(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 714 784**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.09.2006 PCT/CN2006/002329**

(87) Fecha y número de publicación internacional: **15.03.2007 WO07028342**

(96) Fecha de presentación y número de la solicitud europea: **08.09.2006 E 06775633 (8)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2018 EP 1906584**

(54) Título: **Procedimiento, sistema y dispositivo de transmisión de datos de juego**

(30) Prioridad:

10.09.2005 CN 200510037255

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.05.2019

(73) Titular/es:

TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED (100.0%)
4/F., East 2 Block, SEG Park, Zhenxing Rd., Futian District Shenzhen
Guangdon 518044, CN

(72) Inventor/es:

WANG, HAIBING;
GUO, BIJIAN y
YANG, XIAOHU

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento, sistema y dispositivo de transmisión de datos de juego

Campo de la invención

La presente invención se refiere a la tecnología de comunicación por ordenador y, en particular, se refiere a un procedimiento y sistema para la transmisión de datos de juego y el correspondiente aparato del cliente y servidor.

Antecedentes de la invención

Flash es un lenguaje de programa de animación usado en internet. Flash adopta la tecnología de medios de transmisión en red y, por lo tanto, está fuera de la restricción del ancho de banda de la red. Flash puede proporcionar animación en redes a mayor velocidad, realizar interacciones animadas, dar libertad a la creatividad e imaginación de las personas, y proporcionar las páginas web más hermosas, presentaciones animadas vívidas y juegos interactivos. El juego Flash existente implementa las lógicas del juego en terminales de clientes individuales mediante el uso de la tecnología Flash, y proporciona una interfaz en un nivel más alto para que la comunicación en red transmita los datos de los resultados del juego de manera unidireccional a otros ordenadores, como se muestra en la figura 1 en la que se considera que el remitente de los datos del resultado del juego es un cliente y el receptor como un servidor. En la actualidad dos formas son utilizadas generalmente para la transmisión de datos de juego. De acuerdo con la primera forma, un servidor web estándar y una aplicación web se dispondrán en el lado del servidor. La aplicación web puede utilizar un lenguaje de página web dinámico, tal como el lenguaje Common Gateway Interface (CGI), el lenguaje Active Server Pages (ASP), el lenguaje Java Server Pages (JSP) o el lenguaje de preprocesador de hipertexto (PHP). La aplicación Flash en el lado del cliente invoca la aplicación web utilizando un Localizador Uniforme de Recursos (URL), y la aplicación web recibe los datos de la aplicación Flash a través del URL. La segunda forma utiliza una interfaz de comunicación de red de conectores en el motor de Flash, es decir, un conector de lenguaje de marcado extensible (XML). De acuerdo con la segunda forma, el remitente encapsula los datos en mensajes XML antes de enviar los datos al lado del servidor. El lado del servidor escucha en un puerto acordado previamente, recibe los datos enviados desde el lado del cliente en el puerto y analiza los mensajes XML para recuperar los datos.

Se puede ver que los terminales de cliente de los juegos Flash existentes envían los datos finales del juego a los servidores y los servidores confían incondicionalmente en los datos de los terminales de cliente. Los terminales de cliente no tienen lógicas confiables para garantizar la validez y exactitud de los datos de juego y, por lo tanto, no tienen medios para proteger los datos de resultados del juego para que no sean falsificados o manipulados.

El documento US 6152824 A revela un sistema y proceso de juego de ordenador en línea en red, organizado en una arquitectura de juego en línea cliente / servidor y utilizado para ejecutar programas de juego. Los ordenadores del servidor ejecutan programas del servidor que incluyen un programa de control maestro (MCP) que gobierna el acceso de los programas del servidor a la arquitectura de juegos en línea, un programa servorum (SV) para crear instancias de un programa servidor, un programa emparejador (MM) que soporta servicios de reuniones, un programa servidor de clase de instancias de juego (GICS) que permite juegos y proporciona comunicación de usuario a usuario, y un programa servidor de protocolo de nivel superior (GULP) que soporta la comunicación de usuario a usuario proporcionada por el citado GICS.

El documento US 2002/133707 A1 revela procedimientos y sistemas para distribuir software de forma segura en un entorno en base a suscripciones. En una realización de ejemplo, un Equipo de Seguridad de Juego ("GSF") asociada con un servidor de juegos se usa para administrar comunicaciones seguras con los clientes del juego. El GSF generalmente administra la comunicación segura de la información de contabilidad y facturación y la comunicación segura de los datos de la sesión de juego.

