República Federativa do Brasil

Ministério do Desenvolvimento, Indústria, Comércio e Serviços

Instituto Nacional da Propriedade Industrial

(11) BR 112017011074-1 B1

(22) Data do Depósito: 27/05/2015

(45) Data de Concessão: 22/02/2023

(54) Título: APARELHO E MÉTODO PARA PROCESSAR UM COMPORTAMENTO DE ATAQUE EM UM SISTEMA DE COMPUTAÇÃO EM NUVEM

(51) Int.Cl.: G06F 21/56.

(30) Prioridade Unionista: 26/11/2014 CN 201410709018.9.

(73) Titular(es): HUAWEI TECHNOLOGIES CO., LTD..

(72) Inventor(es): ZECHAO MENG; HEWEI LIU.

(86) Pedido PCT: PCT CN2015079897 de 27/05/2015

(87) Publicação PCT: WO 2016/082501 de 02/06/2016

(85) Data do Início da Fase Nacional: 25/05/2017

(57) Resumo: MÉTODO, APARELHO E SISTEMA PARA PROCESSAR COMPORTAMENTO DE ATAQUE DE APLICAÇÃO DE NUVEM EM SISTEMA DE COMPUTAÇÃO EM NUVEM. Um aparelho (20) para processar um comportamento deataque de uma aplicação de nuvem em um sistema de computação em nuvem é divulgado, incluindo: um gestor de políticas (201) que é configurado para armazenar uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa; um analisador de segurança (202) sendo configurado para receber dados de comportamento de aplicação enviados por um detector de segurança (205), e quando determina que a aplicação de nuvem executada no hospedeiro de nuvem tem um comportamento de ataque, envia os dados de comportamento de aplicação para um processador de segurança (203); e o processador de segurança (203) é configurado para invocar, de acordo com a regra de processamento de aplicação maliciosa, uma interface fornecida por um controlador de nuvem (206), para processar a aplicação de nuvem tendo um comportamento de ataque. O aparelho (20) executa proteção de segurança com base em um nível de aplicação de computação em nuvem, o que pode impedir ataques mútuos entre diferentes aplicações em um mesmo hospedeiro, e reduzir o impacto em uma aplicação normal.

"APARELHO E MÉTODO PARA PROCESSAR UM COMPORTAMENTO DE ATAQUE EM UM SISTEMA DE COMPUTAÇÃO EM NUVEM"

CAMPO TÉCNICO

[001] A presente invenção refere-se ao campo das tecnologias de computador e, em particular, a um método e a um aparelho para processar um comportamento de ataque de uma aplicação de nuvem em um sistema de computação em nuvem, e um sistema.

FUNDAMENTOS

[002] Como definido pelo Instituto Nacional de Padrões e Tecnologia (NIST), computação em nuvem tem três modos de serviço, nomeadamente, software como UM serviço (SaaS), plataforma como UM serviço (PaaS) e infraestrutura como um serviço (IaaS). O PaaS é um modo comercial de fornecer uma plataforma de servidor como um serviço. A PaaS fornece principalmente recursos de hardware, como uma CPU e uma memória e recursos de software, como um sistema operacional e uma biblioteca em que um programa depende de uma aplicação de nuvem, e um desenvolvedor da aplicação de nuvem não precisa considerar ambientes de software e hardware em que a aplicação é executada, e se concentra no desenvolvimento do programa de aplicação. O surgimento da PaaS acelera o desenvolvimento e a implantação de aplicações de nuvem; portanto, nesta era da Internet, mais aplicações de nuvem podem ser implantadas em um sistema de computação em nuvem.

[003] No sistema de computação em nuvem (que pode ser brevemente referido como um sistema de nuvem), para aumentar a utilização de recursos de hardware do sistema, geralmente, várias aplicações de nuvem podem ser executadas em um mesmo hospedeiro de nuvem (que é um hospedeiro de hardware ou um hospedeiro virtual, e tem implementações diferentes para

diferentes sistemas de computação em nuvem), e o sistema de computação em nuvem fornece isolamento de recursos de sistema necessário para as aplicações de nuvem, para garantir que as aplicações de nuvem executadas no mesmo hospedeiro de nuvem não interfiram entre si. Além disso, o sistema de computação em nuvem fornece ainda uma rede virtual no hospedeiro de nuvem, de modo que as aplicações de nuvem se comunicam entre si.

[004] Em outro aspecto, no campo de segurança de rede, antes de atacar uma máquina alvo, os hackers geralmente procuram zumbis (máquinas de fantoches que podem ser controladas) em uma rede primeiro, e lançam ataques usando os zumbis, para ocultar suas identidades. Desta forma, mesmo que as partes atacadas detectem os ataques, eles podem encontrar apenas endereços dos zumbis, mas não conseguem encontrar endereços reais dos hackers. Após o surgimento do sistema de computação em nuvem, os hackers de rede não precisam mais pesquisar zumbis, mas executam diretamente seus programas de ataque no sistema de computação em nuvem, e podem executar várias instâncias dos programas de ataque, para formar um sistema de ataque em larga escala. No sistema de computação em nuvem, os hackers não só podem atacar o alvo usando o programa de ataque original, mas também podem atacar programas de aplicação em diferentes hospedeiros de nuvem no sistema de computação em nuvem e até mesmo outros programas de aplicação em um mesmo hospedeiro de nuvem usando o programa de ataque e usando uma característica que muitos programas de aplicação de nuvem executam no sistema de computação em nuvem.

[005] Na técnica anterior, um problema que o sistema de computação em nuvem é atacado é geralmente resolvido por

meio de detecção de tráfego e limpeza de tráfego. Conforme ilustrado na Figura 1, um aparelho de detecção de tráfego é adicionado no sistema de computação em nuvem, e é conectado a um hospedeiro de nuvem do sistema de computação em nuvem utilizando um comutador para detectar uma entrada de fluxo de dados para o hospedeiro de nuvem no sistema de computação em nuvem, em que o fluxo de dados inclui um fluxo de dados gerado quando um usuário fora do sistema de computação em nuvem acessa uma aplicação de nuvem, e um fluxo de dados gerado quando hospedeiros de nuvem no sistema de computação em nuvem interagem uns com os outros. O aparelho de detecção de tráfego coleta estatísticas em um volume de tráfego de um fluxo de dados que é introduzido em um hospedeiro de nuvem dentro da duração predefinida, e quando o volume de tráfego obtido através da coleta de estatísticas excede um limiar predefinido, a entrada de tráfego para o hospedeiro de nuvem é considerada anormal. Depois de detectar que o tráfego é anormal, o aparelho de detecção de tráfego pode instruir um aparelho de limpeza de tráfego para iniciar. O dispositivo de limpeza de tráfego limpa a entrada de fluxo de dados para o hospedeiro de nuvem, remove um pacote de ataque, e envia o fluxo de dados limpo para o hospedeiro de nuvem.

[006] A solução da técnica anterior pode impedir somente ataques entre hospedeiros de nuvem em um sistema de computação em nuvem ou ataques externos lançados em um hospedeiro de nuvem em um sistema de computação em nuvem, mas não pode impedir ataques mútuos entre diferentes aplicações de nuvem em um mesmo hospedeiro de nuvem, ou ataques internos lançados em um hospedeiro de nuvem. Além disso, na solução da técnica anterior, monitoramento e

limpeza de tráfego são realizados utilizando um hospedeiro de nuvem como uma unidade, o que pode afetar todas as aplicações de nuvem em um hospedeiro de nuvem alvo.

SUMÁRIO

[007] Modalidades da presente invenção fornecem um método e um aparelho para processar um comportamento de ataque de uma aplicação de nuvem em um sistema de computação em nuvem, e um sistema, que são utilizados para executar proteção de segurança de nível de aplicação em um sistema de computação em nuvem, e reduzir o impacto sobre uma aplicação de nuvem normal no sistema de computação em nuvem, tanto quanto possível.

[008] De acordo com um primeiro aspecto, uma modalidade da presente invenção fornece um aparelho para processar um comportamento de ataque de uma aplicação de nuvem em um sistema de computação em nuvem, incluindo:

um analisador de segurança, um processador de segurança e um gestor de políticas, em que

o gestor de políticas é configurado para armazenar uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa;

o analisador de segurança é configurado para receber dados de comportamento de aplicação enviados por um detector de segurança em pelo menos um hospedeiro de nuvem entre múltiplos hospedeiros de nuvem em um sistema de computação em nuvem, determinar, de acordo com os dados de comportamento de aplicação e a regra de determinação de segurança que é armazenada na gestor de políticas, se uma aplicação de nuvem executando em pelo menos um hospedeiro de nuvem tem um comportamento de ataque, e ao determinar que a aplicação de

nuvem executando no pelo menos um hospedeiro de nuvem tem um comportamento de ataque, enviar os dados de comportamento de aplicação para o processador de segurança, em que os dados de comportamento de aplicação são obtidos depois que o detector de segurança no pelo menos um hospedeiro de nuvem detecta a aplicação de nuvem de acordo com uma regra de detecção de comportamento, e os dados de comportamento de aplicação são utilizados para representar um estado de execução da aplicação de nuvem; e

o processador de segurança é configurado para invocar, de acordo com a regra de processamento de aplicação maliciosa armazenada no gestor de políticas, uma interface fornecida por um controlador de nuvem no sistema de computação em nuvem, para processar a aplicação de nuvem tendo um comportamento de ataque, em que o controlador de nuvem é comunicativamente conectado aos hospedeiros de nuvem no sistema de computação em nuvem ou é integrado a um hospedeiro de nuvem, e é configurado para controlar aplicações de nuvem em execução em nuvem os hospedeiros no sistema de computação em nuvem.

[009] Em uma primeira forma possível de implementação do primeiro aspecto, o aparelho inclui ainda: um notificador de informação, em que o gestor de políticas é ainda configurado para armazenar uma regra de notificação de informação;

o analisador de segurança é ainda configurado para: ao determinar que a aplicação de nuvem tem um comportamento de ataque, adquirir informação inicial da aplicação de nuvem, e enviar a informação inicial ao processador de segurança, em que a informação inicial é utilizada para identificar unicamente a aplicação de nuvem;

o processador de segurança é ainda configurado para pesquisar, de acordo com a informação inicial da aplicação de nuvem, a informação de usuário à qual a aplicação de nuvem pertence, e enviar a informação de usuário e os dados de comportamento de aplicação da aplicação de nuvem para o notificador de informação; e

o notificador de informação é configurado para armazenar os dados de comportamento de aplicação recebidos e a informação de usuário, e executar processamento de notificação de informação de ataque de acordo com a regra de notificação de informação armazenada no gestor de políticas.

[0010] Com referência ao primeiro aspecto ou à primeira forma possível de implementação do primeiro aspecto, em uma segunda forma possível de implementação, o gestor de políticas é configurado para converter a regra de determinação de segurança na regra de detecção de comportamento, e entregar a regra de detecção de comportamento ao detector de segurança de cada dos hospedeiros de nuvem.

[0011] Com referência ao primeiro aspecto, ou a qualquer uma da primeira e segunda formas possíveis de implementação do primeiro aspecto, em uma terceira forma possível de implementação, a aplicação maliciosa é uma aplicação de nuvem tendo um comportamento de ataque; e o processador de segurança é configurado especificamente para executar processamento correspondente na aplicação de nuvem de acordo com um tipo do comportamento de ataque da aplicação de nuvem, e uma maneira de processar o tipo de aplicação que é indicada pela regra de processamento de aplicação maliciosa; ou o processador de segurança é configurado especificamente para executar processamento correspondente na aplicação de nuvem

de acordo com um nível de perigo do comportamento de ataque da aplicação de nuvem, e uma maneira de processar uma aplicação tendo o nível de perigo que é indicada pela regra de processamento de aplicação maliciosa.

[0012] Com referência a qualquer uma da primeira à terceira formas possíveis de implementação do primeiro aspecto, em uma quarta forma possível de implementação, o processamento de notificação de informação de ataque inclui especificamente uma ou qualquer combinação do seguinte: gerar informação de alarme, exibir uma aplicação de nuvem tendo um comportamento de ataque e informação de usuário à qual a aplicação de nuvem pertence, e notificar um centro de alarme de informação de usuário à qual uma aplicação de nuvem tendo um comportamento de ataque pertence.

[0013] Com referência ao primeiro aspecto, ou a qualquer uma da primeira à quarta formas possíveis de implementação do primeiro aspecto, em uma quinta forma possível de implementação, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é integrado no controlador de nuvem.

[0014] Com referência a qualquer uma da primeira à quinta formas possíveis de implementação do primeiro aspecto, em uma sexta forma possível de implementação, a interface de configuração do gestor de políticas inclui pelo menos uma de uma janela de configuração e uma interface de programação de aplicação.

[0015] Com referência ao primeiro aspecto, ou a qualquer uma da primeira à quinta formas possíveis de implementação do primeiro aspecto, em uma sétima forma possível de implementação, a regra de detecção de comportamento inclui

uma regra de detecção de processo ou uma regra de detecção de rotina; e os dados de comportamento de aplicação são obtidos depois que o detector de segurança detecta um processo ou uma rotina da aplicação de nuvem de acordo com a regra de detecção de comportamento.

[0016] Com referência à sétima forma possível de implementação do primeiro aspecto, em uma oitava forma possível de implementação, o analisador de segurança é ainda configurado para: ao determinar que a aplicação de nuvem não tem um comportamento de ataque, descartar os dados de comportamento de aplicação de nuvem.

[0017] Com referência a todas as formas possíveis de implementação do primeiro aspecto, em uma nona forma possível de implementação, o hospedeiro de nuvem pode ser uma máquina física ou uma máquina virtual em execução em uma máquina física.

[0018] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma décima forma possível de implementação, um programa de aplicação em execução em um hospedeiro de nuvem é uma aplicação de nuvem, e uma ou mais aplicações de nuvem são executadas em cada hospedeiro de nuvem, em que cada aplicação de nuvem é configurada para implementar uma função de serviço correspondente.

[0019] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma décima primeira forma possível de implementação, um detector de segurança é implementado em cada hospedeiro de nuvem, em que o detector de segurança é configurado para coletar, de acordo com a regra de detecção de comportamento, comportamentos de uma

aplicação de nuvem executando no hospedeiro de nuvem, gerar dados de comportamento de aplicação de acordo com um resultado de coleta, e relatar os dados de comportamento de aplicação ao analisador de segurança.

[0020] Com referência à décima primeira forma possível de implementação do primeiro aspecto, em uma décima segunda forma possível de implementação, o detector de segurança relata os dados de comportamento de aplicação para o analisador de segurança periodicamente, ou com base em uma solicitação, ou de acordo com uma política de relatório pré-configurada.

[0021] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma décima terceira forma possível de implementação, a regra de determinação de segurança é utilizada para definir qual comportamento de uma aplicação de nuvem é um comportamento de ataque; a regra de processamento de aplicação maliciosa é utilizada para definir uma forma de processar uma aplicação de nuvem tendo um comportamento de ataque; e a regra de detecção de comportamento é utilizada para indicar um indicador de detecção utilizado para detectar uma aplicação de nuvem.

[0022] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma décima quarta forma possível de implementação, uma aplicação de nuvem tendo um comportamento de ataque é definida como uma aplicação maliciosa.

[0023] Com referência a qualquer uma da terceira à quarta formas possíveis de implementação do primeiro aspecto, em uma décima quinta forma possível de implementação, o analisador de segurança ou o processador de segurança é

configurado para pesquisar uma biblioteca de recursos de aplicação pré-configurada de acordo com os dados de comportamento da aplicação de nuvem, para determinar um tipo do comportamento de ataque da aplicação, em que a biblioteca de recursos de aplicação é utilizada para descrever uma relação de mapeamento entre um recurso de comportamento de uma aplicação e um tipo de um comportamento de ataque da aplicação.

[0024] Com referência à décima primeira forma possível de implementação do primeiro aspecto, em uma décima sexta forma possível de implementação, a biblioteca de recursos de aplicação é um conjunto de dados independente no sistema de computação em nuvem ou um subconjunto da regra de determinação de segurança; após determinar, de acordo com a regra de determinação de segurança, que uma aplicação de nuvem é uma aplicação maliciosa, o analisador de segurança determina ainda um tipo de um comportamento de ataque da aplicação maliciosa de acordo com a biblioteca de recursos de aplicação incluída na regra de determinação de segurança.

[0025] Com referência a qualquer uma da terceira à décima sexta forma possível de implementação do primeiro aspecto, em uma décima sétima forma possível de implementação, um nível de perigo de uma aplicação de nuvem é utilizado para representar um grau de dano causado ao sistema de computação em nuvem pela aplicação de nuvem; e o analisador de segurança ou o processador de segurança é configurado para determinar um nível de perigo do comportamento de ataque da aplicação de acordo com o tipo de comportamento de ataque da aplicação e por pesquisar uma tabela de mapeamento, em que a tabela de mapeamento é utilizada para representar uma correspondência

entre um tipo de um comportamento de ataque de uma aplicação e um nível de perigo da aplicação.

[0026] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma décima oitava forma possível de implementação, a informação de usuário da aplicação de nuvem inclui, mas não está limitada a um ou mais de um nome de usuário, um endereço de correio eletrônico de usuário, e um número de identidade de usuário.

[0027] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma décima nona forma possível de implementação, a informação inicial da aplicação de nuvem inclui um ID de processo e um nome de processo.

[0028] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma vigésima forma possível de implementação, a invocação de um controlador de nuvem para processar uma aplicação maliciosa inclui uma ou qualquer combinação dos seguintes: fechar a aplicação maliciosa, migrar a aplicação maliciosa para um hospedeiro de nuvem isolado, e desativar uma conta de usuário da aplicação maliciosa.

