



(12) 发明专利申请

(10) 申请公布号 CN 103778379 A

(43) 申请公布日 2014. 05. 07

(21) 申请号 201310503089. 9

(22) 申请日 2013. 10. 23

(30) 优先权数据

12189773. 0 2012. 10. 24 EP

(71) 申请人 黑莓有限公司

地址 加拿大安大略省沃特卢市

申请人 QNX 软件系统有限公司

(72) 发明人 克里斯多佛·莱尔·本德 崔正贤

詹森·保罗·弗依

西瓦库玛·纳加拉扬

(74) 专利代理机构 中科专利商标代理有限责任

公司 11021

代理人 赵伟

(51) Int. Cl.

G06F 21/62 (2013. 01)

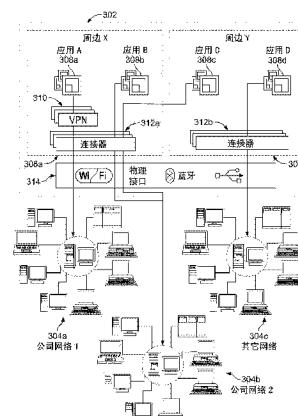
权利要求书1页 说明书11页 附图4页

(54) 发明名称

管理设备上的应用执行和数据访问

(57) 摘要

这里所描述的内容的一些方面涉及管理移动设备上的应用执行和数据访问。从与设备上的第一周边相关联的应用接收用于访问数据的请求。该数据与设备上的不同的第二周边相关联，并且具有数据类型。基于数据类型确定与第一周边相关联的管理策略准许应用访问数据，而与指派给第二周边的不同的第二管理策略无关。基于该确定，向应用提供对数据的访问。



1. 一种计算机执行的方法,包括 :

从与设备上的第一周边相关联的应用接收对与所述设备上的不同的第二周边相关联的数据进行访问的请求,其中,所述数据具有数据类型;

基于所述数据类型,确定与所述第一周边相关联的第一管理策略准许所述应用访问所述数据,而与和所述第二周边相关联的不同的第二管理策略无关;以及

基于所述确定,向所述应用提供对所述数据的访问。

2. 根据权利要求 1 所述的方法,还包括 :

配置与所述第二周边相关联的所述第二管理策略,以拒绝与所述第二周边不相关联的应用对所述数据的访问;以及

配置与所述第一周边相关联的所述第一管理策略,以超控与所述第二周边相关联的所述第二管理策略并准许所述应用访问所述数据。

3. 根据权利要求 1 或 2 所述的方法,还包括 :在将所述应用安装在所述设备上时,将所述应用与所述第一周边相关联。

4. 根据前述权利要求中任意一项所述的方法,还包括 :在将所述数据存储在所述设备上时,将所述数据与所述第二周边相关联。

5. 根据前述权利要求中任意一项所述的方法,还包括 :配置与所述第一周边相关联的所述第一管理策略,以准许与所述第一周边相关联的应用访问所述设备上的个人数据,以及其中,所述数据包括与工作有关的联系人信息。

6. 根据权利要求 5 所述的方法,其中,所述应用是电话应用,以及所述方法还包括 :

从所述电话应用接收访问所述与工作有关的联系人信息的请求;以及
提供所请求的与工作有关的联系人信息。

7. 根据前述权利要求中任意一项所述的方法,其中,所述第一周边包括能够执行以控制与所述第一周边相关联的应用对所述第一周边之内或之外的数据的访问的计算资源,以及所述第二周边包括能够执行以控制对与所述第二周边相关联的数据的访问的计算资源。

8. 根据前述权利要求中任意一项所述的方法,其中,向所述应用提供对所述数据的访问包括 :在所述第二周边被锁定时向所述应用提供对与所述第二周边相关联的数据的访问。

9. 一种设备,包括 :

数据处理装置;以及

计算机可读介质,所述计算机可读介质存储能够由所述数据处理装置执行以执行根据权利要求 1 至 8 中任意一项所述的方法的指令。

10. 一种计算机可读介质,所述计算机可读介质存储能够由所述数据处理装置执行以执行根据权利要求 1 至 8 中任意一项所述的方法的指令。

管理设备上的应用执行和数据访问

技术领域

[0001] 本公开涉及管理设备上对应用的执行和对数据的访问。

背景技术

[0002] 通信设备可以包括数据、应用和网络资源，其可访问性由安全协议来控制。例如，用户账户、管理权、密码保护、数据库管理等可以由不同的实体（例如，企业、个体等）来管理或者与不同的实体相关联。

附图说明

[0003] 图 1 是示出了示例数据通信系统的示意图。

[0004] 图 2 是示出了示例移动设备的示意图。

[0005] 图 3 是示出了对移动设备上的资源的示例性使用的示意图。

[0006] 图 4 是示出了用于管理移动设备上的数据访问的示例性过程的流程图。

[0007] 各个附图中的相同的附图标记和标志指示相似的元素。

具体实施方式

[0008] 本公开中使用的周边 (perimeter) 通常是指具有公共管理方案的资源组，并且每一个周边通常包括一个或多个资源、以及与一个或多个资源的使用或者对一个或多个资源的访问有关的一个或多个策略。周边可以在包括设备的数据通信系统上实现，并且可被用于在逻辑上分隔设备上的信息（例如，文件、应用、证书、配置数据、网络连接、数据等）。例如，设备可以实现两个或更多个周边，这些周边可以包括个人周边、企业或工作周边、这些和其它类型的周边的任何适当的组合。在一些实施例中，设备可以包括多个个人周边、多个企业周边、或者这二者。个人周边可以由设备用户管理，而企业周边可以由企业或公司管理者管理。在一些实现中，企业或公司管理者可以另外管理个人周边或设备或者这二者。由企业、雇主或公司购买、拥有、或以其它方式提供的设备通常可以称作公司负责设备，而由员工或个体购买的、拥有或以其它方式提供的设备通常可以称作个人负责设备或个体负责设备。

[0009] 在一些实现中，设备上的每一个周边在设备上具有其自己的文件系统，并且可以通过设备上文件系统的分隔来至少部分地提供周边之间的分隔。在一些情况下，每一个周边的资源中的一些（例如，数据和策略）被存储在周边的专用文件系统中，而每一个周边的其它资源（例如，应用）被存储在专用文件系统之外。

[0010] 文件系统的分隔可以是逻辑的、物理的或者这二者。例如，可以通过针对每一个文件系统指定在物理上分隔的存储位置（例如，分隔的存储设备、或者相同的存储器中的分隔块）来实现文件系统的物理分隔。例如，可以通过针对每一个文件系统指定在逻辑上分隔的数据结构（例如，分隔的目录等）来实现文件系统的逻辑分隔。在一些实现中，每一个文件系统具有其自己的加密参数。例如，公司周边的文件系统可以具有其自己的加密密

钥和较高的加密强度,而个人周边的文件系统可以具有其自己的加密密钥和较低的加密强度。在一些实例中,个人周边的文件系统具有与公司周边相同的加密强度,或者个人周边的文件系统可以是非加密的。

