(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 605 929**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.06.2013 E 13170745 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2811708**

(54) Título: **Sistema y método para la autentificación de un usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.03.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
22-24, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

AUMASSON, JEAN-PHILIPPE

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Sistema y método para la autentificación de un usuario

Introducción

[0001] La presente solicitud se refiere a los sistemas o métodos para la autentificación de un usuario cuando éste desea acceder a un servicio a distancia.

Generalidades

[0002] Muchos servicios en línea exigen una identificación y una autentificación de un usuario cuando éste desea acceder a una parte privada de este servicio, por ejemplo acceder a su espacio Facebook™ o poder leer sus mensajes.
Para ello, el servidor de dicho servicio requiere al usuario dar un identificador y una contraseña.

[0003] Estos datos son verificados con los de referencia almacenados por el servidor para comprobar que, por una parte, el identificador está bien clasificado en el servidor y, por otra parte, que la contraseña corresponde con la de referencia.
Una vez se han hecho estas verificaciones, el servidor autoriza el acceso al servicio para dicho usuario.

Estado de la técnica

[0004] Las soluciones actuales han ya tenido en cuenta los riesgos de almacenar estas informaciones en claro en una base de datos, aunque esta base esté protegida.
Por esta razón, un primer enfoque consiste en ejecutar una función hash (función de sentido único) tal como SHA-1 o MD5 sobre el identificador y la contraseña y almacenar estas dos informaciones bajo esta forma: se debe señalar que estas funciones de elección arbitraria son consideradas de sentido único, es decir, que no es posible calcular el valor de origen disponiendo del valor del hash.

[0005] El documento US2007/234408, por ejemplo, describe un método de autentificación de un usuario a través de una función de sentido único y de dos servidores distintos.

[0006] Se ha comprobado, sin embargo, que cuando se produce un robo de datos, ciertas herramientas especializadas (ataque de fuerza bruta, ataque de diccionario, por ejemplo) permitían mediante intentos sucesivos recuperar la contraseña en claro.
El uso de funciones criptográficas más costosas de evaluar, por ejemplo el estándar NIST PBKDF2, ha hecho estos ataques menos eficaces.

[0007] Otro enfoque es el almacenamiento de estos datos sensibles en un elemento de seguridad material en forma cifrada.
La imaginación y la determinación de los piratas no tiene límite, y ni siquiera estos elementos de seguridad están a salvo de robos.

[0008] En estos diferentes enfoques, los datos sensibles se almacenan en un solo lugar que será por lo tanto el centro de atención de los piratas para apropiarse manera ilegítima de las informaciones privadas de los usuarios.

[0009] Otro problema que la presente invención se propone resolver se refiere a la actualización de la seguridad de las contraseñas.
En efecto, si un servidor desea modificar la función hash por una nueva función que ofrece más seguridad, es necesario que cada usuario sea advertido para que se identifique con su contraseña, éste estando verificada gracias a la primera función hash.
Luego, el usuario es invitado a introducir un nueva contraseña que será codificada por la segunda función hash después almacenada.
Tal actualización normalmente está motivada por la necesidad de adaptarse a la potencia de cálculo de los atacantes y a la del usuario legítimo.

Breve descripción de la invención

[0010] La presente invención tiene dos objetivos, a saber, por una parte, el refuerzo de la seguridad para la protección no sólo de la contraseña sino también del identificador de un usuario; y, por otra parte, permitir una actualización de la seguridad sin tener que hacer intervenir al usuario.
Estos objetivos se pueden perseguir separadamente o en combinación.

[0011] La presente invención se describe en las reivindicaciones anexas.

[0012] La presente invención se basa en el uso de dos servidores, ninguno de los cuales dispone de la totalidad de las informaciones sobre un usuario.
El primer servidor comprende una primera base de datos y el segundo servidor comprende una segunda base de datos.

[0013] En particular, el servidor frontal (o primer servidor), en comunicación con la red pública, no dispone de información sensible que pueda ser útil a un tercero malicioso si estos datos fueran pirateados.

[0014] El primer servidor almacena en la primera base de datos protegida un registro por usuario, este registro que comprende según una primera versión únicamente el primer criptograma H.

