

(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 12 月 29 日 (29.12.2016)



(10) 国际公布号
WO 2016/206565 A1

- (51) 国际专利分类号:
G06F 21/00 (2013.01)
- (21) 国际申请号: PCT/CN2016/086103
- (22) 国际申请日: 2016 年 6 月 17 日 (17.06.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510360075.5 2015 年 6 月 26 日 (26.06.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 周灿 (ZHOU, Can); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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: MALICIOUS PROGRAM DETECTION METHOD AND DEVICE

(54) 发明名称: 恶意程序检测方法及装置

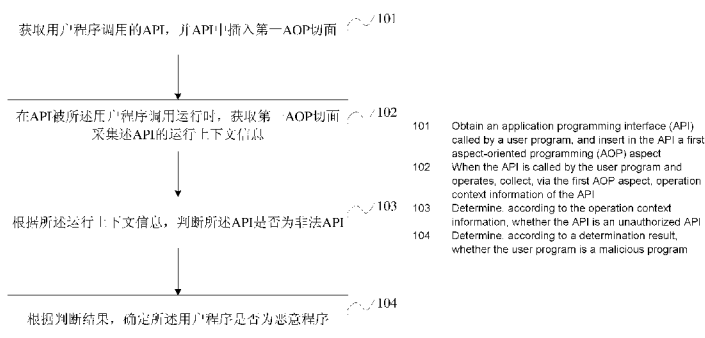


图 1

(57) Abstract: A malicious program detection method and device. The method comprises: obtaining an application programming interface (API) called by a user program, and inserting in the API a first aspect-oriented programming (AOP) aspect (101); when the API is called by the user program and operates, collecting, via the first AOP aspect, operation context information of the API (102); determining, according to the operation context information, whether the API is an unauthorized API (103); and determining, according to a determination result, whether the user program is a malicious program (104). The malicious program detection method and device decrease detection difficulty and realize an effective detection for detecting a malicious program.

(57) 摘要: 一种恶意程序检测方法及装置, 所述方法包括: 获取用户程序调用的 API, 并在所述 API 中插入第一 AOP 切面 (101); 在所述 API 被所述用户程序调用运行时, 通过所述第一 AOP 切面采集所述 API 的运行上下文信息 (102); 根据所述运行上下文信息, 判断所述 API 是否为非法 API (103); 根据判断结果, 确定所述用户程序是否为恶意程序 (104)。该恶意程序检测方法及装置降低了检测难度, 实现了恶意程序的有效检测。

WO 2016/206565 A1

恶意程序检测方法及装置

本申请要求 2015 年 06 月 26 日递交的申请号为 201510360075.5、发明名称为“恶意程序检测方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本申请属于网络技术领域，具体地说，涉及一种恶意程序检测方法及装置。

背景技术

云计算是近年来在科研机构 and 工业界快速发展的一个新生领域。云计算平台是一个
10 开放式服务、多租户共享的平台，云租户可以租用云计算平台，上传任意的用户程序运行，同时整个平台的计算和存储资源也是被所有用户程序所共享。云计算平台的这种服务形式带来了巨大的安全挑战，云租户上传的程序可能具有恶意行为，而影响平台其他租户程序运行、窃取平台其他租户数据等，因此，云租户之间通常通过安全隔离技术，如“沙箱”进行安全隔离。但是任何安全隔离技术都是可能存在漏洞，被恶意程序突破。

15 为了减少恶意程序带来的危害，还需要进行恶意程序检测。在现有技术中，一种恶意程序检测方式是采用静态代码扫描方式，直接扫描用户程序源码或者通过反汇编技术得到用户程序源码，然后将用户程序源码在特征数据库中进行特征匹配，以确定是否恶意程序。

但是，静态代码扫描的方式，需要一个庞大且全面的云平台恶意程序特征数据库，
20 而构建丰富全面的云平台恶意程序特征数据库难度极大。且攻击者很容易通过对代码修改生成变体或者利用反射、字符串填充、加壳等混淆技术来绕过静态扫描的特征匹配，使得仍不能有效的进行恶意程序的检测。

发明内容

25 有鉴于此，本申请所要解决的技术问题是提供了恶意程序检测方法及装置，使得能够有效检测实现恶意程序的检测，无需构建复杂的程序特征数据库。

为了解决上述技术问题，本申请开了一种恶意程序检测方法，包括：

获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面；

在所述 API 被所述用户程序调用运行时，通过所述第一 AOP 切面采集所述 API 的
30 运行上下文信息；

根据所述运行上下文信息，判断所述 API 是否为非法 API；

根据判断结果，确定所述用户程序是否为恶意程序。

优选地，所述根据判断结果，确定所述用户程序是否为恶意程序包括：

在所述 API 为非法 API 时，判断所述 API 是否为通过合法调用程序调用的，所述合法调用程序为高权限程序，所述高权限程序至少包括沙箱、核心库、语言解释器或第三方库；

在所述 API 是通过合法调用程序调用的，或者所述 API 为合法 API 时，确定所述用户程序不是恶意程序；

在所述 API 不是通过合法调用程序调用的时，确定所述用户程序是恶意程序。

10 优选地，预先在合法调用程序中插入第二 AOP 切面，所述第二 AOP 切面定义了合法调用非法 API 的所述合法调用程序的相关信息；

所述判断所述 API 是否为通过合法调用程序调用的包括：

在获取到所述第二 AOP 切面定义的所述合法调用程序的相关信息时，判断所述 API 的调用链中的调用来源是否为所述合法调用程序的相关信息对应的合法调用程序。

15 优选地，预先在合法调用程序中插入第三 AOP 切面，所述第三 AOP 切面定义了所述合法调用程序合法调用的非法 API；

所述判断所述 API 是否为通过合法调用程序调用的包括：

判断是否获得所述第三 AOP 切面定义的合法调用的非法 API，以及所述 API 是否为所述合法调用的非法 API，如果均为是，表明所述 API 为通过合法调用程序调用的，否则表明所述 API 不是通过合法调用程序调用的。

20 优选地，所述获取用户程序调用的 API，并在所述 API 中插入 AOP 切面包括：

在高权限程序初始化结束之后，获取用户程序调用的 API，并在所述 API 中插入 AOP 切面。

一种恶意程序检测装置，包括：

25 切面插入模块，用于获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面；
信息采集模块，用于在所述 API 被所述用户程序调用运行时，通过所述第一 AOP 切面采集所述 API 的运行上下文信息；

