(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 478 824**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.10.2009 E 09740098 (0)**

(97) Fecha y número de publicación de la concesión europea: **14.05.2014 EP 2489153**

(54) Título: **Método de gestión de políticas de privacidad para un dispositivo de usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.07.2014

(73) Titular/es:

NOKIA SOLUTIONS AND NETWORKS OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

BODI, MIKLOS TAMAS y
MARTON, GABOR

(74) Agente/Representante:

ZUAZO ARALUZE, Alexander

DESCRIPCIÓN

Método de gestión de políticas de privacidad para un dispositivo de usuario.

La invención se refiere a la gestión de políticas, tales como políticas de privacidad que pueden definir, por ejemplo, la medida en la que una aplicación (tal como una aplicación de Internet) puede acceder a detalles de usuario.

Existe un número creciente de servicios y aplicaciones (tales como aplicaciones de Internet) que almacenan datos personales de usuarios. Dado que los individuos usan cada vez más servicios, una cantidad creciente de datos personales quedan expuestos a tales aplicaciones y, por tanto, quedan expuestos potencialmente fuera de esas aplicaciones. Muchos usuarios no son conscientes (o al menos son conscientes sólo parcialmente) de quién tiene acceso a sus datos personales, y para qué fines, y quién puede revelar su identidad personal y otros datos. Como resultado, existe una demanda creciente de protección de la identidad y privacidad.

Un enfoque en la protección de la privacidad es formular políticas de control de acceso para datos personales. Las políticas están constituidas por reglas que definen los derechos de acceso de entidades de un sistema a los atributos personales de los usuarios. Tales políticas pueden formarse en lenguajes de política tales como el lenguaje de marcado de control de acceso extensible (XACML), el proyecto de plataforma para la protección de la privacidad (P3P) y la política común.

Sin embargo, dado que la exposición de datos personales a múltiples aplicaciones y servicios ha aumentado, las políticas de privacidad se han vuelto cada vez más complejas y confusas para el usuario. En un sistema sofisticado, la políticas incluso pueden generarse y modificarse automáticamente.

Es difícil para los usuarios seguir políticas de privacidad que cambian regularmente y estar pendientes de qué servicios (u otras entidades) tienen acceso a qué atributo y por qué. El seguimiento de tales políticas requiere una cantidad de tiempo y esfuerzo que muchos usuarios no están dispuestos a emplear.

La publicación US-2006/212924-A1 da a conocer un método de gestión de políticas con características resumidas en los preámbulos de las reivindicaciones independientes adjuntas.

Sigue existiendo la necesidad de permitir que los usuarios establezcan y modifiquen políticas de privacidad según sus necesidades y deseos, sin que el establecimiento y la modificación de tales políticas no sean excesivamente complejos.

La presente invención busca abordar al menos algunos de los problemas explicados anteriormente.

La presente invención proporciona un método de gestión de políticas de privacidad que comprende: determinar una similitud entre un primer usuario y cada uno de una pluralidad de otros usuarios; determinar, basándose en dicha similitud, cuáles de la pluralidad de otros usuarios son los vecinos más próximos al primer usuario; y proporcionar uno o más parámetros de política de privacidad recomendados al primer usuario basándose en parámetros de política de privacidad de dichos vecinos más próximos determinados.

La presente invención también proporciona un aparato que comprende: una primera entrada para recibir datos en relación con una pluralidad de usuarios; un primer procesador para determinar, basándose en dichos datos, una similitud entre un primer usuario y cada uno de una pluralidad de otros usuarios (a menudo aplicando una o más funciones de distancia); un segundo procesador para determinar, basándose en dicha similitud, cuáles de la pluralidad de otros usuarios son los vecinos más próximos al primer usuario; y un tercer procesador para generar uno o más parámetros de política de privacidad recomendados al primer usuario basándose en parámetros de política de privacidad de dichos vecinos más próximos determinados.

Por tanto, la presente invención proporciona un aparato y un método que buscan ayudar a usuarios a establecer y modificar políticas de privacidad y similares. La invención pretende proporcionar una mejor experiencia de usuario permitiendo que un usuario establezca tales políticas según sus necesidades y deseos, pero con un esfuerzo reducido en comparación con las soluciones conocidas. La invención busca evitar la necesidad de que los usuarios monitoricen continuamente conjuntos de políticas complejas y cambien reglas de política una por una, sin requerir que el usuario acepte conjuntos de políticas globales. La invención pretende proponer parámetros de control de acceso que son los más apropiados para el usuario, mientras se proporciona la flexibilidad para permitir que los usuarios decidan si deben aceptarse parámetros propuestos o no.

Determinar la similitud entre el primer usuario y cada uno de la pluralidad de otros usuarios comprende normalmente determinar, para cada uno de la pluralidad de otros usuarios, la similitud de un primer conjunto de datos asociados con el primer usuario y un segundo conjunto de datos asociados con cada uno de la pluralidad de otros usuarios. Puede definirse una función de distancia para convertir las diferencias entre los conjuntos de datos en una clasificación numérica.

Determinar la similitud entre un primer usuario y uno de dicha pluralidad de otros usuarios puede comprender aplicar una o más funciones de distancia (tal como una función de distancia de atributo de usuario). Las funciones de distancia expresan la similitud entre los datos y, por tanto, entre los usuarios. La función de distancia puede proporcionar un resultado indicativo de la similitud que tiene un valor numérico entre -1 (que indica disimilitud total) y +1 (que indica similitud total).

La invención también puede incluir definir al menos una de dichas una o más funciones de distancia. La función de distancia puede estar relacionada con una variedad de factores, tales como las direcciones particulares de los usuarios o las edades de los usuarios. Las funciones de distancia pueden ponderarse, de manera que las funciones de distancia más importantes tienen más impacto sobre la medida general de similitud entre usuarios que los factores menos importantes.