[0011] 如上所述,周边可以包括共享公共管理方案的资源组,其中,公共管理方案管理对组中的资源的使用,并且周边可以包括资源以及描述可以如何使用资源的管理策略。管理策略可以包括针对周边规定的安全限制。可由设备运行的应用可以包括当被执行时请求访问其它资源或者向其它应用提供资源(或者这二者)的资源。对于被指派给周边或者与周边相关联的应用,应用中包括的资源可被包括在周边中包括的资源组中。此外,针对周边规定的安全限制可以将应用限制到组中包括的资源。因此,当在周边中运行应用时,周边的管理策略中包括的安全限制可以确定与应用相关联的资源是否可以访问其它资源,例如,组中包括的资源或者组之外的资源(或者这二者),或者是否授予对其它应用的访问权限,该其他应用例如被指派给周边或者与周边相关联的应用或者未被指派给周边或者与周边不相关联的应用(或者这二者)。

[0012] 当资源(例如,应用)“进入(launch into)”周边时,在周边中对应用的实例进行实例化。应用所进入的周边的管理策略可以至少部分地确定应用可以访问或执行哪些资源(例如,数据资源、网络资源等)。因此,当应用的实例在周边中运行时,至少部分地基于周边的管理策略来确定针对应用的实例的许可(permission)。对于一些应用,可以至少部分地基于其它周边的策略来确定对周边之外的资源的访问。

[0013] 在一些实现中,安全周边可以从操作系统级一直到用户界面对不同类别的数据(例如,工作数据、个人数据等)进行划分或分隔。因此,周边架构可以在操作系统级、文件级、用户界面级、以及设备的其它级提供对数据的保护。在一些情况下,安全周边可以确保不同类别的数据、应用和用户体验之间的完全分隔,同时如果需要还允许不同类别的数据在相同的应用中共存并且共享数据。安全周边可以允许“混合应用”,例如,显示个人电子邮件和公司电子邮件二者的统一收信信箱。在一些实例中,可以将应用限制于相应的周边场景(例如,“工作”或“个人”周边场景)。例如,社交网络应用可以被配置为仅在个人周边中出现。在一些实例中,相同应用的不同实例可以在多个周边中运行。例如,设备可以具有针对用户的个人账户在的个人周边中运行的社交网络应用(例如,Facebook、Twitter等)的实例,并且设备可以具有针对用户的单位或用户的公司账户在公司周边中运行的相同的社交网络应用的实例。

[0014] 设备可以包括安装在数据通信系统中包括的设备上并且可以由该设备运行的各种类别的应用。系统提供对可以通过设备得到的数据的不同程度的安全访问。在一些实例中,在控制访问环境中,每一个应用在安装在设备上的一个或多个周边中是可执行的,该控制访问环境由用户选择或企业策略(或者这二者的组合)规定和限定(scope)。在一些实现中,相同应用的多个版本可以安装在相应周边中,在相应的周边中,每一个版本是可执行的,并且被授予对相应周边中的数据的访问权限。一些应用可以在未被关联到任何周边的情况下被安装,从而允许该应用在该应用所进入的周边中运行并且访问该周边中的数据。一些应用可被执行以同时访问多个周边。在一些实现中,可以在具有扩展应用对周边之外的数据的访问的能力的周边中安装应用。

[0015] 用户偏好可以限定要向在设备上的一个或多个周边或安全限制中执行的应用授

予的能力和许可。例如,可以配置针对设备加密、安全数字 (SD) 卡加密、密码超时、对针对照相机访问的许可进行限制等的用户偏好。类似地,企业策略可以限定与设备上的数据管理有关的规则、密码规则等。在用户偏好与企业策略之间,设备可以执行较严格的规则。例如,如果企业策略需要 SD 加密但是用户偏好未指定这种加密,则设备可以执行 SD 卡加密。类似地,如果企业策略建立至少 5 分钟的空闲时间并且用户偏好设置 2 分钟的超时,则设备可以执行用户偏好而不是企业策略。通过这种方式,可以对设备执行精细控制,以通过应用规则和用户选择来影响设备功能。由设备平台在不了解应用开发者的情况下执行的这种粒度的控制可以使设备平台呈现出灵活性,同时维持设备安全性。

[0016] 图 1 是示出了示例性数据通信系统 100 的示意图。示例性数据通信系统 100 包括设备 102、企业网络 104a、以及一个或多个其它网络 104b。根据其它实施例的数据通信系统可以视情况包括其他的、不同的或更少的特征。图 1 中的示意图还示出了用户 106a、106b、设备所有者 105、以及管理者 108a、108b、108c 进行的交互。在一些情况下,设备所有者 105 可以是用户 106a 或 106b、工商企业、或另一实体之一。在各种实现中,其他的、不同的或更少的实体可以视情况与数据通信系统进行交互。

[0017] 设备 102 可以是任何适当的计算设备。通常,计算设备包括计算机可读介质和数据处理装置。计算机可读介质可以包括被配置为存储机器可读信息的任何适当的存储器、磁盘、存储设备或者其它装置。计算机可读介质可以存储可以由数据处理装置执行的指令。数据处理装置可以包括被配置为基于机器可读指令来执行操作的任何适当的处理器、控制器、电路或者其它装置。数据处理装置可以包括可编程处理器、数字逻辑电路、固件、或任何其它适当的设备。计算机可读介质可以包括单个介质或多个介质,并且数据处理装置可以包括单个装置或多个装置。计算机可读介质可以是传播的信号,可以通过编码处理将这里描述的操作编码在该信号中。

[0018] 示例性设备 102 能够操作以经由用户界面(例如图形用户界面或任何其它适当的用户界面)从用户接收请求。如图 1 所示,设备 102 被可通信地耦合到企业网络 104a 和一个或多个其它网络 104b。示例性设备 102 能够操作以接收、发送、处理和存储任何适当的数据。例如,设备 102 可以包括智能电话、平板计算机、个人计算机、膝上型计算机、个人数字助理 (PDA)、或其它类型的设备。设备 102 可以包括输入设备(例如,键盘、触摸屏、鼠标、或可以接受信息的其它设备)和传递与资源的操作相关联的信息的输出设备(例如,显示屏)。输入设备和输出设备都可以包括用于通过显示器从用户接收输入并且向用户提供输出的固定或可拆卸的存储介质(例如,存储器等)。

[0019] 如图 1 所示,设备 102 可以包括三个示例性周边 110a、110b、以及 110c(无论单独地还是共同地都称为“周边 110”)。每一个周边 110 包括数据 112、网络访问资源 114、一个或多个应用 116、一个或多个配置文件 118、以及一个或多个策略 120。周边 110 可以仅包括所示出的资源的子集,或者周边 110 可以包括其他的或不同的资源。

[0020] 示例性周边 110 可以在逻辑上分隔资源(例如,应用、数据、网络访问资源、配置文件等),使得在一些实例中,可以防止给定周边中的资源访问不同周边中包括的资源。例如,可以防止一个周边中的个人资源访问另一周边中的公司资源,反之亦然。在一些情况下,企业可以在不干扰单个用户设备上的用户的个人体验的情况下在相同设备上扩展受保护的周边。周边还可以准许对资源的跨周边访问。可以通过向每一个周边限定策略、向每一个

