(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 957**

(51) Int. CI.:

H04L 12/24 (2006.01)
G06F 21/31 (2013.01)
G06F 9/455 (2006.01)
H04L 29/06 (2006.01)
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.11.2012 PCT/CN2012/085008**

(87) Fecha y número de publicación internacional: **30.05.2014 WO2014079009**

(96) Fecha de presentación y número de la solicitud europea: **22.11.2012 E 12888666 (0)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2017 EP 2913956**

(54) Título: **Procedimiento y dispositivo de control de gestión para máquinas virtuales**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.06.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District , Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

YE, SIHAI y
SHI, XUN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento y dispositivo de control de gestión para máquinas virtuales

Campo técnico

La presente invención se refiere a las tecnologías de comunicaciones y, en particular, a un procedimiento, aparato y sistema de control de gestión para una máquina virtual.

Antecedentes

Mediante la integración eficaz de varios recursos informáticos interconectados y la implementación de una virtualización y abstracción de múltiples capas, una plataforma informática en la nube puede proporcionar a los usuarios de manera eficaz recursos informáticos masivos en forma de una máquina virtual fiable. La plataforma informática en la nube no solo debe proporcionar una tecnología de garantía de seguridad fiable para impedir ataques de seguridad procedentes de Internet y entre las máquinas virtuales, sino que también debe garantizar la credibilidad de la plataforma informática en la nube y de varias aplicaciones de los usuarios para impedir la filtración de datos de privacidad del usuario que incluyen un secreto industrial, la filtración de códigos, etc.

La tecnología de garantía de seguridad proporcionada por una plataforma informática en la nube existente incluye, por ejemplo, una tecnología de autenticación de identidad de usuario de máquina virtual, o una tecnología de protección contra malware, o una tecnología de prevención de filtración de datos (DLP).

Sin embargo, la tecnología de garantía de seguridad proporcionada según la plataforma informática en la nube existente presenta muchos problemas. Por ejemplo, la tecnología de autenticación de identidad de usuario de máquina virtual no puede resolver un problema de amenaza a la seguridad provocado por un privilegio de un administrador de la plataforma informática en la nube; como otro ejemplo, la tecnología de protección contra malware solo puede proteger contra malware y programas troyanos que pueden ser identificados mediante software de seguridad, pudiendo producirse un falso negativo; como otro ejemplo, la tecnología de prevención de filtración de datos solo admite un número limitado de sistemas operativos o aplicaciones, y no soporta Windows de 64 bits, Linux, etc., no se aplica en un escenario de múltiples grupos de usuarios en la nube y no puede controlar las filtraciones en las transmisiones de datos entre máquinas virtuales, o no es transparente a los usuarios, lo que afecta a la eficacia de la compartición de información en una empresa.

Por lo tanto, la tecnología de garantía de seguridad proporcionada por la plataforma informática en la nube existente tiene el problema de que ofrece una seguridad relativamente baja.

El documento WO2012-148324 A1 da a conocer un procedimiento en una unidad de provisión que proporciona de manera segura una máquina virtual en una plataforma objetivo que presenta una configuración específica. El procedimiento comprende: recibir (404) una clave de vinculación pública desde la plataforma objetivo (107), estando vinculada la clave de vinculación pública a la configuración específica, cifrar (410) un comando de provisión de máquina virtual usando la clave de vinculación pública, y enviar (412) a la plataforma objetivo (107) el comando de provisión de máquina virtual cifrado. Mediante el dispositivo y procedimiento proporcionados se consigue la provisión segura de una máquina virtual en una plataforma objetivo.

El documento WO2011-141579A2 da a conocer un procedimiento para un intercambio de claves seguro, un almacenamiento de claves y un uso de las claves para proteger un sistema informático en la nube que presenta un servicio informático en la nube que ofrece recursos informáticos y que proporciona medios para acceder a los recursos a través de una red, un ordenador principal y un dispositivo de seguridad portátil conectado al ordenador principal.

El documento WO2011-116459A1 da a conocer un procedimiento que ofrece una plataforma informática segura en la nube. Una máquina virtual (VM) asociada a un cliente se ejecuta en un ordenador que pertenece a una plataforma informática fiable en la nube. Se obtiene una imagen que incluye información de estado de la VM; se almacena la imagen; se determina una función *hash* de renovación de la imagen; y la función *hash* de renovación se envía al cliente. Después, en el mismo ordenador o en un ordenador diferente de la plataforma informática fiable en la nube puede recuperarse la imagen almacenada; puede determinarse una función *hash* de renovación de la imagen recuperada; la función *hash* de renovación de la imagen recuperada puede enviarse al cliente; y puede recibirse una indicación desde el cliente que verifica la integridad de la función *hash* de renovación de la imagen almacenada.

Resumen

La presente invención proporciona un procedimiento, un aparato y un sistema de control de gestión para una máquina virtual, que pueden mitigar el problema de la seguridad relativamente baja que existe en la tecnología de garantía de seguridad proporcionada por una plataforma informática en la nube existente.

La invención está definida por las reivindicaciones independientes. Las reivindicaciones dependientes definen formas de realización ventajosas.

A partir de las anteriores soluciones técnicas se sabe que, en formas de realización de la presente invención, cuando se recibe desde un equipo de usuario un mensaje de solicitud de habilitación de máquina virtual que se ha cifrado usando una clave de una plataforma fiable de terceros y se reenvía mediante una plataforma de gestión, una plataforma de control de seguridad invoca en primer lugar una función de descifrado de la plataforma fiable de terceros para descifrar el mensaje de solicitud de habilitación de máquina virtual, obtiene información de usuario y un identificador de una máquina virtual que es necesario habilitar, incluidos en el mensaje de solicitud de habilitación de máquina virtual, autentica además la información de usuario y, después, tras una autenticación satisfactoria, invoca de nuevo la función de descifrado de la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar, garantizándose así que otro equipo de usuario (incluida la plataforma de gestión) no pueda obtener la clave, de la plataforma fiable de terceros, para cifrar el mensaje de solicitud de habilitación de máquina virtual, ni pueda obtener una clave de encapsulación, de la plataforma fiable de terceros, para realizar operaciones de encapsulación y cifrado en la máquina virtual. Es decir, la máquina virtual de un usuario solo puede habilitarse por el usuario, lo que mejora la seguridad del control de la gestión en la máquina virtual, además de mejorar la seguridad de una plataforma informática en la nube.

Breve descripción de los dibujos

Para describir más claramente las soluciones técnicas de las formas de realización de la presente invención o de la técnica anterior, a continuación se introducen brevemente los dibujos adjuntos necesarios para describir las formas de realización o la técnica anterior. Evidentemente, los dibujos adjuntos de la siguiente descripción muestran algunas formas de realización de la presente invención.

La FIG. 1 es un diagrama de flujo esquemático de un procedimiento de control de gestión para una máquina virtual según una forma de realización de la presente invención.

La FIG. 2 es un diagrama de arquitectura de un sistema de aplicaciones de la forma de realización del procedimiento de control de gestión para una máquina virtual mostrada en la FIG. 1.

La FIG. 3 es un diagrama de flujo esquemático de un procedimiento de control de gestión para una máquina virtual según otra forma de realización de la presente invención.

La FIG. 4 es un diagrama de flujo esquemático de un procedimiento de control de gestión para una máquina virtual según otra forma de realización de la presente invención.

La FIG. 5 es un diagrama estructural esquemático de una plataforma de control de seguridad según otra forma de realización de la presente invención.

La FIG. 6 es otro diagrama estructural esquemático de la plataforma de control de seguridad según la forma de realización mostrada en la FIG. 5.

La FIG. 7 es otro diagrama estructural esquemático de la plataforma de control de seguridad según la forma de realización mostrada en la FIG. 5.

Descripción de las formas de realización

Para entender mejor los objetivos, las soluciones técnicas y las ventajas de las formas de realización de la presente invención, a continuación se describe de manera clara y completa las soluciones técnicas de las formas de realización de la presente invención con referencia a los dibujos adjuntos de las formas de realización de la presente invención. Evidentemente, las formas de realización descritas son algunas y no todas las formas de realización de la presente invención.

En las formas de realización de la presente invención, una plataforma de control de seguridad incluye un dominio de servicio fiable (TSD); la plataforma de control de seguridad es un módulo que proporciona un servicio de seguridad fiable, y una forma de implantación de la plataforma de control de seguridad puede ser un módulo de software, un ordenador principal físico o una máquina virtual, lo cual no tiene un carácter limitativo en la presente invención. La plataforma de control de seguridad está configurada para: cuando un equipo de usuario activa una máquina virtual protegida de un usuario, invocar una plataforma fiable de terceros para completar la autenticación realizada en información de usuario, e impedir que usuarios no autorizados (incluido un administrador) activen la máquina virtual protegida del usuario. La plataforma de control de seguridad está configurada además para prefijar una tabla de política de control de seguridad de la máquina virtual protegida, con el fin de autorizar programas de aplicación que pueden instalarse en la máquina virtual protegida. La plataforma de control de seguridad está configurada además para prefijar una tabla de política de control de acceso de la máquina virtual protegida, con el fin de autorizar otras

máquinas virtuales y sus programas de aplicación que pueden acceder a datos de almacenamiento virtual en la máquina virtual protegida.

En las formas de realización de la presente invención, la plataforma fiable de terceros incluye un módulo de plataforma fiable (TPM) o un módulo criptográfico fiable (TCM), y una forma de implantación de la plataforma fiable de terceros puede ser un chip de hardware instalado en la placa base de un servidor de una plataforma informática en la nube. La plataforma fiable de terceros es un sistema informático integrado que incluye funciones de seguridad y confidencialidad, así como capacidades antiataque, antimanipulación y antidetección en un aspecto de seguridad física; por lo tanto, la plataforma fiable de terceros puede garantizar que la plataforma fiable de terceros y los datos de la plataforma informática en la nube estén protegidos contra un ataque ilegal, y proporciona fundamentos básicos para un funcionamiento fiable y seguro de la plataforma informática en la nube.

La FIG. 1 es un diagrama de flujo esquemático de un procedimiento de control de gestión para una máquina virtual según una forma de realización de la presente invención, y como se muestra en la FIG. 1, el procedimiento de control de gestión para una máquina virtual en esta forma de realización puede incluir:

101: Una plataforma de control de seguridad recibe un mensaje de solicitud de activación de máquina virtual procedente de un equipo de usuario y reenviado por una plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual incluye un identificador de una máquina virtual que es necesario habilitar e información de usuario.

La FIG. 2 es un diagrama de arquitectura de un sistema de aplicaciones del procedimiento de control de gestión para una máquina virtual mostrada en esta forma de realización de la presente invención, y como se muestra en la FIG. 2, a continuación se describen varios componentes del sistema de aplicaciones mostrado en la FIG. 2:

Una capa de hardware puede ser un ordenador principal físico que incluye una CPU, una memoria y un recurso de red, donde el ordenador principal físico incluye un chip TPM, y el ordenador principal físico que incluye el chip TPM constituye la plataforma fiable de terceros en esta forma de realización de la presente invención.

Una unidad de supervisión de máquina virtual (VMM) que está ubicada entre la capa de hardware y un sistema operativo se encarga de proporcionar un recurso de hardware virtualizado al sistema operativo que se ejecuta en una capa superior, gestiona y asigna el recurso de hardware virtualizado y garantiza que las máquinas virtuales de la capa superior estén aisladas entre sí.

