(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 762 373**

(51) Int. CI.:

G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.10.2014 E 14189367 (7)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3009950**

(54) Título: **Procedimiento y aparato para la autenticación local continua e implícita de usuarios de móviles inalámbricos basada en el perfilado dinámico de patrones de conducta**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.05.2020

(73) Titular/es:

FUNDACIÓ EURECAT (50.0%)
Parc Tecnològico del Vallès, Avenida Universitat Autònoma 23
08290 Cerdanyola del Vallès, ES y
CAIXABANK S.A. (50.0%)

(72) Inventor/es:

PAREDES, IGNASI;
PARRA, JAVIER;
REYES, MARIO y
MAAWAD, MARIO

(74) Agente/Representante:

MOHAMMADIAN SANTANDER, Dario

DESCRIPCIÓN

Procedimiento y aparato para la autentificación local continua e implícita de usuarios de móviles inalámbricos basada en el perfilado dinámico de patrones de conducta

CAMPO TÉCNICO

La presente invención se emplaza generalmente en el campo de la seguridad y control de acceso de dispositivos móviles inalámbricos, y en particular, a mejorar la autenticación de usuarios inalámbricos.

ANTECEDENTES DE LA INVENCIÓN

Durante los últimos años, la penetración global de teléfonos inteligentes conectados a Internet ha incrementado considerablemente. En consecuencia, la cantidad de riesgos y vulnerabilidades asociadas han incrementado de forma análoga dada la lista constantemente creciente de aplicaciones disponibles, desde el chatting hasta los correos electrónicos y la banca electrónica. Existen ciertos tipos de aplicaciones, como la banca electrónica, o el comercio electrónico, que tratan información extremadamente sensible. En cambio, desde el punto de vista de la seguridad, estas aplicaciones todavía dependen sobre todo únicamente en autenticaciones basadas en contraseñas, haciéndolas vulnerables a ataques, como a imitaciones a partir de credenciales robadas.

Las aproximaciones biométricas, es decir, la autenticación basada en, por ejemplo, el reconocimiento de voz, el reconocimiento facial, o las huellas dactilares, han existido durante años, pero no han sido completamente integrados en la prevaleciente electrónica de consumidor dada su complejidad y precio. La publicación WO-A-2013/155 143 se refiere a la autenticación basada en la ubicación previa de un dispositivo, divulgando la generación de un patrón de uso familiar a partir de la recolección de información de ubicación, y conceder acceso al usuario del dispositivo siempre que la ubicación del dispositivo se corresponda con el patrón de uso familiar. La publicación EP-A-2629228 se refiere a un protocolo de seguridad dependiente de la ubicación para un dispositivo electrónico portable en el que, cuando un usuario intenta acceder al dispositivo o a una aplicación del dispositivo, el dispositivo implementa un primer proceso de autenticación si el dispositivo se encuentra en una de las áreas familiares, o un proceso de autenticación diferente si el dispositivo no se encuentra en una de las áreas familiares. La publicación US-A-2010/175116 se refiere a la comparación de las características de uso o movilidad de un dispositivo electrónico (por ejemplo, la ubicación) con parámetros actuales. Una determinación de si permitir una operación (por ejemplo, acceso, transacción de comercio electrónico) en el dispositivo se puede basar al menos en parte sobre el grado de conformación de los parámetros actuales con las características de uso o movilidad.

Se ha propuesto también la autenticación implícita como una solución al control de acceso. La autenticación implícita elimina esencialmente la necesidad de utilizar contraseñas o datos biométricos y se enfoca exclusivamente sobre el comportamiento de usuario. Mediante la autenticación implícita se identifica al usuario simplemente reconociendo su comportamiento, sin ninguna solicitud de autenticación explícita. Esta aproximación es más robusta que las propuestas anteriores de autenticación explícita dadas las múltiples variables que identifican a una persona o usuario. Dada esta cantidad grande de información personal, se debería falsificar cuidadosamente un número elevado de variables para suplantar la identidad de una persona (por ejemplo, ubicación, últimas llamadas, lista de pagos, las aplicaciones más usadas, las preferencias de usuario, las ubicaciones frecuentes, las personas recurrentemente contactadas, y demás).

Una desventaja de este nuevo mecanismo es que se lleva a cabo de forma remota, que plantea serios riesgos de seguridad y privacidad dados principalmente por la conexión de datos normalmente insegura y la cantidad elevada de datos y variables relacionada con usuarios intercambiada sobre estas conexiones inseguras. En otras palabras, se pone en peligro la confidencialidad de la información sensible y privada de los usuarios. Como depende del intercambio de datos con un servidor remoto, en caso de que el dispositivo inalámbrico se encuentre sin comunicación externa, pierde toda capacidad de autenticación implícita.

Además, dada su naturaleza remota, tal autenticación se lleva a cabo bajo demanda, es decir, solamente valida que un usuario es legítimo una vez que un recurso remoto se accede, ni antes ni después. Por lo tanto, no es generalmente fiable, ya que se utiliza una cantidad pequeña de datos de comportamiento que, más frecuentemente que no, están caducados.

Otra desventaja es que requiere que el usuario autorice explícitamente las actualizaciones de modelo. En otras palabras, el modelo no integra de forma automática los cambios de conducta del usuario. En tales situaciones, la autenticación falla ya que el mecanismo no reconoce al usuario legítimo, y asume que los cambios en la información relacionada con el usuario son debidos a un acceso no autorizado por un usuario no legítimo, resultando en muchas determinaciones de falsos negativos. Considerando el número de aplicaciones que se ejecutan actualmente en tiempo real en los dispositivos de teléfono inteligente, o dispositivos similares, se

necesitan numerosas solicitudes de autenticación explícita, resultando en un mecanismo de autenticación engorroso y no fácil de utilizar para los usuarios.

Por lo tanto, existe la necesidad de solventar de forma efectiva estos problemas anteriormente mencionados.

RESUMEN

Es por lo tanto un objeto de la presente invención proporcionar soluciones a los problemas anteriormente descritos. En particular, es un objetivo de la invención proporcionar una autenticación implícita mejorada a usuarios de dispositivos de comunicación inalámbrica en el que los problemas descritos se han resuelto. Esto se consigue llevando a cabo de forma continua la autenticación implícita y siempre de forma local en el dispositivo. Esto quiere decir que la identidad de usuario se verifica localmente continuamente mientras se usa el dispositivo, no solamente cuando se está accediendo a un servicio remoto.

Esto es más seguro que las propuestas anteriores ya que:

1. Evita enviar información sensible sobre una conexión de datos. El usuario no tiene por qué confiar en una entidad externa, como un servidor de autenticación o un operador de red. Es, por lo tanto, más seguro.

2. Funciona incluso en situaciones de aislamiento, sin capacidad de comunicación externa. Esto se debe a que el proceso de autenticación se lleva a cabo de forma local y el dispositivo no necesita establecer una conexión con un operador de red. Es, por lo tanto, más robusto.

3. Proporciona más precisión que la autenticación bajo demanda ya que es capaz de determinar continuamente, utilizando una gran cantidad de información de usuario recientemente actualizada, si el usuario actual del dispositivo móvil tiene permiso de utilizar el teléfono inalámbrico o no. Es, por lo tanto, más preciso.

4. Se adapta de forma dinámica al comportamiento del usuario, y por lo tanto, identifica automáticamente cambios de comportamiento significantes por el mismo usuario sin necesidad de solicitar confirmación. Con lo cual se refleja el comportamiento más reciente en tiempo real, eliminando las imprecisiones de los modelos estáticos y proporcionando una autenticación más fácil y menos engorroso para el usuario. Es, por lo tanto, más fácil se operar.

