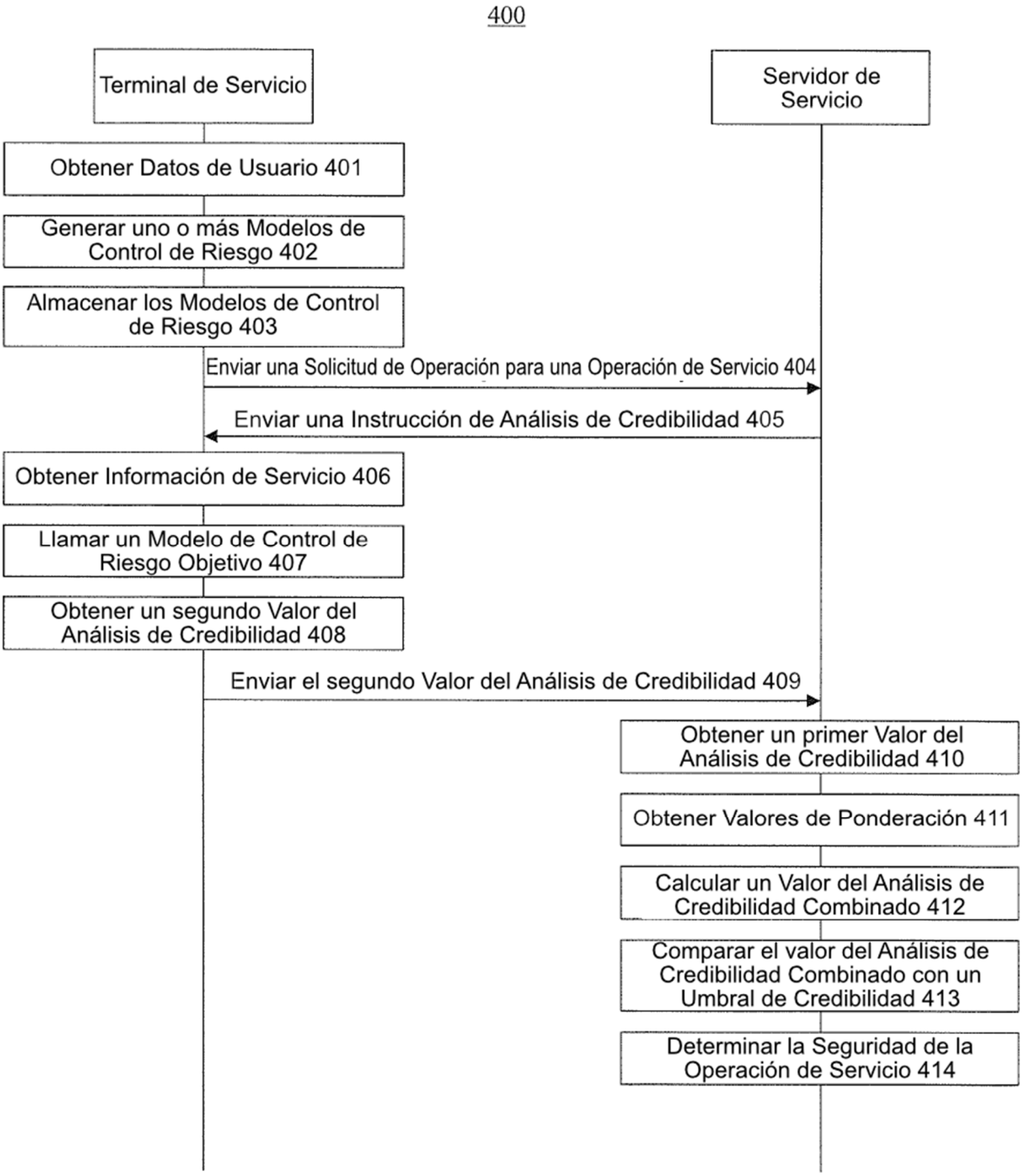
400
Terminal de Servicio
Servidor de Servicio
Obtener Datos de Usuario 401
Generar uno o más Modelos de Control de Riesgo 402
Almacenar los Modelos de Control de Riesgo 403
Enviar una Solicitud de Operación para una Operación de Servicio 404
Enviar una Instrucción de Análisis de Credibilidad 405
Obtener Información de Servicio 406
Llamar un Modelo de Control de Riesgo Objetivo 407
Obtener un segundo Valor del Análisis de Credibilidad 408
Enviar el segundo Valor del Análisis de Credibilidad 409
Obtener un primer Valor del Análisis de Credibilidad 410
Obtener Valores de Ponderación 411
Calcular un Valor del Análisis de Credibilidad Combinado 412
Comparar el valor del Análisis de Credibilidad Combinado con un Umbral de Credibilidad 413
Determinar la Seguridad de la Operación de Servicio 414