[0015] El segundo servidor almacena en la segunda base de datos protegida el parámetro de seguridad R y un cifrado del triplete identificador, contraseña, y parámetro de seguridad.

[0016] Se debe señalar que la función de sentido único la conoce únicamente el segundo servidor, esta función pudiendo ser inicializada por una clave secreta propia del segundo servidor.

Breve descripción de las figuras

[0017] La presente invención se comprenderá mejor gracias a las figuras anexas, en las cuales:
- La figura 1 ilustra la etapa de inscripción,
- La figura 2 ilustra la etapa de verificación.

Descripción detallada

[0018] El sistema de la invención comprende al menos dos servidores, el primer servidor S1 (front-end) siendo accesible por un usuario o usuarios y el segundo servidor S2 (back-end) estando conectado localmente al primer servidor S1.
La conexión entre el primer servidor y el segundo servidor está protegida, es decir, que el carácter confidencial y la integridad de los datos intercambiados están asegurados.
Cada uno de estos servidores dispone de una base de datos para almacenar los datos que sirven para la autentificación de un usuario.

[0019] Una vez el sistema está instalado, el segundo servidor inicializa el parámetro de seguridad R que será almacenado en la segunda base de datos protegida de dicho servidor.
Se debe señalar que este parámetro puede depender de la aplicación solicitada, en el caso de que el primer servidor proponga más de un servicio.
Este es el caso, por ejemplo, de un banco que ofrece un acceso de gestión a una cuenta privada, o a una cuenta de inversiones.
En tal caso, es posible que cada uno de estos servicios corresponda a un parámetro de seguridad diferente.

[0020] Con el fin de permitir al segundo servidor seleccionar el parámetro correcto, el primer mensaje enviado del primer servidor al segundo servidor comprenderá también el tipo de servicio para el cual la autentificación se requiere en ese caso o varios servicios son controlados por el segundo servidor.

Inscripción

[0021] La primera etapa es la inscripción de un usuario en el sistema como se ilustra por la figura 1.
De manera convencional, este usuario es invitado a introducir un identificador de referencia U y una contraseña de referencia P en una interfaz del primer servidor S1.

[0022] Estas dos informaciones se transmiten al segundo servidor S2 a través de la conexión protegida.
El primer servidor puede añadir informaciones complementarias tales como el tipo de servicio y/o un identificador de sistema ID asignado a este usuario para el servicio propuesto.
El identificador de referencia U es el conocido por el usuario, mientras que el identificador de sistema ID es un número o serie alfanumérica propia del sistema que propone el servicio.
El identificador sistema es único por usuario.

[0023] Una vez estas informaciones han sido recibidas por el segundo servidor S2, éste determina el parámetro de seguridad R y ejecuta la función de sentido único Hash sobre el identificador de referencia U y la contraseña P. El resultado es un criptograma H = Hash(U, P,R).
Este resultado H se transmite al primer servidor S1, que lo almacena en su base de datos protegida.

[0024] El segundo servidor S2 cifra igualmente el identificador de referencia U y la contraseña P con un método de cifrado asimétrico que toma como argumento una clave pública almacenada por dicho servidor S2, la clave privada correspondiente siendo almacenada de manera protegida fuera de la red (por ejemplo en una caja física).

Según una variante, el conjunto cifrado puede comprender el parámetro de seguridad R, permitiendo de este modo saber qué parámetro ha sido utilizado para este usuario.

[0025] Dicho método de cifrado asimétrico puede estar, por ejemplo, basado en RSA, o en curvas elípticas.

[0026] Como se ha dicho anteriormente, el primer servidor S1 almacena el primer criptograma H en su base de datos protegida.
Así, durante la verificación, el primer servidor, después de haber recibido el segundo criptograma H' del segundo servidor, va a barrer su base de datos con el fin de determinar si un primer criptograma H tiene el mismo valor que el segundo criptograma H' y, de este modo, determinar si la autentificación se ha realizado.

[0027] En esta forma de realización, es posible añadir una verificación antes de la aceptación de los datos seleccionados por el usuario, por ejemplo verificar que el primer criptograma H de este usuario ya no existe en la base de datos.
En tal caso, se pide al usuario que elija otra contraseña, por ejemplo.

