(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 808 974**

(51) Int. CI.:

***H04W 12/12*** (2009.01)
***H04L 29/06*** (2006.01)
***G06F 21/57*** (2013.01)
***H04W 12/06*** (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.04.2016 PCT/CN2016/080446**

(87) Fecha y número de publicación internacional: **08.12.2016 WO16192495**

(96) Fecha de presentación y número de la solicitud europea: **28.04.2016 E 16802418 (0)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 3306512**

(54) Título: **Procedimiento de identificación de riesgo de robo de cuenta, aparato de identificación y sistema de prevención y control**

(30) Prioridad:

**29.05.2015 CN 201510289825**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**02.03.2021**

(73) Titular/es:

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

(72) Inventor/es:

**TAN, CHUNPING**

(74) Agente/Representante:

**LEHMANN NOVO, María Isabel**

## DESCRIPCIÓN

Procedimiento de identificación de riesgo de robo de cuenta, aparato de identificación y sistema de prevención y control

**Campo técnico**

La presente solicitud se refiere a tecnologías de seguridad en redes y, en particular, a un procedimiento de identificación de riesgo de robo de cuenta, un aparato de identificación y un sistema de prevención y control.

**Antecedentes de la técnica**

Las transacciones en línea, el pago mediante móviles y otras aplicaciones, pese a ofrecer comodidad a los usuarios tienen graves riesgos relacionados con la seguridad. Si se roba una cuenta, un usuario no solo puede sufrir una pérdida de propiedad, sino que también puede tener que asumir el riesgo de conductas ilegales llevadas a cabo por un ladrón de cuentas que usa la cuenta robada. La manera de identificar de manera rápida y eficaz el robo de una cuenta para proporcionar a los usuarios un entorno de red lo más seguro posible es un problema importante que un proveedor de servicio de aplicaciones de red no puede evitar y tiene que resolver. En la técnica anterior se han propuesto muchas soluciones de identificación de riesgo de robo de cuentas, las cuales se describen brevemente a continuación mediante ejemplos.

Un tipo de solución es identificar el riesgo de robo de una cuenta determinando si una solicitud de transacción de un usuario que realiza una transacción es anómala. Por ejemplo, se detecta si un usuario inicia sesión en la cuenta en una ubicación remota y si se produce un inicio de sesión remoto es necesario verificar el usuario; si la verificación no es satisfactoria, se bloqueará la cuenta del usuario. El inicio de sesión remoto es una manifestación habitual del robo de una cuenta. Por lo tanto, supervisar solicitudes de inicio de sesión remotas ayuda a identificar a tiempo el riesgo del robo de una cuenta. Sin embargo, puesto que un operador de red puede cambiar su propio grupo de direcciones IP, especialmente durante la asignación de direcciones IP entre ciudades, un usuario habitual puede ser identificado como un usuario sospechoso, lo que puede dar como resultado una tasa de error relativamente alta en la identificación del robo de cuentas.

Otro tipo de solución es identificar el riesgo de robo de una cuenta supervisando un dispositivo clave. Por ejemplo, se cuenta el número de usuarios de transacciones que inician sesión en un dispositivo de inicio de sesión de transacciones y se usa como variable de entrada de un modelo de calificación para identificar el riesgo de robo de una cuenta, evaluando de este modo el nivel de riesgo de robo de cuentas de este dispositivo. Si hay relativamente pocos usuarios de transacciones en un dispositivo, la probabilidad del riesgo de robo de una cuenta es relativamente bajo; de lo contrario, si hay muchos usuarios de transacciones en el dispositivo, la probabilidad del riesgo de robo de cuenta aumenta significativamente. Por lo tanto, los eventos de robo de cuentas pueden identificarse hasta cierto punto, principalmente con la supervisión de este tipo de dispositivos que tienen un número elevado de usuarios de transacciones. Sin embargo, la capacidad diferenciadora y la estabilidad de la variable, es decir, el número de usuarios de transacciones en el dispositivo, son relativamente malas, y en una situación habitual de una transacción realizada por múltiples usuarios en un único dispositivo, esta solución tiende a generar un error de identificación.

Las soluciones de identificación de riesgo de robo de cuentas en otros comportamientos de operación en red tienen habitualmente problemas de juicios erróneos, así como falsos negativos, y su capacidad diferenciadora del riesgo de robo de cuentas no es demasiado alta, lo que da como resultado un efecto global no satisfactorio de estas soluciones. Por lo tanto, es necesario diseñar una nueva solución de identificación de riesgo de robo de cuentas.

El documento US 8.904.496 describe un procedimiento y sistema para su uso en la autenticación de una entidad en relación con un recurso informático. Una solicitud de autenticación se recibe desde una entidad para acceder al recurso informático. Una señal de entrada se recibe desde un dispositivo de comunicaciones asociado a la entidad. La señal de entrada comprende la ubicación actual del dispositivo de comunicaciones. La ubicación actual del dispositivo de comunicaciones se obtiene a partir de la señal de entrada. Se adquiere un historial de ubicaciones en relación con el dispositivo de comunicaciones. El historial de ubicaciones comprende un registro de ubicaciones discretas visitadas por el dispositivo de comunicaciones durante un periodo de tiempo. Se realiza un análisis entre la ubicación actual del dispositivo de comunicaciones y el historial de ubicaciones en relación con el dispositivo de comunicaciones. Se genera un resultado de autenticación en función del análisis entre la ubicación actual del dispositivo de comunicaciones y el historial de ubicaciones en relación con el dispositivo de comunicaciones. El resultado de la autenticación puede usarse para autenticar la entidad.

**Sumario de la invención**

En vista de los defectos de la técnica anterior, un objetivo de la presente solicitud es proporcionar un procedimiento de identificación de riesgo de robo de cuenta, un aparato de identificación y un sistema de prevención y control, para mejorar de manera eficaz la capacidad de distinguir un riesgo de robo de cuenta.

Para resolver el problema técnico anterior, la presente solicitud proporciona un procedimiento de identificación de riesgo de robo de cuenta, que incluye:
recopilar información de dispositivo de un dispositivo que tiene un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual;
adquirir toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo dentro de un periodo de tiempo preestablecido anterior al comportamiento de operación actual;
analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo; y
determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo.

Preferentemente, la información de identidad de usuario incluye información de credencial en información de registro de usuario; y la etapa de analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo incluye específicamente: adquirir la ubicación de análisis de identidad de usuario de este tipo de dispositivos que tienen un número elevado de usuarios de transacciones. Sin embargo, la capacidad diferenciadora y la estabilidad de la variable, es decir, el número de usuarios de transacciones en el dispositivo, son relativamente malas, y en una situación habitual de una transacción realizada por múltiples usuarios en un único dispositivo, esta solución tiende a generar un error de identificación.

Las soluciones de identificación de riesgo de robo de cuentas en otros comportamientos de operación en red tienen habitualmente problemas de juicios erróneos, así como falsos negativos, y su capacidad diferenciadora de riesgo de robo de cuentas no es demasiado alta, lo que da como resultado un efecto global no satisfactorio de estas soluciones. Por lo tanto, es necesario diseñar una nueva solución de identificación de riesgo de robo de cuentas.

**Sumario de la invención**

En vista de los defectos de la técnica anterior, un objetivo de la presente solicitud es proporcionar un procedimiento de identificación de riesgo de robo de cuenta, un aparato de identificación y un sistema de prevención y control, para mejorar de manera eficaz la capacidad de distinguir un riesgo de robo de cuenta.

Para resolver el problema técnico anterior, la presente solicitud proporciona un procedimiento de identificación de riesgo de robo de cuenta, que incluye:
recopilar información de dispositivo de un dispositivo que tiene un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual;
adquirir toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo dentro de un periodo de tiempo preestablecido anterior al comportamiento de operación actual;
analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo; y
determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo.

Preferentemente, la información de identidad de usuario incluye información de credencial en información de registro de usuario; y la etapa de analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo incluye específicamente: adquirir la ubicación de análisis de identidad de usuario de acuerdo con un tipo de credencial y un número de credencial en cada fragmento de información de registro de usuario, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

Preferentemente, la etapa de adquirir la ubicación de análisis de identidad de usuario de acuerdo con un tipo de credencial y un número de credencial en cada fragmento de información de registro de usuario y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo incluye:
determinar un modo de análisis para la ubicación de análisis de identidad de usuario de acuerdo con una clase del tipo de credencial; y
analizar los seis primeros dígitos de cada número de credencial para adquirir la ubicación de análisis de identidad de usuario cuando el tipo de credencial es una tarjeta de ID de un residente local chino, y contar en consecuencia el número de ubicaciones de análisis de identidad de usuario en el dispositivo; o
suponer que cada tipo de credencial o cada número de credencial corresponde a una ubicación de análisis de identidad de usuario cuando el tipo de credencial es una tarjeta de ID que no es de un residente local chino o es un credencial extranjero, y contar en consecuencia el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

Preferentemente, la etapa de recopilar información de dispositivo de un dispositivo que tiene un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual incluye: adquirir información de dispositivo correspondiente del dispositivo recopilando un código de identificación de dispositivo del dispositivo.

