(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 105308923 B
(45)授权公告日 2018.12.04

(21)申请号 201380076963.3
(22)申请日 2013.09.17
(65)同一申请的已公布的文献号
申请公布号 CN 105308923 A
(43)申请公布日 2016.02.03
(30)优先权数据
61/806,577 2013.03.29 US
13/886,889 2013.05.03 US
61/861,736 2013.08.02 US
61/861,758 2013.08.02 US
14/021,227 2013.09.09 US
(85)PCT国际申请进入国家阶段日
2015.11.27
(86)PCT国际申请的申请数据
PCT/US2013/060047 2013.09.17
(87)PCT国际申请的公布数据
WO2014/158222 EN 2014.10.02
(73)专利权人 思杰系统有限公司
地址 美国佛罗里达州
(72)发明人 忠民·朗 盖瑞·巴顿 N·德赛 詹姆斯·R·沃克
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 周靖 郑霞
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 4/50(2018.01)
H04W 12/08(2009.01)
(56)对比文件
CN 101322379 A,2008.12.10,
CN 101727274 A,2010.06.09,
US 2010100825 A1,2010.04.22,
US 2012042036 A1,2012.02.16,
EP 2523107 A1,2012.11.14,
US 8020192 B2,2011.09.13,
审查员 孟维志

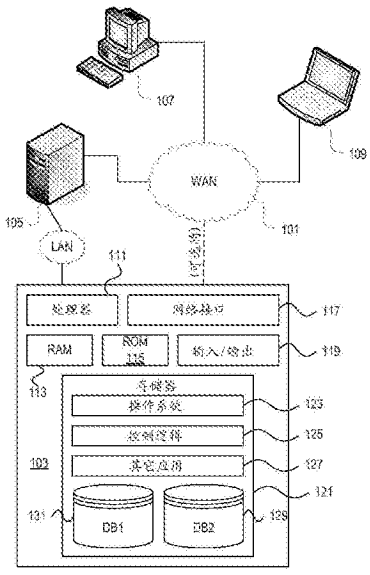
权利要求书2页 说明书32页 附图12页

(54)发明名称

对具有多操作模式的应用的数据管理

(57)摘要

描述了用于管理具有多个模式的应用的方法和系统。管理移动设备的设备管理器可监测移动设备。设备管理器可检测在受管模式(或在多个受管模式中)和非受管模式运行的应用的第一类型安装在移动设备上。当应用在设备上执行时,如,基于位置、用户、角色、工业呈现或其它预定背景,根据所选择的应用模式执行应用。



CN 105308923 B

1.一种用于管理具有多操作模式的应用的方法,包括:

从移动设备接收对可下载应用的列表的请求;

确定所述移动设备是否配备了能够在非受管模式中和受管模式中执行应用的应用管理框架,其中,所述非受管模式和所述受管模式提供不同等级的访问、安全和资源;以及

将可下载应用的列表发送到所述移动设备,其中:

当所述应用管理框架被确定为能用时,所述可下载应用的列表包括所述应用的第一版本,所述应用的所述第一版本在所述非受管模式和所述受管模式中可执行,以及

当所述应用管理框架被确定为不能用时,所述可下载应用的列表不包括所述应用的所述第一版本并且包括所述应用的第二版本,所述应用的所述第二版本在所述非受管模式中可执行而在所述受管模式中不可执行。

2.如权利要求1所述的方法,其中,确定所述移动设备是否配备了能够在所述非受管模式中和所述受管模式中执行所述应用的所述应用管理框架还包括检测与所述应用管理框架相关的受管应用安装在所述移动设备上。

3.如权利要求1所述的方法,其中,所述应用的所述第一版本与所述应用管理框架相关。

4.如权利要求3所述的方法,其中,将所述可下载应用的列表发送到所述移动设备还包括:

从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本,其中,基于与所述应用管理框架的关联,选择所述应用的所述第一版本。

5.如权利要求1所述的方法,其中,确定所述移动设备是否配备了能够在所述非受管模式中和所述受管模式中执行所述应用的所述应用管理框架还包括检测所述移动设备由与所述应用管理框架相关的设备管理器管理。

6.如权利要求5所述的方法,其中,所述应用的所述第一版本与所述设备管理器相关。

7.如权利要求6所述的方法,其中,将所述可下载应用的列表发送到所述移动设备还包括:

从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本,其中,基于与所述设备管理器的关联,选择所述应用的所述第一版本。

8.如权利要求1所述的方法,其中,所述应用的所述第一版本包括非受管应用,所述非受管应用被雇用所述移动设备的用户的企业修改以作为受管应用操作。

9.一种计算设备,包括:

处理器,其中,所述计算设备被配置为至少:

从移动设备接收对可下载应用的列表的请求;

确定所述移动设备是否配备了能够在非受管模式中和受管模式中执行应用的应用管理框架,其中,所述非受管模式和所述受管模式提供不同等级的访问、安全和资源;以及

将可下载应用的列表发送到所述移动设备,其中:

当所述应用管理框架被确定为能用时,所述可下载应用的列表包括所述应用的第一版本,所述应用的所述第一版本在所述非受管模式和所述受管模式中可执行,以及

当所述应用管理框架被确定为不能用时,所述可下载应用的列表不包括所述应用的所

述第一版本并且包括所述应用的第二版本，所述应用的所述第二版本在所述非受管模式中可执行而在所述受管模式中不可执行。

10.如权利要求9所述的计算设备，其中，确定所述移动设备是否配备了能够在所述非受管模式中和所述受管模式中执行所述应用的所述应用管理框架还包括检测与所述应用管理框架相关的受管应用安装在所述移动设备上。

11.如权利要求9所述的计算设备，其中，所述应用的所述第一版本与所述应用管理框架相关。

12.如权利要求11所述的计算设备，其中，将所述可下载应用的列表发送到所述移动设备还包括：

从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述应用管理框架的关联，选择所述应用的所述第一版本。

13.如权利要求9所述的计算设备，其中，确定所述移动设备是否配备了能够在所述非受管模式中和所述受管模式中执行所述应用的所述应用管理框架还包括检测所述移动设备由与所述应用管理框架相关的设备管理器管理。

14.如权利要求13所述的计算设备，其中，所述应用的所述第一版本与所述设备管理器相关。

15.如权利要求14所述的计算设备，其中，将所述可下载应用的列表发送到所述移动设备还包括：

从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述设备管理器的关联，选择所述应用的所述第一版本。

对具有多操作模式的应用的数据管理

[0001] 相关申请的交叉引用

[0002] 本申请要求2013年9月9日提交的题目为“对具有多操作模式的应用的数据管理(Data Management for an Application with Multiple Operation Modes)”的序列号为14/021,227的美国申请的权益,其相应地要求2013年8月2日提交的题目为“基于策略的应用管理(Policy-Based Application Management)”的临时申请61/861,736、2013年8月2日提交的题目为“对具有多操作模式的应用的数据管理(Data Management for an Application with Multiple Operation Modes)”的临时申请61/861,758以及2013年3月29日提交的题目为“用于企业移动性管理的系统和方法(Systems and Methods for Enterprise Mobility Management)”的临时申请61/806,557的权益并且是2013年5月2日提交的题目为“具有多操作模式的应用(Application with Multiple Operation Modes)”美国专利申请13/886,889的延续部分,其每个通过引用以其整体并入本文。

技术领域

[0003] 本申请涉及,但不限于对具有多操作模式的应用的数据管理。

[0004] 背景

[0005] 移动计算设备的使用日益增长。具体地,商务和其它企业已经开始依赖移动计算设备来允许个人远程访问各种企业资源。例如,这种资源可包括电子邮件服务、文件服务、数据和由企业的计算系统提供的其它电子资源。

[0006] 由于商务使用的这种不断渗入,个人开始将他们的移动计算设备用于商务和私人方式。例如,公司的员工可从相同的移动计算设备访问公司邮件账号和私人邮件账号。相应地,移动计算设备的特定功能可共享商务和私人方面。然而,商务信息通常需要安全通信和存储。另外,储存在移动设备上的商务信息可能需要管理。因此,需要设备管理器来管理储存在移动设备上的信息。

[0007] 概述

[0008] 下面呈现本文描述的各个方面的简要概述。这个概述不是广泛的概括,并且并不旨在标识关键的或决定性的元素或描绘权利要求的范围。下面的概述作为对以下提供的更详细描述的介绍性前奏仅以简化的形式呈现一些概念。

[0009] 本文描述了用于管理具有多操作模式的应用的方法和系统。管理移动设备的设备管理器可监测移动设备。设备管理器可检测在非受管模式和受管模式运行的预定类型的应用安装在移动设备上。操作模式可基于设备背景或设备相关的信息。例如,当用户凭证将用户授权为受信用户时,应用可在第一受管模式运行,并且应用可以其它方式在第二较低的安全模式运行。还可基于设备的物理位置、网络位置、用户凭证、用户角色、位置类型(如,医疗、金融机构经营场所、学校、政府实体等,还被称为工作场所环境类型)等选择操作模式。应用可在多于两个操作模式中执行,并且可在提供不同等级的访问、安全、资源等的多个不同的受管模式中操作。

[0010] 本申请的实施方案包括以下方面:

[0011] 1)一种方法，包括：

[0012] 从移动设备接收对可下载应用的列表的请求；

[0013] 确定所述移动设备是否配备了能够在非受管模式中和受管模式中执行应用的应用管理框架；

[0014] 将可下载应用的列表发送到所述移动设备，其中：

[0015] 当所述应用管理框架被确定为能用时，所述列表包括所述应用的第一版本，所述应用的所述第一版本在所述非受管模式和所述受管模式中可执行，以及

[0016] 当所述应用管理框架被确定为不能用时，所述列表不包括所述应用的所述第一版本并且包括所述应用的第二版本，所述应用的所述第二版本在所述非受管模式中可执行而在所述受管模式中不可执行。

[0017] 2)如项目1)所述的方法，其中，确定所述移动设备是否配备了能够在所述非受管模式和所述受管模式中执行应用的应用管理框架还包括检测与应用管理框架相关的受管应用安装在所述移动设备上。

[0018] 3)如项目1)所述的方法，其中，所述可下载应用的所述第一版本与所述应用管理框架相关。

[0019] 4)如项目3)所述的方法，其中，将可下载应用的列表发送到所述移动设备还包括：

[0020] 从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述应用管理框架的关联，选择所述应用的所述第一版本。

[0021] 5)如项目1)所述的方法，其中，确定所述移动设备是否配备了能够在所述非受管模式和所述受管模式中执行应用的应用管理框架还包括检测所述移动设备由与所述应用管理框架相关的设备管理器管理。

[0022] 6)如项目5)所述的方法，其中，所述可下载应用的所述第一版本与所述设备管理器相关。

[0023] 7)如项目6)所述的方法，其中，将可下载应用的列表发送到所述移动设备还包括：

[0024] 从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述设备管理器的关联，选择所述应用的所述第一版本。

[0025] 8)如项目1)所述的方法，其中，所述应用的所述第一版本包括非受管应用，所述非受管应用被雇用所述移动设备的用户的企业修改以作为受管应用操作。

[0026] 9)一种计算设备，包括：

[0027] 处理器，其中，所述计算设备被配置为至少：

[0028] 从移动设备接收对可下载应用的列表的请求；

[0029] 确定所述移动设备是否配备了能够在非受管模式中和受管模式中执行应用的应用管理框架；

[0030] 将可下载应用的列表发送到所述移动设备，其中：

[0031] 当所述应用管理框架被确定为能用时，所述列表包括所述应用的第一版本，所述应用的所述第一版本在所述非受管模式和所述受管模式中可执行，以及

[0032] 当所述应用管理框架被确定为不能用时，所述列表不包括所述应用的所述第一版

本并且包括所述应用的第二版本，所述应用的所述第二版本在所述非受管模式中可执行而在所述受管模式中不可执行。

[0033] 10)如项目9)所述的计算设备，其中，确定所述移动设备是否配备了能够在所述非受管模式和所述受管模式中执行应用的应用管理框架还包括检测与应用管理框架相关的受管应用安装在所述移动设备上。

[0034] 11)如项目9)所述的计算设备，其中，所述可下载应用的所述第一版本与所述应用管理框架相关。

[0035] 12)如项目11)所述的计算设备，其中，将可下载应用的列表发送到所述移动设备还包括：

[0036] 从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述应用管理框架的关联，选择所述应用的所述第一版本。

[0037] 13)如项目9)所述的计算设备，其中，确定所述移动设备是否配备了能够在所述非受管模式和所述受管模式中执行应用的应用管理框架还包括检测所述移动设备由与所述应用管理框架相关的设备管理器管理。

[0038] 14)如项目13)所述的计算设备，其中，所述可下载应用的所述第一版本与所述设备管理器相关。

[0039] 15)如项目14)所述的计算设备，其中，将可下载应用的列表发送到所述移动设备还包括：

[0040] 从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述设备管理器的关联，选择所述应用的所述第一版本。

[0041] 16)如项目9)所述的计算设备，其中，所述应用的所述第一版本包括非受管应用，所述非受管应用被雇用所述移动设备的用户的企业修改以作为受管应用操作。

[0042] 17)一种或多种储存了计算机可执行指令的非暂时的计算机可读存储介质，当所述计算机可执行指令被数据处理系统的一个或多个处理器执行时，所述计算机可执行指令促使所述系统实现：

[0043] 从移动设备接收对可下载应用的列表的请求；

[0044] 确定所述移动设备是否配备了能够在非受管模式中和受管模式中执行应用的应用管理框架；

[0045] 将可下载应用的列表发送到所述移动设备，其中：

[0046] 当所述应用管理框架被确定为能用时，所述列表包括所述应用的第一版本，所述应用的所述第一版本在所述非受管模式和所述受管模式中可执行，以及

[0047] 当所述应用管理框架被确定为不能用时，所述列表不包括所述应用的所述第一版本并且包括所述应用的第二版本，所述应用的所述第二版本在所述非受管模式中可执行而在所述受管模式中不可执行。

[0048] 18)如项目17)所述的计算机可读存储介质，其中，确定所述移动设备是否配备了能够在所述非受管模式和所述受管模式中执行应用的应用管理框架还包括检测与应用管理框架相关的受管应用安装在所述移动设备上。

[0049] 19)如项目18)所述的计算机可读存储介质，其中，所述可下载应用的所述第一版本与所述应用管理框架相关。

[0050] 20)如项目19)所述的计算机可读存储介质，其中，将可下载应用的列表发送到所述移动设备还包括：

[0051] 从所述应用的在所述非受管模式和所述受管模式中可执行的多个版本中选择所述应用的所述第一版本，其中，基于与所述应用管理框架的关联，选择所述应用的所述第一版本。

[0052] 结合下面更详细讨论的公开的益处，将理解这些和其它方面。

[0053] 附图简述

[0054] 可通过下面参照附图考虑的描述获得本文描述的方面的更完整的理解和其优势，其中相似的参考数字表示相似的特征，且其中：

[0055] 图1描绘的是可依据说明性实施方案使用的说明性计算机系统架构。

[0056] 图2描绘的是可依据说明性实施方案使用的说明性远程访问系统架构。

[0057] 图3描绘的是可依据说明性实施方案使用的说明性虚拟(超级管理器(hypervisor))系统架构。

[0058] 图4描绘的是可依据说明性实施方案使用的说明性基于云的系统的架构。

[0059] 图5描绘的是可依据说明性实施方案使用的说明性企业移动性管理系统。

[0060] 图6描绘的是可依据说明性实施方案使用的另一个说明性企业移动性管理系统。

[0061] 图7描绘的是依据说明性实施方案的移动设备的示例界面。

[0062] 图8是依据说明性实施方案的用于确定应用的应用模式的流程图。

[0063] 图9是依据说明性实施方案的用于确定应用的账号类型背景的流程图。

[0064] 图10是依据说明性实施方案的用于确定应用的位置背景的流程图。

[0065] 图11是依据说明性实施方案的用于确定应用的预定应用状态背景的流程图。

[0066] 图12是依据说明性实施方案的用于确定应用的网络连接背景的流程图。

[0067] 图13是依据说明性实施方案的用于确定应用的设置背景的流程图。

[0068] 图14是依据说明性实施方案的用于切换应用的应用模式的流程图。

[0069] 图15是依据说明性实施方案的用于管理具有多操作模式的应用的流程图。

[0070] 图16是依据说明性实施方案的用于管理多模式应用的流程图。

[0071] 图17是依据说明性实施方案的用于应用商店的流程图。

[0072] 详细描述

[0073] 在各个实施方案的下列描述中，参考了上面提到并形成各个实施方案的一部分的附图，并且其中以说明各个实施方案的方式示出，本文所描述的各方面可在各个实施方案中被实践。应当理解的是，可利用其它实施方案，并且在不脱离本文所描述的范围的情况下可做出结构和功能的修改。各种方面能够是其它实施方案并能够以各种不同的方式实践或执行。

[0074] 作为对下面更详细描述的主题的概述，本文所描述的方面针对在移动计算设备处使用受管移动应用(尤其是与能够在多操作模式执行的应用一起使用时)来控制对企业计算系统处的资源的远程访问。访问管理器可执行验证过程，其确定请求访问企业资源的移动应用是否已经准确地确定其自身身份，以及随后在安装在移动计算设备之后是否未被更

改。以这种方式，访问管理器可保证请求访问企业资源的移动应用可被信任并且没有尝试避开用于保护那些企业资源的安全性机制。因此，与企业关联的个人可有利地在他们的个人移动设备处使用预先审核的应用来利用企业资源。

[0075] 应当理解的是，本文所使用的短语和术语是出于描述的目的，并且不应被视为限制性的。更确切地说，本文所使用的短语和术语被给出它们最广泛的解释和意义。“包括”和“包含”及其变型的使用旨在包括下文中列出的项目及其等效物以及附加项目及其等效物。术语“安装”、“连接”、“耦合”、“定位”、“啮合”和类似术语的使用旨在包括直接和间接的安装、连接、耦合、定位和啮合。

[0076] 计算架构

[0077] 计算机软件、硬件和网络可用于多种不同的系统环境中，除了别的之外，包括单机、连网、远程访问(又叫做远程桌面)、虚拟化和/或基于云的环境。图1示出了系统架构和数据处理设备的一个示例，其被用于在单机环境和/或网络环境中执行本文描述的一个或多个说明性方面。各个网络节点103、105、107和109可经由诸如互联网的广域网(WAN)101进行互连。还可使用或可选地使用其它网络，包括私有内联网、企业网络、LAN、城域网(MAN)无线网、个人网络(PAN)等。网络101用于说明的目的并且可以用更少或附加的计算机网络来代替。局域网(LAN)可具有任何已知的LAN拓扑中的一个或多个，并且可使用多种不同协议中的一个或多个，诸如以太网。设备103、105、107、109和其它设备(未示出)可经由双绞线、同轴电缆、光纤、无线电波或其它通信媒介连接到一个或多个网络。

[0078] 本文所使用以及附图中所描述的术语“网络”不仅指其中远程存储设备经由一个或多个通信路径耦合在一起的系统，还指有时可耦合到该类系统的具有存储能力的单机设备。因此，术语“网络”不仅包括“物理网络”还包括“内容网络”，其由单个实体引起的、驻留在所有的物理网络上的数据组成。