Determinar la similitud entre usuarios puede incluir considerar la similitud entre al menos algunos de los atributos de usuario de dichos usuarios. Alternativa o adicionalmente, determinar la similitud entre usuarios puede incluir considerar la similitud entre al menos algunas de las decisiones de política de privacidad de dichos usuarios. Los atributos de usuario y las decisiones de política de privacidad son a menudo particularmente relevantes en un entorno de gestión de políticas y perfectamente pueden estar disponibles fácilmente. Naturalmente pueden usarse otras variables además de, o en lugar de, atributos de usuario y/o decisiones de política de privacidad.

En algunas formas de la invención, el vecino más próximo al primer usuario de dicha pluralidad de otros usuarios es aquél de los otros usuarios que tiene la mayor similitud con el primer usuario.

Determinar cuáles de la pluralidad de otros usuarios son los vecinos más próximos al primer usuario puede comprender determinar un número predeterminado de dicha pluralidad de otros usuarios que tienen la mayor similitud con el primer usuario.

En algunas formas de la invención, proporcionar parámetros de política de privacidad recomendados comprende determinar, para una política potencial, si más de una primera proporción predeterminada de dichos vecinos más próximos han establecido dicha política. Por ejemplo puede recomendarse una política de privacidad si más de una primera proporción (por ejemplo dos tercios) de los vecinos más próximos han seleccionado la política.

Alternativa o adicionalmente, proporcionar parámetros de política de privacidad recomendados puede comprender determinar, para una política potencial, si menos de una segunda proporción predeterminada de dichos vecinos más próximos han establecido dicha política. Por ejemplo, puede recomendarse no establecer una política de privacidad particular si menos de una segunda proporción (por ejemplo un tercio) de los vecinos más próximos han seleccionado la política.

En algunas formas de la invención, la etapa de determinar, para una política potencial, si una proporción de dichos vecinos más próximos han establecido dicha política considera sólo los vecinos más próximos que han tomado una decisión con respecto a si establecer dicha política o no. Puede considerarse un número predeterminado de los vecinos más próximos. Si algunos se omiten de la consideración basándose en que estos usuarios no han tomado una decisión sobre la política en cuestión, entonces el número de los vecinos más próximos relevantes puede ser menor. Alternativamente pueden considerarse más vecinos más próximos, incluyendo usuarios adicionales con una similitud ligeramente menor con el primer usuario que los vecinos más próximos.

La invención puede incluir comparar una política de privacidad recomendada para el primer usuario con una actitud principal de dicho primer usuario. Si la actitud principal parece entrar en conflicto con la política de privacidad recomendada, esto puede indicarse al usuario.

La presente invención puede proporcionar un programa informático que comprende: un código (o algún otro medio) para determinar una similitud entre un primer usuario y cada uno de una pluralidad de otros usuarios; un código (o algún otro medio) para determinar, basándose en dicha similitud, cuáles de la pluralidad de otros usuarios son los vecinos más próximos al primer usuario; y un código (o algún otro medio) para proporcionar uno o más parámetros de política de privacidad recomendados al primer usuario basándose en parámetros de política de privacidad de dichos vecinos más próximos determinados. El programa informático puede ser un producto de programa informático que comprende un medio legible por ordenador que porta un código de programa informático incorporado en el mismo para su uso con un ordenador.

A continuación se describen realizaciones ilustrativas de la invención, sólo a modo de ejemplo, con referencia a los siguientes dibujos numerados.

La figura 1 es un diagrama de flujo que muestra un algoritmo según un aspecto de la presente invención;

la figura 2 es una tabla que muestra datos de usuario ilustrativos;

la figura 3 es un diagrama de flujo que muestra un algoritmo según un aspecto de la presente invención;

la figura 4 es un diagrama de flujo que muestra un algoritmo según un aspecto de la presente invención; y

la figura 5 es un diagrama de flujo que muestra un algoritmo según un aspecto de la presente invención.

La presente invención propone un sistema y un método que ayuda a que los usuarios establezcan o modifiquen políticas de privacidad haciendo recomendaciones al usuario con respecto a cómo establecer o modificar tales políticas. Las recomendaciones se basan en información que se conoce sobre el usuario en cuestión, tal como propiedades y preferencias de usuario del usuario, y posiblemente también las propiedades y preferencias usuario de otros, tales como amigos del usuario. Proporcionar recomendaciones dependiendo de las propiedades o preferencias de usuario conocidas hace más fácil que los usuarios formulen sus políticas y conduce así a políticas que reflejan apropiadamente requerimientos de usuario, mientras se reduce la carga para el usuario.

La figura 1 es un diagrama de flujo que muestra un algoritmo, indicado en general mediante el número de referencia 1, según un aspecto de la presente invención. Tal como se describe detalladamente a continuación, el algoritmo 1 busca hacer recomendaciones a un usuario basadas en identificar usuarios similares, determinar políticas aplicadas por los usuarios similares identificados y recomendar que el usuario elija opciones establecidas en las políticas de esos usuarios similares.

Para hacer recomendaciones a un usuario basadas en determinar políticas aplicadas por usuarios similares, en primer lugar el algoritmo debe determinar qué usuarios son usuarios similares. Por tanto, el algoritmo 1 se inicia en la etapa 2, en la que se definen funciones de distancia relacionadas con un número de atributos de usuario. Las funciones de distancia determinan la metodología para representar la distancia entre dos usuarios en relación con un atributo de usuario dado en una escala numérica, tal como se describe adicionalmente a continuación.

Luego, en la etapa 4 se usan datos de usuario para determinar la similitud entre usuarios aplicando las funciones de distancia definidas en la etapa 2. Una vez que se ha determinado la similitud entre un usuario particular y otros usuarios en la etapa 4, el algoritmo pasa a la etapa 6, en la que se determina un número de los vecinos más próximos al usuario. Un vecino próximo es simplemente un usuario que obtiene una calificación alta en las pruebas de similitud de usuario explicadas anteriormente.