周边指派策略或以其它方式将策略关联到每一个周边,来控制对周边资源的访问。

[0021] 可以使用任何适当的信息以任何适当的格式实现针对周边的策略。策略可以指定对可以由(在周边中运行的)内部应用访问的(另一周边中的)外部资源和可以由外部应用访问的内部资源二者的访问。例如,给定周边的策略可以标识可以访问的其它周边、不可由其它周边访问的内部资源、或者这二者。周边的策略可以标识可以访问或不可以访问周边中指定资源的特定用户。在一些实现中,来自两个周边的策略确定是否授予跨周边访问的许可,或者如果存在冲突,则可以应用最严格的策略。在一些实现中,针对一个周边的策略确定授予该周边中的应用对另一周边中的数据的访问权限。例如,可以授予第一周边中的应用对第二周边中的数据的访问权限,而与第二周边的策略无关。

[0022] 周边架构实现了计算资源的逻辑分隔,使得可以控制周边之间的数据传送和对其它周边的资源的访问。资源可以包括应用、文件系统、网络访问、或其它计算资源。除了实现对周边中的资源的访问之外,示例性数据通信系统 100 还可以包括标识周边中的资源可以访问的特定外部资源的策略。执行周边构思的示例性数据通信系统 100 可以管理无缝用户体验。

[0023] 周边 110 可以包括密码保护、加密、以及用于控制对被指派给周边的资源的访问的其它过程。周边 110 可以是由设备所有者、用户、管理者等产生的。在一些示例中,周边 110a 可以是针对用户 106a 创建并且由用户 106a 管理的个人周边。在一些示例中,周边 110b 可以是由管理者 108b 针对企业创建的企业周边,并且可以由远程管理服务器来管理。此外,给定周边可以由设备所有者 105、用户、管理者、或任何适当的组合来访问。在一些实现中,每一个周边可以与单个用户相关联,并且至少一些用户可以访问多个设备周边。例如,第一用户 106a 可以访问周边 110a 和周边 110b 二者中的资源,第二用户 106b 可以仅有权访问周边 110c。

[0024] 在一些实例中,可以添加、删除或修改相应周边。设备所有者 105 可以有能力添加或从设备 102 移除相应周边 110。在一些实现中,用户可以创建周边。在一些实例中,与企业网络 104a 相关联的组织可以向设备发送标识新周边的初始资源(例如,应用、策略、配置等)的信息。周边管理者可以指派针对周边的策略,并且发起周边更新。在一些实现中,周边管理者可以在远程锁定和 / 或擦除周边。

[0025] 可以在设备 102 上在任何适当的存储器或数据库模块中存储信息。示例性存储器包括易失性存储器和非易失性存储器、磁性介质、光学介质、随机存取存储器(RAM)、只读存储器(ROM)、可拆卸介质等。数据 112 可以包括任何适当的信息。设备 102 可以存储各种对象,包括:文件、类(class)、框架、备份数据、商业对象、工作、网页、网页模板、数据库表格、存储商业信息或动态信息的知识库、以及包括任何参数、变量、算法、指令、规则、约束、对其的引用的任何其它适当的信息。数据 112 可以包括与应用、网络、用户相关联的信息、以及其它信息。

[0026] 网络访问资源 114 可以包括用于准许访问网络的任何适当的参数、变量、策略、算法、指令、设置、或规则。例如,网络访问资源 114a 可以包括或标识用于访问企业网络 104a 的防火墙策略。作为另一示例,网络访问资源 114b 可以包括或标识用于访问一个或多个其它网络 104b 的账户数据。在一些实现中,网络访问资源包括或以其它方式标识以下各项中的一项或多项:用户名、密码、安全令牌、虚拟专用网(VPN)配置、防火墙策略、通信协议、加

密密钥证书等。

[0027] 应用 116 可以包括可执行、改变、删除、生成或处理信息的任何适当的程序、模块、脚本、过程或其它对象。例如，应用可被实现为企业 Java 组件 (Enterprise Java Bean, EJB)。设计时的组件可以有能力将执行时的实现生成到不同的平台中，这些平台例如是 J2EE (Java2 平台, 企业版)、ABAP (高级商业应用编程) 对象、或微软的 .NET。此外，虽然被示出为在设备 102 之内，但是可以在远程存储、引用或执行与应用 116 相关联的一个或多个过程。例如，应用 116 的一部分可以是针对在远程执行的网站服务的接口。此外，应用 116 可以是另一软件模块 (未示出) 的次模块或子模块。

[0028] 配置文件 118 可以包括用于配置设备 102 的软件的任何适当的参数、变量、策略、算法、指令、设置、或规则。例如，配置文件 118 可以包括标识一个或多个应用 116 的设置的表格。在一些实现中，配置文件 118 标识一个或多个应用 116 和其它类型的应用的初始设置，例如，操作系统设置。可以通过任何适当的格式来书写配置文件 118，例如 ASCII 和面向行等。

[0029] 策略 120 可以包括用于启用或防止对一个或多个周边中的资源的访问的任何参数、变量、策略、算法、指令、设置、或规则。例如，策略 120a 可以标识在周边 110a 之外的可以由周边 110a 中的资源访问的资源。给定周边的策略可以包括或以其它方式标识周边的可访问性 (通常是周边中的特定资源的可访问性)、周边中的资源访问其它周边的能力、以及其它可访问性信息。策略可以指定用户的可访问性、动作类型、时间段等。在一些实现中，策略可以标识周边的、可以由外部资源访问的特定资源。例如，针对周边 110a 的策略 120a 可以指示另一周边 110b 中的特定应用可以或不可以访问第一周边 110a 中的数据或资源。作为另一示例，针对周边 110a 的策略 120a 可以指示其它周边 110b 或 110c 中的任意应用可以或不可以访问第一周边 110a 中的数据或资源。

[0030] 在一些实现中，策略 120 可以限定或以其它方式标识用户认证过程。例如，策略 120 可以标识用户认证的类型和内容 (例如，密码强度、生命周期)，以应用于跨周边请求。当用户提供对多个周边的访问的请求时，可以由双方周边的策略来评估请求。在一些实例中，如果双方策略授予访问权限，则可以批准跨周边请求。策略可以标识或包括用于确定可以由不同周边中的外部资源使用哪些网络访问资源的信息。

[0031] 设备 102 可以连接到多个网络，例如，企业网络 104a 和其它网络 104b。企业网络 104a 可以包括无线网络、虚拟专用网、有线网络、或任何适当的网络。企业可以是公司或商业实体、政府机构、非营利机构、或任何其它组织。企业可以是设备所有者 105。企业还可以租用设备 102 或者可以雇佣负责维护、配置、控制或管理设备 102 的承包商或代理。其它网络 104b 可以包括可由用户访问的任何适当的网络。例如，其它网络可以包括用户具有账户的公共网络、专用网络、自组织网络、或其它类型的网络。在一些情况下，其它网络 104b 包括蜂窝数据网络。在一些情况下，其它网络 104b 包括用户的家庭网络。

