(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105745663 B
(45)授权公告日 2018.11.16

(21)申请号 201380081043.0
(22)申请日 2013.12.19
(65)同一申请的已公布的文献号
申请公布号 CN 105745663 A
(43)申请公布日 2016.07.06
(85)PCT国际申请进入国家阶段日
2016.05.19
(86)PCT国际申请的申请数据
PCT/US2013/076489 2013.12.19
(87)PCT国际申请的公布数据
WO2015/094271 EN 2015.06.25
(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 T·M·科兰伯格 I·塔托里安
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 黄嵩泉
(51)Int.Cl.
G06F 21/50(2006.01)
G06F 11/30(2006.01)
(56)对比文件
US 2012110174 A1,2012.05.03,
US 2013097709 A1,2013.04.18,
CN 1221912 A,1999.07.07,
CN 102638617 A,2012.08.15,
CN 1860476 A,2006.11.08,
CN 101572691 A,2009.11.04,
US 2006020814 A1,2006.01.26,
审查员 邱爽

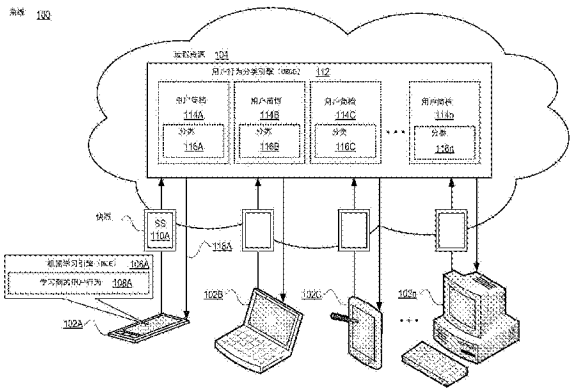
权利要求书3页 说明书12页 附图4页

(54)发明名称

包括机器学习快照评估的保护系统

(57)摘要

本公开涉及一种包括机器学习快照评估的保护系统。设备可以包括用于生成设备操作的快照的机器学习引擎(MLE)。MLE可以使用快照中的活跃操作或计划操作以学习用户行为。一旦为设备建立了正常的用户行为,MLE就可能能够确定快照何时包括可能指示对设备的威胁的不寻常行为。被确定为包括不寻常行为的快照可以被传输到远程资源以进行评估。远程资源可以至少包括用户行为分类引擎(UBCE),所述UBCE用于通过将用户行为表征为至少一种用途类型而对用户行为进行分类。可以由UBCE分析快照以便判定潜在的威胁是否存在于设备中,并且可将威胁分析提供给设备以进行评估和/或校正动作。



CN 105745663 B

1.一种配置成用于机器学习快照评估的设备,包括:

通信模块,所述通信模块用于至少与远程资源交互;

存储器模块,所述存储器模块用于至少存储学习到的用户行为;以及

机器学习引擎,所述机器学习引擎用于:

接收与所述设备的用户相关联的用户数据;

生成设备操作的快照,所述快照用于标识生成所述快照时所述设备中的至少一个活跃操作和生成所述快照时所述设备中的至少一个计划操作;

基于对所述快照与所述学习到的用户行为的比较来判定不寻常的用户行为是否已发生;

响应于确定了不寻常的用户行为已发生,使得所述通信模块将所述快照和所述用户数据传输到所述远程资源;

经由所述通信模块从所述远程资源接收威胁分析,所述威胁分析是响应于所述快照的所述传输而接收的;以及

至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁。

2.如权利要求1所述的设备,其中,所述机器学习引擎进一步用于:

判定所述设备是否是新的;以及

如果确定了所述设备是新的,则至少将所述快照和所述用户数据传输到所述远程资源。

3.如权利要求1所述的设备,其中,所述机器学习引擎进一步用于:基于经由所述通信模块而从所述远程资源接收到的验证的结果来判定所述设备中是否需要校正动作。

4.如权利要求1所述的设备,其中,所述不寻常的用户行为包括常见的活跃操作或计划操作的缺失、或者新的活跃操作或计划操作的发生。

5.如权利要求1所述的设备,其中,所述机器学习引擎进一步用于:验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名。

6.如权利要求1所述的设备,其中,所述机器学习引擎进一步用于基于以下比较来学习用户行为:将在所述快照中标识的所述至少一个活跃操作或计划操作与存储在所述存储器模块中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。

7.如权利要求1所述的设备,其中,所述机器学习引擎用于判定不寻常的用户行为是否已发生包括:所述机器学习引擎用于基于所述学习到的用户行为来判定所述至少一个活跃操作或计划操作是否是未预期到的。

8.一种用于机器学习快照评估的方法,包括以下步骤:

接收与设备的用户相关联的用户数据;

生成所述设备中的至少一个计划操作和至少一个活跃操作的快照;

基于对所述快照与存储在所述设备中的学习到的用户行为的比较来判定不寻常的用户行为是否已发生;

响应于确定了不寻常的用户行为已发生,使得所述快照和所述用户数据被传输到远程资源;

响应于所述快照的所述传输而从所述远程资源接收威胁分析;以及

至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁。

9.如权利要求8所述的方法,进一步包括以下步骤:

判定所述设备是否是新的;以及

如果确定了所述设备是新的,则至少将所述快照和所述用户数据传输到所述远程资源。

10.如权利要求8所述的方法,进一步包括以下步骤:

基于从所述远程资源接收到的验证的结果来判定在所述设备中是否需要校正动作。

11.如权利要求8所述的方法,其中,所述不寻常的用户行为包括常见的活跃操作或计划操作的缺失、或者新的活跃操作或计划操作的发生。

12.如权利要求8所述的方法,进一步包括以下步骤:

验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名。

13.如权利要求8所述的方法,进一步包括以下步骤:

基于以下比较来学习用户行为:将在所述快照中标识的所述至少一个活跃操作或计划操作与存储在所述设备中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。

14.如权利要求8所述的方法,其中,判定不寻常的用户行为是否已发生的步骤包括以下步骤:基于所述学习到的用户行为来判定所述至少一个活跃操作或计划操作是否是未预期到的。

15.一种用于机器学习快照评估的系统,所述系统包括:

用于接收与设备的用户相关联的用户数据的装置;

用于生成所述设备中的至少一个计划操作和至少一个活跃操作的快照的装置;

用于基于对所述快照与存储在所述设备中的学习到的用户行为的比较来判定不寻常的用户行为是否已发生的装置;

用于响应于确定了不寻常的用户行为已发生而使得所述快照和所述用户数据被传输到远程资源的装置;

用于响应于所述快照的所述传输而从所述远程资源接收威胁分析的装置;以及

用于至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁的装置。

16.如权利要求15所述的系统,进一步包括:

用于判定所述设备是否为新的装置;以及

用于如果确定了所述设备是新的则至少将所述快照和所述用户数据传输到所述远程资源的装置。

17.如权利要求15所述的系统,进一步包括:

用于基于从所述远程资源接收到的验证的结果来判定在所述设备中是否需要校正动作的装置。

18.如权利要求15所述的系统,其中,所述不寻常的用户行为包括常见的活跃操作或计划操作的缺失、或者新的活跃操作或计划操作的发生。

19.如权利要求15所述的系统,进一步包括:

用于验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名的装置。

20.如权利要求15所述的系统，进一步包括：

用于基于以下比较来学习用户行为的装置：将在所述快照中标识的所述至少一个活跃操作或计划操作与在存储在所述设备中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。

21.如权利要求15所述的系统，其中，所述用于判定不寻常的用户行为是否已发生的装置包括用于基于所述学习到的用户行为来判定所述至少一个活跃操作或计划操作是否是未预期到的装置。