[0079] 组件可包括数据服务器103、网络服务器105和客户端计算机107、109。数据服务器103提供对数据库和控制软件的全面访问、控制和管理，用于执行本文描述的一个或多个说明性方面。数据服务器103可连接到网络服务器105，其中用户通过该网络服务器105根据请求与数据交互并获得数据。可选地，数据服务器103可充当网络服务器本身，并直接地连接到互联网。数据服务器103可通过网络101(例如，互联网)经由直接或间接连接或经由一些其它网络连接到网络服务器105。用户可使用远程计算机107、109与数据服务器103交互，如使用经由网络服务器105托管的一个或多个对外公开的网站连接至数据服务器103的网络浏览器。客户端计算机107、109可用于与数据服务器103合作以访问存储在其中的数据，或可用于其它目的。例如，如本领域中已知的，用户可使用互联网浏览器从客户端设备107访问网络服务器105，或通过执行经由计算机网络(如互联网)与网络服务器105和/或数据服务器103通信的软件应用来访问网络服务器105。

[0080] 服务器和应用可被组合在相同的物理机器上，并且保留不同的虚拟或逻辑地址，或可驻留在不同的物理机器上。图1仅示出可以被使用的网络架构的一个示例，并且本领域中的技术人员应当理解，如在本文进一步所描述的，所使用的特定网络架构和数据处理设备可以改变，并且对于它们提供的功能来说是次要的。例如，通过网络服务器105和数据服务器103提供的服务可被组合在单一服务器上。

[0081] 每个组件103、105、107、109可以是任何类型的已知计算机、服务器或数据处理设

备。例如，数据服务器103可包括控制速率服务器103的总体操作的处理器111。数据服务器103还可包括RAM 113、ROM 115、网络接口117、输入/输出接口119(例如，键盘、鼠标、显示器、打印机等等)，以及存储器121。I/O 119可包括用于读取、写入、显示和/或打印数据或文件的各种接口单元和驱动器。存储器121还可存储用于控制数据处理设备103的整体操作的操作系统软件123、用于指示数据服务器103以执行本文描述的方面的控制逻辑125以及提供辅助、支持、和/或其它可用于或不可用于与本文描述的方面结合使用的功能的其它应用软件127。本文中，控制逻辑还可被称为数据服务器软件125。数据服务器软件的功能可指基于被编码到控制逻辑中的规则自动进行的操作或决定、通过用户将输入提供到系统中来手动进行的操作或决定和/或基于用户输入(例如，查询、数据更新等等)的自动处理的组合。

[0082] 存储器121还可存储在本文描述的一个或多个方面的性能中使用的数据，包括第一数据库129和第二数据库131。在一些实施方案中，第一数据库可包括第二数据库(例如，作为分离的表、报告等)。即，该信息可存储在单个数据库中，或分离成不同的逻辑、虚拟或物理数据库，其取决于系统设计。设备105、107、109可以具有如关于设备103所述的相似或不同的架构。本领域技术人员应理解，如本文所述的数据处理设备103(或设备105、107、109)的功能可遍布多个数据处理设备，例如，以将处理负载分配到多个计算机、以基于地理位置、用户访问级别、服务质量(QoS)等分开事务。

[0083] 一个或多个方面可以在通过本文所描述的一个或多个计算机或其它设备执行的、诸如一个或多个程序模块中的计算机可用或可读数据和/或计算机可执行指令来体现。通常，程序模块包括例程、程序、对象、组件、数据结构等等，当被计算机或其它设备中的处理器执行时，该程序模块执行特定任务或实施特定抽象数据类型。该模块可以用源代码编程语言来写，随后被编译用于执行，或可以用诸如(但不限于)HTML或XML的脚本语言来写。计算机可执行指令可被存储在诸如非易失性存储设备的计算机可读介质上。可使用任何适合的计算机科组存储介质，包括硬盘、CD-ROM、光存储设备、磁存储设备和/或其任意组合。另外，可以用电磁波的形式在源和目的之间传递表示本文所描述的数据或事件的各种传输(非存储)介质，该电磁波通过诸如金属丝、光纤、和/或无线传输介质(例如，空气和/或空间)的信号-传导介质传播。本文所描述的各个方面可被体现为方法、数据处理系统或计算机程序产品。因此，各种功能可整体或部分地体现在软件、固件和/或硬件或硬件等同物，诸如集成电路、现场可编程门阵列(FPGA)，等等。特定的数据结构可用于更有效地执行本文所述的一个或多个方面，且预期这种数据结构在本文所述的计算机可执行指令和计算机可用数据的范围内。

[0084] 进一步参考图2，可在远程访问环境中实现本文所述的一个或多个方面。图2描绘了示例性的系统架构，包括在说明性计算环境200中的通用计算设备201，其可根据本文所述的一个或多个说明性方面来使用。通用计算设备201可以被用作单服务器或多服务器桌面虚拟化系统(例如，远程访问或云系统)中的服务器206a，所述系统经配置提供用于客户端访问设备的虚拟机。通用计算设备201可具有用于控制服务器及其相关组件(包括随机存取存储器(RAM)205、只读存储器(ROM)207、输入/输出(I/O)模块209和存储器215)的整体操作的处理器203。

[0085] I/O模块209可包括鼠标、键盘、触摸屏、扫描仪、光学阅读器和/或手写笔(或其它输入设备)(通用计算设备201的用户可通过这些输入设备提供输入)，并且也可包括用于提

供音频输出的扬声器和用于提供文本、视听和/或图形输出的视频显示设备中的一个或多个。软件可存储在存储器215和/或其它储存器中，以提供指令给处理器203用于将通用计算设备201配置为专用计算设备，以便执行如本文所述的各种功能。例如，存储器215可以存储由计算设备201使用的软件(诸如操作系统217、应用219和关联的数据库221)。

[0086] 计算设备201可在网络化环境中操作，该网络化环境支持到诸如终端240(也被称为客户端设备)的一个或多个远程计算机的连接。终端240可以是个人计算机、移动设备、膝上计算机、平板电脑或服务器，其包括以上描述的关于通用计算设备103或201的许多或全部元素。在图2中描绘的网络连接包括局域网(LAN)225和广域网(WAN)229，但还可包括其它网络。当用于LAN网络环境中时，计算设备201可通过网络接口或适配器223连接到LAN 225。当在WAN联网环境中使用时，计算设备201可包括调制解调器227或用于建立在WAN 229(诸如计算机网络230(例如，互联网))上的通信的其它广域网接口。将认识到的是，所示的网络连接是说明性的，且可使用在计算机之间建立通信链路的其它装置。计算设备201和/或终端240还可为移动终端(例如，移动电话、智能电话、PDA、笔记本等等)，其包括各种其它部件，诸如电池、扬声器和天线(未示出)。

[0087] 本文描述的各方面也可以用许多其它通用或专用计算系统环境或配置来运行。可适合于结合本文所述的方面使用的其它计算系统、环境和/或配置的实例，包括，但不限于，个人计算机、服务器计算机、手持或笔记本设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境，等等。

[0088] 如图2所示，一个或多个客户端设备240可与一个或多个服务器206a-206n(在本文中统称为“服务器206”)通信。在一个实施方案中，计算环境200可包括在服务器206和客户机240之间安装的网络装置。该网络装置可管理客户端/服务器连接，并在某些情况下可在多个后端服务器206之间负载平衡客户端连接。

[0089] 在一些实施方案中，客户端机器240可被称为单一客户端机器240或单一组客户端机器240，而服务器206可被称为单一服务器206或单一组服务器206。在一个实施方案中，单一客户端机器240与多于一台服务器206通信，而在另一个实施方案中，单一服务器206与多于一台客户算机器通信240。在又一个实施方案中，单一客户端机器240与单一服务器206通信。

[0090] 在一些实施方案中，可通过下列非穷举术语中的任何一个指代客户端机器240：客户端机器；客户端；客户端计算机；客户端设备；客户端计算设备；本地机器；远程机器；客户端节点；端点；或端点节点。在一些实施方案中，可通过下列非穷举术语中的任何一个指代服务器206：服务器；本地机器；远程机器；服务器群；或主机计算设备。

[0091] 在一个实施方式中，客户端机器240可以是虚拟机。虚拟机可以是任何虚拟机，而在一些实施方案中虚拟机可以是由1型或2型的超级管理器所管理的任何虚拟机，例如，由Citrix Systems、IBM、VMware开发的超级管理器，或任何其它超级管理器。在一些方面中，虚拟机可由超级管理器管理，而在其它方面中，虚拟机可由在服务器206上执行的超级管理器或在客户端240上执行的超级管理器管理。

[0092] 一些实施方案包括客户端设备240，其显示由在服务器206上远程执行的应用或由其它远程放置的机器上远程执行的应用生成的应用输出。在这些实施方案中，客户端设备

240可以执行虚拟机接收器程序或应用，以在应用窗口、浏览器或其它输出窗口中显示输出。在一个实例中，应用是桌面，而在其它实例中应用是生成或呈现桌面的应用。桌面可包括为操作系统的实例提供用户界面的图形壳，在该操作系统中可集成本地和/或远程应用。如在本文所使用的，应用是在操作系统(和可选地，还有桌面)的实例已经被加载之后执行的程序。

[0093] 在一些实施方案中，服务器206使用远程表示协议或其它程序以将数据发送给瘦客户端或在客户端上执行的远程显示应用，以便呈现通过在服务器206上执行的应用生成的显示输出。瘦客户端或远程显示协议可以是下列非穷举协议列表中的任意一个：通过佛罗里达州劳德代尔堡(Ft.Lauderdale,Florida)的Citrix系统公司开发的独立计算架构(ICA)协议；或通过华盛顿雷德蒙德(Redmond,Washington)的微软公司制造的远程桌面协议(RDP)。

[0094] 远程计算环境可包括多于一个的服务器206a-206n，使得，例如在云计算环境中，服务器206a-206n逻辑组合在一起成服务器群206。服务器群206可包括地理上分散而同时逻辑分组在一起的服务器206，或彼此接近放置同时在逻辑上分组在一起的服务器206。在一些实施方案中，在服务器群206中的地理上分散的服务器206a-206n使用WAN(广域网)、MAN(城域网)、或LAN(局域网)通信，其中不同的地理区域可表征为：不同大陆；大陆的不同区域；不同的国家；不同的州；不同的城市；不同的校区；不同的房间；或前述地理位置的任何组合。在一些实施方案中，服务器群206可作为单一实体进行管理，而在其它实施方案中，服务器群206可包括多个服务器群。

[0095] 在一些实施方案中，服务器群可包括服务器206，其执行基本上类似类型的操作系统平台(例如，WINDOWS、UNIX、LINUX、iOS、ANDROID、SYMBIAN，等)。在其它实施方案中，服务器群206可包括执行第一类型的操作系统平台的一个或多个服务器的第一组，以及执行第二类型的操作系统平台的一个或多个服务器的第二组。

[0096] 服务器206可根据需要配置成任何类型的服务器，例如，文件服务器、应用服务器、web服务器、代理服务器、装置、网络装置、网关、应用网关、网关服务器、虚拟服务器、部署服务器、SSL VPN服务器、防火墙、网络服务器、应用服务器或作为主应用服务器、执行活动目录的服务器、或执行提供防火墙功能、应用功能、或负载平衡功能的应用加速程序的服务器。还可使用其它服务器类型。

[0097] 一些实施方案包括第一服务器106a，其接收来自客户端机器240的请求、转发该请求至第二服务器106b，并使用来自第二服务器106b的响应对由客户端机器240生成的请求响应。第一服务器106a可以获得可用于客户端机器240的应用的列举以及与托管在应用列举内被识别的应用的应用服务器206相关联的地址信息。然后，第一服务器106a可使用web接口呈现对客户端请求的响应，并直接与客户端240通信以给客户端240提供对所标识的应用的访问。一个或多个客户端240和/或一个或多个服务器206可经由例如网络101的网络230传输数据。

[0098] 图2示出说明性桌面虚拟化系统的高层架构。如图所示，桌面虚拟化系统可以是单服务器或多服务器系统、或云系统，包括配置为给一个或多个客户端访问设备240提供虚拟桌面和/或虚拟应用的至少一个虚拟化服务器206。如本文所使用的，桌面指图形环境或空间，其中一个或多个应用可被托管和/或执行。桌面可包括为操作系统的实例提供用户界面

的图形壳，本地和/或远程应用可集成在操作系统中。应用可包括装载了操作系统(和，可选地，还有桌面)的实例之后执行的程序。操作系统的每个实例可以是真实的(例如每个设备一个操作系统)或虚拟的(例如在单个设备上运行的OS的很多实例)。每个应用可在本地设备上执行或在远程定位的设备上执行(例如远程)。

[0099] 进一步参考图3，计算机装置301可以被配置为虚拟化环境或云计算环境中的虚拟化服务器(例如单个服务器、多个服务器)。在图3中示出的虚拟化服务器301可以被部署为在图2中示出的服务器206的一个或多个实施方案和/或由其实现，或通过其它已知的计算设备实现。包括在虚拟化服务器301中的是硬件层，其可以包括一个或多个物理盘304、一个或多个物理装置306、一个或多个物理处理器308和一个或多个物理存储器316。在一些实施方式中，固件312可存储在物理存储器316中的存储器元件内并可由一个或多个物理处理器308执行。虚拟化服务器301还可以包括操作系统314，其可以被存储在物理存储器316的存储器元件中并由物理处理器308中的一个或多个执行。而且，超级管理器302可存储在物理存储器316中的存储器元件中，并可由一个或多个物理处理器308执行。

[0100] 在物理处理器308中的一个或多个上执行的可以是一个或多个虚拟机332A-C(一般称为332)。每个虚拟机332可以具有虚拟盘326A-C和虚拟处理器328A-C。在一些实施方案中，第一虚拟机332A可使用虚拟处理器328A执行包括工具堆栈324的控制程序320。控制程序320可以被称为控制虚拟机、Dom0、域0，或用于系统管理和/或控制的其它虚拟机。在某些实施方案中，一个或多个虚拟机332B-C可以使用虚拟处理器328B-C执行访客(guest)操作系统330A-B。

[0101] 虚拟化服务器301可以包括与虚拟化服务器301通信且具有一个或多个硬件的硬件层310。在某些实施方案中，硬件层310可以包括一个或多个物理盘304、一个或多个物理装置306、一个或多个物理处理器308和一个或多个存储器216。物理组件304、306、308和316可以包括例如上文所述的组件中的任意一个。物理装置306可以包括例如网络接口卡、视频卡、键盘、鼠标、输入装置、监视器、显示装置、扬声器、光学驱动器、存储装置、通用串行总线连接、打印机、扫描器、网络元件(例如，路由器、防火墙、网络地址转换器、负载平衡器、虚拟专用网络(VPN)网关、动态主机配置协议(DHCP)路由器等)或与虚拟化服务器301连接或通信的任何装置。硬件层310中的物理存储器316可包括任何类型的存储器。物理存储器316可以存储数据，并且在某些实施方案中可以存储一个或多个程序或一组可执行指令。图3示出其中固件312被存储在虚拟化服务器301的物理存储器316内的实施方案。存储在物理存储器316中的程序或可执行指令可以由虚拟化服务器301的一个或多个处理器308来执行。

[0102] 虚拟化服务器301还可包括超级管理器302。在某些实施方案中，超级管理器302可以是一种程序，其由虚拟化服务器301上的处理器308来执行，以创建和管理任何数量的虚拟机332。超级管理器302可以被称为虚拟机监视器或平台虚拟化软件。在一些实施方案中，超级管理器302可以是监视在计算机器上执行的虚拟机的可执行指令以及硬件的任何组合。超级管理器302可以是类型2的超级管理器，其中，该超级管理器在执行于虚拟化服务器301上的操作系统314内执行。虚拟机然后在超级管理器之上的层执行。在一些实施方案中，2型超级管理器在用户的操作系统的背景内执行，以使2型超级管理器与用户的操作系统进行交互。在其它实施方案中，在虚拟化环境中的一个或多个虚拟化服务器201可以替代地包括类型1的超级管理器(未示出)。类型1的超级管理器可通过直接访问硬件层310内的硬件

和资源而在虚拟化服务器301上执行。就是说，虽然2型超级管理器302通过如所示出的主机操作系统314访问系统资源，但是1型超级管理器可无需主机操作系统314而直接访问所有系统资源。1型超级管理器可以在虚拟化服务器301的一个或多个物理处理器308上直接执行，并且可以包括存储在物理存储器316中的程序数据。

[0103] 在某些实施方案中，超级管理器302可以模拟直接访问系统资源的操作系统330或控制程序320的任何方式向在虚拟机332上执行的操作系统330或控制程序320提供虚拟化资源。系统资源可以包括但不限于物理装置306、物理盘304、物理处理器308、物理存储器316和包括在虚拟化服务器301硬件层310中的任何其它组件。超级管理器302可以被用于模拟虚拟化硬件、分区物理硬件、虚拟化物理硬件和/或执行提供访问计算环境的虚拟机。在另外的其它实施方案中，超级管理器302控制用于在虚拟化服务器301上执行的虚拟机332的处理器调度和存储器分区。超级管理器302可包括由加利福尼亚州帕罗奥多的VMWare公司制造的那些超级管理器；XEN超级管理器，一种开源产品，其开发由开源Xen.org社区监督；由微软公司提供的HyperV、VirtualServer或虚拟PC超级管理器；或其它超级管理器。在某些实施方案中，虚拟化服务器301执行创建虚拟机平台的超级管理器302，访客操作系统可以在该虚拟机平台上执行。在这些实施方案中，虚拟化服务器301可以被称为主机服务器。这样的虚拟化服务器的例子是由佛罗里达州罗德岱堡的Citrix系统公司提供的XEN SERVER。

[0104] 超级管理器302可以创建访客操作系统330在其中执行的一个或多个虚拟机332B-C(总称为332)。在某些实施方案中，超级管理器302可以加载虚拟机镜像以创建虚拟机332。在其它实施方案中，超级管理器302可在虚拟机332内执行访客操作系统330。在另外的其它实施方案中，虚拟机332可以执行访客操作系统330。

[0105] 除了创建虚拟机332之外，超级管理器302可控制至少一个虚拟机332的执行。在其它实施方案中，超级管理器302可以向至少一个虚拟机332呈现由虚拟化服务器301提供的至少一个硬件资源(例如，硬件层310内可用的任何硬件资源)的抽象。在其它实施方案中，超级管理器302可以控制虚拟机332访问虚拟化服务器301中可用的物理处理器308的方式。控制对物理处理器308的访问可包括确定虚拟机332是否应有权访问处理器308，以及如何将物理处理器能力提供给虚拟机332。