El Tribunal de Distrito de los Estados Unidos, E.D. Missouri: "Memorándum y Orden, Davidson & Associates Inc. vs. Internet Gateway" revela que para iniciar sesión en el servicio de Battle.net y acceder al modo Battle.net, el juego inicia una secuencia de autenticación o un "saludo secreto" entre el juego y el servidor de Battle.net

El documento US 2003/229779 A1 revela una implementación ejemplar de una pasarela de seguridad para una operación de juegos en línea en base a consola que funciona como una pasarela entre una red pública (por ejemplo, Internet) y una red privada (por ejemplo, una red de centro de datos interna). La pasarela de seguridad permite establecer canales de comunicación seguros con las consolas de juegos a través de la red pública, y permite la comunicación segura entre las consolas de juegos en la red pública y los dispositivos de servicio en la red privada.

Sumario

La presente invención proporciona un procedimiento, sistema y aparato para la transmisión de datos de juego tal como se define en las reivindicaciones independientes, para resolver el problema en el juego Flash existente de que un terminal cliente no tiene lógicas confiables para garantizar la validez y precisión de los datos de juego ni medios

para evitar que los datos de juego sean falsificados o manipulados durante la transmisión de los datos de juego a un servidor.

El procedimiento proporcionado por la presente invención para la transmisión de datos de juego incluye:

adquirir por un cliente (100) al iniciar sesión (1) en un servidor (200) una clave de sesión asignada por el servidor (200) y verificar si se recibe la clave de sesión asignada por el servidor (200) y lanzar (3), por el cliente (100), un programa de juego si la clave de sesión es recibida, que en caso contrario impediría que se lanzase el programa de juego,

en el que la clave de sesión es generada cambiando los datos de bits que contienen una ID de cliente del cliente (100) y un tiempo de conexión del cliente (100) de acuerdo con una regla, y además se insertan bytes y se realiza una operación a nivel de bits sobre los datos de bits;

generar, por el cliente (100), una recopilación de resultados en base a los datos de juego que se enviarán, el tiempo de someter los datos de juego y la clave de la sesión mediante el uso de un algoritmo MD5, y el envío de los datos de juego, el tiempo de someter los datos de juego, la clave de la sesión y el resumen de los resultados generados al servidor (200); y

generar otro resumen de resultados por el servidor (200) en base a los datos recibidos del juego, el tiempo de someter los datos de juego por el cliente (100) y la clave de sesión utilizando el mismo algoritmo MD5 usado por el cliente (100), comparar el resumen de resultados generado por el servidor (200) con el resumen de resultados del cliente (100), y considerar los datos de juego como válidos si los dos resúmenes de resultados son idénticos.

La presente invención proporciona un sistema, así como el procedimiento, para la transmisión de datos de juego, que incluye:

un servidor (200) como se reivindica en cualquiera de las reivindicaciones 9 a 11, y un cliente (100) como se reivindica en cualquiera de las reivindicaciones 5 a 7 en comunicación con el servidor (200).

Un aparato cliente (100) en el sistema que se ha descrito en la descripción anterior, que incluye:

un primer módulo de interfaz (101), adaptado para intercambiar datos entre el cliente (100) y un servidor (200);

un módulo de solicitud de autenticación (102), adaptado para iniciar sesión en el servidor (200) a través del primer módulo de interfaz (101) y adquirir una clave de sesión asignada por el servidor (200), verificar si la clave de sesión asignada por el servidor (200) es recibida e invocar un módulo de aplicación (103) para lanzar un programa de juego si se recibe la clave de sesión; en caso contrario, evitar que se lance el programa de juego.

en el que la clave de sesión es generada cambiando los datos de bits que contienen una ID de cliente del cliente (100) y un tiempo de conexión del cliente (100) de acuerdo con una regla, y además insertar bytes y realizar una operación a nivel de bits sobre los datos de bits;

el módulo de aplicación (103), adaptado para recibir la clave de sesión del servidor (200) a través del módulo de solicitud de autenticación (102), ejecuta un programa de juego y envía datos de juego cifrados al servidor (200) a través del primer módulo de interfaz (101) cuando se requiere que se envíen los datos de juego, de modo que el servidor (200) descifre y verifique los datos recibidos del juego, y guarde los datos de juego si se demuestra que los datos de juego son válidos; y

un primer módulo (104) adaptado para generar un resumen de resultados en base a los datos de juego que se enviarán, el tiempo de someter los datos de juego y la clave de la sesión mediante el uso de un algoritmo MD5, y enviar los datos de juego, el tiempo de someter los datos de juego, la clave de sesión y el resumen de resultados generado al módulo de aplicación (103).