[0029] Com referência a qualquer uma das formas possíveis de implementação do primeiro aspecto, em uma vigésima primeira forma possível de implementação, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é um hospedeiro de nuvem no sistema de computação em nuvem; o hospedeiro de nuvem é uma máquina virtual em execução em uma máquina física; a máquina física inclui uma camada de hardware, um monitor de máquina virtual em execução acima da camada de hardware, e uma máquina de hospedeiro e várias máquinas virtuais em execução acima do monitor de máquina

virtual, em que a camada de hardware inclui um processador e uma memória; um programa executável é executado no hospedeiro de nuvem, em que o programa executável inclui: um módulo de gestor de políticas, um módulo de analisador de segurança, um módulo de processador de segurança e um módulo de notificador de informação, em que o módulo de gestor de políticas é configurado para implementar funções do gestor de políticas em qualquer uma das formas possíveis de implementação anteriores, o módulo de analisador de segurança é configurado para implementar funções do analisador de segurança de qualquer uma das formas possíveis de implementação anteriores, o módulo de processador de segurança é configurado para implementar funções do processador de segurança em qualquer uma das módulo de processador de segurança anteriores, e o módulo de notificador de informação é configurado para implementar funções do notificador de informação em qualquer uma das formas possíveis de implementação anteriores.

[0030] Com referência ao primeiro aspecto ou a qualquer uma da primeira à vigésima formas possíveis de implementação do primeiro aspecto, em uma vigésima segunda forma possível de implementação, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem inclui pelo menos um processador, uma memória, e pelo menos um barramento de comunicações, em que o barramento de comunicações é configurado para implementar conexão e comunicação entre esses componentes, e a memória armazena os seguintes elementos, módulos executáveis, ou estruturas de dados, ou seu subconjunto, ou seu conjunto estendido:

um sistema operacional, que inclui vários programas de

sistema e é configurado para implementar vários serviços básicos e processar uma tarefa baseada em hardware; e

um módulo de programa de aplicação, que inclui várias aplicações de nuvem e é configurado para implementar vários serviços de aplicação, em que

o módulo de programa de aplicação inclui módulos implementando as funções do gestor de políticas, o analisador de segurança, o processador de segurança e o notificador de informação.

[0031] De acordo com um segundo aspecto, uma modalidade da presente invenção fornece um método para processar um comportamento de ataque de uma aplicação de nuvem, utilizado em um sistema de computação em nuvem incluindo múltiplos hospedeiros de nuvem, incluindo:

receber dados de comportamento de aplicação relatados por pelo menos um hospedeiro de nuvem entre os múltiplos hospedeiros de nuvem, em que os dados de comportamento de aplicação são obtidos depois que um detector de segurança no hospedeiro de nuvem detecta, de acordo com uma regra de detecção de comportamento, e os dados de comportamento de aplicação são utilizados para representar um estado de execução da aplicação de nuvem executando no hospedeiro de nuvem;

determinar, de acordo com os dados de comportamento de aplicação e uma regra de determinação de segurança, se a aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque; e

se for determinado que a aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque, invocar, de acordo com uma regra de processamento de aplicação

maliciosa, uma interface fornecida por um controlador de nuvem no sistema de computação em nuvem, para processar a aplicação de nuvem tendo um comportamento de ataque, em que o controlador de nuvem é conectado ao hospedeiro de nuvem ou é integrado ao hospedeiro de nuvem, e é configurado para controlar uma aplicação de nuvem executando no hospedeiro de nuvem.

[0032] Em uma primeira forma possível de implementação do segundo aspecto, o método inclui ainda:

se for determinado que a aplicação de nuvem executada no hospedeiro de nuvem tem um comportamento de ataque, pesquisar, de acordo com informação inicial da aplicação de nuvem tendo um comportamento de ataque, informação de usuário à qual a aplicação de nuvem pertence, em que a informação inicial é utilizada para identificar a aplicação de nuvem; e

armazenar os dados de comportamento de aplicação da aplicação de nuvem tendo um comportamento de ataque e a informação de usuário que é obtida através da pesquisa, e executar processamento de notificação de informação de ataque de acordo com uma regra de notificação de informação.

[0033] Com referência ao segundo aspecto ou à primeira forma possível de implementação do segundo aspecto, em uma segunda forma possível de implementação, o método inclui ainda:

se for determinado que a aplicação de nuvem executada no hospedeiro de nuvem não tem um comportamento de ataque, descartar os dados de comportamento de aplicação recebidos.

[0034] Com referência ao segundo aspecto, ou a qualquer uma da primeira e segunda formas possíveis de implementação do segundo aspecto, em uma terceira forma possível de

implementação, uma aplicação maliciosa é uma aplicação de nuvem tendo um comportamento de ataque; e a invocação de uma interface fornecida por um controlador de nuvem, para executar processamento correspondente na aplicação de nuvem tendo um comportamento de ataque inclui: executar processamento correspondente na aplicação de nuvem de acordo com um tipo do comportamento de ataque da aplicação de nuvem, e uma maneira de processamento do tipo de aplicação que é indicada pela regra de processamento de aplicação maliciosa; ou executar processamento correspondente na aplicação de nuvem de acordo com um nível de perigo do comportamento de ataque da aplicação de nuvem, e uma maneira de processamento de uma aplicação tendo o nível de perigo que é indicada pela regra de processamento de aplicação maliciosa.

[0035] Com referência a qualquer uma da primeira forma possível de implementação para a terceira forma possível de implementação do segundo aspecto, em uma quarta forma possível de implementação, a execução de processamento de notificação de informação de ataque de acordo com uma regra de notificação de informação inclui uma ou de qualquer combinação dos seguintes:

gerar informação de alarme, exibir uma aplicação de nuvem tendo um comportamento de ataque e informação de usuário à qual a aplicação de nuvem pertence, e notificar um centro de alarme de informação de usuário à qual uma aplicação de nuvem tendo um comportamento de ataque pertence.

[0036] Com referência ao segundo aspecto ou a qualquer uma da primeira à quarta formas possíveis de implementação do segundo aspecto, em uma quinta forma possível de implementação, o método inclui ainda: converter a regra de

determinação de segurança na regra de detecção de comportamento, e enviar a regra de detecção de comportamento ao detector de segurança.

[0037] Com referência ao segundo aspecto ou a qualquer uma da primeira à quinta formas possíveis de implementação do segundo aspecto, em uma sexta forma possível de implementação, uma ou mais das regras de determinação de segurança, a regra de processamento de aplicação maliciosa e a regra de notificação de informação são configuradas utilizando uma interface de configuração, em que a interface de configuração inclui pelo menos uma de uma janela de configuração e uma interface de programação de aplicação.

[0038] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma sétima forma possível de implementação, o hospedeiro de nuvem pode ser uma máquina física ou uma máquina virtual em execução em uma máquina física.

[0039] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma oitava forma possível de implementação, um programa de aplicação em execução em um hospedeiro de nuvem é uma aplicação de nuvem, e uma ou mais aplicações de nuvem são executadas em cada hospedeiro de nuvem, em que cada aplicação de nuvem é configurada para implementar uma função de serviço correspondente.

[0040] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma nona forma possível de implementação, um detector de segurança é implementado em cada hospedeiro de nuvem, em que o detector de segurança é configurado para coletar, de acordo com a regra de detecção

de comportamento, comportamentos de uma aplicação de nuvem executando no hospedeiro de nuvem, gerar dados de comportamento de aplicação de acordo com um resultado de coleta, e relatar os dados de comportamento de aplicação ao analisador de segurança.

[0041] Com referência à nona forma possível de implementação do segundo aspecto, em uma décima forma possível de implementação, o detector de segurança relata os dados de comportamento de aplicação periodicamente, ou com base em uma solicitação, ou de acordo com uma política de relatório pré-configurada.

[0042] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma décima primeira forma possível de implementação, a regra de determinação de segurança é utilizada para definir qual comportamento de uma aplicação de nuvem é um comportamento de ataque; a regra de processamento de aplicação maliciosa é utilizada para definir uma forma de processar uma aplicação de nuvem tendo um comportamento de ataque; e a regra de detecção de comportamento é utilizada para indicar um indicador de detecção utilizado para detectar uma aplicação de nuvem.

[0043] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma décima segunda forma possível de implementação, uma aplicação de nuvem tendo um comportamento de ataque é definida como uma aplicação maliciosa.

[0044] Com referência a qualquer uma da terceira à décima segunda formas possíveis de implementação do segundo aspecto, em uma décima terceira forma possível de implementação, uma biblioteca de recursos de aplicação pré-

configurada é pesquisada de acordo com os dados de comportamento de aplicação de nuvem, para determinar um tipo do comportamento de ataque da aplicação, em que a biblioteca de recursos de aplicação é utilizada para descrever uma relação de mapeamento entre um recurso de comportamento de uma aplicação e um tipo de um comportamento de ataque da aplicação.

[0045] Com referência à décima terceira forma possível de implementação do segundo aspecto, em uma décima quarta forma possível de implementação, a biblioteca de recursos de aplicação é um conjunto de dados independente no sistema de computação em nuvem ou um subconjunto da regra de determinação de segurança; após determinar, de acordo com a regra de determinação de segurança, que uma aplicação de nuvem é uma aplicação maliciosa, um tipo de um comportamento de ataque da aplicação maliciosa é ainda determinado de acordo com a biblioteca de recursos de aplicação incluída na regra de determinação de segurança.

[0046] Com referência a qualquer uma da terceira à décima quarta formas possíveis de implementação do segundo aspecto, em uma décima quinta forma possível de implementação, um nível de perigo de uma aplicação de nuvem é utilizado para representar um grau de dano causado ao sistema de computação em nuvem pela aplicação de nuvem; um nível de perigo do comportamento de ataque da aplicação é determinado de acordo com o tipo do comportamento de ataque da aplicação e por pesquisar uma tabela de mapeamento, em que a tabela de mapeamento é utilizada para representar uma correspondência entre um tipo de um comportamento de ataque de uma aplicação e um nível de perigo da aplicação.

[0047] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma décima sexta forma possível de implementação, a informação de usuário da aplicação de nuvem inclui, mas não estão limitada a, um ou mais de um nome de usuário, um endereço de correio eletrônico de usuário, e um número de identidade de usuário.

[0048] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma décima sétima forma possível de implementação, a informação inicial da aplicação de nuvem inclui um ID de processo ou um nome de processo ou ambos.

[0049] Com referência a todas as formas possíveis de implementação do segundo aspecto, em uma décima oitava forma possível de implementação, a invocação de um controlador de nuvem para processar uma aplicação maliciosa inclui um ou qualquer combinação dos seguintes: fechar a aplicação maliciosa, migrar a aplicação maliciosa para um hospedeiro de nuvem isolado, e desativar uma conta de usuário da aplicação maliciosa.

[0050] De acordo com um terceiro aspecto, uma modalidade da presente invenção fornece um sistema de proteção de segurança de uma aplicação de nuvem, incluindo: um aparelho para processar um comportamento de ataque de uma aplicação de nuvem, um controlador de nuvem, e múltiplos detectores de segurança, em que os múltiplos detectores de segurança são implantados em múltiplos hospedeiros de nuvem, e cada dos hospedeiros de nuvem corresponde a um dos detectores de segurança; o controlador de nuvem é comunicativamente conectado aos múltiplos hospedeiros de nuvem, e é configurado para gerenciar e controlar os múltiplos hospedeiros de nuvem,

e uma ou mais aplicações de nuvem executadas em cada dos hospedeiros de nuvem; e o aparelho para processar um comportamento de ataque de uma aplicação de nuvem armazena uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa;

cada dos detectores de segurança é configurado para detectar uma ou mais aplicações de nuvem de acordo com uma regra de detecção de comportamento, para obter dados de comportamento de aplicação, e relatar os dados de comportamento de aplicação para o aparelho para processar um comportamento de ataque de uma aplicação de nuvem, em que a uma ou mais aplicações de nuvem são executadas em um hospedeiro de nuvem correspondente ao detector de segurança; e

o aparelho para processamento de um comportamento de ataque de uma aplicação de nuvem é configurada para receber os dados de comportamento de aplicação notificados por um detector de segurança em pelo menos um hospedeiro de nuvem entre os múltiplos hospedeiros de nuvem, determinar, de acordo com os dados de comportamento de aplicação e a regra de determinação de segurança, se uma aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque, e se determinar que a aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque, invocar, de acordo com a regra de processamento de aplicação maliciosa, uma interface fornecida pelo controlador de nuvem, para executar processamento correspondente na aplicação de nuvem tendo um comportamento de ataque.

[0051] Em uma primeira forma possível de implementação do terceiro aspecto, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é ainda configurado para

converter a regra de determinação de segurança na regra de detecção de comportamento, e entregar a regra de detecção de comportamento para o detector de segurança de cada dos hospedeiros de nuvem.

[0052] Com referência ao terceiro aspecto, ou à primeira forma possível de implementação do terceiro aspecto, em uma segunda forma possível de implementação, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é ainda configurado para: se determinar que a aplicação de nuvem em execução no hospedeiro de nuvem não tem um comportamento de ataque, descartar os dados de comportamento de aplicação recebidos.

[0053] Com referência ao terceiro aspecto ou à primeira forma possível de implementação do terceiro aspecto, em uma terceira forma possível de implementação, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é ainda configurado para: se determinar que a aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque, exibir a aplicação de nuvem tendo um comportamento de ataque e informação de usuário à qual a aplicação de nuvem pertence, ou notificar um centro de alarme de informação de usuário à qual a aplicação de nuvem tendo um comportamento de ataque pertence.

[0054] Com referência ao terceiro aspecto ou a qualquer uma da primeira à terceira formas possíveis de implementação do terceiro aspecto, em uma quarta forma possível de implementação, o aparelho para processamento de um comportamento de ataque de uma aplicação é comunicativamente conectado ao controlador de nuvem, ou o aparelho para processamento de um comportamento de ataque de uma aplicação

de nuvem é integrado no controlador de nuvem.

[0055] Com referência ao terceiro aspecto, ou a qualquer uma da primeira à quarta formas possíveis de implementação do terceiro aspecto, em uma quinta forma possível de implementação, uma aplicação maliciosa é uma aplicação de nuvem tendo um comportamento de ataque; e o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é configurado especificamente para executar processamento correspondente na aplicação de nuvem de acordo com um tipo do comportamento de ataque da aplicação de nuvem, e uma maneira de processar o tipo de aplicação que é indicada pela regra de processamento de aplicação maliciosa; ou executar processamento correspondente na aplicação de nuvem de acordo com um nível de perigo do comportamento de ataque da aplicação de nuvem, e uma maneira de processar uma aplicação tendo o nível de perigo que é indicada pela regra de processamento de aplicação maliciosa.

[0056] Com referência ao terceiro aspecto ou a qualquer uma da primeira à quinta formas possíveis de implementação do terceiro aspecto, em uma sexta forma possível de implementação, uma ou mais das regras de determinação de segurança, a regra de processamento de aplicação maliciosa e a regra de notificação de informação são configuradas utilizando uma interface de configuração, em que a interface de configuração inclui pelo menos uma de uma janela de configuração e uma interface de programação de aplicação.

[0057] Com referência ao terceiro aspecto, ou a qualquer uma da primeira à sexta formas possíveis de implementação do terceiro aspecto, em uma sétima forma possível de implementação, a regra de detecção de comportamento inclui

uma regra de detecção de processo ou uma regra de detecção de rotina; e os dados de comportamento de aplicação são obtidos depois que o detector de segurança detecta um processo ou uma rotina da aplicação de nuvem de acordo com a regra de detecção de comportamento.

[0058] Com referência ao terceiro aspecto, ou a qualquer uma da primeira à sétima formas possíveis de implementação do terceiro aspecto, em uma oitava forma possível de implementação, a regra de determinação de segurança é utilizada para definir qual comportamento de uma aplicação de nuvem é um comportamento de ataque; a regra de processamento de aplicação maliciosa é utilizada para definir uma forma de processar uma aplicação de nuvem tendo um comportamento de ataque; e a regra de detecção de comportamento é utilizada para indicar um indicador de detecção utilizado para detectar uma aplicação de nuvem.

[0059] Com referência ao terceiro aspecto ou a qualquer uma da primeira à oitava formas possíveis de implementação do terceiro aspecto, em uma nona forma possível de implementação, o aparelho para processar um comportamento de ataque de uma aplicação é configurado para pesquisar uma biblioteca de recursos de aplicação pré-configurada de acordo com os dados de comportamento de aplicação de nuvem, para determinar um tipo do comportamento de ataque da aplicação, em que a biblioteca de recursos de aplicação é utilizada para descrever uma relação de mapeamento entre um recurso de comportamento de uma aplicação e um tipo de um comportamento de ataque da aplicação.

[0060] Com referência à nona forma possível de implementação do terceiro aspecto, em uma décima forma possível de

implementação, a biblioteca de recursos de aplicação é um conjunto de dados independente no sistema de computação em nuvem ou um subconjunto da regra de determinação de segurança; e o aparelho para processar um comportamento de ataque de uma aplicação é configurado para: depois de determinar, de acordo com a regra de determinação de segurança, que uma aplicação de nuvem é uma aplicação maliciosa, determinar um tipo de um comportamento de ataque da aplicação maliciosa de acordo com a biblioteca de recursos de aplicação incluída na regra de determinação de segurança.

[0061] Com referência a qualquer uma da quinta forma possível de implementação do terceiro aspecto, em uma décima primeira forma possível de implementação, um nível de perigo de uma aplicação de nuvem é utilizado para representar um grau de dano causado ao sistema de computação em nuvem pela aplicação de nuvem; e o aparelho para processar um comportamento de ataque de uma aplicação é configurado para determinar um nível de perigo do comportamento de ataque da aplicação de acordo com o tipo de comportamento de ataque da aplicação e por pesquisar uma tabela de mapeamento, em que a tabela de mapeamento é utilizada para representar uma correspondência entre um tipo de um comportamento de ataque de uma aplicação e um nível de perigo da aplicação.