Preferentemente, la etapa de adquirir información de dispositivo correspondiente del dispositivo recopilando un código de identificación de dispositivo del dispositivo incluye:
determinar contenido de la información de dispositivo recopilada de acuerdo con el tipo de dispositivo;
donde la información de dispositivo recopilada incluye una dirección MAC, una dirección IP y/o un UMID cuando el dispositivo es un PC; y
la información de dispositivo recopilada incluye una dirección MAC, un IMEI, un TID y/o un número de teléfono móvil cuando el dispositivo es un terminal móvil.

Preferentemente, la etapa de adquirir información de dispositivo correspondiente del dispositivo recopilando un código de identificación de dispositivo del dispositivo incluye:
determinar un modo de contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo de acuerdo con una cantidad de dispositivos identificada a partir del código de identificación de dispositivo;
analizar y contar, cuando se identifica un único dispositivo, el número de ubicaciones de análisis de identidad de usuario en el dispositivo; o
analizar y contar, cuando se identifican múltiples dispositivos, el número de ubicaciones de análisis de identidad de usuario en cada dispositivo; o
fijar a 0 el número de ubicaciones de análisis de identidad de usuario en el dispositivo cuando no se identifica ningún dispositivo; y
usar el número obtenido de ubicaciones de análisis de identidad de usuario en el dispositivo como variable de entrada de un modelo de calificación preestablecido para evaluar el nivel de riesgo de robo de cuenta del dispositivo.

Preferentemente, la etapa de determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo incluye: evaluar el nivel de riesgo de robo de cuenta de un usuario del comportamiento de operación actual en combinación con el número total de usuarios en el dispositivo, la cantidad de números de teléfono móvil vinculados al usuario del comportamiento de operación actual, el número de dispositivos relativos a comportamientos de operación de historial del usuario actual, el número de direcciones IP de los comportamientos de operación de historial del usuario actual, una diferencia entre la información acerca del comportamiento de operación actual e información acerca de los comportamientos de operación de historial del usuario actual, y/o si la información de características de encaminamiento del comportamiento de operación actual es idéntica a información de características de encaminamiento de los comportamientos de operación de historial.

Preferentemente, la etapa de determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo incluye además: calcular un valor de riesgo de robo de cuenta en combinación con el nivel de riesgo de robo de cuenta del dispositivo y el nivel de riesgo de robo de cuenta del usuario del comportamiento de operación actual, e identificar un robo de cuenta cuando el valor de riesgo es mayor que un umbral preestablecido.

En base a esto, la presente solicitud proporciona además un aparato de identificación de riesgo de robo de cuenta, que incluye:
un módulo de recopilación de información de dispositivo configurado para recopilar información de dispositivo de un dispositivo que tiene un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual;
un módulo de adquisición de información de usuario configurado para adquirir toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo dentro de un periodo de tiempo preestablecido anterior al comportamiento de operación actual;
un módulo de análisis de identidad de usuario configurado para analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo; y
un módulo de evaluación de riesgo de robo de cuenta configurado para determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo.

Preferentemente, la información de identidad de usuario incluye información de credencial en la información de registro de usuario; y el módulo de análisis de identidad de usuario adquiere la ubicación de análisis de identidad de usuario de acuerdo con un tipo de credencial y un número de credencial en cada fragmento de información de registro de usuario y cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

Preferentemente, el módulo de análisis de identidad de usuario determina un modo de análisis para la ubicación de análisis de identidad de usuario de acuerdo con una clase del tipo de credencial; y analiza los seis primeros dígitos de cada número de credencial para adquirir la ubicación de análisis de identidad de usuario cuando el tipo de credencial es una tarjeta de ID de un residente local chino, y cuenta en consecuencia el número de ubicaciones de análisis de

identidad de usuario en el dispositivo; o supone que cada tipo de credencial o cada número de credencial corresponde a una ubicación de análisis de identidad de usuario cuando el tipo de credencial es una tarjeta de ID que no es de un residente local chino o es una credencial extranjera, y cuenta en consecuencia el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

Preferentemente, el módulo de recopilación de información de dispositivo adquiere información de dispositivo correspondiente del dispositivo recopilando un código de identificación de dispositivo del dispositivo.

Preferentemente, el módulo de recopilación de información de dispositivo determina contenido de la información de dispositivo recopilada acerca de un tipo del dispositivo, donde la información de dispositivo recopilada incluye una dirección MAC, una dirección IP y/o un UMID cuando el dispositivo es un PC; y la información de dispositivo recopilada incluye una dirección MAC, un IMEI, un TID y/o un número de teléfono móvil cuando el dispositivo es un terminal móvil.

Preferentemente, el módulo de análisis de identidad de usuario determina un modo de contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo de acuerdo con una cantidad de dispositivos identificada por el módulo de recopilación de información de dispositivo a partir del código de identificación de dispositivo; analiza y cuenta, cuando se identifica un único dispositivo, el número de ubicaciones de análisis de identidad de usuario en el dispositivo; o analiza y cuenta, cuando se identifican múltiples dispositivos, el número de ubicaciones de análisis de identidad de usuario en cada dispositivo; o fija a 0 el número de ubicaciones de análisis de identidad de usuario en el dispositivo cuando no se identifica ningún dispositivo; y usa el número obtenido de ubicaciones de análisis de identidad de usuario en el dispositivo como una variable de entrada de un modelo de calificación preestablecido del módulo de evaluación de riesgo de robo de cuenta para evaluar el nivel de riesgo de robo de cuenta del dispositivo.

Preferentemente, el módulo de evaluación de riesgo de robo de cuenta evalúa el nivel de riesgo de robo de cuenta de un usuario del comportamiento de operación actual en combinación con el número total de usuarios en el dispositivo, la cantidad de números de teléfono móvil vinculados al usuario del comportamiento de operación actual, el número de dispositivos relativos a comportamientos de operación de historial del usuario actual, el número de direcciones IP de los comportamientos de operación de historial del usuario actual, una diferencia entre la información acerca del comportamiento de operación actual e información acerca de los comportamientos de operación de historial del usuario actual, y/o si la información de características de encaminamiento del comportamiento de operación actual es idéntica a información de características de encaminamiento de los comportamientos de operación de historial.

Preferentemente, el módulo de evaluación de riesgo de robo de cuenta calcula un valor de riesgo de robo de cuenta en combinación con el nivel de riesgo de robo de cuenta del dispositivo y el nivel de riesgo de robo de cuenta del usuario del comportamiento de operación actual, e identifica un robo de cuenta cuando el valor de riesgo es mayor que un umbral preestablecido.

En base a esto, la presente solicitud proporciona además un sistema de prevención y control de riesgo de robo de cuentas, que incluye el aparato de identificación de riesgo descrito anteriormente, un aparato de notificación de robo de cuenta y un aparato de procesamiento de riesgo, donde
el aparato de identificación de riesgo está configurado para calcular un valor de riesgo de robo de cuenta en una plataforma de comportamiento de operación, y para identificar un robo de cuenta cuando el valor de riesgo es mayor que un umbral preestablecido;
el aparato de notificación de robo de cuenta está configurado para notificar un mensaje de robo de cuenta al aparato de procesamiento de riesgo y a un dispositivo receptor de usuario cuando el aparato de identificación de riesgo identifica un robo de cuenta; y
el aparato de procesamiento de riesgo está configurado para bloquear una cuenta robada de un usuario y para interceptar datos de riesgo asociados a la cuenta robada cuando se recibe el mensaje de robo de cuenta.

Preferentemente, el sistema incluye una base de datos de casos configurada para almacenar los datos de riesgo interceptados por el aparato de procesamiento de riesgo, de modo que el aparato de procesamiento de riesgo examina los datos de riesgo y el aparato de identificación de riesgo verifica el modelo de calificación.

En comparación con la técnica anterior, la presente solicitud proporciona una solución para identificar un riesgo de robo de cuenta en función del número de ubicaciones de análisis de identidad de usuario en un dispositivo, que recopila toda la información de identidad de usuario en un dispositivo de inicio de sesión en un periodo de tiempo anterior a un comportamiento de operación, para analizar y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo, y usa el cómputo como variable de entrada de un modelo de calificación de riesgo para evaluar el nivel de riesgo de robo de cuenta, lo que mejora así de manera eficaz la capacidad de distinguir un riesgo de robo de cuenta. Esto se debe a que: las diferentes ubicaciones de análisis de identidad de todos los usuarios de comportamiento de operación en un dispositivo de inicio de sesión en un periodo de tiempo reciente es una variable más eficaz y estable. Si el dispositivo tiene múltiples ubicaciones de análisis de identidad diferentes en un periodo de tiempo reciente cuando se produce un comportamiento de operación, una cuenta del comportamiento de operación tiene un alto riesgo de ser robada. Por otro lado, en un dispositivo, la situación de comportamientos de operación de diferentes usuarios en una misma ubicación es más común que la situación de comportamientos de operación de diferentes usuarios en ubicaciones diferentes y, por lo tanto, la variable puede eliminar de forma eficaz algunas situaciones en las que los

comportamientos de operación son realizados por múltiples usuarios, pero el riesgo no es alto, lo que ayuda a mejorar la capacidad diferenciadora de riesgo y la estabilidad de la variable del modelo de calificación de riesgo.

Las características del procedimiento, aparato y sistema de acuerdo con la presente invención se definen en las reivindicaciones independientes, y las características preferidas de acuerdo con la presente invención se definen en las reivindicaciones dependientes.

