

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 834 400**

51 Int. Cl.:

H04L 29/08 (2006.01)

H04L 29/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **03.07.2015** **PCT/CN2015/083251**

87 Fecha y número de publicación internacional: **28.01.2016** **WO16011884**

96 Fecha de presentación y número de la solicitud europea: **03.07.2015** **E 15824942 (5)**

97 Fecha y número de publicación de la concesión europea: **07.10.2020** **EP 3174268**

54 Título: **Método y aparatos para usar recursos de red exhaustivos**

30 Prioridad:

24.07.2014 CN 201410356190

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

17.06.2021

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:

WANG, JIN y
DENG, YULIANG

74 Agente/Representante:

SÁEZ MAESO, Ana

ES 2 834 400 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y aparatos para usar recursos de red exhaustivos

5 Campo técnico

La presente solicitud se refiere al uso de recursos de red y, más particularmente, a métodos y aparatos para usar recursos de red exhaustivos.

10 Antecedentes de la invención

Existen varios tipos de recursos en las redes. En general, se permite realizar algunas operaciones específicas solo en presencia de ciertos recursos, de esta manera logrando objetivos específicos a través de estas operaciones específicas. Por ejemplo, los tiempos de descarga de un documento valioso pueden considerarse como un tipo de recurso. Cuando los tiempos de descarga están dentro de un límite, los usuarios de la red pueden descargar el documento libremente. Cuando los tiempos de descarga alcanzan el límite preestablecido, los usuarios de la red no están autorizados a descargar. Al igual que los recursos naturales, dichos recursos en una red pueden clasificarse por analogía en recursos renovables y recursos no renovables. Los recursos no renovables no se pueden regenerar repetidamente dentro de un período determinado (o solo se pueden adquirir nuevamente mediante un procedimiento relativamente complejo). Este tipo de recursos también se puede denominar recursos exhaustivos.

Según las características anteriores de los recursos exhaustivos, puede existir un uso malintencionado de estos recursos en la red. Una vez que los recursos exhaustivos se agotan debido al uso malintencionado, el proceso de uso normal es limitado. Tomando como ejemplo los tiempos de errores de contraseña, un proveedor de servicios de red generalmente proporciona varias veces que se permite ingresar una contraseña incorrectamente. Se supone que el número de veces se establece en 3. Cuando un usuario con intenciones maliciosas ingresa arbitrariamente una contraseña que resulta ser incorrecta tres veces, se agota el recurso permitido en tiempos de errores de contraseña asignados por el proveedor de servicios de red. Cuando un usuario válido del servicio de red tiene la intención de utilizar el servicio, el nombre de usuario y la contraseña se bloquean. Podría afectar la utilización normal del servicio por parte del usuario de la red.

CN 1975789 A divulga un sistema integrado de alarma, monitoreo y control de acceso multifuncional que emplea procesos de autenticación de múltiples factores, como la combinación de autenticación de contraseña y reconocimiento facial. US 2012/0304260 A1 divulga un servidor de autenticación de usuarios, mediante el uso del seguimiento de la ubicación para determinar si se presenta un desafío de identidad mejorado a un usuario. US 2017/0136573 A1 divulga un sistema de autenticación y un método que usa dos o más formas de autenticación de múltiples factores, como una contraseña en combinación con un segundo método de autenticación mediante el uso de la contraseña. CN 102880560A divulga el intento de autenticar a un usuario que busca acceso a un dispositivo móvil a través del reconocimiento facial, el cambio a la autenticación de contraseña después de un número predefinido de intentos fallidos sucesivos y la autodestrucción de datos del dispositivo móvil después de un número predefinido de entradas de contraseña incorrectas sucesivas. US 2004/123158 A1 divulga que, si un usuario ya ha iniciado sesión desde un dispositivo de confianza, si se recibe otro intento de inicio de sesión desde un dispositivo que no es de confianza, se le pide al usuario que vuelva a escribir su contraseña en un servicio de mensajería instantánea del dispositivo de confianza, para confirmar el intento de inicio de sesión del dispositivo que no es de confianza. Si el usuario confirma que el intento de inicio de sesión del dispositivo que no es de confianza es legítimo, se permite el acceso desde el dispositivo que no es de confianza. De lo contrario, se deniega el acceso, ya que el intento de inicio de sesión desde el dispositivo que no es de confianza se considera malicioso.

Resumen

De acuerdo con aspectos de la invención, se proporcionan un método y un aparato, mediante el uso de un recurso de red exhaustivo como se establece en las reivindicaciones 1 y 8, respectivamente. En las reivindicaciones dependientes se establecen modalidades adicionales.

Para resolver el problema técnico anterior, las modalidades de la presente solicitud proporcionan un método mediante el uso de recursos de red exhaustivos y un aparato correspondiente de los mismos. Puede reducir o evitar el impacto en el funcionamiento normal del servicio causado por el consumo malintencionado de los recursos de red exhaustivos.

En un aspecto, la presente divulgación está dirigida a un método mediante el uso recursos de red exhaustivos. El método puede incluir determinar un tipo de entorno de operación del servicio actual, el tipo incluye un entorno confiable y un entorno no confiable. La operación del servicio actual puede influir en el valor de los recursos de red exhaustivos. Cuando el tipo de entorno de operación de servicio actual es un entorno no confiable, el método también puede incluir limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de primer grado. Cuando el tipo de entorno de operación de servicio actual es un entorno confiable, el método puede incluir además limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de segundo grado, siendo el valor de recurso de segundo grado mayor que el valor de los recursos de primer grado.

El entorno confiable puede incluir: un entorno de operación determinado correspondiente a una operación de un recurso de red exhaustivo realizada por un operador adecuado; un entorno operativo correspondiente durante la recuperación del valor del recurso de segundo grado; o un entorno operativo determinado correspondiente a un funcionamiento normal.

5 Las operaciones para determinar el tipo de entorno de operación del servicio actual pueden incluir el establecimiento de un conjunto de entornos confiables que contengan información de entornos confiables. Cuando la información del entorno de operación del servicio actual coincide con la información de los entornos confiables en el grupo de entornos confiables, las operaciones para determinar el tipo de entorno de operación del servicio actual pueden incluir determinar el entorno de operación del servicio actual como un entorno confiable. Cuando la información del entorno de operación del servicio actual no coincide con la información de los entornos confiables en el grupo de entornos confiables, las operaciones para determinar el tipo de entorno de operación del servicio actual también pueden incluir determinar que el entorno de operación del servicio actual es un entorno no confiable.

15 Las operaciones de establecer el conjunto de entornos confiables que contienen información de entornos confiables pueden incluir el registro de información de los entornos operativos del servicio y la escritura de la información de los entornos operativos del servicio en el conjunto de entornos confiables. Cuando el conjunto de entornos confiables contiene información de un entorno de operación de servicio determinado correspondiente a una operación de un recurso de red exhaustivo realizada por un operador inadecuado, o información de un entorno de operación de servicio determinado correspondiente a una operación de robo, las operaciones de establecimiento del conjunto de Los entornos confiables pueden incluir eliminar la información del entorno de operación del servicio del grupo de entornos confiables.

25 En algunas modalidades, las operaciones de establecer el conjunto de entornos confiables que contienen información de entornos confiables pueden incluir elementos determinantes de la información de entornos confiables relacionados con el conjunto de entornos confiables. Las operaciones de establecer el conjunto de entornos confiables también pueden incluir determinar el peso de cada elemento de acuerdo con la importancia del elemento de la información de entornos confiables para la determinación de un entorno confiable. Las operaciones de establecimiento del conjunto de entornos confiables pueden incluir además el cálculo de un valor ponderado de la información registrada del entorno operativo de acuerdo con los elementos. Cuando el valor ponderado es mayor que un valor preestablecido, las operaciones para establecer el grupo de entornos confiables pueden incluir escribir la información del entorno operativo en el grupo de entornos confiables.

35 Las operaciones de limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro del valor de recurso de primer grado pueden incluir actualizar el valor de recurso del recurso de red exhaustivo cuando falla una operación de la operación de servicio actual. Cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de primer grado, las operaciones de limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro del valor de recurso de primer grado pueden incluir la limitación de cualquier operación adicional del funcionamiento actual del servicio.