Finalmente, en la etapa 8, se hacen recomendaciones de política basadas en las preferencias del/de los vecino(s) más próximo(s) determinado(s).

Tal como se indicó anteriormente, el algoritmo 1 se inicia en la etapa 2, con la definición de funciones de distancia relacionadas con cada uno de un número de atributos. Los atributos de usuario, que perfectamente pueden ser conocidos en un entorno de parámetro de privacidad, pueden usarse para obtener una indicación del nivel de similitud entre dos usuarios diferentes.

Los siguientes son ejemplos del tipo de atributos de usuario que pueden usarse para determinar la similitud entre dos usuarios:

- atributos de perfil tales como nombre, número de teléfono, edad, dirección, puesto laboral, etc.

- atributos de comunidad tales como grupos de comunidad preferidos en sitios web sociales, clubes deportivos favoritos del usuario, religión, etc.

- atributos de identidad tales como identificación de usuario, nombre, sobrenombre, seudónimos del usuario en proveedores de servicio diferentes, etc.

- atributos de contexto tales como ubicación geográfica, actividad, tipo de dispositivo de usuario final, entorno de vida, etc.

La distancia entre dos usuarios según un atributo dado puede definirse de maneras diferentes. Consideremos, por ejemplo, el atributo “dirección particular” de dos usuarios diferentes. Por un lado podemos definir la distancia entre los dos usuarios a partir del aspecto de distancia física de los domicilios de los usuarios. Por otro lado, la “dirección particular” puede hacer referencia al entorno de vida de los usuarios y, a partir de este aspecto, un pueblo en el campo puede representarse muy lejos de una ciudad en otra escala; sin embargo, los dos asentamientos pueden ser relativamente próximos entre sí físicamente.

Los diferentes aspectos del mismo atributo de usuario pueden tratarse como atributos de usuario diferentes. De esta manera, el conjunto de atributos de usuario se extiende con atributos de usuario “nuevos” que representan los diferentes aspectos del mismo atributo.

La presente invención define una función de distancia (d) relacionada con cada atributo de usuario y con los diferentes aspectos del mismo atributo con la restricción de que el codominio de la función de distancia es el conjunto de (-1,+1). El valor de -1 indica disimilitud total y +1 indica similitud total.

En el caso del ejemplo anterior, la función de distancia (d) del atributo “dirección particular” a partir del aspecto de distancia física puede definirse tal como se muestra en la tabla 10 de la figura 2.

La tabla 10 tiene dos columnas. La primera columna muestra la distancia entre la dirección particular de dos usuarios, que se expresa matemáticamente como: $|a_{ki} - a_{kj}|$, donde a_{ki} y a_{kj} son el atributo “dirección particular” del primer usuario (i) y del segundo usuario (j) respectivamente.

La tabla 10 tiene cinco filas. La primera fila indica que si la distancia física entre las direcciones de los usuarios primero y segundo es mayor que 20.000 km, entonces la función de distancia se establece en -1 (lo que indica disimilitud total). La segunda fila indica que si la distancia física es mayor que 5.000 km, pero menos que o igual a 20.000 km, entonces la función de distancia se establece en -0,5 (disimilitud moderada). La tercera fila indica que si la distancia física es mayor que 100 km, pero menos que o igual a 5000 km, entonces la función de distancia se establece en 0 (ni similar ni disimilar). La cuarta fila indica que si la distancia física es mayor que 0, pero menos que o igual a 100 km, entonces la función de distancia se establece en 0,5 (similitud moderada). Finalmente, la quinta fila indica que si la distancia física es 0, entonces la función de distancia se establece en 1 (similitud total).

Para dar otro ejemplo, en el caso del atributo “edad” podemos dividir el ciclo de vida humano en grupos de edad y asignar a cada grupo de edad un número en una escala.

Una vez definidos los métodos sobre cómo definir la distancia entre dos usuarios en relación con cada atributo (y los diferentes aspectos del mismo atributo), puede compararse la similitud entre usuarios diferentes en relación con cada atributo en una escala numérica. Por ejemplo, en el caso de los atributos “dirección particular” tratados anteriormente con referencia a la tabla 10, si los usuarios están separados 12.000 km entre sí, entonces el atributo según la tabla 10 tiene un valor de distancia de -0,5. Naturalmente, la tabla de la figura 2 es uno de muchos ejemplos. Por ejemplo, la tabla puede reemplazarse por una fórmula que define la función de manera que una distancia de 12.000 km puede dar como resultado un valor de función de distancia de entre -0,5 y -1, tal como se define mediante esa fórmula.

Cuantos más aspectos se encuentran para medir la distancia entre dos usuarios, más exactamente puede estimarse la similitud entre usuarios. Los diferentes atributos y aspectos del mismo atributo pueden calcularse con pesos diferentes en la definición de similitud entre dos usuarios. Al configurar pesos es posible afinar la medición de similitudes de usuario a usuario. Por ejemplo, la distancia física entre los atributos “dirección particular” de dos usuarios puede considerarse más importante (y, por tanto, tener un peso mayor) que la diferencia en el atributo “edad” de dos usuarios, cuando se hacen recomendaciones de política de privacidad.