**Breve descripción de los dibujos**

Otras diversas ventajas y beneficios resultarán evidentes a los expertos en la técnica después de leer la siguiente descripción detallada de las implementaciones preferidas. Los dibujos adjuntos solo se usan para ilustrar las implementaciones preferidas, y no deben considerarse una limitación de la presente solicitud. Además, en todos los dibujos adjuntos se usan números de referencia idénticos para representar partes idénticas. En los dibujos:
la FIG. 1 muestra una relación entre el número de ubicaciones de análisis de identidad de usuario en un dispositivo MAC de una plataforma de red y un riesgo de robo de cuenta 7 días antes de un comportamiento de operación actual;
la FIG. 2 es un diagrama de flujo de un procedimiento de identificación de riesgo de robo de cuenta de acuerdo con una forma de realización de la presente solicitud;
la FIG. 3 es un diagrama de bloques de un aparato de identificación de riesgo de robo de cuenta de acuerdo con una forma de realización de la presente solicitud; y
la FIG. 4 es un diagrama de bloques de un sistema de prevención y de control de riesgo de robo de cuenta de acuerdo con una forma de realización de la presente solicitud.

**Descripción detallada**

En las siguientes formas de realización de la presente solicitud, una variable de entrada de este tipo, es decir, el número de ubicaciones de análisis de identidad de usuario en un dispositivo en un periodo de tiempo anterior a un comportamiento de operación actual, se introduce en un modelo de calificación de riesgo para mejorar la capacidad diferenciadora de riesgo de la variable del modelo. Esta solución necesita establecer un modelo de calificación de riesgo en función de una tecnología de minería de datos. Las principales etapas de modelado incluyen determinar un objeto de investigación, determinar una fuente de datos, tomar muestras, explorar los datos, desarrollar un modelo, verificar el modelo, etc. La presente solicitud se centra en construir una variable de entrada adecuada para el modelo de calificación. Puesto que el modelo de calificación no es el principal objetivo de la presente solicitud, no se describirán otros detalles de modelado; para más detalles, consúltese la técnica anterior convencional.

Para generar una variable adecuada, el inventor de la presente solicitud recopila una gran cantidad de datos de comportamientos de operación de usuarios en una plataforma de red para llevar a cabo un análisis de datos y una minería de datos. Por ejemplo, para la plataforma, la información de dispositivo puede recopilarse cuando se produce cada comportamiento de operación de un usuario y, además, puede contarse el número de usuarios que tienen comportamientos de operación en la plataforma en estos dispositivos en un periodo de tiempo reciente. Puede identificarse un riesgo de robo de cuenta de acuerdo con el número de usuarios en la plataforma en los dispositivos. Sin embargo, se produce con frecuencia el problema de un juicio erróneo. En función del análisis de los datos, el inventor de la presente solicitud determina que: en cuanto a los comportamientos de operación en la plataforma, en el mismo dispositivo, la situación de comportamientos de operación realizados por personas en la misma ubicación es más habitual que la situación de comportamientos de operación realizados por personas en diferentes ubicaciones. Por lo tanto, una variable más eficaz y estable es el número de diferentes ubicaciones de análisis de identidad de usuarios que llevan a cabo comportamientos de operación en la plataforma en el dispositivo en un periodo de tiempo reciente, y la granularidad de análisis de la ubicación de análisis de identidad es preferentemente un municipio (ciudad). Si el dispositivo tiene múltiples ubicaciones de análisis de identidad diferentes en el periodo de tiempo reciente cuando se produce un comportamiento de operación, un comportamiento de operación de este tipo tiene un riesgo extremadamente alto.

La regla anterior es muy estable en los comportamientos de operación en la plataforma. Puede apreciarse que esta regla también se aplica a comportamientos de operación en otras aplicaciones de red. Por consiguiente, el "comportamiento de operación" en la presente solicitud es un concepto generalizado que no está limitado a comportamientos empresariales de transferencia de fondos y bienes existentes en la plataforma anterior. Los intercambios de datos entre un usuario y una plataforma de servicio y entre diferentes usuarios en diversas aplicaciones de red también pertenecen al alcance del "comportamiento de operación" en la presente solicitud. Por ejemplo, un evento de inicio de sesión de una red social pertenece al "comportamiento de operación" en la presente solicitud.

Puesto que el número de ubicaciones de análisis de identidad de usuario en un dispositivo en un periodo de tiempo anterior a un comportamiento de operación actual está altamente asociado a un riesgo de robo de cuenta, el inventor de la presente solicitud usa el número de ubicaciones de análisis de identidad de usuario en el dispositivo en un periodo de tiempo preestablecido anterior a un comportamiento de operación como variable de entrada de un modelo de calificación de riesgo. Una variable de este tipo puede eliminar algunas situaciones en las que los comportamientos

de operación son realizados por múltiples usuarios pero el riesgo no es alto, lo que mejora la capacidad diferenciadora de riesgo y la estabilidad de la variable.

Por consiguiente, el inventor de la presente solicitud propone el siguiente concepto básico: tomando como variable de entrada el número de ubicaciones de análisis de identidad de usuario en un dispositivo en un periodo de tiempo anterior a un comportamiento de operación actual, el nivel de riesgo de robo de cuenta del dispositivo se evalúa usando un modelo de calificación preestablecido para identificar el riesgo de robo de cuenta de un usuario de manera más oportuna y eficaz. El concepto técnico implica principalmente contenido en tres aspectos: la generación de la variable, un proceso de identificación y una verificación de modelo, los cuales se describen a continuación en mayor detalle.

**1. Generación de la variable**

Para generar una variable válida, es necesario considerar factores tales como un sujeto variable, un objeto variable, un intervalo de tiempo y un índice estadístico, que se describen específicamente de la siguiente manera:
(1) Sujeto variable: información de dispositivo de un dispositivo de inicio de sesión de un comportamiento de operación (tal como un comportamiento de operación en una plataforma de pago). La información de dispositivo puede identificarse recopilando un código de identificación de dispositivo del dispositivo, tal como una dirección física de control de acceso a medios (MAC), un identificador de material único (UMID), una dirección de protocolo de Internet (IP), una identidad de equipo móvil internacional (IMEI), un identificador de amenazas (TID) o un número de teléfono móvil. Generalmente, en relación con un ordenador personal (PC) puede recopilarse una dirección MAC, una dirección IP y/o un UMID del dispositivo, y en relación con un terminal móvil puede recopilarse una dirección MAC, un IMEI, un TID y/o un número de teléfono móvil del dispositivo. Para soluciones específicas de recopilación e identificación, consúltese la técnica anterior convencional. Los detalles no se describen de nuevo.
(2) Objeto variable: una ubicación de análisis de identidad de usuario en el dispositivo de inicio de sesión del comportamiento de operación. La ubicación de análisis de identidad de usuario se determina habitualmente de acuerdo con un tipo de credencial y un número de credencial. Por ejemplo, los seis primeros dígitos de una tarjeta de ID de un residente chino pueden representar un municipio (ciudad). Con la identificación de los seis primeros dígitos puede conocerse la región administrativa a la que pertenece el usuario y, por lo tanto, se adquiere la ubicación de análisis de identidad de usuario.
(3) Intervalo de tiempo: un intervalo de tiempo anterior al comportamiento de operación (por ejemplo, 30 minutos, 2 horas, 12 horas, 1 día, 3 días, 7 días, etc.). El intervalo de tiempo difiere mucho en diversas plataformas de comportamiento de operación, y puede determinarse específicamente de acuerdo con factores tales como una solicitud de comportamiento de operación y la naturaleza del comportamiento de operación. Los detalles no se describen en el presente documento.
(4) Índice estadístico: se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo. En un entorno de comportamiento de operación normal, el número de ubicaciones de análisis de identidad de usuario en el dispositivo es generalmente pequeño; si el número de ubicaciones de análisis de identidad de usuario en el dispositivo es relativamente grande, esto indica que el riesgo de robo de cuenta es relativamente alto. Esto es una conclusión muy fiable obtenida de acuerdo con un análisis basado en una gran cantidad de datos.

Con la combinación de los factores anteriores, la presente solicitud determina una variable específica como el número de diferentes ubicaciones de análisis de identidad de todos los usuarios que llevan a cabo comportamientos de operación en un dispositivo en un intervalo de tiempo preestablecido anterior a un comportamiento de operación actual. Esta variable estadística puede aumentar la capacidad diferenciadora de riesgo de la variable del modelo. La variable está altamente asociada al riesgo de robo de cuentas. Si hay múltiples ubicaciones de análisis de identidad diferentes en un dispositivo en un periodo de tiempo reciente anterior a un comportamiento de operación, el comportamiento de operación en el dispositivo tiene un riesgo de robo de cuenta relativamente alto.

