(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113190835 A
(43)申请公布日 2021.07.30

(21)申请号 202110157024.8

(22)申请日 2021.02.04

(71)申请人 恒安嘉新(北京)科技股份公司
地址 100098 北京市海淀区北三环西路25号27号楼五层5002室

(72)发明人 马栋 傅强 蔡琳 梁彧 田野 王杰 杨满智 金红 陈晓光 张振涛 李鹏超 尚城

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

(51)Int.Cl.
G06F 21/53(2013.01)

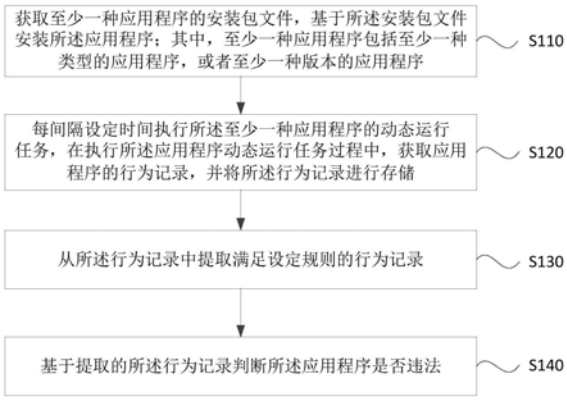
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种应用程序违法检测方法、装置、设备及存储介质

(57)摘要

本发明实施例提供了一种应用程序违法检测方法、装置、设备及存储介质，其中，该方法沙箱养殖设备，该设备中安装至少一套包含沙箱环境的操作系统，该方法包括：获取至少一种应用程序的安装包文件，基于安装包文件安装应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序；每间隔设定时间执行至少一种应用程序的动态运行任务，在执行应用程序动态运行任务过程中，获取应用程序的行为记录，并将行为记录进行存储；从行为记录中提取满足设定规则的行为记录；基于提取的行为记录判断应用程序是否违法，可以对多种应用程序进行违法检测，可以全面监控应用程序，可以更安全更稳定的实现检测。



CN 113190835 A

1.一种应用程序违法检测方法,其特征在于,所述方法应用于沙箱养殖设备,所述设备中安装至少一套包含沙箱环境的操作系统,所述方法包括:

获取至少一种应用程序的安装包文件,基于所述安装包文件安装所述应用程序;其中,至少一种应用程序包括至少一种类型的应用程序,或者至少一种版本的应用程序;

每间隔设定时间执行至少一种应用程序的动态运行任务,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,并将所述行为记录进行存储;

从所述行为记录中提取满足设定规则的行为记录;

基于提取的所述行为记录判断所述应用程序是否违法。

2.根据权利要求1所述的方法,其特征在于,所述沙箱养殖设备中安装有至少一个磁盘,所述磁盘中安装有至少一套包含沙箱环境的操作系统。

3.根据权利要求1所述的方法,其特征在于,所述从所述行为记录中提取满足设定规则的行为记录,包括:

从所述行为记录中剔除与所述应用程序的功能相关的行为记录,提取与所述应用程序的功能不相关的行为记录。

4.根据权利要求1所述的方法,其特征在于,所述每间隔设定时间执行至少一种应用程序的动态运行任务,包括:

每间隔设定时间控制对应应用程序运行在对应的操作系统中;

相应的,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,包括:

在所述应用程序在对应操作系统运行过程中,获取应用程序在对应操作系统中运行的行为记录;其中,不同操作系统的版本或者类型不同。

5.根据权利要求1所述的方法,其特征在于,所述每间隔设定时间执行至少一种应用程序的动态运行任务,包括:

每间隔设定时间控制多个应用程序同时运行;

相应的,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,包括:

在所述多个应用程序同时运行过程中,获取多个应用程序的行为记录。

6.根据权利要求1所述的方法,其特征在于,还包括:

基于提取的所述行为记录以及违法行为记录形成分析报告。

7.根据权利要求6所述的方法,其特征在于,还包括

对应用程序的动态运行任务、行为记录的提取任务、行为记录的获取任务、应用程序违法判断任务以及分析报告形成任务进行管理。

8.一种应用程序违法检测的装置,其特征在于,所述装置配置于沙箱养殖设备,所述设备中安装至少一套包含沙箱环境的操作系统,所述装置包括:

文件上传模块,用于获取至少一种应用程序的安装包文件,基于所述安装包文件安装所述应用程序;

行为收集存储模块,用于每间隔设定时间执行至少一种应用程序的动态运行任务,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,并将所述行为记录进行存储;

提取规则配置模块,用于从所述行为记录中提取满足设定规则的行为记录;

行为分析研判模块,用于基于提取的所述行为记录判断所述应用程序是否违法。

9.一种沙箱养殖设备,其特征在于,包括:

一个或多个处理器;

存储装置,用于存储一个或多个程序,

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-7任一项所述的方法。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-7任一项所述的方法。