Los atributos de usuario personales no proporcionan las únicas variables que pueden usarse para determinar una similitud de usuario. Cuando se registran en un servicio nuevo, los usuarios normalmente deben tomar decisiones relacionadas con la privacidad tales como si desean compartir algunos de sus atributos personales con el servicio o no. En la mayoría de los casos deben aceptar compartir atributos que son obligatorios para el servicio y habitualmente pueden tomar decisiones sobre compartir atributos que son voluntarios. Basándose en estas decisiones es posible medir similitudes entre dos usuarios diferentes. Podemos asumir que es probable que personas que han tomado decisiones similares en el pasado tomen decisiones similares en el futuro. Como enfoque simple, si dos usuarios compartieron un atributo con un servicio, entonces su similitud desde el punto de vista de este par de atributos de servicio es máxima; de lo contrario la similitud es mínima. Usando este enfoque pueden ubicarse decisiones de usuario en una escala binaria desde puntos de vista de atributo de servicio diferentes.

En el contexto de la presente invención, los atributos de usuario y las decisiones de política de privacidad son medidas convenientes para determinar una similitud de usuario; sin embargo no son las únicas medidas disponibles. Pueden usarse otras medidas además de, o en lugar de, atributos de usuario y/o decisiones de política de privacidad cuando se determina una similitud de usuario. Por ejemplo, un servicio que busca hacer recomendaciones de política a un usuario puede indagar en las relaciones sociales del usuario desde un sitio web de red social usado por el usuario (con el consentimiento del usuario). Puede usarse información dentro de un sitio web de red social de este tipo para medir similitudes entre dos usuarios (por ejemplo determinando si ambos son miembros de una comunidad particular dentro del sitio web de red social).

Una vez que se ha elegido la metodología de definición de distancia con respecto a cada atributo (u otras medidas), la siguiente etapa (etapa 4 del algoritmo 1) es determinar realmente las similitudes entre usuarios.

El mecanismo propuesto para determinar la similitud entre un primer usuario (i) y un segundo usuario (j) es calcular la suma ponderada (α_k) de las diferentes distancias de usuario a usuario (d) con respecto a cada atributo de usuario (a).

La definición anterior determina la siguiente fórmula:

$$s_{ij} = \sum_{k=1}^{n} = \alpha_k \cdot d(a_{ki}, a_{kj}),$$

donde:

α_k es el peso del atributo de usuario correspondiente o de diferentes aspectos del mismo atributo de usuario con la restricción de que $\sum_{k=1}^{n} \alpha_k = 1$; y

$d(a_{ki}, a_{kj})$ es la distancia entre el atributo a_k del usuario (i) y el atributo a_k del usuario (j) definida por la metodología de definición de función de distancia (etapa 2 del algoritmo 1) con la restricción de que $d(a_{ki}, a_{kj}) = (-1,+1)$.

El resultado de la fórmula anterior (s_{ij}) representa la similitud entre los dos usuarios. El valor de +1 indica similitud total y el valor de -1 indica disimilitud total.

Tal como se describió anteriormente, la distancia física entre la dirección particular de dos usuarios y la edad de esos usuarios son dos de muchos atributos posibles que pueden usarse para determinar una similitud. Tal como se sugirió anteriormente, en una implementación ilustrativa de la invención, la distancia física entre las dos direcciones particulares se considera más importante cuando se define una similitud entre dos usuarios. Por consiguiente, el atributo “dirección particular” puede tener un peso mayor que el atributo “edad”. Por tanto, la similitud general entre los usuarios puede darse, por ejemplo, como: $s_{ij} = \frac{1}{3} d_1 + \frac{2}{3} d_2$

donde d_1 es la función de distancia “edad” y d_2 es la función de distancia “dirección particular”.

Tal como se trató anteriormente con referencia a la figura 1, una vez que se han definido las definiciones de funciones de distancia en relación con cada atributo de usuario (etapa 2 del algoritmo 1) y se han determinado las similitudes de usuario según las funciones de distancia definidas (etapa 4), se determinan los vecinos más próximos (etapa 6).

Determinar los vecinos más próximos al usuario implica seleccionar los otros usuarios que tienen el mayor valor de similitud (es decir más cercano a +1). Normalmente, la etapa 6 implica seleccionar un conjunto de k vecinos más próximos, donde k es un valor predefinido. Por ejemplo, si k=10, entonces la etapa 6 implica seleccionar los otros 10 usuarios con el mayor valor de similitud, determinado en la etapa 4.

Una vez que se ha determinado el conjunto de los vecinos más próximos, la siguiente etapa (etapa 8) es hacer recomendaciones al usuario. Una recomendación puede hacerse, por ejemplo, cuando un usuario llega a un punto de decisión (por ejemplo cuando un usuario se registra en un servicio o, por ejemplo, cuando un servicio se modifica en una medida en la que requiere una entrada de política de usuario adicional).

La figura 3 muestra un algoritmo, indicado generalmente mediante el número de referencia 20, que puede usarse para hacer recomendaciones. El algoritmo 20 se activa cuando se requiere una decisión con respecto a si debe activarse un parámetro de privacidad particular o no.

El algoritmo 20 se inicia en la etapa 22, en la que se verifica el parámetro de privacidad correspondiente de cada uno del grupo predefinido de los vecinos más próximos. El algoritmo 20 pasa entonces a la etapa 24, en la que se determina si al menos dos tercios de los vecinos más próximos han activado el parámetro de privacidad relevante o no.

Si al menos dos tercios de los vecinos más próximos han activado el parámetro de privacidad, entonces el algoritmo 20 pasa a la etapa 26, en la que se recomienda activar el parámetro de privacidad. Si menos de dos tercios de los vecinos más próximos han activado el parámetro de privacidad, entonces el algoritmo pasa a la etapa 28, en la que no se recomienda activar el parámetro de privacidad. Naturalmente, los detalles del algoritmo 20 variarán de caso en caso. Por ejemplo puede seleccionarse una proporción diferente de dos tercios.

Naturalmente, el algoritmo 20 puede ser más sofisticado que el ejemplo descrito anteriormente.