判断模块，用于根据所述运行上下文信息，判断所述 API 是否为非法 API；

确定模块，用于根据所述判断模块的判断结果，确定所述用户程序是否为恶意程序。

30 优选地，所述确定模块包括：

判断单元，用于所述判断模块判断出所述 API 为非法 API 时，判断所述 API 是否通过合法调用程序调用的，所述合法调用程序为高权限程序，所述高权限程序至少包括沙箱、核心库、语音解释器或第三方库；

确定单元，用于在所述判断单元判断出所述 API 为通过合法调用程序调用的时，确定所述用户程序不是恶意程序；在所述判断单元判断出所述 API 不是通过合法调用程序调用的，或者所述判断模块判断出所述 API 为合法 API 时，确定所述用户程序是恶意程序。

优选地，所述装置还包括：

第一预设置模块，用于预先在合法调用程序中插入第二 AOP 切面，所述第二 AOP 切面定义了合法调用非法 API 的所述合法调用程序的相关信息；

所述判断单元具体用于：

在获取到所述第二 AOP 切面定义的合法调用程序的相关信息时，判断所述 API 调用链中的调用来源是否为所述合法调用程序的相关信息对应的合法调用程序。

优选地，所述装置还包括：

第二预设置模块，用于预先在合法调用程序中插入第三 AOP 切面，所述第三 AOP 切面定义了所述合法调用程序合法调用的非法 API；

所述判断单元具体用于：

判断是否获得所述第三 AOP 切面定义的合法调用的非法 API，以及所述 API 是否为所述合法调用的非法 API，如果均为是，表明所述 API 为通过合法调用程序调用的，否则表明所述 API 不是通过合法调用程序调用的。

优选地，所述切面插入模块具体用于在高权限程序初始化结束之后，获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面。

与现有技术相比，本申请可以获得包括以下技术效果：

无需构建云平台恶意程序特征数据库，降低了检测难度，且不对用户程序有任何侵入性，也避免了攻击者利用混淆技术绕过代码扫描的问题，实现了恶意程序的有效检测。

当然，实施本申请的任一产品必不一定需要同时达到以上所述的所有技术效果。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 是本申请实施例的一种恶意程序检测方法一个实施例的流程图；

图 2 是本申请实施例的非法 API 的定义示意图；

图 3 是本申请实施例的一种恶意程序检测方法另一个实施例的流程图；

图 4 是本申请实施例的一种恶意程序检测装置一个实施例的结构示意图；

5 图 5 是本申请实施例的一种恶意程序检测装置另一个实施例的结构示意图；

图 6 是本申请实施例的一种恶意程序检测装置又一个实施例的结构示意图；

图 7 是本申请实施例的一种恶意程序检测装置又一个实施例的结构示意图。

具体实施方式

10 以下将配合附图及实施例来详细说明本申请的实施方式，藉此对本申请如何应用技术手段来解决技术问题并达成技术功效的实现过程能充分理解并据以实施。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

15 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM)和/或非易失性内存等形式，如只读存储器 (ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带、磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

25

图 1 为本申请实施例提供的一种恶意程序检测方法一个实施例的流程图，该方法可以包括以下几个步骤：

101：获取用户程序调用的 API，并在所述 API 中插入第一 AOP(Aspect oriented programming，面向切面编程)切面。

30

102: 在所述 API 被所述用户程序调用运行时,通过所述第一 AOP 切面采集所述 API 的运行上下文信息。

103: 根据所述运行上下文信息,判断所述 API 是否为非法 API。

104: 根据判断结果,确定所述用户程序是否为恶意程序。

5 在所述判断结果表明所述 API 为非法 API 时,则可以确定用户程序为恶意程序,在所述判断结果表明所述 API 为合法 API 时,则可以确定用户程序不是恶意程序。

在实际应用中,本申请实施例具体应用于云计算平台上,用户程序为云租户在云计算平台上上传的程序。云计算平台提供了 API 接口供不同云租户的用户程序调用,使得用户程序在云计算平台上能够运行。

10 其中,获取用户程序调用的 API 可以在所述用户程序运行之前预先获取;可以预先扫描用户程序,获得用户程序将要调用的 API。

或者,在所述用户程序运行之后,其每调用一次 API,即获取所调用的 API,比如用户程序为 Java 程序时,是边运行边加载 API 的,Java 解释器解释执行 Java 程序的指令序列时,首次执行到某个 API 时,才会加载这个 API,第一 AOP 切面注入时机,利用了 Java 对切面编程 aop 的支持功能,在 java 解释器首次执行到某个 API 准备加载时,拦截该 API 的加载动作,并在这个时刻在该 API 中注入切面,然后再交由解释器继续加载运行该 API。

当判断用户程序不是恶意程序时,即可以继续执行该用户程序。

在代码加载阶段,读取用户程序时,即可以获知用户程序需要调用的 API。从而本申请实施例中能够在用户程序调用的 API 中插入 AOP 切面。

AOP 是一种新的程序设计范型,它的目标是将代码各个部分进行分离,从而获得程序逻辑中各部分代码低耦合性的隔离效果。利用 AOP,可以不修改程序字节码或者汇编代码文件,而是在代码插入 AOP 切面,然后再将代码解释执行。通过 AOP,不对用户程序有任何侵入性,也即不需要用户修改自己代码,不需要用户提供程序源码给云服务商,不对用户依赖的程序语言核心 API 有任何修改(切面注入是在内存中完成,不实际修改 API 文件),可以避免侵犯第三方库和语言标准库函数的知识产权,也不需要修改查看和修改云租户程序的源代码。

插入的第一 AOP 切面编译为监控逻辑,在 API 被调用运行时,第一 AOP 切面被运行,使得能够采集 API 的运行上下文信息。

30 通过第一 AOP 切面采集的运行上下文信息,即可以判定该运行上下文信息是否为预

先设定的非法 API 的运行上下文信息，从而能够确定用户程序调用的 API 是否为非法 API，如果为非法 API，则可以确定用户程序为恶意程序；如果不是非法 API，则可以确定用户程序不是恶意程序。