一种应用程序违法检测方法、装置、设备及存储介质

技术领域

[0001] 本发明实施例涉及计算机技术领域，尤其涉及一种应用程序违法检测方法、装置、设备及存储介质。

背景技术

[0002] 现有技术中应用程序违法检测方式可以是虚拟机沙箱检测方式。具体的，是通过ROM镜像方式模拟应用程序(Application，App)的运行环境，使App 长时间运行，让App展现出自身的行为，并存储App行为记录，以行为记录判断App是否违法。

[0003] 但是现有技术中的上述方法中，通过虚拟机沙箱来模拟App的运行环境进行App违法检测存在一定的局限性，某些情况可能会导致无法对App进行违法检测，并且虚拟机沙箱的兼容性不足，对APP违法检测有限。

发明内容

[0004] 本发明实施例提供了一种应用程序违法检测方法、装置、设备及存储介质，可以对多种应用程序进行违法检测，可以全面监控应用程序，可以更安全更稳定的实现检测。

[0005] 第一方面，本发明实施例提供了一种应用程序违法检测方法，所述方法应用于沙箱养殖设备，所述设备中安装至少一套包含沙箱环境的操作系统，所述方法包括：

[0006] 获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序；

[0007] 每间隔设定时间执行至少一种应用程序的动态运行任务，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，并将所述行为记录进行存储；

[0008] 从所述行为记录中提取满足设定规则的行为记录；

[0009] 基于提取的所述行为记录判断所述应用程序是否违法。

[0010] 第二方面，本发明实施例还提供了一种应用程序违法检测的装置，所述装置配置于沙箱养殖设备，所述设备中安装至少一套包含沙箱环境的操作系统，所述装置包括：

[0011] 文件上传模块，用于获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；

[0012] 行为收集存储模块，用于每间隔设定时间执行至少一种应用程序的动态运行任务，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，并将所述行为记录进行存储；

[0013] 提取规则配置模块，用于从所述行为记录中提取满足设定规则的行为记录；

[0014] 行为分析研判模块，用于基于提取的所述行为记录判断所述应用程序是否违法。

[0015] 第三方面，本发明实施例还提供了一种沙箱养殖设备，包括：

[0016] 一个或多个处理器；

[0017] 存储装置，用于存储一个或多个程序，

[0018] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理

器实现本发明实施例提供的方法。

[0019] 第四方面，本发明实施例提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本发明实施例提供的方法。

[0020] 本发明实施例提供的技术方案，通过沙箱养殖设备获取至少一种应用程序的安装包文件，并基于安装包文件进行安装应用程序，通过在执行至少一个应用程序的动态运行任务中，获取应用程序的行为记录，并将行为记录进行存储，并提取满足设定规则的行为记录，通过提取的行为记录判断应用程序是否违法，其中，沙箱养殖设备中包含至少一套包含沙箱环境的操作系统。本发明实施例提供的技术方案可以对多种应用程序进行违法检测，可以全面监控应用程序，可以更安全更稳定的实现检测。

附图说明

[0021] 图1是本发明实施例提供的一种应用程序违法检测方法流程图；

[0022] 图2是本发明实施例提供的一种应用程序违法检测方法流程图；

[0023] 图3是本发明实施例提供的一种应用程序违法检测方法流程图；

[0024] 图4是本发明实施例提供的一种应用程序违法检测装置结构框图；

[0025] 图5是本发明实施例提供的一种设备结构示意图。

具体实施方式

[0026] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部结构。

[0027] 图1是本发明实施例提供的一种应用程序违法检测方法流程图，所述方法可以由应用程序违法检测装置来执行，所述装置可以由软件和/或硬件来实现，所述装置可以配置在沙箱养殖设备中，所述设备中可以安装至少一套包含沙箱环境的操作系统，一套操作系统中可以运行一种或者多种应用程序。所述方法应用于对运行于真实环境中的应用程序进行违法检测的场景中。

[0028] 如图1所示，本发明实施例提供的技术方案包括：

[0029] S110：获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序。

[0030] 本发明实施例提供的方法可以由沙箱养殖设备来执行，该设备可以安装至少一套包含沙箱环境的操作系统。其中，该设备可以安装至少一个磁盘，每个磁盘中安装有至少一套包含沙箱环境的操作系统。

[0031] 在本发明实施例中，可以人为选定(根据自己的检测分析需求)需要进行检测的至少一种应用程序，并按照规定支持的文件传输手段将应用程序的安装包文件上传至沙箱养殖设备的指定位置，沙箱养殖设备获取到应用程序的安装包文件，并基于安装包文件安装应用程序。

[0032] S120：每间隔设定时间执行所述至少一种应用程序的动态运行任务，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，并将所述行为记录进行存储。

[0033] 在本发明实施例中，设定时间可以根据需要进行设置，每间隔设定时间执行至少一种应用程序的动态运行任务可以具体是：每间隔设定时间可以控制一个或者多个应用程序运行。其中，可以尽可能使应用程序展现较多的自身行为。