Una plataforma de gestión (dominio de gestión) es un gestor y controlador de otras máquinas virtuales. Es una máquina virtual con privilegios que tiene el privilegio de hacer funcionar un recurso de entrada/salida, puede acceder directamente al hardware físico y se encarga de recibir una instrucción de gestión de un sistema de gestión y de interactuar con una interfaz de programación de aplicaciones (API) proporcionada por la unidad de supervisión de máquina virtual para gestionar otras máquinas virtuales (VM) de usuario.

Un dominio de servicio fiable (TSD) es la plataforma de control de seguridad en esta forma de realización de la presente invención.

La máquina virtual (VM) es una máquina virtual protegida sin privilegios proporcionada a un usuario autorizado, ejecuta un sistema operativo cliente y es una zona de seguridad privada o un espacio fiable para el usuario.

El equipo de usuario (UE) puede ser cualquier dispositivo terminal que se conecte a una plataforma informática en la nube para acceder a la máquina virtual del usuario autorizado.

Tomando como base el sistema mostrado en la FIG. 2, si el usuario autorizado desea habilitar la máquina virtual protegida (VM) del usuario autorizado usando el equipo de usuario, el equipo de usuario envía un mensaje de solicitud de activación de máquina virtual a la plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual incluye información de usuario y un identificador, ID, de la máquina virtual que es necesario habilitar. La información de usuario incluye, pero sin limitarse a, información acerca del equipo de usuario, tal como un identificador ID, una cuenta de usuario, una contraseña y una contraseña dinámica.

En un modo de implementación opcional de la presente invención, para garantizar que la habilitación de la máquina virtual es segura y fiable, el anterior mensaje de solicitud de activación de máquina virtual puede cifrarse usando una clave de la plataforma fiable de terceros, tal como una clave 1 mostrada en la FIG. 2, que es la clave de la plataforma fiable de terceros. La clave de la plataforma fiable de terceros puede ser una clave privada de bus serie universal (USB) o una tarjeta inteligente proporcionada por la plataforma fiable de terceros al usuario. Solamente el usuario autorizado puede usar la clave privada para cifrar el mensaje de solicitud de activación de máquina virtual, y ni la plataforma de gestión ni otros usuarios pueden usar la clave.

En un modo de implementación opcional de la presente invención, para garantizar que la habilitación de la máquina virtual es segura y fiable, el equipo de usuario puede añadir una firma digital al mensaje de solicitud de activación de

máquina virtual según una clave que se fija usando una instrucción del usuario autorizado, y después cifra el mensaje de solicitud de activación de máquina virtual usando una clave pública de la plataforma fiable de terceros.

Como se muestra en la FIG. 2, después de que la plataforma de gestión reciba el mensaje de solicitud de activación de máquina virtual enviado por el equipo de usuario, la plataforma de gestión identifica si el equipo de usuario que envía el mensaje de solicitud de activación de máquina virtual es un usuario que se abona a un servicio fiable, y si es así, el mensaje de solicitud de activación de máquina virtual se envía a la plataforma de control de seguridad. El mensaje de solicitud de activación de máquina virtual se cifra usando la clave de la plataforma fiable de terceros, y la plataforma de gestión no puede obtener la clave de la plataforma fiable de terceros, lo que puede garantizar que la habilitación de la máquina virtual sea segura y fiable, así como resolver un problema de amenaza a la seguridad provocado por un privilegio de un administrador de la plataforma informática en la nube.

102: Invocar una plataforma fiable de terceros para determinar que el mensaje de solicitud de activación de máquina virtual es generado por el equipo de usuario según una instrucción de un usuario autorizado.

En un modo de implementación opcional de la presente invención, el mensaje de solicitud de activación de máquina virtual enviado por el equipo de usuario a la plataforma de control de seguridad usando la plataforma de gestión puede no estar cifrado. Para garantizar que la habilitación de la máquina virtual sea segura y fiable, la plataforma de control de seguridad puede invocar una función de cifrado de la plataforma fiable de terceros para generar un dato cifrado usando una clave de la plataforma fiable de terceros. La plataforma de control de seguridad envía los datos cifrados al equipo de usuario usando la plataforma de gestión. El equipo de usuario descifra los datos cifrados usando una clave privada (por ejemplo, una clave USB o una tarjeta inteligente) proporcionada por la plataforma fiable de terceros al usuario, y envía datos descifrados a la plataforma de control de seguridad. La plataforma de control de seguridad compara y determina si los datos descifrados son iguales a los datos cifrados, y si los datos descifrados son iguales a los datos cifrados, determina que el mensaje de solicitud de activación de máquina virtual ha sido generado por el usuario autorizado. La clave USB privada o la tarjeta inteligente solo pueden usarse por el usuario autorizado, y ni la plataforma de gestión ni otros usuarios pueden obtener la clave USB privada o la tarjeta inteligente del usuario autorizado, lo que garantiza que la habilitación de la máquina virtual sea segura y fiable.

En un modo de implementación opcional de la presente invención, si en la etapa 101 el anterior mensaje de solicitud de activación de máquina virtual se cifra mediante el equipo de usuario usando la clave privada proporcionada por la plataforma fiable de terceros al usuario, la plataforma de control de seguridad invoca una función de descifrado de la plataforma fiable de terceros para descifrar el mensaje de solicitud de activación de máquina virtual, dicho de otro modo, para descifrar el mensaje de solicitud de activación de máquina virtual usando la clave privada proporcionada por la plataforma fiable de terceros al usuario. Tras el descifrado, la plataforma de control de seguridad puede obtener la información de usuario y el identificador de la máquina virtual que es necesario habilitar, incluidos en el mensaje de solicitud de activación de máquina virtual.

En un modo de implementación opcional de la presente invención, si en la etapa 101 el equipo de usuario añade la firma digital al mensaje de solicitud de activación de máquina virtual según la clave fijada usando la instrucción del usuario autorizado, y después cifra el mensaje de solicitud de activación de máquina virtual usando la clave pública de la plataforma fiable de terceros, la plataforma de control de seguridad también necesita invocar una función de descifrado de la plataforma fiable de terceros para descifrar el mensaje de solicitud de activación de máquina virtual, dicho de otro modo, para descifrar el mensaje de solicitud de activación de máquina virtual usando la clave pública (por ejemplo, una clave raíz) de la plataforma fiable de terceros. Además, por ejemplo, la información de firma digital del usuario autorizado se almacena de antemano en la plataforma de control de seguridad, y la plataforma de control de seguridad puede determinar, según la información de firma digital del mensaje de solicitud de activación de máquina virtual, que el mensaje de solicitud de activación de máquina virtual es enviado por el equipo de usuario según la instrucción del usuario autorizado, lo que garantiza que la habilitación de la máquina virtual sea segura y fiable. Tras el descifrado, la plataforma de control de seguridad obtiene la información de usuario y el identificador de la máquina virtual que es necesario habilitar, incluidos en el mensaje de solicitud de activación de máquina virtual.

103: Autenticar la información de usuario y, si la autenticación es satisfactoria, invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar.

En un modo de implementación opcional de la presente invención, para garantizar que la habilitación de la máquina virtual sea segura y fiable, después de obtener la información de usuario, la plataforma de control de seguridad autentica la información acerca del usuario autorizado para garantizar que la máquina virtual sea habilitada por el usuario autorizado.

En un modo de implementación opcional de la presente invención, para garantizar la seguridad y la fiabilidad de la máquina virtual que es necesario habilitar, la máquina virtual que es necesario habilitar se cifra usando una clave de encapsulación (o una clave raíz) de la plataforma fiable de terceros y, por lo tanto, puede determinarse que la máquina virtual que es necesario habilitar es una zona de seguridad absolutamente privada o un espacio fiable para el usuario. Por lo tanto, tras obtener el identificador de la máquina virtual que es necesario habilitar, la plataforma de control de seguridad tiene que invocar una función de descifrado de la plataforma fiable de terceros para

desencapsular la máquina virtual correspondiente al identificador de la máquina virtual, dicho de otro modo, para desencapsular la máquina virtual usando la clave de encapsulación proporcionada por la plataforma fiable de terceros a la máquina virtual que es necesario habilitar o la clave raíz de la plataforma fiable de terceros.

En un modo de implementación opcional de la presente invención, en la anterior etapa 101, si el mensaje de solicitud de activación de máquina virtual incluye además una clave de encapsulación para la máquina virtual que es necesario habilitar, después de autenticar de manera satisfactoria la información de usuario, la plataforma de control de seguridad desencapsula directamente, usando la clave de encapsulación incluida en el mensaje de solicitud de activación de máquina virtual, la máquina virtual que es necesario habilitar.

En un modo de implementación opcional de la presente invención, para garantizar la seguridad y la fiabilidad de la máquina virtual, tras la desencapsulación de la máquina virtual que es necesario habilitar, la plataforma de control de seguridad puede invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual desencapsulada, por ejemplo para verificar al menos uno de entre un sistema operativo, un registro, un directorio de sistema y un registro de acceso de la máquina virtual. Si un valor de verificación de integridad de la verificación actual no es coherente con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, esto indica que el entorno operativo de la máquina virtual ha cambiado. Para garantizar la seguridad y la fiabilidad de la máquina virtual, la plataforma de control de seguridad puede restringir la habilitación de la máquina virtual, por ejemplo restringiendo el acceso a datos críticos por parte de la máquina virtual y el permiso de envío de la máquina virtual, y además puede pedir información al equipo de usuario, por ejemplo haciendo que introduzca una contraseña de recuperación o estableciendo contacto con un proveedor de servicios para su gestión. Si el valor de verificación de integridad es coherente con el valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, esto indica que el entorno operativo de la máquina virtual no ha cambiado y que la máquina virtual es segura y fiable, y la máquina virtual se habilita.

En esta forma de realización de la presente invención, cuando se recibe desde un equipo de usuario un mensaje de solicitud de habilitación de máquina virtual que se cifra usando una clave de una plataforma fiable de terceros y se reenvía mediante una plataforma de gestión, una plataforma de control de seguridad invoca en primer lugar una función de descifrado de la plataforma fiable de terceros para descifrar el mensaje de solicitud de habilitación de máquina virtual, obtiene información de usuario y un identificador de una máquina virtual que es necesario habilitar, incluidos en el mensaje de solicitud de habilitación de máquina virtual, autentica además la información de usuario y, después, tras una autenticación satisfactoria, invoca de nuevo la función de descifrado de la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar, garantizándose así que otro equipo de usuario (incluida la plataforma de gestión) no pueda obtener la clave, de la plataforma fiable de terceros, para cifrar el mensaje de solicitud de habilitación de máquina virtual, ni obtener una clave de encapsulación, de la plataforma fiable de terceros, para realizar operaciones de encapsulación y cifrado en la máquina virtual. Es decir, una máquina virtual de un usuario autorizado solo puede habilitarse mediante el usuario autorizado, lo que mejora la seguridad del control de la gestión en la máquina virtual, además de mejorar la seguridad de una plataforma informática en la nube.

La FIG. 3 es un diagrama de flujo esquemático de un procedimiento de control de gestión para una máquina virtual según otra forma de realización de la presente invención; este procedimiento es una extensión adicional basada en la forma de realización de procedimiento mostrada en la FIG. 1 y en el sistema de aplicaciones mostrado en la FIG. 2. Después de que el usuario autorizado habilite la máquina virtual del usuario autorizado usando el equipo de usuario, si el entorno operativo cambia durante la ejecución de la máquina virtual, por ejemplo se instala un nuevo programa de aplicación en la máquina virtual para implementar una ejecución segura de la máquina virtual, la plataforma de control de seguridad puede invocar una plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual, y un proceso de implementación específico se muestra en la FIG. 3, que incluye:

301: La plataforma de control de seguridad detecta, usando una unidad de supervisión de máquina virtual, que un nuevo programa de aplicación se ha instalado en la máquina virtual.