Por lo tanto, la invención proporciona una autenticación de usuario mejorada que es fácil de usar, más segura, precisa y robusta.

Por eso, es un objeto de la presente invención proporcionar un aparato en un dispositivo de comunicación inalámbrica para la autenticación de usuario mejorada.

Es otro objeto de la presente invención proporcionar un procedimiento para la autenticación de usuario mejorada en un dispositivo de comunicación inalámbrica.

Es otro objeto de la invención proporcionar un medio legible por ordenador que comprende instrucciones, que una vez ejecutadas en un procesador, llevan a cabo las etapas de un procedimiento para la autenticación de usuario mejorada en un dispositivo de comunicación inalámbrica.

La invención proporciona procedimientos y dispositivos que implementan varios aspectos, realizaciones, y características de la invención, y se implementan mediante medios variados. Los medios variados pueden comprender, por ejemplo, hardware, software, firmware, o una combinación de los mismos, y se pueden implementar estas técnicas en cualquier una, o combinación de, los medios variados.

Para una implementación hardware, los medios variados pueden comprender unidades de procesamiento implementados en uno o más circuitos integrados de aplicación específica (ASICs), procesadores de señales digitales (DSPs), dispositivos de procesamiento de señales digitales (DSPDs), dispositivos de lógica programable (PLDs), conjuntos de puertas programables in situ (FPGAs), procesadores, controladores, microcontroladores, microprocesadores, otras unidades electrónicas diseñadas para llevar a cabo funciones descritas, o una combinación de las mismas.

Para una implementación software, los medios variados pueden comprender módulos (por ejemplo, procesos, funciones, y demás) que llevan a cabo las funciones descritas. El código de software puede almacenarse en una unidad de memoria y ser ejecutadas por un procesador. La unidad de memoria puede implementarse dentro del procesador o externo al procesador.

Se describen varios aspectos, configuraciones, y realizaciones de la invención. En particular, la invención proporciona procedimientos, aparatos, sistemas, procesadores, código de programa, medios legibles por ordenador, y otros aparatos y elementos que implementan varios aspectos, configuraciones y características de la invención, tal como descrito en lo siguiente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Las características y ventajas de la presente invención se harán más aparentes a partir de la descripción detallada que sigue en conjunción con los dibujos, en los que caracteres de referencia iguales identifican elementos correspondientes en diferentes dibujos. Se pueden también referenciar a los elementos correspondientes mediante caracteres distintos.

La **FIG. 1** muestra un dispositivo de comunicación inalámbrica que comprende un aparato de acuerdo a una realización de la invención.

La **FIG. 2** muestra componentes del aparato de autenticación.

La **FIG. 3** muestra un procedimiento de autenticación implícita mejorada de acuerdo a una realización de la invención.

La **FIG. 4** muestra un procedimiento para generar modelos de usuario.

La **FIG. 5** muestra un procedimiento para actualizar modelos de usuario.

La **FIG. 6** muestra un procedimiento para restaurar modelos de usuario.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La **FIG. 1** muestra un dispositivo 100 de comunicación inalámbrica que comprende un aparato 110 de acuerdo a una realización de la invención. El aparato opera para autenticar implícitamente y/o identificar un usuario mientras utiliza el dispositivo. El proceso es continuo en que la identidad se verifica constantemente sin ninguna interacción explícita requerida por parte del usuario. En una primera fase de aprendizaje, se monitoriza el comportamiento del usuario para generar un perfil de usuario que capture los patrones de conducta más significantes. Opcionalmente, también se puede implementar manualmente por el usuario mismo, introduciendo los datos de comportamiento más comunes. La introducción manual de datos puede reemplazar la preferida generación automática de perfil de usuario, o complementarla.

En una segunda fase operativa, el perfil de usuario se usa para autenticar el usuario implícitamente, es decir, sin intervención de usuario. Adicionalmente, en un aspecto de la invención, se actualiza continuamente el perfil de usuario de tal forma que la autenticación implícita es adaptativa a cambios en el comportamiento del usuario, o a la interacción con su entorno.

El perfil de usuario modela los patrones de comportamiento del usuario en base a métricas 130 proporcionadas por el dispositivo. Las métricas monitorizadas tanto en la fase de aprendizaje como en la fase operativa comprenden:

- Histórico de datos de ubicación (GPS, señales de teléfono), ubicaciones más frecuentes
- Histórico de navegación Web, páginas de Internet más frecuentemente visitadas
- Histórico de llamadas, contactos más frecuentes
- Histórico SMS, contactos más frecuentes
- Histórico de uso de aplicaciones, aplicaciones más frecuentemente utilizadas
- Histórico de puntos de acceso WiFi, puntos más frecuentados
- Lista de pagos, transacciones más frecuentes
- Preferencias de usuario, interacción con el dispositivo de uno mismo

No obstante, la invención no está limitada a esta lista de métricas, y la persona de oficio derivará fácilmente otra información relacionada con el usuario que puede extraerse del dispositivo de comunicación y que proporciona una indicación de su persona o comportamiento.

En un aspecto, el proceso de autenticación se puede llevar a cabo localmente dentro de un entorno de ejecución de confianza TEE 120. Por lo tanto, su ejecución está completamente aislada y, como tal, garantiza que todo código y datos estén protegidos durante la ejecución. También se encuentran protegidos los datos almacenados persistentemente pertenecientes al sistema de autenticación que son continuamente accedidos por otras aplicaciones.

La **FIG. 3** muestra un procedimiento para la autenticación implícita mejorada. El procedimiento es iterativo con el fin de actualizar dinámicamente los datos y el modelo de usuarios. Se recolectan 300 las muestras de datos por el gestor de datos en una primera etapa para actualizar la información relacionada con el usuario recolectada más reciente. Se lleva a cabo una prueba para determinar 320 si el modelo de usuario ya existe. En caso negativo, se lleva a cabo una prueba para determinar 310 si se han recolectado un número suficiente de muestras. En caso negativo, el proceso retorna a la primera etapa para recolectar 300 más muestras.

Una vez que se han recolectado un número suficientemente elevado de muestras representativas del comportamiento habitual del usuario, se genera 330 el modelo de usuario. En general, cuantas más muestras de datos, mejor es la precisión. Existen muchos algoritmos para la detección de anomalías desde técnicas clásicas basadas en la predicción al análisis de señales o la reducción de la dimensionalidad. En particular, la primera categoría incluye algoritmos como el promedio móvil ponderado exponencialmente (del inglés "*Exponentially Weighted Moving Average*") EWMA, y el promedio móvil integrado autorregresivo (del inglés "*Auto-Regressive Integrated Moving Average*") ARIMA. El análisis de señal comprende esencialmente transformadas de Fourier y técnicas similares. Finalmente, el análisis de componente principal PCA, uno de los métodos más comúnmente utilizados para la reducción de dimensionalidad, se utiliza para transformar el conjunto de datos original a un conjunto nuevo de variables o componentes principales (PC), que se ordenan en orden decreciente según su varianza. Cada PC se forma a partir de una combinación lineal de los campos originales. Basado en el hecho que los patrones más fuertes usualmente reflejan la normalidad, el PCA se usa para extraer solamente los PCs más relevantes. Este conjunto de componentes se define como el subespacio normal y todos los demás PCs que representan variaciones menos significantes definen el subespacio anormal. El número de PCs se deben configurar de acuerdo a cada entorno y la sensibilidad deseada para el detector.

