(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 632 167**

(21) Número de solicitud: 201630267

(51) Int. CI.:

G06F 21/62 (2013.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

07.03.2016

(43) Fecha de publicación de la solicitud:

11.09.2017

Fecha de la concesión:

02.03.2018

(45) Fecha de publicación de la concesión:

09.03.2018

(73) Titular/es:

SHOKESU, S.L. (100.0%)
Plaza Sancho Avarca, nº 2
31014 PAMPLONA (Navarra) ES

(72) Inventor/es:

ECHEVERRIA ARAMBILLET, Alfonso;
GONZÁLEZ GONZÁLEZ, Diana y
LABARGA, Alberto

(74) Agente/Representante:

BARBOZA, Gonzalo

(54) Título: **SISTEMA DE MONITOREO Y EXTRACCIÓN DE INFORMACIONES PÚBLICAS DE USUARIOS REGISTRADOS EN REDES SOCIALES, ALOJADAS EN SERVIDORES Y NUBES DE DATOS DE REDES SOCIALES**

(57) Resumen:

Método de monitoreo y extracción de informaciones publicadas de usuarios registrados en redes sociales que comprende transmitir periódicamente a las API de redes sociales de forma que cada mensaje de consulta (1) comprende al menos una identificación de una cuenta de usuario (4) asignada a una credencial de acceso (2) a la API de la red social y se envía sólo cuando la credencial de acceso (2) comprende una clave de estado disponible (9a) y después de un tiempo transcurrido desde que la credencial de acceso (2) ha sido utilizada por última vez para la transmisión de un mensaje de consulta (1), siendo el número de identificaciones de cuentas de usuario (4) contenido en cada mensaje de consulta (1) menor que un número máximo de peticiones de información efectuadas con una credencial de acceso (2) admitido en un intervalo de tiempo determinado por la API (7) de la red social (8). El sistema que se describe sirve para realizar este método.

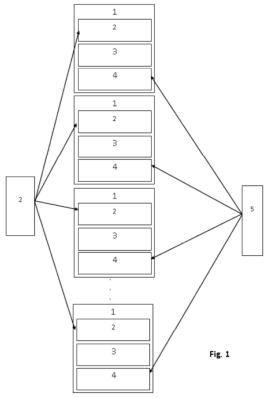

Fig. 1

ES 2 632 167 B1

DESCRIPCIÓN

SISTEMA DE MONITOREO Y EXTRACCIÓN DE INFORMACIONES PÚBLICAS DE USUARIOS REGISTRADOS EN REDES SOCIALES, ALOJADAS EN SERVIDORES Y NUBES DE DATOS DE REDES SOCIALES

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención se encuadra en el campo técnico de los sistemas de monitoreo y extracción de datos públicos de redes sociales alojados en servidores y nubes de datos.

ESTADO DE LA TÉCNICA ANTERIOR A LA INVENCIÓN

Las redes sociales en internet están adquiriendo una relevancia cada vez mayor en los últimos tiempos. Permiten a sus usuarios interaccionar estableciendo contactos formando comunidades según intereses, intercambiando conocimientos y mensajes y coordinando actividades comunes. Existe un gran número de redes sociales de diferentes tipos tales como las conocidas redes sociales Facebook, Linkedin, Twitter, Goggle+, Twitter, Youtube, Myspace, SoundCloud, etc. Se basan en sitios o páginas web diseñadas para facilitar la comunicación entre los usuarios mediante herramientas fáciles de usar. Los contenidos de estos sitios web y de las publicaciones realizadas por sus usuarios están alojados en servidores y/o en nubes de datos. Las redes sociales son sin duda una inmensa fuente de información y hoy en día hay cientos de millones de usuarios registrados en las mismas.

Las redes sociales suelen estar constituidas por comunidades de usuarios miembros de la red social que están registrados y acreditados en la red social por credenciales de usuario, por ejemplo una cuenta y una contraseña, que le permiten, por una parte, publicar informaciones en su propio nombre y, por otra parte, acceder a las informaciones publicadas por otros usuarios miembros de la misma red social. Los usuarios pueden ser personas particulares, instituciones públicas y privadas, empresas, asociaciones culturales, deportivas y políticas, etc.

Los servicios de redes sociales permiten a los usuarios registrados crear un perfil para ellos mismos y publicar mensajes, artículos y enlaces. Estos perfiles pueden ser públicos

y la información estar accesible para todos los usuarios de internet o, en su gran mayoría, públicos solo para usuarios registrados en la misma red social. Estos servicios generalmente disponen de un sistema API (= interfaz de programación de aplicaciones), que permite a aplicaciones de terceros hacer uso de la información disponible, así como de diversas otras funcionalidades.

Las API de las redes sociales tienen una limitación de peticiones de información por cada aplicación usada que restringe el número de peticiones de información que un usuario registrado en la red social o un tercero pueden realizar en un determinado intervalo de tiempo, de manera que, una vez superadas este número de peticiones, la API entra en un periodo de bloqueo temporal durante el que la API rechaza por defecto las nuevas peticiones de información formuladas utilizando una misma credencial de usuario.

Ante el creciente número de redes sociales y ante el hecho de que muchos de sus usuarios están registrados en más de una red social, es cada vez más difícil monitorear y recopilar las informaciones publicadas en las redes sociales de una forma eficaz y con unas capacidades de computación físicas (hardware) razonablemente dimensionadas.

El documento US7886000B1 describe un sistema que, entre otros servicios, comprende una aplicación que permite a un usuario visualizar la información y realizar múltiples acciones sobre distintas cuentas de usuario privadas, de una pluralidad de redes sociales. Estas cuentas de usuario son generalmente propietarias del mismo usuario y es necesario hacer entrar en y autorizar la aplicación para poder obtener la información requerida.

El documento US20110179161A1 describe un procedimiento que permite combinar en un sistema local controlado por el usuario datos agregados de perfiles públicos de varias redes sociales con perfiles privados del propio usuario residentes en el sistema local.

Ninguno de estos sistemas presenta la capacidad de recopilar, almacenar y visualizar las publicaciones de otros perfiles públicos de usuarios que no estén asociados a las cuentas que el usuario registrado ha autorizado. Tampoco contemplan la posibilidad de hacer público en una página web el contenido generado por estos perfiles.

Era, por tanto, deseable, diseñar un sistema eficaz de monitoreo y extracción de datos

públicos alojados en servidores y nubes de datos de redes sociales y correspondientes a usuarios registrados en estas redes sociales.

Descripción de la invención

La presente invención tiene por objeto mejorar los sistemas y métodos de monitoreo y extracción de informaciones públicas de usuarios registrados de redes sociales, alojadas en servidores y nubes de datos de redes sociales del estado de la técnica mediante un procedimiento, así como un sistema de monitoreo y extracción de tales informaciones públicas. Características y realizaciones de la invención se describirán a continuación.

El método conforme a la invención comprende transmitir mensajes de consulta que comprenden credenciales de acceso a un API (=interfaz de programación de aplicaciones) de cada red social, de identificaciones de cuentas de usuario de usuarios registrados en las redes públicas, a las direcciones URL de las redes sociales para obtener las informaciones publicadas por los usuarios monitorizados, recibir las informaciones publicadas y guardarlas en una base de datos de informaciones.

Conforme a este método, los mensajes de consulta se transmiten periódicamente a las API de las redes sociales de forma que cada mensaje de consulta comprende al menos una identificación de una cuenta de usuario registrada en la red social, asignada a una credencial de acceso a la API de una red social, y cada mensaje de consulta se envía sólo cuando la credencial de acceso comprende una clave de estado disponible y después de un tiempo transcurrido desde que la credencial de acceso ha sido utilizada por última vez para la transmisión de un mensaje de consulta, calculado desde una fecha y hora de último acceso identificada por una clave de último acceso.

Cada mensaje de consulta transmitido se marca con un código de completación identificativo de una fecha y hora de completación de la transmisión del mensaje de consulta. El código de completación del mensaje de consulta transmitido se asigna a la credencial de acceso como la clave de último acceso.

Después de un periodo de tiempo predeterminado, calculado desde la fecha y hora de último acceso identificada por la clave de último acceso, se vuelve a enviar un mensaje de consulta con la credencial de acceso a la que se ha asignado el código de último

acceso. El número de identificaciones de cuentas de usuario contenido en cada mensaje de consulta es menor que un número máximo de peticiones de información efectuadas con una credencial de acceso admitido en un intervalo de tiempo determinado por la API de la red social sin entrar en un periodo de bloqueo temporal.

El periodo de tiempo predeterminado puede ser mayor que un periodo de bloqueo temporal durante el que la API a la que se transmite el mensaje de consulta rechaza por defecto nuevas peticiones de información efectuadas con una misma credencial de acceso.