La figura 4 muestra un algoritmo, indicado generalmente mediante el número de referencia 30, que muestra una variante del algoritmo 20. El algoritmo 30 se inicia en la etapa 32, en la que se verifica el parámetro de privacidad correspondiente de cada uno del grupo predefinido de los vecinos más próximos. El algoritmo 30 pasa entonces a la etapa 34, en la que se determina si al menos una primera proporción (por ejemplo dos tercios) de los vecinos más próximos han activado el parámetro de privacidad relevante o no.

Si al menos la primera proporción de los vecinos más próximos han activado el parámetro de privacidad, entonces el algoritmo 30 pasa a la etapa 36, en la que se recomienda activar el parámetro de privacidad. Entonces, el algoritmo 30 termina. Si menos de dos tercios de los vecinos más próximos han activado el parámetro de privacidad, entonces el algoritmo 30 pasa a la etapa 38.

En la etapa 38 se determina si menos de una segunda proporción de los vecinos más próximos han activado el parámetro de privacidad. La segunda proporción es menor que la primera y puede ser, por ejemplo, un tercio. Si menos de la segunda proporción de los vecinos más próximos han activado el parámetro de privacidad, entonces el algoritmo pasa a la etapa 40, en la que se recomienda que el parámetro de privacidad no se active. Entonces, el algoritmo 30 termina. Si más de la segunda proporción de los vecinos más próximos han activado el parámetro de privacidad, entonces el algoritmo 30 termina en la etapa 42, en la que no se hace ninguna recomendación con respecto a si el usuario debe activar ese parámetro de privacidad o no.

Naturalmente, los algoritmos 20 y 30 son dos de muchos ejemplos de maneras en las que pueden hacerse recomendaciones, basándose en los parámetros de los vecinos más próximos.

En muchas circunstancias, cuando está haciéndose una recomendación con respecto a si un usuario debe aceptar un parámetro particular o no, al menos algunos de los vecinos más próximos determinados en la etapa 6 descrita anteriormente pueden no haber tomado una decisión sobre el punto. Por ejemplo, asúmase que un usuario se registra en un servicio y debe hacerse una recomendación con respecto a si el usuario debe compartir un atributo con el servicio o no. Se determina un número de los vecinos más próximos a ese usuario, pero muchos de (o todos) los vecinos más próximos no han decidido si el atributo debe compartirse o no (por ejemplo porque los usuarios similares aún no se han registrado en el servicio en cuestión). En este caso, la política para compartir del usuario similar con respecto al atributo puede encontrarse en el estado por defecto determinado mediante las políticas por defecto del usuario similar. Esta cuestión puede abordarse de varias maneras, algunas de las cuales se explican a continuación.

Los usuarios similares descubiertos en la etapa 6 pueden simplemente ignorarse cuando se hacen recomendaciones si no han tomado una decisión sobre la cuestión considerada. Por tanto, la etapa 24 del algoritmo 20 descrito anteriormente puede determinar si una primera proporción de los vecinos más próximos que han tomado una decisión con respecto al parámetro de privacidad relevante han activado ese parámetro.

Otro enfoque sería encontrar otros atributos o parámetros similares a aquél para el que está solicitándose una recomendación y hacer una recomendación partiendo de esa base. Este enfoque sería más sofisticado que el anterior, pero sería más difícil de implementar.

Un enfoque adicional sería seleccionar un número predeterminado de los vecinos más próximos que han tomado una decisión con respecto al parámetro de privacidad relevante. Por tanto, si un número sustancial de los vecinos cercanos no han tomado una decisión del parámetro de privacidad en cuestión, entonces se consideran vecinos que están menos cerca (es decir tienen una medida de similitud menor).

La figura 5 muestra un algoritmo, indicado en general mediante el número de referencia 50, según un aspecto de la presente invención. El algoritmo 50 muestra una implementación ilustrativa de la presente invención por parte de un operador de telecomunicaciones.

El algoritmo 50 se inicia en la etapa 52, en la que usuarios nuevos hacen uso del sistema proporcionado por el operador de telecomunicaciones. En la etapa 52, el usuario nuevo establece parámetros de perfil iniciales. Por ejemplo, en la etapa 52, un usuario puede proporcionar información tal como su nombre, género, etc. y también debe elegir el nivel de protección de sus datos. Por ejemplo puede elegirse uno de tres conjuntos de políticas predefinidos marcados como “paranoico”, “precavido” o “exhibicionista”.

El algoritmo 50 pasa entonces a la etapa 54, en la que se establece una política por defecto para el usuario. La política por defecto puede contener políticas con respecto a los servicios más populares y refleja la actitud principal del usuario. Por ejemplo puede asumirse que los usuarios “paranoicos” nunca desearán compartir su atributo de ubicación con ningún servicio.

Tras el estado inicial, el algoritmo 50 pasa a la etapa 56, en la que el sistema hace recomendaciones a los usuarios sobre cómo cambiar sus conjuntos de políticas basándose en los algoritmos de los vecinos más próximos descritos anteriormente. En este momento, la determinación de similitudes de usuario a usuario no sólo se basa en el perfil y conjunto de políticas real de los usuarios, sino también en su historia de telecomunicaciones (que usa datos tal como número marcados, ubicación, frecuencia de llamadas, etc.) porque el operador de telecomunicaciones puede acceder a estos datos. La clasificación de estos atributos específicos de telecomunicaciones puede hacerse de manera similar a la que se hizo en el caso de los atributos de usuario anteriores. Por ejemplo, si dos usuarios marcan el mismo número frecuentemente (por ejemplo su restaurante favorito), pueden desear tener otras similitudes en sus políticas de privacidad (por ejemplo ambos desean compartir su dirección de correo electrónico con el restaurante para obtener el menú semanal).

En la etapa 56, el usuario puede elegir aceptar una recomendación o no, tal como se describió anteriormente con referencia a los algoritmos 1, 20 y 30.