Seguidamente, la autenticación implícita determina 340 si el usuario actual del dispositivo inalámbrico está autorizado para utilizar el dispositivo mediante la comparación del modelo de usuario con la muestra de datos actual. Si el comportamiento actual no se corresponde con el modelo de usuario, el sistema no puede garantizar que el usuario sea el legítimo, y, consecuentemente, bloquea 370 el dispositivo. Esta desviación, usando el PCA, se detecta midiendo la magnitud de la proyección de los datos de entrada al subespacio residual anteriormente descrito (si dicha magnitud sobrepasa un umbral, se marca una anomalía). Notar que la detección de una falta de correspondencia no está limitada solamente al algoritmo PCA. En este punto, se requiere de un mecanismo de autenticación explícita para desbloquear el dispositivo.

Contrariamente, si la muestra actual se corresponde con el modelo de usuario, se actualiza 350 el modelo consecuentemente usando la información más reciente relacionada con el usuario. Esta actualización se lleva a cabo también en caso de que el mecanismo de autenticación explícita se exitosa. Seguidamente, se solicita al usuario del dispositivo que notifique si la autenticación implícita ha fallado en el reconocimiento del usuario, o si ha sido un usuario no legitimo o un atacante que ha tomado control del dispositivo.

En caso de que el usuario confirme que su dispositivo no ha sido ni robado ni comprometido, se confirma el modelo de usuario actualmente utilizado como un modelo de usuario válido para su operación continuada. En cambio, en caso de que la autenticación explícita sea exitosa pero la legitimización no se confirma por ningún usuario legítimo, una vez que el dispositivo se recupera por su dueño, se restaura 360 el modelo de usuario a la última versión almacenada en el almacenamiento de datos.

La **FIG. 2** muestra componentes del aparato 200 de autenticación, que comprende un Gestor de Datos DM 210, un Gestor de Modelos MM 220, un Gestor de Autenticación AM 230, un Gestor de Sistema SM 240 y un Almacenamiento de Datos DS 250. Tal como descrito, el aparato de autenticación se alberga localmente dentro del dispositivo de comunicación. El dispositivo inalámbrico se muestra sólo para representar la provisión de datos relacionados con el usuario e información, en forma de métricas 130.

El primer componente del aparato de autenticación es el gestor de datos 210, o medios para la gestión de datos, que recolecta los datos relacionados con el usuario 130 relacionados con el comportamiento de usuario, y prepara los datos en un formato apto para el análisis posterior. Este componente recolecta los datos directamente del dispositivo inalámbrico para entregarlos a los gestores de modelos y de autenticación. Se encarga de interactuar con los APIs del Sistema Operativo móvil y de preparar todos los datos. En particular, en primer lugar, homogeniza todas las fuentes de datos con el fin de eliminar cualquier hueco posible en las series temporales de cada métrica monitorizada (por ejemplo, las coordenadas GPS). Seguidamente, agrega o resume los datos de una cierta manera: por ejemplo, en vez de reportar la lista de llamadas en el último minuto, podría proporcionar el número de llamadas, su entropía, o cualquier otra variación que pueda ser conveniente dependiendo de cada caso.

En un aspecto, puede también tomar en cuenta un parámetro de frecuencia de muestreo que determina cuán frecuentemente se procesan y envían al gestor de modelos las muestras de datos. Por ejemplo, las muestras de datos pueden agregarse durante ventanas temporales de 1 minuto o 10 minutos. Dependiendo de este parámetro, el gestor de datos agrupa y resume los datos de cada serie temporal en consecuencia. Así, el parámetro de frecuencia de muestreo determina cuán regularmente se lleva a cabo la validación de la autenticación. Si, por ejemplo, se procesan muestras solamente cada 3 horas, el sistema no puede detectar anomalías antes de que

expire ese tiempo. Por el contrario, una alta frecuencia de actualizaciones, como segundos o minutos, mientras mejora la efectividad del sistema de autenticación, requerirá también más recursos, y por lo tanto, podría tener un impacto importante sobre el rendimiento del mismo dispositivo.

El gestor de modelos 220, o medios de gestión de modelos, es responsable para la generación de un perfil de usuario, o modelo de usuario, basado en los datos relacionados con el usuario. También actualiza el modelo de usuario continuamente mediante la extracción periódica de información actualizada relacionada con el usuario. El gestor de modelos mantiene una versión identificada del último modelo de usuario en el almacenamiento de datos 250, o medios de almacenamiento, en caso de que se tenga que restaurar. En un aspecto, la generación automática de modelos se sustituye, o complementa, por información adicional proporcionada por el usuario mismo. La versión identificada comprende información adicional como tiempo, o fecha, o ubicación, de cuando se actualizó por última vez el modelo de usuario con datos relacionados con el usuario válidos.

En cuanto a la generación del modelo de usuario, en general, cuantas más muestras se recolectan, más alta es la precisión del modelo, ya que reflejará más precisamente el comportamiento de usuario. En cambio, es necesario cierto compromiso entre dicha precisión y otros requisitos (por ejemplo, duración de batería o uso de CPU). Por ejemplo, mientras la recolección de muestras de datos durante cinco días es más representativa que las muestras correspondientes a un solo día, la recolección de datos para periodos más largos como meses podría no servir el propósito de obtener precisiones más elevadas, más bien malgastar vida útil de la batería, espacio de almacenamiento y uso de CPU. Bajo la suposición que la mayoría de personas se comportan de acuerdo a patrones semanales con variaciones menores, es decir, generalmente trabajan durante los días laborables y llevan a cabo otras actividades durante los fines de semana, los inventores proponen un periodo que se corresponde a datos a lo largo de una semana para generar el modelo de usuario. Notar que la presente invención no está limitada a esta configuración y que otras configuraciones pueden ser mejores dependiendo de cada usuario.

La **FIG. 4** muestra un procedimiento 400 para la generación del modelo de usuario. El gestor de datos, que recolecta continuamente nueva información relacionada con el usuario del dispositivo de comunicación, transmite 410 continuamente estos datos recientemente obtenidos al gestor de modelos. Una vez que se obtienen un número suficiente de muestras de datos, se genera 420 el modelo de usuario en base al comportamiento del usuario. Una vez que se construye este modelo de usuario, el gestor de modelos se comunica 430 continuamente con el almacenamiento de datos. Así, el almacenamiento de datos almacena la información más reciente relacionada con el usuario, así como diferentes versiones del modelo de usuario. Con el fin de permitir la recuperación de modelos de usuarios específicos almacenados en momentos específicos, se almacenan los modelos de usuarios con información adicional.

En cuanto a la actualización del modelo de usuario, a medida que el tiempo pasa y el gestor de datos sigue recolectando y recibiendo nuevas muestras de datos de comportamiento de usuario, el gestor de modelos actualiza el modelo de usuario consecuentemente con el fin de reflejar lo antes posible cualquier cambio menor en los patrones de conducta del usuario. No obstante, la frecuencia de actualización, la frecuencia de muestreo, se puede establecer con el fin de evitar operaciones de CPU innecesarias, en particular operaciones de escritura-lectura al almacenamiento de datos. Si el gestor de modelos determina que la última muestra se corresponde bien al modelo de usuario actual, el modelo se mantiene sin cambio, consecuentemente ahorrando potencia de procesamiento. En el caso de que haya un cambio en comportamiento mínimo, el modelo actualizado nuevo se escribe al almacenamiento de datos con la información adicional. En un aspecto, no se elimina el modelo de usuario anterior, es decir, se mantiene en el almacenamiento de datos para cualquier restauración futura que pueda ser necesaria. En un aspecto, el sistema almacena un número finito de modelos. Tal número se puede establecer dependiendo de requisitos de usuario (por ejemplo, una cantidad máxima de almacenamiento a utilizar).