Un servidor (200) en el sistema que se ha descrito en la descripción anterior, que incluye:

un segundo módulo de interfaz (201), adaptado para intercambiar datos entre el servidor (200) y un cliente (100);

un módulo de confirmación de autenticación (202), adaptado para asignar una clave de sesión al cliente (100) a través del segundo módulo de interfaz (201) para que el cliente (100) lance un programa de juego si se recibe la clave de sesión y, en caso contrario, impedir que el programa de juego se lance, en el que la clave de sesión es generada al cambiar los datos de bits que contienen una ID de cliente del cliente (100) y

un tiempo de conexión del cliente (100) de acuerdo con una regla, y además insertar bytes y realizar una operación a nivel de bits en los datos de bits;

un módulo de almacenamiento de datos (205), adaptado para guardar los datos de juego que han probado que son válidos por el módulo de descifrado de datos (203);

un módulo (203) adaptado para generar otro resumen de resultados en base a los datos recibidos del juego, el tiempo de envío de los datos de juego por parte del cliente (100) y la clave de sesión utilizando el mismo algoritmo MD5 utilizado por el cliente (100), comparar el resumen de resultados generado por sí mismo con un resumen de resultados del cliente (100), y considerar los datos de juego como válidos si los dos resúmenes de resultados son idénticos.

La presente invención también describe un terminal móvil que contiene el aparato cliente (100) que se ha descrito en la descripción anterior.

El procedimiento de la presente invención garantiza que el cliente puede transmitir datos de juego de manera segura al servidor y protege los datos de juego para que no sean manipulados o falsificados.

Breve descripción de los dibujos

La figura 1 es un esquema de la transmisión de datos de juego Flash en la técnica anterior;

La figura 2 es un diagrama de flujo de la transmisión de datos de juego Flash en una realización preferida de la presente invención;

La figura 3 es un diagrama de estructura del sistema proporcionado por una realización preferida de la presente invención para la transmisión de datos de juego Flash.

Realizaciones de la invención

La presente invención se explica adicionalmente en la presente memoria descriptiva y en lo que sigue con referencia a los dibujos que se acompañan, así como a las realizaciones para hacer más evidentes el objetivo, la solución técnica y sus méritos. Se debe entender que las realizaciones en la presente memoria descriptiva se usan solo para ilustrar la presente invención y no se deben usar para limitar el alcance de protección de la presente invención.

En una realización preferida de la presente invención, el cifrado se adopta en la etapa de lanzamiento y en la etapa de ejecución lógica del guión de un juego para garantizar la seguridad de los datos de juego. La realización se puede aplicar a los juegos lanzados a los clientes por los usuarios y en los que los usuarios necesitan cargar los datos de juego a los servidores para grabar, por ejemplo, juegos Flash.

La figura 2 muestra el flujo de transmisión de datos de juego en la realización.

Etapa 1: un cliente inicia sesión en un servidor utilizando una identidad (ID) asignada de antemano.

El experto en el campo puede comprender que la ID utilizada por el cliente se puede obtener en el proceso normal de registro de usuarios. También se puede configurar una contraseña correspondiente a la ID de usuario en el proceso de registro de usuario para evitar que la ID de usuario sea robada. Cuando se configura una contraseña, el cliente utilizará la contraseña y el ID de usuario para iniciar sesión en el servidor en esta etapa.

Etapa 2: el servidor genera una clave de sesión y devuelve la clave de sesión al cliente.

En la etapa anterior, si el cliente proporciona una contraseña durante el registro, el servidor en primer lugar verificará la identidad del cliente que se está registrando en base a la contraseña. Y este etapa se realizará solo cuando se demuestre que la identidad del cliente es válida; en caso contrario, se informará al cliente que la contraseña es incorrecta.

La clave de sesión generada en esta etapa es una cadena generada por el servidor en base a la identidad del cliente, por ejemplo, la ID de usuario o el nombre de usuario, y el tiempo de conexión del cliente mediante el uso de un algoritmo de cifrado predeterminado.

En esta etapa, el algoritmo de cifrado convierte la información de texto claro y significativo en texto cifrado irreconocible sin sentido mediante el desplazamiento de los datos de bits que representan la ID del cliente y el tiempo de conexión de acuerdo con una regla determinada, y la inserción adicional de bytes y la operación a nivel de bits en los datos de bits.

Etapa 3: el cliente inicia el programa de juego Flash correspondiente al recibir la clave de sesión del servidor.

En esta realización, el cliente puede verificar además si la clave de sesión es recibida antes de lanzar el programa de juego Flash para mantener a los usuarios ilegales fuera del juego. La comprobación incluye: verificar, mediante el guión del programa Flash, si se recibe la clave de sesión del servidor, y evitar que se lance el programa de juego si el cliente no tiene la clave de sesión o lanzar el programa de juego si el cliente ha recibido clave de sesión Por lo tanto, se puede garantizar que el cliente autorizado por el servidor solo lanzará el juego en un entorno servidor por el cliente autorizado por el servidor, de modo que los usuarios ilegales se mantengan fuera del juego y no puedan manipular los datos de juego.