40 Una vez que el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de primer grado, el método puede incluir limitar la operación de la siguiente operación de servicio cuando el entorno operativo de la siguiente operación de servicio es un entorno no confiable. El método también puede incluir limitar los tiempos máximos de falla de la operación de la siguiente operación de servicio como la diferencia entre el valor de recurso de segundo grado y el valor de recurso de primer grado del valor de recurso del recurso de red exhaustivo cuando el entorno de operación de la próxima operación de servicio es un entorno confiable.

45 Las operaciones de limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro del valor de recurso de segundo grado pueden incluir actualizar el valor de recurso del recurso de red exhaustivo cuando falla una operación de la operación de servicio actual. Cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de segundo grado, las operaciones de limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro del valor de recurso de segundo grado pueden incluir limitar cualquier operación adicional del funcionamiento actual del servicio.

50 En otro aspecto, la presente divulgación está dirigida a un aparato mediante el uso de un recurso de red exhaustivo. El aparato puede incluir un tipo de unidad de determinación que determina un tipo de entorno de operación del servicio actual. El tipo puede incluir un entorno confiable y un entorno no confiable. La operación del servicio actual puede influir en el valor de los recursos de red exhaustivos. El aparato también puede incluir una primera unidad limitadora que limita el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de primer grado cuando el tipo de entorno de operación de servicio actual es un entorno no confiable. El aparato puede incluir además una segunda unidad limitadora que limita el valor del recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de segundo grado cuando el tipo de entorno de operación de servicio actual es un entorno confiable, el valor de recurso de segundo grado siendo mayor que el valor del recurso de primer grado.

65 Además, el aparato puede incluir un conjunto de entornos confiables que almacenan información de entornos confiables. La unidad de determinación de tipo puede incluir una subunidad de determinación que determina el entorno de operación de servicio actual como un entorno confiable cuando la información del entorno de operación de servicio actual coincide con la información de entornos confiables en el conjunto de entornos confiables. La subunidad de determinación también

puede determinar que el entorno de operación del servicio actual es un entorno no confiable cuando la información del entorno de operación del servicio actual no coincide con la información de los entornos confiables en el conjunto de entornos confiables.

5 Además, la primera unidad limitadora puede incluir una subunidad de actualización que actualiza el valor del recurso del recurso de red exhaustivo cuando falla una operación de la operación de servicio actual. La subunidad limitadora puede limitar cualquier operación adicional de la operación de servicio actual cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el recurso de primer grado.

10 En las modalidades de la presente solicitud, un entorno de operación de servicio se clasifica en un entorno confiable y un entorno no confiable. Un valor de recurso de un recurso de red exhaustivo correspondiente a la operación del servicio actual está limitado por diferentes grados de acuerdo con los diferentes tipos de entornos operativos. En consecuencia, puede reducir o evitar el impacto en el funcionamiento normal del servicio causado por el consumo malintencionado de los recursos de red exhaustivos.

15 Breve descripción de los dibujos

Para ilustrar claramente las soluciones técnicas de acuerdo con las formas de las modalidades de la presente solicitud, los dibujos adjuntos necesarios para describir las formas de las modalidades se introducen brevemente a continuación. Aparentemente, los dibujos que se acompañan a continuación son solo algunas modalidades de la presente solicitud. Los expertos en la técnica pueden obtener otros dibujos de los dibujos adjuntos sin esfuerzos creativos.

La Figura 1 es un diagrama de flujo ilustrativo de un método ilustrativo mediante el uso de recursos de red exhaustivos, de acuerdo con una modalidad de la presente solicitud.

25 La Figura 2 es un diagrama de flujo ilustrativo de un método ilustrativo para establecer un conjunto de entornos confiables, de acuerdo con una modalidad de la presente solicitud.

La Figura 3 es un diagrama de flujo ilustrativo de otro método ilustrativo para establecer un conjunto de entornos confiables, de acuerdo con una modalidad de la presente solicitud.

30 La Figura 4 es un diagrama de flujo ilustrativo de un método ilustrativo mediante el uso de recursos de red exhaustivos, de acuerdo con una modalidad de la presente solicitud.

La Figura 5 es un diagrama de bloques estructural ilustrativo de un aparato ilustrativo mediante el uso de recursos de red exhaustivos, de acuerdo con una modalidad de la presente solicitud.

35 Descripción detallada

Para que los expertos en la técnica comprendan mejor las soluciones técnicas de la presente solicitud, las soluciones técnicas en las modalidades de la presente solicitud se describen clara y completamente con referencia a los dibujos adjuntos en las modalidades de la presente solicitud. Las modalidades descritas son simplemente algunas de las modalidades de la presente solicitud y no todas. Basándose en las modalidades de la presente solicitud, todas las demás modalidades derivadas por personas con conocimientos ordinarios en la técnica sin ningún esfuerzo creativo caerán dentro del alcance de protección de la presente solicitud.

La Figura 1 es un diagrama de flujo ilustrativo de un método ilustrativo mediante el uso de recursos de red exhaustivos, de acuerdo con una modalidad de la presente solicitud. El método puede incluir:

45 Etapa S11: Determinar un tipo de entorno de operación del servicio actual. El tipo puede incluir un entorno confiable y un entorno no confiable. La operación del servicio actual puede influir en el valor de los recursos de red exhaustivos. Cuando el tipo de entorno de operación de servicio actual es un entorno no confiable, el método también puede incluir realizar la Etapa S12. Cuando el tipo de entorno de operación de servicio actual es un entorno confiable, el método puede incluir realizar la Etapa S13.

50 Un usuario de red normalmente necesita realizar una operación de servicio de acuerdo con los requisitos relacionados con el fin de acceder a las funciones de servicio proporcionadas por un proveedor de servicios de red. Por ejemplo, un usuario de red necesita realizar una operación de inicio de sesión para iniciar sesión en un sistema, realizar una operación de autenticación de identidad para utilizar un servicio específico proporcionado por un proveedor de servicios de red, o realizar una operación de descarga para adquirir algunos datos del lado de la red. Estas operaciones de servicio tienen una característica común de que los recursos de red existen de manera correspondiente a estas operaciones. El proceso de operación de cada operación de servicio puede influir en el valor del recurso del recurso de red correspondiente. Este tipo de recursos suele agotarse durante una operación de servicio. En otras palabras, una vez que los recursos se agotan durante un proceso de operación del servicio, estos recursos no se pueden usar en otras operaciones relacionadas. Estos recursos se conocen como recursos de red exhaustivos.

65 Tomando el inicio de sesión en un sistema de correo electrónico como ejemplo, las operaciones de ingresar un nombre de usuario, ingresar una contraseña y presionar un botón de inicio de sesión pertenecen a las operaciones de servicio para completar una operación de inicio de sesión. Existe un recurso de red de intentos de contraseña incorrectos en la operación del servicio. En otras palabras, el número máximo de intentos que se permite ingresar una contraseña incorrecta es un valor establecido de los intentos de contraseña incorrecta. El recurso está preasignado por el sistema de correo

electrónico. El proceso de operación del servicio de un usuario de la red puede influir en el valor de recurso del recurso. Cada vez que se ingresa una contraseña de forma incorrecta, los intentos de contraseña incorrecta preasignados se reducen en uno. Una vez que se ingresa una contraseña correctamente, se eliminan los intentos incorrectos anteriores y se restablece el número de veces. Si los intentos de contraseña incorrecta llegan a los intentos de contraseña incorrecta preasignados en una operación de servicio, el recurso preasignado se agota. La cuenta está bloqueada temporal o permanentemente. Por consiguiente, las operaciones posteriores no se pueden realizar en esta operación de servicio.

