(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 642 116**

(51) Int. CI.:

G06F 21/57 (2013.01)
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.03.2014 PCT/EP2014/054039**

(87) Fecha y número de publicación internacional: **12.09.2014 WO14135485**

(96) Fecha de presentación y número de la solicitud europea: **03.03.2014 E 14714602 (1)**

(97) Fecha y número de publicación de la concesión europea: **28.06.2017 EP 2965257**

(54) Título: **Procedimiento para medir y monitorizar los niveles de acceso a datos personales generados por recursos de un dispositivo de usuario**

(30) Prioridad:

05.03.2013 IT MI20130325

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.11.2017

(73) Titular/es:

TELECOM ITALIA S.p.A.
Via Gaetano Negri, 1
20123 Milan, IT

(72) Inventor/es:

ANTONELLI, FABRIZIO;
CAPPELLOTTO, ANDREA y
CARAVIELLO, MICHELE

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Procedimiento para medir y monitorizar los niveles de acceso a datos personales generados por recursos de un dispositivo de usuario

Antecedentes de la invención

[0001] Hoy en día existe un alza de dispositivos (la mayoría de los cuales son personales) equipados con recursos que generan muchos datos mientras que perciben el entorno, interactuando con el usuario, comunicándose con recursos externos, etc.

[0002] Un ejemplo de tales dispositivos son los smartphones o tabletas: actualmente, todos los smartphones o tabletas tienen de 6 a 8 sensores físicos propios (aquí referidos como "recursos físicos") y casi cien de sensores virtuales ("recursos virtuales"). Los recursos físicos son, por ejemplo, el acelerómetro, el receptor de GPS, el módulo de transmisión NFC, etc. Los recursos virtuales son, por ejemplo, el software de gestión de la cuenta personal, el administrador de conexión *Bluetooth*, etc. (la mayoría de los recursos virtuales son software). Esto no es solo aplicable a los móviles desde la llegada de sistemas operativos independientes de dispositivos (como Android), ya que existen tipos de dispositivos con capacidades similares y otros recursos novedosos: este es el caso de los televisores inteligentes, las cámaras de nueva generación, coches con equipamiento interactivo, etc.

[0003] Los dispositivos mencionados anteriormente albergan servicios de terceros y aplicaciones que tienen acceso a los medios propios de los dispositivos: estos generan una cantidad inusitada de datos que, ya que la mayoría de los dispositivos son personales y su uso está tan generalizado, puede ser crítico desde el punto de vista de la privacidad.

[0004] En el documento de Adrienne Porter Felt, Kate Greenwood, David Wagner, "La efectividad de los permisos de la aplicación", de la Universidad de California, Berkeley, Conferencia USENIX sobre el desarrollo de las aplicaciones web (Webapps) de 2011, 956 aplicaciones Android fueron analizadas. Los autores observaron que un 93% de las aplicaciones gratuitas (un total de 856) y el 82% de las aplicaciones de pago (un total de 100) tienen al menos un permiso peligroso. Los permisos peligrosos incluyen acciones que podrían costar dinero al usuario o filtrar información personal. En particular, los autores muestran que los permisos de internet se usan en gran medida y, en la mayoría de aplicaciones, este permiso podría usarse para guardar información personal de los usuarios.

[0005] En el documento de W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, y A. N. Sheth, "TaintDroid: Un sistema de seguimiento de flujo de información para la monitorización a tiempo real de la privacidad en los smarthphones", los autores analizan si los datos y qué tipo de datos personales se almacenan en una aplicación. Desarrollaron un núcleo plugin para analizar los datos enviados a un servidor por todas las aplicaciones que tienen el permiso de conexión a internet junto con otros permisos como cámara, ubicación, etc. Los autores encontraron 358 aplicaciones gratuitas que requerían conexión a internet junto con otros permisos y analizaron 20 de ellas. Entre estos últimos, dos enviaron información del teléfono a servidores de contenidos, siete enviaron la identificación del dispositivo a servidores de contenidos y 15 enviaron la ubicación a servidores de publicidad. De este modo, los autores demostraron que una gran cantidad de aplicaciones podían enviar datos personales para diferentes propósitos.

[0006] En el documento de Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin y David Wagner "Permisos de Android: atención del usuario, comprensión y comportamiento", se analiza la atención y comprensión del usuario durante la instalación de aplicaciones. Solo el 17% de los participantes prestó atención a los permisos durante la instalación. Solo un 3% de los encuestados pudo responder correctamente las tres preguntas de comprensión de los permisos. Esto indica que las advertencias de los permisos actuales de Android no ayudan a la mayoría de usuarios a tomar las decisiones de seguridad correctas. Durante esta prueba, solo el 20% de los usuarios fueron capaces de dar detalles sobre por qué no tenían cierta aplicación instalada. Además, los participantes demostraron una muy baja comprensión de la autorización de permisos durante la instalación.

[0007] La patente WO 2012/109512 describe sistemas y procedimientos para regular el acceso a los recursos en el tiempo de ejecución de una aplicación. Se invocan permisos de aplicación. Cada permiso se asocia con el correspondiente recurso en una pluralidad de recursos de dispositivos. La información almacenada especifica qué aplicaciones tienen permiso para acceder a qué recursos del dispositivo. Se ejecuta una aplicación en el dispositivo que solicita una petición a un recurso mientras que la aplicación se está ejecutando. Respondiendo a la petición, los permisos de la aplicación determinan si la aplicación tiene permiso de acceso en el tiempo de ejecución para usar el

recurso. Cuando la aplicación tiene permiso de acceso en el tiempo de ejecución para usar el recurso, se autoriza el acceso en el tiempo de ejecución al recurso. Cuando la aplicación no tiene permiso de acceso en el tiempo de ejecución para usar el recurso, no se autoriza el acceso en el tiempo de ejecución al recurso, pero se le permite que se siga ejecutando en el dispositivo sin el recurso solicitado.

[0008] En Eric Struse et al., "Creando concienciación en el usuario de los permisos de aplicaciones en sistemas móviles", 13 de noviembre de 2012, Ambient Intelligence, Springer Berlin Heidelberg, páginas 65-80, se presenta una aplicación Android que ofrece a los usuarios información de concienciación sobre otras aplicaciones y permite comprobar en el conjunto de permisos la autorización individual de las aplicaciones.

[0009] En la patente US 2010/257577 se presentan procedimientos para gestionar los ajustes de privacidad para una red social usando un dispositivo electrónico, incluyendo: provocar que el dispositivo electrónico reciba un hecho desencadenante en la red social; y provocar que el dispositivo electrónico determine un número de índices de privacidad en respuesta al evento desencadenante, donde el número de índices de privacidad corresponde con al menos un usuario meta, donde el número de índices de privacidad está normalizado por la suma de un número de puntuaciones, donde el número de las puntuaciones de privacidad está derivado de una suma de puntuaciones atributo y donde la suma de las puntuaciones atributo está derivada de un valor de sensibilidad ponderada de un atributo y un valor de la relación de distancia entre el usuario y el usuario meta.

Resumen de la invención

[0010] La descripción anterior del estado de la técnica muestra que el problema de la seguridad en el acceso a recursos de dispositivos (y a los datos generados por los recursos del dispositivo) por aplicaciones alojadas ha sido estudiado.

[0011] La presente invención no está dirigida principalmente al problema de la seguridad, sino que está dirigida a un proceso para ofrecer a los usuarios de dispositivos un indicativo del nivel de acceso a los datos personales generados por los recursos que conforman el dispositivo.

[0012] De acuerdo con una forma de realización, el procedimiento de la presente invención evalúa el nivel de acceso a datos personales ofreciendo al usuario un indicador numérico y/o gráfico que es independiente de la aplicación de los derechos de acceso y ayuda al usuario a comprender qué datos han sido usados por las aplicaciones alojadas.

[0013] La gestión de las políticas de seguridad no es el principal objetivo de la presente invención, el objeto de la presente invención es medir el nivel de acceso a datos personales generados por un recurso al que se acceda.

