(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 541 610**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.10.2010 E 10781602 (7)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2015 EP 2494763**

(54) Título: **Procedimiento para soportar un mecanismo de reputación en una red y red**

(30) Prioridad:

29.10.2009 EP 09013609

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.07.2015

(73) Titular/es:

NEC EUROPE LTD. (100.0%)
Kurfürsten-Anlage 36
69115 Heidelberg, DE

(72) Inventor/es:

GIRAO, JOAO y
GÓMEZ MÁRMOL, FÉLIX

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Procedimiento para soportar un mecanismo de reputación en una red y red.

Las investigaciones que han dado lugar a los resultados dados a conocer en la presente invención han sido financiadas por el Séptimo Programa Marco de la Unión Europea (FP7/2007-2013) gracias a la subvención n.º 215832.

La presente invención se refiere a un procedimiento para soportar un mecanismo de reputación en una red, donde dicha red incluye uno o más dominios con uno o más usuarios que están conectados a dichos dominios, uno o más proveedores de identidad que gestionan información de identidad en nombre de dichos usuarios, y al menos una entidad que funciona como un consumidor de servicios web para dichos usuarios.

Además, la invención se refiere a una red que incluye un mecanismo de reputación, comprendiendo dicha red uno o más dominios con uno o más usuarios que están conectados a dichos dominios, uno o más proveedores de identidad que gestionan información de identidad en nombre de dichos usuarios, y al menos una entidad que funciona como un consumidor de servicios web para dichos usuarios.

En el campo de Internet y de la *World Wide Web*, las transacciones electrónicas son cada vez más importantes. Muchas tareas diarias como hacer la compra, ver las noticias o llamar a los amigos pueden realizarse mediante transacciones electrónicas. Pero incluso tareas más tediosas como reservar un vuelo o una habitación de hotel, o matricularse en la universidad, entre otras muchas, se han simplificado gracias a Internet.

Sin embargo, a medida que surgen más aplicaciones y se vuelven populares, muchos problemas de seguridad amenazan su funcionamiento seguro. Debido a su naturaleza impersonal, las transacciones electrónicas adolecen de varias deficiencias de seguridad que aún no se han resuelto de manera precisa y, por lo tanto, ralentizan el uso generalizado de estas útiles tecnologías por parte de la sociedad.

Proveedores de servicios del mismo dominio e incluso de diferentes dominios tienen que abordar estos problemas diariamente. Una entidad, denominada en lo sucesivo como consumidor de servicios web (WSC), tiene el gran problema de que cuando proporciona un servicio solicitado a un determinado usuario, el consumidor de servicios web necesita intercambiar previamente determina información con otra entidad, denominada en lo sucesivo como proveedor de servicios web (WSP). En la actualidad, muchos dominios llevan a cabo una transacción de este tipo de manera segura mediante un acuerdo de nivel de servicio (SLA), así como usando infraestructuras de autenticación, autorización y contabilización (AAA). Sin embargo, el problema es que un acuerdo de nivel de servicio no está siempre disponible entre cada par de dominios. Además, el acuerdo de nivel de servicio no es siempre fácil de conseguir y normalmente tiene unos costes asociados. Por tanto, muchas veces no se dispone de tal acuerdo para garantizar la validez de la información proporcionada por otro dominio.

El documento US 2004/088348 A1 se refiere a la gestión de la distribución de contenido usando agentes móviles en redes de dispositivos homólogos. El documento da a conocer un procedimiento para recopilar información de reputación de un dispositivo homólogo, donde un dispositivo homólogo puede evaluar las reputaciones de otros dispositivos homólogos en función de recomendaciones recopiladas por un agente móvil. La información de reputación recopilada se usa para calcular la confianza en otros dispositivos homólogos.

Por lo tanto, un objeto de la presente invención es mejorar y, además, desarrollar un procedimiento y una red del tipo descrito inicialmente de manera que, utilizando mecanismos que puedan implementarse fácilmente, un consumidor de servicios web de un dominio pueda determinar de manera eficaz si la información proporcionada por un proveedor de servicios web de otro dominio puede considerarse fiable o no.

Según la invención, el objeto antes mencionado se consigue mediante un procedimiento que comprende las características de la reivindicación 1. Según esta reivindicación, tal procedimiento está caracterizado porque, en caso de que un usuario solicite a un consumidor de servicios web de uno de dichos dominios un servicio web proporcionado por un proveedor de servicios web, en particular de otro de dichos dominios, dicho consumidor de servicios web solicitado solicita a sus proveedores de identidad conocidos una recomendación de dicho proveedor de servicios web, donde dichos proveedores de identidad funcionan como agregadores de recomendaciones recopilando valoraciones de reputación de dicho proveedor de servicios web proporcionadas por entidades que están registradas en dichos proveedores de identidad, en particular usuarios y/o consumidores de servicios web, donde dichos proveedores de identidad devuelven una recomendación agregada a dicho consumidor de servicios

web solicitado que, en función de dicha recomendación agregada, determina una valoración de confianza acerca de dicho proveedor de servicios web, y donde se utiliza un homomorfismo de privacidad para proporcionar un intercambio cifrado de información relacionada con recomendaciones entre dichos proveedores de identidad y dicho consumidor de servicios web solicitado.

Además, el objeto antes mencionado se consigue mediante una red que comprende las características de la reivindicación 21. Según esta reivindicación, tal red está caracterizada porque, en caso de que un usuario solicite a un consumidor de servicios web de uno de dichos dominios un servicio web proporcionado por un proveedor de servicios web, en particular de otro de dichos dominios, dicho consumidor de servicios web solicitado solicita a sus proveedores de identidad conocidos una recomendación de dicho proveedor de servicios web, donde dichos proveedores de identidad funcionan como agregadores de recomendaciones recopilando valoraciones de reputación de dicho proveedor de servicios web proporcionadas por entidades que están registradas en dichos proveedores de identidad, en particular usuarios y/o consumidores de servicios web, donde dichos proveedores de identidad devuelven una recomendación agregada a dicho consumidor de servicios web solicitado que, en función de dicha recomendación agregada, determina una valoración de confianza acerca de dicho proveedor de servicios web, y donde se utiliza un homomorfismo de privacidad para proporcionar un intercambio cifrado de información relacionada con recomendaciones entre dichos proveedores de identidad y dicho consumidor de servicios web solicitado.

Según la invención se ha reconocido en primer lugar que la necesidad de un acuerdo de nivel de servicio entre un par de dominios para permitir que las entidades de un dominio accedan de manera segura e ininterrumpida a datos o sistemas de otro dominio puede solventarse utilizando un mecanismo de reputación. Específicamente, se ha reconocido que un mecanismo de reputación puede utilizarse de manera ventajosa para que pueda determinarse la fiabilidad de un proveedor de servicios. Según la invención, en caso de que un usuario solicite a un consumidor de servicios web de uno de los dominios un servicio web proporcionado por un proveedor de servicios web, en particular de otro de los dominios, el consumidor de servicios web solicitado solicita a todos sus proveedores de identidad conocidos una recomendación del proveedor de servicios web. En este contexto, un servicio web proporcionado por un proveedor de servicios web puede significar que el consumidor de servicios web necesita recuperar e intercambiar determinada información con el proveedor de servicios web con el fin de proporcionar o suministrar el servicio web correspondiente al usuario solicitante. Además, cada uno de los proveedores de identidad funciona como un agregador de recomendaciones recopilando valoraciones de reputación del proveedor de servicios web proporcionadas por entidades que están registradas en el proveedor de identidad, en particular usuarios y/o consumidores de servicios web. Esto significa que los proveedores de identidad recopilan las opiniones de las entidades registradas en los mismos. Además, cada uno de los proveedores de identidad devuelve una recomendación agregada al consumidor de servicios web solicitado que, en función de la recomendación agregada, determina una valoración de confianza acerca del proveedor de servicios web. Por consiguiente, el consumidor de servicios web puede decidir, en virtud de la valoración de confianza, si la información recibida en el contexto del servicio web desde el proveedor de servicios web es fiable o no. En lo que respecta a la seguridad, un homomorfismo de privacidad se utiliza para proporcionar un intercambio cifrado de información relacionada con recomendaciones entre los proveedores de identidad y el consumidor de servicios web solicitado. El uso del homomorfismo de privacidad permite la agregación de determinada información sensible en el mecanismo de reputación de tal modo que se mantiene la privacidad sin revelar la información.

Por tanto, el procedimiento o la red según la invención puede ayudar a un dominio a decidir si intercambiar o no determinada información necesaria con otro dominio, dependiendo de la fiabilidad y la reputación del otro dominio.

Según una realización preferida, la recomendación agregada devuelta por los proveedores de identidad al consumidor de servicios web solicitado puede ser un único valor agregado para recomendaciones de los usuarios que están registrados en los proveedores de identidad. Asimismo, la recomendación agregada puede ser un único valor agregado para recomendaciones de los consumidores de servicios web que están registrados en los proveedores de identidad. Además, la recomendación agregada puede ser un único valor agregado para recomendaciones de los usuarios y los consumidores de servicios web que están registrados en los proveedores de identidad.