[0032] 网络 104a 和 104b 促进与设备 102 的通信。网络 104a 和 104b 中的任意一个可以例如在网络地址之间传送互联网协议 (IP) 分组、帧中继帧、异步传输模式 (ATM) 信元、语音、视频、数据和其它适当的信息。此外，虽然企业网络 104a 和其它网络 104b 均被示出为单个网络，但是每一个网络可以包括多个网络，并且可以提供对其他网络的访问。简言之，企业网络 104a 和其它网络 104b 可以包括被配置为与设备 102 进行通信的任何适当的网络。

[0033] 图 2 是示出了包括显示器 202、可选择的键盘 204 和其他特征的示例性移动设备 200 的示意图。设备可以包括其他的或不同的特征。可以在设备 200 上安装分层次的应用。可以由设备 200 执行各个应用，以共同地提供对可以通过设备 200 得到的数据的不同程度的安全访问。可以对该分层次的应用进行归类，以包括单周边应用（例如，由对象 206a 和 206b 表示，其可以包括例如图形图标）、双周边应用（例如，由对象 210a 和 210b 表示）、以及混合应用（例如，由对象 208 和 209 表示）。

[0034] 当将单周边应用安装在设备 200 上时，可以将单周边应用指派给特定周边或者与特定周边相关联，例如，个人周边或企业周边。因此，在安装时将应用指派所至的周边来确定单周边应用的许可和访问授权。如果在安装时将应用指派给个人周边或者与个人周边相关联，则可以在个人周边 110a 中显示表示应用的对象 206a。作为另一示例，如果在安装时将应用指派给企业周边或者与企业周边相关联，则可以在企业周边 110b 中显示表示应用的对象 206b。应用可以受制于由企业管理者设置的宏观层面的周边规则和微观层面的应用规则。企业管理者可能不希望用户安装的应用（例如，恶意软件等）访问企业网上的资源，而是可以向特定的其它可靠的应用授予对企业网络的访问权限。

[0035] 通过周边来限定的安全限制可以防止单周边应用访问未被指派给应用所指派至的相同周边或者与该相同周边相关联的数据。在一些实现中，可以在设备 200 上安装相同的单周边应用的两个版本——指派给个人周边的个人版本和指派给企业周边的企业版本。例如，可以从指派给个人周边的多个应用中下载应用的个人版本，并且类似地可以从指派给企业周边的多个应用中下载企业版本。在这些实现中，对象 206a 和对象 206b 可以分别同时显示在周边 110a 和周边 110b 中。个人版本和企业版本分别仅在个人周边和企业周边中是可执行的。在一些实现中，设备 200 一次只可以执行单周边应用的一个实例。也即是说，设备 200 可以被配置为不允许同时执行单周边应用的个人版本和企业版本二者。可以被实现为单周边应用的应用包括游戏应用、社交网络应用（例如，Facebook、Twitter 等）、费用报告应用等。在一个实施例中，任何第三方应用（例如，由除了设备制造者之外的一方提供的应用）可以实现为单周边应用。

[0036] 第三方应用，即，除了由设备 200 的制造者提供的应用之外的应用，可以始终是单周边应用。但是，这些应用不需要是周边知晓的，并且可以安装到个人周边或企业周边。当被安装到个人周边或企业周边时，可以将应用作为可以单独管理的相同应用的两个不同实例（即，个人版本和企业版本）来进行安装。

[0037] 另一类基于周边的应用是双周边应用。（在这里，因为当前示例性实施例包括两个周边，因此使用术语双周边；然而，在其它实施例中可以提供多于两个周边，并且可以在这些实施例中使用术语多周边）。可以安装双周边应用，而无需在安装在设备 200 上时将其指派给任何特定周边或者与任何特定周边相关联。取而代之地，双周边应用可以进入到设备 200 上的（例如，两个或更多个）周边中的任意周边中。例如，可以将双周边应用预先安装在设备 200 上，并且可以在个人周边中或者在企业周边中启动该双周边应用。当在个人周边中启动时，可以在个人周边 110a 中显示表示应用的对象 210a，并且可以授予应用对指派给个人周边的数据和网络资源的访问权限。类似地，当在企业周边中启动时，可以在周边 110b 中显示表示应用的对象 210b，并且应用可以访问指派给企业周边的资源，例如，数据和网络资源。在这个意义上，双周边应用可以在启动时被指派给周边并且可以在运行时

访问其所指派至的周边的资源（例如，数据和网络资源等）而不是在其所指派至的周边之外的资源（例如，数据和网络资源等）。与单周边应用类似，设备 200 可以被配置为不允许在多个一个周边内同时执行双周边应用。换言之，在任何给定时刻，设备 200 可以仅允许在周边中执行双周边应用的一个实例。可以实现为双周边应用的应用的示例包括文档编辑应用（例如，DocsToGo）、应用分发应用（例如，AppWorld）、文档阅读器应用（ADOBE®阅读器）、图片应用、视频应用、地图应用、导航应用等。

[0038] 在一些实现中，如果在周边中执行双周边应用，则只能在该周边而不能在其它周边中显示表示该应用的对象。备选地，可以在所有周边之外显示最初表示双周边应用的对象。响应于从周边中选择了对象，可以在该周边中执行应用。双周边应用的示例可以包括文档编辑应用。当在个人周边中执行时，设备 200 可以将文档编辑应用限制为仅访问个人周边中的资源而不访问企业周边中的资源；换言之，设备 200 可以将文档编辑应用限制到个人周边中的资源，同时不允许访问企业周边中的资源。相反，当在企业周边中执行时，设备 200 可以将文档编辑应用限制到企业周边中的资源而不是个人周边中的资源。

[0039] 另一类基于周边的应用是混合应用。混合应用可以被配置为同时访问指派给多个周边的资源。这些应用可以知晓周边分隔逻辑和周边运行时状态，并且当例如由于密码保护或不活跃而将这些周边锁定时，隐藏 (obscure) 来自受保护的周边的数据。混合应用可以区分源自不同周边的数据，并且可以使其对各个数据源的所有访问保持彼此分隔，从而维持设备 200 上的周边分隔的完整性。由于混合应用可以同时被指派给多个周边或者与多个周边相关联，因此可以在所有周边（例如，周边 110a、110b）之外显示表示混合应用的对象（例如，对象 208、209）。

[0040] 混合应用的示例可以是可以使用户能够管理日历上的事件的日历应用。日历应用是混合应用，这是因为它可以访问来自用户的个人日历的数据（即，与事件有关的数据等）和来自用户的企业（即，工作）日历的数据。为了维持设备 200 上的周边分隔的完整性，当在一个周边中执行时，日历应用可以模糊 (obfuscate) 指派给另一周边的数据。也即是说，如果日历应用在个人周边中执行以调度个人日历上的事件，则日历应用可以显示企业日历上的冲突事件，而无需显示该冲突事件的细节。例如，日历应用可以在个人日历中将冲突事件显示为空白对象。通过这种方式，混合应用可以提供可统一对源自不同周边的数据的查看同时为了安全完整性而维持其分隔的功能。可以实现为混合应用的应用的示例包括电子邮件应用（例如，统一收信信箱）、联系人应用、日历应用、统一搜索应用、任务 / 备忘录应用、电话应用等。