其中，API 的运行上下文信息可以包括 API 的类型、调用方法名、方法具体参数值以及方法返回值等。

在本申请实施例中，对于任一个用户程序，可以通过在其调用的 API 中插入第一 AOP 切面的方式，使得被调用的 API 运行时，运行第一 AOP 切面，即会采集 API 的运行上下文信息，从而根据运行上下文信息，可以确定被调用的 API 是否为非法 API，进而可以有效确定用户程序是否为恶意程序。不需要构建云平台恶意程序特征数据库，不对用户程序有任何侵入性，也避免了攻击者利用混淆技术绕过代码扫描的问题，实现了恶意程序的有效检测。

非法 API 以及合法 API 可以预先设定。在云计算平台中，云租户之间通过安全隔离技术，如沙箱进行隔离。安全隔离技术定义了被隔离的云租户允许调用的合法 API，即沙箱内的 API，以及禁止运行的 API，即沙箱外 API，因此所述非法 API 可以为根据安全隔离技术的安全策略文件定义的禁止运行的 API。

如图 2 所示的示意图中，安全隔离技术为沙箱，云租户只能允许调用沙箱允许操作的 API，即合法 API。沙箱外为定义的禁止运行的 API。

进一步的，禁止调用的 API 中，有些 API 操作危险性较高，比如会访问密码文件、扫描其他用户文件、发起网络连接等，因此非法 API 可以具体为禁止调用的 API 中的危险 API。

恶意程序在利用漏洞突破安全隔离防护后，就会获得部分或者全部非法 API 操作的调用权限，加载最高权限的 payload、扫描本地文件、下载和执行外部程序、执行本地命令等危险操作，利用这些非法 API，会尝试关闭安全管理，以便进行进一步的渗透。

因此本申请实施例中，利用第一 AOP 切面采集的 API 运行上下文信息，可以确定被调用的 API 为非法 API 时，则可以确定用户程序为恶意程序。当前的用户程序没有权限执行某些操作。

根据所述运行上下文信息，判断 API 是否为非法 API 具体可以是根据规则和启发式来判定的。

在实际应用中，用户程序执行过程中，由于语言解释器、核心库、沙箱或者第三方库等高权限程序，可能会触发用户程序而调用某些非法 API。也即用户程序执行过程中，是调用这些高权限程序执行，而高权限程序可能调用非法 API，从而使得用户程序调用的 API 的调用来源为高权限程序。

5 而高权限程序调用非法 API 是可能被允许的，不代表用户程序是恶意程序。也即存在合法调用非法 API 的合法调用程序。

例如，被安全隔离的禁止运行的 API 中，有些危险操作的 API，比如 java 中的 defineClass()，是 java 解释器和沙箱可以执行的，但是用户程序确不能自行调用。

因此为了避免误检测的问题，在本申请实施例的另一个实施例中，如图 3 所示，恶意程序检测方法可以包括以下几个步骤：

301：获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面。

302：在所述 API 被所述用户程序调用运行时，通过所述 AOP 切面采集所述 API 的运行上下文信息。

303：根据所述运行上下文信息，判断所述 API 是否为非法 API，如果是，执行步骤

15 304，如果否，执行步骤 305。

304：判断所述 API 是否为通过合法调用程序调用的，如果是，执行步骤 305，如果否，执行步骤 306。

所述合法调用程序具体为高权限程序，所述高权限程序至少包括沙箱、核心库、语音解释器或第三方库等。

20 第三方库也就是第三方 API，第三方库是在系统库 API 基础上实现的，可以认为是由几个系统库 API 及相关代码组合而成，用户也可以合法使用。

305：确定所述用户程序不是恶意程序。

306：确定所述用户程序是恶意程序。

一旦确定是合法调用程序调用 API，则可以确定该用户程序并非为恶意程序，从而

25 可以避免误检测。

其中，判断所述用户程序调用的 API，是否为通过合法调用程序调用的可以有多种可能的实现方式：

在一种可能的实现方式中，可以通过提取所述 API 的调用链进行分析。确定该 API 的调用来源是用户程序还是预定义的合法调用程序，如语言解释器、沙箱等。

30 可以通过反射机制或者分析整个系统调用栈来提取 API 的整个调用链，从 API 的直

接调用者往上逐级检查各个调用者的合法性，检测规则为检测到第三方库或者沙箱等预定义的可以合法调用非法 API 的高权限程序则停止检测，说明 API 的调用来源为合法调用程序，如果检测到用户程序也停止检测，说明用户程序突破了安全隔离直接调用了 API。因此，可以进一步通过 AOP 切面采集的运行上下文信息，判断被调用的 API 是否为非法 API。

当然，判断所述 API 是否为通过合法调用程序调用的操作也可以是获取用户程序的 API 之后执行；

在所述 API 为通过合法调用程序调用的时，则可以直接确定用户程序不是恶意程序；

在所述 API 不是通过合法调用程序调用的时，再执行在所述 API 中插入第一 AOP 切面的步骤。

由于并不是所有的高权限程序均被允许调用非法 API。

因此，作为又一个实施例，可以预先在合法调用程序中插入第二 AOP 切面，所述第二 AOP 切面定义了合法调用非法 API 的所述合法调用程序的相关信息；一旦用户通过调用所述合法调用程序，而触发调用 API 时，就会执行合法调用程序中的第二 AOP 切面，从而获得合法调用程序的相关信息。然后再分析 API 的调用链中的调用来源是否为该合法调用程序的相关信息对应的合法调用程序，如果存在，则表明该 API 的调用时合法的，用户程序不被判定为恶意程序。

具体的，步骤 304 中，所述判断所述 API 是否为通过合法调用程序调用的可以包括：在通过所述第二 AOP 切面获取到所述合法调用程序的相关信息时，判断所述 API 调用链中的调用来源是否为所述合法调用程序的相关信息对应的合法调用程序。

如果是，则可以确定用户程序不是恶意程序，如果否，则可以确定用户程序为恶意程序。

从所述 API 的直接调用者往上逐级检查各个调用者的合法性，按照检测规则，如果检测到的调用来源为所述合法调用程序的相关信息对应的合法调用程序，则用户程序不是恶意程序。如果检测到的调用来源即为用户程序，则用户程序为恶意程序。

另外，由于高权限程序并不是允许可以调用全部的非法 API。有些 API 的性质为非常危险，比如 Java 中关闭安全管理器（Set Security Manager）的 API，这种 API 是不应当被任何用户程序或者高权限程序调用的。