Después de que el usuario autorizado habilite la máquina virtual del usuario autorizado usando el equipo de usuario, el nuevo programa de aplicación se instala en la máquina virtual durante la ejecución de la máquina virtual. Como se muestra en la FIG. 2, la unidad de supervisión de máquina virtual puede detectar que el nuevo programa de aplicación está instalado en la máquina virtual y obtener un identificador del programa de aplicación recién instalado, y la unidad de supervisión de máquina virtual informa a la plataforma de control de seguridad acerca del identificador del programa de aplicación recién instalado.

302: Determinar que el nuevo programa de aplicación se ha instalado mediante el equipo de usuario según una instrucción del usuario autorizado.

303: Invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual, y actualizar un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad.

En un modo de implementación opcional de la presente invención, el equipo de usuario puede prefijar, en la plataforma de control de seguridad y según una instrucción del usuario autorizado, una tabla de política de control de seguridad de una máquina virtual protegida del usuario. La Tabla 1 es una tabla de política de control de seguridad aplicada en esta forma de realización de la presente invención. Debe observarse que, en una aplicación real, las tablas de política de control de seguridad de múltiples máquinas virtuales protegidas están ubicadas en la plataforma de control de seguridad. Como se muestra en la Tabla 1, un identificador de una máquina virtual se usa para representar una entrada de tabla de política de control de seguridad de la máquina virtual correspondiente en la tabla de política de control de seguridad. Por ejemplo, identificadores de programas de aplicación cuya instalación en una máquina virtual 1 está autorizada de antemano, tal como un identificador de un programa de aplicación 1 y un identificador de un programa de aplicación 2, se añaden a una tabla de política de control de seguridad correspondiente a la máquina virtual.

Tabla de política de control de seguridad	
Identificador de máquina virtual 1	Identificador de programa de aplicación 1
	Identificador de programa de aplicación 2
Identificador de máquina virtual 2	Identificador de programa de aplicación 3
	Identificador de programa de aplicación 4
Identificador de máquina virtual 3	Identificador de programa de aplicación 5
	Identificador de programa de aplicación 6

Cuando se detecta, usando la unidad de supervisión de máquina virtual, que el nuevo programa de aplicación está instalado en la máquina virtual, la plataforma de control de seguridad consulta la tabla de política de control de seguridad correspondiente a la máquina virtual según el identificador del programa de aplicación recién instalado. Si se determina que la tabla de política de control de seguridad correspondiente a la máquina virtual incluye el identificador del programa de aplicación recién instalado, la plataforma de control de seguridad determina que el nuevo programa de aplicación ha sido instalado por el equipo de usuario según la instrucción del usuario autorizado, invoca la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual y actualiza el valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad con un valor de verificación de integridad de la verificación actual.

En un modo de implementación opcional de la presente invención, después de que el usuario autorizado habilite la máquina virtual del usuario autorizado usando el equipo de usuario, el usuario autorizado puede instalar el nuevo programa de aplicación en la máquina virtual del usuario autorizado usando el equipo de usuario durante la ejecución de la máquina virtual. En una implementación específica, el equipo de usuario puede enviar, según la instrucción del usuario autorizado, una solicitud de instalación del nuevo programa de aplicación a la plataforma de control de seguridad usando la plataforma de gestión.

Por ejemplo, para garantizar que el nuevo programa de aplicación se instale mediante el equipo de usuario según la instrucción del usuario autorizado, la solicitud anterior para instalar el nuevo programa de aplicación se cifra usando una clave de la plataforma fiable de terceros, donde la clave de la plataforma fiable de terceros puede ser una clave privada de bus serie universal (USB) o una tarjeta inteligente proporcionada por la plataforma fiable de terceros al equipo de usuario. Solamente el usuario puede usar la clave privada para cifrar la solicitud de instalación del nuevo programa de aplicación, y ni la plataforma de gestión ni otros usuarios pueden usar la clave.

La plataforma de control de seguridad invoca una función de descifrado de la plataforma fiable de terceros para descifrar la solicitud de instalación del nuevo programa de aplicación, dicho de otro modo, para descifrar la solicitud de instalación del nuevo programa de aplicación usando la clave proporcionada por la plataforma fiable de terceros al usuario. Después, la plataforma de control de seguridad determina que el nuevo programa de aplicación ha sido instalado por el equipo de usuario según la instrucción del usuario autorizado, invoca la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual y actualiza el valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad con el valor de verificación de integridad de la verificación actual.

Como otro ejemplo, para garantizar que el nuevo programa de aplicación se instala mediante el equipo de usuario según la instrucción del usuario autorizado, el equipo de usuario puede firmar, según una clave fijada usando una instrucción del usuario autorizado, la solicitud de instalación del nuevo programa de aplicación, y después cifrar, usando una clave pública de la plataforma fiable de terceros, la solicitud de instalación del nuevo programa de aplicación.

La plataforma de control de seguridad también necesita invocar la función de descifrado de la plataforma fiable de terceros para descifrar la solicitud de instalación del nuevo programa de aplicación, dicho de otro modo, para descifrar la solicitud de instalación del nuevo programa de aplicación usando la clave pública (por ejemplo, una clave

raíz) de la plataforma fiable de terceros. Además, por ejemplo, la información de firma digital del usuario autorizado se almacena de antemano en la plataforma de control de seguridad, y la plataforma de control de seguridad puede determinar, según información de firma digital de la solicitud de instalación del nuevo programa de aplicación, que la solicitud de instalación del nuevo programa de aplicación es enviada por el equipo de usuario según la instrucción del usuario autorizado, lo que garantiza que la instalación del nuevo programa de aplicación sea segura y fiable.

Como otro ejemplo, la solicitud de instalación del nuevo programa de aplicación, enviada por el equipo de usuario a la plataforma de control de seguridad usando la plataforma de gestión, no se cifra; para garantizar que el nuevo programa de aplicación se instala mediante el equipo de usuario según la instrucción del usuario autorizado, la plataforma de control de seguridad puede invocar una función de cifrado de la plataforma fiable de terceros para generar un dado cifrado usando una clave de la plataforma fiable de terceros. La plataforma de control de seguridad envía los datos cifrados al equipo de usuario usando la plataforma de gestión. El equipo de usuario descifra los datos cifrados usando una clave privada (por ejemplo, una clave USB o una tarjeta inteligente) proporcionada por la plataforma fiable de terceros al usuario, y envía datos descifrados a la plataforma de control de seguridad. La plataforma de control de seguridad compara y determina si los datos descifrados son iguales a los datos cifrados, y si los datos descifrados son iguales a los datos cifrados, determina que la solicitud de instalación del nuevo programa de aplicación se ha generado por el usuario autorizado. La clave USB privada o la tarjeta inteligente solo pueden usarse por el usuario autorizado, y ni la plataforma de gestión ni otros usuarios pueden obtener la clave USB privada o la tarjeta inteligente del usuario autorizado, lo que garantiza que la instalación del nuevo programa de aplicación sea segura y fiable.

En un modo de implementación opcional de la presente invención, después de habilitarse la máquina virtual, el usuario autorizado de la máquina virtual puede iniciar, usando el equipo de usuario en cualquier momento, una verificación de integridad en la máquina virtual durante la ejecución de la máquina virtual. Específicamente, el equipo de usuario envía un mensaje de solicitud de verificación de integridad de máquina virtual a la plataforma de gestión, donde el mensaje de solicitud de verificación de integridad de máquina virtual incluye un identificador de una máquina virtual que requiere una verificación de integridad; la plataforma de gestión reenvía el mensaje de solicitud de verificación de integridad de máquina virtual a la plataforma de control de seguridad y, tras recibir el mensaje de solicitud de verificación de integridad de máquina virtual enviado por la plataforma de gestión, la plataforma de control de seguridad puede invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual; un valor de verificación de integridad de la verificación actual se compara con el valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad; después, tras la comparación, si se determina que el valor de verificación de integridad de la máquina virtual cambia, se determina, según un archivo de registro, que acaba de instalarse un programa de aplicación no autorizado. La plataforma de control de seguridad envía un resultado de comparación de valor de verificación de integridad al equipo de usuario usando la plataforma de gestión, de modo que el equipo de usuario desinstala el programa de aplicación no autorizado según el resultado de comparación de valor de verificación de integridad o restaura la máquina virtual usando una operación de restauración del sistema.

En esta forma de realización, si un programa de aplicación no autorizado, por ejemplo, malware, se instala en una máquina virtual, una plataforma de control de seguridad ni lleva a cabo una verificación de integridad en la máquina virtual ni refresca un valor de verificación de integridad de la máquina virtual; por lo tanto, incluso si se instala malware no autorizado en la máquina virtual, la plataforma de control de seguridad puede restringir el acceso a datos críticos por parte de la máquina virtual en la que se ha instalado el malware, así como el permiso de envío de la máquina virtual, ya que el malware recién instalado no pasará la verificación de integridad realizada por la plataforma de control de seguridad. Por lo tanto, en cualquier máquina virtual en la que se instale un programa de aplicación no autorizado (incluido malware), la plataforma de control de seguridad puede restringir el acceso a datos críticos por parte de la máquina virtual, así como el permiso de envío de la máquina virtual, lo que soluciona el problema de que una tecnología de protección contra malware solo pueda proteger contra malware y programas troyanos que puedan ser identificados mediante software de seguridad y pueda producirse un falso negativo.

En esta forma de realización de la presente invención, cuando una plataforma de control de seguridad detecta que un nuevo programa de aplicación está instalado en una máquina virtual, si se determina que una tabla de política de control de seguridad correspondiente a la máquina virtual incluye un identificador del nuevo programa de aplicación, la plataforma de control de seguridad invoca una plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual, y actualiza un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad. Puede implementarse que no se realice ninguna verificación de integridad en la máquina virtual cuando un programa de aplicación recién instalado en la máquina virtual no sea un programa de aplicación de la tabla de política de control de seguridad prefijada. Por lo tanto, puede garantizarse que solo pueda instalarse y ejecutarse en la máquina virtual un programa de aplicación cuya instalación esté autorizada por un usuario; en caso contrario, no se pasará la verificación de integridad realizada por la plataforma de control de seguridad. La plataforma de control de seguridad puede restringir el acceso a datos críticos por parte de la máquina virtual y el permiso de envío de la máquina virtual. Por lo tanto, puede garantizarse la seguridad de una máquina virtual de usuario protegida, se mejora la seguridad del control de gestión en la máquina virtual y, por lo tanto, también se mejora la seguridad de una plataforma informática en la nube.