[0106] 如图3中所示，虚拟化服务器301可以托管或执行一个或多个虚拟机332。虚拟机332是可执行指令集，其在由处理器308执行时，模仿物理计算机的操作，使得虚拟机332可以非常类似于物理计算设备来执行程序和过程。虽然图3示出其中的虚拟化服务器301托管三个虚拟机332的实施方案，但是在其它实施方案中，虚拟化服务器301可以托管任何数量的虚拟机332。在某些实施方案中，超级管理器302向每个虚拟机332提供该虚拟机332可用的物理硬件、存储器、处理器和其它系统资源的独特虚拟视图。在某些实施方案中，该独特虚拟视图可以基于虚拟机许可、策略引擎对一个或多个虚拟机标识符的应用、访问虚拟机的用户、在虚拟机上执行的应用、由虚拟机访问的网络、或任何其它期望的标准中的一个或多个。例如，超级管理器302可以创建一个或多个非安全虚拟机332和一个或多个安全虚拟机332。非安全虚拟机332可被禁止访问安全虚拟机332可被允许访问的资源、硬件、存储器位置和程序。在其它实施方案中，超级管理器302可以向每个虚拟机332提供该虚拟机332可用的物理硬件、存储器、处理器和其它系统资源的大致相似的虚拟视图。

[0107] 每一个虚拟机332可包括虚拟盘326A-C(统称为326)和虚拟处理器328A-C(统称为328)。虚拟盘326在一些实施方式中是虚拟化服务器301的一个或多个物理磁盘304或虚拟化服务器301的一个或多个物理磁盘304的一部分的虚拟化视图。物理磁盘304的虚拟化视图可由超级管理器302产生、提供并管理。在一些实施方案中,超级管理器302给每个虚拟机332提供物理磁盘304的不同视图。因此,在这些实施方案中,当与其它虚拟盘326比较时,包括在每个虚拟机332中的特定虚拟盘326可以是不同的。

[0108] 虚拟处理器328可以是虚拟服务器301的一个或多个物理处理器308的虚拟化视图。在一些实施方案中,可通过超级管理器302生成、提供和管理物理处理器308的虚拟化视图。在一些实施方案中,虚拟处理器328基本上具有至少一个物理处理器308的所有相同特性。在其它实施方案中,虚拟化处理器308提供物理处理器308的更改视图,使得虚拟处理器328的特性中的至少某些特性不同于对应物理处理器308的特性。

[0109] 进一步参考图4,本文所描述的一些方面可在基于云的环境中实施。图4说明了云计算环境(或云系统)400的实例。如在图4中看到的,客户端计算机411-414可与云管理服务器410通信以访问云系统的计算资源(例如主机服务器403、存储资源404和网络资源405)。

[0110] 管理服务器410可以在一个或多个物理服务器上实施。管理服务器410除了可以运行其它软件以外,还可以运行例如Ft.Lauderdale,FL Citrix Systems公司的CLOUDSTACK或OPENSTACK。管理服务器410可管理各种计算资源,包括云硬件和软件资源,例如主机计算机403、数据存储设备404和联网设备405。云硬件和软件资源可以包括专用和/或公共组件。例如,云可被配置为由一个或多个特定的消费者或客户端计算机411-414和/或通过私有网络使用的私有云。在其它实施方式中,公共云或混合公共-专用云可通过开放或混合网络由其它消费者使用。

[0111] 管理服务器410可被配置成提供用户界面,云操作员和云客户可通过用户界面与云系统交互。例如,管理服务器410可提供一组API和/或具有用户界面的一个或多个云操作员控制台应用(例如基于web的单机应用)以允许云操作员管理云资源,配置虚拟化层,管理客户账户,并执行其它云管理任务。管理服务器410还可以包括一组API和/或带有用户界面的一个或多个客户控制台应用,该用户界面经配置经由客户端计算机411-414接收来自终端用户的云计算请求(例如形成、更改或破坏云内的虚拟机的请求)。客户端计算机411-414可以经由互联网或其它通信网络连接到管理服务器410,并且可以请求访问由管理服务器410管理的计算资源中的一个或多个计算资源。响应于客户端请求,管理服务器410可包括被配置成基于客户端请求来选择并提供在云系统的硬件层中的物理资源的资源管理器。例如,管理服务器410和云系统的另外组件可以经配置通过网络(例如,互联网)提供、形成和管理用于在客户端计算机411-414的客户的虚拟机和它们的运行环境(例如,超级管理器、存储资源、由网络元件提供的服务等),向客户提供计算资源、数据存储服务、联网性能以及计算机平台和应用支持。云系统还可被配置成提供各种特定的服务,包括安全系统、开发环境、用户界面等。

[0112] 特定客户端411-414可以是相关的,例如,不同客户端计算机代表相同终端用户或附属于相同公司或组织的不同用户创建虚拟机。在其它示例中,特定客户端411-414可以是不相关的,例如附属于不同公司或组织的用户。对于不相关的客户端,可对其它用户隐藏关于任一个用户的虚拟机或储存器的信息。

[0113] 现在参考云计算环境的物理硬件层，可用区401-402(或各区)可以指的是布置的一组物理计算资源。区可以在地理上与计算资源的整个云中的其它区分离。例如，区401可以是位于加利福尼亚州的第一云数据中心，以及区402可以是位于佛罗里达州的第二云数据中心。管理服务器410可以被定位在各可用区中的一个可用区或分开的位置。每个区可包括通过网关与在区之外的设备(例如管理服务器410)通过接口连接的内部网络。云的终端用户(例如，客户端411-414)可能或可能未感知到各区之间的区别。例如，终端用户可请求创建具有指定量的存储器、处理能力和网络容量的虚拟机。管理服务器410可对用户的请求做出响应并可分配资源以在用户不知道使用来自区401还是来自区402的资源创建虚拟机的情况下创建虚拟机。在其它示例中，云系统可以允许终端用户请求将虚拟机(或其它云资源)分配在指定区中或区内的指定资源403-405上。

[0114] 在这个例子中，每个区401-402可包括各种物理硬件组件(或计算资源)403-405(例如物理托管资源(或处理资源)、物理网络资源、物理存储资源、交换机和可用于向客户提供云计算服务的额外的硬件资源)的布置。在云区401-402中的物理托管资源可以包括一个或多个计算机服务器403(诸如上述的经配置可以形成和托管虚拟机实例的虚拟化服务器301)。在云区401或402中的物理网络资源可以包括一个或多个网络元件405(例如，网络服务供应商)，其包括经配置向云客户提供网络服务的硬件和/或软件(诸如防火墙、网络地址转换器、负载平衡器、虚拟专用网络(VPN)网关、动态主机配置协议(DHCP)路由器等等)。在云区401-402中的存储资源可包括存储磁盘(例如固态硬盘(SSD)、磁硬盘等)和其它存储设备。

[0115] 在图4中示出的示例云计算环境还可以包括虚拟化层(例如，如图1-3中所示)，该虚拟化层具有经配置形成和管理虚拟机和使用云中的物理资源向客户提供其它服务的另外硬件和/或软件资源。虚拟化层可以包括如上面在图3中所述的超级管理器以及提供网络虚拟化、存储虚拟化等的其它组件。该虚拟化层可以作为与物理资源层分开的层，或可以与物理资源层共享相同的硬件和/或软件资源的部分或全部。例如，虚拟化层可以包括被安装在带有物理计算资源的虚拟化服务器403中的每个中的超级管理器。可以另选使用已知的云系统，例如WINDOWS AZURE(华盛顿雷德蒙德的微软公司)，AMAZON EC2(华盛顿西雅图的Amazon.com公司)，IBM BLUE CLOUD(纽约阿蒙克的IBM公司)或其它云系统。

[0116] 企业移动性管理架构

[0117] 图5表示用于在BYOD环境中使用的企业移动技术架构500。该架构允许移动设备502的用户从移动设备502访问企业或个人资源两方面并使用移动设备502用于个人用途。用户可使用用户所购买的移动设备502或者企业提供给用户的移动设备502来访问此类企业资源504或企业服务508。用户可使用移动设备502仅用于商业用途或用于商业和个人用途。移动设备可以运行iOS操作系统和安卓操作系统或类似操作系统。企业可以选择实施以管理移动设备504的策略。该策略可以通过防火墙或网关以移动设备可以被识别、保障或安全被验证并提供选择性访问或全部访问企业资源的方式来植入。该策略可以是移动设备管理策略、移动应用管理策略、移动数据管理策略或移动设备、应用和数据管理策略的某些组合。通过移动设备管理策略的应用来管理的移动设备504可以被称为受管设备。

[0118] 在一些实施方案中，移动设备的操作系统可分成受管分区510和非受管分区512。受管分区510可具有施用于其的策略，以保护受管分区中运行的应用和存储的数据。在受管

分区上运行的应用可以是安全应用。在其它实施方案中，所有的应用可根据从与应用分开接收的一组一个或多个策略文件执行，且当该应用在设备上执行时，其定义一个或多个安全参数、特征、资源的限制、和/或其它由移动设备管理系统执行的访问控制。通过根据它们各自的策略文件进行操作，每个应用可被允许或限制与一个或多个其它应用和/或资源的通信，从而创建虚拟分区。因此，如本文所用，分区可指存储器的物理分区部分(物理分区)，存储器的逻辑分区部分(逻辑分区)，和/或创建的虚拟分区，作为如本文描述的跨多个应用一个或多个策略和/或策略文件执行的结果(虚拟分区)。换句话说，通过在受管应用上强制执行策略，这些应用可只限于能够与其它受管应用和值得信赖的企业资源通信，从而创建非受管应用和设备不能渗入的虚拟分区。

[0119] 安全应用可以是电子邮件应用、web浏览应用、软件即服务(SaaS)访问应用、Windows Application访问应用，等等。安全应用可以是安全本地应用514，由安全应用启动器518执行的安全远程应用522，由安全应用启动器518执行的虚拟化应用526，等等。安全本地应用514可由安全应用封装器520封装。当安全本地应用在设备上执行时，安全应用封装器520可包括在移动设备502上执行的综合策略。安全应用封装器520可包括元数据，其指引在移动设备502上运行的安全本地应用514到在企业托管的资源，其中安全本地应用514可需要该资源以完成在安全本地应用514执行时所请求的任务。由安全应用启动器518执行的安全远程应用522可以在安全应用启动器应用518内执行。由安全应用启动器518执行的虚拟化应用526可利用移动设备502、企业资源504等等的资源。由安全应用启动器518执行的虚拟化应用526在移动设备502上使用的资源，可包括用户交互资源、处理资源，等等。用户交互资源可用于收集和传输键盘输入、鼠标输入、摄像机输入、触觉输入、音频输入、可视化输入、手势输入，等等。处理资源可用来呈现用户接口、从企业资源504接收的过程数据，等等。由安全应用启动器518执行的虚拟化应用526在企业资源504上使用的资源可包括用户接口生成资源、处理资源，等等。用户接口生成资源可用于组装用户接口、修改用户接口、刷新用户接口，等等。处理资源可用于创建信息、读取信息，更新信息、删除信息，等等。例如，虚拟化应用可记录与GUI相关联的用户交互，并将它们传送到服务器应用，其中服务器应用将使用用户交互数据作为到在服务器上运行的应用的输入。在这种布置中，企业可选择维护服务器端的应用以及与应用相关联的数据、文件等。而企业可按照本文原则，通过保护其用于在移动设备上部署，选择“调动”一些应用，这种布置也可选择用于某些应用。例如，虽然某些应用可以安全用在移动设备上，但是其它应用可能未准备好或适合用于部署在移动设备上，因此，企业可以选择通过虚拟化技术向移动用户提供对未准备好应用的访问。作为另一实例，企业可具有带有大量和复杂的数据集的大型复杂的应用(例如，材料资源计划应用)，定制用于移动设备的应用将是非常困难的或是不期望的，所以企业可选择提供通过虚拟化技术对应用的访问。作为另一个示例，企业可具有维护高度安全地数据(例如，人类资源数据、客户数据、工程数据)的应用，其可被企业认为甚至对于安全的移动环境也过于敏感，因此企业可选择使用虚拟化技术以允许对该类应用和数据的移动访问。企业可选择提供在移动设备上完全安全和全功能的应用，以及虚拟化应用以允许对被认为更适合在服务器端运行的应用的访问。在实施方案中，虚拟化应用可在安全存储位置之一的移动电话上存储一些数据、文件等。例如，企业可选择允许在电话上存储某些信息，而不允许存储其它信息。

[0120] 如本文所描述，与虚拟化应用有关，移动设备可具有虚拟化应用，其被设计为呈现GUI并然后记录/通过与GUI的用户交互。该应用可将用户交互传送到由服务器侧应用所使用的服务器侧来作为用户与该应用的交互。作为响应，在服务器端的应用可发送新GUI返回到移动设备。例如，新GUI可以为静态页面、动态页面、动画等等，从而提供对远程定位资源的访问。

[0121] 安全应用可以访问存储在移动设备的管理分区510中的安全数据容器528中的数据。在安全数据容器中保护的数据可由以下应用访问，安全封装的应用514、由安全应用启动器522执行的应用、由安全应用启动器522执行的虚拟化应用526，等等。存储在安全数据容器528中的数据可包括文件、数据库，等等。存储在安全数据容器528中的数据可以包括被限制到特定安全应用530、在安全应用532之间共享等的数据。被限制到安全应用的数据可以包括一般安全数据534和高度安全数据538。一般安全数据可使用强加密形式，诸如AES 128位加密等等，而高度安全数据538可使用非常强的加密形式，诸如AES 254位加密。在接收来自设备管理器524的命令时，可从设备删除存储在安全数据容器528中的数据。安全应用可以具有双模式选项540。双模式选项540可为用户呈现以非安全模式操作安全应用的选项。在非安全模式中，安全应用可访问存储在移动设备502的非受管分区512的非安全数据容器542中的数据。存储在非安全数据容器中的数据可为个人数据544。存储在非安全数据容器542中的数据，也可由在移动设备502的非受管分区512上运行的非安全应用548访问。当存储在安全数据容器528中的数据从移动设备502中删除时，存储在非安全数据容器542中的数据可保持在移动设备502上。企业可能想从移动装置删除该企业拥有、许可或控制的选定或全部数据、文件和/或应用(企业数据)，而留下或以其它方式保存用户所拥有、许可或控制的个人数据、文件和/或应用(个人数据)。该操作可称为选择性擦除。利用根据本文所述的各方面安排的企业和个人数据，企业可以执行选择性擦除。

[0122] 移动设备可以将在企业的企业资源504和企业服务508连接到公共互联网548等。通过虚拟私有网络连接，移动设备可连接到企业资源504和企业服务508。虚拟私有网络连接，其也被称为微VPN(MicroVPN)或专用VPN，可特定于特定应用550、特定设备、移动设备上的特定安全区域等等552。例如，电话的安全区中的封装应用中的每个可以通过指定应用VPN访问企业资源，使得对VPN的访问将基于与该应用相关联的属性(可能的话，结合用户或装置属性信息)来授权。虚拟私有网络连接可携带Microsoft Exchange流量、Microsoft Active Directory流量、HTTP流量、HTTPS流量、应用管理流量，等等。虚拟私有网络连接可支持并实现单点登录认证过程554。单点登录过程可允许用户提供单个认证凭证集，然后其由认证服务558验证。然后，认证服务558可授权用户访问多个企业资源504，而无需用户提供认证凭证到每个单个的企业资源504。

[0123] 虚拟私有网络连接可由接入网关560建立和管理。接入网关560可以包括管理、加速并提高企业资源504向移动装置502的输送的性能增强功能。接入网关还可将流量从移动设备502重新路由到公共互联网548，使得移动设备502能够访问在公共互联网548上运行的公共可用的和未保护的应用。移动设备可经由传输网络562连接到接入网关。传输网络562可以是有线网络、无线网络、云网络、局域网、城域网、广域网、公共网络、私有网络等。

[0124] 企业资源504可包括电子邮件服务器、文件共享服务器、SaaS应用、Web应用服务器、Windows应用服务器等。电子邮件服务器可包括Exchange服务器、Lotus Notes服务器

等。文件共享服务器可包括ShareFile服务器等。SaaS应用可包括Salesforce等。Windows应用服务器可以包括经构建提供旨在于本地Windows操作系统上运行的应用的任何应用服务器等。企业资源504可以是基于内建式(premise-based)的资源、基于云的资源等。企业资源504可以由移动设备502直接访问或通过接入网关560来访问。企业资源504可以由移动设备502经由传输网络562来访问。传输网络562可以是有线网络、无线网络、云网络、局域网、城域网、广域网、公共网络、私有网络等。

[0125] 企业服务508可以包括认证服务558、威胁检测服务564、设备管理器服务524、文件共享服务568、策略管理器服务570、社交集成服务572、应用控制器服务574等。认证服务558可以包括用户认证服务、设备认证服务、应用认证服务、数据认证服务等。认证服务558可以使用证书。证书可以由企业资源504等存储在移动设备502上。存储在移动设备502上的证书可以被存储在移动设备上的加密位置,证书可以被暂时存储在移动设备502上用于在认证时使用等等。威胁检测服务564可包括入侵检测服务、未经授权的访问尝试检测服务等。未经授权的访问尝试检测服务可以包括未经授权尝试访问设备、应用、数据等。设备管理服务524可以包括配置、供应、安全、支持、监测、报告和停止使用服务。文件共享服务568可以包括文件管理服务、文件存储服务、文件协调服务等。策略管理器服务570可包括设备策略管理服务、应用策略管理器服务、数据策略管理器服务等。社交集成服务572可包括联系人集成服务、协作服务、社交网络集成,诸如Facebook、Twitter和LinkedIn等。应用控制器服务574可包括管理服务、供应服务、部署服务、分配服务、撤销服务、封装服务等。

[0126] 企业移动性技术架构500可包括应用商店578。应用商店578可包括未封装的应用580、预封装的应用582等。应用可以从应用控制器574被移置到应用商店578中。应用商店578可以由移动设备502通过接入网关560、通过公共互联网548等来访问。应用商店可以设置有直观并易于使用的用户界面。应用商店578可以提供对软件开发工具包584的访问。通过如本说明书中先前的描述的对应用进行封装,软件开发工具包584可向用户提供使用户所选的应用安全的能力。使用软件开发工具包584进行封装的应用可以随后通过使用应用控制器574将其移置到应用商店578中来提供给移动设备502。

[0127] 企业移动性技术架构500可以包括管理和分析能力588。管理和分析能力588可以提供有关如何使用资源、多久使用资源等的信息。资源可包括设备、应用、数据等。如何使用资源可包括哪些设备下载哪些应用、哪些应用访问哪些数据等。资源被多久使用一次可包括应用多久被下载一次、特定的数据集被应用访问了多少次等。

[0128] 图6是另一说明性企业移动性管理系统600。为了简化起见,上面参考图5所述的移动管理系统500的某些组件已被省略。图6所示的系统600的架构在许多功能方面类似于上面参考图5所述的系统500的架构,并且可以包括未在上面提到的另外的功能。

[0129] 在此情况下,左手侧表示具有客户端代理604的受管移动设备602,其与网关服务器606(该网关服务器包括接入网关和应用控制器功能)交互以访问各种企业资源608和服务609(诸如在上面右手侧所示的Exchange、Sharepoint、PKI资源、Kerberos资源、证书发行(Certificate Issuance)服务。虽然未具体示出,移动设备602还可以与企业应用商店(StoreFront)交互用于选择和下载应用。