Según una realización preferida puede aplicarse el esquema de cifrado de ElGamal como homomorfismo de privacidad. El esquema de cifrado según ElGamal descrito en el documento "*A public key cryptosystem and a signature scheme base on discrete logarithms*", de Taher ElGamal, Springer-Verlag, 1998, es un homomorfismo de privacidad multiplicativo. Este esquema de cifrado puede adaptarse a una correlación del homomorfismo con curvas elípticas (EC) en un grupo aditivo. Al igual que en la mayoría de esquemas basados en curvas elípticas, la seguridad

del esquema dependerá de la elección de la curva elíptica *E*, un número primo *p* y la elección de un generador *G*. La curva elíptica *E* debería elegirse de modo que se verifique el problema del logaritmo discreto en curvas elípticas (ECDLP).

EC-EG ofrece las propiedades requeridas, por ejemplo un bajo coste de ancho de banda, flexibilidad y operaciones eficientes. Por ejemplo, en caso de que *p* se tome como un número de 163 bits, el texto cifrado ocupará 2*(163+1) bits. El esquema es versátil y flexible. Además, el coste de la suma y multiplicación con un escalar supone una suma de puntos y dos multiplicaciones de puntos con pequeños números, lo que es aceptable. Una suma de puntos se considera una operación sencilla en EC y la complejidad de la multiplicación de puntos depende del tamaño de los operandos. Esto hace que el siguiente esquema sea el candidato perfecto que se aplicará en el procedimiento según la invención:

Esquema de cifrado de ElGamal (EC-EG)

Clave pública	$E, p, G, Y = xG$, donde $G, Y \in F_p$
Clave privada	$x \in F_p$
Cifrado	Texto plano $M = map(m)$, $r \in_R F_p$, Texto cifrado $C = (R, S)$, donde $R = kG$, $S = M + kY$
Descifrado	$M = -xR + S = -xkG + M + xkG$, $m = rmap(M)$

Propiedades homomórficas EC-EG

Suma	$(R_1, S_1) + (R_2, S_2) =$ $(k_1G + k_2G, M_1 + M_2 + k_1Y + k_2Y)$ $((k_1 + k_2)G, (M_1 + M_2) + (k_1 + k_2)Y)$
Multiplicación escalar	$\alpha * (R, S) =$ $(\alpha * kG, \alpha * (M + kY))$

Propiedades de la función *map(x)*

Suma	$map(m_1) + map(m_2) = m_1G + m_2G =$ $(m_1 + m_2)G = map(m_1 + m_2)$
Multiplicación escalar	$\alpha * map(m) =$ $\alpha * mG = map(\alpha * m)$

Puesto que EC-EG funciona en lo que respecta a los puntos de la EC, puede necesitarse una función *map*(*x*) y su función inversa *rmap*(*x*). Estas funciones deberían correlacionar un número entero con un punto de la curva, y viceversa, de modo que las propiedades del homomorfismo de privacidad se mantengan en todas las operaciones llevadas a cabo en el texto cifrado. Aunque hay mecanismos estándar para convertir un número entero en un punto de la curva, debido a la restricción explicada anteriormente, puede optarse por un mecanismo introducido en el documento "*Public key based cryptoschemes for data concealment in wireless sensor networks*", de Mykletun, Girao y Westhoff, en la Conferencia Internacional sobre Comunicaciones del IEEE, Estambul, Turquía, junio de 2006, que define *map*(*x*) = *xG* y *rmap*(*x*) como la fuerza bruta del ECDLP. Puesto que en el contexto de la invención se pretende trabajar con números relativamente pequeños, en particular inferiores a 32 bits, esta restricción es aceptable. Por tanto, usando esta herramienta criptográfica puede obtenerse un sistema meramente privado, donde puntos de almacenamiento e intermediarios, en particular proveedores de identidad, no tienen un acceso directo a datos sensibles.

En lo que respecta al cifrado de información sensible, puede establecerse que en una primera etapa el consumidor de servicios web solicitado envíe su clave pública a los proveedores de identidad junto con un peso inicial por defecto para todas las entidades que están registradas en los proveedores de identidad, donde el peso inicial se cifra con la clave pública del consumidor de servicios web solicitado.

De manera ventajosa, puede establecerse que cada uno de los proveedores de identidad almacene un peso proporcionado por el consumidor de servicios web solicitado a cada una de las entidades que están registradas en los proveedores de identidad, donde el peso se cifra con una clave pública del consumidor de servicios web solicitado. Por tanto, los proveedores de identidad no pueden descubrir el peso real de una entidad.

En una etapa adicional, el consumidor de servicios web solicitado puede descifrar la recomendación agregada devuelta por los proveedores de identidad con su clave privada para obtener una recomendación ponderada de las entidades que están registradas en los proveedores de identidad.

Según una realización preferida, cada uno de los proveedores de identidad puede llevar a cabo la recomendación agregada de usuarios que están registrados en los proveedores de identidad de acuerdo con:

$$\sum_{i=0}^{n} \varphi(\omega_{u_i}) \cdot Rec_{u_i} = \varphi\left(\sum_{i=1}^{n} \omega_{u_i} \cdot Rec_{u_i}\right), \qquad (1)$$

donde Rec_{ui} es una recomendación proporcionada por un usuario u_i, que es uno de n usuarios que están registrados en el proveedor de identidad correspondiente, donde ω_{ui} es el peso asignado a la recomendación del usuario u_i, y donde φ es un homomorfismo de privacidad que permite la suma y la multiplicación escalar. Por tanto, el consumidor de servicios web solicitado puede ponderar la recomendación de cada usuario individualmente usando algunos mensajes, y la recomendación real o el valor de recomendación de cada usuario solo es conocido por su proveedor de identidad correspondiente.

Además, los proveedores de identidad pueden llevar a cabo la recomendación agregada de consumidores de servicios web que están registrados en los proveedores de identidad de acuerdo con:

$$\sum_{i=0}^{m} \varphi(\omega_{WSC_i}) \cdot Rec_{WSC_i} = \varphi\left(\sum_{i=1}^{m} \omega_{WSC_i} \cdot Rec_{WSC_i}\right), \qquad (2)$$

donde Rec_{WSCi} es una recomendación proporcionada por un consumidor de servicios web WSC_i, que es uno de m consumidores de servicios web que están registrados en el proveedor de identidad correspondiente, donde ω_{WSCi} es el peso asignado a la recomendación del consumidor de servicios web WSC_i, y donde φ es un homomorfismo de privacidad que permite la suma y la multiplicación escalar.

Así, en caso de que las recomendaciones del proveedor de servicios web se hayan recopilado a partir de entidades que están registradas en los proveedores de identidad, una valoración de confianza en forma de un valor de confianza global puede proporcionarse al proveedor de servicios web, agregando las recomendaciones recopiladas. La confianza de los usuarios en lo que respecta al proveedor de servicios web, por ejemplo $T_U \in [0,1]$, puede calcularse mediante una suma ponderada de las recomendaciones de cada usuario u_i y, por ejemplo, $Rec_{ui} \in [0,1]$, de acuerdo con:

$$T_U = \sum_{i=1}^{n} \omega_{u_i} \cdot Rec_{u_i} ,$$

donde ω_{ui}, por ejemplo $\omega_{ui} \in [0,1]$, es el peso proporcionado al usuario u_i por el consumidor de servicios web solicitado.

Asimismo, la confianza de los consumidores de servicios web en el proveedor de servicios web puede calcularse de acuerdo con:

$$T_{WSC} = \sum_{i=1}^{m} \omega_{WSC_i} \cdot Rec_{WSC_i} .$$

Con respecto a la valoración del proveedor de servicios web, la valoración de confianza puede determinarse de acuerdo con:

$$GT = (\omega_D \cdot T_D) + (\omega_U \cdot T_U) + (\omega_{WSC} \cdot T_{WSC}), \qquad (3)$$

donde GT es la valoración de confianza en forma de un valor de confianza global asignado al proveedor de servicios web, donde T_D es una confianza directa, es decir, experiencias directas, depositada en el proveedor de servicios web, donde T_U es la confianza agregada recibida desde otros usuarios, donde T_{WSC} es la confianza agregada recibida desde otros consumidores de servicios web, y donde ω_D, ω_U y ω_{WSC} son los pesos correspondientes donde, por ejemplo, $\omega_D, \omega_U, \omega_{WSC} \in [0,1]$. Si el consumidor de servicios web solicitado no tiene experiencias pasadas con el proveedor de servicios web, entonces T_D puede tomar un valor inicial de 0,5; en caso contrario, T_D puede tomar la última valoración de confianza calculada, es decir $T_D = GT$.

De manera ventajosa, puede establecerse que se aplique la fórmula (3) la primera vez que se realice una transacción entre el consumidor de servicios web solicitado y el proveedor de servicios web. Sin embargo, para la enésima transacción puede establecerse que la valoración de confianza GT del proveedor de servicios web pueda calcularse de acuerdo con:

$$GT^{(n)} = \omega_D^n \cdot T_D + (\omega_U \cdot T_U + \omega_{WSC} \cdot T_{WSC}) \cdot \sum_{i=0}^{n-1} \omega_D^i$$

que es igual a:

$$GT^{(n)} = \omega_D^n \cdot T_D + (\omega_U \cdot T_U + \omega_{WSC} \cdot T_{WSC}) \cdot \frac{1-\omega_D^n}{1-\omega_D}$$

Al hacer esto, debe observarse que debería aplicarse:

$$\sum_{i=1}^{n} \omega_{u_i} = \sum_{i=1}^{m} \omega_{WSC_i} = \omega_D + \omega_U + \omega_{WSC} = 1 \qquad (4)$$

Por lo tanto, si, por ejemplo, $\omega_D = 1$, entonces $GT^{(n)} = T_D$, es decir, solo se tiene en cuenta la confianza directa, y si $\omega_D = 0$, entonces $GT^{(n)} = \omega_U \cdot T_U + \omega_{WSC} \cdot T_{WSC}$, lo que significa que solo se acepta la confianza de los usuarios y de los consumidores de servicios web.