**2. Proceso de identificación**

Después de usar la estadística anterior como variable de entrada del modelo de calificación de riesgo, puede identificarse el riesgo de robo de cuenta en función de las ubicaciones de análisis de identidad de usuario en diferentes dispositivos. La ventaja radica en que puede mejorarse la capacidad diferenciadora de riesgo y la estabilidad de la variable. Específicamente, deben seguirse los siguientes procedimientos durante la identificación de riesgo de robo de cuenta.
(1) Adquisición del número de ubicaciones de análisis de identidad en el dispositivo, que incluye:
a. Se adquiere información de dispositivo de un comportamiento de operación actual; y se adquiere toda la información de identidad de usuario de comportamientos de operación en el dispositivo en un periodo de tiempo específico (tal como 3 días) anterior al comportamiento de operación;
b. La información de identificación se analiza para adquirir regiones de usuario correspondientes en la información de identidad, y se cuenta el número de diferentes ubicaciones de análisis de identidad de usuario en el dispositivo. La ubicación de análisis de identidad de usuario se identifica en el presente documento de manera general como una ciudad y, en el presente documento, la "ciudad" se refiere a una región administrativa y no puede interpretarse en sentido estricto como un concepto opuesto a un área rural.

c. Procesamiento en un caso especial: Si hay múltiples dispositivos, se cuentan números respectivos de ubicaciones de análisis de identidad de usuario; si no se puede adquirir ninguna información de dispositivo, el número de ubicaciones de análisis de identidad de usuario se fija a 0.

(2) Evaluar un nivel de riesgo

El nivel de riesgo del dispositivo se evalúa de acuerdo con el número de ubicaciones de análisis de identidad de usuario. Específicamente, después de adquirir el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación actual, se introduce como variable en el modelo de calificación de riesgo para la realizar la calificación. Después de considerar de manera exhaustiva pesos de diversas variables en el modelo, puede obtenerse el nivel de riesgo de robo de cuenta del dispositivo. Una calificación elevada indica un alto riesgo de nivel de cuenta y, en este caso, es esencialmente necesario supervisar el dispositivo.

**3. Verificación de modelo**

Es necesario verificar cómo influye la variable de entrada (el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación actual) en el efecto de predicción del modelo de calificación de riesgo. Si la variable es eficaz, el riesgo de robo de cuenta de un usuario puede identificarse automáticamente de acuerdo con el proceso en la segunda etapa anterior; en caso contrario, el modelo de calificación y la variable de entrada relacionada tienen que ajustarse de nuevo.

En la presente solicitud, es necesario tener en cuenta los siguientes factores durante la verificación del modelo:

(1) Si una etiqueta de comportamiento de operación de historial es un caso. Cuando se menciona en la presente solicitud, la estadística "número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación actual" tiene que asociarse a datos de comportamiento de operación de historial en el dispositivo para probar que la variable introducida es eficaz. Es decir, el que la variable sea eficaz tiene que medirse usando datos de comportamiento de operación de historial; dicho de otro modo, los datos de comportamiento de operación de historial pueden distinguir si se roba una cuenta.

Se supone que una etiqueta es "mala" cuando un comportamiento de operación de historial es un robo de cuenta; en caso contrario, la etiqueta es "buena". Si el resultado de riesgo de robo de cuenta identificado a través de la segunda etapa es "malo" y la etiqueta del comportamiento de operación de historial es también "mala", o si el resultado de riesgo de robo de cuenta identificado a través de la segunda etapa es "bueno" y la etiqueta del comportamiento de operación de historial es también "buena", se considera que la verificación es satisfactoria; en caso contrario, la verificación falla. Si la probabilidad de verificación satisfactoria es alta, esto indica que el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación actual introducido como variable de entrada en el modelo de calificación es eficaz, es decir, la variable tiene una capacidad diferenciadora de riesgo relativamente alta.

(2) Cuantificación de la capacidad diferenciadora de riesgo

La capacidad diferenciadora de riesgo de la variable también puede cuantificarse. Específicamente, un índice de capacidad diferenciadora de robo de cuenta del "número de ubicaciones de análisis de identidad en el dispositivo en el periodo de tiempo preestablecido antes del comportamiento de operación actual" puede calcularse por partes para implementar la cuantificación. Estos índices cuantitativos incluyen principalmente dos tipos: un incremento y un valor de información (IV) de intervalo.

Fórmulas para calcular el índice de capacidad diferenciadora de robo de cuenta se muestran como sigue:

Lift=interval stolen account transaction concentration/average stolen account transaction concentration

Incremento = concentración de transacciones de cuenta robada en intervalo/concentración promedio de transacciones de cuenta robada

*WOE* = ln(relación entre transacciones de cuenta no robada en intervalo y todas las transacciones de cuenta no robada/relación entre transacciones de cuenta robada en intervalo y todas las transacciones de cuenta robada)x100

*IV* de intervalo = *WOE* x (relación entre transacciones de cuenta no robada en intervalo y todas las transacciones de cuenta no robada - relación entre transacciones de cuenta robada en intervalo y todas las transacciones de cuenta robada)

*IV* = suma de *IV* de intervalo

En las fórmulas anteriores, para facilitar el análisis, el Peso de la Evidencia (WOE) se multiplica por un coeficiente 100, y su significado no es muy diferente de un WOE de índice en la minería de datos. Puede apreciarse que la "transacción" en la fórmula anterior puede interpretarse como un comportamiento de operación de red generalizado, pero no está limitado a actividades empresariales concretas, tales como un pago de fondos y una transferencia de productos.

Al calcular el resultado de capacidad diferenciadora de riesgo de la variable "número de ubicaciones de análisis de identidad en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación actual" de acuerdo con las fórmulas anteriores, puede verificarse de manera eficaz la eficacia de la variable introducida en el modelo de calificación. En la descripción se usa como ejemplo un índice de capacidad diferenciadora de robo de cuenta del "número de ubicaciones de análisis de identidad de usuario en un dispositivo MAC 7 días antes de un comportamiento de operación actual". El resultado del cálculo se muestra en la Tabla 1:

Tabla 1: Capacidad diferenciadora de robo de cuenta del número de ubicaciones de análisis de identidad de usuario en un dispositivo MAC 7 días antes de un comportamiento de operación

| Intervalo | Número de intervalo | Número de robo de cuenta | Operación de robo de cuenta en intervalo | Operación de robo de cuenta en promedio | Incremento | Valor IV de intervalo | Valor IV |
|---|---|---|---|---|---|---|---|
| 0 | 578.007 | 1.934 | 0,3% | 1,0% | 0,33 | 32,07 | 171,74 |
| [1,2] | 704.478 | 4.602 | 0,7% | 1,0% | 0,65 | 7,9 | 171,74 |
| (2,327] | 48.887 | 6.756 | 13,8% | 1,0% | 13,82 | 131,77 | 171,74 |

La Tabla 1 puede representarse de manera gráfica. Con referencia a la FIG. 1, se muestra una relación entre el número de ubicaciones de análisis de identidad de usuario en un dispositivo MAC de una plataforma de pago 7 días antes de un comportamiento de operación actual y un riesgo de robo de cuenta. Puede deducirse a partir de la Tabla 1 y la FIG. 1 que el incremento es 13,82 cuando el número de ubicaciones de análisis de identidad de usuario en el dispositivo es mayor que 2, es decir, la capacidad de distinguir el riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario de comportamientos de operación en el dispositivo MAC en 7 días aumenta 13,82 veces. Esto indica que la capacidad diferenciadora de robo de cuenta de la variable es muy eficaz.

Asimismo, en lo que respecta a la verificación en otros casos específicos, los índices cuantitativos son relativamente deseables, lo que indica que, al introducirse una variable de entrada de este tipo, es decir, el número de ubicaciones de análisis de identidad de usuario en un dispositivo en un periodo de tiempo anterior a un comportamiento de operación actual, en el modelo de calificación de riesgo para evaluar el nivel de riesgo de robo de cuenta, la presente solicitud puede mejorar la capacidad diferenciadora de riesgo de la variable de modelo, de modo que el efecto de identificación de riesgo de robo de cuenta es relativamente deseable.

Debe observarse que los valores IV de la Tabla 1 y la FIG. 1 son relativamente elevados y, en algunos casos, puede producirse un fenómeno de "sobrepredicción". Para eliminar dicho fenómeno, en la presente solicitud, el riesgo de que se robe una cuenta de usuario se evalúa además de manera exhaustiva en combinación con el número total de usuarios en el dispositivo, la cantidad de números de teléfono móvil vinculados al usuario del comportamiento de operación actual, el número de dispositivos relativos a comportamientos de operación de historial del usuario actual, el número de direcciones IP de los comportamientos de operación de historial del usuario actual, una diferencia entre la información acerca del comportamiento de operación actual e información acerca de los comportamientos de operación de historial del usuario actual, y/o si la información de características de encaminamiento del comportamiento de operación actual es idéntica a información de características de encaminamiento de los comportamientos de operación de historial, para eliminar el efecto negativo provocado por la "sobrepredicción" de una única variable.

El concepto técnico de usar una estadística del número de ubicaciones de análisis de identidad de usuario en un dispositivo en un periodo de tiempo preestablecido anterior a un comportamiento de operación actual para identificar un riesgo de robo de cuenta en la presente solicitud se ilustra de forma sistemática en el principio anterior. Soluciones de implementación específicas del concepto técnico se describen adicionalmente a continuación. En función del análisis anterior, después de que el modelo de calificación de riesgo y la variable de entrada se determinen y se verifiquen de manera satisfactoria, solo es necesario implantar una aplicación en una sección de servidor de acuerdo con la segunda etapa descrita anteriormente para una implementación específica, aunque no es necesario repetir ni el modelado ni la verificación.