En esta fase se ha establecido una política por defecto inicial en la etapa 54 y pueden haberse hecho modificaciones basadas en recomendaciones en la etapa 56. El usuario puede proceder entonces a hacer uso de los servicios proporcionados por el operador de telecomunicaciones, con los parámetros de seguridad y privacidad elegidos.

En algún punto en el futuro se llega a un punto de decisión (etapa 58). Cuando los usuarios llegan a un punto de decisión (por ejemplo registrarse en un servicio nuevo), el sistema recomienda la política establecida por la mayoría de los vecinos más próximos de los usuarios. Al mismo tiempo, esta recomendación se compara con la actitud principal de los usuarios (realmente con el conjunto de políticas por defecto) y se destaca cualquier diferencia al usuario. Por ejemplo, si la actitud principal del usuario es “paranoico”, entonces el usuario presumiblemente no desea compartir su atributo de ubicación. Sin embargo, si la mayoría de sus vecinos más próximos comparten los datos de ubicación, entonces el sistema también le recomendará compartir datos de ubicación, pero destacará la diferencia con respecto a su actitud principal.

Nuevamente, el usuario puede elegir si aceptar las recomendaciones hechas en la etapa 56 o no. El algoritmo 50 avanza entonces a la etapa 58 hasta que se llega a otro punto de decisión.

La presente invención proporciona sistemas y métodos para ayudar a usuarios a establecer y modificar políticas de privacidad y similares. La invención pretende proporcionar una mejor experiencia de usuario permitiendo que un usuario establezca tales políticas según sus necesidades y deseos, pero con un esfuerzo reducido en comparación con las soluciones conocidas. La invención busca evitar la necesidad de que los usuarios monitoricen continuamente conjuntos de políticas complejas y cambien reglas de política una por una, sin requerir que el usuario acepte conjuntos de políticas globales. La invención pretende proponer parámetros de control de acceso que son los más apropiados para el usuario, mientras se proporciona la flexibilidad para permitir que los usuarios decidan si deben aceptarse parámetros propuestos o no.

Las realizaciones de la invención descrita anteriormente son ilustrativas más que restrictivas. Resultará evidente para los expertos en la técnica que los dispositivos y métodos anteriores puede incorporar varias modificaciones sin desviarse del alcance general de la invención. Se pretende incluir todas estas modificaciones dentro del alcance de la invención en la medida en que se encuentren dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método de gestión de políticas de privacidad que comprende:

proporcionar una determinación de similitud entre un primer usuario y otros usuarios;

determinar, basándose en dicha determinación de similitud, al menos un vecino más próximo al primer usuario; estando el método caracterizado por

proporcionar uno o más parámetros de política de privacidad recomendados al primer usuario basándose en parámetros de política de privacidad de dicho al menos un vecino más próximo determinado.

2. Método según la reivindicación 1, en el que la determinación de similitud entre el primer usuario y uno de dichos otros usuarios comprende aplicar una o más funciones de distancia.

3. Método según la reivindicación 2, que comprende además definir al menos una de dichas una o más funciones de distancia.

4. Método según cualquier reivindicación anterior, en el que la determinación de similitud entre usuarios incluye considerar la similitud entre al menos un atributo de usuario de dichos usuarios.

5. Método según cualquier reivindicación anterior, en el que la determinación de similitud entre usuarios incluye considerar la similitud entre al menos algunas de las decisiones de política de privacidad de dichos usuarios.

6. Método según cualquier reivindicación anterior, en el que determinar el al menos un vecino más próximo comprende determinar un número predeterminado de dichos otros usuarios que tienen la mayor similitud con el primer usuario.

7. Método según cualquier reivindicación anterior, en el que proporcionar parámetros de política de privacidad recomendados comprende determinar, para una política potencial, si más de una primera proporción predeterminada de los vecinos más próximos han establecido dicha política.

8. Método según cualquier reivindicación anterior, en el que proporcionar parámetros de política de privacidad recomendados comprende determinar, para una política potencial, si menos de una segunda proporción predeterminada de los vecinos más próximos han establecido dicha política.

9. Método según la reivindicación 7 u 8, en el que la etapa de determinar, para una política potencial, si una proporción de dichos vecinos más próximos han establecido dicha política considera sólo los vecinos más próximos que han tomado una decisión con respecto a si establecer dicha política o no.

10. Método según cualquier reivindicación anterior, que comprende además comparar una política de privacidad recomendada para el primer usuario con una actitud principal de dicho primer usuario.

11. Aparato que comprende:

una primera entrada para recibir datos en relación con una pluralidad de usuarios; y

al menos un procesador para una determinación de similitud, basándose en dichos datos, entre un primer usuario y otros usuarios, para determinar, basándose en dicha determinación de similitud, al menos un vecino más próximo al primer usuario, y estando el aparato caracterizado porque el procesador está adaptado para

generar uno o más parámetros de política de privacidad recomendados al primer usuario basándose en parámetros de política de privacidad de dicho al menos un vecino más próximo determinado.

12. Aparato según la reivindicación 11, que comprende además una primera salida para proporcionar dichos parámetros de política de privacidad recomendados a dicho primer usuario.

13. Aparato según la reivindicación 11 ó 12, en el que el al menos un procesador determina la similitud entre usuarios aplicando una o más funciones de distancia.

14. Aparato según una cualquiera de las reivindicaciones 11 a 13, en el que cuando se determina la similitud entre usuarios, dicho al menos un procesador considera la similitud entre al menos un atributo de usuario de dichos usuarios.

15. Aparato según una cualquiera de las reivindicaciones 11 a 14, en el que cuando se determina la similitud entre usuarios, dicho al menos un procesador considera la similitud entre al menos algunas de las decisiones de política de privacidad de dichos usuarios.