22.一种机器可读介质，包括多条指令，响应于在计算设备上执行所述多条指令，所述多条指令使所述计算设备执行如权利要求8至14中的任一项所述的方法。

包括机器学习快照评估的保护系统

技术领域

[0001] 本公开涉及保护系统，并且更具体地涉及一种具有用于评估设备操作的快照的机器学习引擎的威胁监测系统。

背景技术

[0002] 现代设备日益依赖于众多电子技术来进行日常交互。例如，正在使用电子通信来进行个人和专业通信、购物交易、账户访问、金融交易、合同协议等。这种增加的依赖性的结果是，正在电子设备上存储过多的个人、私有和/或机密信息。可以存储个人和/或商业标识信息、地址信息、账户标识符、医疗数据、关系信息等以支持提供进行电子交易功能的各种应用或接口。个人、私有和/或机密信息在一个位置的可用性对于寻求将此类信息用于自身利益的未授权方可能是有吸引力的。结果是，在电子设备中实现保护性措施对于防止个人、私有和/或机密信息落入坏人之手是必要的。

[0003] 典型的保护模型可以包括安装在设备中用于监测威胁的软件组件。软件组件可以由集中式主体管理，此集中式主体提供对软件组件的更新和/或用于监测威胁的规则。虽然这个架构在某种程度上已经是有效的，但是它已经成为标准过久，使得许多攻击(例如，恶意软件(诸如，病毒或蠕虫)、尝试未授权访问等)已经被专门设计以克服这种类型的保护系统。例如，可更改恶意软件的外观以便绕过监测规则，或者恶意软件可以被插入到低级设备操作中(例如，在比保护组件更高的特权等级下操作)来绕过检测。如果不能由设备中的本地保护性措施检测到攻击，则可认为此设备为对此攻击无防备。

附图说明

[0004] 随着以下具体实施方式的进行且在参考附图之后，要求保护的主题的各实施例的特征和优点将变得明显，其中相似的参考号指示相似的部件，并且在附图中：

[0005] 图1示出根据本公开的至少一个实施例的包括机器学习快照评估的示例保护系统；

[0006] 图2示出根据本公开的至少一个实施例的用于设备的示例配置；

[0007] 图3示出根据本公开的至少一个实施例的用于远程资源的示例配置；以及

[0008] 图4示出根据本公开的至少一个实施例的用于包括机器学习快照评估的保护系统的示例操作。

[0009] 尽管将参考说明性实施例进行以下具体实施方式，但是其许多替代、修改和变型将对本领域普通技术人员将是明显的。

具体实施方式

[0010] 本公开涉及一种包括机器学习快照评估的保护系统。在一个实施例中，设备可以包括用于生成设备操作的快照的机器学习引擎(MLE)。所述MLE可以利用所述快照中的活跃操作或计划操作以学习用户行为。一旦为所述设备建立了正常的用户行为，MLE就可能能够

确定快照何时包括可能指示对所述设备的威胁的不寻常行为。被所述MLE确定为包括不寻常行为的快照可以传输到远程资源以进行评估。所述远程资源可以至少包括例如用户行为分类引擎(UBCE),所述UBCE可以通过将用户行为表征为至少一种用途类型来对所述用户行为进行分类。可以由所述UBCE分析所述快照以判定潜在的威胁是否存在于所述设备中,并且可将所述威胁分析提供给所述设备以进行评估和/或校正动作。在一个实施例中,如果设备对于系统是新的,则所述MLE还可以将快照和用户数据提供给所述远程资源。所述远程资源可以创建用户账户(如果必要),将所述设备与所述用户账户相关联,并且分析所述设备以判定所述设备是否是"干净的"(例如,不具有威胁)。

[0011] 在一个实施例中,配置成用于机器学习快照评估的设备可以包括例如通信模块、存储器模块和MLE。所述通信模块用于至少与远程资源交互。所述存储器模块可以用于至少存储学习到的用户行为。所述MLE可以用于:生成设备操作的快照;基于鉴于所述学习到的用户行为对所述快照的评估来判定不寻常的用户行为是否已发生;如果确定不寻常的用户行为已发生,则使所述通信模块将所述快照和用户数据传输到所述远程资源;经由所述通信模块从所述远程资源接收威胁分析,所述威胁分析是响应于所述快照的传输而接收到的;以及至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁。

[0012] 在一个实施例中,所述MLE可以进一步用于:判定所述设备是否是新的;以及如果确定了所述设备是新的,则至少将所述快照和所述用户数据传输到所述远程资源。所述MLE可以进一步用于:基于经由所述通信模块而从所述远程资源接收到的验证的结果来判定在所述设备中是否需要校正动作。所述MLE用于生成设备操作的快照可包括所述机器学习引擎用于基于以下至少一项来标识所述设备中的至少一个操作:在生成快照时在所述设备中的活跃操作或在生成快照时在所述设备中的计划操作。所述MLE可以进一步用于:验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名。所述MLE可以进一步用于基于以下比较来学习用户行为:将在所述快照中标识的所述至少一个活跃操作或计划操作与存储在所述设备中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。所述MLE用于判定不寻常的用户行为是否已发生可以包括:所述MLE用于基于学习到的用户行为来判定所述至少一个活跃操作或计划操作是否是未预期到的。

[0013] 在相同或不同的实施例中,配置成用于作为远程资源操作的设备可以包括例如通信模块和UBCE。所述通信模块可以用于至少与用户设备交互。所述UBCE可以用于:从用户设备接收至少用户设备操作的快照和用户数据;至少基于所述用户数据来判定是否需要新的用户账户;如果确定了需要新的用户账户,则建立新的用户账户;将所述用户设备与现有的用户账户或所述新的用户账户相关联;至少基于所述快照来验证所述用户设备是否是新的;以及将所述验证的结果提供给所述用户设备。

[0014] 所述UBCE可以进一步用于至少基于所述快照来开发用户分类。所述UBCE用于开发用户分类可以包括:所述UBCE用于至少基于所述快照来表征所述设备的至少一种用途类型。符合本公开的一种用于机器学习快照评估的方法可以包括例如以下步骤:生成设备中的操作的快照;基于鉴于存储在所述设备中的学习到的用户行为对快照的评估来判定不寻常的用户行为是否已发生;如果确定了不寻常的用户行为已发生,则致使将所述快照和用户数据传输到远程资源;响应于所述快照的传输而从所述远程资源接收威胁分析;以及至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁。符合本公开的另一种用于机

器学习快照评估的方法可以包括例如以下步骤：在远程资源中，至少从用户设备接收用户设备操作的快照和用户数据；至少基于所述用户数据来判定是否需要新的用户账户；如果确定了需要新的用户账户，则建立新的用户账户；将所述用户设备与现有的用户账户或所述新的用户账户相关联；至少基于所述快照来验证所述用户设备是否是新的；以及将所述验证的结果提供给所述用户设备。

[0015] 图1示出根据本公开的至少一个实施例的包括机器学习快照评估的示例保护系统。系统100可以包括至少一个设备102(例如，设备102A、设备102B、设备102C…设备102n或统称为“设备102A...n”)和远程资源104。在图1中公开的示例中，仅出于解释的目的已经公开了四个(4个)设备102A...n。在实践中，设备的数量可以取决于实现方式而改变。设备102A...n的示例可以包括但不限于，移动通信设备(诸如，基于安卓®OS、iOS®、Windows®OS、Mac®OS、Tizen OS、火狐OS、黑莓®OS、Palm®OS、塞班®OS等的蜂窝手持式设备或智能电话)、移动计算设备(诸如，平板计算机，像iPad®、Surface®、Galaxy Tab®、Kindle Fire®等等)、包括英特尔公司制造的低功率芯片组的超极本®、上网本、笔记本、膝上型计算机、掌上计算机等、典型固定式的计算设备(诸如，台式计算机、服务器、智能电视)、小形状因子计算解决方案(例如，用于空间受限应用、电视机顶盒等)(像来自英特尔公司的下一代计算单元(NUC)平台)。远程资源104可以包括可由设备102A...n经由局域网(LAN)、广域网(WAN)(诸如，因特网)等访问的至少一个计算设备。在一个实施例中，远程资源104可以包括在云计算配置中组织的一个或多个服务器。