El método anteriormente descrito puede implantarse mediante un sistema de monitoreo y extracción de informaciones públicas de usuarios registrados de redes sociales, alojadas en servidores y nubes de datos de redes sociales que comprende un dispositivo transmisor, un dispositivo receptor de publicaciones y un dispositivo de almacenamiento.

El dispositivo transmisor está diseñado para transmitir mensajes de consulta a cuentas de usuario seleccionadas empleando credenciales de acceso a APIs de una pluralidad de redes sociales, mientras que el dispositivo receptor de informaciones está diseñado para recibir y extraer datos de las informaciones publicadas en las cuentas de usuario seleccionadas a las que se ha accedido a través de los APIs. Por otra parte, el dispositivo de almacenamiento está diseñado para almacenar los datos publicados clasificados de cada perfil monitorizado.

Conforme a la invención, el sistema comprende además un dispositivo seleccionador de credenciales, un dispositivo formador de mensajes de consulta, un dispositivo detector, un dispositivo asignador, un dispositivo cambiador de claves de estado, así como un dispositivo iterador.

El dispositivo seleccionador de credenciales está diseñado para seleccionar credenciales de acceso disponibles contenidas en una base de datos de credenciales. En esta base de datos a cada credencial de acceso le están asignadas una clave de último acceso y una clave de estado. La clave de último acceso es identificativa de una fecha y hora de último acceso en la que la credencial de acceso ha sido utilizada por última vez en un mensaje de consulta transmitido, mientras que la clave de estado es una clave de estado ocupado o una clave de estado disponible. Cada credencial de acceso disponible comprende una

clave de estado disponible y una clave de último acceso identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado.

El dispositivo formador de mensajes de consulta está diseñado para formar mensajes de consulta dirigidas a cada API. Cada mensaje de consulta comprende al menos una identificación de cuenta de usuario registrada en la red social, asignada a una credencial de acceso a la API de dicha red social. El número del grupo de identificaciones de cuentas de usuario en cada mensaje de consulta es menor que un número máximo de peticiones de información efectuadas con una credencial de acceso admitido en un intervalo de tiempo determinado por la API sin entrar en un periodo de bloqueo temporal.

El dispositivo detector está diseñado para detectar la fecha y hora en la que un mensaje de consulta ha sido transmitido y para marcar cada mensaje de consulta transmitido con un código de completación identificativo de la fecha y hora de completación de la transmisión del mensaje. El dispositivo asignador está diseñado para asignar el código de completación como fecha y hora de último acceso, a la credencial de acceso contenida en cada mensaje de consulta transmitido.

El dispositivo cambiador de claves de estado está diseñado para cambiar la clave de estado disponible de cada una de las credenciales de acceso seleccionadas a la clave de estado ocupado, y para cambiar la clave de estado ocupado asignada a la credencial de acceso contenida en cada mensaje de consulta transmitido a una clave de estado disponible,

Por su parte, el dispositivo iterador está diseñado para ordenar al dispositivo seleccionador la selección de nuevas credenciales de acceso disponibles contenidas en la base de credenciales para iniciar sucesivamente la formación de nuevos mensajes de consulta.

De acuerdo con una realización de la invención, el método comprende una etapa de selección, una etapa de cambio de estado, una etapa de formación de mensajes de consulta, una etapa de transmisión, una etapa de reseteo de estado, una etapa de asignación. Estas etapas se pueden iterar.

La etapa de selección comprende seleccionar credenciales de acceso disponibles en una base de datos de credenciales en la que cada credencial de acceso está asignada a la clave de último acceso y a la clave de estado. La clave de estado es una clave de estado ocupado o una clave de estado disponible. Cada credencial de acceso disponible comprende una clave de estado disponible y una clave de último acceso identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado.

La etapa de cambio de estado comprende cambiar la clave de estado disponible de cada una de las credenciales de acceso seleccionadas a la clave de estado ocupado.

La etapa de formación de mensajes comprende formar mensajes de consulta seleccionando identificaciones de cuentas de usuario disponibles en una cola de mensajería. La cola de mensajería comprende una pluralidad de identificaciones de cuentas de usuario. Se agrupa al menos una identificación de cuenta de usuario a una de las credenciales de acceso disponibles seleccionadas, de tal manera que los mensaje de consulta comprenden identificaciones de cuenta de usuario diferentes.

La etapa de transmisión comprende transmitir los mensajes de consulta y marcar el mensaje de consulta con un código de completación identificativo de la fecha y hora en la que el mensaje de consulta ha sido transmitido.

La etapa de reseteo de estado comprende cambiar la clave de estado ocupado asignada a la credencial de acceso contenida en cada mensaje de consulta transmitido a una clave de estado disponible, mientras que la etapa de asignación comprende asignar el código de completación como fecha y hora de último acceso, a la credencial de acceso contenida en el mensaje de consulta transmitido.

Las etapas anteriormente indicadas, es decir, la etapa de selección, la etapa de cambio de estado, la etapa de formación de mensajes de consulta, la etapa de transmisión, la etapa de reseteo de estado y la etapa de asignación, pueden iterarse para crear continuamente mensajes de consulta con credenciales que han vuelto a quedar disponibles a los que se agrupan identificaciones de cuentas de usuario seleccionadas sucesivamente de la cola de mensajería. Cada iteración se inicia con una nueva orden de seleccionar nuevas credenciales de acceso disponibles contenidas en la base de

credenciales para iniciar sucesivamente la formación de nuevos mensajes de consulta.

La etapa de formación de mensajes de consulta se puede realizar seleccionando, en una base de datos de colas de mensajería que comprende una pluralidad de identificaciones de cuentas de usuario monitorizadas y en la que cada identificación de usuario está asignada a una clave de disponibilidad o a una clave de no-disponibilidad, las identificaciones de cuentas de usuario disponibles que comprenden la clave de disponibilidad para obtener identificaciones disponibles seleccionadas y cambiando, en la base de datos de colas de mensajería, la clave de disponibilidad de cada identificación de cuenta de usuario disponible seleccionada a la clave de no-disponibilidad.

En la base de datos de colas de mensajería, la clave de no-disponibilidad de cada identificación de cuenta de usuario contenida en un mensaje de consulta transmitida se puede cambiar a la clave de disponibilidad cuando la identificación de cuenta de usuario ha sido transmitida en un mensaje de consulta transmitido.

Para implantar esta realización del método, conforme a una realización de la invención puede comprender la base de datos de credenciales, y además de una base de datos de colas de mensajería, un dispositivo seleccionador de identificaciones, un dispositivo agrupador de identificaciones y un dispositivo asignador de credenciales.

La base de datos de colas de mensajería contiene identificaciones de cuentas de usuario, y en la que cada identificación de usuario está asignada a una clave de disponibilidad o a una clave de no-disponibilidad, mientras que el dispositivo seleccionador de identificaciones está diseñado para seleccionar, de entre las identificaciones de cuentas de usuario contenidas en la base de datos de colas de mensajería, las identificaciones de cuentas de usuario disponibles.

El dispositivo agrupador de identificaciones está diseñado para formar grupos de identificaciones disponibles, de manera que cada grupo de identificaciones al menos comprende una identificación de cuenta de usuario. A su vez, el dispositivo asignador de credenciales está diseñado para asignar cada grupo de identificaciones disponibles a una credencial de acceso disponible seleccionada por el dispositivo seleccionador de credenciales.

A cada mensaje se le puede asignar además un código de consulta seleccionado entre códigos de fecha y hora, códigos de número y combinaciones de los mismos. El código de fecha y hora define una fecha y hora a partir de la que se piden informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario comprendida en el mensaje de consulta, mientras que el código de número define un número máximo de últimas informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario comprendida en el mensaje de consulta. Para asignar los códigos de consulta el dispositivo formador de mensajes del sistema puede estar provisto de un dispositivo asignador de códigos de consulta.

Las informaciones devueltas por las APIs en respuesta a los mensajes se pueden almacenar generando mensajes de respuesta en una cola de almacenamiento de publicaciones. Los procesos de almacenamiento de publicaciones pueden generar, por ejemplo, mensajes en la cola de peticiones de páginas web.

La información contenida en el mensaje, consistente en la URL de la página y el ID de la publicación almacenada en las bases de datos puede extraerse. Si la página ha sido almacenada con antelación (vinculada con otra publicación), guarda en la base de datos la relación con el ID de la publicación. A partir de cada enlace obtenido, se puede hacer una petición HTTP.

En caso de éxito en la petición HTTP, el sistema puede tomar el contenido HTML de la página correspondiente y pasarlo por un filtro (Open Source) que toma el contenido relevante de la página, eliminando código y contenido innecesario como banners, pies de páginas, menús, etc. Este contenido puede ser pasado por un filtro para estructurar los datos de una manera particular.