El consumidor de servicios web solicitado puede definir niveles de confianza, donde el consumidor de servicios web solicitado asigna la valoración de confianza del proveedor de servicios web a uno de los niveles de confianza. De manera ventajosa, puede establecerse la utilización de conjuntos difusos para representar los niveles de confianza.

Según una realización preferida, el consumidor de servicios web solicitado puede solicitar el servicio web al proveedor de servicios web, donde el proveedor de servicios web solicitado proporciona más o menos parámetros dependiendo del nivel de confianza asignado al proveedor de servicios web. Por tanto, después de calcular la valoración de confianza, el consumidor de servicios web solicitado puede tener que decidir si llevar a cabo toda la transacción con el proveedor de servicios web, si llevarla a cabo parcialmente o incluso si omitir cualquier interacción con el proveedor de servicios web. Esta decisión puede depender del nivel de confianza asignado al proveedor de servicios web. Al hacer esto, el consumidor de servicios web solicitado puede definir sus propios niveles de confianza.

Según una realización preferida, puede premiarse y/o castigarse a los usuarios y/o los consumidores de servicios web que están registrados en los proveedores de identidad según la precisión y la fiabilidad de sus recomendaciones.

De manera ventajosa, puede establecerse que el usuario solicitante proporcione información de respuesta al

consumidor de servicios web solicitado, donde la información de respuesta incluye la satisfacción del usuario solicitante con el servicio web proporcionado.

Según una realización preferida, el consumidor de servicios web solicitado puede enviar la satisfacción junto con un umbral δ a los proveedores de identidad, donde el umbral δ se utiliza para determinar si castigar o premiar a los usuarios y/o a los proveedores de servicios web que están registrados en los proveedores de identidad. No es necesario cifrar la satisfacción ni el umbral.

De manera ventajosa, la divergencia entre la satisfacción *Sat* del usuario solicitante y una recomendación proporcionada anteriormente Rec_{ui} de un usuario u_i puede medirse calculando el valor de $|Sat - Rec_{ui}|$, donde se premia a un usuario u_i en caso de que $|Sat - Rec_{ui}| < \delta$, y donde se castiga al usuario u_i en caso de que $|Sat - Rec_{ui}| \geq \delta$.

Además, en caso de que se premie a un usuario u_i, el peso del usuario u_i puede aumentarse de acuerdo con:

$$\varphi(\omega_{u_i})^{|Sat-Rec_{ui}|} = \varphi\left(\omega_{u_i}^{|Sat-Rec_{ui}|}\right); \text{ and} \qquad (5)$$

y donde en caso de que se castigue a un usuario u_i, el peso ω_{ui} del usuario u_i puede reducirse de acuerdo con:

$$\varphi\left(\omega_{u_i}\right)^{\frac{1}{|Sat-Rec_{ui}|}} = \varphi\left(\omega_{u_i}^{\frac{1}{|Sat-Rec_{ui}|}}\right) \qquad (6)$$

En caso de que se premie al consumidor de servicios web WSC_i, el peso ω_{WSCi} del WSC_i de usuario puede aumentarse de acuerdo con:

$$\varphi(\omega_{WSC_i})^{|Sat-Rec_{WSC_i}|} = \varphi\left(\omega_{WSC_i}^{|Sat-Rec_{WSC_i}|}\right), \text{ and} \qquad (7)$$

y donde en caso de que se castigue al usuario u_i, el peso del usuario u_i puede reducirse de acuerdo con:

$$\varphi\left(\omega_{WSC_i}\right)^{\frac{1}{|Sat-Rec_{WSC_i}|}} = \varphi\left(\omega_{WSC_i}^{\frac{1}{|Sat-Rec_{WSC_i}|}}\right) \qquad (8)$$

Según una realización preferida, cada uno de los proveedores de identidad puede calcular una desviación media de la satisfacción del usuario solicitante con las recomendaciones de los usuarios y/o de los consumidores de servicios web que están registrados en los proveedores de identidad, donde los proveedores de identidad envían la desviación media al consumidor de servicios web solicitado.

De manera ventajosa, el consumidor de servicios web solicitado puede premiar o castigar de manera correspondiente en lo que respecta a los pesos ω_U y ω_{WSC} en función de la desviación media recibida desde los proveedores de identidad.

Existen varias maneras de diseñar y de desarrollar adicionalmente las enseñanzas de la presente invención de manera ventajosa. Para ello, se hace referencia, por un lado, a las reivindicaciones de patente subordinadas a la reivindicación 1 de patente y, por otro lado, a la siguiente explicación de realizaciones preferidas de la invención a modo de ejemplo, ilustradas mediante los dibujos. Realizaciones generalmente preferidas y desarrollos adicionales de las enseñanzas se explicarán en relación con la descripción de las realizaciones preferidas de la invención con la ayuda de los dibujos. En los dibujos:

la Fig. 1 ilustra un escenario de aplicación del procedimiento y la red según la presente invención,

la Fig. 2 ilustra las etapas principales de un modelo de confianza y reputación que describe un procedimiento según la presente invención,

la Fig. 3 muestra con la Fig. 3a, la Fig. 3b y la Fig. 3c tres enfoques diferentes de recopilación de información con el fin de proporcionar una valoración de confianza del proveedor de servicios web según la presente invención,

la Fig. 4 muestra otro enfoque de recopilación de información con el fin de proporcionar una valoración de confianza del proveedor de servicios web según la presente invención,

la Fig. 5 muestra la utilización de conjuntos difusos con el fin de modelar niveles de confianza según una realización preferida de la presente invención,

la Fig. 6 muestra un mecanismo para medir la divergencia entre la satisfacción del usuario y la recomendación proporcionada anteriormente de cada usuario,

la Fig. 7 ilustra la actualización de pesos de las fuentes de información según una realización de la presente invención,

la Fig. 8 muestra un escenario de aplicación adicional según un procedimiento y una red según la presente invención e ilustra las etapas llevadas a cabo en detalle, y

la Fig. 9 es un diagrama de secuencias que ilustra las etapas de la Fig. 8, donde las etapas están incluidas en las etapas genéricas de la Fig. 2.

La Fig. 1 muestra un escenario de aplicación del procedimiento y la red según la invención y precisa el problema a resolver. Según la Fig. 1, hay varios usuarios (móviles) conectados a diferentes dominios en un determinado momento. Algunas de las entidades que pertenecen a estos dominios actúan como un proveedor de servicios web WSP o como un consumidor de servicios web WSC para usuarios que están actualmente conectados a los mismos. Sin embargo, para proporcionar los servicios a los usuarios, un consumidor de servicios web necesita recuperar e intercambiar determinada información con otro proveedor de servicios web.

Este intercambio de información entre dos dominios se realiza normalmente mediante un acuerdo de nivel de servicio (SLA), ampliamente conocido y aceptado. Por medio del SLA, cada dominio puede asegurarse de que la información proporcionada por el otro dominio sea fiable.

Sin embargo, no siempre es posible encontrar un SLA entre cada par de dominios. Por lo tanto, existe la necesidad de un mecanismo para permitir que un dominio determine de alguna manera si la información proporcionada por otro dominio, posiblemente desconocido, pueda considerarse fiable o no. El mecanismo que se aplica es un modelo de reputación y confianza. Los proveedores de identidad (IdP) gestionan información de identidad en nombre de los usuarios y corroboran la autenticación de los usuarios a otros proveedores. Los proveedores de identidad actúan como agregadores de recomendaciones, es decir, los proveedores de identidad recopilan las opiniones de los usuarios que pertenecen a cada proveedor de identidad IdP y devuelven un único valor agregado.

Según el escenario de aplicación de la Fig. 1, un usuario solicita un determinado servicio al consumidor de servicios web WSC_1 del dominio A. Después, el WSC_1 necesita intercambiar determinada información con el proveedor de servicios web WSP del dominio B para ofrecer el servicio solicitado al usuario solicitante. Por tanto, en primer lugar, el WSC_1 comprueba si ha tenido experiencias pasadas, es decir, transacciones, con el WSP, y si estas experiencias pasadas fueron satisfactorias o no.

Una vez que se ha realizado esta revisión, el WSC_1 pregunta a otros usuarios que hayan tenido experiencias pasadas con el WSP, independientemente del dominio al que estén conectados, acerca de su comportamiento. Finalmente, el WSC_1 también pregunta a otros WSC que hayan tenido interacciones pasadas con el WSP acerca de su satisfacción con la interacción realizada. Al hacer esto, cada usuario y cada WSC tiene que registrar su satisfacción con cada transacción (o al menos con las n últimas) llevada a cabo con cada WSP que pertenece a otro dominio.

En cuanto el WSC_1 haya recopilado toda esa información, el WSC_1 valora la fiabilidad o reputación del WSP según algunos niveles de confianza definidos por él mismo. Eso significa que cada dominio puede determinar sus propios niveles de confianza en función de sus necesidades y de lo confiado que sea. Por tanto, según el nivel de confianza

otorgado por el WSC_1 al WSP, el intercambio de información se realizará total o parcialmente, o incluso no se llevará a cabo.