La **FIG. 5** muestra un procedimiento 500 para actualizar el modelo de usuario. Primero, el gestor de modelos recibe 510 una muestra de datos relacionados con el usuario del gestor de datos. Seguidamente, con el fin de determinar si dicha muestra se corresponde con el comportamiento habitual del usuario, el gestor de modelos obtiene 520 el último modelo del almacenamiento de datos. Una vez obtenido 530, el gestor de modelos envía 540 tanto la muestra de datos como el modelo al gestor de autenticación para proceder con la autenticación. En caso de que el gestor de autenticación determine que ha habido un fallo de autenticación, instruye 550 al gestor de sistema para bloquear el dispositivo y solicitar al usuario a llevar a cabo 560 una autenticación explícita.

En caso de una autenticación explícita exitosa, el gestor de autenticación determina si el fallo de autenticación se debió a un cambio menor en el uso legítimo, es decir, si fue el mismo usuario que estaba utilizando el dispositivo al bloquearse el mismo. Esto se implementa preguntando 570 al usuario por confirmación. Si el usuario confirma 580 y el resultado es positivo, se actualiza 580, 590 el modelo de usuario y almacena 595 en al almacenamiento de datos. Por el contrario, en caso de que el usuario no estaba utilizando el dispositivo de comunicación (por ejemplo, debido a un robo), el procedimiento procede a restaurar el último modelo de usuario válido.

Volviendo al resultado de la autenticación, en caso de un resultado positivo, y se autentica implícitamente al usuario, el gestor de autenticación instruye al gestor de modelos de actualizar el modelo de usuario como válido usando el último conjunto de datos y almacenándolo en el almacenamiento de datos para su uso continuado.

En cuanto a la restauración del modelo de usuario, el gestor de modelos restaura un modelo creado anteriormente en aquellos escenarios que falla la autenticación implícita y el dispositivo se ha robado o comprometido. En aquellos escenarios, las últimas muestras de comportamiento de usuario recolectadas por el dispositivo no reflejan su conducta, más bien el de otra persona. Así, una vez que el propietario recupera su dispositivo, debe indicar información específica que solamente un usuario fidedigno podría saber, como, por ejemplo, la hora, y/o fecha, y/o ubicación en que se acuerde de haber utilizado su dispositivo por última vez por sí solo. En base a tal indicador temporal, el gestor de modelos comunica con el almacenamiento de datos para buscar el modelo de usuario más cercano a ese instante de tiempo y lo restaura como el modelo de usuario actual. Este modelo actual es entonces utilizado para la continuación de la autenticación implícita.

La **FIG. 6** muestra el procedimiento 600 para restaurar el modelo de usuario. Primero, el gestor de modelos determina si la última muestra de datos relacionados con el usuario se corresponde con el modelo de usuario más reciente. Esto se implementa mediante la recolección y recepción 610 de la muestra de datos actual del gestor de datos, solicitando 620 el modelo de usuario actual, y recibiéndolo 630 del almacenamiento de datos. Seguidamente instruye al gestor de autenticación de llevar a cabo 640 una comparación de los datos y el modelo para verificar si se corresponden, es decir, analizar si el usuario actual gestionando el dispositivo es realmente el dueño legítimo. En caso de que el resultado de la comparación sea negativo, y no se corresponden, la autenticación ha fallado y el dispositivo se bloquea. En este punto, se necesita de la interacción explícita del usuario para desbloquearla 650. Hasta este punto, el proceso de operación es idéntico al procedimiento para actualizar el modelo de usuario.

Después de la autenticación explícita, se solicita 660 al usuario confirmación de uso legítimo. Si la confirmación es positiva, el usuario está indicando que el cambio del patrón de comportamiento que detonó la autenticación falsa es parte de un comportamiento estándar, común, o normal, que debería integrarse en el modelo de usuario. En caso de que el resultado es negativo, y el dueño legítimo del dispositivo perdió el control del dispositivo durante un cierto periodo de tiempo, el usuario confirma 670 mediante la provisión de información relacionada con cuando se acuerda de haber tenido control del dispositivo por última vez. Esta información comprende al menos uno de tiempo, fecha, y ubicación. Se pasa 680 esta información al gestor de autenticación, que lo comunica 690 directamente al almacenamiento de datos. Utilizando la información introducida por el usuario, el almacenamiento de datos obtiene el modelo de usuario con la mejor correspondencia, y lo restaura, que quiere decir que reemplaza el modelo de usuario actual con la versión restaurada, asegurando así que se utilizará el último modelo de usuario válidamente autenticado para la posterior autenticación implícita. En caso de que la información proporcionada por el usuario sea, por ejemplo, sólo el tiempo, el almacenamiento de datos obtiene el modelo de usuario con el sello de tiempo más cercano al instante de tiempo indicado y envía 695 el modelo de usuario al gestor de modelos para establecerlo como el nuevo modelo de usuario, reemplazando así el actual.

Tal y como mencionado, el gestor de autenticación 230, o medios para gestionar la autenticación, es responsable de llevar a cabo la autenticación de usuario en base a la comparación entre el modelo de usuario, generado y mantenido por el gestor de modelos, y una actualización periódica de los datos relacionados con el usuario obtenidos del gestor de datos. En caso de que el resultado de la comparación sea positivo, se autentica la identidad del usuario, y se almacena una instancia del modelo de usuario almacenado junto a la información adicional como el tiempo, y/o fecha, y/o ubicación, de cuando se actualizó el modelo de usuario por última vez con datos válidos relacionados con el usuario. Seguidamente se permite al usuario seguir operando el dispositivo. En cambio, en caso de que el resultado sea negativo, no se autentica la identidad del usuario y el dispositivo se bloquea de su uso posterior.

La autenticación implícita básicamente determina si las muestras de datos relacionados con el usuario recibidos del dispositivo se pueden describir en términos del último modelo de usuario, o, en otras palabras, si dichas muestras podrían haber sido generadas a partir del mismo. El resultado de la verificación es un número que puede tomar valores en el intervalo [0, 1], e indica la extensión que la autenticación implícita es fiable o no. Dependiendo de este resultado, el módulo determina que las muestras han sido obtenidas a partir de este modelo. En este caso, notifica al gestor de modelos y se mantiene en reposo hasta que se necesita una nueva verificación. Si el gestor de autenticación determina que las muestras no podían haber sido obtenidas a partir de este modelo, entonces se utiliza un mecanismo secundario de autenticación explícita.

La frecuencia en la que se lleva a cabo la autenticación implícita es la misma frecuencia de muestreo utilizada por el gestor de datos para obtener la información actualizada relacionada con el usuario. Esta frecuencia de muestreo está preestablecida y puede ser definida por el usuario. Cuanta más alta la frecuencia, más rápida es la detección de un uso no legítimo del dispositivo, pero también más alta la carga computacional y consecuentemente más alto el consumo de batería. En otras palabras, hay una relación inversa inherente a la ejecución de esta tarea entre seguridad y consumo de energía. Por lo tanto, se permite una autenticación implícita permitiendo que usuarios seleccionen un punto de operación óptimo en el seno de la relación de compensación seguridad-consumo. En particular, los usuarios pueden escoger el nivel de seguridad que desean alcanzar, o alternativamente, el consumo de batería que están dispuestos a sacrificar.