[0028] Según una variante de la invención, es posible almacenar para cada primer criptograma H el identificador de referencia U o un derivado U" de este identificador de referencia.
Las otras informaciones, en particular la contraseña de referencia P, son borradas desde la terminación de la fase de inscripción.

[0029] El derivado U" del identificador corriente U es un valor resultante de una operación criptográfica sobre el identificador corriente U. Puede tratarse de una función de codificación F o de una función hash H1.
En este segundo caso, como la operación de elección arbitraria efectuada por el segundo servidor no es conocida por el primer servidor, se tratará de una función de tipo hash diferente.

Autentificación

[0030] Esta etapa es ilustrada por la figura 2.
En un segundo momento, el usuario se conecta al primer servidor S1 para acceder al servicio deseado.
El primer servidor S1 recibe el identificador corriente U' y la contraseña corriente P'.
El primer servidor S1 transmite estas informaciones al segundo servidor S2 de manera protegida.
Una vez recibido por el segundo servidor, este último ejecuta la función de sentido único Hash sobre el identificador corriente U' y la contraseña P', así como el parámetro de seguridad R para obtener un segundo criptograma H'. Éste reenvía este criptograma H' al primer servidor S1. Este último busca en su base de datos si existe un primer criptograma igual al segundo criptograma, y genera un mensaje de error si y solamente si no encuentra ningún rastro de este criptograma H'.
En el caso contrario, el primer servidor S1 puede autorizar el acceso al servicio deseado.

[0031] En caso de que sólo los criptogramas H de los usuarios que han pasado la fase de alistamiento se almacenen en el primer servidor S1, esta etapa de verificación de la existencia de una entrada en su base de datos no puede hacerse antes de la transmisión de los datos al segundo servidor.
En efecto, el primer servidor S1 no puede determinar si el identificador corriente ha sido registrado en el sistema.
Al realizarse las mismas operaciones para un identificador registrado que para un identificador no registrado, es imposible utilizar el sistema como un oráculo para determinar si un identificador ha sido registrado.

[0032] Si el primer servidor está conectado a varios ordenadores para la realización del servicio, el primer servidor transmitirá el identificador corriente U' (que es el mismo que el identificador de referencia U', puesto que la comparación es positiva) a los ordenadores con una información de autentificación positiva.
En caso de que el conjunto de recursos de los ordenadores funcione con un identificador de sistema único ID, el primer servidor S1 tiene una base de datos organizada en colección de registros, donde cada usuario representa un registro.
Un registro comprende un primer criptograma H y un identificador de sistema ID correspondiente.
En caso de verificación positiva, el primer servidor envía a un servidor de servicio el identificador de sistema (ID) con un mensaje que da fe de la verificación positiva del identificador corriente (U').

[0033] En la variante en la que el primer servidor conserva, con el primer criptograma de referencia H, el identificador de referencia U (o el derivado del identificador de referencia U"), el barrido de la base de datos del primer servidor no es necesario porque el criptograma de referencia H se puede recuperar directamente.
Si la base de datos protegida del primer servidor contiene el derivado U" del identificador de referencia U, el primer servidor realizará la operación criptográfica sobre el identificador de corriente U' para obtener el derivado del identificador corriente y aprovecharse de este dato para recuperar el criptograma de referencia H. Por lo tanto, la comparación puede hacerse entre el primer criptograma de referencia H y el segundo criptograma corriente H' recibido del segundo servidor S2.

[0034] En caso de que no encuentre ningún rastro de este identificador, genera un mensaje de error.

Se debe señalar que esta etapa de verificación de la existencia de una entrada en su base de datos puede hacerse antes de la transmisión de los datos al segundo servidor.
En efecto, si el identificador corriente no es conocido por el primer servidor, no es necesario verificar la contraseña que ha sido introducida por el usuario.

Actualización de las contraseñas

[0035] Una particularidad del sistema es poder permitir la actualización de los medios de seguridad sin modificar el valor de la contraseña.
Por ejemplo, se desea cambiar el parámetro de seguridad R o la función de sentido único Hash.