[0130] 客户端代理604充当用于在企业数据中心中托管的Windows应用/桌面的UI(用户界面)中间件,使用HDX/ICA显示远程协议来访问Windows应用/桌面。客户端代理604还支持

移动设备602上的本地应用的安装和管理，诸如本地iOS或Android应用。例如，在以上图中所示的受管应用610(邮件、浏览器、封装的应用)全都是在设备上本地执行的本地应用。这种架构的客户端代理604和应用管理框架起到提供策略驱动管理能力以及诸如连接和SSO(单点登录)到企业资源/服务608的功能的作用。客户端代理604以到其它网关服务器组件的SSO的认证处理主要用户对企业的认证，通常到接入网关(AG))的认证。客户端代理604从网关服务器606获得策略以控制移动装置602上的受管应用610的行为。

[0131] 本地应用610与客户端代理604之间的安全IPC链接612表示管理通道，该管理通道允许客户端代理提供通过应用管理框架614“包装”每个应用来执行的策略。IPC通道612还允许客户端代理604提供能够连接和SSO到企业资源608的凭证和认证信息。最后，IPC通道612允许应用管理框架614调用由客户端代理604所实施的用户界面功能，诸如在线认证和离线认证。

[0132] 客户端代理604与网关服务器606之间的通信基本上是来自包装每个本地受管应用610的应用管理框架614的管理通道的延伸。应用管理框架614从客户端代理604请求策略信息，客户端代理604相应从网关服务器606请求该策略信息。应用管理框架614请求认证，并且客户端代理604登录进入网关服务器606的网关服务部分(也称之为NetScaler接入网关)。客户端代理604还可以调用在网关服务器606上的支持服务，其可以产生获得用于本地数据仓库616的加密密钥的输入材料，或提供其可以允许对KPI受保护资源直接认证的客户端证书，如下面将更全面解释的。

[0133] 更详细地，应用管理框架614“封装”每个受管应用610。这可经由明确的构建步骤或经由构建后处理步骤合并。应用管理框架614可以在应用610的首次启动时与客户端代理604“配对”以初始化安全IPC通道并获得用于该应用的策略。应用管理框架614可以执行本地应用的策略的相应部分(诸如客户端代理登录的依赖关系和限制如何可以使用本地OS服务或本地OS服务如何可以与应用610交互的遏制策略中的某些遏制策略)。

[0134] 应用管理框架614可以使用客户端代理604在安全IPC通道612上所提供的服务以促进认证和内部网络访问。私有和共享数据仓库616(容器)的密钥管理也可以通过受管应用610与客户端代理604之间的适当交互来管理。仓库616可以只是在在线认证后可用，或如果策略允许，则可以在离线认证后可用。仓库616的第一次使用可以要求在线认证，并且离线访问可以在再次要求在线认证前被至多限于策略更新阶段。

[0135] 对内部资源的网络访问可以通过接入网关606从独立的受管应用610直接发生。应用管理框架614负责精心安排代表每个应用610的网络访问。通过提供遵循在线认证获得的合适时间限制次级凭证，客户端代理604可以促进这些网络连接。可以使用多种网络连接模式，诸如逆向网络代理连接以及端到端VPN式隧道618。

[0136] 邮件和浏览器受管应用610具有特定状态并且可以使用一般可能不适合随机封装应用的设施。例如，邮件应用可以使用特殊后台网络访问机制，该访问机制允许邮件应用在延长的时间段内访问Exchange而无需完全AG登录。浏览器应用可以使用多种专用数据仓库以分隔不同种类的数据。

[0137] 这种架构支持各种其它安全功能的并入。例如，在某些情况下，网关服务器606(包括其网关服务)将不需要验证AD密码。这可以留给企业来判断AD密码是否用作某些情况下的某些用户的认证因素。如果用户在线或离线(即，连接到网络或未连接到网络)，则可以使

用不同的认证方法。

[0138] 加强认证是这样一种特征，其中，网关服务器606可以识别被允许访问需要强认证的高度机密数据的受管本地应用610，并且确保对这些应用的授权仅在执行适当的认证后被允许，即使这意味着在先前的较弱级别登录后用户需要再次认证。

[0139] 这种解决方案的另一安全特征是移动设备602上的数据仓库616(容器)的加密。仓库616可以被加密，使得所有设备上的数据(包括文件、数据库和配置)被保护。对于在线仓库，密钥可存储在服务器(网关服务器606)上，且对于离线仓库，密钥的本地副本可由用户密码保护。当数据被本地存储在设备602上的安全容器616中时，优选最少使用AES 256加密算法。

[0140] 还可实现其它安全容器的特征。例如，日志特征可以被包括，其中，发生在应用610内的所有安全事件被记入日志并报告给后端。可以支持数据擦除，诸如如果应用610检测到篡改，则相关的加密密钥可以用随机数据改写、没有留下对用户数据被破坏的文件系统的提示。屏幕截图保护是另一功能，其中，应用可以防止任何数据被存储在屏幕截图中。例如，密钥窗口的隐藏属性可以被设置为“是”。这可能会导致屏幕上当前显示的无论什么内容将被隐藏，产生任何内容将通常驻留其中的空白屏幕截图。

[0141] 可以防止本地数据转移，诸如防止任何数据被本地转移到应用容器外面(例如通过复制本地数据或发送本地数据到外部应用)。可以运行键盘缓存功能以禁用敏感文本字段的自动更正功能。SSL证书验证可以是可操作的，使得应用具体验证服务器的SSL证书，而不是将其存储在密钥链中。可以使用加密密钥生成功能，使得用于加密装置上的数据的密钥使用用户提供的密码来生成(如果需要离线访问的话)。如果不需要离线访问，则可以与随机生成并存储在服务器侧上的另一密钥“异或”。密钥衍生功能可操作，使得从用户密码生成的密钥使用KDF(密钥衍生功能，尤其是PBKDF2)而不是创建它的密码散列(cryptographic hash)。密码散列使得密钥易受蛮力或字典攻击。

[0142] 此外，一个或多个初始化向量可用于加密方法。初始化向量会导致相同加密数据的多个副本产生不同的密文输出，从而阻止重放和密码分析攻击两者。如果用于加密数据的特定初始化向量是未知的，则这也将甚至防止攻击者用偷来的加密密钥解密任何数据。此外，可以使用认证接解密，其中，应用数据只在用户已在应用内被认证后才被解密。另一特征可能涉及到内存中的敏感数据，只有当需要敏感数据时，该敏感数据会被保存在内存中(而不是在磁盘中)。例如，登录凭据可以在登录后从内存擦除，并且加密密钥和在objective-C的示例变量中的其它数据不被存储，因为它们可以很容易被参考。相反，可以向内存手动分配这些加密密钥和其它数据。

[0143] 可以实施休止超时，其中在策略定义的休止期后，用户对话被终止。

[0144] 可以以其它方式阻止应用管理框架614的数据泄露。例如，当应用610被放在后台中时，内存可以在预定(可配置)时间段后被清除。当被放在后台时，对应用的最后显示屏幕可能会被拍快照以加快转到前台的过程。屏幕截图可能包含机密数据，并且因此应被清除。

[0145] 另一安全特征涉及使用OTP(一次性密码)620，无需使用访问一个或多个应用的AD(活动目录)622密码。在某些情况下，某些用户不知道(或不允许知道)他们的AD密码，那么这些用户可以使用OTP620来认证，诸如通过使用像SecurID的硬件OTP系统(OTP也可以由不同的供应商来提供，例如Entrust或Gemalto)。在某些情况下，在用户利用用户ID认证之后，

用OTP 620发送文本到用户。在某些情况下，这可以仅在在线使用时，利用单一字段的提示来实施。

[0146] 对于针对其经由企业策略允许离线使用的那些应用610，离线密码可以被实施用于离线认证。例如，企业可能想要StoreFront以这种方式被访问。在此情况下，客户端代理604可以要求用户设置自定义的离线密码，并且不使用AD密码。网关服务器606可以提供策略以控制和执行关于最小长度、字符类组成和密码年限的密码标准(诸如通过标准的Windows服务器密码复杂性要求所描述的，尽管这些要求可以被更改)。

[0147] 另一功能涉及到作为次级凭证用于特定应用610的客户端侧证书的启用(用于经由应用管理框架微VPN功能访问KPI受保护web资源的目的)。例如，应用，诸如@WorkMail，可利用这种证书。在此情况下，可以支持使用ActiveSync协议的基于证书的认证，其中，来自客户端代理604的证书可以被网关服务器606检索并用在密钥链中。每个受管应用可以具有通过在网关服务器606中定义的标签来识别的一个关联的客户端证书。

[0148] 网关服务器606可以与企业专用web服务交互，以支持客户端证书的颁布，以允许相关的受管应用认证到内部PKI受保护资源。

[0149] 客户端代理604和应用管理框架614可以被加强以支持获得和使用用于认证内部PKI受保护网络资源的客户端证书。可以支持一个以上的证书，诸如匹配各种安全级别和/或分隔要求的证书。该证书可以被邮件和浏览器受管应用使用，并最终被任意包装的应用使用(假设那些应用使用web服务方式的通信模式，其中这对于调解http请求的应用管理框架是合理的)。

[0150] 在iOS上的应用管理客户端证书支持可能依赖每次使用期间，将PKCS12BLOB(二进制大对象)输入到每个受管应用的iOS密钥链中。应用管理框架客户端证书支持可以使用具有专用存储器内密钥存储的HTTPS实施。客户端证书将不再存在于iOS密钥链中，并且除了潜在的存在于受强保护的“只在线”数据值中以外，不会被存续。

[0151] 通过要求移动装置602被企业认证，相互SSL也可以被实施以提供另外的安全，并且反之亦然。也可以实施用于对网关服务器606认证的虚拟智能卡。

[0152] 受限和完全Kerberos支持两者可以是另外的特征。完整支持特征涉及使用AD密码或受信任客户端证书对AD 622执行完整Kerberos登录的能力，并且获得Kerberos服务票据(service ticket)来响应HTTP协商身份验证挑战。受限的支持功能涉及AFEE中的受约束委托，其中，AFEE支持调用Kerberos协议传输，因此，它可获得和使用Kerberos服务票据(服从受约束的委托)以对HTTP协商询问做出响应。这种机制以逆向web代理(也叫做CVPN)模式工作，并且当http(但不是https)连接以VPN代理时，以微VPN模式工作。

[0153] 另一特征涉及应用容器锁定和擦除，这可在检测到越狱和获取了管理员权限(root)时自动出现，并且作为来自管理控制台的推送命令出现，并且可以包括远程擦除功能(即使当应用610不运行时)。

[0154] 可以支持StoreFront和应用控制器的多站点架构或配置，该多站点架构或配置允许用户在故障的情况下从几个不同位置中的一个位置得到服务。

[0155] 在一些情况下，受管应用610可以被允许经由API(示例OpenSSL)访问证书和私有密钥。企业的受信任受管应用610可以被允许利用应用的客户端证书和私有密钥来执行指定的公共密钥操作。各种使用情况可以被识别并因此受信任，诸如当应用像浏览器一样表

现并且不需要证书访问时、当应用读取“我是谁”的证书时、当应用使用证书构建安全对话令牌时，以及当应用使用私有密钥用于重要数据(例如，事务日志)的数字签名或用于暂时数据加密时。

[0156] 示例性实施方案

[0157] 图7示出移动设备的示例界面，并且图8-14示出用于确定应用的操作模式的方法的示例实施方案。在图8-14中描绘的方法可以任何合适的方式组合到各种实施方案中。在图7中描述的示例界面可在移动设备(诸如设备107、109、240、502和/或602)上显示，并且在图8-14中描绘的方法可通过该移动设备实现。

[0158] 在图8中，示出用于确定应用的应用模式的示例方法步骤的流程图。图8的方法可以在步骤802开始，其中，在该步骤呈现多个应用。例如，多个应用可以在移动设备上向用户呈现。图7示出实施方案，其中，在移动设备(如，平板电脑、智能手机等)上显示的用户界面700向用户呈现应用A700、B701、C702和E703。这仅是示例，并且多个应用可以以任何合适的方式来呈现。在实施方案中，多个应用可包括电子邮件应用、网页浏览应用、软件即服务(SaaS)访问应用等。

[0159] 图8的方法可从步骤802进行到步骤804，其中接收对多个应用中的一个应用的选择。参考图7中所示的实施方案，移动设备的用户可通过例如按压移动设备的显示器选择所呈现的应用中的一个，以选择应用。这仅仅是示例，并且应用可以任何合适的方式来选择。

[0160] 图8的方法可以从步骤804进行到步骤806，其中，基于执行被选定应用的设备的一个或多个操作参数来确定被选定应用的背景。例如，背景可以基于要被应用访问的账户、移动设备的位置或执行应用的移动设备的网络连接状态，或基于任何其它操作参数。如下面进一步描述的，图9-13的方法示出其中描述示例背景的各种实施方案。

[0161] 图8的方法可以从步骤804进行到步骤806，其中，基于背景来确定用于选定应用的操作模式。在实施方案中，操作模式可包括受管模式和非受管模式，如，表示设备的工作模式和非工作模式，各自用于当用户在执行工作相关活动和私人活动。工作模式可提供对企业资源的访问并包括一个或多个内容过滤器和/或限制，而非工作模式可应用允许仅访问非企业相关资源的策略(或无策略)和/或内容过滤器/限制(或没有)。

[0162] 此外，可以有多种不同的受管模式，例如，基于各个用户的不同安全级别或由用户提供的凭证集，由凭证集识别的不同用户角色(例如，经理对职员和员工)、操作装置的地理位置、网络位置、操作环境(例如，医疗保健相关的受管模式对金融业受管模式)或基于任何其它的背景确定。一些模式可基于多个背景，如位置和角色。在这种结合中，第一受管模式可提供可应用策略给医疗提供方，而第二受管模式可将可应用的策略应用于患者。当设备在两个用户之间传递时，用户(或基于用户动作的软件)可在设备被传递到具有不同角色的用户时启动模式的改变。可需要新用户输入适当的凭证来改变模式，如，当变化到更安全的模式时。医疗提供方模式可提供对一系列广泛的患者记录、资源、调度详情、财务记录和其它信息的访问，而患者模式例如基于HIPPA和其它隐私考虑可限制在仅有该患者的信息。还可使用背景决策的其它组合。

[0163] 在实施方案中，所确定的背景可以与存储的策略比较，以便确定操作模式。诸如移动设备502的移动设备可存储一个或多个策略，其用于确定应用的操作模式。在实施方案中，各策略可以如上参考图5所述在策略管理器570被远程存储，或可以本地存储在装置上。

在示例中，背景可包括被配置成访问安全账户的选定应用，诸如被配置成访问安全电子邮件账户的电子邮件应用。该背景可与存储的策略进行比较。例如，所存储的策略可以定义经配置访问安全的电子邮件账户的电子邮件应用作为受管应用运行。所存储的策略可进一步指示当电子邮件应用被配置为访问设备用户的个人账户时，其可以非受管模式进行操作。将参考图9-13描述附加背景和策略。

[0164] 图8的方法可从步骤806进行到步骤808，其中所选择的应用以所确定的操作模式运行。例如，操作模式可确定为非受管的，或为多个受管模式中的一个，并且所选择的应用可以所确定的模式运行。

[0165] 在实施方案中，受管操作模式可包括作为移动设备502的受管分区510的部分运行应用，如以上参考图5所描述。如此，受管应用可作为安全本机应用514、通过安全应用启动器518执行的安全远程应用522、通过安全应用启动器518执行的虚拟化应用526等等运行。

[0166] 在实施方案中，以受管模式运行的应用可访问存储在移动设备的受管分区510(物理、逻辑或虚拟)中的安全数据容器528中的数据。安全数据容器528中所存储的数据可包括被限制到具体安全/受管应用530、在其它安全/受管应用之间共享的数据等。被限制到安全应用的数据可以包括一般安全数据534和高度安全数据538。不同级别和类型的安全性特征可用于区分安全数据的级别。在实施方案中，以受管模式运行的应用可保存、修改或删除安全数据容器528中的数据。可类似于安全数据容器528中所存储的其它数据对所保存的或修改的数据加密。

[0167] 在实施方案中，以受管模式运行的应用可以通过如关于参考图5所述的虚拟专用网络连接来连接到企业资源504和企业服务508。虚拟专用网络连接可以是微VPN，该微VPN指定用于特定应用，诸如选定应用、特定设备、移动设备上的特定安全区等。例如，电话的安全区域中的封装的应用可通过应用专用VPN访问企业资源，使得将基于与应用关联的属性、还可能结合用户或设备属性信息和策略信息，授予对VPN的访问。

[0168] 在实施方案中，以受管模式运行的应用可以对从应用传输的数据加密。例如，以受管模式运行的应用可通过网络与计算设备通信，并且从应用传输到设备的数据可被加密。另外，从计算设备传输到应用的数据也可被加密，并且以受管模式运行的应用可被配置成对所接收的数据解密。

[0169] 在实施方案中，以受管模式运行的应用可访问安全门户(portal)。例如，应用可通过网络(例如，微VPN)连接到计算设备，并且可访问不可以被非安全应用(诸如以非受管模式运行的应用)访问的安全门户。

[0170] 在实施方案中，非受管操作模式可以包括运行作为如上文参考图5所述的移动设备502的非受管分区512(物理的、逻辑的或虚拟的)的一部分的应用。在非受管模式中，应用可访问存储在移动设备502上的非受管分区512上的非安全数据容器542中的数据。存储在非安全数据容器中的数据可为个人数据544。

[0171] 在实施方案中，其中多于一个受管模式是可能的，以较低安全受管模式运行的应用可类似于以较高安全受管模式运行的应用，但可不包括后者的所有方面。例如，以较低安全受管模式运行的应用可以具有加密的来自应用的通过网络传送的信息，但是该应用可能不能访问如参考图5所述的安全数据容器528。在另一个示例中，以较低安全受管模式运行的应用可有权访问安全数据容器528，但可能不能够通过虚拟私有网络连接来连接到企业

资源504和企业服务508。因此，根据所确定的背景，以较低安全受管模式运行的应用可包括以更安全受管模式运行的应用的方面以及以非受管模式运行的应用的方面。

[0172] 在图9-13中，示出了用于确定应用的背景和操作模式的示例方法步骤的流程图。在实施方案中，图8的步骤806和808可包括图9-13中的任何一个或多个的方法步骤。图9的方法可在步骤902处开始，在步骤902处，检测待被选定应用访问的账户。例如，选定应用可包括电子邮件应用，并且电子邮件应用经配置访问的电子邮件账户可被检测。在本示例中，电子邮件应用可以能够访问多个电子邮件账户，诸如企业电子邮件账户和个人电子邮件账户，并且电子邮件应用经配置在运行时访问的账户可被确定为将被访问的背景账户。

[0173] 图9的方法可从步骤902进行到步骤904，在步骤904处，将被访问的账户的账户类型可被确定。账户类型可构成选定应用的背景。例如，选定应用可包括电子邮件应用，并且电子邮件应用可经配置访问企业账户。在另一个示例中，电子邮件应用可经配置访问个人账户。