[0062] No método e aparelho para processar um comportamento de ataque de uma aplicação de nuvem, e o sistema que são fornecidos nas modalidades da presente invenção, um gestor de políticas fornece uma regra de detecção de comportamento para um detector de segurança em cada hospedeiro de nuvem, o detector de segurança executa detecção de acordo com a regra de detecção de comportamento, e relata dados de

comportamento de uma aplicação, um analisador de segurança analisa os dados de comportamento de aplicação para determinar uma aplicação tendo um comportamento de ataque, e invoca um controlador de nuvem para executar processamento correspondente. Em comparação com a solução de segurança da técnica anterior, as modalidades da presente invenção realizam proteção de segurança com base em um nível de aplicação de computação em nuvem, que pode satisfazer um cenário de implementação de aplicação de um sistema de computação em nuvem, impedir ataques mútuos entre diferentes aplicações em um mesmo hospedeiro, ou um ataque interno lançado em um hospedeiro, e reduzir o impacto em uma aplicação normal.

BREVE DESCRIÇÃO DOS DESENHOS

[0063] Para descrever as soluções técnicas nas modalidades da presente invenção ou na técnica anterior mais claramente, o que segue apresenta brevemente os desenhos anexos necessários para descrever as modalidades ou a técnica anterior. Aparentemente, os desenhos anexos na descrição que segue mostram apenas algumas modalidades da presente invenção, e uma pessoa com conhecimentos normais na técnica pode ainda derivar outros desenhos a partir destes desenhos anexos sem esforços criativos.

[0064] A Figura 1 é um diagrama esquemático de um princípio de um método para processar um ataque em um sistema de processamento de nuvem na técnica anterior;

[0065] A Figura 2 é um diagrama de uma arquitetura de um sistema de computação em nuvem de acordo com uma modalidade da presente invenção;

[0066] A Figura 3 é um diagrama esquemático de um aparelho

para processar um comportamento de ataque de uma aplicação de nuvem de acordo com uma modalidade da presente invenção;

[0067] A Figura 4 é um diagrama esquemático de um aparelho para processar um comportamento de ataque de uma aplicação de nuvem de acordo com uma modalidade da presente invenção;

[0068] A Figura 5 é um diagrama estrutural esquemático de um gestor de políticas de acordo com uma modalidade da presente invenção;

[0069] A Figura 6 é um fluxograma de trabalho de um analisador de segurança de acordo com uma modalidade da presente invenção;

[0070] A Figura 7 é um diagrama estrutural esquemático de um processador de segurança de acordo com uma modalidade da presente invenção;

[0071] A Figura 8 é um diagrama estrutural esquemático de um notificador de informação de acordo com uma modalidade da presente invenção;

[0072] A Figura 9 é um fluxograma de um método para processar um comportamento de ataque de uma aplicação de nuvem de acordo com uma modalidade da presente invenção;

[0073] A Figura 10 é um fluxograma de um método para processar um comportamento de ataque de uma aplicação de nuvem de acordo com uma modalidade da presente invenção;

[0074] A Figura 11 é um diagrama esquemático de um sistema de proteção de segurança de uma aplicação de nuvem de acordo com uma modalidade da presente invenção;

[0075] A Figura 12 é um diagrama esquemático de um aparelho para processar um comportamento de ataque de uma aplicação de nuvem de acordo com uma modalidade da presente invenção; e

[0076] A Figura 13 é um diagrama esquemático de um aparelho para processar um comportamento de ataque de uma aplicação de nuvem de acordo com uma modalidade da presente invenção.

DESCRIÇÃO DE MODALIDADES

[0077] Para fazer um especialista na técnica compreender melhor as soluções técnicas da presente invenção, o seguinte descreve as soluções técnicas nas modalidades da presente invenção com referência aos desenhos anexos nas modalidades da presente invenção. Aparentemente, as modalidades descritas são apenas algumas, em vez de todas as modalidades da presente invenção.

[0078] As soluções técnicas fornecidas nas modalidades da presente invenção podem ser tipicamente aplicadas em um sistema de computação em nuvem (brevemente referido como um sistema de nuvem), em que o sistema de computação em nuvem pode ser visto como um sistema de agrupamento no qual computação, armazenamento e gestão distribuídos são realizados em hardware geral, e o sistema de computação em nuvem pode fornecer acesso de dados de alta taxa de transferência, e pode ser aplicado em computação e armazenamento de dados de larga escala. A Figura 2 mostra uma arquitetura física de um sistema de computação em nuvem. O sistema de computação em nuvem geralmente inclui vários computadores físicos (que podem ser brevemente referidos como máquinas físicas) que são interligados usando um comutador, e essas máquinas físicas podem ser interconectadas com uma rede externa usando um comutador de agregação e um comutador de núcleo. Uma máquina física pode ser especificamente uma entidade física, como um computador ou um servidor. Em alguns cenários em rede, uma máquina

física no sistema de computação em nuvem pode ser referida como um hospedeiro de nuvem. Com o desenvolvimento de tecnologias de computação em nuvem, atualmente, uma ou mais máquinas virtuais podem ser simuladas em um computador físico usando o software de máquina virtual, e essas máquinas virtuais podem funcionar como computadores reais. Um sistema operacional e um programa de aplicação podem ser instalados em uma máquina virtual, e a máquina virtual pode acessar recursos de rede e similares. Um programa de aplicação é executado em uma máquina virtual como trabalhando em um computador real. Portanto, um sistema de computação em nuvem pode incluir milhares de máquinas virtuais, e um programa de aplicação pode executar independentemente em cada máquina virtual; portanto, em alguns outros cenários em rede mais gerais, uma máquina virtual em um sistema de computação em nuvem é geralmente referida como um hospedeiro de nuvem ou um hospedeiro de nuvem virtual, e um programa de aplicação em execução em um hospedeiro de nuvem é referido como uma aplicação de nuvem. Portanto, o hospedeiro de nuvem descrito em todas as modalidades da presente invenção não está limitado a uma máquina virtual ou a uma máquina física, e depende de um cenário de rede específico. Além disso, o sistema de computação em nuvem inclui ainda um controlador de nuvem, configurado para controlar e gerenciar um hospedeiro de nuvem no sistema de computação em nuvem. O controlador de nuvem pode ser uma das várias máquinas virtuais incluídas no sistema de computação em nuvem. Em alguns casos, o controlador de nuvem também pode ser uma máquina física independente. Certamente, pode haver um ou mais controladores de nuvem; um controlador de nuvem é

comunicativamente conectado a um hospedeiro de nuvem no sistema de computação em nuvem ou é integrado em um hospedeiro de nuvem, e configurado para controlar aplicações de nuvem executadas em múltiplos hospedeiros de nuvem no sistema de computação em nuvem. As soluções nas modalidades da presente invenção podem ser implementadas por um hospedeiro de nuvem no sistema de computação em nuvem e, em alguns casos, podem ser implementadas por um controlador de nuvem. De acordo com uma arquitetura lógica, o sistema de computação em nuvem é geralmente dividido em uma camada de infraestrutura e virtualização (uma camada de IaaS), uma camada de plataforma (uma camada de PaaS), e uma camada de aplicação (uma camada de SaaS). As soluções nas modalidades da presente invenção podem ser implementadas pela camada de plataforma do sistema de computação em nuvem, e podem ser especificamente implementadas por um controlador de nuvem ou outra unidade de função independente na camada de plataforma.

[0079] Uma modalidade da presente invenção fornece um aparelho para processar um comportamento de ataque de uma aplicação de nuvem, em que o aparelho de processamento pode ser aplicado a um sistema de computação em nuvem, para executar proteção de segurança no sistema de computação em nuvem. A Figura 3 é um diagrama esquemático do aparelho para processar um comportamento de ataque de uma aplicação de nuvem de acordo com esta modalidade da presente invenção. Em uma modalidade específica, o aparelho de processamento pode ser um hospedeiro de nuvem no sistema de computação em nuvem, ou pode ser utilizado como uma unidade de função em um controlador de nuvem e integrado no controlador de nuvem. De acordo com a Figura 3, o sistema de computação em nuvem

inclui um aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem, um controlador de nuvem 206 e múltiplos hospedeiros de nuvem (por exemplo, hospedeiros de nuvem 10, 11 e 12 na Figura 3). Uma ou mais aplicações de nuvem são executadas em cada dos hospedeiros de nuvem, e um detector de segurança é implantado em cada dos hospedeiros de nuvem, e é responsável por coletar, de acordo com uma regra de detecção de comportamento fornecida pelo aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem, comportamentos de uma aplicação de nuvem executando no hospedeiro de nuvem, e relatar dados de comportamento de aplicação da aplicação para o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem, em que os dados de comportamento de aplicação são utilizados para representar um estado de execução da aplicação de nuvem, por exemplo, informação de enlace TCP, informação de tráfego de rede, uma quantidade de vezes de invocação de sistema que são da aplicação de nuvem. Opcionalmente, os dados de comportamento de aplicação da aplicação de nuvem podem ser relatados periodicamente ou com base em um pedido. Especificamente, o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem inclui um gestor de políticas 201, um analisador de segurança 202 e um processador de segurança 203.

[0080] O gestor de políticas 201 é principalmente configurado para armazenar, converter e entregar uma regra. Especificamente, o gestor de políticas 201 pode armazenar uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa, em que a regra de determinação de segurança é utilizada para definir qual

comportamento de uma aplicação de nuvem é um comportamento de ataque, e a regra de processamento de aplicação maliciosa é utilizada para definir uma maneira de processar uma aplicação de nuvem tendo um comportamento de ataque. Em uma modalidade, o gestor de políticas 201 pode converter a regra de determinação de segurança na regra de detecção de comportamento, em que a regra de detecção de comportamento é utilizada para definir qual comportamento de uma aplicação de nuvem deve ser detectado, isto é, a regra de detecção de comportamento indica um indicador de detecção para detectar uma aplicação de nuvem. Geralmente, a regra de detecção de comportamento está intimamente relacionada com a regra de determinação de segurança e, portanto, podem ser mutuamente convertidas. Por exemplo, se a regra de determinação de segurança for: se uma quantidade de portas TCP externas solicitadas por uma aplicação de nuvem exceder 100, é determinado que a aplicação de nuvem tem um comportamento de *"sniffing"* de porta; correspondentemente, a regra de detecção de comportamento é: coletar uma quantidade de portas TCP diferentes solicitadas pela aplicação de nuvem. Deste modo, o detector de segurança no servidor de nuvem deve detectar a quantidade de portas TCP diferentes solicitadas pela aplicação de nuvem, e relatar um resultado de detecção ao analisador de segurança 202, e o analisador de segurança 202 pode determinar se a aplicação de nuvem tem um comportamento de "sniffing" de porta.

[0081] O analisador de segurança 202 é configurado principalmente para receber dados de comportamento de aplicação que são relatados por um detector de segurança em pelo menos um hospedeiro de nuvem entre os múltiplos

hospedeiros de nuvem no sistema de computação em nuvem e, em seguida, determinar de acordo com a regra de determinação de segurança armazenada no gestor de políticas 201, se a aplicação de nuvem no hospedeiro de nuvem tem um comportamento de ataque; se determinar que a aplicação de nuvem tem um comportamento de ataque, enviar informação inicial da aplicação de nuvem tendo um comportamento de ataque ao processador de segurança 203, em que a informação inicial da aplicação de nuvem é utilizada para identificar unicamente a aplicação de nuvem. Por exemplo, em uma modalidade específica, a informação inicial pode ser um ID de processo ou um nome de processo, ou incluir ambos. Opcionalmente, o detector de segurança pode relatar os dados de comportamento de aplicação da aplicação de nuvem periodicamente, ou com base em uma solicitação, ou de acordo com uma política de relatório pré-configurada, o que não é especialmente limitado nesta modalidade da presente invenção.

[0082] O processador de segurança 203 é configurado principalmente para: depois de receber a informação inicial da aplicação de nuvem tendo um comportamento de ataque que é enviada pelo analisador de segurança 202, invocar, de acordo com a regra de processamento de aplicação maliciosa armazenada no gestor de políticas 201, uma interface fornecida pelo controlador de nuvem 206, para processar a aplicação de nuvem tendo um comportamento de ataque (nesta modalidade da presente invenção, uma aplicação de nuvem tendo um comportamento de ataque é referida como uma aplicação maliciosa). Em uma modalidade, o processador de segurança 203 pode processar todas as aplicações maliciosas em

conjunto, por exemplo, fechar as aplicações maliciosas, migrar as aplicações maliciosas para um hospedeiro de nuvem isolado, ou desabilitar uma conta de usuário das aplicações maliciosas. Opcionalmente, o processador de segurança 203 pode também executar diferentes graus de processamento ou diferentes tipos de processamento nas aplicações maliciosas de acordo com os tipos de comportamentos de ataque das aplicações maliciosas ou níveis de perigo de comportamentos de ataque das aplicações maliciosas. Por exemplo, uma aplicação maliciosa tendo um nível de perigo relativamente baixo pode ser migrada ou isolada, e uma conta de usuário e semelhantes de uma aplicação maliciosa tendo um nível de perigo elevado podem ser desativados. Pode ser entendido que, neste caso, para determinar um tipo ou um nível de perigo de um comportamento de ataque de uma aplicação maliciosa, o analisador de segurança 202 precisa comunicar dados de comportamento de aplicação e informação inicial da aplicação maliciosa ao processador de segurança 203, de modo que o processador de segurança 203 determina um tipo ou um nível de perigo do comportamento de ataque da aplicação maliciosa de acordo com os dados de comportamento de aplicação maliciosa. Certamente, o analisador de segurança 202 também pode determinar o tipo ou o nível de perigo do comportamento de ataque da aplicação de acordo com os dados de comportamento de aplicação, e retornar um resultado de análise ao processador de segurança 203, o que não é especialmente limitado nesta modalidade da presente invenção. Por exemplo, o analisador de segurança 202 pode distinguir uma aplicação maliciosa de uma aplicação normal de acordo com os dados de comportamento de aplicação de nuvem

e a regra de determinação de segurança e, em seguida, o analisador de segurança 202 ou o processador de segurança 203 pode pesquisar adicionalmente uma biblioteca de recursos de aplicação pré-configurada, para determinar um tipo do comportamento de ataque da aplicação maliciosa, por exemplo, ataque de negação de serviço, ataque de Trojan ou ataque de *"worm"*. Para outro exemplo, depois do analisador de segurança 202 determinar, de acordo com os dados de comportamento de aplicação de nuvem e a regra de determinação de segurança, a aplicação maliciosa tendo um comportamento de ataque, o analisador de segurança 202 ou o processador de segurança 203 pode pesquisar uma biblioteca de recursos de aplicação pré-configurada de acordo com os dados de comportamento de aplicação de nuvem, para determinar um tipo do comportamento de ataque da aplicação e, além disso, determinar um nível de perigo do comportamento de ataque da aplicação de acordo com o tipo de comportamento de ataque da aplicação, em que a biblioteca de recursos de aplicação é utilizada para descrever uma relação de mapeamento entre um recurso de comportamento de uma aplicação e um tipo de um comportamento de ataque da aplicação. Opcionalmente, a biblioteca de recursos de aplicação pode ser um conjunto de dados independente no sistema de computação em nuvem e, depois de determinar, de acordo com os dados de comportamento de aplicação de nuvem e a regra de determinação de segurança, que a aplicação maliciosa tem um comportamento de ataque, por ainda pesquisar a biblioteca de recursos de aplicação para determinar o tipo do comportamento de ataque da aplicação maliciosa. Certamente, a biblioteca de recursos de aplicação pode também ser um subconjunto da regra de

determinação de segurança, e depois de determinar, de acordo com a regra de determinação de segurança, que uma aplicação de nuvem é uma aplicação maliciosa, o analisador de segurança 202 pode determinar um tipo de um comportamento de ataque da aplicação maliciosa de acordo com a biblioteca de recursos de aplicação incluída na regra de determinação de segurança. Pode ser entendido que, diferentes tipos de comportamentos de ataque têm diferentes níveis de perigo, e um nível de perigo precisa ser determinado de acordo com um grau de dano causado ao sistema por um comportamento de ataque. Um comportamento de ataque causando danos mais severos ao sistema de computação em nuvem tem um nível de perigo mais alto. Geralmente, uma tabela de mapeamento pode ser configurada para representar uma correspondência entre um tipo de um comportamento de ataque de uma aplicação e um nível de perigo da aplicação. Desta forma, o nível de perigo do comportamento de ataque da aplicação pode ser determinado de acordo com o tipo de comportamento de ataque da aplicação e por pesquisar na tabela. Opcionalmente, em outra modalidade opcional, o processador de segurança 203 pode também processar uma aplicação maliciosa de acordo com um nível de segurança do sistema de computação em nuvem, em que diferentes níveis de segurança correspondem a diferentes modos de processamento. Por exemplo, o nível de segurança do sistema de computação em nuvem pode ser definido como "alto", "médio" e "baixo". Quando o nível de segurança do sistema de computação em nuvem é "alto", o processador de segurança 203 pode fechar a aplicação maliciosa e desabilitar uma conta de usuário da aplicação maliciosa; quando o nível de segurança do sistema de computação em nuvem é "baixo", o processador

de segurança 203 pode migrar a aplicação maliciosa para um hospedeiro de nuvem específico para isolar a aplicação maliciosa. Por fim, deve ser notado que, três formas em que o processador de segurança 203 processa aplicações maliciosas, isto é, processa as aplicações maliciosas em conjunto, processa as aplicações maliciosas de acordo com tipos ou níveis de perigo de comportamentos de ataque e processa as aplicações maliciosas de acordo com um nível de segurança do sistema de computação em nuvem, podem ser indicados por uma regra de processamento de aplicação maliciosa. Diferentes maneiras de processamento correspondem a diferentes regras de processamento de aplicação maliciosa, e as regras de processamento de aplicação maliciosa podem ser configuradas por um administrador utilizando uma interface de configuração do gestor de políticas 201. Por exemplo, as regras de processamento de aplicação maliciosa podem ser utilizadas para indicar maneiras de processar diferentes tipos de aplicações maliciosas, ou maneiras de processar aplicações maliciosas com diferentes níveis de perigo, ou maneiras de processar aplicações maliciosas sob diferentes níveis de segurança do sistema de computação em nuvem. Desta forma, o processador de segurança 203 pode executar especificamente o processamento correspondente em uma aplicação maliciosa de acordo com um tipo do comportamento de ataque da aplicação, e uma maneira de processar o tipo de aplicação que é indicada pela regra de processamento de aplicação maliciosa; ou o processador de segurança 203 pode executar especificamente o processamento correspondente na aplicação maliciosa de acordo com um nível de perigo do comportamento de ataque da aplicação, e uma

maneira de processar uma aplicação tendo o nível de perigo que é indicada pela regra de processamento de aplicação maliciosa; ou o processador de segurança 203 pode executar especificamente o processamento correspondente na aplicação maliciosa de acordo com um nível de segurança atual do sistema de computação em nuvem, e uma maneira de processar uma aplicação maliciosa sob o nível de segurança indicada pela regra de processamento de aplicação maliciosa.