[0016] 图1的示例进一步包括针对设备102示出的、还可适用于设备102B...n但出于清晰目的被省略的各种特征。在一个实施例中，设备102A可以至少包括MLE 106A。MLE 106A可以包括配置成用于通过生成设备操作的快照(SS)110A来学习用户行为108A的装备和/或软件。学习到的用户行为108A可以包括例如，通常作为由设备102A的至少一个用户的正常使用的结果而在设备102A中发生的操作。可以在由设备102A的用户在MLE 106A中设置的时间中由MLE 160周期性地生成SS 110A，应用户手动的请求、在设备102A中的事件的发生时等手动生成SS 110A。SS 110A可以包括例如在生成SS 110A时在设备102中活跃的或者在生成SS 110A时计划在设备102中操作的装备和/或软件的标识。可以在SS 110A内标识的各种活跃操作的示例可以包括以下各项中的至少一项：运行的应用、网络活动、注册表活动、文件系统活动、进程和线程活动或概况分析(profiling)活动。SS 110A还可以标识从例如以下各项中的至少一项中导出的各种计划的操作：与运行、运行一次、开机、安装的组件对应的注册表设置、与浏览器相对应的注册表设置(诸如，协议、ShellEx等)、与互联网浏览器、OS调度器、服务、驱动程序、编解码器、boot.exe、图像劫持、AppInit、已知dll、WinLogon、Winsock提供商、打印机监视器、本地安全认证(LSA)提供商、网络提供商等对应的注册表设置。在一个实施例中，SS 110A可以进一步包括捕捉到SS 110A时的日期和时间以及有关设备102A的细节，所述细节诸如例如，制造商、型号、配置标识符、序列号、建立日期、OS、活跃网络连接，等等。

[0017] 在一个实施例中，MLE 106A可以至少将先前生成的SS 110A存储在设备102A中。随后，MLE 106A可能能够将近期捕捉的SS 110A至少与先前生成的SS 110A进行比较，以便学习用户行为108A。可以使用例如机器学习算法重复地从一个SS 110A到另一个来学习用户行为108A，所述机器学习算法跟踪发生的或计划将发生的操作。在多个SS 110A中出现相同

的操作可以指示，操作的发生可以与设备102A中的正常操作相关联。以此方式学习，MLE 106A可以开始制定构成用户行为108A的操作模式。

[0018] 在MLE 106A已经学习了用户行为108A之后(例如，当评估了在正在使用设备102A的时间段内捕捉的一系列SS 110A之后)，MLE 106A随后可以开始对后续的SS 110A评估不寻常的行为(例如，作为设备102中的可能威胁的指示符)。例如，常见操作的缺失或者新的操作的发生可以指示在设备102A中缺失了某种事物。MLE 106A可以检测例如不常由用户访问的资源正在当前的SS 110A中被访问，通常在快照中出现的操作不再运行(或者可能已经由另一类似的操作替换)，新的软件已经被加载到不与通常由用户访问的其他软件对应的设备102A，等等。在一个实施例中，MLE 106A还可以利用预测性分析技术(诸如例如，贝叶斯网络)，以便标识从一个SS 110A移动到另一个的可能性。此知识可以允许对可疑的离群值的更快的标识，并且允许标识何时存在恶意软件可能干扰设备102A中的快照生成以及例如当系统已经受到危害时使得SS 110A看起来是良性的迹象。回滚到如上文讨论的先前快照仅是可以利用专家试探法的一个示例。在相同或不同的实施例中，用户可以具有将SS 110A存储在安全位置(例如，私有云)中且随后仅与全局云共享对预测性分析有用的数据的选项，以便增加其个人隐私性。这将在维护用户的隐私性的同时提供共享学习的益处。

[0019] 在MLE 106A确定了SS 110A可能包括不寻常的行为之后，MLE 106A可以使SS 110A被传输到远程资源104。远程资源104可以包括UBCE 112以便对用户行为108A进行分类，并且基于此分类来诊断可能构成对设备102A的威胁的异常行为。在一个实施例中，UBCE 112可以基于设备102A的用途类型来对用户行为108A进行分类。示例用途类型可以包括但不限于诸如，游戏系统(例如，用于玩游戏)，例如，商业系统(例如，用于文字处理、电子表格等)、教育系统(例如，用于执行教学程序)、设计系统(例如，用于计算机辅助绘图(CAD)或计算机辅助制造(CAM))、web浏览系统等。这些类型可以包括进一步的特性，诸如，年龄(例如，用于幼儿的教育系统)、风险类别(例如，通常访问有风险的或可疑网站的web浏览器系统)等等。分类可以包括多于一种类型，并且可以基于新的信息(例如，经由SS 110A接收到的信息)连续地更新经分类的类型。

[0020] 可以在UBCE 112中注册用户时发起分类。在UBCE 112中的注册可以通过例如由用户手动注册(例如，经由网页)，由设备(例如，设备102a)自动注册用户，或提示用户注册等而发生。注册可以包括通知用户关于共享个人和/或设备数据的信息，使得用户可以作出关于参与系统100的知情决定。用户注册可以导致用户简档114A至少包括用户标识信息。用户简档114A还可以包括其他信息，诸如，用户住所信息、用户商业信息、用户账单信息(例如，如果远程资源104与支付服务相关联)，等等。设备102A以及在系统100中登记的用户的任何其他设备可以与用户简档114A相关联，并且分类116A可以基于用户简档114A和/或从设备102A中的MLE 106A接收到SS 110中的信息而开始为设备102A生成。在一个实施例中，“新的”设备可以经历初始验证以确保此设备是干净的(例如，没有威胁，并且准备好发起用户行为学习)。新的设备可以是例如直接从制造商、从零售商等处获得的全新的设备、未使用的设备或仅是与用户简档114A新关联的设备。初始验证可能是重要的，因为用户可能相信设备102A是干净的(例如，是来自制造商的新的且未更改的，或者至少没有恶意软件)，但是实际上可能已经添加/移除/更改了硬件和/或软件，恶意软件可能已经发现进入到设备上的方式，等等。在操作的示例中，新的设备102A可以将第一SS 110A传输至UBCE 112以进行

验证。UBCE 112可以从各种设备(例如,设备102B...n)接收数据,并且能够从这个数据中制定基线操作配置,可将SS 110A与此基线操作配置比较以验证设备102A是干净的。例如,UBCE 112可以从用户简档114A和/或SS 110A中确定设备102A的制造商、型号、配置、建立日期、OS等,可以使用这个数据以便基于从其他设备(例如,SS 110B...n)接收到的信息来确定设备102A的干净配置,并且随后可以将SS 110A与此干净配置比较以判定SS 110A中是否存在差异。随后,UBCE 112可以将来自验证的、指出配置中的任何差异的结果提供给设备102A。随后,可使设备102A的用户确信他们的设备在学习用户行为108A之前从干净的状态开始。此外,初始的SS 110A可以为设备102A提供基线配置以供由UBCE在生成分类116A时使用。

[0021] 在已经建立了分类116A之后,无论何时检测到不寻常行为,设备102A(例如,MLE 106A)都可以将SS 110A(例如,如果还未包含在SS 110A中则连同标识用户的信息一起)传输到远程资源104。随后,UBCE 112可以将SS 110A与分类116A进行比较以判定此行为是否符合具有分类116A的设备。例如,UBCE 112可以基于从其他设备(例如,设备102B…n)接收到的数据,在与设备102A相同或类似的分类116A中生成“模型配置”(例如,示例性SS 110)。在生成示例性SS 110时,还可以考虑其他因素,诸如,设备102A的类型、设备102A的制造商/型号/建立年份,等等。随后,UBCE 112可以继续将示例性SS 110的内容与SS 110A进行比较以便判定在SS 110A中标识的操作中的任何操作是否是可疑的。如果SS 110A中的行为被认为有问题,则UBCE 112可以将标识设备102A中可能存在的威胁的威胁分析118A传输至设备102A。在一个实施例中,MLE 106A可以评估从UBCE 112接收到威胁分析118以判定设备中是否存在潜在的威胁。如果相信存在威胁,则MLE 106可以触发校正动作,所述校正动作诸如但不限于,向用户通知潜在的威胁,隔离包括潜在威胁的文件,删除包括潜在威胁的文件,禁用网络访问和/或其他动作以使威胁无效。

[0022] 图2示出根据本公开的至少一个实施例的用于设备102A’的示例配置。具体地,设备102A’可能能够执行诸如图1中公开的示例功能。然而,设备102A’仅旨在作为可以在符合本公开的实施例中使用的装备的示例,并且不旨在将这些各种实施例限制为任何特定的实现方式。在图2中公开的设备102A’的示例配置还可以适用于也在图1中公开的设备102B...n。

