(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 701 926**

(51) Int. CI.:

H04W 12/06 (2009.01)
G06F 21/36 (2013.01)
H04L 29/06 (2006.01)
H04W 4/00 (2008.01)
H04W 4/80 (2008.01)
H04M 15/00 (2006.01)
G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.01.2015 PCT/CN2015/070328**

(87) Fecha y número de publicación internacional: **30.07.2015 WO15109947**

(96) Fecha de presentación y número de la solicitud europea: **08.01.2015 E 15740512 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.09.2018 EP 3044987**

(54) Título: **Método y sistema para verificar una operación de cuenta**

(30) Prioridad:

24.01.2014 CN 201410035894

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.02.2019

(73) Titular/es:

TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED (100.0%)
Room 403, East Block 2 SEG Park, Zhenxing Road Futian District Shenzhen City Guangdong 518044, CN

(72) Inventor/es:

ZHANG, XIAOLONG;
WEI, YONGLONG;
ZHA, WEN;
CEN, LIFANG;
YAN, JUNHONG y
HUANG, WENHAO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y sistema para verificar una operación de cuenta

REIVINDICACIÓN DE PRIORIDAD Y SOLICITUDES RELACIONADAS

Esta aplicación reivindica prioridad a la solicitud de patente china nº. 201410035894.8, titulada “Method, Apparatus, and System for Identity Verification” ("Método, Aparato y Sistema para Verificación de Identidad") presentada el 24 de Enero de 2014.

CAMPO DE LA INVENCIÓN

Las realizaciones descritas se refieren al campo de los ordenadores y, en particular, a métodos y sistemas para verificar una operación de cuenta (o para la verificación de cuenta). Las características del preámbulo de las reivindicaciones independientes son conocidas a partir del documento US 8 627 438 B1.

ANTECEDENTES DE LA INVENCIÓN

Cuando utiliza Internet, un usuario puede garantizar la seguridad de una cuenta de usuario configurando la información de verificación de cuenta o utilizando una herramienta de verificación de cuenta, para poder evitar situaciones tales como operaciones de cuenta accidentales o maliciosas, tal como un borrado accidental de la cuenta de usuario. Por ejemplo, la verificación se realiza introduciendo una contraseña de cuenta predeterminada e introduciendo un código de verificación recibido por un teléfono móvil vinculado de antemano a la cuenta de usuario, utilizando una plataforma de verificación de terceros tal como OpenID y/o OAuth (sistema de identificación abierto). La verificación también se puede realizar utilizando un dispositivo de hardware tal como una tarjeta de contraseña, una llave USB (certificado digital móvil) o un certificado RSA (algoritmo criptográfico asimétrico). Sin embargo, cuando una cuenta de usuario de Internet se registra directamente en un dispositivo móvil, la verificación de la cuenta de usuario no se puede realizar sin configurar la información de verificación de la cuenta, y el coste de utilizar una herramienta de verificación de cuenta es alto. En general, incluso cuando se configura la información de verificación de la cuenta o se utiliza una herramienta de verificación de cuenta, la verificación de la cuenta todavía adolece de baja seguridad, baja fiabilidad e insuficiencia para evitar un comportamiento de borrado malicioso de un hacker de cuentas.

COMPENDIO DE LA INVENCIÓN

Las realizaciones de la presente descripción proporcionan métodos y sistemas para verificar una operación de cuenta (o para la verificación de cuenta). La presente invención se ha definido en las reivindicaciones independientes.

En algunas realizaciones, se realiza un método para verificar una operación de cuenta en un sistema servidor (por ejemplo, sistema servidor 108, figuras 1-2A) con uno o más procesadores, y memoria. El método incluye: obtener una solicitud de verificación desde un primer dispositivo para una operación de cuenta solicitada por un usuario que utiliza una primera cuenta, la solicitud de verificación incluye información asociada con la primera cuenta y una ID de dispositivo asociada con el primer dispositivo; identificando, desde el sistema de servidor, los datos del historial de uso asociados con la primera cuenta, incluyendo los datos con respecto al uso de la primera cuenta en el primer dispositivo; determinando, de acuerdo con los datos con respecto al uso de la primera cuenta en el primer dispositivo y uno o más criterios de historial de uso predeterminados, si la operación de cuenta asociada con la primera cuenta en el primer dispositivo es segura; y de acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el primer dispositivo no es segura, iniciar un proceso de verificación basado en un segundo dispositivo que es calificado como seguro para la operación de cuenta basada en los datos del historial de uso asociados con una o más cuentas del usuario y uno o más criterios predeterminados de historial de uso.

En algunas realizaciones, un sistema servidor (por ejemplo, el sistema servidor 108, figuras 1-2A), incluye uno o más procesadores, y la memoria almacena uno o más programas para su ejecución por uno o más procesadores, uno o más programas incluyen instrucciones para realizar las operaciones de cualquiera de los métodos descritos en la presente memoria.

Varias ventajas de la presente solicitud son evidentes a la luz de las siguientes descripciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para una mejor comprensión de los aspectos antes mencionados de la aplicación, así como aspectos y realizaciones adicionales de los mismos, se debe hacer referencia a la Descripción Detallada a continuación, junto con los siguientes dibujos en los cuales los mismos números de referencia se refieren a partes correspondientes a través de las figuras.

La Figura 1 es un diagrama de bloques de un entorno servidor-cliente de acuerdo con algunas realizaciones.

La Figura 2A es un diagrama de bloques de un sistema servidor de acuerdo con algunas realizaciones.
La Figura 2B es un diagrama de bloques de un dispositivo de cliente de acuerdo con algunas realizaciones.
La Figura 3A es un diagrama de flujo de un método para verificar una operación de cuenta de acuerdo con algunas realizaciones.
La Figura 3B es una vista esquemática en bloque de un sistema informático para verificar una operación de cuenta de acuerdo con algunas realizaciones.
La Figura 3C es una vista esquemática en bloque de un módulo de verificación del sistema informático para verificar una operación de cuenta de acuerdo con algunas realizaciones.
La Figura 4A ilustra un diagrama de flujo de un método para verificar una operación de cuenta de acuerdo con algunas realizaciones.
Las Figuras 4B-4G son realizaciones ejemplares de interfaces de usuario de verificación de cuentas de acuerdo con algunas realizaciones.
Las Figuras 5A-5F son un diagrama de flujo de un método para verificar una operación de cuenta de acuerdo con algunas realizaciones.
Los números de referencia similares se refieren a partes correspondientes a lo largo de las diversas vistas de los dibujos.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Ahora se hará referencia en detalle a las realizaciones, cuyos ejemplos se ilustran en los dibujos adjuntos. En la siguiente descripción detallada, se describen numerosos detalles específicos a fin de proporcionar una comprensión exhaustiva del tema presentado en la presente memoria. Pero será evidente para un experto en la técnica que el tema se puede poner en práctica sin estos detalles específicos. En otros casos, métodos, procedimientos, componentes y circuitos bien conocidos no se han descrito en detalle con el objetivo de no oscurecer innecesariamente aspectos de las realizaciones.

Las soluciones técnicas de la presente solicitud se describen clara y completamente a continuación con referencia a los dibujos adjuntos. Es obvio que las realizaciones que se describen son solo una parte en vez de todas las realizaciones de la presente solicitud. Todas las demás realizaciones obtenidas por un experto en la técnica basadas en las realizaciones de la presente solicitud sin esfuerzos creativos caerán dentro del alcance de protección de la presente solicitud.

En algunas realizaciones de la presente solicitud, un sistema informático para verificación de cuenta incluye un servidor, y un usuario puede registrase en una cuenta en un dispositivo móvil, tal como una tableta, un teléfono inteligente, o puede registrarse en una cuenta a través de un módulo de cliente en un dispositivo móvil, donde el módulo de cliente en el dispositivo móvil es, por ejemplo, un cliente de navegador de página web, un cliente de mensajería instantánea (tal como QQ, WeChat, Weibo) y/o similares. Un método, un sistema y un dispositivo para verificación de cuentas proporcionados en las realizaciones de la presente solicitud son aplicables a diversos sistemas, tales como un sistema de comercio electrónico y/o una aplicación de mensajería instantánea, que requiere verificación de cuenta. Por ejemplo, la verificación de cuenta se realiza en una cuenta en un sistema de comercio electrónico, para un registro en una cuenta en un sistema de aplicación de mensajería instantánea o durante una o más operaciones de cuenta, tal como un borrado de cuenta.

Como se muestra en la figura 1, la verificación de la cuenta se implementa en un entorno 100 servidor-cliente de acuerdo con algunas realizaciones. En algunas realizaciones, el entorno 100 servidor-cliente incluye el procesamiento servidor-cliente 102-1, 102-2... de lado-cliente (de aquí en adelante "módulo 102 de lado-cliente") ejecutado en un dispositivo 104-1, 104-2... de cliente, y el procesamiento 106 de lado-servidor (de aquí en adelante "módulo 106 de lado-servidor") ejecutado en un sistema servidor 108. El módulo 102 de lado-cliente se comunica con el módulo 106 de lado-servidor a través de una o más redes 110. El módulo 102 de lado-cliente proporciona funcionalidades lado-cliente (por ejemplo, mensajería instantánea y servicios de redes sociales) y comunicaciones con el módulo 106 de lado-servidor. El módulo 106 de lado-servidor proporciona funcionalidades de lado-servidor (por ejemplo, mensajería instantánea y servicios de redes sociales) para cualquier cantidad de módulos 102 cliente residiendo cada uno en un dispositivo 104 de cliente respectivo.

En algunas realizaciones, el módulo 106 de lado-servidor incluye uno o más procesadores 112, una o más bases de datos 114, una interfaz de E/S para uno o más clientes 118, y una interfaz de E/S para uno o más servicios 120 externos. La interfaz de E/S para uno o más clientes 118 facilita el procesamiento de entradas y salidas asociadas con los dispositivos de cliente para el módulo 106 de lado-servidor. Uno o más procesadores 112 obtienen solicitudes para realizar operaciones de cuenta desde uno o más dispositivos 104 de cliente, procesan las solicitudes, identifican datos de uso asociados con la cuenta de usuario en uno o más dispositivos de cliente, verifican la información de cuenta en uno o más dispositivos de cliente y envían los resultados de verificación de cuenta en respuesta a las solicitudes a los módulos 102 de lado-cliente de uno o más dispositivos 104 de cliente. La base de datos 114 almacena información diversa, que

incluye pero no está limitada a, información de cuenta asociada con cada usuario, información de dispositivo asociada con cada cuenta de usuario y datos de uso asociados con cada cuenta de usuario en un determinado dispositivo cliente. La base de datos 114 también puede almacenar una pluralidad de entradas de registro relevantes para las actividades de las respectivas cuentas de cada usuario, y dispositivos asociados con cada usuario. La interfaz E/S con uno o más servicios 120 externos facilita comunicaciones con uno o más servicios 122 externos (por ejemplo, sitios web comerciales, compañías de tarjetas de crédito, plataformas de redes sociales y/u otros servicios de procesamiento).

Ejemplos de dispositivo 104 de cliente incluyen, pero no están limitados, entre otros, un ordenador de mano, un dispositivo informático portátil, un asistente digital personal (PDA), una tableta, un ordenador portátil, un ordenador de escritorio, un teléfono celular, un teléfono inteligente, un teléfono móvil de servicio general de radio por paquetes mejorado (EGPRS), un reproductor multimedia, un dispositivo de navegación, una consola de juegos, un televisor, un control remoto o una combinación de dos o más de estos dispositivos de procesamiento de datos u otros dispositivos de procesamiento de datos.

Los ejemplos de una o más redes 110 incluyen redes de área local (LAN) y redes de área amplia (WAN) tales como Internet. Una o más redes 110 son, opcionalmente, implementadas utilizando cualquier protocolo de red conocido, incluyendo varios protocolos alámbricos o inalámbricos, tales como Ethernet, Bus Serie Universal (USB), FIREWIRE, Sistema Global para Comunicaciones Móviles (GSM), Entorno GSM Mejorado de Datos (EDGE), acceso múltiple por división de código (CDMA), acceso múltiple por división de tiempo (TDMA), Bluetooth, Wi-Fi, voz sobre Protocolo de Internet (VoIP), Wi-MAX o cualquier otro protocolo de comunicación adecuado.

El sistema servidor 108 se implementa en uno o más aparatos de procesamiento de datos autónomos o en una red distribuida de ordenadores. En algunas realizaciones, el sistema servidor 108 también emplea varios dispositivos virtuales y/o servicios de proveedores de servicios externos (por ejemplo, proveedores de servicios en la nube de terceros) para proporcionar los recursos informáticos y/o recursos de infraestructura subyacentes del sistema servidor 108.

El entorno 100 servidor-cliente que se muestra en la figura 1 incluye tanto una parte de lado-cliente (por ejemplo, el módulo 102 de lado-cliente) como una parte de lado-servidor (por ejemplo, el módulo 106 de lado-servidor). En algunas realizaciones, el procesamiento de datos se implementa como una aplicación autónoma instalada en el dispositivo 104 de cliente. Además, la división de funcionalidades entre las partes de cliente y servidor del procesamiento de datos de entorno de cliente puede variar en diferentes realizaciones. Por ejemplo, en algunas realizaciones, el módulo 102 de lado-cliente es un cliente-ligero que proporciona solo funciones de procesamiento de entrada y salida frente al usuario y delega todas las demás funcionalidades de procesamiento de datos a un servidor principal de la aplicación (por ejemplo, sistema servidor 108).

La Figura 2A es un diagrama de bloques que ilustra un sistema servidor 108 de acuerdo con algunas realizaciones. El sistema servidor 108, normalmente, incluye una o más unidades 112 de procesamiento (CPU), una o más interfaces 204 de red (por ejemplo, incluyendo interfaz de E/S a uno o más clientes 118 e interfaz de E/S a uno o más servicios 120 externos), la memoria 206 y uno o más buses 208 de comunicación para interconectar estos componentes (a veces denominados un conjunto de chips).

