(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 105074718 A
(43)申请公布日 2015.11.18

(21)申请号 201480008643.9
(22)申请日 2014.02.06
(30)优先权数据
61/765,461 2013.02.15 US
13/937,462 2013.07.09 US
(85)PCT国际申请进入国家阶段日
2015.08.13
(86)PCT国际申请的申请数据
PCT/US2014/015088 2014.02.06
(87)PCT国际申请的公布数据
WO2014/126779 EN 2014.08.21
(71)申请人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 R·古普塔 M·巴普斯特
M·H·雷沙迪 S·库马尔
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张立达 王英
(51)Int.Cl.
G06F 21/55(2006.01)
H04L 29/06(2006.01)

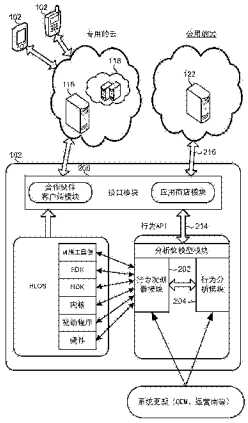
权利要求书7页 说明书22页 附图12页

(54)发明名称

具有多个分析仪模型提供商的移动设备中的在线行为分析引擎

(57)摘要

用于在客户端-云的通信系统中生成数据模型的方法、系统和设备，其可以包括应用机器学习技术来生成描述行为矢量的云语料库的第一类分类器模型。可以分析这种矢量，以在第一类分类器模型中识别具有使得移动设备能够更好地确定移动设备行为是恶意的还是良性的最高概率的因素。基于这种分析，可以生成第二类分类器模型，所述第二类分类器模型将明显较少的因素和数据点识别为与使得移动设备能够基于所确定的因素来更好地确定移动设备行为是恶意的还是良性的有关。基于第二类分类器模型，可以由移动设备（包括贡献行为矢量的设备）生成移动设备分类器模块并使得其可用于下载。



CN 105074718 A

1. 一种用于在移动设备中监视移动设备行为的方法，包括：

在移动设备处理器中从应用下载服务接收行为模型，所接收的行为模型识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；

结合被安装到所述移动设备中的现有的行为分析仪引擎来将所接收的行为模型安装到所述移动设备中；以及

使用所安装的行为模型来监视一个或多个移动设备行为。

2. 根据权利要求 1 所述的方法，其中，接收所述行为模型包括接收软件应用，所述软件应用识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

3. 根据权利要求 1 所述的方法，其中，接收所述行为模型包括接收选自包括 XML、JSON、YAML 和 HTML/XHTML 的组的文件，所述文件识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

4. 根据权利要求 1 所述的方法，其中，接收所述行为模型包括接收有限状态机表示，所述有限状态机表示包括特征至行为类别的映射。

5. 根据权利要求 1 所述的方法，还包括：

利用所接收的行为模型来替代现有的行为模型；以及

将所接收的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所接收的行为模型来这样做。

6. 根据权利要求 1 所述的方法，还包括：

利用包括在所接收的行为模型中的信息来更新现有的行为模型；以及

将所更新的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所更新的行为模型来这样做。

7. 根据权利要求 1 所述的方法，还包括：

从多个公用的网络接收多个行为模型；以及

利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型。

8. 根据权利要求 1 所述的方法，其中，从所述应用下载服务接收所述行为模型包括从以下各项中的一项来接收所述行为模型：

云服务网络服务器；

应用商店服务器；

经由统一资源定位符地址所识别的网络服务器；以及

文件传送协议服务网络服务器。

9. 根据权利要求 1 所述的方法，其中，从所述应用下载服务接收所述行为模型包括：

由所述移动设备处理器访问并认证在线应用商店；

从所述在线应用商店下载可用于下载或更新的行为模型的菜单；

在所述移动设备处理器中接收用户选择输入；

从所述在线应用商店请求对用户选择的行为模型的下载或更新；以及

在所述移动设备的下载缓冲区中接收所请求的、用户选择的行为模型。

10. 根据权利要求 1 所述的方法，其中，结合被安装在所述移动设备中的所述现有的行为分析仪引擎来将所接收的行为模型安装到所述移动设备中包括：

验证所接收的行为模型；

将所验证的行为模型安装到所述移动设备的存储器中；以及

向所述移动设备的观测器模块登记所安装的行为模型。

11. 根据权利要求 1 所述的方法，其中，使用所安装的行为模型来监视一个或多个移动设备行为包括：

在一段时间内观测移动设备行为；

基于在所述一段时间内对移动设备行为的观测，识别与正常的移动设备操作不一致的移动设备行为；

基于被识别为与所述正常的移动设备操作不一致的移动设备行为来生成行为矢量；以及

将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的。

12. 根据权利要求 11 所述的方法，还包括：

接收新的行为模型，所述新的行为模型将额外的因素和数据点识别为与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的相关；

响应于确定所识别的移动设备行为是可疑的，利用包括在所述新的行为模型中的信息来更新所安装的行为模型；以及

将所生成的行为矢量与所更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的。

13. 一种移动计算设备，包括：

移动设备处理器；

用于从应用下载服务接收行为模型的单元，所接收的行为模型识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；

用于结合现有的行为分析仪引擎来安装所接收的行为模型的单元；以及

用于使用所安装的行为模型来监视一个或多个移动设备行为的单元。

14. 根据权利要求 13 所述的移动计算设备，其中，用于接收所述行为模型的单元包括用于接收软件应用的单元，所述软件应用识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

15. 根据权利要求 13 所述的移动计算设备，其中，用于接收所述行为模型的单元包括用于接收 XML 文件的单元，所述 XML 文件识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

16. 根据权利 13 所述的移动计算设备，其中，用于接收所述行为模型的单元包括用于接收有限状态机表示的单元，所述有限状态机表示包括特征至行为类别的映射。

17. 根据权利要求 13 所述的移动计算设备，还包括：

用于利用所接收的行为模型来替代现有的行为模型的单元；以及

用于将所接收的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所接收的行为模型来这样做

的单元。

18. 根据权利要求 13 所述的移动计算设备，还包括：

用于利用包括在所接收的行为模型中的信息来更新现有的行为模型的单元；以及

用于将所更新的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所更新的行为模型来这样做的单元。

19. 根据权利要求 13 所述的移动计算设备，还包括：

用于从多个公用的网络接收多个行为模型的单元；以及

用于利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型的单元。

20. 根据权利要求 13 所述的移动计算设备，其中，用于从所述应用下载服务接收所述行为模型的单元包括用于从以下各项中的一项来接收所述行为模型的单元：

云服务网络服务器；

应用商店服务器；

经由统一资源定位符地址所识别的网络服务器；以及

文件传送协议服务网络服务器。

21. 根据权利要求 13 所述的移动计算设备，其中，用于从所述应用下载服务接收所述行为模型的单元包括：

用于由所述移动设备处理器访问并认证在线应用商店的单元；

用于从所述在线应用商店下载可用于下载或更新的行为模型的菜单的单元；

用于在所述移动设备处理器中接收用户选择输入接收的单元；

用于从所述在线应用商店请求对用户选择的行为模型的下载或更新的单元；以及

用于在下载缓冲区中接收所请求的、用户选择的行为模型的单元。

22. 根据权利要求 13 所述的移动计算设备，其中，用于结合所述现有的行为分析仪引擎来安装所接收的行为模型的单元包括：

用于验证所接收的行为模型的单元；

用于将所验证的行为模型安装到存储器中的单元；以及

用于向观测器模块登记所安装的行为模型的单元。

23. 根据权利要求 13 所述的移动计算设备，其中，用于使用所安装的行为模型来监视一个或多个移动设备行为的单元包括：

用于在一段时间内观测移动设备行为的单元；

用于基于在所述一段时间内对移动设备行为的观测来识别与正常的移动设备操作不一致的移动设备行为的单元；

用于基于被识别为与所述正常的移动设备操作不一致的移动设备行为来生成行为矢量的单元；以及

用于将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的单元。

24. 根据权利要求 23 所述的移动计算设备，还包括：

用于接收新的行为模型的单元，所述新的行为模型将额外的因素和数据点识别为与使

得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的相关；

用于响应于确定所识别的移动设备行为是可疑的，利用包括在所述新的行为模型中的信息来更新所安装的行为模型的单元；以及

用于将所生成的行为矢量与所更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的单元。

25. 一种移动计算设备，包括：

处理器，其被配置有处理器可执行指令，以执行包括以下各项的操作：

从应用下载服务接收行为模型，所接收的行为模型识别与使得所述处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；

结合现有的行为分析仪引擎来安装所接收的行为模型；以及

使用所安装的行为模型来监视一个或多个移动设备行为。

26. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得接收所述行为模型包括接收软件应用，所述软件应用识别与使得所述处理器能够更好地确定移动设备行为是良性的或还是恶意的最相关的因素和数据点。

27. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得接收所述行为模型包括接收 XML 文件，所述 XML 文件识别与使得所述处理器能够更好地确定移动设备行为是良性的或恶意的最相关的因素和数据点。

28. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得接收所述行为模型包括接收有限状态机表示，所述有限状态机表示包括特征至行为类别的映射。

29. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行还包括以下各项的操作：

利用所接收的行为模型来替代现有的行为模型；以及

将所接收的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所接收的行为模型来这样做。

30. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行还包括以下各项的操作：

利用包括在所接收的行为模型中的信息来更新现有的行为模型；以及

将所更新的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所更新的行为模型来这样做。

31. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行还包括以下各项的操作：

从多个公用的网络接收多个行为模型；以及

利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型。

32. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得从所述应用下载服务接收所述行为模型包括从以下各项中的一项来接收所述行为模型：

云服务网络服务器；

应用商店服务器；

经由统一资源定位符地址所识别的网络服务器；以及

文件传送协议服务网络服务器。

33. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得从所述应用下载服务接收所述行为模型包括：

访问并认证在线应用商店；

从所述在线应用商店下载可用于下载或更新的行为模型的菜单；

接收用户选择输入；

从所述在线应用商店请求对用户选择的行为模型的下载或更新；以及

在下载缓冲区中接收所请求的、用户选择的行为模型。

34. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得结合所述现有的行为分析仪引擎来安装所接收的行为模型包括：

验证所接收的行为模型；

将所验证的行为模型安装到存储器中；以及

向观测器模块登记所安装的行为模型。

35. 根据权利要求 25 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行操作来使得使用所安装的行为模型来监视一个或多个移动设备行为包括：

在一段时间内观测移动设备行为；

基于在所述一段时间内对移动设备行为的观测来识别与正常的移动设备操作不一致的移动设备行为；

基于被识别为与所述正常的移动设备操作不一致的所识别的移动设备行为来生成行为矢量；以及

将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的。

36. 根据权利要求 35 所述的移动计算设备，其中，所述处理器被配置有处理器可执行指令，以执行还包括以下各项的操作：

接收新的行为模型，所述新的行为模型将额外的因素和数据点识别为与使得所述处理器能够更好地确定行为是良性的还是恶意的相关；

当确定所识别的移动设备行为是可疑的时，利用包括在所述新的行为模型中的信息来更新所安装的行为模型；以及

将所生成的行为矢量与所更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的。

37. 一种具有存储于其上的处理器可执行软件指令的非暂时性计算机可读存储介质，所述处理器可执行软件指令被配置为使移动设备处理器执行包括以下各项的操作：

从应用下载服务接收行为模型，所接收的行为模型识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；

结合现有的行为分析仪引擎来安装所接收的行为模型；以及

使用所安装的行为模型来监视一个或多个移动设备行为。

38. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可

执行软件指令被配置为使所述移动设备处理器执行操作来使得接收所述行为模型包括接收软件应用，所述软件应用识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

39. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行操作来使得接收所述行为模型包括接收 XML 文件，所述 XML 文件识别与使得所述移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

40. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行操作来使得接收所述行为模型包括接收有限状态机表示，所述有限状态机表示包括特征至行为类别的映射。

41. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行还包括以下各项的操作：

利用所接收的行为模型来替代现有的行为模型；以及

将所接收的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所接收的行为模型来这样做。

42. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行还包括以下各项的操作：

利用包括在所接收的行为模型中的信息来更新现有的行为模型；以及

将所更新的行为模型链接到所述现有的行为分析仪引擎，以便当所述现有的行为分析仪引擎执行分析操作时，所述现有的行为分析仪引擎使用所更新的行为模型来这样做。

43. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行还包括以下各项的操作：

从多个公用的网络接收多个行为模型；以及

利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型。

44. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行操作来使得从所述应用下载服务接收所述行为模型包括从以下各项中的一项来接收所述行为模型：

云服务网络服务器；

应用商店服务器；

经由统一资源定位符地址所识别的网络服务器；以及

文件传送协议服务网络服务器。

45. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行操作来使得从所述应用下载服务接收所述行为模型包括：

访问并认证在线应用商店；

从所述在线应用商店下载可用于下载或更新的行为模型的菜单；

接收用户选择输入；

从所述在线应用商店请求对用户选择的行为模型的下载或更新；以及

在下载缓冲区中接收所请求的、用户选择的行为模型。

46. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行操作来使得结合所述现有的行为分析仪引擎来安装所接收的行为模型包括：

验证所接收的行为模型；

将所验证的行为模型安装到存储器中；以及

向观测器模块登记所安装的行为模型。

47. 根据权利要求 37 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行操作来使得使用所安装的行为模型来监视一个或多个移动设备行为包括：

在一段时间内观测移动设备行为；

基于在所述一段时间内对移动设备行为的观测来识别与正常的移动设备操作不一致的移动设备行为；

基于被识别为与所述正常的移动设备操作不一致的移动设备行为来生成行为矢量；以及

将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的。

48. 根据权利要求 47 所述的非暂时性计算机可读存储介质，其中，所存储的处理器可执行软件指令被配置为使所述移动设备处理器执行还包括以下各项的操作：

接收新的行为模型，所述新的行为模型将额外的因素和数据识别为与使得所述移动设备处理器能够更好地确定行为是良性的还是恶意的相关；

响应于确定所识别的移动设备行为是可疑的，利用包括在所述新的行为模型中的信息来更新所安装的行为模型；以及

将所生成的行为矢量与所更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的。

具有多个分析仪模型提供商的移动设备中的在线行为分析引擎

[0001] 相关申请

[0002] 本申请要求于2013年2月15日递交的、名称为“On-Line Behavioral Analysis Engine in Mobile Device with Multiple Analyzer Model Providers”的美国临时专利申请No.61/765,461的优先权的权益，针对所有的目的通过引用方式将其整体内容并入本文。

背景技术

[0003] 在过去的若干年里，蜂窝和无线通信技术已爆炸性地增长。更好的通信、硬件、更大的网络和更可靠的协议加剧了这种增长。无线服务提供商现在能够给他们的客户提供不断扩大的大量特征和服务，并且为用户提供前所未有的对信息、资源和通信的访问级别。为了与这些服务增强保持同步，移动电子设备（例如，蜂窝电话、平板、膝上型计算机等）比以往任何时候都变得更加强大和复杂。这种复杂性已经为恶意软件、软件冲突、硬件故障和其它类似的错误或现象创造了负面地影响移动设备的长期的与持久的性能以及功率使用级别的新机会。因此，识别并校正可能负面地影响移动设备的长期的与持久的性能和功率使用级别的情况和/或移动设备行为，对于用户来说是受益的。

发明内容

[0004] 各个方面包括在移动设备中监视移动设备行为的方法，所述方法可以包括从应用下载服务接收行为模型，所述行为模型识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；结合被安装在移动设备中的现有的行为分析仪引擎来将所接收的行为模型安装到移动设备中；以及使用所安装的行为模型来监视一个或多个移动设备行为。

[0005] 在一个方面，接收行为模型可以包括接收软件应用，所述软件应用识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，接收行为模型可以包括接收XML、JSON、YAML、HTML/XHTML或其它标记语言文件，所述XML、JSON、YAML、HTML/XHTML或其它标记语言文件识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，接收行为模型可以包括接收有限状态机表示，所述有限状态机表示可以包括特征至行为类别的映射。

[0006] 在又一方面，该方法可以包括用所接收的行为模型替代现有的行为模型。在一个方面，该方法还可以包括将所接收的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用所接收的行为模型来这样做。

[0007] 在又一方面，该方法可以包括通过利用包括在所接收的行为模型中的信息来对现有的行为模型进行扩展来更新现有的行为模型；和/或将更新的行为模型链接到现有的行

为分析仪引擎，以便当执行分析操作时，现有的行为分析仪引擎使用更新的行为模型来这样做。

[0008] 在又一方面，该方法可以包括从多个公用的网络接收多个行为模型；以及利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型。

[0009] 在又一方面，从应用下载服务接收行为模型可以包括从云服务网络服务器、应用商店服务器、经由统一资源定位符地址所识别的网络服务器、以及文件传送协议服务网络服务器中的一个来接收行为模型。

[0010] 在又一方面，从应用下载服务接收行为模型可以包括由移动设备处理器访问并认证在线应用商店；从在线应用商店下载可用于下载或更新的行为模型的菜单；在移动设备处理器中接收用户选择输入；从在线应用商店请求对用户选择的行为模型的下载或更新；以及在移动设备的下载缓冲区中接收所请求的、用户选择的行为模型。

[0011] 在又一方面，结合被安装到移动设备中的现有的行为分析仪引擎来将所接收的行为模型安装到移动设备中可以包括验证所接收的行为模型；将所验证的行为模型安装到移动设备的存储器中；以及向移动设备的观测器模块和／或分析仪模块登记所安装的行为模型。