[0014] De acuerdo con un aspecto de la presente invención, se proporciona un procedimiento para medir y monitorizar el uso de datos personales generados por los recursos del dispositivo del usuario. El procedimiento puede entrar a valorar cómo se usan los recursos disponibles en un dispositivo (p. ej., en términos de tiempo y frecuencia), el número de recursos a los que se acceden y el tipo de datos generados por esto recursos.

[0015] El procedimiento comprende:

a) para cada uno de dichos recursos, asignar un valor de sensibilidad al recurso en una escala predeterminada de sensibilidad, los valores de sensibilidad al recurso de os diferentes recursos siendo adaptados para permitir dichos recursos basados en la sensibilidad de los datos que generan;
b) para cada una de dichas aplicaciones, calcular un nivel de acceso a la aplicación respectivo a dichos datos combinando mediante una primera función predeterminada los valores del recurso de sensibilidad de los recursos que generan datos a los que se acceden mediante dicha aplicación,
c) calcular un nivel de acceso de los dispositivos a dichos datos por dichas aplicaciones, en el que dicho nivel de acceso del dispositivo es calculado combinando mediante una segunda función predeterminada los niveles de acceso a la aplicación de las aplicaciones instaladas en el dispositivo, y
d) asociar con cada aplicación una respectiva indicación del calculado nivel de acceso a la aplicación.

[0016] Para cada aplicación, la respectiva indicación del calculado nivel de acceso a la aplicación se muestra en una pantalla del dispositivo del usuario.

[0017] Una indicación del calculado nivel de acceso a la aplicación a dichos datos por dichas aplicaciones se

muestra en la pantalla del dispositivo del usuario.

[0018] El procedimiento puede comprender, además:

- Para cada una de dichas aplicaciones, comprar el nivel de acceso a la aplicación calculado respectivamente con un primer valor umbral predeterminado, y
- Para cada una de dichas aplicaciones, presentar al dispositivo del usuario una primera indicación si el nivel de acceso de la aplicación calculado está por debajo del primer valor umbral, o una segunda indicación si el nivel de acceso de la aplicación no está por debajo del primer valor umbral.

[0019] El procedimiento puede comprender, también:

- Para cada una de dichas aplicaciones, comparar el respectivo nivel de acceso a la aplicación calculado con un segundo valor umbral, superior al primer valor umbral, y
- Para cada una de dichas aplicaciones, presentar en el dispositivo del usuario la segunda indicación si el nivel de acceso a la aplicación calculado está por debajo del segundo valor umbral, o una tercera indicación si el nivel de acceso a la aplicación no está por debajo del segundo valor umbral.

[0020] El procedimiento puede comprender, asimismo:

- Definir al menos dos estados operacionales distintos en los que cualquiera de dichas aplicaciones puede existir; y
- Repetir las etapas a) a d) de la reivindicación 1 siempre que cualquiera de dichas aplicaciones cambie su estado operativo de uno a otro de los dos estados operativos, o viceversa.

[0021] Dichos dos estados operativos pueden comprender:

- Un primer estado operativo, cuando una aplicación se está ejecutando en el dispositivo del usuario y en el modo usuario-interactivo;
- Un segundo estado operativo, cuando una aplicación se está ejecutando en el dispositivo del usuario, pero no en el modo usuario-interactivo;
- Un tercer estado operativo, cuando una aplicación no se está ejecutando en el dispositivo del usuario, pero está escuchado al menos uno de dichos recursos y puede activarse cuando ocurre un evento relacionado con los recursos que se escuchan;
- Un cuarto estado operativo, cuando una aplicación no está ejecutándose y no se está escuchando ninguno de dichos recursos.

[0022] Dicho cálculo, para cada aplicación, el respectivo nivel de acceso a la aplicación comprende preferentemente conceder un peso mayor, en dicha combinación, a los valores de sensibilidad de estos recursos que permiten la conexión y la comunicación de datos desde el dispositivo a una red externa de datos.

[0023] Conceder más peso puede comprender ajustar los valores de dichos recursos que permiten la conexión y la comunicación de datos desde el dispositivo a una red externa de datos.

[0024] Dicha primera función predeterminada puede comprender una entre: un producto de valores de sensibilidad de los recursos que generan datos a los que se acceden por dicha aplicación, una suma de los valores de sensibilidad de los recursos que generan datos a los que se acceden por dicha aplicación.

[0025] Dicha segunda función predeterminada puede comprender un producto de los niveles de acceso a la aplicación calculados de las aplicaciones instaladas en el dispositivo.

[0026] De acuerdo con otro aspecto de la presente invención, se proporciona un programa informático que comprende porciones de código del programa informático adaptadas a realizar el procedimiento expuesto anteriormente cuando el programa informático se ejecuta en un dispositivo de procesamiento de datos.

[0027] De acuerdo con otro aspecto de la presente invención, se facilita un dispositivo de usuario que comprende medios configurados para realizar el procedimiento de la presente invención.

Breve descripción de los dibujos

[0028] Estas y otras características y ventajas de la presente invención aparecerían mejor mediante la lectura de la siguiente descripción detalla de algunas formas de realización ejemplares y no limitativas de las mismas, haciendo referencia a los dibujos anexos, donde:

La **figura 1** muestra esquemáticamente los elementos, alojados en un dispositivo de usuario, que se consideran por el procedimiento de la presente invención;
La **figura 2** es un diagrama que muestra una posible tendencia en el tiempo de la cantidad de datos a los que se acceden, generados por recursos del dispositivo de usuario, al que acceden aplicaciones alojadas en el dispositivo de usuario de la **figura 1**;
Las **figuras 3, 4** y **5** son capturas de pantallas ejemplares de un dispositivo de visualización cuando se ejecuta una aplicación que incluye el procedimiento de la presente invención.

Descripción detallada de formas de realización ejemplares de la invención

[0029] Con referencia a los dibujos, la **figura 1** muestra esquemáticamente los elementos, alojados en un dispositivo de usuario **100**, que son considerados por el procedimiento de la presente invención. El dispositivo de usuario **100** puede ser, por ejemplo, un smartphone o tableta.

[0030] El dispositivo **100** comprende una unidad de procesamiento (CPU) **105**, una pantalla **110**, p. ej., una pantalla multitáctil, recursos de memoria ROM y RAM (no mostrados), una o más unidades transmisoras/receptoras **115** (p. ej. para wifi, redes móviles 2g-3g-4g, *Bluetooth*, NFC).

[0031] Un "recurso" $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ destinado como componente físico o virtual (recurso físico o recurso virtual) del dispositivo **100**, como componente físico o virtual capaz de generar datos $\mathbf{d_1}$, $\mathbf{d_2}$, $\mathbf{d_3}$… $\mathbf{d_m}$, mediante, por ejemplo, la detección del entorno circundante, interactuando con el usuario, comunicándose con recursos externos, etc. En el caso de que el dispositivo sea un smartphone o tableta, un ejemplo de recurso físico es el acelerómetro, el receptor de GPS, el módulo de transmisión NFC, etc., mientras que un ejemplo de recurso virtual es el administrador de conexión *Bluetooth.*

[0032] Una lista de recursos del dispositivo R_D es la lista de recursos $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ disponibles en un dispositivo D, como el dispositivo **100** [1]:

$$R_{D=\{r_1,r_2,\ldots,r_n\}}$$

[0033] Cada recurso $\mathbf{r_i}$ (i= 1-n) puede generar múltiples datos. Por ejemplo, con referencia a la **figura 1,** el recurso **r2** genera los datos $\mathbf{d_1}$, $\mathbf{d_3}$. La lista de datos generados por un recurso genérico $\mathbf{r_i}$ se llama Fuente de recurso de datos $v(r_i)$, y se define del modo siguiente.