[0023] 设备102A’可以包括例如配置成用于管理设备操作的系统模块200。系统模块200可以包括例如处理模块202、存储器模块204、功率模块206、用户接口模块208以及通信接口模块210。设备102A’可进一步包括通信模块212和MLE 106’。尽管通信模块212和MLE 106’已示出为与系统模块200分开,但是仅出于解释的目的而提供在图2中示出的示例实现方式。与通信模块212和/或MLE 106’相关联的功能中的一些或全部也可以并入在系统模块200中。

[0024] 在设备102A’中,处理模块202可以包括位于分开的组件中的一个或多个处理器,或者可替代地,可以包括具体化在单个组件中(例如,在片上系统(SoC)配置中)的一个或多个处理核以及任何处理器相关的支持电路(例如,桥接接口等)。示例处理器可以包括但不限于,可从英特尔公司获得的各种基于x86的微处理器(包括奔腾、至强、安腾、赛扬、凌动、i系列酷睿产品族中的那些微处理器)、高级RISC(例如,精简指令集计算)机器或“ARM”处理器,等等。支持电路的示例可以包括芯片组(例如,可从英特尔公司获得的北桥、南桥等),这

些芯片组配置成用于提供接口，处理模块202可通过此接口与可以在设备102'内在不同速度下、在不同总线上等操作的其他系统组件交互。与支持电路相关联的功能中的一些或全部还可以被包括在与处理器相同的物理封装中(例如，诸如被包括在可从英特尔公司获得的Sandy Bridge处理器族中)。

[0025] 处理模块202可以配置成用于执行设备102A'中的各种指令。指令可以包括程序代码，这些程序代码配置成用于使处理模块202执行与读取数据、写入数据、处理数据、制定数据、转换数据、变换数据等相关的活动。信息(例如，指令、数据等)可以存储在存储器模块204中。存储器模块204可以包括固定或可移除格式的随机存取存储器(RAM)或只读存储器(ROM)。RAM可以包括配置成用于在设备102A'的操作期间保持信息的易失性存储器，诸如例如，静态RAM(SRAM)或动态RAM(DRAM)。ROM可以包括配置成用于当设备102A'激活时提供指令的基于BIOS、UEFL等的非易失性(NV)存储器模块、诸如电可编程ROM(EPROM)之类的可编程存储器、闪存等。其他固定和/或可移除存储器可以包括但不限于：磁存储器，诸如例如，软盘、硬盘驱动器等；电子存储器，诸如，固态闪存(例如，嵌入式多媒体卡(eMMC)等)、可移除存储器卡或棒(例如，微型存储设备(uSD)、USB等)；光学存储器，诸如，基于紧致盘的ROM(CD-ROM)、数字视频盘(DVD)、蓝光盘，等等。

[0026] 功率模块206可以包括内部电源(例如，电池、燃料电池等)和/或外部电源(例如，机电或太能发电机、电网、燃料电池等)以及相关电路，所述相关电路配置成用于将操作所需的功率供应给设备102A'。用户接口模块208可以包括用于允许用户与设备102A'交互的装备和/或软件，诸如例如，各种输入机制(例如，话筒、开关、按钮、旋钮、键盘、扬声器、触敏表面、配置成用于捕捉图像和/或感测接近度、距离、运动、姿势、定向等的一个或多个传感器)以及各种输出机制(例如，扬声器、显示器、发光/闪烁指示器、用于振动、运动等的机电组件)。用户接口模块208中的装备可以并入在设备102A'中和/或可以经由有线或无线通信介质而耦合到设备102A'。

[0027] 通信接口模块210可以配置成用于管理通信模块212的分组路由和其他控制功能，这可以包括配置成用于支持有线和/或无线通信的资源。在一些实例中，设备102A'可以包括全都由集中式通信接口模块210管理的多于一个的通信模块212(例如，包括用于有线协议和/或无线无线电的分开的物理接口模块)。有线通信可以包括串行和并行有线介质，诸如例如，以太网、通用串行总线(USB)、火线、数字视频接口(DVI)、高清晰度多媒体接口(HDMI)，等等。无线通信可以包括例如，近接近度无线介质(例如，射频(RF)，诸如，基于近场通信(NFC)标准、红外(IR)等)、短距离无线介质(例如，蓝牙、WLAN、Wi-Fi等)、长距离无线介质(例如，蜂窝广域无线电通信技术、基于卫星的通信等)、经由声波的电子通信，等等。在一个实施例中，通信接口模块210可以配置成用于防止通信模块212中活跃的无线通信彼此干扰。当执行此功能时，通信接口模块210可以基于例如等待传输的消息的相对优先级来调度通信模块212的活动。尽管在图2中公开的实施例示出通信接口模块210与通信模块212分开，但是通信接口模块210和通信模块212的功能合并到相同的模块中也可以是可能的。

[0028] 在图2中公开的示例中，MLE 106'可以配置成用于至少与存储器模块206、通信模块212和/或用户接口模块208交互。在操作的示例中，MLE 106'可以生成SS 110A，并且可以将SS 110A与存储在存储器模块204中的先前的SS110A进行比较，以便学习用户行为108A。在学习了用户行为108A之后，如果确定了不寻常的行为存在于SS 110A中，则MLE 106'可以

使通信模块212将SS 110A传输至UBCE 112。稍后，ME 106'可以经由通信模块212来接收威胁分析118A。随后，MLE 106'可以评估威胁分析118A以判断任何潜在的威胁是否存在于设备102A'中。如果任何威胁确定为存在，则MLE 106A'可以致使经由用户接口模块208而将向用户通知潜在威胁的通知呈现给设备102A'的用户，和/或可以致使在设备102A'中执行校正动作。

[0029] 图3示出根据本公开的至少一个实施例的远程资源104'的示例配置。已经在图3中使用相同的附图参考标号标识了与参照在图2中呈现的示例设备102A'相同或基本上类似的模块和/或其他元件。

[0030] 远程资源104'可以是用于执行诸如在图1的示例中公开的那些活动之类的各种活动的独立式计算设备、或单独或协同操作的多个计算设备中的一个计算设备。在远程资源104'中，用户接口模块208已经被示出为是任选的，因为一些设备(例如，服务器)可能不包括用户接口模块208，而是可能依赖于其他设备(例如，远程终端)来促进与远程资源104'之间的用户交互。在一个实施例中，UBCE 112'可以至少与处理模块202、存储器模块204和通信模块201交互。在操作的示例中，UBCE 112'可以经由通信模块212而从设备102A中的ME 106A接收SS 110A。随后，UBCE 112'可依赖于处理模块202和/或存储器模块204来定位对应于设备102A的用户的用户简档114A，从而访问分类116A并且基于分类116A来生成模型配置(例如，示例性SS 110)。此外，处理模块202和/或存储器模块204可以基于将SS 110A与示例性SS 110进行比较来辅助确定任何威胁是否存在于设备102A'中。随后，UBCE 112'可以使通信模块212至少将源自SS 110A的分析的威胁分析118A传输到设备102A。

[0031] 图4示出根据本公开的至少一个实施例的、用于包括机器学习快照评估的保护系统的示例操作。在操作400中，可以(例如，由设备中的MLE)生成设备操作的快照。可以自动地(例如，周期性地、在发生事件时)或者可由设备的用户手动地触发快照。随后，在操作402中，可作出关于用户和/或设备对于系统是否是新的(例如，还未在远程资源中注册)的判定。如果在操作402中确定了设备是新的，则在操作404中，可以将快照和用户数据(例如，至少标识用户的数据)传输到远程资源。随后，在操作406中，可作出关于用户是否是新用户(例如，还未在远程资源中注册)的判定。如果在操作406中确定了用户还未向远程资源注册，则在操作408中，可以为用户创建新的用户简档。当在操作406中确定了用户简档已经存在之后，或者当在操作408中创建了用户简档之后，在操作410中，随后可将设备与此用户简档相关联。随后，在操作412中，可执行验证以判定设备是否是干净的(例如，设备的快照包含将针对这种类型、制造商、型号、建立日期、具有某个OS等的新设备预期的操作)。随后，可将验证的结果提供给设备，使得用户和/或MLE可以作出使任何检测到的威胁、漏洞或缺陷无效所需的任何改变。随后，可以发起分类，这由至操作416的虚线箭头指示，在操作416中，远程资源中的UBCE可以开始分类设备由用户使用的至少一种用途类型(例如，游戏设备、web浏览、商业/教育/设计用途，等等)。