[0012] 在又一方面，使用所安装的行为模型来监视一个或多个移动设备行为可以包括在一段时间内观测移动设备行为；基于在一段时间内对移动设备行为的观测，识别与正常的移动设备操作不一致的移动设备行为；基于被识别为与正常的移动设备操作不一致的移动设备行为来生成行为矢量；以及将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的。在又一方面，该方法可以包括接收新的行为模型，所述新的行为模型将额外的因素和数据点识别为与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的有关；响应于确定所识别的移动设备行为是可疑的，利用包括在新的行为模型中的信息来更新所安装的行为模型；以及将所生成的行为矢量与所更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的。

[0013] 又一方面包括具有移动设备处理器的计算设备；用于从应用下载服务接收行为模型的单元，所述行为模型识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；用于结合现有的行为分析仪引擎来安装所接收的行为模型的单元；以及用于使用所安装的行为模型来监视一个或多个移动设备行为的单元。

[0014] 在一个方面，用于接收行为模型的单元可以包括用于接收软件应用的单元，所述软件应用识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，用于接收行为模型的单元可以包括用于接收 XML 文件的单元，所述 XML 文件识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，用于接收行为模型的单元可以包括用于接收有限状态机表示的单元，所述有限状态机表示可以包括特征至行为类别的映射。

[0015] 在又一方面，计算设备可以包括用于用所接收的行为模型来替代现有的行为模型的单元；以及用于将所接收的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用所接收的行为模型来这样做的单

元。

[0016] 在又一方面，计算设备可以包括用于利用包括在所接收的行为模型中的信息来更新现有的行为模型的单元；以及用于将更新的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用更新的行为模型来这样做的单元。

[0017] 在又一方面，计算设备可以包括用于从多个公用的网络接收多个行为模型的单元；以及用于利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型的单元。

[0018] 在又一方面，用于从应用下载服务接收行为模型的单元可以包括用于从云服务网络服务器、应用商店服务器、经由统一资源定位符地址所识别的网络服务器、以及文件传送协议服务网络服务器中的一个来接收行为模型的单元。

[0019] 在又一方面，用于从应用下载服务接收行为模型可以包括用于由移动设备处理器访问并认证在线应用商店的单元；用于从在线应用商店下载可用于下载或更新的行为模型的菜单的单元；用于在移动设备处理器中接收用户选择输入的单元；用于从在线应用商店请求对用户选择的行为模型的下载或更新的单元；以及用于在下载缓冲区中接收所请求的、用户选择的行为模型的单元。

[0020] 在又一方面，用于结合现有的行为分析仪引擎来安装所接收的行为模型的单元可以包括用于验证所接收的行为模型的单元；用于将所认证验证的行为模型安装到存储器中的单元；以及用于向观测器模块登记所安装的行为模型的单元。

[0021] 在又一方面，用于使用所安装的行为模型来监视一个或多个移动设备行为的单元可以包括用于在一段时间内观测移动设备行为的单元；用于基于在一段时间内对移动设备行为的观测来识别与正常的移动设备操作不一致的移动设备行为的单元；用于基于被识别为与正常的移动设备操作不一致的移动设备行为来生成行为矢量的单元；以及用于将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的单元。在又一方面，计算设备可以包括用于接收新的行为模型的单元，所述新的行为模型识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的有关的额外的因素和数据点；用于响应于确定所识别的移动设备行为是可疑的，利用包括在新的行为模型中的信息来更新所安装的行为模型的单元；以及用于将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的单元。

[0022] 又一方面包括具有被配置有处理器可执行指令，以执行包括以下操作的处理器的移动计算设备：从应用下载服务接收行为模型，所述行为模型识别与使得处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；结合现有的行为分析仪引擎来安装所接收的行为模型；以及使用所安装的行为模型来监视一个或多个移动设备行为。

[0023] 在一个方面，处理器可以被配置有处理器可执行指令，以执行操作来使得接收行为模型可以包括接收软件应用，所述软件应用识别与使得处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，处理器可以被配置有处理器可执行指令，以执行操作来使得接收行为模型可以包括接收 XML 文件，所述 XML 文件识别

与使得处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，处理器可以被配置有处理器可执行指令，以执行操作来使得接收行为模型可以包括接收有限状态机表示，所述有限状态机表示包括特征至行为类别的映射。

[0024] 在又一方面，处理器可以被配置有处理器可执行指令，以执行包括以下的操作：用所接收的行为模型来替代现有的行为模型；以及将所接收的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用所接收的行为模型来这样做。

[0025] 在又一方面，处理器可以被配置有处理器可执行指令，以执行包括以下的操作：利用包括在所接收的行为模型中的信息来更新现有的行为模型；以及将所更新的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用更新的行为模型来这样做。

[0026] 在又一方面，处理器可以被配置有处理器可执行指令，以执行包括以下的操作：从多个公用的网络接收多个行为模型；以及利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型。

[0027] 在又一方面，处理器可以被配置有处理器可执行指令，以执行操作来使得从应用下载服务接收行为模型可以包括从云服务网络服务器、应用商店服务器、经由统一资源定位符地址所识别的网络服务器、以及文件传送协议服务网络服务器中的一个来接收行为模型。

[0028] 在又一方面，处理器可以被配置有处理器可执行指令，以执行操作来使得从应用下载服务接收行为模型可以包括访问并认证在线应用商店；从在线应用商店下载可用于下载或更新的行为模型的菜单；接收用户选择输入；从在线应用商店请求对用户选择的行为模型的下载或更新；以及在下载缓冲区中接收所请求的、用户选择的行为模型。

[0029] 在又一方面，处理器可以被配置有处理器可执行指令，以执行操作来使得结合现有的行为分析仪引擎来安装所接收的行为模型可以包括验证所接收的行为模型；将所验证的行为模型安装到存储器中；以及向观测器模块登记所安装的行为模型。

[0030] 在又一方面，处理器可以被配置有处理器可执行指令，以执行操作来使得使用所安装的行为模型来监视一个或多个移动设备行为可以包括在一段时间内观测移动设备行为；基于在一段时间内对移动设备行为的观测来识别与正常的移动设备操作不一致的移动设备行为；基于被识别为与正常的移动设备操作不一致的移动设备行为来生成行为矢量；以及将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的。在又一方面，处理器可以被配置有处理器可执行指令，以执行包括以下的操作：接收新的行为模型，所述新的行为模型将额外的因素和数据点识别为与使得处理器能够更好地确定移动设备行为是良性的还是恶意的有关；响应于确定所识别的移动设备行为是可疑的，利用包括在新的行为模型中的信息来更新所安装的行为模型；以及将所生成的行为矢量与更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的。

[0031] 又一方面包括具有存储于其上的处理器可执行软件指令的非暂时性计算机可读存储介质，所述处理器可执行软件指令被配置为使移动设备处理器执行包括以下各项的操作：从应用下载服务接收行为模型，所接收的行为模型识别与使得移动设备处理器能够更

好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点；结合现有的行为分析仪引擎来安装所接收的行为模型；以及使用所安装的行为模型来监视一个或多个移动设备行为。

[0032] 在一个方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作来使得接收行为模型可以包括接收软件应用，所述软件应用识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作来使得接收行为模型可以包括接收 XML 文件，所述 XML 文件识别与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作来使得接收行为模型可以包括接收有限状态机表示，所述有限状态机表示包括特征至行为类别的映射。

[0033] 在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行包括以下各项的操作：用所接收的行为模型来替代现有的行为模型；以及将所接收的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用所接收的行为模型来这样做。在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行包括以下的操作：利用包括在所接收的行为模型中的信息来更新现有的行为模型；以及将更新的行为模型链接到现有的行为分析仪引擎，以便当现有的行为分析仪引擎执行分析操作时，现有的行为分析仪引擎使用更新的行为模型来这样做。

[0034] 在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行包括以下各项的操作：从多个公用的网络接收多个行为模型；以及利用包括在所接收的多个行为模型中的一个或多个行为模型中的信息来更新至少一个现有的行为模型。

[0035] 在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作，以使得从应用下载服务接收行为模型可以包括从云服务网络服务器、应用商店服务器、经由统一资源定位符地址所识别的网络服务器、以及文件传送协议服务网络服务器中的一个来接收行为模型。

[0036] 在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作，以使得从应用下载服务接收行为模型可以包括访问并认证在线应用商店；从在线应用商店下载可用于下载或更新的行为模型的菜单；接收用户选择输入；从在线应用商店请求对用户选择的行为模型的下载或更新；以及在下载缓冲区中接收所请求的、用户选择的行为模型。

[0037] 在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作，以使得结合现有的行为分析仪引擎来安装所接收的行为模型可以包括验证所接收的行为模型；将所验证的行为模型安装到存储器中；以及向观测器模块登记所安装的行为模型。

[0038] 在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行操作，以使得使用所安装的行为模型来监视一个或多个移动设备行为可以包括在一段时间内观测移动设备行为；基于在一段时间内对移动设备行为的观测来识别与正常的移动设备操作不一致的移动设备行为；基于被识别为与正常的移动设备操作不一致的移动设备行

为来生成行为矢量；以及将所生成的行为矢量与所安装的行为模型进行比较，以确定所识别的移动设备行为是良性的、可疑的还是恶意的。在又一方面，所存储的处理器可执行软件指令可以被配置为使移动设备处理器执行包括以下的操作：接收新的行为模型，所述新的行为模型将额外的因素和数据点识别为与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的有关；响应于确定所识别的移动设备行为是可疑的，利用包括在新的行为模型中的信息来更新所安装的行为模型；以及将所生成的行为矢量与更新的行为模型进行比较，以更好地确定所识别的可疑的移动设备行为是良性的还是恶意的。

附图说明

[0039] 被并入本文并构成本说明书的一部分的附图示出了本发明的示例性的方面，并且与上面给出的概括描述和下面给出的详细描述一起用来解释本发明的特征。

[0040] 图 1 是示出了适合于用在各个方面的示例性电信系统的网络组件的通信系统框图。

[0041] 图 2A-2B 是示出了在被配置为确定特定的移动设备行为、软件应用或进程是性能恶化的、可疑的还是良性的方面的移动设备中的示例性逻辑组件和信息流程的框图。

[0042] 图 3 是示出了在被配置为根据一个方面执行动态和自适应观测的观测器模块中的示例性逻辑组件和信息流程的框图。

[0043] 图 4 是示出了在根据另一方面实现观测器后台程序 (daemons) 的计算系统中的逻辑组件和信息流程的框图。

[0044] 图 5 是示出了用于在移动设备上执行自适应观测的一个方面的方法的过程流程图。

[0045] 图 6 是示出了用于从应用商店向移动设备下载行为分析模块 / 应用的方面方法的过程流程图。

[0046] 图 7 是示出了用于下载并使用行为分析模型的方面方法的过程流程图。

[0047] 图 8 是示出了用于下载并使用替换行为分析模块 / 应用的方面移动设备方法的过程流程图。

[0048] 图 9 是示出了用于从应用商店向移动设备下载行为分析模块 / 应用的方面移动设备方法的过程流程图。

[0049] 图 10 是示出了用于从多个公用网络下载多个行为分析模块 / 应用的方面移动设备方法的过程流程图。

[0050] 图 11 是示出了用于使用从公用网络所接收的更新的行为模型来执行行为分析操作的方面移动设备方法的过程流程图。

[0051] 图 12 是适合于用在一个方面的移动设备的组件的框图。

[0052] 图 13 是适合于用在一个方面的服务器设备的组件的框图。

具体实施方式

[0053] 将参照附图来详细地描述各个方面。在任何可能的情况下，贯穿附图将使用相同的附图标记来指代相同的或相似的部分。对特定示例和实现方式所做的参考是出于说明性的目的，并不旨在限制本发明或权利要求的范围。

[0054] 在本文使用单词“示例性的”来表示“充当示例、实例或说明”的意思。本文被描述为“示例性的”任何实现方式均不必被解释为比其它实现方式优选或有利。

[0055] 各个方面提供了用于对经常随着时间降低移动设备的性能、功率使用级别、网络的使用级别、安全和/或隐私的情况和/或移动设备行为进行有效地识别、分类、建模、防止和/或校正。与如果所有这些分析都在每个移动设备内独立地完成相比，通过将关于这种情况和校正动作的信息存储到诸如“云”的中央数据库中并且使得移动设备能够存取并使用存储在该数据库中的信息，各个方面使得移动设备能够更快且用更低的功耗来对性能限制和不期望的操作情况作出反应。此外，对方面应用程序接口(API)和模块的使用在不同的时间和/或以不同的频率进行以下各项：启用以下各项的通信：行为模型、分类器和移动设备与多个第三方之间的行为信息、应用商店、公用网络、专用网络、原始的设备制造商(OEM)、电信服务提供商以及其它，并且使得移动设备行为分析引擎能够被频繁地更新；与多个行为或分析仪模型提供商合作，和/或从一个或多个源(例如，多个云服务)接收更新的模型。尤其是，方面API和模块使得能够从互联网或诸如“应用商店”(例如，Apple®应用商店、Windows®商店、Google®市场等)的应用下载服务、云服务或服务器、URL地址、FTP服务器等下载行为模型。在各个方面，移动设备可以基于从应用下载服务(例如，与移动设备中的客户端模块相通信的云服务器)所接收的信息或模型来更新或替换预先存在的或所生成的行为模型。

[0056] 许多不同的蜂窝与移动通信服务和标准在未来是可用的或是被预期的，所有的这些服务和标准都可以实现并从各个方面受益。这些服务和标准包括：例如，第三代合作伙伴计划(3GPP)、长期演进(LTE)系统、第三代无线移动通信技术(3G)、第四代无线移动通信技术(4G)、全球移动通信系统(GSM)、通用移动电信系统(UMTS)、3GSM、通用分组无线业务(GPRS)、码分多址(CDMA)系统(例如，cdmaOne、CDMA1020TM)、增强型数据速率GSM演进技术(EDGE)、高级移动电话系统(AMPS)、数字AMPS(IS-136/TDMA)、演进数据优化(EV-DO)、数字增强型无绳通信(DECT)、微波接入全球性互通(WiMAX)、无线局域网(WLAN)、Wi-Fi保护接入I&II(WPA、WPA2)以及整体数字增强网络(iden)。这些技术中的每一种都涉及，例如，语音、数据、信令和/或内容消息的发送与接收。应当理解的是，对与单独的电信标准或技术有关的术语和/或技术细节的任何参考都是仅出于说明性的目的，并不旨在将权利要求的范围限制于特定的通信系统或技术，除非其在权利要求的语言中被明确地列举。

[0057] 本文可互换地使用术语“移动计算设备”和“移动设备”来指代蜂窝电话、智能手机、个人的或移动的多媒体播放器、个人数字助理(PDA)、膝上型计算机、平板计算机、智能本、超级本、掌上计算机、无线电子邮件接收机、启用多媒体互联网的蜂窝电话、无线游戏控制器，以及包括存储器、其性能重要的可编程处理器、并且在电池供电下操作使得节约用电方法是有好处的类似的个人电子设备中的任一种或全部。虽然各个方面对于具有有限的资源并且运行在电池上的移动计算设备(诸如智能手机)来说尤其有用，但是，方面通常在包括处理器并执行应用程序的任意电子设备(例如连接到物联网(IOT)的设备)中有用。

[0058] 本文使用术语“性能恶化”来指代各种各样不期望的移动设备操作和特性，例如，较长的处理时间、较慢的实时响应能力、较低的电池寿命、专用数据的损失、恶意的经济活动(例如，发送未被授权的高价的SMS消息)、拒绝服务(DoS)、与强占移动设备或利用电话

来秘密监视或僵尸网络活动等有关的操作。

[0059] 通常，移动设备的性能和电源效率随时间降低。最近，防病毒公司（例如，McAfee、Symantec 等）已经开始在市场上出售目的在于减缓这种恶化的移动防病毒、防火墙和加密产品。然而，这些方案中的许多方案都依赖于移动设备上的计算密集型扫描引擎的定期执行，这可能消耗许多移动设备的处理资源和电池资源、使减缓或致使移动设备无用的时间段延长、和 / 或以别的方式降低用户的体验。此外，这些方案通常被限于检测已知的病毒和恶意软件，而不处理随着时间经常结合以促成移动设备的恶化的多个复杂因素和 / 或相互作用（例如，当性能恶化不是由病毒或恶意软件所引起的时候）。针对这些和其它的原因，现有的防病毒、防火墙和加密产品没有为识别可能随着时间促成移动设备的恶化的大量因素提供足够的解决方案、没有为防止移动设备的恶化提供足够的解决方案、或者没有为有效地将老化的移动设备恢复到它的原始状况提供足够的解决方案。

[0060] 移动设备是具有相对有限的处理资源、存储资源和能源资源的受限系统。现代的移动设备还是复杂的系统，并且存在随着时间可能促成移动设备的性能恶化和功率消耗级别的降低的各种各样的因素，包括粗劣设计的软件应用、恶意软件、病毒、碎片化的存储器、后台处理等。由于这些因素的数量、多样性和复杂性，对可能降低现代移动设备的复杂的且资源受限的系统的性能和 / 或功率消耗级别的所有的各种进程、行为或因素（或它们的组合）进行评估经常是不可行的。

[0061] 鉴于这些事实，为了提供更好的性能，各个方面包括移动设备，所述移动设备被配置为与任意数量的公用的和专用的云服务 / 网络（例如，应用商店、防病毒合作伙伴、安全合作伙伴等）、或公用的和专用的云服务 / 网络的任意组合结合在一起工作，以智能地且有效地识别可能随着时间促成移动设备的性能恶化和功率消耗级别降低的因素。这种云服务可以提供计算的卸载、众包 (crowd sourcing) 以及提供其它的益处，以便移动设备可以识别关于移动设备的性能恶化的因素，而不消耗移动设备的过量的处理资源、存储资源或能源。