Los datos son publicados en un mensaje en la cola de publicaciones a guardar.

Los mensajes de respuesta pueden estar contenidos en la cola de almacenamiento de páginas. Varios procesos iguales son lanzados y controlados para consumir estos mensajes. Cada uno de estos procesos puede consistir en:

tomar la información contenida en el mensaje

guardar en una base de datos la información y relacionarla con el ID de la publicación.

publicar un mensaje en la cola de mensajería de peticiones de análisis semántico con los datos de la página.

Los mensajes pueden procesarse además tomando la información contenida en el mensaje, realizando una petición al servicio meaningcloud.com, enviando como cuerpo del mensaje el contenido de la publicación o la página, tomando los datos y publicándose estos datos en un mensaje en la cola de contenido semántico a guardar.

Asimismo, la información contenida en el mensaje puede guardarse en la base de datos relacionándola con el ID de la publicación o de la página.

De lo anterior se desprende, que la presente invención permite monitorizar automáticamente las publicaciones de usuarios registrados en redes sociales de forma rápida, eficaz y simple, basado en una arquitectura fácilmente escalable conforme aumente el volumen de publicaciones de usuario de redes sociales a monitorizar.

BREVE DESCRIPCIÓN DE LAS FIGURAS

A continuación se describirán realizaciones de la invención en base a unos dibujos esquemáticos, en los que

la figura 1 muestra características de una realización de los mensajes de consulta conforme a la presente invención y de su conformación.

la figura 2 muestra cómo se forman nuevos mensajes de consulta.

la figura 3 muestra las características de una primera realización del método conforme a la invención,

la figura 4 muestra las características del sistema conforme a la invención con el que se puede realizar el método ilustrado en la figura 3,

la figura 5 muestra las características de una segunda realización del método conforme a

la invención,

la figura 6 muestra las características de una realización del sistema conforme a la invención con el que se puede realizar el método ilustrado en la figura 5.

MODOS DE REALIZACIÓN DE LA INVENCIÓN

En la realización mostrada en la figura 1 puede apreciarse que los mensajes de consulta -1- comprenden cada uno credencial de acceso -2- a una API, un código de consulta -3- y un número predeterminado de identificaciones de cuentas de usuario -4- registradas en la red social a la que corresponde la API a la que se accede mediante la credencial de acceso -2-. El número de identificaciones de cuentas de usuario -4- contenido en cada mensaje de consulta -1- es menor que el número máximo de peticiones de información efectuadas con una credencial de acceso -2- admitido en un intervalo de tiempo determinado por la API sin entrar en un periodo de bloqueo temporal. El código de consulta -3- está seleccionado entre códigos de fecha y hora, códigos de número y combinaciones de los mismos. El código de fecha y hora define una fecha y hora a partir de la que se piden informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario -4- comprendida en el mensaje de consulta -1-, mientras que el código de número define un número máximo de últimas informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario comprendida en el mensaje de consulta -1-. Para asignar los códigos de consulta -3- el dispositivo formador de mensajes del sistema puede estar provisto de un dispositivo asignador de códigos de consulta.

Las respectivas credenciales de acceso -2- contenidas en los mensajes de consulta -1- provienen de credenciales de acceso -2- disponibles seleccionadas en una base de datos de credenciales (figuras 4 a 6), mientras que las identificaciones de cuentas de usuario -4- contenidas en cada mensaje de consulta -1- están seleccionadas entre identificaciones de cuentas de usuario provistas de una clave de disponibilidad provenientes de una cola de mensajería -5- que contiene identificaciones de cuentas de usuario registradas en la red social a cuya API se accede mediante las credenciales de acceso -2- contenidas en los mensajes de consulta -1-.

La figura 2 muestra una realización de cómo se forman nuevos mensajes de consulta -1-

Cuando un mensaje de consulta -1- ha sido transmitido, la credencial de acceso -2- contenida en ese mensaje de consulta -1- queda marcada con una clave de estado disponible -9a-, y la fecha y hora de transmisión del mensaje de consulta -1- es detectada y convertida en un código de completación -6- que se asigna a la credencial de acceso -2- como clave de último acceso identificativa de la fecha y hora en la que la credencial de acceso -2- ha sido empleada por última vez en un mensaje de consulta transmitido. Por otra parte, las identificaciones de cuentas de usuario -4- contenidas en el mensaje de consulta -1- han quedado marcadas con una clave de no disponibilidad -4a-.

Después de que haya transcurrido un periodo de tiempo –t- desde la fecha y hora identificada por la clave de último acceso -2a-, la credencial de acceso -2- vuelve estar disponible, de manera que, entre las identificaciones de cuentas de usuario -4- que en la cola de mensajería -5-, están marcadas con clave de disponibilidad, se selecciona un número de nuevas identificaciones de cuentas de usuario -4- registradas en la red social a la que corresponde la API, y se agrupa a la credencial de acceso -2- que ha vuelto a quedar disponible, para formar un nuevo mensaje de consulta -1-. De acuerdo con lo anteriormente indicado, el número de identificaciones de cuentas de usuario -4- contenido en cada mensaje de consulta -1- es menor que el número máximo de peticiones de información efectuadas con una credencial de acceso -2- admitido en un intervalo de tiempo determinado por la API sin entrar en un periodo de bloqueo temporal.

Para iniciar reiterativamente la formación de mensajes de consulta, se ordena al dispositivo seleccionador la selección de credenciales de acceso disponibles contenidas en la base de credenciales.

La figura 3 muestra una realización del método conforme a la invención, en la que los mensajes de consulta que cada uno comprenden un credencial de acceso a la que se ha agrupado un número de identificaciones de cuentas de usuario, se transmiten periódicamente a las API -7- de una red social -8-.

En una etapa de selección (paso A) se seleccionan credenciales de acceso disponibles en una base de datos de credenciales -10-. En la base de datos de credenciales -10-, cada credencial de acceso -2- está asignada a la clave de último acceso -2a- mencionada anteriormente en relación con la figura 2 y a una clave de estado -9-. La clave de estado -9- es la clave de estado disponible -9a- descrita anteriormente con referencia a la figura

2, o una clave de estado ocupado -9b-. Cada credencial de acceso -2- disponible comprende una clave de estado disponible -9a- y la clave de último acceso -2a- identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado. Después de esta selección (paso A), la clave de estado disponible -9a- de cada credencial de acceso -2- seleccionada se cambia (paso B) a la clave de estado ocupado -9b-.

Los mensajes de consulta se forman en una etapa de formación de mensajes (paso C) que comprende formar mensajes de consulta seleccionando identificaciones de cuentas de usuario disponibles, y agrupando un número de identificaciones de cuenta de usuario a cada una de las credenciales de acceso disponibles seleccionadas, de tal manera que los mensajes de consulta comprenden identificaciones de cuenta de usuario diferentes. De acuerdo con lo anteriormente indicado, el número de identificaciones de cuentas de usuario contenido en el mensaje de consulta es menor que el número máximo de peticiones de información efectuadas con la credencial de acceso que la API -7- admite en un intervalo de tiempo determinado sin entrar en un periodo de bloqueo temporal.

Los mensajes de consulta se transmiten (paso D) a la API -7- de la red social -8- a la que se refieren las credenciales de acceso y en la que están registradas las cuentas de usuario correspondientes a las identificaciones de cuentas de usuario contenidas en los respectivos mensajes. Cada mensaje de consulta transmitido se marca (paso E) con un código de completación identificativo de la fecha y hora en la que el mensaje de consulta ha sido transmitido. La transmisión (paso A) del mensaje también desencadena un reseteo de estado (paso F) que comprende cambiar la clave de estado ocupado asignada a la credencial de acceso contenida en cada mensaje de consulta transmitido a una clave de estado disponible. El código de completación se asigna (paso G) como clave de último acceso a la credencial de acceso contenida en el mensaje de consulta transmitido.

El mensaje de consulta se envía sólo cuando la credencial de acceso comprende una clave de estado disponible y después de un tiempo transcurrido desde que la credencial de acceso ha sido utilizada por última vez para la transmisión de un mensaje de consulta, calculado desde una fecha y hora de último acceso identificada por la clave de último acceso.

Las informaciones proporcionadas por la API -7- en respuesta a cada mensaje de

consulta se reciben (paso H) y se almacenan (paso I) para su procesamiento.

La etapa de selección (paso A), la etapa de cambio de estado (paso B), la etapa de formación de mensajes de consulta (paso C), la etapa de transmisión (paso D), la etapa de reseteo de estado (paso F) y la etapa de asignación (paso AG) se realizan de acuerdo con lo anteriormente descrito con respecto a la figura 2, de manera que después de un periodo de tiempo predeterminado, calculado desde la fecha y hora de último acceso identificada por la clave de último acceso, se vuelve a enviar un mensaje de consulta con la credencial de acceso a la que se había asignado la clave de último acceso.

