(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2016 年 6 月 2 日 (02.06.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/082501 A1

(51) 国际专利分类号:
G06F 21/56 (2013.01)

(21) 国际申请号: PCT/CN2015/079897

(22) 国际申请日: 2015 年 5 月 27 日 (27.05.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410709018.9 2014 年 11 月 26 日 (26.11.2014) CN

(71) 申请人: **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **蒙泽超 (MENG, Zechao)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **刘赫伟 (LIU, Hewei)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: METHOD, APPARATUS AND SYSTEM FOR PROCESSING CLOUD APPLICATION ATTACK BEHAVIOURS IN CLOUD COMPUTING SYSTEM

(54) **发明名称** : 一种云计算系统中云应用攻击行为处理方法、装置及系统

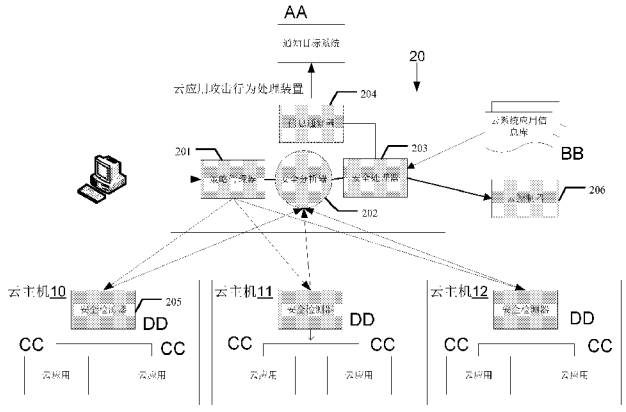


图 3 / Fig. 3

10,11,12 Cloud host
20 Cloud application attack behaviour processing apparatus
201 Policy manager
202 Security analyser
203 Security processor
204 Information notifier
205 Security detector
206 Cloud controller
AA Notification target system
BB Cloud system application information base
CC Cloud application
DD Security detector

(57) **Abstract**: Disclosed is an apparatus for processing cloud application attack behaviours in a cloud computing system, comprising: a security analyser, a security processor and a policy manager, wherein the policy manager is used for storing a security judgement rule and a malicious application processing rule; the security analyser is used for receiving application behaviour data sent by a security detector, determining whether cloud applications running on a cloud host have attack behaviours according to the application behaviour data and the security judgement rule, and sending the application behaviour data to the security processor when it is determined that the cloud applications running on the cloud host have attack behaviours; and the security processor is used for invoking an interface provided by a cloud controller in the cloud computing system to process the cloud applications having the attack behaviours according to the malicious application processing rule. The solution in the present invention performs security protection based on a cloud computing application level, can prevent mutual attacks between different applications inside the same host, and also reduces the influence on normal applications.

(57) **摘要**:

[见续页]

WO 2016/082501 A1

本发明公开了一种云计算系统中云应用攻击行为的处理装置，包括：安全分析器，安全处理器和策略管理器，其中：策略管理器用于存储安全判断规则和恶意应用处理规则；安全分析器用于接收安全检测器发送的应用行为数据，根据该应用行为数据以及安全判断规则，确定该云主机上运行的云应用是否存在攻击行为，并在确定该云主机上运行的云应用存在攻击行为时，将该应用行为数据发送给安全处理器；安全处理器，用于根据恶意应用处理规则，调用云计算系统中的云控制器提供的接口对存在攻击行为的云应用进行处理。本发明方案基于云计算应用级别进行安全防护，能防止同一个主机内部不同应用之间的相互攻击，同时减少对正常应用的影响。

一种云计算系统中云应用攻击行为处理方法、装置及系统

技术领域

本发明涉及计算机技术领域，尤其涉及一种云计算系统中云应用攻击行为的处理方法、装置及系统。

背景技术

根据美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）的定义，云计算有三大服务模式，分别是 SaaS (software as a service, 软件即服务)、PaaS (platform as a service 平台即服务)和 IaaS (infrastructure as a service, 基础设施即服务)。其中 PaaS 是把服务器平台作为一种服务提供的商业模式。PaaS 主要为云应用提供 CPU、内存等硬件资源以及操作系统、程序依赖库等软件资源，云应用的开发者不必关心应用运行的软硬件环境，集中精力在开发应用程序本身。PaaS 的出现，加快了云应用的开发和部署，因此在互联网时代，越来越多的云应用将会被部署到云计算系统中。

在云计算系统（可简称云系统）中，为了增加系统硬件资源的利用率，通常会将多个云应用运行在同一个云主机中（硬件主机或虚拟主机，不同的云计算系统有不同的实现），云计算系统为云应用提供必要的系统资源隔离，保证运行在同一云主机中运行的云应用之间不会相互干扰。同时云计算系统还提供云主机内的虚拟网络以供云应用之间的通信。

在另一方面的网络安全领域，黑客们向目标机器发起攻击之前，为了隐藏自己的身份，通常会在网络上寻找肉鸡（可被控制的傀儡机），然后通过肉鸡再来发起攻击。这样就算被攻击者检查到攻击，也只能查到肉鸡的地址，查不到黑客们的真实地址。在云计算系统兴起之后，网络黑客便可以不用再寻找肉鸡，而是直接将他们的攻击程序运行在云计算系统上，并且能够运行多份攻击程序的实例，形成一个大规模的攻击系统。在云计算系统中，黑客不仅能利用原有的攻击程序向目标进行攻击，并且可以利用云计算系统内部运行有大量的云应用程序这个特点，通过攻击程序攻击云计算系统内部不同云主机上的应用程序，甚至是同一云主机内部的其他应用程序。

现有技术中一般是通过流量检测与流量清洗方法解决云计算系统受到攻击的问题。如图 1 所示，在云计算系统内部新增流量检测装置，通过交换机与

云计算系统的云主机连接，用以检测云计算系统内注入云主机的数据流，包括云计算系统外部的用户访问云应用的数据流，以及云计算系统内部各云主机之间相互交互的数据流。通过流量检测装置统计出预定时长内注入某一云主机的数据流流量大小，当统计得到的流量数值超过了预定的阈值时，就认为注入该云主机的流量发生异常。检测到流量发生异常后，流量检测装置会通知流量清洗装置启动，流量清洗装置将对注入该云主机的数据流量进行清洗，过滤掉攻击报文，再将清洗后的数据流发送给该云主机。

现有技术的方案只能防止云计算系统内部云主机之间的攻击，或者外部向云计算系统内部云主机的攻击，但是无法防止同一个云主机内部不同云应用之间的相互攻击，或者云主机内部对云主机本身进行的攻击。另外，现有技术方案以云主机为单位进行流量监控和清洗，会影响到目标云主机中的所有云应用。

发明内容

本发明实施例提供一种云计算系统中云应用攻击行为的处理方法、装置及系统，用于对云计算系统进行应用级别的安全防护，并且尽可能减少对云计算机系统内正常的云应用的影响。

第一方面，本发明实施例提供了一种云计算系统中云应用攻击行为的处理装置，包括:

安全分析器，安全处理器和策略管理器，其中:

策略管理器用于存储安全判断规则和恶意应用处理规则;

安全分析器用于接收云计算系统中的多个云主机中的至少一个云主机上的安全检测器发送的应用行为数据，根据该应用行为数据以及策略管理器中存储的安全判断规则，确定该云主机上运行的云应用是否存在攻击行为，并在确定该云主机上运行的云应用存在攻击行为时，将该应用行为数据发送给安全处理器；其中，该应用行为数据是该云主机上的安全检测器根据行为检测规则对该云应用进行检测后得到的，且该应用行为数据用于表示该云应用的运行状态;

安全处理器，用于根据策略管理器中存储的恶意应用处理规则，调用云计算系统中的云控制器提供的接口对存在攻击行为的云应用进行处理，该云控制

器与云计算系统中的云主机通信连接或集成于一个云主机上，用于控制云计算系统中的云主机上运行的云应用。

在第一方面的第一种可能的实现方式中，该装置还包括：信息通知器；策略管理器中还用于存储信息通知规则；

安全分析器还用于，当确定云应用存在攻击行为时，获取该云应用的初始信息并发送给安全处理器，其中，初始信息用于唯一标识云应用；

安全处理器还用于，根据云应用的初始信息查询该云应用所属的用户信息，将该用户信息和该云应用的应用行为数据发送给信息通知器；

信息通知器用于，将接收到的应用行为数据和用户信息存储并按照策略管理器中存储的信息通知规则进行攻击信息通知处理。

结合第一方面，或者第一方面第一种可能的实现方式，在第二种可能的实现方式中，

策略管理器用于，将安全判断规则转化为行为检测规则，并将该行为检测规则下发给各个云主机的安全检测器。

结合第一方面，或者第一方面第一至第二种任意一种可能的实现方式，在第三种可能的实现方式中，其中，所述恶意应用为存在攻击行为的云应用；所述安全处理器，具体用于根据所述云应用的攻击行为的类型，以及所述恶意应用处理规则所指示的对该类型应用的处理方式，对所述云应用进行相应处理；或者所述安全处理器，具体用于根据所述云应用的攻击行为的危险程度，以及所述恶意应用处理规则所指示的对该危险程度的应用的处理方式，对所述云应用进行相应处理。

结合第一方面第一至第三种任意一种可能的实现方式，在第四种可能的实现方式中，攻击信息通知处理具体包括以下之一或其任意组合：产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、以及将存在攻击行为的云应用所属的用户信息通知网警中心。

结合第一方面，或者第一方面第一至第四种任意一种可能的实现方式，在第五种可能的实现方式中，云应用攻击行为处理装置集成于云控制器。

结合第一方面第一到第五种中任意一种可能的实现方式，在第六种可能的实现方式中，策略管理器的配置接口包括：配置界面和应用程序接口中的至少一种。

结合第一方面，或者第一方面第一至第五种任意一种可能的实现方式，在第七种可能的实现方式中，所述行为检测规则包括：进程检测规则或线程检测规则；应用行为数据是安全检测器根据该行为检测规则对所述云应用的进程或线程进行检测后得到的。

结合第一方面第七种可能的实现方式，在第八种可能的实现方式中，安全分析器还用于在确定云应用不存在攻击行为时，丢弃该云应用的行为数据。

结合第一方面上述所有可能的实现方式，在第九种可能的实现方式中，云主机可以为物理机，或者运行于物理机之上的虚拟机。

结合第一方面上述任意一种可能的实现方式，在第十种可能的实现方式中，运行于云主机上的应用程序为云应用，且一个云主机上上运行有一个或多个云应用，其中，每一个云应用用于实现相应的业务功能。

结合第一方面上述任意一种可能的实现方式，在第十一种可能的实现方式中，每一台云主机上部署有一安全检测器，该安全检测器用于依据行为检测规则对该云主机上运行的云应用的行为进行采集，并根据采集结果生成应用行为数据上报给安全分析器。

结合第一方面第十一种可能的实现方式，在第十二种可能的实现方式中，安全检测器将应用行为数据定期，或者基于请求，或者根据预先配置的上报策略上报给安全分析器。

结合第一方面上述任意一种可能的实现方式，在第十三种可能的实现方式中，安全判断规则用于定义云应用的何种行为为攻击行为，恶意应用处理规则用于定义对于存在攻击行为的云应用采取何种处理方式；行为检测规则用于指示对云应用进行检测的检测指标。

结合第一方面上述任意一种可能的实现方式，在第十四种可能的实现方式中，将存在攻击行为的云应用定义为恶意应用。

结合第一方面第三种至第十四种可能的实现方式中的任一种，在第十五种可能的实现方式中，安全分析器或安全处理器用于根据云应用的行为数据，查询预先配置的应用特征库，以确定应用攻击行为的类型，其中，应用特征库用于描述应用的行为特征与应用的攻击行为类型的映射关系。

结合第一方面第十五种可能的实现方式，在第十六种可能的实现方式中，应用特征库是云计算系统中的一个独立的数据集或者是安全判断规则的子集；

安全分析器在根据安全判断规则判断出某一云应用为恶意应用之后，进一步根据安全判断规则中包含的应用特征库，确定恶意应用的攻击行为类型。

结合第一方面第三种至第十六种可能的实现方式中的任一种，在第十七种可能的实现方式中，云应用的危险程度用于表征云应用对云计算系统的危害程度；安全分析器或安全处理器用于根据根据应用攻击行为的类型，通过查询映射表的方式确定应用的攻击行为的危险程度，其中，该映射表用于表征应用攻击行为的类型与其危险程度的对应关系。

结合第一方面的上述任意一种可能的实现方式，在第十八种可能的实现方式中，云应用的用户信息包括但不限于：用户名、用户邮箱或用户身份证号中的一项或多项。

结合第一方面的上述任意一种可能的实现方式，在第十九种可能的实现方式中，云应用的初始信息包括但不限于：进程 ID 和进程名称中一项或多项。

结合第一方面的上述任意一种可能的实现方式，在第二十种可能的实现方式中，调用云控制器对恶意进行处理包括以下之一或其任意组合：关闭恶意应用，或者将恶意应用迁移到隔离的云主机，以及禁止恶意应用的用户账户。

结合第一方面的上述任意一种可能的实现方式，在第二十一种可能的实现方式中，云应用攻击行为处理装置为云计算系统中的一台云主机，该云主机为运行在物理机上的虚拟机；该物理机包括硬件层，运行在硬件层之上的虚拟机监视器，以及运行在虚拟机监视器之上的宿主机和若干虚拟机，其中，硬件层包括处理器和存储器，该云主机上运行有可执行程序，该可执行程序包括：策略管理器模块、安全分析器模块、安全处理器模块以及信息通知器模块，其中策略管理器模块用于实现上述任一可能的实现方式中的策略管理器的功能，安全分析器模块用于实现上述任一可能的实现方式中的安全分析器的功能，安全处理器模块用于实现上述任一可能的实现方式中的安全处理器的功能，信息通知器模块用于实现上述任一可能的实现方式中的信息通知器的功能。