[0062] 在一方面，移动设备的观测器进程、后台程序、模块或子系统（本文统称为“模块”）可以在移动设备系统的各个层级处用器械装备或协调各个应用程序接口 (API)、寄存器、计数器或其它可用的信息或组件（本文统称为“器械装备的组件”），并且从器械装备的组件收集行为信息。在一个方面，移动设备还可以包括分析仪模块和 / 或分类器模块。观测器模块可以（例如，经由存储器写入操作、函数调用等）将所收集的行为信息传送给移动设备的分类器模块和 / 或分析仪模块（例如，经由存储器写入操作等），所述分类器模块和 / 或分析仪模块可以对所收集的行为信息进行分析和 / 或分类；生成行为矢量；基于行为矢量和从各个其它的移动设备子系统所收集的信息来生成空间相关和 / 或时间相关；并且确定特定的移动设备行为、软件应用或进程是良性的、可疑的、恶意的还是性能恶化的。

[0063] 移动设备的分析仪模块和 / 或分类器模块可以被配置为执行实时分析操作，其可以包括完成、执行、和 / 或将数据、算法和 / 或模型应用于由观测器模块所收集的实时行为信息，以确定移动设备行为是良性的、可疑的、恶意的还是性能恶化的。由分析仪模块和 / 或分类器模块所应用的数据、算法和 / 或模型可以被预先安装到移动设备上，在移动设备上生成，和 / 或从任意数量的公用的和专用的云服务 / 网络或公用的和专用的云服务 / 网络的任意组合来下载，或由任意数量的公用的和专用的云服务 / 网络或公用的和专用的云

服务 / 网络的任意组合所升级，所述公用的和专用的云服务 / 网络包括第三方供应商和应用商店。可以在安装或更新进程中将所下载的数据、算法和 / 或模型安装到或链接到分析仪模块和 / 或分类器模块，以便当分析仪模块和 / 或分类器模块执行实时的分析操作时，所述分析仪模块和 / 或分类器模块使用所下载的数据、算法和 / 或模型来这样做。

[0064] 各个方面可以包括移动设备，所述移动设备被配置有接口模块，所述的接口模块促进移动设备与一个或多个专用的和 / 或公用的网络和服务（例如，应用下载服务）之间的通信并且使得分析仪模块能够与多个云服务结合在一起工作。接口模块还通过使得移动设备能够与一个或多个安全的云合作伙伴、在移动设备中所生成的模型以及来自其它合作伙伴（例如，OEM、网络运营商等）的模型一起工作来增强移动设备的安全性和可靠性。接口模块还使得移动设备能够下载或以别的方式接收对链接至分析仪模块和分类器模块的数据、算法和 / 或模型的增量更新。

[0065] 接口模块还可以提供应用级的下载机制，所述应用级的下载机制允许移动设备被分发有观测器模块和工作分析仪算法，并且能够在稍后的时间接收从应用下载服务或第三方所下载的机器学习或行为模型。这些方面使得移动设备的用户能够购买最能满足用户的安全性和偏好的最新的和有针对性的模型。同样地，这些方面使得能够增量地和 / 或通过已经被部署的用于通过应用商店和其它第三方软件更新机制来更新应用的机制来更新所安装的模型。以这种方式，可以使用现有的软件分发和支持的基础设施，将移动设备配置为具有最新的数据分析器模块和 / 或分类器模块，而不消耗移动设备的过量的处理资源、存储资源或能源。

[0066] 在一个方面，接口模块可以被配置为使得应用下载服务（例如，云网络中的服务器、应用商店等）能够向移动设备发送数据模型 / 行为模型。移动设备可以接收并实现、应用或使用数据模型 / 行为模型来识别并校正可疑的、恶意的或性能恶化的移动设备行为。这可以通过移动设备替换或更新移动设备的现有的数据 / 行为模型的全部或部分、并且将新的模型 / 更新的模型应用于移动设备中所收集的信息来实现。数据模型 / 行为模型可以是分类器、由 OEM 所提供的功耗模型、由网络运营商所提供的网络业务使用的模型、由安全的合作伙伴所提供的恶意活动的模型、减小的特征模型 (RFM) 等。

[0067] 在各个方面，移动设备可以被配置为与包括离线分类器和 / 或实时在线分类器的网络服务器相通信。离线分类器可以基于先前从云服务 / 网络所接收的信息生成稳健的数据模型 / 行为模型。实时在线分类器可以基于对从云服务 / 网络所接收的信息所生成的较大的且较复杂的行为模型的分析，来生成精简的数据模型 / 行为模型。精简的数据模型 / 行为模型可以包括以下模型，其考虑或评估可能指示可疑的或恶意行为的信息的子集和 / 或有限数量的状态情况和行为、而同时降低了分析仪必须处理的数据的数量。在线分类器和离线分类器均可以生成包括由云服务 / 网络实现的可用于特定的移动设备的、所减少的信息的子集的数据模型 / 行为模型。在一个方面，生成精简的数据模型 / 行为模型可以包括生成一个或多个减小的特征模型 (RFM) 和 / 或利用众包模型。

[0068] 在各个方面，移动设备，包括被配置有所下载的分析仪模块 / 分类器模型的移动设备，可以向诸如支持所下载的分析仪 / 分类器模型的服务器的网络服务器转发行为矢量、分析结果和其它行为分析数据。行为矢量和 / 或分析结果的这个反馈可以实时地或在方便的时候发生，并且这个反馈可以使得网络服务器能够开发和细化分析仪 / 分类器模

型，然后，可以通过公用的云网络，例如，经由应用商店的基础设施将所述分析仪 / 分类器模型作为应用更新向移动设备提供。

[0069] 在一个方面，移动设备可以被配置为利用经由公用的云网络或应用商店类型的机制从网络服务器所接收的众包模型。可以经由服务器完成、执行、和 / 或将机器学习和 / 或上下文建模技术应用于由许多移动设备所提供的行为信息和 / 或行为分析的结果来在网络服务器中生成众包模型。例如，网络服务器可以从许多移动设备接收大量的报告，并且分析、合并或以其他方式将这种众包的信息变成可用的信息，尤其是能够被所有移动设备使用或存取的精简的数据集或集中的行为模型。

[0070] 在一个方面，网络服务器可以向移动设备发送增量的更新，并且移动设备可以被配置为基于从网络服务器接收的增量的更新来更新其模型。例如，如果网络服务器包括存储一万条行为规则或记录的数据库，并且（例如，经由从许多移动设备接收的众包数据）将新的规则 / 记录添加到数据库，则网络服务器可以被配置为仅向移动设备发送模型的一部分和 / 或新的规则或记录（与所有的一万条记录完全相对）。移动设备可以接收新的规则 / 记录，并更新其现有模型，以包括该规则。可以经由应用商店接口完成这个对新的规则 / 记录和对现有模型的更新的下载。

[0071] 在一个方面，随着从移动设备接收到新的行为报告 / 分析报告，网络服务器可以连续地重新评估现有的精简的数据模型 / 行为模型，和 / 或基于历史的（例如，从在前的执行、行为模型的先前应用等所收集的）信息、新的信息、机器学习、上下文建模、以及在可用的信息、移动设备状态、环境情况、网络情况、移动设备性能、电池消耗级别等中所检测到的变化来生成新的或更新的精简的数据模型 / 行为模型。

[0072] 在一个方面，网络服务器可以被配置为生成精简的数据 / 行为模型，以包括初始的特征集（例如，初始的减少的特征模型）和一个或多个后续的特征集（例如，后续的减少的特征模型）。初始的特征集可以包括以下信息：其被确定为具有使得移动设备的分类器模块能够更好地确定特定的移动设备行为、软件应用或进程是恶意的 / 性能恶化的还是良性的最高可能性。每个后续的特征集可以包括以下信息：其被确定为具有决定性地确定移动设备行为、软件应用或进程是恶意的 / 性能恶化的或良性的下一个最高可能性。每个随后的特征集可以包括比它的前面的特征集更大的数据集，并且因此，针对每个后续的特征集，与应用数据模型 / 行为模型相关联的性能和功耗成本可能逐渐地增大。

[0073] 在一个方面，移动设备的分类器模块可以包括或实现使得移动设备处理器能够按阶段评估移动设备行为的渐进式行为模型（或分类器）。例如，分类器模块可以被配置为首先应用包括初始的特征集的精简的数据 / 行为模型，然后应用包括逐渐更大的特征集的模型，直到分类器模块确定移动设备行为是良性的或恶意的 / 性能恶化的。然后，分类器模块可以向网络服务器发送与每个模型的应用相关联的其操作结果和 / 或成功率。网络服务器可以使用这种结果来更新其精简的数据模型 / 行为模型（例如，包括在每个模型中的特征集等），由此基于所有报告移动设备的结果 / 成功率来细化数据和 / 或模型。然后，网络服务器可以将更新的精简数据模型 / 行为模型作为新的模型应用或对先前所下载的应用的升级使其可用于移动设备，因此移动设备可以访问所细化的精简的数据模型 / 行为模型。以这种方式，移动设备能够快速地从利用由应用商店基础设施所提供的软件分发和更新机制的其它移动设备的行为和结论而受益。

[0074] 在一个方面，网络服务器可以被配置为连续地更新在线分类器和离线分类器、模型生成器和/或云模型。网络服务器可以被配置为智能地确定何时变化基本足以保证生成新的模型以及何时可以忽略该变化。例如，网络服务器可以从多个不同的移动设备接收更新；执行机器学习操作以生成第一个类分类器；确定对所生成的第一类(family)分类器是否存在足够的变化，以保证生成新的模型；当确定对第一类分类器存在足够的变化时，在所生成的第一类分类器中确定哪个特征是最佳的特征；基于最佳的特征生成第二类分类器；确定对所生成的第二类分类器是否存在足够的变化；以及当确定对第二类分类器存在足够的变化时，生成/更新移动设备的分类器的数据模型/行为模型。

[0075] 在一个方面，相比于通常地从专用的云服务所接收的那些更新，接口模块可以被配置为使得移动设备能够接收较少或更不频繁的更新。这允许移动设备以灵活的方式而不需要至云服务的持续的连接、按用户的判断力来接收更新的模型。

[0076] 在各个方面，分析仪模块的全部或部分可以从多个源下载、被预先载入到移动设备上、被下载到移动设备的客户端应用中、以及作为软件应用从应用下载服务（例如，应用商店等）下载。

[0077] 可以在诸如图1中所示的示例的通信系统100的各种各样的通信系统内实现各个方面。典型的蜂窝电话网络104包括被耦合至网络操作中心108的多个小区基站106，所述网络操作中心108操作以诸如经由电话陆上线路（例如，POTS网络，未示出）和互联网110来连接移动设备102（例如，手机、膝上型计算机、平板等）与其它网络目的地之间的语音呼叫和数据。可以经由诸如4G、3G、CDMA、TDMA、LTE和/或其它的手机通信技术的双向无线通信链路112来完成移动设备102与电话网络104之间的通信。电话网络104还可以包括被耦合至网络操作中心108或被耦合到网络操作中心108内的一个或多个服务器114，所述一个或多个服务器114提供至互联网110的连接。

[0078] 通信系统100还可以包括被连接至电话网络104和至互联网110的专用网络服务器116和公用网络服务器122。网络服务器116、122与电话网络104之间的连接可以是通过互联网110的，通过专用网络的（如由虚箭头所示的），或任意其它公用的或半公用的网络的（例如，应用下载架构）。在一个方面，专用网络服务器116还可以被实现为云服务提供商网络118的网络架构内的服务器。可以通过电话网络104、互联网110、专用网络（未示出）或其任意组合来实现网络服务器116、122与移动设备102之间的通信。

[0079] 网络服务器116、122可以向移动设备102发送数据模型/行为模型，所述移动设备102可以接收并使用精简的数据模型/行为模型来识别可疑的或性能恶化的移动设备行为、软件应用、进程等。网络服务器116、122还可以向移动设备102发送分类和建模信息，以替代、更新、创建和/或维护移动设备的数据模型/行为模型。

[0080] 移动设备102可以收集移动设备102中的行为信息、状态信息、分类信息、建模信息、成功率信息和/或统计信息，并且（例如，经由电话网络104）将所收集的信息发送给网络服务器116，以用于分析。网络服务器116可以使用从移动设备102所接收的信息来更新或细化数据模型/行为模型或分类信息/建模信息，以包括针对性较强的和/或减少了的特征的子集。

[0081] 图2A示出了被配置为确定特定的移动设备行为、软件应用或进程是恶意的/性能恶化的、可疑的还是良性的方面移动设备102中的示例性逻辑组件和信息流程。在图2A中

所示的示例中，移动设备 102 包括行为观测器模块 202、行为分析仪模块 204、外部的上下文信息模块 206、分类器模块 208 以及执行器模块 210。在一个方面，分类器模块 208 可以被实现为行为分析仪模块 204 的一部分。在一个方面，行为分析仪模块 204 可以被配置为生成一个或多个分类器模块 208，所述一个或多个分类器模块 208 中的每一个分类器模块都可以包括一个或多个分类器。

[0082] 可以在软件、硬件或其任意组合中实现模块 202-210 中的每一个模块。在各个方面，可以在部分操作系统内（例如，内核内、内核空间中、用户空间中等）、在单独的程序或应用内、在专用的硬件缓冲区或处理器中、或在它们的任意组合中实现模块 202-210。在一个方面，模块 202-210 中的一个或多个模块可以被实现为在移动设备 102 的一个或多个处理器上执行的软件指令。

[0083] 行为观测器模块 202 可以被配置为在移动设备的各个层级 / 模块处用器械装备或协调应用程序接口 (API) 和其它组件（例如，寄存器、计数器等）；并且经由器械装备的组件在各个层级 / 模块处监视 / 观测移动设备操作和事件（例如，系统事件、状态变化等）；收集关于所观测的操作 / 事件的信息；智能地过滤所收集的信息；基于所过滤的信息生成一个或多个观测结果；并且将所生成的观测结果存储到存储器中（例如，日志文件中等）；和 / 或（例如，经由存储器写入、函数调用等）将所生成的观测结果发送给行为分析仪模块 204。

[0084] 行为观测器模块 202 可以通过从器械装备的组件收集信息来监视 / 观测移动设备操作和事件，包括关于应用框架或运行时间库中的库 API 调用、系统调用 API、文件系统以及建立子系统的操作、设备（包括传感器设备）状态变化以及其它类似事件的关系网 (networking) 的信息。行为观测器模块 202 还可以监视文件系统活动，所述文件系统活动可以包括搜索文件名、文件存取的类别（个人信息或标准数据文件）、创建或删除文件（例如，类型：可执行程序 (exe)、压缩程序 (zip) 等）、文件读操作 / 写操作 / 寻找操作、改变文件权限等。

[0085] 行为观测器模块 202 还可以监视数据网络活动，所述数据网络活动可以包括连接的类型、协议、端口号、设备被连接至的服务器 / 客户端、连接的数量、通信的容量或频率等。行为观测器模块 202 可以监视电话网络活动，其可以包括对所发送的、所接收的或所拦截的呼叫或消息（例如，SMS 等）的类型和数量（例如，所拨打的高价的呼叫的数量）进行监视。

[0086] 行为观测器模块 202 还可以监视系统资源的使用，其可以包括监视叉路的数量、存储访问操作、文件打开的数量等。行为观测器模块 202 可以监视移动设备的状态，其可以包括监视各种因素，例如，显示器是打开还是关闭、设备是锁定的还是解锁的、电池剩余的量、照相机的状态等。行为观测器模块 202 还可以通过例如监视对关键服务（浏览器、合同供应商 (contracts provider) 等）的意图、进程间通信的数量或程度、弹出的视窗等来监视进程间的通信 (IPC)。

[0087] 行为观测器模块 202 还可以监视 / 观测一个或多个硬件组件的驱动程序的统计信息和 / 或状态，所述一个或多个硬件组件可以包括照相机、传感器、电子显示器、WiFi 通信组件、数据控制器、存储控制器、系统控制器、访问端口、定时器、外围设备、无线通信组件、外部存储器芯片、稳压器、振荡器、锁相环、外围的桥接器以及被用于支持运行在移动计算

设备上的处理器和客户端的其它类似的组件。

[0088] 行为观测器模块 202 还可以监视 / 观测表示移动计算设备和 / 或移动设备子系统的状况或状态的一个或多个硬件计数器。硬件计数器可以包括被配置为存储移动计算设备中发生的与硬件有关的活动或事件的数目或状态的处理器 / 内核的专用寄存器。

[0089] 行为观测器模块 202 还可以监视 / 观测软件应用的动作或操作、来自应用下载服务器（例如，Apple® 应用商店服务器、Google® Play 服务器）的软件软件下载、由软件应用所使用的移动设备信息、呼叫信息、文本消息传送信息（例如，SendSMS、BlockSMS、ReadSMS 等）、媒体消息传送信息（例如，ReceiveMMS）、用户账号信息、位置信息、照相机信息、加速计信息、浏览器信息、基于浏览器的通信的内容、基于话音的通信的内容、短距离无线通信（例如，蓝牙、WiFi 等）、基于文本通信的内容、被记录的音频文件的内容、电话簿或联系人信息、通讯录等。由于行为观测器模块 202 是内部进程，其对信息和通信的内容的观测不应当危害用户的隐私，并且缩减或以别的方式缓解恶意行为的目的应当起作用以保护用户个人的和保密的信息免于被恶意软件未被授权的分发。