Suponiendo que el WSC_1 confía en el WSP lo suficiente como para permitir el intercambio de información, el servicio es proporcionado al usuario que lo solicitó. Este usuario también informa al WSC_1 acerca de su satisfacción con ese servicio específico recibido. Esta información de respuesta puede ayudar a que el WSC_1 aumente o reduzca su confianza en el proveedor de servicios web, según los niveles de confianza definidos por él mismo, y también a castigar o premiar las recomendaciones ofrecidas en la etapa anterior. Sin embargo, más importante que el WSC_1 confíe en la información intercambiada del proveedor de servicios web, puede ser que el proveedor de servicios web confíe en que el WSC_1 sea el receptor legítimo de esa información, ya que si esto no es así la información no se proporcionará al WSC_1 y el servicio no será ofrecido.

Sin embargo, aunque el WSC_1 no confíe en la información del WSP, el intercambio de información puede realizarse de todas formas si el usuario lo autoriza. Asimismo, si el WSC_1 confía en el WSP pero el usuario no confía en absoluto en el WSP, no se proporcionará el servicio. Por tanto, la opinión del usuario acerca del WSP será decisiva a la hora de calcular el nivel de confianza desde el punto de vista del WSC_1.

La Fig. 2 ilustra las etapas principales de un modelo de confianza y reputación que describe un procedimiento según la invención. En particular, la Fig. 2 muestra las etapas genéricas principales que cada modelo de reputación puede seguir para un entorno como el ilustrado en la Fig. 1.

La primera etapa de la Fig. 2 consiste en recopilar tanta información como sea posible acerca del comportamiento de la entidad que está evaluándose, en particular un proveedor de servicios web. Esta información puede proceder de experiencias directas pasadas, experiencias de conocidos, entidades ya fiables, etc. En el escenario de aplicación de la Fig. 1, las fuentes de información de un dominio serán sus experiencias directas pasadas y las experiencias pasadas de otros usuarios y otros dominios con el dominio objetivo, en particular el proveedor de servicios web objetivo. Sin embargo, no todas las fuentes de información deberían tener el mismo peso o la misma fiabilidad. Asimismo, para una determinada fuente de información no todos los usuarios deberían tener la misma fiabilidad.

En la segunda etapa de la Fig. 2, el modelo de confianza y reputación debe agregar toda la información obtenida en la etapa anterior con el fin de obtener un valor de clasificación o de puntuación para el proveedor de servicios web. Una vez que se haya calculado este valor, el dominio evaluado se asignará a alguno de los niveles de confianza del dominio evaluador. Estos niveles, definidos por cada dominio, pueden oscilar entre no ser en absoluto fiables y ser totalmente fiables, lo que sería equivalente a tener un SLA.

En la tercera etapa de la Fig. 2, según el nivel de confianza asignado al domino evaluado, el intercambio de información se lleva a cabo total o parcialmente, o incluso no se realiza. Una vez que el dominio evaluador haya recibido la información desde el dominio evaluado suponiendo que éste último se considere suficientemente fiable, el servicio puede proporcionarse al usuario que lo solicitó.

Después de recibir el servicio, el usuario envía su satisfacción con ese determinado servicio al dominio que lo proporcionó, concretamente al consumidor de servicios web. En la última etapa de la Fig. 2, este dominio usa la información de respuesta para modificar el resultado de confianza proporcionado al dominio que intercambió la información necesaria para suministrar el servicio, aumentándolo o reduciéndolo. Los pesos de las fuentes de recomendaciones, es decir, los usuarios y los consumidores de servicios web, también se ajustan.

La Fig. 3 muestra tres enfoques diferentes para recopilar información con el fin de proporcionar una valoración de confianza del proveedor de servicios web. Por lo general, se consideran tres fuentes de información: el propio consumidor de servicios web que está evaluando al proveedor de servicios web, los usuarios que han tenido experiencias pasadas con ese proveedor de servicios web y otros consumidores de servicios web que también han tenido transacciones anteriores con el proveedor de servicios web. Por tanto, cuando el consumidor de servicios web solicitado WSC_1 calcula su confianza en el proveedor de servicios web WSC_1, comprueba si ya ha tenido alguna interacción con el proveedor de servicios web en el pasado. Si es así, el último valor de confianza global calculado para el proveedor de servicios web se toma ahora como la confianza directa T_D. Por otro lado está la confianza T_U que otros usuarios depositan en el proveedor de servicios web y la confianza T_{WSC} de otros consumidores de servicios web en ese determinado proveedor de servicios web. En este caso, el problema es la manera en que el WSC_1 puede hallar usuarios y otros consumidores de servicios web que hayan tenido alguna interacción con el proveedor de servicios web.

La Fig. 3a muestra el primer enfoque, donde el WSC_1 pregunta a todos los usuarios a través de su proveedor de identidad IdP correspondiente si han realizado alguna transacción con el proveedor de servicios web cada vez que necesita calcular su confianza en ese proveedor de servicios web específico. En caso afirmativo, el WSC_1 les solicita su recomendación acerca del proveedor de servicios web. Para ello, el WSC_1 puede ponderar individualmente la recomendación de cada usuario.

La Fig. 3b muestra un segundo enfoque que consiste en que el WSC_1 pregunta solamente a aquellos usuarios que hayan realizado realmente alguna transacción con el proveedor de servicios web. El WSC_1 puede ponderar individualmente la recomendación de cada usuario pero usando menos mensajes que en el enfoque de la Fig. 3a.

La Fig. 3c muestra un tercer enfoque para recopilar recomendaciones de los usuarios acerca del proveedor de servicios web, en el que el WSC_1 solo pregunta a los proveedores de identidad que conoce. Cada proveedor de identidad IdP devolverá una recomendación agregada de todos sus usuarios que hayan realizado alguna transacción con el proveedor de servicios web en el pasado. Por tanto, el WSC_1 no necesita saber quién ha tenido alguna interacción con el proveedor de servicios web. Este enfoque usa menos mensajes de los enfoques de la Fig. 3a y la Fig. 3b. Sin embargo, las opiniones de los usuarios no pueden ponderarse de manera individual.

Los tres enfoques de la Fig. 3 pueden aplicarse en la recuperación de información de las opiniones de otros consumidores de servicios web acerca del proveedor de servicios web.

La Fig. 4 muestra un cuarto enfoque, basado en los tres enfoques ilustrados en la Fig. 3. En esta realización, cada proveedor de identidad IdP almacena el peso proporcionado por el consumidor de servicios web solicitado WSC_1 a cada uno de sus usuarios, pero cifrado con la clave pública del WSC_1, de modo que el proveedor de identidad IdP no puede descubrir el peso real.

Según la Fig. 4, en la primera etapa el WSC_1 envía su clave pública al IdP junto con el peso inicial por defecto para todos sus usuarios. Después, el IdP calcula la agregación ponderada de las recomendaciones de todos sus usuarios y la proporciona al WSC_1, cifrada con la clave pública del WSC_1. Después, el WSC_1 descifra esa agregación con su clave privada para obtener la recomendación ponderada de todos los usuarios que pertenecen a ese IdP. Para llevar esto a cabo se proporciona un homomorfismo privado que cumple lo siguiente:

$$\sum_{i=0}^{n} \varphi(\omega_{u_i}) \cdot Rec_{u_i} = \varphi\left(\sum_{i=1}^{n} \omega_{u_i} \cdot Rec_{u_i}\right)$$

Por tanto, el WSC_1 puede ponderar individualmente la recomendación de cada usuario usando algunos mensajes, y el valor de recomendación real de cada usuario solo es conocido por su IdP correspondiente.

Según la Fig. 4, el consumidor de servicios web WSC_1 solicitado envía al IdP la satisfacción del usuario que solicitó el servicio, junto con un determinado umbral $\delta \in [0, 1]$, ambos sin cifrar, y que se usa para determinar si castigar o premiar a los usuarios o a los otros consumidores de servicios web.

La Fig. 5 muestra la utilización de conjuntos difusos para modelar niveles de confianza según una realización preferida de la presente invención. Después de calcular el valor de confianza global del proveedor de servicios web, el consumidor de servicios web solicitado WSC_1 tiene que decidir si llevar a cabo toda la transacción con el proveedor de servicios web, llevarla a cabo de manera parcial o incluso omitir cualquier interacción con el proveedor de servicios web. Esta decisión depende del nivel de confianza asignado al proveedor de servicios web. Cada consumidor de servicios web puede definir sus propios niveles de confianza.

Cada nivel de confianza tiene asociada una cantidad y/o un tipo de información que puede intercambiarse si la parte comunicante tiene asignado ese nivel. Por ejemplo, en el ejemplo mostrado en la Fig. 5 hay cuatro niveles de confianza. Si un proveedor de servicios web tiene asignado el nivel “fiable”, entonces puede llevarse a cabo toda la transacción. Si el nivel de confianza es “+/- fiable”, entonces solo se intercambia determinada información no crítica. Si el proveedor de servicios web tiene asignado el nivel “+/- no fiable”, entonces se intercambia muy poca información relevante o no crítica. Si el nivel es “no fiable”, entonces no lleva a cabo ninguna transacción.