结合第一方面，或者第一方面第一至第二十种任意一种可能的实现方式，，在第二十二种可能的实现方式中，云应用攻击行为处理装置包括：至少一个处理器，存储器，至少一个通信总线。通信总线用于实现这些组件之间的连接通信。存储器存储了如下的元素，可执行模块或者数据结构，或者他们的子集，或者他们的扩展集：

操作系统，包含各种系统程序，用于实现各种基础业务以及处理基于硬件的任务；

应用程序模块，包含各种云应用，用于实现各种应用业务等。

应用程序模块包括实现策略管理器、安全分析器、安全处理器以及信息通知器的功能的模块。

第二方面，本发明实施例提供了一种云应用攻击行为处理方法，用于包括多个云主机的云计算系统，该方法包括：

接收该多个云主机中的至少一个云主机上报的应用行为数据，其中，该应用行为数据是该云主机上的安全检测器根据行为检测规则对所述该云主机上运行的云应用进行检测后得到的，且该应用行为数据用于表示该云主机上运行的云应用的运行状态；

根据该应用行为数据以及安全判断规则，判断该云主机上运行的云应用是否存在攻击行为；

如果判断该云主机上运行的云应用存在攻击行为，则根据恶意应用处理规则，调用云计算系统中的云控制器提供的接口对存在攻击行为的云应用进行处理，其中该云控制器连接该云主机或集成于该云主机，用于控制该云主机上运行的云应用。

在第二方面的第一种可能的实现方式中，该方法还包括：

如果判断该云主机上运行的云应用存在攻击行为，则根据该存在攻击行为的云应用的初始信息查询该云应用所属的用户信息，其中，该初始信息用于标识该云应用；

将存在攻击行为的云应用的应用行为数据和查询到的用户信息存储，并按照信息通知规则进行攻击信息通知处理。

结合第二方面，或者第二方面第一种可能的实现方式，在第二种可能的实现方式中，该方法还包括：

如果判断该云主机上运行的云应用不存在攻击行为，则丢弃接收到的该应用行为数据。

结合第二方面，或者第二方面第一至第二种任意一种可能的实现方式，在第三种可能的实现方式中，其中，恶意应用为存在攻击行为的云应用；调用云控制器提供的接口对存在攻击行为的云应用进行相应处理，包括：根据云应用

的攻击行为的类型，以及恶意应用处理规则所指示的对该类型应用的处理方式，对该云应用进行相应处理；或者根据该云应用的攻击行为的危险程度，以及恶意应用处理规则所指示的对该危险程度的应用的处理方式，对该云应用进行相应处理。

结合第二方面第一种可能的实现方式以及第三种可能的实现方式中的任意一种可能的实现方式，在第四种可能的实现方式中，按照信息通知规则进行攻击信息通知处理包括以下之一或其任意组合：

产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、以及将存在攻击行为的云应用所属的用户信息通知网警中心。

结合第二方面，或者第二方面第一至第四种任意一种可能的实现方式，在第五种可能的实现方式中，该方法还包括：将安全判断规则转化为行为检测规则，并将该行为检测规则发送给安全检测器。

结合第二方面，或者第二方面第一至第五种任意一种可能的实现方式，在第六种可能的实现方式中，安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项是通过配置接口配置的；其中所述配置接口包括：配置界面和应用程序接口中的至少一种。

结合第二方面上述所有可能的实现方式，在第七种可能的实现方式中，云主机可以为物理机，或者运行于物理机之上的虚拟机。

结合第二方面上述所有可能的实现方式，在第八种可能的实现方式中，运行于云主机上的应用程序为云应用，且一个云主机上上运行有一个或多个云应用，其中，每一个云应用用于实现相应的业务功能。

结合第二方面上述所有可能的实现方式，在第九种可能的实现方式中，每一台云主机上部署有一安全检测器，该安全检测器用于依据行为检测规则对该云主机上运行的云应用的行为进行采集，并根据采集结果生成应用行为数据上报。

结合第二方面第九种可能的实现方式，在第十种可能的实现方式中，安全检测器将应用行为数据定期上报，或者基于请求上报，或者根据预先配置的上报策略上报。

结合第二方面上述所有可能的实现方式，在第十一种可能的实现方式中，安全判断规则用于定义云应用的何种行为为攻击行为，恶意应用处理规则用于

定义对于存在攻击行为的云应用采取何种处理方式；行为检测规则用于指示对云应用进行检测的检测指标。

结合第二方面上述所有可能的实现方式，在第十二种可能的实现方式中，将存在攻击行为的云应用定义为恶意应用。

结合第二方面第三种至第十二种可能的实现方式，在第十三种可能的实现方式中，根据云应用的行为数据，查询预先配置的应用特征库，以确定应用攻击行为的类型，其中，应用特征库用于描述应用的行为特征与应用的攻击行为类型的映射关系。

结合第二方面第十三种可能的实现方式，在第十四种可能的实现方式中，应用特征库是云计算系统中的一个独立的数据集或者是安全判断规则的子集；在根据安全判断规则判断出某一云应用为恶意应用之后，进一步根据安全判断规则中包含的应用特征库，确定恶意应用的攻击行为类型。

结合第二方面第三种至第十四种可能的实现方式中的任一种，在第十五种可能的实现方式中，云应用的危险程度用于表征云应用对云计算系统的危害程度；根据根据应用攻击行为的类型，通过查询映射表的方式确定应用的攻击行为的危险程度，其中，该映射表用于表征应用攻击行为的类型与其危险程度的对应关系。

结合第二方面的上述所有可能的实现方式，在第十六种可能的实现方式中，云应用的用户信息包括但不限于：用户名、用户邮箱或用户身份证号中的一项或多项。

结合第二方面的上述所有可能的实现方式，在第十七种可能的实现方式中，云应用的初始信息包括但不限于：进程 ID 和进程名称中一项或多项。

结合第二方面的上述所有可能的实现方式，在第十八种可能的实现方式中，调用云控制器对恶意进行处理包括以下之一或其任意组合：关闭恶意应用，或者将恶意应用迁移到隔离的云主机，以及禁止恶意应用的用户账户。

第三方面，本发明实施例提供了一种云应用安全防护系统，包括：云应用攻击行为处理装置、云控制器，以及多个安全检测器；其中，多个安全检测器分别部署于多个云主机上，且每一云主机对应于一个安全检测器；云控制器与多个云主机通信连接，用于管理和控制多个云主机，每一云主机上运行有一个或多个云应用；云应用攻击行为处理装置中存储有安全判断规则和恶意应用处

理规则;

安全检测器用于，根据行为检测规则对一个或多个云应用进行检测，以得到应用行为数据，并将该应用行为数据上报给云应用攻击行为处理装置；其中，所述一个或多个云应用运行于该安全检测器对应的云主机上;

云应用攻击行为处理装置用于，接收多个云主机中的至少一个云主机上的安全检测器上报的应用行为数据，根据该应用行为数据以及安全判断规则，判断该云主机上运行的云应用是否存在攻击行为；如果判断该云主机上运行的云应用存在攻击行为，则根据恶意应用处理规则，调用云控制器提供的接口对存在攻击行为的云应用进行相应处理。

在第三方面的第一种可能的实现方式中，云应用攻击行为处理装置还用于，将安全判断规则转化为行为检测规则，并将该行为检测规则下发给各个云主机的安全检测器。

结合第三方面，或者第三方面第一种可能的实现方式，在第二种可能的实现方式中，云应用攻击行为处理装置还用于，如果判断该云主机上运行的云应用不存在攻击行为，则丢弃接收到的该应用行为数据。

结合第三方面，或者第三方面第一种可能的实现方式，在第三种可能的实现方式中，云应用攻击行为处理装置还用于，如果判断该云主机上运行的云应用存在攻击行为，则显示存在攻击行为的云应用以及该云应用所属的用户信息、或者将存在攻击行为的云应用所属的用户信息通知网警中心。

结合第三方面，或者第三方面第一至第三种任意一种可能的实现方式，在第四种可能的实现方式中，应用攻击行为处理装置与云控制器通信连接，或者云应用攻击行为处理装置集成于云控制器上。

结合第三方面，或者第三方面第一至第四种任意一种可能的实现方式，在第五种可能的实现方式中，恶意应用为存在攻击行为的云应用；云应用攻击行为处理装置具体用于：根据云应用的攻击行为的类型，以及恶意应用处理规则所指示的对该类型应用的处理方式，对云应用进行相应处理；或者根据云应用的攻击行为的危险程度，以及恶意应用处理规则所指示的对该危险程度的应用的处理方式，对该云应用进行相应处理。结合第三方面，或者第三方面第一至第五种任意一种可能的实现方式，在第六种可能的实现方式中，安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项是通过配置接口配置的；其

中所述配置接口包括：配置界面和应用程序接口中的至少一种。

结合第三方面，或者第三方面第一至第六种任意一种可能的实现方式，在第七种可能的实现方式中，行为检测规则包括：进程检测规则或线程检测规则；应用行为数据是安全检测器根据该行为检测规则对云应用的进程或线程进行检测后得到的。

结合第三方面，或者第三方面第一至第七种任意一种可能的实现方式，在第八种可能的实现方式中，安全判断规则用于定义云应用的何种行为为攻击行为，恶意应用处理规则用于定义对于存在攻击行为的云应用采取何种处理方式；行为检测规则用于指示对云应用进行检测的检测指标。

结合第三方面，或者第三方面第一至第八种任意一种可能的实现方式，在第九种可能的实现方式中，应用攻击行为处理装置用于根据云应用的行为数据，查询预先配置的应用特征库，以确定应用攻击行为的类型，其中，应用特征库用于描述应用的行为特征与应用的攻击行为类型的映射关系。

结合第三方面第九种可能的实现方式，在第十种可能的实现方式中，应用特征库是云计算系统中的一个独立的数据集或者是安全判断规则的子集；应用攻击行为处理装置用于根据安全判断规则判断出某一云应用为恶意应用之后，进一步根据安全判断规则中包含的应用特征库，确定恶意应用的攻击行为类型。

结合第三方面第五种至第十种可能的实现方式中的任一种，在第十一种可能的实现方式中，云应用的危险程度用于表征云应用对云计算系统的危害程度；应用攻击行为处理装置用于根据根据应用攻击行为的类型，通过查询映射表的方式确定应用的攻击行为的危险程度，其中，该映射表用于表征应用攻击行为的类型与其危险程度的对应关系。

本发明实施例提供的云应用攻击行为处理方法、装置及系统中，策略管理器下发行为检测规则给分布于各个云主机的安全检测器，安全检测器根据行为检测规则检测并上报应用的行为数据，安全分析器通过分析应用的行为数据，确定出存在攻击行为的应用，并调用云控制器进行相应处理，相比于现有技术中的安全方案，本发明实施例基于云计算应用级别进行安全防护，能满足云计算系统应用部署场景，防止同一个主机内部不同应用之间的相互攻击，或者主机内部对主机本身进行的攻击，同时减少对正常应用的影响。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是现有技术中云计算系统攻击处理方法的原理示意图；

图 2 是本发明实施例提供的云计算系统架构图；

图 3 是本发明实施例提供的云应用攻击行为处理装置示意图；

图 4 是本发明实施例提供的云应用攻击行为处理装置示意图；

图 5 是本发明实施例提供的策略管理器结构示意图；

图 6 是本发明实施例提供的安全分析器的工作流程图；

图 7 是本发明实施例提供的安全处理器结构示意图；

图 8 是本发明实施例提供的信息通知器结构示意图；

图 9 是本发明实施例提供的云应用攻击行为处理方法流程图；

图 10 是本发明实施例提供的云应用攻击行为处理方法流程图；

图 11 是本发明实施例提供的云应用安全防护系统示意图；

图 12 是本发明实施例提供的云应用攻击行为处理装置示意图；

图 13 是本发明实施例提供的云应用攻击行为处理装置示意图。

具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

本发明实施例提供的技术方案可典型地应用于云计算系统（可简称为云系统）中，云计算系统可看成是在通用硬件上进行分布式计算、存储及管理的一种集群系统，云计算系统可提供高吞吐量的数据访问，能够应用于大规模数据计算和存储。图 2 描述了云计算系统的物理架构，云计算系统通常包括通过交换机互联的多个物理计算机（可简称为物理机），并且这些物理机可以通过汇

聚交换机以及核心交换机与外部网络互联；其中，物理机具体可以为计算机或服务器等物理实体，在某些组网场景下，云计算系统的一台物理机可以称为一台云主机。随着云计算技术的发展，目前通过虚拟机软件，可以在一台物理计算机上模拟出一台或多台虚拟机，而这些虚拟机可以像真正的计算机那样进行工作，虚拟机上可安装操作系统、安装应用程序、访问网络资源等等。对于在虚拟机中运行的应用程序而言，就像是在真正的计算机中进行工作。因此，一个云计算系统可能包括成千上万个虚拟机，每个虚拟机上都可以独立运行应用程序，因此，在另一些更为通用的组网场景下，云计算系统中的虚拟机通常被称为云主机或者虚拟云主机，而云主机上运行的应用程序称为云应用。故本发明所有实施例所描述的云主机，并不限制为是虚拟机或物理机，需要视具体的组网场景而定。另外，云计算系统还包括有云控制器，用于对云计算系统中的云主机进行控制和管理，云控制器可以是云计算系统包含的若干虚拟机中的一个，某些情形下，云控制器也可是一台独立的物理机，当然，云控制器可以有一个，也可以有多个；云控制器与云计算系统中的云主机通信连接或集成于一个云主机上，用于控制云计算系统中的多个云主机上运行的云应用。本发明实施例的方案具体可以由云计算系统中的云主机来实施，某些情形下，也可以有云控制器来实施。如果依据逻辑架构来划分，云计算系统通常分为基础设施与虚拟化层（IaaS 层）、平台层（PaaS 层）以及应用层（SaaS 层），本发明实施例的方案可以由云计算系统的平台层来实施，具体可以由平台层的云控制器或者另一单独的功能单元来实施。