作为又一个实施例，可以通过 AOP 预先在合法调用程序中插入第三 AOP 切面，该第三 AOP 切面定义了合法调用程序允许合法调用的非法 API。一旦用户程序调用了合法调用程序，即会运行第三 AOP 切面，获得该合法调用程序能够合法调用的非法 API。从而如果获取的用户程序调用的 API 为该第三 AOP 切面定义的合法调用的非法 API，则表明用户程序并不是恶意程序，其调用的 API 是通过合法调用程序调用的，是被允许的。

具体的，步骤 304 中，所述判断所述 API 是否为通过合法调用程序调用的可以包括：

判断是否获得所述第三 AOP 切面定义的合法调用的非法 API，以及所述 API 是否为所述第三 AOP 切面定义的合法调用的非法 API，如果均为是，表明所述 API 为通过合法调用程序调用的，否则表明所述 API 不是通过合法调用程序调用的。

本实施中，如果用户程序调用的 API 是否通过合法调用程序调用的，则也可以无需分析所述 API 的调用链，只需在合法调用程序中预先插入第三 AOP 切面，通过运行所述第三 AOP 切面即可以获得合法调用程序合法调用的非法 API。

从而如果获得了合法调用的非法 API，且用户程序的调用的所述 API 为所述合法调用的非法 API，则表明用户程序的 API 是通过合法调用程序调用的，从而可以确定用户程序不是恶意程序；否则即为恶意程序。

此外，在本申请实施例的又一个实施例中：

由于一些高权限程序，如沙箱，调用非法 API 的操作时通常是在初始化时完成，跳转至用户程序后，沙箱执行非法 API 的情况几乎不存在，因此本申请实施例中，获取用户程序调用的 API 具体可以是：

在高权限程序初始化结束之后，获取用户程序调用的 API，并在所述 API 中插入 AOP 切面。从而可以避免不必要的操作，简化了检测操作。

本申请实施例可以适用于多种云场景中，如 PaaS（Platform-as-a-Service，平台即服务）中的 app engine，开放式数据处理服务中 open MR（open mapreduce service）开放式 mapreduce 等。

用户程序，在 PaaS 平台上，可以是 java、python、c 和 c++等，在开放式数据处理服务中，可以是一段数据分析代码等。

AOP 切面的插入操作，以 java 程序为例，可以是基于 java 字节码驱动库 javassist 来辅助进行，利用 java 语言对 AOP 的支持接口 instrument 包接口，会拦截用户程序在加

载器中的加载过程，在加载的过程中在调用的 API 中插入已经生成好的 AOP 切面。

AOP 切面在 API 被调用时被触发采集 API 的运行上下文信息。并可以触发分析运行上下文信息。

python 程序，也可以利用其内在 AOP 的支持，配合 python 的字节码驱动包生成 AOP
5 切面和进行切面插入。

甚至对于 C 语言程序，利用 ptrace 系统调用也可以拦截 C 程序的 API 调用，以在 API 中插入 AOP 切面。

图 4 为本申请实施例提供的一种恶意程序检测装置一个实施例的结构示意图，该装
10 置可以包括：

切面插入模块 401，用于获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面；

信息采集模块 402，用于在所述 API 被所述用户程序调用运行时，通过所述第一 AOP 切面采集所述 API 的运行上下文信息；

15 判断模块 403，用于根据所述运行上下文信息，判断所述 API 是否为非法 API；

确定模块 404，用于根据判断模块 403 的判断结果，确定所述用户程序是否为恶意程序。

在所述 API 为非法 API 时，则可以确定用户程序为恶意程序，在所述 API 为合法 API 时，则可以确定用户程序不是恶意程序。

20 在本申请实施例中，对于任一个用户程序，可以通过在其调用的 API 中插入 AOP 切面的方式，使得被调用的 API 运行时，运行 AOP 切面，即会采集 API 的运行上下文信息，从而根据运行上下文信息，可以确定被调用的 API 是否为非法 API，进而可以有效确定用户程序是否为恶意程序。不需要构建云平台恶意程序特征数据库，不对用户程序有任何侵入性，也避免了攻击者利用混淆技术绕过代码扫描的问题，实现了恶意程序
25 的有效检测。

其中，获取用户程序调用的 API 可以在所述用户程序运行之前预先获取，或者在所述用户程序运行之后获取。

非法 API 以及合法 API 可以预先设定。在云计算平台中，云租户之间通过安全隔离
30 技术，如沙箱进行隔离。安全隔离技术定义了被隔离的云租户允许调用的合法 API，以

及禁止调用的 API，因此所述非法 API 可以为根据安全隔离技术的安全策略文件定义的禁止调用的 API。

进一步的，禁止调用的 API 中，有些 API 操作危险性较高，比如会访问密码文件、扫描其他用户文件、发起网络连接等，因此非法 API 可以具体为禁止调用的 API 中的危险 API。

在实际应用中，由于语言解释器、核心库、沙箱或者第三方库等高权限程序，可能会通过用户程序而调用某些非法 API，从而使得非法 API 的调用来源为高权限程序。而高权限程序调用非法 API 是可能被允许的，不代表用户程序是恶意程序。也即存在合法调用非法 API 的合法调用程序。

因此为了避免误检测的问题，在本申请实施例的另一个实施例中，如图 5 所示，所述确定模块 404 可以包括：

判断单元 501，用于所述判断模块 403 判断出所述 API 为非法 API 时，判断所述 API 是否为通过合法调用程序调用的，所述合法调用程序为高权限程序，所述高权限程序至少包括沙箱、核心库、语音解释器或第三方库；

确定单元 502，用于在所述判断单元 501 判断出所述 API 为通过合法调用程序调用的时，确定所述用户程序不是恶意程序；在所述判断单元 501 判断出所述 API 不是通过合法调用程序调用的，或者所述判断模块 403 判断出所述 API 为合法 API 时，确定所述用户程序是恶意程序。