La memoria 206 incluye una memoria de acceso aleatorio de alta velocidad, tal como DRAM, SRAM, DDR RAM, u otros dispositivos de memoria de estado sólido de acceso aleatorio; y, opcionalmente, incluye memoria no volátil, tal como uno o más dispositivos de almacenamiento de disco magnético, uno o más dispositivos de almacenamiento de disco óptico, uno o más dispositivos de memoria flash, o uno o más de otros dispositivos de almacenamiento de estado sólido no volátiles. La memoria 206, opcionalmente, incluye uno o más dispositivos de almacenamiento ubicados remotamente desde una o más unidades 112 de procesamiento. La memoria 206, o alternativamente la memoria no volátil dentro de la memoria 206, incluye un medio de almacenamiento legible por ordenador no transitorio. En algunas implementaciones, la memoria 206, o el medio de almacenamiento legible por ordenador no transitorio de la memoria 206, almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto o superconjunto de los mismos:

- sistema 210 operativo que incluye procedimientos para manejar varios servicios de sistema básicos y para realizar tareas dependientes del hardware;

- módulo 212 de comunicación de red para conectar el sistema servidor 108 a otros dispositivos informáticos (por ejemplo, dispositivos 104 de cliente y servicio(s) 122 externos) conectados a una o más redes 110 a través de una o más interfaces 204 de red (alámbricas o inalámbricas);

- módulo 106 de lado-servidor, que proporciona procesamiento de datos de lado-servidor (por ejemplo, verificación de cuenta de usuario, mensajería instantánea y servicios de redes sociales), incluye, pero no está limitado a:

módulo 222 de gestión de solicitudes para gestionar y responder a diversas solicitudes enviadas desde dispositivos de cliente, incluidas solicitudes para verificación de cuentas de usuario asociadas con operaciones de cuentas;

módulo 224 de identificación de datos para identificar datos de uso asociados con una cuenta de usuario, que incluye datos con respecto al uso de la cuenta de usuario en un dispositivo de cliente asociado con el usuario;

módulo 226 de identificación de dispositivo para identificar un dispositivo de cliente que se califica como seguro para una operación de cuenta de usuario basado en los datos de historial de uso asociados con la cuenta de usuario y uno o más criterios de historial de uso predeterminados;

módulo 228 de detección de dispositivo para detectar un dispositivo de cliente que está registrado con una o más cuentas de usuario asociadas con un usuario del dispositivo de cliente;

módulo 230 de verificación para verificar la operación de la cuenta de usuario, que incluye, pero no está limitado a:

módulo 232 de promoción para promover que un usuario realice una interacción con el propósito de verificación , tal como enviar una imagen codificada para su visualización en un dispositivo de cliente calificado como seguro, y promover que el usuario escanee la imagen codificada utilizando el dispositivo de cliente que ha de ser verificado por la operación de cuenta;

módulo 234 de verificación de interacción para verificar los resultados de interacción, tal como comparar la imagen codificada escaneada por el dispositivo de cliente con la imagen codificada generada y enviada al dispositivo de cliente calificado como seguro; y

módulo 236 de verificación de datos para verificar los datos de uso identificados para determinar si los datos de uso identificados coinciden con uno o más criterios predeterminados; y

- una o más bases de datos 114 de servidor que almacenan datos para la plataforma de redes sociales, que incluyen pero no se limitan a:

datos 242 de cuenta de usuario que almacenan perfiles de usuario para una pluralidad de usuarios, en donde un perfil de usuario respectivo para un usuario puede incluir una o más cuentas del usuario, credenciales de registro para cada cuenta de usuario, datos de pago (por ejemplo, información de tarjeta de crédito vinculada, aplicación de crédito o saldo de la tarjeta de regalo, dirección de facturación, dirección de envío, etc.) asociados con cada cuenta de usuario, parámetros personalizados (por ejemplo, edad, ubicación, pasatiempos, etc.) para el usuario y contactos de redes sociales asociados con cada cuenta de usuario; y

datos 246 de uso de cuenta de usuario que almacenan la información de dispositivo asociada con cada cuenta de usuario, y los datos de uso de cada cuenta de usuario en cada dispositivo de cliente.

Cada uno de los elementos identificados anteriormente se pueden almacenar en uno o más de los dispositivos de memoria mencionados anteriormente, y corresponde a un conjunto de instrucciones para realizar una función descrita anteriormente. Los módulos o programas identificados anteriormente (es decir, conjuntos de instrucciones) no necesitan implementarse como programas de software, procedimientos o módulos separados, y así varios subconjuntos de estos módulos se pueden combinar o redistribuir de otra forma en varias implementaciones. En algunas implementaciones, la memoria 206, opcionalmente, almacena un subconjunto de módulos y estructuras de datos identificados anteriormente. Además, la memoria 206, opcionalmente, almacena módulos adicionales y estructuras de datos no descritos anteriormente.

La Figura 2B es un diagrama de bloques que ilustra un dispositivo 104 de cliente representativo de acuerdo con algunas realizaciones. El dispositivo 104 de cliente, normalmente, incluye una o más unidades 252 de procesamiento (CPU), una o más interfaces 254 de red, memoria 256 y uno o más buses 258 de comunicación para interconectar estos componentes (a veces denominados conjuntos de chips). El dispositivo 104 de cliente también incluye una interfaz 260 de usuario. La interfaz 260 de usuario incluye uno o más dispositivos 262 de salida que permiten la presentación de contenido multimedia, que incluye uno o más altavoces y/o una o más pantallas de visualización. La interfaz 260 de usuario también incluye uno o

más dispositivos 264 de entrada, que incluyen componentes de interfaz de usuario que facilitan la entrada del usuario como un teclado, un ratón, una unidad de entrada de comando de voz o micrófono, una pantalla táctil, un panel de entrada sensible al tacto, una cámara (por ejemplo, para escanear una imagen codificada), una cámara de captura de gestos u otros botones o controles de entrada. Además, algunos dispositivos 104 de cliente usan un micrófono y reconocimiento de voz o una cámara y reconocimiento de gestos para complementar o reemplazar el teclado.

La memoria 256 incluye memoria de acceso aleatorio de alta velocidad, tal como DRAM, SRAM, DDR RAM, u otros dispositivos de memoria de estado sólido de acceso aleatorio; y, opcionalmente, incluye memoria no volátil, tal como uno o más dispositivos de almacenamiento de disco magnético, uno o más dispositivos de almacenamiento de disco óptico, uno o más dispositivos de memoria flash o uno o más dispositivos de almacenamiento de estado sólido no volátiles. La memoria 256, opcionalmente, incluye uno o más dispositivos de almacenamiento ubicados remotamente desde una o más unidades 252 de procesamiento. La memoria 256, o alternativamente la memoria no volátil dentro de la memoria 256, incluye un medio de almacenamiento legible por ordenador no transitorio. En algunas implementaciones, la memoria 256 o el medio de almacenamiento legible por ordenador no transitorio de la memoria 256, almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto o superconjunto de los mismos:

- sistema 270 operativo que incluye procedimientos para manejar varios servicios básicos del sistema y para realizar tareas dependientes del hardware;

- módulo 272 de comunicación de red para conectar el dispositivo 104 de cliente a otros dispositivos informáticos (por ejemplo, sistema servidor 108 y servicio(s) 122 externos) conectados a una o más redes 110 a través de una o más interfaces 254 de red (alámbricas o inalámbricas);

- módulo 274 de presentación para permitir la presentación de información (por ejemplo, una interfaz de usuario para una plataforma de red social, pequeña aplicación, página web, juego y/o aplicación, contenido de audio y/o video, texto y/o visualización de una imagen codificada para escanear) en el dispositivo 104 de cliente a través de uno o más dispositivos 264 de salida (por ejemplo, pantallas, altavoces, etc.) asociados con la interfaz 260 de usuario;

- módulo 276 de procesamiento de entrada para detectar una o más entradas o interacciones de usuario desde uno o más dispositivos de entrada 264 e interpretar la entrada o interacción detectada (por ejemplo, procesar la imagen codificada escaneada por la cámara del dispositivo de cliente);

- una o más aplicaciones 278-1 - 278-N para ejecución por el dispositivo 104 de cliente (por ejemplo, juegos, mercados de aplicaciones, plataformas de pago, plataformas de redes sociales y/u otras aplicaciones que implican diversas operaciones de usuario);

- el módulo 102 de lado-cliente, que proporciona funcionalidades y procesamiento de datos de lado-cliente, que incluyen pero no se limitan a:

  módulo 282 de envío de solicitudes para generar y enviar solicitudes para verificar una o más operaciones de cuenta; y

- datos 284 de cliente que almacenan datos de un usuario asociado con el dispositivo de cliente, que incluyen, pero no se limitan a:

  datos 286 de cuenta de usuario que almacenan una o más cuentas de usuario asociadas con un usuario del dispositivo 104 de cliente, incluyendo los datos de cuenta de usuario una o más cuentas de usuario, credenciales de registro para cada cuenta de usuario, datos de pago (por ejemplo, información de tarjeta de crédito vinculada, aplicación de crédito o saldo de tarjeta de regalo, dirección de facturación, dirección de envío, etc.) asociados con cada cuenta de usuario, parámetros personalizados (por ejemplo, edad, ubicación, pasatiempos, etc.) para cada cuenta de usuario, contactos de redes sociales de cada cuenta de usuario; y datos 288 de uso de cuenta de usuario que almacenan datos de uso de cada cuenta de usuario en el dispositivo 104 de cliente.

Cada uno de los elementos identificados anteriormente puede almacenarse en uno o más de los dispositivos de memoria mencionados anteriormente, y corresponde a un conjunto de instrucciones para realizar una función descrita anteriormente. Los módulos o programas identificados anteriormente (es decir, conjuntos de instrucciones) no necesitan ser implementados como programas de software, procedimientos, módulos o estructuras de datos separados, y así varios subconjuntos de estos módulos pueden ser combinados o reorganizados de otra forma en varias implementaciones. En algunas implementaciones, la memoria 256, opcionalmente, almacena un subconjunto de los módulos y estructuras de datos identificados anteriormente.

Además, la memoria 256, opcionalmente, almacena módulos adicionales y estructuras de datos no descritos anteriormente.

En algunas realizaciones, al menos algunas de las funciones del sistema servidor 108 son realizadas por el dispositivo 104 de cliente, y los sub-módulos correspondientes de estas funciones pueden estar ubicados dentro del dispositivo 104 de cliente en vez de en el sistema servidor 108. En algunas realizaciones, al menos algunas de las funciones del dispositivo 104 de cliente son realizadas por el sistema servidor 108, y los correspondientes sub-módulos de estas funciones pueden ser ubicados dentro del sistema servidor 108 en vez del dispositivo 104 de cliente. El dispositivo 104 de cliente y el sistema servidor 108 mostrados en las figuras 2A-2B, respectivamente, son meramente ilustrativos, y diferentes configuraciones de los módulos para implementar las funciones descritas en la presente memoria son posibles en diversas realizaciones.

La figura 3A es un diagrama de flujo de un método 300 para verificar una operación de cuenta de acuerdo con algunas realizaciones. En algunas realizaciones, el método 300 se ejecuta mediante un sistema informático (por ejemplo, el sistema servidor 108, figuras 1 y 2A) para verificar la operación de la cuenta. El sistema servidor 108 recibe (302) una solicitud de verificación de cuenta la cual se envía mediante un dispositivo móvil (por ejemplo, dispositivo 104-1 de cliente, figuras 1 y 2B) durante un registro a una cuenta en el dispositivo 104-1 móvil. La solicitud de verificación de cuenta incluye un identificador de dispositivo móvil (por ejemplo, ID de dispositivo).

El sistema servidor 108 obtiene (304) el historial de uso de la cuenta en el dispositivo 104-1 móvil asociado con el identificador de dispositivo móvil. El historial de uso incluye datos del historial de registro y/o datos operativos del historial de registro en la cuenta en el dispositivo 104-1 móvil correspondiente al identificador de dispositivo móvil.

El sistema servidor 108 determina (306), de acuerdo con los datos de historial de uso de la cuenta en el dispositivo 104-1 móvil, si el dispositivo 104-1 móvil asociado con el identificador de dispositivo móvil es un dispositivo de confianza (es decir, un dispositivo seguro). De acuerdo con un resultado de determinación, el sistema servidor 108 devuelve un resultado de verificación de cuenta al dispositivo 104-1 móvil en respuesta a la solicitud de verificación de cuenta.

En algunas realizaciones, antes de recibir (302) la solicitud de verificación de cuenta, el sistema servidor 108 genera además información de código bidimensional y envía la información de código bidimensional a una página de destino, para que la página destino genere un código bidimensional de acuerdo con la información del código bidimensional y muestre el código bidimensional en la página de destino.

En algunas realizaciones, el sistema servidor 108 genera información de código bidimensional, donde la información de código bidimensional es información utilizada para verificar el funcionamiento de la cuenta, tal como un proceso de registro de cuenta, y el sistema servidor 108 puede generar dinámicamente información de código bidimensional de acuerdo con cuentas diferentes. La información de código bidimensional puede ser una cadena de caracteres tal como un identificador de WeChat, y el sistema servidor 108 entrega la información de código bidimensional generada a una página de destino, donde la página de destino puede ser una página de visualización en un dispositivo terminal (por ejemplo, dispositivo 104-2 de cliente, figura 1) como un ordenador personal o un ordenador portátil. En algunas realizaciones, se ha verificado que el dispositivo 104-2 terminal es seguro para una operación de cuenta de usuario. En algunas realizaciones, la página de destino puede ser una página web o una página almacenada en el dispositivo 104-2 terminal. En algunas realizaciones, la página de destino recibe la información del código bidimensional, luego genera un código bidimensional de acuerdo con la información del código bidimensional, y muestra el código bidimensional en la página de destino. Entonces se requiere que el dispositivo 104-1 móvil escanee el código bidimensional en la página de destino utilizando una cámara del dispositivo 104-1 móvil, y analiza el código bidimensional escaneado para obtener la información del código bidimensional para verificar el registro en una cuenta en el dispositivo 104-1 móvil. En algunas realizaciones, el código bidimensional es, por ejemplo, una Respuesta Rápida (QR, un tipo de código bidimensional) y similares.

En algunas realizaciones, antes de recibir (302) la solicitud de verificación de cuenta, el sistema servidor 108 además (1) obtiene datos de operación de registro durante un registro en una cuenta en el dispositivo 104-1 móvil; (2) determina si los datos de operación de registro adquiridos de la cuenta coinciden con los criterios inseguros predeterminados, por ejemplo, datos de operación inseguros predeterminados; y (3) si los datos de registro de la cuenta obtenidos coinciden con los criterios inseguros predeterminados, envía una instrucción de verificación de cuenta al dispositivo 104-1 móvil. La instrucción de verificación de cuenta puede solicitar el identificador de dispositivo asociado con el dispositivo 104-1 móvil. En tales implementaciones, el dispositivo 104-1 móvil envía una solicitud de verificación de cuenta que incluye un identificador de dispositivo de acuerdo con la instrucción de verificación de cuenta.

En algunas realizaciones, el servidor 108 de sistema puede adquirir datos de operación de registro durante un registro en una cuenta en el dispositivo 104-1 móvil. Los datos de operación de registro incluyen los datos de registro durante el registro en la cuenta y los datos de uso después del registro en la cuenta. Los datos de registro, por ejemplo, los datos de registro de la cuenta, durante el registro en la cuenta, pueden incluir además una dirección de registro, una plataforma de registro, un modo de registro y similares. Los datos de uso incluyen, por ejemplo, una operación de cancelación de la cuenta, una consulta de datos personales, tal como una identidad personal, un número de teléfono móvil, un amigo de la cuenta, una consulta de información de propiedad de la cuenta, un cambio de la información de propiedad de la cuenta, y similares.