Una operación de servicio tiene un entorno de operación de servicio correspondiente. El entorno de operación del servicio puede tener dos propiedades de acuerdo con las situaciones reales, incluido un entorno confiable y un entorno no confiable. El entorno confiable puede incluir: un entorno de operación determinado correspondiente a una operación de un recurso de red exhaustivo realizada por un operador adecuado; un entorno operativo correspondiente durante la recuperación del valor del recurso de segundo grado; o un entorno operativo determinado correspondiente a un funcionamiento normal. Un entorno de operación de servicio opuesto a las situaciones anteriores o situaciones similares puede considerarse un entorno no confiable. Una operación de servicio realizada en un entorno confiable generalmente se considera segura. Puede que no se produzca el problema del uso malintencionado de los recursos de red exhaustivos. Es muy probable que un operador en un entorno no confiable sea determinado como un usuario inadecuado de la operación del servicio (un usuario adecuado incluye un usuario válido y un usuario autorizado de la operación del servicio). En este caso, puede surgir el problema del uso malintencionado de los recursos de red exhaustivos. Después de que los recursos de red exhaustivos se agotan maliciosamente, el usuario adecuado de la operación del servicio tiene que recuperar los recursos agotables mediante un procedimiento complejo. Es posible que deba solicitar un asignador del recurso exhaustivo para la reasignación. Incluso puede ser imposible recuperar los recursos. Esto puede afectar la utilización del servicio por parte del usuario de la red. Por ejemplo, los intentos de contraseña incorrectos se utilizan como recursos de red exhaustivos. Cuando un usuario con intenciones maliciosas de utilizar los intentos de contraseña incorrectos asignados por el sistema, el número de cuenta se bloquea. Un usuario válido de la cuenta de correo electrónico debe desbloquear la cuenta a través de un manual o autoservicio proporcionado por el sistema de servicio de correo electrónico y adquirir nuevos intentos de contraseña incorrecta en una próxima operación de servicio.

Debido a que el entorno de operación del servicio se clasifica en un entorno confiable y un entorno no confiable, la determinación del tipo de entorno de operación de servicio actual puede conducir a dos resultados: uno es que el entorno de operación de servicio actual es un entorno no confiable y el otro es que el entorno actual de operación del servicio es un entorno confiable. En la primera condición, se puede realizar la Etapa S12. En la última condición, se puede realizar la Etapa S13. Las dos etapas proporcionan diferentes usos del valor del recurso de los recursos de red exhaustivos correspondientes a la operación del servicio actual.

Etapa S12: Limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de primer grado.

Etapa S13: Limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de segundo grado. El valor de los recursos de segundo grado puede ser mayor que el valor de los recursos de primer grado.

Para ilustrar la solución técnica en la modalidad de la presente solicitud de forma clara y explícita, a continuación, se describen brevemente varios conceptos. Uno es el funcionamiento del servicio y el funcionamiento específico. La operación de servicio corresponde a una determinada función de servicio y es un concepto general relacionado con la operación específica. Por ejemplo, el inicio de sesión en un sistema de correo electrónico puede considerarse como una operación de servicio, mediante la cual se logra el propósito de ingresar a un sistema de correo electrónico. Sin embargo, la operación del servicio no es un movimiento específico y generalmente está constituida por una serie de operaciones específicas, como ingresar un nombre de usuario, ingresar una contraseña y hacer clic en un botón de inicio de sesión. Además, en cuanto a una operación de servicio de descarga, de manera similar, la operación de servicio de descarga sirve como una operación de servicio general e incluye operaciones específicas, como seleccionar un objeto de descarga, hacer clic en un botón de descarga, seleccionar un destino de almacenamiento y confirmar la descarga. También debe tenerse en cuenta que el servicio en una operación de servicio tiene una amplia gama, no limitada a un tipo específico. Puede ser un servicio de inicio de sesión, un servicio de autenticación de identidad, un servicio de descarga o un servicio de transmisión. En otras palabras, cualquier servicio capaz de lograr una determinada función y proporcionado por un proveedor de servicios de red a un usuario puede considerarse una operación de servicio. Otro concepto son los recursos de red exhaustivos. En esta aplicación, la propiedad de un recurso de red se define como exhaustivo, pero diferente de un recurso natural común que no es absolutamente renovable una vez agotado. En función de la característica de repetibilidad (inagotabilidad) de la información electrónica, un recurso de red agotado puede volverse a adquirir mediante una rutina (procedimiento) específica. Por lo tanto, el concepto de recurso exhaustivo destacado en la presente solicitud tiene un significado relativo. Es decir, como para una operación de servicio, una vez que el recurso exhaustivo se agota en el proceso de operación de servicio, el procedimiento de algunas operaciones es limitado. Tomando el inicio de sesión en un sistema de correo electrónico como ejemplo, cuando los intentos de contraseña incorrectos preasignados por el sistema se agotan en un proceso de operación de servicio, la operación de inicio de sesión de correo electrónico ya no puede realizarse. Es necesario desbloquear la cuenta y adquirir tiempos renovados de intentos de contraseña incorrectos para volver a iniciar sesión en el correo electrónico. De esta forma, los intentos de contraseña incorrectos como recursos son exhaustivos en esta operación de servicio y son recursos de red exhaustivos.

De acuerdo con la introducción anterior del proceso del método mediante el uso de recursos de red exhaustivos en la presente solicitud y la descripción de los términos relacionados, los expertos en la técnica pueden encontrar que la modalidad anterior tiene los siguientes efectos técnicos.

5 En primer lugar, en la modalidad anterior, un entorno de operación de servicio actual puede clasificarse en un entorno confiable y un entorno no confiable. Tal clasificación de los tipos de entorno se ajusta a la situación realista. Las operaciones realizadas en un entorno confiable pueden ser confiables. El consumo de recursos de red exhaustivos en un entorno confiable se considera normal en lugar de malicioso. Por ejemplo, cuando un usuario válido de una cuenta tiene la intención de iniciar sesión en un sistema de correo electrónico, un intento de contraseña incorrecta se considera
10 causado por un mal funcionamiento o una memoria vaga del usuario. Las operaciones realizadas en un entorno no confiable no son confiables. El consumo de recursos de red exhaustivos en esta condición puede ser causado por el hecho de que un usuario inadecuado realiza un inicio de sesión mediante el uso de la cuenta ingresa intencionalmente una contraseña incorrecta para atacar la cuenta, o incluso realiza una operación de descifrado de contraseña mediante el uso de un diccionario de contraseñas. En este caso, el consumo de los recursos de red exhaustivos puede traer problemas al usuario válido. En la modalidad anterior, mediante la determinación del tipo de propiedad del entorno de operación del servicio actual, se puede adoptar una medida correspondiente para excluir el consumo anormal de los recursos de red exhaustivos en la presente solicitud. Sin embargo, en la técnica anterior, no se sabe que puede existir una relación estrecha entre un entorno operativo y recursos de red exhaustivos. Por lo tanto, estas dos propiedades del entorno de operación del servicio actual no se identifican ni distinguen. Cualquier comportamiento que resulte en el
20 consumo de un recurso de red se considera realizado por un usuario válido. Podría dar lugar a un resultado grave porque los recursos de red exhaustivos que pertenecen a un usuario válido se consumen maliciosamente. Para recuperar los recursos (solicitar la reasignación del sistema), el usuario válido tiene que pasar por un complejo procedimiento de proporcionar materiales relacionados para la autenticación de identidad, resolver algunos problemas de autenticación, analizar el grado de correlación con otros usuarios y similares antes de adquirir un recurso. reasignados por el sistema. Por ejemplo, un proceso de desbloqueo de un número QQ actualmente bloqueado puede requerir que el usuario siga estas etapas. Puede hacer perder mucho tiempo y energía al usuario y degradar en gran medida la experiencia del usuario. También puede consumir el recurso de CPU del sistema, aumentar el costo y reducir la eficiencia del sistema debido al establecimiento de un mecanismo de reasignación de recursos, la respuesta a una solicitud de reasignación del usuario válido y la reasignación de los recursos de red exhaustivos.

30 Además, en la modalidad anterior, el valor de recurso de los recursos de red exhaustivos se clasifica en un valor de recurso de primer grado y un valor de recurso de segundo grado. Los diferentes grados corresponden a diferentes valores de recursos y causan diferentes grados de limitación en las operaciones del servicio. Debido a que los valores de recursos de los recursos de red exhaustivos se clasifican por grados, si la propiedad del entorno de operación del servicio actual es un ambiente confiable o un ambiente no confiable se convierte en un factor crítico para decidir la utilización de los recursos de red exhaustivos. En un entorno no confiable, el consumo de los recursos exhaustivos es limitado incluso si ocurre un consumo malintencionado de los recursos de red exhaustivos. Los recursos exhaustivos se pueden consumir hasta el valor de recurso de primer grado como máximo. Los recursos exhaustivos no se agotarían realmente. Un usuario válido al menos tiene la oportunidad de utilizar el recurso exhaustivo. Al menos el usuario válido puede intentar el número
40 de veces igual a la diferencia entre el valor del recurso de segundo grado y el valor del recurso de primer grado. Por lo tanto, el comportamiento de consumo malicioso de un usuario inválido puede no tener un impacto sustancial en el funcionamiento del servicio del usuario válido. Las siguientes dos circunstancias existen en un entorno confiable.