Etapa 4: cuando el cliente necesita enviar datos de juego al servidor, el cliente cifra los datos de juego con la clave de sesión del servidor.

En esta etapa, el cliente puede generar un resumen de resultados en base a los datos de juego que se enviarán, el momento actual y la clave de la sesión mediante el uso de un algoritmo MD5, y enviar los datos de juego, el momento actual, la clave de la sesión y el resumen de resultados generado. al servidor.

Etapa 5: el cliente carga los datos de juego encriptados al servidor.

Etapa 6: al recibir los datos de juego del cliente, el servidor descifra los datos de juego y verifica si los datos del resultado del juego del cliente son válidos, y guarda los datos de juego si se demuestra que son válidos.

En esta etapa, al recibir los datos de juego, el momento actual, la clave de la sesión y el resumen de resultados del cliente, el servidor genera otro resumen de resultados utilizando el mismo algoritmo MD5 y compara el resumen de resultados recién generado con el resumen de resultados del cliente; Si los dos resúmenes de resultados son idénticos, los datos de juego se considerarán válidos.

El tiempo de conexión del usuario sometido por el cliente puede compararse con el momento actual en el servidor para verificar si el registro de usuario ha caducado, es decir, para verificar si el tiempo de conexión del usuario está dentro del límite de caducidad predeterminado, si el registro del usuario ha caducado, los datos de juego recibidos se considerarán como no válidos.

De acuerdo con la presente invención, como un medio para evitar la falsificación de datos de juego hecha por los usuarios maliciosos, la conversión de características se puede aplicar a los datos de juego generados por el juego Flash antes o después de la etapa de cifrado, por ejemplo, características como el formato o la presentación de los datos de juego se convierten de acuerdo con los criterios del servidor o de acuerdo con un acuerdo entre el cliente y el servidor, por lo que se puede garantizar que los datos se generan mediante la lógica del juego Flash y no se falsifican fuera del juego. En consecuencia, el servidor aplicará una conversión de características inversa a los datos de juego recibidos antes o después de la etapa de descifrado para restaurar y guardar los datos.

La figura 3 muestra la estructura de un sistema en una realización preferida de la presente invención para la transmisión de datos de juego. Como se muestra en la figura 3, el sistema incluye un Cliente 100 y un Servidor 200, en los cuales el Cliente 100 se comunica con el Servidor 200 a través de Internet. El Cliente 100 y el Servidor 200 pueden estar conectados por otros medios además de Internet. El Cliente 100 puede ser cualquier tipo de dispositivo terminal, por ejemplo, un terminal móvil tal como un teléfono móvil o asistente digital personal, o un terminal fijo tal como un ordenador personal. El servidor 200 puede ser un servidor grande, mediano o pequeño.

El procedimiento para la comunicación entre el Cliente 100 y el Servidor 200 se muestra en el proceso de transmisión de datos de juego en la figura 2.

En lo que se refiere a los componentes internos del Cliente 100 y del Servidor 200, el Cliente 100 puede incluir: Un Primer Módulo de Interfaz 101, conectado al servidor 200 y utilizado para el intercambio de datos entre el cliente 100 y el servidor 200.

Un Módulo de Solicitud de Autentificación 102, conectado al Primer Módulo de Interfaz 101 y un Módulo de Aplicación 103, son utilizados para iniciar sesión en el Servidor 200 utilizando una identificación de usuario, recibir una clave de sesión del servidor e invocar el Módulo de Aplicación 103 utilizando la clave de sesión recibida para lanzar una aplicación Flash u otro programa de juego.

El Módulo de Aplicación 103, conectado al Primer Módulo de Interfaz 101, son utilizados para ejecutar una aplicación Flash fijada localmente en el Cliente 100 o un programa de aplicación descargado por el Cliente 100 desde el Servidor 200 después de iniciar sesión en el Servidor 200, por ejemplo, ejecutando un juego Flash en una página web del Servidor 200 después de iniciar sesión en la página web del Servidor 200; y además, para enviar datos de juego encriptados al Servidor 200 a través del Primer Módulo de Interfaz 101 cuando los datos de juego deben ser enviados al Servidor 200.

Un Módulo de Cifrado de Datos 104, conectado al Módulo de Aplicación 103, es utilizado para cifrar los datos de juego del Módulo de Aplicación 103 con la clave de sesión del Servidor 200 cuando el Cliente 100 necesita enviar

los datos de juego al Servidor 200 y devolver los datos de juego cifrados al Módulo de Aplicación 103 para su posterior transmisión al Servidor 200.