[0090] 行为观测器模块 202 可以监视 / 观测移动设备的传输或通信，包括包含语音信箱 (VoiceMailComm)、设备标识符 (DeviceIDComm)、用户账号信息 (UserAccountComm)、日历信息 (CalendarComm)、位置信息 (LocationComm)、所记录的音频信息 (RecordAudioComm)、加速计信息 (AccelerometerComm) 等的通信。

[0091] 行为观测器模块 202 可以监视 / 观测对指南针信息、移动设备设置、电池寿命、陀螺仪信息、压力传感器、磁感应器、屏幕活动等的使用以及更新 / 变化。行为观测器模块 202 可以监视 / 观测被传送给软件应用、应用更新等的通知 (AppNotifications)、以及从软件应用、应用更新等所传送的通知。行为观测器模块 202 可以监视 / 观测关于第一软件应用请求下载和 / 或安装第二应用软件的情况或事件。行为观测器模块 202 可以监视 / 观测关于用户验证的情况或事件，例如通行码的输入等。

[0092] 行为观测器模块 202 还可以监视 / 观测移动设备的多个层级（包括应用层、无线层和传感层）处的情况或事件。

[0093] 为了将被监视的因素的数量降低到可管理的程度，在一个方面，行为观测器模块 202 可以通过监视 / 观测行为或因素的初始集来执行粗略的观测，所述行为或因素的初始集是可能促成移动设备的恶化的所有因素的小的子集。在一个方面，行为观测器模块 202 可以从网络服务器 116 和 / 或云服务或网络 118 中的组件接收行为和 / 或因素的初始集。在一个方面，可以在从网络服务器 116 或云服务 / 网络 118 所接收的数据模型 / 行为模型中指定行为 / 因素的初始集。在一个方面，可以在所减小的特征模型 (RFM) 中指定行为 / 因素的初始集。

[0094] 虽然行为观测器模块 202 可以被提供有移动设备制造商或服务提供商，但是，在一个方面，行为观测器模块 202 可以被从应用商店所下载的行为观测应用所替代、补充或更新。换句话说，在这个方面，所下载的模块可以包括行为观测器模块、行为分析仪模块和 / 或分类器模块。

[0095] 行为分析仪模块 204 和 / 或分类器模块 208 可以从行为观测器模块 202 接收观测结果，将所接收的信息（即，观测结果）与从外部的上下文信息模块 206 所接收的上下文信息进行比较，并识别与所接收的观测结果相关联的子系统、进程和 / 或应用，所接收的观测

结果随着时间促成（或可能促成）设备的恶化，或可以以别的方式在设备上引起问题。

[0096] 在一个方面，行为分析仪模块 204 和 / 或分类器模块 208 可以包括以下智能 ：其用于利用信息的有限集（即，粗略的观测结果）来识别随着时间促成（或可能促成）设备的恶化或可以以别的方式在设备上引起问题的行为、进程或程序。例如，行为分析仪模块 204 可以被配置为分析从各个模块（例如，行为观测器模块 202、外部的上下文信息模块 206 等）所收集的信息（例如，以观测结果的形式）、学习移动设备的正常操作行为以及基于比较的结果生成一个或多个行为矢量。行为分析仪模块 204 可以向分类器模块 208 发送所生成的行为矢量，用于进一步的分析。

[0097] 分类器模块 208 可以接收行为矢量，并将它们和一个或多个行为模块进行比较，以确定特定的移动设备行为、软件应用或进程是性能恶化的 / 恶意的、良性的还是可疑的。

[0098] 当分类器模块 208 确定行为、软件应用或进程是恶意的或性能恶化的时，分类器模块 208 可以通知执行器模块 210，所述执行器模块 210 可以执行各种动作或操作，以校正被确定是恶意的或性能恶化的移动设备行为，和 / 或执行操作以治愈、解决、隔离、通知用户或以别的方式解决所识别的问题。

[0099] 当分类器模块 208 确定行为、软件应用或进程是可疑的时，分类器模块 208 可以通知行为观测器模块 202，所述观测器模块 202 可以调节其观测的粒度（即，移动设备行为被观测的细节的程度）和 / 或基于从分类器模块 208 所接收的信息（例如，实时分析操作的结果）改变所观测的行为、生成或收集新的或额外的行为信息，并向行为分析仪模块 204 和 / 或分类器模块 208 发送新的 / 额外的信息，用于进一步的分析 / 分类。行为观测器模块 202 与分类器模块 208 之间的这种反馈通信使得移动设备 102 能够递归地增大观测结果的粒度（即，实现更精细的或更详细的观测）或改变被观测的特征 / 行为，直到识别了可疑的或性能恶化的移动设备行为的来源为止、直到达到了处理或电池消耗量的门限为止、或直到移动设备处理器确定不能从观测粒度的进一步增大来识别可疑的或性能恶化的移动设备行为的来源为止。这种反馈通信还使得移动设备 102 能够在移动设备中本地地调节或修改数据模型 / 行为模型，而不消耗移动设备的过量的处理资源、存储资源或能源。

[0100] 在一个方面，行为观测器模块 202 和行为分析仪模块 204 可以单独地或共同地提供对计算系统的行为的实时行为分析，以从有限的和粗略的观测结果识别可疑的行为、以动态地确定要更详细地观测的行为、并且以动态地确定观测所需要的细节的程度。以这种方式，行为观测器模块 202 使得移动设备 102 能够有效地识别并防止问题发生在移动设备上，而不需要设备上的大量的处理器资源、存储资源或电池资源。

[0101] 图 2B 示出了被配置为确定行为、软件应用和 / 或进程是恶意的、性能恶化的、可疑的还是良性的方面移动设备 102 中的其它示例性逻辑组件和信息流程。在图 2B 中所示的示例中，移动设备 102 包括行为观测器模块 202、行为分析仪模块 204、接口模块 206 和可以被实现为模块或组件的行为 API 214。接口模块可以包括合作伙伴客户端模块和应用商店模块。可以在软件、硬件或其任意组合中实现模块 202-208、214 中的每一个模块。在各个方面，可以在高级的操作系统 210 内的一部分中（例如，内核内、内核空间中、用户空间中等）、在单独的程序或应用内、在专用的硬件缓冲区或处理器中、或其任意组合中实现模块 202-208、214。在一个方面，可以将模块 202-208、214 中的一个或多个模块实现为在移动设备 102 的一个或多个处理器上执行的软件指令。

[0102] 行为观测器模块 202 可以被配置为在包含网络工具包 (webkit)、SDK、NDK、内核、驱动器、浏览器、网页层软件和硬件的各种移动设备的模块和子系统上执行跨层的观测，以便表征移动设备行为。

[0103] 行为观测器模块 202 可以基于所接收的模型监视 / 观测移动设备行为、生成观测结果、并向行为分析仪模块 204 发送观测结果。行为分析仪模块 204 可以执行实时分析操作，其可以包括将数据模型 / 行为模型应用于由行为观测器模块 202 所收集的行为信息，以确定移动设备行为是良性的、可疑的还是恶意的 / 性能恶化的。可以在移动设备中生成行为模型，或可以从诸如应用下载服务（例如，Apple® 应用商店、Window® 商店、Google® 市场等）的外部源接收行为模型。例如，在各个方面，行为分析仪模块 204 可以经由接口模块 206 从第三方的网络服务器 116、云服务或网络 118 中的组件或应用下载服务器 122 接收行为模型。

[0104] 接口模块 206 可以存储（或具有对进行存储的数据库或服务器的访问）适合于解释从应用下载服务器 122 所接收的模型的协作信息和 / 或数据结构。这种协作信息 / 数据结构可以包括行为特征和文法的字典数据库，所述字典数据库用于解释、分析、合并和 / 或应用行为模型和 / 或将行为特征映射到移动设备行为、应用或进程的分类或分析的各种表示（例如，有限状态机、决策树等）。每种表示都可以包括一个或多个数据结构，其可以描述一组复杂的关系、映射、互连、依赖关系、转换和 / 或状态，并且可以组织信息以便创建新的知识要素。所述表示可以描述移动设备行为及其特征、行为类别以及与其它行为、分类或系统的关系。

[0105] 在一个方面，接口模块 206 可以被配置为将所观测的行为信息、移动设备特征和数据模型解码、解释、评估、合并、组织和 / 或编码为适合于经由通信链路 216 传输至应用下载服务器 122 的通信消息，和 / 或适合于经由行为 API 214 发送至行为观测器模块和分析仪模块的通信消息。

[0106] 在各个方面，接口模块 206 可以被配置为允许应用下载服务器 122 经由行为 API 214 模块 / 组件与移动设备 102 中的行为观测器模块 202 和分析仪模块 204 交互。例如，被授予用户权限的应用开发者可以经由接口模块 206 访问行为观测器模块 202 和分析模块 204，以执行以下操作：发现移动设备的能力；在设备上执行客户端登记操作和认证操作；访问可以在移动设备中观测 / 分析的一组移动设备行为或特征；生成、填入和 / 或更新将特征映射到良性的、可疑的或恶意的 / 性能恶化的行为的有限状态机描述；发布对移动设备行为的额外的、更详细的或针对性更强的观测的请求；发布从观测具体应用（例如，白名单）回退的请求；发布接收（好的、坏的、可疑的等）行为日志的请求；发布使移动设备（例如，经由执行模块 208）发起校正动作的请求；和 / 或在移动设备中执行其它类似的操作。

[0107] 分类器模块 208 可以被配置为当分类器模块 208 确定设备的行为是可疑的时候，向行为观测器模块 202 传送其实时分析操作的结果。行为观测器模块 202 可以调节其观测的粒度（即，以其观测移动设备行为的细节的程度）和 / 或基于从分类器模块 208 所接收的信息（例如，基于实时分析操作的结果）改变被观测的行为，生成或收集新的或额外的行为信息，并（例如，以新模型的形式）向分类器模块发送新的 / 额外的信息，以用于进一步的分析 / 分类。以这种方式，移动设备 102 可以递归地增大观测的粒度（即，实现更精细的或更详细的观测）或改变被观测的特征 / 行为，直到识别了可疑的或性能恶化的移动设备

行为的来源为止、直到达到了处理或电池消耗门限为止、或者直到移动设备处理器确定不能从观测粒度的进一步增大来识别可疑的或性能恶化的移动设备行为的来源为止。

[0108] 移动设备 102 可以向网络服务器 116 发送与模型的应用相关联的、其操作的结果和 / 或成功率。网络服务器 116 可以基于供模型生成器使用的结果 / 成功率来（例如，经由训练数据模型）生成训练数据，所述模型生成器可以生成更新的模型并向移动设备 102 发送更新的模型。

[0109] 图 3 示出了根据一个方面被配置为收集可以被应用于从应用下载服务所接收的模型的行为信息的计算系统的行为观测器模块 202 中的示例性逻辑组件和信息流程。行为观测器模块 202 可以包括自适应过滤模块 302、节流器模块 304、观测器模式模块 306、高级的行为检测模块 308、行为矢量生成器 310 和安全的缓冲区 312。高级的行为检测模块 308 可以包括空间相关模块 314 和时间相关模块 316。

[0110] 观测器模式模块 306 可以从各种源接收控制信息，所述各种源可以包括分析仪单元（例如，上面关于图 2 所描述的行为分析仪模块 204）、应用 API、和 / 或任意器械装备的组件。观测器模式模块 306 可以向自适应过滤模块 302 和高级的行为检测模块 308 发送关于各种观测器模式的控制信息。

[0111] 自适应过滤模块 302 可以从多个源接收数据 / 信息，并且智能地过滤所接收的信息，以生成选自所接收信息的、较小的信息子集。可以基于从分析仪模块或通过 API 的高级的进程通信所接收的信息或控制来适配这个过滤器。可以将所过滤的信息发送至节流器模块 304，所述节流器模块 304 可以负责控制来自过滤器的信息的量，以确保高级的行为检测模块 308 不被请求或信息所充满或过载。

[0112] 高级的行为检测模块 308 可以接收来自节流器模块 304 的数据 / 信息，来自观测器模式模块 306 的控制信息以及来自移动设备的其它组件的上下文信息。高级的行为检测模块 308 可以使用所接收的信息来执行空间相关和时间相关，以检测或识别可以使设备在次佳的层级处执行的高级行为。可以将空间相关的结果和时间相关的结果发送给行为矢量生成器 310，所述行为矢量生成器 310 可以接收相关信息并生成行为矢量，所述行为矢量描述特定进程、应用或子系统的行为。在非限制性方面，行为矢量生成器 310 可以生成行为矢量，使得特定进程、应用或子系统的高级行为可能是行为矢量的要素。在一个方面，可以将所生成的行为矢量存储在安全的缓冲区 312 中。高级的行为检测的示例可以包括对特定事件的存在的检测、对另一事件的数量或频率的检测、对多个事件之间的关系的检测、对事件发生的顺序的检测、对某些事件的发生之间的时间差的检测等。

[0113] 在各个方面，行为观测器模块 202 可以执行自适应的观测并控制观测粒度。即，行为观测器模块 202 可以动态地识别要被观测的相关行为，以及动态地确定所识别的行为要被观测的细节的程度。以这种方式，行为观测器模块 202 使得系统能够在各个层级（例如，多个粗略的和精细的层级）处监视移动设备行为。行为观测器模块 202 可以使得系统能够适应正被观测的对象。行为观测器模块 202 可以使得系统能够基于可以从各种各样的源获得的集中的信息的子集来动态地改变正被观测的因素 / 行为。

[0114] 如上所讨论的，行为观测器模块 202 可以执行自适应的观测技术，并基于从各种各样的源所接收的信息来控制观测粒度。例如，高级的行为检测模块 308 可以接收来自节流器模块 304、观测器模式模块 306 的信息以及从移动设备的其它组件（例如，传感器）所

接收的上下文信息。作为示例，执行时间相关的高级的行为检测模块 308 可以检测到照相机已经被使用以及移动设备正尝试向服务器上传图片。高级的行为检测模块 308 还可以执行空间相关，以在设备被皮套套住并被附着到用户的腰带时、或者如果在没有用户交互的情况下后台进程触发照相机快照事件中，确定移动设备上的应用是否拍照。高级的行为检测模块 308 可以确定这个所检测的高级行为（例如，当被皮套套住时，对照相机的使用）是否是可接受的或常见的行为，这可以通过将移动设备的当前行为与过去的行为进行比较和 / 或访问从多个设备所收集的信息（例如，从众包服务器所接收的信息）来实现。由于当被皮套套住时拍照并将照片上传到服务器是异常行为（如可以从正被皮套套住的上下文中所观测到的正常行为来确定），在这种情形下，高级的行为检测模块 308 可以将这个辨识为潜在的威胁行为，并发起适当的响应（例如，关闭照相机、发出警报等）。

[0115] 在一个方面，可以在多个部分中实现行为观测器模块 202。

[0116] 图 4 示出了实现方面观测器后台程序的计算系统 400 中的逻辑组件和信息流程。在图 4 中所示的示例中，计算系统 400 包括用户空间中的行为检测器 402 模块、数据库引擎 404 模块和行为分析仪模块 204，以及内核空间中的环形缓冲区 414、过滤规则 416 模块、节流规则 418 模块和安全的缓冲区 402。计算系统 400 还可以包括观测器后台程序，所述观测器后台程序包括用户空间中的行为检测器 402 和数据库引擎 404，以及内核空间中的安全缓冲区管理器 406、规则管理器 408 和系统健康监视器 410。

[0117] 各个方面可以在包含网络工具包、SDK、NDK、内核、驱动器和硬件的移动设备上提供跨层的观测，以便表征系统行为。可以实时地实现行为观测。

[0118] 观测器模块可以执行自适应观测技术，并控制观测粒度。如上所述，存在可能促成移动设备的恶化的大量的（即，数以千计的）因素，并且监视 / 观测可能促成移动设备的性能的恶化的所有不同因素是不可行的。为了克服这个问题，各个方面可以动态地识别要被观测的相关的行为，并且动态地确定所识别的行为要被观测的细节的程度。可以将所识别的行为用作众包模型的一部分，以便即使在其它移动设备中的任意移动设备都遭受相同的或类似的行为之前，也可以使用在第一移动设备上所学习的信息来使其它的移动设备受益。

[0119] 图 5 示出了用于根据一个方面执行动态的和自适应的观测的示例性方法 500。在框 502 中，移动设备处理器可以通过监视 / 观测可能促成移动设备的恶化的大量因素 / 行为的子集来执行粗略的观测。在框 503 中，移动设备处理器可以基于粗略的观测生成表征粗略的观测和 / 或移动设备行为的行为矢量。在框 504 中，移动设备处理器可以识别与可能潜在地促成移动设备的恶化的粗略的观测结果相关联的子系统、进程和 / 或应用。例如，这可以通过将从多个源所接收的信息与从移动设备的传感器所接收的上下文信息进行比较来实现。在框 506 中，移动设备处理器可以基于粗略的观测结果执行行为分析操作。在一个方面，作为框 503 和 504 的一部分，移动设备处理器可以执行上面关于图 2-4 所讨论的一个或多个操作。

[0120] 在确定框 508 中，移动设备处理器可以确定是否能够基于行为分析的结果来识别和校正可疑的行为或潜在的问题。当移动设备处理器确定能够基于行为分析的结果来识别和校正可疑的行为或潜在的问题（即，确定框 508 ＝“是”）时，在框 518 中，处理器可以发起用以校正行为的进程，并返回到框 502 来执行额外的粗略的观测。