45 A modo de comparación, un caso es que el valor del recurso de segundo grado es igual al valor del recurso encontrado en otros sistemas que no tienen las modalidades descritas en esta solicitud. Por ejemplo, los intentos de contraseña incorrectos podrían establecerse en tres, tanto en la modalidad anterior de la presente divulgación como en estos otros sistemas. Por lo tanto, un usuario válido que se encuentra en un entorno confiable normalmente puede usar los recursos de red exhaustivos de manera inconsciente (teniendo tres posibilidades de ingresar una contraseña de manera incorrecta). Es decir, para el usuario válido, la modalidad anterior logra una transición suave a la solución desde estos otros sistemas. 50 El hecho de que, además del valor del recurso de segundo grado igual al valor del recurso en estos otros sistemas, no cause ninguna influencia, la presente solicitud establece el valor del recurso de primer grado. En este caso, debido a que el valor del recurso de primer grado es menor que el valor del recurso de segundo grado, un usuario no válido que se encuentra en un entorno no confiable ya no tiene tres posibilidades de consumo malicioso como en estos otros sistemas, pero tiene menos de tres oportunidades. Puede evitar hasta cierto punto el impacto causado por el consumo malintencionado del recurso de red.

Otro caso es que el valor del recurso de segundo grado es mayor que el valor del recurso en otros sistemas que no tienen las modalidades descritas en esta solicitud. Por ejemplo, se supone que el valor del recurso de primer grado es tres, que es igual al valor del recurso en estos otros sistemas, mientras que el valor del recurso de segundo grado es cinco. En este escenario, un usuario válido tiene dos posibilidades más de ingresar una contraseña incorrectamente, además del número normal de oportunidades para los recursos de red exhaustivos en estos otros sistemas (es decir, tener tres oportunidades de ingresar una contraseña incorrectamente). Puede mejorar la experiencia del usuario.

60 Aunque la modalidad anterior (denominada en lo sucesivo modalidad básica) puede lograr buenos efectos técnicos en comparación con la técnica anterior, la solución técnica en la modalidad anterior no es inmodificable. Los expertos en la

técnica pueden realizar diversas variaciones o mejoras simples o complejas a la modalidad anterior según los requisitos reales. Es posible obtener más modalidades de la presente solicitud y lograr mejores efectos técnicos.

Por ejemplo, en otra modalidad, las Etapas S12 y S13 en la realización básica pueden no aparecer ambos en una modalidad. Es decir, solo se realizan las Etapas S11 y S12, o solo se realizan las Etapas S11 y S13. La modalidad modificada tiene evidentemente escenarios de aplicación más amplios que la modalidad anterior. En la primera situación (una solución técnica que incluye las Etapas S11 y S12), el método se centra en las operaciones cuando el entorno operativo actual es un entorno no confiable. Solo un entorno de este tipo puede tener efectos negativos sobre los recursos de red exhaustivos. Para una operación en un entorno confiable, un usuario válido de un entorno confiable puede usar recursos de red exhaustivos de la misma manera que en otros sistemas que no tienen las modalidades descritas en esta solicitud. En consecuencia, la complejidad y la dificultad de implementación de toda la solución técnica se reducen en gran medida, y la ocupación del recurso del sistema también se reduce en gran medida. Por otro lado, en la última situación (una solución técnica que incluye las Etapas S11 y S13), el método se centra en las operaciones cuando el entorno operativo actual es un entorno confiable. Solo el consumo de recursos de red exhaustivos por las operaciones en el entorno confiable es efectivo. El consumo malicioso de las operaciones en un entorno no confiable se excluye del rango del valor del recurso de segundo grado. Por lo tanto, no importa si el valor del recurso de segundo grado es idéntico o diferente del valor del recurso en la técnica anterior, esta solución es superior al enfoque de la técnica anterior en el que se considera que el consumo de un recurso de red se realiza por un usuario válido sin importar en un entorno confiable o un entorno no confiable.

En otra modalidad de la presente solicitud, se puede adoptar un método ilustrativo que se describe a continuación para realizar el Etapa S11 en la realización básica (determinar el tipo de entorno operativo actual): establecer un conjunto de entornos confiables que incluyen información de entorno confiable. Al determinar el tipo de entorno operativo actual, el método puede incluir hacer coincidir la información adquirida del entorno operativo actual con la información del entorno confiable almacenada en el conjunto de entornos confiables. Cuando hay una coincidencia, el método puede incluir determinar que el entorno de operación actual es un entorno confiable. De lo contrario, el método puede incluir la determinación de que el entorno operativo actual es un entorno no confiable. El emparejamiento puede ser en un modo completamente igual o conteniendo. Por ejemplo, la información de un entorno operativo confiable en el grupo de entornos confiables puede incluir: mediante el uso de un sistema operativo N, una dirección de un dispositivo de red que sea OFFE y una dirección IP que sea 168.192.03.4. Cuando la información del entorno operativo actual también incluye: mediante el uso de un sistema operativo N, una dirección de un dispositivo de red que es OFFE y una dirección IP que es 168.192.03.4, se determina que el entorno operativo actual es un entorno confiable en un entorno completamente igual. modo. Cuando la información del entorno operativo actual incluye: mediante el uso de un sistema operativo N y una dirección IP que sea 168.192.03.4. No hay una coincidencia completa. Si se determina que el entorno de operación actual es un entorno confiable o un entorno no confiable puede depender de un umbral de coincidencia preestablecido. Cuando un grado de coincidencia preestablecido solo requiere que dos elementos sean idénticos, el entorno operativo actual puede determinarse como un entorno confiable. Este tipo de coincidencia es un modo contenedor.

En algunas modalidades, el enfoque para establecer un conjunto de entornos confiables puede ilustrarse adicionalmente mediante dos métodos ilustrativos que se proporcionan a continuación.

La Figura 2 es un diagrama de flujo ilustrativo de un método ilustrativo para establecer un conjunto de entornos confiables, de acuerdo con una modalidad de la presente solicitud.

S211: Registrar la información de los entornos de operación del servicio y escriba la información de los entornos de operación del servicio en el grupo de entornos confiables.

La información registrada de los entornos operativos puede incluir información de todos los entornos operativos, incluidos algunos entornos operativos que en realidad pueden no ser fiables. Por lo tanto, esta Etapa es principalmente para la inicialización del grupo de entornos confiables. En algunas modalidades, cuando se determina con certeza que un entorno operativo es un entorno confiable en esta Etapa, el entorno operativo puede registrarse en el conjunto de entornos confiables y marcarse específicamente. Es posible que todos los entornos de operación específicamente marcados no necesiten pasar por el proceso de selección posterior.

S212: Determinar si el conjunto de entornos confiables contiene la siguiente información de los entornos de operación del servicio: información de un entorno de operación de servicio determinado correspondiente a una operación de un recurso de red exhaustivo realizada por un operador inadecuado, o información de un entorno de operación de servicio determinado correspondiente a un robo operación. Cuando el conjunto de entornos confiables contiene uno de los dos tipos de información, el método puede incluir realizar Etapa S213.

En esta Etapa, se examinan los entornos de operación en el grupo de entornos confiables. Las reglas de selección pueden diversificarse. Un entorno de operación en el grupo de entornos confiables que satisfaga una regla de detección preestablecida se mantendrá en el grupo de entornos confiables. De lo contrario, el entorno operativo se elimina del conjunto de entornos confiables mediante la Etapa S213. En algunas modalidades, la regla de cribado puede incluir: la información del entorno de operación del servicio determinado correspondiente a una operación de un recurso de red exhaustivo realizada por una operación incorrecta. Esta regla de selección puede determinar si un entorno de operación

es confiable o no de acuerdo con la identidad de un operador del entorno de operación. Cuando el operador es un operador inadecuado (por ejemplo, un operador inválido o un operador no autorizado) de los recursos de red exhaustivos, se determina que el entorno de operación es un entorno de operación no confiable. De lo contrario, se determina que el entorno operativo es un entorno operativo confiable. La regla de selección puede incluir, además: la información del entorno de operación de servicio determinado correspondiente a una operación de robo. Esta regla de selección puede determinar si el entorno de operación es confiable o no desde el aspecto de la operación. Por ejemplo, si un usuario proporciona información relacionada en la correspondencia para cambiar o recuperar correctamente la contraseña, el entorno operativo en el que se introdujo correctamente la contraseña la última vez es un entorno operativo de robo. Puede determinarse que es un entorno de operación poco confiable.

