(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 614 640**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.09.2007 PCT/EP2007/060059**

(87) Fecha y número de publicación internacional: **26.03.2009 WO09036810**

(96) Fecha de presentación y número de la solicitud europea: **21.09.2007 E 07820470 (8)**

(97) Fecha y número de publicación de la concesión europea: **09.11.2016 EP 2203868**

(54) Título: **Sistemas y métodos para búsquedas de coincidencia parcial de datos retenidos cifrados**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.06.2017

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

LA ROCCA, MAURIZIO y
IMBIMBO, AMEDEO

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistemas y métodos para búsquedas de coincidencia parcial de datos retenidos cifrados

Campo técnico

La presente invención versa en general sobre la recuperación de datos retenidos de una base de datos. Más específicamente, la presente invención versa sobre la recuperación de datos cifrados usando criterios de coincidencia parcial de búsqueda.

Técnica antecedente

El cifrado es el procedimiento de transformación de datos para hacerlos ilegibles para cualquiera que no posea conocimiento especial. El conocimiento especial es denominado a menudo llave de apertura de los datos protegidos. El cifrado se usa para restringir el acceso a datos únicamente a usuarios autorizados en diversas bases de datos civiles y del gobierno y en sistemas de redes tales como, por ejemplo, redes telefónicas móviles, cajeros automáticos y comercio electrónico por Internet. También se usa cifrado en la gestión de derechos digitales para restringir el uso de material protegido por derechos de autor, así como en soportes lógicos, para proteger contra la piratería de soporte lógico y la ingeniería inversa.

En muchos países, se requiere de las empresas explotadoras y de los proveedores de servicios de Internet que retengan el tráfico de datos generados desde redes públicas de telecomunicaciones, incluyendo servicios de Internet. Los organismos policiales autorizados pueden acceder legalmente a estos datos retenidos en proveedores de servicios por diversas razones, tales como la detección, la investigación y el enjuiciamiento de una amplia gama de delitos o tramas criminales. Debido a las diversas leyes nacionales, así como por razones de seguridad y privacidad, el acceso a estos datos retenidos debería estar restringido a entidades autorizadas, tales como los organismos policiales. Para mantener la seguridad de los datos retenidos, estos son almacenados de forma cifrada.

Cuando una entidad autorizada buscada datos retenidos específicos, relacionados, por ejemplo, con una única llamada telefónica realizada por un solo individuo, debe ser localizada en una base de datos que puede ser sumamente grande. Cuando estos datos retenidos cifrados son almacenados en sistemas de ficheros, bases de datos u otras formas de almacenamiento, no es posible llevar a cabo una búsqueda de estos datos basándose en criterios de coincidencia parcial. En consecuencia, las consultas de búsqueda deben incluir una coincidencia exacta del término de la búsqueda. Esto da como resultado una búsqueda más lenta y menos eficiente. Además, las claves de cifrado son susceptibles a ataques de entidades no autorizadas, tales como piratas informáticos. En caso de ataque, debe cambiarse la clave de cifrado. Esto requiere el descifrado de toda la base de datos con la vieja clave, seguido por un nuevo cifrado de toda la base de datos con una nueva clave. Este también es un procedimiento que lleva tiempo y es costoso e ineficiente.

El documento US5787428 da a conocer un método de recuperación de datos de una base de datos. La base de datos comprende una tabla de empleo, una tabla de seguridad y una tabla de usuario. Las entradas entre la tabla de empleo y la tabla de usuario están ligadas usando diferentes identificadores almacenados en la tabla de seguridad.

Exposición de la Invención

Teniendo en cuenta lo anterior, resulta evidente que existe una necesidad directa de soluciones que permitan la recogida, el almacenamiento, la retención y la entrega de datos retenidos generados por servicios de telecomunicaciones y de Internet en redes públicas fijas y móviles mientras se mantiene la seguridad de los datos retenidos. Además, es deseable permitir una búsqueda segura en bases de datos implementando criterios de búsqueda de coincidencia parcial y recuperar únicamente un subconjunto de los datos retenidos o acceder al mismo. Esto mejora la velocidad y la eficiencia del traspaso de datos a las entidades autorizadas, y disminuye el coste.

Así, el objetivo de la presente invención es superar los problemas mencionados anteriormente mediante un método de recuperación de datos diana retenidos de una base de datos según la reivindicación 1.

El objeto anteriormente mencionado y otros también se logran mediante un sistema de recuperación de datos diana retenidos de una base de datos según la reivindicación 7.

Estos objetivos y objetos se logran mediante los métodos y los sistemas según la reivindicación independiente 1 y cualesquiera otras reivindicaciones independientes. en las restantes reivindicaciones dependientes pueden encontrarse detalles adicionales.

Otros aspectos y ventajas de los sistemas y los métodos dados a conocer en la presente memoria resultarán evidentes a partir de la siguiente descripción detallada, tomada junto con los dibujos adjuntos, que ilustran los principios de la invención únicamente a título de ejemplo.

Breve descripción de los dibujos

Los objetos, las características y las ventajas anteriores y otros de los sistemas y los métodos dados a conocer en el presente documento se entenderán más plenamente a partir de la siguiente descripción de diversas realizaciones cuando sea leída junto con los dibujos adjuntos, en los que:

la Fig. 1 es una tabla que representa datos retenidos cifrados;
la Fig. 2 es una tabla que representa datos retenidos cifrados;
la Fig. 3 es un diagrama de flujo que representa un método de recuperación de datos retenidos según una realización de la invención;
la Fig. 4 es un diagrama de bloques que representa un sistema de recuperación de datos retenidos según una realización de la invención;
la Fig. 5 es una tabla que representa una primera tabla que incluye una columna en claro y una columna cifrada de índices según una realización de la invención;
la Fig. 6 es una tabla que representa una segunda tabla que incluye una columna de índices en claro y una columna de datos retenidos según una realización de la invención; y
la Fig. 7 representa dos tablas en las que la primera tabla incluye una columna en claro y una columna cifrada de índices, y en las que la segunda tabla incluye una columna de índices en claro y una columna de datos retenidos en texto legible según una realización de la invención.

Maneras de realización de la Invención

Según se muestra en los dibujos con fines de ilustración, la invención puede ser implementada en sistemas y métodos de recuperación de datos diana retenidos de una base de datos. Las realizaciones de los sistemas y los métodos dados a conocer en la presente memoria permiten el uso de algoritmos de cifrado que garantizan la confidencialidad de datos sensibles retenidos, así como el uso de criterios de coincidencia parcial de búsqueda cuando se recupera, se accede o se transmiten datos diana retenidos a una entidad autorizada.

Generalmente, la coincidencia parcial en búsquedas permite la recuperación de datos almacenados o retenidos en función de una búsqueda de esos datos en función de una cadena de búsqueda que incluye caracteres variables, a veces denominados comodines. Pueden usarse muchos indicadores para este carácter variables, tal como, por ejemplo, un asterisco “*”. Por ejemplo, se pueden buscar en una base de datos datos retenidos asociados con un usuario llamado “John”. Una búsqueda exacta incluiría criterios de búsqueda con el nombre “John”. Sin embargo, en situaciones en las que el que efectúa la búsqueda conoce, por ejemplo, solo el primer carácter del nombre que ha de buscarse, puede no ser posible una búsqueda exacta. En este ejemplo, un buscador podría usar criterios de coincidencia parcial de búsqueda que incluyan un carácter variable, tal como “J*”. Generalmente, esto produce como resultado una búsqueda en una base de datos de todos los nombres de usuario que comiencen con la letra “J” o la incluyan, tales como, por ejemplo, James, Jack, Jessica. Sin embargo, los datos se almacenan en forma cifrada en los sistemas existentes, no pueden usarse criterios de coincidencia parcial de búsqueda.

En una breve visión general, la Figura 1 es una tabla 100 que representa datos retenidos cifrados en un sistema existente. La tabla 100 incluye una columna cifrada 105 y una columna 110 de datos no cifrados. Generalmente, cuando se almacenan datos en sistemas de ficheros, bases de datos u otros formados de almacenamiento, no puede usarse una coincidencia parcial en búsquedas para llevar a cabo una búsqueda de datos que están almacenados en una base de datos. En jerga típica de criptografía, $y = f(x)$ es la función que devuelve el cifrado de x; y $x = f^{1}(y)$ es la función que devuelve el descifrado de y. En la tabla 100, la columna cifrada 105 almacena f(x), que es la función de devuelve el cifrado de “x” en las casillas 115, 120, 125 y 130. El número de casillas que aparecen en la columna cifrada 105 está limitado a cuatro únicamente con fines de ilustración, y es posible un número cualquiera de casillas. Dado que la tabla 100 almacena los nombres 115 - 130 de usuario de forma cifrada, no es posible buscar “J*” para encontrar los datos asociados con la casilla 115 (“John”) o la casilla 125 (“Jack”), porque f(J*) no coincide con f(John) ni con f(Jack), incluyendo generalmente una “casilla”, tal como se usa en la presente memoria, una fila o datos de una fila de una columna de cualquier tabla descrita en la presente memoria. Dado que la columna cifrada 105 almacena datos de nombre de usuario (o cualesquiera otros) únicamente de forma cifrada, indicada por f(x), para mantener la confidencialidad prevista por el cifrado, así como para satisfacer diversos requisitos legales y de la industria, una búsqueda parcial que implemente comodines no llega a producir una coincidencia cuando se aplica a la tabla 100, porque el cifrado de la búsqueda parcial (por ejemplo, f(J*)) diferirá de los nombres de usuario cifrados (por ejemplo, f(John)). En consecuencia, una búsqueda en la tabla 100 de datos retenidos, tal como el contenido de llamadas o los datos administrativos contenidos en la columna 110 de datos no cifrados en cualquiera de las casillas 135 - 150 y asociados con cualquiera de las casillas 115 - 130 no puede incluir comodines.