16. Producto de programa informático que comprende:

medios para una determinación de similitud entre un primer usuario y otros usuarios;

medios para determinar, basándose en dicha determinación de similitud, al menos un vecino más próximo al primer usuario; y estando el producto de programa informático caracterizado por

medios para proporcionar uno o más parámetros de política de privacidad recomendados al primer usuario basándose en parámetros de política de privacidad de dicho al menos un vecino más próximo determinado.

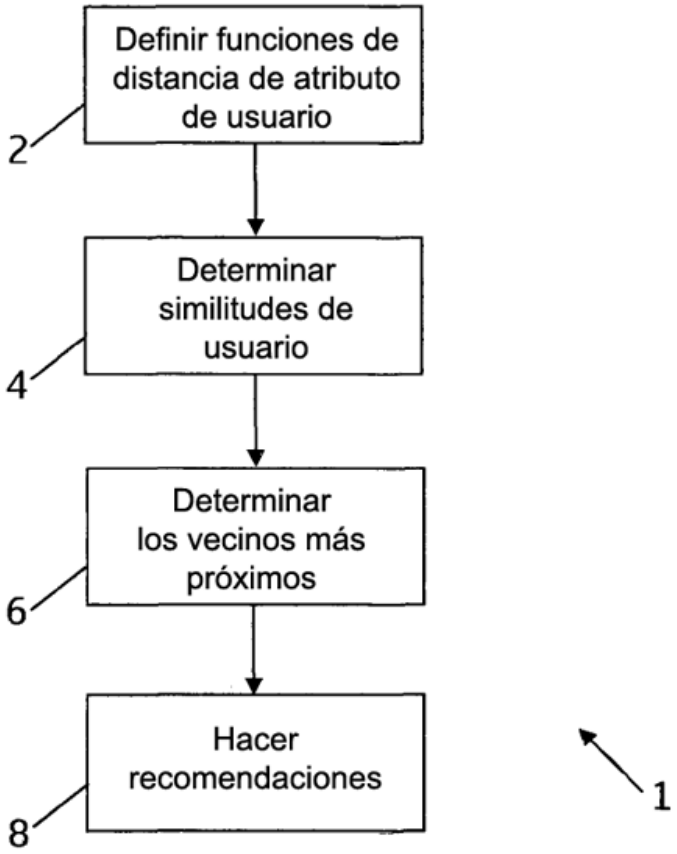

Fig. 1

$\lvert a_{ki} - a_{kj} \rvert$	$d(a_{ki}, a_{kj})$
>20.000 km	-1
>5.000, ≤20.000 km	-0,5
>100, ≤5.000 km	0
>0, ≤100 km	0,5
0 km	1

10

Fig. 2

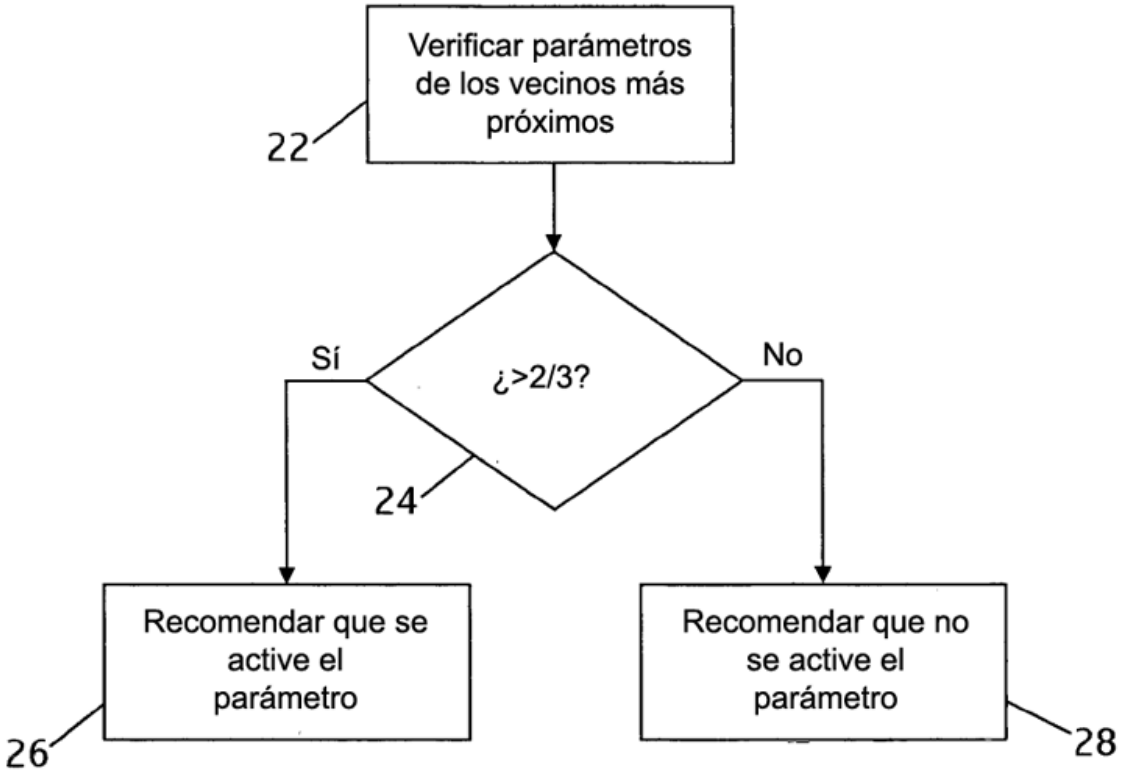
Verificar parámetros de los vecinos más próximos
22
¿>2/3?
24
Sí
No
Recomendar que se active el parámetro
26
Recomendar que no se active el parámetro
28
20