S213: Eliminar la información del entorno de operación del servicio del grupo de entornos confiables.

La Figura 3 es un diagrama de flujo ilustrativo de otro método ilustrativo para establecer un conjunto de entornos confiables, de acuerdo con una modalidad de la presente solicitud.

Etapas S311: Determinar elementos de la información de entornos confiables afectados por el conjunto de entornos confiables.

Etapas S312: Determinar el peso de cada elemento de acuerdo con la importancia del elemento de información de ambientes confiables para la determinación de un ambiente confiable.

Etapas S313: Calcular un valor ponderado de la información registrada del entorno operativo de acuerdo con los elementos.

Etapas S314: Escribir la información del entorno de operación en el grupo de entornos confiables cuando el valor ponderado sea mayor que un valor preestablecido.

En otra modalidad de la presente solicitud, las Etapas S12 y S13 en la realización básica tienen sus propias formas de implementación específicas. Por ejemplo, la Etapa de limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro del valor de recurso de primer grado puede incluir: actualizar el valor de recurso del recurso de red exhaustivo cuando falla una operación de la operación de servicio actual. Cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de primer grado, la Etapa puede incluir limitar cualquier operación adicional de la operación de servicio actual. Asimismo, la Etapa de limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro del valor de recurso de segundo grado puede incluir: actualizar el valor de recurso del recurso de red exhaustivo cuando falla una operación de la operación de servicio actual. Cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de segundo grado, la Etapa puede incluir limitar cualquier operación adicional de la operación de servicio actual. En la situación anterior, cuando el bloqueo se debe a entornos poco confiables, puede ocurrir la siguiente situación. Se puede realizar una operación de servicio nuevamente, y el enfoque para limitar la operación de servicio puede diferir de acuerdo con el tipo de propiedad del siguiente entorno de operación de servicio. Cuando el entorno de operación de la siguiente operación de servicio es un entorno no confiable, indica que es probable que el recurso de red se consuma maliciosamente porque el bloqueo de los recursos de red exhaustivos es causado por la operación anterior en un entorno no confiable. Por lo tanto, la siguiente operación de la operación del servicio actual debe limitarse a detener el comportamiento de un operador de mala intención. Cuando el entorno operativo de la siguiente operación de servicio es un entorno confiable, la operación de servicio la realiza un usuario válido. Si la utilización de los recursos de red exhaustivos por parte del usuario válido es limitada, es injusto para el usuario válido. La trama del usuario inválido tiene éxito. Por lo tanto, deben aumentarse los tiempos de falla máximos de la operación específica de la operación del servicio. El usuario válido al menos tiene posibilidades. El número de oportunidades puede ser igual a la diferencia entre el valor de los recursos de segundo grado y el valor de los recursos de primer grado de los recursos de red exhaustivos.

Se realizan variaciones o mejoras a la modalidad básica en varios aspectos para obtener una serie de nuevas modalidades. Para ilustrar más la solución técnica de la presente solicitud, a continuación, se proporciona un ejemplo específico para su descripción. En este ejemplo, se supone que la operación del servicio es iniciar sesión en una cuenta. Los recursos de red exhaustivos son intentos de contraseña incorrectos. El valor de los recursos de primer grado es C1 y el valor de los recursos de segundo grado es C2. La Figura 4 ilustra el diagrama de flujo de un método ilustrativo mediante el uso de recursos de red exhaustivos, de acuerdo con una modalidad de la presente solicitud.

Etapas S41: Iniciar una operación de servicio de una cuenta.

Etapas S42: Adquirir información del entorno de operación del servicio de la operación del servicio actual y enviar el ID de cuenta y la información del entorno de operación del servicio a un grupo de entornos confiables.

Etapas S43: Hacer coincidir el entorno de operación del servicio con un entorno de operación confiable correspondiente a la cuenta en el grupo de entornos confiables. Si no hay coincidencia, realizar la Etapa S44. Si hay una coincidencia, realizar la Etapa S49.

Etapas S44: Determinar si la cuenta está bloqueada. Si es así, realizar la Etapa S54. Si no es así, realizar la Etapa S45.

Etapa S45: Realizar una operación de ingreso de contraseña. Si la contraseña se ingresa correctamente, realizar la Etapa S46. Si la contraseña se ingresa incorrectamente, realizar la Etapa S47.

Etapa S46: Restablezca los intentos de contraseña incorrectos y finalice el proceso.

Etapa S47: Aumentar los intentos de contraseña incorrecta en 1 y realizar la Etapa S48.

Etapa S48: Determinar si los intentos de contraseña incorrectos llegan a C1. Si es así, ejecute S48a para bloquear la cuenta y finalizar el proceso. Si no es así, vuelva a la Etapa S45.

Etapa S49: Determinar si la cuenta está profundamente bloqueada. Si es así, realizar la Etapa S54. Si no es así, realizar la Etapa S50.

Etapa S50: Realizar una operación de ingreso de contraseña. Si la contraseña se ingresa correctamente, realizar la Etapa S51. Si la contraseña se ingresa incorrectamente, realizar la Etapa S52.

Etapa S51: Restablecer los intentos de contraseña incorrectos y finalice el proceso.

Etapa S52: Aumentar los intentos de contraseña incorrecta en 1 y realizar la Etapa S53.

Etapa S53: Determinar si los intentos de contraseña incorrectos llegan a C2. En caso afirmativo, realizar la Etapa S53a para bloquear profundamente el número de cuenta y finalizar el proceso. Si no es así, vuelva a la Etapa S50.

Etapa S54: Indicar que la operación falla y finalice el proceso.

La modalidad del método mediante el uso de recursos de red exhaustivos de acuerdo con la presente solicitud se describe anteriormente en detalle. En otro aspecto, la presente solicitud divulga además una modalidad ilustrativa de un aparato, mediante el uso de recursos de red exhaustivos. La Figura 5 ilustra un diagrama de bloques estructural de un aparato ilustrativo, mediante el uso de recursos de red exhaustivos, de acuerdo con una modalidad de la presente solicitud. El aparato puede incluir una unidad de determinación de tipo U51, una primera unidad limitadora U52 y una segunda unidad limitadora U53.

La unidad de determinación de tipo U51 está configurada para determinar el tipo de entorno de operación del servicio actual. El tipo puede incluir un entorno confiable y un entorno no confiable. La operación del servicio actual puede influir en el valor de los recursos de red exhaustivos.

La primera unidad limitadora U52 está configurada para limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de primer grado cuando el tipo de entorno de operación de servicio actual es un entorno no confiable.

La segunda unidad limitadora U53 está configurada para limitar el valor de recurso del recurso de red exhaustivo de la operación de servicio actual dentro de un valor de recurso de segundo grado cuando el tipo de entorno de operación de servicio actual es un entorno confiable. El valor de los recursos de segundo grado puede ser mayor que el valor de los recursos de primer grado.

El proceso de trabajo de la modalidad del aparato es el siguiente: la unidad de determinación de tipo U51 determina el tipo de entorno de operación del servicio actual. Cuando el entorno de operación actual es un entorno no confiable, la primera unidad limitadora U52 se activa para limitar el valor de recurso de los recursos de red exhaustivos de la operación de servicio actual dentro del valor de recurso de primer grado. Cuando el tipo de entorno de operación de servicio actual es un entorno confiable, se activa la segunda unidad limitadora U53 para limitar el valor de recurso de los recursos de red exhaustivos de la operación de servicio actual dentro del valor de recurso de segundo grado.

La modalidad del aparato puede lograr los mismos efectos técnicos que las modalidades del método. En resumen, la modalidad del aparato puede reducir o evitar el impacto en el funcionamiento normal del servicio de un usuario válido que resulta del uso de recursos de red exhaustivos por parte de un usuario con malas intenciones. Las Etapas y operaciones detallados pueden referirse a los de las modalidades del método anteriores.