[0121] 当移动设备处理器确定不能基于行为分析的结果来识别和/或校正可疑的行为或潜在的问题（即，确定框 508 =“否”）时，在确定框 509 中，移动设备处理器可以确定是否存在问题的可能性。在一个方面，移动设备处理器可以通过计算移动设备遭受潜在问题和/或参与可疑的行为的概率并确定所计算的概率是否大于预定的门限来确定存在问题的可能性。当移动设备处理器确定所计算的概率不大于预定的门限和/或不存在可疑的行为或潜在的问题存在和/或可检测的可能性（即，确定框 509 =“否”）时，处理器可以返回到框 502 来执行额外的粗略的观测。

[0122] 当移动设备处理器确定存在可疑的行为或潜在的问题存在和/或可检测的可能性（即，确定框 509 =“是”）时，在框 510 中，移动设备处理器可以关于所识别的子系统、进程或应用执行更深入的日志记录。在框 512 中，移动设备处理器可以基于更深入的日志记录关于所识别的子系统、进程或应用执行更深入的和更详细的观测。在框 514 中，移动设备处理器可以基于更深入的和更详细的观测执行进一步的和/或更深入的行为分析。

[0123] 在确定框 508 中，移动设备处理器可以再次地确定是否能够基于更深入的行为分析的结果来识别和校正可疑的行为或潜在的问题。当移动设备处理器确定不能基于更深入的行为分析的结果来识别和校正可疑的行为或潜在的问题（即，确定框 508 =“否”）时，处理器可以重复框 510-514 中的操作，直到细节的程度对于识别问题足够精细为止，或者直到确定不能用额外的细节来识别问题或没有问题存在为止。

[0124] 图 6 示出了用于从应用商店向移动设备下载行为观测器/分析仪/分类器模块或行为模型的方面方法 600。在框 602 中，响应于用户输入，移动设备可以经由诸如互联网的网络来访问在线应用商店。作为框 602 的一部分，移动设备还可以执行认证例程，以确认所访问的应用商店的确是可信的网站，而不是执行中间人攻击的恶意软件或服务器的源。由于方面模型/应用旨在防止移动设备遭受性能恶化的行为和软件，因此这种认证进程对于各个方面来说是尤其必要的，以便防止移动设备遭受恶意软件。对应用和数据进行签名并在移动设备上对它们的签名进行验证是一种能够被用于实现信任的方法。

[0125] 在框 604 中，一旦应用商店被认证，移动设备就可以下载可用于下载或更新的模型的菜单，并在移动设备的显示器上呈现该菜单。移动设备可以交替地向应用商店上传其配置偏好。在框 606 中，移动设备处理器可以接收用户选择输入，并且在框 608 中，基于用户的选择或设备的预安装的配置向应用商店发送下载或更新请求。

[0126] 在框 610 中，移动设备处理器可以接收对所请求的模型或应用的下载，并将代码存储到存储器的缓冲区部分中。在确定框 612 中，移动设备处理器可以关于所下载的代码执行软件校验和认证过程，以确定自从所下载的代码被受信任的第三方认证以来是否已经被准确地下载并且尚未被修改。用于校验和认证所下载的代码的机制在本领域中是公知的，并且可以在确定框 612 中实现。如果所下载的代码未被校验或认证（即，确定框 612 =“否”），则在框 620 中，处理器可以将代码从缓冲区的存储器删除。

[0127] 如果所下载的代码被校验和认证（即，确定框 612 =“是”），则在框 614 中，处理器可以安装所下载的模型或应用。这个安装过程可以涉及从缓冲区将代码复制到存储器的适当部分中用于执行。这还可以涉及替换先前所安装的模型或应用，尤其是在更新的情况下。或者，可以将新的行为规则添加到预先存在的规则集。在框 616 中，处理器可以通过向分析仪模块和/或分类器模块登记模型或应用来完成安装过程。如上面所提到的，可以在

安装或更新进程中将所下载的数据、算法和/或模型安装到或链接至分析仪模块和/或分类器模块，以便当分析仪模块和/或分类器模块执行实时分析操作时，所述分析仪模块和/或分类器模块使用所下载的数据、算法和/或模型来这样做。在框 618 中，一旦安装过程完成，进程就可以使用所下载的模型/应用来开始对设备行为进行监视、分析和/或分类。

[0128] 图 7 示出了用于下载并使用行为分析模型的方面方法 700。在框 702 中，移动设备处理器可以从应用下载服务接收行为模型。行为模型可以识别被确定为与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。

[0129] 在框 704 中，移动设备处理器可以与被安装在移动设备中的现有的分析引擎相结合地将所下载的行为模型安装到移动设备中。在一个实施例中，这可以通过访问由 API 模块所存储的信息来实现，所述信息诸如适合于解释从应用下载服务器所接收的模型的协同信息和/或数据结构。这种协同信息/数据结构可以包括行为特征和文法的字典数据库，所述字典数据库用于解释、分析、合并和/或应用行为模型和/或将行为特征映射到移动设备行为、应用或进程的分类或分析的各种表示（例如，有限状态机、决策树等）。在框 706 中，移动设备处理器可以使用所下载的行为模型来监视移动设备行为。

[0130] 图 8 示出了用于下载并使用替换行为分析模块/应用的方面移动设备方法 800。在框 802 中，移动设备处理器可以从应用下载服务接收行为模型。行为模型可以识别被确定为与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在框 804 中，移动设备处理器可以用所接收的模型来替代现有的行为模型。在框 806 中，移动设备处理器可以将所接收的模型链接到分析引擎，以便当分析引擎执行分析操作时，所述分析引擎使用所接收的模式来这样做。

[0131] 图 9 示出了用于从应用商店向移动设备下载行为分析模块/应用的方面移动设备方法 900。在框 902 中，移动设备处理器可以从应用下载服务接收行为模型。行为模型可以识别被确定为与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在框 904 中，移动设备处理器可以利用包括在所接收的模型中的信息来更新现有的行为模型的全部或一部分。在框 906 中，移动设备处理器可以将更新的模型链接到分析引擎，以便当分析引擎执行分析操作时，分析引擎使用更新的行为模型来这样做。

[0132] 图 10 示出了可以在移动设备中实现的、用于从多个公用的网络下载多个行为分析模块/应用的方面方法 1000。在框 1002 中，移动设备处理器可以从多个公用的网络来接收多个行为模型。每个行为模型都可以识别被确定为与使得移动设备处理器能够更好地确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在框 1004 中，移动设备处理器可以利用包括在一个或多个所接收的模型中的信息来更新一个或多个现有的行为模型的全部或一部分。在框 1006 中，移动设备处理器可以将所更新的模型链接到分析引擎，以便当分析引擎执行分析操作时，分析引擎使用更新的行为模型来这样做。

[0133] 图 11 示出了可以在移动设备中实现的、用于使用从公用的网络所接收的更新的行为模型来执行行为分析操作的方面方法 1100。在框 1102 中，移动设备中的处理器可以在移动设备的系统的各个层级处用器械装备或协调各个 API、寄存器、计数器或其它可用的信息或组件。在框 1104 中，移动设备处理器可以从器械装备的组件收集行为信息。在框 1106 中，移动设备处理器可以（例如，经由存储器写入操作、函数调用等）向移动设备的分类器

模块和/或分析仪模块发送(例如,经由存储器写入操作等)所收集的行为信息。

[0134] 在框 1108 中,移动设备处理器可以分析和/或分类所收集的行为信息,生成行为矢量,基于行为矢量、行为模型从各个其它的移动设备子系统所收集的信息来生成空间相关和/或时间相关。在框 1110 中,移动设备处理器可以开始执行各种分析操作,以确定特定的移动设备行为、软件应用或进程是良性的、可疑的、恶意的还是性能恶化的。

[0135] 在框 1112 中,移动设备处理器可以接收新的行为模型,所述新的行为模型更好地识别与确定移动设备行为是良性的还是恶意的最相关的因素和数据点。在框 1114 中,移动设备处理器可以用所接收的模型来替代现有的行为模型。在框 1116 中,移动设备处理器可以将所接收的模型链接到分析引擎。在确定框 1118 中,移动设备可以确定是否已经将移动设备行为类别为良性的或恶意的和/或确定是否已经识别出问题。如果移动设备处理器确定已经识别出问题(即,确定框 1118 =“是”),则在框 1120 中,移动设备处理器可以执行操作来解决该问题。如果移动设备处理器确定问题尚未被识别(即,确定框 1118 =“否”),则可以重复框 1108-1116 中的操作,直到识别出问题为止。

[0136] 移动设备的分析仪模块和/或分类器模块可以被配置为执行实时分析操作,其可以包括完成、执行和/或将数据、算法和/或模型应用于由观测器模块所收集的实时行为信息,以确定移动设备行为是良性的、可疑的、恶意的还是性能恶化的。可以将由分析仪模块和/或分类器模块所应用的数据、算法和/或模型预先安装到移动设备上,生成在移动设备上和/或从任意数量的公用的和专用的云服务/网络(包括第三方供应商和应用商店)所下载,或者由公用的和专用的云服务/网络的任意组合所升级。可以在安装或更新过程中将所下载的数据、算法和/或模型安装到或链接至分析仪模块和/或分类器模块,以便当分析仪模块和/或分类器模块执行实时分析操作时,分析仪模块和/或分类器模块使用所下载的数据、算法和/或模型来这样做。

[0137] 可以在各种各样的移动计算设备上实现各个方面,在图 12 中以智能手机的形式示出了各种各样的移动计算设备的示例。智能手机 1202 可以包括被耦合至内部存储器 1202、显示器 1203 以及至扬声器的处理器 1201。此外,智能手机 1202 可以包括用于发送和接收电磁辐射、可以被连接至无线数据链路和/或蜂窝电话收发机 1205 的天线 1204,其中,所述蜂窝电话收发机 1205 被耦合至处理器 1201。智能手机 1202 通常还包括用于接收用户输入的菜单选择按钮或摇杆开关 1206。

[0138] 典型的智能手机 1202 还包括声音编码/解码 (CODEC) 电路 1212,所述声音编码/解码 (CODEC) 电路 1212 将从麦克风所接收的声音数字化成适合于无线传输的数据分组,并且对所接收的声音数据分组进行解码,以生成模拟信号,将所生成的模拟信号提供给扬声器以发出声音。另外,一个或多个处理器 1201、无线收发机 1205 和 CODEC 1212 可以包括数字信号处理器 (DSP) 电路(未单独地示出)。

[0139] 可以在客户端-服务器的架构中用一些发生在服务器中的处理来完成方面方法的一部分,例如,维护正常的操作行为的数据库,在执行方面方法时,可以由移动设备处理器来访问该数据库。可以在诸如图 13 中所示的服务器 1300 的、各种各样的商业上可用的服务器设备中的任一个上实现这些方面。这种服务器 1300 通常包括处理器 1301,所述处理器 1301 被耦合至易失性存储器 1302 和诸如硬盘驱动器 1303 的大容量非易失性存储器。服务器 1300 还可以包括被耦合至处理器 1301 的软盘驱动器、压缩光盘 (CD) 或 DVD 光盘驱

动器 1301。服务器 1300 还可以包括被耦合至处理器 1301 的、用于与网络 1305（例如，被耦合至其它广播系统计算机和服务器的局域网）建立数据连接的网络接入端口 1304。

[0140] 处理器 1201、1301 可以是能够被软件指令（应用）所配置以执行各种各样的功能（包括以下所描述的各个方面的功能）的任意可编程微处理器、微型计算机或多个处理器芯片。在一些移动设备中，可以提供多个处理器 1201，例如，专用于无线通信功能的一个处理器以及专用于运行其它应用的一个处理器。通常地，在将软件应用被存取和加载到处理器 1201、1301 中之前，可以将它们存储在内部的存储器 1202、1302、1303 中。处理器 1201、1301 可以包括足够存储应用软件指令的内部存储器。

[0141] 可以以诸如 C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、结构化查询语言（例如，Transact-SQL）、Perl 的高级编程语言或以各种其它编程语言来编写用于在可编程处理器上执行以实现各个方面的操作的计算机程序代码或“程序代码”。存储在如在本申请中所使用的计算机可读存储介质上的程序代码或程序可以指的是其格式是处理器可理解的机器语言代码（例如，目标代码）。

[0142] 许多移动计算设备的操作系统内核被组织为用户空间（在此，非特权代码运行）和内核空间（在此，特权代码运行）。这种隔离在Android®和其它的通用公开执照 (GPL) 环境或开源环境中是尤其重要的，在上述环境中，必须是内核空间的一部分的代码必须被许可，而运行在用户空间中的代码则不需要这种许可。应当理解的是，可以在内核空间或用户空间中实现这里所讨论的各种软件组件 / 模块，除非明确地声明以别的方式实现。

[0143] 前述的方法描述和过程流程图仅被提供作为说明性的示例，而不旨在需要或暗示必须按照所呈现的顺序来执行各个方面的步骤。如本领域的技术人员将意识到的，可以按照任意的顺序来执行前述方面中的步骤顺序。诸如“此后”、“然后”、“接下来”等单词并不旨在限制步骤的顺序，这些单词仅仅被用于通过对方法的描述来引导读者。此外，例如，使用冠词“一 (a)”、“一个 (an)”或“所述”对单数形式的权利要求的要素的任意引用都不被解释为将该要素限定为单数形式。

[0144] 如在本申请中所使用的，术语“组件”、“模块”、“系统”、“引擎”、“生成器”、“管理器”等旨在包括与计算机有关的实体，其例如但不限于硬件、固件、硬件与软件的组合、软件、或者被配置为执行特定的操作或函数的执行中的软件。例如，组件可以是但不限于 :运行在处理器上的进程、处理器、对象、可执行文件、执行的线程、程序和 / 或计算机。通过说明的方式，运行在计算设备上的应用和计算设备均可以被称为组件。一个或多个组件可以存在于进程和 / 或执行的线程内，并且组件可以位于一个处理器或内核上和 / 或被分布在两个或更多个处理器或内核之间。此外，这些组件可以根据具有存储于其上的各种指令和 / 或数据结构的各种非暂时性计算机可读介质来进行执行。组件可以通过本地和 / 或远程进程、函数或过程调用、电子信号、数据分组、存储器读 / 写以及与其它已知的网络、计算机、处理器和 / 或进程有关的通信方法等方式来通信。

[0145] 可以将结合本文所公开的方面所描述的各种说明性的逻辑框、模块、电路和算法步骤实现为电子硬件、计算机软件或两者的组合。为了清楚地示出硬件和软件的这种可互换性，在上面已经围绕其功能概括地描述了各种说明性的组件、框、模块、电路和步骤。至于这种功能是实现为硬件还是软件取，决于特定的应用和施加给整个系统的设计约束。熟练的技术人员可以针对每种特定应用，以不同的方式实现所描述的功能，但是，这种实现决定

不应当被解释为导致对本发明的范围的背离。

[0146] 可以用被设计为执行本文所描述的功能的通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑器件、分立门或晶体管逻辑器件、分立的硬件组件或它们的任意组合来实现或执行结合本文所公开的方面所描述的、用于实现各种说明性的逻辑器件、逻辑框、模块和电路的硬件。通用处理器可以是多处理器，但是，在替代的方案中，处理器可以是任意传统的处理器、控制器、微控制器或状态机。还可以将处理器实现为计算设备的组合（例如，DSP、GPU 和多个处理器的组合）、多个多处理器、一个或多个多处理器与 DSP 内核的结合、或任意其它此种结构。或者，可以通过专用于给定功能的电路来执行一些步骤或方法。

[0147] 在一个或多个示例性的方面，可以在硬件、软件、固件或其任意组合中实现所描述的功能。如果在软件中实现，则可以将功能作为一个或多个指令或代码存储在非暂时性计算机可读介质或非暂时性处理器可读介质上。可以将本文所公开的方法或算法的步骤体现在处理器可执行软件模块中，所述处理器可执行软件模块可以存在于非暂时性计算机可读或处理器可读存储介质上。非暂时性计算机可读或处理器可读存储介质可以是可以由计算机或处理器存取的任意存储介质。通过示例而非限定的方式，这种非暂时性计算机可读或处理器可读介质可以包括 RAM、ROM、EEPROM、FLASH 存储器、CDM-ROM 或其它光盘存储器、磁盘存储器或其它磁性存储设备或可以被用于存储指令或数据结构形式的期望的程序代码并且可以由计算机存取的任意其它介质。如本文所使用的，磁盘和光盘包括压缩光盘 (CD)、激光光盘、光盘、数字多功能光盘 (DVD)、软盘和蓝光光盘，其中，磁盘通常磁性地复制数据，而光盘则用激光光学地复制数据。上面的组合也包括在非暂时性计算机可读和处理器可读介质的范围内。此外，方法或算法的操作可以作为代码和 / 或指令、或代码和 / 或指令的任意组合、或一组代码和 / 或指令而存在于非暂时性处理器可读介质和 / 或计算机可读介质上，其可以被合并到计算机程序产品中。

[0148] 提供所公开方面的前面的描述，以使得本领域任何技术人员能够实现或使用本发明。对于本领域中的技术人员来说，对这些方面的各种修改将是显而易见的，并且在不脱离本发明的精神或范围的情况下，可以将本文所定义的一般原则应用于其它方面。因此，本发明并不旨在受限于本文所示出的方面，而是要符合与以下权利要求和本文所公开的原理与新颖的特征相一致的最广范围。