[0032] 如果在操作402中确定了用户和设备两者都不是新的，则在操作418中，可以进一步作出关于是否已经学习到设备的用户行为的判定。例如，可能需要一系列快照来达到学习了新设备的用户行为的某个点。如果在操作418中确定了还未学习到用户行为，则在操作420中，MLE可以继续基于快照中的活动来学习用户行为。操作420之后可以是返回操作400以生成附加的快照。如果在操作418中确定了已经学习到用户行为，则在操作422中，可以作

出关于快照是否包含任何不寻常行为(例如,与学习到的用户行为不一致的操作)的进一步判定。在操作422中作出的快照不包含任何不寻常的用户行为的确定之后可以是操作420,在操作420中,包含在快照中的活动可以用于继续细化由MLE学习到的用户行为。如果在操作422中确定了快照包含不寻常的行为,则在操作424中,快照可以传输到远程资源(例如,包括用户数据)。

[0033] 当在远程资源中接收到快照时,随后,在操作426中,可作出关于是否已经基于用户行为对设备的至少一种用途类型分类的判定。如果在操作426中确定了还未对用户行为进行分类,则在操作416中,对分类的开发可以继续直到完成为止(例如,可能需要更多的快照来完成分类)。另一方面,如果在操作426中确定了分类完成,则在操作428中,可以基于鉴于分类评估快照(例如,基于对应于分类中的至少一种用途类型的示例性快照)作出关于设备是否包括潜在威胁的进一步判定。如果在操作428中确定了没有潜在的威胁存在于快照中,则在操作430中,可利用快照中的活动来更新分类。如果在操作428中,基于快照而确定了至少一个潜在威胁存在于设备中,则在操作432中,可以将威胁分析传输到设备,威胁分析描述例如在操作428中确定的对设备的任何潜在威胁。设备可以接收威胁分析,并且在操作434中,可以在需要时评估威胁分析和/或对此威胁分析作出反应(例如,可以执行预防措施、校正动作,等等)。

[0034] 尽管图4可以示出根据实施例的操作,但是将要理解的是,并非在图4中描绘的所有操作对于其他实施例都是必需的。实际上,在本文中完全构想了在本公开的其他实施例中,能以未在任何附图中明确示出的方式组合图4中描绘的操作和/或本文中描述的其他操作,但是仍完全符合本公开。由此,涉及未在一个附图中确切地示出的特征和/或操作的权利要求被认为在本公开的范围和内容内。

[0035] 如在本申请中和在权利要求书中所使用,由术语“和/或”连结的项目列表可意味着所列出的项目的任何组合。例如,短语“A、B和/或C”可以指A;B;C;A和B;A和C;B和C;或A、B和C。如在本申请中和在权利要求书中所使用,由术语“...中的至少一个”连结的项目列表可以意味着所列出的项目的任何组合。例如,短语“A、B或C中的至少一个”可以意味着A;B;C;A和B;A和C;B和C;或A、B和C。

[0036] 如在本文中任何实施例中所使用,术语“模块”可以是指配置成用于执行任何前述操作的软件、固件和/或电路。软件可以具体化为记录在非暂态机器可读存储介质上的软件包、代码、指令、指令集和/或数据。固件可以具体化为硬编码(例如,非易失性的)在存储器设备中的代码、指令或指令集和/或数据。如在本文中的任何实施例中所使用,“电路”可以单独地或以任何组合包括例如,硬连线电路、可编程电路(诸如,包括一个或多个单独的指令处理核的计算机处理器)、状态机电路和/或存储由可编程电路执行的指令的固件。这些模块可以共同地或单独地具体化为形成较大的系统的部分的电路,所述较大的系统例如,集成电路(IC)、片上系统(SoC)、台式计算机、膝上型计算机、平板计算机、服务器、智能电话,等等。

[0037] 可以在包括一种或多种存储介质(例如,非暂态存储介质)的系统中实现本文中所描述的操作中的任意操作,所述一种或多种存储介质在其上单独地或结合地存储指令,当由一个或多个处理器执行所述指令时,所述执行方法。在此,处理器可以包括例如,服务器CPU、移动设备CPU和/或其他可编程电路。同样,本文中所描述的操作旨在可以跨多个物理

设备(诸如,在多于一个的不同物理位置处的处理结构)分布。存储介质可以包括任何类型的有形介质,例如,任何类型的盘,包括硬盘、软盘、光盘、紧致盘只读存储(CD-ROM)、紧致盘可重写(CD-RW)、以及磁光盘;半导体器件,诸如,只读存储器(ROM)、随机存取存储器(RAM)(诸如,动态和静态RAM)、可擦可编程只读存储器(EPROM)、电可擦可编程只读存储器(EEPROM)、闪存、固态盘(SSD)、嵌入式多媒体卡(eMMC)、安全数字输入/输出(SDIO)卡、磁卡或光卡;或适合用于存储电子指令的任何其他类型的介质。其他实施例可以实现为由可编程控制器件执行的软件模块。

[0038] 由此,本公开涉及一种包括机器学习快照评估的保护系统。设备可以包括用于生成设备操作的快照的机器学习引擎(MLE)。所述MLE可以使用所述快照中的活跃操作或计划操作以学习用户行为。一旦为所述设备建立了正常的用户行为,所述MLE就可能能够确定快照何时包括可能指示对所述设备的威胁的不寻常行为。被确定为包括不寻常行为的快照可以传输到远程资源以进行评估。所述远程资源可以至少包括用户行为分类引擎(UBCE),所述UBCE用于通过将用户行为表征为至少一种用途类型来对所述用户行为进行分类。可以由所述UBCE分析所述快照以便判定潜在的威胁是否存在于所述设备中,并且可将所述威胁分析提供给所述设备以进行评估和/或校正动作。

[0039] 以下示例涉及进一步的实施例。如下文所提供,本公开的以下示例可以包括主题素材,诸如,设备、方法、用于存储指令的至少一种机器可读介质(当执行所述指令时,所述指令使机器基于方法来执行动作)、用于基于方法来执行动作的装置和/或包括机器学习快照评估的保护系统。

[0040] 根据示例1,提供了一种用于机器学习快照评估的设备。所述设备可以包括:通信模块,所述通信模块用于至少与远程资源交互;存储器模块,所述存储器模块用于至少存储学习到的用户行为;以及机器学习引擎,所述机器学习引擎用于:生成设备操作的快照;基于鉴于所述学习到的用户行为对所述快照的评估来判定不寻常的用户行为是否已发生;如果确定了不寻常的用户行为已,则使所述通信模块将所述快照和用户数据传输到所述远程资源;经由所述通信模块从所述远程资源接收威胁分析,所述威胁分析是响应于所述快照的所述传输而接收的;以及至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁。

[0041] 示例2可以包括示例1的元素,其中,所述机器学习引擎进一步用于:判定所述设备是否是新的;以及如果确定了所述设备是新的,则至少将所述快照和所述用户数据传输到所述远程资源。

[0042] 示例3可以包括示例1至2中的任一项的元素,其中,所述机器学习引擎进一步用于:基于经由所述通信模块从所述远程资源接收到的验证的结果来判定在所述设备中是否需要校正动作。

[0043] 示例4可以包括示例1至2中任一项的元素,其中,所述机器学习引擎用于生成设备操作的快照包括:所述机器学习引擎用于基于以下至少一项来标识所述设备中的至少一个操作:在生成所述快照时在所述设备中的活跃操作;或在生成所述快照时在所述设备中的计划操作。

[0044] 示例5可以包括示例4的元素,其中,所述活跃操作包括以下各项中的至少一项:运行的应用、网络活动、注册表活动、文件系统活动、进程和线程活动或概况分析活动。