[0034] Dada la Fuente de recurso de datos DD que es la lista de todos los datos posibles $\mathbf{d_1}$, $\mathbf{d_2}$, $\mathbf{d_3}$… $\mathbf{d_m}$ que pueden ser generados por el dispositivo [2]:

$$DD = \{\mathbf{d_1}, \mathbf{d_2}, \mathbf{d_3}, \ldots, \mathbf{d_m}\}$$

La fuente de recurso de datos $v(\mathbf{r_i})$ de un recurso dado $\mathbf{r_i}$ es [2]:

$$v(r_i) = \left\{ d_j \middle| d_j \in DD \bigwedge r_i \xrightarrow{gen} d_j \right\}$$

[0035] Las Fuentes de recurso de datos $v(r_i)$ (i= 1-n) de todos los recursos $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ de un dispositivo D pueden solaparse, lo que quiere decir que cualquier dato dado $\mathbf{d_1}$, $\mathbf{d_2}$, $\mathbf{d_3}$… $\mathbf{d_m}$ puede generarse desde múltiples recursos $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$.

[0036] Los datos generados $\mathbf{d_1}$, $\mathbf{d_2}$, $\mathbf{d_3}$… $\mathbf{d_m}$ pueden agruparse en clases de datos generados referidos a tipos similares de datos, p. ej. datos de POSICIONAMIENTO, datos de COMUNICACIÓN, etc. (se pueden definir otras clases).

[0037] La tabla de abajo muestra como un subconjunto de ejemplos de recursos $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ pueden agruparse en clases (p. ej. basado en la similaridad de los datos generados $\mathbf{d_1}$, $\mathbf{d_2}$, $\mathbf{d_3}$… $\mathbf{d_m}$):

Tabla 1: subconjunto de recursos

Clase	Recurso	Descripción
Posicionamiento	ACCESS_CHECKIN_PROPERTIES	Permite leer/escribir acceso en las tablas de "propiedades" en el registro de la base de datos, para cambiar valores que son cargados
	ACCESS_COARSE_LOCATION	Permite que una aplicación acceda a una ubicación aproximada derivada de fuentes de ubicación de red tales como torres de telefonía y wifi.
	ACCESS_FINE_LOCATION	Permite que una aplicación acceda a una ubicación precisa desde otras fuentes de ubicación tales como el GPS, torres de telefonía y wifi.
	ACCESS_LOCATION_EXTRA_COMMANDS	Permite que una aplicación acceda a comandos extras del proveedor de la ubicación.
	CONTROL_LOCATION_UPDATES	Permite activar/desactivar las notificaciones de actualización de ubicación desde radioenlace.
	ACCESS_MOCK_LOCATION	Permite que una aplicación cree proveedores con ubicación de prueba para testeo.
Comunicación	CALL_PHONE	Permite que una aplicación inicie una llamada sin pasar por la interfaz de marcación para que el usuario confirme la llamada.
	CALL_PRIVILEGED	Permite que una aplicación llame a cualquier número, incluyendo números de emergencia, sin pasar por la interfaz de marcación para que el usuario confirme la llamada.
	PROCESS_OUTGOING_CALLS	Permite que una aplicación monitorice, modifique o aborte llamadas salientes.
	READ_SMS	Permite que una aplicación lea los SMS.
	RECEIVE_MMS	Permite que una aplicación monitorice los mensajes MMS entrantes, registrar o realizar un procesamiento de los mismo.
	RECEIVE_SMS	Permite que una aplicación monitorice los mensajes SMS entrantes, registrar o realizar un procesamiento de los mismo.
	RECEIVE_WAP_PUSH	Permite que una aplicación monitorice los mensajes WAP entrantes.
	SEND_SMS	Permite que una aplicación envíe mensajes SMS.
	WRITE_SMS	Permite que una aplicación escriba mensajes SMS.
	READ_CALL_LOG	Permite que una aplicación lea el registro de llamadas del usuario.
	READ_SOCIAL_STREAM	Permite que una aplicación lea el ámbito social del usuario.
	ADD_VOICEMAIL	Permite que una aplicación añada buzones de voz al sistema operativo (p. ej. Android)
	USE_SIP	Permite que una aplicación use el servicio SIP.
	WRITE_CALL_LOG	Permite que una aplicación escriba (pero o lea) los datos de los contactos del usuario.

[0038] Una aplicación alojada $\mathbf{a_1}$, $\mathbf{a_2}$… $\mathbf{a_p}$ es un servicio, ya sea alojada física o virtualmente en el dispositivo (p. ej. mediante una conexión remota), que puede acceder a los recursos $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ del dispositivo D. La lista de aplicaciones alojadas de un dispositivo D se llama Lista de aplicaciones del dispositivo A_D. Dado el dispositivo D, la

Lista de aplicaciones de dispositivo A_D se define como el conjunto de aplicaciones **a1**, **a2**… **ap** alojadas en el dispositivo [4]:

$$A_D = \left\{ a_1, a_2, \ldots, a_p \middle| D \xrightarrow{host} a \right\}$$

[0039] La lista de recursos **r1**, **r2**… **rn** (y los datos generados asociados **d1, d2**, **d3**… **dm**) que pueden ser accedidos por una aplicación alojada **a1**, **a2**… **ap** se llama Informe de aplicación $w(a_i)$. En una aplicación alojada a_i (¡ = 1-p), su informe de aplicación queda definido como [5]:

$$w(a_i) = \left\{ r_j \middle| r_j \in R_D \bigwedge a_i \xrightarrow{reg} r_j \right\}$$

Donde *reg* es la función de registro, que es la función que se aplica a cualquier recurso que se requiera por una aplicación alojada **a1**, **a2**… **ap** cuando la aplicación alojada es instalada en el dispositivo del usuario, o cuando la aplicación alojada instalada accede por primera vez al recurso (dependiendo de la arquitectura del sistema operativo del dispositivo del usuario 100)

[0040] De [5] se puede deducir que una aplicación alojada a_i (¡ = 1-p) tiene acceso a la fuente del conjunto de datos $v(r_i)$ (i= 1-n) de todos los recursos **r1**, **r2**… **rn** en su informe de aplicación $w(a_i)$ [6]:

$$\left\{ d_j \middle| r_k \in w(a_i) \bigwedge d_j \in v(r_k) \right\}$$

[0041] Se asume que en el primer acceso todas las aplicaciones alojadas a_i (¡ = 1-p) declaran explícitamente la respectiva fuente del conjunto de datos $v(r_i)$ (i= 1-n), y esto autoriza a esa aplicación alojada el acceso a la lista de recursos.

[0042] Los procedimientos de seguridad o las tecnologías para evitar acceso fraudulento a los recursos del dispositivo pueden contemplarse, pero este no es la prioridad de la presente invención.

[0043] Una aplicación alojada **a1**, **a2**… **ap** en un tiempo genérico t, puede estar en cuatro estados diferentes:

- ACTIVO: si la aplicación alojada está en ejecución y en la modalidad de usuario interactivo;
- EJECUTANDO: si la aplicación alojada está en ejecución (por lo que puede acceder a un recurso) pero sin estar en la modalidad de usuario interactivo (p. ej. en segundo plano);
- ESCUCHANDO: si la aplicación alojada no está en ejecución, pero está registrada como “oyente” de algunos recursos (todos o parte de aquellos en el informe de aplicaciones de la misma), p. ej. la aplicación alojada puede activarse si ocurre cualquier evento en lo recursos escuchados (p. ej. cuando un recurso se activa en el dispositivo o genera datos);
- APAGADO: si la aplicación alojada no está en ejecución y no está registrada como “oyente” de ningún recurso

[0044] El procedimiento de medición de acuerdo con una forma de realización de la presente invención asume que cada recurso en la lista de recursos del dispositivo R_D se asocia con un valor de sensibilidad al recurso respectivo. El valor de sensibilidad del recurso permite la discriminación de recursos **r1**, **r2**… **rn** basado en la sensibilidad de los datos **d1, d2**, **d3**… **dm** que generan en términos de privacidad, precisión, etc. Esto viene de la hipótesis de que no todos los datos tienen la misma importancia para el usuario en diferentes contextos (p. ej. la posición GPS puede decir mucho más sobre un usuario que los valores del acelerómetro).