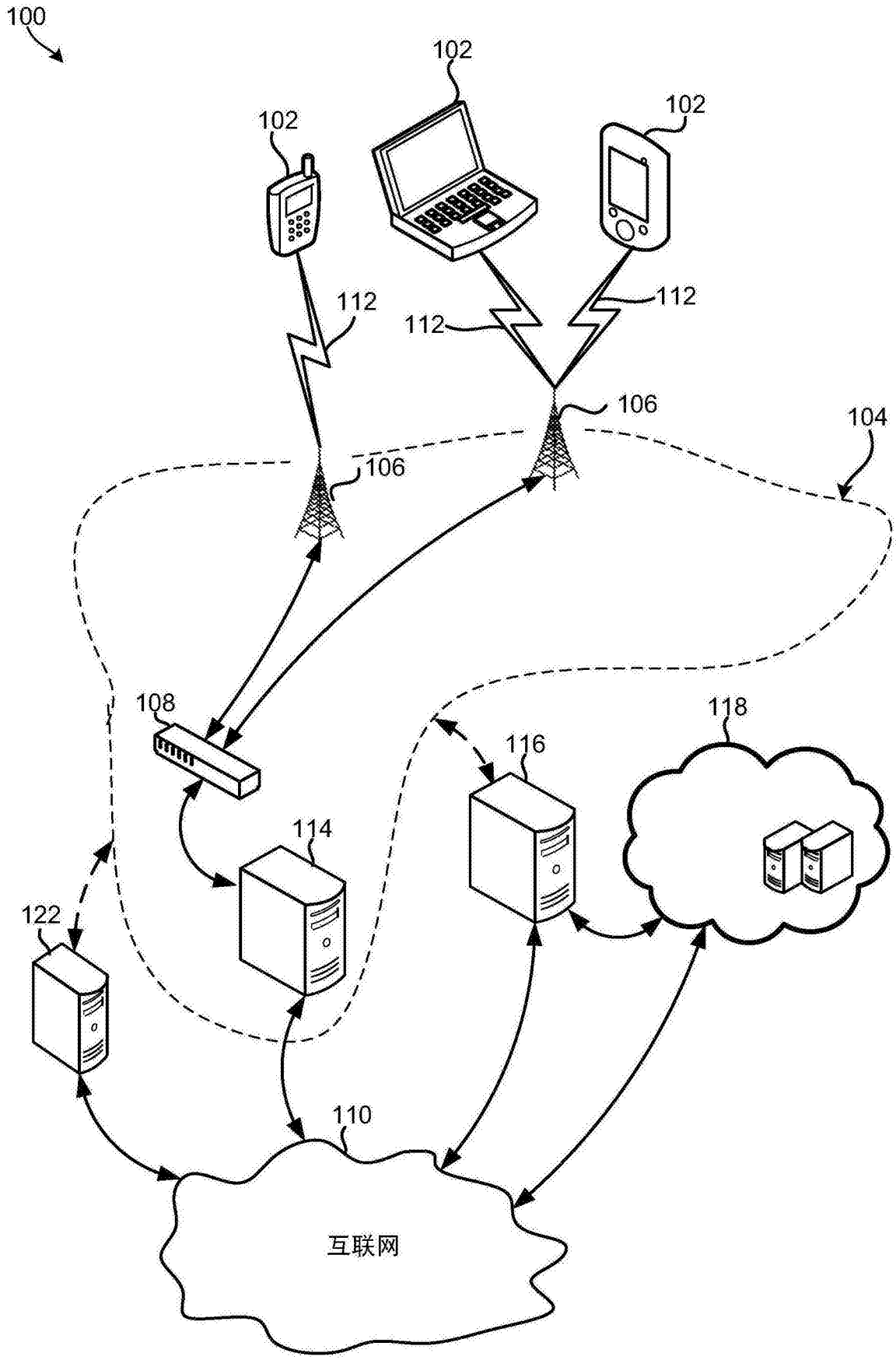

100
102
102
102
112
112
112
106
106
104
108
116
118
114
122
110
互联网

图 1

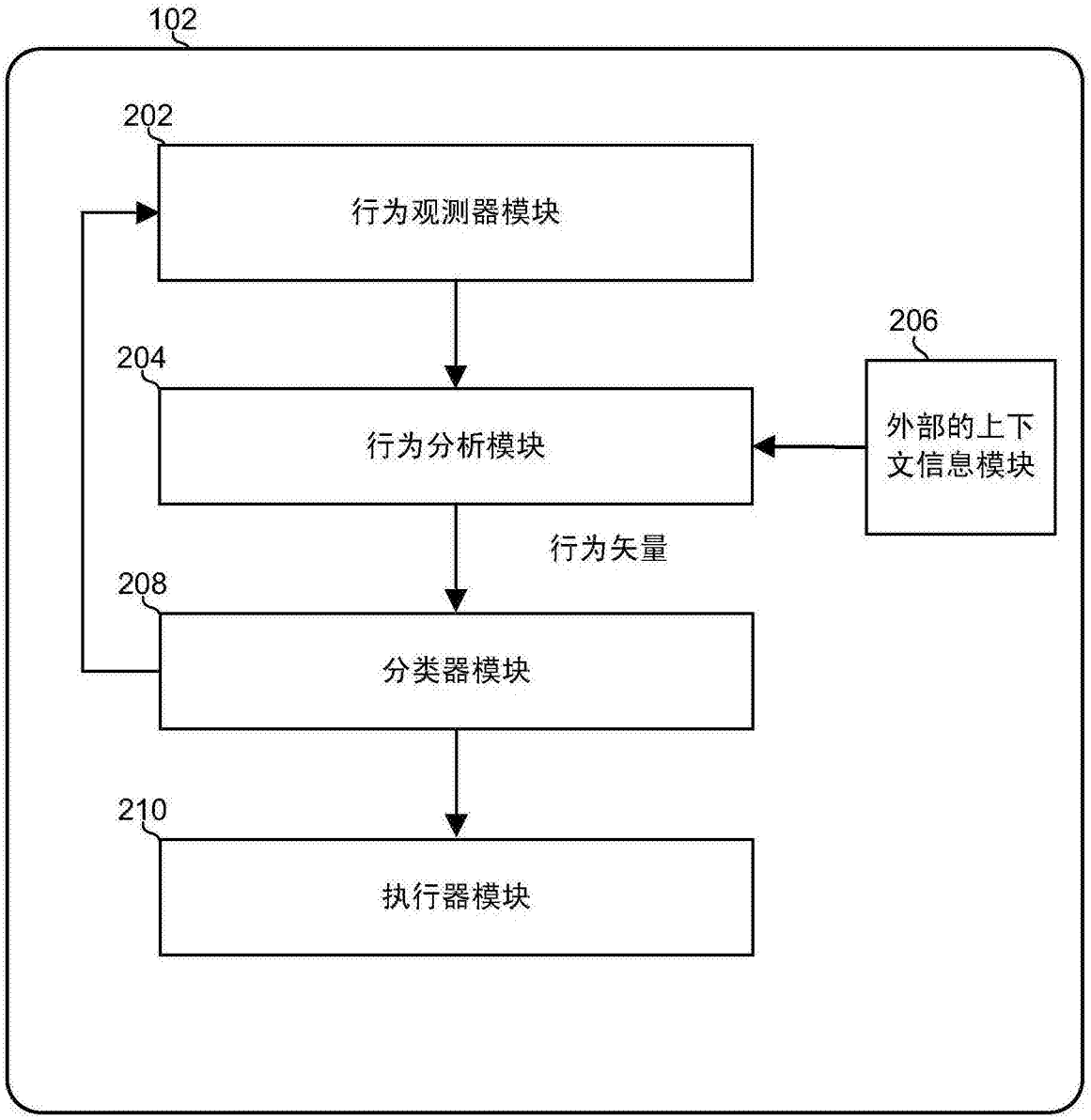

102
202
行为观测器模块
206
204
行为分析模块
外部的上下文信息模块
行为矢量
208
分类器模块
210
执行器模块

图 2A

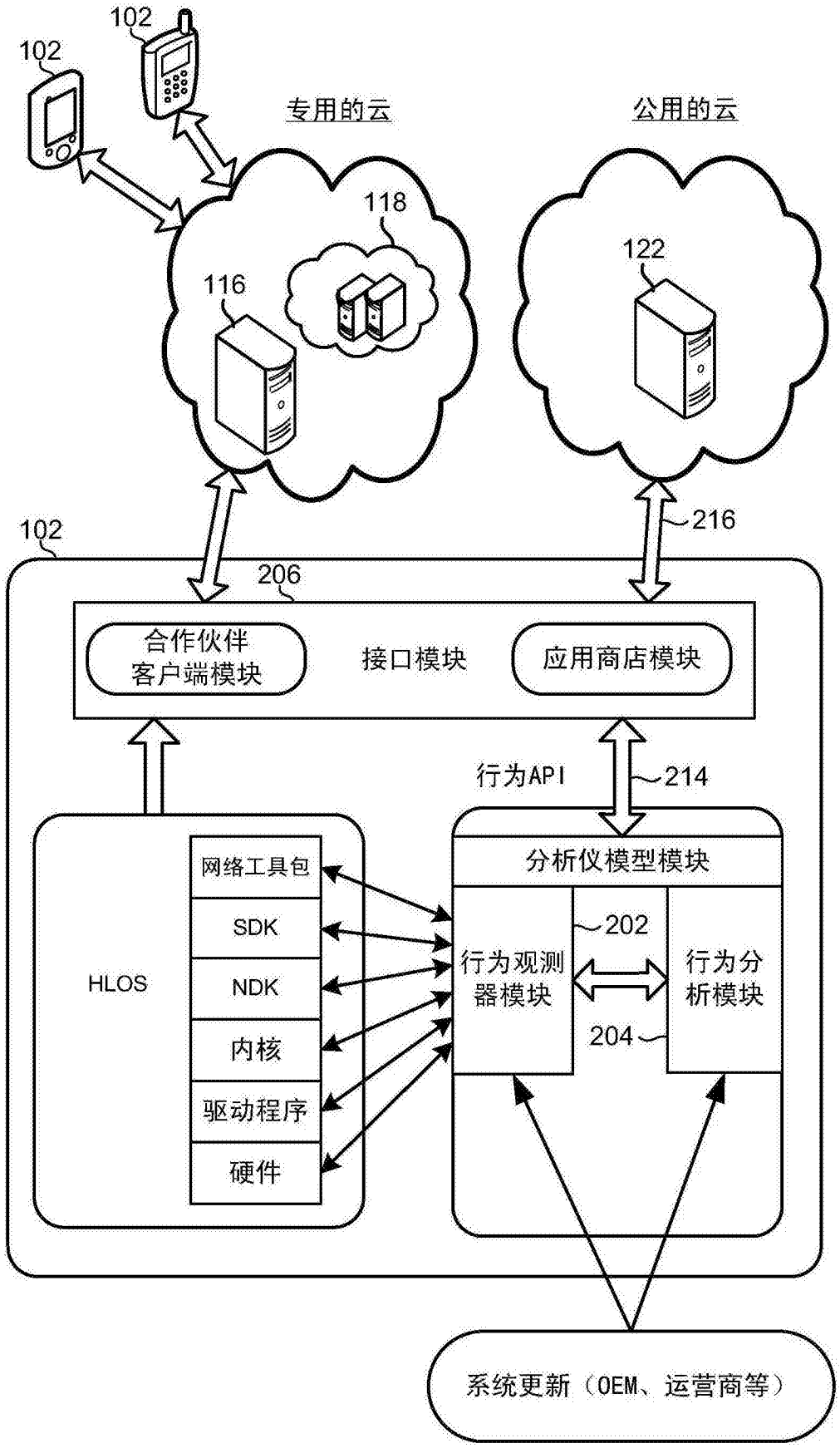

102
102
专用的云
公用的云
118
116
122
102
216
206
合作伙伴
客户端模块
接口模块
应用商店模块
行为API
214
网络工具包
SDK
NDK
内核
驱动程序
硬件
HLOS
分析仪模型模块
202
行为观测
器模块
行为分
析模块
204
系统更新（OEM、运营商等）

图 2B

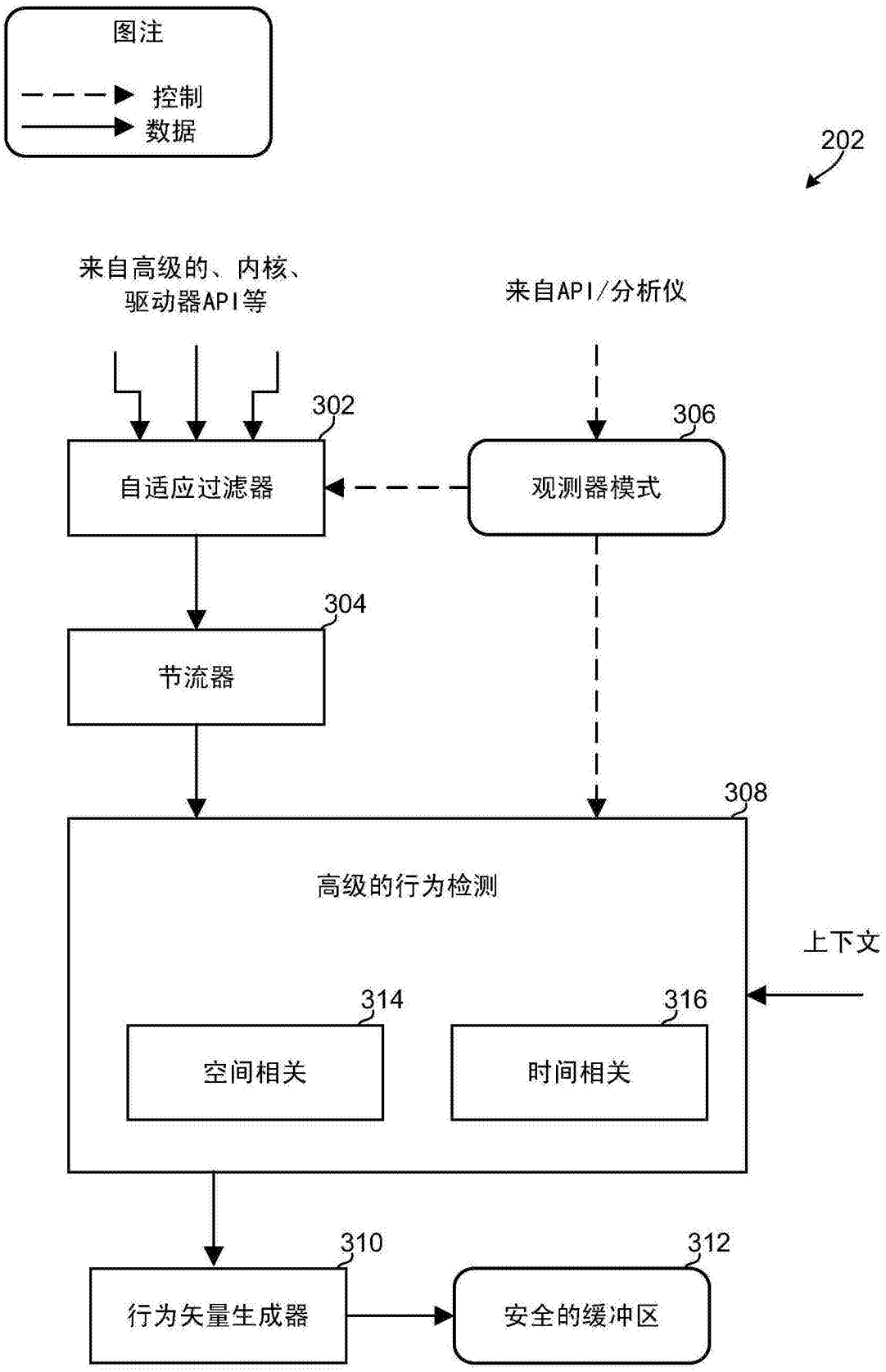

图注
控制
数据
202
来自高级的、内核、
驱动器API等
来自API/分析仪
302
306
自适应过滤器
观测器模式
304
节流器
308
高级的行为检测
上下文
314
316
空间相关
时间相关
310
312
行为矢量生成器
安全的缓冲区