[0036] Con este fin, el segundo servidor S2 dispone del identificador de referencia U y de la contraseña P en forma cifrada.
La clave privada correspondiente a la clave asimétrica utilizada para el cifrado es extraída del lugar protegido o estaba almacenada y puesta a disposición del segundo servidor S2.

[0037] El procedimiento es el siguiente:

- el segundo servidor descifra un conjunto identificador/contraseña y calcula el primer criptograma como durante la fase de inscripción. Además, calcula un nuevo criptograma de referencia H" sobre la base de un nuevo valor del parámetro de seguridad R' o de una nueva función de sentido único, o incluso una combinación de los dos. Este nuevo criptograma H" se envía al primer servidor S1 con el primer criptograma H. En el caso de que el parámetro de seguridad R esté incluido con el conjunto identificador/contraseña, también es descifrado.
- el servidor S2 cifra igualmente el identificador de referencia U y la contraseña P según los nuevos parámetros (función de sentido único y/o parámetro de seguridad) con el método de cifrado asimétrico que toma como argumento una clave pública almacenada de dicho servidor S2, la clave privada correspondiente siendo almacenada de manera protegida fuera de la red (por ejemplo en una caja física). Según una variante, el conjunto cifrado puede comprender el parámetro de seguridad R, permitiendo de este modo saber qué parámetro ha sido utilizado para este usuario. Estos nuevos datos cifrados se almacenan en la base de datos del segundo servidor S2.
- tras la recepción de los dos criptogramas, el primer servidor S1 busca el criptograma de referencia H almacenado en su base de datos y lo reemplaza por el nuevo criptograma H". Así, los medios de seguridad pueden evolucionar sin que se solicite a los usuarios que vuelvan a iniciar la introducción de una contraseña.

Parámetro de seguridad

[0038] Varias versiones pueden ser previstas en el marco de la presente invención para el parámetro de seguridad R.
Como se ha indicado anteriormente, puede tratarse de un parámetro que es propio del segundo servidor S2 y que, por lo tanto, es almacenado en su memoria protegida.
Se utiliza para todos los cálculos del criptograma H, H'.

[0039] El objetivo principal del parámetro de seguridad R es adaptar el coste de cálculo de la función Hash a la tecnología de los atacantes y a la del servidor.
Por ejemplo, y respectivamente, si se descubre un nuevo método de ataque de diccionario o si el material del servidor S2 se actualiza con un procesador más potente.
El coste de cálculo se refiere por ejemplo al número de operaciones aritméticas o a la capacidad de almacenamiento (memoria) necesarios para la valoración de la función.

[0040] Según una variante, este parámetro puede variar en función del tipo de servicio que requiere el usuario y una información que indica el tipo de servicio Sn que acompaña al conjunto identificador / contraseña que es transmitido al segundo servidor por el primer servidor.
Esto permite recuperar el parámetro de seguridad propio de este servicio (R1, R2 ... Rn) en la memoria protegida del segundo servidor que ha de calcular el criptograma.

[0041] Según otra variante, el parámetro de seguridad R pertenece a un identificador de referencia Un y, por lo tanto, propio de un usuario.
Durante la fase de inscripción, un parámetro Rn es generado por una función aleatoria por el segundo servidor S2 desde la recepción del conjunto identificador/contraseña.
Es entonces necesario que el segundo servidor S2 pueda recuperar el parámetro de seguridad Rn durante la fase de autentificación.
Con este fin, el segundo servidor memorizará el parámetro de seguridad Rn propio de un identificador Un en su base de datos.

[0042] Por supuesto, puede almacenar simplemente el conjunto Un, Rn en una memoria protegida.

Sin embargo, es preferible que el identificador Un no sea almacenado en claro y, por lo tanto, una función de sentido único H' sea efectuada sobre el identificador Un para obtener un criptograma H'(Un) H'(Un).
La memoria protegida del segundo servidor almacenará el conjunto H'(Un) H'(Un), Rn.

[0043] Aunque estos datos fueran extraídos de la memoria por una persona malintencionada, no le sería posible recuperar el valor del identificador Un.