El sistema servidor 108 determina si los datos de operación de registro de cuenta obtenidos coinciden con los criterios inseguros predeterminados, por ejemplo, datos de operación no seguros predeterminados. De acuerdo con una determinación de que los datos de operación de registro obtenidos coinciden con los criterios inseguros predeterminados, el sistema servidor 108 envía una instrucción de verificación de cuenta al dispositivo 104-1 móvil, para que el dispositivo móvil 104-1 pueda enviar, de acuerdo con la instrucción de verificación de cuenta, al sistema servidor 108, una solicitud de verificación de cuenta que incluya el identificador de dispositivo asociado con el dispositivo 104-1 móvil. En algunas realizaciones, los criterios inseguros predeterminados incluyen, pero no se limitan a: cancelar la cuenta, cambiar la información de propiedad de la cuenta, datos operativos únicos tales como información de fraude relacionada con la propiedad para enviar a un amigo durante la mensajería instantánea.

En algunas realizaciones, los datos operativos de registro obtenidos de la cuenta se pueden analizar y autentificar para obtener múltiples palabras clave, y luego las múltiples palabras clave se comparan con palabras clave en los datos de operación insegura predeterminados. Si una palabra clave en los datos operativos de registro coincide con una palabra clave en los datos operativos inseguros, se determina que los datos operativos de registro obtenidos de la cuenta coinciden con los criterios inseguros predeterminados y se envía una instrucción de verificación de cuenta al dispositivo 104-1 móvil, por lo que el dispositivo 104-1 móvil puede enviar, de acuerdo con la instrucción de verificación de cuenta al sistema servidor 108, la solicitud de verificación de cuenta que incluye el identificador del terminal móvil. Por lo tanto, se puede implementar la detección y determinación de una operación de cuenta insegura, y si se determina que ocurre una operación insegura de la cuenta, se ejecuta el método 300 de la figura 3A y se necesita realizar la verificación de cuenta para garantizar la seguridad y fiabilidad de la operación de la cuenta.

En algunas realizaciones, la solicitud de verificación de cuenta enviada desde el dispositivo 104-1 móvil durante un registro a una cuenta y recibida (302) por el sistema servidor 108 incluye un identificador de dispositivo. En algunas realizaciones, la solicitud de verificación de cuenta incluye, pero no se limita a, información de código bidimensional obtenida por el dispositivo 104-1 móvil escaneando un código bidimensional mostrado en una página de destino y analizando el código bidimensional escaneado. La solicitud de verificación de cuenta puede incluir además otra información de verificación, tal como una contraseña y un código de acceso único, introducido para la cuenta. El sistema servidor 108 recibe la solicitud de verificación de cuenta que se envía mediante el dispositivo 104-1 móvil e incluye el identificador de dispositivo móvil, donde el identificador de dispositivo móvil es un identificador único del dispositivo 104-1 móvil. En algunas realizaciones, el identificador de dispositivo móvil puede ser un identificador de hardware único del dispositivo móvil, tal como una identidad de tarjeta multimedia insertada (EMMC ID, que es una identidad de hardware globalmente única de EMMC Flash, y es un valor numérico hexadecimal de 32 bits), una identidad de identificador de equipo móvil (ME ID, que es una identidad de identificador de terminal móvil de 56 bits globalmente única), y una identidad de equipo móvil internacional (IMEI).

El identificador de terminal móvil también puede ser un identificador generado de una manera combinada de acuerdo con el identificador de hardware del terminal móvil.

En algunas realizaciones, se obtienen los datos históricos de una cuenta correspondiente al identificador de dispositivo móvil, donde los datos históricos incluyen datos históricos de registro y/o datos de operación históricos del registro de la cuenta en el dispositivo 104-1 móvil correspondiente al identificador del dispositivo móvil. En algunas realizaciones, los datos de registro históricos son los datos obtenidos durante un registro de la cuenta en el dispositivo 104-1 móvil. En algunas realizaciones, los datos de registro de la cuenta incluyen, pero no están limitados a, una frecuencia de registro dentro de un período preestablecido, y los datos de registro de la cuenta pueden incluir además: un Protocolo de Internet (IP) de registro, una plataforma de registro o una forma de registro. La plataforma de registro es, por ejemplo, un cliente de registro de teléfono móvil o un cliente de registro de página web. La información de modo de registro es, por ejemplo, un registro automático, un registro después de la entrada de una respuesta de protección de registro o un registro después de la entrada de una contraseña de cuenta.

La frecuencia de registro dentro de un período predeterminado puede ser la cantidad total de registros dentro del período predeterminado, y el período predeterminado es un período predeterminado y editable, tal

como 18 horas, 3 días, 15 días y 30 días. La frecuencia de registro dentro de un período preestablecido es que, por ejemplo, hay 6 registros en WeChat en el dispositivo 104-1 móvil dentro de los últimos 15 días. En algunas realizaciones, el período predeterminado puede incluir además múltiples sub-períodos predeterminados, por tanto la frecuencia de registro dentro de un período predeterminado incluye que : el número de registros en cada sub-período predeterminado es mayor que 1. Por ejemplo, el período predeterminado es 3 días y cada sub-período predeterminado es de 1 día, por tanto el número de registros en WeChat en el dispositivo 104-1 móvil cada día es mayor que 1.

Los datos de operación históricos incluyen, pero no se limitan a, una duración de uso. Los datos de operación históricos incluyen además todos los registros de operación desde un registro en la cuenta. Específicamente, la duración de uso es un intervalo de tiempo desde un registro en la cuenta y el último registro de operación después del registro en la cuenta. Por ejemplo, hay 2 registros en la cuenta dentro de un día. El primer registro tiene lugar a las 11:25 y los registros de operación son conservados a las 11:23, 12:00, ..., 12:15 y 13:25. El segundo registro tiene lugar a las 14:00. Por lo tanto, dentro del tiempo antes del segundo registro, el tiempo, cuando se conserva un registro de operación, más cercano al segundo registro se determina como el último tiempo de funcionamiento en el primer registro, es decir, 13:25 como el último tiempo de funcionamiento y se calcula que la duración de utilización es de 2 horas.

En algunas realizaciones, los datos históricos pueden incluir además un identificador de confianza predefinido o una clave predefinida. El identificador de confianza predefinido es un identificador de dispositivo móvil almacenado en el sistema servidor 108 de antemano, y es un identificador de dispositivo móvil que ha pasado la verificación de seguridad (es decir, calificado como seguro). La clave predefinida es una clave generada dinámicamente por el sistema servidor 108 de acuerdo con un algoritmo predefinido, y la clave generada dinámicamente se incluye en los datos intercambiados en el dispositivo 104-1 móvil cada vez, donde el dispositivo 104-1 móvil no puede descifrar la clave. El sistema servidor 108 implementa tanto la generación como el análisis de la clave, y la clave preestablecida entregada por el sistema servidor 108 está incluida en los datos devueltos por el dispositivo 104-1 móvil al sistema servidor 108, de modo que el sistema servidor 108 puede realizar el descifrado y la verificación en la clave preestablecida.

En algunas realizaciones, el sistema servidor 108 determina (306), de acuerdo con los datos históricos de la cuenta correspondiente al identificador de dispositivo móvil, si el identificador de dispositivo móvil es un identificador de confianza y de acuerdo con un resultado de determinación, una respuesta de verificación de cuenta correspondiente a la solicitud de verificación de cuenta se devuelve al dispositivo 104-1 móvil.

En algunas realizaciones, si los datos de registro históricos incluyen una frecuencia de registro dentro de un período preestablecido, y los datos de operación históricos incluyen una duración de uso, la determinación de si el identificador de dispositivo móvil es un identificador de confianza según los datos históricos de la cuenta correspondiente al identificador de dispositivo móvil puede incluir específicamente: si la frecuencia de registro dentro del período preestablecido cumple con un umbral de frecuencia preestablecido, y/o la duración de uso cumple con un umbral de tiempo preestablecido, el sistema servidor 108 determina que el identificador de dispositivo móvil es un identificador de confianza.

Por ejemplo, si una cuenta 1 se registra sesión en o sobre un dispositivo móvil 1, un período preestablecido es de 15 días, hay un total de 8 registros en la cuenta 1 por un cliente en el dispositivo 1 móvil dentro de los 15 días, y un umbral de frecuencia preestablecido es de al menos 5 registros dentro de los 15 días, se puede determinar que un identificador de dispositivo móvil del dispositivo 1 móvil es un identificador de confianza. Si una cuenta 2 se registra en o sobre un dispositivo 2 móvil, un período preestablecido es de 3 días, hay 2 registros cada día en la cuenta 2 por un cliente en el dispositivo 2 móvil en tres días, una frecuencia de registro dentro del período preestablecido es al menos 2 registros cada día, y un umbral de frecuencia preestablecido es que el número de registros en cada sub-período preestablecido es mayor que 1, se puede determinar que un identificador de dispositivo móvil del dispositivo 2 móvil es un identificador de confianza. Si una cuenta 3 se registra por un cliente en un dispositivo 3 móvil, una duración de uso es de 3 horas, y un umbral de tiempo preestablecido es más de 2 horas, se puede determinar que el identificador de dispositivo móvil del dispositivo móvil 3 es un identificador de confianza.

En algunas realizaciones, si la frecuencia de registro dentro de un período preestablecido no cumple con el umbral de frecuencia preestablecido, y/o la duración del uso no cumple con el umbral de tiempo preestablecido, se determina que el identificador del dispositivo móvil no es un identificador de confianza.

En algunas realizaciones, si los datos históricos incluyen: un identificador de confianza preestablecido, la determinación de si el identificador de dispositivo móvil es un identificador de confianza de acuerdo con los datos históricos de la cuenta correspondiente al identificador de dispositivo móvil puede incluir específicamente determinar si el identificador de dispositivo móvil es idéntico al identificador de confianza predeterminado, si es así, se determina que el identificador de dispositivo móvil es un identificador de confianza.

El identificador de confianza es un identificador de dispositivo móvil añadido en el sistema servidor 108 de antemano, y es un identificador de dispositivo móvil que ha pasado la verificación de seguridad. Si se encuentra que un identificador de confianza preestablecido es idéntico al identificador de dispositivo móvil en los identificadores de confianza preestablecidos almacenados, se determina que el identificador de dispositivo móvil es un identificador de confianza.

En algunas realizaciones, si el identificador de dispositivo móvil no es idéntico al identificador de confianza preestablecido, puede verificarse de otras maneras si el identificador de dispositivo móvil es un identificador de confianza.

En algunas realizaciones, si los datos históricos incluyen: una clave preestablecida. Después de recibir (302) la solicitud de verificación de cuenta, el método 300 puede incluir además el análisis de una solicitud de verificación de cuenta para obtener una clave de la solicitud de verificación de cuenta. Determinar (306) si el identificador de dispositivo móvil es un identificador de confianza de acuerdo con los datos históricos adquiridos de una cuenta correspondiente al identificador de dispositivo móvil puede incluir además determinar si la clave de la solicitud de verificación de cuenta es idéntica a la clave preestablecida, si es así, el identificador de dispositivo móvil se determina que es un identificador de confianza.

La clave preestablecida es una clave generada dinámicamente por el sistema servidor 108 de acuerdo con un algoritmo preestablecido, y si la clave de la solicitud de verificación de cuenta obtenida a través del análisis es idéntica a la clave preestablecida, se determina que el identificador del dispositivo es un identificador de confianza.

En algunas realizaciones, si se determina, de acuerdo con los datos históricos adquiridos de la cuenta correspondiente al identificador de dispositivo móvil, que el identificador de dispositivo móvil es un identificador de confianza, se devuelve una respuesta positiva a la solicitud de verificación de cuenta al dispositivo móvil. De lo contrario, se devuelve una respuesta negativa a la solicitud de verificación de cuenta al dispositivo móvil. En algunas realizaciones, después de devolver la respuesta positiva a la solicitud de verificación de la cuenta al dispositivo móvil, también puede ser recibida, información de verificación, tal como una contraseña o un código de acceso único, enviado por el dispositivo móvil, para además realizar la verificación de la cuenta.

En el método 300 para verificación de cuenta proporcionado en la presente solicitud, se puede recibir una solicitud de verificación de cuenta enviada por un dispositivo móvil, donde la solicitud de verificación de cuenta incluye un identificador de dispositivo móvil. Se pueden obtener datos históricos de una cuenta correspondiente al identificador del dispositivo móvil. Se puede determinar de acuerdo con los datos históricos adquiridos de la cuenta correspondiente al identificador del dispositivo móvil si el identificador del dispositivo móvil es un identificador de confianza. De acuerdo con una determinación que, puede devolverse una respuesta de verificación de cuenta correspondiente a la solicitud de verificación de cuenta al dispositivo móvil. Por lo tanto, en algunas implementaciones de la presente solicitud, se determina, de acuerdo con los datos históricos de una cuenta correspondiente a un identificador de dispositivo móvil, si el identificador de dispositivo móvil es un identificador de confianza, para realizar la verificación de seguridad y fiabilidad de un dispositivo móvil dispositivo en el cual la cuenta está registrada, y se mejora la seguridad y la fiabilidad de la verificación de la cuenta.

La figura 3B es una vista esquemática de bloques de un sistema 310 informático (por ejemplo, el sistema servidor 108) para verificar una operación de cuenta de acuerdo con algunas realizaciones. El sistema 310 informático de la figura 3B para la verificación de la cuenta se utiliza para ejecutar el método 300 de acuerdo con la realización mostrada en la figura 3A de la presente solicitud. Para facilitar la descripción, solo se muestran partes relacionadas con la realización de la presente solicitud, y para detalles técnicos específicos no descritos, se puede hacer referencia a la realización mostrada en la figura 3A de la presente solicitud.

Como se muestra en la figura 3B, el sistema 310 informático incluye: un módulo 311 de recepción, un módulo 312 de obtención y un módulo 314 de verificación. En algunas realizaciones, el sistema 310 informático puede incluir además: un módulo 320 de generación y un módulo 318 de envío. En algunas realizaciones, el módulo 320 de generación se utiliza para generar información de código bidimensional. El módulo 318 de envío se utiliza para enviar la información de código bidimensional a una página de destino, de modo que la página de destino genera un código bidimensional de acuerdo con la información de código bidimensional, y muestra el código bidimensional en la página de destino. En algunas realizaciones, el sistema 310 informático puede incluir además un módulo 316 de determinación.

El módulo 312 de obtención se utiliza para obtener datos de operación de registro durante el registro en la cuenta en el dispositivo móvil. El módulo 316 de determinación se utiliza para determinar si los datos de operación de registro de la cuenta obtenidos coinciden con los criterios inseguros predeterminados, por ejemplo, datos de operación insegura predeterminados. El módulo 318 de envío se utiliza para, cuando el módulo 316 de determinación determina que los datos de operación de registro obtenidos coinciden con los

criterios inseguros predeterminados, enviando una instrucción de verificación de cuenta al dispositivo móvil. En algunas realizaciones, el módulo 312 de obtención obtiene los datos de operación de registro durante un registro en una cuenta en un dispositivo móvil.