[0034] 在本发明实施例中，应用程序的行为记录包含文件、网络、通信、系统、应用程序接口(API)调研等行为记录，并将获取到的行为记录进行存储。

[0035] 由此，通过每间隔设定时间执行所述至少一种应用程序的动态运行任务，可以将应用程序的行为记录尽可能多的展现，从而及时发现违法行为。

[0036] S130：从所述行为记录中提取满足设定规则的行为记录。

[0037] 在本发明实施例的一个实施方式中，可选的，所述从所述行为记录中提取满足设定规则的行为记录，包括：从所述行为记录中剔除与所述应用程序的功能相关的行为记录，提取与所述应用程序的功能不相关的行为记录。由于与应用程序功能相关的行为属于应用程序的正常行为，与应用程序的功能不相关的行为往往会出现违法行为，因此，为了减少数据的处理，可以提取与应用程序的功能不相关的行为记录。例如，一个购物应用程序的行为记录中包含了获取通讯录的行为记录，则获取通讯录的行为与购物应用程序的功能不相关，很有可能为违法行为，所以可以在该购物应用程序的行为记录中提取获取通讯录的行为记录。其中，设定规则并不局限与上述还可以根据需要进行设置。

[0038] S140：基于提取的所述行为记录判断所述应用程序是否违法。

[0039] 在本发明实施例中，可以对提取的行为记录进行自动化分析以及其他方式进行综合分析研判，判断应用程序是否违法。

[0040] 在本发明实施例中，可以基于提取的应用程序的一条行为记录判断应用程序是否违法；其中，例如，若一个应用程序的行为记录中存在私自获取通信记录的行为记录，则可以判断该应用程序违法。

[0041] 在本发明实施例中，还可以基于提取的应用程序的多条不同的行为记录判断应用程序是否违法。具体的，可以通过应用程序的多条连续的行为记录判断应用程序是否违法。

[0042] 在本发明实施例中，由于应用程序的违法行为需要运行较长时间才能表现出来，所以对应用程序的动态监测不低于24小时，且最大动态监测时间不超过 100天。

[0043] 在上述实施例的基础上，本发明实施例提供的方法还可以包括基于提取的所述行为记录以及违法行为记录形成分析报告。其中，将提取的行为记录以及违法行为记录形成分析报告，可以将违法行为记录进行标识，将分析报告进行展示或者输出等。

[0044] 在上述实施例的基础上，本发明实施例提供的方法还可以包括：对所述应用程序的动态运行任务、行为记录的提取任务、行为记录的获取任务、应用程序违法判断任务以及分析报告形成任务进行管理。其中，可以对应用程序违法行为检测过程中的不同形式的任务进行在线管理，具体的，可以对应用程序的动态运行任务、行为记录的提取任务、行为记录的获取任务、应用程序违法判断任务以及分析报告形成任务进行创建、删除、加载以及取消等。

[0045] 相关技术中，通过虚拟机沙箱来模拟应用程序的运行环境，并获取应用程序的行为记录来进行违法检测的方法使应用程序运行环境具有一定的局限性。具体的，随着技术的不断更新迭代，很多应用程序具备虚拟环境的检测机制，能够检测自身运行环境，一旦检测到虚拟环境会自动退出，无法通过应用程序的运行状态及行为记录来完成应用程序的违

规违法检测。本发明实施例提供的技术方案应用程序违法检测的方法通过沙箱养殖设备来执行，避免了应用程序运行环境自动退出的情况，从而获取应用程序的行为记录，从而对应用程序违法行为进行检测。

[0046] 在相关技术中的应用程序违法检测方法中，虚拟机沙箱的兼容性不足。具体的，应用程序一般具有多个版本、多种开发框架的情况，虚拟机沙箱无法对多版本、多框架的应用程序进行兼容，导致在运行时出现崩溃、异常退出等现象，导致对应用程序的行为监控、网络监控不够全面。本发明实施例通过在沙箱养殖设备中至少一套包含沙箱环境的操作系统，可以对至少一种类型或者至少一种版本的应用程序进行检测，具有对多版本以及多框架的应用程序进行兼容，更全面的对应用程序进行监控。

[0047] 相关技术中的应用程序违法检测方法，画面渲染技术落后，应用程序的画面渲染技术架构有2D和3D两种形式，游戏类应用程序同时需要虚拟机沙箱兼容2D、3D的渲染方式，相关技术中的虚拟机沙箱由于渲染画面的不支持导致该类应用程序在运行时出现崩溃、退出等异常现象，导致不能对应用程序进行全面的、完整的行为记录，从而无法准确对该类应用程序的进行违法检测。本发明实施例通过配置有至少一条包含沙箱环境的操作系统的沙箱养殖设备执行应用程序违法检测的方法，可以支持应用程序各种形式的画面渲染。