[0045] El valor de sensibilidad del recurso $s(r_i)$ de un recurso r_i es un valor numérico en la escala de sensibilidad S [7]:

$$S = (0; s_{max}] in R$$

[0046] Tanto es así que si $s(r_i) > s(r_j)$, el recurso r_i genera datos que son más sensibles que aquellos generados por el recurso r_j de acuerdo con algún parámetro, p. ej. la privacidad del dueño del dispositivo. Por ejemplo, en referencia con la tabla 1, el recurso "ACCESS_FINE_LOCATION" se caracteriza por un mayor valor de sensibilidad que el recurso "USE_SIP": el acceso a la posición real del dispositivo (y, por tanto, del dueño) es más sensible, desde el punto de vista de la privacidad, que la posibilidad de activar el protocolo de comunicación SIP.

[0047] La tabla de abajo muestra un subconjunto de todos los recursos disponibles $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ (columna "recurso") agrupado por clases (columna "clases") y, para cada recurso r_i (i= 1-n), un ejemplo del valor de sensibilidad del recurso asociado $s(r_i)$:

Clase	Recurso $r_i(i$=1-n)	Sensibilidad del recurso $s(r_i)$
Posicionamiento	ACCESS_CHECKIN_PROPERTIES	3
	ACCESS_COARSE_LOCATION	11
	ACCESS_FINE_LOCATION	11
	ACCESS_LOCATION_EXTRA_COMMANDS	5
	CONTROL_LOCATION_UPDATES	1
	ACCESS_MOCK_LOCATION	10
Comunicación	CALL_PHONE	10
	CALL_PRIVILEGED	10
	PROCESS_OUTGOING_CALLS	10
	READ_SMS	10
	RECEIVE_MMS	10
	RECEIVE_SMS	10
	RECEIVE_WAP_PUSH	3
	SEND_SMS	1
	WRITE_SMS	1
	READ_CALL_LOG	10
	READ_SOCIAL_STREAM	10
	ADD_VOICEMAIL	1
	USE_SIP	1

[0048] La escala de sensibilidad S puede ser global o adaptada al nivel usuario, nivel del dispositivo, etc. Y está relacionada con el contexto de la medición (p. ej. privacidad, trazabilidad, etc.). En una forma de realización de la presente invención, $s_{max}= 100$.

Medición del nivel de acceso

[0049] De acuerdo con la presente invención, se mide el nivel de acceso a datos personales. En particular, el nivel de acceso a datos personales se mide a nivel de las aplicaciones alojadas individuales (nivel de acceso por aplicación alojada o nivel de acceso de aplicación), y a nivel del dispositivo en su totalidad (nivel de acceso por el dispositivo o nivel de acceso del dispositivo).

[0050] En una forma de realización de la presente invención, el nivel de acceso se mide a tres diferentes niveles de granularidad, de ahora en adelante referidos como:

- Nivel de acceso a datos personales por la aplicación alojada;
- Nivel de acceso a datos personales instantáneos por el dispositivo;
- Nivel de acceso a datos personales globales por el dispositivo.

[0051] El nivel de acceso a los datos personales por la aplicación alojada clasifica una aplicación alojada a_i (¡ = 1-p) basada en el número de recursos que requeridos por la aplicación alojada y el valor de sensibilidad del recurso $s(r_i)$ (i= 1-n) de tales recursos.

[0052] Dada una aplicación alojada a_i (¡ = 1-p) y su informe de aplicación $w(a_i)$, el nivel de acceso a datos personales $P_A(a_i)$ puede definirse como sigue [8]:

$$P_A(a_i) = \begin{cases} \log\left(\prod s(r_k)\right), \forall r_k \in w(a_i) \quad if\ r_c \neg\in w(a_i) \\ \log\left(\prod s(r_k)^2\right), \forall r_k \in w(a_i) \quad if\ r_c \in w(a_i) \end{cases}$$

[0053] Donde r_c es un recurso de comunicación, p. ej. un recurso que activa la conexión y la comunicación de datos desde el dispositivo (p. ej. el recurso de gestión de wifi). Un recurso de comunicación entre aquellos en el informe de aplicación $w(a_i)$ amplifica la accesibilidad de datos personales generados por el dispositivo D. Por consiguiente, en el cálculo del nivel de acceso a los datos personales por la aplicación alojada para cierta aplicación alojada a_i, la presencia, en el informe de aplicación $w(a_i)$ de esa aplicación alojada, de un recurso de comunicación r_c, puede otorgársele más peso mediante, p. ej., ajustando los valores de sensibilidad a todos los recursos requeridos por la aplicación alojada.

[0054] Cuanto mayor es el valor del nivel de acceso a datos personales $P_A(a_i)$ para una aplicación alojada $\mathbf{a}_i$ ($_i$ = 1-p), más sensible es la aplicación.

[0055] Un nivel de acceso a datos personales normalizado por la aplicación alojada es una variable de la medida introducida arriba, que enfatiza el valor medio de sensibilidad de todos los recursos empleados por la aplicación alojada, dando menos influencia a los valores de sensibilidad de los recursos más sensibles.

[0056] Dada la definición [8], el nivel de acceso a datos personales normalizado por la aplicación alojada puede ser calculado de la siguiente forma [9]:

$$\tilde{P}_A(a_i) = \begin{cases} \frac{\prod s(r_k)}{|w(a_i)|}, \forall r_k \in w(a_i) \quad if\ r_c \neg\in w(a_i) \\ \frac{\prod s(r_k)^2}{|w(a_i)|}, \forall r_k \in w(a_i) \quad if\ r_c \in w(a_i) \end{cases}$$

Donde $|w(a_i)|$denota el número de recursos en el informe de aplicación $w(a_i)$ de la aplicación alojada a_i.

[0057] La clasificación del nivel de acceso a datos personales por la aplicación alojada [8] y el nivel de acceso a datos personales normalizado por la aplicación alojada [9] puede ser evaluados usando una suma en lugar de un producto. En este caso es ([8'] y [9']):

$$P_A(a_i) = \begin{cases} \log\left(\sum s(r_k)\right), \forall r_k \in w(a_i) & if\ r_c \neg\in w(a_i) \\ \log\left(\sum s(r_k)^2\right), \forall r_k \in w(a_i) & if\ r_c \in w(a_i) \end{cases}$$

$$\tilde{P}_A(a_i) = \begin{cases} \frac{\sum s(r_k)}{|w(a_i)|}, \forall r_k \in w(a_i) & if\ r_c \neg\in w(a_i) \\ \frac{\sum s(r_k)^2}{|w(a_i)|}, \forall r_k \in w(a_i) & if\ r_c \in w(a_i) \end{cases}$$

[0058] Sin embargo, el uso del producto enfatiza la contribución de los recursos más sensibles.

[0059] Las funciones [8] y [8'] siguen siendo válidas, en lugar de la función "log", se usa una función genérica *f(x)*, como:

$$f(x) = \begin{cases} x \in R, & f(x) \in R \\ f'(x) > 0 & \forall x \in R \end{cases}$$

[0060] El nivel de acceso a datos personales instantáneos por el dispositivo es una variable de [8] y [9] que tiene en cuenta el número actual de veces que una aplicación alojada hace uso de un recurso. Esta variable es aplicable a aquellos servicios que hacen accesible la cuenta a los eventos de acceso.

[0061] Siendo t_{l-1} y t_l los instantes a ser consideradas en la medición, donde t_l es un instante genérico, t_{l-1} es el instante previo y T_l es la franja de tiempo como [10]:

$$T_l = [t_{l-1}, t_l] \ , \ t_{l-1} < t_l$$

Y se permite a count (a_i, rk, T_l) ser el número de accesos al recurso $\mathbf{r_k}$ por una aplicación alojada a_i en la franja de tiempo T_l. El nivel de acceso a datos personales instantáneos por una aplicación alojada en t_l es [11]:

$$\hat{P}_A(a_i, t_l) = \begin{cases} \log\left(\prod s(r_k) \cdot count(a_i, r_k, T_l)\right), \forall r_k \in w(a_i) & if\ r_c \neg\in w(a_i) \\ \log\left(\prod s(r_k)^2 \cdot count(a_i, r_k, T_l)\right), \forall r_k \in w(a_i) & if\ r_c \in w(a_i) \end{cases}$$

[0062] El nivel de acceso a datos personales instantáneos por la aplicación alojada en t_l es "ponderado" en el sentido de que los valores de sensibilidad al recurso en las fórmulas son multiplicados por un coeficiente que representa el número de accesos a los datos generados por un recurso considerado en la franja de tiempo. Así, cuanto mayor es el número de veces que una aplicación alojada accede a los datos de cierto recurso, mayor es el peso dado a ese recurso en el cálculo del nivel de acceso a los datos personales instantáneos por la aplicación alojada.