Para averiguar el nivel de confianza de un proveedor de servicios web a partir de su valor de confianza global *GT* es

necesario conocer los valores devueltos por las funciones de pertenencia de cada conjunto difuso que contiene *GT* como un elemento. En el ejemplo mostrado en la Fig. 5, la función de pertenencia del conjunto difuso "no fiable" devuelve el valor ε_1 para *GT*, mientras que la función de pertenencia del conjunto difuso "+/- no fiable" devuelve ε_2 para el mismo valor preciso. Una vez que tiene todos estos valores, la probabilidad de que al proveedor de servicios web se le asigne un nivel de confianza u otro se calcula de la siguiente manera:

$$P(\text{" No fiable "}) = \frac{\varepsilon_1}{\varepsilon_1 + \varepsilon_2}$$

$$P(\text{"+/- No fiable "}) = \frac{\varepsilon_2}{\varepsilon_1 + \varepsilon_2}$$

De manera genérica, la probabilidad de asignar al proveedor de servicios web el nivel de confianza TL_j, siendo ε_1 e i=1…,n los valores devueltos por cada función de pertenencia (y n el número de niveles de confianza), puede obtenerse con la siguiente fórmula:

$$P(TL_j) = \frac{\varepsilon_j}{\sum_{i=1}^{n} \varepsilon_i}$$

Si $\varepsilon_j = 0, \forall j$, se selecciona el conjunto difuso TL_K, donde $\varepsilon_k \neq 0$ para el valor más cercano a $v < GT$.

La Fig. 6 muestra un mecanismo para medir la divergencia entre la satisfacción final *Sat* del usuario y la recomendación proporcionada anteriormente Rec_i de cada usuario, donde se calcula el valor de $|Sat - Rec_i|$. Por tanto, como puede observarse en la Fig. 6, si $|Sat - Rec_i| < \delta$, entonces se premia al usuario u_i. En caso contrario, si $|Sat - Rec_i| \geq \delta$, entonces se castiga al usuario u_i.

El castigo y el premio son proporcionales a la diferencia entre la recomendación dada por el usuario y la satisfacción percibida por el cliente. Es decir, cuanto más similares sean estos valores mayor será el premio, y cuanto más dispares sean estos valores mayor será el castigo.

Puesto que $|Sat - Rec_i|$, $\omega_i \in [0, 1]$, se necesita el homomorfismo privado φ para llevar a cabo las siguientes operaciones: si $|Sat - Rec_i| < \delta$, es decir, si va a premiarse al usuario u_i, se aumenta su peso ω_i,

$$\varphi(\omega_i)^{|Sat - Rec_i|} = \varphi\left(\omega^{|Sat - Rec_i|}\right)$$

y si $|Sat - Rec_i| \geq \delta$, es decir, si va a castigarse al usuario u_i, se reduce su peso ω_i,

$$\varphi(\omega_i)^{\frac{1}{|Sat - Rec_i|}} = \varphi\left(\omega_i^{|Sat - Rec_i|}\right)$$

Una vez que se hayan modificado de manera apropiada todos los pesos de usuario almacenados en un IdP, los pesos tienen que normalizarse para mantener la condición mostrada en la ecuación (4) de acuerdo con:

$$\varphi(\omega_i) = \frac{\varphi(\omega_i)}{\sum_{j=1}^{n} \varphi(\omega_j)} = \varphi\left(\frac{\omega_i}{\sum_{j=1}^{n} \omega_j}\right)$$

Es importante observar que un valor $\delta \to 1$ significa un premio y un castigo bajos, mientras que $\delta \to 0$ significa un premio y un castigo elevados. Es importante observar también la relevancia del parámetro δ, ya que controla el mecanismo de premio y castigo. Un valor bajo de δ implica que muy pocos usuarios serán premiados y muchos serán castigados, pero aquellos que son premiados lo serán en gran medida. Por otro lado, un valor elevado de δ significa que muchos usuarios serán premiados, mientras que los pocos que serán castigados no lo serán severamente.

Por tanto, pueden obtenerse las siguientes implicaciones:

$$\delta \to 0 \Rightarrow \rho \to -1 \Rightarrow \omega \to 0$$

$$\delta \to 1 \Rightarrow \rho \to 1 \Rightarrow \omega \to 1$$

Es decir, cuanto menor sea δ, más estricto y severo será el castigo. Cuanto mayor sea δ, mayor será el premio. Por tanto, un buen valor inicial es $\delta = 0{,}5$. Sin embargo, también puede actualizarse dinámicamente a lo largo del tiempo para evitar cambios en el comportamiento del proveedor de servicios web, y cada consumidor de servicios web se ocupará de gestionar de manera individual su propio valor de parámetro δ.

La Fig. 7 ilustra la actualización de los pesos de las fuentes de información según una realización de la presente invención. En lo que respecta al valor inicial de los pesos proporcionados a cada fuente de información, se considera que un buen conjunto de valores podría ser el siguiente:

$$\omega_D = 0.5$$

$$\omega_U = \omega_{WSC} = 0.25$$

Además, la evolución de estos pesos a lo largo del tiempo depende de la precisión y la fiabilidad de cada fuente. Por tanto, si los usuarios (así como los consumidores de servicios web) son siempre castigados, la influencia de sus opiniones en la valoración de confianza en forma de la confianza global *GT* se reducirá. Por otro lado, si las entidades de una fuente de información son siempre premiadas, a esa fuente precisa se le proporcionará un mayor peso cuando se calcule el valor de confianza global.

Por tanto, sea ρ_U la media entre la cantidad de premios y castigos recibidos por todos los usuarios consultados, calculada de la siguiente manera:

$$\rho_U = \frac{\sum_{i=1}^{n} \left((1 - |Sat - Rec_i|_{<\delta}) - |Sat - Rec_i|_{\geq\delta}\right)}{n} \qquad (9)$$

ρ_{WSC} se obtendría de manera muy similar. Es muy importante observar que ρ_U, $\rho_{WSC} \in [-1, 1]$. Un valor $\rho_U = -1$ significa que absolutamente todos los usuarios han recibido el máximo castigo (es decir, $|Sat - Rec_i| = 1 \geq \delta, \forall i$), de modo que su peso debería reducirse a 0.

Como alternativa, $\rho_U = 1$ implica que todos los usuarios han recibido el máximo premio posible (es decir, $|Sat - Rec_i| = 0 \leq \delta, \forall i$), de modo que su peso debería tomar el valor máximo.

Finalmente, si $\rho_U = 0$, por término medio la mitad de los usuarios ha dado una mala recomendación (y por lo tanto han sido castigados), y la otra mitad ha recibido un buen premio debido a sus recomendaciones precisas. En este caso, el peso ω_U proporcionado a los usuarios en la fórmula (3) debería permanecer invariable.

Para conseguir estas condiciones, ambos pesos ω_U y ω_{WSC} pueden redefinirse después de que haya finalizado la última etapa de castigo y gratificación, siguiendo las siguientes fórmulas, como puede observarse en la Fig. 7:

$$\omega_U \leftarrow \omega_U^{\frac{2}{1+\rho_U}-1} \qquad \omega_{WSC} \leftarrow \omega_{WSC}^{\frac{1}{1+\rho_{WSC}}-1} \qquad (10)$$

Finalmente, para mantener la relación mostrada en la ecuación (4), los pesos deben normalizarse, es decir:

$$\omega_D = \frac{\omega_D}{\omega_D + \omega_U + \omega_{WPC}} \qquad \omega_U = \frac{\omega_U}{\omega_D + \omega_U + \omega_{WPC}} \qquad \omega_{WPC} = \frac{\omega_{WPC}}{\omega_D + \omega_U + \omega_{WPC}}$$

Otra normalización es también necesaria cuando un nuevo usuario se une o se registra en el proveedor de identidad. En ese caso, al nuevo usuario se le proporciona inicialmente el peso por defecto $\varphi(\omega_0)$, pero ya que esta incorporación rompe la condición mostrada en la ecuación (4), debe realizarse de nuevo la siguiente operación:

$$\varphi(\omega_i) = \frac{\varphi(\omega_i)}{\sum_j^{n+1} \varphi(\omega_j)} = \varphi\left(\frac{\omega_i}{\sum_{j=1}^{n+1} \omega_j}\right)$$

La Fig. 8 muestra un escenario de aplicación adicional según un procedimiento y una red según la presente invención, e ilustra en detalle las etapas llevadas a cabo.

Las etapas ilustradas en la Fig. 8, son:

1. Un usuario solicita un servicio a un determinado consumidor de servicios web WSC_1.

2. El WSC_1 solicita a todos sus proveedores de identidad IdP conocidos sus recomendaciones agregadas acerca del proveedor de servicios web WSP seleccionado, proporcionadas por los usuarios y por los consumidores de servicios web (WSC) registrados en los mismos.

3. Cada IdP comprueba las recomendaciones de sus usuarios y los WSC acerca del WSP consultado y lleva a cabo la recomendación agregada según las fórmulas (1) y (2).

4. Cada IdP devuelve la recomendación agregada al WSC_1 solicitado.

5. El WSC_1 evalúa su valoración de confianza en forma del valor de confianza global acerca del WSP usando la fórmula (3) y la asigna a uno de sus niveles de confianza.

6. El WSC_1 solicita después el servicio al WSP, proporcionando más o menos parámetros, dependiendo del nivel de confianza asignado al WSP en la etapa anterior.