本发明实施例提供一种云应用攻击行为处理装置，该处理装置可以应用于云计算系统中，以对云计算系统进行安全防护，图 3 为本发明实施例提供的云应用攻击行为处理装置的示意图，在一个具体的实施例中，该处理装置可以为云计算系统的一台云主机，或者作为云控制器中的一个功能单元，集成于云控制器中。根据图 3，云计算系统包括云应用攻击行为处理装置 20、云控制器 206 以及多台云主机（如图 3 中的云主机 10、11 和 12）；其中，每一台云主机上运行有一个或多个云应用，且每一台云主机上部署有一安全检测器，负责依据云应用攻击行为处理装置 20 下发的行为检测规则，对该云主机上运行的云应用的行为进行采集，并将应用的应用行为数据上报给云应用攻击行为处理装置 20，其中应用行为数据用于表示云应用的运行状态，比如云应用的 TCP 链

接信息、网络流量信息、系统调用次数等等。可选的，云应用的应用行为数据上报可以是定期的或基于请求的。具体地，云应用攻击行为处理装置 20 包括：策略管理器 201、安全分析器 202、安全处理器 203。

策略管理器 201 主要用于规则的存储、转化以及下发。具体地，策略管理器 201 中可存储安全判断规则和恶意应用处理规则；安全判断规则用于定义云应用的何种行为为攻击行为，恶意应用处理规则用于定义对于存在攻击行为的云应用采取何种处理方式。在一个优选的实施例中，策略管理器 201 可以将安全判断规则转化为行为检测规则，行为检测规则用于定义对云应用的何种行为进行检测，即行为检测规则指示了对云应用进行检测的检测指标。通常行为检测规则和安全判断规则是密切联系的，因此可以互相转化。举例来说，如果安全判断规则为：云应用向外请求的 TCP 端口数量超过 100 则判断云应用有端口嗅探的行为；那么相应的行为检测规则就为：采集云应用请求不同 TCP 端口的个数。这样，云主机上的安全检测器就应该检测云应用请求不同 TCP 端口的个数并将检测结果上报给安全分析器 202，安全分析器 202 就可以判断云应用是否有端口嗅探的行为。

安全分析器 202 主要用于接收云计算系统中的多个云主机中的至少一个云主机上的安全检测器上报的应用行为数据，然后根据策略管理器 201 中存储的安全判断规则，判断该云主机上的云应用是否存在攻击行为。如果确定云应用存在攻击行为，则将存在攻击行为的云应用的初始信息发送给安全处理器 203；其中，云应用的初始信息用于唯一标识该云应用，比如，在一个具体的实施例中，初始信息可以为进程 ID 或进程名称，或者两者同时包含。可选的，安全检测器上报云应用的应用行为数据，可以是定期上报，也可以是基于请求上报，也可以是根据预先配置的上报策略来上报，本发明实施例不做特别限定。

安全处理器 203 主要用于在接收到安全分析器 202 发送的存在攻击行为的云应用的初始信息后，根据策略管理器 201 中存储的恶意应用处理规则，调用云控制器 206 提供的接口对该存在攻击行为的云应用（本发明实施例中将存在攻击行为的云应用统称为恶意应用）进行处理。在一个实施例中，安全处理器 203 可以对所有恶意应用采用统一处理方式，比如关闭恶意应用，或者将恶意应用迁移到隔离的云主机，或者禁止恶意应用的用户账户。可选地，安全处理

器 203 也可以根据恶意应用攻击行为的类型或者攻击行为的危险程度，对恶意应用进行不同程度或不同类型的处理，比如，对于危险程度较低的恶意应用，可以采取迁移或隔离等方式处理，对于高危险的恶意应用，可以禁止该恶意应用的用户账户等等。可以理解的是，在这种情形下，为了判断恶意应用攻击行为的类型或者危险程度，安全分析器 202 需要将恶意应用的应用行为数据和初始信息一并上报给安全处理器 203，以便安全处理器 203 根据该恶意应用的行为数据来判断该恶意应用的攻击行为的类型或危险程度；当然，安全分析器 202 也可以自己根据应用的行为数据来判断应用攻击行为的类型或者危险程度，然后将分析结果反馈给安全处理器 203，本发明实施例不做特别限定。比如，安全分析器 202 可以根据云应用的行为数据以及安全判断规则，区分出恶意应用和正常应用，然后安全分析器 202 或安全处理器可以进一步查询预先配置的应用特征库，以确定恶意应用的攻击行为的类型，例如为拒绝服务攻击，木马攻击或蠕虫攻击等等。又比如，在安全分析器 202 根据云应用的行为数据以及安全判断规则，确定出存在攻击行为的恶意应用之后，安全分析器 202 或安全处理器 203 可以根据云应用的行为数据，查询预先配置的应用特征库，以确定出应用攻击行为的类型，然后进一步根据应用攻击行为的类型，确定应用攻击行为的危险程度。其中，应用特征库用于描述应用的行为特征与应用的攻击行为类型的映射关系；可选地，应用特征库可以是云计算系统中的一个独立的数据集，在安全分析器 202 根据云应用的行为数据以及安全判断规则，确定出存在攻击行为的恶意应用之后，可以进一步查询该应用特征库以确定该恶意应用的攻击行为的类型；当然，应用特征库也可以是安全判断规则的子集，当安全分析器 202 根据安全判断规则判断出某一云应用为恶意应用之后，可以进一步根据安全判断规则中包含的应用特征库，确定恶意应用的攻击行为类型。可以理解的是，不同类型的攻击行为的危险程度是不同的，需要根据该攻击行为对系统的危害程度来确定，对云计算系统造成的危害越大的攻击行为，其危险程度也越高。通常可以配置一个映射表，用于表征应用攻击行为的类型与其危险程度的对应关系，这样根据根据应用攻击行为的类型，通过查表的方式就可以确定应用的攻击行为的危险程度。可选地，在另一个可选的实施例中，安全处理器 203 也可以根据云计算系统的安全级别来对恶意应用进行处理，不同的安全级别对应不同的处理方式。比如云计算系统的安全级别可以设置为

“高”、“中”、“低”三个级别，当云计算系统的安全级别为“高”时，安全处理器 203 可以关闭恶意应用，同时禁止该恶意应用的用户账户；当云计算系统的安全级别为“低”时，安全处理器 203 可以将恶意应用迁移到特定的云主机进行隔离。最后需要说明的是，安全处理器 203 对恶意应用的三种处理模式，即上述的统一处理方式，根据攻击行为类型或危险程度处理的方式，以及根据云计算系统安全级别的处理方式，可以通过恶意应用处理规则来指示，不同的处理模式对应有不同的恶意应用处理规则，且该恶意应用处理规则可以由管理员通过策略管理器 201 的配置接口来配置。例如，恶意应用处理规则可以用于指示对不同类型恶意应用的处理方式，或者对不同危险程度的恶意应用的处理方式，或者云计算系统的不同安全级别下对恶意应用的处理方式；这样，安全处理器 203 具体可以根据应用的攻击行为的类型，以及恶意应用处理规则所指示的对该类型应用的处理方式，对恶意应用进行相应处理；或者安全处理器 203 具体可以根据应用的攻击行为的危险程度，以及恶意应用处理规则所指示的对该危险程度的应用的处理方式，对恶意应用相应进行处理；或者安全处理器 203 具体可以根据云计算系统当前的安全级别，以及恶意应用处理规则所指示的该安全级别下对恶意应用的处理方式，对恶意应用进行相应处理。

本发明实施例提供的云应用攻击行为处理装置，策略管理器下发行为检测规则给分布于各个云主机的安全检测器，安全检测器根据行为检测规则检测并上报云应用的行为数据，安全分析器通过分析云应用的行为数据，确定出存在攻击行为的云应用，并调用云控制器进行相应处理，相比于现有技术中的安全方案，本发明实施例基于云计算应用级别进行安全防护，能满足云计算系统应用部署场景，防止同一个主机内部不同云应用之间的相互攻击，或者主机内部对主机本身进行的攻击，同时减少对正常云应用的影响。进一步地，恶意应用处理策略可配置，进而可根据不同安全级别或不同的攻击类型对恶意应用进行区别处理。

优选地，云应用攻击行为处理装置 20 还可以包括：信息通知器 204；策略管理器 201 中还存储有信息通知规则；

安全处理器 203 还用于，根据存在攻击行为的云应用的初始信息查询该云应用所属的用户信息，将查询到的用户信息和该云应用的行为数据发送给信息

通知器 204；其中，云应用的用户信息包括但不限于：用户名、用户邮箱或用户身份证号。

信息通知器 204 用于，将接收到的应用行为数据和云应用所属的用户信息备份，并按照策略管理器中存储的信息通知规则进行攻击信息通知处理。其中，将应用行为数据和云应用所属的用户信息备份，具体可以是以表格、日志或文档等数据格式存储在可靠存储介质中，以便管理员查看。

具体地，在一个实施例中，信息通知器 204 进行攻击信息通知处理包括但不限于下列操作中的一项或多项：产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、以及将存在攻击行为的云应用所属的用户信息通知网警中心。

优选地，在另一个实施例中，当安全分析器接收到安全检测器上报的应用行为数据后，根据安全判断规则确定云应用不存在攻击行为时，可以丢弃改应用行为数据。

优选地，在另一个实施例中，策略管理器 201 包括有配置接口，管理员可以通过该配置接口配置安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项。其中，该配置接口可以为图形用户界面（GUI）、网页形式的配置界面或者应用程序接口（API）中的一种或多种。进一步地，在配置恶意应用处理规则的时候，可以根据恶意应用的攻击类型或者危险程度，配置不同的处理规则，以进行区别处理，从而实现安全防护的灵活性和可扩展性。当然，可以理解的是，这三种规则中的一种和多种也可以不需要管理员配置，由云计算系统按照默认规则自定义。

进一步地，为了实现更细粒度的安全防护，策略管理器下发给安全检测器的行为检测规则可以包括：进程检测规则或线程检测规则。这样，安全检测器可以对云应用进行进程或线程级别的检测，安全分析器可以基于安全检测器的检测结果，确定出存在攻击行为的进程或线程，然后安全处理器可以对存在攻击行为的进程或线程进行处理，进而可以实现进程或线程界别的安全防护。

下面结合具体的实例，进一步详细阐述本发明实施例提供的云应用攻击行为处理装置，如图 4 所示，该云应用攻击行为处理装置为一云主机 30。云主

机 30 的主要工作流程如下:

1.通过策略管理器 201 的配置接口配置用于判断应用攻击行为的安全判断规则，其中配置动作可以由管理员或由运行于云计算系统的配置程序完成。在一个具体的例子中，该安全判断规则为: require different tcp port > 100，即请求的 TCP 端口数目超过 100 个，该判断规则表示当云应用向外请求的 TCP 端口数量超过 100，则判定该云应用有端口嗅探的行为;

2. 策略管理器 201 将安全判断规则转换为行为检测规则: 检测云应用请求 TCP 端口的个数，并将行为检测规则下发给部署于云主机 10 上的安全检测器 205;

3. 安全检测器 205 检测 App A 和 App B 的行为，例如，统计 App A 和 App B 请求 TCP 端口的数目，并生成应用行为数据上报给安全分析器 202;

4. 安全分析器 202 根据收集到的应用行为数据与安全判断规则，判断发现 App B 请求的 TCP 端口数超出了 100，因此判断 App B 有攻击行为;

5. 安全分析器 202 将 App B 的初始信息，比如进程 ID，或进程名称，发送给安全处理器 203;

6. 安全处理器 203 根据 App B 的初始信息从云计算系统应用库查询 App B 的用户信息;

7. 安全处理器 203 调用云控制器关闭 App B，或将 App B 迁移到隔离的云主机，或者禁止 App B 的用户账户;

8. 安全分析器将 App B 的用户信息通知信息通知器 204，信息通知器 204 上报网警中心备案。

该示例中，云应用攻击行为处理装置成功的检测并处理了 App B 的端口嗅探行为，并且没有对 App A 造成严重影响。进一步地，安全分析器在发现 App B 有攻击行为之后，可以进一步根据 App B 的攻击行为的类型或者危险程度，对 App 采用不同的处理方式。其中，对恶意应用的处理方式可以由恶意应用处理规则来指示，且该恶意应用处理规则可以由管理员通过策略管理器 201 的配置接口来配置。其中，该配置接口可以为 WEB 界面或者 API 等等。

下面对云应用攻击行为处理装置 20 中的各个模块进行详细介绍:

（1）策略管理器 201: 策略管理器向管理员或自动配置程序提供配置接口，同时主要负责规则存储，规则转化，规则下发等操作。如图 5 所示，策略管理器 201 包括有: 配置接口 2011，规则转化单元 2012、规则下发单元 2013 和规则存储单元 2014; 其中配置接口 2011 包括但不限于: 图形用户界面（GUI）、网页形式的配置界面或者应用程序接口（API）中的一种或多种。通过配置接口 2011 可配置的规则包括: 安全判断规则、恶意应用处理规则、信息通知规则。规则存储单元 2014 将管理员通过配置接口 2011 配置的各种规则存储到对应的规则库中; 规则转化单元 2012 可以将管理员配置的安全判断规则转化为行为检测规则，规则下发单元 2013 负责将行为检测规则下发至云主机上的安全检测器。

（2）安全分析器 202: 如图 6 所示，安全分析器主要负责接收安全检测器发送来的应用行为数据，然后根据策略管理器中存储的安全判断规则，判断云应用是否存在攻击行为。如果判断存在攻击行为，则将该云应用的初始信息（包括进程 ID、进程名称等）发送给安全处理器。如果判断不存在攻击行为，则可以丢弃该应用行为数据。

（3）安全处理器 203: 安全处理器负责用恶意应用的处理。具体地，如图 7 所示，安全处理器 203 主要包括: 应用信息接收单元 2031，用户信息查询单元 2032，应用处理单元 2033，以及信息上报单元 2034。应用信息接收单元 2031 接收安全分析器上报的恶意应用的初始信息，用户信息查询单元 2032 从云计算系统应用信息库中查询云应用所属的用户信息，包括但不限于用户名、用户邮箱、用户身份证等信息。然后用户信息查询单元 2032 将用户信息和恶意应用的行为信息通过信息上报单元 2034 上报给信息通知器，使得信息通知器按照策略管理器中存储的信息通知规则进行攻击信息通知处理。应用处理单元 2033 依据策略管理器中存储的恶意应用处理规则，调用云控制器提供的接口对恶意应用进行处理。处理方式包括但不限于: 关闭应用、将应用迁移到隔离的云主机、禁止用户账户等。

（4）信息通知器 204: 如图 8 所示，信息通知器包括: 应用信息接收单元 2041，信息通知策略判断单元 2042; 其中，应用信息接收单元 2041 负责接

收应用行为信息和云应用所属的用户信息；然后信息通知策略判断单元 2042 根据策略管理器中存储的信息通知规则进行攻击信息通知处理。具体地，信息通知策略判断单元 2042 可以调用或触发告警产生单元 2043 产生告警信息，比如生成告警界面；可选地，信息通知策略判断单元 2042 可以调用或触发信息呈现单元 2044 在 WEB 页面以表格形式呈现恶意应用的信息；可选地，信息通知策略判断单元 2042 也可以调用或触发信息通知单元将恶意应用的信息上报网警中心。可以理解的是，信息通知器可以包括告警产生单元 2043，信息呈现单元 2044 和信息通知单元 2045 中的某一个，也可以同时包含三者中的任意两个，也可以同时包含三者，需要视具体的应用场景需求来确定，本发明实施例不做特别限定。

本发明实施例提供的云应用攻击行为处理装置能够能满足云计算系统应用部署场景，基于云计算应用级别进行安全防护，防止同一个主机内部不同云应用之间的相互攻击，或者主机内部对主机本身进行的攻击，同时减少对正常云应用的影响。进一步地，恶意应用处理策略可配置，进而可根据不同安全级别或不同的攻击类型对恶意应用进行区别处理。

需要说明的是，本发明实施例提供的云应用攻击行为处理装置，具体可以为云计算系统中的一台云主机，该云主机可以为运行在物理机上的虚拟机。如图 12 所示，物理机 1200 包括硬件层 100，运行在硬件层 100 之上的 VMM（Virtual Machine Monitor，虚拟机监视器）110，以及运行在 VMM 110 之上的宿主机 Host 1201 和若干虚拟机（VM，Virtual Machine），其中，硬件层包括但不限于：I/O 设备、CPU 和 memory。本发明实施例提供的云应用攻击行为处理装置具体可以为物理机 1200 中的一台虚拟机，比如 VM 1202，VM 1202 上运行有一个或多个云应用，其中，每一个云应用都用于实现相应的业务功能，比如数据库应用、地图应用等等，这些云应用可以由开发者开发然后部署到云计算系统中。此外 VM1202 还运行有可以执行程序，VM 1202 通过运行该可执行程序，并在程序运行的过程中通过宿主机 Host 1201 来调用硬件层 100 的硬件资源，以实现云应用攻击行为处理装置的策略管理器、安全分析器、安全处理器以及信息通知器的功能，具体而言，策略管理器、安全分析器、安全处理器以及信息通知器可以以软件模块或函数的形式被包含在上述可执行程序

中，比如该可执行程序可以包括：策略管理器模块、安全分析器模块、安全处理器模块以及信息通知器模块，VM1202 通过调用硬件层 100 中的 CPU、Memory 等资源，以运行该可执行程序，从而实现策略管理器、安全分析器、安全处理器以及信息通知器的功能。在另一种可能的场景下，本发明实施例提供的云应用攻击行为处理装置，也可以为云计算系统中的一台物理机，如图 13 所示，物理机 1300 包括：至少 1 个处理器 1301，例如 CPU，至少 1 个网络接口 1304，存储器 1305，至少一个通信总线 1302。通信总线 1302 用于实现这些组件之间的连接通信。物理机 1300 可选的包含输入/输出设备 1303，包括显示器，键盘或者点击设备（例如，鼠标，轨迹球（trackball），触感板或者触感显示屏）。存储器 1305 可能包含高速 RAM 存储器，也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。存储器 1305 可选的可以包含至少一个位于远离前述处理器 1301 的存储装置。存储器 1305 存储了如下的元素，可执行模块或者数据结构，或者他们的子集，或者他们的扩展集：

操作系统 13051，包含各种系统程序，用于实现各种基础业务以及处理基于硬件的任务；

应用程序模块 13052，包含各种云应用，用于实现各种应用业务，比如数据库应用、地图应用等等。

应用程序模块 13052 中包括但不限于实现云应用攻击行为处理装置的策略管理器、安全分析器、安全处理器以及信息通知器的功能的模块。

应用程序模块 13052 中各模块的具体实现可参见本发明装置及方法实施例，在此不赘述。

相应地，本发明实施例提供的安全检测器，可以为云计算系统中的云主机上的一个功能模块，例如，若云主机为虚拟机时，安全检测器可以为独立运行在该虚拟机上的一个应用程序，该应用程序在被该虚拟机执行的过程中，可以检测该虚拟机上运行的其它云应用的行为。若云主机为物理机时，安全检测器可以为存储于该物理机的存储器中的一个应用程序，该物理机的 CPU 通过读取并执行该应用程序，可以实现对该物理机上运行的其它云应用的行为检测的功能。

基于上述装置实施例，本发明实施例还提供一种应用于云计算系统中的云应用攻击行为处理方法，其中，该云计算系统包含有多台云主机，云主机可以为物理机，也可以为虚拟机；云计算系统的多台云主机中至少有一台为云控制器，云控制器与云计算系统中的各个云主机通信连接或集成于某一云主机上，用于控制云计算系统中的多个云主机上运行的云应用；每一台云主机上运行有一个或多个云应用，且每一台云主机上部署有一安全检测器；安全检测器负责依据行为检测规则，对云主机上运行的云应用的行为进行检测。本发明实施例提供的云应用攻击行为处理方法可以由云计算系统中的一台云主机来执行，也可以由云控制器来执行，如图 9 所示，该方法包括：

S901：接收云计算系统中的多个云主机中的至少一个云主机上报的应用行为数据；该应用行为数据是该云主机上部署的安全检测器根据行为检测规则对该云主机上运行的云应用进行检测后得到的，且该应用行为数据用于表示该云主机上运行的云应用的运行状态；

S902：根据应用行为数据以及安全判断规则，判断该云主机上运行的云应用是否存在攻击行为；

S903：如果判断云主机上运行的云应用存在攻击行为，则根据恶意应用处理规则，调用云计算系统的云控制器提供的接口对存在攻击行为的云应用进行处理。

优选地，调用云控制器提供的接口对将存在攻击行为的云应用进行相应处理，包括：调用云控制器：关闭所述云应用、将所述云应用迁移到隔离的云主机、或者禁止所述云应用的用户账户。

优选地，在步骤 S903 中，如果判断云主机上运行的云应用存在攻击行为，还可以根据该存在攻击行为的云应用的初始信息查询该云应用所属的用户信息，然后将该存在攻击行为的云应用的应用行为数据和查询到的用户信息备份，并按照信息通知规则进行攻击信息通知处理；其中，云应用的初始信息用于唯一标识该云应用，初始信息可以为进程 ID 或进程名称，或者两者同时包含；云应用的用户信息包括但不限于：用户名、用户邮箱或用户身份证号。需要说明的是，将应用行为数据和云应用所属的用户信息备份，具体可以是以表格、日志或文档等数据格式存储在可靠存储介质中，以便管理员查看。

进一步地，进行攻击信息通知处理包括但不限于以下操作之一或其任意组合：产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、或者将存在攻击行为的云应用所属的用户信息通知网警中心。

可选地，在步骤 S903 中，如果判断云主机上运行的云应用不存在攻击行为，则丢弃接收到的该云应用的应用行为数据。

需要说明的是，安全判断规则用于定义云应用的何种行为为攻击行为，恶意应用处理规则用于定义对于存在攻击行为的云应用采取何种处理方式，行为检测规则用于定义对云应用的何种行为进行检测，即行为检测规则指示了对云应用进行检测的检测指标。通常行为检测规则和安全判断规则是密切联系的，可以互相转化，因此在一个优选的实施例中，可以将安全判断规则转化为行为检测规则，然后下发给安全检测器。举例来说，如果安全判断规则为：云应用向外请求的 TCP 端口数量超过 100 则判断云应用有端口嗅探的行为；那么相应的行为检测规则就为：采集云应用请求不同 TCP 端口的个数。这样，云主机上的安全检测器就应该检测云应用请求不同TCP端口的个数并将检测结果。

可选地，在步骤 S903 中，可以对所有存在攻击行为的云应用（恶意应用）采用统一处理方式，比如关闭恶意应用，或者将恶意应用迁移到隔离的云主机，或者禁止恶意应用的用户账户。可选地，也可以根据恶意应用攻击行为的类型或者攻击行为的危险程度，对恶意应用进行不同程度或不同类型的处理，比如，对于危险程度较低的恶意应用，可以采取迁移或隔离等方式处理，对于高危险的恶意应用，可以禁止该应用的用户账户等等。可以理解的是，在这种情形下，为了判断恶意应用攻击行为的类型或者危险程度，需要根据恶意应用的行为数据来判断该恶意应用的攻击行为的类型或危险程度。比如，可以根据云应用的行为数据以及安全判断规则，区分出恶意应用和正常应用，然后可以进一步查询预先配置的应用特征库，以确定恶意应用的攻击行为的类型，例如为拒绝服务攻击，木马攻击或蠕虫攻击等等。又比如，在根据云应用的行为数据以及安全判断规则，确定出存在攻击行为的恶意应用之后，可以根据云应用的行为数据，查询预先配置的应用特征库，以确定出应用攻击行为的类型，然后进一步根据应用攻击行为的类型，确定应用攻击行为的危险程度。其中，应用特征库用于描述应用的行为特征与应用的攻击行为类型的映射关系；可选地，应用特

征库可以是云计算系统中的一个独立的数据集，在根据云应用的行为数据以及安全判断规则，确定出存在攻击行为的恶意应用之后，可以进一步查询该应用特征库以确定该恶意应用的攻击行为的类型；当然，应用特征库也可以是安全判断规则的子集，当根据安全判断规则判断出某一云应用为恶意应用之后，可以进一步根据安全判断规则中包含的应用特征库，确定恶意应用的攻击行为类型。可以理解的是，不同类型的攻击行为的危险程度是不同的，需要根据该攻击行为对系统的危害程度来确定，对云计算系统造成的危害越大的攻击行为，其危险程度也越高。通常可以配置一个映射表，用于表征应用攻击行为的类型与其危险程度的对应关系，这样根据根据应用攻击行为的类型，通过查表的方式就可以确定应用的攻击行为的危险程度。。可选地，也可以根据云计算系统的安全级别来对恶意应用进行处理，不同的安全级别对应不同的处理方式。比如云计算系统的安全级别可以设置为“高”、“中”、“低”三个级别，当云计算系统的安全级别为“高”时，关闭恶意应用，同时禁止该恶意应用的用户账户；当云计算系统的安全级别为“低”时，将恶意应用迁移到特定的云主机进行隔离。最后需要说明的是，对恶意应用的三种处理模式，即上述的统一处理方式，根据攻击行为类型或危险程度处理的方式，以及根据云计算系统安全级别的处理方式，可以通过恶意应用处理规则来指示，不同的处理模式对应有不同的恶意应用处理规则。

优选地，在另一个实施例中，管理员可以通过配置接口配置安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项。其中，该配置接口可以为WEB 界面或者 API 等等。进一步地，在配置恶意应用处理规则的时候，可以根据恶意应用的攻击类型或者危险程度，配置不同的处理规则，以进行区别处理，从而实现安全防护的灵活性和可扩展性。当然，可以理解的是，这三种规则中的一种和多种也可以不需要管理员配置，由云计算系统按照默认规则自定义。

可选地，为了实现更细粒度的安全防护，行为检测规则可以包括：进程检测规则或线程检测规则。这样，可以对应用进行进程或线程级别的检测，然后基于检测结果确定出存在攻击行为的进程或线程，对存在攻击行为的进程或线程进行处理，进而可以实现进程或线程界别的安全防护。