Sobre la base de la modalidad del aparato, los expertos en la técnica pueden realizar diversas modificaciones. Por ejemplo, se pueden proporcionar la primera unidad limitadora U52 y la segunda unidad limitadora U53 en la modalidad del aparato, o se puede proporcionar cualquiera de ellas. La modalidad del aparato puede incluir además un conjunto de entornos confiables U54 para almacenar información de un entorno confiable. La unidad de determinación de tipo U51 puede incluir una subunidad de determinación U511 para determinar el entorno de operación de servicio actual como un entorno confiable cuando la información del entorno de operación de servicio actual coincide con la información de entornos confiables en el conjunto de entornos confiables. Cuando la información del entorno de operación del servicio actual no coincide con la información de los entornos confiables en el grupo de entornos confiables, la determinación de la subunidad U511 determina el entorno de operación del servicio actual como un entorno no confiable. La primera unidad

limitadora U52 puede incluir una subunidad de actualización U521 y una subunidad limitadora U522. La subunidad de actualización U521 puede configurarse para actualizar el valor de recurso del recurso de red exhaustivo cuando falla una operación de la operación de servicio actual. La subunidad limitadora U522 puede configurarse para limitar cualquier operación adicional de la operación de servicio actual cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el recurso de primer grado.

Cabe señalar que las modalidades anteriores de la especificación y diversas implementaciones alternativas de las modalidades se centran en las diferencias con las otras modalidades o implementaciones alternativas. Se puede hacer referencia entre sí para partes idénticas o similares en diversas circunstancias. Especialmente, al ser sustancialmente similar a la modalidad del método, algunas variaciones de la modalidad del aparato se describen de forma sencilla. Se puede hacer referencia a las descripciones correspondientes en las modalidades del método para las partes relacionadas. Las unidades en las modalidades del aparato descritas anteriormente pueden estar o no separadas físicamente, y pueden disponerse en un lugar o distribuirse a múltiples entornos de red. En la aplicación real, algunas o todas las unidades pueden seleccionarse para lograr el objetivo de la solución de la modalidad de acuerdo con las demandas reales. Las personas con conocimientos ordinarios en la técnica pueden comprender e implementar la presente divulgación sin esfuerzos creativos.

Las descripciones anteriores son simplemente implementaciones específicas de la presente solicitud. Cabe señalar que las personas con conocimientos ordinarios en la técnica pueden realizar diversas modificaciones y variaciones sin apartarse del principio de la presente solicitud. Todas estas modificaciones y variaciones caerán dentro del alcance de protección de la presente solicitud.

REIVINDICACIONES

1. Un método para limitar el acceso a una cuenta basada en la red, el método que comprende:
determinar (S11) un tipo de entorno de operación de servicio actual, en el que se está realizando una operación de servicio de inicio de sesión, en donde el tipo de entorno de operación de servicio actual es un entorno confiable o un entorno no confiable,
si el tipo de entorno de operación del servicio actual es un entorno no confiable:
limitar (S12) un valor de recurso de un recurso de red exhaustivo de la operación del servicio de inicio de sesión dentro de un valor de recurso de primer grado,
actualizar el valor del recurso en respuesta a un error de inicio de sesión y
cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de primer grado, se limita cualquier operación de servicio de inicio de sesión adicional desde el entorno no confiable de cualquier otra manera:
limitar (S13) el valor de recurso del recurso de red exhaustivo de la operación del servicio de inicio de sesión dentro de un valor de recurso de segundo grado, el valor de recurso de segundo grado que es mayor que el valor de recurso de primer grado;
actualizar el valor del recurso en respuesta a un error de inicio de sesión; y
cuando el recurso de la red exhaustivo se ha agotado según lo indicado por el valor de recurso actualizado que alcanza el valor de recurso de segundo grado y el entorno de operación del servicio actual es confiable, se limita cualquier operación de servicio de inicio de sesión adicional,
en donde el recurso de red exhaustivo son intentos de contraseña incorrectos y
en donde la operación del servicio de inicio de sesión es un servicio de inicio de sesión capaz de acceder a una cuenta proporcionada por un proveedor de servicios de red.
2. El método de la reivindicación 1, en donde determinar el tipo de entorno de operación del servicio actual incluye:
establecer un grupo de entornos confiables que contengan información de entornos confiables; y
cuando la información del entorno de operación del servicio actual coincide con la información de los entornos confiables en el grupo de entornos confiables, determinar el entorno de operación del servicio actual como un entorno confiable; o
cuando la información del entorno de operación del servicio actual no coincide con la información de los entornos confiables en el grupo de entornos confiables, determinar el entorno de operación del servicio actual es un entorno no confiable.
3. El método de la reivindicación 2, en donde establecer el conjunto de entornos confiables que contienen información de entornos confiables incluye:
registrar (S211) información de los entornos de operación del servicio y escribir la información de los entornos de operación del servicio en el grupo de entornos confiables; y
cuando el conjunto de entornos confiables contiene información de un entorno de operación de servicio determinado correspondiente a una operación de un recurso de red exhaustivo realizada por un operador inadecuado, o información de un entorno de operación de servicio determinado correspondiente a una operación de robo, eliminar (S213) la información del entorno de operación del servicio del conjunto de entornos confiables.
4. El método de la reivindicación 2, en donde se establece el conjunto de entornos confiables que contienen información de entornos confiables incluye:
determinar (S311) elementos de la información de entornos confiables afectados por el conjunto de entornos confiables;
determinar (S312) el peso de cada elemento de acuerdo con la importancia del elemento de la información de ambientes confiables para la determinación de un ambiente confiable;
calcular (S313) un valor ponderado de la información registrada del entorno de operación de acuerdo con los elementos; y
cuando el valor ponderado es mayor que un valor preestablecido, escribir (S314) la información del entorno de operación en el grupo de entornos confiables.
5. El método de la reivindicación 1, en donde después de que el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de primer grado:
cuando el entorno operativo de la siguiente operación de servicio es un entorno no confiable, se limita la operación de la siguiente operación de servicio de inicio de sesión; y/o
cuando el entorno operativo de la siguiente operación del servicio de inicio de sesión es un entorno confiable, limitar los tiempos máximos de falla de la operación de la siguiente operación del servicio de inicio de sesión como la diferencia entre el valor del recurso de segundo grado y el valor del recurso de primer grado del valor del recurso del recurso de red exhaustivo.
6. El método de la reivindicación 1, en donde limitar el valor de recurso del recurso de red exhaustivo de la operación del servicio de inicio de sesión dentro del valor de recurso de segundo grado incluye:
cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de segundo grado, limitar cualquier operación de servicio de inicio de sesión adicional.

7. El método de cualquiera de las reivindicaciones 1 a 6, en donde el entorno confiable incluye:
un entorno de operación determinado correspondiente a una operación de un recurso de red exhaustivo realizada por un operador adecuado;
5 un entorno operativo correspondiente durante la recuperación del valor del recurso de segundo grado; o
un entorno de operación determinado correspondiente a un funcionamiento normal.
8. Un aparato para limitar el acceso a una cuenta basada en la red, el aparato que comprende:
10 una unidad de determinación de tipo (U51) configurada para determinar (S11) un tipo de entorno de operación de servicio actual, en el que se realiza una operación de servicio de inicio de sesión, en donde el tipo de entorno de operación de servicio actual es un entorno confiable o un entorno no confiable;
una primera unidad limitadora (U52) configurada para limitar (S12) un valor de recurso del recurso de red exhaustivo de la operación del servicio de inicio de sesión dentro de un valor de recurso de primer grado cuando el tipo de entorno de operación de servicio actual es un entorno no confiable; y
15 una segunda unidad limitadora (U53) configurada para limitar (S13) el valor de recurso del recurso de red exhaustivo de la operación del servicio de inicio de sesión dentro de un valor de recurso de segundo grado cuando el tipo de entorno de operación de servicio actual es un entorno confiable, el valor de recurso de segundo grado es mayor que el valor del recurso de primer grado,
20 en donde, el aparato está configurado además para, cuando falla la operación del servicio de inicio de sesión, actualizar el valor del recurso del recurso de red exhaustivo y cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el valor de recurso de primer grado y la operación de servicio actual el entorno no es confiable, el aparato se configura además para limitar el funcionamiento adicional de las operaciones del servicio de inicio de sesión desde dentro del entorno no confiable;
25 y cuando el recurso de red exhaustivo se ha agotado según lo indicado por el valor de recurso actualizado que alcanza el valor de recurso de segundo grado, y el entorno de operación del servicio actual es confiable, el dispositivo se configura para limitar cualquier operación de servicio de inicio de sesión adicional, y en donde los recursos de red exhaustivos es intentos de contraseña incorrectos; y
en donde la operación del servicio de inicio de sesión es un servicio capaz de lograr acceso a una cuenta proporcionada por un proveedor de servicios de red.
30
9. El dispositivo de acuerdo con la reivindicación 8, que comprende, además:
un grupo de entornos confiables (U54) configurado para almacenar información de entornos confiables,
en donde la unidad de determinación de tipo incluye:
35 una subunidad de determinación (U511) configurada para:
determinar el entorno de operación del servicio actual como un entorno confiable cuando la información del entorno de operación del servicio actual coincida con la información de los entornos confiables en el grupo de entornos confiables; o
determinar que el entorno de operación del servicio actual es un entorno no confiable cuando la información del entorno de operación del servicio actual no coincida con la información de los entornos confiables en el grupo de entornos confiables.
40
10. El aparato de la reivindicación 8, en donde la primera unidad limitadora (U52) incluye:
una subunidad de actualización (U521) configurada para actualizar el valor de recurso del recurso de red exhaustivo cuando falla una operación del servicio de inicio de sesión; y
45 la subunidad limitadora (U522) configurada para limitar cualquier operación de servicio de inicio de sesión adicional cuando el valor de recurso actualizado del recurso de red exhaustivo alcanza el recurso de primer grado.