Tal y como descrito, una vez que falla la autenticación implícita y se lleva a cabo la autenticación explícita, en un aspecto de la invención se lleva a cabo una etapa adicional de validación de modelo de usuario que garantiza que

el modelo de usuario siendo utilizado es el correcto. En caso de una autenticación explícita exitosa, el usuario confirma que el dispositivo estaba siendo utilizado de forma legítima y el gestor de autenticación instruye al gestor de modelos de validar el modelo de usuario actual como el valido para continuar con su uso. Por otro lado, si el usuario legítimo confirma que el dispositivo no estaba bajo su control, el gestor de autenticación instruye al gestor de modelos de restaurar el modelo de usuario al último válido antes del fallo de la autenticación implícita.

El gestor de sistema SM 240, o medios para la gestión de sistema, es responsable de gestionar la comunicación entre los diferentes componentes, así como con las partes restantes del dispositivo. Una de sus funciones es la de interactuar con el dispositivo inalámbrico para bloquearlo en caso de un fallo de autenticación. También se comunica con el usuario para preguntar por tokens de autenticación explícita que son enviados al gestor de autenticación que validará los tokens para determinar si se permite al usuario actual desbloquear y operar el dispositivo.

En este contexto, los esquemas de autenticación explícita (por ejemplo, el reconocimiento facial basado en biometría, o huellas dactilares, o la entrada de código PIN convencional) se consideran solo como mecanismos para recuperar del robo del dispositivo o bloqueo una vez que la autenticación implícita ha fallado. Así, en caso de que falle la autenticación implícita, el gestor de autenticación lleva a cabo la autenticación explícita y restaura el dispositivo de comunicación a su estado correspondiendo con la última autenticación implícita válida. Todo este proceso se ejecuta dentro del entorno de ejecución de confianza que asegura que tanto los datos como la ejecución están aislados y seguros de otras aplicaciones maliciosas que intentan ganar acceso y manipularlos.

Durante la operación de la autenticación implícita, el gestor de autenticación valida la identidad del usuario manteniendo continuamente el perfil de usuario actualizado y verificando si las últimas muestras validadas se le corresponden. Como el modelo de usuario contiene información de usuario privada y sensible, se lleva a cabo la comparación localmente, en otras palabras, los datos siempre se mantienen dentro del dispositivo. Tal y como mencionado, algunas ventajas son que los datos sensibles no se transmiten sobre enlaces de comunicación inseguros y se puede llevar a cabo la autenticación incluso en lugares remotos sin cobertura, o enlaces de comunicación fijas o inalámbricas. Como el proceso es continuo, el modelo de usuario actualiza de forma dinámica sus datos y es por lo tanto adaptativo a los cambios en comportamiento relacionado con el usuario, resultando en resultados más precisos en el que se minimizan los falsos negativos.

El almacenamiento de datos es responsable de almacenar un cierto número de instancias del modelo de usuario, dicho número siendo definible por el usuario dependiendo de requisitos específicos de usuario. Adicionalmente, cada instancia tiene cierta información adicional (sello de tiempo, antigüedad y última ubicación válida) para facilitar su identificación más eficiente:

- Sello de tiempo
    - Contiene el tiempo y fecha de creación de la plantilla de perfil asociado.
- Última ubicación válida
    - Contiene la ubicación donde la actualización de modelo se almacenó/actualizó en la base de datos por última vez (por ejemplo, si existe un bloqueo, este campo contendría la última vez que se almacenó el modelo en el almacenamiento de datos antes del fallo de autenticación).

La siguiente tabla muestra la información almacenada a modo de ejemplo:

Perfil Plantilla	**Sello de Tiempo**	**Última ubicación válida**
modelo1	01.05.2014 09:00	41.387015, 2.170047 (Plaça Catalunya, Barcelona)
modelo2	15.07.2014 22:00	41.3818188, 2.1635233 (Ronda Sant Antoni, Barcelona)
modelo3	16.07.2014 17:00	41.429639, 2.143603 (Vall Hebron, Barcelona)

Las variables m*odelo1, modelo2* y *modelo3* representan los modelos de usuario específicos usados en un momento particular, es decir, contienen los modelos definiendo el comportamiento normal del usuario en esta ventana temporal específica. El gestor de autenticación compara las muestras de datos de entrada con estos modelos para determinar si se permite al usuario utilizar el dispositivo o no.

Por lo tanto, las distintas realizaciones de la invención proporcionan un procedimiento y aparato para la autenticación implícita mejorada de usuarios de dispositivos inalámbricos que es más fácil de usar, más segura, precisa y robusta, que las implementaciones existentes.

Además, se entiende que las realizaciones y aspectos descritos se pueden implementar por medios variados en hardware, software, firmware, middleware, micro-código, o cualquier combinación de los mismos. Varios aspectos o características descritas pueden implementarse, por un lado, como un método o procedimiento o función, y por el otro lado, como un aparato, dispositivo, sistema, o programa de ordenador accesible por cualquier dispositivo legible por ordenador, portador o medio. Los procedimientos o algoritmos descritos pueden implementarse directamente en hardware, en un módulo software ejecutado por un procesador, o una combinación de las dos.

Los varios medios pueden comprender módulos de software residentes en memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, disco duro, disco removible, un CD-ROM, o cualquier otro tipo de medio de almacenamiento conocido en la técnica.

Los varios medios pueden comprender bloques de lógica, módulos, y circuitos se pueden implementar o llevado a cabo por un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de aplicación (ASIC), un conjunto de puertas programable in situ (FPGA), u otros dispositivos de lógica programable, de puerta discreta o de lógica de transistor, componentes discretos de hardware, o cualquier combinación de los mismos diseñados para llevar a cabo las funciones descritas. Un procesador de propósito general puede ser un micro procesador, pero en la alternativa, el procesador puede ser un procesador convencional, controlador, microcontrolador, o máquina de estado.

Los varios medios pueden comprender medios legibles por ordenador incluyendo, pero no limitado a, dispositivos de almacenamiento magnético (por ejemplo, discos duros, discos floppy, tiras magnéticas, y demás), discos ópticos (por ejemplo, discos compactos CD o versátiles DVD, y demás), tarjetas inteligentes y unidades de almacenamiento flash temporales (por ejemplo, EPROM, lápiz tarjeta, unidad llave, y demás). Adicionalmente, la variedad de medios de almacenamiento descritos puede representar uno o más dispositivos y/o medios legibles por ordenador para almacenar información. El término medio legible por ordenador puede comprender, sin estar limitado a ello, una variedad de medios capaces de almacenar, guardar, o transportar instrucciones y/o datos. Adicionalmente, un producto de programa de ordenador puede comprender un medio legible por ordenador con una o más instrucciones o códigos operativos para hacer que un ordenador lleve a cabo las funciones descritas una vez ejecutadas en el ordenador.

Lo que se ha descrito comprende una o más realizaciones a modo de ejemplo. En cambio, la persona de oficio se dará cuenta que muchas otras combinaciones y permutaciones de realizaciones varias son posibles dentro del concepto inventivo después de una lectura directa y objetiva de esta divulgación. Consecuentemente, la intención es acoger todas dichas alteraciones, modificaciones y variaciones que entran dentro del ámbito de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un aparato en un dispositivo de comunicación inalámbrica para la autenticación implícita mejorada del usuario del dispositivo, en el que el aparato comprende:

medios (210) para gestionar datos, configurados para recibir datos relacionados con el usuario recolectados del dispositivo de comunicación inalámbrica, los datos relacionados con el usuario siendo indicativos de los patrones de comportamiento del usuario del dispositivo;
medios (230) para gestionar autenticación, configurados para autenticar implícitamente el usuario del dispositivo sin la intervención del usuario mediante la comparación de los datos relacionados con el usuario con un modelo de usuario; y
medios (220) para gestionar el modelo, configurados para actualizar el modelo de usuario como válido usando los datos relacionados con el usuario si el resultado de la autenticación implícita es positivo, y autenticar explícitamente (560) el usuario del dispositivo si el resultado de la autenticación implícita es negativo; comprendiendo adicionalmente
solicitar (570), del usuario del dispositivo, confirmación de comportamiento legítimo en caso de que el resultado de la autenticación explícita sea positivo, y actualizar (580, 590, 595) el modelo de usuario con los últimos datos relacionados con el usuario si el resultado de la confirmación de legitimidad es positivo, y
si el resultado de la autenticación explícita es negativo, solicitar (670) al usuario del dispositivo por información correspondiente al último uso del dispositivo, en el que la información del último uso del dispositivo comprende al menos uno de tiempo, fecha y/o ubicación;
obtener de los medios de almacenamiento el modelo de usuario que mejor se corresponde con la información del último uso del dispositivo proporcionada; y
usar el modelo de usuario obtenido como el modelo de usuario actual.