[0174] 图9的方法可从步骤904进行到步骤906，其中账户类型可与账户类型策略比较。例如，策略可定义访问企业账户的电子邮件应用应以受管模式运行，并且访问个人账户的电子邮件应用应以非受管模式运行。图9的方法可以从步骤906进行到步骤908，其中基于该比较来确定操作模式。

[0175] 图10的方法可在步骤1002处开始，在步骤1002处，移动设备的位置被确定。例如，移动设备(诸如移动设备502)可实现图10的方法，并且移动设备的位置可被确定。位置可通过GPS、信号三角定位、或任何其它合适的或以其它方式已知的方式来确定。位置可构成选定应用的背景。

[0176] 图10的方法可从步骤1002进行到步骤1004，其中所确定的位置可与位置策略比较。例如，策略可以定义，当在某位置(例如公司处所)时，选定应用以更安全的受管模式运行。在实施方案中，策略可定义当在某一位置中时，例如，当所确定的位置在美国内部但不在公司场所时，选定应用以较低安全受管模式运行。例如，较低安全受管模式可对往返选定应用的通信加密，但可不允许访问企业资源，诸如资源504。在另一个实施方案中，策略可定义，当在某一位置中时，例如，当所确定的位置在美国之外时，所选择的应用以非受管模式运行。图10的方法可以从步骤1004进行到步骤1006，其中基于该比较来确定操作模式。

[0177] 可选地或除了物理位置以外，网络位置还可或转而用于确定是否允许访问。例如，网络位置可指用户是否在数据中心(或预批准的WiFi访问点)内部或在数据中心外部。适当的访问模式可以基于该确定。

[0178] 图11的方法可在步骤1102处开始，在步骤1102处，监控预定的应用是否在设备上运行。例如，移动设备(诸如移动设备502)可实现图11的方法，并且移动设备可被监控以确定预定的应用是否在运行。预定的应用可包括能够在移动设备上运行的任何应用，诸如参考图6描述的客户端代理604。所监控的预定的应用可构成选定应用的背景。

[0179] 图11的方法可从步骤1102进行到步骤1104，其中所监测的应用与策略比较。例如，策略可定义，当预定的应用(诸如客户端代理604)运行时，选定应用以受管模式运行，并且当预定的应用未运行时，选定应用以非受管模式运行。图11的方法可以从步骤1104进行到步骤1106，其中基于该比较来确定操作模式。

[0180] 图12的方法可在步骤1202处开始，一个或多个网络连接被检测。例如，移动设备

(诸如移动设备502)可实现图12的方法,并且移动设备所接通的网络连接可被检测。在示例中,网络连接可包括到蜂窝网络的连接、到WIFI网络的连接、或到无线局域网(WLAN)的连接等。一个或多个网络连接可构成选定应用的背景。

[0181] 图12的方法可从步骤1202进行到步骤1204,其中所检测的网络连接与网络连接策略比较。例如,策略可定义,当移动设备连接到内部网络,诸如公司内部的WLAN时,选定应用以受管模式运行,以及当移动设备仅连接到无线网络,诸如蜂窝网络或WIFI网络时,选定应用以非受管模式运行。图12的方法可以从步骤1204进行到步骤1206,其中基于该比较来确定操作模式。

[0182] 图13的方法可在步骤1302处开始,在步骤1302处,移动设备的一个或多个设置被检测。例如,移动设备(诸如移动设备502)可实现图13的方法,并且移动设备的一个或多个设置可被检测。在示例中,可检测移动设备是否具有锁屏,诸如使用移动设备所需的PIN,或者可检测移动设备是否被越狱/获得管理员权限,例如,已经经过进入市场后(after-market)的修改。一个或多个设置可构成选定应用的背景。

[0183] 图13的方法可从步骤1302进行到步骤1304,其中所检测的设置与设置策略比较。例如,策略可定义,如果移动设备不具有锁定屏幕,或者如果移动设备被越狱/获得管理员权限,则选定应用可不以受管模式运行。图13的方法可以从步骤1304进行到步骤1306,其中基于该比较来确定操作模式。在实施方案中,当选定应用以所确定的模式运行时,通知用户特定策略(诸如在允许移动设备以受管模式运行选定应用之前移动设备具有锁屏的要求)的指示符可以在移动设备上显示。图9-13描述多个背景和任何其它合适的背景,并且可实施的相应策略。

[0184] 在实施方案中,在图9-13中描述的背景中的一个或多个可组合,并且这些背景可与用于选定应用的策略进行比较。例如,选定应用的背景可包括将作为企业电子邮件账户访问的账户类型和检测为蜂窝网络的网络连接。在该示例中,策略可定义,当试图经由蜂窝网络访问企业账户时,所选择的应用应以受管模式运行。由于选定应用可加密与企业电子邮件账户的通信,因此可以用这种方式定义策略,并且因此可减缓经由蜂窝网络发送安全流量的风险。

[0185] 在另一个示例中,选定应用的背景可包括在美国之外的所确定的位置和与公司内部WLAN的网络连接。策略可定义,当所确定的位置在美国之外以及网络连接是与公司内部的WLAN连接时,选定应用以受管模式运行。由于连接到公司内部的WLAN的网络连接减轻与美国之外的安全通信关联的风险,因此可以用这种方式定义策略。

[0186] 在实施方案中,如图9-13描述的一个或多个背景可包括优先级。例如,选定应用的背景可包括越狱或获得管理员权限的移动设备设置,并且策略可定义,当背景指示越狱/获得管理员权限的移动设备时,选定应用将仅以非受管模式运行,而与其它背景所指示的内容无关。因此,即使当移动设备连接到公司内部的WLAN或者如果选定应用试图访问企业账户时,越狱/获得管理员权限的移动设备将使选定应用以非受管模式运行。

[0187] 在实施方案中,策略可基于如图9-13描述的多个背景,指示选定应用将以较低安全受管模式运行。例如,选定应用的背景可包括将作为企业电子邮件账户访问的账户类型和检测为蜂窝网络的网络连接。在该示例中,策略可定义,当试图经由蜂窝网络访问企业账户时,选定应用应以较低安全受管模式运行。较低安全受管模式可对往返选定应用的通信

加密，但可不允许访问企业资源，诸如资源504。由于被加密的与企业电子邮件账户的通信可能是低风险通信，且允许访问企业资源可能是高风险通信，因此可以用这种方式定义策略。

[0188] 在图14中，示出用于切换应用的操作模式的示例方法步骤的流程图。例如，图14的方法步骤可遵循图8的方法步骤。图14的方法可在步骤1402处开始，其中当选定应用运行时，可监测一个或多个背景。在实施方案中，参考图9-13描述的背景中的一个或多个可被监测。例如，运行选定应用的移动设备可连接到蜂窝网络，并且在选定应用正在运行的同时，移动设备可接通与公司内部WLAN的新的网络连接。

[0189] 图14的方法可从步骤1402进行到步骤1404，在步骤1404处，基于监测来检测选定应用的操作模式变化。换言之，移动设备可检测信息变化，该信息变化构成用于选择特定操作模式的基础。例如，选定应用可以以非受管模式运行，并且一旦运行选定应用的移动应用连接到公司内部的WLAN，则策略可定义，选定应用的操作模式应切换到受管模式。图14的方法可从步骤1404进行到步骤1406，在步骤1406切换选定应用的操作模式。

[0190] 在实施方案中，诸如移动设备管理器的管理器可管理一台或多台移动设备。在该示例中，移动设备可被称为登记设备。在实施方案中，可基于安装在受管设备上的诸如图6的客户端代理604的软件管理移动设备。

[0191] 在实施方案中，客户端代理604还可包括连接管理软件开发包(SDK)、连接管理器520、连接/状态应用程序编程接口(API)、虚拟化服务组、运行时SDK、平台SDK和客户端核。

[0192] 例如，在客户端代理架构中的虚拟化服务可包括图形服务、桌面集成服务、多媒体服务、输入/输出服务、智能卡服务、打印服务等。例如，运行时SDK可以是独立计算架构(ICA)运行时SDK，包括ICA引擎。例如，平台SDK可以是ICA平台SDK或其它平台SDK，并且平台SDK可包括各种子组件，诸如虚拟通道SDK、配置和负载管理器、跟踪子组件、平台抽象SDK等。例如，客户端核可包括用于远程访问终端服务(如，具有核ICA协议的Winstation驱动)的核协议、配置为执行压缩和优先化的缩减器子组件、多流ICA、具有会话可靠性的TCP栈、代理和SSL以及UDP子组件。客户端核还可包括平台专用子组件的实现，诸如图形智能卡和线程支持、配置和负载管理器库、SSL SDK等。

[0193] 例如，移动设备可在企业系统中使用客户端代理604登记。例如，在登记的客户端代理602中，客户端代理604可与网关服务器606或其它访问网关交互以访问各种企业资源608和服务609。登记设备可涉及自带设备办公(BYOD)和相关的技术，以及可涉及选择进入MDM或类似系统。具有公司账号(或其它组织账号)的设备的登记可涉及推送凭证到设备和将设备注册到企业系统的设备管理服务器。登记后，使用移动设备管理(MDM)和/或推送到设备的移动设备体验技术(应用管理框架)策略，设备可由公司管理员(或其它组织管理员)“管辖”。登记的设备还可被称为受管设备。换言之，登记后，设备可变成如本文所描述的受管设备。在特定示例中，为了企业系统中登记设备，客户端代理604和/或应用登记令牌可被下载并安装在设备上。应用登记令牌可从设备将登记到的公司或其它组织的证书获得。下载客户端代理604和应用登记令牌后，可提示设备用户打开令牌并将公司账号(或其它组织账号)添加到设备。

[0194] 在实施方案中，诸如图5中的移动设备502的登记的移动设备可由诸如图5中的设备管理器524的服务管理。设备管理器524可提供包括配置、设置、安全、支持、监测、报告和

停止运行的服务。例如，设备管理器524可监测安装在登记的/受管移动设备的应用。在这个示例中，设备管理器524可储存/访问黑名单应用列表并还可确定登记的/受管移动设备上的黑名单应用的安装。黑名单应用可包括怀疑是恶意软件的应用或任何其它适合的应用。在另一个示例中，设备管理器524可监测登记的移动设备的操作状态。在这个示例中，设备管理器524可确定登记的移动设备已经被越狱/获得管理员权限。设备管理器524可基于这些判定在登记的设备上执行各种管理活动。

[0195] 在另一个示例中，设备管理器524可监测移动设备的网络连接。在这个示例中，设备管理器524可确定登记的移动设备被连接到蜂窝网络、无线局域网(WLAN)、局域网(LAN)、这些的结合或任何其它适合的网络。在另一个示例中，设备管理器524可监测移动设备的位置。在这个示例中，设备管理器524可确定移动设备的地理位置，诸如纬度和经度、国家、州、任何合适的区域或移动设备的任何其它适合位置。

[0196] 在另一个示例中，设备管理器524可监测特定应用是否在移动设备上运行。在这个示例中，设备管理器524可确定诸如图6的客户端代理604的特定应用是否在移动设备上运行。设备管理器524可基于这些决定在登记的设备上执行各种管理活动。

[0197] 在实施方案中，安装在登记的移动设备上的应用可在受管模式或非受管模式中运行，如上面所描述的。在实施方案中，受管操作模式可包括作为移动设备502的受管分区510的部分运行应用，如以上参考图5所描述。在实施方案中，以受管模式运行的应用可访问存储在移动设备的受管分区510中的安全数据容器528中的数据。安全数据容器528中所存储的数据可包括被限制到具体安全应用530、在其它安全应用之间共享的数据等。被限制到安全应用的数据可以包括一般安全数据534和高度安全数据538。一般安全数据可使用强加密形式，诸如AES 128位加密等等，而高度安全数据538可使用非常强的加密形式，诸如AES 254位加密。可以使用其它类型的加密，并且其它级别和类型的安全措施可以基于预期安全级别和/或类型以及不同的密钥恢复特征来应用。在实施方案中，以受管模式运行的应用可保存、修改或删除安全数据容器528中的数据。可类似于安全数据容器528中所存储的其它数据对所保存的或修改的数据加密。

[0198] 在实施方案中，受管模式可包括企业模式而非受管模式可包括私人模式。例如，当应用在受管模式或企业模式中运行时，应用可具有对储存在安全服务器的资源(如，企业数据)的访问权限。管理设备的设备管理器524可与企业关联。在这个示例中，在受管模式中运行的应用可能够与授权应用对企业数据的访问的一台或多台服务器(如，网关服务器606)通信。当应用在非受管模式或私人模式运行时，应用可不具有对企业数据的访问权限。

[0199] 在实施方案中，能够以受管模式或非受管模式运行的应用可利用用于存储与应用相关的数据的存储策略。在图15中，示出用于管理在多模式运行的应用的示例方法步骤的流程图。图15可在步骤1502处开始，其中，应用以受管模式或非受管模式中的一种模式在移动设备上运行。例如，如上面所描述的，能够在受管模式或非受管模式中运行的应用可在这些模式中的一种模式中运行。

[0200] 图15的过程可从步骤1502行进到步骤1504，其中，储存与应用相关的数据的请求被接收。例如，当应用在受管模式中运行时，请求可被接收以储存数据，诸如从安全服务器(如网关服务器606)中得到的安全数据。在这种示例中，安全数据可包括企业数据，如上面所描述的。在另一个示例中，当应用在非受管模式中运行时，请求可被接收以储存数据，诸

如私人数据。

[0201] 图15的过程可从步骤1504进行到步骤1506，其中，根据存储协议，数据可被储存在移动设备上。存储协议可限定请求的数据储存在移动设备上的方式。例如，当应用在受管模式中运行时，可根据第一协议存储数据，而当应用在非受管模式中运行时，可根据第二协议储存数据。

[0202] 在实施方案中，第一存储协议可限定所请求的数据可存储在第一数据容器中，诸如安全数据容器(如，安全数据容器528)。在这个示例中，当应用在非受管模式中运行时，储存在第一数据容器中的数据不能被应用访问。在实施方案中，第二存储协议可限定所请求的数据可存储在不同于第一数据容器的第二数据容器中。例如，第二数据容器可包括存储私人数据的通用数据容器。

[0203] 在实施方案中，第一存储协议可限定所请求的数据可在存储前加密。在这个示例中，可使用第一密钥加密数据，并且在一些实施方案中，第一密钥可与管理该设备的设备管理器(如，设备管理器524)关联。在实施方案中，第二存储协议可限定使用不同于第一密钥的第二密钥在存储前将所请求的数据加密。在另一个示例中，第一存储协议可限定所请求的数据可不加密存储。

[0204] 当存储协议更新或更改时，存储的数据可自动更新。例如，策略可被更新，即用于数据存储的加密方案从第一加密类型改变到第二加密类型。当它发生时，移动设备可基于第一加密类型自动解密并基于第二加密类型使用新的或修正的策略重新加密存储的数据。以这种方式，存储的数据可总是与当前存储策略保持一致。

[0205] 在实施方案中，第一存储协议可限定所请求的数据可与受管账号关联存储。在受管模式中运行的应用可与受管账号相关。例如，当在受管模式中运行时，云存储应用允许访问与受管账号有关的安全数据，该受管账号用于获取对安全数据的访问。所请求的数据可与该受管账号关联存储。在实施方案中，第一存储协议可限定所请求的数据存储可由设备管理器524管理。

[0206] 相应地，当应用在受管模式中运行时，可根据第一协议存储数据，如上面所描述的。当应用在非受管模式中运行时，可根据第二协议存储数据，如上面所描述的。

[0207] 在一些实施方案中，存储的类型和/或位置可取决于所使用的操作模式。例如，存储协议或策略可指定数据将储存在基于云存储中。存储协议或策略还可指定企业或非企业云存储应基于操作模式被使用。当在受管模式时，数据可被保存到企业云存储或其它云存储，其中提供了由企业或策略来选择的预定义的安全等级。可选地，当在非受管模式中时，数据可被保存或储存在较低安全云存储服务或位置，如，由用户来选择的。说明性实施方案可包括混合存储策略，其中，基于移动设备或应用的特定环境，当应用在非受管模式中运行时数据可被本地储存而当应用在受管模式中运行时数据可储存在云存储中，或反之亦然。

[0208] 图15的过程可从步骤1506行进到步骤1508，其中信号被接收以禁用应用的模式。例如，信号可被接收以禁用应用的受管模式。在实施方案中，设备管理器524可监测登记的移动设备、检测移动设备的状态和发送信号以禁用安装在移动设备上的应用的受管模式。例如，设备管理器524可检测到登记的移动设备被越狱/获得管理员权限，并且可基于该检测确定禁用应用的受管模式。在另一个实施方案中，设备管理器524可检测到黑名单应用已经被安装在登记的移动设备上，并且可基于该检测确定禁用应用的受管模式。

[0209] 在另一个实施方案中，设备管理器524可检测到与应用相关的受管账号已经过期或已经被删除，并且可基于该检测确定禁用应用的受管模式。例如，当在受管模式中运行时，云存储应用允许访问与受管账号有关的安全数据，该受管账号用于获取对安全数据的访问。设备管理器524可检测到受管账号已经过期或已经被删除并且可基于该检测发送信号以禁用云存储应用的受管模式。在实施方案中，当接收到禁用应用的受管模式的信号时，应用可被转换到不在受管模式中运行的应用。

[0210] 在实施方案中，基于所接收的禁用应用的受管模式的信号，可确定根据第一协议储存的数据将被选择性地删除。例如，根据第一协议储存的数据可与将被禁用的受管模式关联，并且根据第一协议储存的数据可作为禁用受管模式的一部分被选择性地删除。

[0211] 图15的过程可从步骤1508进行到步骤1510，其中，定位了根据协议储存在移动设备上的数据。例如，设备管理器524可监测登记的移动设备并定位根据第一协议储存的数据。根据第一协议储存的数据可包括与在第一模式中运行的特定应用相关的数据，诸如在受管模式中运行的应用。在实施方案中，所定位的数据可包括用于应用的企业数据。

[0212] 在实施方案中，根据第一协议储存的数据可基于账号定位。例如，账号可与受管账号关联。应用可在受管模式中运行并且所储存的数据可与受管账号关联。在这个实施方案中，根据第一协议储存的数据可与受管账号关联，并且根据第一协议储存的数据可基于受管账号被定位。

[0213] 在另一个实施方案中，根据第一协议储存的数据可基于存储容器定位。例如，诸如图5中的安全数据容器528的安全存储容器可与根据第一协议储存的数据关联。应用可在受管模式中运行并且根据第一协议储存的数据可储存在安全数据容器中。在这个实施方案中，根据第一协议储存的数据可储存在安全数据容器中，并且根据第一协议储存的数据可基于安全存储容器中的存储被定位。

[0214] 在另一个实施方案中，根据第一协议储存的数据可基于加密术定位。例如，根据第一协议储存的数据可使用特定加密术被加密，诸如使用第一密钥的加密术。应用可在受管模式中运行并且根据第一协议储存的数据可基于特定加密术被加密。在这个实施方案中，根据第一协议储存的数据可基于数据加密术定位。在示例中，第一密钥可与设备管理器524关联。