7. El WSP proporciona el servicio solicitado, o uno peor, o incluso uno mejor, dependiendo de su bondad.

8. El WSC_1 suministra el servicio al usuario.

9. El usuario proporciona información de respuesta al WSC_1, que incluye su satisfacción con el servicio recibido.

10. El WSC_1 envía la satisfacción del usuario, junto con el umbral δ, a cada IdP conocido.

11. Cada IdP calcula ρ_U y ρ_{WSC} según la fórmula (9) y las transfiere al WSC_1.

12. Cada IdP y el WSC_1 otorgan el castigo o premio correspondiente según las fórmulas (5), (6), (7) y (8) para el IdP, y según la fórmula (10) para el WSC_1.

La Fig. 9 es un diagrama de secuencias que ilustra las etapas de la Fig. 8, donde las etapas están incluidas en las etapas genéricas de la Fig. 2.

Muchas modificaciones y otras realizaciones de la invención descrita en el presente documento resultarán evidentes

a los expertos en la técnica, a los cuales pertenece la invención con el beneficio de las enseñanzas presentadas en la anterior descripción y los dibujos asociados. Por lo tanto, debe entenderse que la invención no está limitada a las realizaciones específicas dadas a conocer y que las modificaciones y otras realizaciones están incluidas dentro del alcance de las reivindicaciones adjuntas. Aunque en el presente documento se utilizan términos específicos, se usan solamente de manera genérica y descriptiva, y no con fines limitativos.

REIVINDICACIONES

1. Procedimiento para soportar un mecanismo de reputación en una red, donde dicha red incluye:

uno o más dominios (dominio A, dominio B, dominio C) con uno o más usuarios que están conectados a dichos dominios,

uno o más proveedores de identidad (IdP) que gestionan información de identidad en nombre de dichos usuarios, y

al menos una entidad que funciona como un consumidor de servicios web (WSC_1, WSC_2) para dichos usuarios,

caracterizado porque, en caso de que un usuario solicite a un consumidor de servicios web de uno de dichos dominios un servicio web proporcionado por un proveedor de servicios web (WSP), en particular de otro de dichos dominios, dicho consumidor de servicios web solicitado solicita a sus proveedores de identidad conocidos una recomendación de dicho proveedor de servicios web,

en el que dichos proveedores de identidad funcionan como agregadores de recomendaciones recopilando valoraciones de reputación de dicho proveedor de servicios web proporcionadas por entidades que están registradas en dichos proveedores de identidad, en particular usuarios y/o consumidores de servicios web,

en el que dichos proveedores de identidad devuelven una recomendación agregada a dicho consumidor de servicios web solicitado que, en función de dicha recomendación agregada, determina una valoración de confianza acerca de dicho proveedor de servicios web, y

en el que se utiliza un homomorfismo de privacidad para proporcionar un intercambio cifrado de información relacionada con recomendaciones entre dichos proveedores de identidad y dicho consumidor de servicios web solicitado.

2. Procedimiento según la reivindicación 1, en el que dicha recomendación agregada devuelta por dichos proveedores de identidad a dicho consumidor de servicios web solicitado en cada caso es un único valor agregado para recomendaciones de dichos usuarios que están registrados en dichos proveedores de identidad y/o un único valor agregado para recomendaciones de dichos consumidores de servicios web que están registrados en dichos proveedores de identidad.

3. Procedimiento según la reivindicación 1 ó 2, en el que se aplica el esquema de cifrado de ElGamal como dicho homomorfismo de privacidad.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que en una primera etapa, dicho consumidor de servicios web solicitado envía su clave pública a dichos proveedores de identidad junto con un peso inicial por defecto para dichas entidades que están registradas en dichos proveedores de identidad, donde dicho peso inicial se cifra con dicha clave pública de dicho consumidor de servicios web solicitado, y/o

en el que dichos proveedores de identidad (IdP) almacenan un peso proporcionado por dicho consumidor de servicios web solicitado a cada una de dichas entidades que están registradas en dichos proveedores de identidad, donde dicho peso se cifra con una clave pública de dicho consumidor de servicios web solicitado.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que dicho consumidor de servicios web solicitado descifra dicha recomendación agregada devuelta por dichos proveedores de identidad con su clave privada para obtener una recomendación ponderada de dichas entidades que están registradas en dichos proveedores de identidad, y/o

en el que cada uno de dichos proveedores de identidad lleva a cabo dicha recomendación agregada de usuarios que están registrados en dichos proveedores de identidad de acuerdo con:

$$\sum_{i=0}^{n} \varphi(\omega_{u_i}) \cdot Rec_{u_i} = \varphi\left(\sum_{i=1}^{n} \omega_{u_i} \cdot Rec_{u_i}\right),$$

donde Rec_{ui} es una recomendación proporcionada por un usuario u_i, que es uno de n usuarios que están registrados

en el proveedor de identidad correspondiente, donde ω_{ui} es el peso asignado a dicha recomendación de dicho usuario u_i, y donde φ es un homomorfismo de privacidad que permite la suma y la multiplicación escalar.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5, en el que cada uno de dichos proveedores de identidad lleva a cabo dicha recomendación agregada de consumidores de servicios web que están registrados en dichos proveedores de identidad de acuerdo con:

$$\sum_{i=0}^{m} \varphi(\omega_{WSC_i}) \cdot Rec_{WSC_i} = \varphi\left(\sum_{i=1}^{m} \omega_{WSC_i} \cdot Rec_{WSC_i}\right),$$

donde Rec_{WSCi} es una recomendación proporcionada por un consumidor de servicios web WSC_i, que es uno de m consumidores de servicios web que están registrados en el proveedor de identidad correspondiente, donde ω_{WSCi} es el peso asignado a dicha recomendación de dicho consumidor de servicios web WSC_i, y donde φ es un homomorfismo de privacidad que permite la suma y la multiplicación escalar.

7. Procedimiento según cualquiera de las reivindicaciones 1 a 6, en el que dicha valoración de confianza se determina de acuerdo con:

$$GT = (\omega_D \cdot T_D) + (\omega_U \cdot T_U) + (\omega_{WSC} \cdot T_{WSC});$$

donde GT es dicha valoración de confianza asignada a dicho proveedor de servicios web, donde T_D es una confianza directa depositada en dicho proveedor de servicios web, donde T_U es la confianza agregada recibida desde otros usuarios, donde T_{WSC} es la confianza agregada recibida desde otros consumidores de servicios web, y donde ω_D, ω_U y ω_{WSC} son los pesos correspondientes.

8. Procedimiento según cualquiera de las reivindicaciones 1 a 7, en el que dicho consumidor de servicios web solicitado define niveles de confianza, donde dicho consumidor de servicios web solicitado asigna dicha valoración de confianza a uno de dichos niveles de confianza,

en el que pueden utilizarse conjuntos difusos con el fin de representar dichos niveles de confianza.

9. Procedimiento según cualquiera de las reivindicaciones 1 a 8, en el que dicho consumidor de servicios web solicitado solicita dicho servicio web a dicho proveedor de servicios web,

en el que dicho proveedor de servicios web solicitado proporciona más o menos parámetros dependiendo del nivel de confianza asignado a dicho proveedor de servicios web, y/o

en el que se premia o se castiga a dichos usuarios y/o a dichos consumidores de servicios web que están registrados en dichos proveedores de identidad según la precisión y la fiabilidad de sus recomendaciones.

10. Procedimiento según cualquiera de las reivindicaciones 1 a 9, en el que dicho usuario solicitante proporciona información de respuesta a dicho consumidor de servicios web solicitado, donde dicha información de respuesta incluye la satisfacción de dicho usuario solicitante en relación con dicho servicio web proporcionado.

11. Procedimiento según cualquiera de las reivindicaciones 1 a 10, en el que dicho consumidor de servicios web solicitado envía dicha satisfacción junto con un umbral δ a dichos proveedores de identidad, donde dicho umbral δ se utiliza para determinar si castigar o premiar a dichos usuarios y/o proveedores de servicios web que están registrados en dichos proveedores de identidad,

en el que la divergencia entre la satisfacción Sat de dicho usuario solicitante y una recomendación proporcionada anteriormente Rec_{ui} de un usuario u_i puede medirse calculando el valor de $|Sat - Rec_{ui}|$, donde se premia al usuario u_i en caso de que $|Sat - Rec_{ui}| < \delta$, y donde se castiga al usuario u_i en caso de que $|Sat - Rec_{ui}| \geq \delta$.