El módulo 311 de recepción se utiliza para recibir la solicitud de verificación de cuenta que se envía por el dispositivo móvil durante un registro en una cuenta. El módulo 312 de obtención se utiliza para obtener datos históricos de la cuenta correspondiente al identificador del dispositivo móvil. El módulo 314 de verificación se utiliza para determinar si el identificador de dispositivo móvil es un identificador de confianza de acuerdo con los datos históricos de la cuenta correspondiente al identificador de dispositivo móvil, y de acuerdo con un resultado de determinación, devolver una respuesta de verificación de cuenta correspondiente a la solicitud de verificación de cuenta al dispositivo móvil.

La figura 3C es una vista esquemática en bloque de un módulo 314 de verificación del sistema informático para verificar una operación de cuenta de acuerdo con algunas realizaciones. El módulo 314 de verificación puede incluir una o más unidades, tales como una primera unidad 332 de verificación, una segunda unidad 334 de verificación y una tercera unidad 336 de verificación.

En algunas realizaciones, si los datos históricos de registro incluyen una frecuencia de registro dentro de un período preestablecido, y los datos de operación históricos incluyen una duración de uso, la primera unidad 332 de verificación se utiliza para determinar si el identificador de dispositivo móvil es un identificador de confianza al comparar la frecuencia de registro dentro de un período preestablecido con un umbral de frecuencia preestablecido y/o comparando la duración de uso con un umbral de tiempo preestablecido.

En algunas realizaciones, la primera unidad 332 de verificación se utiliza además para determinar que el identificador de dispositivo móvil es un identificador inseguro, cuando la frecuencia de registro dentro de un período preestablecido no cumple el umbral de frecuencia preestablecido, y/o la duración de uso no cumple el umbral de tiempo preestablecido.

En algunas realizaciones, si los datos históricos incluyen un identificador de confianza preestablecido, la segunda unidad 334 de verificación se utiliza para determinar que el identificador de dispositivo móvil es un identificador de confianza cuando el identificador de dispositivo móvil es idéntico al identificador de confianza preestablecido.

En algunas realizaciones, si el identificador de dispositivo móvil no es idéntico al identificador de confianza preestablecido, la primera unidad 332 de verificación o la tercera unidad 336 de verificación pueden realizar una verificación para encontrar si el identificador de dispositivo móvil es un identificador de confianza.

Volviendo a la figura 3B, en algunas realizaciones, si los datos históricos incluyen una clave preestablecida, el sistema 310 informático incluye además un módulo 322 de análisis. El módulo 322 de análisis se utiliza para analizar la solicitud de verificación de cuenta para obtener una clave de la solicitud de verificación de cuenta.

En la figura 3C, la tercera unidad 336 de verificación se utiliza para determinar que el identificador de dispositivo móvil es un identificador de confianza cuando la clave de la solicitud de verificación de cuenta es idéntica a la clave preestablecida.

En algunas realizaciones, el módulo 314 de verificación se utiliza además para devolver una respuesta de fallo de verificación de cuenta al terminal móvil, cuando se determina que el identificador de dispositivo móvil es un identificador inseguro. En algunas realizaciones, después de que se haya devuelto una respuesta de éxito de verificación de cuenta al dispositivo móvil, el módulo 311 de recepción puede recibir además información de verificación, tal como una contraseña o un código de paso de una sola vez , enviado por el dispositivo móvil, y así se pueda realizar además la verificación del módulo 314.

En el sistema 310 informático para la verificación de cuenta que proporciona la presente solicitud, el módulo 311 de recepción puede recibir una solicitud de verificación de cuenta enviada por un dispositivo móvil; el módulo 312 de obtención puede obtener datos históricos de una cuenta que corresponde al identificador de dispositivo móvil; el módulo 314 de verificación puede determinar, de acuerdo con los datos históricos obtenidos de la cuenta correspondiente al identificador de dispositivo móvil, si el identificador de dispositivo móvil es un identificador de confianza y, de acuerdo con un resultado de determinación, devolver una respuesta de verificación de cuenta que corresponde a la solicitud de verificación de cuenta al dispositivo móvil. Por lo tanto, en algunas implementaciones de la presente solicitud, se determina, de acuerdo con los datos históricos de una cuenta correspondiente a un identificador de dispositivo móvil, si el identificador de dispositivo móvil es un identificador de confianza, para realizar la verificación de seguridad y fiabilidad de un dispositivo móvil en el que la cuenta está registrada, y se mejora la seguridad y la fiabilidad de la verificación de la cuenta.

La figura 4A ilustra un diagrama de flujo de un método 400 de verificación de una operación de cuenta de acuerdo con algunas realizaciones. En algunas realizaciones, el método 400 se realiza en el entorno 100 de cliente-servidor (figura 1) con el sistema servidor 108, el dispositivo 104-1 de cliente y el dispositivo 104-2 de cliente, cada uno de los cuales incluye uno o más procesadores y memoria. Como se muestra en la figura 4A, el dispositivo 104-1 de cliente envía (402) una solicitud de verificación al sistema servidor 108 para verificar una operación de cuenta. En algunas realizaciones, la solicitud de verificación incluye información asociada con la cuenta de usuario y una ID de dispositivo asociada con el dispositivo 104-1 de cliente.

Después de recibir la solicitud de verificación, el sistema servidor 108 identifica (404) datos de uso de la cuenta del usuario almacenados en el sistema servidor 108 (por ejemplo, datos 246 de uso de cuenta de usuario, figura 2A). El sistema servidor 108 luego verifica (404) los datos de uso identificados de la cuenta de usuario, por ejemplo, determinando si la operación de cuenta asociada con la cuenta de usuario en el dispositivo 104-1 de cliente es segura. De acuerdo con una determinación de que la operación de cuenta asociada con la cuenta de usuario en el dispositivo 104-1 de cliente es segura, el sistema servidor 108 responde (406) al dispositivo 104-1 de cliente con una respuesta positiva a la solicitud de verificación. De acuerdo con una determinación de que la operación del usuario asociada con la cuenta de usuario en el dispositivo 104-1 de cliente no es segura, el sistema servidor 108 inicia un proceso de verificación basado en una interacción entre el dispositivo 104-2 de cliente y el dispositivo 104-1 de cliente. Por ejemplo, el sistema servidor 108 genera (408) una imagen 408 codificada para visualizar en el dispositivo 104-2 de cliente, y promueve que el usuario del dispositivo 104-1 de cliente escanee la imagen codificada. En algunas realizaciones, el dispositivo 104-2 de cliente es calificado como seguro para la operación de la cuenta basado en los datos del historial de uso asociados con una o más cuentas del usuario y uno o más criterios de historial de uso predeterminados. En algunas realizaciones, el sistema servidor 108 envía (410) la imagen codificada al dispositivo 104-2 de cliente para su visualización. El sistema servidor 108 promueve (412) que el usuario del dispositivo 104-1 de cliente escanee la imagen codificada mostrada en el dispositivo 104-2 de cliente.

En algunas realizaciones, el dispositivo 104-1 de cliente escanea (414) la imagen codificada mostrada en el dispositivo 104-2 de cliente, y el dispositivo 104-1 de cliente envía (416) la imagen codificada escaneada al sistema servidor 108.

En algunas realizaciones, el sistema servidor 108 recibe la imagen codificada escaneada desde el dispositivo 104-1 de cliente, el sistema servidor 108 verifica (418) la imagen codificada escaneada. Por ejemplo, el sistema servidor 108 determina si la imagen codificada escaneada coincide con la imagen codificada enviada al dispositivo 104-2 de cliente. El sistema servidor 108 envía (420) el resultado de verificación al dispositivo 104-1 de cliente. Por ejemplo, el resultado de la verificación incluye que la operación de la cuenta en el dispositivo 104-1 de cliente es segura, si la imagen codificada escaneada coincide con la imagen codificada enviada al dispositivo 104-2 de cliente.

La figura 4B es una realización ejemplar de una interfaz 430 de usuario para registrarse en una cuenta 431 de usuario en el dispositivo 104-1 de cliente. La cuenta 431 de usuario está asociada con el usuario del dispositivo 104-1 de cliente. Como se muestra en la figura 4B, la interfaz 430 de usuario corresponde a una plataforma de aplicación (por ejemplo, plataforma WeChat). Durante el registro de la cuenta 431 de usuario, se solicita al usuario que introduzca credenciales 432 de registro, tales como el nombre de cuenta de usuario y la contraseña para la cuenta 431 de usuario. En algunas realizaciones, después de presionar el botón 433 de envío en la interfaz 430 de usuario, se envía una solicitud de verificación al sistema servidor 108 para la verificación. En algunas realizaciones, la solicitud de verificación incluye las credenciales 432 de registro introducidas y la ID de dispositivo del dispositivo 104-1 de cliente.

La figura 4C es una realización ejemplar de la interfaz 430 de usuario en el dispositivo 104-1 de cliente durante la verificación. En algunas realizaciones, de acuerdo con una determinación de que el proceso de registro asociado con la cuenta 431 de usuario en el dispositivo 104-1 de cliente no es seguro, el sistema servidor 108 inicia un proceso de verificación entre el dispositivo 104-1 de cliente y un dispositivo de cliente (por ejemplo, dispositivo 104-2 de cliente) que califica como segura la operación de cuenta de usuario en el dispositivo 104-2 de cliente. En algunas realizaciones, el sistema servidor 108 promueve que el usuario escanee una imagen codificada mostrada en el dispositivo 104-2 cliente mostrando un cuadro 434 de notificación como se muestra en la figura 4C.

La figura 4D es una realización ejemplar de una interfaz 440 de usuario de la misma plataforma de aplicación (por ejemplo, plataforma Wechat) registrada en el dispositivo 104-2 de cliente. En algunas realizaciones, la plataforma Wechat es registrada por el mismo usuario del dispositivo 104-1 de cliente utilizando la misma cuenta 431 de usuario en el dispositivo 104-2 de cliente.

La figura 4E es una realización ejemplar de una interfaz 450 de usuario de una plataforma de aplicación diferente (por ejemplo, la plataforma QQ) registrada en el dispositivo 104-2 de cliente. En algunas realizaciones, la plataforma QQ es registrada por el mismo usuario del dispositivo 104-1 de cliente usando

una cuenta 451 de usuario en el dispositivo 104-2 de cliente. La cuenta 451 de usuario es distinta de la cuenta 431 de usuario.

La figura 4F es una realización ejemplar de una interfaz de usuario que muestra una imagen 460 codificada para un proceso de verificación de interacción entre el dispositivo 104-1 de cliente y el dispositivo 104-2 de cliente. En algunas realizaciones como se muestra en la figura 4C, después de que se determina que las credenciales 432 de registro no son seguras, el sistema servidor 108 promueve que el usuario escanee la imagen 430 codificada mostrada en el dispositivo 104-2 de cliente utilizando el dispositivo 104-1 de cliente. El sistema servidor 108 genera y envía la imagen 460 codificada para su visualización en el dispositivo 104-2 de cliente como se muestra en la figura 4F.

Aunque no se muestra en las figuras, en algunas realizaciones, el sistema servidor 108 detecta que el dispositivo 104-2 de cliente es capaz de escanear imágenes, pero el dispositivo 104-1 de cliente no incluye una funcionalidad para realizar el escaneo. En tales implementaciones, el sistema servidor 108 envía la imagen codificada al dispositivo 104-1 de cliente para su visualización, y promueve que el usuario del dispositivo 104-2 de cliente escanee la imagen codificada mostrada en el dispositivo 104-1 de cliente.

La figura 4G es una realización ejemplar de la interfaz 430 de usuario en el dispositivo 104-1 de cliente durante la verificación. En algunas realizaciones, de acuerdo con una determinación de que el proceso de registro asociado con la cuenta 431 de usuario en el dispositivo 104-1 de cliente no es seguro, el sistema servidor 108 inicia un proceso de verificación entre el dispositivo 104-1 de cliente y el dispositivo 104-2 de cliente. En algunas realizaciones como se indica en el cuadro 470 de notificación, el sistema servidor 108 promueve que el usuario se registre en una cuenta 471 de usuario que es distinta de la cuenta 431 de usuario, en una misma plataforma de aplicación (por ejemplo, plataforma Wechat) o una plataforma de aplicación diferente (por ejemplo, plataforma QQ), en el dispositivo 104-2 de cliente. En algunas realizaciones como se muestra en la instrucción 472, el sistema servidor 108 requiere que el usuario realice la verificación indicada dentro de un umbral de tiempo predeterminado (por ejemplo, 10 minutos).

Las figuras 5A-5F ilustran un diagrama de flujo de un método 500 para verificar una operación de cuenta de acuerdo con algunas realizaciones. En algunas realizaciones, el método 500 se realiza mediante el sistema servidor 108 con uno o más procesadores y memoria. Por ejemplo, en algunas realizaciones, el método 500 se realiza mediante el sistema servidor 108 (figuras 1-2A) o un componente del mismo (por ejemplo, el módulo 106 del lado-servidor, figuras 1-2A). En algunas realizaciones, el método 500 se controla por las instrucciones que están almacenadas en un medio de almacenamiento legible por por ordenador no transitorio y las instrucciones son ejecutadas por uno o más procesadores del sistema de servidor. Las operaciones opcionales se indican mediante líneas discontinuas (por ejemplo, cuadros con bordes de líneas discontinuas).

En el método 500, el sistema servidor 108 obtiene (502) una solicitud de verificación desde un primer dispositivo (por ejemplo, dispositivo 104-1 de cliente , figuras 1 y 2B) para una operación de cuenta solicitada por un usuario que utiliza una primera cuenta (por ejemplo, cuenta 431 de usuario, figura 4B). En algunas realizaciones, la solicitud de verificación incluye información asociada con la primera cuenta y una ID de dispositivo asociada con el primer dispositivo.

En algunas realizaciones, el usuario pretende realizar una operación en una plataforma (por ejemplo, plataforma 430, figura 4B) en el primer dispositivo, se envía una solicitud de verificación desde el primer dispositivo al sistema servidor 108 para determinar si la cuenta la operación asociada con la primera cuenta en el primer dispositivo es segura. En algunas realizaciones, la operación de cuenta incluye, pero no se limita a: (1) registrarse en una plataforma de aplicación en el primer dispositivo utilizando una primera cuenta, (2) borrar la primera cuenta en el primer dispositivo, (3) modificar la información de cuenta de la primera cuenta, tal como contraseña, nombre de cuenta, etc., (4) consultar información de privacidad personal, información financiera y/o información de identidad, (5) publicar datos personales al público, por ejemplo, publicación de fotos o notas almacenadas en el primer dispositivo para WeChat, etc.