[0215] 图15的过程可从步骤1510进行到步骤1512，其中所定位的数据被选择性地删除。例如，设备管理器524可监测登记的移动设备、定位根据第一协议储存在登记的移动设备上的数据和选择性地删除所定位的数据。在实施方案中，选择性地删除所定位的数据不删除储存在移动设备上的任何其它数据。例如，在所定位的数据包括用于应用的企业数据时，用于应用的私人数据可不被删除。可选地，对根据第一协议储存的数据的访问可被锁定或阻止，直到设备重新登记或应用能够再次在受管模式中运行。

[0216] 在图16中，示出用于管理能够在多模式运行的应用的账号的示例方法步骤的流程图。图16的过程可在检测到所安装的应用能够在多模式中执行时使用，以配置由在受管模式中执行的应用对企业资源的使用。另外，资源可基于特定事件被预供应(如，新员工从公司开始以及资源作为新员工程序的部分被预供应)，从而加速受管应用的第一次执行。图16可开始于步骤1602，其中监测移动设备的新的应用。例如，设备管理器524可监测登记的移动设备，诸如移动设备502，如上面所描述的。设备管理器可监测在移动设备上安装的应用。

在实施方案中，设备管理器可定期监测移动设备的新应用的安装。

[0217] 图16的过程可从步骤1602进行到步骤1604，其中检测到能够在受管模式和非受管模式中运行的应用被安装在移动设备上。例如，设备管理器524可监测登记的移动设备并确定能够在受管模式和非受管模式运行的应用被安装在移动设备上。基于与应用相关的元数据或基于任何其它合适的检测方式，设备管理器可检测能够在受管模式和非受管模式运行的所安装的应用。

[0218] 图16的过程可从步骤1604行进到步骤1606，其中供应了资源以与所检测的应用通信。例如，当应用在受管模式中运行时，诸如网关服务器(如，网关服务器560)的资源可被供应以与所检测的应用通信。

[0219] 在实施方案中，资源可包括云存储资源。云存储资源可储存安全数据，诸如企业数据。在这个示例中，云存储资源可被供应以与在受管模式中运行的所检测的应用通信，使得在供应后在受管模式中运行的所检测的应用可访问储存在云存储资源中的安全数据。

[0220] 在实施方案中，供应资源可包括创建用于应用的账号。在这种实施方案中，图16的过程可从步骤1604进行到步骤1606，其中，创建了用于应用的账号，该账号与移动设备的标识信息相关。例如，登记的移动设备可具有与移动设备相关和/或与移动设备的用户相关的标识信息。在实施方案中，标识信息可包括企业凭证，诸如企业的活动目录的登录名和密码。在另一个实施方案中，标识信息可包括与企业相关的令牌。例如，登记的移动设备可从识别登记的移动设备和/或登记的移动设备的用户的企业服务器接收令牌，诸如安全断言标记语言(SAML)令牌或任何其它适合的令牌。该标识信息可包括任何其它合适的标识信息。设备管理器(如，设备管理器524)可访问移动设备上的标识，诸如令牌，或移动设备可提供标识信息。

[0221] 在实施方案中，可创建用于能够在受管模式和非受管模式中执行的应用的账号，该账号与标识信息相关。在这个示例中，标识信息可包括用户凭证，例如企业凭证、令牌或任何其它适合的标识信息。在实施方案中，基于与用于应用的标识信息相关的账号还不存在的确定，可创建账号。例如，服务器可基于标识信息搜索用于应用的账号并且可基于服务器未找到账号而创建账号。

[0222] 在实施方案中，所创建的账号可与配置为与在受管模式中运行的应用通信的资源关联。例如，所创建的账号可与配置为与在受管模式中运行的应用通信的云存储资源关联。

[0223] 图16的过程可以从步骤1606进行到步骤1608，其中基于标识信息可识别账号。例如，基于诸如用户的凭证的标识信息，诸如与企业相关的用户的用户账号可被识别。所识别的账号可包括企业活动目录账号、隶属于企业资源权限的账号或任何其它适合的企业账号。在实施方案中，通过注册到所识别的账号，可在登记的移动设备上访问企业资源，如上面所描述的。

[0224] 图16的过程可从步骤1608行进到步骤1610，其中所创建的账号可与所识别的账号链接。例如，为能够在受管模式和非受管模式中运行的应用创建的账号可与诸如活动目录账号的企业账号链接。使用该链接，基于所识别账号的访问权限，在受管模式中运行的应用可能够访问系统资源。例如，在配置为与在受管模式中运行的应用通信的资源包括云存储资源时，在受管模式中运行的应用可基于该链接访问云存储资源中的安全数据。

[0225] 在实施方案中，在根据图16创建用于能够在受管模式中运行的应用的账号后，应

用可基于所创建的账号访问安全数据。例如，用户可使用在受管模式中运行的应用和诸如用户名和密码或令牌的用户的凭证登陆到所创建的账号。诸如网关服务器560的服务器可许可在受管模式中运行的应用基于所提供的用户凭证登录到所创建的账号。应用可请求对企业数据的访问，诸如用户的电子邮件或安全文档。服务器可基于所链接的账号许可对应用的访问。例如，所链接的账号可包括活动目录账号和/或包括用户的访问权限的账号。根据包括在所链接账号内的访问权限，可许可应用访问企业数据。

[0226] 在实施方案中，应用可包括自带应用并且设备管理器524可改变和/或配置该应用。例如，改变和/或配置可包括调整该应用以使应用可在受管模式中运行。例如，应用可被改变和/或配置以使由在受管模式中运行的应用储存的数据被加密或储存在安全数据容器中。在另一个示例中，应用可被改变和/或配置以使在受管模式运行的应用可与一个或多个安全资源(如，网关服务器560)通信。在这个示例中，安全资源可包括云存储资源，其已经供应为与在受管模式中运行的应用通信，如上面所描述的。

[0227] 在一些实施方案中，应用商店可提供能够在多操作模式中执行的应用。应用商店可提供可下载的应用到移动设备。例如，移动设备可请求可下载的应用列表，并且应用商店可提供所请求的列表。然后，移动设备可从应用商店下载所列出的应用中的一个并安装所下载的应用。

[0228] 在实施方案中，应用商店可提供应用的多个版本并可提供能够在多操作模式运行的版本。例如，应用商店可提供能够在受管模式或非受管模式中运行的应用的版本，如上面所描述的。

[0229] 在图17中，根据实施方案示出用于提供能够在多模式中运行的可下载的应用的示例方法步骤的流程图。图17可开始于步骤1702，其中对可下载的应用的请求被接收。例如，诸如移动设备502的移动设备可请求来自应用商店的可下载应用列表。

[0230] 图17的过程可从步骤1702进行到步骤1704，其中，确定移动设备是否配置为在多模式中执行应用。例如，可确定移动设备是否配置为在受管模式中和非受管模式中执行应用。

[0231] 在实施方案中，可确定移动设备是否配备了能够在受管模式中和非受管模式中执行应用的应用管理框架。可确定移动设备是否配备了诸如应用管理框架614的应用管理框架。

[0232] 在实施方案中，确定移动设备是否配备了能够在受管模式中和非受管模式中执行应用的应用管理框架可包括检测与应用管理框架相关的受管应用安装在移动设备上。例如，可检测诸如客户端代理604的受管应用是否安装在移动设备上，受管应用与诸如应用管理框架614的应用管理框架相关。检测到诸如客户端代理604的应用安装在移动设备上可允许确定移动设备配备有能够在受管模式和非受管模式中执行应用的应用管理框架。

[0233] 在实施方案中，确定移动设备是否配备了能够在受管模式中和非受管模式中执行应用的应用管理框架可包括检测移动设备由与应用管理框架相关的设备管理器管理。例如，可检测诸如设备管理器524的设备管理器是否管理移动设备，设备管理器与诸如应用管理框架614的应用管理框架相关。检测到诸如设备管理器524的设备管理器管理移动设备可允许确定移动设备配备有能够在受管模式和非受管模式中执行应用的应用管理框架。

[0234] 图17的过程可从步骤1704行进到步骤1706，其中基于该确定可下载应用列表可被

发送到移动设备上。例如，当确定移动设备配备了能够在受管模式中和非受管模式中执行应用的应用管理框架时，可提供可下载应用列表，该列表包括可在受管模式和非受管模式中执行的应用的第一版本。在另一个示例中，当确定移动设备没有配备能够在受管模式中和非受管模式中执行应用的应用管理框架时，可提供可下载应用列表，该列表不包括可在受管模式和非受管模式中执行的应用的第一版本。例如，应用可包括文件共享应用并且文件共享应用的第一版本可包括可在受管模式和非受管模式中执行的应用，如上面所描述的。

[0235] 在实施方案中，可在受管模式和非受管模式中执行的应用的第一版本可与移动设备上的应用管理框架关联，诸如应用管理框架614。基于与由移动设备实施的应用管理框架的关联，可选择应用的第一版本。例如，应用商店可包括在受管模式和非受管模式中可执行的应用的多个版本，并且应用的第一版本可选择为列出，因为第一版本配置为由应用管理框架执行和/或管理。通过基于给定的移动设备的应用管理框架选择适合的应用版本，单一应用商店可给一系列广泛的移动设备提供应用而不考虑由设备实施的应用管理框架。因此，每一个应用管理框架提供者不需要维护专用应用商店并且应用开发者可简单地供应应用的一个或多个版本到用于分发的单一应用商店。

[0236] 在实施方案中，可在非受管模式和受管模式中执行的应用的第一版本可与管理移动设备的设备管理器关联，诸如设备管理器524。基于与设备管理器的关联，可选择应用的第一版本。例如，应用商店可包括在受管模式和非受管模式中可执行的应用的多个版本，并且基于与管理移动设备的设备管理器的关联，应用的第一版本可选择为列出。

[0237] 在实施方案中，基于可下载应用的列表，移动设备可下载并安装应用。例如，在列表包括应用在受管模式和非受管模式中可执行的版本的实施方案中，移动设备可下载应用的该版本并安装应用的该版本。然后，移动设备在受管模式中或非受管模式中执行所安装的应用。

[0238] 在另一个实施方案中，安装在登记的移动设备上的应用可包括外部应用。例如，登记的移动设备可从不隶属于移动设备的设备管理器(如，设备管理器524)的外部源—诸如通用应用商店接收应用，而不是从隶属于登记的移动设备的设备管理器(如，设备管理器524)的企业资源—诸如企业应用商店接收应用。在实施方案中，外部应用可包括与企业应用商店不相关的通用应用。

[0239] 在实施方案中，外部应用可请求登录到企业账号和/或企业服务器。企业账号可包括与企业相关的账号，诸如与企业活动目录相关的账号。例如，外部应用可包括电子邮件客户端，并且该电子邮件客户端可请求登录到企业电子邮件账号。在另一个示例中，外部应用可包括云存储应用，并且该云存储应用可请求登录到允许访问企业资源的服务器，诸如网关服务器。

[0240] 在实施方案中，诸如图5中的登记的移动设备502的登记的移动设备可具有安装的外部应用，并且外部应用可提交请求到诸如图5中的网关服务器560的服务器以访问企业账号。这可包括自带应用(BYOA)实施方案的示例。

[0241] 在实施方案中，安装在受管移动设备上的自带应用可被管理移动设备的设备管理器改变和/或配置。例如，安装在移动设备502上的自带应用可被设备管理器524改变。改变和/或配置可包括调整该应用以使应用可在受管模式中运行。例如，应用可被改变和/或配

置以使由在受管模式中运行的应用储存的数据被加密或储存在安全数据容器中。在另一个示例中，应用可被改变和/或配置以使在受管模式运行的应用可与一个或多个安全资源(如，网关服务器560)通信。

[0242] 虽然已经以针对结构特征和/或方法动作的语言描述了本主题，但是应该理解的是，在所附权利要求中定义的主题不必限于以上所述的具体特征或动作。相反，上述的具体特征和动作作为所附权利要求的示例性实现来描述，并且可实践其它实施方案。例如，下面包括，但不限于，各种其它实施方案。

[0243] 一个实施方案可包括方法，该方法包括：在移动设备上以第一模式运行应用，其中，第一模式是受管模式；在移动设备上以第二模式运行应用，其中，第二模式是非受管模式，其中，所述应用在第二模式中运行的时间与当所述应用在第一模式中运行的时间互相排斥；接收请求以储存与应用相关的数据；当应用在受管模式中运行时根据第一协议储存数据和应用在非受管模式中运行时根据第二协议储存数据。在这种实施方案中，第一协议可包括将数据储存在第一数据容器中和第二协议可包括将数据储存在与第一数据容器互相排斥的第二数据容器中。这种实施方案还可包括当应用在非受管模式中运行时限制应用访问第一数据容器。这种实施方案还可包括：第一协议，包括在储存数据前用第一密钥加密该数据；以及第二协议，包括储存数据前用第二密钥加密数据和储存未加密数据中的至少一个。在一些情况中，根据与应用分开并适用于多个应用的一个或多个策略文件，在受管模式中运行的应用由设备管理器管理。一些方面还可包括从设备管理器接收信号以禁用应用的受管模式。当此发生时，响应于所接收的信号，实施方案可定位根据第一协议储存的数据并可选择地删除所定位的数据。定位根据第一协议储存的数据可包括确定与应用相关的受管账号，并基于受管账号定位数据。在一些情况中，定位根据第一协议储存的数据还包括定位根据第一协议储存数据的容器。在一些方面，定位根据第一协议储存的数据还包括确定与第一协议相关的加密密钥；并基于所确定加密密钥定位数据。在一些实施方案中，设备管理器禁用受管模式以响应于识别安装在移动设备上的黑名单应用。设备管理器可禁用受管模式以响应于检测到与应用相关的受管账号已经过期。设备管理器可禁用受管模式以响应于检测到移动设备已经被越狱或获得管理员权限。在一些情况中，可选择地删除所定位的数据而不删除与储存在移动设备上的应用相关的私人数据。

[0244] 另一个实施方案可包括计算设备，该计算设备包括：处理器，其中，该计算设备配置为在第一模式中运行应用，其中，第一模式是在与应用分开的一个或多个策略文件的控制下操作并对管理在计算设备上执行的多个应用的操作有用的受管模式；在第二模式中运行应用，其中，所述应用在第二模式中运行的时间与当所述应用在第一模式中运行的时间互相排斥；接收请求以储存与应用相关的数据；当应用在第一模式中运行时根据第一协议储存数据和应用在第二模式中运行时根据第二协议储存数据。在一些方面，第一协议包括将数据储存在第一数据容器中和第二协议包括将数据储存在与第一数据容器不同的第二数据容器中。在一些实施方案中，计算设备还配置为当应用在第二模式中运行时限制应用访问第一数据容器。在一些实施方案中，第一协议包括储存数据前用第一密钥加密该数据并且第二协议包括储存数据前用第二密钥加密数据和储存未加密数据中的至少一个。在一些实施方案中，第一模式是第一受管模式，并且第二模式是根据不同于第一受管模式的策略文件中的至少一个策略文件管理的第二受管模式。

[0245] 又一个实施方案可包括储存计算机可读指令的一个或多个非暂时性计算机可读存储介质，当计算机可读指令被数据处理系统的一个或多个处理器执行时，促使该系统：在第一模式中运行应用，其中，第一模式是受管模式；在第二模式中运行应用，其中，第二模式是非受管模式，其中，所述应用在第二模式中运行的时间与当所述应用在第一模式中运行的时间互相排斥；接收请求以储存与应用相关的数据；当应用在受管模式中运行时根据第一协议储存数据和当应用在非受管模式中运行时根据第二协议储存数据。

[0246] 在另一个说明性实施方案中，方法可包括周期性地监测移动设备以确定新的软件应用被安装在移动设备上；检测该应用能够在第一模式和第二模式中运行，其中，第一模式是在与应用分开的一个或多个策略文件的控制下操作并对管理在计算设备上执行的多个应用的操作有用的受管模式；供应资源以与应用通信，以使资源被供应为仅当应用在第一模式中运行时与应用通信，并且当应用在第二模式中运行时不与应用通信。在一些方面，资源包括储存安全数据的云存储资源。在一些方面，当应用在第一模式中运行时，供应资源包括供应云数据存储以允许应用访问储存在云数据存储资源中的数据。在一些方面，移动设备由设备管理器管理，并且其中，设备管理器管理一个或多个策略文件。在一些方面，供应资源还包括创建用于应用的带资源的账号，其与来自移动设备的标识信息相关；基于标识信息定位受管账号；以及将受管账号链接到所创建的账号。在一些方面，第二模式是在不同于第一模式的一个或多个策略文件的控制下操作的第二受管模式。在一些方面，第一模式与第一用户角色相关，且第二模式与不同于第一用户角色的第二用户角色相关。在一些方面，第一模式与第一工作地点环境类型相关，并且第二模式与第二工作地点环境类型相关。在一些方面，方法包括检测应用在第一模式运行；并且基于所创建的账号允许应用访问安全数据。在一些方面，方法包括从在第一模式中运行的应用接收请求，其中，该请求包括访问安全数据的请求；并基于所创建的账号授权该应用对安全数据的访问。在一些方面，应用由企业分配到设备。

[0247] 在另一个说明性实施方案中，具有处理器的设备配置为：周期性地监测移动设备以确定新的软件应用被安装在移动设备上；检测应用能够在第一模式和第二模式中运行，其中，第一模式是在与应用分开的一个或多个策略文件的控制下操作并对管理在计算设备上执行的多个应用的操作有用的受管模式；供应资源以与应用通信，以使资源被供应为仅当应用在第一模式中运行时与应用通信，并且当应用在第二模式中运行时不与应用通信。在一些方面，资源包括储存安全数据的云存储资源。在一些方面，当应用在第一模式中运行时，供应资源包括配置云数据存储以允许应用访问储存在云数据存储资源中的数据。在一些方面，移动设备由设备管理器管理，其中，设备管理器管理一个或多个策略文件。在一些方面，供应资源还包括创建用于应用的带资源账号，其与来自移动设备的标识信息相关；基于标识信息定位受管账号；以及将受管账号链接到所创建的账号。在一些方面，第二模式是在不同于第一模式的一个或多个策略文件的控制下操作的第二受管模式。在一些方面，第一模式与第一用户角色相关，且第二模式与第二用户角色相关。在一些方面，设备还配置为：检测应用在第一模式中运行；并基于所创建的账号允许应用访问安全数据。

[0248] 在另一个说明性实施方案中，一个或多个非暂时性计算机可读程序储存计算机可读介质，当程序由数据处理系统的一个或多个处理器执行时，促使系统实现：周期性地监测移动设备以确定新的软件应用被安装在移动设备上；检测应用能够在第一模式和第二模式

中运行，其中，第一模式是在与应用分开的一个或多个策略文件的控制下操作并对管理在计算设备上执行的多个应用的操作有用的受管模式；供应资源以与应用通信，以使资源被供应为仅当应用在第一模式中运行时与应用通信，并且当应用在第二模式中运行时不与应用通信。