De modo similar, la Figura 2 también es una tabla 200 que representa datos retenidos cifrados en un sistema existente. La tabla 200 incluye una columna 205 de datos de llamada cifrados y una columna 210 de datos no cifrados. En este ejemplo de un sistema existente, en vez de nombres de usuario tales como los almacenados en la columna cifrada 105, la tabla 200 incluye datos de llamada, tales como un número de red digital de servicios integrados de estaciones móviles (MSISDN), como indicadores de identificación de llamadas que identifican a usuarios. Pueden usarse otros números de identificación de usuarios, tales como los números de identidad internacional de abonado móvil (IMSI) o de identidad internacional de equipo móvil (IMEI). Dado que generalmente se considera que estos números, indicados en las casillas 215 - 230 de la columna cifrada 205 son datos sensibles y

confidenciales, son retenidos de forma cifrada. Como en la tabla 100, una búsqueda parcial usando un comodín, cuando sea transformada por el cifrado, no coincidirá con ninguno de estos números de identidad del usuario y la búsqueda fallará en su empeño por recuperar de la columna 210 de datos datos no cifrados en texto legible. En el ejemplo mostrado en la tabla 200, la columna 210 de datos almacena datos asociados con las llamadas hechas por los usuarios en una red telefónica o de otro tipo, tales como la hora de inicio de una transmisión de datos, tal como una llamada telefónica. Estos datos son almacenados en las casillas 235 - 250.

En una breve visión general, la Figura 3 es un diagrama de flujo que representa un método 300 de recuperación de datos retenidos de una base de datos según una realización de la invención. El método 300 incluye normalmente recibir una solicitud de acceso a datos diana retenidos asociados con un usuario diana, incluyendo la solicitud criterios de coincidencia parcial de búsqueda asociados con el usuario diana (ETAPA 305). La etapa de recepción (ETAPA 305) puede incluir la recepción de un mandamiento de autorización de recuperación de datos que estén retenidos en una base de datos. Este mandamiento puede ser emitido por un tribunal o una autoridad competente. La solicitud puede incluir una solicitud de acceder a todos los datos, tales como comunicaciones electrónicas que tuvieran lugar en una red y que estén almacenadas en una base de datos, así como datos administrativos (hora, fecha, duración de la llamada, etc.) asociados con la comunicación electrónica. La solicitud puede ser recibida electrónica, verbal o manualmente. La solicitud también puede tener la forma de una comunicación electrónica recibida por un tercero. La etapa de recepción (ETAPA 305) puede incluir la recepción por un procesador, un receptor o una función de administración de un mandamiento procedente de un organismo policial con identificación de usuarios, servicios u otras dianas cuyos datos asociados hayan de recuperarse. La etapa de recepción (ETAPA 305) normalmente incluye la recepción de cualquier señal o indicación que autorice, ordene o solicite la recuperación de datos retenidos que estén almacenados en una base de datos y estén relacionados con una comunicación electrónica, tal como un teléfono que se haga, se hiciera o se hará en una red en cualquier formato, tal como una red telefónica o Internet. Normalmente, la recepción de una solicitud de acceso a datos diana retenidos (ETAPA 305) puede incluir la recepción de una solicitud de acceso a todos los datos retenidos destinados a un usuario diana o procedentes del mismo. La solicitud puede ser para un periodo temporal abierto, o para un periodo de tiempo dado, tal como una hora, un día o un mes particular. La solicitud también puede ordenar la recuperación de datos relacionados a diversos servicios especificados, tales como voz, vídeo o similares.

Normalmente, el método 300 también incluye la etapa de acceso a una primera tabla (ETAPA 310). Generalmente, esto incluye el acceso a una primera tabla (ETAPA 310) que incluye tanto una columna en claro que tiene datos de identificación no cifrados asociados con varios usuarios, como una columna cifrada de índices que tiene un índice cifrado asociado con cada uno de los varios usuarios. El acceso a la primera tabla (ETAPA 310) incluye generalmente uno o más procesadores que dirigen operaciones lógicas suficientes para interactuar con una base de datos en la que la primera tabla puede estar almacenada. El acceso a la primera tabla (ETAPA 310) incluye generalmente la interconexión con cualquier dato —y su lectura o manipulación— retenido en la primera tabla, tal como, por ejemplo, el acceso a la primera tabla para buscar cualquier dato contenido en la misma en busca de coincidencias en una consulta de búsqueda que incluya criterios de coincidencia parcial de búsqueda, tales como caracteres comodín.

Generalmente, en respuesta a una solicitud de búsqueda que incluya criterios de coincidencia parcial de búsqueda, el método 300 selecciona de la primera tabla al menos un índice cifrado que coincide con los criterios de coincidencia parcial de búsqueda (ETAPA 315). En una realización ilustrativa, se recibe una consulta de búsqueda (ETAPA 305) que incluye un comodín u otros criterios de coincidencia parcial de búsqueda. Normalmente se accede a la primera tabla (ETAPA 310). Generalmente, la primera tabla contiene una columna de texto en claro no cifrado y una columna cifrada de índices. La consulta de búsqueda que incluye cualquier criterio de coincidencia parcial de búsqueda se ejecuta, por ejemplo, en la columna de texto en claro no cifrado y puede devolver como resultado datos incluidos en filas de una columna cifrada de índices que están asociadas con filas de una columna no cifrada de texto legible que coinciden con la consulta de búsqueda parcial. Esta operación puede ser implementada por un procesador o un dispositivo lógico similar que esté adaptado para determinar si la consulta de búsqueda basada en comodines coincide con entradas en la columna de texto en claro de la primera tabla, y si existen datos en la columna cifrada de índices de la primera tabla que correspondan a las entradas coincidentes en la columna de texto en claro.

Normalmente, el método 300 también accede a una segunda tabla (ETAPA 320). El acceso a la segunda tabla (ETAPA 320) incluye generalmente el acceso a una segunda tabla que incluye tanto una columna índice de texto legible con un índice no cifrado asociado con cada uno de varios usuarios, como una columna de datos retenidos con varios datos retenidos que incluyen datos diana retenidos que son normalmente el objeto de la solicitud recibida (ETAPA 310). El acceso a la segunda tabla (ETAPA 320) incluye generalmente uno o más procesadores que dirigen operaciones lógicas suficientes para interactuar con una base de datos en la que la segunda tabla puede estar almacenada. El acceso a la segunda tabla (ETAPA 320) incluye generalmente la interconexión con cualquier dato —y su lectura o manipulación— retenido en la segunda tabla, tal como, por ejemplo, el acceso a la segunda tabla para determinar la existencia de índices no cifrados de texto legible que correspondan a los índices cifrados de la primera tabla, correspondiente los índices cifrados a la columna no cifrada de texto legible de la primera tabla que fue objeto de la búsqueda que incluía criterios de coincidencia parcial de búsqueda.

Generalmente, el método 300 también incluye la etapa de seleccionar de la segunda tabla al menos un índice no cifrado (ETAPA 325), tal como, por ejemplo, un índice de texto legible, que está asociado con al menos un índice cifrado seleccionado de la primera tabla. Normalmente, el al menos un índice no cifrado que está seleccionado (ETAPA 325) incluye una casilla de datos de una columna índice no cifrada de texto legible de la segunda tabla. Generalmente, la o las casillas seleccionadas del índice no cifrado son el homólogo no cifrado de las casillas del índice cifrado incluidas en la columna cifrada de índices de la primera tabla. Continuando esta realización ilustrativa, estas mismas casillas de índice cifrado son las homólogas de las casillas de la columna de texto en claro no cifrado de la primera tabla que coinciden con la búsqueda de comodines que se recibió (ETAPA 305) como parte de la solicitud de acceso a los datos retenidos de un usuario diana.

Generalmente, el método 300 continúa identificando (ETAPA 330) y recuperando (ETAPA 335), en la columna de datos retenidos de la segunda tabla, los datos diana retenidos asociados con el al menos un índice no cifrado seleccionado (ETAPA 325). La etapa (330) de identificación incluye normalmente un procesador o un dispositivo lógico, tal como una función de administración que determina la existencia de una casilla situada en la columna de datos retenidos de la segunda tabla que corresponde a una casilla identificada o seleccionada de la columna de texto en claro no cifrado de la segunda tabla, la cual, a su vez, corresponde a una o más casillas tanto de la columna cifrada de índices como de la columna no cifrada de texto legible de la primera tabla. Los datos identificados (ETAPA 330) en las casillas de datos retenidos como correspondientes a los criterios de coincidencia parcial de búsqueda pueden ser transferidos a copiados de su ubicación existente en una base de datos. Esta manipulación de datos puede incluir recuperar (ETAPA 335), crear, mostrar o poner a disposición de una entidad autorizada una representación electrónica de los datos retenidos identificados (ETAPA 330), así como copiar o transferir estos datos retenidos identificados (ETAPA 330). Generalmente, la recuperación (ETAPA 335) de los datos diana retenidos que se ha identificado que coinciden con los criterios de búsqueda parcial incluye la salida de los datos diana retenidos o una copia de los mismos desde la base de datos en la que están almacenados.