[0048] 本发明实施例提供的技术方案，通过沙箱养殖设备获取至少一种应用程序的安装包文件，并基于安装包文件进行安装应用程序，通过在执行至少一个应用程序的动态运行任务中，获取应用程序的行为记录，并将行为记录进行存储，并提取满足设定规则的行为记录，通过提取的行为记录判断应用程序是否违法，其中，沙箱养殖设备中包含至少一套包含沙箱环境的操作系统。本发明实施例提供的技术方案可以对多种应用程序进行违法检测，可以全面监控应用程序，可以更安全更稳定的实现检测。

[0049] 图2是本发明实施例提供的一种应用程序违法检测方法流程图，在本发明实施例中，可选的，所述每间隔设定时间执行至少一种应用程序的动态运行任务，包括：

[0050] 每间隔设定时间控制对应应用程序运行在对应的操作系统中；

[0051] 相应的，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，包括：

[0052] 在所述应用程序在对应操作系统运行过程中，获取应用程序在对应操作系统中运行的行为记录；其中，不同操作系统的版本或者类型不同。

[0053] 如图2所示，本发明实施例提供的技术方案包括：

[0054] S210：获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序。

[0055] S220：每间隔设定时间控制对应的应用程序运行在对应的操作系统中。

[0056] 在本发明实施例中，每间隔不同的设定时间运行不同的应用程序，不同的应用程序运行在不同的操作系统中，从而可以适应不同版本的应用程序，兼容性更强。

[0057] S230：在所述应用程序在对应操作系统运行过程中，获取应用程序在对应操作系统中运行的行为记录；其中，不同操作系统的版本或者类型不同。

[0058] 在本发明实施例中，应用程序在对应的操作系运行时，具有对应的行为记录，获取应用程序在对应操作系统中运行的行为记录。

[0059] S240:从所述行为记录中提取满足设定规则的行为记录。

[0060] S250:基于提取的所述行为记录判断所述应用程序是否违法。

[0061] 图3是本发明实施例提供的一种应用程序违法检测方法流程图,在本实施例中,可选的,所述每间隔设定时间执行至少一种应用程序的动态运行任务,包括:

[0062] 每间隔设定时间控制多个应用程序同时运行;

[0063] 相应的,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,包括:

[0064] 在所述多个应用程序同时运行过程中,获取多个应用程序的行为记录。

[0065] 如图3所示,本发明实施例提供的技术方案包括:

[0066] S310:获取至少一种应用程序的安装包文件,基于所述安装包文件安装所述应用程序;其中,至少一种应用程序包括至少一种类型的应用程序,或者至少一种版本的应用程序。

[0067] S320:每间隔设定时间控制多个应用程序同时运行。

[0068] 在本发明实施例中,每间隔设定时间可以控制多个应用程序在一个操作系统或者多套操作系统中运行,从而可以实现对多个应用程序是否违法的检测,可以提高检测的效率。

[0069] S330:在所述多个应用程序同时运行过程中,获取多个应用程序的行为记录,并将所述行为记录进行存储。

[0070] S340:从所述行为记录中提取满足设定规则的行为记录。

[0071] S350:基于提取的所述行为记录判断所述应用程序是否违法。

[0072] 为了更清楚的表述本发明实施例提供的技术方案,本发明实施例提供的方法可以包括如下步骤:

[0073] 步骤1:人为选定需要进行分析检测的应用程序,将应用程序上传至沙箱养殖设备中。所谓人为选定就是根据用户自己的分析检测需求,选定应用程序,并按规定支持的文件传输技术手段将应用程序的安装上传至沙箱养殖设备中。

[0074] 步骤2:以步骤1中上传的应用程序为检测主体,开启定时的动态运行任务,让应用程序尽可能多的展现出自身的行为。

[0075] 步骤3:收集步骤2中应用程序的动态行为,包含文件、网络、通信、系统、API调研等行为记录并存储。

[0076] 步骤4:针对步骤3中收集存储的行为记录,配置行为记录的提取规则,并按指定格式提取导出。

[0077] 步骤5:以步骤4提取的应用程序的行为记录为样本进行自动化分析和专家确认的方式进行综合分析研判,确认应用程序是否为违法,并结合违法的行为记录和提取的行为记录形成分析报告。

[0078] 图4是本发明实施例提供的一种应用程序违法检测的装置结构框图,所述装置配置于沙箱养殖设备,所述设备中安装至少一套包含沙箱环境的操作系统,如图4所示,所述装置包括:文件上传模块410、行为收集存储模块420、提取规则配置模块430和行为分析研判模块440。

[0079] 文件上传模块410,用于获取至少一种应用程序的安装包文件,基于所述安装包文

件安装所述应用程序；

[0080] 行为收集存储模块420，用于每间隔设定时间执行至少一种应用程序的动态运行任务，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，并将所述行为记录进行存储；