Con referencia a la FIG. 2, se muestra un diagrama de flujo de un procedimiento de identificación de riesgo de robo de cuenta de acuerdo con una forma de realización de la presente solicitud. Como se muestra en la FIG. 2, el procedimiento de identificación de riesgo incluye las siguientes etapas principales, tales como las etapas 210 a 240, que se describen a continuación en mayor detalle.

S210: Recopilar información de dispositivo de un dispositivo de inicio de sesión de un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual.

Esta etapa responde a la información acerca del comportamiento de operación actual, y un dispositivo correspondiente de un terminal de servidor recopila la información de dispositivo del dispositivo de inicio de sesión del comportamiento de operación, que se obtiene generalmente recopilando un código de identificación de dispositivo del dispositivo.

Generalmente, los dispositivos de inicio de sesión de terminales cliente se clasifican en múltiples tipos. Por ejemplo, un dispositivo de tipo PC tiene habitualmente una dirección MAC, una dirección IP y/o un UMID, y un terminal móvil tiene habitualmente una dirección MAC, un IMEI, un TID y/o un número de teléfono móvil, etc. Por lo tanto, el contenido de la información de dispositivo recopilada tiene que determinarse de acuerdo con el tipo de dispositivo. Generalmente, en relación con un PC se recopila una dirección MAC, una dirección IP y/o un UMID; en relación con un terminal móvil se recopila una dirección MAC, un TID y/o un número de teléfono móvil. En lo que respecta a procedimientos específicos de recopilación e identificación de información, consúltese la técnica anterior. Los detalles no se describen en el presente documento.

Cabe destacar que el comportamiento de operación actual en la etapa S210 puede ser una solicitud de inicio de sesión para una cuenta de usuario, o puede ser una solicitud de operación de datos preestablecida para una cuenta de usuario, etc. La solicitud de operación de datos preestablecida para una cuenta de usuario puede incluir: una solicitud de modificación de contraseña para la cuenta de usuario, una solicitud de transferencia de saldos para la cuenta de usuario y una solicitud de transacción de bienes para la cuenta de usuario. Puede apreciarse que la solicitud de operación de datos preestablecida puede fijarse de antemano por un servidor o puede fijarse de antemano por un usuario a través de un terminal cliente, lo cual no está limitado en el presente documento.

Cuando un usuario inicia una solicitud de inicio de sesión para una cuenta de usuario en un terminal cliente, la información de inicio de sesión del usuario incluye generalmente un identificador de usuario, información acerca del terminal cliente en el que el usuario inicia la solicitud de inicio de sesión e información acerca de un servidor que recibe la solicitud de inicio de sesión. Por lo tanto, una ruta de encaminamiento de inicio de sesión del usuario se adquiere de acuerdo con la información de inicio de sesión del usuario, y la información de característica de encaminamiento actual se extrae de la ruta de encaminamiento de inicio de sesión del usuario. Al comparar si la información de características de encaminamiento del comportamiento de operación actual es idéntica a la información de características de encaminamiento de comportamientos de operación de historial, también puede evaluarse el nivel de riesgo de robo de cuenta del usuario del comportamiento de operación actual.

S220: Adquirir toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo en un periodo de tiempo preestablecido anterior al comportamiento de operación.

Puede apreciarse que es muy complejo y difícil identificar el riesgo de un único comportamiento de operación de una única cuenta, mientras que un procedimiento muy eficaz incluye identificar el riesgo mediante la determinación de una asociación entre comportamientos de operación de múltiples cuentas. Como se ha descrito anteriormente, en la presente solicitud, el riesgo de robo de cuenta del dispositivo se evalúa de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación actual. Esto requiere la extracción de toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo en este periodo de tiempo, y la extracción de ubicaciones de análisis de identidad de usuario es particularmente importante.

En una aplicación concreta, el intervalo de tiempo (tal como 30 minutos, 2 horas, 12 horas, 1 día, 3 días y 7 días) para usuarios del dispositivo puede determinarse, generalmente, de acuerdo con factores tales como una plataforma de comportamiento de operación, una solicitud de comportamiento de operación y una naturaleza de comportamiento de operación. Después de adquirir información de usuario de los comportamientos de operación de historial en el periodo de tiempo, pueden analizarse adicionalmente regiones de identidad de los usuarios. Tras su cómputo, el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo puede usarse como variable del modelo de calificación de riesgo para la realizar la calificación.

S230. Analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo.

Como se ha descrito anteriormente, el número de diferentes ubicaciones de análisis de identidad de usuarios que llevan a cabo comportamientos de operación en una plataforma de pago del dispositivo dentro de un periodo de tiempo reciente anterior al comportamiento de operación actual es una variable eficaz y estable. Por lo tanto, la estadística del número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo puede introducirse como variable en el modelo de calificación de riesgo para realizar la calificación y conseguir finalmente el objetivo de identificar si se ha robado la cuenta de usuario.

Puede apreciarse que la granularidad diferenciadora de la ubicación de análisis de identidad de usuario está altamente correlacionada con el resultado de salida del modelo de calificación. Preferentemente, se toma la ciudad como la granularidad diferenciadora de la ubicación de análisis de identidad de usuario en la presente solicitud, de modo que el efecto de identificación de riesgo de robo de cuenta es relativamente deseable.

En muchas plataformas de comportamiento de operación en redes, es necesario realizar una autenticación de nombre real durante el registro de cuenta de usuario, lo que es bueno para mejorar la seguridad de la red. Por lo tanto, la

etapa S230 de adquirir la ubicación de análisis de identidad de usuario de acuerdo con un tipo de credencial y un número de credencial en cada fragmento de información de registro de usuario y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo incluye específicamente determinar un modo de análisis para la ubicación de análisis de identidad de usuario de acuerdo con la clase del tipo de credencial.

Si el tipo de credencial es una tarjeta de ID de un residente local chino, los seis primeros dígitos de la misma representan una región administrativa a nivel de municipio (ciudad) y, por lo tanto, la ubicación de análisis de identidad de usuario puede adquirirse simplemente analizando los seis primeros dígitos de cada número de credencial y, en consecuencia, se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

Cuando el tipo de credencial es una tarjeta de ID que no es de un residente local chino (tal como un certificado de funcionarios) o es una credencial extranjera (tal como un pasaporte), no puede identificarse directamente la región administrativa en la que está ubicada la identidad de usuario. Sin embargo, dichas situaciones son relativamente inusuales y, por lo tanto, puede suponerse simplemente que cada tipo de credencial o cada número de credencial corresponde a una ubicación de análisis de identidad de usuario y, en consecuencia, se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo. En definitiva, si el modo de numerar estos tipos de credenciales se obtiene durante el modelado, la ubicación de análisis de identidad de usuario puede obtenerse de acuerdo con un número de credencial específico. Los detalles no se describen en el presente documento.

Cabe destacar que la información de dispositivo adquirida en la etapa S210 puede tener diferentes situaciones: en la mayoría de casos puede recopilarse múltiples tipos de información de dispositivo al mismo tiempo, por ejemplo, una dirección MAC, un IMEI, etc. Sin embargo, debido a razones técnicas, la información de dispositivo durante el comportamiento de operación no puede recopilarse en algunos escenarios o restricciones de sistema, o la información de dispositivo recopilada durante el comportamiento de operación se refiere a, evidentemente, un punto de acceso que tiene que eliminarse, etc. En estos casos, los modos de analizar y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo tienen que ajustarse de manera correspondiente.

Por lo tanto, en las etapas S220 a S230, es necesario determinar el modo de contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo de acuerdo con una cantidad de dispositivos identificada a partir del código de identificación de dispositivo, lo que incluye específicamente:

si se identifica un único dispositivo, analizar cada ubicación de análisis de identidad de usuario en el dispositivo único, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo;

si se identifican múltiples dispositivos, analizar por separado cada ubicación de análisis de identidad de usuario en cada dispositivo y contar el número de ubicaciones de análisis de identidad de usuario en cada dispositivo;

si no se identifica ningún dispositivo, fijar a 0 el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

El número de ubicaciones de análisis de identidad de usuario en el dispositivo obtenido de la manera anterior se introduce como variable de entrada del modelo de calificación preestablecido en el modelo de calificación de riesgo para evaluar el nivel de riesgo de robo de cuenta del dispositivo, de modo que la capacidad diferenciadora de riesgo de robo de cuenta de la variable en el modelo de calificación se mide usando datos de comportamiento de operación de historial.

S240: Determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo.

Generalmente, el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo se usa como una variable de entrada del modelo de calificación preestablecido para evaluar el nivel de riesgo de robo de cuenta del dispositivo. El nivel de riesgo de robo de cuenta representa un riesgo de robo de cuenta, y si el nivel de riesgo de robo de cuenta supera un umbral especificado, esto identifica que se ha robado la cuenta; en caso contrario, esto identifica que no se ha robado la cuenta.

Después de obtener, de acuerdo con las etapas S210 a S230 anteriores, la estadística del número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido anterior al comportamiento de operación, la estadística puede introducirse en el modelo de calificación de riesgo para realizar la calificación y obtener el nivel de riesgo de robo de cuenta del dispositivo, identificándose así el riesgo de robo de cuenta, de modo que se toman a tiempo medidas de procesamiento para eliminar el riesgo.