2. El aparato de la reivindicación 1, en el que los datos relacionados con el usuario y el modelo de usuario se almacenan en medios (250) de almacenamiento y se buscan de los medios de almacenamiento.

3. El aparato de la reivindicación 2, comprendiendo además medios (240) para la gestión de sistema, configurados para gestionar la comunicación entre los distintos medios de aparato, así como con el dispositivo.

4. El aparato de la reivindicación 3, en el que los datos relacionados con el usuario se recolectan y el modelo de usuario se actualiza a una velocidad determinada por una frecuencia de muestreo definida por el usuario.

5. El aparato de la reivindicación 3, en el que los medios (220) para la gestión de modelo son adicionalmente configurados para generar automáticamente el modelo de usuario a partir de los datos relacionados con el usuario recolectados.

6. El aparato de la reivindicación 5, en el que el modelo de usuario se genera una vez que se han recolectado un número predefinido de muestras de datos relacionados con el usuario.

7. El aparato de la reivindicación 6, en el que la generación automática del modelo de usuario se complementa con la introducción manual de datos relacionados con el usuario por el usuario del dispositivo.

8. El aparato de la reivindicación 5, en el que el modelo de usuario se genera y compara usando los datos relacionados con el usuario en base a una técnica de análisis de componente principal PCA.

9. El aparato de la reivindicación 3, comprendiendo adicionalmente bloquear (550) el dispositivo si el resultado de la autenticación implícita (560) es negativo y autenticar explícitamente el usuario del dispositivo mediante verificación de contraseña y/o medios biométricos, como el reconocimiento facial, o la verificación de huellas dactilares.

10. El aparato de la reivindicación 3, en el que los datos relacionados con el usuario comprenden al menos uno de histórico de datos de ubicación, ubicaciones más frecuentes, histórico de navegación web, páginas de Internet más visitadas, histórico de llamadas, contactos más frecuentes, histórico de SMS, histórico de uso de aplicaciones, aplicaciones más frecuentemente usadas, histórico de puntos de acceso WiFi, puntos WIFI más frecuentados, lista de pagos, transacciones más frecuentes, preferencias de usuario, o la interacción con el dispositivo de uno mismo.

11. El aparato de la reivindicación 3, en el que el aparato está albergado en un entorno seguro del dispositivo de comunicación inalámbrica, tal como el entorno de ejecución de confianza TEE (120).

12. El aparato de la reivindicación 3, en el que los medios (210) de gestión de datos están además configurados para el pre-procesamiento de los datos relacionados con el usuario, tal como armonizar y/o agregar y/o resumir los datos.

13. Un procedimiento en un aparato de un dispositivo de comunicación inalámbrica para la autenticación implícita mejorada del usuario del dispositivo, en el que el procedimiento comprende llevar a cabo iterativamente:

recibir (510) datos relacionados con el usuario recolectados del dispositivo de comunicación inalámbrica, los datos relacionados con el usuario siendo indicativos de los patrones de comportamiento del usuario del dispositivo;
autenticar implícitamente (540) el usuario del dispositivo sin la intervención del usuario mediante la comparación de los datos relacionados con el usuario con un modelo de usuario; y
actualizar el modelo de usuario como válido usando los datos relacionados con el usuario si el resultado de la autenticación implícita es positivo, y autenticar explícitamente (560) el usuario del dispositivo si el resultado de la autenticación implícita es negativo; comprendiendo adicionalmente
solicitar (570), del usuario del dispositivo, confirmación de comportamiento legítimo en caso de que el resultado de la autenticación explícita sea positivo, y actualizar (580, 590, 595) el modelo de usuario con los últimos datos relacionados con el usuario si el resultado de la confirmación de legitimidad es positivo; y
si el resultado de la autenticación explícita es negativo, solicitar (670) al usuario del dispositivo por información correspondiente al último uso del dispositivo, en el que la información del último uso del dispositivo comprende al menos uno de tiempo, fecha y/o ubicación;
obtener de los medios de almacenamiento el modelo de usuario que mejor se corresponde con la información del último uso del dispositivo proporcionada; y
usar el modelo de usuario obtenido como el modelo de usuario actual.

14. Un medio legible por ordenador que comprende instrucciones para llevar a cabo las etapas de procedimiento de la reivindicación 13 una vez ejecutadas en un procesador de un dispositivo de comunicación inalámbrica para la autenticación implícita mejorada del usuario del dispositivo.