[0081] 提取规则配置模块430，用于从所述行为记录中提取满足设定规则的行为记录；

[0082] 行为分析研判模块440，用于基于提取的所述行为记录判断所述应用程序是否违法。

[0083] 可选的，所述沙箱养殖设备中安装有至少一个磁盘，所述磁盘中安装有至少一套包含沙箱环境的操作系统。

[0084] 可选的，所述从所述行为记录中提取满足设定规则的行为记录，包括：

[0085] 从所述行为记录中剔除与所述应用程序的功能相关的行为记录，提取与所述应用程序的功能不相关的行为记录。

[0086] 可选的，所述每间隔设定时间执行至少一种应用程序的动态运行任务，包括：

[0087] 每间隔设定时间控制对应应用程序运行在对应的操作系统中；

[0088] 相应的，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，包括：

[0089] 在所述应用程序在对应操作系统运行过程中，获取应用程序在对应操作系统中运行的行为记录；其中，不同操作系统的版本或者类型不同。

[0090] 可选的，所述每间隔设定时间执行至少一种应用程序的动态运行任务，包括：

[0091] 每间隔设定时间控制多个应用程序同时运行；

[0092] 相应的，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，包括：

[0093] 在所述多个应用程序同时运行过程中，获取多个应用程序的行为记录。

[0094] 可选的，所述装置还包括分析报告分析模块450，用于基于提取的所述行为记录以及违法行为记录形成分析报告。

[0095] 可选的，所述装置还包括任务管理模块460，用于对应用程序的动态运行任务、行为记录的提取任务、行为记录的获取任务、应用程序违法判断任务以及分析报告形成任务进行管理。

[0096] 上述装置可执行本发明任意实施例所提供的方法，具备执行方法相应的功能模块和有益效果。

[0097] 图5是本发明实施例提供的一种设备结构示意图，该设备可以是沙箱养殖设备，如图5所示，该设备包括：

[0098] 一个或多个处理器510，图5中以一个处理器510为例；

[0099] 存储器520；

[0100] 所述设备还可以包括：输入装置530和输出装置540。

[0101] 所述设备中的处理器510、存储器520、输入装置530和输出装置540可以通过总线或者其他方式连接，图5中以通过总线连接为例。

[0102] 存储器520作为一种非暂态计算机可读存储介质，可用于存储软件程序、计算机可执行程序以及模块，如本发明实施例中的一种应用程序违法检测方法对应的程序指令/模

块(例如,附图4所示的文件上传模块410、行为收集存储模块420、提取规则配置模块430和行为分析研判模块440)。处理器510通过运行存储在存储器520中的软件程序、指令以及模块,从而执行计算机设备的各种功能应用以及数据处理,即实现上述方法实施例的一种应用程序违法检测方法,即:

[0103] 获取至少一种应用程序的安装包文件,基于所述安装包文件安装所述应用程序;其中,至少一种应用程序包括至少一种类型的应用程序,或者至少一种版本的应用程序;

[0104] 每间隔设定时间执行至少一种应用程序的动态运行任务,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,并将所述行为记录进行存储;

[0105] 从所述行为记录中提取满足设定规则的行为记录;

[0106] 基于提取的所述行为记录判断所述应用程序是否违法。

[0107] 存储器520可以包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一种功能所需要的应用程序;存储数据区可存储根据计算机设备的使用所创建的数据等。此外,存储器520可以包括高速随机存取存储器,还可以包括非暂态性存储器,例如至少一种磁盘存储器件、闪存器件、或其他非暂态性固态存储器件。在一些实施例中,存储器520可选包括相对于处理器510 远程设置的存储器,这些远程存储器可以通过网络连接至终端设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0108] 输入装置530可用于接收输入的数字或字符信息,以及产生与计算机设备的用户设置以及功能控制有关的键信号输入。输出装置540可包括输出接口等。

[0109] 本发明实施例提供了一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现如本发明实施例提供的一种文件处理方法:

[0110] 获取至少一种应用程序的安装包文件,基于所述安装包文件安装所述应用程序;其中,至少一种应用程序包括至少一种类型的应用程序,或者至少一种版本的应用程序;

[0111] 每间隔设定时间执行至少一种应用程序的动态运行任务,在执行所述应用程序动态运行任务过程中,获取应用程序的行为记录,并将所述行为记录进行存储;

[0112] 从所述行为记录中提取满足设定规则的行为记录;

[0113] 基于提取的所述行为记录判断所述应用程序是否违法。

[0114] 可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0115] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括——但不限于——电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者

传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0116] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于——无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0117] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如"C"语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN) —连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0118] 注意，上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解，本发明不限于这里所述的特定实施例，对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此，虽然通过以上实施例对本发明进行了较为详细的说明，但是本发明不仅仅限于以上实施例，在不脱离本发明构思的情况下，还可以包括更多其他等效实施例，而本发明的范围由所附的权利要求范围决定。