El Módulo de Cifrado de Datos 104 puede cifrar los datos de juego utilizando el algoritmo de cifrado descrito en la Etapa 4 anterior.

En esta realización, como un medio para evitar que los usuarios ilegales se introduzcan en el juego y manipulen los datos de juego, el guión del programa Flash, antes de que el Módulo de Aplicación 103 ejecute la aplicación Flash, debería verificar si la clave de sesión ha sido recibida del Módulo de Petición de Solicitud 102. Si no se ha recibido una clave de sesión, se evitará que el juego sea lanzado. Por lo tanto, se puede garantizar que el juego solo se pueda lanzar en el entorno del Servidor 200 por el cliente autorizado por el Servidor 200.

El servidor 200 incluye los siguientes módulos internos:

Un Segundo Módulo de Interfaz 201, conectado al Cliente 100 y utilizado para el intercambio de datos entre el Cliente 100 y el Servidor 200.

Un Módulo de Confirmación de Autentificación 202, conectado al Segundo Módulo de Interfaz 201 y utilizado para asignar una clave de sesión al Cliente 100, mientras el Cliente 100 inicia sesión y enviar la clave de la sesión al Cliente 100 a través del Segundo Módulo de Interfaz 201.

Cuando el cliente envía una contraseña, así como la ID de usuario mientras se está registrando, el Módulo de Confirmación de Autenticación 202 también verificará la identidad del cliente en base a la ID de usuario y la contraseña, y la clave de sesión se asignará al cliente solo después de que se demuestre que el cliente es válido.

En esta realización, la clave de sesión es una cadena generada por el Módulo de Confirmación de Autenticación 202 en base a la identidad del Cliente 100, por ejemplo, la ID de usuario o el nombre de usuario, y el tiempo de conexión del cliente mediante el uso de un algoritmo de cifrado predeterminado.

Un Módulo de Descifrado de Datos 203, conectado al Segundo Módulo de Interfaz 201 y es utilizado para recibir datos de juego del Cliente 100, el descifrado de los datos de juego recibidos y la verificación de si los datos de juego del Cliente 100 son válidos.

El Módulo de Descifrado de Datos 203 puede verificar la validez de los datos de juego recibidos a través del proceso de verificación que se ha descrito en la Etapa 6.

Un Módulo de Almacenamiento de Datos 204, conectado al Módulo de Descifrado de Datos 203 es utilizado para guardar los datos de juego que son del Cliente 100 y que el Módulo de Descifrado de Datos 203 prueba que son válidos.

En esta realización, el módulo puede ser cualquier tipo de medio de almacenamiento en el Servidor 200, por ejemplo, la memoria del sistema o el espacio de almacenamiento asignado al Cliente 100 en un disco duro.

El Cliente 100 puede incluir además un Módulo de Conversión de Datos 105 para evitar que los usuarios maliciosos falsifiquen los datos de juego. El Módulo de Conversión de Datos 105 está conectado al Módulo de Aplicación 103 y se utiliza para aplicar la conversión de características al formato o presentación de los datos de juego antes o después del cifrado de los datos de juego de acuerdo con los criterios del Servidor 200 o de un acuerdo entre el Cliente 100 y el Servidor 200. Por lo tanto, se puede garantizar que los datos no se falsifiquen fuera del juego, sino que se generen mediante la lógica del juego Flash. En consecuencia, el Servidor 200 puede incluir además un Módulo de Conversión de Datos Inversos 205, que está conectado al Módulo de Descifrado de Datos 203 y se utiliza para aplicar, antes o después del descifrado de los datos de juego, la conversión inversa de características a los datos de juego del Cliente 100 para restaurar los datos y enviar los datos al Módulo de Almacenamiento de Datos 204 por medio del Módulo de Descifrado de Datos 203.

Se debe tener en cuenta que, aunque las realizaciones preferidas se describen en función de los juegos Flash, el procedimiento de transmisión de datos de juego, el sistema, el cliente y el servidor proporcionados por las realizaciones pueden aplicarse a la transmisión de datos de otros juegos sin exceder el alcance de protección de la presente invención. Cualquier modificación, reemplazo equivalente y mejora realizada bajo los principios de la presente invención tal como se define en las reivindicaciones debe incluirse en el alcance de protección de la misma.