Después de evaluarse el nivel de riesgo de robo de cuenta a través del proceso anterior, con el fin de mejorar adicionalmente la capacidad de identificación de riesgo de robo de cuenta, la presente solicitud evalúa además el nivel de riesgo de robo de cuenta de un usuario del comportamiento de operación actual en combinación con factores tales como el número total de usuarios en el dispositivo, la cantidad de números de teléfono móvil vinculados al usuario del comportamiento de operación actual, el número de dispositivos relativos a comportamientos de operación de historial del usuario actual, el número de direcciones IP de los comportamientos de operación de historial del usuario actual, una diferencia entre la información acerca del comportamiento de operación actual e información acerca de los comportamientos de operación de historial del usuario actual, y/o si la información de características de encaminamiento del comportamiento de operación actual es idéntica a información de características de

encaminamiento de los comportamientos de operación de historial. De esta manera, en combinación con múltiples factores, se mejora significativamente la capacidad de identificación de riesgo de robo de cuenta de la presente solicitud.

La presente solicitud calcula un valor de riesgo de robo de cuenta en combinación con el nivel de riesgo de robo de cuenta del dispositivo y el nivel de riesgo de robo de cuenta del usuario del comportamiento de operación actual, identifica un robo de cuenta cuando el valor de riesgo es mayor que un umbral preestablecido y proporciona una pronta información de robo de cuenta correspondiente cuando se identifica el robo de una cuenta, de modo que la plataforma de comportamiento de operación y el usuario realizan a tiempo un procesamiento para eliminar una posible amenaza relacionada con el robo de cuentas, evitándose así una pérdida de propiedad u otros problemas.

El procedimiento de identificación de riesgo de robo de cuentas (denominado en lo sucesivo procedimiento) se ha descrito en detalle anteriormente. En base a esto, la presente solicitud proporciona, además, de manera correspondiente, un aparato de identificación de riesgo de robo de cuentas (denominado en lo sucesivo aparato), que se describe en detalle a continuación.

En lo que se refiere a aspectos no descritos en detalle del aparato de esta forma de realización, consúltese el contenido descriptivo del procedimiento anterior. Del mismo modo, en lo que respecta a estructuras de aparato implicadas en el procedimiento anterior, puede hacerse referencia al siguiente contenido descriptivo.

Con referencia a la FIG. 3, se muestra un aparato de identificación de riesgo de robo de cuenta de acuerdo con una forma de realización de la presente solicitud. El aparato 300 incluye partes tales como un módulo de recopilación de información de dispositivo 310, un módulo de adquisición de información de usuario 320, un módulo de análisis de identidad de usuario 330 y un módulo de evaluación de riesgo de robo de cuenta 340, que se describen en lo sucesivo.

El módulo de recopilación de información de dispositivo 310 puede recopilar información de dispositivo de un dispositivo de inicio de sesión de un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual. En el presente documento, el módulo de recopilación de información de dispositivo 310 adquiere información de dispositivo correspondiente del dispositivo recopilando un código de identificación de dispositivo del dispositivo, y determina específicamente contenido de la información de dispositivo recopilada de acuerdo con el tipo de dispositivo, es decir, para un PC se recopila una dirección MAC, una dirección IP y/o un UMID, y para un terminal móvil se recopila una dirección MAC, un IMEI, un TID y/o un número de teléfono móvil.

El módulo de adquisición de información de usuario 320 puede adquirir toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo dentro de un periodo de tiempo preestablecido anterior al comportamiento de operación. Después de adquirir información de usuario de comportamientos de operación de historial en el periodo de tiempo correspondiente, el módulo de adquisición de información de usuario 320 proporciona la información de usuario al módulo de análisis de identidad de usuario 330 para analizar y obtener una región de identidad de cada usuario y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo; después, el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo puede usarse como variable de un modelo de calificación de riesgo para realizar la calificación.

El módulo de análisis de identidad de usuario 330 puede analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo. En particular, el módulo de análisis de identidad de usuario 330 usa la ciudad como granularidad diferenciadora de la ubicación de análisis de identidad de usuario. La información de identidad de usuario incluye información de credencial en información de registro de usuario. La ubicación de análisis de identidad de usuario se adquiere de acuerdo con un tipo de credencial y un número de credencial en cada fragmento de información de registro de usuario y se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo, lo que incluye específicamente determinar un modo de análisis para la ubicación de análisis de identidad de usuario de acuerdo con la clase del tipo de credencial. Específicamente, si el tipo de credencial es una tarjeta de ID de un residente local chino, los seis primeros dígitos de cada número de credencial se analizan para adquirir la ubicación de análisis de identidad de usuario y, en consecuencia, se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo; y si el tipo de credencial es una tarjeta de ID que no es de un residente local chino o es una credencial extranjera, se supone que cada tipo de credencial o cada número de credencial corresponde a una ubicación de análisis de identidad de usuario y, en consecuencia, se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo.

Además, el módulo de análisis de identidad de usuario 330 puede determinar un modo de contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo de acuerdo con una cantidad de dispositivos identificada por el módulo de recopilación de información de dispositivo 310 a partir de un código de identificación de dispositivo. Es decir, si se identifica un único dispositivo, se realiza un análisis y se cuenta el número de ubicaciones de análisis de identidad de usuario en el dispositivo; si se identifican múltiples dispositivos, se realiza un análisis y se cuenta el número de ubicaciones de análisis de identidad de usuario en cada dispositivo; y si no se identifica ningún dispositivo, el número de ubicaciones de análisis de identidad de usuario en el dispositivo se fija a 0. El número obtenido de ubicaciones de análisis de identidad de usuario en el dispositivo se usa como variable de entrada de un

modelo de calificación preestablecido del módulo de evaluación de riesgo de robo de cuenta 340 para evaluar el nivel de riesgo de robo de cuenta del dispositivo.

El módulo de evaluación de riesgo de robo de cuenta 340 puede usar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo como variable de entrada del modelo de calificación preestablecido para evaluar el nivel de riesgo de robo de cuenta del dispositivo. El módulo de evaluación de riesgo de robo de cuenta 340 evalúa además el nivel de riesgo de robo de cuenta de un usuario del comportamiento de operación actual en combinación con el número total de usuarios en el dispositivo, la cantidad de números de teléfono móvil vinculados al usuario del comportamiento de operación actual, el número de dispositivos relativos a comportamientos de operación de historial del usuario actual, el número de direcciones IP de los comportamientos de operación de historial del usuario actual, una diferencia entre la información acerca del comportamiento de operación actual e información acerca de los comportamientos de operación de historial del usuario actual, y/o si la información de características de encaminamiento del comportamiento de operación actual es idéntica a información de características de encaminamiento de los comportamientos de operación de historial. En base a esto, el módulo de evaluación de riesgo de robo de cuenta 340 calcula un valor de riesgo de robo de cuenta en combinación con el nivel de riesgo de robo de cuenta del dispositivo y el nivel de riesgo de robo de cuenta del usuario del comportamiento de operación actual, e identifica un robo de cuenta cuando el valor de riesgo es mayor que un umbral preestablecido.

El aparato de identificación de riesgo de robo de cuenta de la presente solicitud se ha descrito anteriormente, el cual tiene una capacidad diferenciadora deseable en la identificación de riesgo de robo de cuenta y tiene una estabilidad relativamente buena en la identificación de riesgo. En base a esto, un sistema de prevención y de control de riesgo de robo de cuenta se establece de manera correspondiente en la presente solicitud y se describe brevemente en lo sucesivo.

Con referencia a la FIG. 4, se muestra un sistema de prevención y de control de riesgo de robo de cuenta de acuerdo con una forma de realización de la presente solicitud. El sistema de prevención y de control de riesgo puede aplicarse a la prevención y el control de riesgos de comportamiento de operación entre un usuario (no mostrado en la figura) y una plataforma de comportamiento de operación (no mostrada en la figura). El sistema tiene un aparato de identificación de riesgo 300, un aparato de notificación de robo de cuenta 200, un aparato de procesamiento de riesgo 100 y una base de datos de casos 400.

Una relación de conexión entre las partes del sistema de prevención y de control de riesgo es como la mostrada en la FIG. 4 y un proceso correspondiente para implementar funciones es como sigue: el aparato de identificación de riesgo 300 calcula un valor de riesgo de robo de cuenta en una plataforma de comportamiento de operación e identifica un robo de cuenta cuando el valor de riesgo es mayor que un umbral preestablecido; el aparato de notificación de robo de cuenta 200 notifica un mensaje de robo de cuenta al aparato de procesamiento de riesgo 400 y a un dispositivo receptor de usuario (tal como un teléfono móvil) 500 cuando el aparato de identificación de riesgo 100 identifica el robo de una cuenta; el aparato de procesamiento de riesgo 100 bloquea una cuenta robada de un usuario e intercepta los datos de riesgo asociados a la cuenta robada cuando recibe el mensaje de robo de cuenta; y la base de datos de casos 400 almacena los datos de riesgo interceptados por el aparato de procesamiento de riesgo 100, de modo que el aparato de procesamiento de riesgo 300 examina los datos de riesgo y el aparato de identificación de riesgo 300 verifica el modelo de calificación.

En lo que respecta al aparato de identificación de riesgo 300 del sistema de prevención y de control de riesgo anterior, consúltese la estructura mostrada en la FIG. 3. Otros aparatos pueden elegirse de entre dispositivos o aplicaciones convencionales. Un sistema de prevención y de control de riesgo de este tipo puede identificar a tiempo un riesgo de robo de cuenta de usuario y, una vez que se confirme que una cuenta ha sido robada, puede llevar a cabo a tiempo un procesamiento, de modo puede proporcionarse de mejor manera un entorno seguro de comportamiento de operación en red, consiguiéndose así un valor de aplicación deseable.