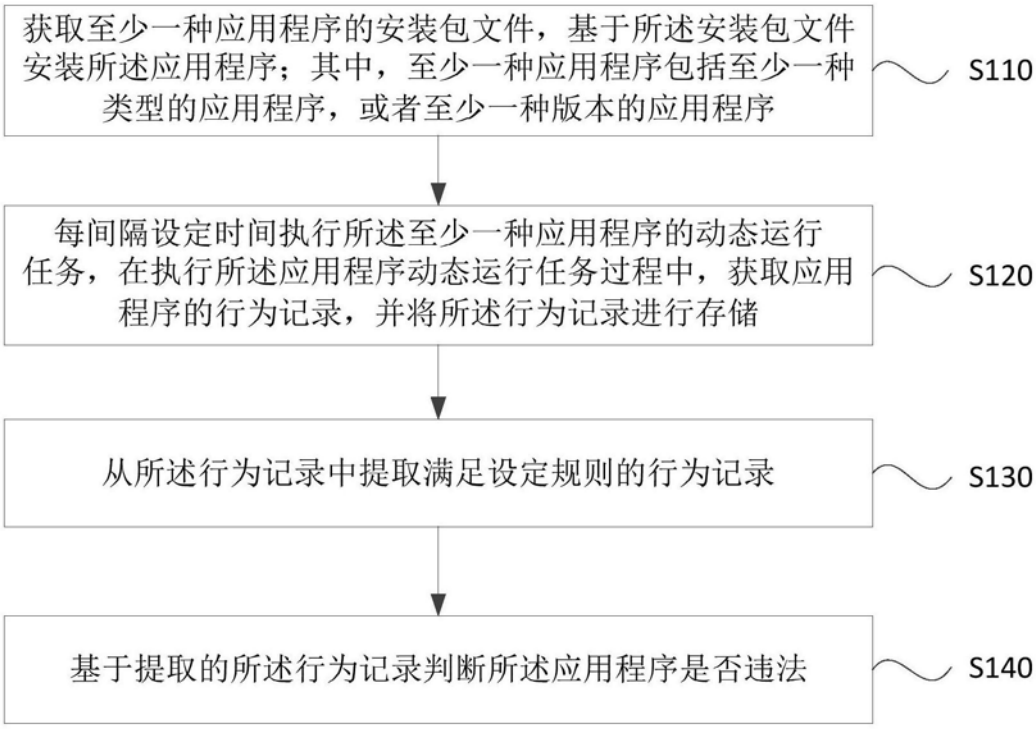

获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序
S110
每间隔设定时间执行所述至少一种应用程序的动态运行任务，在执行所述应用程序动态运行任务过程中，获取应用程序的行为记录，并将所述行为记录进行存储
S120
从所述行为记录中提取满足设定规则的行为记录
S130
基于提取的所述行为记录判断所述应用程序是否违法
S140