FIG. 4

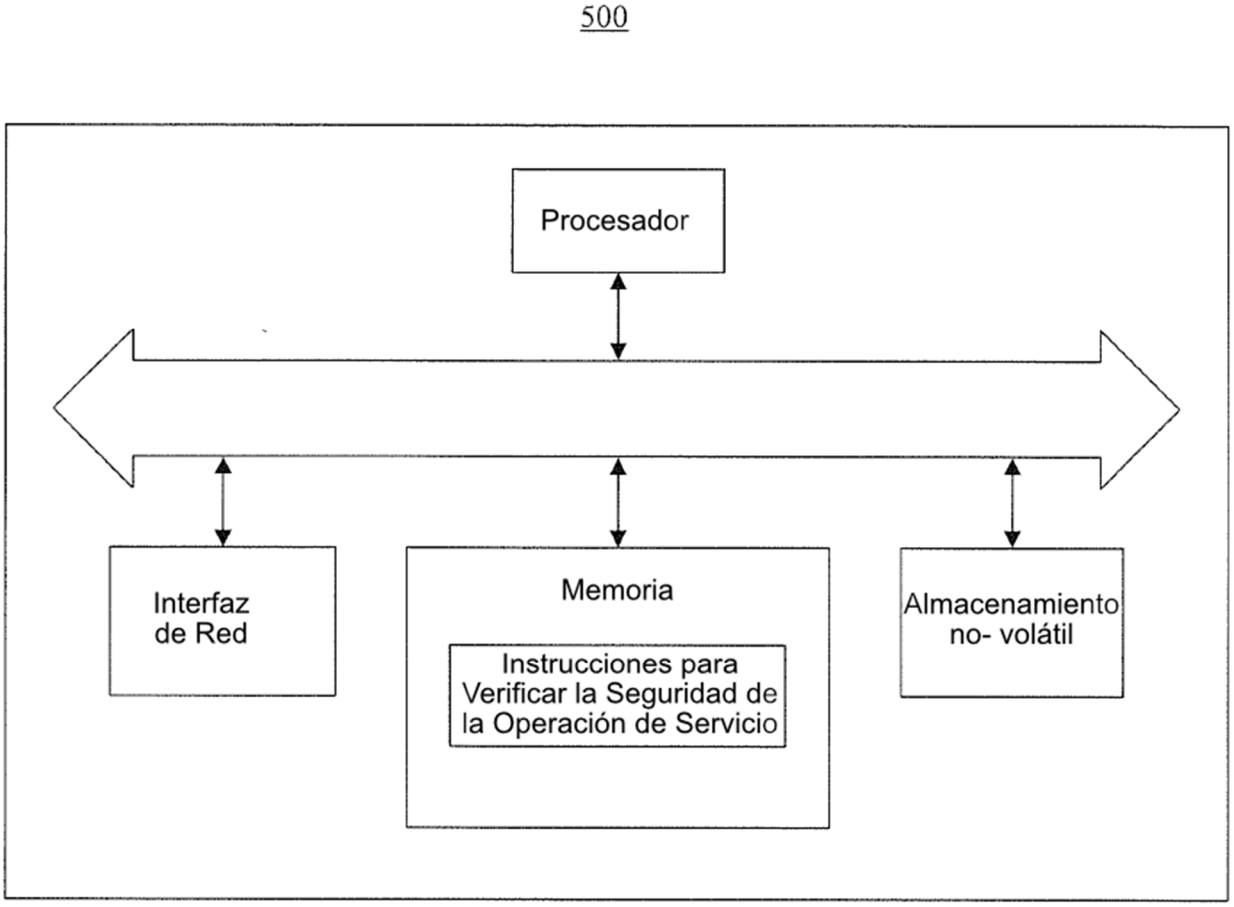
500
Procesador
Interfaz de Red
Memoria
Instrucciones para Verificar la Seguridad de la Operación de Servicio
Almacenamiento no- volátil