Para iniciar reiterativamente la formación de mensajes de consulta, se ordena iterativamente (paso K) la selección de credenciales de acceso disponibles contenidas en la base de credenciales.

La realización del sistema conforme a la invención ilustrada en la figura 4 permite realizar el método mostrado en la figura 3. Según esta realización, el, sistema comprende un dispositivo transmisor -11-, un dispositivo receptor de informaciones -12- y un dispositivo de almacenamiento de informaciones -13-, un dispositivo seleccionador de credenciales -14-, un dispositivo formador de mensajes de consulta -15-, un dispositivo detector -16-, un dispositivo asignador -17-, un dispositivo cambiador de claves de estado -18-, así como un dispositivo iterador -19-.

El dispositivo seleccionador de credenciales -14- selecciona credenciales de acceso disponibles contenidas en la base de datos de credenciales -10- en la que a cada credencial de acceso le están asignadas una clave de último acceso y una clave de estado. La clave de último acceso es identificativa de una fecha y hora de último acceso en la que la credencial de acceso ha sido utilizada por última vez en un mensaje de consulta transmitido, mientras que la clave de estado es una clave de estado ocupado o una clave de estado disponible. Cada credencial de acceso disponible comprende una clave de estado disponible y una clave de último acceso identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado.

El dispositivo formador de mensajes de consulta -15- forma los mensajes de consulta dirigidas a cada API -7-. Cada mensaje de consulta comprende al menos una

identificación de cuenta de usuario registrada en la red social -8-, asignada a una credencial de acceso a la API -7- de dicha red social -8-. De acuerdo con lo anteriormente indicado, el número de identificaciones de cuentas de usuario en cada mensaje de consulta es menor que un número máximo de peticiones de información efectuadas con una credencial de acceso admitido en un intervalo de tiempo determinado por la API -7- sin entrar en un periodo de bloqueo temporal.

El dispositivo detector -16- detecta la fecha y hora en la que un mensaje de consulta ha sido transmitido y marca cada mensaje de consulta transmitido con un código de completación identificativo de la fecha y hora de completación de la transmisión del mensaje. El dispositivo asignador -17- asigna el código de completación como fecha y hora de último acceso a la credencial de acceso contenida en cada mensaje de consulta transmitido.

El dispositivo cambiador de claves de estado -18- cambia la clave de estado disponible de cada una de las credenciales de acceso seleccionadas a la clave de estado ocupado, y cambia la clave de estado ocupado asignada a la credencial de acceso contenida en cada mensaje de consulta transmitido en una clave de estado disponible,

El dispositivo iterador -19- ordena al dispositivo seleccionador la selección de credenciales de acceso disponibles contenidas en la base de credenciales para iniciar reiterativamente la formación de mensajes de consulta.

El dispositivo transmisor -11- transmite mensajes de consulta a cuentas de usuario seleccionadas empleando credenciales de acceso a APIs -7- de la red social -8-, mientras que el dispositivo receptor de informaciones -12- está diseñado para recibir y extraer datos de las informaciones publicadas en las cuentas de usuario seleccionadas a las que se ha accedido a través de los APIs -7-. Por otra parte, el dispositivo de almacenamiento -13- está diseñado para almacenar los datos publicados clasificados de cada cuenta de usuario monitorizada.

En la segunda realización del método conforme a la invención ilustrado en la figura 5, un mensaje se forma seleccionando primero una credencial disponible (paso A) en la base de datos de credenciales -10-. Las credenciales de acceso y la base de datos de credenciales de acceso tienen las características ya descritas anteriormente con

referencia a las figuras 3 y 4. Cuando la credencial disponible ha sido seleccionada, su clave de estado disponible (paso B) se cambia a la clave de estado ocupado.

En una base de datos de colas de mensajería -20- que comprende una pluralidad de identificaciones de cuentas de usuario, se selecciona (paso L) un número predeterminado de identificaciones de cuentas de usuario marcadas con clave de disponibilidad que se agrupa (paso C) a la credencial de acceso seleccionada para formar un grupo -2, 4- al que se asigna un código de consulta -3- cuyas características se han descrito anteriormente con referencia a la figura 1, quedando así formado el mensaje de consulta -1-. En la base de datos de colas de mensajería -20-, se cambia (paso M) la clave de disponibilidad de cada identificación de cuenta de usuario seleccionada a la clave de no-disponibilidad.

El mensaje de consulta que se transmite (paso D) a la API -7- de la red social -8- y, al igual que lo que ya se ha descrito con referencia a la figura 3, las informaciones proporcionadas por la API -7- en respuesta a cada mensaje de consulta -1- se reciben (paso H) y se almacenan (paso I) para su procesamiento.

Una vez enviado el mensaje de consulta -1- se detecta su fecha y hora de transmisión y se le asigna un código de completación (paso E) identificativo de la fecha y hora en la que el mensaje de consulta -1- ha sido transmitido. La transmisión del mensaje de consulta -1- también desencadena un reseteo de estado que comprende cambiar (paso G), en la base de datos de credenciales -10- la clave de estado ocupado asignada a la credencial de acceso contenida en cada mensaje de consulta -1- transmitido a la clave de estado disponible. El código de completación se asigna (paso F) como clave de último acceso a la credencial de acceso contenida en el mensaje de consulta transmitido.

La realización del sistema ilustrada en la figura 6 sirve para realizar la realización del método que muestra la figura 5 y comprende además de los elementos ya descritos con referencia a la figura 4, la base de datos de colas mensajería -20-, un dispositivo seleccionador de identificaciones disponibles -21- y un dispositivo cambiador de claves de disponibilidad -22-, así como un dispositivo asignador de códigos consulta -23-, y un dispositivo asignador de credenciales -24- integrados en el dispositivo formador de mensajes de consulta -15-.

El dispositivo seleccionador de identificaciones -21- disponibles está previsto para detectar y seleccionar, en la base de datos de colas de mensajería -20-, las identificaciones marcadas con una clave de disponibilidad que van a formar parte de los respectivos mensajes de consulta. El dispositivo cambiador de claves de disponibilidad -22- está previsto para, en la base de datos de colas de mensajería -20-, cambiar la clave de disponibilidad de cada identificación de cuenta de usuario seleccionada a la clave de no-disponibilidad.

El dispositivo asignador de códigos de consulta -23- está previsto para asignar los códigos de consulta a los mensajes de consulta mientras que el dispositivo asignador de credenciales -24- está previsto para asignar un número de identificaciones de cuentas de usuario seleccionadas a la credencial de acceso seleccionada para formar el mensaje de consulta.

REIVINDICACIONES

1. Un método de monitoreo y extracción de informaciones publicadas de usuarios registrados en redes sociales alojadas en servidores y nubes de datos de redes sociales que comprende transmitir mensajes de consulta que comprenden credenciales de acceso a un API de cada red social, e identificaciones de cuentas de usuario de usuarios registrados en las redes públicas, a las direcciones URL de las redes sociales para obtener datos de las informaciones publicadas por los usuarios monitorizados, recibir las informaciones publicadas y guardarlas en una base de datos de informaciones, **caracterizado** porque

los mensajes de consulta (1) se transmiten periódicamente a las API (7) de las redes sociales (8) de forma que cada mensaje de consulta (1) comprende al menos una identificación de una cuenta de usuario (4) registrada en la red social (8), asignada a una credencial de acceso (2) a la API (7) de una red social (8);

cada mensaje de consulta (1) se envía sólo cuando la credencial de acceso (2) comprende una clave de estado disponible (9a) y después de un tiempo transcurrido desde que la credencial de acceso (2) ha sido utilizada por última vez para la transmisión de un mensaje de consulta (1), calculado desde una fecha y hora de último acceso identificada por una clave de último acceso (2a);

cada mensaje de consulta (1) se marca con un código de completación (6) identificativo de una fecha y hora de completación de la transmisión del mensaje de consulta (1);

el código de completación (6) del mensaje de consulta (1) transmitido se asigna a la credencial de acceso (2) como la clave de último acceso (2a),

después de un periodo de tiempo predeterminado (t), calculado desde la fecha y hora de último acceso identificada por la clave de último acceso (2a), se vuelve a enviar un mensaje de consulta (1) con la credencial de acceso (2) a la que se ha asignado el código de último acceso (2a);

el número de identificaciones de cuentas de usuario (4) contenido en cada mensaje de consulta (1) es menor que un número máximo de peticiones de información efectuadas

con una credencial de acceso (2) admitido en un intervalo de tiempo determinado por la API (7) de la red social (8) sin entrar en un periodo de bloqueo temporal.