其中，所述判断单元判断所述用户程序调用的 API，是否为通过高权限程序调用的可以有多种可能的实现方式：

在一种可能的实现方式中，可以通过提取所述 API 的调用链进行分析。确定该 API 的调用来源是用户程序还是语言解释器、沙箱等合法调用程序。

由于并不是所有的高权限程序均会调用非法 API，或者高权限程序会调用全部的非法 API。有些 API 的性质为非常危险，比如 Java 中关闭安全管理器 (Set Security Manager) 的 API，这种 API 是不应当被任何用户程序或者高权限程序调用的，因此在判断出用户程序调用的 API 为非法 API，且为预设的危险 API，则可以直接确定用户程序为恶意程序。

作为又一个实施例，如图 6 所述，所述装置还可以包括：

第一预设置模块 601，用于预先在合法调用程序中插入第二 AOP 切面，所述第二 AOP 切面定义了合法调用非法 API 的所述合法调用程序的相关信息；

所述判断单元 501 具体用于：

在获取到所述第二 AOP 切面定义的合法调用程序的相关信息时，判断所述 API 调用链中的调用来源是否为所述合法调用程序的相关信息对应的合法调用程序。

如果是，则可以确定用户程序不是恶意程序，如果否，则可以确定用户程序为恶意程序。

另外，作为又一个实施例，如图 7 所示，所述装置还可以包括：

10 第二预设置模块 701，用于预先在合法调用程序中插入第三 AOP 切面，所述第三 AOP 切面定义了所述合法调用程序合法调用的非法 API；

所述判断单元 501 则可以具体用于：

判断是否获得所述第三 AOP 切面定义的合法调用的非法 API，以及所述 API 是否为所述合法调用的非法 API，如果均为是，表明所述 API 为通过合法调用程序调用的，否则表明所述 API 不是通过合法调用程序调用的。

本实施中，如果用户程序调用的 API 是否通过合法调用程序调用的，则也可以无需分析所述 API 的调用链，只需在合法调用程序中预先插入第三 AOP 切面，通过运行所述第三 AOP 切面即可以获得合法调用程序合法调用的非法 API。

从而如果获得了合法调用的非法 API，且用户程序的调用的所述 API 为所述合法调用的非法 API，则表明用户程序的 API 是通过合法调用程序调用的，从而可以确定用户程序不是恶意程序；否则即为恶意程序。

另外，由于高权限程序，如沙箱，调用非法 API 的操作时是在初始化时完成，跳转至用户程序后，沙箱等执行非法 API 的情况极少，因此本申请实施例中，所述切面插入模块具体用于在合法调用程序初始化结束之后，获取用户程序调用的 API，并在所述 API 25 中插入第一 AOP 切面。

如在说明书及权利要求当中使用了某些词汇来指称特定组件。本领域技术人员应可理解，硬件制造商可能会用不同名词来称呼同一个组件。本说明书及权利要求并不以名称的差异来作为区分组件的方式，而是以组件在功能上的差异来作为区分的准则。如在通篇说明书及权利要求当中所提及的“包含”为一开放式用语，故应解释成“包含但不限于”。 “大致”是指在可接收的误差范围内，本领域技术人员能够在一定误差范围 30

内解决所述技术问题，基本达到所述技术效果。此外，“耦接”一词在此包含任何直接及间接的电性耦接手段。因此，若文中描述一第一装置耦接于一第二装置，则代表所述第一装置可直接电性耦接于所述第二装置，或通过其他装置或耦接手段间接地电性耦接至所述第二装置。说明书后续描述为实施本申请的较佳实施方式，然所述描述乃以说明
5 本申请的一般原则为目的，并非用以限定本申请的范围。本申请的保护范围当视所附权利要求所界定者为准。

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的商品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种商品或者系统所固有的要素。在没有更多限制
10 的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的商品或者系统中还存在另外的相同要素。

上述说明示出并描述了本申请的若干优选实施例，但如前所述，应当理解本申请并非局限于本文所披露的形式，不应看作是对其他实施例的排除，而可用于各种其他组合、修改和环境，并能够在本文所述申请构想范围内，通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本申请的精神和范围，则都应在
15 本申请所附权利要求的保护范围内。

权 利 要 求 书

1、一种恶意程序检测方法，其特征在于，包括：

获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面；

5 在所述 API 被所述用户程序调用运行时，通过所述第一 AOP 切面采集所述 API 的运行上下文信息；

根据所述运行上下文信息，判断所述 API 是否为非法 API；

根据判断结果，确定所述用户程序是否为恶意程序。

2、如权利要求 1 所述的方法，其特征在于，所述根据判断结果，确定所述用户程序是否为恶意程序包括：

10 在所述 API 为非法 API 时，判断所述 API 是否为通过合法调用程序调用的，所述合法调用程序为高权限程序，所述高权限程序至少包括沙箱、核心库、语言解释器或第三方库；

在所述 API 是通过合法调用程序调用的，或者所述 API 为合法 API 时，确定所述用户程序不是恶意程序；

15 在所述 API 不是通过合法调用程序调用的时，确定所述用户程序是恶意程序。

3、如权利要求 2 所述的方法，其特征在于，预先在合法调用程序中插入第二 AOP 切面，所述第二 AOP 切面定义了合法调用非法 API 的所述合法调用程序的相关信息；

所述判断所述 API 是否为通过合法调用程序调用的包括：

20 在获取到所述第二 AOP 切面定义的所述合法调用程序的相关信息时，判断所述 API 的调用链中的调用来源是否为所述合法调用程序的相关信息对应的合法调用程序。

4、如权利要求 2 所述的方法，其特征在于，预先在合法调用程序中插入第三 AOP 切面，所述第三 AOP 切面定义了所述合法调用程序合法调用的非法 API；

所述判断所述 API 是否为通过合法调用程序调用的包括：

25 判断是否获得所述第三 AOP 切面定义的合法调用的非法 API，以及所述 API 是否为所述合法调用的非法 API，如果均为是，表明所述 API 为通过合法调用程序调用的，否则表明所述 API 不是通过合法调用程序调用的。