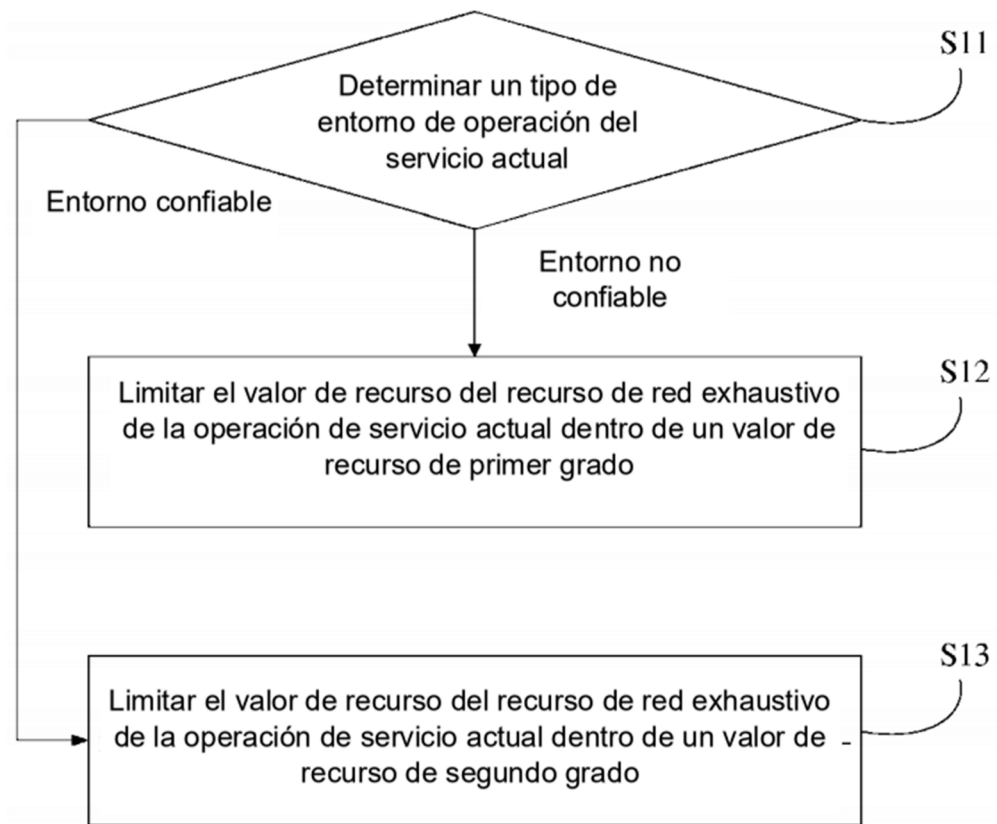


Figura 1

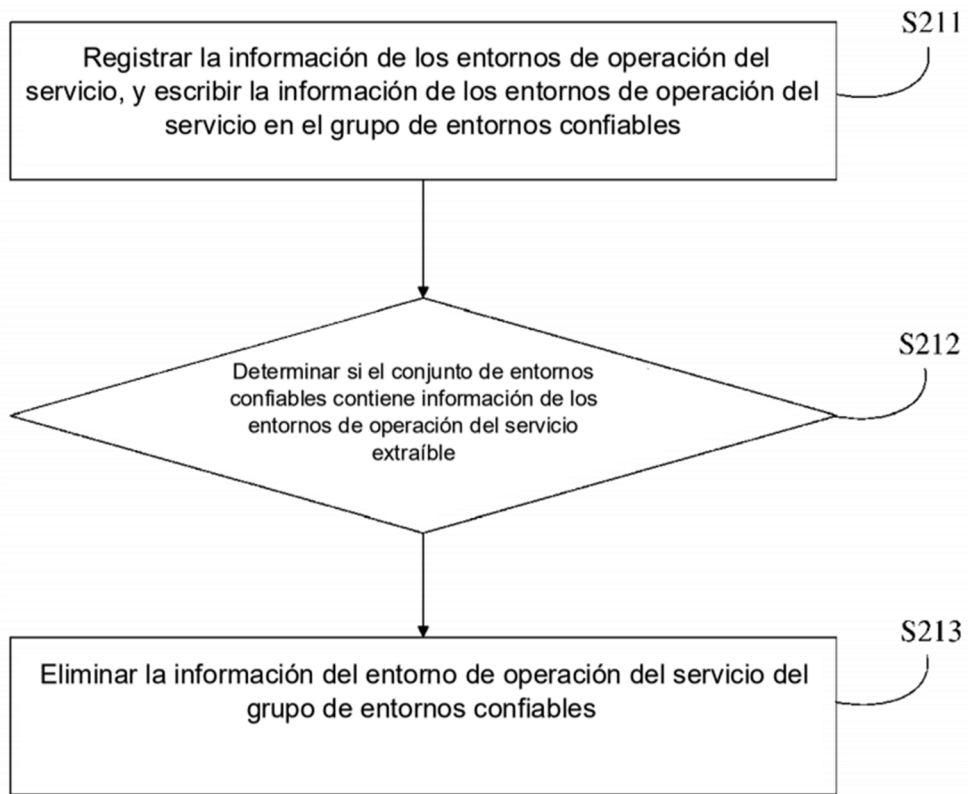


Figura 2

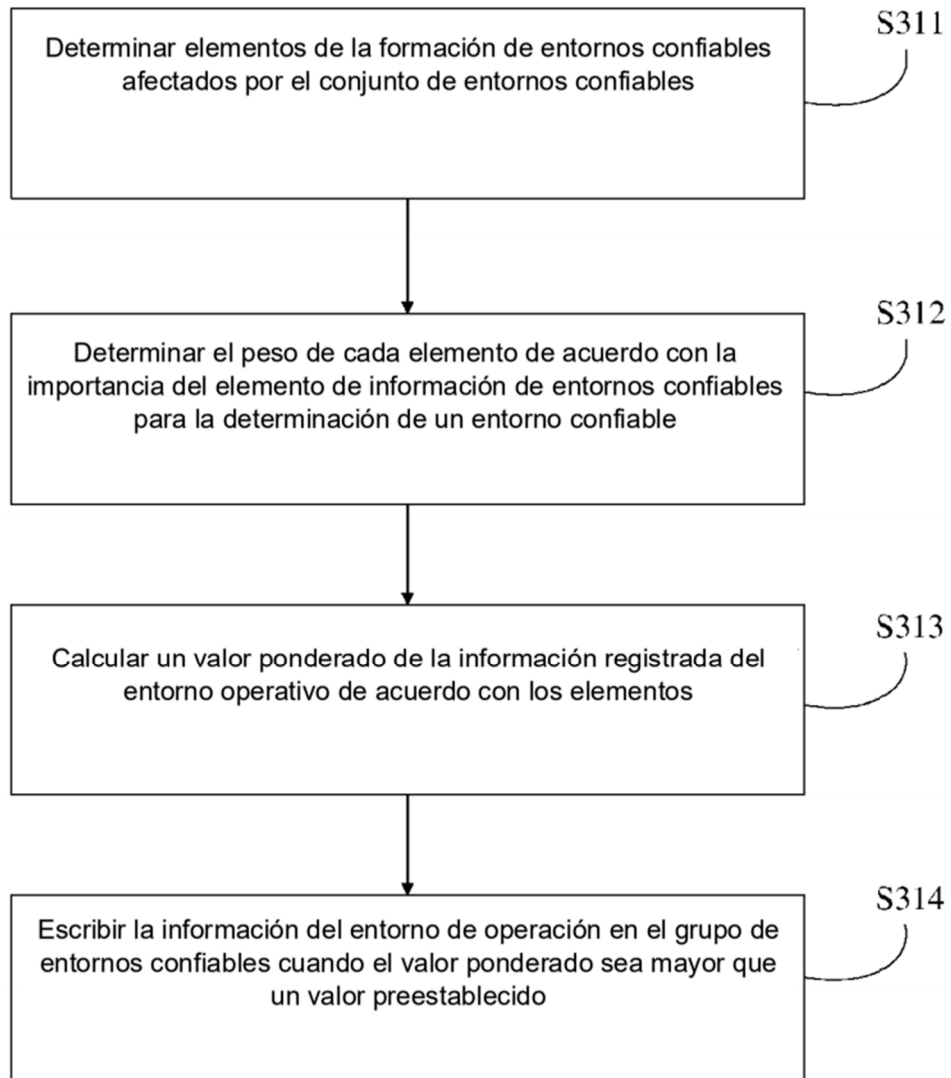