2. Método, según la reivindicación 1, caracterizado porque el periodo de tiempo predeterminado (t) es mayor que un periodo de bloqueo temporal durante el que la API (7) a la que se transmite el mensaje de consulta (1) rechaza por defecto nuevas peticiones de información efectuadas con una misma credencial de acceso (2).

3. Método, según la reivindicación 1 o 2, caracterizado porque comprende

una etapa de selección (A) que comprende seleccionar credenciales de acceso (2) disponibles en una base de datos de credenciales (10) en la que cada credencial de acceso (2) está asignada a la clave de último acceso (2a) y a la clave de estado (9), siendo la clave de estado (9) una clave de estado disponible (9a) o una clave de estado ocupado (9b), donde cada credencial de acceso (2) disponible comprende una clave de estado disponible (9a) y una clave de último acceso (2a) identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado (t),

una etapa de cambio de estado (B) que comprende cambiar la clave de estado disponible (9a) de cada una de las credenciales de acceso (2) seleccionadas a la clave de estado ocupado (9b);

una etapa de formación de mensajes (C) que comprende formar mensajes de consulta (1) seleccionando identificaciones de cuentas de usuario (4) disponibles en una cola de mensajería (5) que comprende una pluralidad de identificaciones de cuentas de usuario (4), y agrupando al menos una identificación de cuenta de usuario (4) a una de las credenciales de acceso (2) disponibles seleccionadas, de tal manera que los mensajes de consulta (1) comprenden identificaciones de cuenta de usuario (4) diferentes,

una etapa de transmisión (D) que comprende transmitir los mensajes de consulta (1) y marcar (E) el mensaje de consulta (1) transmitido con un código de completación (6) identificativo de la fecha y hora en la que el mensaje de consulta (1) ha sido transmitido;

una etapa de reseteo de estado (F) que comprende cambiar la clave de estado ocupado

(9a) asignada a la credencial de acceso (2) contenida en cada mensaje de consulta (1) transmitido a una clave de estado disponible (9a);

una etapa de asignación (G) que comprende asignar el código de completación (6) como clave de último acceso (2a) a la credencial de acceso (2) contenida en el mensaje de consulta (1) transmitido,

iterar la etapa de selección (A) para iniciar sucesivamente la formación de nuevos mensajes de consulta (1).

4. Método, según la reivindicación 1, 2 ó 3, caracterizado porque la etapa de formación de mensajes de consulta comprende

seleccionar, de una cola de mensajería (5) contenida en una base de datos de colas de mensajería (20) que comprende una pluralidad de identificaciones de cuentas de usuario (4) monitorizadas y en la que cada identificación de usuario (4) está asignada a una clave de disponibilidad o a una clave de no-disponibilidad (4a), las identificaciones de cuentas de usuario (4) disponibles que comprenden la clave de disponibilidad para obtener identificaciones de cuentas de usuario (4) disponibles seleccionadas;

cambiar, en la base de datos de colas de mensajería (20), la clave de disponibilidad de cada identificación de cuenta de usuario (4) disponible seleccionada a la clave de no-disponibilidad (4a).

5. Método, según la reivindicación 4, caracterizado porque comprende cambiar, en la base de datos de colas de mensajería (20), la clave de no-disponibilidad (4a) de cada identificación de cuenta de usuario (4) contenida en un mensaje de consulta (1) transmitido a la clave de disponibilidad cuando la identificación de cuenta de usuario (4) ha sido transmitida en un mensaje de consulta (1) transmitido.

6. Método, según la reivindicación 1, 2, 3 ó 4 caracterizado porque a cada mensaje de consulta (1) se le asigna un código de consulta (3) seleccionado entre códigos de fecha y hora, códigos de número y combinaciones de los mismos, definiendo cada código de fecha y hora una fecha y hora a partir de la que se piden informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario (4) comprendida en el

mensaje de consulta (1), y cada código de número define un número máximo de últimas informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario (4) comprendida en el mensaje de consulta (1).

7. Sistema de monitoreo y extracción de informaciones públicas de usuarios registrados de redes sociales, alojadas en servidores y nubes de datos de redes sociales que comprende

un dispositivo transmisor (11) para transmitir mensajes de consulta (1) a cuentas de usuario seleccionadas empleando credenciales de acceso (2) a APIs (7) de cada red social (8),

un dispositivo receptor de informaciones (12) para recibir y extraer datos de las informaciones publicadas en las cuentas de usuario seleccionadas a las que se ha accedido a través de cada API (7) mediante la transmisión de un mensaje de consulta (1),

un dispositivo de almacenamiento (13) para almacenar los datos publicados clasificados de cuenta de usuario monitorizada,

caracterizado porque comprende

un dispositivo seleccionador de credenciales (21), diseñado para seleccionar credenciales de acceso (2) disponibles contenidas en una base de datos de credenciales (10) en la que a cada credencial de acceso (2) le están asignadas a una clave de último acceso (2a) y una clave de estado (9), siendo la clave de último acceso (2a) identificativa de una fecha y hora de último acceso en la que la credencial de acceso (2) ha sido utilizada por última vez en un mensaje de consulta (1) transmitido, y siendo la clave de estado (9) una clave de estado disponible (9a) o una clave de estado ocupado (9b), donde cada credencial de acceso (2) disponible comprende una clave de estado disponible (9a) y una clave de último acceso (2a) identificativa de un periodo de tiempo transcurrido con una fecha y hora inicial anterior a la fecha y hora inicial de un periodo de tiempo transcurrido predeterminado (t),

un dispositivo formador de mensajes de consulta (15) para formar mensajes de consulta (1) dirigidas a cada API (7), comprendiendo cada mensaje de consulta (1) al menos una

identificación de cuenta de usuario (4) registrada en la red social, asignada a una credencial de acceso (2) a la API (7) de dicha red social (8), siendo el número de identificaciones de cuentas de usuario (4) en cada mensaje de consulta (1) menor que un número máximo de peticiones de información efectuadas con una misma credencial de acceso (2) admitido en un intervalo de tiempo determinado por la API (7) sin entrar en un periodo de bloqueo temporal,

un dispositivo detector (16) diseñado para detectar la fecha y hora en la que un mensaje de consulta (1) ha sido transmitido y para marcar cada mensaje de consulta (1) transmitido con un código de completación (6) identificativo de la fecha y hora de completación de la transmisión del mensaje de consulta (1),

un dispositivo asignador (17) diseñado para asignar el código de completación (6) como fecha y hora de último acceso a la credencial de acceso (2) contenida en cada mensaje de consulta (1) transmitido;

un dispositivo cambiador de claves de estado (22), diseñado para cambiar la clave de estado disponible (9a) de cada una de las credenciales de acceso (2) seleccionadas a la clave de estado ocupado (9b), y para cambiar la clave de estado ocupado (9b) asignada a la credencial de acceso (2) contenida en cada mensaje de consulta (1) transmitido en una clave de estado disponible (9a),

un dispositivo iterador (19) diseñado para ordenar al dispositivo seleccionador la selección de nuevas credenciales de acceso (2) disponibles contenidas en la base de credenciales (10) para iniciar sucesivamente la formación de nuevos mensajes de consulta (1).

8. Sistema, según la reivindicación 7, caracterizado porque la base de datos de credenciales (10) está comprendida en el sistema, y porque el sistema comprende además

una base de datos de colas de mensajería (20) que contiene colas de mensajería (5) que comprende identificaciones de cuentas de usuario (4), y en la que cada identificación de cuenta de usuario (4) está asignada a una clave de disponibilidad o a una clave de no-disponibilidad (4a);

un dispositivo seleccionador de identificaciones (21) diseñado para seleccionar identificaciones de cuentas de usuario (4) disponibles de entre las identificaciones de cuentas de usuario disponibles contenidas en cada cola de mensajería (5);

un dispositivo asignador de credenciales diseñada para asignar un número de identificaciones de cuentas de usuario (4) disponibles a una credencial de acceso (2) disponible seleccionada por el dispositivo seleccionador de credenciales (14).

9. Método, según la reivindicación 8, caracterizado porque comprende un dispositivo asignador de códigos de consulta (23) diseñado para asignar un código de consulta (3) a cada mensaje de consulta (1), seleccionado entre códigos de fecha y hora, códigos de número y combinaciones de los mismos, en los que cada código de fecha y hora define una fecha y hora a partir de la que se piden informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario (4) comprendida en el mensaje de consulta (1), y cada código de número define un número máximo de últimas informaciones publicadas en las cuentas identificadas en cada identificación de cuenta de usuario (4) comprendida en el mensaje de consulta (1).