Una vez que al menos algunos de los datos retenidos identificados (ETAPA 330) han sido recuperados (ETAPA 335), el método 300 puede incluir entonces la transmisión de al menos una porción de los datos retenidos recuperados a al menos una entidad autorizada (ETAPA 340). Esta transmisión (ETAPA 340) puede tener lugar desde elementos asociados con un nodo de una red informática que ha identificado (ETAPA 330) y recuperado (ETAPA 335) los datos diana retenidos, y puede incluir uno o más de un transmisor, un receptor, una función de administración, una función de entrega o una función de mediación, así como una o más interfaces de traspaso. Al menos una porción de los datos diana retenidos, incluyendo los datos administrativos asociados, puede ser transmitida (ETAPA 340) a al menos una entidad autorizada, tal como, por ejemplo, un centro de monitorización policial. En una realización general, los datos diana retenidos pueden ser transmitidos desde una función de mediación de un nodo en una red informática a través de diversas interfaces de traspaso a una o más entidades autorizadas, tales como centros de monitorización policial.

En una breve visión general, la Figura 4 es un diagrama de bloques que representa un sistema 400 para recuperar según una realización de la invención datos retenidos. El sistema 400 ilustra un sistema que puede ser usado para cumplir, por ejemplo, la directriz 2006/24/EC de la Unión Europea sobre la retención de datos o estándares industriales tales como las normas ETSI DTS/LI-0039 5 o ETSI DTS/LI-0033 5. Generalmente, el sistema 400 incluye o está asociado con al menos una red 405. La red 405 puede incluir cualquier red de telecomunicaciones a través de la cual pasen transmisiones de datos. Generalmente, la red 405 puede incluir cualesquiera de una red fija, una red móvil o una red central convergente fija y móvil, y puede soportar tráfico conmutado por circuitos o conmutado por paquetes. La red 405 puede ser implementada en conformidad con algunos estándares internacionales, por ejemplo los estándares del Proyecto de Asociación de Tercera Generación o del Instituto Europeo de Estándares de Telecomunicaciones. La red 405 también puede incluir una o más redes de banda ancha que pueden incluir redes de acceso, de agregación, metropolitanas o de área ancha para banda ancha cableada, así como Internet.

Generalmente, la red 405 interactúa o está asociada con al menos un receptor 410, que generalmente es un dispositivo capaz de recibir o aceptar señales, datos, solicitudes o instrucciones entrantes. El receptor 410 puede ser un componente de un ordenador u otro dispositivo usado para implementar el sistema 400. Alternativamente, el receptor 410 puede ser un dispositivo autónomo capaz tanto de recibir como de transmitir instrucciones o datos. Generalmente, el receptor 410 puede recibir una solicitud de acceso a cualquier data retenido que esté almacenado en una base de datos y relacionado con una transmisión de datos en una red, incluyendo cualquier dato administrativo asociado, tal como la fecha, la hora, la duración, la ubicación u otra información administrativa; el receptor 410 puede recibir una solicitud introducida directamente en el receptor 410, por ejemplo, por parte de un operario humano. Generalmente, el receptor 410 recibe como entrada una solicitud de acceso a datos diana retenidos asociados con un usuario diana, incluyendo la solicitud criterios de coincidencia parcial de búsqueda asociados con el usuario diana, tales como, por ejemplo, los tres primeros caracteres del nombre del usuario diana, o los 4 primeros dígitos del MSISDN del usuario diana u otro número de identificación.

En diversas realizaciones, un operario humano puede introducir en el receptor 410 una solicitud de acceso a datos retenidos, tales como un mensaje de audio, vídeo, u otro mensaje de datos dirigido a cualquier tipo de equipo de usuario o procedente del mismo. La solicitud puede surgir, por ejemplo, de un mandamiento de búsqueda emitido

por un gobierno o una institución autorizada que autorice la interceptación de una transmisión de datos. En diversas realizaciones, esta solicitud puede ser comunicada al receptor 410 directamente desde la institución autorizada. En realizaciones alternativas, la solicitud puede ser comunicada mediante un intermediario, tal como un operario humano que reciba la solicitud de una fuente autorizada, y que luego introduzca la solicitud en el sistema 400 por medio del receptor 410 o de una interfaz gráfica de usuario. Normalmente, la solicitud recibida por el receptor 410 incluye criterios de coincidencia parcial de búsqueda, tales como una solicitud que use símbolos comodines.

Generalmente, el receptor 410 interactúa con al menos un procesador 415, o está asociado con el mismo, y, en una realización ilustrativa, ambos pueden estar incluidos en el mismo dispositivo lógico físico. El procesador 415 puede estar situado en la red 405 o ser externo a la misma. Generalmente, el procesador 415 es cualquier dispositivo lógico capaz de efectuar una manipulación de datos, tal como un chip microprocesador capaz de efectuar un procesamiento de datos, con suficiente potencia de procesamiento para llevar a cabo las operaciones descritas en la presente memoria. En diversas realizaciones el procesador 415 puede estar incluido como una unidad central de procesamiento de un ordenador. El procesador 415 es generalmente adaptable para determinar si existen en una base de datos datos retenidos correspondientes a los criterios de coincidencia parcial de búsqueda en función de una solicitud recibida de acceso a datos diana retenidos recibidos.

Normalmente, el procesador 415 está adaptado para acceder a una primera tabla, incluyendo la primera tabla una columna en claro que generalmente contiene datos de identificación no cifrados en varias casillas. Estos datos de identificación no cifrados, tales como un nombre de usuario, un MSISDN u otro medio de identificación de un usuario particular, están contenidos normalmente en casillas dentro de la columna de datos en claro, y cada casilla (es decir, fila) puede estar asociada con un usuario particular, o con una transmisión particular de datos retenidos realizada por un usuario particular en la red 405. Normalmente, la primera tabla también incluye una columna cifrada de índices asociada con datos retenidos que contienen, en varias casillas, un índice cifrado data correspondiente a los datos de identificación no cifrados almacenados en las casillas de la columna en claro.

En una realización ilustrativa, el procesador 415 toma del receptor 410 la solicitud con comodines de acceso a datos diana retenidos y accede a la primera tabla. Si la columna en claro de la primera tabla incluye coincidencias que satisfacen los criterios parciales de búsqueda, el procesador 410 selecciona de la primera tabla al menos una casilla de índice cifrado del índice cifrado que está asociado con una casilla de columna en claro de la columna en claro que coincide con la solicitud que incluye criterios de coincidencia parcial de búsqueda.

Normalmente, el procesador 415 también está adaptado para acceder a una segunda tabla. La segunda tabla incluye generalmente una columna de índices en claro, y la columna de índices en claro incluye normalmente varias casillas que contienen índices no cifrados de texto legible correspondientes a los índices cifrados de la primera tabla y asociados con cada uno de varios usuarios. La segunda tabla también incluye generalmente una columna de datos retenidos que normalmente contiene datos retenidos correspondientes a transmisiones de datos de varios usuarios en la red 405. Las transmisiones de datos son retenidas y almacenadas en casillas de la columna de datos retenidos. Los datos retenidos que son objeto de la solicitud recibida por el receptor 410 son generalmente denominados en la presente memoria datos diana retenidos, y normalmente son un subconjunto de los datos retenidos. Tanto los datos retenidos como los datos diana retenidos pueden incluir una transmisión de datos, tal como una llamada telefónica en una red, así como datos administrativos asociados.

El procesador 415 está generalmente adaptado para seleccionar de la segunda tabla al menos un índice no cifrado de texto legible que está asociado con el índice cifrado seleccionado de la primera tabla y, por lo tanto, también asociado con la columna en claro de la primera tabla que coincide con los criterios de coincidencia parcial de búsqueda. A continuación, el procesador 415 generalmente identifica, detecta o localiza en la columna de datos retenidos, los datos diana retenidos que están asociados con el índice no cifrado seleccionado.

Generalmente, el método 300 también incluye el procesador 415 o elementos asociados que recuperan de una base de datos 420 los datos diana retenidos. Generalmente, la base de datos 420 permite el almacenamiento de datos en cualquier soporte o formato electrónico, y puede incluir diversas formas de memoria de solo lectura, memoria de acceso aleatorio, conjuntos redundantes de discos independientes, señales de datos implementadas, por ejemplo, en una o más ondas portadoras, un disco informático (magnético u óptico (por ejemplo, CD o DVD, o ambos), memoria no volátil, cinta, una memoria de sistema y un disco duro de ordenador.