En algunas realizaciones, la solicitud de verificación incluye la primera información de la cuenta, tal como el primer nombre de cuenta y contraseña utilizados para el registro, y la ID del dispositivo asociada con el primer dispositivo. En algunas realizaciones, la solicitud de verificación también incluye una dirección IP de registro, una plataforma de registro (por ejemplo, WeChat, QQ, etc.) y/o una forma de registro (por ejemplo, desde un teléfono móvil, una tableta o un PC) que se utilizan para registrarse en la primera cuenta en el primer dispositivo.

El sistema servidor 108 identifica (504) datos del historial de uso asociados con la primera cuenta desde el sistema de servidor. En algunas realizaciones, datos del historial de uso incluyen datos con respecto al uso de la primera cuenta en el primer dispositivo.

En algunas realizaciones, después de recibir la solicitud de verificación, el sistema servidor 108 identifica la primera cuenta y el primer dispositivo basado en la ID de dispositivo incluida en la solicitud de verificación, y el sistema servidor 108 identifica datos del historial de uso, en particular, datos del historial de uso asociado con el uso de la primera cuenta realizada en el primer dispositivo. Los datos de historial incluyen datos de registro de historial y/o datos de operación de historial de la primera cuenta asociada con el primer dispositivo. En algunas realizaciones, si no existen tales datos de uso con respecto al uso de la primera cuenta en el primer dispositivo, el hecho de no haber sido utilizado anteriormente se indica para el primer dispositivo.

El sistema servidor 108 determina (506) si la operación de cuenta asociada con la primera cuenta en el primer dispositivo es segura, de acuerdo con los datos con respecto al uso de la primera cuenta en el primer dispositivo y uno o más criterios de historial de uso predeterminados. El servidor puede determinar si la operación asociada con la primera cuenta en el primer dispositivo es segura mediante el examen de los datos del historial identificados en función de uno o más criterios.

En algunas realizaciones, uno o más criterios de historial de uso predeterminados incluyen: (1) una frecuencia de la primera cuenta que intenta registrarse en el primer dispositivo dentro de un umbral de tiempo predeterminado está por debajo de un umbral predeterminado (por ejemplo, 10 intentos de registro dentro de los últimos diez minutos), (2) una frecuencia de los primeros registros de cuenta en el primer dispositivo es mayor que un umbral de frecuencia predeterminado (por ejemplo, en promedio 1 vez por día), (3) el tiempo de la primera cuenta de usuario que permanece registrada en el primer dispositivo dentro de un umbral de tiempo predeterminado es mayor que un valor predeterminado (por ejemplo, 10 horas en los últimos 15 días), (4) un tiempo entre el registro actual y el último registro en el primer dispositivo utilizando la primera cuenta está dentro de un umbral de período de tiempo predeterminado (por ejemplo, no mayor de 3 meses).

De acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el primer dispositivo no es segura, el sistema servidor 108 inicia (508) un proceso de verificación basado en un segundo dispositivo (por ejemplo, dispositivo 104-2 de cliente, figura 1) que califica como seguro para la operación de cuenta basado en los datos del historial de uso asociados con una o más cuentas del usuario y uno o más criterios de historial de uso predeterminados.

En algunas realizaciones, cuando se determina que la primera cuenta en el primer dispositivo no es segura basado en los datos de historial relevantes y los criterios de uso predeterminados, el método 500 procede a requerir verificación adicional basada en un segundo dispositivo que es un dispositivo seguro para la primera cuenta basado en los datos de uso históricos con respecto al uso de la primera cuenta en el segundo dispositivo.

En este momento, el segundo dispositivo puede estar cerca de un dispositivo que ya se ha registrado, y luego el registro del usuario en el segundo dispositivo se verifica que es seguro por el servidor. El segundo dispositivo también puede ser buscado primero basado en los datos históricos almacenados en el servidor, y luego el sistema servidor 108 promueve que el usuario se registre en el segundo dispositivo. Los datos de historial asociados con el usuario en el segundo dispositivo utilizado para verificación de seguridad incluyen: registros de registro de historial y/o registros de historial de operación del usuario en el segundo dispositivo utilizando una cuenta determinada, que puede ser la misma cuenta de usuario o una cuenta de usuario diferente de la primera cuenta. En algunas realizaciones, se puede determinar que el segundo dispositivo está asociado con, o cerca, del primer dispositivo mediante las direcciones IP.

En algunas realizaciones como se muestra en la figura 5B, una o más cuentas del usuario utilizadas para determinar que el segundo dispositivo es calificado como seguro incluyen (510) la primera cuenta. En algunas realizaciones, el sistema servidor 108 que inicia (512) el proceso de verificación basado en el segundo dispositivo comprende además identificar (512) el segundo dispositivo basado en uno o más criterios de historial de uso predeterminados y los datos de historial de uso asociados con la primera cuenta; promover (512) que el usuario realice una interacción especificada que implique al primer dispositivo y al segundo dispositivo; y proporcionar (512) una respuesta de verificación al primer dispositivo de acuerdo con una verificación de la interacción entre el primer dispositivo y el segundo dispositivo. En algunas realizaciones, los datos del historial de uso incluyen datos con respecto al uso de la primera cuenta en el segundo dispositivo.

En algunas realizaciones en la figura 5C, la interacción especificada incluye (520) utilizar el primer dispositivo para escanear una imagen que contiene información codificada visualizada en el segundo dispositivo. En algunas realizaciones, la interacción especificada incluye (522) utilizar el segundo dispositivo para escanear una imagen que contiene información codificada visualizada en el primer dispositivo. En algunas realizaciones, la interacción especificada incluye (524) transmitir información a través de un medio de interacción de corto alcance. En algunas realizaciones, el sistema servidor 108 primero determina cuál del primer dispositivo y del segundo dispositivo tiene la capacidad de escaneo (por ejemplo, qué dispositivo

tiene una cámara que es capaz de escanear), y luego decide qué dispositivo debe recibir la imagen codificada, y qué dispositivo debe enviar el resultado escaneado.

En algunas realizaciones en la figura 5D, el sistema servidor 108 detecta (526) un dispositivo registrado (por ejemplo, dispositivo 104-2 de cliente, figura 4D) que está actualmente registrado a la primera cuenta (por ejemplo, cuenta 431 de usuario, figura 4D). El sistema servidor 108 determina (528) si la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura de acuerdo con los datos de historial de uso de la primera cuenta, y basado en uno o más criterios de historial de uso predeterminados. Los datos del historial de uso incluyen los datos del historial de uso asociados con el dispositivo registrado. De acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura, el sistema servidor 108 identifica (530) el dispositivo registrado como el segundo dispositivo para utilizar en el proceso de verificación.

En algunas realizaciones en la figura 5B, una o más cuentas del usuario utilizadas para determinar que el segundo dispositivo es calificado como seguro incluyen (514) la segunda cuenta vinculada a la primera cuenta. En algunas realizaciones, el sistema servidor 108 que inicia (508) el proceso de verificación basado en el segundo dispositivo comprende además identificar (516) el segundo dispositivo basado en uno o más criterios de historial de uso predeterminados y los datos de historial de uso asociados con la segunda cuenta; promover (516) que el usuario realice una interacción específica que implique el primer dispositivo y el segundo dispositivo; y proporcionar (516) una respuesta de verificación al primer dispositivo de acuerdo con una verificación de la interacción entre el primer dispositivo y el segundo dispositivo. En algunas realizaciones, los datos del historial de uso incluyen (516) datos con respecto al uso de la segunda cuenta en el segundo dispositivo.

En algunas realizaciones en la figura 5C, la interacción especificada incluye (520) utilizar el primer dispositivo para escanear una imagen que contiene información codificada mostrada en el segundo dispositivo. En algunas realizaciones, la interacción especificada incluye (522) utilizar el segundo dispositivo para escanear una imagen que contiene información codificada mostrada en el primer dispositivo. En algunas realizaciones, la interacción especificada incluye (524) transmitir información a través de un medio de interacción de corto alcance. En algunas realizaciones, el sistema servidor 108 primero determina cuál del primer dispositivo y el segundo dispositivo tiene la capacidad de escaneo (por ejemplo, qué dispositivo tiene una cámara que es capaz de escanear), y luego decide qué dispositivo debe recibir la imagen codificada, y qué dispositivo debe enviar el resultado escaneado.

En algunas realizaciones en la figura 5D, el sistema servidor 108 detecta (532) un dispositivo registrado que está actualmente registrado a una segunda cuenta asociada con el usuario que está vinculado a la primera cuenta. El sistema servidor 108 determina (534) si una operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura, de acuerdo con los datos del historial de uso de la segunda cuenta y basado en uno o más criterios de historial de uso predeterminados. En algunas realizaciones, los datos del historial de uso de la segunda cuenta incluyen (534) datos del historial de uso asociados con el dispositivo registrado. De acuerdo con una determinación de que la operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura, el sistema 109 servidor identifica (536) el dispositivo registrado como el segundo dispositivo para utiliza en el proceso de verificación. En algunas realizaciones, la primera cuenta y la segunda cuenta son (538) cuentas en dos plataformas distintas.

En algunas realizaciones, la primera cuenta y la segunda cuenta son cuentas para diferentes plataformas operativas, en vez de una cuenta duplicada del usuario en la misma plataforma. En algunos ejemplos, la primera cuenta es una cuenta de pago y la segunda cuenta es una cuenta de red social que está vinculada a la cuenta de pago, o viceversa. En algunas realizaciones, se determina que la primera cuenta y la segunda cuenta estén asociadas al mismo usuario por el servidor. Por ejemplo, la primera cuenta y la segunda cuenta han utilizado con frecuencia la misma dirección IP, en el mismo dispositivo(s), y/o la información registrada asociada a la primera cuenta y a la segunda cuenta comparten la misma información.

En algunas realizaciones en la figura 5E, el sistema servidor 108 envía (542) una imagen codificada al segundo dispositivo para su visualización en el segundo dispositivo. En algunas realizaciones, el sistema servidor 108 envía (544) una instrucción (por ejemplo, cuadro 404 de notificación) al primer dispositivo para requerir una interacción entre el primer dispositivo y el segundo dispositivo. En algunas realizaciones, el sistema servidor 108 recibe (546) un resultado escaneado del primer dispositivo después de que el primer dispositivo escanee la imagen codificada visualizada en el segundo dispositivo. En algunas realizaciones, el sistema servidor 108 verifica (548) si el resultado escaneado recibido desde el primer dispositivo coincide con la imagen codificada enviada al segundo dispositivo. En respuesta a una verificación de que el resultado escaneado recibido desde el primer dispositivo coincide con la imagen codificada enviada al segundo dispositivo, el sistema servidor 108 proporciona (550) una respuesta de verificación positiva al primer dispositivo para permitir que el usuario realice la operación de la cuenta en el primer dispositivo utilizando la primera cuenta.

En algunas realizaciones, la imagen codificada incluye un código QR 2-D, o un código de barras, o cualquier otra etiqueta óptica adecuada que se pueda escanear. En algunas realizaciones, la imagen codificada se visualiza a través de la interfaz de la aplicación de cliente correspondiente a la primera cuenta que está actualmente registrada en el segundo dispositivo. En algunas realizaciones, si el segundo dispositivo es calificado como seguro para una segunda cuenta vinculada a la primera cuenta, entonces la imagen codificada se visualiza a través de la interfaz de la aplicación de cliente correspondiente con la segunda cuenta que está actualmente registrada en el segundo dispositivo.

En algunas realizaciones, el segundo dispositivo es el mismo dispositivo que el primer dispositivo, y el primer dispositivo es calificado como seguro para una segunda cuenta vinculada a la primera cuenta, en dicho caso, la imagen codificada puede ser copiada desde la interfaz de la segunda cuenta, y pegada en la interfaz de la primera cuenta en el primer dispositivo. En algunas realizaciones, tal copiado y pegado puede no ser requerido, ya que el servidor puede determinar que el primer dispositivo se considera seguro para una segunda cuenta que está vinculada a la primera cuenta, y así proporcionar una respuesta de verificación positiva sin requerir que el usuario haga nada.

En algunas realizaciones, la verificación incluye verificar si la imagen codificada enviada al segundo dispositivo coincide con la imagen de la etiqueta escaneada recibida desde el primer dispositivo, y/o verificar si la información incluida en la etiqueta escaneada recibida desde el primer dispositivo coincide con la información incluida en la etiqueta enviada al segundo dispositivo. En algunos ejemplos, la información incluida en la etiqueta escaneada recibida desde el primer dispositivo puede responder o correlacionarse con la información incluida en la etiqueta enviada al segundo dispositivo.

En algunas realizaciones en la figura 5F, el sistema servidor 108 identifica (554) el segundo dispositivo que es calificado como seguro para la operación de cuenta de acuerdo con los datos de historial de uso asociados con una o más cuentas de usuario y los criterios de historial de uso predeterminados. En algunas realizaciones, el sistema servidor 108 determina (556) si el segundo dispositivo está actualmente registrado a una cuenta de una o más cuentas respectivas de usuario para las cuales el segundo dispositivo es calificado como seguro. De acuerdo con una determinación de que el segundo dispositivo no está actualmente registrado a la cuenta de una o más cuentas respectivas de usuario para las cuales el segundo dispositivo es calificado como seguro, el sistema servidor envía (558) una instrucción (por ejemplo, cuadro 470 de instrucciones de la figura 4G), al primer dispositivo, para requerir que el usuario se registre en una o más cuentas respectivas de usuario en el segundo dispositivo dentro de una ventana de tiempo predeterminada (por ejemplo, la instrucción 472 de la figura 4G). En algunas realizaciones, el sistema servidor 108 controla (560) si el usuario se ha registrado en una o más cuentas respectivas de usuario en el segundo dispositivo dentro de la ventana de tiempo predeterminada.

En algunas realizaciones, el sistema servidor 108 busca los datos del historial en la base de datos para identificar un segundo dispositivo seguro. La instrucción (por ejemplo, cuadro 470 de instrucciones de la figura 4G) enviada al primer dispositivo puede solicitar al usuario que inicie sesión en el segundo dispositivo utilizando la primera cuenta, o cualquier otra cuenta asociada con el usuario. En algunas realizaciones, la instrucción puede no identificar explícitamente el segundo dispositivo, pero en cambio proporcionar una descripción más críptica del segundo dispositivo, y el usuario debe confiar en su conocimiento del segundo dispositivo y de su uso pasado del segundo dispositivo para saber qué dispositivo debe usar y en qué cuenta debe registrarse.

Cada uno de los métodos descritos en la presente memoria se controlan normalmente por instrucciones que se almacenan en un medio de almacenamiento legible por ordenador y que se ejecutan por uno o más procesadores de uno o más servidores o dispositivos de cliente. Los módulos o programas identificados anteriormente (es decir, conjuntos de instrucciones) no necesitan implementarse como programas de software, procedimientos o módulos separados, y así varios subconjuntos de estos módulos se combinarán o reorganizarán de otro modo en diversas realizaciones.