5、如权利要求 1 所述的方法，其特征在于，所述获取用户程序调用的 API，并在所述 API 中插入 AOP 切面包括：

30 在高权限程序初始化结束之后，获取用户程序调用的 API，并在所述 API 中插入 AOP 切面。

6、一种恶意程序检测装置，其特征在于，包括：

切面插入模块，用于获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面；

信息采集模块，用于在所述 API 被所述用户程序调用运行时，通过所述第一 AOP

5 切面采集所述 API 的运行上下文信息；

判断模块，用于根据所述运行上下文信息，判断所述 API 是否为非法 API；

确定模块，用于根据所述判断模块的判断结果，确定所述用户程序是否为恶意程序。

7、如权利要求 6 所述的装置，其特征在于，所述确定模块包括：

10 判断单元，用于所述判断模块判断出所述 API 为非法 API 时，判断所述 API 是否为通过合法调用程序调用的，所述合法调用程序为高权限程序，所述高权限程序至少包括沙箱、核心库、语音解释器或第三方库；

确定单元，用于在所述判断单元判断出所述 API 为通过合法调用程序调用的时，确定所述用户程序不是恶意程序；在所述判断单元判断出所述 API 不是通过合法调用程序调用的，或者所述判断模块判断出所述 API 为合法 API 时，确定所述用户程序是恶意程
15 序。

8、如权利要求 7 所述的装置，其特征在于，所述装置还包括：

第一预设置模块，用于预先在合法调用程序中插入第二 AOP 切面，所述第二 AOP 切面定义了合法调用非法 API 的所述合法调用程序的相关信息；

所述判断单元具体用于：

20 在获取到所述第二 AOP 切面定义的合法调用程序的相关信息时，判断所述 API 调用链中的调用来源是否为所述合法调用程序的相关信息对应的合法调用程序。

9、如权利要求 7 所述的装置，其特征在于，所述装置还包括：

第二预设置模块，用于预先在合法调用程序中插入第三 AOP 切面，所述第三 AOP 切面定义了所述合法调用程序合法调用的非法 API；

25 所述判断单元具体用于：

判断是否获得所述第三 AOP 切面定义的合法调用的非法 API，以及所述 API 是否为所述合法调用的非法 API，如果均为是，表明所述 API 为通过合法调用程序调用的，否则表明所述 API 不是通过合法调用程序调用的。

10、如权利要求 6 所述的装置，其特征在于，所述切面插入模块具体用于在高权限
30 程序初始化结束之后，获取用户程序调用的 API，并在所述 API 中插入第一 AOP 切面。