En una realización ilustrativa, los datos diana retenidos, una vez localizados, identificados y recuperados de la base de datos 420, pueden ser transmitidos por el transmisor 425 a la entidad autorizada 430. Normalmente, el transmisor 425 envía o transmite la transmisión de datos a la entidad autorizada 430. En ciertas realizaciones, el transmisor 425 puede transmitir datos retenidos que incluyen el contenido de la comunicación, tal como el fichero en sí de audio o vídeo, u otra información relacionada, tal como la identidad del equipo de usuario asociado con el origen o el destino de los datos retenidos, o con un usuario diana cuyas comunicaciones a través de la red 405 han sido retenidas en la base de datos 420 y están ahora sometidas a una solicitud de acceso. Generalmente, el transmisor 425 es capaz de transmitir los datos retenidos o una copia de los mismos de cualquier manera. Esto puede incluir una transmisión electrónica cableada o inalámbrica, así como transmitir una transmisión codificada. El transmisor 425 puede acceder a la red 405 o a otra red para transmitir los datos retenidos recuperados en cualquier soporte, incluyendo un soporte

diferente del soporte de transmisión original. En ciertas realizaciones, el transmisor 425 es capaz de transmitir datos relacionados, tales como el número marcado, el número que realizó la llamada, el tipo de servicio, el inicio y el fin de la comunicación u otros datos. En una realización alternativa, el transmisor 425 puede incluir una impresora para imprimir el contenido de la transmisión interceptada, transmitiéndose a continuación a la entidad autorizada 430 el contenido impreso.

En diversas realizaciones el transmisor 425 puede incluir un dispositivo separado para transmitir. En otras realizaciones, el transmisor 425 puede estar incluido en el mismo dispositivo que el procesador 415, el receptor 410 o cualquier otro elemento asociado con el procesador 415. El transmisor 425 puede incluir una o más funciones de mediación que transmitan transmisiones de datos interceptados por una o más interfaces, tal como interfaces de traspaso, a su destino previsto. En algunas realizaciones puede incluirse en un único dispositivo, tal como un ordenador, cualquier combinación de receptor 410, procesador 415 u otros elementos expuestos más abajo. El transmisor 425 es generalmente capaz de transmitir cualquier señal en cualquier formato, incluyendo ficheros de audio, vídeo o imágenes, tales como voz humana codificada, un mensaje de texto, una fecha de transmisión, una hora de transmisión, una ubicación de la transmisión o datos que identifiquen un origen o el destinatario previsto de la transmisión.

La entidad autorizada 430 es generalmente el organismo o la persona autorizado para recibir los datos diana retenidos recuperados. Generalmente, la autoridad para que la entidad autorizada 430 reciba estos datos es otorgada por un gobierno o una organización gubernativa. En algunas realizaciones, la entidad autorizada 430 puede ser la entidad que envió la solicitud inicial, recibida por el receptor 410, de acceso a datos diana retenidos. En algunas realizaciones, la entidad autorizada 430 puede incluir al menos un organismo policial o un centro 435 de monitorización policial. En diversas realizaciones, puede haber más de una entidad autorizada 430, y en algunas realizaciones las múltiples entidades autorizadas 430 no son conscientes de la existencia de las demás. Múltiples entidades autorizadas 430 también pueden recibir, por ejemplo, diferentes porciones de los datos diana retenidos o información relacionada diferente asociada con los datos retenidos.

La entidad autorizada 430 puede incluir un centro de monitorización diseñado para permitir el acceso de personal autorizado a los datos diana retenidos. Normalmente, la entidad autorizada 430 es capaz de recibir cualquier dato asociado con la transmisión de datos. En diversas realizaciones, puede transmitirse a las entidades autorizadas 430 un informe autónomo con información relacionada informándolas de datos administrativos asociados con los datos diana retenidos.

En una realización ilustrativa, se guarda en la base de datos 420 como datos retenidos una transmisión de datos o una copia de la misma que se desplace por la red 405. Cuando una entidad, tal como la entidad autorizada 430, tiene necesidad legítima de acceder a datos específicos retenidos (es decir, datos diana retenidos), puede enviar una solicitud al receptor 410 o al elemento asociado para acceder a estos datos diana retenidos para que puedan ser transmitidos a la entidad autorizada 430. Los datos diana retenidos o los datos administrativos asociados pueden ser transmitidos hacia, desde o entre el procesador 415 y la entidad autorizada 430 mediante una o más de una función 440 de entrega, una función 445 de administración, funciones 450 de mediación, una primera interfaz 455 de traspaso, o una segunda interfaz 460 de traspaso, todo lo cual puede estar asociado con el procesador 415, el receptor 410 o el transmisor 425, o formar parte integral de los mismos.

Generalmente, una transmisión de datos entre cualesquiera de la red 405, la base de datos 420 y la entidad autorizada 430 es remitida a al menos una función 440 de entrega. Normalmente, la función 440 de entrega está asociada con el procesador 415, el receptor 410 o el transmisor 425, o forma parte integral de los mismos. La función 440 de entrega es generalmente capaz de recibir al menos porciones de transmisiones de datos, incluyendo datos retenidos que se introducen en la base de datos 420, datos retenidos transmitidos desde la base de datos 420, y transmisiones de datos diana retenidos que son enviadas a la entidad autorizada 430. En una realización, los datos diana retenidos pueden ser remitidos de la base de datos 420 a la función 440 de entrega. En algunas realizaciones, las funciones 440 de entrega pueden impedir que múltiples entidades autorizadas 430 sean conscientes de la existencia de las demás.

Según puede verse en la Figura 4, el procesador 415 incluye generalmente al menos una función 415 de administración (ADMF). La función 415 de administración, así como la función 440 de entrega o la función 450 de mediación pueden todas interconectarse con las entidades autorizadas 430, y pueden ser integrales al procesador 415, al receptor 410 y al transmisor 425. Aunque puede usarse cualquier interfaz adecuada, la interfaz entre la ADMF 445 y la entidad autorizada 430 puede incluir una primera interfaz 455 de traspaso o una segunda interfaz 460 de traspaso. Las funciones 450 de mediación generalmente convierten datos de la primera interfaz 455 de traspaso y de la segunda interfaz 460 de traspaso a un formato compatible con la entidad autorizada 430 y con los requisitos normativos de la legislación nacional o industriales. Normalmente, las funciones 450 de mediación también reciben la totalidad o parte de los datos retenidos, tales como cualquier contenido o comunicación (CC) y los reenvía, siendo finalmente recibidos por una o más entidades autorizadas 430. En realizaciones que incluyen más de una entidad autorizada 430, la ADMF 445 puede actuar guardando instancias separadas de datos diana retenidos de cada entidad autorizada individual separada 430. La ADMF 445 puede ser dividida para garantizar la debida separación de las transmisiones de datos diana retenidos entre diferentes entidades autorizadas 430.

En una realización, las interfaces primero y segundo 455 y 460 de traspaso separan lógicamente los datos diana retenidos —tales como los de una llamada telefónica realizada a través de la red 405 que quedaron retenidos en la base de datos 420— de los datos administrativos tales como la información de solicitud o de respuesta. En una realización ilustrativa, la primera interfaz 455 de traspaso puede transportar diversos tipos de información administrativa o de solicitud y respuesta encaminada hacia o procedente de una autoridad solicitante, tal como la entidad autorizada 430 o un proveedor de servicios de comunicaciones que pueda ser responsable de retener transmisiones de datos a través de la red 405. Por ejemplo, la primera interfaz 455 de traspaso puede transportar datos que indiquen la fecha de transmisión, la hora de transmisión, la duración de la transmisión, los participantes implicados u otros datos administrativos similares relativos a los datos diana retenidos. Siguiendo con esta realización ilustrativa, la segunda interfaz 460 de traspaso puede transportar hasta la entidad autorizada 430 los datos diana retenidos en sí procedentes de un proveedor de servicios de comunicaciones que contra la base de datos 420. Normalmente, la primera interfaz 455 de traspaso y la segunda interfaz 460 de traspaso son intercambiables, de modo que cualquiera de las dos bases de datos puede transportar ya sea los propios datos diana retenidos o cualquier dato asociado, tal como datos administrativos. En algunas realizaciones puede haber un número cualquiera de interfaces de traspaso, de una a más de dos. En una realización, la primera interfaz 460 de traspaso puede ser usada para enviar solicitudes de consultas, y la segunda interfaz 460 de traspaso puede ser usada para remitir los resultados de las consultas, tales como los datos retenidos, a un centro de monitorización policial o a otra entidad autorizada 430.