[0083] No aparelho para processamento de um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção, um gestor de políticas fornece uma regra de detecção de comportamento para um detector de segurança em cada hospedeiro de nuvem, o detector de segurança executa detecção de acordo com a regra de detecção de comportamento, e relata dados de comportamento de uma aplicação de nuvem, um analisador de segurança analisa os dados de comportamento de aplicação de nuvem para determinar uma aplicação de nuvem tendo um comportamento de ataque, e invoca um controlador de nuvem para executar processamento correspondente. Comparada com a solução de segurança da técnica anterior, esta modalidade da presente invenção executa proteção de segurança baseada em um nível de aplicação de computação em nuvem, que pode satisfazer um cenário de implementação de aplicação de um sistema de computação em nuvem, impedir ataques mútuos entre diferentes aplicações de nuvem em um mesmo hospedeiro, ou um ataque interno lançado em um hospedeiro, e reduzir o impacto em uma aplicação de nuvem normal. Além disso, uma política de processamento de aplicação maliciosa pode ser configurada para processar diferentemente diferentes aplicações

maliciosas de acordo com diferentes níveis de segurança ou diferentes tipos de ataques.

[0084] De preferência, o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem pode incluir ainda um notificador de informação 204; o gestor de políticas 201 armazena ainda uma regra de notificação de informação.

[0085] O processador de segurança 203 é ainda configurado para pesquisar, de acordo com a informação inicial da aplicação de nuvem tendo um comportamento de ataque, informação de usuário à qual a aplicação de nuvem pertence, e enviar a informação de usuário obtida através da pesquisa e os dados de comportamento de aplicação de nuvem para o notificador de informação 204, em que a informação de usuário da aplicação de nuvem inclui, mas não estão limitada a, um nome de usuário, um endereço de correio eletrônico de usuário, e um número de identidade de usuário.

[0086] O notificador de informação 204 é configurado para armazenar os dados de comportamento de aplicação recebidos e a informação de usuário recebida a qual a aplicação de nuvem pertence, e executar processamento de notificação de informação de ataque de acordo com a regra de notificação de informação armazenada no gestor de políticas. Os dados de comportamento de aplicação e a informação de usuário a qual a aplicação de nuvem pertence são copiados. Especificamente, os dados de comportamento de aplicação e a informação de usuário são armazenados em um meio de armazenamento confiável em um formato de dados, como uma tabela, um registro ou um documento, para que o administrador possa visualizá-los.

[0087] Especificamente, em uma modalidade, que o notificador

de informação 204 executa o processamento de notificação de informação de ataque inclui, mas não está limitado a uma ou mais das seguintes operações: gerar informação de alarme, exibir uma aplicação de nuvem tendo um comportamento de ataque e informação de usuário à qual a aplicação de nuvem pertence, e notificar um centro de alarme de informação de usuário para o qual uma aplicação de nuvem tendo um comportamento de ataque pertence.

[0088] De preferência, em outra modalidade, depois de receber os dados de comportamento de aplicação relatados pelo detector de segurança, e ao determinar, de acordo com a regra de determinação de segurança, que a aplicação de nuvem não tem um comportamento de ataque, o analisador de segurança 202 pode descartar os dados de comportamento de aplicação.

[0089] De preferência, em outra modalidade, o gestor de políticas 201 inclui uma interface de configuração, e o administrador pode configurar uma ou mais das regras de determinação de segurança, a regra de processamento de aplicação maliciosa e a regra de notificação de informação utilizando a interface de configuração. A interface de configuração pode ser uma ou mais de uma interface gráfica de usuário (GUI), uma janela de configuração em uma forma de uma página Web, e uma interface de programação de aplicação (API). Além disso, durante configuração de uma regra de processamento de aplicação maliciosa, diferentes regras de processamento podem ser configuradas de acordo com tipos de ataque ou níveis de perigo de aplicações maliciosas, para processar diferencialmente as aplicações maliciosas, implementando a flexibilidade e a escalabilidade da proteção de segurança. Certamente, pode ser entendido que uma ou mais

das três regras podem não ser configuradas pelo administrador e podem ser definidas pelo sistema de computação em nuvem de acordo com uma regra padrão.

[0090] Além disso, para implementar uma proteção de segurança de granularidade mais fina, a regra de detecção de comportamento entregue ao detector de segurança pelo gestor de políticas 201 pode incluir uma regra de detecção de processo ou uma regra de detecção de rotina. Desta forma, o detector de segurança pode executar detecção de nível de processo ou nível de rotina em uma aplicação de nuvem; o analisador de segurança 202 pode determinar, com base em um resultado de detecção do detector de segurança, um processo ou rotina que tem um comportamento de ataque e, em seguida, o processador de segurança pode processar o processo ou rotina tendo um comportamento de ataque, para adicionalmente implementar proteção de segurança de nível de processo ou nível de rotina.

[0091] Com referência a um exemplo específico, o seguinte descreve ainda em detalhe o aparelho para processar um comportamento de ataque de uma aplicação de nuvem fornecida nesta modalidade da presente invenção. Conforme ilustrado na Figura 4, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem é um hospedeiro de nuvem 30. Um processo de trabalho principal do hospedeiro de nuvem 30 é como segue:

[0092] 1. Configurar, usando a interface de configuração do gestor de políticas 201, uma regra de determinação de segurança utilizada para determinar um comportamento de ataque de uma aplicação, em que a ação de configuração pode ser implementada por um administrador ou por um programa de

configuração executado no sistema de computação em nuvem. Em um exemplo específico, a regra de determinação de segurança é: requerer uma porta tcp diferente > 100, ou seja, uma quantidade de portas TCP solicitadas excede 100, em que a regra de determinação representa que se uma quantidade de portas TCP externas solicitadas pela aplicação de nuvem exceder 100, é determinado que a aplicação de nuvem tem um comportamento de *"sniffing"* de porta.

[0093] 2. O gestor de políticas 201 converte a regra de determinação de segurança em uma regra de detecção de comportamento, detecta uma quantidade de portas TCP solicitadas pela aplicação de nuvem, e entrega a regra de detecção de comportamento ao detector de segurança 205 implantado no hospedeiro de nuvem 10.

[0094] 3. O detector de segurança 205 detecta os comportamentos de uma App A e de uma App B. Por exemplo, o detector de segurança 205 conta uma quantidade de portas TCP solicitadas pela App A e uma quantidade de portas TCP solicitadas pela App B, gera dados de comportamento de aplicação, e relata os dados de comportamento de aplicação ao analisador de segurança 202.

[0095] 4. O analisador de segurança 202 determina, de acordo com os dados de comportamento de aplicação coletados e a regra de determinação de segurança, que a quantidade de portas TCP solicitadas pela App B excede 100 e, portanto, determina que a App B tem um comportamento de ataque.

[0096] 5. O analisador de segurança 202 envia ao processador de segurança 203 uma informação inicial da App B, por exemplo, um ID de processo ou um nome de processo.

[0097] 6. O processador de segurança 203 pesquisa em uma

biblioteca de aplicações do sistema de computação em nuvem de acordo com a informação inicial da App B para informação de usuário da App B.

[0098] 7. O processador de segurança 203 invoca o controlador de nuvem 206 para fechar a App B, ou migrar a App B para um hospedeiro de nuvem isolado, ou desativa uma conta de usuário da App B.

[0099] 8. O analisador de segurança 202 notifica o notificador de informação 204 da informação de usuário da App B, e o notificador de informação 204 comunica a informação de usuário ao centro de alarme para arquivamento.

[00100] Neste exemplo, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem detecta com êxito e processa um comportamento de *"sniffing"* de porta da App B, o que não afeta gravemente a App A. Além disso, depois de descobrir que a App B tem um comportamento de ataque, o analisador de segurança pode usar maneiras de processamento diferentes para a App de acordo com um tipo ou um nível de perigo do comportamento de ataque da App B. Uma maneira de processar uma aplicação maliciosa pode ser indicada por uma regra de processamento de aplicação maliciosa, e a regra de processamento de aplicação maliciosa pode ser configurada pelo administrador usando a interface de configuração do gestor de políticas 201. A interface de configuração pode ser uma página Web, uma API ou similar.

[00101] O que segue descreve em detalhe os módulos no aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem.

[00102] (1) O gestor de políticas 201: o gestor de políticas fornece uma interface de configuração para o administrador

ou um programa de configuração automática, e é principalmente responsável por operações como armazenamento de regras, conversão de regras e entrega de regras. Conforme ilustrado na Figura 5, o gestor de políticas 201 inclui uma interface de configuração 2011, uma unidade de conversão de regras 2012, uma unidade de entrega de regras 2013 e uma unidade de armazenamento de regras 2014, em que a interface de configuração 2011 inclui, mas não está limitada a uma ou mais interfaces gráficas de usuário (GUI), uma janela de configuração em uma forma de uma página Web, e uma interface de programação de aplicação (API). A regra que pode ser configurada usando a interface de configuração 2011 inclui a regra de determinação de segurança, a regra de processamento de aplicação maliciosa e uma regra de notificação de informação. A unidade de armazenamento de regras 2014 pode armazenar, em bibliotecas de regras correspondentes, várias regras configuradas pelo administrador utilizando a interface de configuração 2011; a unidade de conversão de regras 2012 pode converter a regra de determinação de segurança configurada pelo administrador na regra de detecção de comportamento; e a unidade de entrega de regras 2013 é responsável por entregar a regra de detecção de comportamento para o detector de segurança no hospedeiro de nuvem.

[00103] (2) O analisador de segurança 202: como mostrado na Figura 6, o analisador de segurança é principalmente responsável por receber os dados de comportamento de aplicação enviados pelo detector de segurança e, em seguida, determinar, de acordo com a regra de determinação de segurança armazenada no gestor de políticas, se a aplicação

de nuvem tem um comportamento de ataque; e se determinar que a aplicação de nuvem tem um comportamento de ataque, enviar a informação inicial (por exemplo, o ID de processo ou o nome de processo) da aplicação de nuvem para o processador de segurança; ou se determinar que a aplicação de nuvem não tem um comportamento de ataque, descartar os dados de comportamento de aplicação.

[00104] (3) O processador de segurança 203: o processador de segurança é responsável por processar uma aplicação maliciosa. Especificamente, como mostrado na Figura 7, o processador de segurança 203 inclui principalmente uma unidade de recepção de informação de aplicação 2031, uma unidade de pesquisa de informação de usuário 2032, uma unidade de processamento de aplicação 2033 e uma unidade de relatório de informação 2034, em que a unidade de recepção de informação de aplicação 2031 recebe informação inicial de uma aplicação maliciosa que é relatada pelo analisador de segurança; a unidade de pesquisa de informação de usuário 2032 pesquisa em uma biblioteca de informação de aplicação do sistema de computação em nuvem para informação de usuário à qual a aplicação de nuvem pertence, em que a informação de usuário inclui, mas não está limitada a: um nome de usuário, um endereço de correio eletrônico de usuário, e uma identidade de usuário; a unidade de pesquisa de informação de usuário 2032 relata a informação de usuário e a informação de comportamento da aplicação maliciosa para o notificador de informação utilizando a unidade de relatório de informação 2034, de modo que o notificador de informação executa processamento de notificação de informação de ataque de acordo com a regra de notificação de informação armazenada

no gestor de políticas; e a unidade de processamento de aplicação 2033 invoca, de acordo com a regra de processamento de aplicação maliciosa armazenada no gestor de políticas, a interface fornecida pelo controlador de nuvem, para processar a aplicação maliciosa, em que uma maneira de processamento inclui, mas não se limita a: fechar a aplicação, migrar a aplicação para um hospedeiro de nuvem isolado, e desabilitar uma conta de usuário.

[00105] (4) O notificador de informação 204: como mostrado na Figura 8, o notificador de informação inclui uma unidade de recepção de informação de aplicação 2041 e uma unidade de determinação de política de notificação de informação 2042, em que a unidade de recepção de informação de aplicação 2041 é responsável por receber a informação de comportamento de aplicação e a informação de usuário à qual a aplicação de nuvem pertence e, então, a unidade de determinação de política de notificação de informação 2042 executa processamento de notificação de informação de ataque de acordo com a regra de notificação de informação armazenada no gestor de políticas. Especificamente, a unidade de determinação de política de notificação de informação 2042 pode invocar ou acionar uma unidade de geração de alarme 2043 para gerar informação de alarme, por exemplo, gerar uma interface de alarme. Opcionalmente, a unidade de determinação de política de notificação de informação 2042 pode invocar ou acionar uma unidade de apresentação de informação 2044 para apresentar informação sobre a aplicação maliciosa em uma página web em uma forma de uma tabela. Opcionalmente, a unidade de determinação de política de notificação de informação 2042 também pode invocar ou acionar

a unidade de notificação de informação para reportar a informação sobre a aplicação maliciosa para um centro de alarme. Pode ser entendido que o notificador de informação pode incluir ainda uma da unidade de geração de alarme 2043, a unidade de apresentação de informação 2044 e a unidade de notificação de informação 2045, ou pode incluir quaisquer duas das três unidades, ou pode incluir todas as três unidades, o que depende de um requisito de cenário de aplicação específico, e não está especialmente limitado nesta modalidade da presente invenção.

[00106] O aparelho para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção pode satisfazer um cenário de implementação de aplicação de um sistema de computação em nuvem, executar proteção de segurança com base em um nível de aplicação de computação em nuvem, prevenir ataques mútuos entre diferentes aplicações de nuvem em um mesmo hospedeiro, ou ataques internos lançados em um hospedeiro, e reduzir o impacto em uma aplicação de nuvem normal. Além disso, uma política de processamento de aplicação maliciosa pode ser configurada para processar diferentemente diferentes aplicações maliciosas de acordo com diferentes níveis de segurança ou diferentes tipos de ataque.

[00107] Deve ser notado que o aparelho para processamento de um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção pode ser especificamente um hospedeiro de nuvem no sistema de computação em nuvem, em que o hospedeiro de nuvem pode ser uma máquina virtual em execução em uma máquina física. Conforme ilustrado na Figura 12, a máquina física 1200 inclui

uma camada de hardware 100, um Monitor de Máquina Virtual (VMM) 110 executando acima da camada de hardware 100, e um Hospedeiro 1201 e várias máquinas virtuais (VMs) em execução acima do VMM 100, em que a camada de hardware inclui, mas não se limita a, um dispositivo de I/O, uma CPU e uma memória. O aparelho para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção pode ser especificamente uma máquina virtual na máquina física 1200. Por exemplo, a VM 1202 na qual uma ou mais aplicações de nuvem são executadas, em que cada aplicação de nuvem é utilizada para implementar uma função de serviço correspondente, por exemplo, uma aplicação de banco de dados e uma aplicação de mapa. Um ou mais aplicações de nuvem podem ser desenvolvidas por um desenvolvedor e, em seguida, implantadas no sistema de computação em nuvem. Além disso, a VM 1202 executa ainda um programa executável e invoca recursos de hardware da camada de hardware 100 utilizando o Hospedeiro 1201 ao executar o programa, para implementar funções do gestor de políticas, o analisador de segurança, o processador de segurança e o notificador de informação do aparelho para processar um comportamento de ataque de uma aplicação de nuvem. Especificamente, o gestor de políticas, o analisador de segurança, o processador de segurança e o notificador de informação podem ser incluídos no programa executável em uma forma de módulos ou funções de software. Por exemplo, o programa executável pode incluir um módulo de gestor de políticas, um módulo de analisador de segurança, um módulo de processador de segurança, e um módulo de notificador de informação. A VM 1202 invoca os recursos na camada de hardware 100, como a CPU e a memória, para

executar o programa executável, implementando, assim, as funções do gestor de políticas, o analisador de segurança, o processador de segurança e o notificador de informação. Em um outro cenário possível, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção pode ser uma máquina física no sistema de computação em nuvem. Conforme ilustrado na Figura 13, a máquina física 1300 inclui pelo menos um processador 1301, por exemplo, uma CPU, pelo menos uma interface de rede 1304, uma memória 1305, e pelo menos um barramento de comunicações 1302. O barramento de comunicações 1302 é configurado para implementar conexão e comunicação entre os componentes. Opcionalmente, a máquina física 1300 inclui um dispositivo de entrada/saída 1303, em que o dispositivo de entrada/saída 1303 inclui um monitor, um teclado ou um dispositivo de clicar (por exemplo, um mouse ou uma “trackball”), um painel de toque, ou uma tela de toque). A memória 1305 pode incluir uma memória RAM de alta velocidade, ou pode também incluir uma memória não volátil, por exemplo, pelo menos uma memória magnética. Opcionalmente, a memória 1305 pode incluir pelo menos um aparelho de armazenamento localizado afastado do processador 1301. A memória 1305 armazena os seguintes elementos, módulos executáveis ou estruturas de dados, ou os seus subconjuntos, ou os seus conjuntos estendidos:

um sistema operacional 13051, que inclui vários programas de sistema e é configurado para implementar vários serviços básicos e processar uma tarefa baseada em hardware; e

um módulo de programa de aplicação 13052, que inclui várias aplicações de nuvem, e é configurado para implementar vários

serviços de aplicação, por exemplo, uma aplicação de banco de dados e uma aplicação de mapa, em que
o módulo de programa de aplicação 13052 inclui, mas não está limitado a, um módulo que implementa funções do gestor de políticas, o analisador de segurança, o processador de segurança e o notificador de informação no aparelho para processar um comportamento de ataque de uma aplicação de nuvem.