[0045] 示例6可以包括示例4的元素，其中，可从对应于以下各项中的至少一项中导出经调度的操作：对应于运行、运行一次、开机、安装的组件的注册表设置；对应于浏览器的注册表设置(包括协议或ShellEx)；对应于互联网浏览器、OS调度器中的任务、服务、驱动器、编解码器、boot.exe、图像劫持、Applnit、已知dll、WinLogon、Winsock提供商、打印机监视器、本地安全认证(LSA)提供商或网络提供商的注册表设置。

[0046] 示例7可以包括示例4的元素，其中，所述机器学习引擎进一步用于：验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名。

[0047] 示例8可以包括示例4的元素，其中，所述机器学习引擎进一步用于基于以下比较来学习用户行为：将在所述快照中标识的所述至少一个活跃操作或计划操作与存储在所述存储器模块中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。

[0048] 示例9可以包括示例4的元素，其中，该机器学习引擎用于确定是否已经发生不寻常用户行为包括该机器学习引擎用于基于该所学习的用户行为确定是否该至少一个活跃或计划操作是未预期的。

[0049] 根据示例10，提供了配置成作为远程资源操作的至少一个设备。所述至少一个设备可以包括：通信模块，所述通信模块用于至少与用户设备交互；以及用户行为分类引擎，所述用户行为分类引擎用于：从所述用户设备接收至少用户设备操作的快照和用户数据；至少基于所述用户数据来判定是否需要新的用户账户；如果确定了需要新的用户账户，则建立新的用户账户；将所述用户设备与现有的用户账户或新的用户账户相关联；至少基于所述快照来验证所述用户设备是否是新的；以及将所述验证的结果提供给所述用户设备。

[0050] 示例11可以包括示例10的元素，其中，所述用户行为分类引擎进一步用于：如果确定需要新的用户账户，则致使提示所述设备的用户提供用于设立新的用户账户的信息。

[0051] 示例12可以包括示例10至11中的任一项的元素，其中，所述用户行为分类引擎进一步用于至少基于所述快照来开发用户分类。

[0052] 示例13可以包括示例12的元素，其中，所述用户行为分类引擎用于开发用户分类包括：所述用户行为分类引擎用于至少基于所述快照表征所述设备的至少一种用途类型。

[0053] 根据示例14，提供了一种用于机器学习快照评估的方法。所述方法可以包括以下步骤：生成设备中的操作的快照；基于鉴于存储在所述设备中的学习到的用户行为对所述快照的评估来判定不寻常的用户行为是否已发生；如果确定了不寻常的用户行为已发生，则致使将所述快照和用户数据传输到远程资源；响应于所述快照的所述传输而从所述远程资源接收威胁分析；以及至少基于所述威胁分析来判定是否存在对所述设备的潜在威胁。

[0054] 示例15可以包括示例14的元素，并且可以进一步包括以下步骤：判定所述设备是否是新的；以及如果确定了所述设备是新的，则至少将所述快照和所述用户数据传输到所述远程资源。

[0055] 示例16可以包括示例14至15中的任一项的元素，并且可以进一步包括以下步骤：基于从所述远程资源接收到的验证的结果来判定在所述设备中是否需要校正动作。

[0056] 示例17可以包括示例14至15中的任一项的元素，其中生成设备的快照的步骤可包括以下步骤：基于以下至少一项来标识所述设备中的至少一个操作：在生成所述快照时在所述设备中的活跃操作；或在生成所述快照时在所述设备中的计划操作。

[0057] 示例18可以包括示例17的元素，其中，所述活跃操作包括以下各项中的至少一项：

运行的应用、网络活动、注册表活动、文件系统活动、进程和线程活动或概况分析活动。

[0058] 示例19可以包括示例17的元素，其中，可以从以下各项中的至少一项中导出经调度的操作：对应于运行、运行一次、开机、安装的组件的注册表设置；对应于浏览器的注册表设置(包括协议或ShellEx)；对应于互联网浏览器、OS调度器中的任务、服务、驱动器、编解码器、boot.exe、图像劫持、AppInit、已知dll、WinLogon、Winsock提供商、打印机监视器、本地安全认证(LSA)提供商或网络提供商的注册表设置。

[0059] 示例20可以包括示例17的元素，并且可以进一步包括以下步骤：验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名。

[0060] 示例21可以包括示例17的元素，并且可以进一步包括基于以下比较来学习用户行为：将在所述快照中标识的所述至少一个活跃操作或计划操作与存储在所述设备中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。

[0061] 示例22可以包括示例17的元素，其中判定不寻常的用户行为是否已发生的步骤包括以下步骤：基于所述学习到的用户行为来判定所述至少一个活跃操作或计划操作是否是未预期到的。

[0062] 根据示例23，提供了一种用于机器学习快照评估的方法。所述方法可以包括以下步骤：从用户设备接收至少用户设备操作的快照和用户数据；至少基于所述用户数据来判定是否需要新的用户账户；如果确定了需要新的用户账户，则建立新的用户账户；将所述用户设备与现有的用户账户或新的用户账户相关联；至少基于所述快照来验证所述用户设备是否是新的；以及将所述验证的结果提供给所述用户设备。

[0063] 示例24可以包括示例23的元素，并且可以进一步包括以下步骤：如果确定了需要新的用户账户，则致使提示所述设备的用户提供用于设立新的用户账户的信息。

[0064] 示例25可以包括示例23至24中任一项的元素，并且可以进一步包括以下步骤：至少基于所述快照、使用用户行为分类引擎来开发用户分类。

[0065] 示例26可以包括示例25的元素，其中，开发用户分类的步骤包括以下步骤：至少基于所述快照来表征所述设备的至少一种用途类型。

[0066] 根据示例27，提供了一种包括设备和远程资源的系统，所述系统布置成用于执行上述示例14至26中的任一项的方法。

[0067] 根据示例28，提供了一种芯片组，所述芯片组布置成用于执行上述示例14至26中的任一项的方法。

[0068] 根据示例29，提供了至少一种机器可读介质，包括多条指令，响应于在计算设备上执行所述多条指令，所述多条指令使所述计算设备执行上述示例14至26中的任一项的方法。

[0069] 根据示例30，提供了用于与包括机器学习快照评估的保护系统一起使用的至少一个设备，所述至少一个设备布置成用于执行上述示例14至26中的任一项的方法。

[0070] 根据示例31，提供了一种用于机器学习快照评估的系统。所述系统可以包括：用于生成设备中的操作的快照的装置；用于基于鉴于存储在所述设备中的学习到的用户行为对所述快照的评估来判定不寻常的用户行为是否已发生的装置；用于如果确定了不寻常的用户行为已发生则致使将所述快照和用户数据传输到远程资源的装置；用于响应于所述快照的所述传输而从所述远程资源接收威胁分析的装置；以及用于至少基于所述威胁分析来判

定是否存在对所述设备的潜在威胁的装置。

[0071] 示例32可以包括示例31的元素，并且可以进一步包括：用于判定所述设备是否为新的装置；以及用于如果确定了所述设备是新的则至少将所述快照和所述用户数据传输到所述远程资源的装置。

[0072] 示例33可以包括示例31至32中的任一项的元素，并且可以进一步包括用于基于从所述远程资源接收到的验证的结果来判定在所述设备中是否需要校正动作的装置。

[0073] 示例34可以包括示例31至32中的任一项的元素，并且可以进一步包括用于基于以下至少一项来标识所述设备中的至少一个操作的装置：在生成所述快照时在所述设备中的活跃操作；或在生成所述快照时在所述设备中的计划操作。

[0074] 示例35可以包括示例34的元素，并且可以进一步包括用于验证与在所述快照中标识的所述至少一个活跃操作或计划操作相关联的软件模块的签名的装置。

[0075] 示例36可以包括示例34的元素，并且可以进一步包括用于基于以下比较来学习用户行为的装置：将在所述快照中标识的所述至少一个活跃操作或计划操作与存储在所述设备中的至少一个先前的快照中标识的至少一个活跃操作或计划操作比较。

[0076] 示例37可以包括示例34的元素，其中所述用于判定不寻常的用户行为是否已发生的装置包括用于基于所述学习到的用户行为来判定所述至少一个活跃操作或计划操作是否是未预期到的装置。