REIVINDICACIONES

1. Un método para verificar una operación de cuenta, que comprende:

en un sistema servidor (108) que tiene uno o más procesadores y una memoria:
obtener (302) una solicitud de verificación desde un primer (104-1) dispositivo para una operación de cuenta solicitada por un usuario utilizando una primera cuenta, incluyendo la solicitud de verificación información asociada con la primera cuenta y una ID de dispositivo asociada con el primer dispositivo (104-1);
identificar (304, 404), desde el sistema servidor (108), datos de historial de uso asociados con la primera cuenta, que incluyen datos con respecto al uso de la primera cuenta en el primer dispositivo (104-1);
determinar (306, 406, 408), de acuerdo con los datos con respecto al uso de la primera cuenta en el primer dispositivo (104-1) y uno o más criterios de historial de uso predeterminados, si la operación de cuenta asociada con la primera cuenta en el primer dispositivo (104-1) es segura; y
de acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el primer dispositivo (104-1, 408) no es segura, iniciar (306, 410) un proceso de verificación basado en un segundo dispositivo (104-2) calificado como seguro para la operación de cuenta basado en los datos del historial de uso asociados con una o más cuentas del usuario y uno o más criterios de historial de uso predeterminados,
caracterizado por que
una o más cuentas incluyen una segunda cuenta vinculada a la primera cuenta, y en donde iniciar el proceso de verificación basado en el segundo dispositivo (104-2) comprende además:

identificar el segundo dispositivo (104-2) basado en uno o más criterios de historial de uso predeterminados y datos de historial de uso asociados con la segunda cuenta, en donde los datos del historial de uso incluyen datos con respecto al uso de la segunda cuenta en el segundo dispositivo (104-2);
promover (412) que el usuario realice una interacción específica que implique al primer dispositivo (104-1) y al segundo dispositivo (104-2); y
proporcionar (420) una respuesta de verificación al primer dispositivo (104-1) de acuerdo con una verificación de la interacción entre el primer dispositivo (104-1) y el segundo dispositivo (104-2),

o el paso de identificar el segundo dispositivo comprende:

detectar un dispositivo registrado que actualmente está registrado en la primera cuenta; determinando, de acuerdo con los datos del historial de uso de la primera cuenta, incluidos los datos del historial de uso asociados con el dispositivo registrado, y basado en uno o más criterios de historial de uso predeterminados, si la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura; y
de acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura, identificar el dispositivo registrado como el segundo dispositivo (104-2) para usar en el proceso de verificación,

o el paso de identificar el segundo dispositivo comprende:

detectar un dispositivo registrado que actualmente está registrado a una segunda cuenta asociada con el usuario que está vinculada a la primera cuenta;
determinar, de acuerdo con los datos del historial de uso de la segunda cuenta, que incluyen los datos del historial de uso asociados con el dispositivo registrado, y basado en uno o más criterios de historial de uso predeterminados, si una operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura; y
de acuerdo con una determinación de que la operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura, identificar el dispositivo registrado como el segundo dispositivo (104-2) para utilizar en el proceso de verificación.

2. El método de la reivindicación 1, en donde una o más cuentas incluyen la primera cuenta, y en donde iniciar el proceso de verificación basado en el segundo dispositivo (104-2) comprende además:

identificar el segundo dispositivo (104-2) basado en uno o más criterios de historial de uso predeterminados y los datos del historial de uso asociados con la primera cuenta, en donde los datos del historial de uso incluyen datos con respecto al uso de la primera cuenta en el segundo dispositivo (104- 2);
promover (412) que el usuario realice una interacción específica que implique al primer dispositivo (104-1) y al segundo dispositivo (104-2); y

proporcionar (420) una respuesta de verificación al primer dispositivo (104-1) de acuerdo con una verificación de la interacción entre el primer dispositivo (104-1) y el segundo dispositivo (104-2).

3. El método de la reivindicación 1 o 2, en donde la interacción especificada incluye utilizar el primer dispositivo (104-1) para escanear una imagen que contiene información codificada mostrada en el segundo dispositivo (104-2).

4. El método de la reivindicación 1 o 2, en donde la interacción especificada incluye utilizar el segundo dispositivo (104-2) para escanear una imagen que contiene información codificada mostrada en el primer dispositivo (104-1).

5. El método de la reivindicación 1 o 2, en donde la interacción especificada incluye transmitir información a través de un medio de interacción de corto alcance.

6. El método de cualquiera de las reivindicaciones 1 a 5, en donde iniciar el proceso de verificación basado en el segundo dispositivo (104-2) comprende además:

enviar (410) una imagen codificada al segundo dispositivo (104-2) para visualizar en el segundo dispositivo (104-2);
enviar (412) una instrucción al primer dispositivo (104-1) para requerir una interacción entre el primer dispositivo (104-1) y el segundo dispositivo (104-2);
recibir (416) un resultado escaneado desde el primer dispositivo (104-1) después de que el primer dispositivo (104-1) escanee la imagen codificada que se visualiza en el segundo dispositivo (104-2),
verificar (418) si el resultado escaneado recibido desde el primer dispositivo (104-1) coincide con la imagen codificada enviada al segundo dispositivo (104-2); y
en respuesta a una verificación de que el resultado escaneado recibido del primer dispositivo (104-1) coincide con la imagen codificada enviada al segundo dispositivo (104-2), proporcionar (420) una respuesta de verificación positiva al primer dispositivo (104-1) para permitir al usuario realizar la operación de la cuenta en el primer dispositivo (104-1) utilizando la primera cuenta.

7. El método de la reivindicación 1, en donde la primera cuenta y la segunda cuenta son cuentas en dos plataformas distintas.

8. El método de cualquiera de las reivindicaciones 1 a 7, en donde iniciar el proceso de verificación comprende además:

identificar, de acuerdo con los datos del historial de uso asociados con una o más cuentas de usuario y los criterios del historial de uso predeterminado, el segundo dispositivo (104-2) es calificado como seguro para la operación de la cuenta;
determinar si el segundo dispositivo (104-2) está actualmente registrado a una cuenta respectiva de una o más cuentas del usuario para las cuales el segundo dispositivo (104-2) es calificado como seguro;
de acuerdo con una determinación de que el segundo dispositivo (104-2) no está actualmente registrado a la cuenta respectiva de uno o más cuentas de usuario para las cuales el segundo dispositivo (104-2) es calificado como seguro, enviar una instrucción, al primer dispositivo (104-1), para requerir que el usuario se registre en una o más cuentas respectivas de usuario en el segundo dispositivo (104-2) dentro de una ventana de tiempo predeterminada; y
vigilar si el usuario se ha registrado en una o más cuentas respectivas de usuario en el segundo dispositivo (104-2) dentro de la ventana de tiempo predeterminada.

9. Un sistema servidor (108), que comprende:

uno o más procesadores (112); y memoria (206) que almacena uno o más programas para ser ejecutados por uno o más procesadores, uno o más programas que comprenden instrucciones para:

obtener una solicitud de verificación desde un primer dispositivo (104-1) para una operación de cuenta solicitada por un usuario utilizando una primera cuenta, incuyendo la solicitud de verificación información asociada con la primera cuenta y una ID de dispositivo asociada con el primer dispositivo (104-1);
identificar, desde el sistema servidor (108), los datos del historial de uso asociados con la primera cuenta, que incluyen datos con respecto al uso de la primera cuenta en el primer dispositivo (104-1);
determinando, de acuerdo con los datos con respecto al uso de la primera cuenta en el primer dispositivo (104-1) y uno o más criterios de historial de uso predeterminados, si la operación de la cuenta asociada con la primera cuenta en el primer dispositivo (104-1) es segura; y
de acuerdo con una determinación de que la operación de la cuenta asociada con la primera cuenta en el primer dispositivo (104-1) no es segura, iniciar un proceso de verificación basado en un segundo

dispositivo (104-2) calificado como seguro para la operación de la cuenta basado en los datos del historial de uso asociados con una o más cuentas del usuario y uno o más criterios de historial de uso predeterminados,

caracterizado por que

una o más cuentas incluyen una segunda cuenta vinculada a la primera cuenta, y en donde iniciar del proceso de verificación basado en el segundo dispositivo (104-2) comprende además:

identificar el segundo dispositivo (104-2) basado en uno o más criterios de historial de uso predeterminados y datos de historial de uso asociados con la segunda cuenta, en donde los datos del historial de uso incluyen datos con respecto al uso de la segunda cuenta en el segundo dispositivo (104-2);
promover que el usuario realice una interacción especificada que implique al primer dispositivo (104-1) y al segundo dispositivo (104-2); y proporcionar una respuesta de verificación al primer dispositivo (104-1) de acuerdo con una verificación de la interacción entre el primer dispositivo (104-1) y el segundo dispositivo (104-2),

o el paso de identificar el segundo dispositivo comprende :

detectar un dispositivo registrado que actualmente está registrado a la primera cuenta;
determinar, de acuerdo con los datos del historial de uso de la primera cuenta, incluidos los datos de historial de uso asociados con el dispositivo registrado, y basado en uno o más criterios de historial de uso predeterminados, si la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura; y
de acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura, identificar el dispositivo registrado como el segundo dispositivo (104-2) para utilizar en el proceso de verificación,

o el paso de identificar el segundo dispositivo comprende:

detectar un dispositivo registrado que actualmente está registrado a una segunda cuenta asociada con el usuario que está vinculada a la primera cuenta;
determinar, de acuerdo con los datos del historial de uso de la segunda cuenta, incluidos los datos del historial de uso asociados con el dispositivo registrado, y basado en uno o más criterios de historial de uso predeterminados, si una operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura; y
de acuerdo con una determinación de que la operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura, identificar el dispositivo registrado como el segundo dispositivo (104-2) para utilizar en el proceso de verificación.

10. El sistema de servidor de la reivindicación 9, en el que una o más cuentas incluyen la primera cuenta, y en donde iniciar el proceso de verificación basado en el segundo dispositivo (104 - 2) comprende además:

identificar el segundo dispositivo (104-2) basado en uno o más criterios de historial de uso predeterminados y los datos del historial de uso asociados con la primera cuenta, en donde los datos del historial de uso incluyen datos con relación al uso de la primera cuenta en el segundo dispositivo (104- 2);
promover que el usuario realice una interacción especificada que implique al primer dispositivo (104-1) y al segundo dispositivo (104-2); y
proporcionar una respuesta de verificación al primer dispositivo (104-1) de acuerdo con una verificación de la interacción entre el primer dispositivo y el segundo dispositivo (104-2).

11. El sistema servidor de cualquiera de las reivindicaciones 9 a 10, en donde iniciar el proceso de verificación comprende además:

identificar, de acuerdo con los datos del historial de uso asociados con una o más cuentas de usuario y los criterios del historial de uso predeterminado, el segundo dispositivo (104-2) calificado como seguro para la operación de cuenta;
determinar si el segundo dispositivo está actualmente registrado en una o más cuentas respectivas de usuario para las cuales el segundo dispositivo (104-2) es calificado como seguro ;
de acuerdo con una determinación de que el segundo dispositivo (104-2) no está actualmente registrado en una o más cuentas respectivas de usuario para las cuales el segundo dispositivo (104-2) es calificado como seguro, enviar una instrucción, al primer dispositivo (104-1), para requerir que el usuario se registre en una o más cuentas respectivas de usuario en el segundo dispositivo (104-2) dentro de una ventana de tiempo predeterminada;

y vigilar si el usuario se ha registrado en una o más cuentas respectivas de usuario en el segundo dispositivo (104-2) dentro de la ventana de tiempo predeterminada.

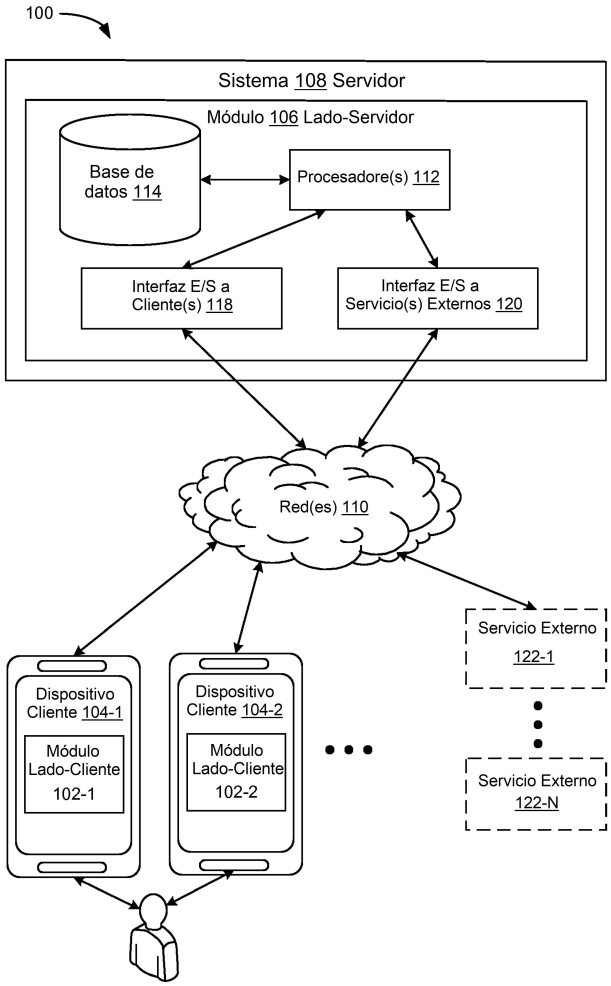
100
Sistema 108 Servidor
Módulo 106 Lado-Servidor
Base de datos 114
Procesadore(s) 112
Interfaz E/S a Cliente(s) 118
Interfaz E/S a Servicio(s) Externos 120
Red(es) 110
Dispositivo Cliente 104-1
Módulo Lado-Cliente 102-1
Dispositivo Cliente 104-2
Módulo Lado-Cliente 102-2
Servicio Externo 122-1
Servicio Externo 122-N