REIVINDICACIONES

1. Un procedimiento de transmisión de datos de juego, que comprende:

adquirir por un cliente (100) al iniciar sesión (1) en un servidor (200), una clave de sesión asignada por el servidor (200), y verificar si la clave de sesión asignada por el servidor (200) es recibida, y lanzar (3), por parte del cliente (100), un programa de juego si se recibe la clave de sesión; en caso contrario, evitar que se lance el programa de juego, en el que la clave de sesión es generada al cambiar los datos de bits que contienen una ID de cliente del cliente (100) y un tiempo de conexión del cliente (100) de acuerdo con una regla, y además insertar bytes y realizar una operación a nivel de bits en los datos de bits;

generar por el cliente (100), un resumen de resultados en base a los datos de juego generados en el programa de juego que se enviará, el tiempo de someter los datos de juego y la clave de la sesión mediante el uso de un algoritmo MD5, y enviar los datos de juego, el tiempo de someter los datos de juego, la clave de la sesión y el resumen de resultados generado al servidor (200); y

generar otro resumen de resultados por el servidor (200) en base a los datos recibidos del juego, el tiempo de someter los datos de juego por el cliente (100) y la clave de sesión utilizando el mismo algoritmo MD5 usado por el cliente (100), comparar el resumen de resultados generado por el servidor (200) con el resumen de resultados del cliente (100), considerar los datos de juego como válidos si los dos resúmenes de resultados son idénticos, y guardar los datos de juego que han probado que son válidos.

2. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

aplicar por el cliente (100), la conversión de características a los datos de juego que se enviarán al servidor (200); y

aplicar por el servidor (200), la conversión inversa de características a los datos de juego recibidos por el servidor (200).

3. El procedimiento de acuerdo con la reivindicación 1, antes de lanzar el programa de juego, que comprende además:

verificar si se recibe la clave de sesión asignada por el servidor (200), y lanzar (3) el programa de juego si se recibe la clave de sesión, que en caso contrario impide que se lance el programa de juego.

4. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

cuando el resumen de resultados generado por el servidor (200) es idéntico al resumen de resultados del cliente (100), comparar el tiempo de conexión del cliente (100) con el momento actual en el servidor (200), verificar si el tiempo de conexión del cliente (100) está dentro de un límite de caducidad predeterminado, en caso afirmativo, considerar los datos de juego recibidos como válidos, en caso contrario considerar los datos de juego recibidos como no válidos

5. Un aparato cliente (100), que comprende:

un primer módulo de interfaz (101), adaptado para intercambiar datos entre el cliente (100) y un servidor (200);

un módulo de solicitud de autenticación (102), adaptado para iniciar sesión en el servidor (200) por medio del primer módulo de interfaz (101) y adquirir una clave de sesión asignada por el servidor (200), verificar que la clave de sesión asignada por el servidor (200) es recibida, e invocar un módulo de aplicación (103) para lanzar un programa de juego si se recibe la clave de sesión; en caso contrario, impedir que se lance el programa de juego, en el que la clave de sesión es generada al cambiar los datos de bits que contienen una ID de cliente del cliente (100) y un tiempo de conexión del cliente (100) de acuerdo con una regla, y además insertar bytes y realizar una operación a nivel de bits en los datos de bits;

el módulo de aplicación (103), adaptado para recibir la clave de sesión del servidor (200) a través del módulo de solicitud de autenticación (102), ejecuta el programa del juego y envía los datos de juego cifrados al servidor (200) a través del primer módulo de interfaz (101) cuando se requiere que se envíen los datos de juego, de modo que el servidor (200) descifra y verifica los datos recibidos del juego, y guarda los datos de juego si se demuestra que los datos de juego son válidos; y

un primer módulo (104), adaptado para generar un resumen de resultados en base a los datos de juego generados por el programa de juego que se enviará, el tiempo de someter los datos de juego y la clave de la sesión utilizando un algoritmo MD5, y enviar los datos de juego, el tiempo de someter los datos de juego, la clave de la sesión y el resumen de resultados generado al módulo de aplicación (103).

6. El aparato cliente (100) de acuerdo con la reivindicación 5, que comprende además:

un módulo de conversión de datos (105), adaptado para aplicar una conversión de características a los datos de juego deben ser sometidos por el módulo de aplicación (103).

7. El aparato cliente (100) de acuerdo con la reivindicación 5, que comprende además: un segundo módulo adaptado para comprobar antes de ejecutar la aplicación si se ha recibido la clave de sesión asignada por el servidor (200), e impedir que la aplicación se ejecute si la clave de sesión no se ha recibido.