[0063] Posiblemente, la franja de tiempo T_l también puede reducirse al instante de tiempo, esto es $t_{l-1} = t_l$.

[0064] El nivel de acceso a datos personales instantáneos por el dispositivo indica, en un cierto momento, el estado de acceso a datos personales basados en las aplicaciones alojadas que están en ejecución en este momento.

[0065] Para un dispositivo dado D, teniendo una lista de aplicaciones del dispositivo A_D, el nivel de acceso a datos personales instantáneos por el dispositivo I_D en el instante de tiempo considerado t_l se calcula de la siguiente forma [12]:

$$\mathbf{I}_D(t_l) = \prod P_A(a_i).$$

$\forall\, a_i \in A_D \wedge status\,(a_i, tl) \in \{ACTIVO, EN\ EJECUCIÓN, ESCUCHANDO\}$ o [13]

$$\mathbf{I}_D(t_l) = \prod \breve{P}_A(a_i).$$

$\forall\, a_i \in A_D \wedge status\,(a_i, tl) \in \{ACTIVO, EN\ EJECUCIÓN, ESCUCHANDO\}$ o [14]

$$\mathbf{I}_D(t_l) = \prod \hat{P}_A(a_i, t_l).$$

[0066] $\forall\, a_i \in A_D \wedge status\,(a_i, tl) \in$ □{*ACTIVO, EN EJECUCIÓN, ESCUCHANDO*} dependiendo del procedimiento empleado para calcular el nivel de acceso a datos personales por la aplicación alojada (p. ej., dependiendo de si se usa la fórmula [8] o [9] o [11] para calcular el nivel de acceso a los datos personales por la aplicación alojada), donde t_l pertenece a T_l como en [10].

[0067] La medición anterior está calculada en base a las aplicaciones alojadas que están en estado ACTIVO, EN EJECUCIÓN O ESCUCHANDO, p. ej. que pueden acceder a cualquiera de los recursos a los que se hayan registrado.

[0068] La medida del nivel de acceso a datos personales por dispositivo también puede ser global, no dependiendo por tanto del instante cuando es calculado sino en relación con la vida completa de un dispositivo D. Dada las asunciones de [12],[13] y [14], el nivel de acceso a datos personales globales por un dispositivo se calcula como [15]:

$$\mathbf{G}_D(t_l) = \prod P_A(a_i). \quad \forall a_i \in A_D$$

O [16]

$$\mathbf{G}_D(t_l) = \prod \breve{P}_A(a_i).\ \forall a_i \in A_D$$

O [17]

$$\mathbf{G}_D(t_l) = \prod \hat{P}_A(a_i, t_l).\ \forall a_i \in A_D$$

Dependiendo del procedimiento empleado para calcular el nivel de acceso a datos personales por la aplicación alojada. En [17] la franja de tiempo considerada T_l coincide con la vida entera del terminal.

[0069] En caso de que el valor resultante del nivel de acceso a datos personales globales por el dispositivo sea muy alto, es posible expresar este valor en decibelios:

$$I'_D(t_l) = 10 * log\,(I_D(t_l))$$

[0070] El nivel de acceso a datos personales globales por dispositivo es una medición más general que da una indicación en cuando al estado del dispositivo D.

[0071] La clasificación de aplicaciones del dispositivo es una lista que indica la relación entre las aplicaciones alojadas de un dispositivo D basado en su medido nivel de acceso a datos personales.

[0072] Dado un dispositivo D y su lista de aplicaciones del dispositivo D_A, la clasificación de aplicaciones del dispositivo D_R queda definido como [18]:

$$D_R = a_1, a_2, ..., a_n, \forall a \in A_D \mid P_A(a_1) > P_A(a_2) > ... > P_A(a_n)$$

[0073] La clasificación de aplicaciones del dispositivo calculada puede emplearse para mostrar a los usuarios de teléfonos móviles que la aplicación alojada en el dispositivo ordenado por el nivel de acceso a los datos personales asociados por la aplicación alojada (como se describirá más adelante).

Monitorización

[0074] Es posible monitorizar cómo cambian con el tiempo el nivel de acceso a datos personales globales por dispositivo y el nivel de acceso a datos personales instantáneos por las mediciones del dispositivo, cuando ocurre un evento en una aplicación alojada.

[0075] Un evento en una aplicación alojada es un evento que modifica la lista de aplicaciones del dispositivo que está en un estado determinado. El nivel de acceso a datos personales globales medidos por el dispositivo y/o el nivel de acceso a datos personales instantáneos medidos por el dispositivo cambiarán en consecuencia.

[0076] Hay cinco eventos de aplicaciones alojadas posibles:

- INSERTAR
- BORRAR
- ACTUALIZAR
- EMPEZAR
- PARAR

[0077] El evento INSERTAR ocurre cuando una aplicación alojada nueva con el estatus de APAGADO se añade a la lista de aplicaciones del dispositivo.

[0078] En consecuencia, el nivel de acceso a datos personales instantáneos por medición del dispositivo no cambiará, pero el nivel de acceso a datos personales globales por medición del dispositivo puede incrementarse.

[0079] Dada las mismas asunciones de [12], [13] y [14], siendo t_e el instante donde el evento INSERTAR relacionado con una aplicación alojada ocurre y dado un instante t' como $t' < t_{e'}$, es:

$$\begin{cases} I_D(t_e) = I_D(t') \\ G_D(t_e) = G_D(t') * \Delta G_D(a) \end{cases}$$

Donde $\Delta G_D(a) > 0$ depende del procedimiento empleado para calcular el nivel de acceso a datos personales por una aplicación alojada:

$$\Delta G_D(a) = \begin{cases} P_A(a) & fórmula\ (15) \\ \breve{P}_A(a_i) & fórmula\ (16) \\ \tilde{P}_A(a, t_e) & fórmula\ (17) \end{cases}$$

[0080] El evento BORRAR ocurre cuando se borra una aplicación alojada nueva con el estado de APAGADO de la lista de aplicaciones del dispositivo.

[0081] Por consecuencia, el nivel de acceso a datos personales instantáneos por la medición del dispositivo no cambiará, pero el nivel de acceso a datos personales globales puede descender.

[0082] Dada las mismas asunciones de [12], [13] y [14], siendo t_e el instante donde el evento INSERTAR relacionado con una aplicación alojada ocurre y dado un instante t' como $t' < t_{e'}$, es:

$$\begin{cases} I_D(t_e) = I_D(t') \\ G_D(t_e) = \dfrac{G_D(t')}{\Delta G_D(a)} \end{cases}$$

Donde $\Delta G_D(a) > 0$ depende del procedimiento empleado para calcular el nivel de acceso a datos personales por una aplicación alojada:

$$\Delta G_D(a) = \begin{cases} P_A(a) & fórmula\ (15) \\ \breve{P}_A(a_i) & fórmula\ (16) \\ \tilde{P}_A(a, t_e) & fórmula\ (17) \end{cases}$$

[0083] El evento ACTUALIZAR ocurre cuando una de las aplicaciones alojadas en la lista de aplicaciones del dispositivo cambia de manera que los recursos $\mathbf{r_1}$, $\mathbf{r_2}$… $\mathbf{r_n}$ que esta emplea, cambian.

[0084] Por consiguiente, el nivel de acceso a datos personales globales por la medición del dispositivo cambiará; el nivel de acceso a datos personales instantáneos por la medición del dispositivo cambiará solo si la actualización de la aplicación no está en estado APAGADO cuando el evento ocurra.