FIG. 1

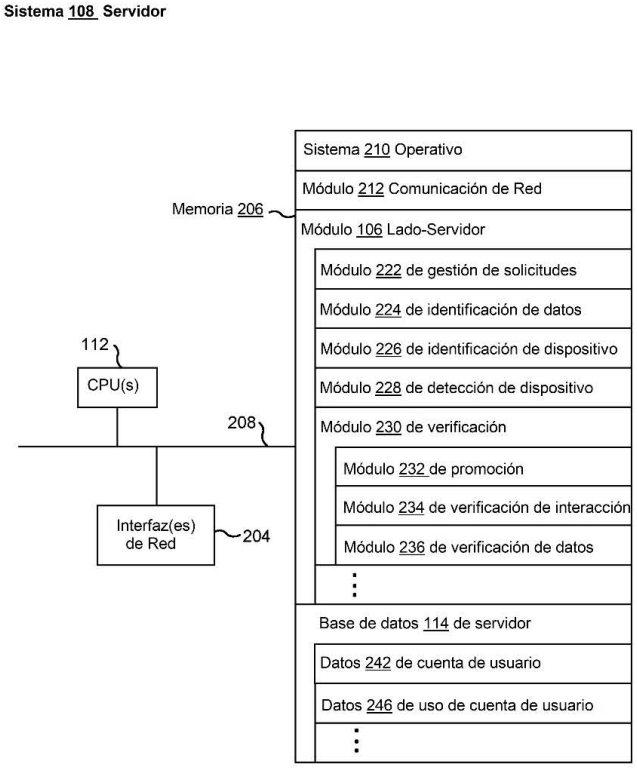
Sistema 108 Servidor
Sistema 210 Operativo
Módulo 212 Comunicación de Red
Memoria 206
Módulo 106 Lado-Servidor
Módulo 222 de gestión de solicitudes
Módulo 224 de identificación de datos
Módulo 226 de identificación de dispositivo
Módulo 228 de detección de dispositivo
112
CPU(s)
208
Módulo 230 de verificación
Módulo 232 de promoción
Módulo 234 de verificación de interacción
Módulo 236 de verificación de datos
Interfaz(es) de Red
204
Base de datos 114 de servidor
Datos 242 de cuenta de usuario
Datos 246 de uso de cuenta de usuario

FIG. 2A

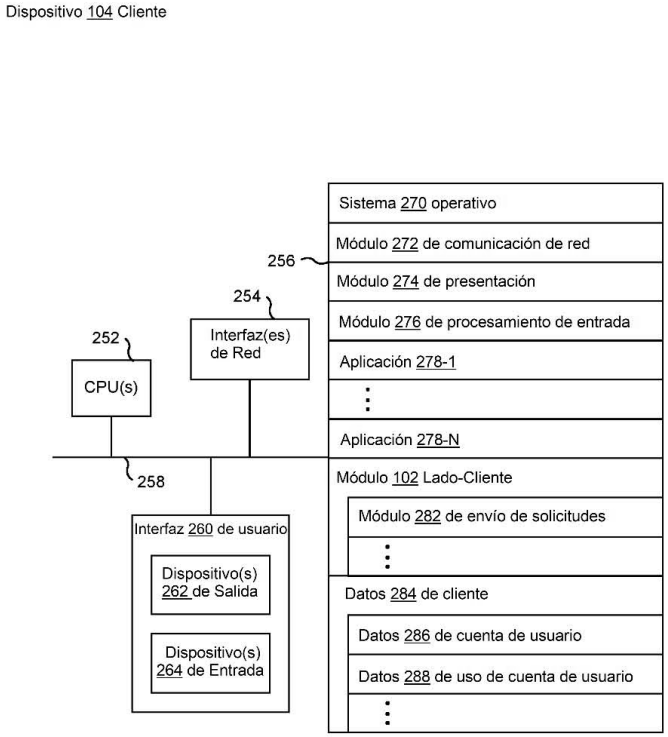
Dispositivo 104 Cliente
Sistema 270 operativo
Módulo 272 de comunicación de red
256
Módulo 274 de presentación
254
Módulo 276 de procesamiento de entrada
Interfaz(es) de Red
252
Aplicación 278-1
CPU(s)
Aplicación 278-N
258
Módulo 102 Lado-Cliente
Módulo 282 de envío de solicitudes
Interfaz 260 de usuario
Dispositivo(s) 262 de Salida
Datos 284 de cliente
Dispositivo(s) 264 de Entrada
Datos 286 de cuenta de usuario
Datos 288 de uso de cuenta de usuario

FIG. 2B

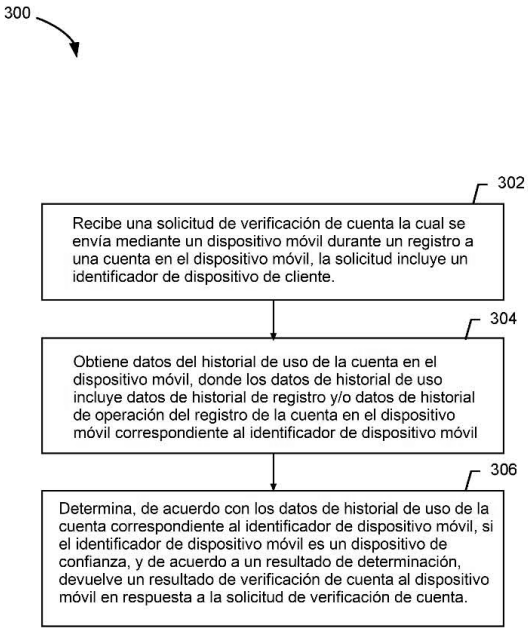
300
302
Recibe una solicitud de verificación de cuenta la cual se envía mediante un dispositivo móvil durante un registro a una cuenta en el dispositivo móvil, la solicitud incluye un identificador de dispositivo de cliente.
304
Obtiene datos del historial de uso de la cuenta en el dispositivo móvil, donde los datos de historial de uso incluye datos de historial de registro y/o datos de historial de operación del registro de la cuenta en el dispositivo móvil correspondiente al identificador de dispositivo móvil
306
Determina, de acuerdo con los datos de historial de uso de la cuenta correspondiente al identificador de dispositivo móvil, si el identificador de dispositivo móvil es un dispositivo de confianza, y de acuerdo a un resultado de determinación, devuelve un resultado de verificación de cuenta al dispositivo móvil en respuesta a la solicitud de verificación de cuenta.

FIG. 3A

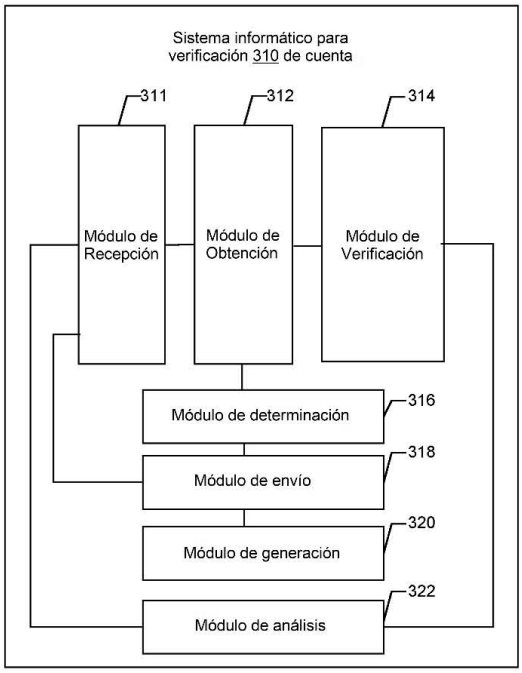
Sistema informático para verificación 310 de cuenta
311
312
314
Módulo de Recepción
Módulo de Obtención
Módulo de Verificación
Módulo de determinación
316
Módulo de envío
318
Módulo de generación
320
Módulo de análisis
322

FIG. 3B

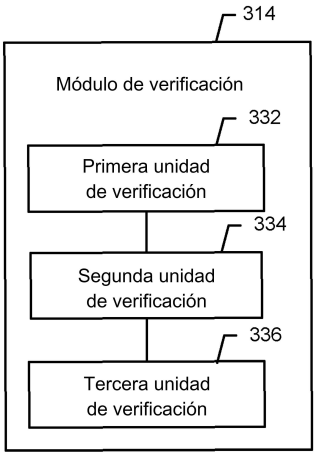
314
Módulo de verificación
332
Primera unidad de verificación
334
Segunda unidad de verificación
336
Tercera unidad de verificación

FIG. 3C

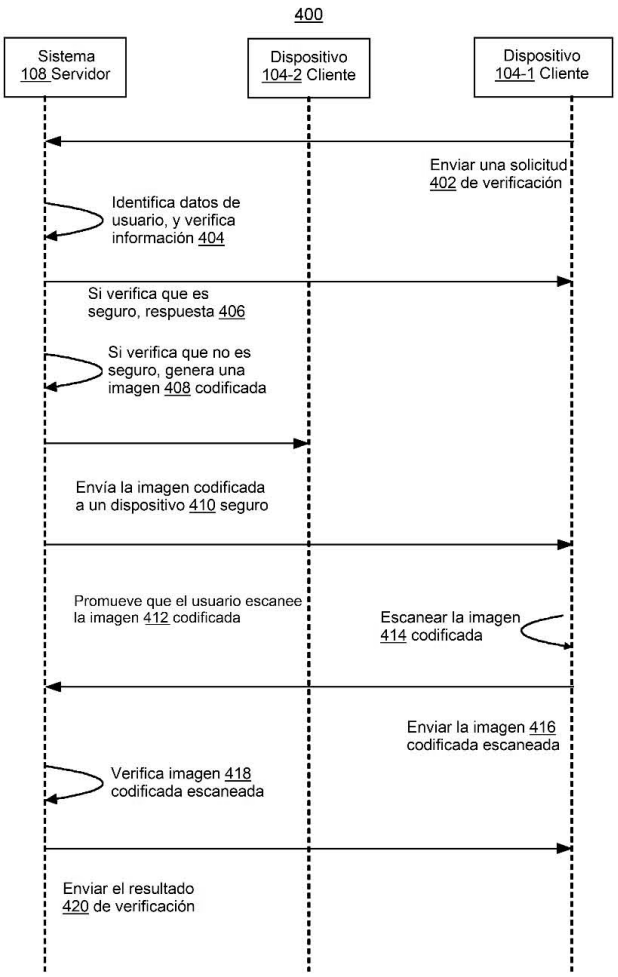
400
Sistema 108 Servidor
Dispositivo 104-2 Cliente
Dispositivo 104-1 Cliente
Enviar una solicitud 402 de verificación
Identifica datos de usuario, y verifica información 404
Si verifica que es seguro, respuesta 406
Si verifica que no es seguro, genera una imagen 408 codificada
Envía la imagen codificada a un dispositivo 410 seguro
Promueve que el usuario escanee la imagen 412 codificada
Escanear la imagen 414 codificada
Enviar la imagen 416 codificada escaneada
Verifica imagen 418 codificada escaneada
Enviar el resultado 420 de verificación

FIG. 4A

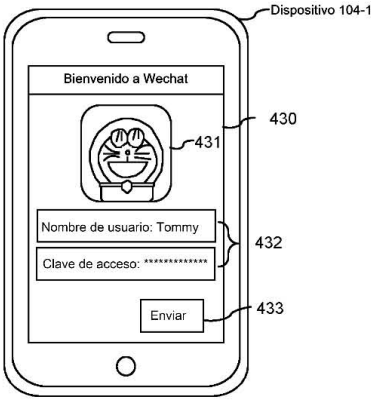
Dispositivo 104-1
Bienvenido a Wechat
430
431
Nombre de usuario: Tommy
Clave de acceso: **********
432
Enviar
433

FIG. 4B

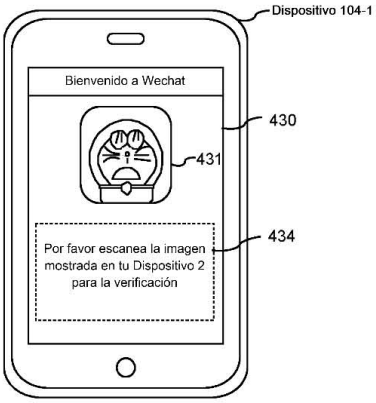
Dispositivo 104-1
Bienvenido a Wechat
430
431
Por favor escanea la imagen mostrada en tu Dispositivo 2 para la verificación
434

FIG. 4C

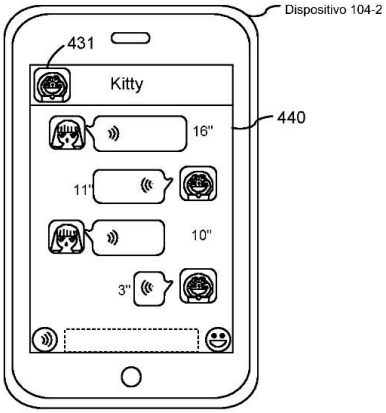
Dispositivo 104-2
431
Kitty
440
16"
11"
10"
3"

FIG. 4D

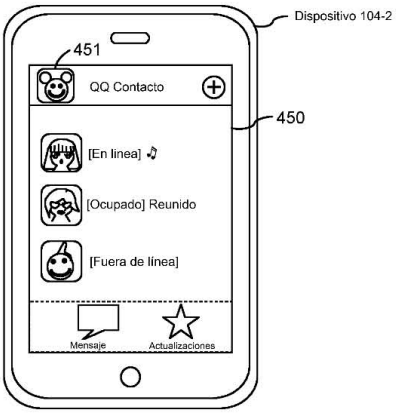
Dispositivo 104-2
451
QQ Contacto
450
[En línea]
[Ocupado] Reunido
[Fuera de línea]
Mensaje
Actualizaciones

FIG. 4E

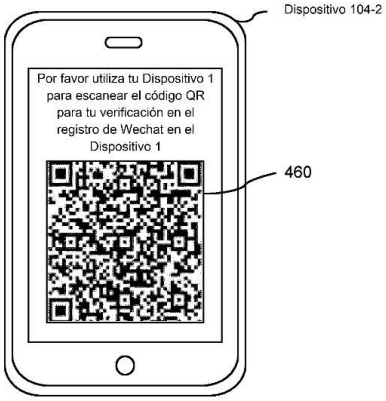
Dispositivo 104-2
Por favor utiliza tu Dispositivo 1 para escanear el código QR para tu verificación en el registro de Wechat en el Dispositivo 1
460

FIG. 4F

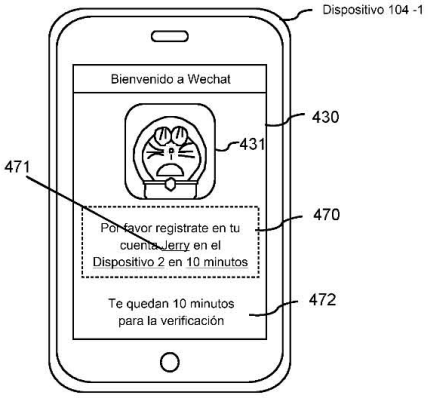
Dispositivo 104 -1
Bienvenido a Wechat
430
431
471
470
Por favor registrate en tu cuenta Jerry en el Dispositivo 2 en 10 minutos
Te quedan 10 minutos para la verificación
472