Fig. 3

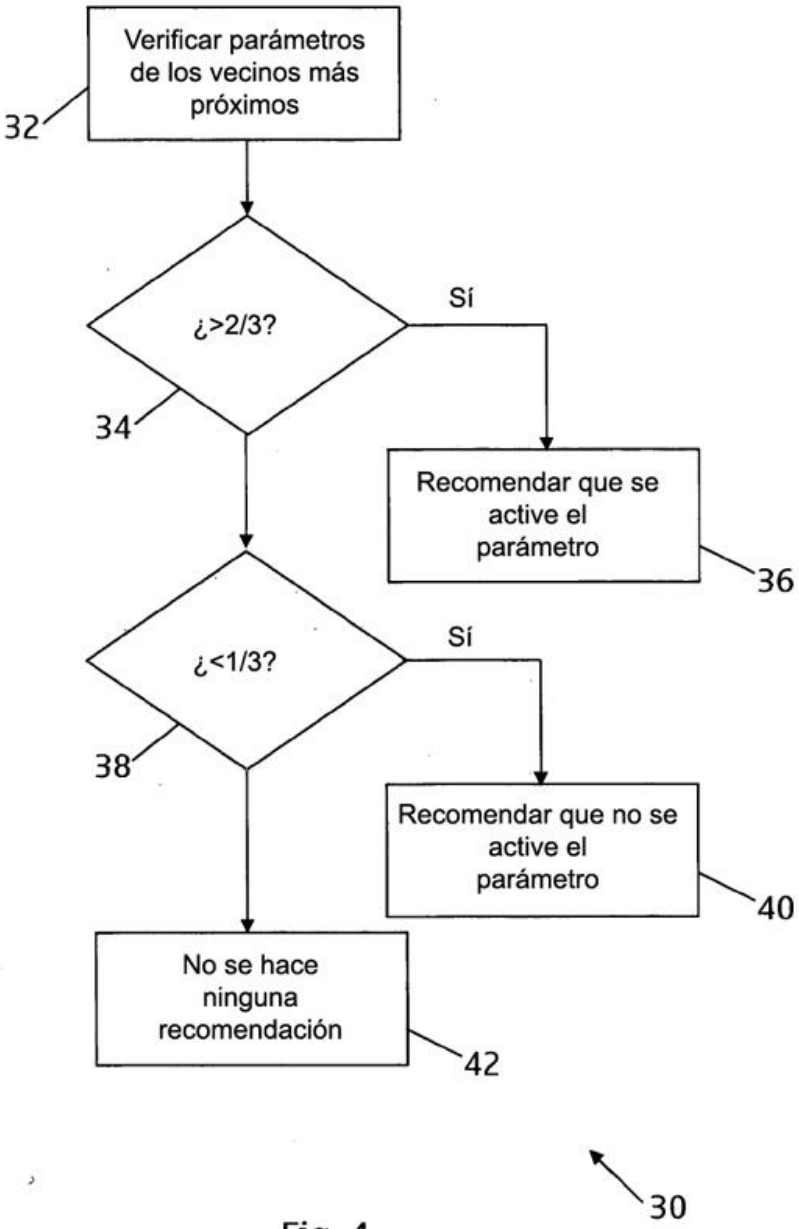
Verificar parámetros de los vecinos más próximos
32
¿>2/3?
Sí
34
Recomendar que se active el parámetro
36
¿<1/3?
Sí
38
Recomendar que no se active el parámetro
40
No se hace ninguna recomendación
42
30

Fig. 4

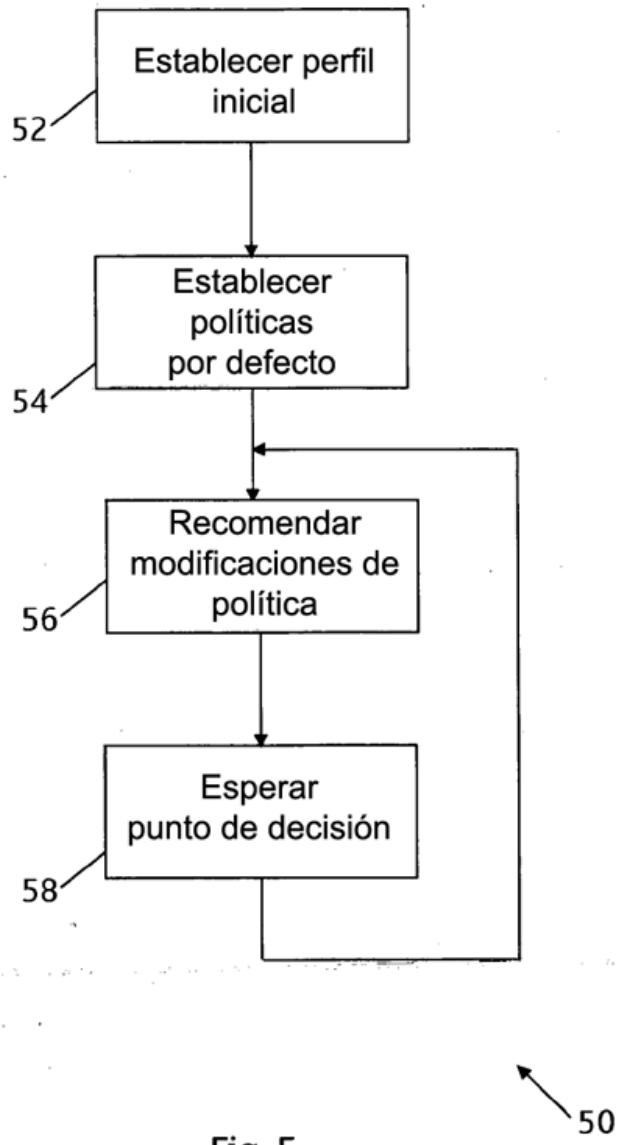
Establecer perfil inicial
52
Establecer políticas por defecto
54
Recomendar modificaciones de política
56
Esperar punto de decisión
58
50

Fig. 5