[0041] 在一些实现中，应用可以被指派给周边，并且具有扩展超出所指派的周边的能力。可以向任何适当的应用（包括上文所描述的类别的应用）提供这种扩展能力。在一些实例中，可以认为具有这种扩展能力的应用是不同类别的应用。在一些实现中，可以在将应用指派至的周边中显示表示应用的对象（例如，周边 110a 中的对象 212a 或者周边 110b 中的对象 212b）。如图 2 所示，可以通过与单周边应用或双周边应用相同的方式来呈现扩展能力的应用；或者可以通过不同的方式来呈现扩展能力的应用。这种应用可以在安装时被指派给周边，并且可以授予该应用对周边之外的数据和网络资源的访问权限，以提供有用的功能。在一些实施例中，扩展能力的周边应用可以包括由设备的制造商开发的特定的核心应用。扩展能力的周边应用的一些示例包括短消息服务 (SMS) 应用、电话应用、呼叫方 ID 应用、社

交网络应用（例如，Facebook、Twitter 等）、地图应用、导航应用等。在一些实施例中，扩展能力的周边应用可以包括需要访问联系人的任何应用。在一些实施例中，扩展能力的周边应用可以包括由设备的制造商提供的应用。

[0042] 在一些实现中，扩展能力的应用有权访问被锁定的周边的资源。当周边被锁定时，与周边相关联的数据通常是不可访问的。在一些实例中，与一个周边相关联的扩展能力的应用可以从另一周边访问数据，即使在该另一周边被锁定时。例如，在一些实现中，企业周边可能由于手动锁定或者不活跃超时或者其它锁定触发而被锁定，并且企业周边可以由诸如接收到适当的密码、手势、生物数据或其它认证令牌等认证过程而被解锁。即使企业周边被锁定，从与企业周边相关联的联系人接收到输入呼叫的电话应用也可以访问与企业周边相关联的联系人信息。然后，即使在企业周边被锁定的时，电话应用也可以提供与呼叫方有关的呼叫方 ID 信息。

[0043] 再次参照图 2，当设备 200 在企业周边 110b 中存储联系人信息时，设备 200 可以将联系人信息指定为可以由电话应用访问的类型。设备 200 可以执行个人周边 110a 中的电话应用，以接收输入呼叫。如果电话应用是扩展能力的周边应用，则设备 200 可以执行电话应用以访问指派给企业周边 110b 的数据和网络资源，而与企业周边 110b 的管理策略无关。这可以允许电话应用在个人周边 110a 中执行，并且访问指派给企业周边 110b 的联系人信息。

[0044] 非混合的应用不知晓应用被指派至或者应用被关联至的周边。可以在原本不了解周边之间的分隔（例如，个人周边和企业周边）的情况下启动这些应用。可以基于在启动时提供给应用的许可来给予这些应用对应用所需或请求（或者这二者）的数据的访问权限。例如，可以由应用在安装时被安装至的周边、生效的企业管理策略、生效的当前用户偏好、或者它们的组合中的任意一个来确定许可。例如，设备 200 可以不授予个人应用（即，指派给个人周边或与个人周边相关联的应用）对工作数据（即，指派给企业周边或者与企业周边相关联的数据）的访问权限。设备可以授予企业应用（即，指派给企业周边或者与企业周边相关联的应用）对个人数据（即，指派给个人周边或者与个人周边相关联的数据）的访问权限。在另一示例中，企业管理策略可以限定允许特定应用访问特定功能或者特定类型的数据或者它们的组合。在另一示例中，可以设置当前用户偏好，使得可以在工作网络中使用个人应用。

[0045] 图 3 是示出了移动设备对网络资源的示例性使用的示意图。图 3 中所示的示例性使用可以在不同的时间发生，或者它们可以同时发生。在所示的示例中，设备 302 被配置为与公司网络 304a 和 304b 以及非公司网络 304c 进行通信。公司网络 304a 和 304b 可以包括企业的虚拟专用网、企业的专用 Wi-Fi 网络、企业的有线网络、由企业管理的另一网络。非公司网络可以包括例如公众可访问的 Wi-Fi 网络、蜂窝数据网络、个人无线网络、或者另一种类型的网络。设备 302 包括企业周边 306a 和个人周边 306b。企业周边 306a 包括企业应用 308a 和 308b，个人周边 306b 包括个人应用 308c 和 308d。企业周边 306a 包括虚拟专用网数据 310 和企业连接数据 312a。个人周边包括其它连接数据 312b。

[0046] 设备 302 可以使用企业周边 306a 的网络资源来访问公司网络 304a 和 304b，并且该设备可以使用个人周边 306b 的网络资源来访问非公司网络 304c。在一些情况下，网络 304a、304b 和 304c 中的每一个可以提供对其它系统的访问。例如，网络 304a、304b 和 304c

中的一个或多个可以为设备 302 提供互联网访问。一些网络可以仅提供对特定服务器、数据库或系统的访问。例如，公司网络 304a 可以仅提供对公司电子邮件服务器的访问。设备 302 可以通过物理接口 314 的任何适当的组件连接到网络 304a、304b、以及 304c 中的任意一个。例如，连接硬件可以包括针对以下各项的硬件：Wi-Fi 连接、蜂窝连接、蓝牙、通用串行总线 (USB)、射频识别 (RFID)、近场通信 (NFC)、或其它连接技术。

[0047] 虚拟专用网数据 310 提供与公司网络 304a 的安全连接。在图 3 所示的示例中，虚拟专用网数据 310 用于将企业应用 308a 的企业数据业务路由到公司网络 304a。企业周边 306a 中的企业连接数据 312a 提供与公司网络 304b 的连接，并且个人周边 306b 中的其它连接数据 312b 提供与其它网络 304c 的连接。在图 3 中所示的示例中，企业连接数据 312a 用于将企业应用 308b 的企业数据业务路由到公司网络 304b，并且企业连接数据 312a 还用于将个人应用 308c 的个人数据业务路由到公司网络 304b。例如，个人应用 308c 可以是通过公司网络 304b 访问互联网的基于网络的应用（例如，在线游戏、社交网络应用）。如图 3 所示，其它连接数据 312b 用于将个人应用 308d 的个人数据业务路由到其它网络 304c。

[0048] 在一些实现中，连接数据 312a 和 312b 可以包括加密信息、网络设置和信息、密码、证书、以及其它数据。每一个周边可以包括针对应用的策略、以及周边之内的网络资源、周边之外的网络资源或者周边之内的网络资源和周边之外的网络资源。设备 302 可以包括允许公司周边 306b 中的公司应用访问个人周边 306b 中的数据（例如，其它连接数据 312b、或者其它数据）的策略（例如，指派给企业周边 306a 的策略）。在一些实例中，可以提供这种访问，而与指派给个人周边 306b 的策略无关。类似地，设备 302 可以包括允许个人周边 306a 中的个人应用访问企业周边 306a 中的数据（例如，连接数据 312a、或其它数据）的策略（例如，指派给个人周边 306b 的策略）。在一些实例中，可以提供这种访问，而与指派给企业周边 306a 的策略无关。