Numerosos detalles se ilustran en la siguiente descripción de modo que se entienda mejor la presenta solicitud. Sin embargo, la presente solicitud puede implementarse de otras muchas maneras diferentes de la manera descrita en el presente documento. Los expertos en la técnica pueden establecer generalidades similares sin apartarse del ámbito de la presente solicitud. Por lo tanto, la presente solicitud no está limitada a las formas de realización específicas desveladas a continuación.

Con referencia a la FIG. 5, se muestra una forma de realización de la presente solicitud.

Aunque la presente solicitud se ha divulgado anteriormente usando formas de realización preferidas, las formas de realización preferidas no pretenden limitar la presente solicitud. Los expertos en la técnica pueden realizar posibles cambios y modificaciones sin apartarse del alcance de la presente solicitud. Por lo tanto, el alcance de protección de la presente solicitud debe estar sujeto al alcance definido por las reivindicaciones de la presente solicitud.

En una configuración típica, un dispositivo informático incluye uno o más procesadores (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria volátil, una memoria de acceso aleatorio (RAM) y/o una memoria no volátil o similar en un medio legible por ordenador, por ejemplo, una memoria de solo lectura (ROM) o una RAM de tipo flash. La memoria es un ejemplo del medio legible por ordenador.

1. El medio legible por ordenador incluye medios volátiles o no volátiles y medios móviles o no móviles, y puede implementar un almacenamiento de información a través de cualquier procedimiento o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos y un módulo de un programa u otros datos. Un medio de almacenamiento de un ordenador incluye, por ejemplo, pero no está limitado a, una memoria de cambio de fase (PRAM), una memoria de acceso aleatorio estática (SRAM), una memoria de acceso aleatorio dinámica (DRAM), otros tipos de memorias de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable eléctricamente borrable (EEPROM), una memoria flash u otras tecnologías de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otros almacenamientos ópticos, una cinta de casete, un almacenamiento en disco magnético/cinta magnética u otros dispositivos de almacenamiento magnético, o cualquier otro medio de no transmisión, y puede usarse para almacenar información accesible por el dispositivo informático. De acuerdo con la definición en este texto, el medio legible por ordenador no incluye medios transitorios, tal como una señal de datos modulada y una portadora.

2. Los expertos en la técnica deben entender que las formas de realización de la presente solicitud pueden proporcionarse como un procedimiento, un sistema o un producto de programa informático. Por lo tanto, la presente solicitud puede implementarse como una forma de realización totalmente en hardware, una forma de realización totalmente en software o una forma de realización que combina software y hardware. Además, la presente solicitud puede utilizar la forma de un producto de programa informático implementado en uno o más medios de almacenamiento utilizables por ordenador (que incluyen, pero sin limitarse a, una memoria de disco magnético, un CD-ROM, una memoria óptica, etc.) que incluyen código de programa utilizable por ordenador.

**REIVINDICACIONES**

1. Un procedimiento de identificación de una cuenta robada en un dispositivo de una plataforma de red, que comprende:

recopilar (S210) información de dispositivo del dispositivo de la plataforma de red, donde un usuario solicita iniciar sesión en una cuenta de usuario en el dispositivo de la plataforma de red;

adquirir (S220) información de identidad de usuario de usuarios que han realizado operaciones en el dispositivo dentro de un periodo de tiempo preestablecido anterior al inicio de sesión, donde la información de identidad de usuario para cada uno de los usuarios comprende información de registro de usuario correspondiente proporcionada por cada uno de los usuarios durante una autenticación de nombre real, donde cada fragmento de la información de identidad de usuario comprende un tipo de credencial y un número de credencial asociados a una tarjeta de identificación respectiva de cada uno de los usuarios;

analizar ubicaciones de identidad de usuario de los usuarios en función del tipo de credencial y el número de credencial en cada fragmento de la información de registro de usuario;

contar (S230) un número de diferentes ubicaciones de identidad de usuario de los usuarios en el dispositivo en el periodo de tiempo preestablecido; e

identificar (S240) la cuenta de usuario como robada en función de una determinación de que el nivel de riesgo de robo de cuenta del dispositivo supera un umbral especificado, donde el nivel de riesgo de robo de cuenta del dispositivo se calcula de acuerdo con el número de diferentes ubicaciones de identidad de usuario de los usuarios en el dispositivo en el periodo de tiempo preestablecido.

**2.** El procedimiento según la reivindicación 1, en el que una ubicación de identidad de usuario de un usuario se determina de acuerdo con el número de credencial.

**3.** El procedimiento según la reivindicación 1, en el que adquirir las ubicaciones de identidad de usuario comprende:

determinar un modo de análisis para las ubicaciones de identidad de usuario de acuerdo con la clase del tipo de credencial; y

analizar seis primeros dígitos de cada número de credencial para adquirir las ubicaciones de análisis de identidad de usuario cuando el tipo de credencial es una tarjeta de ID de un residente local chino, y contar en consecuencia el número de ubicaciones de identidad de usuario en el dispositivo; o

donde cada tipo de credencial o cada número de credencial corresponde a una ubicación de identidad de usuario cuando el tipo de credencial es una tarjeta de ID que no es de un residente local chino o es una credencial extranjera, y contar en consecuencia el número de ubicaciones de identidad de usuario en el dispositivo.

**4.** El procedimiento según la reivindicación 1, en el que recopilar la información de dispositivo del dispositivo comprende:

adquirir información de dispositivo correspondiente del dispositivo recopilando un código de identificación de dispositivo del dispositivo.

**5.** El procedimiento según la reivindicación 4, en el que adquirir la información de dispositivo correspondiente del dispositivo recopilando el código de identificación de dispositivo del dispositivo comprende:

determinar contenido de la información de dispositivo recopilada de acuerdo con el tipo de dispositivo;

donde la información de dispositivo recopilada comprende una dirección MAC, una dirección IP y/o un UMID cuando el dispositivo es un PC; y

la información de dispositivo recopilada comprende una dirección MAC, un IMEI, un TID y/o un número de teléfono móvil cuando el dispositivo es un terminal móvil.

**6.** El procedimiento según la reivindicación 4, en el que adquirir la información de dispositivo correspondiente del dispositivo recopilando el código de identificación de dispositivo del dispositivo comprende:

determinar un modo de contar el número de ubicaciones de identidad de usuario en el dispositivo de acuerdo con una cantidad de dispositivos identificada a partir del código de identificación de dispositivo;

analizar y contar, cuando se identifica un único dispositivo, el número de ubicaciones de identidad de usuario en el dispositivo; o

analizar y contar, cuando se identifican múltiples dispositivos, el número de ubicaciones de identidad de usuario en cada dispositivo; o

fijar a 0 el número de ubicaciones de identidad de usuario en el dispositivo cuando no se identifica ningún dispositivo; y

usar el número obtenido de ubicaciones de identidad de usuario en el dispositivo como variable de entrada de un modelo de calificación preestablecido para evaluar el nivel de riesgo de robo de cuenta del dispositivo.

**7.** El procedimiento según cualquiera de las reivindicaciones 1 a 6, en el que identificar como robada la cuenta de usuario que se está solicitando para el inicio de sesión por el usuario comprende:

evaluar el nivel de riesgo de robo de cuenta del usuario en combinación con un número total de usuarios en el dispositivo, una cantidad de números de teléfono móvil vinculados al usuario, un número de dispositivos relativos a una operación de historial del usuario, un número de direcciones IP de la operación de historial del usuario, una diferencia entre información acerca del usuario que solicita iniciar sesión en la cuenta de usuario e información acerca de la operación de historial del usuario; y/o

evaluar si la información de características de encaminamiento del inicio de sesión solicitado en la cuenta de usuario es idéntica a información de características de encaminamiento de la operación de historial;

calcular un valor de riesgo de robo de cuenta como una combinación del nivel de riesgo de robo de cuenta del dispositivo y el nivel de riesgo de robo de cuenta del usuario; e

identificar la cuenta de usuario como robada cuando el valor de riesgo de robo de cuenta es mayor que un umbral preestablecido.

**8.** Un aparato (300) para identificar cuentas robadas, estando implementado el aparato mediante hardware o una combinación de software y hardware, estado configurado el aparato para realizar el procedimiento según una cualquiera de las reivindicaciones 1 a 7.

**9.** Un sistema para impedir y controlar cuentas en dispositivos en una plataforma de red, comprendiendo el sistema un aparato de identificación de riesgo (300) de acuerdo con la reivindicación 8, un aparato de notificación de robo de cuenta (200) y un aparato de procesamiento de riesgo (100), en el que

el aparato de identificación de riesgo (300) está configurado para calcular un valor de riesgo de robo de cuenta en la plataforma de red, y para identificar una cuenta como robada cuando el valor de riesgo de robo de cuenta es mayor que un umbral preestablecido;

el aparato de notificación de robo de cuenta (200) está configurado para notificar un mensaje de robo de cuenta al aparato de procesamiento de riesgo y a un dispositivo receptor de usuario (500) cuando el aparato de identificación de riesgo (300) identifica el robo de una cuenta; y

el aparato de procesamiento de riesgo (100) está configurado para bloquear la cuenta robada del usuario y para interceptar datos de riesgo asociados a la cuenta robada cuando se recibe el mensaje de robo de cuenta.