En una breve visión general, la Figura 5 es una tabla que representa una primera tabla 500 que incluye una columna 505 en claro y una columna cifrada 510 de índices según una realización de la invención. Normalmente, la columna 505 en claro incluye varias casillas 515 - 530 que incluyen datos de texto legible, y la columna cifrada 510 de índices incluye varias casillas 535 - 550. Estos datos de texto legible de la columna 505 en claro están generalmente no cifrados y, como tales, pueden ser sensibles a una búsqueda de datos basada en criterios de coincidencia parcial de búsqueda, tales como comodines. Normalmente, la columna cifrada 510 de índices está cifrada. Aunque en la tabla 500 se representa un número limitado de casillas, puede existir un número cualquiera de casillas. Por ejemplo, en la primera tabla 500 un criterio de búsqueda parcial “j*” coincidiría tanto con “John”, almacenado en la casilla 515, como con “Jack”, almacenado en la casilla 525. “John”, en la casilla 515, corresponde a la casilla f(1) 535 de la columna cifrada 510 de índices, y “Jack” corresponde a la casilla f(3) 545 de la columna cifrada 510 de índices. En esta realización ilustrativa, los índices (j*) han sido seleccionados de la tabla 500 basándose en una coincidencia parcial en búsquedas, y se devuelven los índices cifrados f(1) y f(3) en respuesta a la búsqueda con comodín f(j*).

Para cada índice (j) obtenido en función de la coincidencia parcial en resultados de búsqueda ejemplificados en lo que antecede, los sistemas y los métodos dados a conocer en la presente memoria prosiguen generalmente a la segunda tabla 600 de la Figura 6 para identificar y recuperar los datos diana retenidos en función de los criterios de coincidencia parcial de búsqueda. En una breve visión general, la Figura 6 es una tabla que representa una segunda tabla 600 que incluye una columna índice 605 de texto legible y una columna 610 de datos retenidos según una realización de la invención. En una realización, tanto la columna índice 605 de texto legible como la columna 610 de datos retenidos pueden no estar cifradas. La columna índice 605 de texto legible generalmente incluye varias casillas 615 - 645 de índice de texto legible, y la columna 610 de datos retenidos generalmente incluye varias casillas 650 - 680 de datos retenidos. En una realización, las casillas 615 - 645 de la columna índice 605 de texto legible puede incluir los índices no cifrados de texto legible asociados con su correspondiente índice cifrado de las casillas 535 - 550 del índice cifrado 510. Para cada índice cifrado obtenido de la columna cifrada 510 de índices (es decir, f(1) y f(3) en el ejemplo descrito anteriormente), los sistemas y los métodos descritos en la presente memoria generalmente pasan a seleccionar, de la segunda tabla 600, la fila de la casilla que coincide con f(j) tanto en la columna índice 605 de texto legible como en la correspondiente columna 610 de datos retenidos.

Siguiendo con la anterior realización ilustrativa, los sistemas y los métodos pueden seleccionar $f^1(j)$, es decir, $f^1(f(1))$ y $f^1(f(3))$. Esta da como resultado una selección de casillas de índice de texto legible con el índice “1” y “3”, es decir, las casillas 615, 625, 630 y 645 de índice de texto legible de la columna índice 605 de texto legible. Estas casillas corresponden a las casillas 650, 660, 665 y 680 de datos retenidos de la columna 610 de datos retenidos. Normalmente, los datos retenidos en cualquiera de las casillas de la columna 610 de datos retenidos pueden incluir cualquier transmisión de datos en la red 405, tal como llamadas telefónicas, de vídeo o de voz sobre protocolo de Internet, así como cualquier dato asociado o relacionado, o eventos relacionados con la fecha, la hora, la duración, la ubicación o el soporte de la transmisión, así como los participantes implicados en la transmisión, u otra información relacionada.

El ejemplo anteriormente descrito da como resultado la identificación de las casillas en la columna 610 de datos retenidos que coinciden con una búsqueda con comodines realizada inicialmente en la columna 505 en claro. Esta búsqueda con comodines devuelve las casillas apropiadas de la columna cifrada 510 de índices, que es asociada entonces con las casillas de la columna índice 605 de texto legible y sus correspondientes casillas de la columna 610 de datos retenidos, que generalmente incluyen los datos diana retenidos almacenados en la base de datos 420, que pueden entonces ser enviados a la entidad autorizada 430, tal como uno o más centros 435 de monitorización policial.

Los sistemas y los métodos dados a conocer en la presente memoria generalmente permiten la selección de un subconjunto de datos retenidos. Este subconjunto es generalmente los datos diana retenidos solicitados por la entidad autorizada 430. En caso de que las técnicas de cifrado hayan sido puestas en peligro debido, por ejemplo, a un ataque informático no autorizado, puede ser necesario un cambio de una clave de cifrado. Dado que estos sistemas y estos métodos permiten la recuperación de un subconjunto específico de los datos retenidos, en una realización únicamente este subconjunto de datos recuperados —los datos diana recuperados— es descifrado con la clave antigua y se lo vuelve a cifrar con una nueva clave en respuesta a un cifrado potencialmente puesto en peligro. Generalmente, esto elimina la necesidad de descifrar y volver a cifrar todos los datos retenidos almacenados en la base de datos 420.

En una breve visión general, la Figura 7 representa un sistema 700 que incluye dos tablas, en las que la tabla MSISDN 705 incluye una columna MSISDN 710 en claro y una columna MSISDN cifrada 715 de índices, y en las que la tabla 720 de datos de llamadas incluye una columna índice 725 de texto legible y una columna 730 de hora de inicio en texto legible según una realización de la invención. La realización ilustrativa representada en el sistema 700 es generalmente análoga a una combinación de las tablas 500 y 600. En el ejemplo anterior, la columna 505 en claro incluía nombres de usuario, “Jack”, “John”, etc. En la Figura 7, la columna MSISDN 710 de texto legible incluye un número de red digital de servicios integrados de estaciones móviles (MSISDN) como indicadores de identificación de llamadas que identifican a los usuarios de las casillas 735 - 750 como alternativa a los nombres de usuario indicados en las casillas 515 - 530 de la columna 505 en claro. En diversas realizaciones pueden usarse otros números de identificación de usuario, tales como los números de identidad internacional de abonado móvil (IMSI) o de identidad internacional de equipo móvil (IMEI). Las casillas 735 - 750 de la columna MSISDN 710 están normalmente en texto legible, es decir, no cifrado. Las casillas 735 - 750 generalmente corresponden a al menos una de las casillas 755 - 770 de la columna MSISDN cifrada 715 de índices.

Normalmente, una búsqueda con comodines de los números de identificación de MSISDN (u otro) contenidos en las casillas de la columna 710 devuelve al menos una correspondiente casilla de la columna MSISDN cifrada 715 de índices. Generalmente, llevar a cabo un procedimiento de descifrado en estas casillas da como resultado, a su vez, la identificación o la selección de una o más de las casillas 775, 777, 779, 781 o 783 de la columna índice 725 de texto legible. Dado que cada casilla de la columna índice 725 de texto legible está asociada normalmente con al menos una casilla de la columna 730 de hora de inicio en texto legible, tal como una o más de las casillas 790, 792, 794, 796 o 798, los datos de estas casillas de la columna 730 de hora de inicio en texto legible pueden ser identificadas y recuperadas como los datos diana retenidos asociados con la búsqueda con comodines. Según se muestra, la columna 730 de hora de inicio en texto legible incluye datos de la hora de inicio de transacciones que se produjeron a través de la red 405; sin embargo, en diversas realizaciones, la columna 730 de la hora de inicio en texto legible puede incluir diversos tipos de datos retenidos, desde el contenido de las comunicaciones en la red 405 hasta otros datos asociados, tales como la fecha, la hora, la ubicación, los intervinientes implicados u otra información relacionada. Almacenar el MSISDN u otros indicadores de identificación en texto legible no cifrado permite búsquedas con comodines precisas y eficientes mientras se sigue manteniendo la confidencialidad de los datos retenidos proporcionando un nivel de cifrado entre la información identificativa y los datos retenidos asociados con un MSISDN dado u otro identificador similar.

Por ejemplo, con referencia a la Figura 7, una búsqueda con comodines de “0815147*” en la columna MSISDN 710 de texto en claro recuperaría las casillas 735 y 740, que corresponden a las casillas cifradas f(1) y f(2) 755 y 760. Llevar a cabo un descifrado de estas casillas devuelve las casillas 775 y 777 de la columna índice 725 de texto legible, y estas casillas corresponden a datos diana retenidos en las casillas 790 y 792, que entonces pueden ser identificados, ser objeto de acceso o ser recuperados según se desee en respuesta a la búsqueda con comodines. Generalmente, puede haber más de una casilla de datos retenidos o de datos diana retenidos asociadas con un solo MSISDN u otro número de identificación. Por ejemplo, la casilla 745 contiene un único número de MSISDN, pero las casillas 794 y 796 de datos retenidos indican dos horas de inicio separadas, por ejemplo, llamadas telefónicas realizadas a través de la red 405. Normalmente, todos los datos retenidos asociados con un solo usuario pueden ser identificados o ser objeto de acceso en respuesta a una búsqueda con comodines que contenga solo una porción de la información de identificación de un usuario diana, tal como un número de MSISDN.

Obsérvese que en las Figuras 1 a 7, los elementos enumerados son mostrados como elementos individuales. Sin embargo, en implementaciones reales de los sistemas y los métodos descritos en la presente memoria, pueden ser componentes inseparables de otros dispositivos electrónicos tales como un ordenador digital. Así, las acciones descritas anteriormente pueden ser implementadas en soporte lógico que puede estar implementado en un producto manufacturado que incluye un soporte de almacenamiento de programas. El soporte de almacenamiento de programas incluye señales de datos implementadas en uno o más de una onda portadora, un disco informático (magnético u óptico (por ejemplo, CD o DVD, o ambos), memoria no volátil, cinta, una memoria de sistema y un disco duro de ordenador.