[0049] 图 4 是示出了用于管理移动设备上的应用执行和数据访问的示例性过程 400 的流程图。过程 400 可以由通信系统中的设备来执行。例如，过程可以由如图 1 中所示的设备 102、如图 2 中所示的设备 200、如图 3 中所示的设备 302、或者另一种类型的系统或模块来执行。可以使用其他的、更少的或不同的操作来执行图 4 中所示的示例性过程 400，其中，可以以所示的顺序或者以不同的顺序来执行这些其他的、更少的或不同的操作。在一些实现中，例如，可以重复或迭代操作中的一个或多个，直到达到终止条件为止。

[0050] 可以在包括多个周边的设备上执行过程 400。例如，围绕第一周边和第二周边描述了过程 400 中的示例性操作。可以通过任何适当的方式来限定和实现周边，并且每一个周边可以包括任何适当的数据、应用、策略和其它资源。每一个周边可以包括其自己的策略或其它数据，所述策略或数据限定了用于访问与周边相关联的资源的规则。例如，设备上的第一周边可以包括对用于访问与第一周边相关联的资源（例如，应用、数据、网络资源等）的规则进行限定的第一策略，第二周边可以包括对用于访问与第二周边相关联的资源（例如，应用、数据、网络资源等）的规则进行限定的第二策略。设备可以包括任意适当数量（例如，一个、两个、三个、四个或者更多个）的周边。

[0051] 在一些实现中，设备可以包括与设备的用户相关联的个人周边。设备可以包括多个个人周边，并且每一个个人周边可以与相同的用户相关联，或者它们可以分别与不同的用户相关联。例如，多个用户可以被授权使用该设备，并且每一个用户可以在设备上具有其

自己的个人周边。在一些实现中，设备包括与企业（例如，工商企业、公司、合伙企业或其它企业）相关联的企业周边。例如，企业可以拥有设备，并且将设备指派给特定的用户。企业管理者可以建立设备策略，或者配置设备以供企业使用。在一些实例中，设备包括多个企业周边。每一个企业周边可以与相同的企业相关联，或者它们可以分别与不同的企业相关联。例如，用户可以拥有设备，并且具有针对与其自身相关联的每一个企业的周边。

[0052] 在 410，设备从指派给设备上的第一周边的应用接收访问数据的请求。所请求的数据被指派给设备上的不同的第二周边，并且具有数据类型。如上所述，所请求的数据的数据类型可以用于确定指派给第一周边的应用是否可以访问指派给第二周边的数据。第一周边可以包括计算资源，该计算资源可执行以控制指派给第一周边的应用对第一周边之内或之外的数据的访问。第一周边中的应用可以包括任何适当的应用（例如，日历、电子邮件、游戏、工具等）。可以在将应用安装到设备上时将该应用指派给第一周边。第二周边可以包括可执行以控制对指派给第二周边的数据的访问的计算资源。第二周边中的网络资源可以包括任何适当的网络资源（例如，虚拟专用网络账户、Wi-Fi 访问数据等）。

[0053] 可以在将请求的数据存储到设备上时将请求的数据指派给第二周边。在一些实现中，设备 200 可以响应于从用户和 / 或通过网络接收的输入，来执行指派给第一周边（例如，个人周边 110a）的应用。当设备 200 执行个人周边 110a 中的应用时，该应用可以请求访问指派给与周边 110a 不同的第二周边（例如，企业周边 110b）的数据。在一些实现中，请求指示所请求的数据的数据类型。在一些实现中，可以根据请求的数据来确定数据类型。

[0054] 在 420，响应于请求访问数据的请求，设备基于数据类型来确定指派给第一周边的第一管理策略准许应用访问所请求的数据，而与指派给第二周边的不同的第二管理策略无关。指派给第二周边的第二管理策略可以被配置为拒绝未被指派给第二周边的应用对所请求的数据的访问。例如，可以将可包括与工作有关的联系人信息的所请求的数据指派给第二周边，即，企业周边 110b。指派给第一周边（即，个人周边 110a）的第一管理策略可以被配置为准许应用访问所请求的数据，而不论指派给企业周边 110b 的管理策略如何。在一些情况下，为了这样做，设备 200 可以确定数据是否具有扩展能力的应用可访问的数据类型并且能够被扩展能力的应用所消费。在一些实现中，个人周边 110a 的管理策略指示可以由特定应用（例如，电话应用）访问的特定类型的数据（例如，联系人信息），而与数据被指派至的周边无关。

[0055] 可以在针对数据的请求中（例如，显式地或隐式地）指定数据类型。例如，如果请求指定了文件名，则可以由文件名扩展、存储数据的目录、或者文件名的其它方面指定数据类型。可以在数据本身或者在与数据相关联的元数据中指定数据类型。在一些情况下，可以将电话号码、街道地址、电子邮件地址等标记为“联系人信息”数据类型。在一些情况下，可以将与约会和会议等有关的信息标记为“日历”数据类型。可以通过创建数据的应用的类型、数据的格式、或其它考虑来确定数据类型。可以由元数据、文件名扩展、文件格式、或者另一数据特征来指定数据类型。

[0056] 在 430，响应于确定第一管理策略准许应用访问所请求的数据，而与第二管理策略无关，设备向应用提供对数据的访问。在一些实现中，设备 200 可以基于所请求的数据的数据类型来做出确定。换言之，设备 200 可以确定扩展能力的周边应用（例如，电话应用）可以访问具有该数据类型的数据，而不论数据被指派至的周边如何。相比之下，不是扩展能力

的周边应用的应用（例如，单周边应用或双周边应用）被指派至的周边的管理策略可以限制对具有指派给其它周边的该数据类型的数据的访问。当设备 200 确定请求这种数据类型的数据的应用是扩展能力的周边应用时，设备 200 可以向应用提供对具有该数据类型的所请求的数据的访问。

[0057] 通常，这里所描述的主题的一些方面可以实现为用于管理移动设备上的应用执行和数据访问的计算机执行方法。从指派给设备上的第一周边的应用接收访问数据的请求。该数据被指派给设备上的不同的第二周边，并且具有数据类型。响应于接收到该请求，基于数据类型来确定指派给第一周边的管理策略准许应用访问所请求的数据，而与指派给第二周边的不同的第二管理策略无关。响应于该确定，向应用提供对数据的访问。

[0058] 这些方面和其它方面的实现可以包括以下特征中的一个或多个。指派给第二周边的第二管理策略可以被配置为拒绝未被指派给第二周边的应用对所请求数据的访问。指派给第一周边的第一管理策略可以被配置为准许应用访问所请求数据，而不论指派给第二周边的第二管理策略如何。可以在将应用安装到设备上时将该应用指派给第一周边。可以在将所请求数据存储在设备上时，将所请求数据指派给第二周边。指派给第一周边的第一管理策略可以被配置为准许指派给第一周边的应用访问设备上的个人数据。所请求数据可以包括与工作有关的联系人信息。应用可以是电话应用。可以从电话应用接收请求访问与工作有关的联系人信息的请求。可以将所请求的与工作有关的联系人信息提供给电话应用。第一周边可以包括可执行以控制指派给第一周边的应用对第一周边之内或之外的数据的访问的计算资源。第二周边可以包括可以执行以控制对指派给第二周边的数据的访问的计算资源。