图1

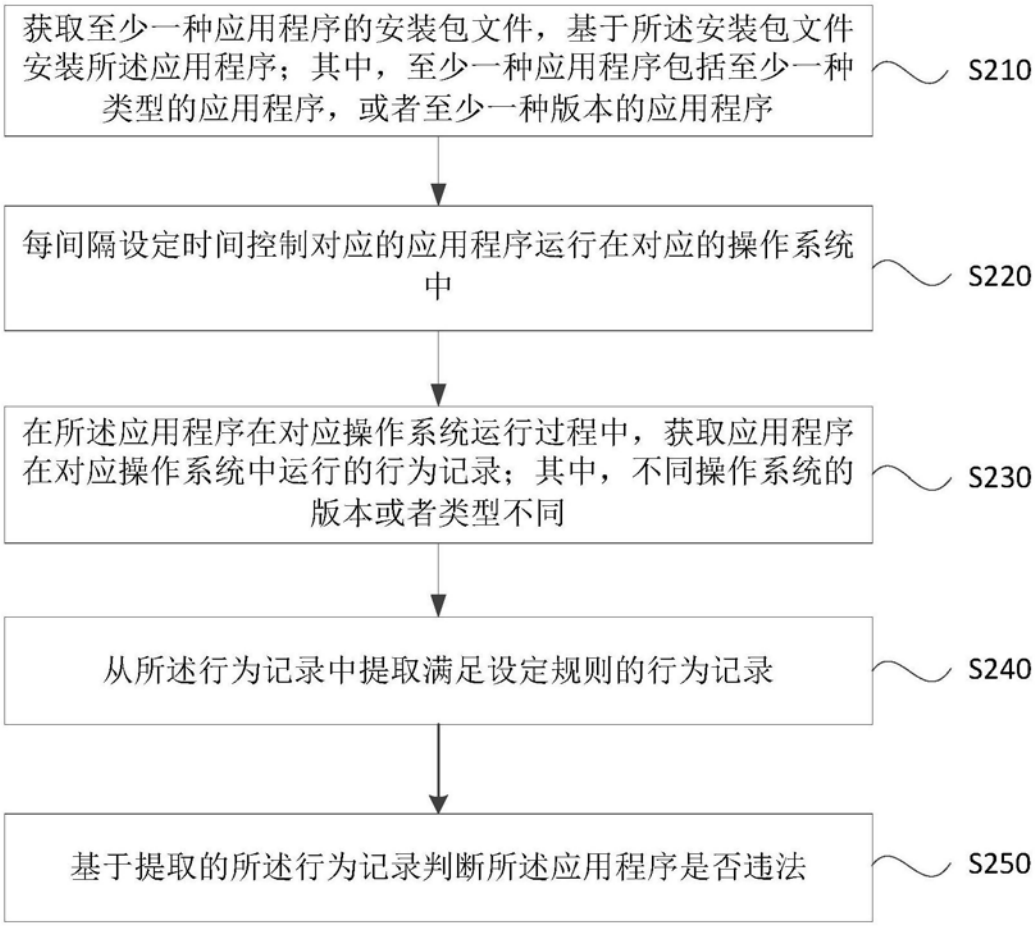

获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序
S210
每间隔设定时间控制对应的应用程序运行在对应的操作系统中
S220
在所述应用程序在对应操作系统运行过程中，获取应用程序在对应操作系统中运行的行为记录；其中，不同操作系统的版本或者类型不同
S230
从所述行为记录中提取满足设定规则的行为记录
S240
基于提取的所述行为记录判断所述应用程序是否违法
S250

图2

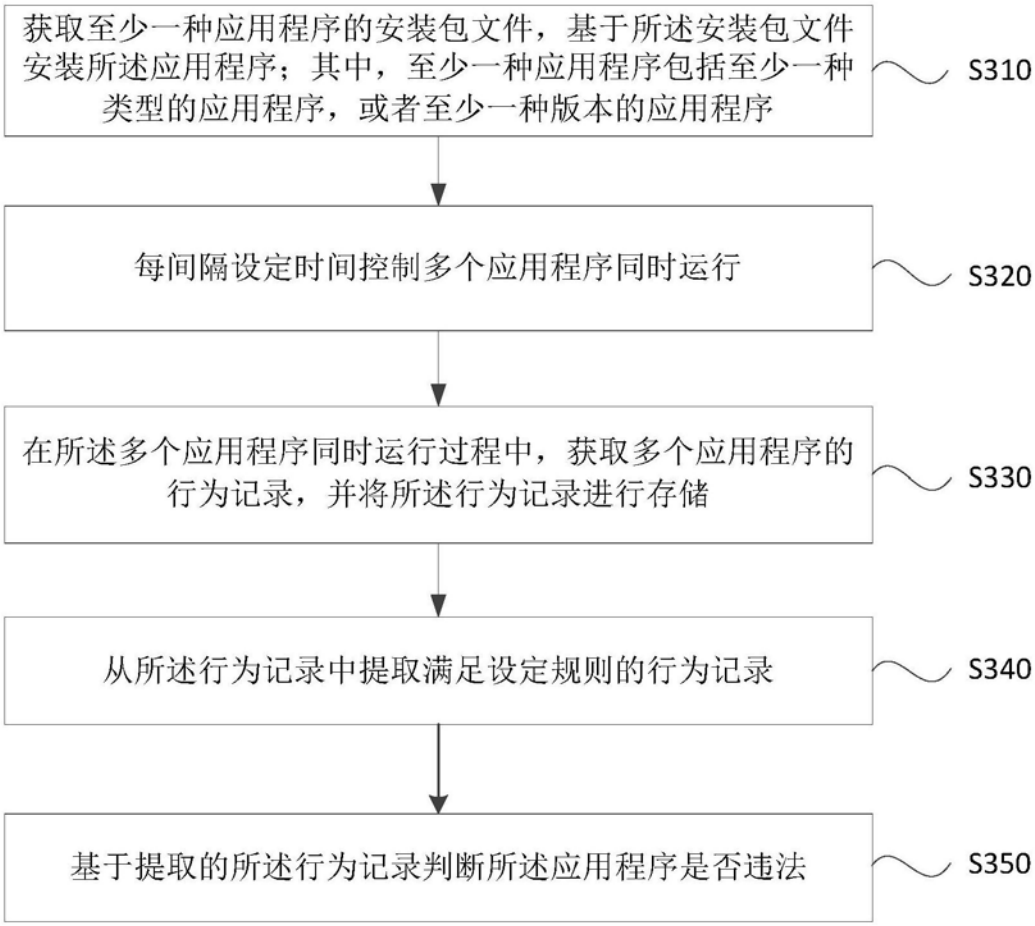

获取至少一种应用程序的安装包文件，基于所述安装包文件安装所述应用程序；其中，至少一种应用程序包括至少一种类型的应用程序，或者至少一种版本的应用程序
S310
每间隔设定时间控制多个应用程序同时运行
S320
在所述多个应用程序同时运行过程中，获取多个应用程序的行为记录，并将所述行为记录进行存储
S330
从所述行为记录中提取满足设定规则的行为记录
S340
基于提取的所述行为记录判断所述应用程序是否违法
S350