Por lo anterior, se apreciará que los sistemas y los métodos descritos en la presente memoria proporcionan una manera simple y efectiva de recuperar datos diana retenidos de una base de datos. Los sistemas y los métodos según diversas realizaciones son capaces de recuperar datos diana retenidos con base en la recepción de una

solicitud que incluye criterios de coincidencia parcial de búsqueda. Esto aumenta la eficiencia y la velocidad operativa, y disminuye el coste.

Cualquier referencia a elementos o etapas de los sistemas y los métodos a los que se hace referencia en la presente memoria en singular también puede abarcar realizaciones que incluyan varios de estos elementos, y cualquier referencia en plural a cualquier elemento o etapa en la presente memoria también puede abarcar realizaciones que incluyan un único elemento. Las referencias en forma singular o plural no están previstas para limitar los sistemas o los métodos actualmente divulgados, sus componentes, sus etapas o sus elementos.

Cualquier realización dada a conocer en la presente memoria puede ser combinada con cualquier otra realización, y referencias tales como “una realización”, “algunas realizaciones”, “una realización alternativa”, “diversas realizaciones” o similares no son necesariamente mutuamente excluyentes y están previstas para indicar que una característica, una estructura o un rasgo particular descrito en conexión con la realización puede estar incluido en al menos una realización. Las apariciones de tales términos en la presente memoria no se refieren todas necesariamente a la misma realización. Cualquier realización puede combinarse con cualquier otra realización de cualquier manera coherente con los objetos, los objetivos y las necesidades dados a conocer en la presente memoria.

Las referencias a “o” pueden ser interpretadas de forma incluyente, de modo que cualesquiera términos descritos usando “o” puedan indicar cualesquiera de un solo término, más de uno o todos los términos descritos.

Cuando las características técnicas mencionadas en cualquier reivindicación son seguidas por signos de referencia, los signos de referencia han sido incluidos con el único fin de aumentar la inteligibilidad de las reivindicaciones y, en consecuencia, ni los signos de referencia ni su ausencia tienen ningún efecto limitante en el alcance de ningún elemento de las reivindicaciones.

Un experto en la técnica se dará cuenta de que los sistemas y los métodos descritos en la presente memoria pueden ser implementados en otras formas específicos sin apartarse de las características esenciales de los mismos. Por lo tanto, ha de considerarse que las realizaciones anteriores son todos los sentidos ilustrativas, no limitantes, de los sistemas y los métodos descritos. Así, el alcance de los sistemas y los métodos descritos en la presente memoria está indicado por las reivindicaciones adjuntas, no por la descripción anterior, y, por lo tanto, se pretende que todos los cambios que se encuentren dentro del significado y la gama de equivalencia de las reivindicaciones estén incluidos en el mismo.

REIVINDICACIONES

1. Un método de recuperación de datos diana retenidos de una base de datos que comprende:

recibir (305) una solicitud de acceso a los datos diana retenidos asociados con un usuario diana, incluyendo la solicitud criterios de coincidencia parcial de búsqueda asociados con el usuario diana;
acceder (310) a una primera tabla, incluyendo la primera tabla una columna en claro que tiene datos de identificación no cifrados asociados con varios usuarios, e incluyendo la primera tabla una columna cifrada de índices que tiene un índice cifrado asociado con cada uno de los varios usuarios;
seleccionar (315) de la primera tabla al menos un índice cifrado que corresponda a entradas en la columna de texto en claro que coincida con los criterios de coincidencia parcial de búsqueda;
acceder (320) a una segunda tabla, incluyendo la segunda tabla una columna de índices en claro que tiene un índice no cifrado asociado con cada uno de los varios usuarios, e incluyendo la segunda tabla una columna de datos retenidos que tiene varios datos retenidos que incluye los datos diana retenidos;
seleccionar (325) de la segunda tabla al menos un índice no cifrado asociado con el al menos un índice cifrado seleccionado, siendo el índice no cifrado el homólogo no cifrado del índice cifrado;
identificar (330), en la columna de datos retenidos, los datos diana retenidos asociados con el al menos un índice no cifrado seleccionado; y
recuperar (340) de la base de datos los datos diana retenidos.

2. El método de la reivindicación 1 que comprende:

descifrar la columna cifrada de índices asociada con los datos diana retenidos usando una primera clave; y
volver a cifrar la columna cifrada de índices asociada con los datos diana retenidos usando una segunda clave.

3. El método de la reivindicación 1 en el que la recepción de la solicitud de acceso a los datos diana retenidos asociados con el usuario comprende al menos una de la recepción de un nombre parcial del usuario diana o la recepción de un número de identidad del usuario diana.

4. El método de la reivindicación 1 que comprende:

transmitir a una entidad autorizada los datos diana retenidos, comprendiendo preferentemente dicha transmisión de los datos diana retenidos transmitir a un centro de monitorización policial los datos diana retenidos.

5. El método de la reivindicación 4 que comprende:

transmitir a la entidad autorizada, a través de una primera interfaz de traspaso, datos administrativos asociados con los datos diana retenidos; y
transmitir a la entidad autorizada, a través de una segunda interfaz de traspaso, los datos diana retenidos.

6. El método de la reivindicación 5 en el que los datos administrativos incluyen al menos uno de una fecha de creación de los datos retenidos, una hora de creación de los datos retenidos, una confirmación de la solicitud de acceso a datos diana retenidos, o datos de identificación del usuario diana.

7. Un sistema de recuperación de datos diana retenidos de una base de datos (420) que comprende:

un receptor (410) asociado con un procesador (415) para recibir una solicitud de acceso a datos diana retenidos asociados con un usuario diana, incluyendo la solicitud criterios de coincidencia parcial de búsqueda asociados con el usuario diana;
estando adaptado el procesador para acceder a una primera tabla, incluyendo la primera tabla una columna en claro que tiene datos de identificación no cifrados asociados con varios usuarios, e incluyendo la primera tabla una columna cifrada de índices que tiene un índice cifrado asociado con cada uno de los varios usuarios;
estando adaptado el procesador para seleccionar de la primera tabla al menos un índice cifrado que corresponda a entradas en la columna de texto en claro que coincida con los criterios de coincidencia parcial de búsqueda;
estando adaptado el procesador para acceder a una segunda tabla, incluyendo la segunda tabla una columna de índices en claro que tiene un índice no cifrado asociado con cada uno de los varios usuarios, e incluyendo la segunda tabla una columna de datos retenidos que tiene varios datos retenidos que incluye los datos diana retenidos;
estando adaptado el procesador para seleccionar de la segunda tabla al menos un índice no cifrado asociado con el al menos un índice cifrado seleccionado, siendo el índice no cifrado el homólogo no cifrado del índice cifrado;
estando adaptado el procesador para identificar, en la columna de datos retenidos, los datos diana retenidos asociados con el al menos un índice no cifrado seleccionado; y

estando adaptado el procesador para recuperar de la base de datos los datos diana retenidos.

8. El sistema de la reivindicación 7 que comprende:

el procesador adaptado para descifrar la columna cifrada de índices asociada con los datos diana retenidos usando una primera clave; y
el procesador adaptado para volver a cifrar la columna cifrada de índices asociada con los datos diana retenidos usando una segunda clave.

9. El sistema de la reivindicación 7 en el que los criterios de coincidencia parcial de búsqueda comprenden al menos uno de un nombre parcial del usuario diana o un número de identidad del usuario diana.

10. El sistema de la reivindicación 7 que comprende:

un transmisor adaptado para transmitir a una entidad autorizada los datos diana retenidos, estando el transmisor preferentemente adaptado para transmitir a un centro de monitorización policial los datos diana retenidos.

11. El sistema de la reivindicación 10 que comprende:

el transmisor adaptado para transmitir a la entidad autorizada, desde una función de administración, a través de una primera interfaz de traspaso, datos administrativos asociados con los datos diana retenidos; y
el transmisor adaptado para transmitir a la entidad autorizada, desde al menos una función de mediación y una función de entrega, a través de una segunda interfaz de traspaso, los datos diana retenidos.

12. El sistema de la reivindicación 11 en el que los datos administrativos incluyen al menos uno de una fecha de creación de los datos retenidos, una hora de creación de los datos retenidos, una confirmación de la solicitud de acceso a datos diana retenidos, o datos de identificación del usuario diana.

13. El sistema de la reivindicación 7 en el que los datos retenidos y los datos diana retenidos comprenden comunicaciones electrónicas de datos por medio de al menos una de una red telefónica pública conmutada y una red telefónica móvil.

14. El sistema de la reivindicación 7 en el que los datos retenidos y los datos diana retenidos están almacenados en una base de datos asociada con el procesador.