**10.** El sistema según la reivindicación 9, en el que el sistema comprende una base de datos de casos (400) configurada para almacenar los datos de riesgo interceptados por el aparato de procesamiento de riesgo (100), de modo que el aparato de procesamiento de riesgo (100) examina los datos de riesgo y el aparato de identificación de riesgo (300) verifica un modelo de calificación preestablecido para calificar datos de estadísticas del número de ubicaciones de identidad de usuario en el dispositivo en el periodo de tiempo preestablecido y para obtener el nivel de riesgo de robo de cuenta del dispositivo.

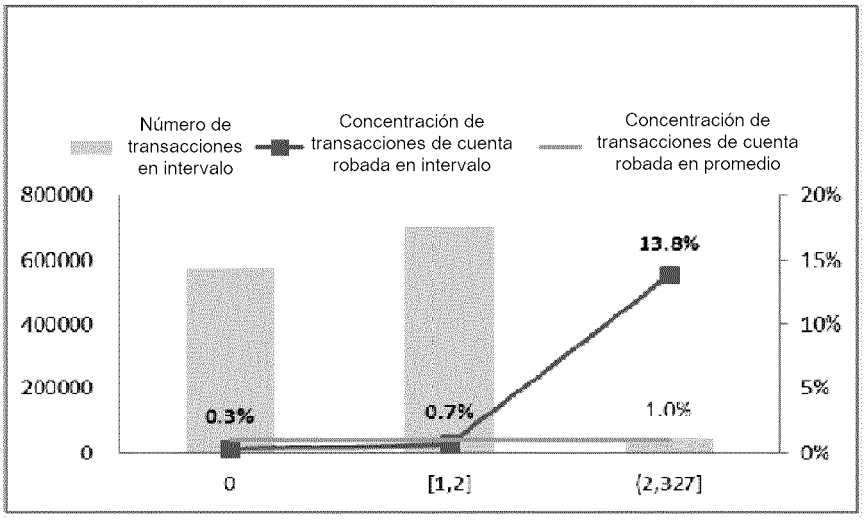
Número de transacciones en intervalo
Concentración de transacciones de cuenta robada en intervalo
Concentración de transacciones de cuenta robada en promedio
800000
600000
400000
200000
0
20%
15%
10%
5%
0%
0.3%
0.7%
13.8%
1.0%
0
[1,2]
(2,327]

FIG. 1

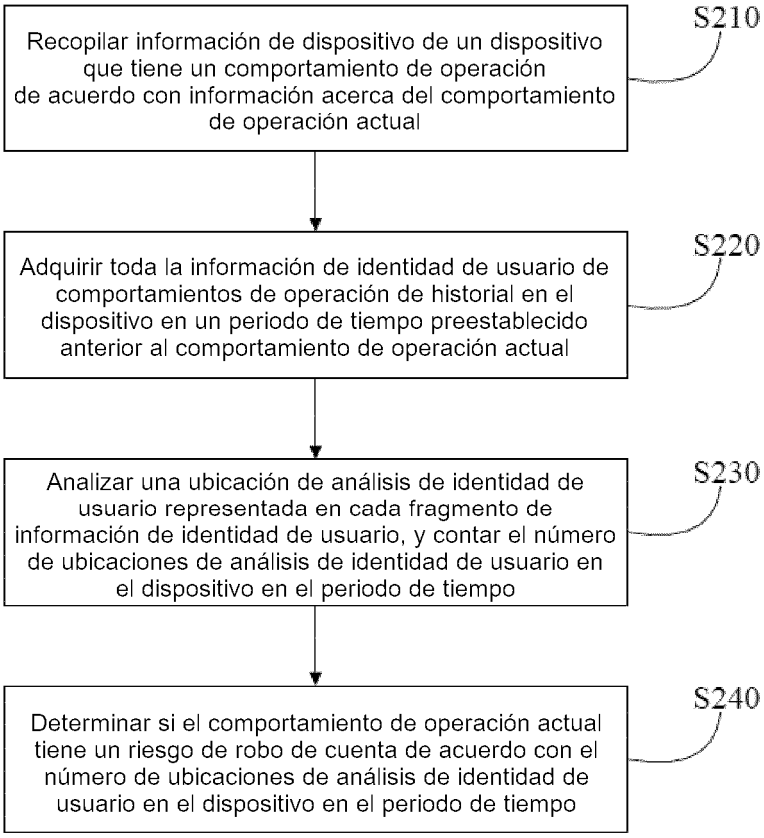
Recopilar información de dispositivo de un dispositivo que tiene un comportamiento de operación de acuerdo con información acerca del comportamiento de operación actual
S210
Adquirir toda la información de identidad de usuario de comportamientos de operación de historial en el dispositivo en un periodo de tiempo preestablecido anterior al comportamiento de operación actual
S220
Analizar una ubicación de análisis de identidad de usuario representada en cada fragmento de información de identidad de usuario, y contar el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo
S230
Determinar si el comportamiento de operación actual tiene un riesgo de robo de cuenta de acuerdo con el número de ubicaciones de análisis de identidad de usuario en el dispositivo en el periodo de tiempo
S240

FIG. 2

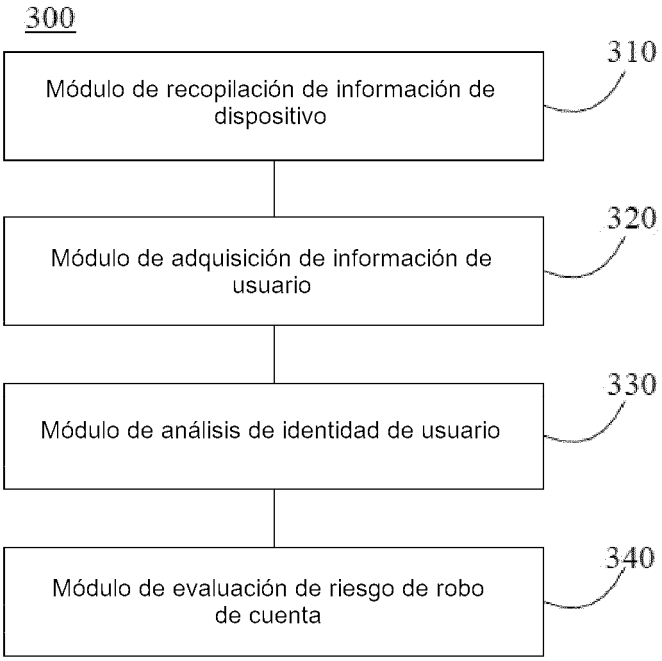
300
Módulo de recopilación de información de dispositivo
310
Módulo de adquisición de información de usuario
320
Módulo de análisis de identidad de usuario
330
Módulo de evaluación de riesgo de robo de cuenta
340

FIG. 3

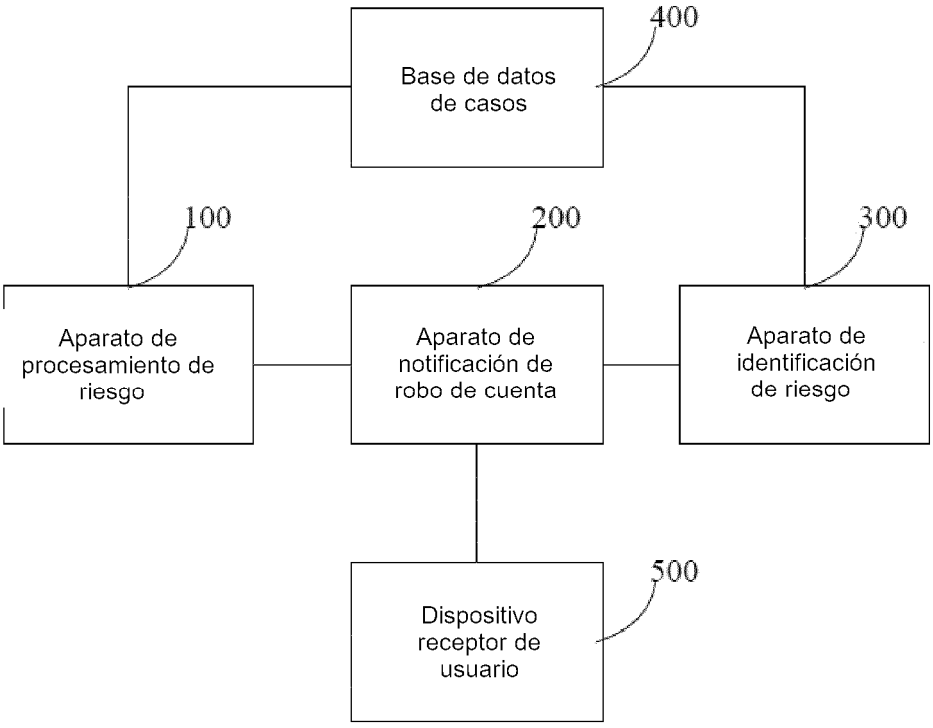
Base de datos de casos
400
100
200
300
Aparato de procesamiento de riesgo
Aparato de notificación de robo de cuenta
Aparato de identificación de riesgo
Dispositivo receptor de usuario
500

FIG. 4