[0085] Dada las mismas asunciones de [12], [13] y [14], siendo t_e el instante donde el evento ACTUALIZAR relacionado con una aplicación alojada ocurre y dado un instante t' como $t' < t_{e'}$, es:

$$\begin{cases} I_D(t_e) = I_D(t') & si\ a\ está\ en\ estado\ APAGADO\ en\ t_e \\ I_D(t_e) = I_D(t') * \Delta P(a) & si\ a\ no\ está\ en\ estado\ APAGADO\ en\ t_e \\ G_D(t'') = G_D(t') * \Delta P(a) \end{cases}$$

donde $\Delta P(a)$ depende del procedimiento empleado para calcular el nivel de acceso a datos personales por la aplicación alojada. $\Delta P(a)$ es mayor o menor que cero dependiendo del nuevo conjunto de recursos que la aplicación

accede siendo más o menos sensible que la antigua.

[0086] El evento EMPEZAR ocurre cuando una de las aplicaciones alojadas en la lista de aplicaciones del dispositivo cambia su estado de APAGADO uno de los otros tres estados (ACTIVO, EN EJECUCIÓN, ESCUCHANDO). Por consiguiente, el nivel de acceso a los datos personales globales por la medición del dispositivo no cambiará, mientras que el nivel de acceso a los datos personales instantáneos por la medición del dispositivo cambiará.

[0087] Dada las mismas asunciones de [12], [13] y [14], siendo t_e el instante donde el evento EMEZAR relacionado con una aplicación alojada **a** ocurre y dado un instante t' como t' < $t_{e'}$, es:

$$\begin{cases} G_D(t_e) = G_D(t') \\ I_D(t_e) = I_D(t') * \Delta I_D(a) \end{cases}$$

Donde $\Delta G_D(a) > 0$ depende del procedimiento empleado para calcular el nivel de acceso a datos personales por una aplicación alojada:

$$\Delta I_D(a) = \begin{cases} P_A(a) \quad fórmula\ (15) \\ \breve{P}_A(a_i) \quad fórmula\ (16) \\ \tilde{P}_A(a, t_e) \quad fórmula\ (17) \end{cases}$$

[0088] El evento PARAR ocurre cuando una de las aplicaciones alojadas en la lista de aplicaciones del dispositivo cambia su estado de uno de los tres estados ACTIVO, EN EJECUCIÓN O ESCUCHANDO al estado APAGADO. Por consiguiente, el nivel de acceso de datos personales globales por la medición del dispositivo disminuirá.

[0089] Dada las mismas asunciones de [12], [13] y [14], siendo t_e el instante donde el evento PARAR relacionado con una aplicación alojada **a** ocurre y dado un instante t' como t' < $t_{e'}$, es:

$$\begin{cases} G_D(t_e) = G_D(t') \\ I_D(t_e) = \dfrac{I_D(t')}{\Delta I_D(a)} \end{cases}$$

Donde $\Delta G_D(a) > 0$ depende del procedimiento empleado para calcular el nivel de acceso a datos personales por una aplicación alojada:

$$\Delta I_D(a) = \begin{cases} P_A(a) \quad fórmula\ (15) \\ \breve{P}_A(a_i) \quad fórmula\ (16) \\ \tilde{P}_A(a, t_e) \quad fórmula\ (17) \end{cases}$$

[0090] El diagrama de la **figura 2** muestra un ejemplo del nivel de acceso a datos personales globales por un dispositivo (I_D, indicado como GPDAL en el dibujo) vs tiempo, calculado como en [15] cuando un usuario realiza una acción sobre las aplicaciones alojadas en su dispositivo D, en particular cuando el número de aplicaciones alojadas que acceden a los recursos de su dispositivo cambian. Estos valores de I_D son calculados por [15] y expresados en

dB.

[0091] La tendencia de la función GPDAL queda explicada por los siguientes eventos ejemplares:

- En t = 10:00, el usuario desinstala una aplicación que usa un recurso de comunicación (evento BORRAR);
- En t = 13:00, el usuario instala una aplicación que no usa un recurso de comunicación (evento INSERTAR);
- En t = 15:00, el usuario desinstala una aplicación que no usa un recurso de comunicación (evento BORRAR);
- En t = 17:00, el usuario instala una aplicación que usa un recurso de comunicación (evento INSERTAR);
- En t = 18:00, el usuario desinstala una aplicación que usa un recurso de comunicación (evento BORRAR);

Trabajo experimental

[0092] El procedimiento de la presente invención ha sido incluido en una aplicación Android, llamada “Privacy Owl”.

[0093] Esta aplicación le da al usuario la indicación de la cantidad de datos compartidos con los proveedores de las aplicaciones instaladas en su teléfono inteligente o tableta.

[0094] La **figura 3, la figura 4** y **la figura 5** muestran algunas capturas de pantalla de la pantalla **110** del dispositivo del usuario cuando la aplicación *Privacy Owl* está siendo ejecutada.

[0095] La **figura 3** muestra la captura de pantalla de la pantalla de inicio de la aplicación *Privacy Owl;* muestra cuántas aplicaciones han sido instaladas en el dispositivo del usuario y un termómetro correlacionado con el valor calculado del acceso a los datos personales globales por el nivel del dispositivo calculado por la fórmula [15].

[0096] Mediante la selección de “cambiar”, el usuario puede cambiar del modo ACTIVO al modo EN EJECUCIÓN de la aplicación *Privacy Owl*.

[0097] Mediante la selección de “detalles” el usuario puede ver la lista de aplicaciones. Cada aplicación A_i tiene su propio logo y un icono asociado que (asumiendo que el dispositivo del usuario tiene una pantalla a color **110**) puede ser rojo, amarillo o verde; en la **figura 4** el icono **405** asociado con cada aplicación se representa como un círculo, y el color rojo se representa con líneas transversales, el color rojo se representa con líneas verticales y el color verde se representa con líneas horizontales. El color del icono asociado con cierta aplicación está correlacionado con el nivel de acceso a datos personales por la aplicación $P_A(A_i)$ por esa aplicación A_i calculado por la fórmula [8]. La lista de las aplicaciones mostradas puede tener en cuenta la clasificación de aplicaciones del dispositivo calculada.

[0098] Si $P_A(A_i)$ es el nivel de acceso a datos personales por la aplicación alojada por aplicación A_i, se fijan dos umbrales p_1 y p_2, con $p_1 < p_2$: el color se asigna a una aplicación A_i mediante la siguiente fórmula:

$$\begin{cases} rojo\ si\ \mathbf{P}_A(A_i) > p_2 \\ amarillo\ si\ p_1 \leq \mathbf{P}_A(A_i) \leq p_2 \\ verde\ si\ \mathbf{P}_A(A_i) < p_1 \end{cases}$$

[0099] Al seleccionar una aplicación, el usuario puede comprobar a qué datos puede acceder la aplicación **(figura 5),** de acuerdo con su informe de aplicación.

[0100] Cada recurso en el informe de aplicación tiene un icono asociado **505** que puede ser rojo, amarillo o verde. En la **figura 5,** el icono **505** asociado con cada aplicación está representado como un círculo, y el color rojo está representado con líneas verticales y el color verde se representa con líneas horizontales.

[0101] El color está correlacionado con el valor de sensibilidad del recurso para ese recurso, cuanto mayor es el valor de la sensibilidad del recurso, más oscuro es el color.

[0102] La presente invención puede ser útil para hacer ver a los usuarios la cantidad y calidad de los datos almacenados en sus dispositivos personales y compartidos por las aplicaciones que instalan y usan. Las medidas

introducidas como se describe anteriormente, expresadas como simple indicadores, proporcionan una manera fácil de entender para acceder a estas informaciones.

[0103] La presente invención tiene múltiples usos prácticos.

[0104] Por ejemplo, la presente invención puede usarse para conducir un estudio para evaluar las modificaciones en el comportamiento de los usuarios debido a este conocimiento, haciéndoles capaces de monitorizar los datos personales generados por los recursos de sus dispositivos.