[00108] Para implementação específica dos módulos no módulo de programa de aplicação 13052, consulte as modalidades de aparelho e de método da presente invenção, e os detalhes não são aqui descritos de novo.

[00109] Correspondentemente, o detector de segurança fornecido nesta modalidade da presente invenção pode ser um módulo de função no hospedeiro de nuvem no sistema de computação em nuvem. Por exemplo, quando o hospedeiro de nuvem é uma máquina virtual, o detector de segurança pode ser um programa de aplicação executado independentemente na máquina virtual, e quando o programa de aplicação está sendo executado pela máquina virtual, os comportamentos de outra aplicação de nuvem executada na máquina virtual podem ser detectados. Quando o hospedeiro de nuvem é uma máquina física, o detector de segurança pode ser um programa de aplicação armazenado em uma memória da máquina física, em que uma CPU da máquina física pode implementar, através da leitura e execução do programa de aplicação, funções de detecção de um comportamento de outra aplicação de nuvem executando na máquina física.

[00110] Com base na modalidade de aparelho anterior, uma modalidade da presente invenção fornece ainda um método para

processar um comportamento de ataque de uma aplicação de nuvem em um sistema de computação em nuvem, em que o sistema de computação em nuvem inclui múltiplos hospedeiros de nuvem e o hospedeiro de nuvem pode ser uma máquina física ou uma máquina virtual. Pelo menos um dos múltiplos hospedeiros de nuvem no sistema de computação em nuvem é um controlador de nuvem, e o controlador de nuvem é conectado de forma comunicativa a cada hospedeiro de nuvem no sistema de computação em nuvem ou é integrado a um hospedeiro de nuvem, e é configurado para controlar aplicações de nuvem em execução nos múltiplos hospedeiros de nuvem no sistema de computação em nuvem. Uma ou mais aplicações de nuvem são executadas em cada dos hospedeiros de nuvem, e um detector de segurança é implantado em cada hospedeiro de nuvem. O detector de segurança é responsável por detectar, de acordo com uma regra de detecção de comportamento, um comportamento de uma aplicação de nuvem executada no hospedeiro de nuvem. O método para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção pode ser executado por um hospedeiro de nuvem no sistema de computação em nuvem, ou um controlador de nuvem. Conforme ilustrado na Figura 9, o método inclui:

[00111] S901: Receber dados de comportamento de aplicação relatados por pelo menos um hospedeiro de nuvem entre os múltiplos hospedeiros de nuvem no sistema de computação em nuvem, em que os dados de comportamento de aplicação são obtidos depois que um detector de segurança no hospedeiro de nuvem detecta, de acordo com uma regra de detecção de comportamento, uma aplicação de nuvem em execução no hospedeiro de nuvem, e os dados de comportamento de aplicação

são utilizados para representar um estado de execução da aplicação de nuvem executando no hospedeiro de nuvem.

[00112] S902: Determinar, de acordo com os dados de comportamento de aplicação e uma regra de determinação de segurança, se a aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque.

[00113] S903: se for determinado que a aplicação de nuvem executada no hospedeiro de nuvem tem um comportamento de ataque, invocar, de acordo com uma regra de processamento de aplicação maliciosa, uma interface fornecida por um controlador de nuvem no sistema de computação em nuvem, para processar a aplicação de nuvem tendo um comportamento de ataque.

[00114] De preferência, a invocação de uma interface fornecida por um controlador de nuvem, para executar processamento correspondente na aplicação de nuvem tendo um comportamento de ataque inclui: invocar o controlador de nuvem para fechar a aplicação de nuvem, migrar a aplicação de nuvem para um hospedeiro de nuvem isolado, ou desabilitar uma conta de usuário da aplicação de nuvem.

[00115] De preferência, no passo S903, se for determinado que a aplicação de nuvem que está sendo executada no hospedeiro de nuvem tem um comportamento de ataque, a informação de usuário à qual a aplicação de nuvem pertence também podem ser pesquisada de acordo com informação inicial da aplicação de nuvem tendo um comportamento de ataque, e depois os dados de comportamento de aplicação de nuvem que têm um comportamento de ataque e a informação de usuário que é obtida através da pesquisa são gravados em backup, e processamento de notificação de informação de ataque é

executado de acordo com uma regra de notificação de informação, em que a informação inicial da aplicação de nuvem é usada para identificar unicamente a aplicação de nuvem, a informação inicial pode ser um ID de processo, um nome de processo ou ambos, e a informação de usuário da aplicação de nuvem inclui, mas não estão limitada a, um nome de usuário, um endereço de e-mail de usuário, e um número de identidade de usuário. Deve ser notado que os dados de comportamento de aplicação e a informação de usuário à qual a aplicação de nuvem pertence são gravados em backup pode ser especificamente: os dados de comportamento de aplicação e a informação de usuário são armazenados em um meio de armazenamento confiável em um formato de dados tal como uma tabela, um registro ou um documento, para que o administrador possa visualizá-los.

[00116] Além disso, a execução de processamento de notificação de informação de ataque inclui, mas não está limitado a uma ou qualquer combinação das seguintes operações: gerar informação de alarme, exibir uma aplicação de nuvem tendo um comportamento de ataque e a informação de usuário à qual a aplicação de nuvem pertence, e notificar um centro de alarme de informação de usuário à qual uma aplicação de nuvem tendo um comportamento de ataque pertence.

[00117] Opcionalmente, no passo S903, se for determinado que a aplicação de nuvem executada no hospedeiro de nuvem não tem um comportamento de ataque, os dados de comportamento de aplicação recebidos da aplicação de nuvem são descartados.

[00118] Deve ser notado que a regra de determinação de segurança é utilizada para definir qual comportamento de uma aplicação de nuvem é um comportamento de ataque, a regra de

processamento de aplicação maliciosa é utilizada para definir uma forma de processar a aplicação de nuvem tendo um comportamento de ataque, e a regra de detecção de comportamento é utilizada para definir qual comportamento de uma aplicação de nuvem deve ser detectado, ou seja, a regra de detecção de comportamento indica um indicador de detecção para detectar uma aplicação de nuvem. Geralmente, a regra de detecção de comportamento e a regra de determinação de segurança estão intimamente relacionadas e podem ser intercambiadas. Por conseguinte, em uma modalidade, a regra de determinação de segurança pode ser convertida na regra de detecção de comportamento, e a regra de detecção de comportamento é entregue ao detector de segurança. Por exemplo, se a regra de determinação de segurança é: se uma quantidade de portas TCP externas solicitadas por uma aplicação de nuvem exceder 100, é determinado que a aplicação de nuvem tem um comportamento de *"sniffing"* de porta, a regra de detecção de comportamento é: coletar uma quantidade de portas TCP diferentes solicitadas pela aplicação de nuvem. Desta forma, o detector de segurança no hospedeiro de nuvem deve detectar a quantidade de portas TCP diferentes solicitadas pela aplicação de nuvem, e enviar um resultado de detecção para o analisador de nuvem.

[00119] Opcionalmente, no passo S903, todas as aplicações de nuvem com comportamentos de ataque (aplicações maliciosas) podem ser processadas juntas, por exemplo, fechar as aplicações maliciosas, migrar as aplicações maliciosas para um hospedeiro de nuvem isolado ou desabilitar contas de usuários das aplicações maliciosas. Opcionalmente, diferentes graus ou tipos diferentes de processamento podem

ser executados nas aplicações maliciosas de acordo com os tipos de comportamentos de ataque das aplicações maliciosas ou níveis de perigo de comportamentos de ataque das aplicações maliciosas. Por exemplo, uma aplicação maliciosa tendo um nível de perigo relativamente baixo pode ser migrada ou isolada, e uma conta de usuário de uma aplicação maliciosa com alto nível de perigo pode ser desativada. Pode ser entendido que, neste caso, um tipo ou um nível de perigo de um comportamento de ataque de uma aplicação maliciosa precisa ser determinado de acordo com os dados de comportamento de aplicação maliciosa. Por exemplo, uma aplicação maliciosa pode ser distinguida de uma aplicação normal de acordo com dados de comportamento de uma aplicação de nuvem e a regra de determinação de segurança e, em seguida, uma biblioteca de recursos de aplicação pré-configurada pode ser pesquisada, para determinar um tipo do comportamento de ataque da aplicação maliciosa, por exemplo, ataque de negação de serviço, ataque de Trojan ou ataque de *"worm"*. Para outro exemplo, após a aplicação maliciosa tendo um comportamento de ataque ser determinada de acordo com os dados de comportamento de aplicação de nuvem e a regra de determinação de segurança, a biblioteca de recursos de aplicação pré-configurada pode ser pesquisada de acordo com os dados de comportamento de aplicação de nuvem, para determinar um tipo de um comportamento de ataque da aplicação e, em seguida, um nível de perigo do comportamento de ataque da aplicação é determinado de acordo com o tipo do comportamento de ataque da aplicação, em que a biblioteca de recursos de aplicação é utilizada para descrever uma relação de mapeamento entre um recurso de comportamento de uma aplicação e um tipo de um

comportamento de ataque da aplicação. Opcionalmente, a biblioteca de recursos de aplicação pode ser um conjunto de dados independente no sistema de computação em nuvem e, após a aplicação maliciosa tendo um comportamento de ataque ser determinada de acordo com os dados de comportamento de aplicação de nuvem e a regra de determinação de segurança, a biblioteca de recursos de aplicação pode ser adicionalmente pesquisada para determinar o tipo do comportamento de ataque da aplicação maliciosa. Certamente, a biblioteca de recursos de aplicação pode ser um subconjunto da regra de determinação de segurança e, depois de determinado, de acordo com a regra de determinação de segurança, que uma aplicação de nuvem é uma aplicação maliciosa, um tipo de um comportamento de ataque da aplicação maliciosa pode ser ainda determinado de acordo com a biblioteca de recursos de aplicação incluída na regra de determinação de segurança. Pode ser entendido que, diferentes tipos de comportamentos de ataque têm diferentes níveis de perigo, e um nível de perigo precisa ser determinado de acordo com um grau de dano causado ao sistema por um comportamento de ataque. Um comportamento de ataque causando danos mais severos ao sistema de computação em nuvem tem um nível de perigo mais alto. Geralmente, uma tabela de mapeamento pode ser configurada, para representar uma correspondência entre um tipo de um comportamento de ataque de uma aplicação e um nível de perigo da aplicação. Desta forma, o nível de perigo do comportamento de ataque da aplicação pode ser determinado de acordo com o tipo do comportamento de ataque da aplicação e por pesquisar na tabela. Opcionalmente, a aplicação maliciosa também pode ser processada de acordo com um nível de segurança do sistema de

computação em nuvem, em que diferentes níveis de segurança correspondem a maneiras de processamento diferentes. Por exemplo, o nível de segurança do sistema de computação em nuvem pode ser definido como "alto", "médio" e "baixo". Quando o nível de segurança do sistema de computação em nuvem é "alto", a aplicação maliciosa é fechada e uma conta de usuário da aplicação maliciosa é desativada; quando o nível de segurança do sistema de computação em nuvem é "baixo", a aplicação maliciosa é migrada para um hospedeiro de nuvem específico para isolar a aplicação maliciosa. Por fim, deve-se notar que três maneiras de processar aplicações maliciosas, ou seja, processar as aplicações maliciosas em conjunto, processar as aplicações maliciosas de acordo com os tipos ou níveis de perigo de comportamentos de ataque e processar as aplicações maliciosas de acordo com um nível de segurança do sistema de computação em nuvem pode ser indicado por uma regra de processamento de aplicação maliciosa. Diferentes maneiras de processamento correspondem a diferentes regras de processamento de aplicação maliciosa.

[00120] De preferência, em outra modalidade, um administrador pode configurar uma ou mais das regras de determinação de segurança, a regra de processamento de aplicação maliciosa e a regra de notificação de informação utilizando a interface de configuração. A interface de configuração pode ser uma página Web, uma API ou semelhante. Além disso, durante configuração de uma regra de processamento de aplicação maliciosa, diferentes regras de processamento podem ser configuradas de acordo com tipos de ataque ou níveis de perigo de aplicações maliciosas, para processar diferencialmente as aplicações maliciosas, implementando a

flexibilidade e a escalabilidade da proteção de segurança. Certamente, pode ser entendido que uma ou mais das três regras podem não ser configuradas pelo administrador e podem ser definidas pelo sistema de computação em nuvem de acordo com uma regra padrão.

[00121] Além disso, para implementar uma proteção de segurança de granularidade mais fina, a regra de detecção de comportamento pode incluir uma regra de detecção de processo ou uma regra de detecção de rotina. Desta forma, a detecção de nível de processo ou nível de rotina pode ser realizada em uma aplicação; um processo ou segmento com um comportamento de ataque é determinado com base em um resultado de detecção do detector de segurança, e o processo ou segmento tendo um comportamento de ataque é processado, para adicionalmente implementar a proteção de segurança de nível de processo ou nível de rotina.

[00122] No método para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção, um cenário de implementação de aplicação de um sistema de computação em nuvem pode ser satisfeito, proteção de segurança pode ser realizada com base em um nível de aplicação de computação em nuvem, ataques mútuos entre diferentes aplicações em um mesmo hospedeiro, ou ataques internos lançados em um hospedeiro podem ser evitados, e o impacto sobre uma aplicação normal pode ser reduzido. Além disso, uma política de processamento de aplicação maliciosa pode ser configurada para processar diferentemente diferentes aplicações maliciosas de acordo com diferentes níveis de segurança ou diferentes tipos de ataque.

[00123] Com referência a um exemplo específico, o seguinte

descreve ainda em detalhe o método para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção. Conforme ilustrado na Figura 10, o método para processar um comportamento de ataque de uma aplicação de nuvem inclui o seguinte processo de trabalho principal.

[00124] (1) Configurar, usando uma interface de configuração, uma regra de determinação de segurança utilizada para determinar um comportamento de ataque de uma aplicação, armazenar a regra de determinação de segurança em uma biblioteca de políticas, converter a regra de determinação de segurança em uma regra de detecção de comportamento, e fornecer a regra de detecção de comportamento para um detector de segurança em um hospedeiro de nuvem.

[00125] (2) O detector de segurança detecta um comportamento de uma aplicação de nuvem de acordo com a regra de detecção de comportamento, e gera e relata os dados de comportamento de aplicação.

[00126] (3) Determinar, de acordo com os dados de comportamento de aplicação coletados e a regra de determinação de segurança, uma aplicação maliciosa tendo um comportamento de ataque.

[00127] (4) Pesquisar uma biblioteca de aplicações do sistema de computação em nuvem de acordo com a informação inicial da aplicação maliciosa para obter informação de usuário da aplicação maliciosa.

[00128] (5) Invocar um controlador de nuvem para fechar a aplicação maliciosa, ou migrar a aplicação maliciosa para um hospedeiro de nuvem isolado, ou desabilitar uma conta de usuário da aplicação maliciosa.

[00129] (6) Notificar a informação de usuário da aplicação maliciosa para um administrador ou um centro de alarme.

[00130] Neste exemplo, o aparelho para processar um comportamento de ataque de uma aplicação de nuvem detecta e processa com sucesso uma aplicação maliciosa, que não afeta gravemente uma aplicação normal. Além disso, depois de verificar que uma aplicação tem um comportamento de ataque, uma maneira de processar a aplicação maliciosa varia com um tipo ou nível de perigo do comportamento de ataque da aplicação maliciosa, em que uma maneira de processar a aplicação maliciosa pode ser indicada por uma regra de processamento de aplicação maliciosa, e a regra de processamento de aplicação maliciosa pode ser configurada pelo administrador usando a interface de configuração, em que a interface de configuração pode ser uma interface gráfica de usuário (GUI), uma janela de configuração em forma de página Web, interface de programação de aplicação (API), ou semelhantes.

[00131] No método para processar um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção, um cenário de implementação de aplicação de um sistema de computação em nuvem pode ser satisfeito, proteção de segurança pode ser realizada com base em um nível de aplicação de computação em nuvem, ataques mútuos entre diferentes aplicações em um mesmo hospedeiro, ou ataques internos lançados em um hospedeiro podem ser evitados, e o impacto sobre uma aplicação normal pode ser reduzido. Além disso, uma política de processamento de aplicação maliciosa pode ser configurada para processar diferentemente diferentes aplicações maliciosas de acordo com diferentes

níveis de segurança ou diferentes tipos de ataque.

[00132] Conforme ilustrado na Figura 11, uma modalidade da presente invenção fornece ainda um sistema de proteção de segurança de uma aplicação de nuvem, que é aplicado a um sistema de computação em nuvem e é configurado para implementar o método para processar um comportamento de ataque de uma aplicação de nuvem. O sistema de proteção de segurança de uma aplicação de nuvem inclui: um aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem, um controlador de nuvem 206 e múltiplos detectores de segurança (utilizando 205 na Figura 11 como exemplo), em que os múltiplos detectores de segurança são implantados em múltiplos hospedeiros de nuvem (por exemplo, 10, 11, 12 e 13 na Figura 11), e cada um dos hospedeiros de nuvem corresponde a um dos detectores de segurança. O controlador de nuvem 206 é comunicativamente conectado aos múltiplos hospedeiros de nuvem, ou é integrado a um hospedeiro de nuvem entre os múltiplos hospedeiros de nuvem, e é configurado para gerenciar e controlar os múltiplos hospedeiros de nuvem, em que uma ou mais aplicações de nuvem são executadas em cada um dos hospedeiros de nuvem. O aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem armazena uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa.

[00133] O detector de segurança 205 é configurado para detectar uma ou mais aplicações de nuvem de acordo com uma regra de detecção de comportamento, para obter dados de comportamento de aplicação, e relatar os dados de comportamento de aplicação ao aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem, em que a

uma ou mais aplicações de nuvem são executadas em um hospedeiro de nuvem 10 correspondente ao detector de segurança 205.