[0044] Durante la fase de autentificación, el segundo servidor, una vez que ha recibido el conjunto identificador/contraseña corriente del primer servidor, ejecuta la función de sentido único H' sobre el identificador corriente U'.
Podrá así recuperar en su base de datos el parámetro de seguridad Rn relativo a este identificador y calcular el criptograma C'.

Función de sentido único

[0045] Existen varios tipos de función de sentido único.
Se llama función hash a una función particular que, a partir de un dato proporcionado en entrada, calcula una huella para identificar rápidamente, aunque que de manera incompleta, el dato inicial.
Las funciones hash son comúnmente utilizadas para la implementación de estructuras de datos y de protocolos criptográficos.

[0046] Una contraseña no debe ser almacenada en claro en una máquina por razones de seguridad. Sólo el resultado de la elección arbitraria de la contraseña es por lo tanto almacenado.
Para identificar un usuario, el ordenador compara la huella de la contraseña de origen (almacenada) con la huella de la contraseña solicitada. Sin embargo, esta realización no es completamente satisfactoria. Si dos usuarios deciden utilizar la misma contraseña, entonces el compendio obtenido será idéntico. Este fallo es potencialmente utilizable por tres métodos:

ataque de diccionario

ataque de fuerza bruta

ataque con tablas arcoíris (rainbow tables)

[0047] Durante un ataque de diccionario, se podría deducir razonablemente que la contraseña elegida por los dos usuarios es relativamente fácil de memorizar.

[0048] Para contrarrestar este tipo de ataque, se agrega un componente aleatorio (parámetro de seguridad R) durante la generación inicial de la huella. Este componente, también llamado « sal », es a menudo almacenado en claro. La contraseña es a continuación mezclada con el parámetro de seguridad R, esta etapa varía según el sistema utilizado. Un método sencillo es concatenar la contraseña con el parámetro de seguridad R. En caso de que el parámetro de seguridad R no sea idéntico para dos usuarios, se obtendrán dos firmas diferentes con la misma contraseña.
Eso reduce fuertemente el margen de un ataque mediante tabla arcoíris, pero no protege contra los ataques de diccionario o de fuerza bruta.

[0049] Los algoritmos SHA-1 (Secure Hash Algorithm 1: 160 bits) y MD5 (Message-Digest Algorithm 5,128 bits, más antiguo y menos seguro) son funciones hash utilizadas frecuentemente.
Los estándares SHA-2 y SHA-3 (224, 256, 384, o 512 bits) están disponibles para reemplazar SHA-1.

[0050] También existen funciones hash dependientes de una clave. Este es el caso, por ejemplo, del algoritmo HMAC-SHA-1, que utiliza SHA-1 en la construcción HMAC para aceptar una clave como parámetro. El parámetro de seguridad R puede desempeñar el papel de clave en este tipo de función dependiente de una clave.

[0051] Otros algoritmos criptográficos optimizados para las contraseñas tales como bcrypt o scrypt pueden ser utilizados. Bcrypt es una función criptográfica creada por Niels Provos y David Mazières y se basa en el algoritmo de cifrado Blowfish.
Además del uso de un parámetro de seguridad para protegerse de los ataques por tabla arcoíris (rainbow table), bcrypt es una función adaptativa, es decir, que se puede aumentar el número de iteraciones para volverla más lenta.
De este modo, sigue siendo resistente a los ataques por búsqueda exhaustiva a pesar del aumento de la potencia de cálculo.