FIG. 4G

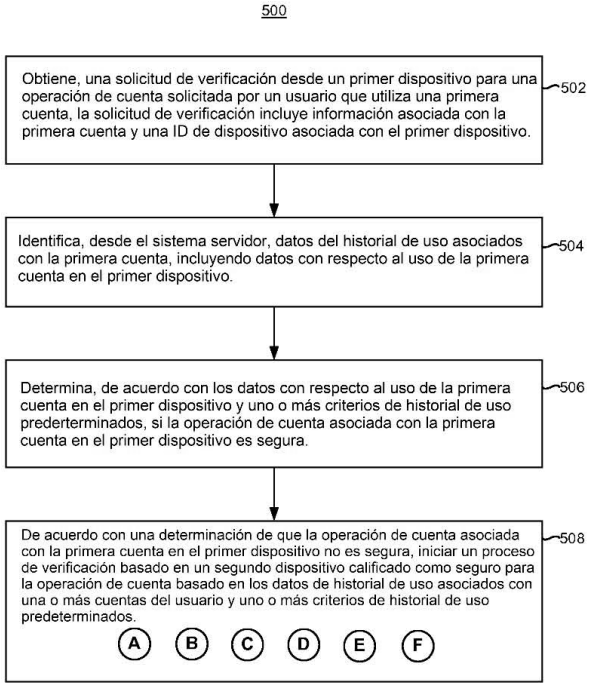
500
Obtiene, una solicitud de verificación desde un primer dispositivo para una operación de cuenta solicitada por un usuario que utiliza una primera cuenta, la solicitud de verificación incluye información asociada con la primera cuenta y una ID de dispositivo asociada con el primer dispositivo.
502
Identifica, desde el sistema servidor, datos del historial de uso asociados con la primera cuenta, incluyendo datos con respecto al uso de la primera cuenta en el primer dispositivo.
504
Determina, de acuerdo con los datos con respecto al uso de la primera cuenta en el primer dispositivo y uno o más criterios de historial de uso predeterminados, si la operación de cuenta asociada con la primera cuenta en el primer dispositivo es segura.
506
De acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el primer dispositivo no es segura, iniciar un proceso de verificación basado en un segundo dispositivo calificado como seguro para la operación de cuenta basado en los datos de historial de uso asociados con una o más cuentas del usuario y uno o más criterios de historial de uso predeterminados.
508
A
B
C
D
E
F

FIG. 5A

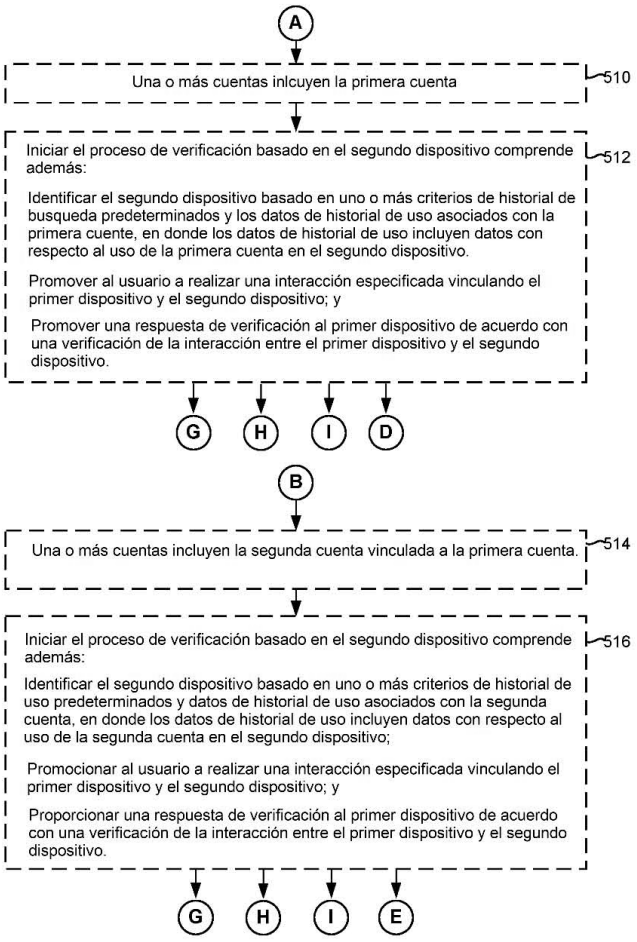
A
Una o más cuentas inlcuyen la primera cuenta
510
Iniciar el proceso de verificación basado en el segundo dispositivo comprende además:
512
Identificar el segundo dispositivo basado en uno o más criterios de historial de busqueda predeterminados y los datos de historial de uso asociados con la primera cuente, en donde los datos de historial de uso incluyen datos con respecto al uso de la primera cuenta en el segundo dispositivo.
Promover al usuario a realizar una interacción especificada vinculando el primer dispositivo y el segundo dispositivo; y
Promover una respuesta de verificación al primer dispositivo de acuerdo con una verificación de la interacción entre el primer dispositivo y el segundo dispositivo.
G
H
I
D
B
Una o más cuentas incluyen la segunda cuenta vinculada a la primera cuenta.
514
Iniciar el proceso de verificación basado en el segundo dispositivo comprende además:
516
Identificar el segundo dispositivo basado en uno o más criterios de historial de uso predeterminados y datos de historial de uso asociados con la segunda cuenta, en donde los datos de historial de uso incluyen datos con respecto al uso de la segunda cuenta en el segundo dispositivo;
Promocionar al usuario a realizar una interacción especificada vinculando el primer dispositivo y el segundo dispositivo; y
Proporcionar una respuesta de verificación al primer dispositivo de acuerdo con una verificación de la interacción entre el primer dispositivo y el segundo dispositivo.
G
H
I
E

FIG. 5B

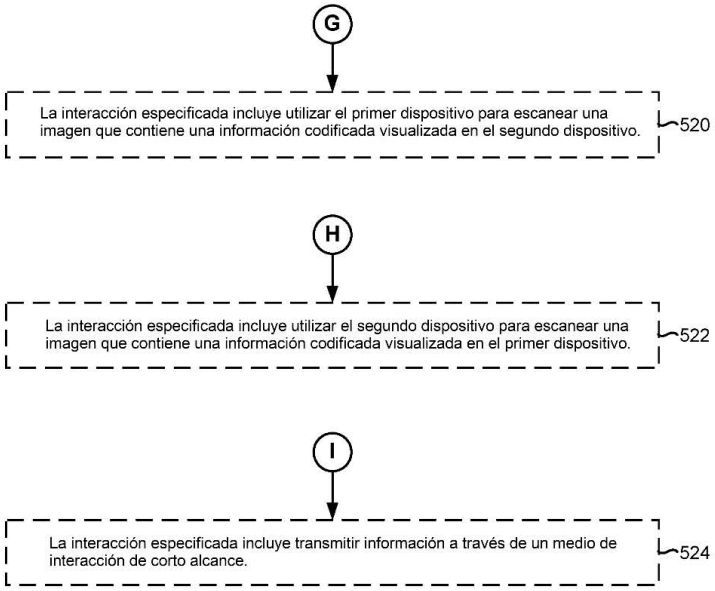
G
La interacción especificada incluye utilizar el primer dispositivo para escanear una imagen que contiene una información codificada visualizada en el segundo dispositivo.
520
H
La interacción especificada incluye utilizar el segundo dispositivo para escanear una imagen que contiene una información codificada visualizada en el primer dispositivo.
522
I
La interacción especificada incluye transmitir información a través de un medio de interacción de corto alcance.
524

FIG. 5C

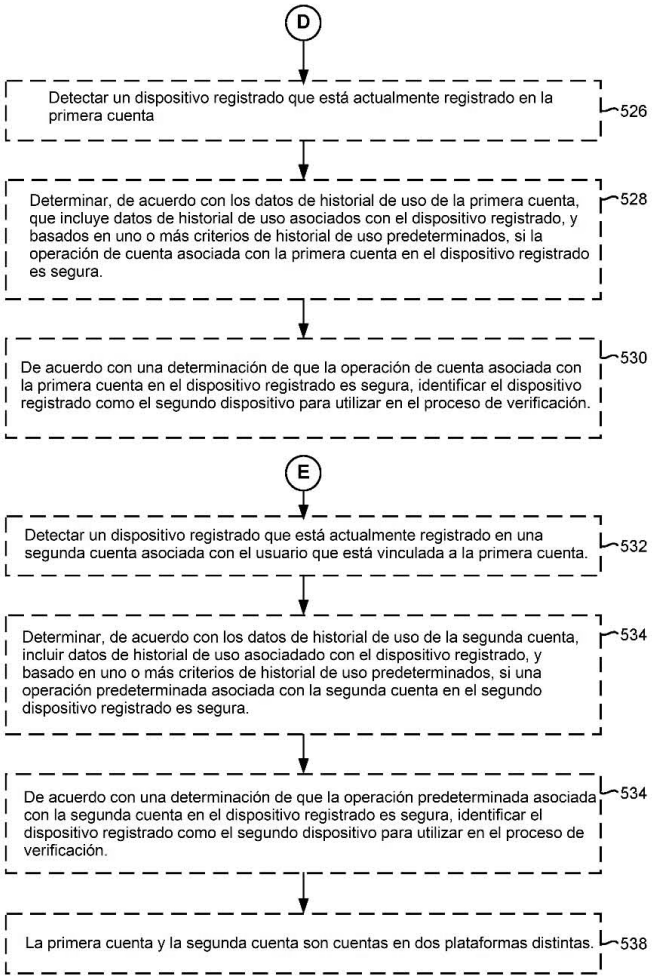
D
Detectar un dispositivo registrado que está actualmente registrado en la primera cuenta
526
Determinar, de acuerdo con los datos de historial de uso de la primera cuenta, que incluye datos de historial de uso asociados con el dispositivo registrado, y basados en uno o más criterios de historial de uso predeterminados, si la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura.
528
De acuerdo con una determinación de que la operación de cuenta asociada con la primera cuenta en el dispositivo registrado es segura, identificar el dispositivo registrado como el segundo dispositivo para utilizar en el proceso de verificación.
530
E
Detectar un dispositivo registrado que está actualmente registrado en una segunda cuenta asociada con el usuario que está vinculada a la primera cuenta.
532
Determinar, de acuerdo con los datos de historial de uso de la segunda cuenta, incluir datos de historial de uso asociadado con el dispositivo registrado, y basado en uno o más criterios de historial de uso predeterminados, si una operación predeterminada asociada con la segunda cuenta en el segundo dispositivo registrado es segura.
534
De acuerdo con una determinación de que la operación predeterminada asociada con la segunda cuenta en el dispositivo registrado es segura, identificar el dispositivo registrado como el segundo dispositivo para utilizar en el proceso de verificación.
534
La primera cuenta y la segunda cuenta son cuentas en dos plataformas distintas.
538

FIG. 5D

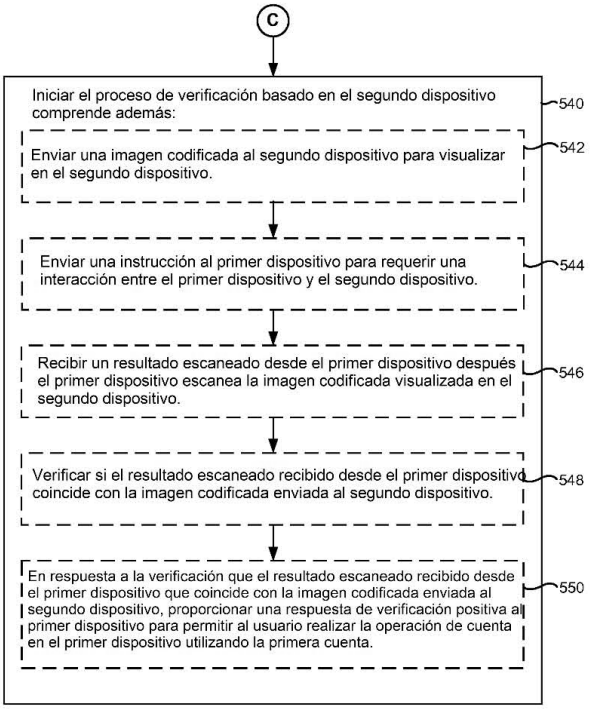
C
Iniciar el proceso de verificación basado en el segundo dispositivo comprende además:
540
Enviar una imagen codificada al segundo dispositivo para visualizar en el segundo dispositivo.
542
Enviar una instrucción al primer dispositivo para requerir una interacción entre el primer dispositivo y el segundo dispositivo.
544
Recibir un resultado escaneado desde el primer dispositivo después el primer dispositivo escanea la imagen codificada visualizada en el segundo dispositivo.
546
Verificar si el resultado escaneado recibido desde el primer dispositivo coincide con la imagen codificada enviada al segundo dispositivo.
548
En respuesta a la verificación que el resultado escaneado recibido desde el primer dispositivo que coincide con la imagen codificada enviada al segundo dispositivo, proporcionar una respuesta de verificación positiva al primer dispositivo para permitir al usuario realizar la operación de cuenta en el primer dispositivo utilizando la primera cuenta.
550

FIG. 5E

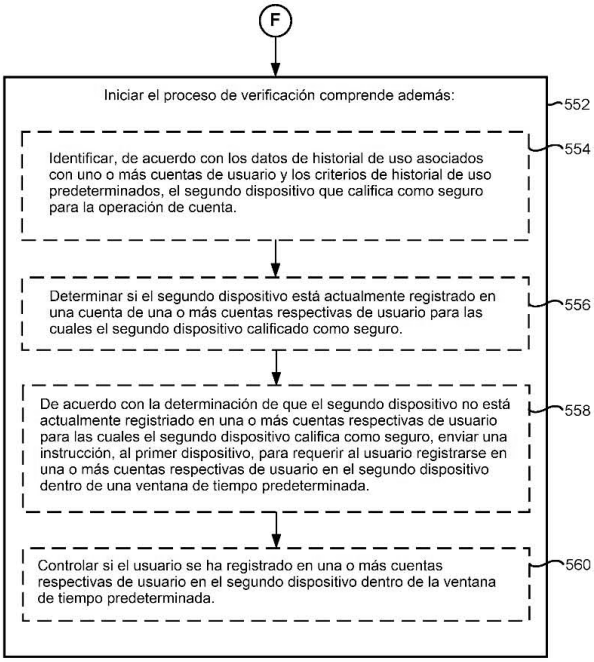
F
Iniciar el proceso de verificación comprende además:
552
Identificar, de acuerdo con los datos de historial de uso asociados con uno o más cuentas de usuario y los criterios de historial de uso predeterminados, el segundo dispositivo que califica como seguro para la operación de cuenta.
554
Determinar si el segundo dispositivo está actualmente registrado en una cuenta de una o más cuentas respectivas de usuario para las cuales el segundo dispositivo calificado como seguro.
556
De acuerdo con la determinación de que el segundo dispositivo no está actualmente registriado en una o más cuentas respectivas de usuario para las cuales el segundo dispositivo califica como seguro, enviar una instrucción, al primer dispositivo, para requerir al usuario registrarse en una o más cuentas respectivas de usuario en el segundo dispositivo dentro de una ventana de tiempo predeterminada.
558
Controlar si el usuario se ha registrado en una o más cuentas respectivas de usuario en el segundo dispositivo dentro de la ventana de tiempo predeterminada.
560

FIG. 5F