图 3

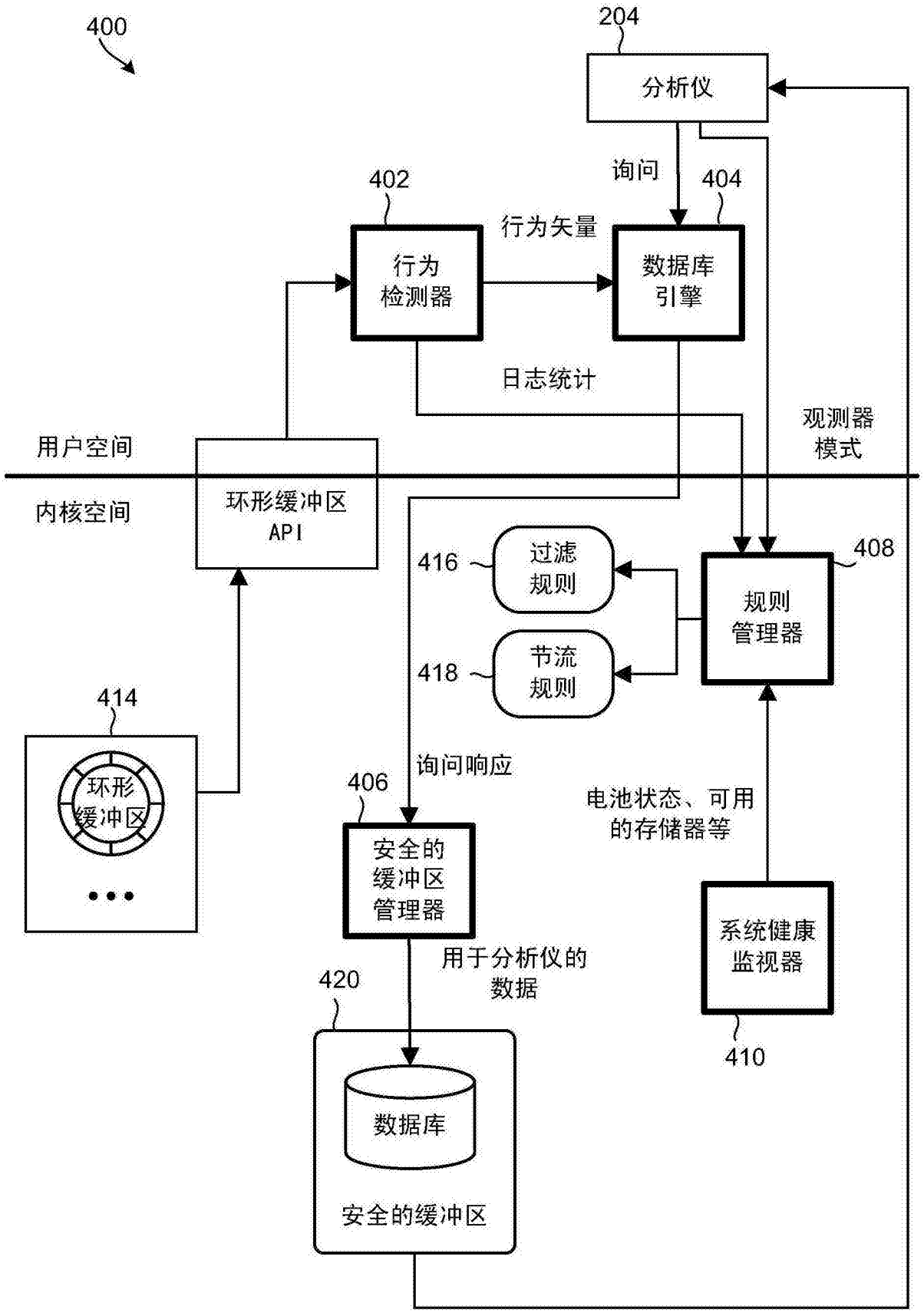

400
204
分析仪
询问
404
402
行为矢量
行为
检测器
数据库
引擎
日志统计
观测器
模式
用户空间
内核空间
环形缓冲区
API
416
过滤
规则
408
规则
管理器
418
节流
规则
414
环形
缓冲区
询问响应
406
电池状态、可用
的存储器等
安全的
缓冲区
管理器
系统健康
监视器
用于分析仪的
数据
420
410
数据库
安全的缓冲区

图 4

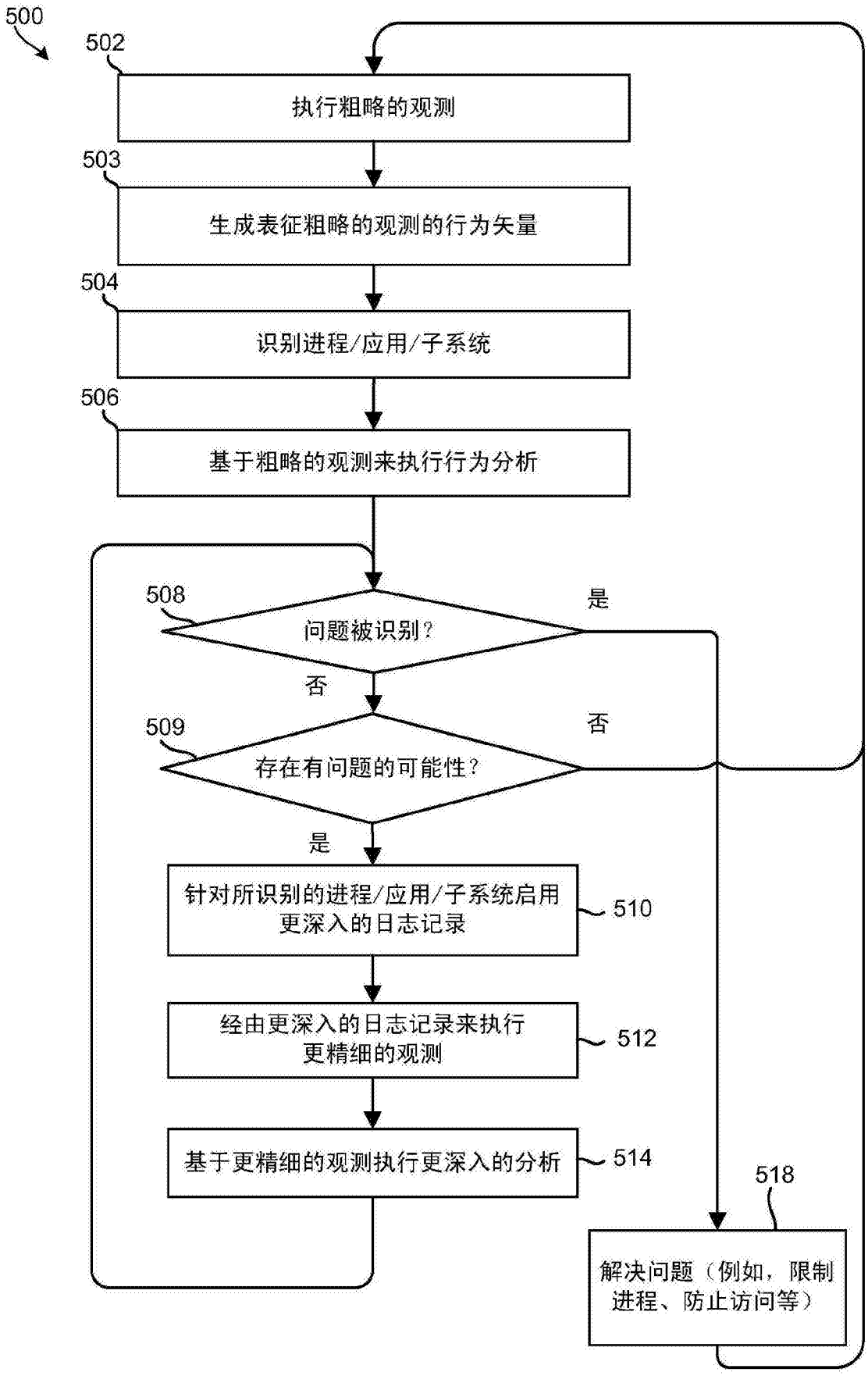

500
502
执行粗略的观测
503
生成表征粗略的观测的行为矢量
504
识别进程/应用/子系统
506
基于粗略的观测来执行行为分析
508
问题被识别？
是
否
509
存在有问题的可能性？
否
是
针对所识别的进程/应用/子系统启用更深入的日志记录
510
经由更深入的日志记录来执行更精细的观测
512
基于更精细的观测执行更深入的分析
514
518
解决问题（例如，限制进程、防止访问等）

图 5

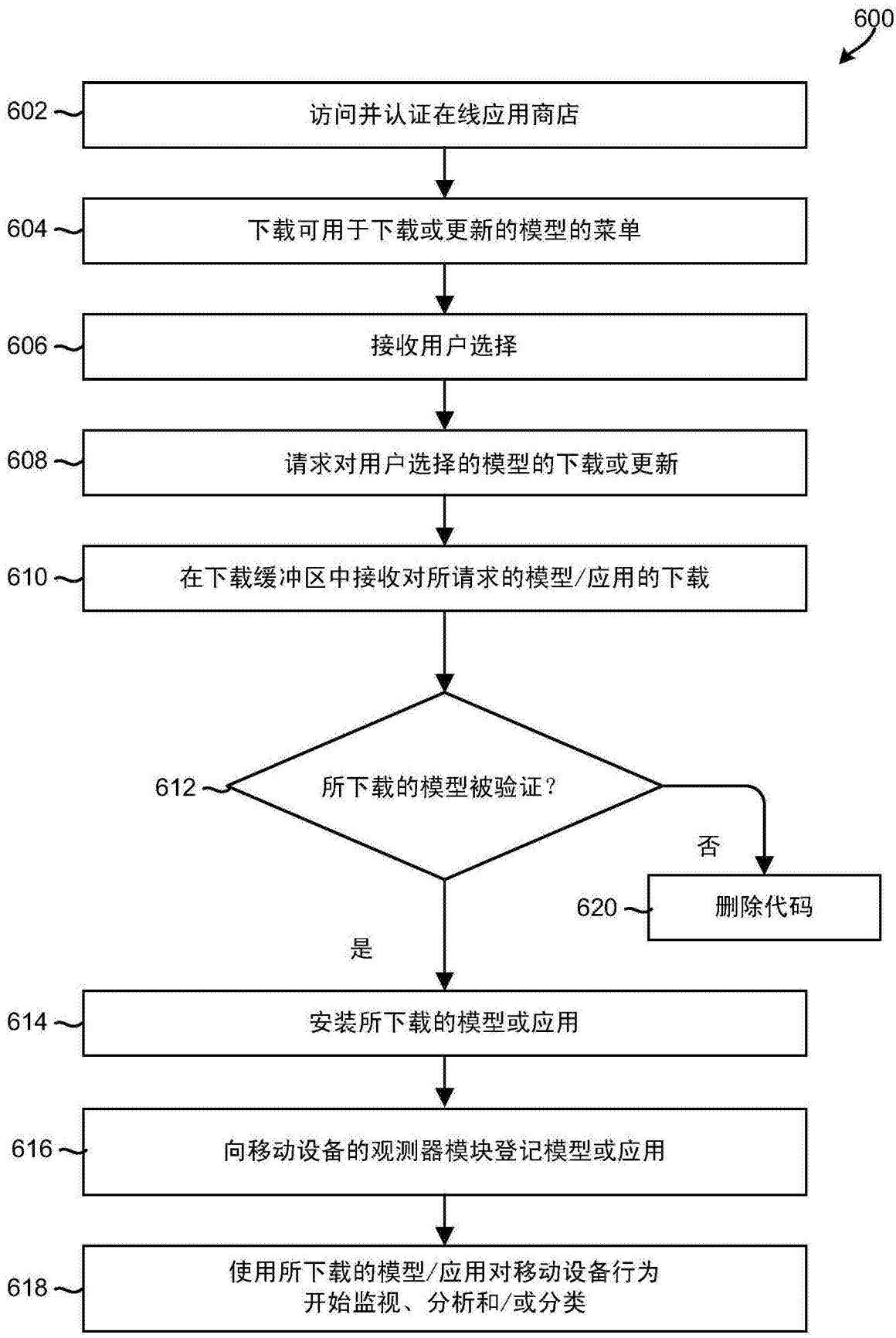

600
602
访问并认证在线应用商店
604
下载可用于下载或更新的模型的菜单
606
接收用户选择
608
请求对用户选择的模型的下载或更新
610
在下载缓冲区中接收对所请求的模型/应用的下载
612
所下载的模型被验证?
否
620
删除代码
是
614
安装所下载的模型或应用
616
向移动设备的观测器模块登记模型或应用
618
使用所下载的模型/应用对移动设备行为
开始监视、分析和/或分类

图 6

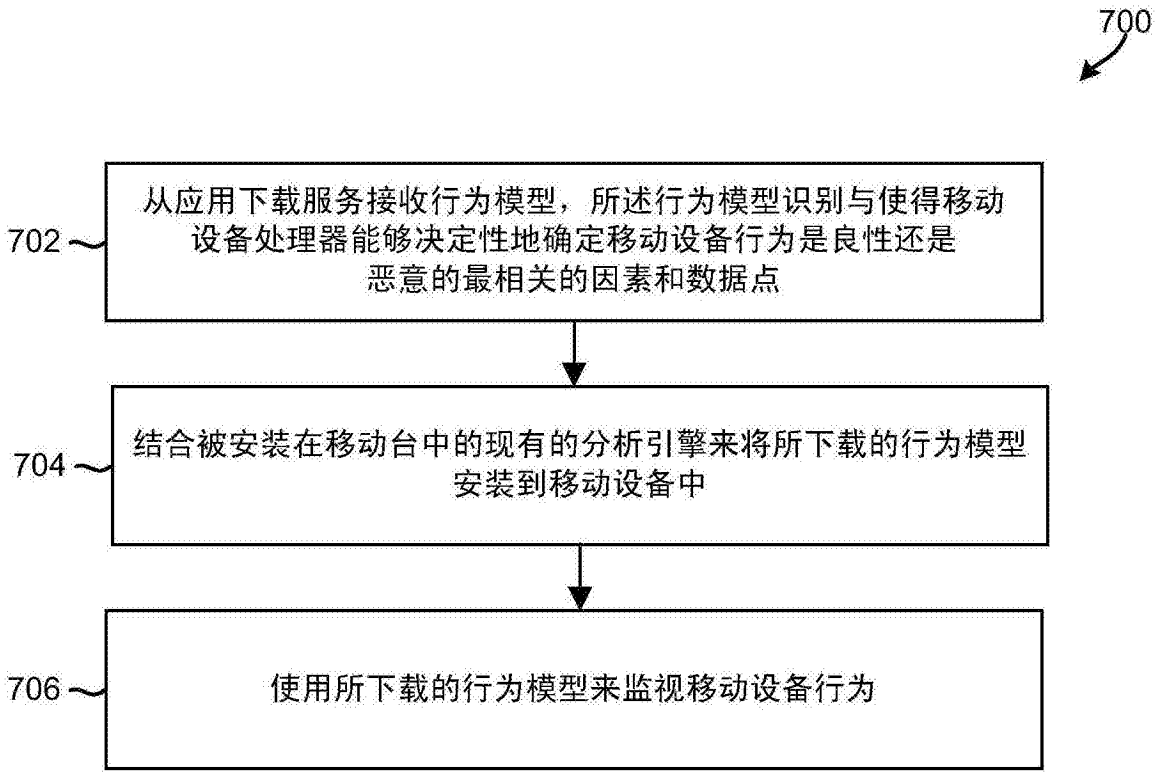

700
从应用下载服务接收行为模型，所述行为模型识别与使得移动设备处理器能够决定性地确定移动设备行为是良性还是恶意的最相关的因素和数据点
702
结合被安装在移动台中的现有的分析引擎来将所下载的行为模型安装到移动设备中
704
使用所下载的行为模型来监视移动设备行为
706

图 7

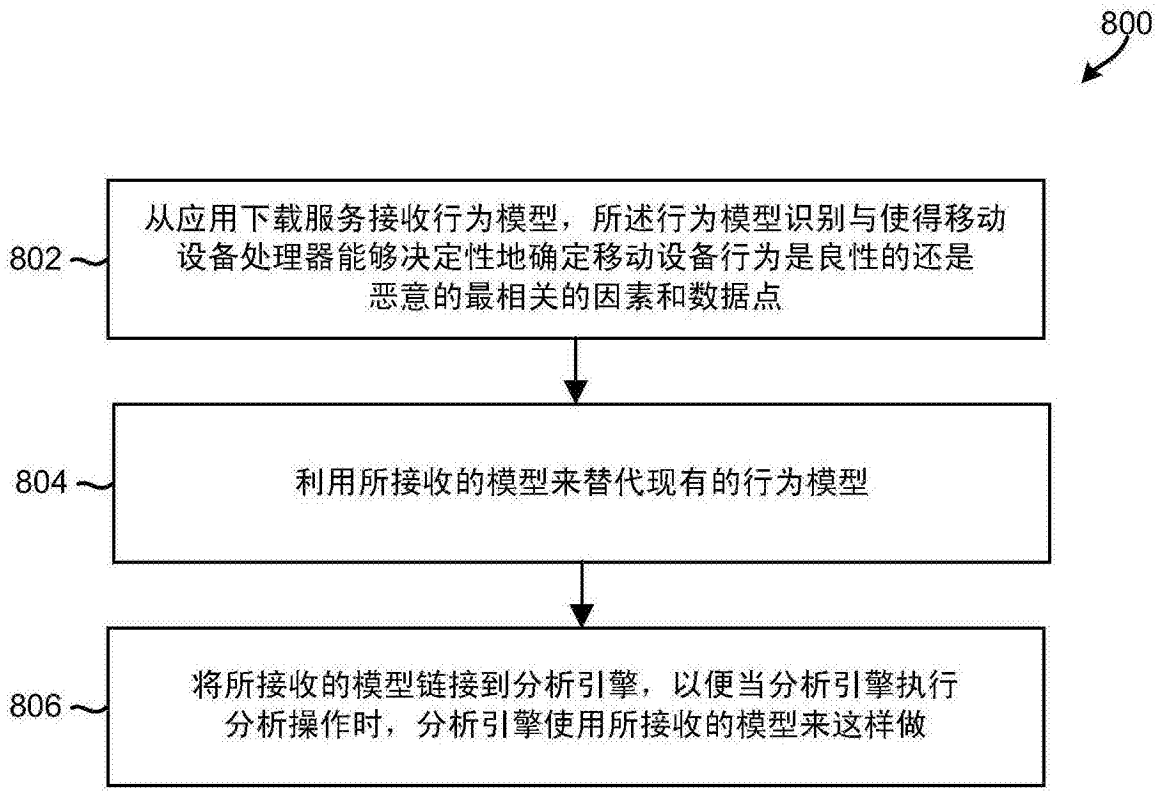

800
从应用下载服务接收行为模型，所述行为模型识别与使得移动设备处理器能够决定性地确定移动设备行为是良性的还是恶意的最相关的因素和数据点
802
利用所接收的模型来替代现有的行为模型
804
将所接收的模型链接到分析引擎，以便当分析引擎执行分析操作时，分析引擎使用所接收的模型来这样做
806