[0059] 已经描述了多个实现。但是，将理解的是，可以进行各种修改。步骤的顺序的其它变形也是可能的。因此，其它实现落入下面的权利要求的范围内。

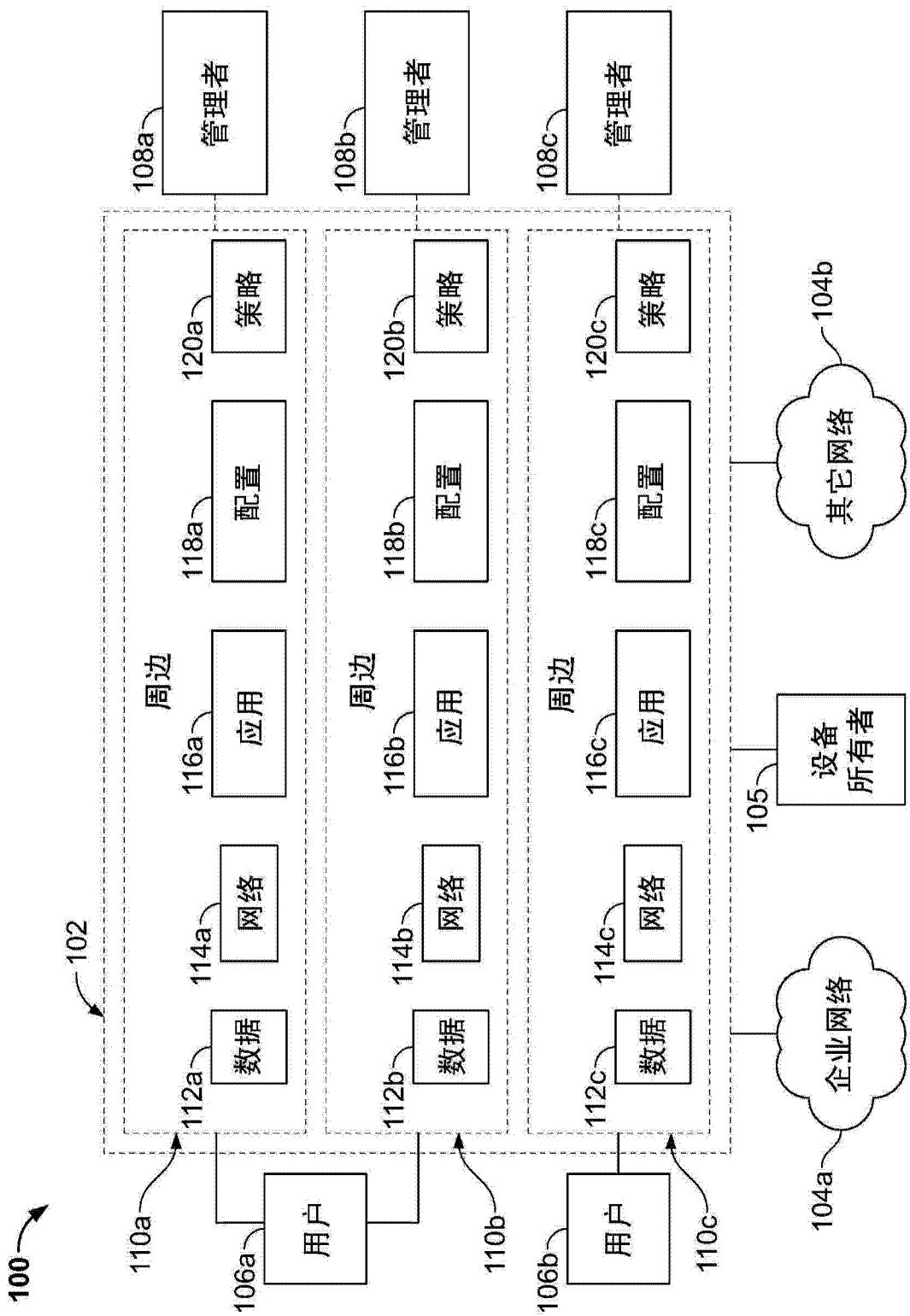


图 1