15. Un producto manufacturado que comprende un soporte de almacenamiento de programas que tiene implementado en el mismo un código de programa legible por ordenador para recuperar de una base de datos diana retenidos, comprendiendo el código de programa legible por ordenador en el producto manufacturado:

código de programa legible por ordenador para hacer que un ordenador reciba una solicitud de acceso a datos diana retenidos asociados con un usuario diana, incluyendo la solicitud criterios de coincidencia parcial de búsqueda asociados con el usuario diana;
código de programa legible por ordenador para hacer que un ordenador acceda a una primera tabla, incluyendo la primera tabla una columna en claro que tiene datos de identificación no cifrados asociados con varios usuarios, e incluyendo la primera tabla una columna cifrada de índices que tiene un índice cifrado asociado con cada uno de los varios usuarios;
código de programa legible por ordenador para hacer que un ordenador seleccione de la primera tabla al menos un índice cifrado que corresponda a entradas en la columna de texto en claro que coincida con los criterios de coincidencia parcial de búsqueda;
código de programa legible por ordenador para hacer que un ordenador acceda a una segunda tabla, incluyendo la segunda tabla una columna de índices en claro que tiene un índice no cifrado asociado con cada uno de los varios usuarios, e incluyendo la segunda tabla una columna de datos retenidos que tiene varios datos retenidos que incluye los datos diana retenidos;
código de programa legible por ordenador para hacer que un ordenador seleccione de la segunda tabla al menos un índice no cifrado asociado con el al menos un índice cifrado seleccionado;
código de programa legible por ordenador para hacer que un ordenador identifique, en la columna de datos retenidos, los datos diana retenidos asociados con el al menos un índice no cifrado seleccionado, siendo el índice no cifrado el homólogo no cifrado del índice cifrado; y
código de programa legible por ordenador para hacer que un ordenador recupere de la base de datos los datos diana retenidos.

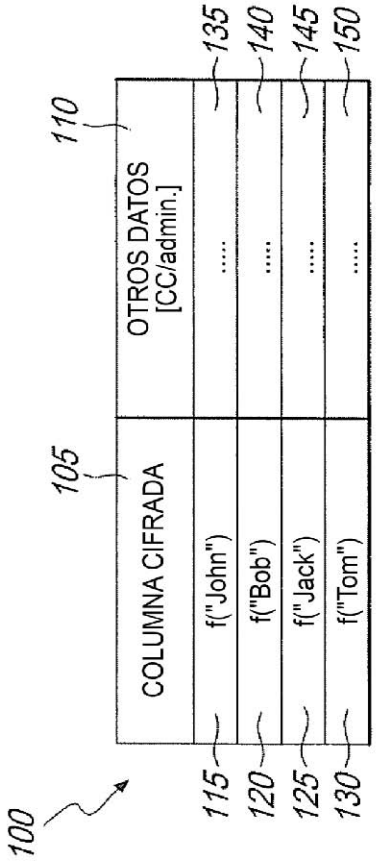
100
105
110
COLUMNA CIFRADA
OTROS DATOS [CC/admin.]
f("John")
f("Bob")
f("Jack")
f("Tom")
.....
115
120
125
130
135
140
145
150

Fig. 1

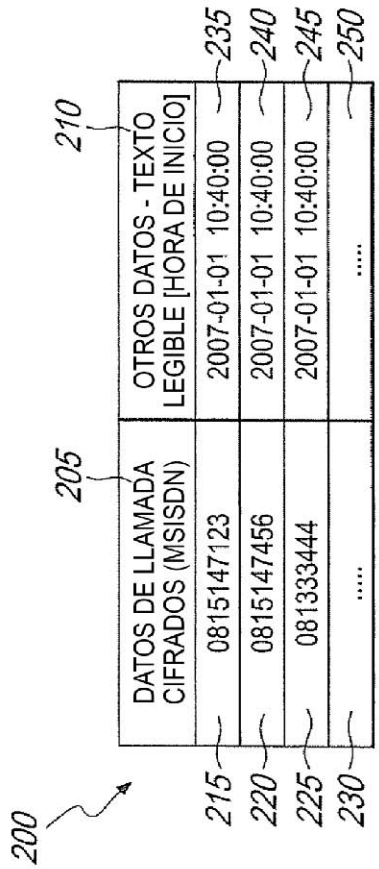
200
205
210
DATOS DE LLAMADA CIFRADOS (MSISDN)
OTROS DATOS - TEXTO LEGIBLE [HORA DE INICIO]
0815147123
0815147456
0813333444
2007-01-01 10:40:00
2007-01-01 10:40:00
2007-01-01 10:40:00
.....
215
220
225
230
235
240
245
250

Fig. 2

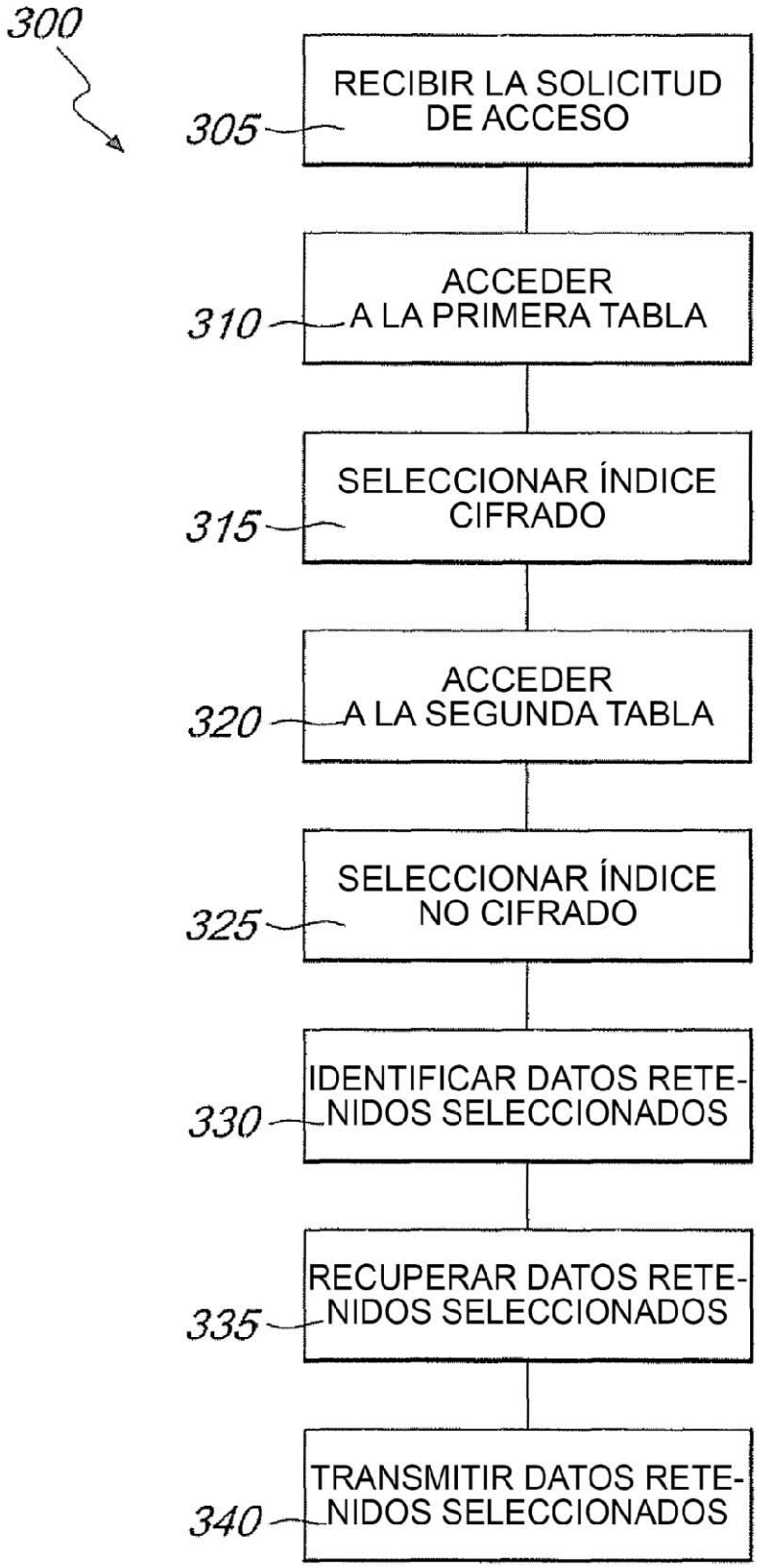
300
305
RECIBIR LA SOLICITUD DE ACCESO
310
ACCEDER A LA PRIMERA TABLA
315
SELECCIONAR ÍNDICE CIFRADO
320
ACCEDER A LA SEGUNDA TABLA
325
SELECCIONAR ÍNDICE NO CIFRADO
330
IDENTIFICAR DATOS RETENIDOS SELECCIONADOS
335
RECUPERAR DATOS RETENIDOS SELECCIONADOS
340
TRANSMITIR DATOS RETENIDOS SELECCIONADOS