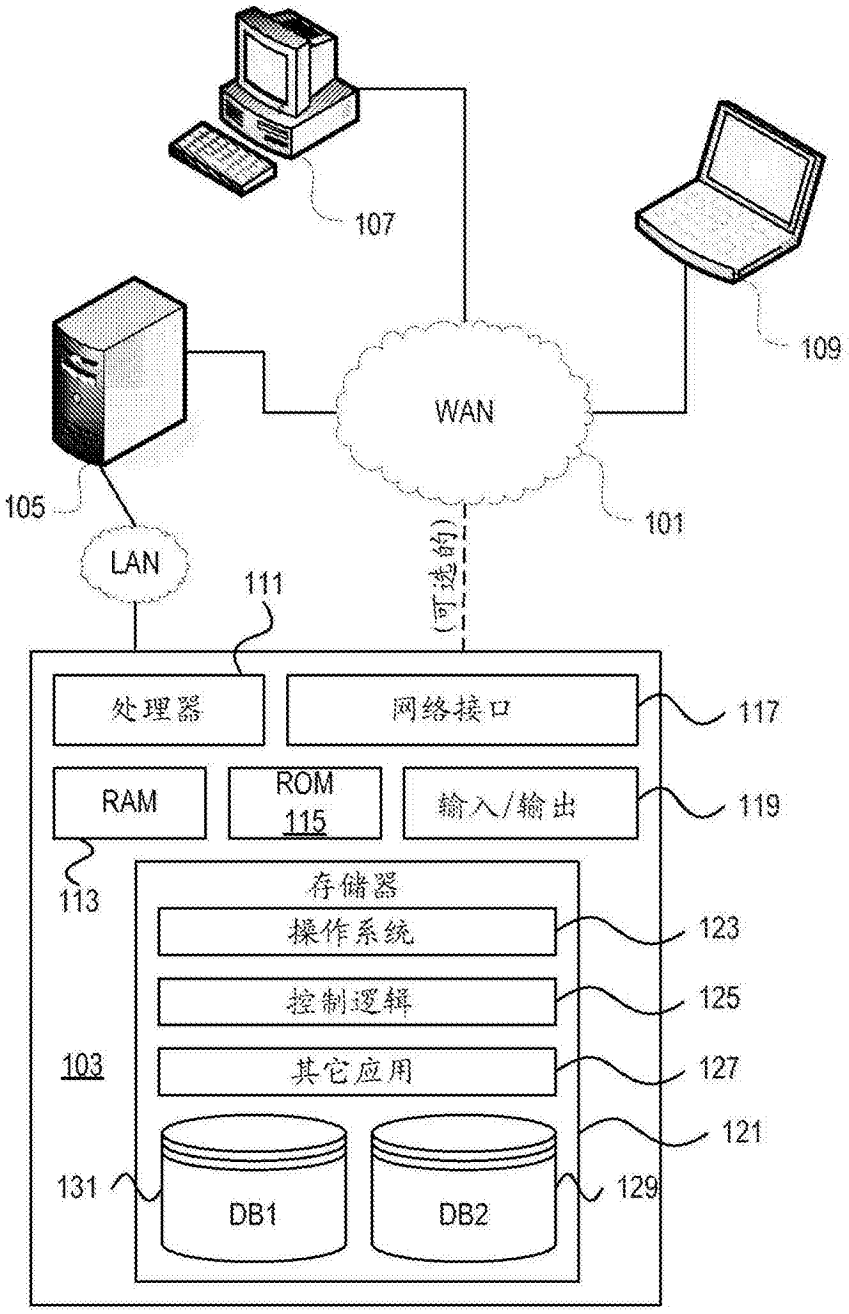

107
109
WAN
105
101
LAN
111
(可选的)
处理器
网络接口
117
RAM
ROM
115
输入/输出
119
113
存储器
操作系统
123
控制逻辑
125
103
其它应用
127
121
131
DB1
DB2
129

图1

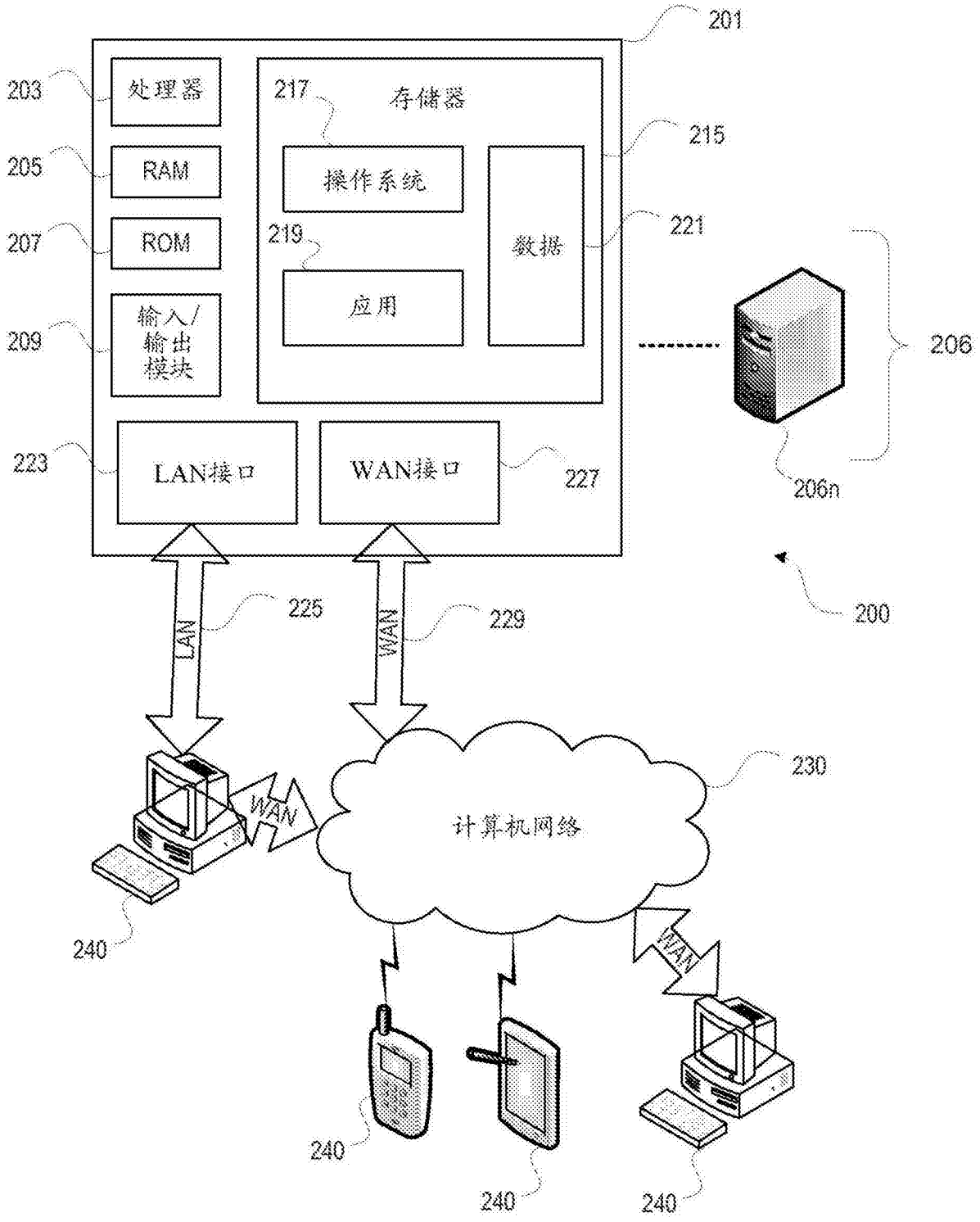

201
203
处理器
217
存储器
205
RAM
215
操作系统
207
ROM
219
221
数据
209
输入/输出模块
应用
206
206n
223
LAN接口
WAN接口
227
200
225
229
LAN
WAN
230
计算机网络
WAN
240
240
240
240

图2

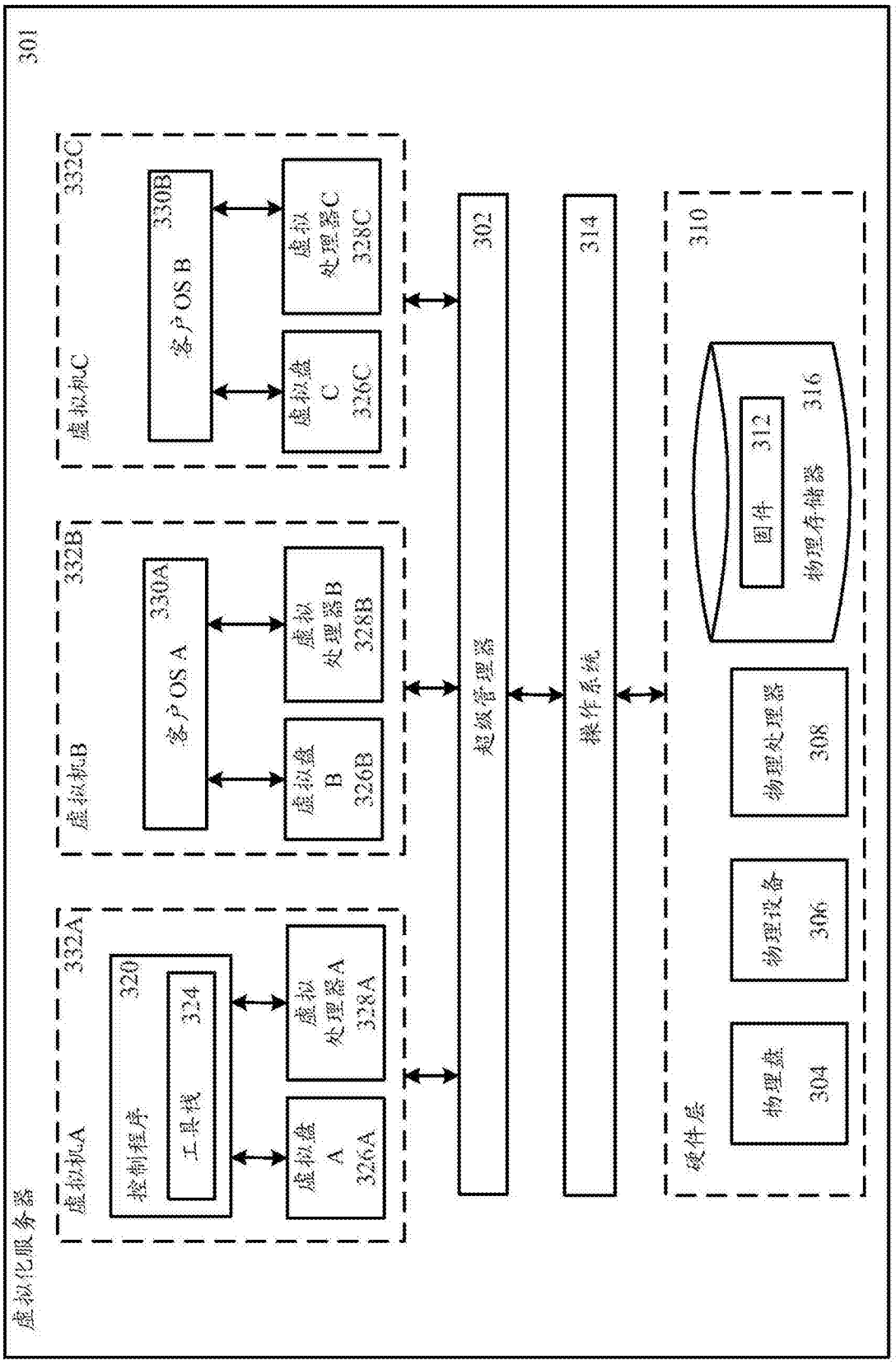

301
虚拟化服务器
虚拟机A
332A
320
控制程序
324
工具栈
虚拟盘
A
326A
虚拟
处理器A
328A
虚拟机B
332B
330A
客户OS A
虚拟盘
B
326B
虚拟
处理器B
328B
虚拟机C
332C
330B
客户OS B
虚拟盘
C
326C
虚拟
处理器C
328C
302
超级管理器
314
操作系统
310
硬件层
物理盘
304
物理设备
306
物理处理器
308
物理存储器
316
固件
312

图3

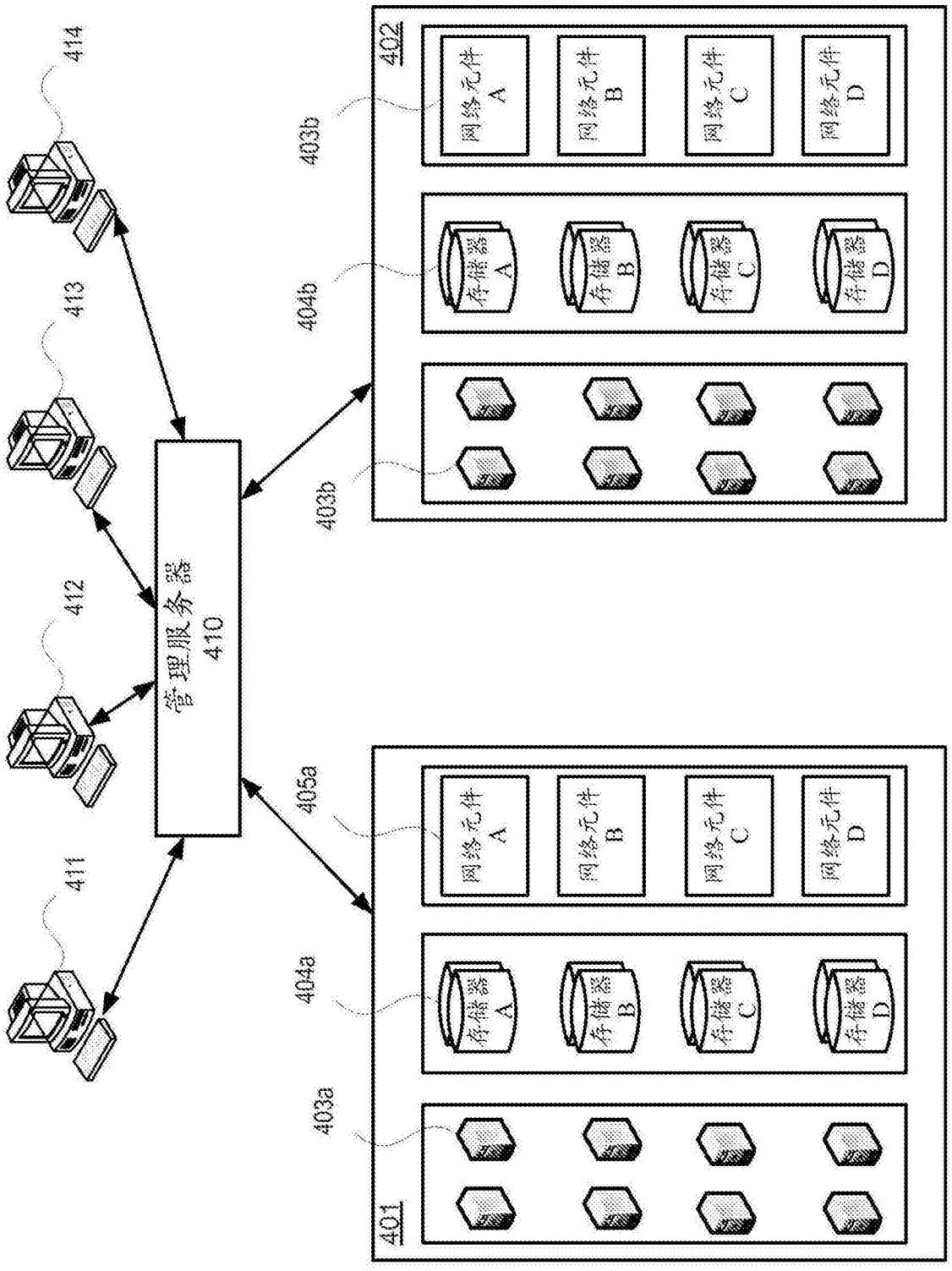

414
413
412
411
管理服务器
410
402
403b
404b
403b
网络元件
A
网络元件
B
网络元件
C
网络元件
D
存储器
A
存储器
B
存储器
C
存储器
D
405a
404a
403a
401

图4

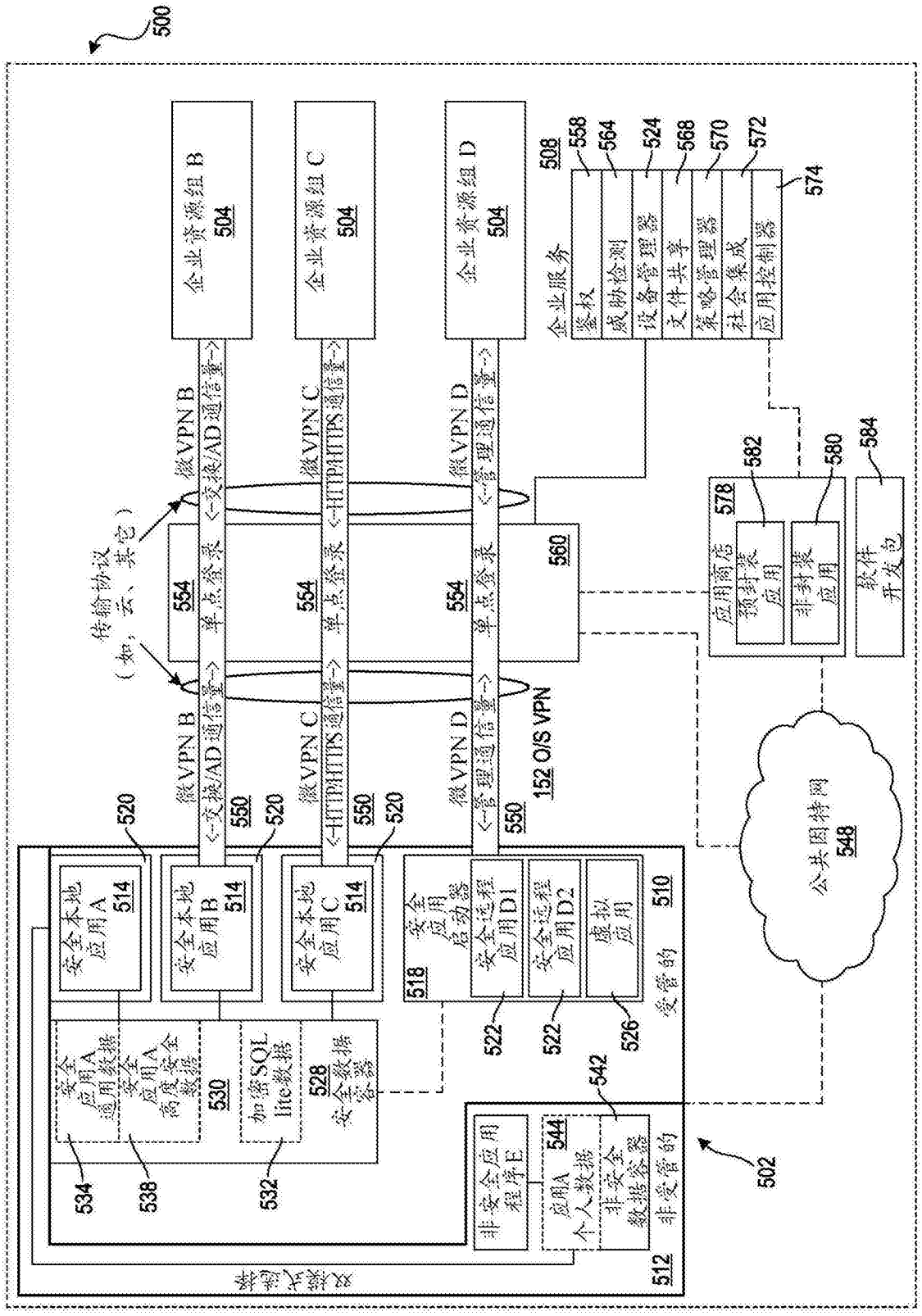

500
企业资源组 B
504
企业资源组 C
504
企业资源组 D
504
508
企业服务
558
564
524
568
570
572
574
鉴权
威胁检测
设备管理器
文件共享
策略管理器
社会集成
应用控制器
传输协议
（如，云、其它）
微VPN B
<-交换/AD通信量->
554
单点登录
560
微VPN C
<-HTTP/HTTPS通信量->
微VPN D
<-管理通信量->
152 O/S VPN
550
520
安全本地
应用A
514
安全本地
应用B
514
安全本地
应用C
514
安全
应用
启动器
518
安全远程
应用D1
安全远程
应用D2
虚拟
应用
510
受管的
522
526
安全
应用A
通用数据
安全
应用A
高度安全
数据
530
加密SQL
lite数据
库
528
安全数据
容器
534
538
532
非安全应用
程序E
542
应用A
个人数据
544
非安全
数据容器
512
非受管的
502
应用商店
578
582
预封装
应用
580
非封装
应用
584
软件
开发包
公共因特网
548