[00134] O aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem é configurado para receber os dados de comportamento de aplicação relatados pelo detector de segurança 205 em pelo menos um hospedeiro de nuvem entre os múltiplos hospedeiros de nuvem, determinar, de acordo com os dados de comportamento de aplicação e a regra de determinação de segurança, se a aplicação de nuvem executada no hospedeiro de nuvem 10 tem um comportamento de ataque, e se determinar que a aplicação de nuvem executada no hospedeiro de nuvem tem um comportamento de ataque, invocar, de acordo com a regra de processamento de aplicação maliciosa, o controlador de nuvem 206 para processar a aplicação da nuvem tendo um comportamento de ataque.

[00135] Opcionalmente, a regra de detecção de comportamento pode ser obtida depois que o aparelho para processar um comportamento de ataque de uma aplicação de nuvem converte a regra de determinação de segurança, e é entregue ao detector de segurança.

[00136] Opcionalmente, se determinar que a aplicação de nuvem em execução no hospedeiro de nuvem tem um comportamento de ataque, o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem pode pesquisar, de acordo com a informação inicial da aplicação de nuvem tendo um comportamento de ataque, informação de usuário à qual a aplicação de nuvem pertence e, em seguida, fazer backup dos dados de comportamento de aplicação da aplicação de nuvem tendo um comportamento de ataque e a informação de usuário

obtida por meio da pesquisa, e executar processamento de notificação de informação de ataque de acordo com uma regra de notificação de informação, em que a informação inicial da aplicação de nuvem é utilizada para identificar unicamente a aplicação de nuvem, a informação inicial pode ser um ID de processo, um processo ou ambos e a informação de usuário da aplicação de nuvem inclui, mas não está limitada a, um nome de usuário, um endereço de e-mail de usuário, e um número de identidade de usuário.

[00137] Deve ser notado que os dados de comportamento de aplicação e a informação de usuário à qual a aplicação de nuvem pertence são gravados em backup pode ser especificamente: os dados de comportamento de aplicação e a informação de usuário são armazenados em um meio de armazenamento confiável em um formato de dados tal como uma tabela, um registro ou um documento, para que o administrador possa visualizá-los.

[00138] Além disso, a execução de processamento de notificação de informação de ataque inclui, mas não está limitada a: gerar informação de alarme, exibir uma aplicação de nuvem tendo um comportamento de ataque e a informação de usuário à qual a aplicação de nuvem pertence, e notificar um centro de alarme de informação de usuário à qual uma aplicação de nuvem tendo um comportamento de ataque pertence.

[00139] Opcionalmente, o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem é comunicativamente conectado ao controlador de nuvem 206 ou o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem é integrado no controlador de nuvem 206.

[00140] De preferência, em outra modalidade, o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem inclui uma interface de configuração, e o administrador ou o programa de configuração pode configurar, utilizando a interface de configuração, uma ou mais regras de determinação de segurança, a regra de processamento de aplicação maliciosa, e a regra de notificação de informação, em que a interface de configuração pode ser uma interface gráfica de usuário (GUI), uma janela de configuração em uma forma de uma página Web, uma interface de programação de aplicação (API) ou semelhantes. Além disso, durante configuração de uma regra de processamento de aplicação maliciosa, regras de processamento diferentes podem ser configuradas de acordo com os tipos de ataque ou níveis de perigo de aplicações maliciosas, para processar diferencialmente as aplicações maliciosas, implementando, desse modo, flexibilidade e escalabilidade da proteção de segurança. Certamente, pode ser entendido que uma ou mais das três regras podem não ser configuradas pelo administrador, e podem ser definidas pelo sistema de computação em nuvem de acordo com uma regra padrão.

[00141] Além disso, para implementar proteção de segurança de granularidade mais fina, a regra de detecção de comportamento entregue ao detector de segurança pelo aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem pode incluir uma regra de detecção de processo ou uma regra de detecção de rotina. Desta forma, o detector de segurança pode realizar detecção de nível de processo ou nível de rotina em uma aplicação de nuvem; o aparelho 20 para processar um comportamento de ataque de uma

aplicação de nuvem pode determinar, com base em um resultado de detecção do detector de segurança, um processo ou rotina tendo um comportamento de ataque, e, em seguida, o aparelho 20 pode processar um processo ou rotina tendo um comportamento de ataque, para adicionalmente implementar proteção de segurança de nível de processo ou nível de rotina.

[00142] Deve ser notado que, o aparelho 20 para processar um comportamento de ataque de uma aplicação de nuvem incluído no sistema de proteção de segurança de uma aplicação de nuvem nesta modalidade da presente invenção pode ser o aparelho para processamento de um comportamento de ataque de uma aplicação de nuvem descrito em qualquer uma das modalidades de aparelho anteriores. Para implementação específica, consulte as modalidades de aparelho e método precedentes, e os detalhes não são novamente descritos neste documento.

[00143] No sistema para processamento de um comportamento de ataque de uma aplicação de nuvem fornecido nesta modalidade da presente invenção, um cenário de implantação de aplicação de um sistema de computação em nuvem pode ser satisfeito, proteção de segurança pode ser realizada com base em um nível de aplicação de computação em nuvem, ataques mútuos entre diferentes aplicações no mesmo um hospedeiro, ou ataques internos lançados em um hospedeiro podem ser prevenidos, e impacto em uma aplicação normal pode ser reduzido. Além disso, uma política de processamento de aplicação maliciosa pode ser configurada, para adicionalmente diferencialmente processar aplicações maliciosas de acordo com diferentes níveis de segurança ou diferentes tipos de ataques.

[00144] Uma pessoa com conhecimentos normais na arte pode

entender que todos ou alguns dos passos dos métodos nas modalidades podem ser implementados por um programa instruindo hardware relacionado (tal como um processador). O programa pode ser armazenado em um meio de armazenamento legível por computador. O meio de armazenamento pode incluir: uma ROM, uma RAM, um disco magnético ou um disco óptico.

[00145] O anterior descreve em detalhe o método e aparelho para processamento de um comportamento de ataque de uma aplicação de nuvem e o sistema que são fornecidos em modalidades da presente invenção. Na presente memória descritiva, exemplos específicos são utilizados para descrever o princípio de formas de implementação da presente invenção, e a descrição das modalidades destina-se apenas a ajudar a compreender o método e a ideia de núcleo da presente invenção. Além disso, uma pessoa com conhecimentos normais na arte pode, com base na ideia da presente invenção, fazer modificações no que diz respeito às formas de implementação específicas e o espaço de aplicação. Portanto, o conteúdo desta especificação não deverá ser interpretado como uma limitação para a presente invenção.

REIVINDICAÇÕES

1. Aparelho (20) para processar um comportamento de ataque em um sistema de computação em nuvem, **caracterizado** pelo fato de que compreende:

um processador de segurança (203);

um gestor de políticas (201), configurado para:

armazenar uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa;

converter a regra de determinação de segurança em uma regra de detecção de comportamento; e

entregar a regra de detecção de comportamento para um detector de segurança (205) implantado em pelo menos um hospedeiro de nuvem (10) entre uma pluralidade de hospedeiros de nuvem (10, 11, 12) no sistema de computação em nuvem, e

um analisador de segurança (202) acoplado ao processador de segurança (203) e o gestor de políticas (201) e configurado para:

receber os dados de comportamento de aplicação do detector de segurança, em que os dados de comportamento de aplicação correspondem a um comportamento de uma aplicação de nuvem executando no pelo menos um hospedeiro de nuvem e em que o comportamento da aplicação de nuvem é detectado pelo detector de segurança usando a regra de detecção de comportamento; e

enviar os dados de comportamento de aplicação para o processador de segurança quando a aplicação de nuvem executando no pelo menos um hospedeiro de nuvem compreende o comportamento de ataque, em que os dados de comportamento de representam um estado de execução da aplicação de nuvem, e em que o comportamento de ataque é detectado de acordo com

os dados de comportamento de aplicação e a regra de determinação de segurança armazenada no gestor de políticas (201), e

em que o processador de segurança (203) é configurado para invocar, de acordo com a regra de processamento de aplicação maliciosa armazenada no gestor de políticas, uma interface fornecida por um controlador de nuvem (206) no sistema de computação em nuvem, para processar a aplicação de nuvem.

2. Aparelho (20), de acordo com a reivindicação 1, **caracterizado** pelo fato de que compreende ainda: um notificador de informação (204), acoplado ao processador de segurança (203), em que o gestor de políticas configurado para armazenar uma regra de notificação de informação;

em que o analisador de segurança (202) é ainda configurado para:

adquirir informação inicial da aplicação de nuvem, e enviar a informação inicial ao processador de segurança (203), quando a aplicação de nuvem tem o comportamento de ataque

em que a informação inicial identifica a aplicação de nuvem;

em que o processador de segurança (203) é ainda configurado para:

pesquisar, de acordo com a informação inicial da aplicação de nuvem, informação de usuário à qual a aplicação de nuvem pertence, e

enviar a informação de usuário e os dados de comportamento de aplicação ao notificador de informação (204) e

em que o notificador de informação é configurado para:

armazenar os dados de comportamento de aplicação e a informação de usuário à qual a aplicação de nuvem pertence; e

executar processamento de notificação de informação de ataque de acordo com a regra de notificação de informação armazenada no gestor de políticas (201).

3. Aparelho (20), de acordo com a reivindicação 1, **caracterizado** pelo fato de que a regra de processamento de aplicação maliciosa indica maneiras de processamento de diferentes tipos de aplicações maliciosas, ou maneiras de processamento de aplicações maliciosas compreendendo diferentes níveis de perigo, em que as aplicações maliciosas são aplicações de nuvem tendo comportamentos de ataque; e em que o processador de segurança (203) é configurado ainda para:

executar processamento na aplicação de nuvem de acordo com um tipo do comportamento de ataque da aplicação de nuvem, e em que uma maneira de processar a aplicação de nuvem que é indicada pela regra de processamento de aplicação maliciosa; ou

executar processamento na aplicação de nuvem de acordo com um nível de perigo do comportamento de ataque da aplicação de nuvem, em que uma maneira de processar a aplicação de nuvem tendo o nível de perigo é indicada pela regra de processamento de aplicação maliciosa.

4. Aparelho (20), de acordo com a reivindicação 2, **caracterizado** pelo fato de que o processamento de notificação de informação de ataque compreende pelo menos uma de:

gerar informação de alarme,

exibir a aplicação de nuvem e a informação de usuário

à qual a aplicação de nuvem pertence; ou

notificar um centro de alarme da informação de usuário para o qual a aplicação de nuvem pertence.

5. Aparelho (20), de acordo com a reivindicação 2, **caracterizado** pelo fato de que o aparelho (20) é integrado no controlador de nuvem (206).

6. Aparelho (20), de acordo com a reivindicação 2, **caracterizado** pelo fato de que uma ou mais das regras de determinação de segurança, regra de processamento de aplicação maliciosa, ou regra de notificação de informação são configuradas usando uma interface de configuração do gestor de políticas, e em que a interface de configuração do gestor de políticas (201) compreende pelo menos uma de uma janela de configuração ou uma interface de programação de aplicação (API).

7. Aparelho (20), de acordo com a reivindicação 1, **caracterizado** pelo fato de que a regra de detecção de comportamento compreende uma regra de detecção de rotina, e

em que os dados de comportamento de aplicação são obtidos depois que o detector de segurança (205) detecta uma rotina da aplicação de nuvem de acordo com a regra de detecção de comportamento.

8. Aparelho (20), de acordo com a reivindicação 7, **caracterizado** pelo fato de que o analisador de segurança (202) é ainda configurado para: descartar os dados de comportamento de aplicação quando a aplicação de nuvem não tem o comportamento de ataque.

9. Método para processar um comportamento de ataque em um sistema de computação em nuvem, **caracterizado** pelo fato de que compreende:

armazenar, por um gestor de políticas (201), uma regra de determinação de segurança e uma regra de processamento de aplicação maliciosa;

converter, pelo gestor de políticas (201), a regra de determinação de segurança na regra de detecção de comportamento;

enviar, pelo gestor de políticas (201), a regra de detecção de comportamento a um detector de segurança implantado em pelo menos um hospedeiro de nuvem entre uma pluralidade de hospedeiros de nuvem no sistema de computação de nuvem;

receber, por um analisador de segurança, dados de comportamento de aplicação de um detector de segurança, em que os dados de comportamento de aplicação representam um estado de execução da aplicação de nuvem executando no pelo menos um hospedeiro de nuvem, em que os dados de comportamento de aplicação correspondem a um comportamento da aplicação de nuvem executando no pelo menos um hospedeiro de nuvem, e em que o comportamento da aplicação de nuvem é detectado por detector de segurança usando a regra de detecção de comportamento;

determinar (902), pelo analisador de segurança, de acordo com os dados de comportamento de aplicação e a regra de determinação de segurança, que é armazenada no gestor de políticas (201), se a aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque; e

invocar, de acordo com uma regra de processamento de aplicação maliciosa, uma interface fornecida por um controlador de nuvem, para processar a aplicação de nuvem quando a aplicação de nuvem executando no pelo menos um

hospedeiro de nuvem tiver um comportamento de ataque.

10. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de que compreende ainda:

pesquisar, de acordo com informação inicial da aplicação de nuvem, para informação de usuário à qual a aplicação de nuvem pertence, em que a informação inicial identifica a aplicação de nuvem;

armazenar os dados de comportamento de aplicação da aplicação de nuvem e a informação de usuário obtida através da pesquisa, e executar processamento de notificação de informação de ataque de acordo com uma regra de notificação de informação.

11. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de que compreende ainda:

descartar os dados de comportamento de aplicação quando a aplicação de nuvem executando no pelo menos um hospedeiro de nuvem não compreende o comportamento de ataque.

12. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de que a regra de processamento de aplicação maliciosa indica maneiras de processamento de diferentes tipos de aplicações maliciosas, ou maneiras de processamento de aplicações maliciosas compreendendo diferentes níveis de perigo, em que as aplicações maliciosas são aplicações de nuvem com comportamentos de ataque, e em que invocação de uma interface fornecida pelo controlador de nuvem, para processar a aplicação de nuvem compreende:

executar processamento na aplicação de nuvem de acordo com um tipo do comportamento de ataque da aplicação de nuvem, em que uma maneira de processamento da aplicação de nuvem é indicada pela regra de processamento de aplicação maliciosa;

ou

executar processamento na aplicação de nuvem de acordo com um nível de perigo do comportamento de ataque da aplicação de nuvem, em que uma maneira de processamento de uma aplicação tendo o nível de perigo é indicada pela regra de processamento de aplicação maliciosa.

13. Método, de acordo com a reivindicação 10, **caracterizado** pelo fato de que a execução de processamento de notificação de informação de ataque compreende pelo menos uma das seguintes operações:

gerar informação de alarme,

exibir a aplicação de nuvem e a informação de usuário para qual a aplicação de nuvem pertence; ou

notificar um centro de alarme da informação de usuário à qual a aplicação de nuvem pertence.

14. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de que uma ou mais das regras de determinação de segurança, regra de processamento de aplicação maliciosa, ou regra de notificação de informação são configuradas usando uma interface de configuração, e em que a interface de configuração compreende pelo menos uma de uma janela de configuração ou uma interface de programação de aplicação (API).

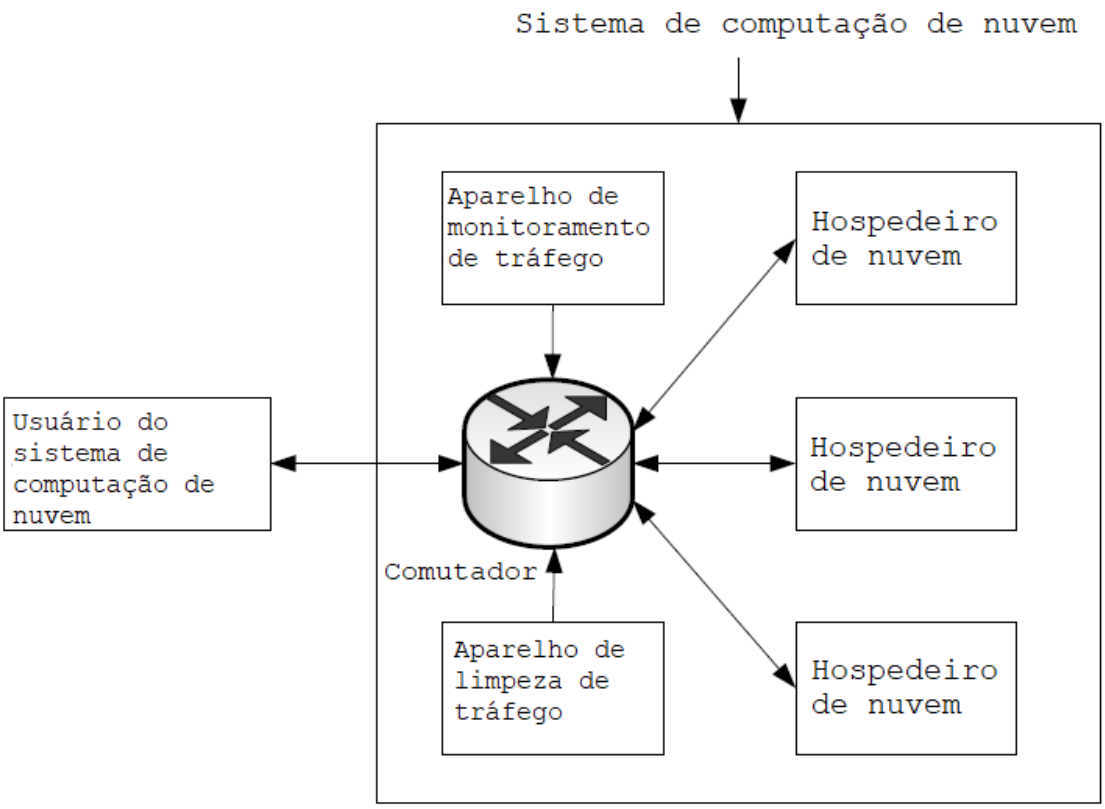
Sistema de computação de nuvem
Aparelho de monitoramento de tráfego
Hospedeiro de nuvem
Usuário do sistema de computação de nuvem
Hospedeiro de nuvem
Comutador
Aparelho de limpeza de tráfego
Hospedeiro de nuvem