[0077] 已经在本文中采用的术语和表达被用作描述而非限制术语，并且不旨在使用此类术语和表达时排除所示出和描述的特征的任何等效方案(或其部分)，并且认识到在权利要求书的范围内各种修改是可能的。因此，权利要求书旨在覆盖所有此类等效方案。

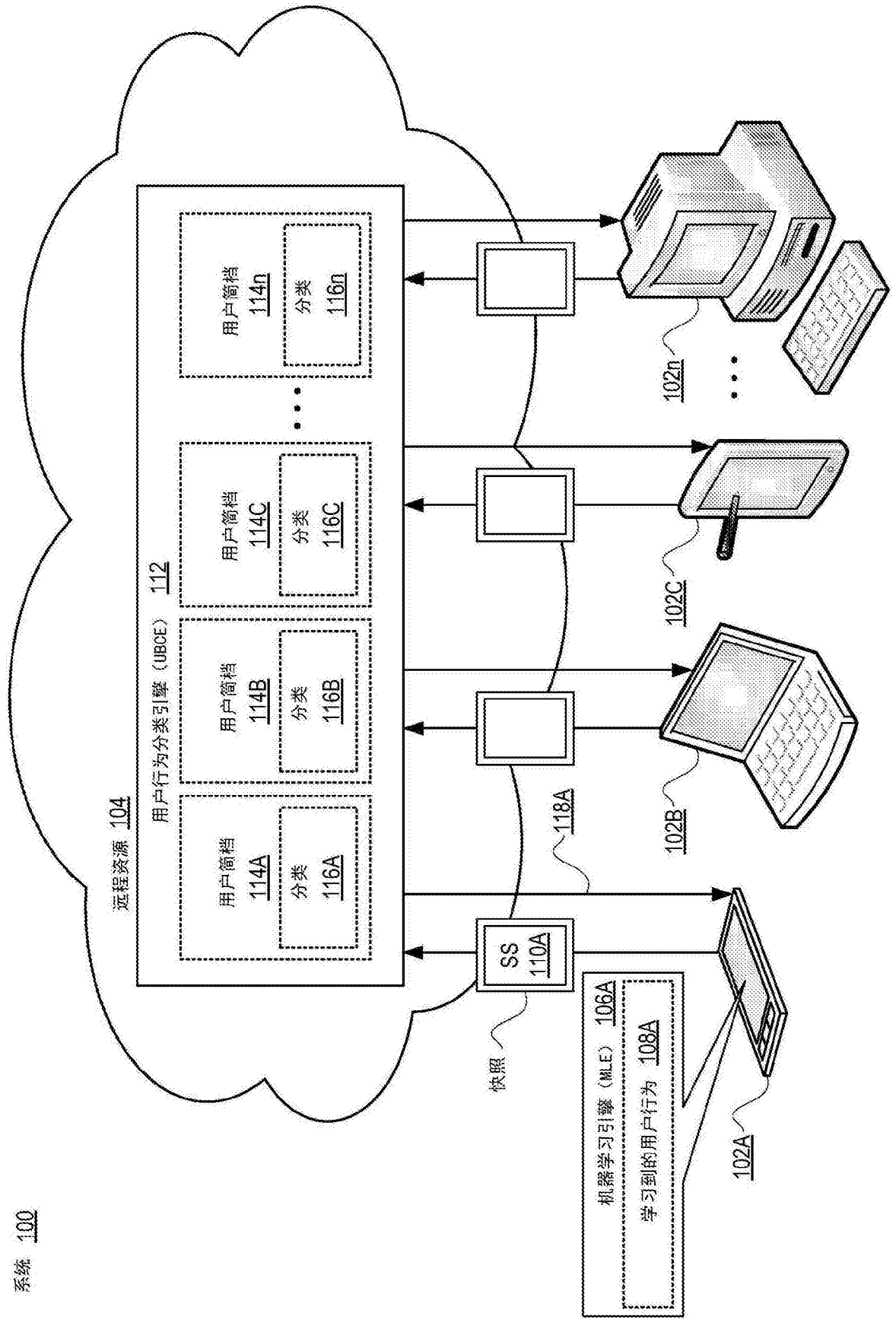

系统 100
远程资源 104
用户行为分类引擎（UBCE） 112
用户简档 114A
分类 116A
用户简档 114B
分类 116B
用户简档 114C
分类 116C
用户简档 114n
分类 116n
SS 110A
118A
快照
机器学习引擎（MLE） 106A
学习到的用户行为 108A
102A
102B
102C
102n

图1

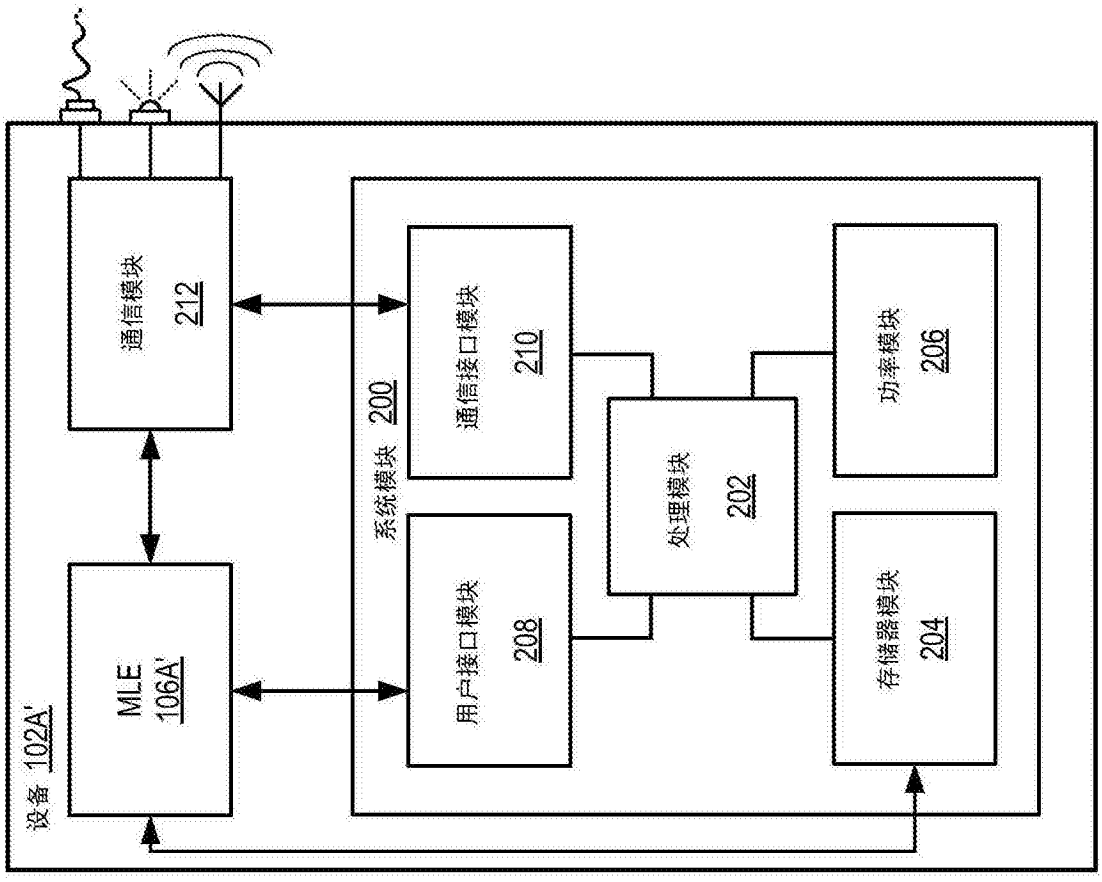

通信模块
212
通信接口模块
210
系统模块
200
处理模块
202
功率模块
206
用户接口模块
208
存储器模块
204
MLE
106A'
设备
102A'