La FIG. 4 es un diagrama de flujo esquemático de un procedimiento de control de gestión para una máquina virtual según otra forma de realización de la presente invención; este procedimiento es una extensión adicional basada en la forma de realización de procedimiento mostrada en la FIG. 1 y en el sistema de aplicaciones mostrado en la FIG. 2. Después de que el usuario autorizado habilite la máquina virtual del usuario autorizado usando el equipo de usuario, cuando un programa de aplicación en una o más otras máquinas virtuales solicita acceder a datos de un almacenamiento virtual de la máquina virtual durante la ejecución de la máquina virtual para garantizar la seguridad de los datos del almacenamiento virtual de la máquina virtual del usuario autorizado, la plataforma de control de seguridad verifica la autorización de la una o más otras máquinas virtuales y el programa de aplicación de la una o más otras máquinas virtuales, y la plataforma de control de seguridad invoca la plataforma fiable de terceros para descifrar los datos del almacenamiento virtual de la máquina virtual solo cuando la verificación sea satisfactoria. Un proceso de implementación específico se muestra en la FIG. 4, que incluye:

401: La plataforma de control de seguridad detecta, usando una unidad de supervisión de máquina virtual, una solicitud de acceso de una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, y obtiene un identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y un identificador de un programa de aplicación en la una o más otras máquinas virtuales.

Como se muestra en la FIG. 2, después de que el usuario autorizado habilite la máquina virtual del usuario autorizado usando el equipo de usuario, cuando la una o más otras máquinas virtuales solicitan acceder a datos del almacenamiento virtual de la máquina virtual del usuario autorizado durante la ejecución de la máquina virtual, la unidad de supervisión de máquina virtual obtiene, siguiendo un flujo de información de la máquina virtual, el identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso. Debe observarse que, en una aplicación real, la solicitud de acceso se genera normalmente por un programa de aplicación de la una o más otras máquinas virtuales y, por lo tanto, la unidad de supervisión de máquina virtual puede obtener además, siguiendo el flujo de información de la máquina virtual, un identificador del programa de aplicación de la una o más otras máquinas virtuales que generan la solicitud de acceso. La unidad de supervisión de máquina virtual envía a la plataforma de control de seguridad el identificador de la una o más otras máquinas virtuales y el identificador del programa de aplicación de la una o más otra máquinas virtuales obtenidos.

402: Si se determina que una tabla de política de control de acceso de la máquina virtual incluye el identificador de la una o más otras máquinas virtuales que inician la solicitud de acceso y el identificador del programa de aplicación de la una o más otras máquinas virtuales, invocar la plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual.

En un modo de implementación de la presente invención, el equipo de usuario puede prefijar, en la plataforma de control de seguridad y según una instrucción del usuario autorizado, una tabla de política de control de acceso de una máquina virtual protegida del usuario. La Tabla 2 es una tabla de política de control de acceso aplicada en esta forma de realización de la presente invención. Debe observarse que, en una aplicación real, las tablas de política de control de acceso de múltiples máquinas virtuales protegidas están ubicadas en la plataforma de control de seguridad. Como se muestra en la Tabla 2, un identificador de una máquina virtual se usa para representar una entrada de tabla de política de control de acceso de la máquina virtual correspondiente en la tabla de política de control de acceso. Por ejemplo, la tabla de política de control de acceso almacena entradas de tabla de política de control de acceso correspondientes a una máquina virtual 1 y una máquina virtual 2. Por ejemplo, identificadores de otra máquina virtual 3 y de otra máquina virtual 4 cuyo acceso a la máquina virtual 1 está autorizado de antemano, un identificador de un programa de aplicación 1 y un identificador de un programa de aplicación 2 que están en la otra máquina virtual 3, y un identificador de un programa de aplicación 3 y un identificador de un programa de aplicación 4 que están en la otra máquina virtual 4 se añaden a una entrada de tabla de política de control de acceso correspondiente a la máquina virtual 1.

Entrada de tabla de política de control de acceso		
Identificador de máquina virtual 1	Identificador de otra máquina virtual 3	Identificador de programa de aplicación 1
		Identificador de programa de aplicación 2
	Identificador de otra máquina virtual 4	Identificador de programa de aplicación 3
		Identificador de programa de aplicación 4
Identificador de máquina virtual 2	Identificador de otra máquina virtual 5	Identificador de programa de aplicación 5
	Identificador de otra máquina virtual 6	Identificador de programa de aplicación 6
		Identificador de programa de aplicación 7

La plataforma de control de seguridad consulta, según el identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y según el identificador del programa de aplicación de la una o más otras máquinas virtuales, la tabla de política de control de acceso correspondiente a la máquina virtual. Si se determina que la tabla

de política de control de acceso correspondiente a la máquina virtual incluye el identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y el identificador del programa de aplicación en la una o más otras máquinas virtuales, la plataforma de control de seguridad determina que la una o más otras máquinas virtuales que generan la solicitud de acceso y el programa de aplicación de la una o más otras máquinas virtuales se autorizan de antemano, e invoca la plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual.

En un modo de implementación de la presente invención, para garantizar la seguridad de los datos de almacenamiento virtual de la máquina virtual, los datos de almacenamiento virtual de la máquina virtual se cifran usando una clave de encapsulación de la plataforma fiable de terceros, lo que puede garantizar que el espacio de la máquina virtual para almacenar los datos de almacenamiento virtual sea una zona y un espacio seguros absolutamente privados para el usuario. Por lo tanto, tras verificar de manera satisfactoria la autorización de la máquina virtual que genera la solicitud de acceso y el programa de aplicación de la máquina virtual, la plataforma de control de seguridad invoca la plataforma fiable de terceros para desencapsular los datos de almacenamiento virtual de la máquina virtual, dicho de otro modo, para desencapsular los datos de almacenamiento virtual de la máquina virtual usando la clave de encapsulación usada en la encapsulación basada en clave realizada por la plataforma fiable de terceros en los datos de almacenamiento virtual de la máquina virtual o una clave raíz de la plataforma fiable de terceros.

403: Enviar datos de almacenamiento virtual descifrados a la una o más otras máquinas virtuales que inician la solicitud de acceso.

En un modo de implementación de la presente invención, la plataforma de control de seguridad consulta, según el identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y según el identificador del programa de aplicación de la una o más otras máquinas virtuales obtenidos, la tabla de política de control de acceso correspondiente a la máquina virtual. Si se determina que la tabla de política de control de acceso de la máquina virtual no incluye el identificador obtenido de la una o más otras máquinas virtuales, o incluye el identificador obtenido de la una o más otras máquinas virtuales pero no incluye el identificador obtenido del programa de aplicación, la plataforma de control de seguridad determina que la solicitud de acceso no está autorizada, y la plataforma de control de seguridad impide que la una o más otras máquinas virtuales accedan a los datos de almacenamiento virtual de la máquina virtual, o solo envía datos de almacenamiento virtual no descifrados a la máquina virtual que inicia la solicitud de acceso.

Los anteriores datos de almacenamiento virtual de la máquina virtual incluyen datos almacenados en una memoria virtual de la máquina virtual y datos de memoria de la máquina virtual.

En esta forma de realización de la presente invención, cuando una plataforma de control de seguridad detecta una solicitud de acceso de una o más otras máquinas virtuales y un programa de aplicación de la una o más otras máquinas virtuales para datos de almacenamiento virtual en una máquina virtual de usuario protegida, si se determina que una tabla de política de control de acceso correspondiente a la máquina virtual de usuario incluye un identificador de la una o más otras máquinas virtuales que inician la solicitud de acceso y un identificador del programa de aplicación de la una o más otras máquinas virtuales, la plataforma de control de seguridad invoca una plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual de usuario, y envía datos descifrados a la una o más otras máquinas virtuales que generan la solicitud de acceso. Por lo tanto, se garantiza que otro equipo de usuario (incluido una plataforma de gestión) no puede obtener una clave de encapsulación de la plataforma fiable de terceros para realizar operaciones de encapsulación y cifrado en los datos de almacenamiento virtual de la máquina virtual de usuario. Es decir, solamente una máquina virtual o un programa de aplicación autorizados por un usuario pueden acceder a los datos de almacenamiento virtual de la máquina virtual de usuario; la plataforma de control de seguridad puede restringir el acceso a los datos de almacenamiento virtual de la máquina virtual de usuario por parte de una o más otras máquinas virtuales y un programa de aplicación que no estén autorizados por el usuario, lo que garantiza la seguridad de los datos de almacenamiento virtual en la máquina virtual de usuario protegida, mejora la seguridad del control de gestión en la máquina virtual y, por tanto, también mejora la seguridad de una plataforma informática en la nube.

Además, la plataforma de control de seguridad de esta forma de realización admite todos los sistemas operativos o aplicaciones, se aplica en un escenario de aplicación de múltiples grupos de usuarios en la nube y puede controlar de manera eficaz la filtración en las transmisiones de datos entre máquinas virtuales.

La FIG. 5 es un diagrama estructural esquemático de una plataforma de control de seguridad según otra forma de realización de la presente invención; como se muestra en la FIG. 5, la plataforma de control de seguridad incluye:

un módulo de recepción 51, configurado para recibir un mensaje de solicitud de activación de máquina virtual procedente de un equipo de usuario y reenviada por una plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual incluye un identificador de una máquina virtual que es necesario habilitar e información de usuario;

un módulo de determinación 52, configurado para: sobre la base de que el módulo de recepción recibe el mensaje de solicitud de activación de máquina virtual procedente del equipo de usuario, invocar una plataforma fiable de terceros para determinar que el mensaje de solicitud de activación de máquina virtual se genera por el equipo de usuario según una instrucción de un usuario autorizado; y

un módulo de desencapsulación 53, configurado para: sobre la base de que el módulo de determinación determina que el mensaje de solicitud de activación de máquina virtual es generado por el equipo de usuario según la instrucción del usuario autorizado, después de que la información de usuario se autentique de manera satisfactoria, invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar.

En un modo de implementación de la presente invención, el módulo de determinación 52 está configurado específicamente para: si se determina que el mensaje de solicitud de activación de máquina virtual se cifra usando una clave proporcionada por la plataforma fiable de terceros al usuario autorizado, determinar que el mensaje de solicitud de activación de máquina virtual se genera mediante el equipo de usuario según la instrucción del usuario autorizado, e invocar la clave proporcionada por la plataforma fiable de terceros al usuario autorizado, con el fin de descifrar el mensaje de solicitud de activación de máquina virtual.

En un modo de implementación de la presente invención, el módulo de determinación 52 está configurado específicamente para: si se determina que el mensaje de solicitud de activación de máquina virtual se ha cifrado usando una clave pública de la plataforma fiable de terceros, invocar la clave pública de la plataforma fiable de terceros para descifrar el mensaje de solicitud de activación de máquina virtual; y obtener información de firma digital del mensaje de solicitud de activación de máquina virtual, y si se determina que la información de firma digital obtenida es coherente con información de firma digital del usuario autorizado almacenada de antemano en la plataforma de control de seguridad, determinar que el mensaje de solicitud de activación de máquina virtual se ha generado por el equipo de usuario según la instrucción del usuario autorizado.

En un modo de implementación de la presente invención, el módulo de determinación 52 está configurado específicamente para: invocar la plataforma fiable de terceros para generar datos cifrados usando una clave de la plataforma fiable de terceros; enviar los datos cifrados al equipo de usuario usando la plataforma de gestión, de modo que el equipo de usuario descifra los datos cifrados usando una clave privada proporcionada por la plataforma fiable de terceros al usuario autorizado, y devuelve datos descifrados a la plataforma de control de seguridad; y si se determina que los datos descifrados son iguales a los datos cifrados, determinar que el mensaje de solicitud de activación de máquina virtual se ha generado por el equipo de usuario según la instrucción del usuario autorizado.