FIG. 1

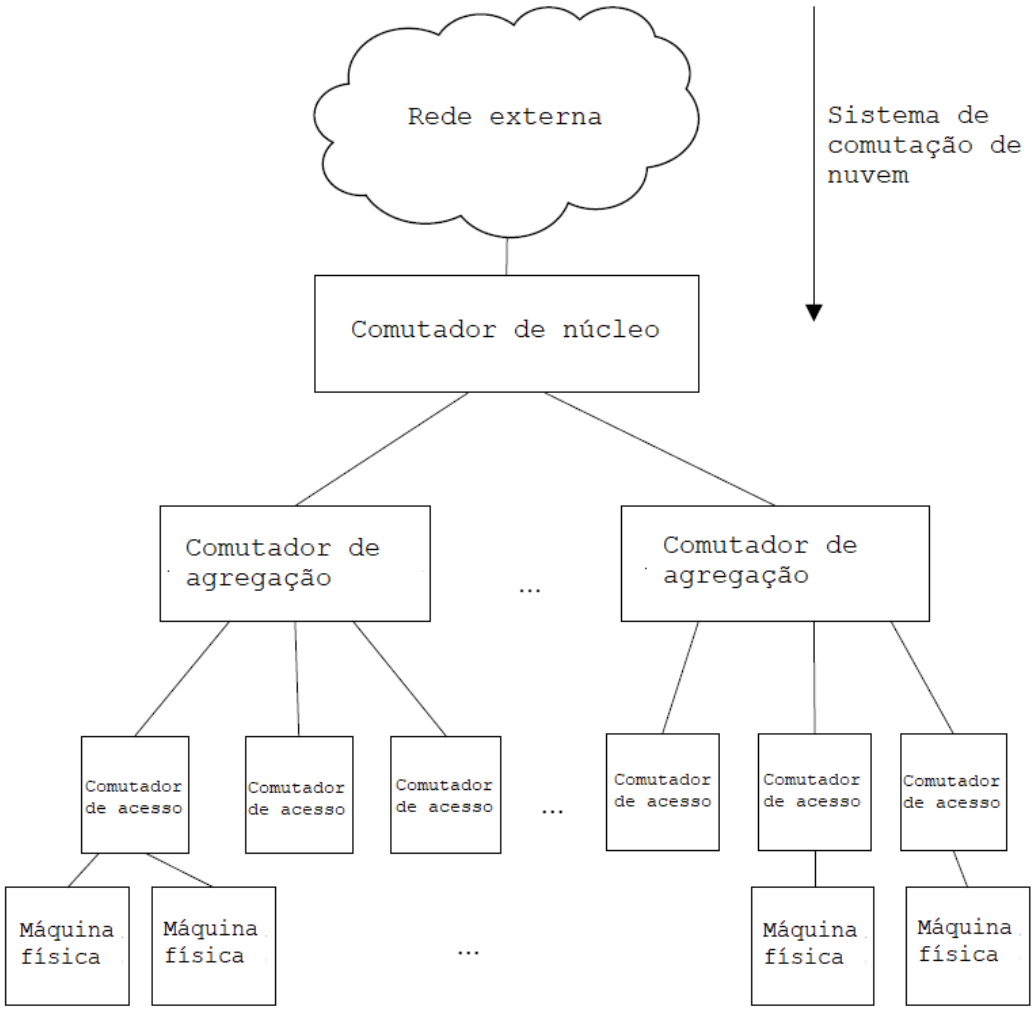
Rede externa
Sistema de comutação de nuvem
Comutador de núcleo
Comutador de agregação
...
Comutador de agregação
Comutador de acesso
Comutador de acesso
Comutador de acesso
...
Comutador de acesso
Comutador de acesso
Comutador de acesso
Máquina física
Máquina física
...
Máquina física
Máquina física

FIG. 2

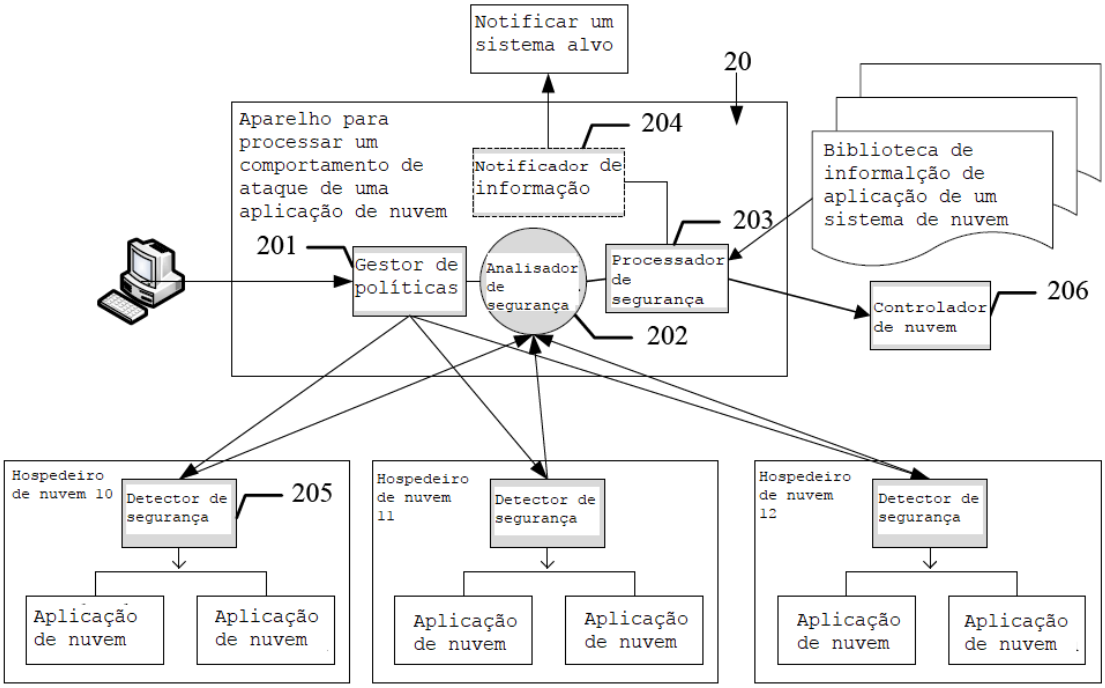
Notificar um sistema alvo
20
Aparelho para processar um comportamento de ataque de uma aplicação de nuvem
204
Notificador de informação
203
Biblioteca de informalção de aplicação de um sistema de nuvem
201
Gestor de políticas
Analisador de segurança
Processador de segurança
202
Controlador de nuvem
206
Hospedeiro de nuvem 10
Detector de segurança
205
Aplicação de nuvem
Aplicação de nuvem
Hospedeiro de nuvem 11
Detector de segurança
Aplicação de nuvem
Aplicação de nuvem
Hospedeiro de nuvem 12
Detector de segurança
Aplicação de nuvem
Aplicação de nuvem

FIG. 3

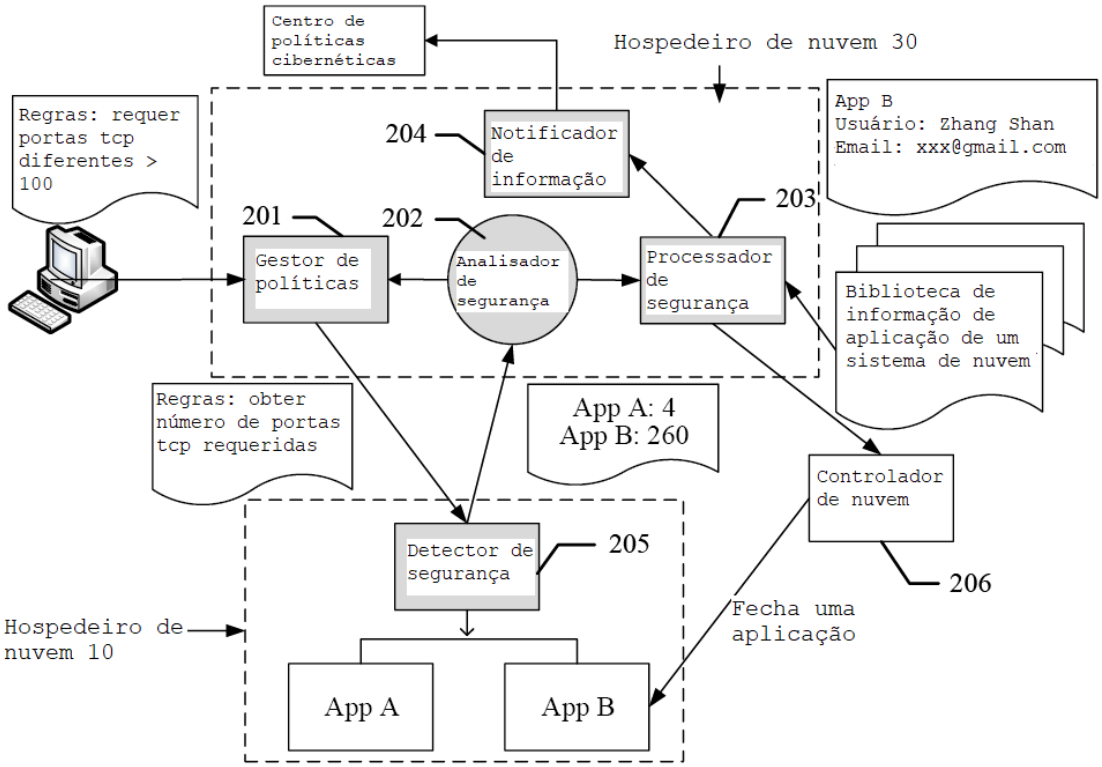
Centro de políticas cibernéticas
Hospedeiro de nuvem 30
Regras: requer portas tcp diferentes > 100
204
Notificador de informação
App B
Usuário: Zhang Shan
Email: xxx@gmail.com
201
202
203
Gestor de políticas
Analisador de segurança
Processador de segurança
Biblioteca de informação de aplicação de um sistema de nuvem
Regras: obter número de portas tcp requeridas
App A: 4
App B: 260
Controlador de nuvem
Detector de segurança
205
206
Hospedeiro de nuvem 10
Fecha uma aplicação
App A
App B

FIG. 4

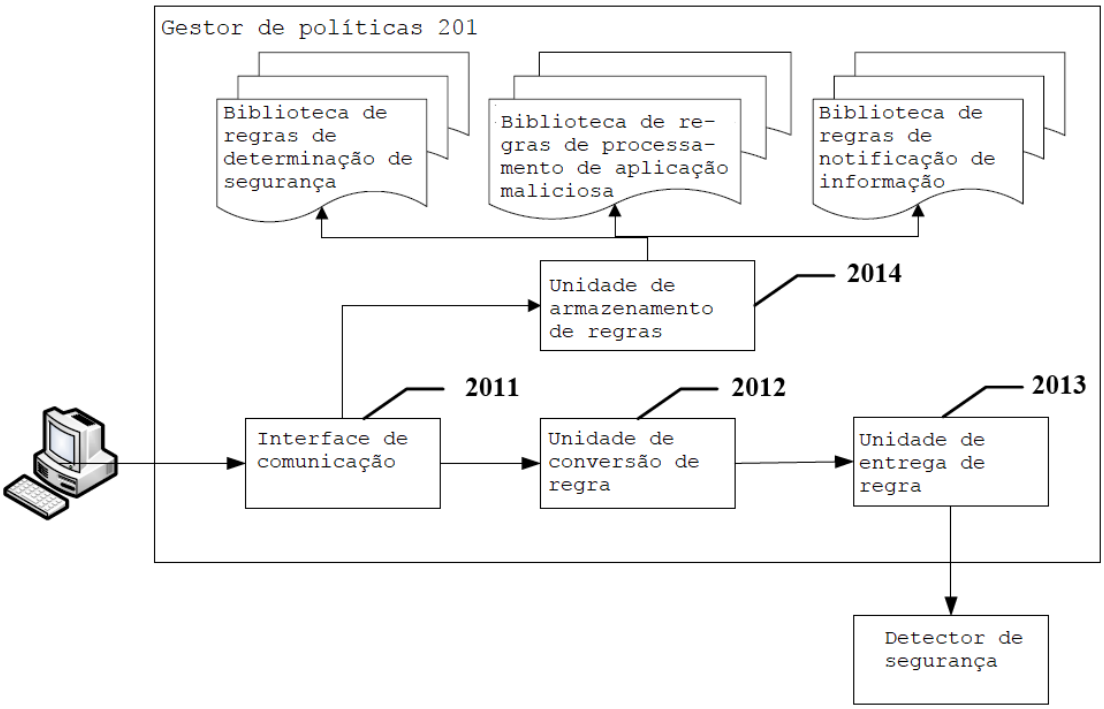
Gestor de políticas 201
Biblioteca de regras de determinação de segurança
Biblioteca de regras de processamento de aplicação maliciosa
Biblioteca de regras de notificação de informação
Unidade de armazenamento de regras
2014
2011
2012
2013
Interface de comunicação
Unidade de conversão de regra
Unidade de entrega de regra
Detector de segurança

FIG. 5

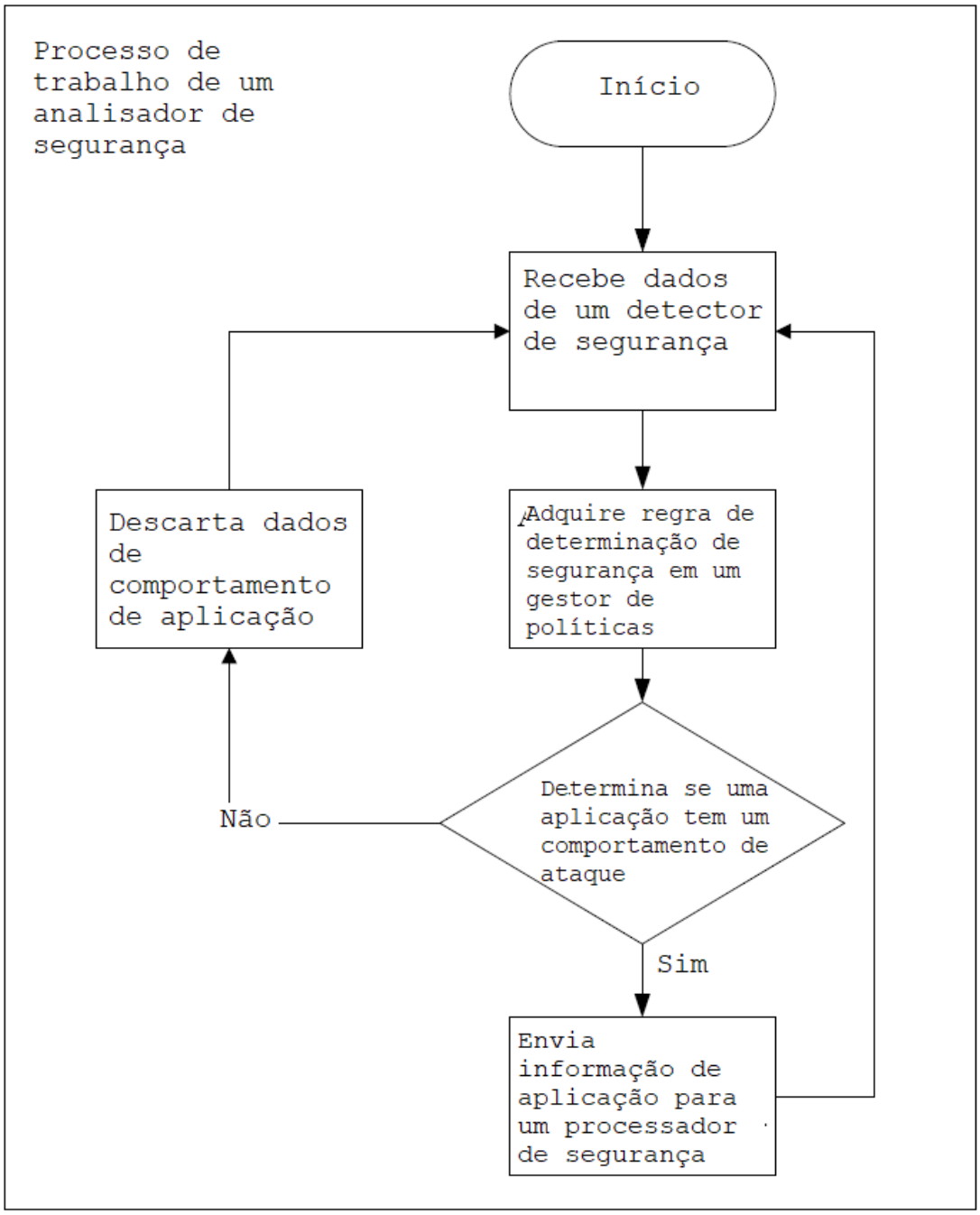
Processo de trabalho de um analisador de segurança
Início
Recebe dados de um detector de segurança
Adquire regra de determinação de segurança em um gestor de políticas
Determina se uma aplicação tem um comportamento de ataque
Não
Descarta dados de comportamento de aplicação
Sim
Envia informação de aplicação para um processador de segurança