本发明实施例提供的云应用攻击行为处理方法能够能满足云计算系统应用部署场景，基于云计算应用级别进行安全防护，防止同一个主机内部不同应用之间的相互攻击，或者主机内部对主机本身进行的攻击，同时减少对正常应用的影响。进一步地，恶意应用处理策略可配置，进而可根据不同安全级别或不同的攻击类型对恶意应用进行区别处理。

下面结合具体的实例，进一步详细阐述本发明实施例的云应用攻击行为处理方法，如图 10 所示，该云应用攻击行为处理方法包含主要工作流程如下：

1. 通过配置接口配置用于判断应用攻击行为的安全判断规则，并存储至策略库；然后将安全判断规则转化为行为检测规则下发至云主机的安全检测器；

2. 安全检测器根据行为检测规则检测云应用行为并生产应用行为数据上报；

3. 根据收集到的应用行为数据与安全判断规则，确定存在攻击行为的恶意应用；

4. 根据恶意应用的初始信息从云计算系统应用库查询恶意应用的用户信息；

5 安调用云控制器关闭恶意应用，或将恶意应用迁移到隔离的云主机，或者禁止恶意应用的用户账户；

6. 将恶意应用的用户信息通知或呈现给管理员或网警中心。

该示例中，云应用攻击行为处理装置成功的检测并处理了恶意应用，并且没有对正常应用造成严重影响。进一步地，在发现应用有攻击行为之后，可以进一步根据恶意应用的攻击行为的类型或者危险程度，对恶意应用采用不同的处理方式。其中，对恶意应用的处理方式可以由恶意应用处理规则来指示，且该恶意应用处理规则可以由管理员通过配置接口来配置。其中，该配置接口可以为图形用户界面（GUI）、网页形式的配置界面或者应用程序接口（API）等等。

本发明实施例提供的云应用攻击行为处理方法能够能满足云计算系统应用部署场景，基于云计算应用级别进行安全防护，防止同一个主机内部不同应

用之间的相互攻击，或者主机内部对主机本身进行的攻击，同时减少对正常应用的影响。进一步地，恶意应用处理策略可配置，进而可根据不同安全级别或不同的攻击类型对恶意应用进行区别处理。

如图 11 所示，本发明实施例还提供了一种云应用安全防护系统，应用于云计算系统中，用于实现上述云应用攻击行为处理方法，该云应用安全防护系统包括：云应用攻击行为处理装置 20、云控制器 206，以及多个安全检测器（以图 11 中的 205 为示例）；其中，多个安全检测器分别部署于多个云主机（如图 11 中的 10、11、12 和 13）上，且每一云主机对应于一个安全检测器；云控制器 206 与多个云主机通信连接，或者集成于上述多个云主机中的一个云主机，用于管理和控制该多个云主机，每一云主机上运行有一个或多个云应用；云应用攻击行为处理装置 20 中存储有安全判断规则和恶意应用处理规则；

安全检测器 205 用于，根据行为检测规则对一个或多个云应用进行检测，以得到应用行为数据，并将应用行为数据上报给云应用攻击行为处理装置 20；其中，该一个或多个云应用运行于安全检测器 205 对应的云主机 10 上；

云应用攻击行为处理装置 20 用于，接收多个云主机的至少一个云主机上的安全检测器 205 上报的应用行为数据，根据该应用行为数据以及安全判断规则，判断云主机 10 上运行的云应用是否存在攻击行为；如果判断存在攻击行为，则根据恶意应用处理规则，调用云控制器 206 对将存在攻击行为的云应用进行处理。

可选地，上述行为检测规则可以是由云应用攻击行为处理装置将安全判断规则转化后得到并下发给安全检测器的。

可选地，如果云应用攻击行为处理装置 20 判断云主机上运行的云应用存在攻击行为，还可以根据该存在攻击行为的云应用的初始信息查询该云应用所属的用户信息，然后将该存在攻击行为的云应用的应用行为数据和查询到的用户信息备份，并按照信息通知规则进行攻击信息通知处理；其中，云应用的初始信息用于唯一标识该云应用，初始信息可以为进程 ID 或进程，或者两者同时包含；云应用的用户信息包括但不限于：用户名、用户邮箱或用户身份证号。

需要说明的是，将应用行为数据和云应用所属的用户信息备份，具体可以

是以表格、日志或文档等数据格式存储在可靠存储介质中，以便管理员查看。

进一步地，进行攻击信息通知处理包括但不限于：产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、或者将存在攻击行为的云应用所属的用户信息通知网警中心。

可选地，云应用攻击行为处理装置 20 与所述云控制器 206 通信连接，或者云应用攻击行为处理装置 20 集成于云控制器 206 上。

优选地，在另一个实施例中，云应用攻击行为处理装置 20 包括有配置接口，管理员或配置程序可以通过该配置接口配置安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项。其中，该配置接口可以为图形用户界面（GUI）、网页形式的配置界面或者应用程序接口（API）等等。进一步地，在配置恶意应用处理规则的时候，可以根据恶意应用的攻击类型或者危险程度，配置不同的处理规则，以进行区别处理，从而实现安全防护的灵活性和可扩展性。当然，可以理解的是，这三种规则中的一种和多种也可以不需要管理员配置，由云计算系统按照默认规则自定义。

进一步地，为了实现更细粒度的安全防护，云应用攻击行为处理装置 20 下发给安全检测器的行为检测规则可以包括：进程检测规则或线程检测规则。这样，安全检测器可以对云应用进行进程或线程级别的检测，云应用攻击行为处理装置 20 可以基于安全检测器的检测结果，确定出存在攻击行为的进程或线程，然后对存在攻击行为的进程或线程进行处理，进而可以实现进程或线程界别的安全防护。

需要说明的是，本发明实施例的云应用安全防护系统所包含的云应用攻击行为处理装置 20 可以为前述任一装置实施例中所描述的云应用攻击行为处理装置，其具体实现细节可以参照前述装置及方法实施例，此处不再赘述。

本发明实施例提供的云应用攻击行为检测系统能够能满足云计算系统应用部署场景，基于云计算应用级别进行安全防护，防止同一个主机内部不同应用之间的相互攻击，或者主机内部对主机本身进行的攻击，同时减少对正常应用的影响。进一步地，恶意应用处理策略可配置，进而可根据不同安全级别或不同的攻击类型对恶意应用进行区别处理。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件（例如处理器）来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：ROM、RAM、磁盘或光盘等。

以上对本发明实施例所提供的云应用攻击行为处理方法、装置及系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权 利 要 求

1、一种云计算系统中云应用攻击行为的处理装置，其特征在于，包括:

安全分析器，安全处理器和策略管理器，其中:

所述策略管理器用于存储安全判断规则和恶意应用处理规则;

所述安全分析器用于接收云计算系统中的多个云主机中的至少一个云主机上的安全检测器发送的应用行为数据，根据所述应用行为数据以及所述策略管理器中存储的安全判断规则，确定所述至少一个云主机上运行的云应用是否存在攻击行为，并在确定所述至少一个云主机上运行的云应用存在攻击行为时，将所述应用行为数据发送给所述安全处理器；其中，所述应用行为数据是所述安全检测器根据行为检测规则对所述云应用进行检测后得到的，且所述应用行为数据用于表示所述云应用的运行状态;

所述安全处理器，用于根据所述策略管理器中存储的恶意应用处理规则，调用所述云计算系统中的云控制器提供的接口对所述云应用进行处理，所述云控制器与所述至少一个云主机通信连接或集成于所述至少一个云主机，用于控制所述至少一个云主机上运行的云应用。

2、根据权利要求1所述的装置，其特征在于，还包括: 信息通知器；所述策略管理器中还存储有信息通知规则;

所述安全分析器还用于，当确定所述云应用存在攻击行为时，获取所述云应用的初始信息并发送给所述安全处理器，其中，所述初始信息用于标识所述云应用;

所述安全处理器还用于，根据所述云应用的初始信息查询所述云应用所属的用户信息，将所述用户信息和所述应用行为数据发送给所述信息通知器;

所述信息通知器用于，将接收到的应用行为数据和云应用所属的用户信息存储并按照所述策略管理器中存储的信息通知规则进行攻击信息通知处理。

3、根据权利要求1或2所述的装置，其特征在于，

所述策略管理器用于，将所述安全判断规则转化为所述行为检测规则，并将所述行为检测规则下发给所述至少一个云主机的安全检测器。

4、根据权利要求1至3任一项所述的装置，其特征在于，所述恶意应用处理规则用于指示对不同类型恶意应用的处理方式，或者对不同危险程度的恶意应用的处理方式，其中，所述恶意应用为存在攻击行为的云应用；所述安全处理器，具体用于根据所述云应用的攻击行为的类型，以及所述恶意应用处理规则所指示的对该类型应用的处理方式，对所述云应用进行相应处理；或者所述安全处理器，具体用于根据所述云应用的攻击行为的危险程度，以及所述恶意应用处理规则所指示的对该危险程度的应用的处理方式，对所述云应用进行相应处理。

5、根据权利要求2至4任一项所述的装置，其特征在于，所述攻击信息通知处理具体包括以下之一或其任意组合：产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、以及将存在攻击行为的云应用所属的用户信息通知网警中心。

6、根据权利要求1至5任一项所述的装置，其特征在于，所述云应用攻击行为处理装置集成于所述云控制器。

7、根据权利要求2至6任一项所述的装置，其特征在于，所述安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项是通过所述策略管理器的配置接口配置的，其中所述策略管理器的配置接口包括：配置界面和应用程序接口API中的至少一种。

8、根据权利要求1至6任一项所述的装置，其特征在于，所述行为检测规则包括：进程检测规则或线程检测规则；

所述应用行为数据是所述安全检测器根据所述行为检测规则对所述云应用的进程或线程进行检测后得到的。

9、根据权利要求8所述的装置，其特征在于，所述安全分析器还用于在确

定所述云应用不存在攻击行为时，丢弃所述应用行为数据。

10、一种云应用攻击行为处理方法，用于包括多个云主机的云计算系统，其特征在于，包括:

接收所述多个云主机中的至少一个云主机上报的应用行为数据，其中，所述应用行为数据是所述至少一个云主机上的安全检测器根据行为检测规则对所述至少一个云主机上运行的云应用进行检测后得到的，且所述应用行为数据用于表示所述至少一个云主机上运行的云应用的运行状态;

根据所述应用行为数据以及安全判断规则，判断所述至少一个云主机上运行的云应用是否存在攻击行为;

如果判断所述至少一个云主机上运行的云应用存在攻击行为，则根据恶意应用处理规则，调用所述云计算系统中的云控制器提供的接口对存在攻击行为的云应用进行处理，其中所述云控制器与所述至少一个云主机通信连接或集成于所述至少一个云主机，用于控制所述至少一个云主机上运行的云应用。

11、根据权利要求10所述的方法，其特征在于，还包括:

如果判断所述至少一个云主机上运行的云应用存在攻击行为，则根据所述存在攻击行为的云应用的初始信息查询所述云应用所属的用户信息，其中，所述初始信息用于标识所述云应用;

将所述存在攻击行为的云应用的应用行为数据和查询到的用户信息存储，并按照信息通知规则进行攻击信息通知处理。

12、根据权利要求10或11所述的方法，其特征在于，还包括:

如果判断所述至少一个云主机上运行的云应用不存在攻击行为，则丢弃接收到的所述应用行为数据。

13、根据权利要求10至12任一项所述的方法，其特征在于，所述恶意应用处理规则用于指示对不同类型恶意应用的处理方式，或者对不同危险程度的恶意应用的处理方式，其中，所述恶意应用为存在攻击行为的云应用;所述调用云控制器提供的接口对将存在攻击行为的云应用进行相应处理，包括:根据所述云应用的攻击行为的类型，以及所述恶意应用处理规则所指示的对该类型应

用的处理方式，对所述云应用进行相应处理；或者根据所述云应用的攻击行为的危险程度，以及所述恶意应用处理规则所指示的对该危险程度的应用的处理方式，对所述云应用进行相应处理。

14、根据权利要求11至13任一项所述的方法，其特征在于，所述按照信息通知规则进行攻击信息通知处理包括以下之一或其任意组合：

产生告警信息、显示存在攻击行为的云应用以及该云应用所属的用户信息、以及将存在攻击行为的云应用所属的用户信息通知网警中心。

15、根据权利要求10至14任一项所述的方法，其特征在于，还包括：将所述安全判断规则转化为所述行为检测规则，并将所述行为检测规则发送给所述安全检测器。

16、根据权利要求10至15任一项所述的方法，其特征在于，所述安全判断规则、恶意应用处理规则和信息通知规则中的一项或多项是通过配置接口配置的；其中所述配置接口包括：配置界面和应用程序接口API中的至少一种。

17、一种云应用安全防护系统，其特征在于，包括：云应用攻击行为处理装置、云控制器，以及多个安全检测器；其中，所述多个安全检测器分别部署于多个云主机上，且每一云主机对应于一个安全检测器；所述云控制器与所述多个云主机通信连接，用于管理和控制所述多个云主机，每一云主机上运行有一个或多个云应用；所述云应用攻击行为处理装置中存储有安全判断规则和恶意应用处理规则；

所述安全检测器用于，根据行为检测规则对一个或多个云应用进行检测，以得到应用行为数据，并将所述应用行为数据上报给所述云应用攻击行为处理装置；其中，所述一个或多个云应用运行于所述安全检测器对应的云主机上；

所述云应用攻击行为处理装置用于，接收所述多个云主机的至少一个云主机上的安全检测器上报的应用行为数据，根据所述应用行为数据以及所述安全判断规则，判断所述至少一个云主机上运行的云应用是否存在攻击行为；如果判断所述至少一个云主机上运行的云应用存在攻击行为，则根据所述恶意应用处理规则，调用云控制器提供的接口对存在攻击行为的云应用进行相应处理。