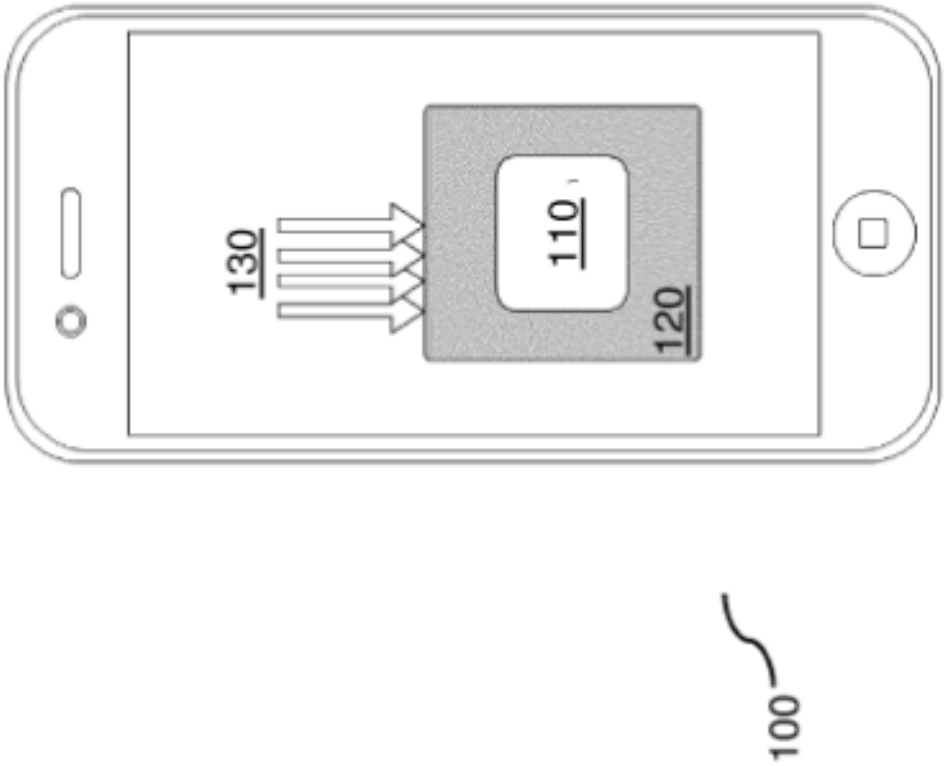

FIG. 1

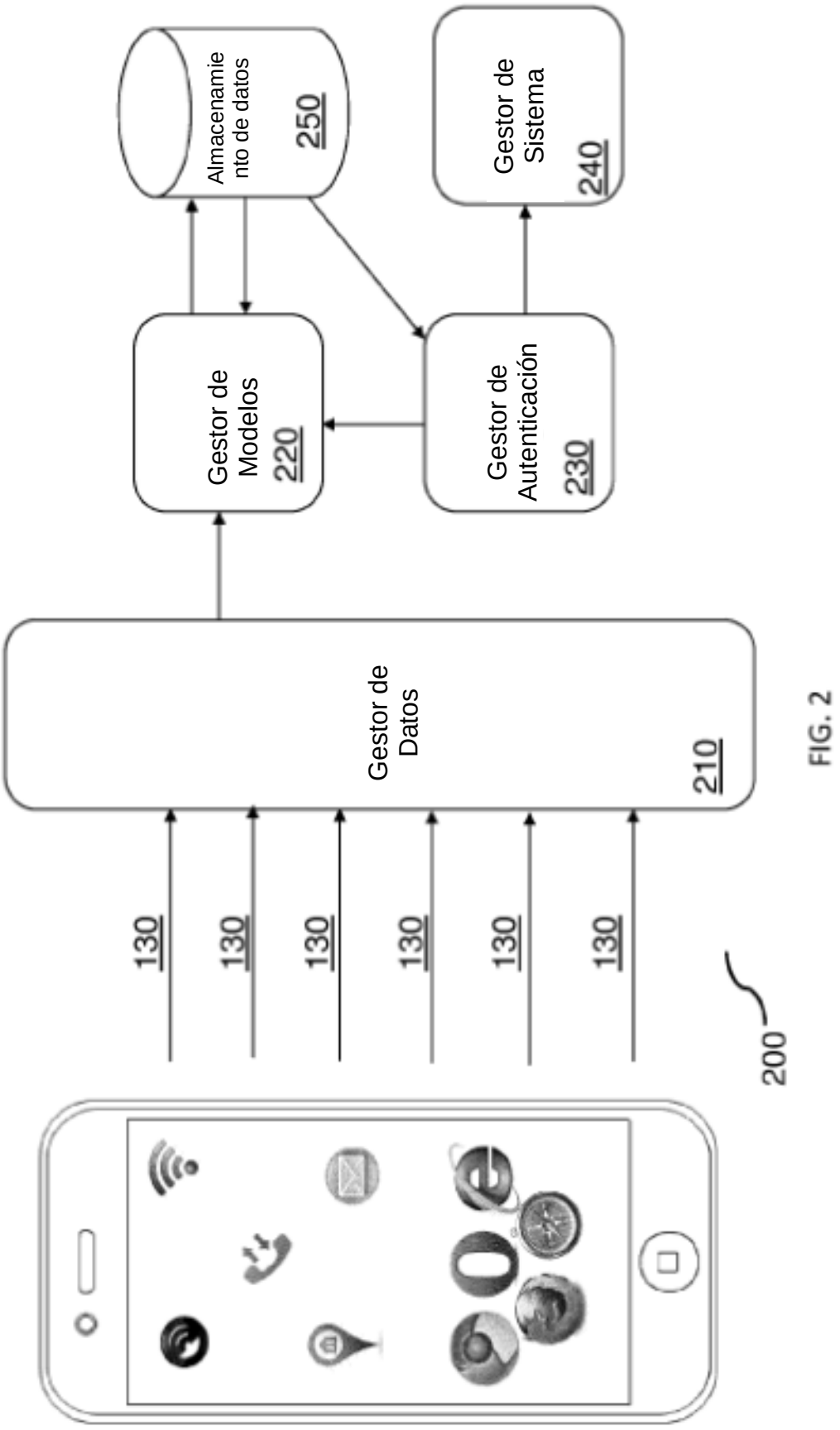
Almacenamiento de datos
250
Gestor de Sistema
240
Gestor de Modelos
220
Gestor de Autenticación
230
Gestor de Datos
210
130
130
130
130
130
130
200

FIG. 2

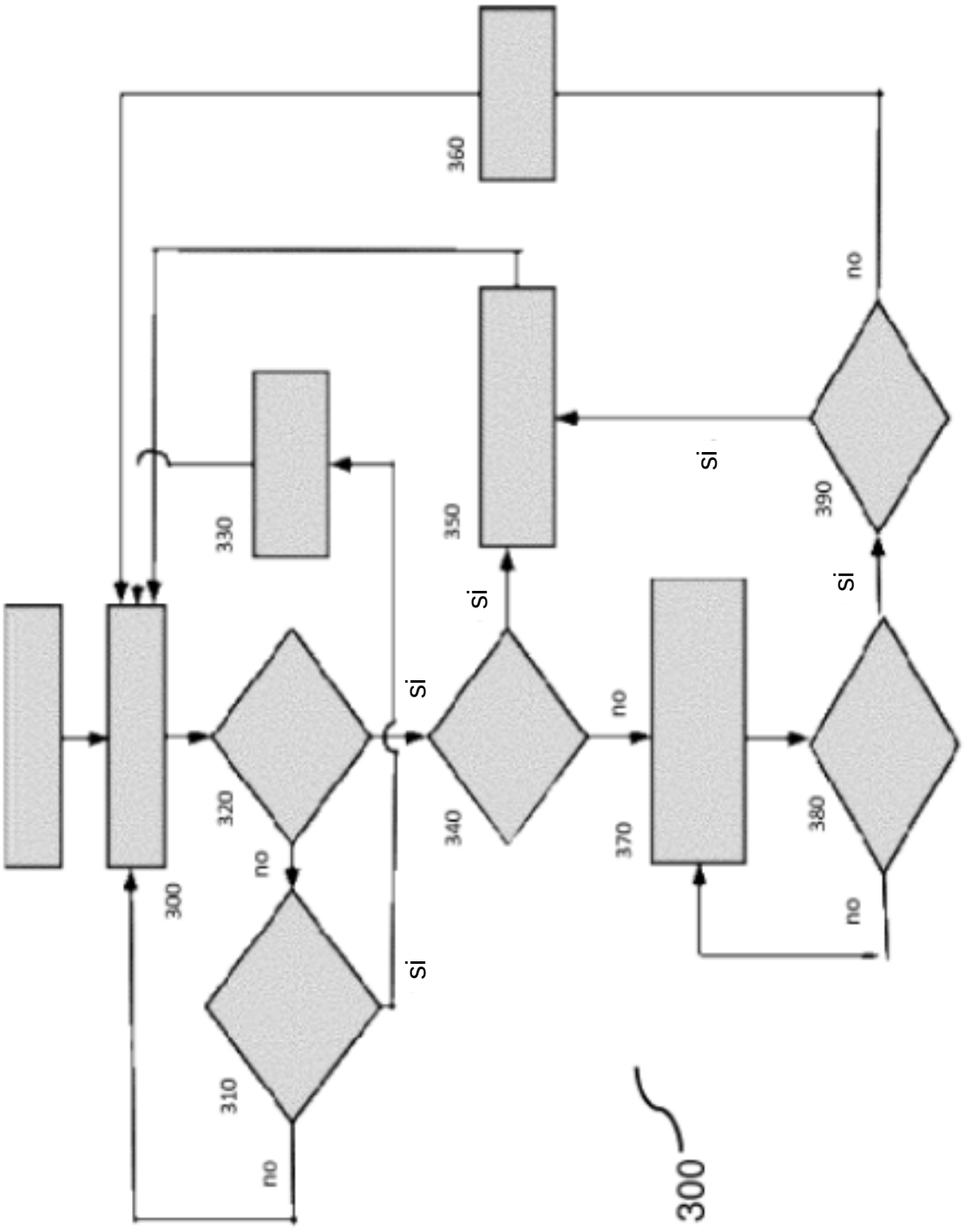
360
no
si
330
350
390
si
si
si
320
340
370
380
no
no
no
300
310
no
si
300