12. Procedimiento según cualquiera de las reivindicaciones 1 a 11, en el que en caso de que se premie a

un usuario u_i , el peso del usuario u_i aumenta de acuerdo con:

$$\varphi(\omega_{u_i})^{|Sat-Rec_{ui}|} = \varphi\left(\omega_{u_i}^{|Sat-Rec_{ui}|}\right), \text{ and}$$

y en el que en caso de que se castigue al usuario u_i, el peso ω_{ui} del usuario u_i disminuye de acuerdo con:

$$\varphi(\omega_{u_i})^{\frac{1}{|Sat-Rec_{ui}|}} = \varphi\left(\omega_{u_i}^{\frac{1}{|Sat-Rec_{ui}|}}\right)$$

13. Procedimiento según cualquiera de las reivindicaciones 1 a 12, en el que en caso de que se premie a un consumidor de servicios web WSC_i, el peso ω_{WSCi} del WSC_i de usuario aumenta de acuerdo con:

$$\varphi(\omega_{WSC_i})^{|Sat-Rec_{WSCi}|} = \varphi\left(\omega_{WSC_i}^{|Sat-Rec_{WSCi}|}\right), \text{ and}$$

y en el que en caso de que se castigue al usuario u_i, el peso del usuario u_i disminuye de acuerdo con:

$$\varphi(\omega_{WSC_i})^{\frac{1}{|Sat-Rec_{WSCi}|}} = \varphi\left(\omega_{WSC_i}^{\frac{1}{|Sat-Rec_{WSCi}|}}\right).$$

14. Procedimiento según cualquiera de las reivindicaciones 1 a 13, en el que cada uno de dichos proveedores de identidad calcula una desviación media de dicha satisfacción de dicho usuario solicitante con dichas recomendaciones de dichos usuarios y/o consumidores de servicios web que están registrados en dichos proveedores de identidad, donde dichos proveedores de identidad envían dicha desviación media a dicho consumidor de servicios web solicitado,

en el que dicho consumidor de servicios web solicitado puede otorgar un premio o castigo correspondiente en relación con dichos pesos ω_U y ω_{WSC} en función de dicha desviación media recibida desde dichos proveedores de identidad.

15. Red que incluye un mecanismo de reputación, en particular para la ejecución del procedimiento según cualquiera de las reivindicaciones 1 a 14, comprendiendo dicha red:

uno o más dominios (dominio A, dominio B, dominio C) con uno o más usuarios que están conectados a dichos dominios,

uno o más proveedores de identidad (IdP) que gestionan información de identidad en nombre de dichos usuarios, y

al menos una entidad que funciona como un consumidor de servicios web (WSC_1, WSC_2) para dichos usuarios,

caracterizada porque, en caso de que un usuario solicite a un consumidor de servicios web de uno de dichos dominios un servicio web proporcionado por un proveedor de servicios web, en particular de otro de dichos dominios, dicho consumidor de servicios web solicitado solicita a sus proveedores de identidad conocidos una recomendación de dicho proveedor de servicios web,

en la que dichos proveedores de identidad funcionan como agregadores de recomendaciones recopilando valoraciones de reputación de dicho proveedor de servicios web proporcionadas por entidades que están registradas en dichos proveedores de identidad, en particular usuarios y/o consumidores de servicios web,

en la que dichos proveedores de identidad devuelven una recomendación agregada a dicho consumidor de servicios web solicitado que, en función de dicha recomendación agregada, determina una valoración de confianza acerca de dicho proveedor de servicios web, y

en la que se utiliza un homomorfismo de privacidad para proporcionar un intercambio cifrado de información relacionada con recomendaciones entre dichos proveedores de identidad y dicho consumidor de servicios web solicitado.

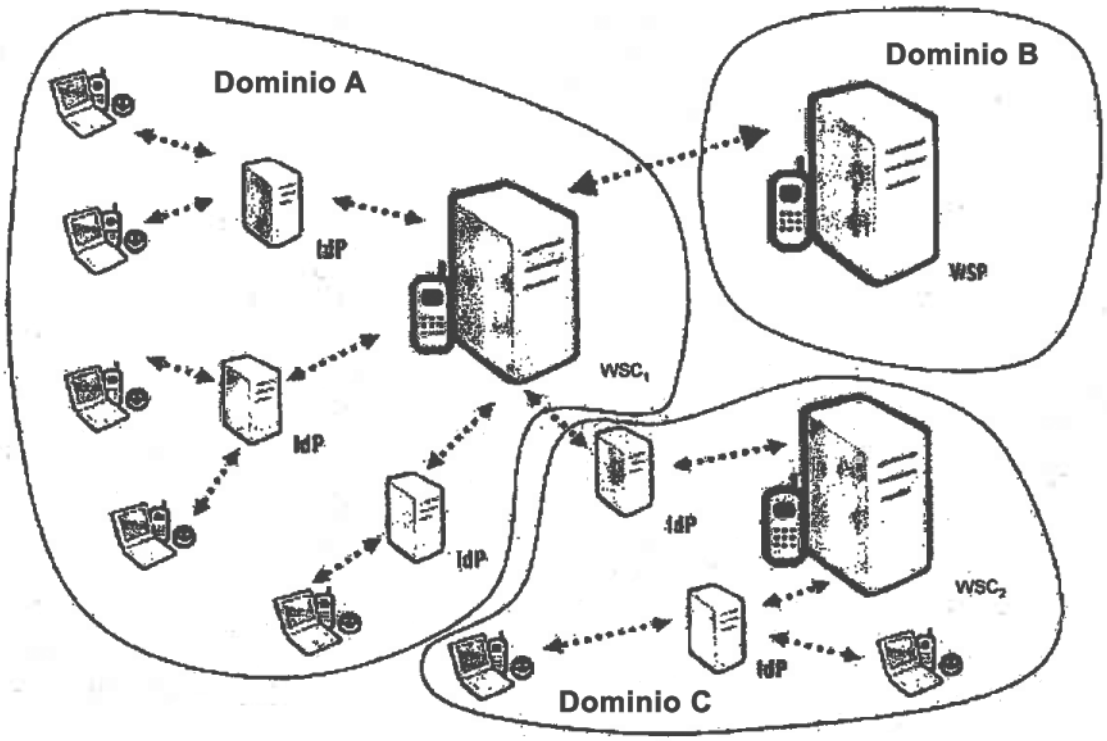
Dominio A
Dominio B
Dominio C
IdP
IdP
IdP
IdP
IdP
WSP
WSC1
WSC2