FIG. 6

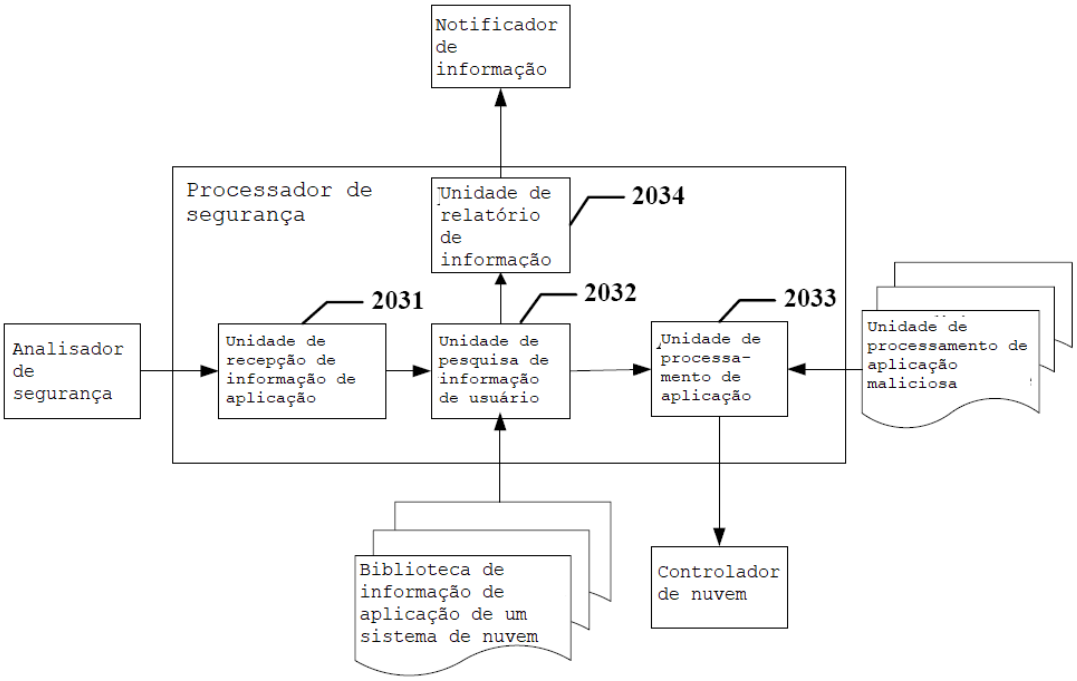
Notificador de informação
Processador de segurança
Unidade de relatório de informação
2034
2031
2032
2033
Analisador de segurança
Unidade de recepção de informação de aplicação
Unidade de pesquisa de informação de usuário
Unidade de processa-mento de aplicação
Unidade de processamento de aplicação maliciosa
Biblioteca de informação de aplicação de um sistema de nuvem
Controlador de nuvem

FIG. 7

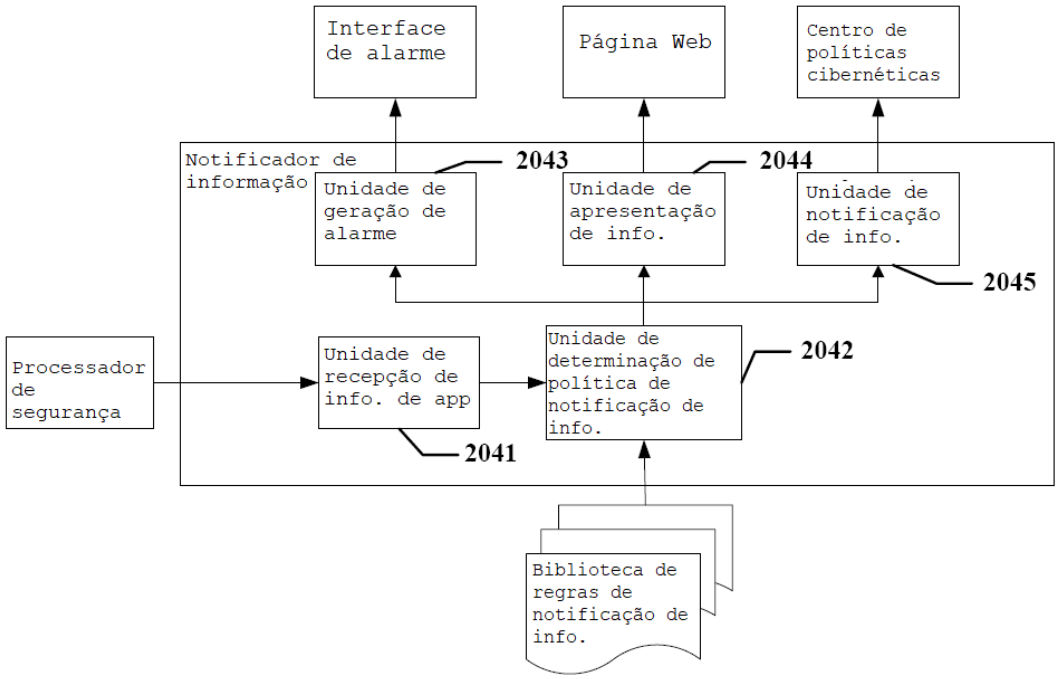
Interface de alarme
Página Web
Centro de políticas cibernéticas
Notificador de informação
2043
2044
Unidade de geração de alarme
Unidade de apresentação de info.
Unidade de notificação de info.
2045
Processador de segurança
Unidade de recepção de info. de app
Unidade de determinação de política de notificação de info.
2042
2041
Biblioteca de regras de notificação de info.

FIG. 8

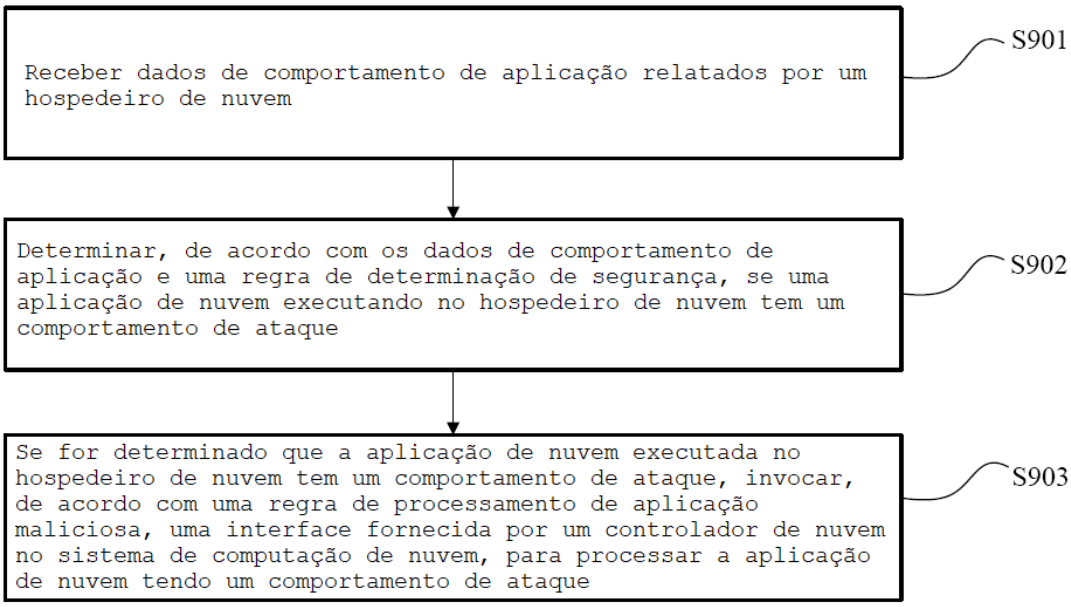
Receber dados de comportamento de aplicação relatados por um hospedeiro de nuvem
S901
Determinar, de acordo com os dados de comportamento de aplicação e uma regra de determinação de segurança, se uma aplicação de nuvem executando no hospedeiro de nuvem tem um comportamento de ataque
S902
Se for determinado que a aplicação de nuvem executada no hospedeiro de nuvem tem um comportamento de ataque, invocar, de acordo com uma regra de processamento de aplicação maliciosa, uma interface fornecida por um controlador de nuvem no sistema de computação de nuvem, para processar a aplicação de nuvem tendo um comportamento de ataque
S903

FIG. 9

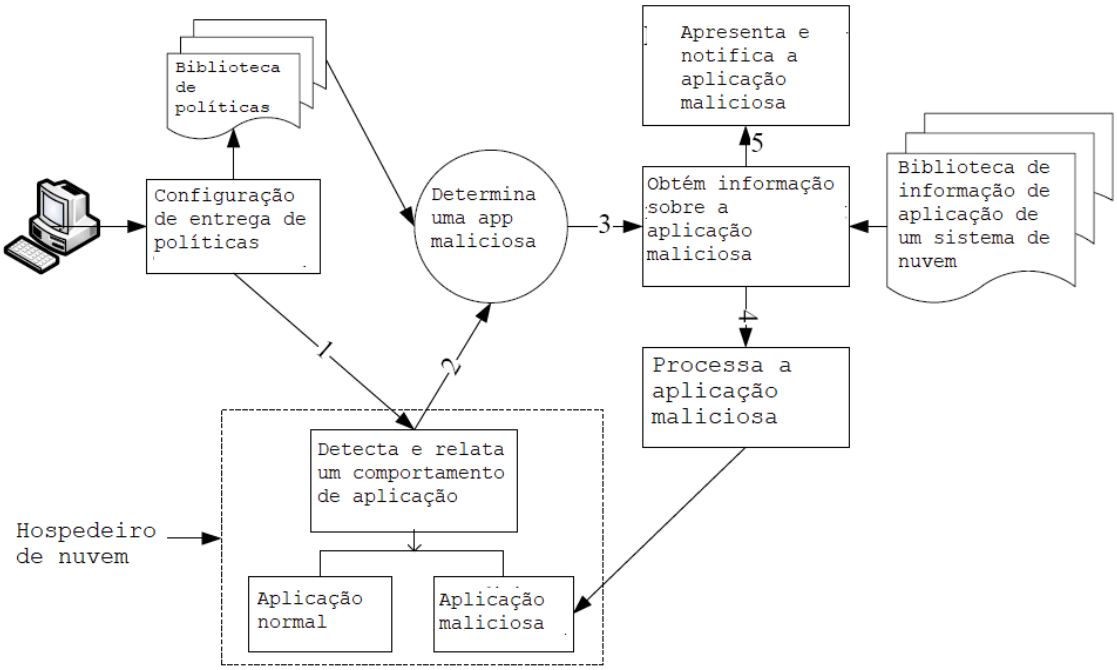
Biblioteca de políticas
Configuração de entrega de políticas
Determina uma app maliciosa
Apresenta e notifica a aplicação maliciosa
Obtém informação sobre a aplicação maliciosa
Biblioteca de informação de aplicação de um sistema de nuvem
Processa a aplicação maliciosa
Detecta e relata um comportamento de aplicação
Hospedeiro de nuvem
Aplicação normal
Aplicação maliciosa
1
2
3
4
5

FIG. 10

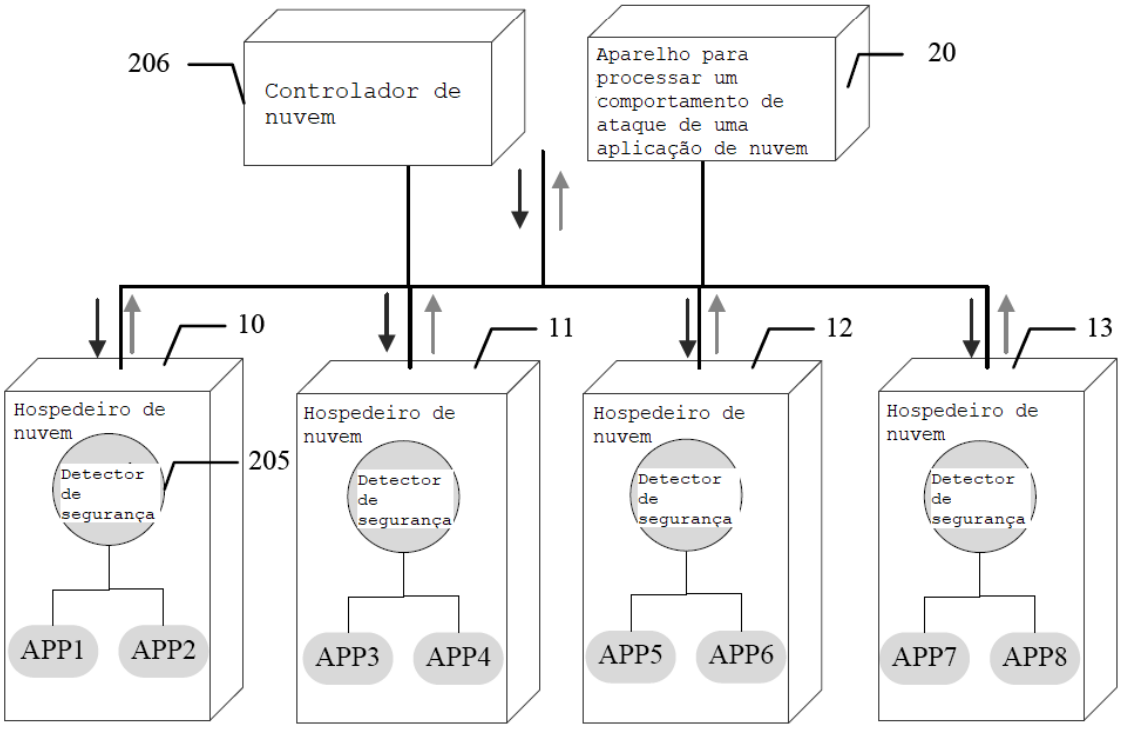
206
Controlador de nuvem
Aparelho para processar um comportamento de ataque de uma aplicação de nuvem
20
10
11
12
13
Hospedeiro de nuvem
Detector de segurança
205
APP1
APP2
APP3
APP4
APP5
APP6
APP7
APP8

FIG. 11

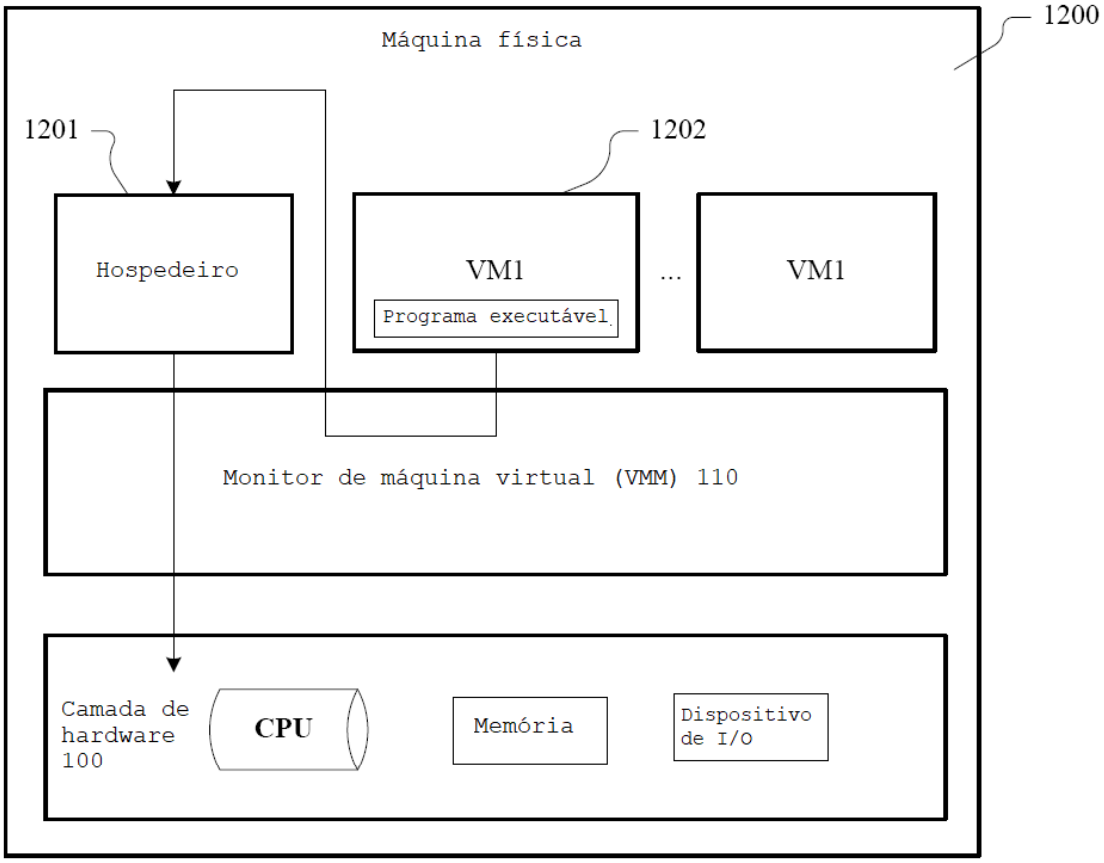
1200
Máquina física
1201
1202
Hospedeiro
VM1
Programa executável
...
VM1
Monitor de máquina virtual (VMM) 110
Camada de hardware 100
CPU
Memória
Dispositivo de I/O

FIG. 12

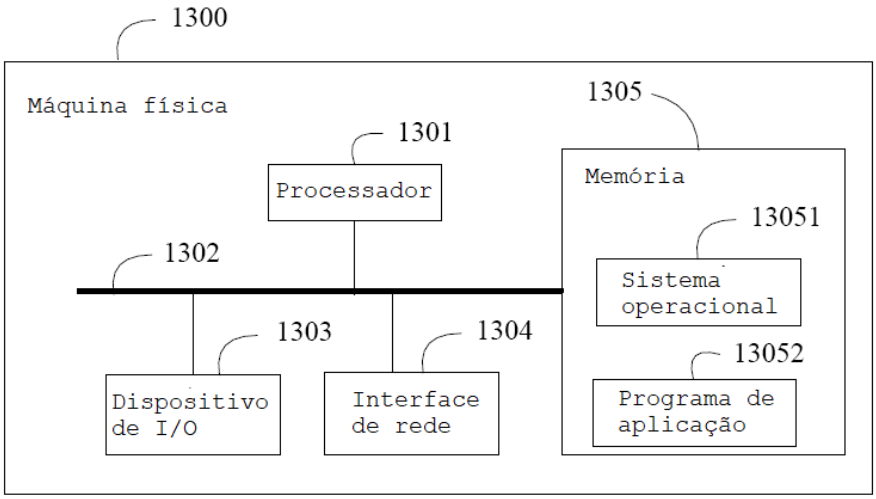
1300
Máquina física
1305
1301
Processador
Memória
13051
1302
Sistema operacional
1303
1304
13052
Dispositivo de I/O
Interface de rede
Programa de aplicação

FIG. 13