8. Un terminal móvil, que comprende un aparato cliente (100) de acuerdo con cualquiera de las reivindicaciones 5 a 7.

9. Un servidor (200) que comprende:

un segundo módulo de interfaz (201), adaptado para intercambiar datos entre el servidor (200) y un cliente (100);

un módulo de confirmación de autenticación (202), adaptado para asignar una clave de sesión al cliente (100) a través del segundo módulo de interfaz (201) para que el cliente (100) lance un programa de juego si se recibe la clave de sesión y, en caso contrario, impedir que se lance el programa de juego, en el que la clave de sesión es generada al cambiar los datos de bits que contienen una ID de cliente del cliente (100) y un tiempo de conexión del cliente (100) de acuerdo con una regla, y además por la inserción de bytes y realizar una operación a nivel de bits en los datos de bits;

un módulo (203), adaptado para generar otro resumen de resultados en base a los datos recibidos del juego, el tiempo de envío de los datos de juego por parte del cliente (100) y la clave de sesión utilizando el mismo algoritmo MD5 utilizado por el cliente (100), comparar el resumen de resultados generado por sí mismo con un resumen de resultados del cliente (100), y considerar los datos de juego como válidos si los dos resúmenes de resultados son idénticos; y

un módulo de almacenamiento de datos (205), adaptado para guardar los datos de juego que han demostrado que son válidos por el módulo de descifrado de datos (203).

10. El servidor (200) de acuerdo con la reivindicación 9, en el que el módulo de almacenamiento de datos (205) es una memoria del sistema en el servidor (200) o un espacio de almacenamiento asignado al cliente (100) en el disco duro del servidor (200).

11. El servidor (200) de acuerdo con la reivindicación 9 o 10, que comprende además: un módulo de conversión inversa de datos (204), adaptado para aplicar la conversión inversa de características a los datos de juego desde el módulo de descifrado de datos (203) para restaurar los datos de juego.

12. Un sistema de transmisión de datos de juego, que comprende:

un servidor (200) como se ha reivindicado en cualquiera de las reivindicaciones 9 a 11, y

un cliente (100) como se ha reivindicado en cualquiera de las reivindicaciones 5 a 7 en comunicación con el servidor (200).

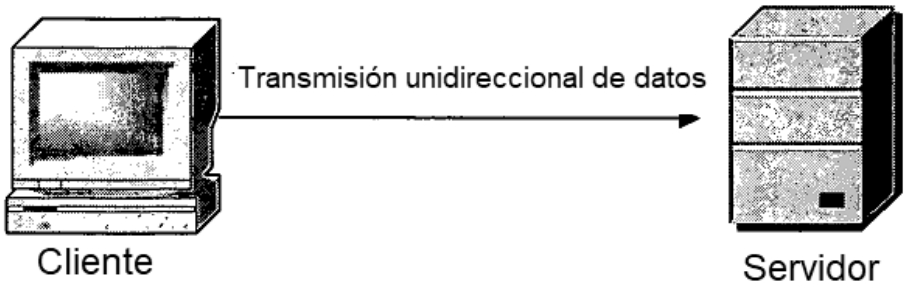
Transmisión unidireccional de datos
Cliente
Servidor

Fig.1

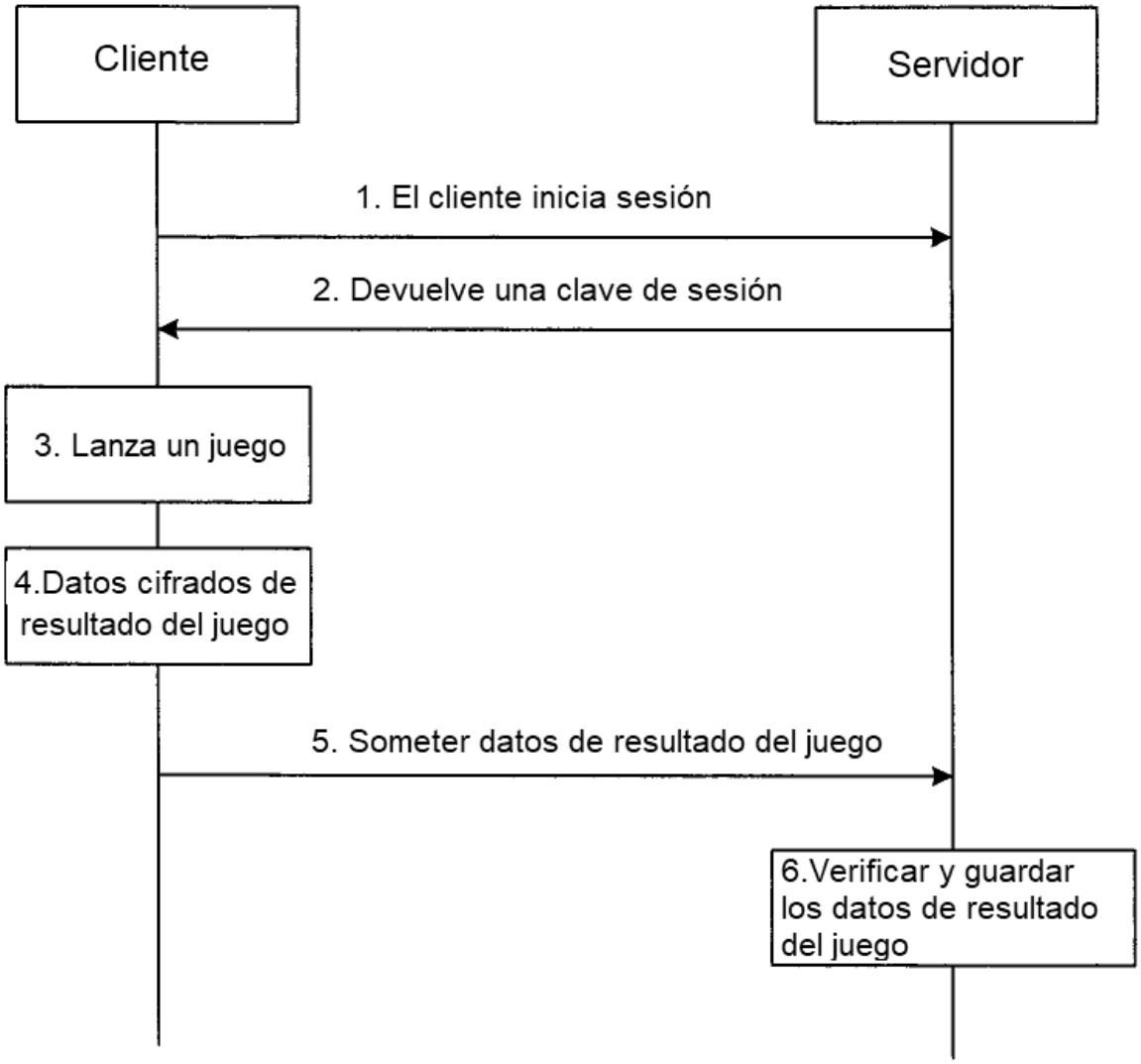
Cliente
Servidor
1. El cliente inicia sesión
2. Devuelve una clave de sesión
3. Lanza un juego
4.Datos cifrados de resultado del juego
5. Someter datos de resultado del juego
6.Verificar y guardar los datos de resultado del juego