REIVINDICACIONES

1. Método de autentificación de un usuario que implementa un primer servidor (S1) conectado a una red pública y un segundo servidor (S2), conectado al primer servidor (S1) pero no conectado a la red pública, este método que comprende una etapa de inscripción que comprende:
- recepción por el primer servidor (S1) de un identificador de referencia (U) y de una contraseña de referencia (P),
- transmisión del identificador de referencia (U) y de la contraseña de referencia (P) al segundo servidor (S2),
- carga de un parámetro de seguridad (R) por el segundo servidor (S2),
- cálculo de un primer criptograma (H) por una función de sentido único (hash) sobre el identificador de referencia (U), la contraseña de referencia (P), y el parámetro de seguridad (R) por el segundo servidor (S2),
- cifrado de por lo menos el identificador de referencia (U) y la contraseña de referencia (P) utilizando un método de cifrado asimétrico que toma como argumento una clave pública, y almacenamiento de los datos cifrados por el segundo servidor (S2),
- reenvío al primer servidor del primer criptograma (H) y almacenamiento de dicho criptograma por el primer servidor (S1), y una etapa de verificación de un usuario que comprende:
- recepción por el primer servidor (S1) del identificador corriente (U') y de la contraseña corriente (P'),
- transmisión del identificador corriente (U') y de la contraseña corriente (P') al segundo servidor (S2),
- cálculo de un segundo criptograma (H') por la función de sentido único (hash) sobre el identificador corriente (U'), la contraseña corriente (P') y el parámetro de seguridad (R) por el segundo servidor (S2),
- reenvío al primer servidor del segundo criptograma (H') y verificación de que el segundo criptograma (H') está incluido en su base de datos, en caso contrario, generación de un mensaje de error.

2. Método según la reivindicación 1, **caracterizado por el hecho de que** el segundo servidor (S2) induye el parámetro de seguridad (R) en el cifrado del identificador de referencia (U) y de la contraseña (P).

3. Método según la reivindicación 1 o 2, **caracterizado por el hecho de que** la verificación de que el segundo criptograma (H') está incluido en su base de datos comprende una etapa de barrido de la base de datos para encontrar un primer criptograma (H) idéntico al segundo criptograma (H').

4. Método según la reivindicación 1 o 2**, caracterizado por el hecho de que** el primer servidor (S1), durante la inscripción, almacena un registro que comprende el primer criptograma (H) y el identificador de referencia (U) o un derivado del identificador de referencia (U") y de que la verificación de que el segundo criptograma (H') está incluido en su base de datos comprende una etapa previa de determinación del registro correspondiente al identificador corriente (U') recibido y del criptograma de referencia (H) asociado a dicho identificador corriente (U').

5. Método según la reivindicación 1 o 2, **caracterizado por el hecho de** que el primer servidor (S1), durante la inscripción, almacena un registro que comprende el primer criptograma (H) y un identificador de sistema (ID) y por el hecho de que, en caso de verificación positiva, envía a un servidor de servicio el identificador de sistema (ID) con un mensaje que da fe de la verificación positiva del identificador corriente (U').

6. Método según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** comprende una etapa de renovación de los criptogramas de referencia (H) almacenados en el primer servidor, por el uso de una nueva función de sentido único y/o un nuevo parámetro de seguridad (R') que comprende las etapas de:
- obtención por el segundo servidor (S2) de la clave privada correspondiente a la clave pública,
- descifrado del identificador de referencia (U) y de la contraseña (P) mediante la clave privada,
- cálculo del primer criptograma (H) por la función de sentido único (hash) sobre el identificador de referencia (U), la contraseña de referencia (P), y el parámetro de seguridad (R) por el segundo servidor (S2),
- cálculo de un nuevo criptograma (H") por la nueva función de sentido único sobre el identificador de referencia (U), la contraseña de referencia (P), y el nuevo parámetro de seguridad (R') por el segundo servidor (S2),
- envío del primer criptograma (H) y del nuevo criptograma (H") al primer servidor (S1),
- reemplazo por el primer servidor (S1) del primer criptograma (H) por el nuevo criptograma (H").

7. Método según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** la comunicación entre el primer servidor (S1) y el segundo servidor (S2) es cifrada.

8. Sistema de autentificación de un usuario que comprende un primer servidor (S1) conectado a una red pública que comprende una primera base de datos y un segundo servidor (S2) que comprende una segunda base de datos, dicho segundo servidor (S2) estando conectado al primer servidor (S1) pero no conectado a la red pública, el primer servidor (S1) que induye medios para:
- recibir un identificador de referencia (U) y una contraseña de referencia (P),
- transmitir el identificador de referencia (U) y la contraseña de referencia (P) al segundo servidor (S2),
- recibir y almacenar en la primera base de datos un primer criptograma (H) relativo a dichos identificador de