FIG. 5

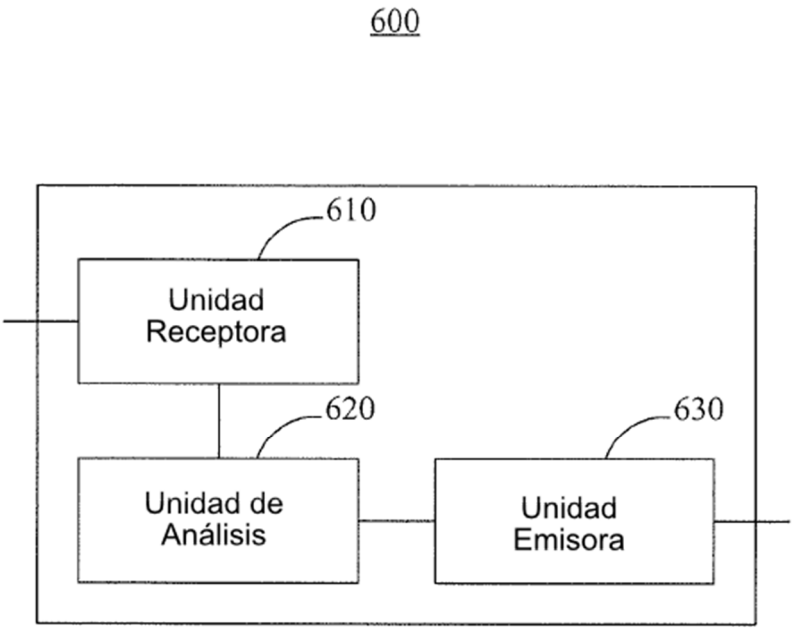
600
610
Unidad Receptora
620
Unidad de Análisis
630
Unidad Emisora

FIG. 6

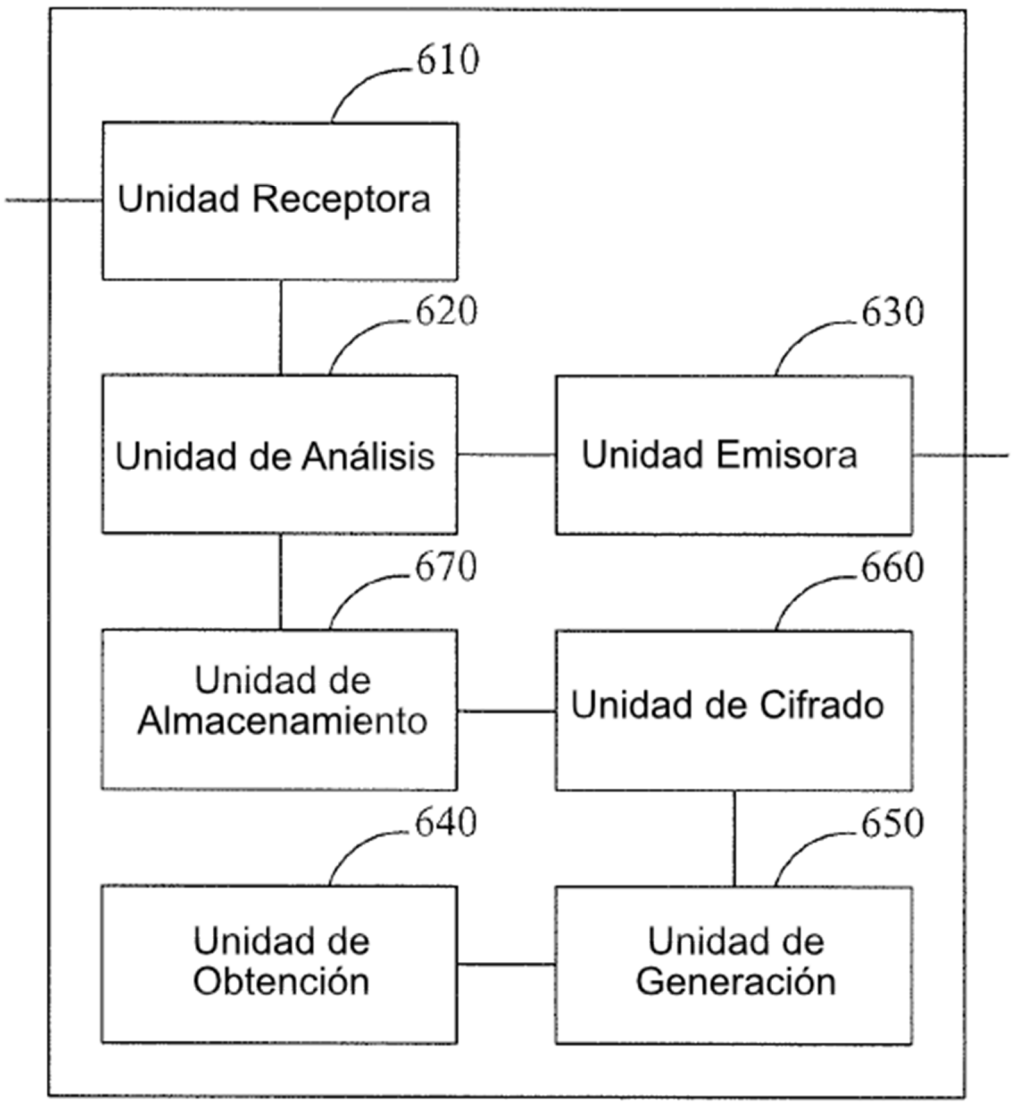
700
610
Unidad Receptora
620
Unidad de Análisis
630
Unidad Emisora
670
Unidad de Almacenamiento
660
Unidad de Cifrado
640
Unidad de Obtención
650
Unidad de Generación