FIG. 3

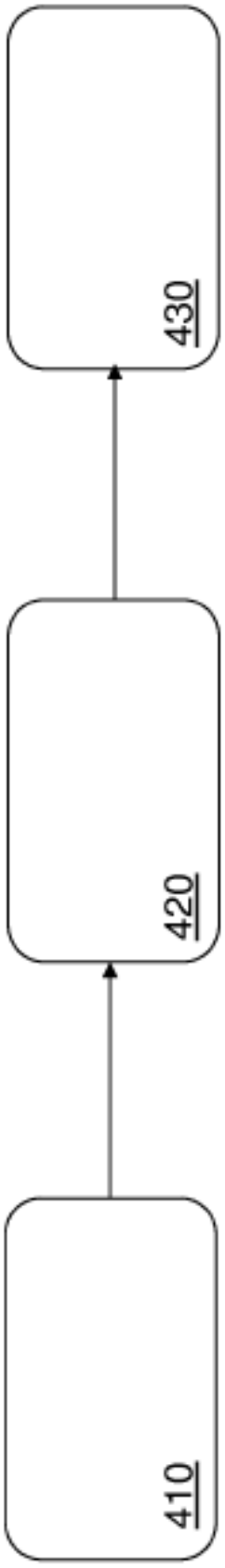

FIG. 4

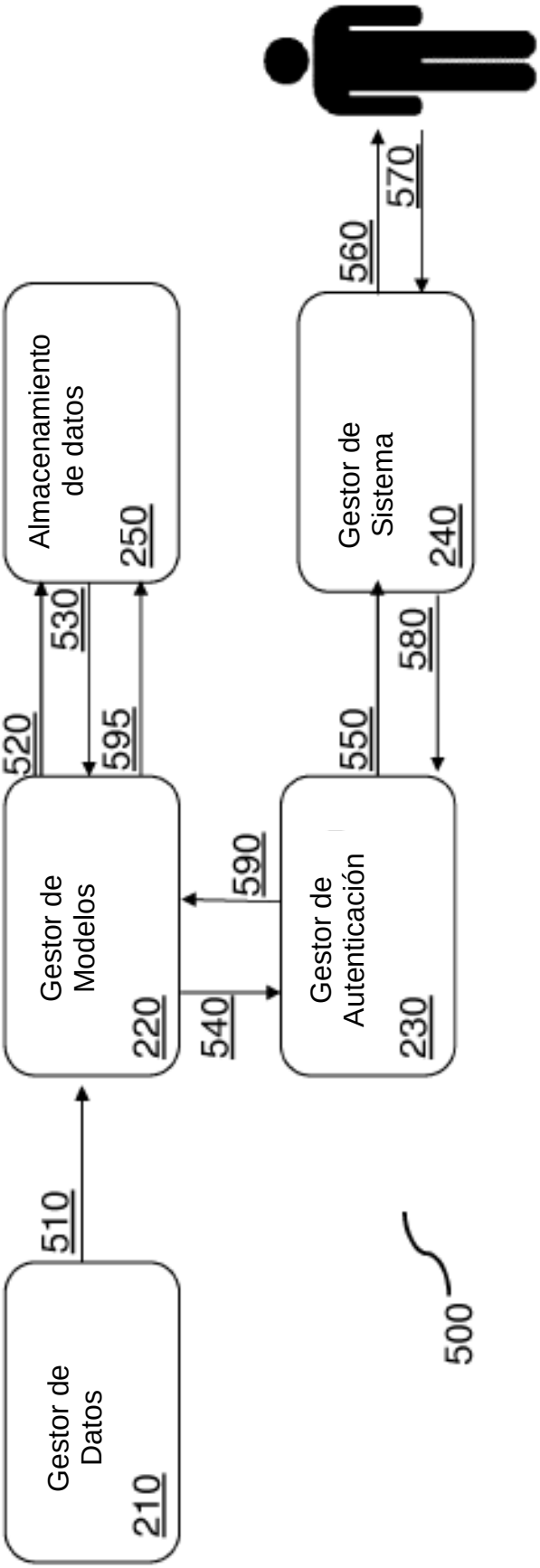
Gestor de Datos
210
510
Gestor de Modelos
220
520
530
595
Almacenamiento de datos
250
540
590
Gestor de Autenticación
230
550
580
Gestor de Sistema
240
560
570
500

FIG. 5

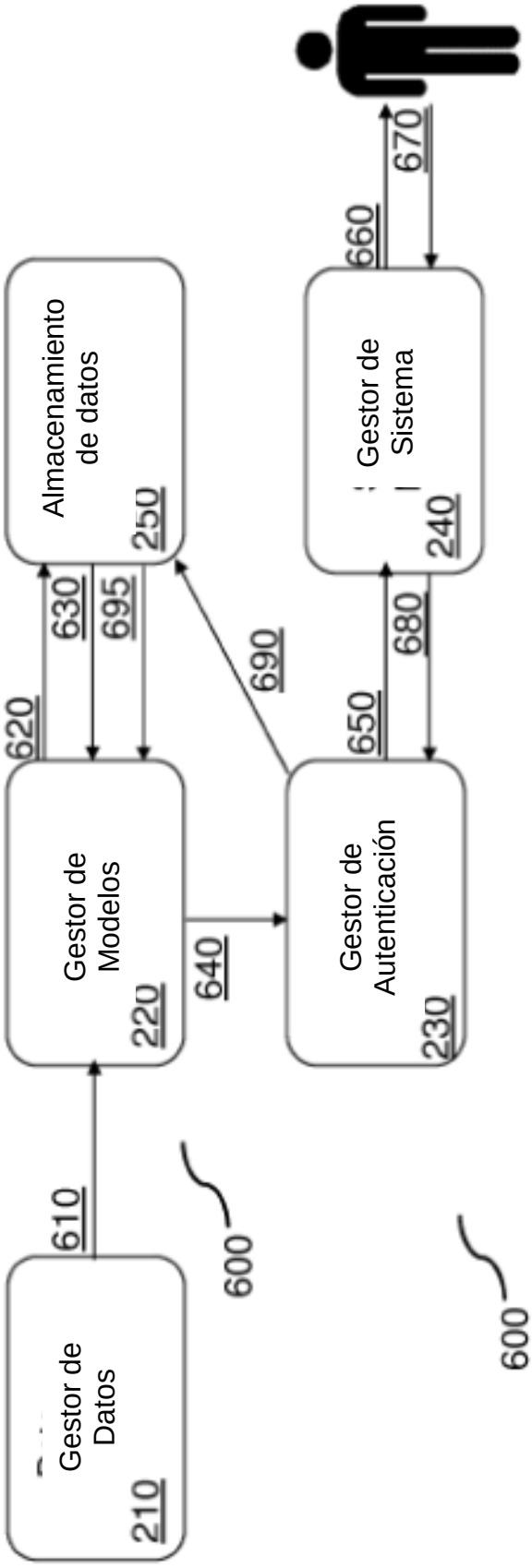
Gestor de Datos
210
610
Gestor de Modelos
220
620
630
695
640
Almacenamiento de datos
250
690
Gestor de Autenticación
230
650
680
Gestor de Sistema
240
660
670
600
600

FIG. 6