18、根据权利要求17所述的系统，其特征在于，所述云应用攻击行为处理

装置还用于，将所述安全判断规则转化为所述行为检测规则，并将所述行为检测规则下发给各个云主机的安全检测器。

19、根据权利要求17或18所述的系统，其特征在于，所述云应用攻击行为处理装置还用于，如果判断所述至少一个云主机上运行的云应用不存在攻击行为，则丢弃接收到的所述应用行为数据。

20、根据权利要求17或18所述的系统，其特征在于，所述云应用攻击行为处理装置还用于，如果判断所述至少一个云主机上运行的云应用存在攻击行为，则显示存在攻击行为的云应用以及该云应用所属的用户信息、或者将存在攻击行为的云应用所属的用户信息通知网警中心。

21、根据权利要求17至20任一项所述的系统，其特征在于，所述云应用攻击行为处理装置与所述云控制器通信连接，或者所述云应用攻击行为处理装置集成于所述云控制器上。

22、根据权利要求 17 至 21 任一项所述的系统，其特征在于，所述恶意应用处理规则用于指示对不同类型恶意应用的处理方式，或者对不同危险程度的恶意应用的处理方式，其中，所述恶意应用为存在攻击行为的云应用；所述云应用攻击行为处理装置具体用于：根据所述云应用的攻击行为的类型，以及所述恶意应用处理规则所指示的对该类型应用的处理方式，对所述云应用进行相应处理；或者根据所述云应用的攻击行为的危险程度，以及所述恶意应用处理规则所指示的对该危险程度的应用的处理方式，对所述云应用进行相应处理。

说 明 书 附 图

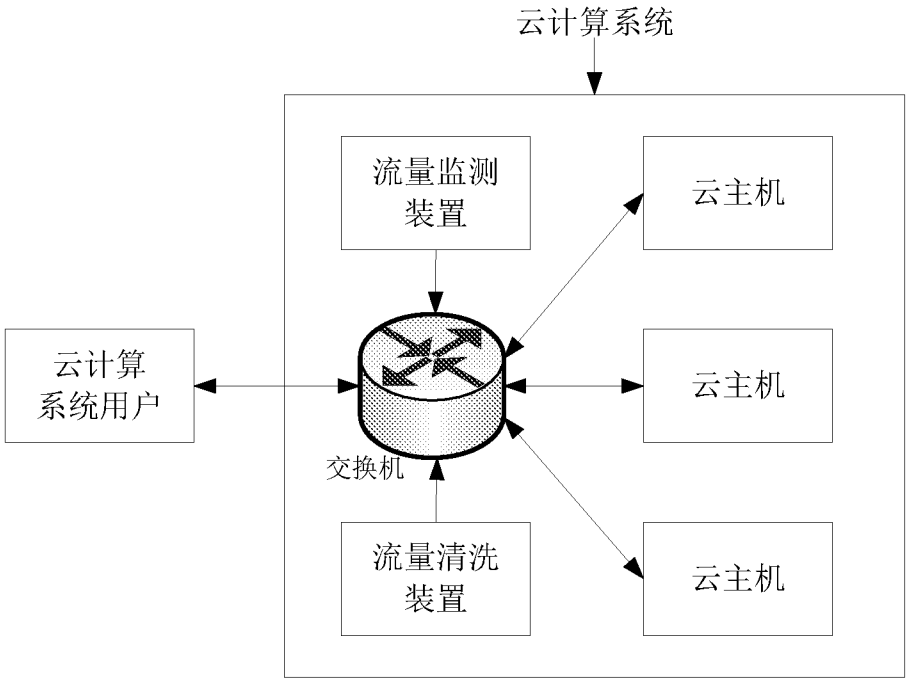

云计算系统
流量监测装置
云主机
云计算系统用户
云主机
交换机
流量清洗装置
云主机

图 1

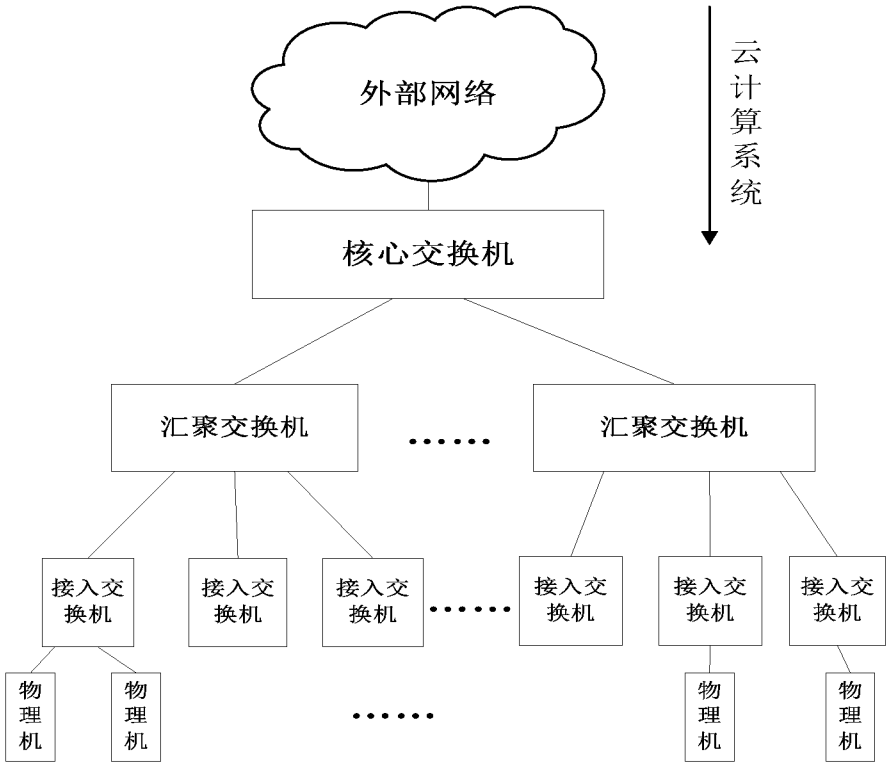

外部网络
云计算系统
核心交换机
汇聚交换机
汇聚交换机
接入交换机
接入交换机
接入交换机
接入交换机
接入交换机
接入交换机
物理机
物理机
物理机
物理机

图 2

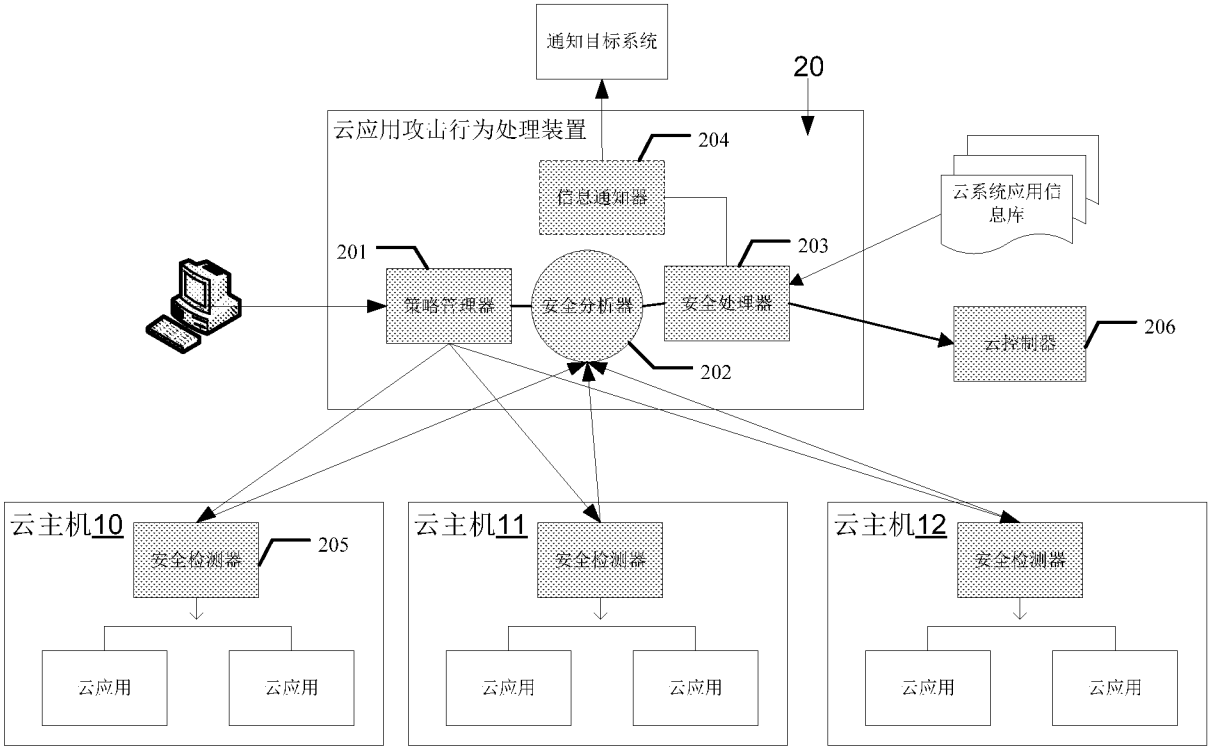

通知目标系统
20
云应用攻击行为处理装置
204
信息通知器
云系统应用信息库
201
203
策略管理器
安全分析器
安全处理器
云控制器
206
202
云主机10
安全检测器
205
云应用
云应用
云主机11
安全检测器
云应用
云应用
云主机12
安全检测器
云应用
云应用

图 3

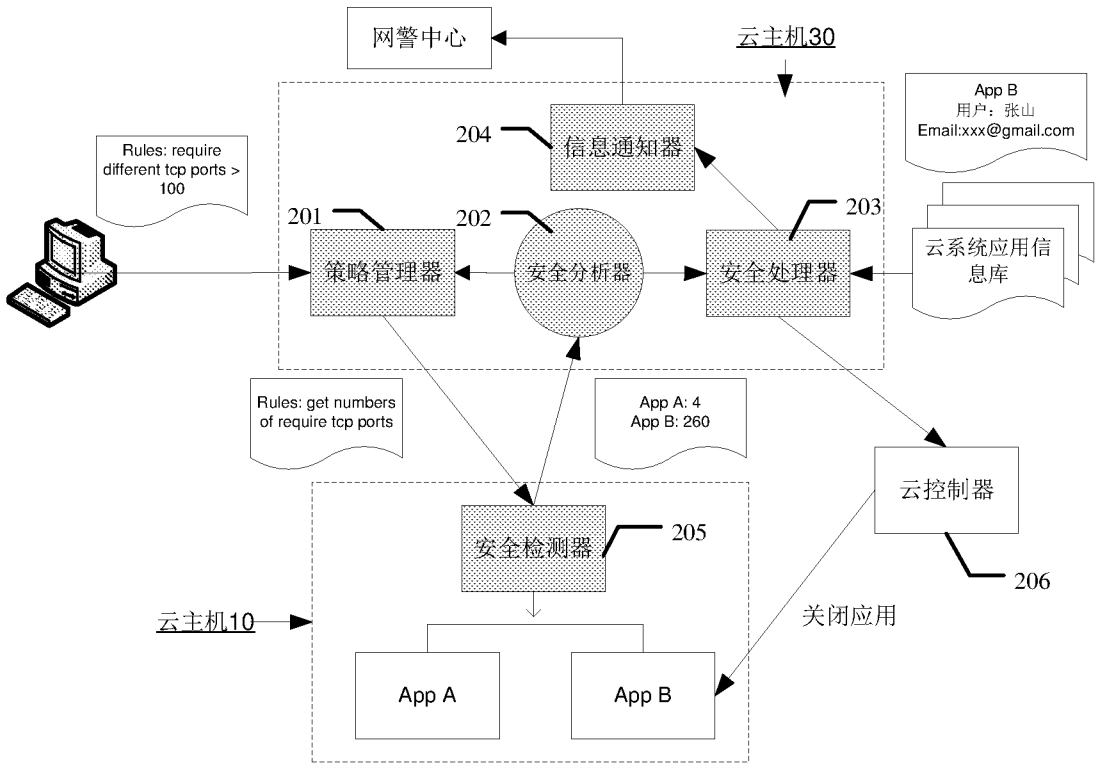

网警中心
云主机30
App B
用户：张山
Email:xxx@gmail.com
Rules: require different tcp ports > 100
204
信息通知器
201
202
203
策略管理器
安全分析器
安全处理器
云系统应用信息库
Rules: get numbers of require tcp ports
App A: 4
App B: 260
云控制器
安全检测器
205
206
云主机10
关闭应用
App A
App B