FIG. 7

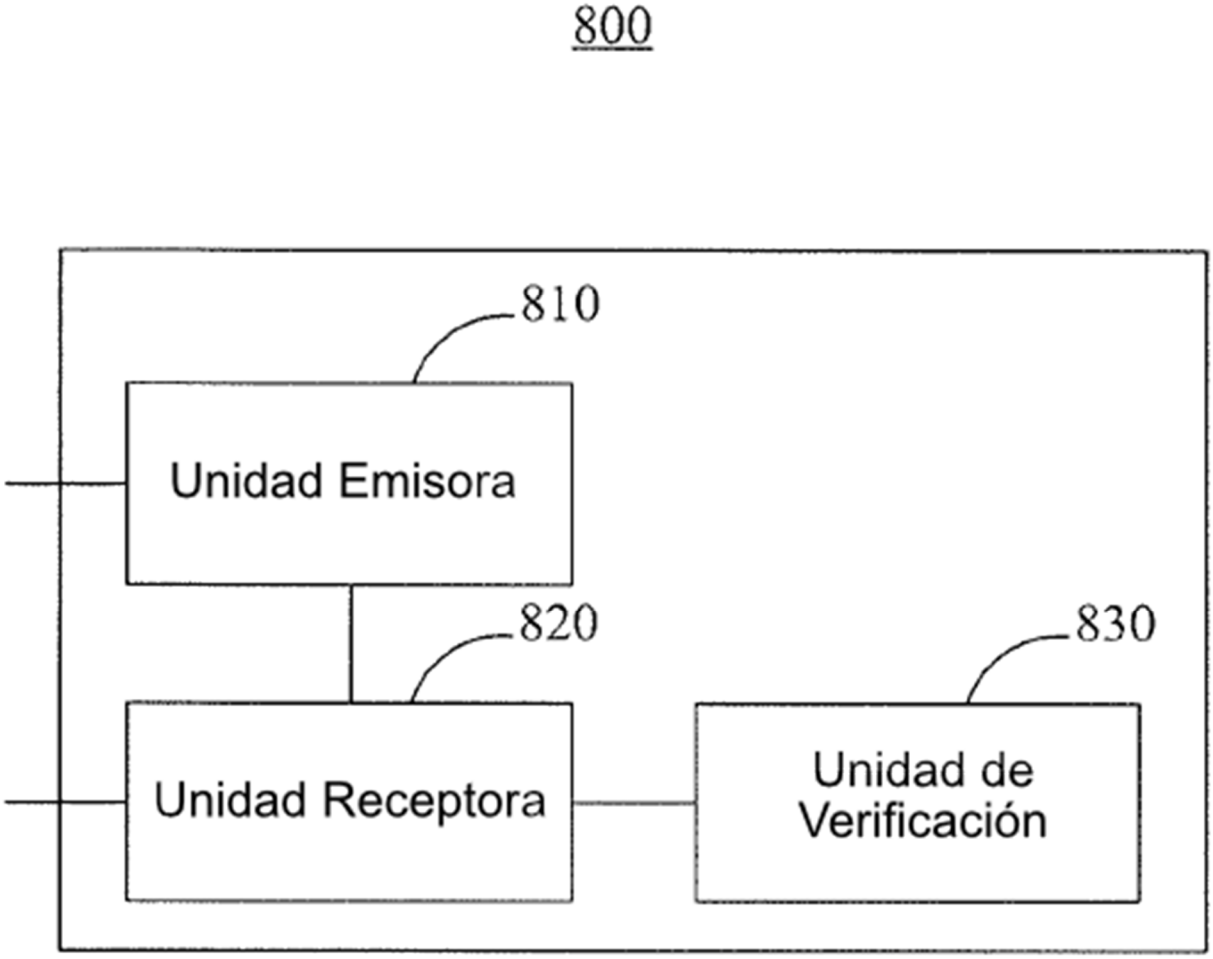
800
810
Unidad Emisora
820
Unidad Receptora
830
Unidad de Verificación

FIG. 8