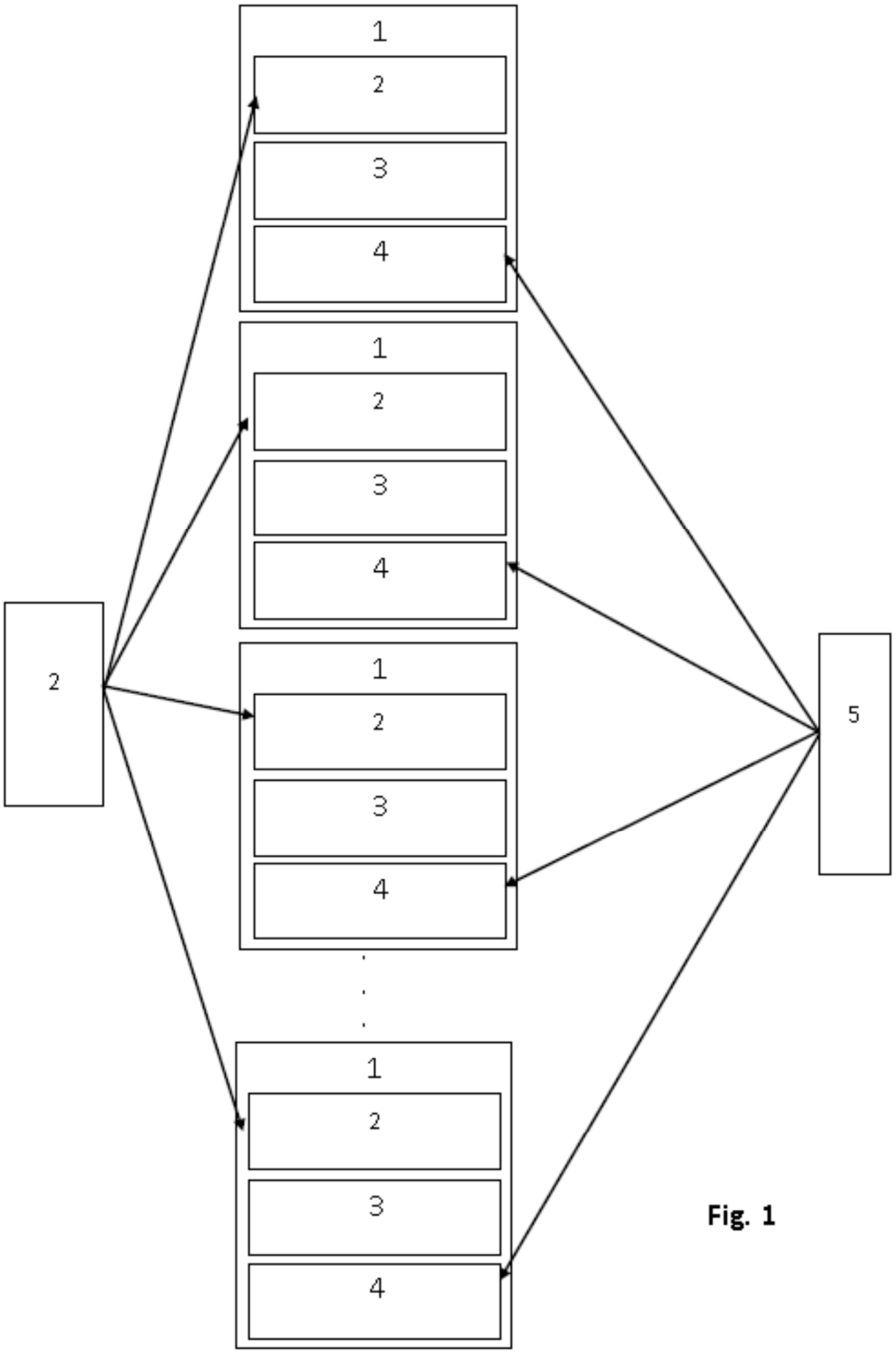

Fig. 1

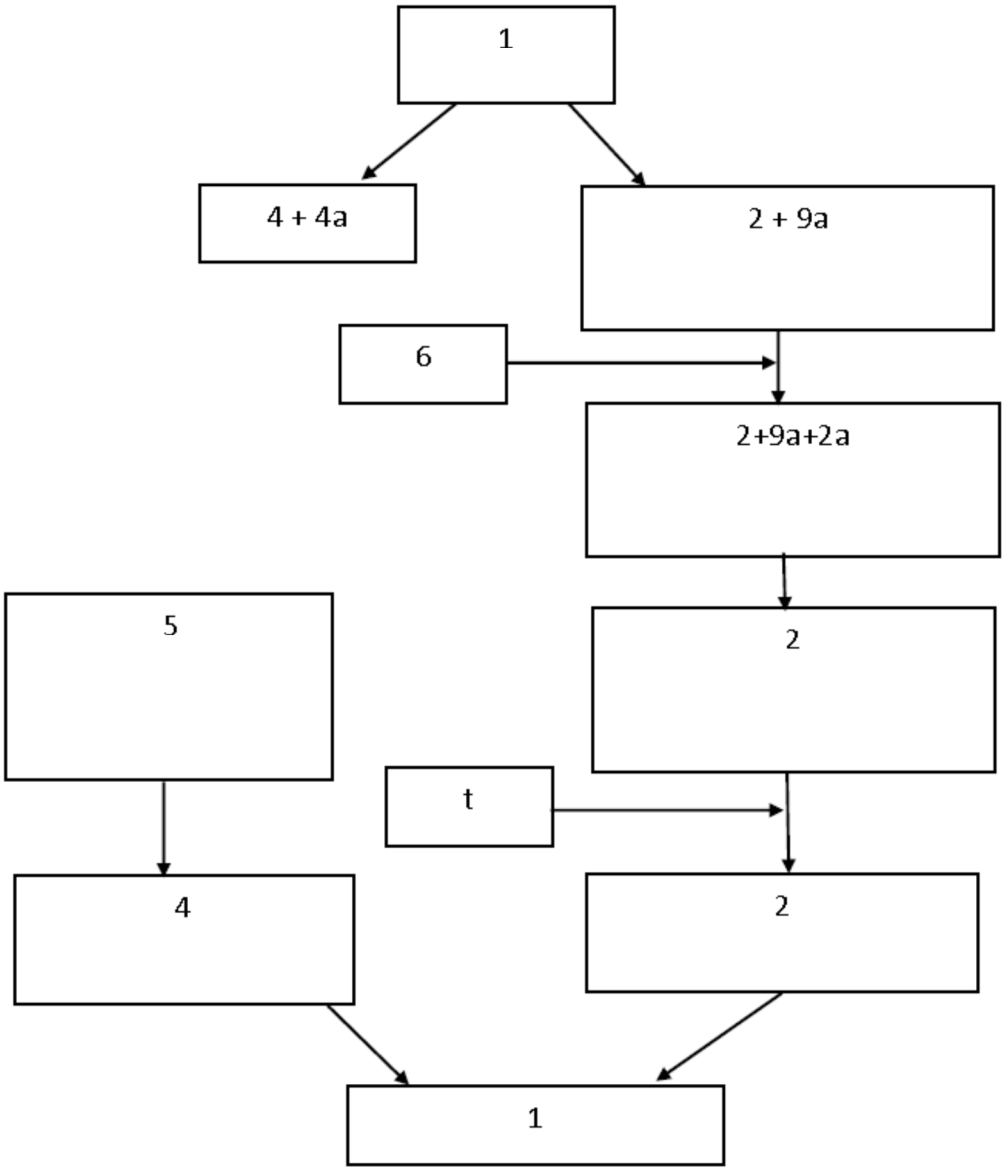

Fig. 2

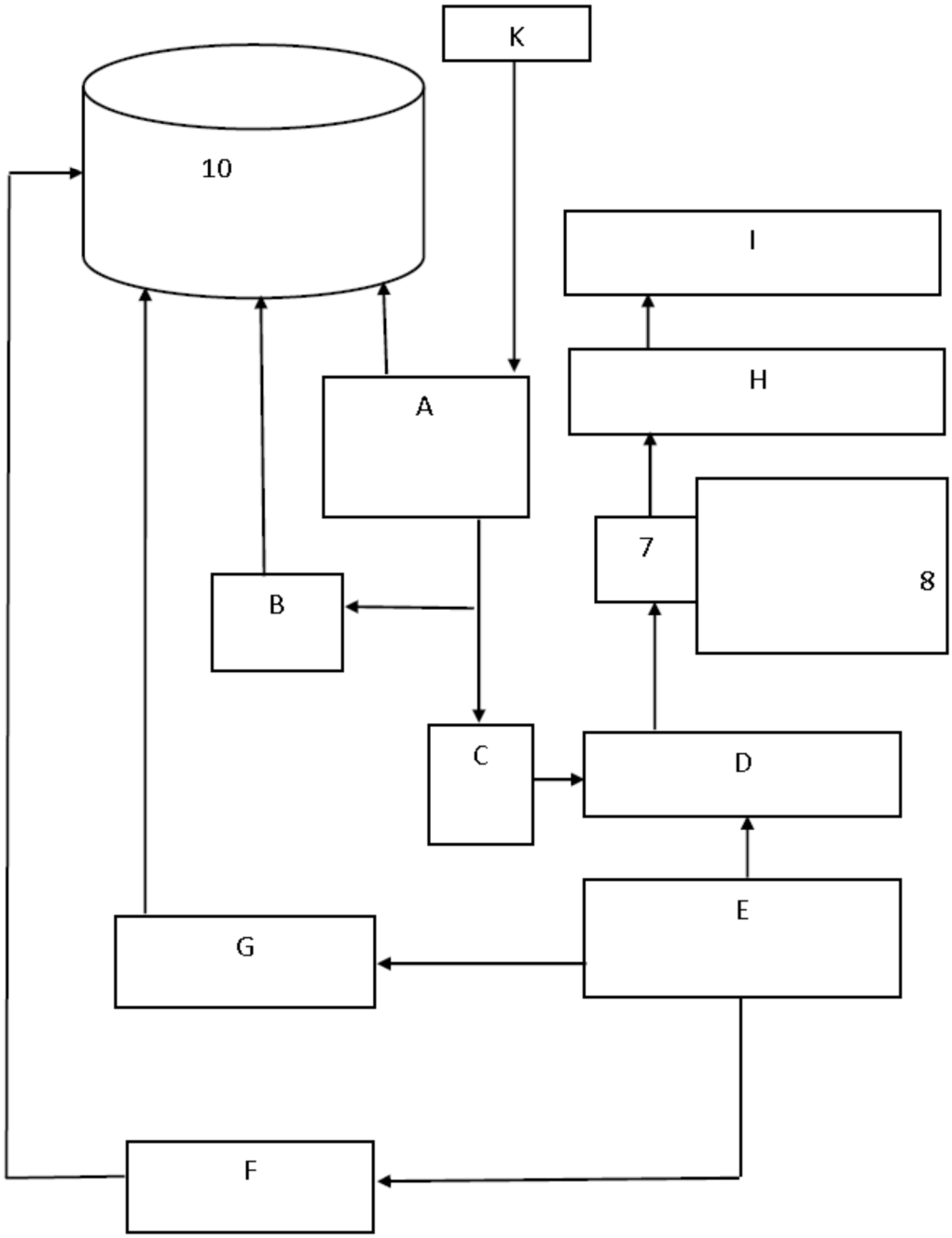

Fig. 3

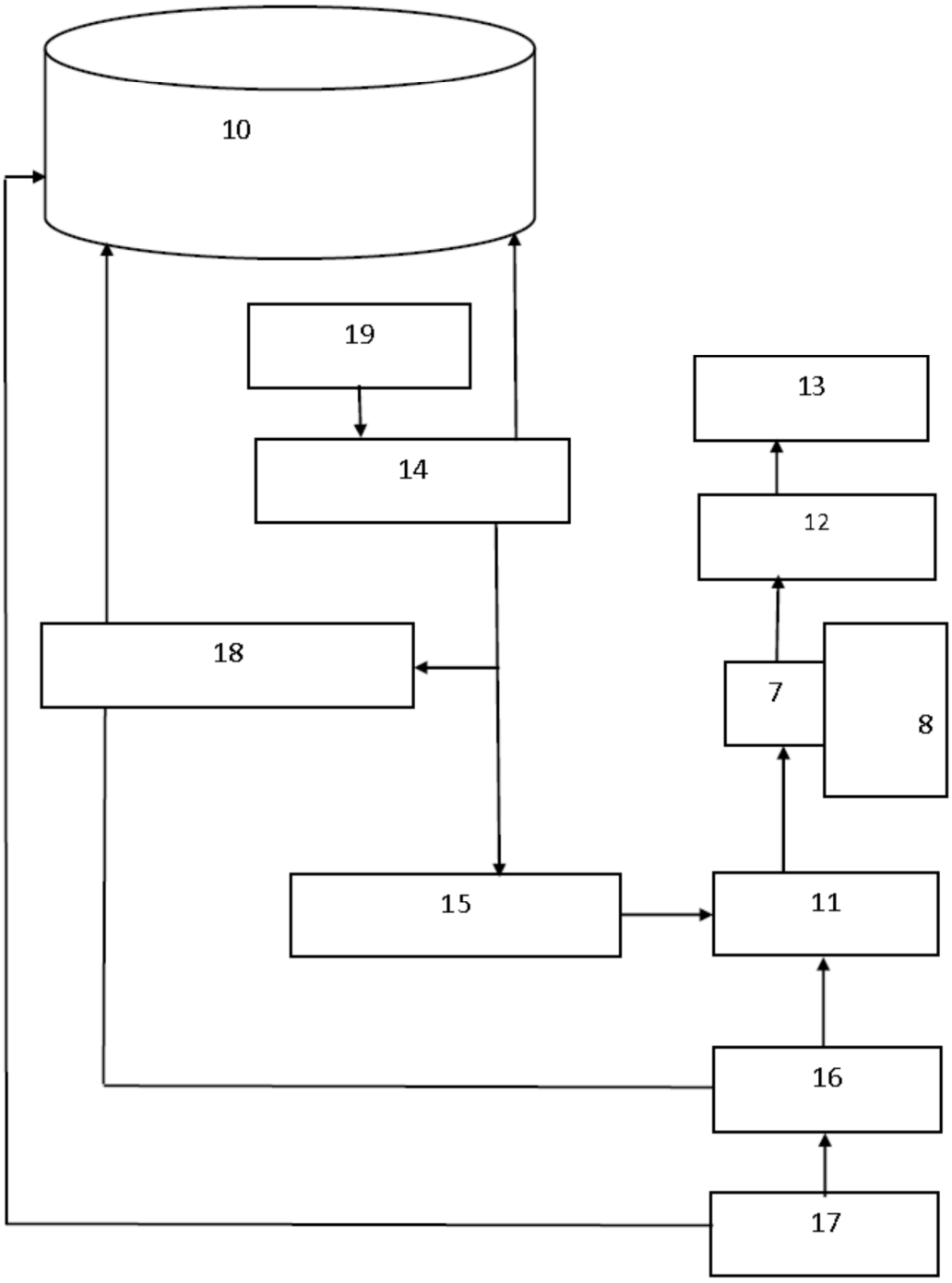

Fig. 4

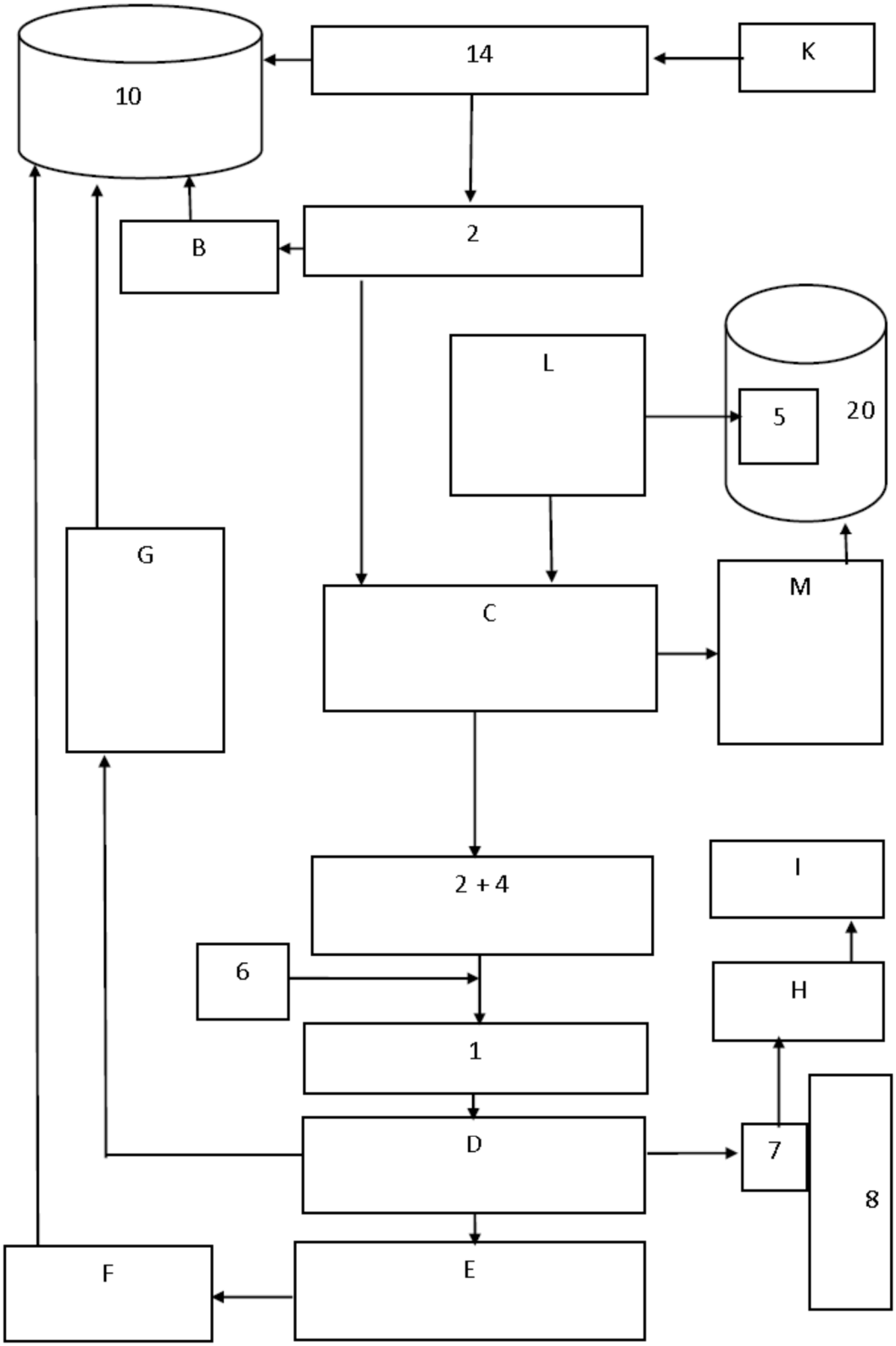

Fig. 5

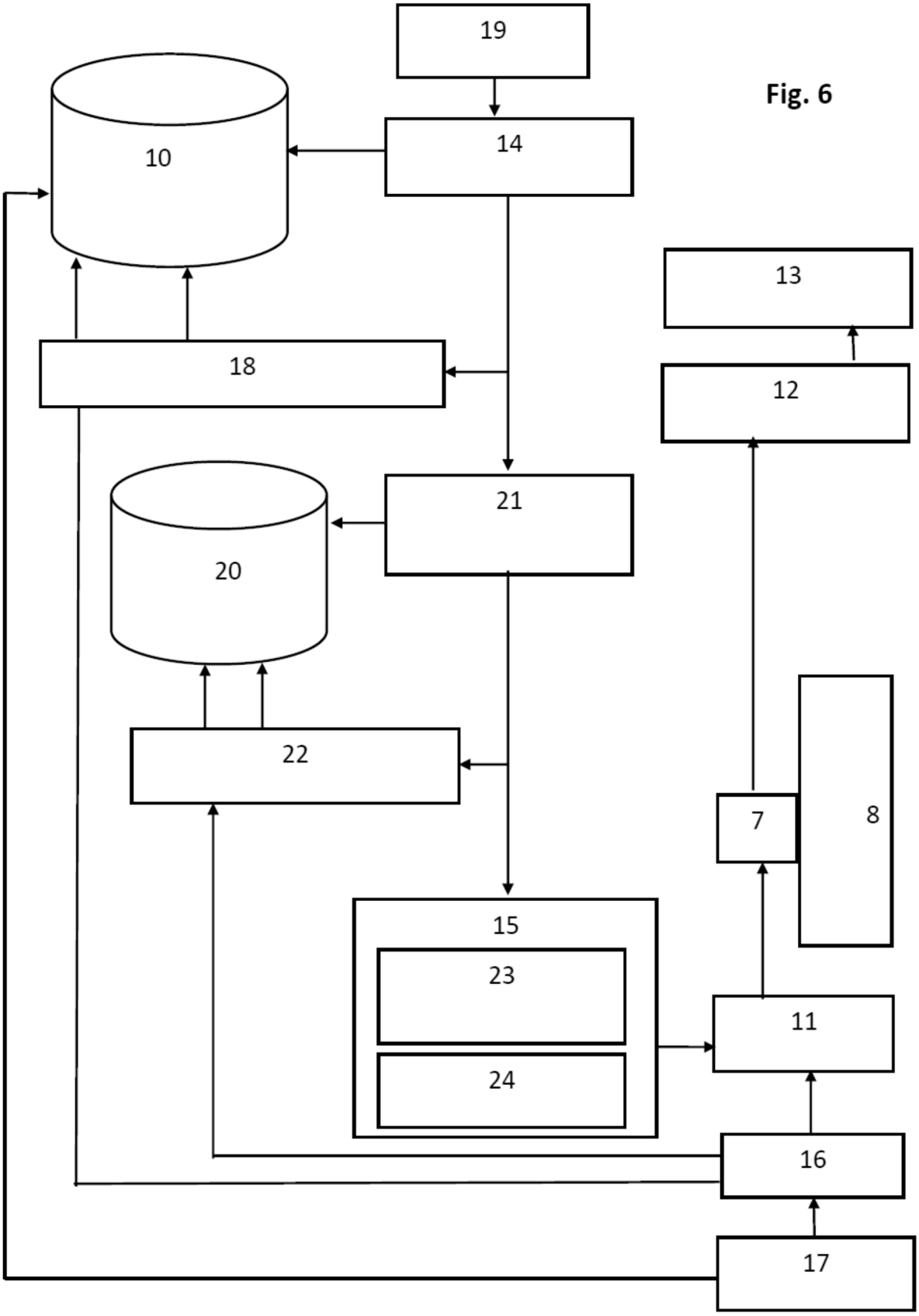

Fig. 6

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201630267

(22) Fecha de presentación de la solicitud: 07.03.2016

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06F21/62*** (2013.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	Jorge Alberto Jiménez Sandoval y Francisco Jiménez Hernández: "APIs de Redes Sociales"; Publicado en : Revista SG #45, núm. Septiembre 2014; Sección: APIs; URL:// https://sg.com.mx/revista/45/apis-redes-sociales#.WIslSGcVCUk	1-9
A	US 2013254401 A1 (MARSHALL JOHN et al.) 26/09/2013, resumen; figuras 1, 14; párrafos [42 - 45, 52, 57 - 59];	1-9
A	US 2011113096 A1 (LONG KEVIN et al.) 12/05/2011, resumen; figura 4.	1-9

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
27.01.2017	**B. Pérez García**	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, G06Q, H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, INSPEC

Fecha de Realización de la Opinión Escrita: 27.01.2017

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-9	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	1-9	**SI**