Figura 3

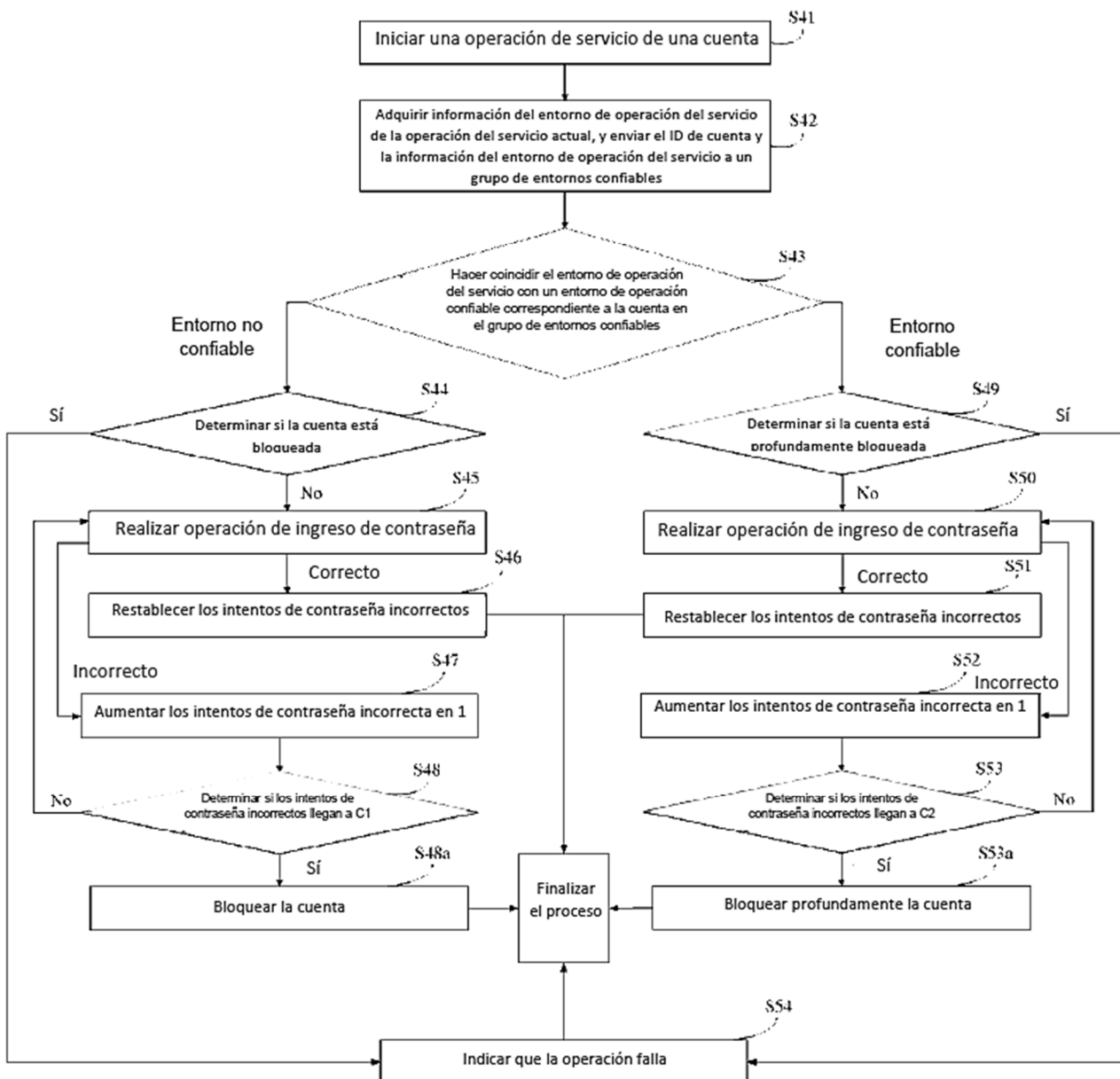


Figura 4

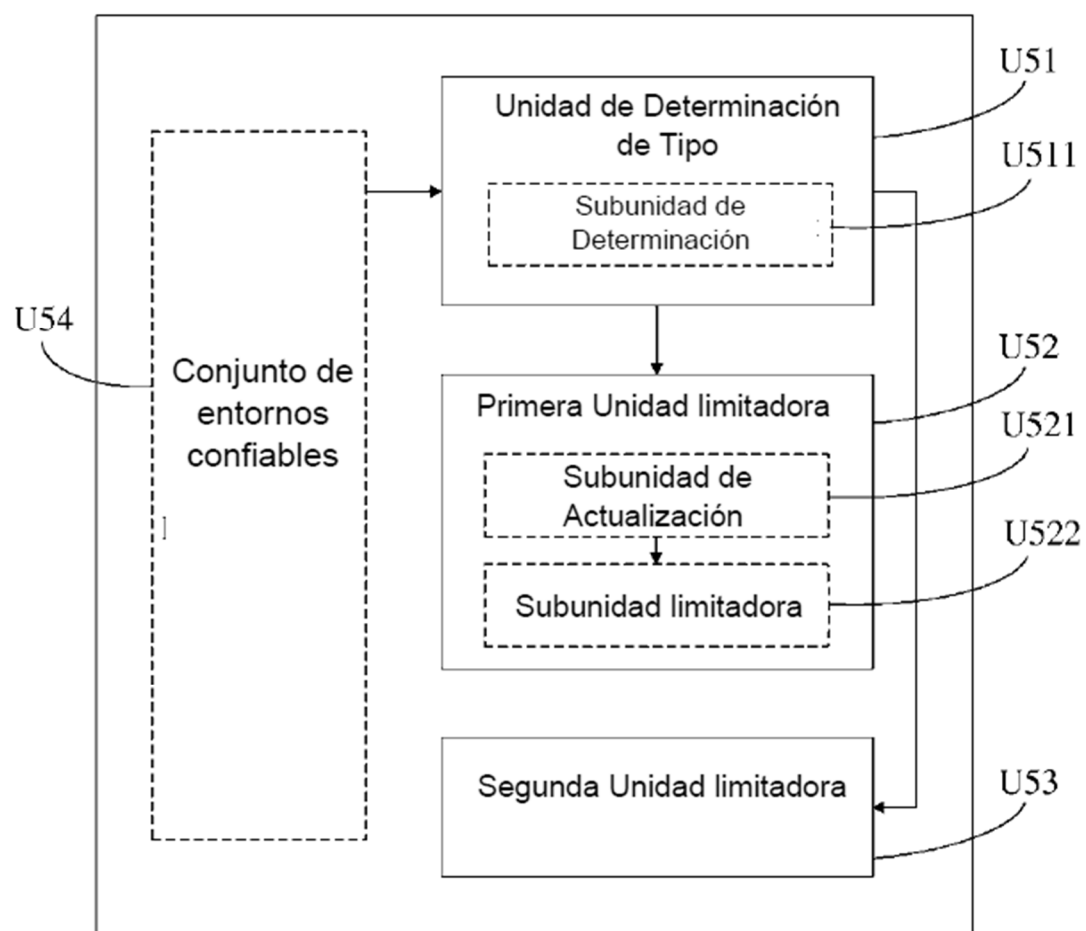


Figura 5