图3

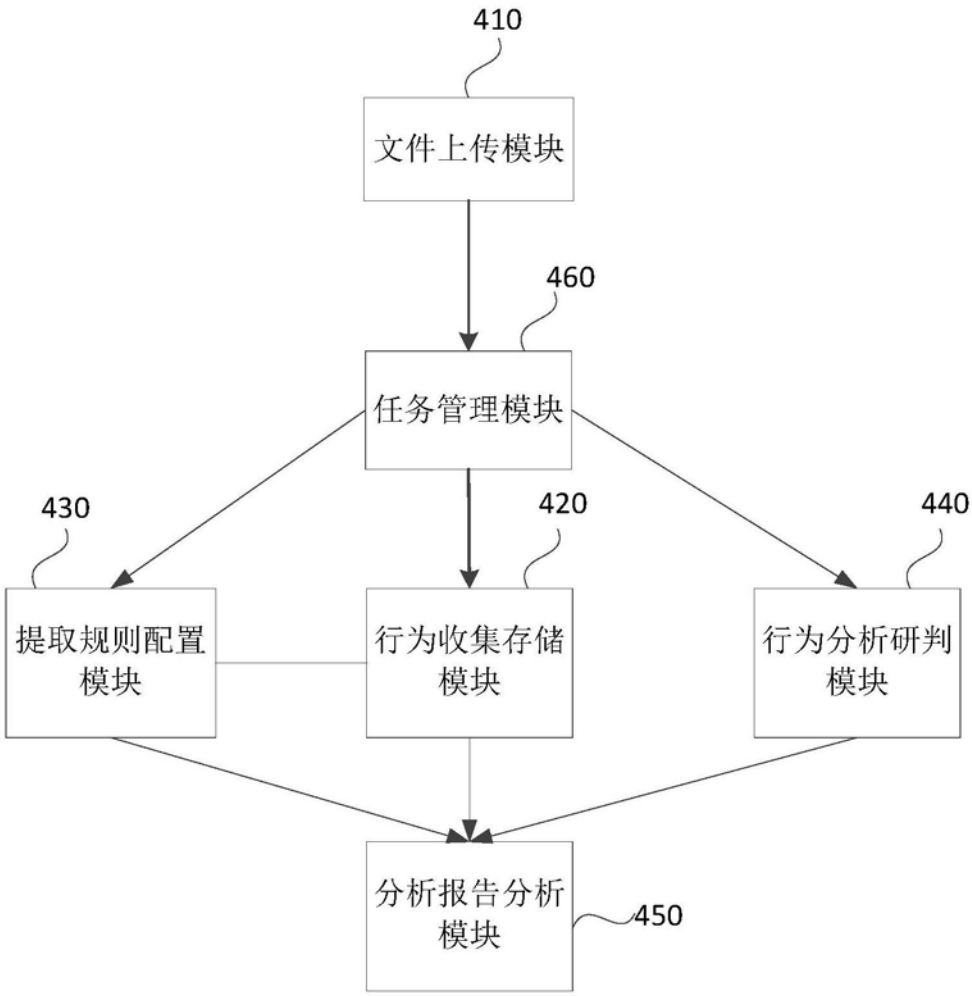

410
文件上传模块
460
任务管理模块
430
420
440
提取规则配置模块
行为收集存储模块
行为分析研判模块
分析报告分析模块
450

图4

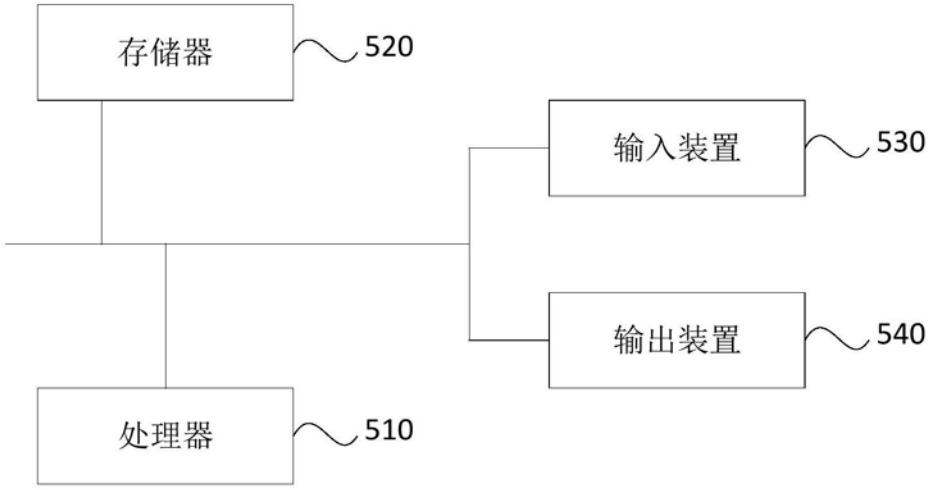

存储器
520
输入装置
530
输出装置
540
处理器
510

图5