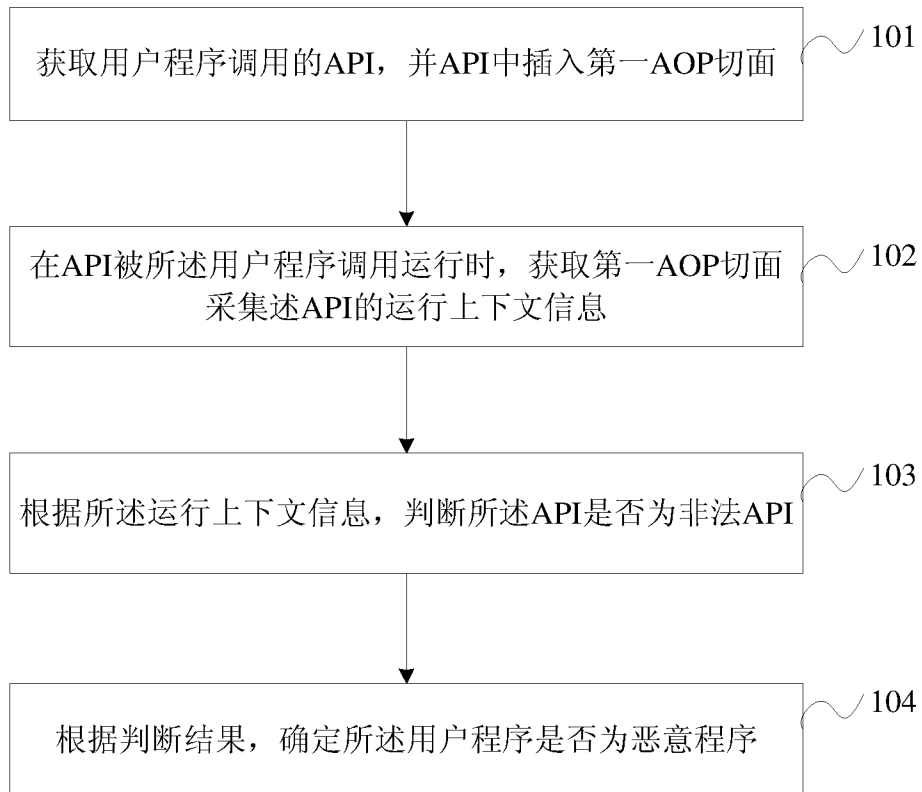


图 1

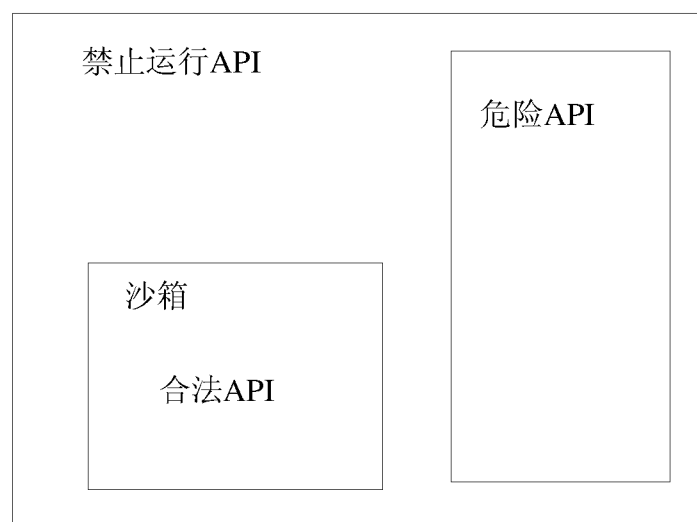


图 2

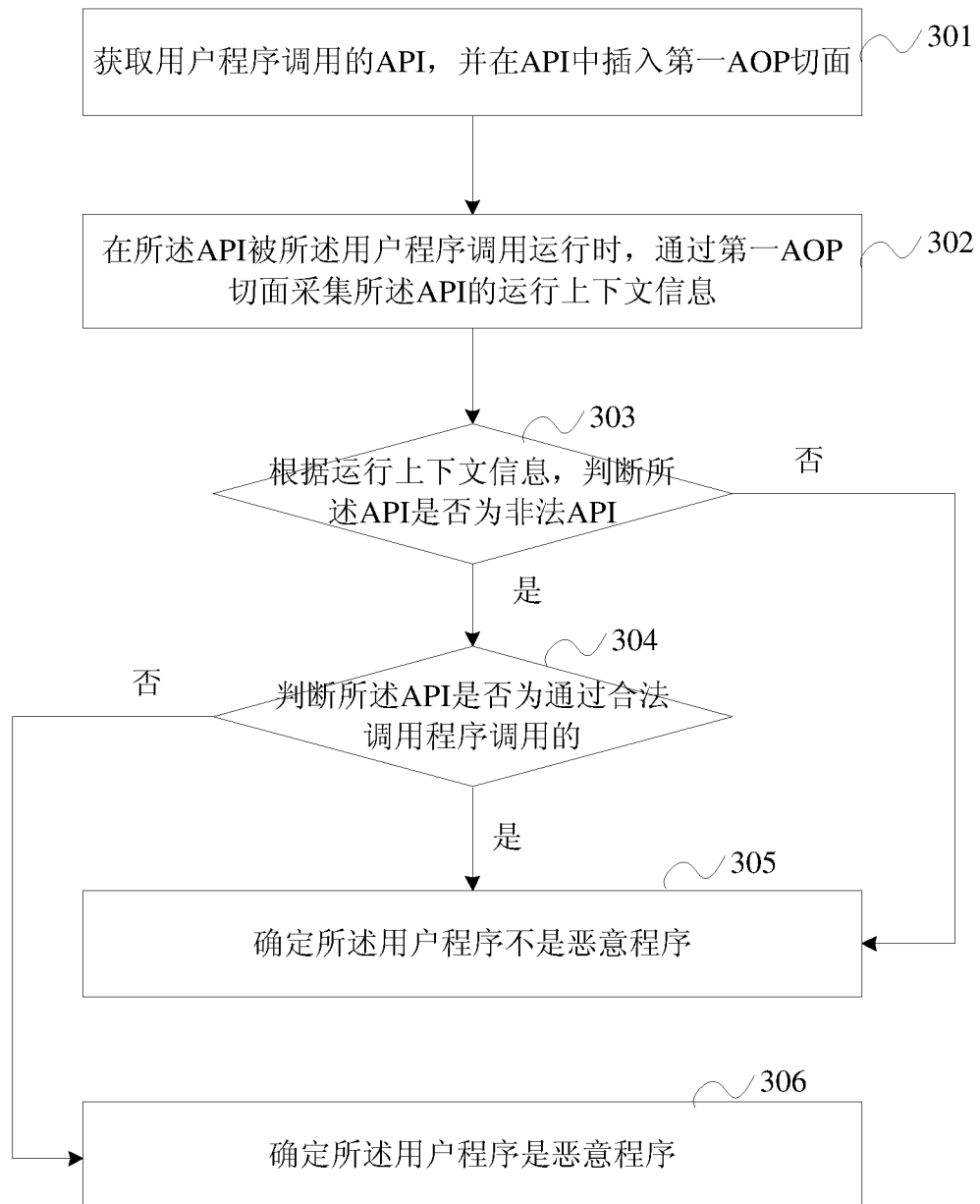


图 3



图 4



图 5

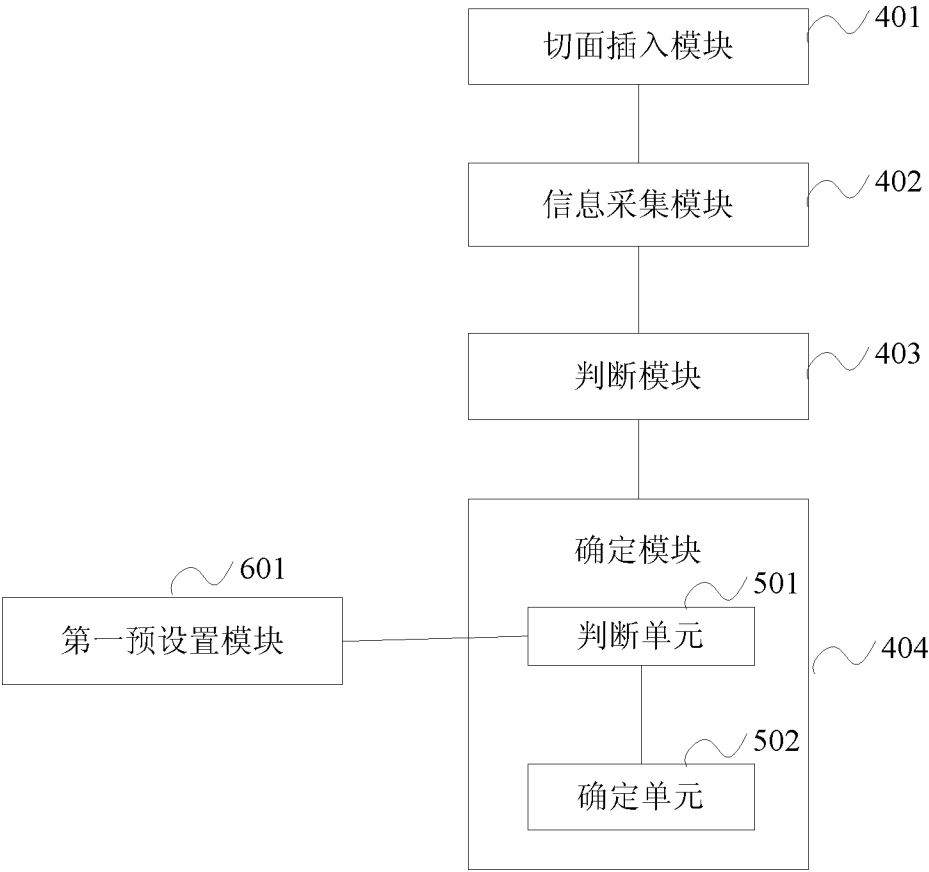


图 6

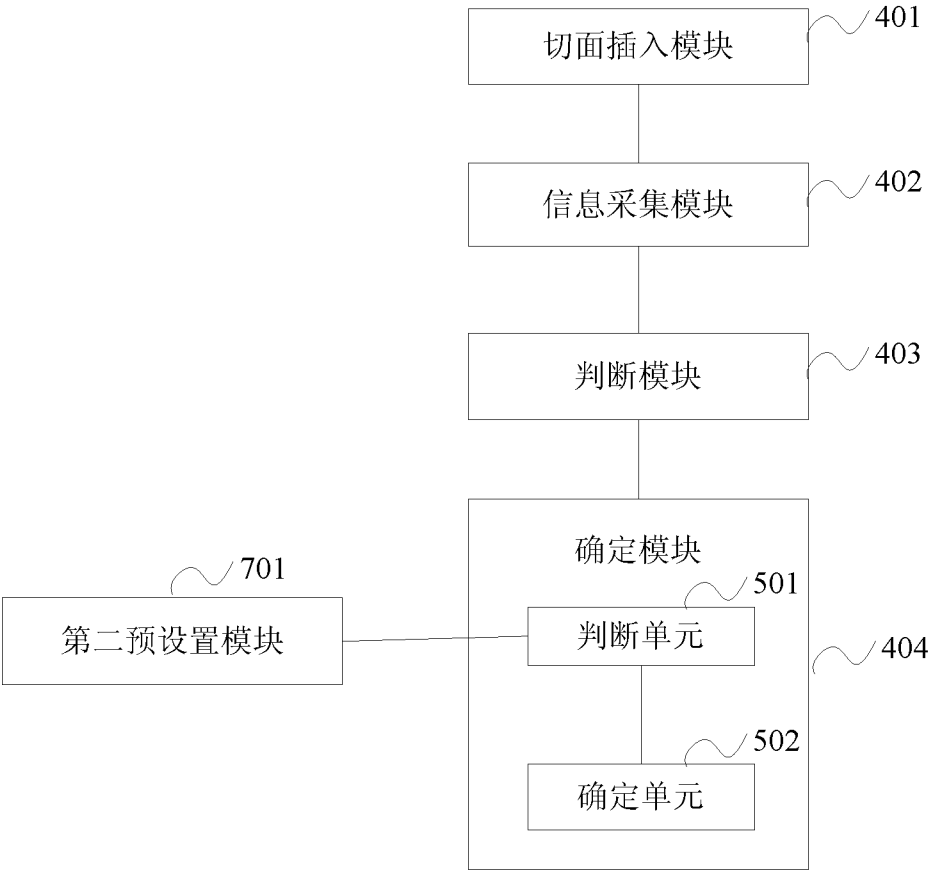


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/086103

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (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)

CNKI, CNPAT, EPODOC, WPI: AOP, aspect-oriented, scan, program, legal, interface function, cloud, allow, sandbox, tenant, malicious, API, platform, call, access, interface, illegal+, forbidde+, detect, monit+, authority, validation, reservation, rights, check+, prelect+, virus+, threat, danger+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101408917 A (XIAMEN MEIYA PICO INFORMATION TECHNOLOGY CO., LTD.), 15 April 2009 (15.04.2009), description, page 5, last paragraph to page 7, paragraph 1, and figures 3 and 4	1-10
A	CN 102737188 A (BEIJING QIHOO TECHNOLOGY CO., LTD.), 17 October 2012 (17.10.2012), the whole document	1-10
A	CN 102930203 A (ZHEJIANG UNIVERSITY CITY COLLEGE), 13 February 2013 (13.02.2013), the whole document	1-10
A	CN 103440459 A (XI'AN JIAOTONG UNIVERSITY), 11 December 2013 (11.12.2013), the whole document	1-10
A	CN 104598824 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER et al.), 06 May 2015 (06.05.2015), the whole document	1-10

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 06 September 2016 (06.09.2016)	Date of mailing of the international search report 21 September 2016 (21.09.2016)
Name and mailing address of the ISA/CN: 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 SUN, Changxin Telephone No.: (86-10) 01061648007

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/086103

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2007113709 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V. et al.), 11 October 2007 (11.10.2007), the whole document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/086103