	Reivindicaciones		**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	Jorge Alberto Jiménez Sandoval y Francisco Jiménez Hernández: "APIs de Redes Sociales";	30.09.2014
D02	US 2013254401 A1 (MARSHALL JOHN et al.)	26.09.2013
D03	US 2011113096 A1 (LONG KEVIN et al.)	12.05.2011

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

No se han encontrado documentos en el estado de la técnica anterior que incluyan todas las características del objeto de la invención.

D01 describe cómo funcionan los APIs de las redes sociales. Estos APIs utilizan el protocolo oAuth para autenticarse y que terceras partes puedan acceder a información de un usuario sin tener que darle su usuario o contraseña. Este documento es interesante porque expresa restricciones en los límites de peticiones de información en Twitter, tal que se limita por usuario y por tiempo. Sin embargo no anticipa al objeto de la invención porque no detalla que realice una monitorización (envío de mensajes) de forma periódica, ni crea las credenciales de acceso con el token + estado (disponible/ocupado) + marca de tiempo (hora y fecha del último acceso). La forma de crear estas credenciales dota de mayor seguridad al sistema de acceso y al mismo tiempo, con los límites temporales, evita que se produzca un bloqueo temporal de la red.

D02 describe un sistema y método para controlar la distribución de recursos y su acceso en una red. El dispositivo cliente *(120)* solicita el acceso a recursos *(165)* mediante una autenticación con credenciales de usuario *(132)* y se le permite el acceso a un recurso si se cumplen unas reglas de distribución *(171).* Estas reglas pueden incluir requisitos HW, SW, de mantenimiento, de configuración… Los requisitos de mantenimiento pueden ser, entre otros, la fecha de la última comunicación entre el cliente *(120)* y el servidor *(150)*, o la fecha de la última conexión del cliente (*120)* o similar. También puede incluirse en estas reglas de distribución unas reglas de tiempo *(191)* (ver párrafos 42-45). Por tanto, D02 permite el acceso a recursos, a través de una red, en función de una serie de reglas entre las que se encuentra registrar la fecha de la última comunicación cliente-servidor.
Este documento presenta ciertas semejanzas con la solicitud pero no realiza una monitorización de una red social y tampoco envía mensajes de forma periódica.

D03 consiste en un sistema de monitorización de redes sociales según parámetros o intereses del usuario. Sin embargo, no establece en qué consisten los mensajes ni las credenciales de usuario enviadas en los mismos.

En resumen, se considera que la solicitud presentada cumple los requisitos de novedad y actividad inventiva establecidos en los Arts. 6 y 8 de la Ley Española de Patentes.