referencia (U) y contraseña de referencia (P),
- recibir un identificador corriente (U') y una contraseña corriente (P'),
- transmitir el identificador corriente (U') y una contraseña corriente (P') al segundo servidor (S2),
- recibir un segundo criptograma (H') relativo a dichos identificador corriente (U') y una contraseña corriente (P'),
- verificar en la primera base de datos la presencia de uno de dichos primeros criptogramas (H) de igual valor que el segundo criptograma (H') y, en caso positivo,
- envío de un mensaje que da fe de la verificación positiva, el segundo servidor (S2) que comprende medios para:
- recibir el identificador de referencia (U) y la contraseña de referencia (P) del primer servidor (S1),
- cargar un parámetro de seguridad (R),
- calcular el primer criptograma (H) por una función de sentido único sobre el identificador de referencia (U), la contraseña de referencia (P), y el parámetro de seguridad (R),
- cifrar el identificador de referencia (U) y la contraseña de referencia (P) utilizando un método de cifrado asimétrico que toma como argumento una clave pública, y almacenar estos datos cifrados en la segunda base de datos,
- reenviar al primer servidor el primer criptograma (H),
- recibir el identificador corriente (U') y la contraseña corriente (P') del primer servidor (S1),
- cargar el parámetro de seguridad (R),
- calcular el segundo criptograma (H') por la función de sentido único sobre el identificador corriente (U'), la contraseña corriente (P') y el parámetro de seguridad (R),
- reenviar al primer servidor (S1) el segundo criptograma (H').

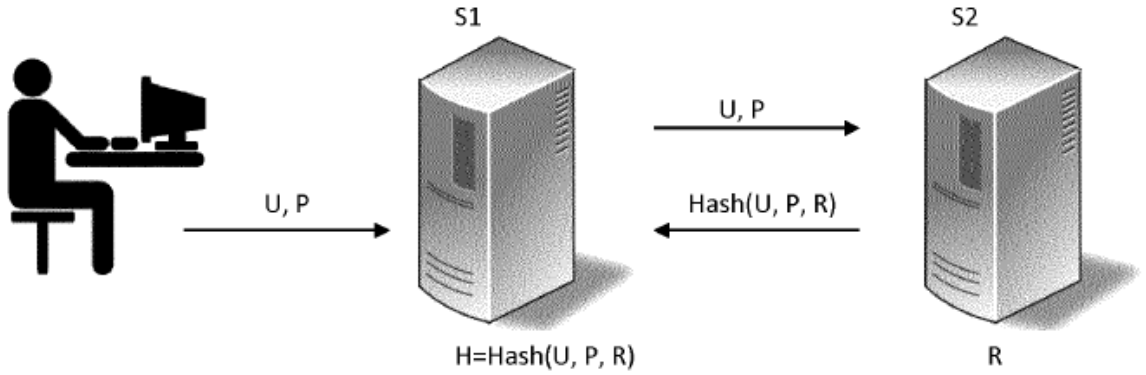

Fig. 1

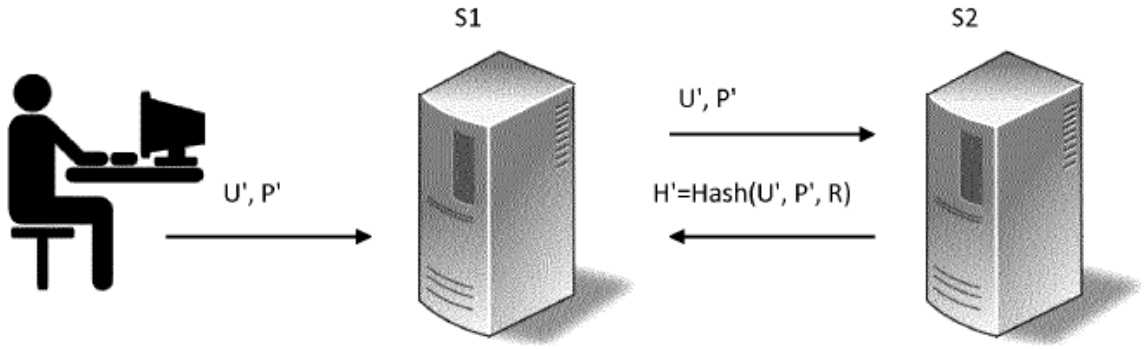

Fig. 2