[0105] El estudio puede estructurarse de la siguiente forma:

1. Se le pide al usuario completar una encuesta para saber sobre sus conocimientos de los problemas de seguridad relacionados con el uso de la aplicación de un dispositivo;
2. En un periodo de tiempo concreto, p. ej. un mes, se hace un seguimiento de los patrones de uso, en términos de tiempo, frecuencia, etc. En el dispositivo del usuario;
3. Proporcionándole al usuario las indicaciones introducidas con esta invención (niveles de acceso a los datos personales globales e instantáneos), se vuelve a hacer un seguimiento de los patrones de uso, en términos de frecuencia, etc., de las aplicaciones instaladas en el dispositivo del usuario. En este periodo, se le impulsa al usuario con qué datos se usan por qué aplicación y cuántos más datos se comparten debido a cierta aplicación:
4. Se repite la encuesta desde el paso 1.

[0106] Desde la perspectiva del cambio de comportamiento, este estudio hace posible rastrear, mientras que al usuario se le proporcionan las indicaciones sobre la cantidad y calidad de los datos personales que usa cierta aplicación, si:

t la aplicación se usa menos;
t la aplicación ya no se usa;
t la aplicación ha sido desinstalada.

[0107] Esta información puede ser de utilidad para los directores de las aplicaciones y también para los desarrolladores de las aplicaciones, para decidir si continuar o no proponiendo una aplicación para los usuarios o rediseñarla.

[0108] La solución, de acuerdo con la presente invención, puede ser utilizada ventajosamente en sistemas para compartir e intercambiar datos personales de usuarios, en lo que una operadora TLC tiene un rol en la garantización y certificación de los datos intercambiados, y el intercambio propio con terceros.

REIVINDICACIONES

1. Un procedimiento para medir y monitorizar el uso de datos (**d_1, d_2,… d_m**) almacenados en un dispositivo por el software de las aplicaciones instaladas en el dispositivo del usuario (**100**), donde dichos datos son generados por recursos (**r_1, r_2, r_n**) del dispositivo del usuario. El procedimiento comprende:

a) Por cada una de dichas aplicaciones, asignar un valor de sensibilidad al recurso en una escala de sensibilidad predeterminada, los valores de la sensibilidad de los recursos de los diferentes recursos adaptado para permitir una discriminación de dichos recursos basados en la sensibilidad de los datos que generan;
b) Por cada una de dichas aplicaciones, calcular un nivel de acceso de la aplicación respectivo a dichos datos al combinar mediante una primera función determinada, los valores de sensibilidad del recurso de los recursos que generan los datos accedidos por dicha aplicación;
c) Calcular el nivel de acceso del dispositivo a dichos datos por dichas aplicaciones, en el que dicho nivel de acceso del dispositivo está calculado combinando mediante una segunda función predeterminada los niveles de acceso de la aplicación de las aplicaciones instaladas en el dispositivo;
d) Asociar con cada aplicación una indicación respectiva (**405**) del nivel de acceso de aplicación calculado;
e) Por cada aplicación, mostrar, en una pantalla (**110**) del dispositivo del usuario, la indicación respectiva del nivel de acceso de la aplicación calculado, y
f) Mostrar, en la pantalla del dispositivo del usuario, una indicación del nivel de acceso a dichos datos por dichas aplicaciones.

2. El procedimiento de la reivindicación 1, también comprende:

- Por cada una de dichas aplicaciones, comparar el nivel de acceso de aplicación calculado con un primer valor umbral predeterminado, y
- Por cada una de dichas aplicaciones, presentar en la pantalla del dispositivo del usuario una primera indicación si el nivel de acceso a la aplicación está por debajo del primer valor umbral, o una segunda indicación

3. El procedimiento de la reivindicación 2, también comprende:

- Por cada una de dichas aplicaciones, comparar el nivel de acceso de las aplicaciones calculado respectivamente con un segundo valor umbral predeterminado, mayor que el primer valor umbral, y
- Por cada una de dichas aplicaciones, presentar en la pantalla del usuario una segunda indicación si el nivel de acceso de las aplicaciones calculado está por debajo de un segundo valor umbral o una tercera indicación si el nivel de acceso de la aplicación calculado no está por debajo del segundo valor umbral.

4. El procedimiento de cualquiera de las reivindicaciones precedentes comprende, asimismo:

- definir al menos dos estados operativos distintos en los que cualquiera de dichas aplicaciones pueda estar, y
- repetir los pasos a) a d) de la reivindicación 1 cuando sea que cualquiera de dichas aplicaciones cambia su estado operativo de uno a otro de los ya dichos dos estados operativos, o viceversa.

5. El procedimiento de la reivindicación 4, en el que dichos dos estados operativos, comprenden:

- Un primer estado operativo, cuando una aplicación está en ejecución en el dispositivo del usuario y en un modo de usuario interactivo;
- un segundo estado operativo, cuando una aplicación está en ejecución en el dispositivo del usuario, pero no está en el modo usuario interactivo.
- un tercer estado operativo, cuando una aplicación no está en ejecución en el dispositivo del usuario, pero está escuchando al menos uno de dichos recursos y puede ser activado cuando ocurre un evento relacionado con los recursos escuchados.
- un cuarto estado operativo, cuando una aplicación no está en ejecución y no está escuchando ninguno de dichos recursos.

6. El procedimiento de cualquiera de las reivindicaciones precedentes, en el que dicho cálculo, para cada aplicación, el nivel de acceso de la aplicación respectiva comprende dar más peso en dicha combinación, a los valores de sensibilidad de aquellos recursos que permiten la conexión y la comunicación de datos desde el dispositivo hacia una red externa de datos.

7. El procedimiento de la reivindicación 6, en el que dicho “dar más peso” comprende ajustar los valores de sensibilidad de dichos recursos que permiten la conexión y la comunicación de datos desde el dispositivo hacia una red externa de datos.

8. El procedimiento de cualquiera de las reivindicaciones precedentes, en el que dicha primera función predeterminada comprende una entre: un producto de los valores de sensibilidad de los recursos que genera datos accedidos por dicha aplicación, una suma de los valores de sensibilidad de los recursos que genera datos accedidos por dicha aplicación

9. El procedimiento por el que cualquiera de las reivindicaciones precedentes, en el que dicha segunda función predeterminada comprende un producto de los niveles de acceso de la aplicación calculados de las aplicaciones instaladas en el dispositivo.

10. Un programa informático que comprende al menos porciones de código del programa informático adaptados a realizar el procedimiento de cualquiera de las reivindicaciones precedentes cuando se ejecuta el programa informático en un dispositivo de procesamiento de datos.

11. Un dispositivo de usuario (**100**) que comprende una unidad de procesamiento (**105**), una pantalla (**110**), una pluralidad de recursos ($\mathbf{r_1}$, $\mathbf{r_2}$, $\mathbf{r_n}$) capaz de generar datos ($\mathbf{d_1}$, $\mathbf{d_2}$,… $\mathbf{d_m}$) y una pluralidad de aplicaciones (a1, a2,…ap) que pueden acceder a dichos recursos, y donde la unidad de procesamiento está configurada para realizar el procedimiento de cualquiera de las reivindicaciones 1 a 9.