图 8

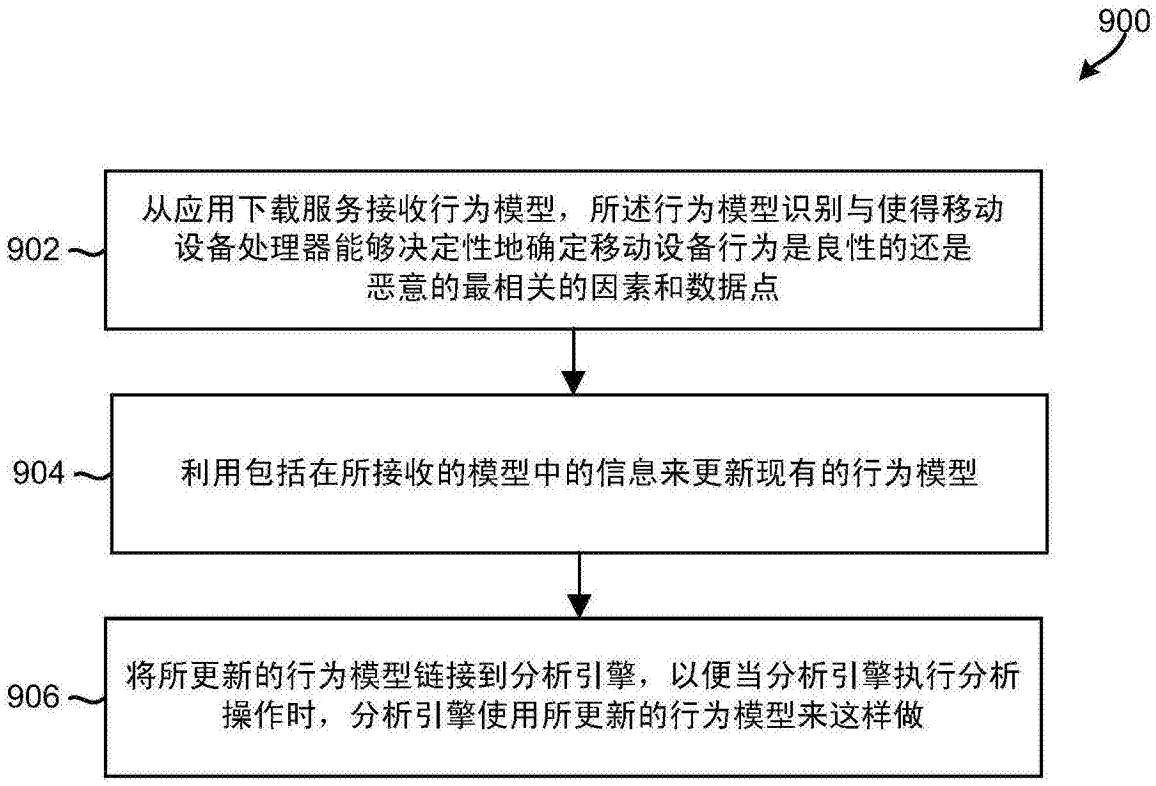

900
902
从应用下载服务接收行为模型，所述行为模型识别与使得移动设备处理器能够决定性地确定移动设备行为是良性的还是恶意的最相关的因素和数据点
904
利用包括在所接收的模型中的信息来更新现有的行为模型
906
将所更新的行为模型链接到分析引擎，以便当分析引擎执行分析操作时，分析引擎使用所更新的行为模型来这样做

图 9

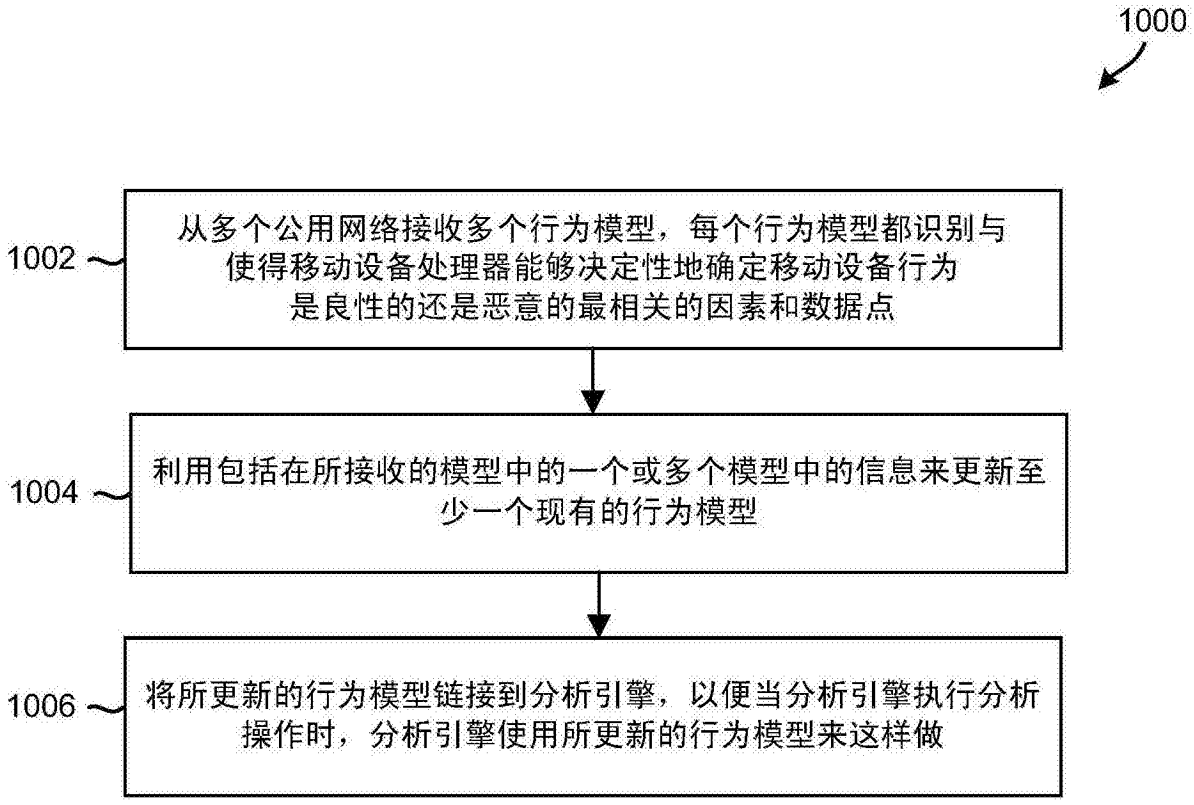

1000
1002
从多个公用网络接收多个行为模型，每个行为模型都识别与使得移动设备处理器能够决定性地确定移动设备行为是良性的还是恶意的最相关的因素和数据点
1004
利用包括在所接收的模型中的一个或多个模型中的信息来更新至少一个现有的行为模型
1006
将所更新的行为模型链接到分析引擎，以便当分析引擎执行分析操作时，分析引擎使用所更新的行为模型来这样做

图 10

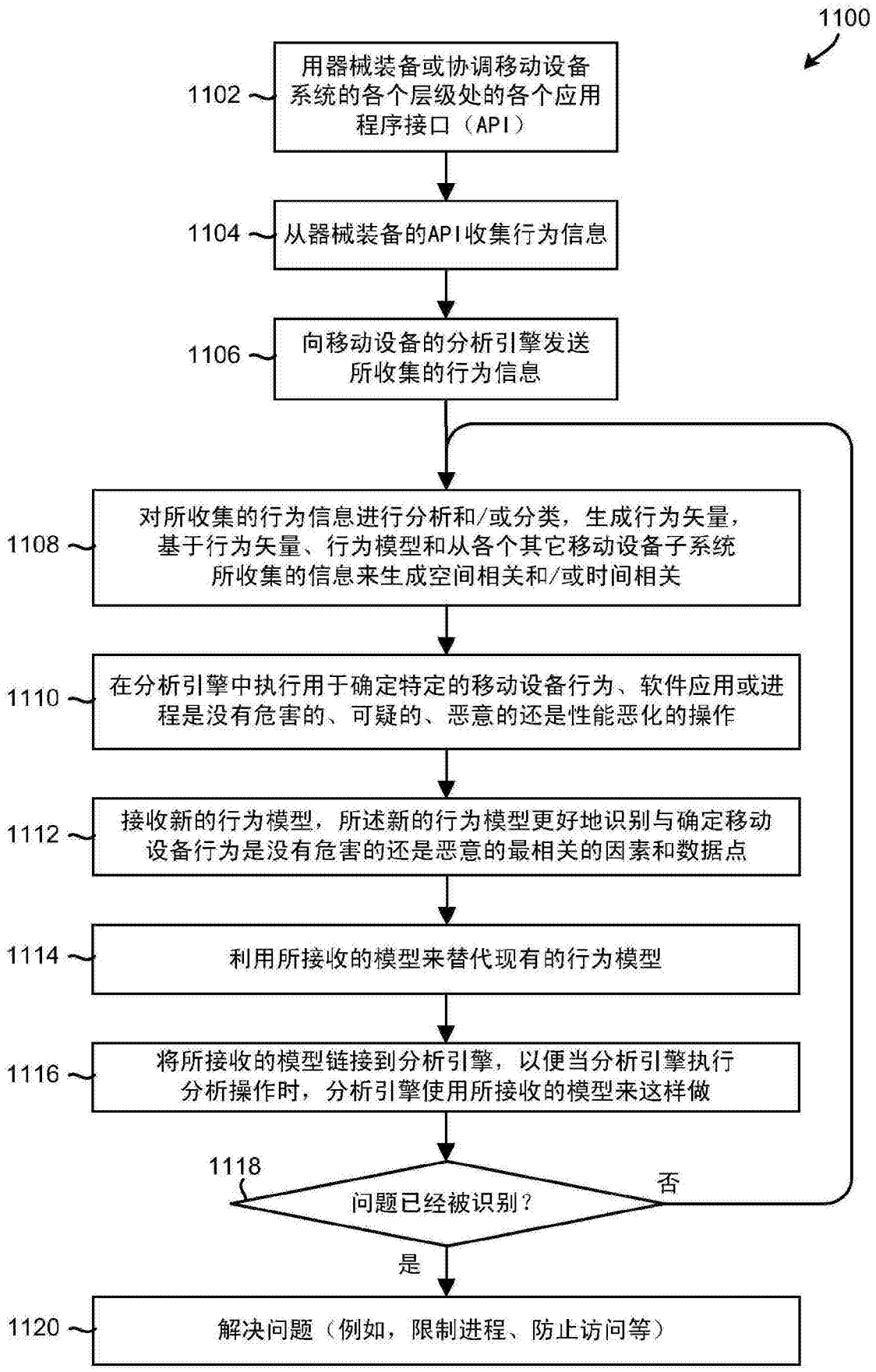

1100
1102
用器械装备或协调移动设备系统的各个层级处的各个应用程序接口（API）
1104
从器械装备的API收集行为信息
1106
向移动设备的分析引擎发送所收集的行为信息
1108
对所收集的行为信息进行分析和/或分类，生成行为矢量，基于行为矢量、行为模型和从各个其它移动设备子系统所收集的信息来生成空间相关和/或时间相关
1110
在分析引擎中执行用于确定特定的移动设备行为、软件应用或进程是没有危害的、可疑的、恶意的还是性能恶化的操作
1112
接收新的行为模型，所述新的行为模型更好地识别与确定移动设备行为是没有危害的还是恶意的最相关的因素和数据点
1114
利用所接收的模型来替代现有的行为模型
1116
将所接收的模型链接到分析引擎，以便当分析引擎执行分析操作时，分析引擎使用所接收的模型来这样做
1118
问题已经被识别？
否
是
1120
解决问题（例如，限制进程、防止访问等）

图 11

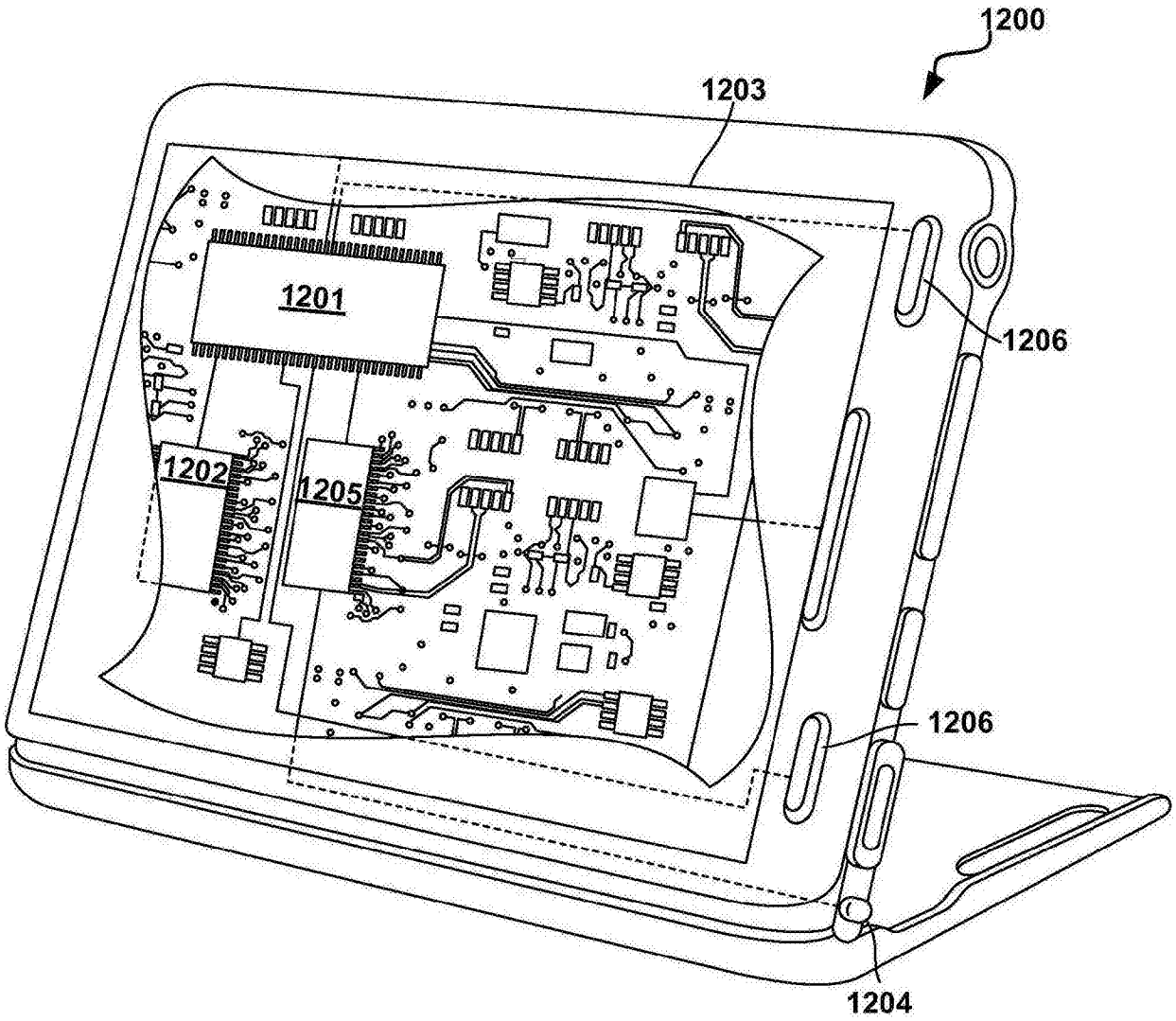


图 12

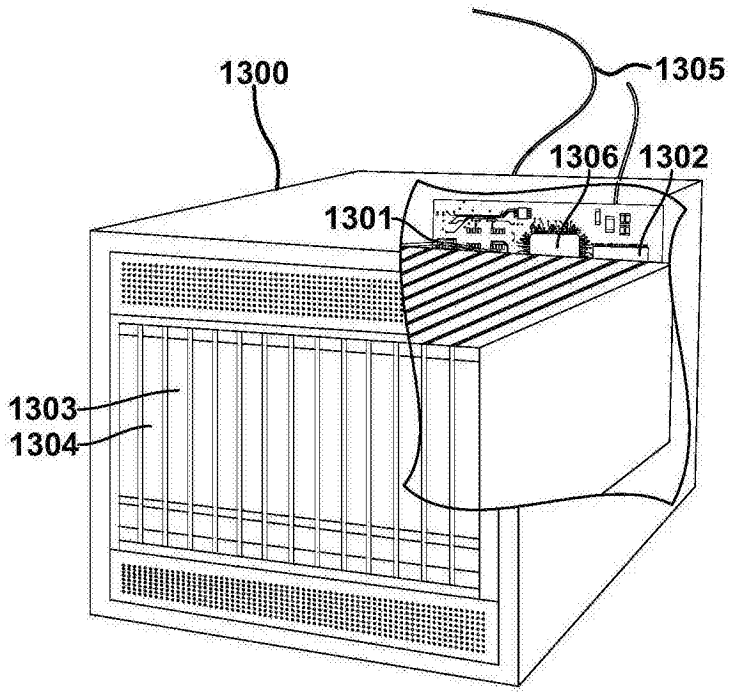


图 13