图 4

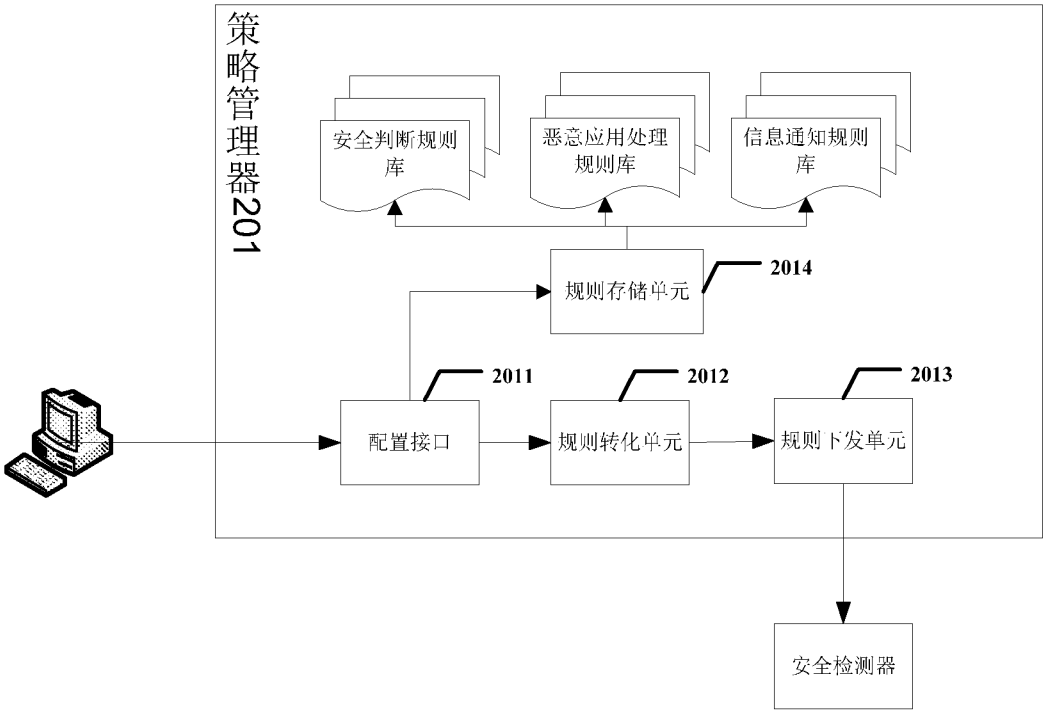

策略管理器201
安全判断规则库
恶意应用处理规则库
信息通知规则库
规则存储单元
2014
2011
2012
2013
配置接口
规则转化单元
规则下发单元
安全检测器

图 5

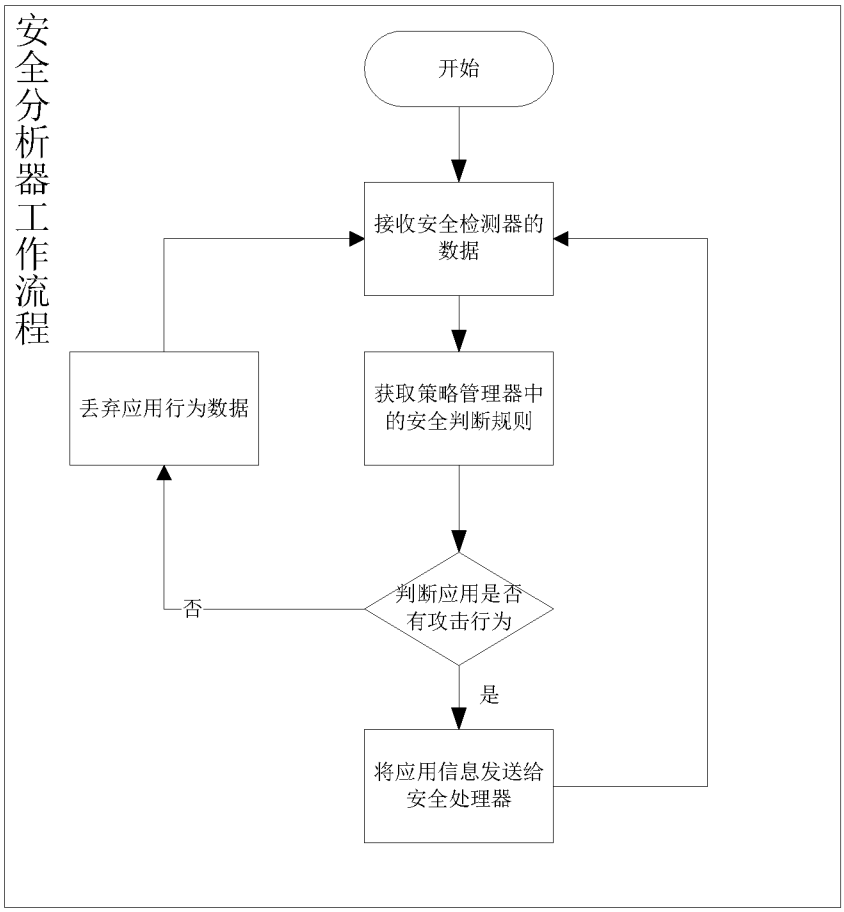

安全分析器工作流程
开始
接收安全检测器的数据
获取策略管理器中的安全判断规则
判断应用是否有攻击行为
否
是
丢弃应用行为数据
将应用信息发送给安全处理器

图 6

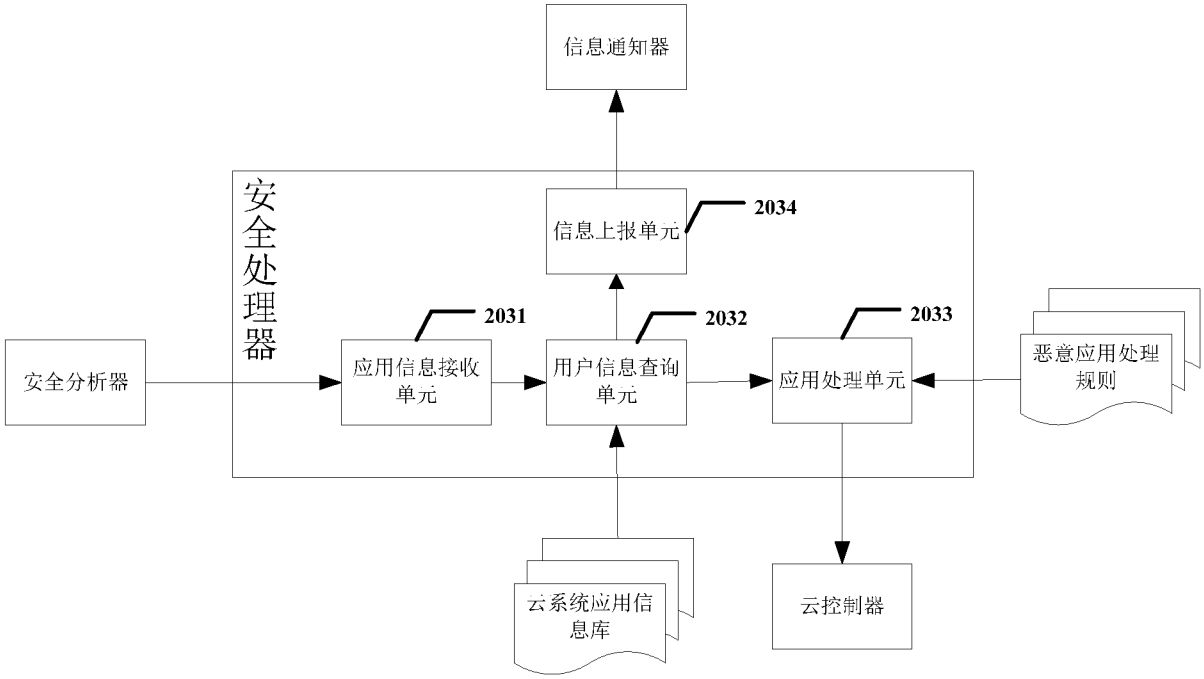

信息通知器
安全处理器
信息上报单元
2034
2031
2032
2033
安全分析器
应用信息接收单元
用户信息查询单元
应用处理单元
恶意应用处理规则
云系统应用信息库
云控制器

图 7

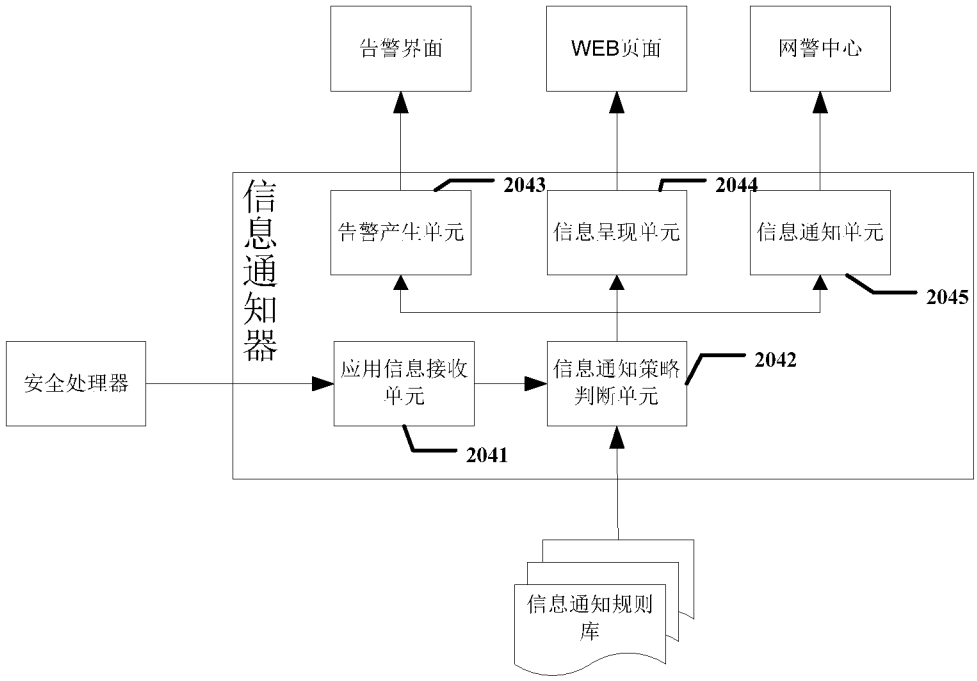

告警界面
WEB页面
网警中心
信息通知器
告警产生单元
信息呈现单元
信息通知单元
2043
2044
2045
安全处理器
应用信息接收单元
信息通知策略判断单元
2042
2041
信息通知规则库

图 8

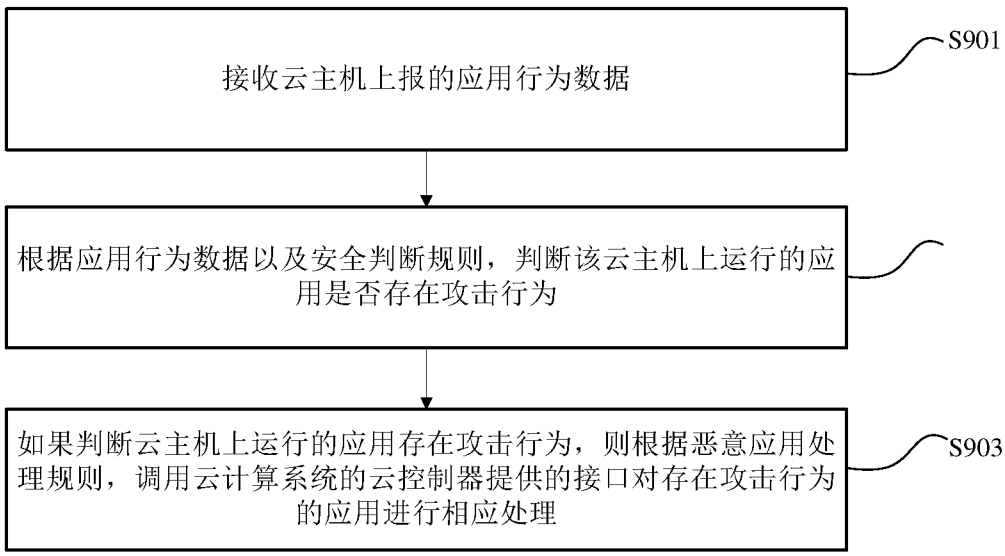

接收云主机上报的应用行为数据
S901
根据应用行为数据以及安全判断规则，判断该云主机上运行的应用是否存在攻击行为
如果判断云主机上运行的应用存在攻击行为，则根据恶意应用处理规则，调用云计算系统的云控制器提供的接口对存在攻击行为的应用进行相应处理
S903

图 9

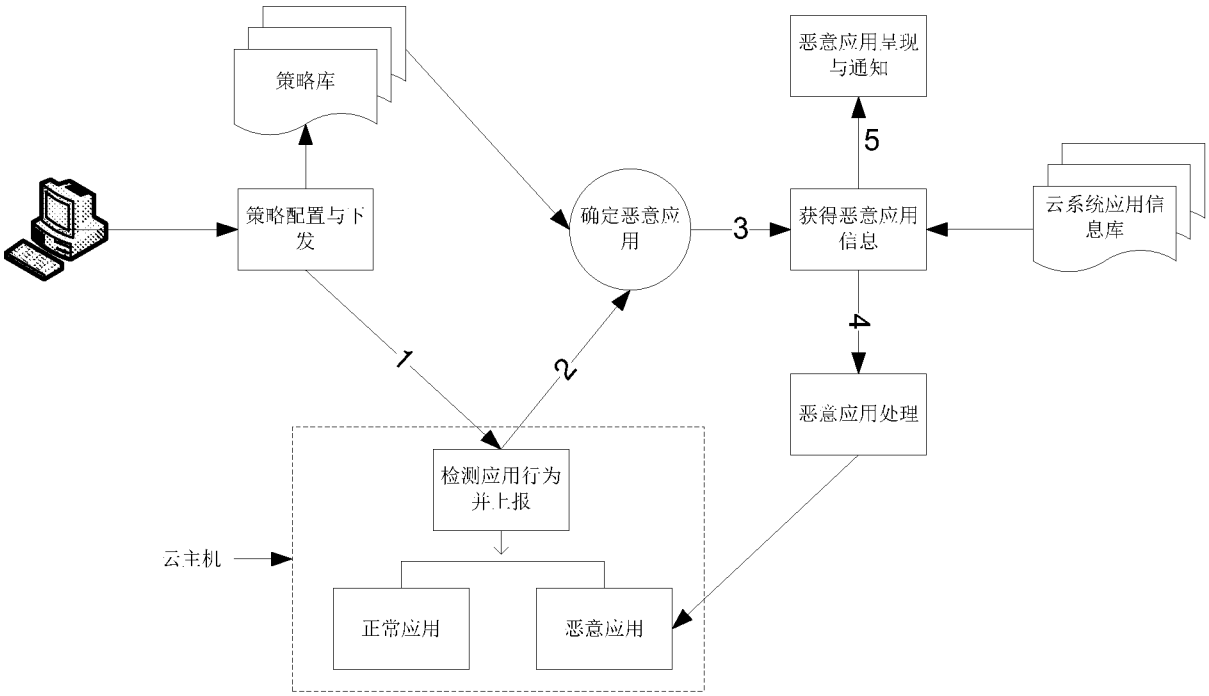

策略库
恶意应用呈现与通知
5
策略配置与下发
确定恶意应用
3
获得恶意应用信息
云系统应用信息库
1
2
4
恶意应用处理
检测应用行为并上报
云主机
正常应用
恶意应用