Fig.2

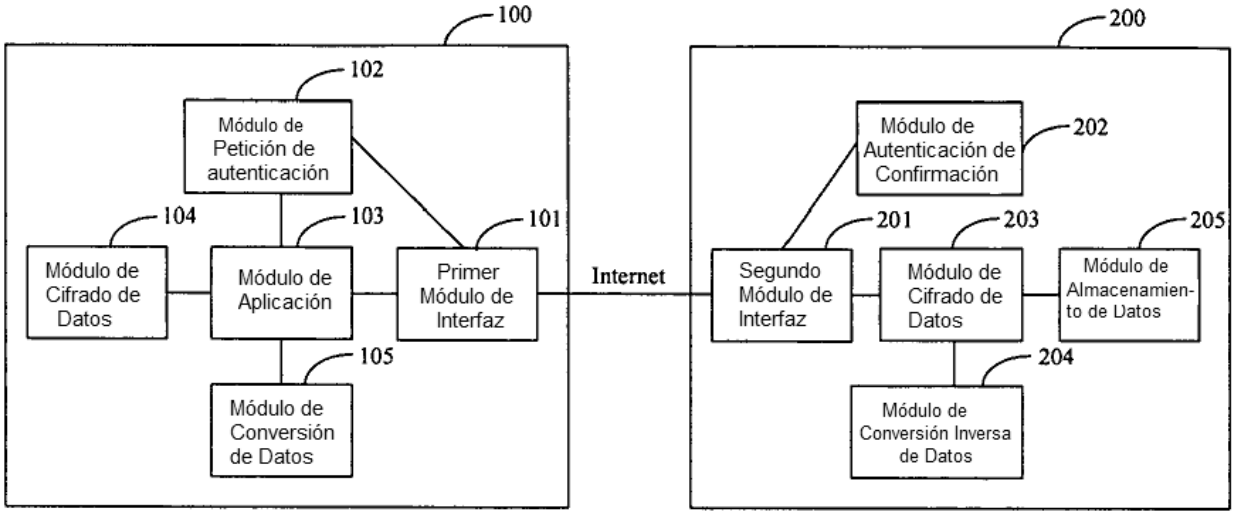
100
102
Módulo de Petición de autenticación
104
103
101
Módulo de Cifrado de Datos
Módulo de Aplicación
Primer Módulo de Interfaz
105
Módulo de Conversión de Datos
Internet
200
Módulo de Autenticación de Confirmación
202
201
203
205
Segundo Módulo de Interfaz
Módulo de Cifrado de Datos
Módulo de Almacenamiento de Datos
204
Módulo de Conversión Inversa de Datos

Fig.3