La FIG. 6 es otro diagrama estructural esquemático de la plataforma de control de seguridad según la forma de realización mostrada en la FIG. 5; como se muestra en la FIG. 6, la plataforma de control de seguridad incluye además:

un módulo de verificación 54, configurado para invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual;

un módulo de restricción de habilitación 55, configurado para: sobre la base de que el módulo de verificación realiza una verificación de integridad en la máquina virtual, si un valor de verificación de integridad no es coherente con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, restringir la habilitación del módulo de desencapsulación que desencapsula la máquina virtual que es necesario habilitar; y

un módulo de habilitación 56, configurado para: sobre la base de que el módulo de verificación realiza una verificación de integridad en la máquina virtual, si un valor de verificación de integridad es coherente con el valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, habilitar el módulo de desencapsulación que desencapsula la máquina virtual que es necesario habilitar.

La FIG. 7 es otro diagrama estructural esquemático de la plataforma de control de seguridad según la forma de realización mostrada en la FIG. 5; como se muestra en la FIG. 7, la plataforma de control de seguridad incluye además:

un módulo de supervisión 57, configurado para detectar, usando una unidad de supervisión de máquina virtual, que un nuevo programa de aplicación se ha instalado en la máquina virtual.

En un modo de implementación de la presente invención, el módulo de verificación 54 está configurado además para: sobre la base de que el módulo de supervisión detecta que el nuevo programa de aplicación se ha instalado en la máquina virtual, si se determina que el nuevo programa de aplicación se ha instalado mediante el equipo de usuario según una instrucción del usuario autorizado, invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual y actualizar un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad.

En un modo de implementación de la presente invención, el módulo de recepción 51 está configurado además para recibir un mensaje de solicitud de verificación de integridad de máquina virtual enviado por la plataforma de gestión, donde el mensaje de solicitud de verificación de integridad de máquina virtual es enviado por el equipo de usuario a la plataforma de gestión, y el mensaje de solicitud de verificación de integridad de máquina virtual incluye un identificador de una máquina virtual que requiere una verificación de integridad.

En un modo de implementación de la presente invención, el módulo de verificación 54 está configurado además para: en función del mensaje de solicitud de verificación de integridad de máquina virtual recibido por el módulo de recepción, invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual.

En un modo de implementación de la presente invención, la plataforma de control de seguridad incluye además:

un módulo de comparación 58, configurado para: sobre la base de que el módulo de verificación realiza una verificación de integridad en la máquina virtual, comparar un valor de verificación de integridad con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad; y enviar un resultado de comparación de valor de verificación de integridad a la plataforma de gestión, de manera que la plataforma de gestión envía el resultado de comparación de valor de verificación de integridad al equipo de usuario.

En un modo de implementación de la presente invención, el módulo de supervisión 57 está configurado además para detectar, usando una unidad de supervisión de máquina virtual, una solicitud de acceso de una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, y obtener un identificador de la una o más otras máquinas virtuales que inician la solicitud de acceso y un identificador de un programa de aplicación.

El módulo de desencapsulación 53 está configurado además para: sobre la base de que el módulo de supervisión detecta la solicitud de acceso de la una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, si se determina que una entrada de tabla de política de control de acceso de la máquina virtual incluye el identificador de la una o más otras máquinas virtuales y el identificador del programa de aplicación obtenidos, invocar la plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual; y enviar los datos de almacenamiento virtual descifrados a la una o más otras máquinas virtuales que inician la solicitud de acceso.

En un modo de implementación de la presente invención, si el anterior mensaje de solicitud de activación de máquina virtual incluye además una clave de encapsulación para la máquina virtual que es necesario habilitar, el módulo de desencapsulación 53 está configurado además para: de acuerdo con el mensaje de solicitud de activación de máquina virtual recibido por el módulo de recepción, desencapsular la máquina virtual correspondiente al identificador de la máquina virtual usando la clave de encapsulación incluida en el mensaje de solicitud de activación de máquina virtual.

La plataforma de control de seguridad incluye un dominio de servicio fiable, TSD, y la plataforma fiable de terceros incluye un módulo de plataforma fiable, TPM, y un módulo criptográfico fiable, TCM.

Los anteriores datos de almacenamiento virtual de la máquina virtual incluyen datos almacenados en una memoria virtual de la máquina virtual y datos de memoria de la máquina virtual.

En esta forma de realización de la presente invención, cuando una plataforma de control de seguridad detecta una solicitud de acceso de una o más otras máquinas virtuales y un programa de aplicación de la una o más otras máquinas virtuales para datos de almacenamiento de una máquina virtual de usuario protegida, si se determina que una tabla de política de control de acceso correspondiente a la máquina virtual de usuario incluye un identificador de la una o más otras máquinas virtuales que inician la solicitud de acceso y un identificador del programa de aplicación de la una o más otras máquinas virtuales, la plataforma de control de seguridad invoca una plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual de usuario, y envía datos descifrados a la una o más otras máquinas virtuales que generan la solicitud de acceso. Por lo tanto, se garantiza que otro equipo de usuario (incluido una plataforma de gestión) no pueda obtener una clave de encapsulación, de la plataforma fiable de terceros, para realizar operaciones de encapsulación y cifrado en los datos de almacenamiento virtual en la máquina virtual de usuario. Es decir, solamente una máquina virtual o un programa de aplicación autorizado por un usuario pueden acceder a los datos de almacenamiento virtual de la máquina virtual de usuario; la plataforma de control de seguridad puede restringir el acceso a los datos de almacenamiento virtual de la máquina virtual de usuario por parte de una o más otras máquinas virtuales y un programa de aplicación que no estén autorizados por el usuario, lo que garantiza la seguridad de los datos de almacenamiento virtual de la máquina virtual de usuario protegida, mejora la seguridad del control de gestión de la máquina virtual y, por tanto, también mejora la seguridad de una plataforma informática en la nube.

Además, la plataforma de control de seguridad en esta forma de realización admite todos los sistemas operativos o aplicaciones, se aplica en un escenario de aplicación de múltiples grupos de usuarios en la nube y puede controlar de manera eficaz la filtración en las transmisiones de datos entre máquinas virtuales.

Otra forma de realización de la presente invención proporciona además una plataforma de control de seguridad, que incluye un procesador, donde el procesador realiza las siguientes etapas durante la ejecución:

recibir un mensaje de solicitud de activación de máquina virtual procedente de un equipo de usuario y reenviado por una plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual incluye un identificador de una máquina virtual que es necesario habilitar e información de usuario;
invocar una plataforma fiable de terceros para determinar que el mensaje de solicitud de activación de máquina virtual se genera por el equipo de usuario según una instrucción de un usuario autorizado; y
después de que la información de usuario se haya autenticado de manera satisfactoria, invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar.

En un primer modo de implementación posible, el procesador realiza además las siguientes etapas:

si se determina que el mensaje de solicitud de activación de máquina virtual se cifra usando una clave proporcionada por la plataforma fiable de terceros al usuario autorizado, determinar que el mensaje de solicitud de activación de máquina virtual se genera mediante el equipo de usuario según la instrucción del usuario autorizado, e invocar la clave proporcionada por la plataforma fiable de terceros al usuario autorizado con el fin de descifrar el mensaje de solicitud de activación de máquina virtual.

En un segundo modo de implementación posible, el procesador realiza además las siguientes etapas:

si se determina que el mensaje de solicitud de activación de máquina virtual se cifra usando una clave pública de la plataforma fiable de terceros, invocar la clave pública de la plataforma fiable de terceros para descifrar el mensaje de solicitud de activación de máquina virtual; y obtener información de firma digital del mensaje de solicitud de activación de máquina virtual, y si se determina que la información de firma digital obtenida es coherente con información de firma digital del usuario autorizado almacenada de antemano en la plataforma de control de seguridad, determinar que el mensaje de solicitud de activación de máquina virtual se ha generado por el equipo de usuario según la autorización del usuario autorizado.

En un tercer modo de implementación posible, el procesador realiza además las siguientes etapas:

invocar la plataforma fiable de terceros para generar datos cifrados usando una clave de la plataforma fiable de terceros; enviar los datos cifrados al equipo de usuario usando la plataforma de gestión, de modo que el equipo de usuario descifra los datos cifrados usando una clave privada proporcionada por la plataforma fiable de terceros al usuario autorizado y devuelve datos descifrados a la plataforma de control de seguridad; y si se determina que los datos descifrados son iguales a los datos cifrados, determinar que el mensaje de solicitud de activación de máquina virtual se ha generado por el equipo de usuario según la instrucción del usuario autorizado.

Basándose en el primer, segundo y tercer modos de implementación posibles, en un cuarto modo de implementación posible, el procesador realiza además las siguientes etapas:

invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual; y
si un valor de verificación de integridad no es coherente con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, restringir la habilitación de la máquina virtual; o
si un valor de verificación de integridad es coherente con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, habilitar la máquina virtual.

Basándose en el primer, segundo y tercer modos de implementación posibles, en un quinto modo de implementación posible, el procesador realiza además las siguientes etapas:

detectar, usando una unidad de supervisión de máquina virtual, que un nuevo programa de aplicación se ha instalado en la máquina virtual, y obtener un identificador del nuevo programa de aplicación; y
si se determina que el nuevo programa de aplicación ha sido instalado por el equipo de usuario según una instrucción del usuario autorizado, invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual y actualizar un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad.

Basándose en el primer, segundo y tercer modos de implementación posibles, en un sexto modo de implementación posible, el procesador realiza además las siguientes etapas:

recibir un mensaje de solicitud de verificación de integridad de máquina virtual enviado por la plataforma de gestión, donde el mensaje de solicitud de verificación de integridad de máquina virtual es enviado por el equipo de usuario a la plataforma de gestión, y el mensaje de solicitud de verificación de integridad de máquina virtual incluye un identificador de una máquina virtual que requiere una verificación de integridad;
invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual;
comparar un valor de verificación de integridad con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad; y
enviar un resultado de comparación de valor de verificación de integridad a la plataforma de gestión, de modo que la plataforma de gestión envía el resultado de comparación de valor de verificación de integridad al equipo de usuario.

Basándose en el primer, segundo y tercer modos de implementación posibles, en un séptimo modo de implementación posible, el procesador realiza además las siguientes etapas:

detectar, usando una unidad de supervisión de máquina virtual, una solicitud de acceso de una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, y obtener un identificador de la una o más otras máquinas virtuales que inician la solicitud de acceso y un identificador de un programa de aplicación; y
si se determina que una entrada de tabla de política de control de acceso de la máquina virtual incluye el identificador de la una o más otras máquinas virtuales y el identificador del programa de aplicación obtenidos, invocar la plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual; y enviar los datos de almacenamiento virtual descifrados a la una o más otras máquinas virtuales que generan la solicitud de acceso.

En un octavo modo de implementación posible, el mensaje de solicitud de activación de máquina virtual incluye además una clave de desencapsulación para la máquina virtual que es necesario habilitar; y

el procesador realizar además la siguiente etapa:
desencapsular la máquina virtual correspondiente al identificador de la máquina virtual usando la clave de encapsulación incluida en el mensaje de solicitud de activación de máquina virtual.