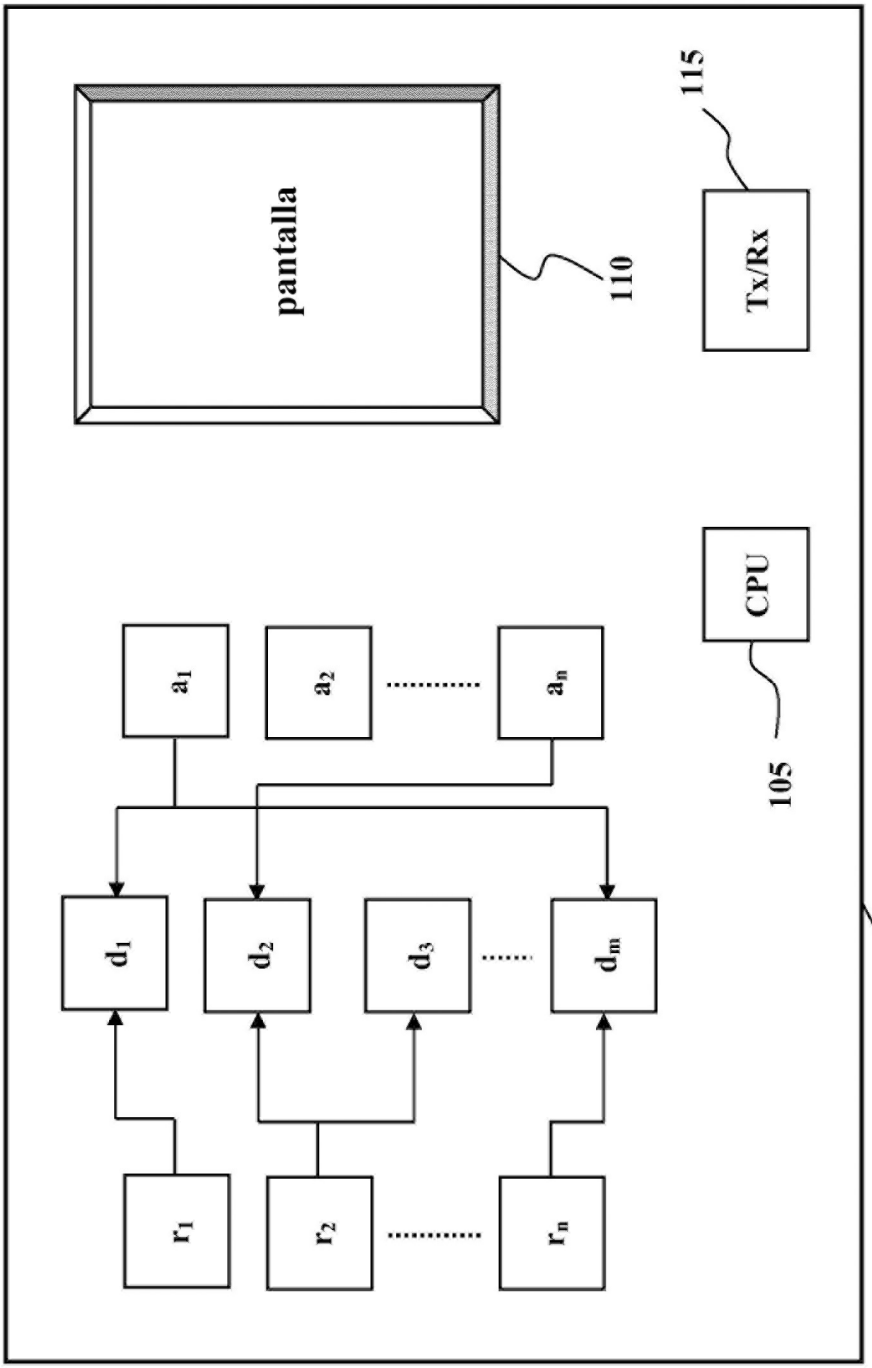

Fig. 1

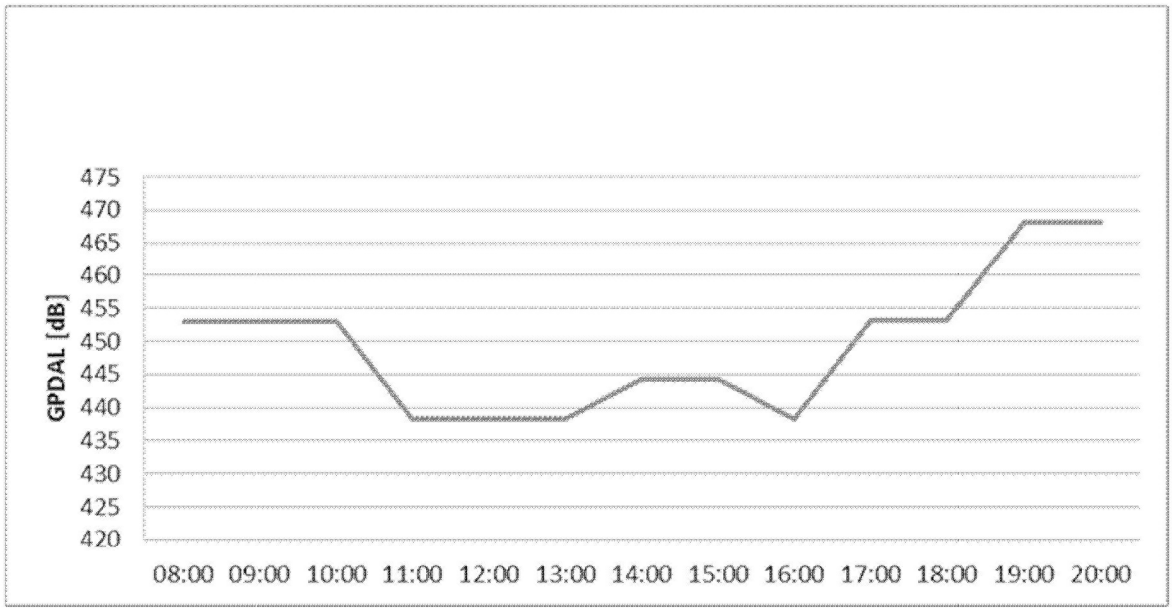
GPDAL [dB]
475
470
465
460
455
450
445
440
435
430
425
420
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00

Fig. 2

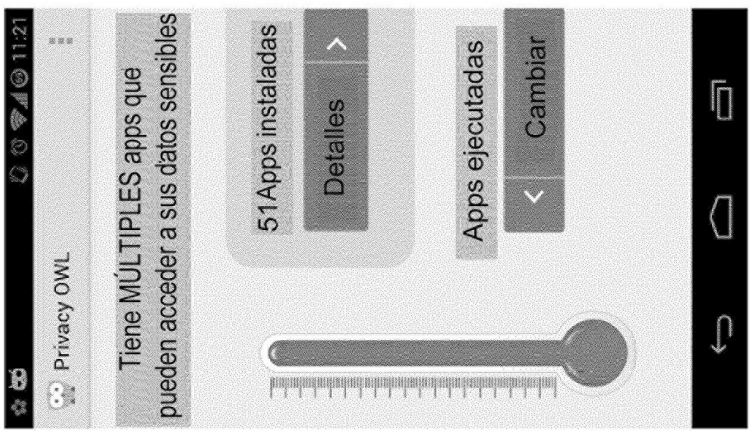

Fig. 3

Fig. 4

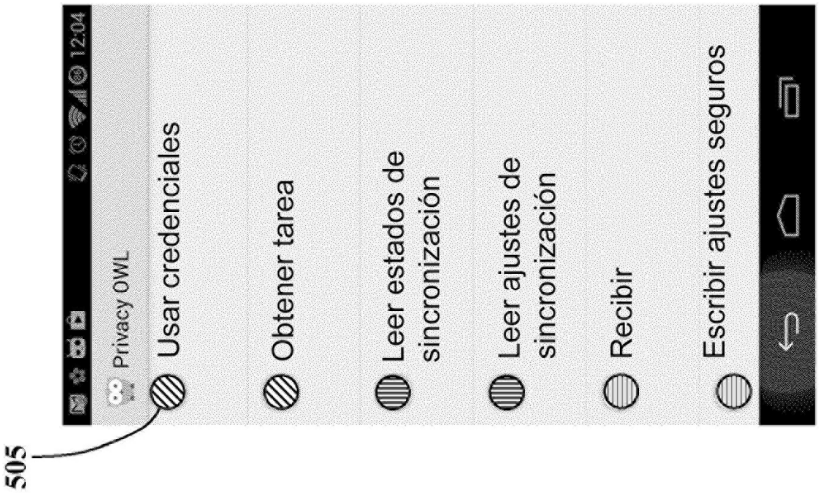

Fig. 5