图2

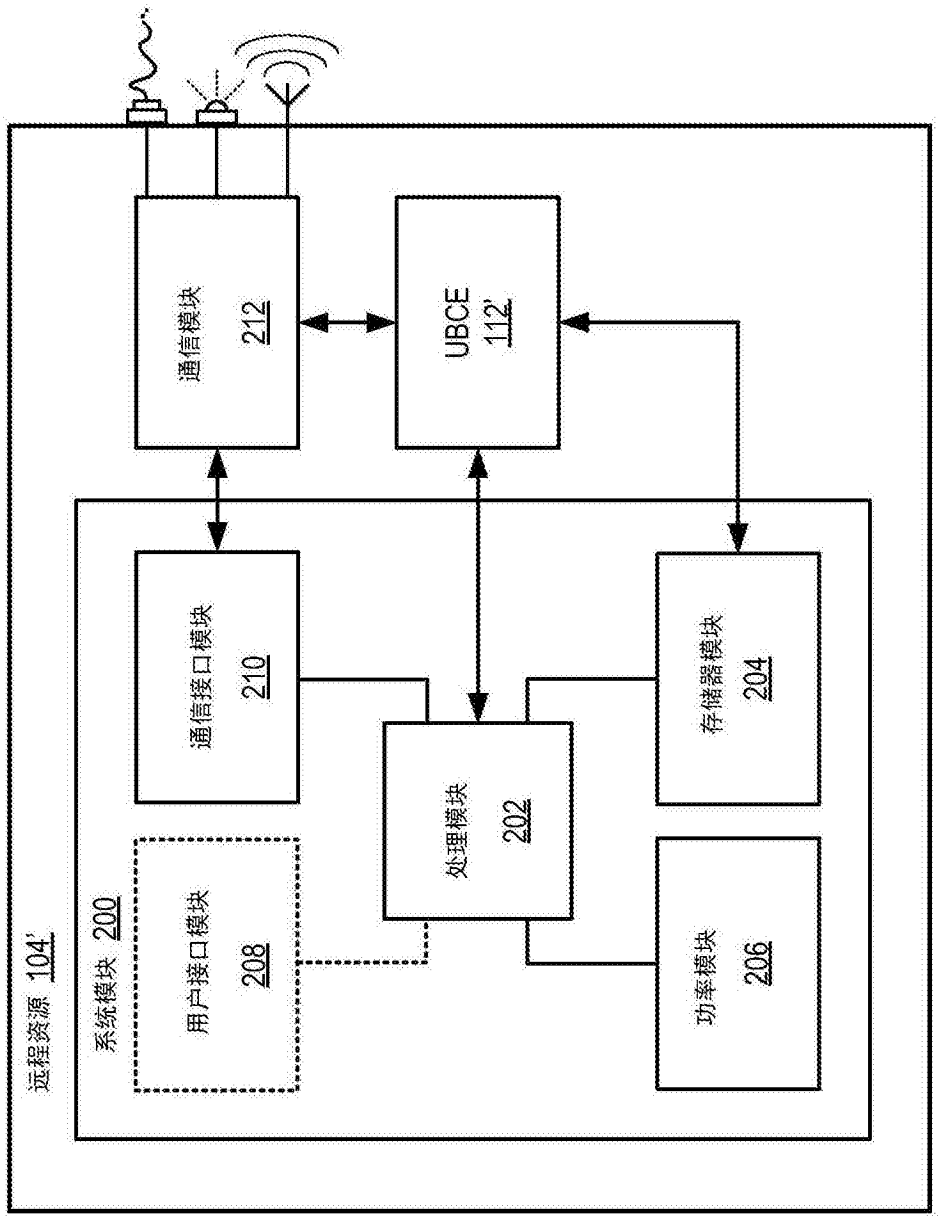

通信模块 212
UBCE 112'
通信接口模块 210
处理模块 202
存储器模块 204
用户接口模块 208
功率模块 206
系统模块 200
远程资源 104'

图3

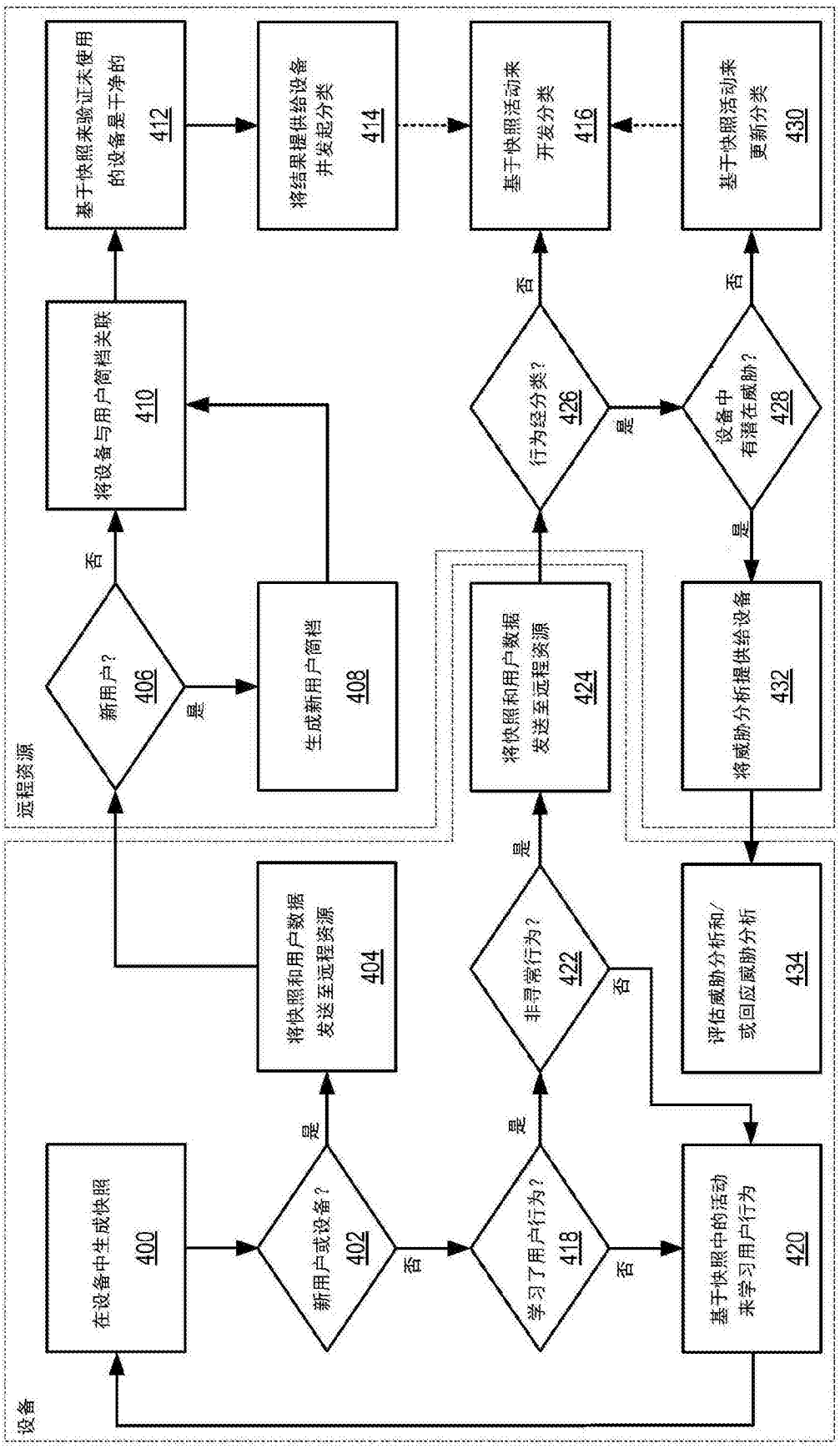

设备
远程资源
在设备中生成快照
400
新用户或设备？
402
是
否
将快照和用户数据发送至远程资源
404
新用户？
406
是
否
生成新用户简档
408
将设备与用户简档关联
410
基于快照来验证来使用的设备是干净的
412
将结果提供给设备并发起分类
414
学习了用户行为？
418
是
否
非寻常行为？
422
是
否
将快照和用户数据发送至远程资源
424
行为经分类？
426
是
否
设备中有潜在威胁？
428
是
否
基于快照中的活动来学习用户行为
420
将威胁分析提供给设备
432
基于快照活动来开发分类
416
基于快照活动来更新分类
430
评估威胁分析和/或回应威胁分析
434

图4