En esta forma de realización de la presente invención, cuando una plataforma de control de seguridad detecta una solicitud de acceso de una o más otras máquinas virtuales y un programa de aplicación de la una o más otras máquinas virtuales para datos de almacenamiento virtual en una máquina virtual de usuario protegida, si se determina que una tabla de política de control de acceso correspondiente a la máquina virtual de usuario incluye un identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y un identificador del programa de aplicación de la una o más otras máquinas virtuales, la plataforma de control de seguridad invoca una plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual de usuario, y envía datos descifrados a la una o más otras máquinas virtuales que inician la solicitud de acceso. Por lo tanto, se garantiza que otro equipo de usuario (incluida una plataforma de gestión) no pueda obtener una clave de encapsulación de la plataforma fiable de terceros para realizar operaciones de encapsulación y cifrado en los datos de almacenamiento virtual en la máquina virtual de usuario. Es decir, solamente una máquina virtual o un programa de aplicación autorizado por un usuario pueden acceder a los datos de almacenamiento virtual de la máquina virtual de usuario; la plataforma de control de seguridad puede restringir el acceso a los datos de almacenamiento virtual de la máquina virtual de usuario por parte de una o más otras máquinas virtuales y un programa de aplicación que no estén autorizados por el usuario, lo que garantiza la seguridad de los datos de almacenamiento virtual de la máquina virtual de usuario protegida, mejora la seguridad del control de gestión de la máquina virtual y, por tanto, también mejora la seguridad de una plataforma informática en la nube.

Específicamente, además del procesador, la plataforma de control de seguridad incluye además una memoria, una interfaz de comunicaciones y un bus de comunicaciones, donde el procesador está conectado a la memoria usando el bus de comunicaciones, y la plataforma de control de seguridad se comunica con otro elemento de red usando la interfaz de comunicaciones.

Además, la plataforma de control de seguridad de esta forma de realización admite todos los sistemas operativos o aplicaciones, se aplica en un escenario de aplicación de múltiples grupos de usuarios en la nube y puede controlar de manera eficaz la filtración en las transmisiones de datos entre máquinas virtuales.

Otra forma de realización de la presente invención proporciona además un sistema de control de gestión para una máquina virtual, incluida la plataforma de control de seguridad en la forma de realización mostrada en una cualquiera de las FIG. 5 a 7 anteriores. En lo que respecta al contenido detallado de la plataforma de control de seguridad, se hace referencia a las descripciones relacionadas en la forma de realización mostrada en una cualquiera de las FIG. 5 a 7, cuyos detalles no se describen de nuevo.

Con vistas a una descripción concisa y breve, a un experto en la técnica le resultará evidente que para describir un proceso de funcionamiento detallado del anterior sistema, aparato y unidad, puede hacerse referencia a un proceso

correspondiente de las anteriores formas de realización de procedimiento, cuyos detalles no se describen de nuevo en el presente documento.

En las diversas formas de realización proporcionadas en la presente solicitud, debe entenderse que el sistema, aparato y procedimiento dados a conocer pueden implementarse de otras maneras. Por ejemplo, la forma de realización de aparato descrita es simplemente ilustrativa. Por ejemplo, la división en unidades es simplemente una división en funciones lógicas y puede ser otra división en una implementación real. Por ejemplo, una pluralidad de unidades o componentes pueden combinarse o integrarse en otro sistema, o algunas características pueden ignorarse o no llevarse a cabo. Además, los acoplamientos mutuos o los acoplamientos o conexiones de comunicación directos mostrados o descritos pueden implementarse por medio de varias interfaces. Los acoplamientos o conexiones de comunicación indirectos entre los aparatos o unidades pueden implementarse de manera electrónica, mecánica o de otra forma.

Las unidades descritas como partes separadas pueden estar, o no, físicamente separadas, y las partes mostradas como unidades pueden ser, o no, unidades físicas, pueden estar ubicadas en una posición o pueden estar distribuidas en una pluralidad de unidades de red. Algunas o todas las unidades pueden seleccionarse según las necesidades reales para conseguir los objetivos de las soluciones de las formas de realización.

Además, las unidades funcionales de las formas de realización de la presente invención pueden estar integradas en una unidad de procesamiento, o cada una de las unidades pueden ser físicamente independientes, o dos o más unidades están integradas en una unidad. La unidad integrada puede implementarse en forma de hardware o puede implementarse en forma de hardware junto con una unidad funcional de software.

Cuando la anterior unidad integrada se implementa en forma de unidad funcional de software, la unidad integrada puede almacenarse en un medio de almacenamiento legible por ordenador. La unidad funcional de software se almacena en un medio de almacenamiento e incluye varias instrucciones para hacer que un dispositivo informático (que puede ser un ordenador personal, un servidor o un dispositivo de red) ejecute algunas de las etapas de los procedimientos descritos en las formas de realización de la presente invención. Tales medios de almacenamiento incluyen: cualquier medio que pueda almacenar código de programa, tal como una unidad flash USB, un disco duro extraíble, una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM), un disco magnético o un disco óptico.

Finalmente, debe observarse que las anteriores formas de realización solo pretenden describir las soluciones técnicas de la presente invención y no limitan la presente invención. Aunque la presente invención se ha descrito en detalle con referencia a las anteriores formas de realización, los expertos en la técnica entenderán que pueden realizarse modificaciones en las soluciones técnicas descritas en las anteriores formas de realización o realizarse sustituciones equivalentes en algunas características técnicas de las mismas sin apartarse del alcance de las soluciones técnicas de las formas de realización de la presente invención.

REIVINDICACIONES

1. Un procedimiento de control de gestión para una máquina virtual, donde el procedimiento se lleva a cabo mediante una plataforma de control de seguridad y que comprende:

recibir (101) un mensaje de solicitud de activación de máquina virtual procedente de un equipo de usuario y reenviado por una plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual comprende un identificador de una máquina virtual que es necesario habilitar e información de usuario;
invocar (102) una plataforma fiable de terceros para generar datos cifrados usando una clave de la plataforma fiable de terceros;
enviar los datos cifrados al equipo de usuario usando la plataforma de gestión, de modo que el equipo de usuario descifra los datos cifrados usando una clave privada proporcionada por la plataforma fiable de terceros al usuario autorizado y devuelve los datos descifrados a la plataforma de control de seguridad; y
si se determina que los datos descifrados son iguales a los datos antes del cifrado, determinar que el mensaje de solicitud de activación de máquina virtual se ha generado mediante el equipo de usuario según la instrucción del usuario autorizado; y
autenticar (103) la información de usuario y, si la autenticación es satisfactoria, invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar.

2. El procedimiento según la reivindicación 1, tras invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar, que comprende:

invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual;
si un valor de verificación de integridad no es coherente con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, restringir la habilitación de la máquina virtual; y
si un valor de verificación de integridad es coherente con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, habilitar la máquina virtual.

3. El procedimiento según la reivindicación 1, tras invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar, que comprende:

detectar (301), usando una unidad de supervisión de máquina virtual, que un nuevo programa de aplicación se ha instalado en la máquina virtual;
determinar (302) que el nuevo programa de aplicación se ha instalado mediante el equipo de usuario según una instrucción del usuario autorizado; e
invocar (303) la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual, y actualizar un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad.

4. El procedimiento según la reivindicación 1, tras invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar, que comprende:

recibir un mensaje de solicitud de verificación de integridad de máquina virtual enviado por la plataforma de gestión, donde el mensaje de solicitud de verificación de integridad de máquina virtual es enviado por el equipo de usuario a la plataforma de gestión, y el mensaje de solicitud de verificación de integridad de máquina virtual comprende un identificador de la máquina virtual que requiere una verificación de integridad;
invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual;
comparar un valor de verificación de integridad con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad; y
enviar un resultado de comparación de valor de verificación de integridad a la plataforma de gestión, de modo que la plataforma de gestión envía el resultado de comparación de valor de verificación de integridad al equipo de usuario.

5. El procedimiento según la reivindicación 1, tras invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar, que comprende:

detectar (401), usando una unidad de supervisión de máquina virtual, una solicitud de acceso de una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, y obtener un identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y un identificador de un programa de aplicación;
si se determina que una entrada de tabla de política de control de acceso de la máquina virtual comprende el identificador de la una o más otras máquinas virtuales y el identificador del programa de aplicación obtenidos, invocar (402) la plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual; y

enviar (403) datos de almacenamiento virtual descifrados a la una o más otras máquinas virtuales que generan la solicitud de acceso.

6. El procedimiento según la reivindicación 1, en el que el mensaje de solicitud de activación de máquina virtual comprende además una clave de encapsulación para la máquina virtual que es necesario habilitar; y
después de autenticar la información de usuario, si la autenticación es satisfactoria, el procedimiento comprende:

desencapsular la máquina virtual correspondiente al identificador de la máquina virtual usando la clave de encapsulación, que está incluida en el mensaje de solicitud de activación de máquina virtual, para la máquina virtual que es necesario habilitar.

7. El procedimiento según una cualquiera de las reivindicaciones 1 a 6, en el que la plataforma de control de seguridad comprende un dominio de servicio fiable, TSD, y la plataforma fiable de terceros comprende un módulo de plataforma fiable, TPM, y un módulo criptográfico fiable, TCM.

8. Una plataforma de control de seguridad, que comprende:

un módulo de recepción (51), configurado para recibir un mensaje de solicitud de activación de máquina virtual procedente de un equipo de usuario y reenviado por una plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual comprende un identificador de una máquina virtual que es necesario habilitar e información de usuario;
un módulo de determinación (52), configurado para: sobre la base de que el módulo de recepción (51) recibe el mensaje de solicitud de activación de máquina virtual procedente del equipo de usuario, invocar la plataforma fiable de terceros para generar datos cifrados usando una clave de la plataforma fiable de terceros; enviar los datos cifrados al equipo de usuario usando la plataforma de gestión, de modo que el equipo de usuario descifra los datos cifrados usando una clave privada proporcionada por la plataforma fiable de terceros al usuario autorizado y devuelve datos descifrados a la plataforma de control de seguridad; y si se determina que los datos descifrados son iguales a los datos antes del cifrado, determinar que el mensaje de solicitud de activación de máquina virtual se ha generado por el equipo de usuario según la instrucción del usuario autorizado; y
un módulo de desencapsulación, configurado para: sobre la base de que el módulo de determinación determina que el mensaje de solicitud de activación de máquina virtual ha sido generado por el equipo de usuario según la instrucción del usuario autorizado, después de que la información de usuario se autentique de manera satisfactoria, invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar.

9. La plataforma de control de seguridad según la reivindicación 8, que comprende además:

un módulo de verificación (54), configurado para invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual;
un módulo de restricción de habilitación (55), configurado para: sobre la base de que el módulo de verificación (54) realiza una verificación de integridad en la máquina virtual, si un valor de verificación de integridad no es coherente con un valor de verificación de integridad de la máquina virtual almacenado en la plataforma de control de seguridad, restringir la habilitación de la máquina virtual; y
un módulo de habilitación (56), configurado para: sobre la base de que el módulo de verificación (54) realiza una verificación de integridad en la máquina virtual, si un valor de verificación de integridad es coherente con el valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad, habilitar la máquina virtual.

10. La plataforma de control de seguridad según la reivindicación 8, que comprende además:

un módulo de supervisión (57), configurado para detectar, usando una unidad de supervisión de máquina virtual, que un nuevo programa de aplicación se ha instalado en la máquina virtual, donde
el módulo de verificación (54) está configurado además para: sobre la base de que el módulo de supervisión (57) detecta que el nuevo programa de aplicación se ha instalado en la máquina virtual, si se determina que el nuevo programa de aplicación se ha instalado mediante el equipo de usuario según una instrucción del usuario autorizado, invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual y actualizar un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad.