图 10

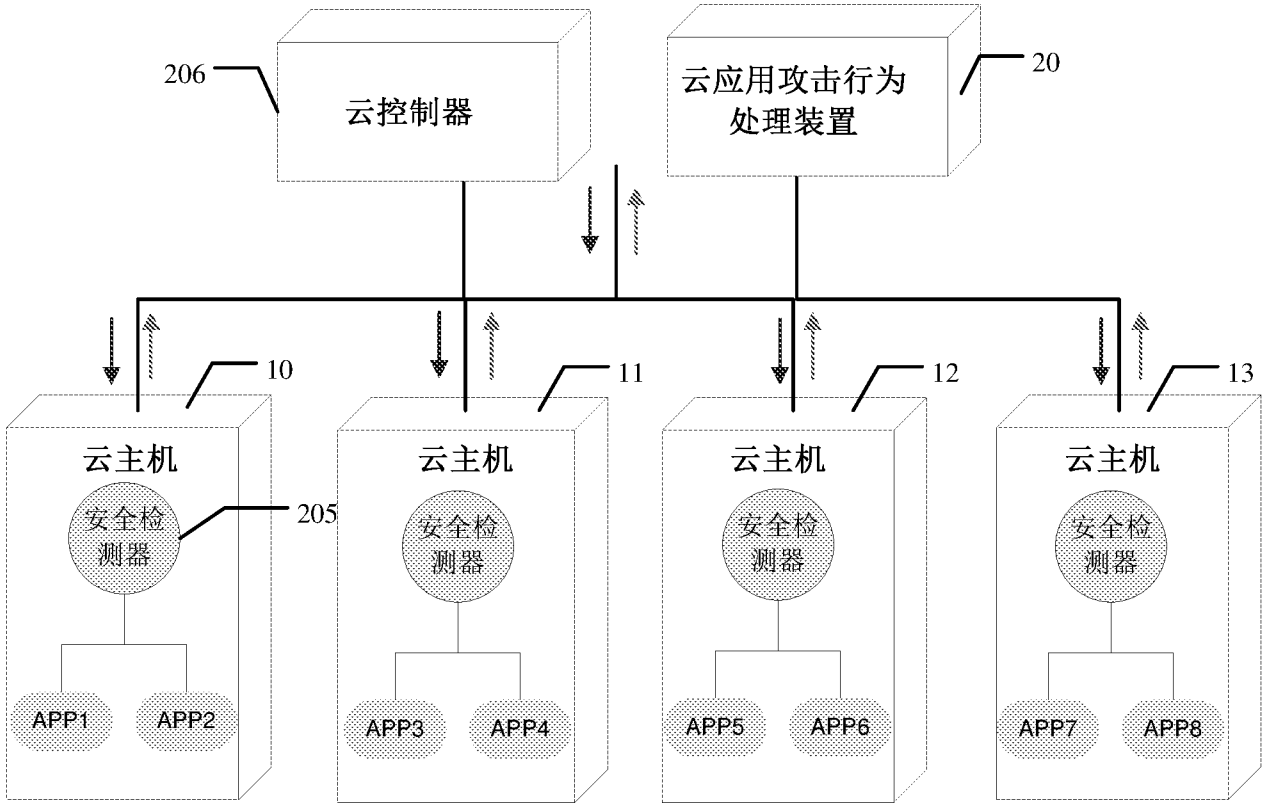

206
云控制器
云应用攻击行为处理装置
20
10
11
12
13
云主机
安全检测器
205
APP1
APP2
APP3
APP4
APP5
APP6
APP7
APP8

图 11

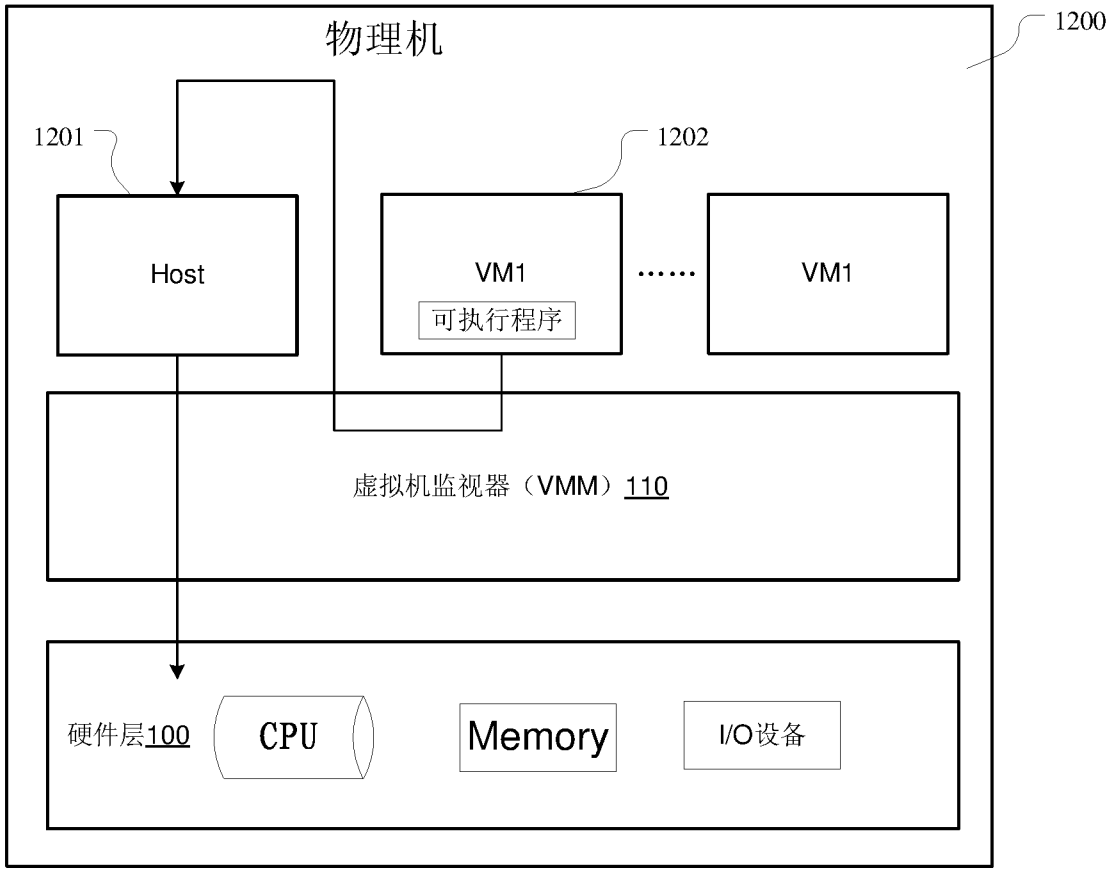

物理机
1200
1201
1202
Host
VM1
可执行程序
……
VM1
虚拟机监视器（VMM）110
硬件层100
CPU
Memory
I/O设备

图 12

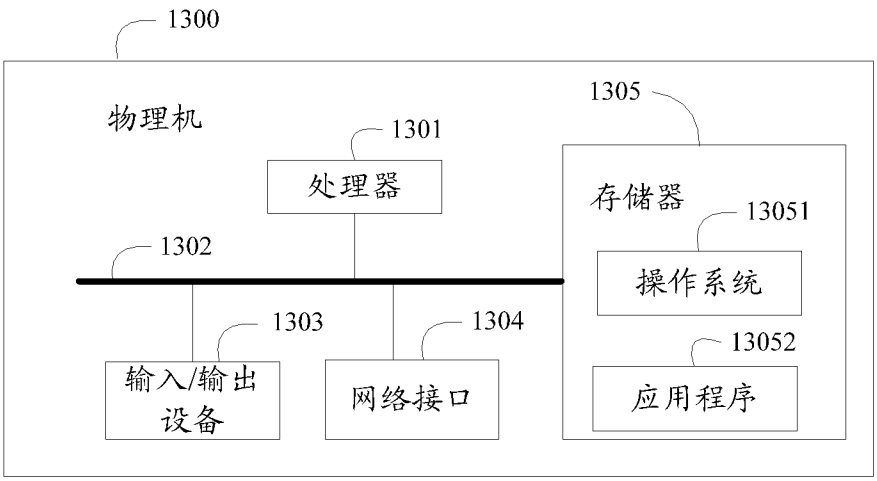

1300
物理机
1305
1301
处理器
存储器
13051
1302
操作系统
1303
1304
13052
输入/输出
设备
网络接口
应用程序

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/079897

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI, CNTXT: cloud, computat+, attack, behave, apply, process+, strategy, manage+, receive, action, data, safe+, connect, detect, rule

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104392175 A (HUAWEI TECHNOLOGIES CO., LTD.) 04 March 2015 (04.03.2015) claims 1-22	1-22
Y	CN 104038466 A (CHINA UNIONPAY CO., LTD.) 10 September 2014 (10.09.2014) claims 1-4, 8 and 9	1, 4-10, 12-14, 16, 17, 19-22
Y	CN 104113521 A (XI AN FUTURE INTERNAT INFORMATION CO., LTD. et al.) 22 October 2014 (22.10.2014) claims 1 and 3, description, paragraphs [0005]-[0008]	1, 4-10, 12-14, 16, 17, 19-22
A	CN 103036745 A (UNIV BEIJING POSTS & TELECOMM) 10 April 2013 (10.04.2013) the whole document	1-22
A	US 8613089 B1 (HOLLOWAY LEE HAHN et al.) 17 December 2013 (17.12.2013) the whole document	1-22
A	CN 103034807 A (TENCENT TECH SHENZHEN CO., LTD.) 10 April 2013 (10.04.2013) the whole document	1-22

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 June 2015	30 July 2015
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIU, Huan Telephone No. (86-10) 62411853

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/079897

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104392175 A	04 March 2015	None	
CN 104038466 A	10 September 2014	None	
CN 104113521 A	22 October 2014	None	
CN 103036745 A	10 April 2013	None	
US 8613089 B1	17 December 2013	US 8856924 B2	07 October 2014
		US 2014157416 A1	05 June 2014
		US 8646064 B1	04 February 2014
		US 2014109225 A1	17 April 2014
		US 2014047539 A1	13 February 2014
		US 2014047542 A1	13 February 2014
		US 2015026766 A1	22 January 2015
CN 103034807 A	10 April 2013	None	

国际检索报告

国际申请号
PCT/CN2015/079897

A. 主题的分类

G06F 21/56(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI,EPODOC,CNPAT,CNKI,CNTXT:云计算，攻击，应用，行为，处理，策略，管理，接收，数据，安全，连接，规则，CLOUD，COMPUTAT+，ATTACK，BEHAVE，APPLY，PROCESS+，STRATEGY，MANAGE+,RECEIVE,ACTION,DATA,SAFE+,CONNECT,DETECT,RULE

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 104392175 A (华为技术有限公司) 2015年 3月 4日 (2015-03-04) 权利要求1-22	1-22
Y	CN 104038466 A (中国银联股份有限公司) 2014年 9月 10日 (2014-09-10) 权利要求1-4，8-9	1，4-10，12-14，16-17，19-22
Y	CN 104113521 A (西安未来国际信息股份有限公司等) 2014年 10月 22日 (2014-10-22) 权利要求1，3，说明书第5-8段	1，4-10，12-14，16-17，19-22
A	CN 103036745 A (北京邮电大学) 2013年 4月 10日 (2013-04-10) 全文	1-22
A	US 8613089 B1 (HOLLOWAY LEE HAHN等) 2013年 12月 17日 (2013-12-17) 全文	1-22
A	CN 103034807 A (腾讯科技深圳有限公司) 2013年 4月 10日 (2013-04-10) 全文	1-22

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2015年 6月 25日	2015年 7月 30日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	刘欢
传真号 (86-10)62019451	电话号码 (86-10)62411853

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/079897

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104392175	A	2015年 3月 4日	无			
CN	104038466	A	2014年 9月 10日	无			
CN	104113521	A	2014年 10月 22日	无			
CN	103036745	A	2013年 4月 10日	无			
US	8613089	B1	2013年 12月 17日	US	8856924	B2	2014年 10月 7日
				US	2014157416	A1	2014年 6月 5日
				US	8646064	B1	2014年 2月 4日
				US	2014109225	A1	2014年 4月 17日
				US	2014047539	A1	2014年 2月 13日
				US	2014047542	A1	2014年 2月 13日
				US	2015026766	A1	2015年 1月 22日
CN	103034807	A	2013年 4月 10日	无			