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101408917 A	15 April 2009	None	
CN 102737188 A	17 October 2012	None	
CN 102930203 A	13 February 2013	CN 102930203 B	26 August 2015
CN 103440459 A	11 December 2013	CN 103440459 B	06 April 2016
CN 104598824 A	06 May 2015	CN 104598824 B	06 April 2016
WO 2007113709 A1	11 October 2007	None	

国际检索报告

国际申请号

PCT/CN2016/086103

A. 主题的分类

G06F 21/00(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))

CNKI, CNPAT, EPODOC, WPI; AOP, 面向切面, 扫描, 程序, 调用, 访问, 检测, 监视, 权限, 合法, 接口函数, 云, 监控, 允许, 非法, 沙箱, 租户, 恶意, 威胁, 危险, 病毒, API, 平台, 接口, call, access, interface, illegal+, forbidde+, detect, monit+, authority, validation, reservation, rights, check+, prectect+, virus+, threat, danger+

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
A	CN 101408917 A (厦门市美亚柏科资讯科技有限公司) 2009年 4月 15日 (2009 - 04 - 15) 说明书第5页最后1段至第7页第1段及附图3、4	1-10
A	CN 102737188 A (北京奇虎科技有限公司) 2012年 10月 17日 (2012 - 10 - 17) 全文	1-10
A	CN 102930203 A (浙江大学城市学院) 2013年 2月 13日 (2013 - 02 - 13) 全文	1-10
A	CN 103440459 A (西安交通大学) 2013年 12月 11日 (2013 - 12 - 11) 全文	1-10
A	CN 104598824 A (国家计算机网络与信息安全管理中心等) 2015年 5月 6日 (2015 - 05 - 06) 全文	1-10

☒ 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

2016年 9月 6日

国际检索报告邮寄日期

2016年 9月 21日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

孙长欣

电话号码 (86-10)01061648077

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
A	WO 2007113709 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V. 等) 2007年 10月 11日 (2007 - 10 - 11) 全文	1-10

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/086103

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	101408917	A	2009年 4月 15日	无	
CN	102737188	A	2012年 10月 17日	无	
CN	102930203	A	2013年 2月 13日	CN 102930203	B 2015年 8月 26日
CN	103440459	A	2013年 12月 11日	CN 103440459	B 2016年 4月 6日
CN	104598824	A	2015年 5月 6日	CN 104598824	B 2016年 4月 6日
WO	2007113709	A1	2007年 10月 11日	无	

表 PCT/ISA/210 (同族专利附件) (2009年7月)