11. La plataforma de control de seguridad según la reivindicación 8, en la que el módulo de recepción (51) está configurado además para recibir un mensaje de solicitud de verificación de integridad de máquina virtual enviado por la plataforma de gestión, donde el mensaje de solicitud de verificación de integridad de máquina virtual es enviado por el equipo de usuario a la plataforma de gestión, y el mensaje de solicitud de verificación de integridad de máquina virtual comprende un identificador de la máquina virtual que requiere una verificación de integridad; y

el módulo de verificación (54) está configurado además para: en función del mensaje de solicitud de verificación de integridad de máquina virtual recibido por el módulo de recepción (51), invocar la plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual; y
la plataforma de control de seguridad comprende además:

un módulo de comparación (58), configurado para: sobre la base de que el módulo de verificación (54) realiza una verificación de integridad en la máquina virtual, comparar un valor de verificación de integridad con un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad; y enviar un resultado de comparación de valor de verificación de integridad a la plataforma de gestión, de manera que la plataforma de gestión envía el resultado de comparación de valor de verificación de integridad al equipo de usuario.

12. La plataforma de control de seguridad según la reivindicación 8, en la que el módulo de supervisión (57) está configurado además para detectar, usando una unidad de supervisión de máquina virtual, una solicitud de acceso de una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, y obtener un identificador de la una o más otras máquinas virtuales que inician la solicitud de acceso y un identificador de un programa de aplicación; y
el módulo de desencapsulación (53) está configurado además para: sobre la base de que el módulo de supervisión (57) detecta la solicitud de acceso de la una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, si se determina que una entrada de tabla de política de control de acceso de la máquina virtual comprende el identificador de la una o más otras máquinas virtuales y el identificador del programa de aplicación obtenidos, invocar la plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual; y enviar los datos de almacenamiento virtual descifrados a la una o más otras máquinas virtuales que inician la solicitud de acceso.

13. La plataforma de control de seguridad según la reivindicación 8, en la que el mensaje de solicitud de activación de máquina virtual comprende además una clave de encapsulación para la máquina virtual que es necesario habilitar; y
el módulo de desencapsulación (53) está configurado además para: en función del mensaje de solicitud de activación de máquina virtual recibido por el módulo de recepción (51), desencapsular la máquina virtual correspondiente al identificador de la máquina virtual usando la clave de encapsulación, que está incluida en el mensaje de solicitud de activación de máquina virtual, para la máquina virtual que es necesario habilitar.

14. La plataforma de control de seguridad según una cualquiera de las reivindicaciones 11 a 13, donde la plataforma de control de seguridad comprende un dominio de servicio fiable, TSD.

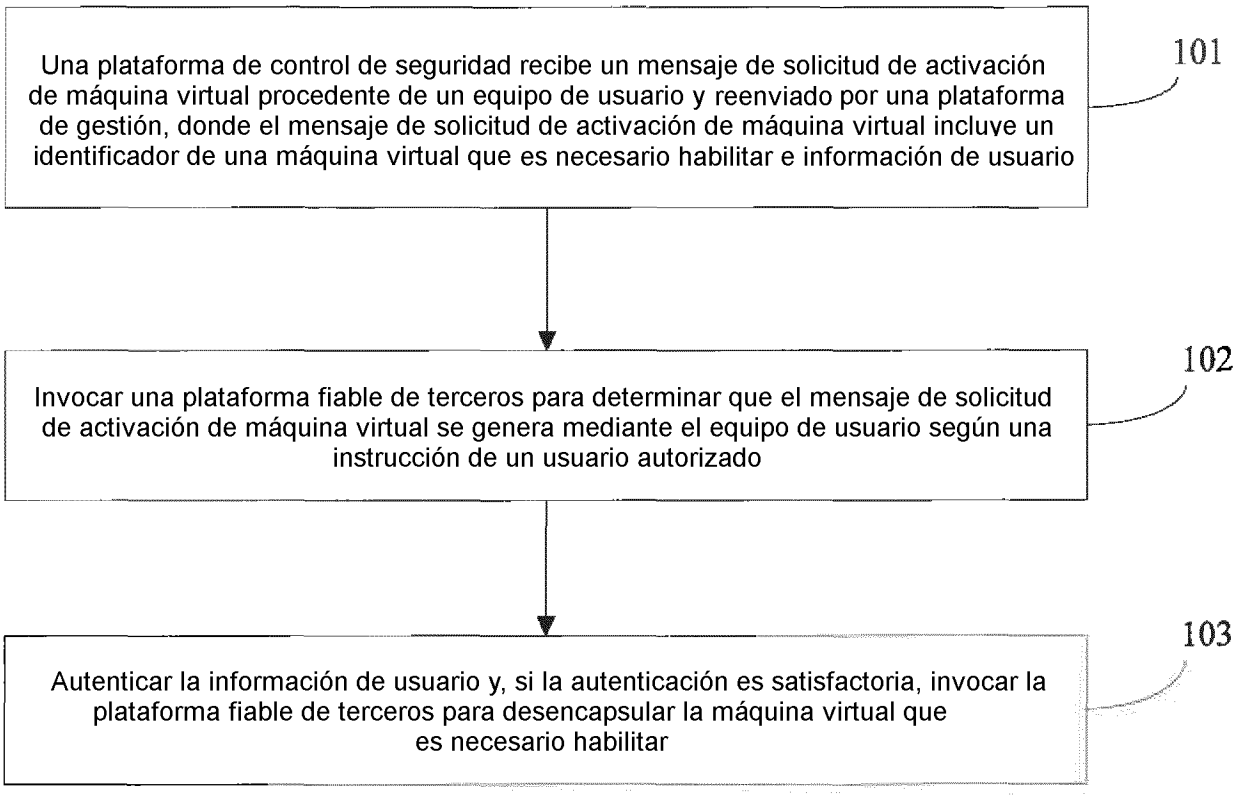
Una plataforma de control de seguridad recibe un mensaje de solicitud de activación de máquina virtual procedente de un equipo de usuario y reenviado por una plataforma de gestión, donde el mensaje de solicitud de activación de máquina virtual incluye un identificador de una máquina virtual que es necesario habilitar e información de usuario
101
Invocar una plataforma fiable de terceros para determinar que el mensaje de solicitud de activación de máquina virtual se genera mediante el equipo de usuario según una instrucción de un usuario autorizado
102
Autenticar la información de usuario y, si la autenticación es satisfactoria, invocar la plataforma fiable de terceros para desencapsular la máquina virtual que es necesario habilitar
103

FIG. 1

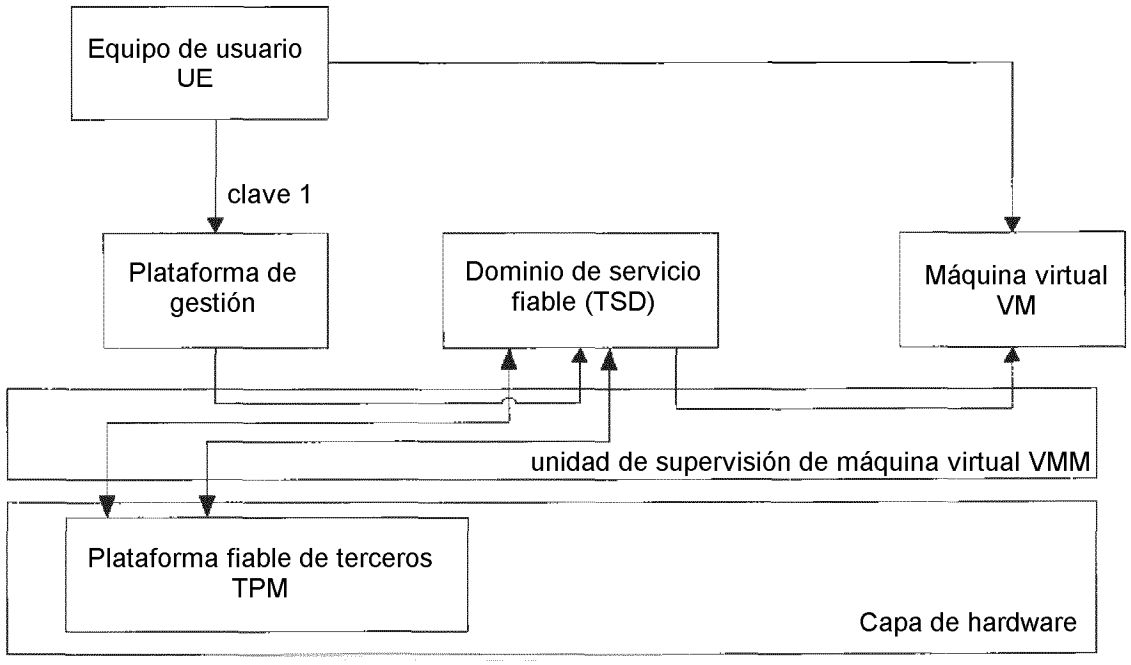
Equipo de usuario UE
clave 1
Plataforma de gestión
Dominio de servicio fiable (TSD)
Máquina virtual VM
unidad de supervisión de máquina virtual VMM
Plataforma fiable de terceros TPM
Capa de hardware

FIG. 2

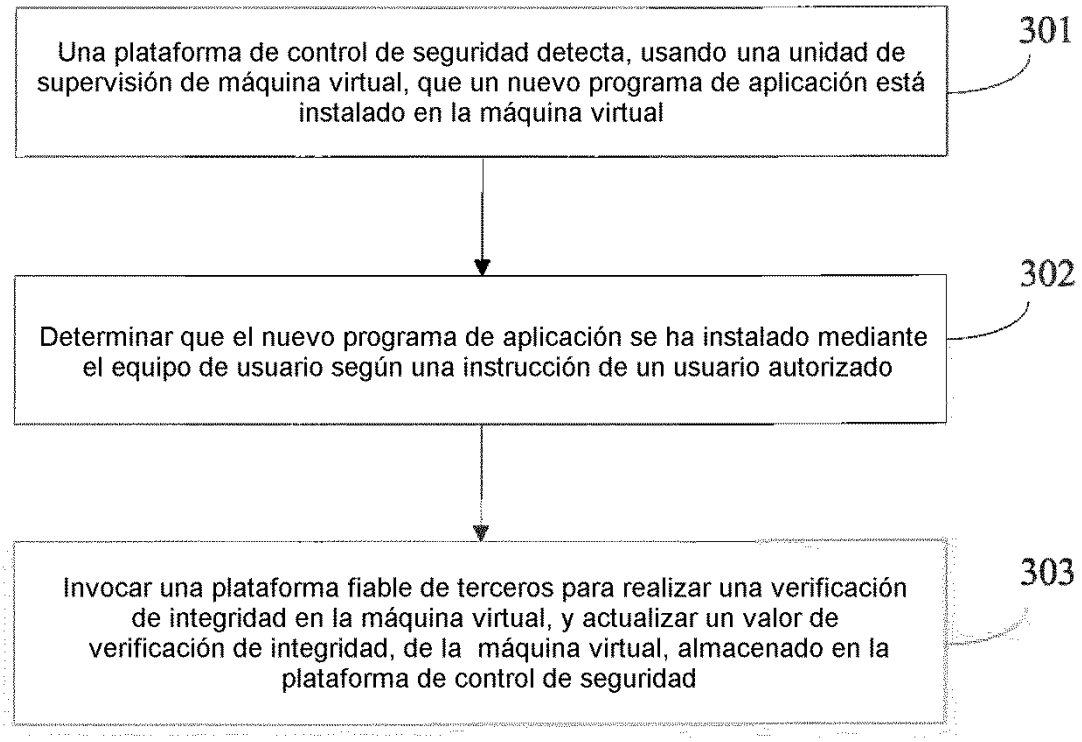
Una plataforma de control de seguridad detecta, usando una unidad de supervisión de máquina virtual, que un nuevo programa de aplicación está instalado en la máquina virtual
301
Determinar que el nuevo programa de aplicación se ha instalado mediante el equipo de usuario según una instrucción de un usuario autorizado
302
Invocar una plataforma fiable de terceros para realizar una verificación de integridad en la máquina virtual, y actualizar un valor de verificación de integridad, de la máquina virtual, almacenado en la plataforma de control de seguridad
303