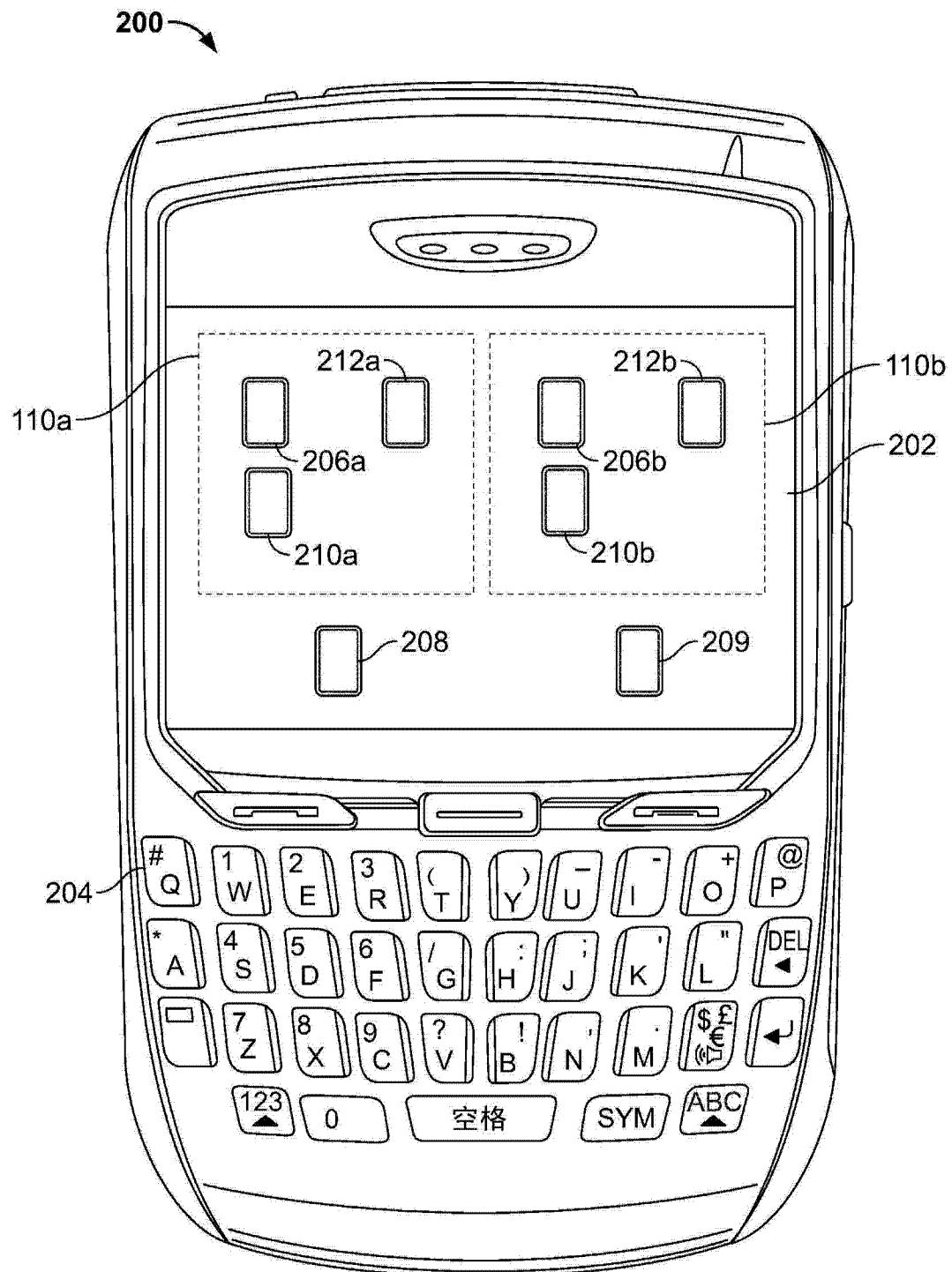


图 2

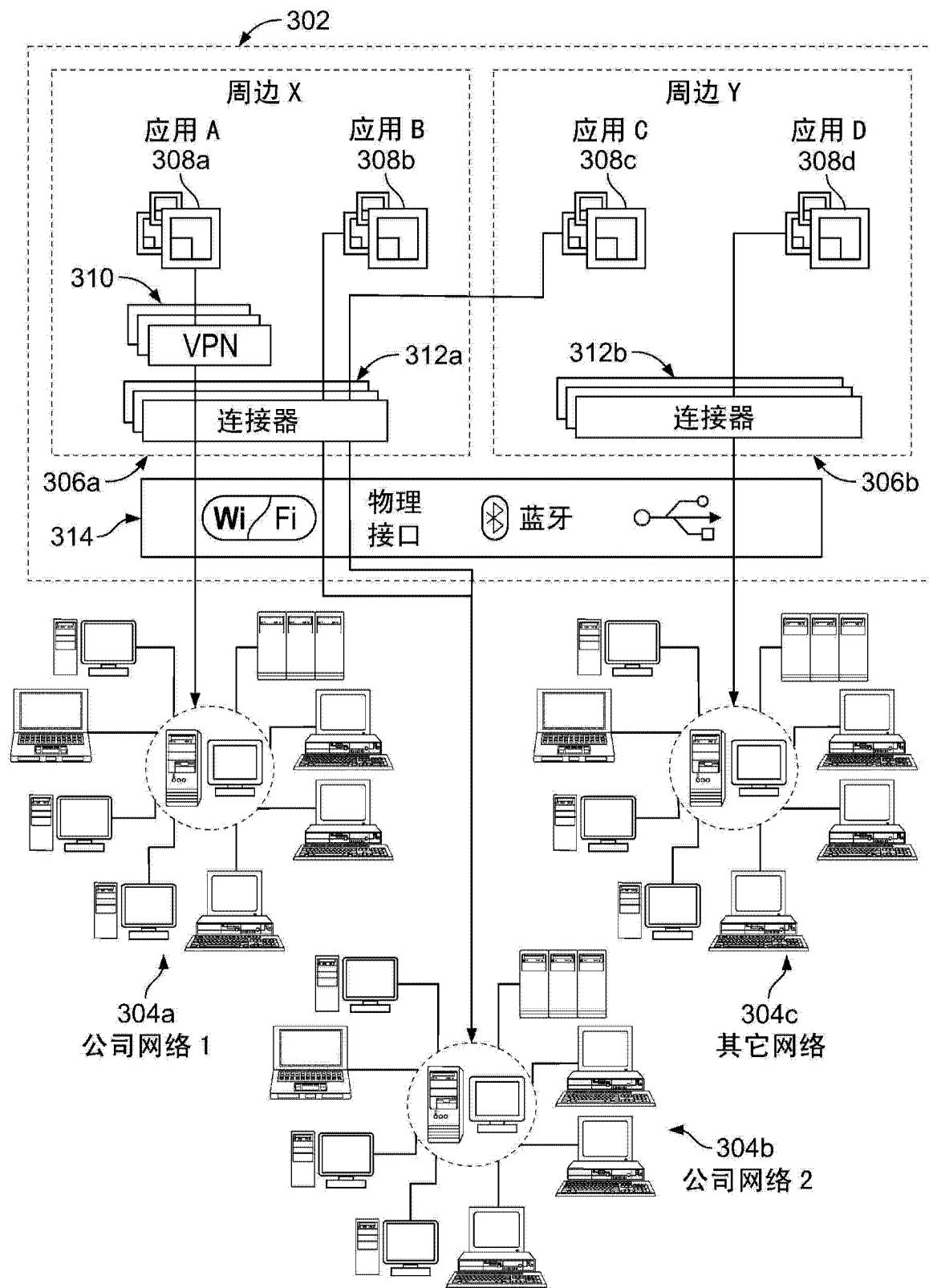


图 3

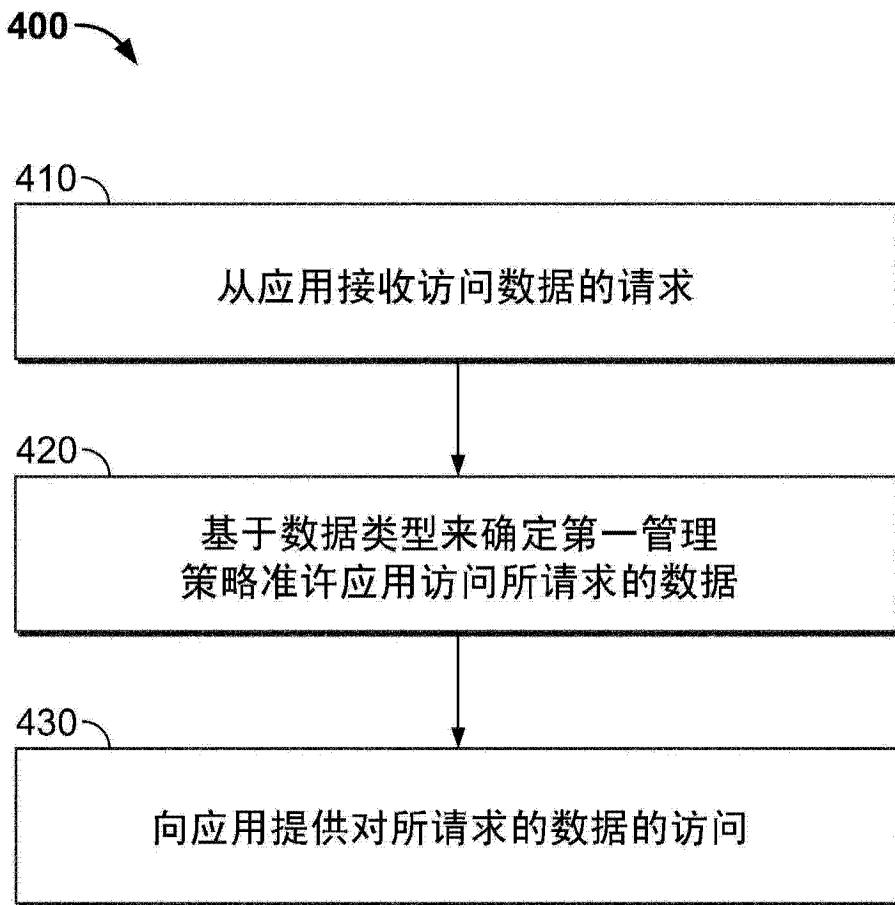


图 4