Fig. 3

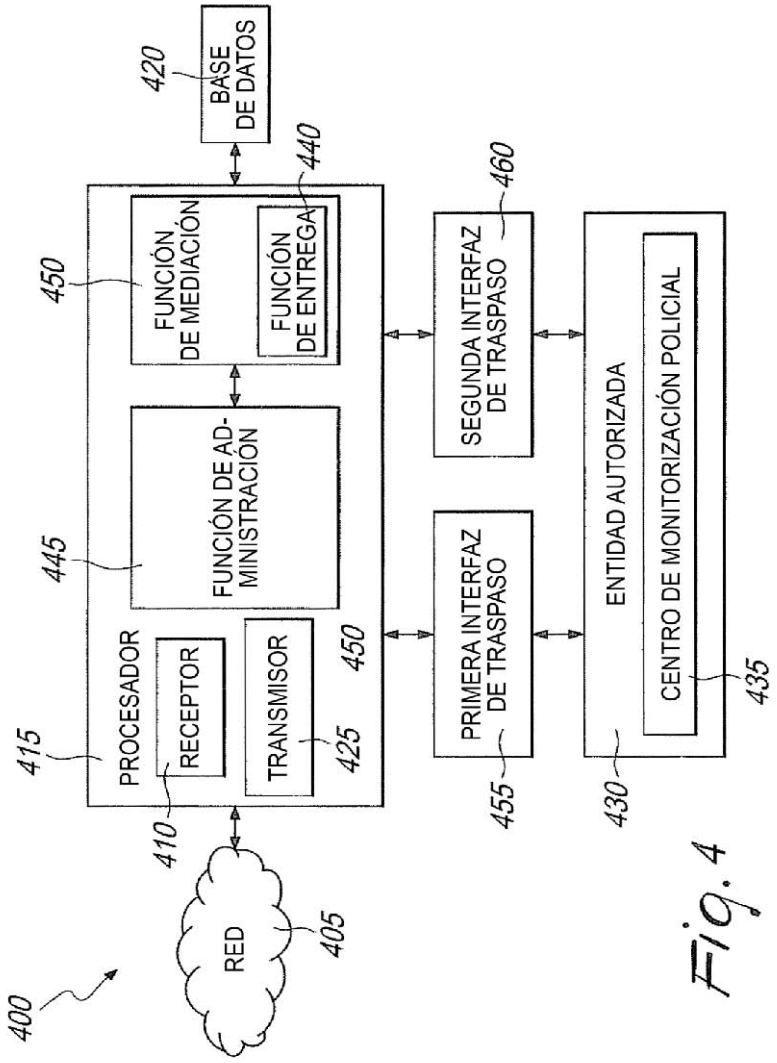
400
RED
405
410
PROCESADOR
415
RECEPTOR
TRANSMISOR
425
450
FUNCIÓN DE AD-MINISTRACIÓN
445
FUNCIÓN DE MEDIACIÓN
450
FUNCIÓN DE ENTREGA
440
BASE DE DATOS
420
PRIMERA INTERFAZ DE TRASPASO
455
SEGUNDA INTERFAZ DE TRASPASO
460
ENTIDAD AUTORIZADA
430
CENTRO DE MONITORIZACIÓN POLICIAL
435

Fig. 4

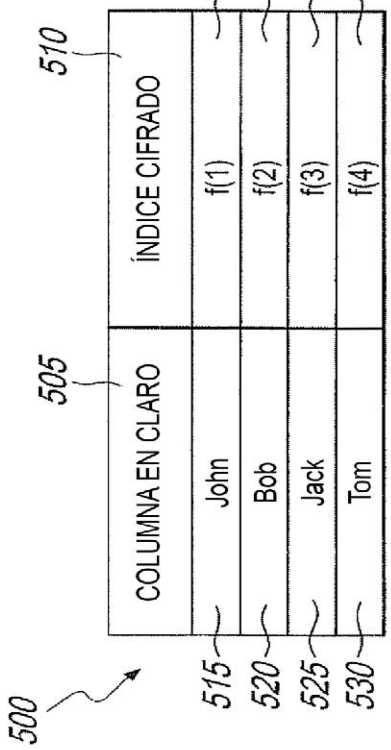
500
505
510
COLUMNA EN CLARO
ÍNDICE CIFRADO
John
Bob
Jack
Tom
f(1)
f(2)
f(3)
f(4)
515
520
525
530
535
540
545
550

Fig. 5

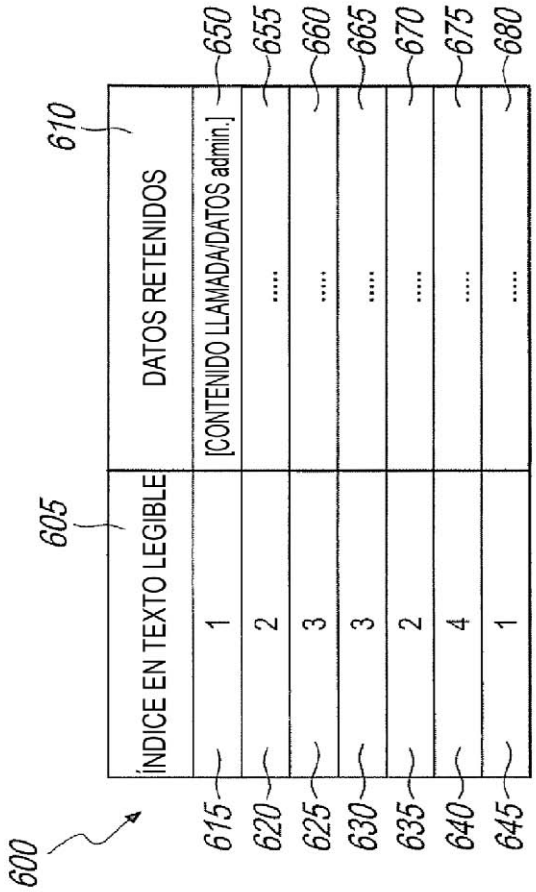
600
605
610
ÍNDICE EN TEXTO LEGIBLE
DATOS RETENIDOS
1
2
3
3
2
4
1
[CONTENIDO LLAMADA/DATOS admin.]
.....
615
620
625
630
635
640
645
650
655
660
665
670
675
680

Fig. 6

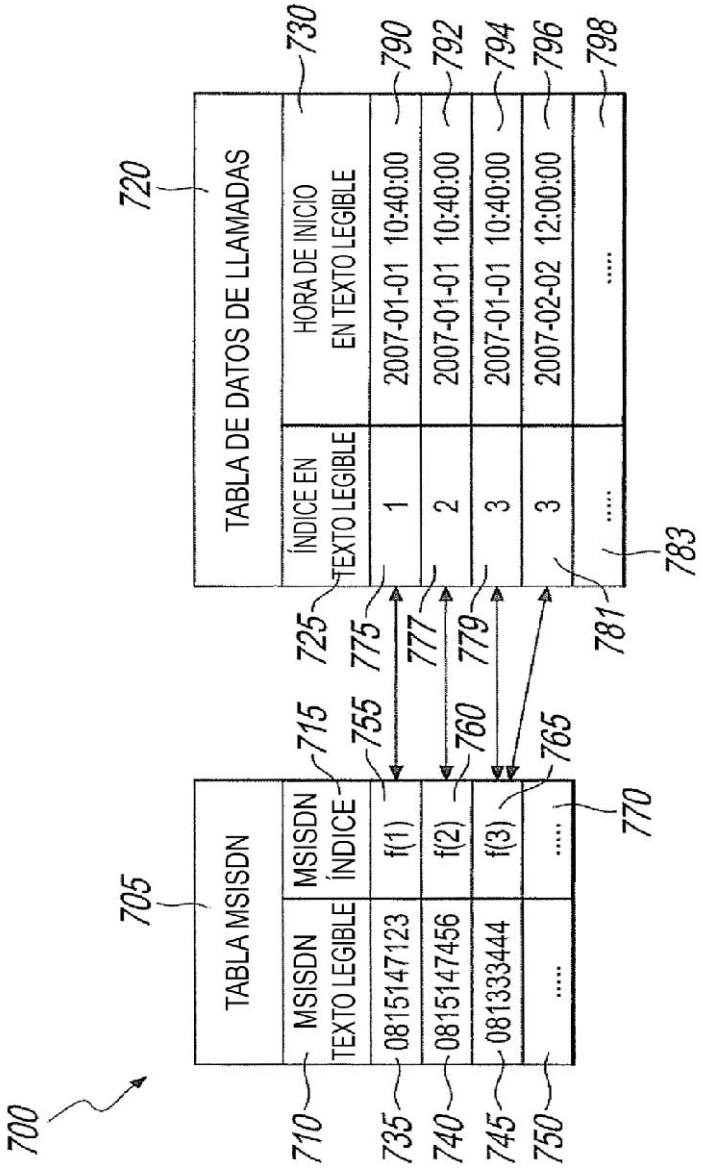
700
705
TABLA MSISDN
MSISDN TEXTO LEGIBLE
MSISDN ÍNDICE
0815147123
0815147456
0813333444
f(1)
f(2)
f(3)
710
715
735
740
745
750
755
760
765
770
720
TABLA DE DATOS DE LLAMADAS
ÍNDICE EN TEXTO LEGIBLE
HORA DE INICIO EN TEXTO LEGIBLE
1
2
3
2007-01-01 10:40:00
2007-01-01 10:40:00
2007-01-01 10:40:00
2007-02-02 12:00:00
730
725
775
777
779
781
783
790
792
794
796
798

Fig. 7