FIG. 3

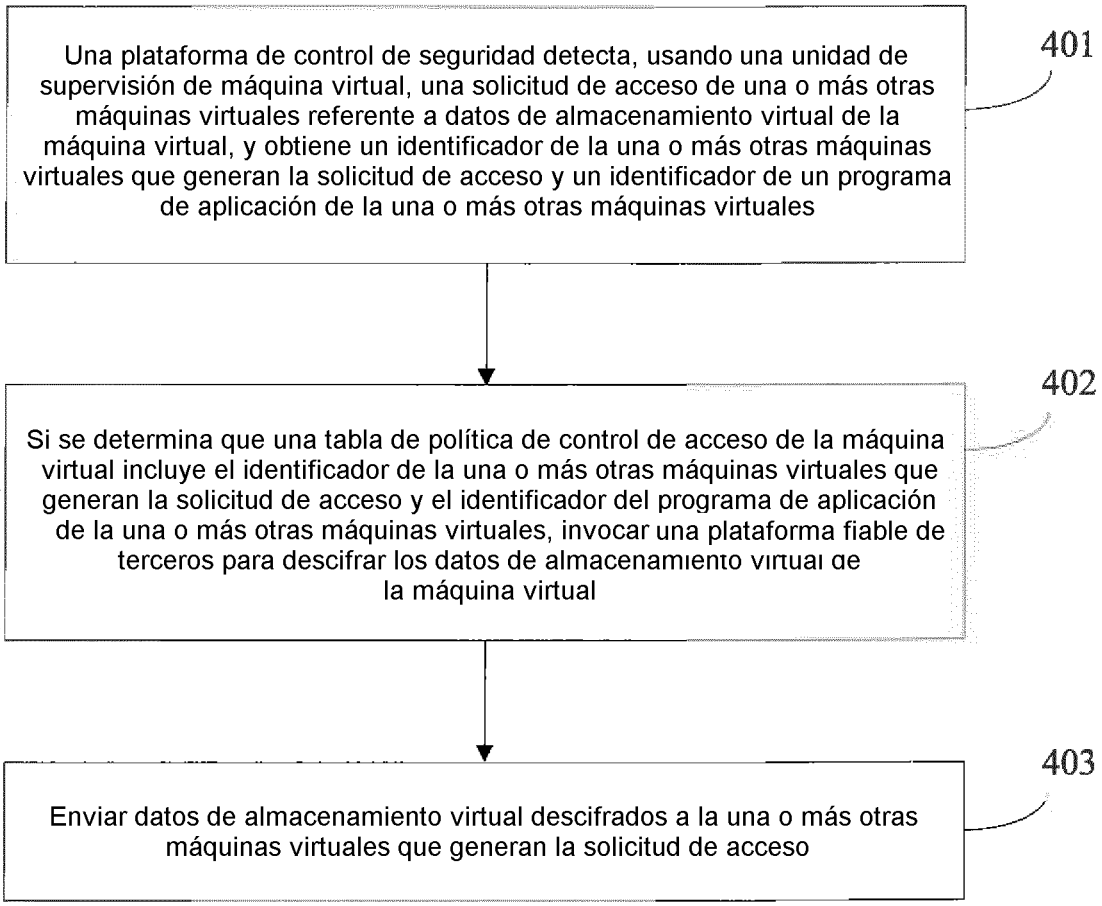
Una plataforma de control de seguridad detecta, usando una unidad de supervisión de máquina virtual, una solicitud de acceso de una o más otras máquinas virtuales referente a datos de almacenamiento virtual de la máquina virtual, y obtiene un identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y un identificador de un programa de aplicación de la una o más otras máquinas virtuales
401
Si se determina que una tabla de política de control de acceso de la máquina virtual incluye el identificador de la una o más otras máquinas virtuales que generan la solicitud de acceso y el identificador del programa de aplicación de la una o más otras máquinas virtuales, invocar una plataforma fiable de terceros para descifrar los datos de almacenamiento virtual de la máquina virtual
402
Enviar datos de almacenamiento virtual descifrados a la una o más otras máquinas virtuales que generan la solicitud de acceso
403

FIG. 4

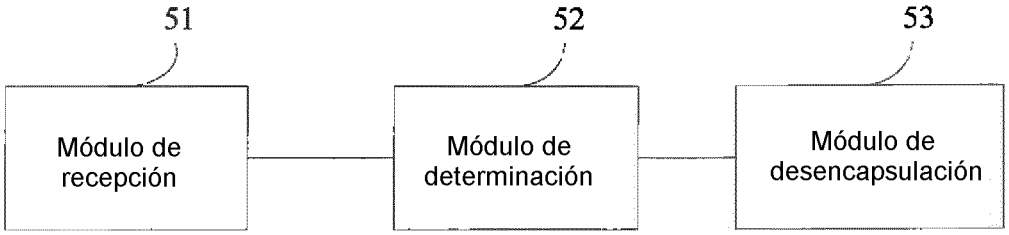
51
Módulo de recepción
52
Módulo de determinación
53
Módulo de desencapsulación

FIG. 5

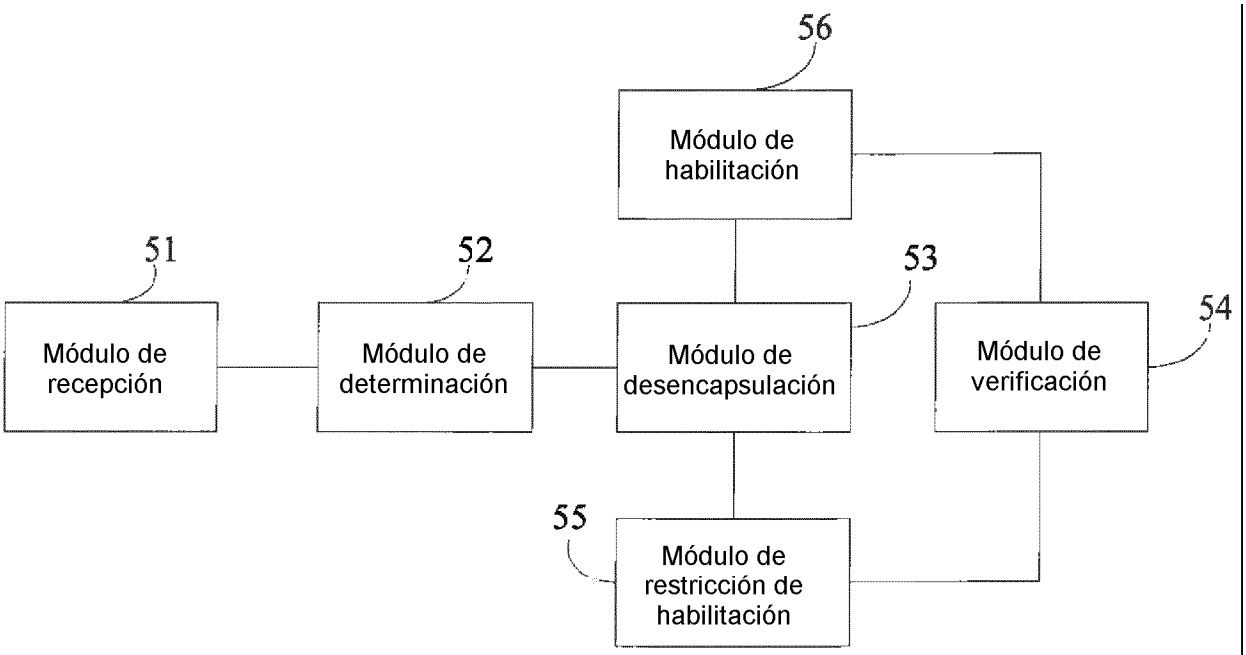
56
Módulo de habilitación
51
Módulo de recepción
52
Módulo de determinación
53
Módulo de desencapsulación
54
Módulo de verificación
55
Módulo de restricción de habilitación

FIG. 6

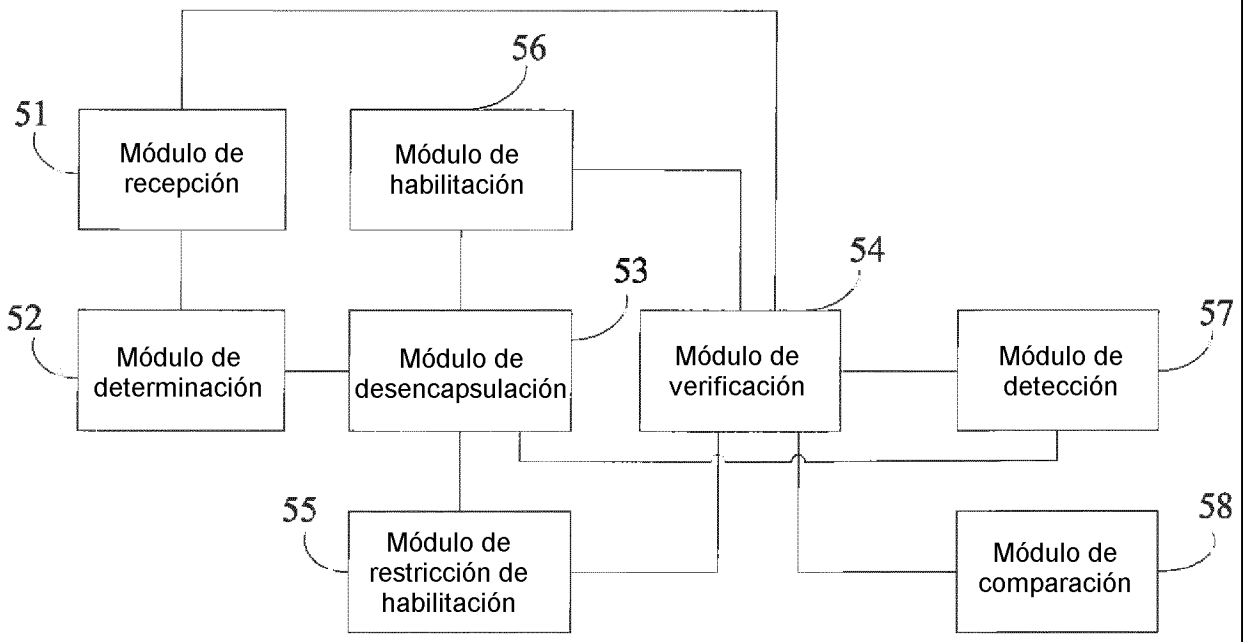
56
51
Módulo de recepción
Módulo de habilitación
53
54
52
Módulo de determinación
Módulo de desencapsulación
Módulo de verificación
57
Módulo de detección
55
Módulo de restricción de habilitación
58
Módulo de comparación

FIG. 7