Fig. 1


1
Recopilar información
2
Puntuar y clasificar
3
Transacción
4
Premiar / Castigar

Fig. 2

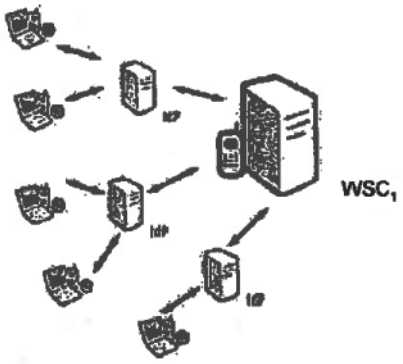

Fig. 3a

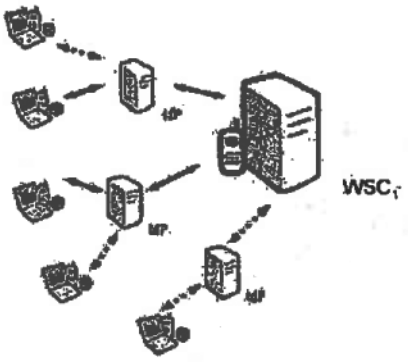

Fig. 3b

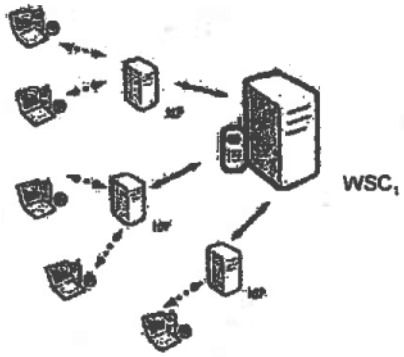

Fig. 3c

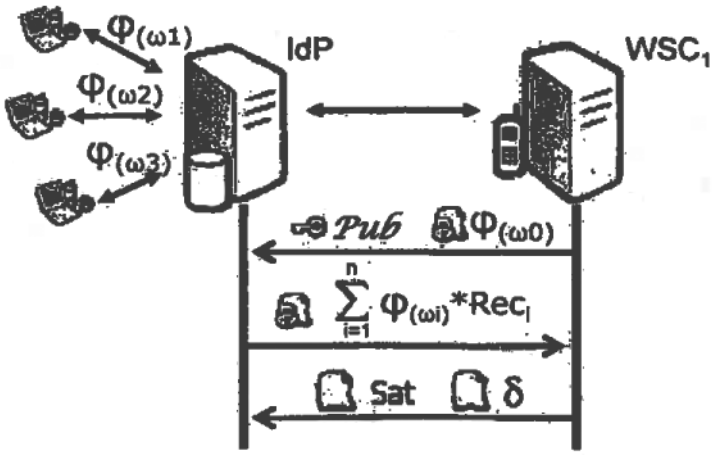

Fig. 4

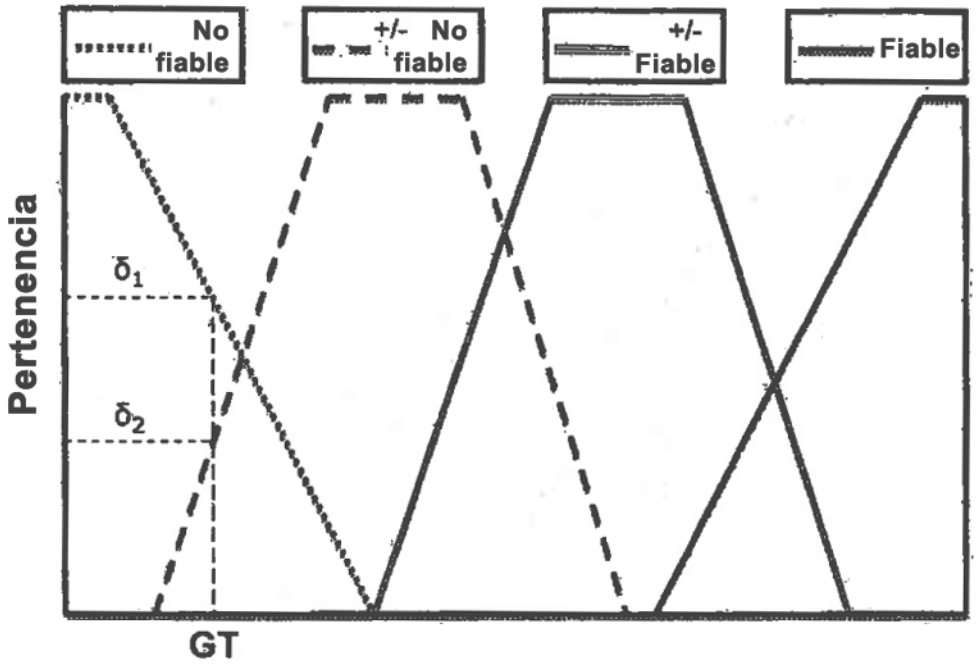

Fig. 5

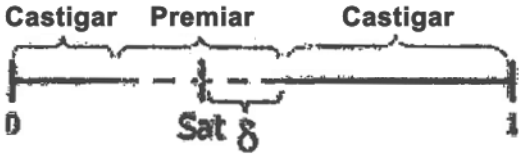

Fig. 6

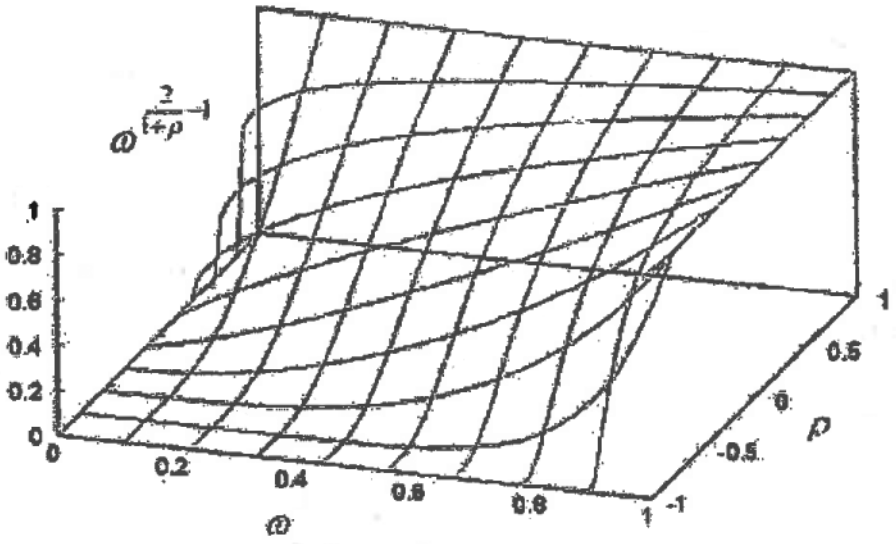
$\omega^{\frac{2}{1+\rho}-1}$
1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1
ω
-1
-0.5
0
0.5
1
ρ

Fig. 7

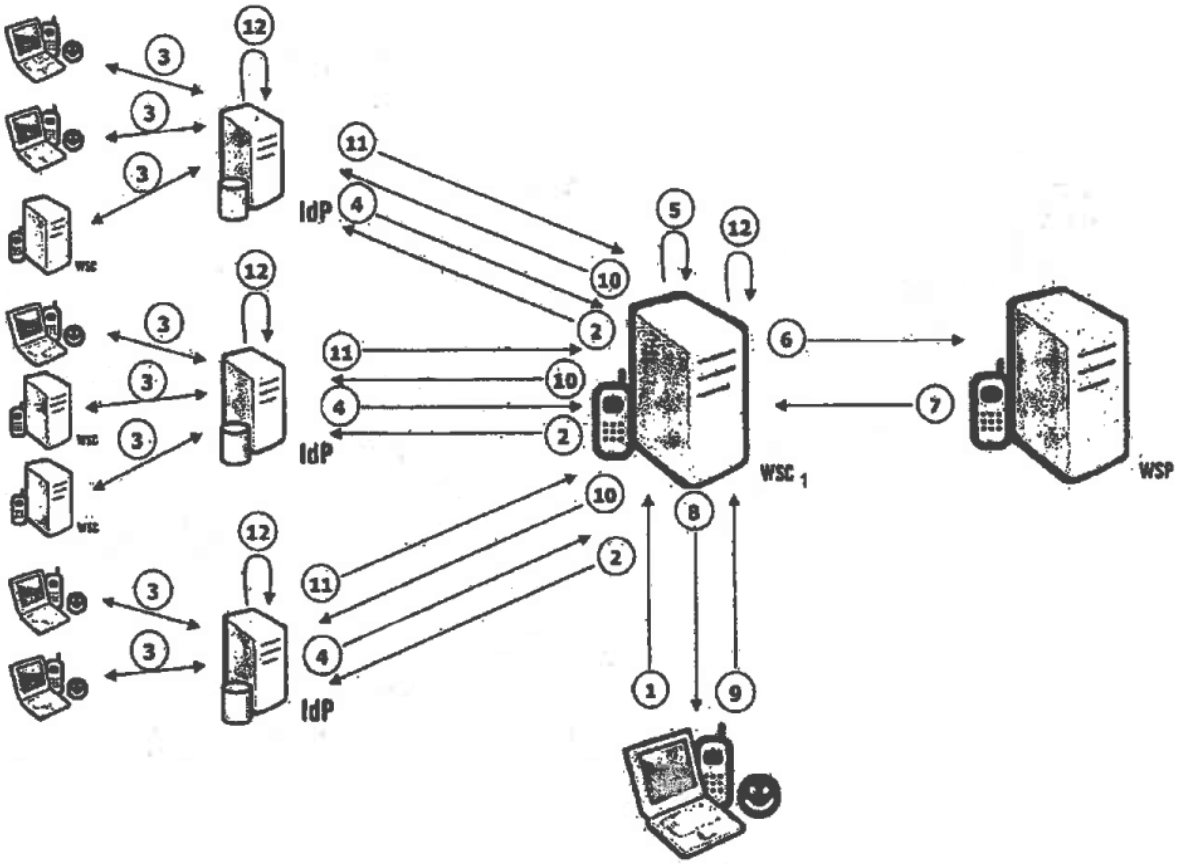

Fig. 8

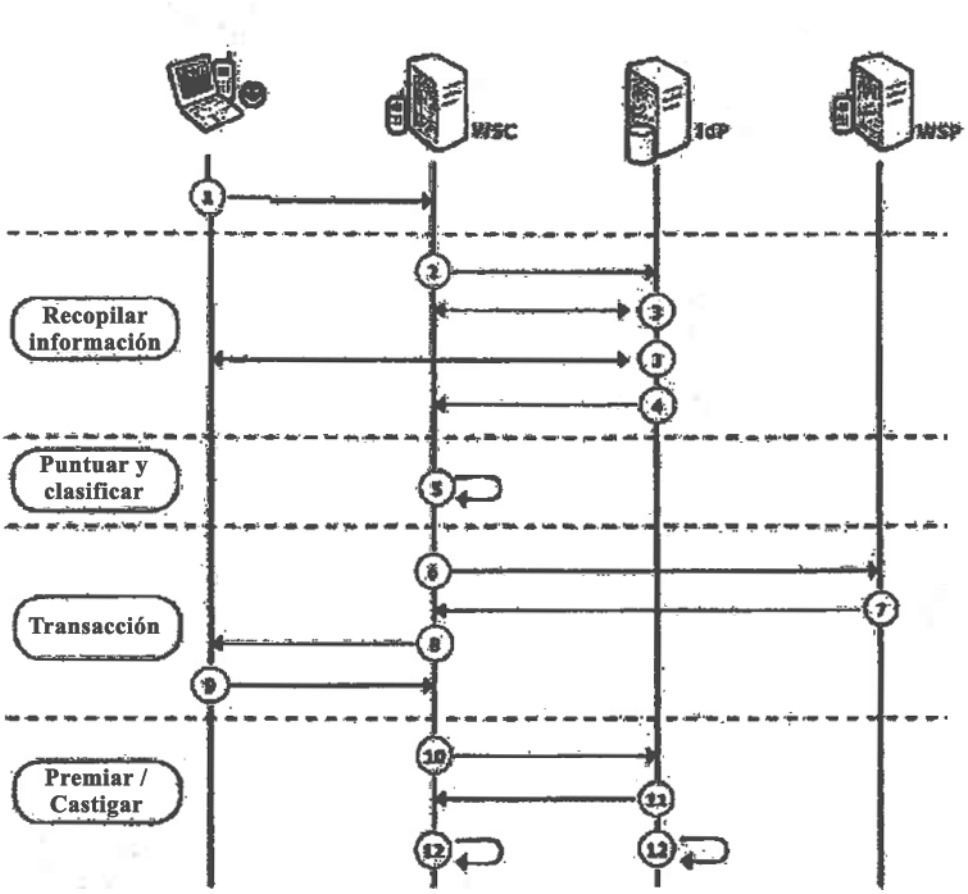
WSC
IGP
WSP
Recopilar información
Puntuar y clasificar
Transacción
Premiar / Castigar
1
2
3
4
5
6
7
8
9
10
11
12
13

Fig. 9