图5

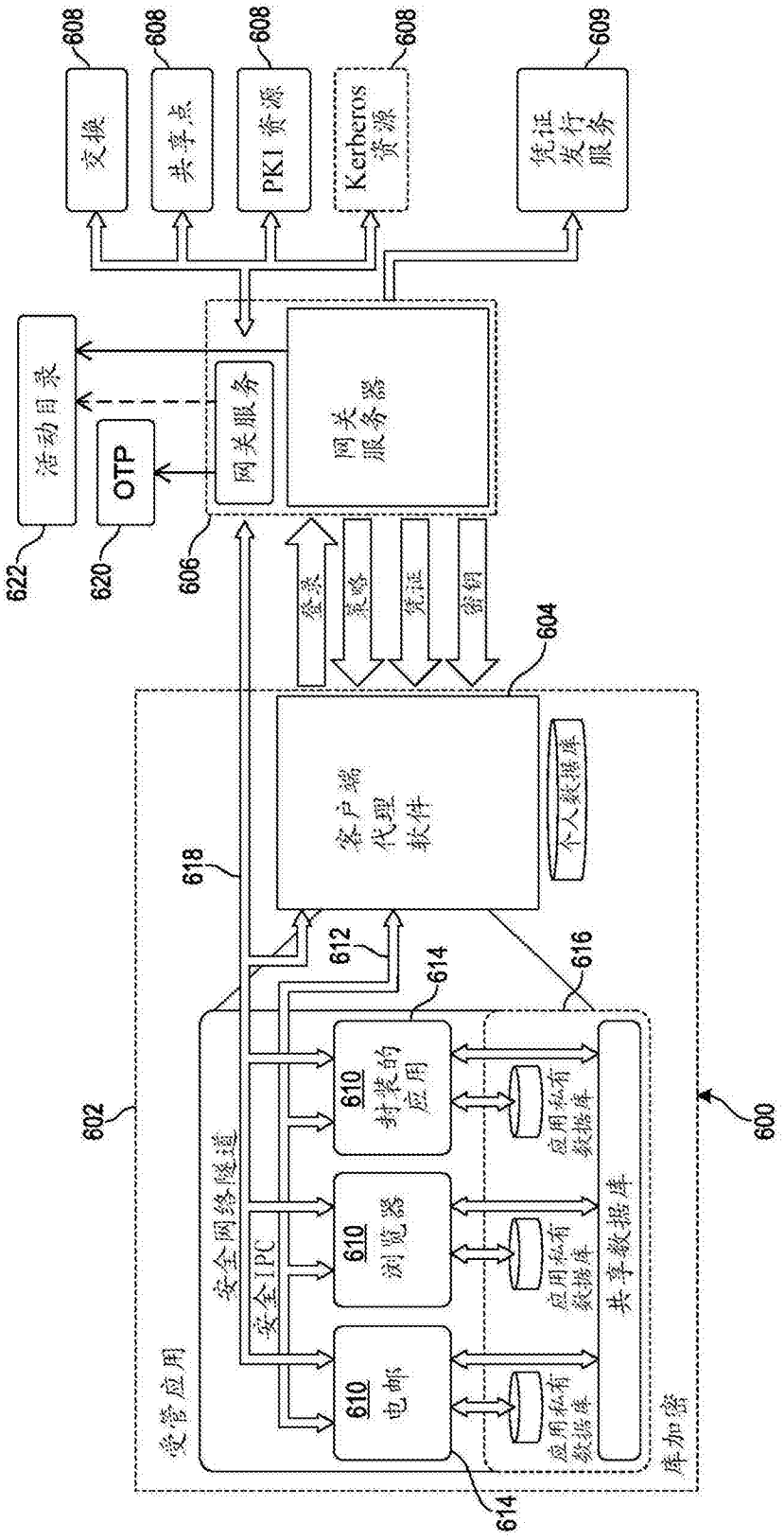

608
交换
608
共享点
608
PKI 资源
608
Kerberos 资源
609
凭证发行服务
活动目录
OTP
网关服务
网关服务器
622
620
606
签发
策略
凭证
密钥
604
客户端代理软件
个人数据库
618
612
614
616
602
600
安全网络隧道
安全IPC
610
封装的应用
610
浏览器
610
电邮
应用私有数据库
应用私有数据库
应用私有数据库
共享数据库
受管应用
库加密
614

图6

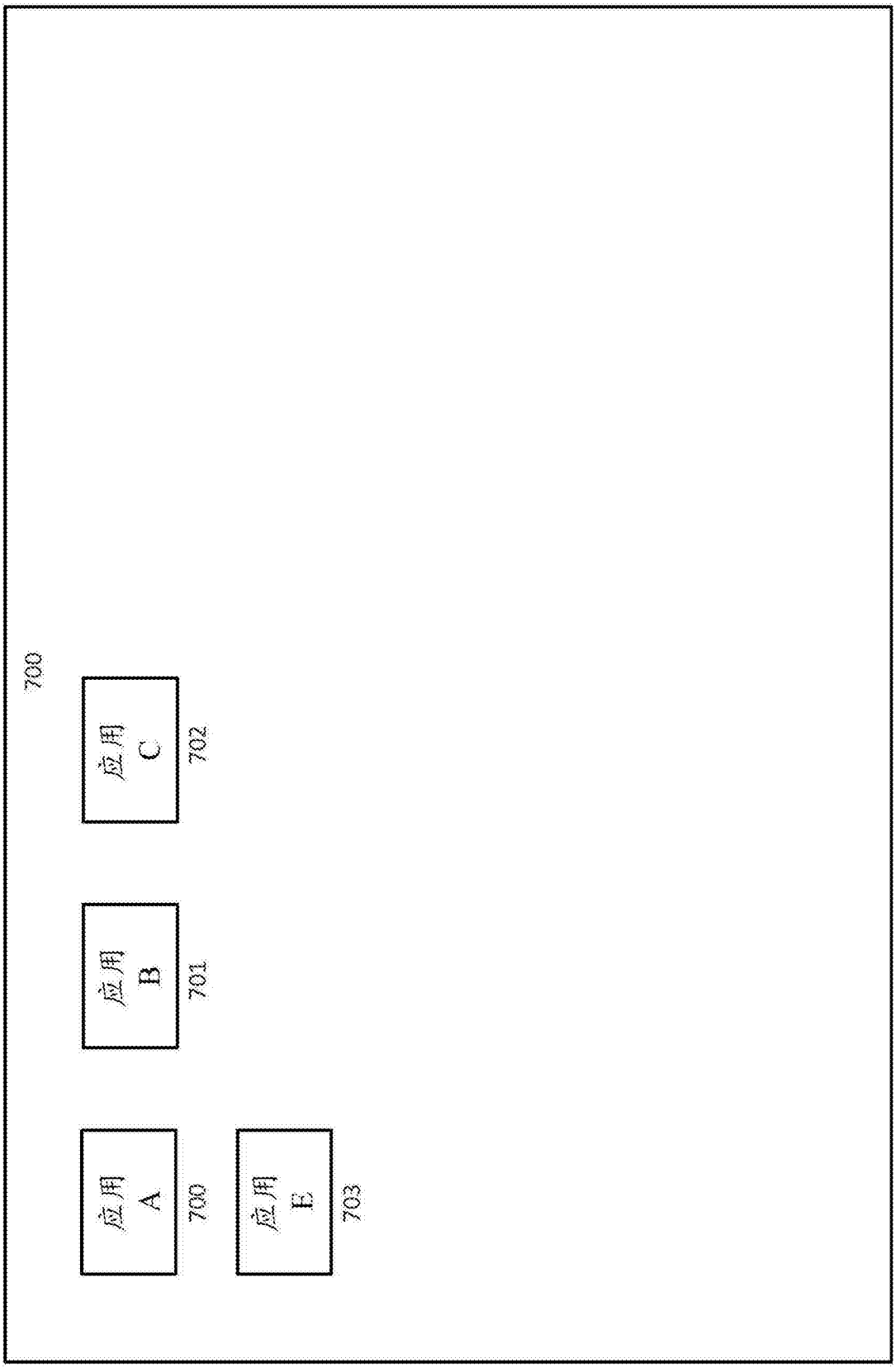


图7

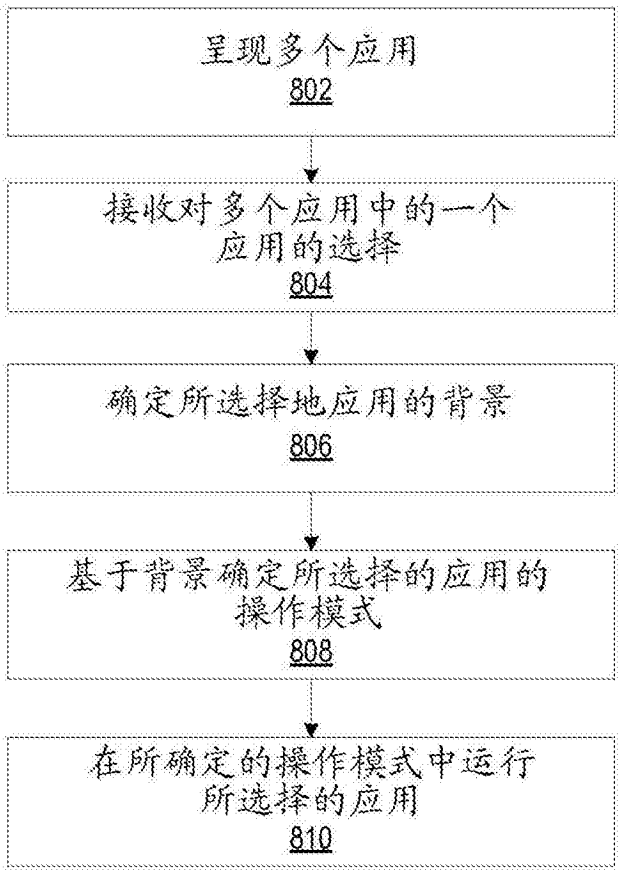

呈现多个应用
802
接收对多个应用中的一个应用的选择
804
确定所选择地应用的背景
806
基于背景确定所选择的应用的操作模式
808
在所确定的操作模式中运行所选择的应用
810

图8

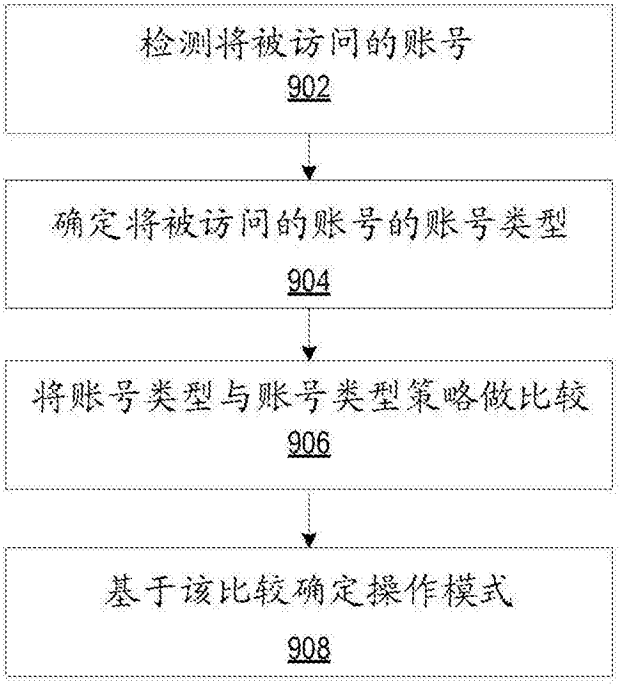

检测将被访问的账号
902
确定将被访问的账号的账号类型
904
将账号类型与账号类型策略做比较
906
基于该比较确定操作模式
908

图9

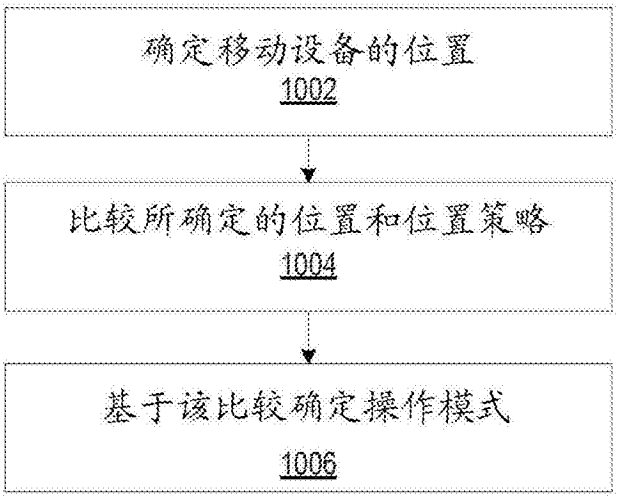

确定移动设备的位置
1002
比较所确定的位置和位置策略
1004
基于该比较确定操作模式
1006

图10

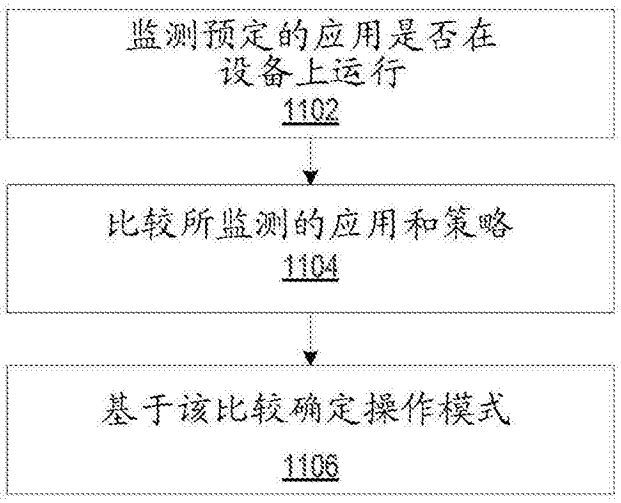

监测预定的应用是否在
设备上运行
1102
比较所监测的应用和策略
1104
基于该比较确定操作模式
1106

图11

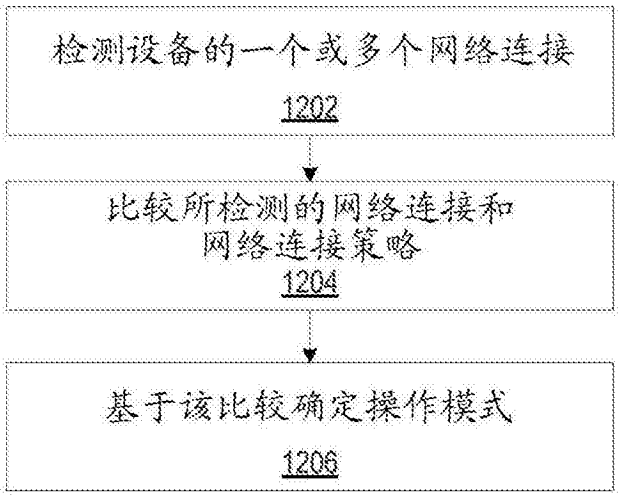

检测设备的一个或多个网络连接
1202
比较所检测的网络连接和
网络连接策略
1204
基于该比较确定操作模式
1206

图12

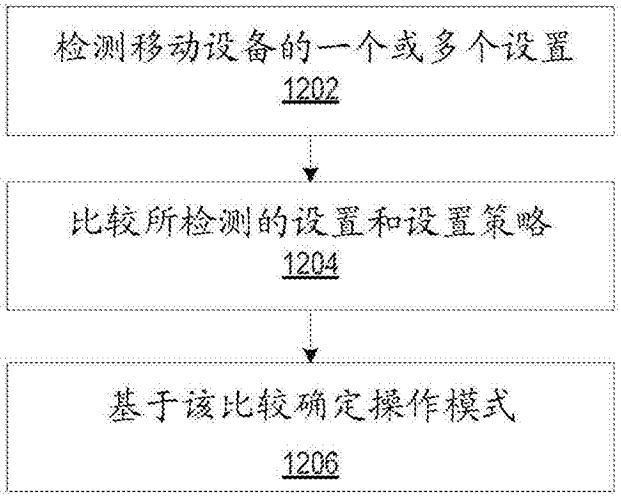

检测移动设备的一个或多个设置
1202
比较所检测的设置和设置策略
1204
基于该比较确定操作模式
1206

图13

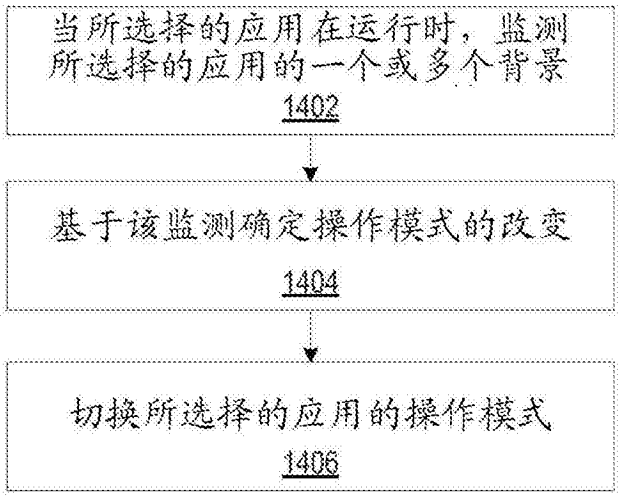

当所选择的应用在运行时，监测所选择的应用的一个或多个背景
1402
基于该监测确定操作模式的改变
1404
切换所选择的应用的操作模式
1406

图14

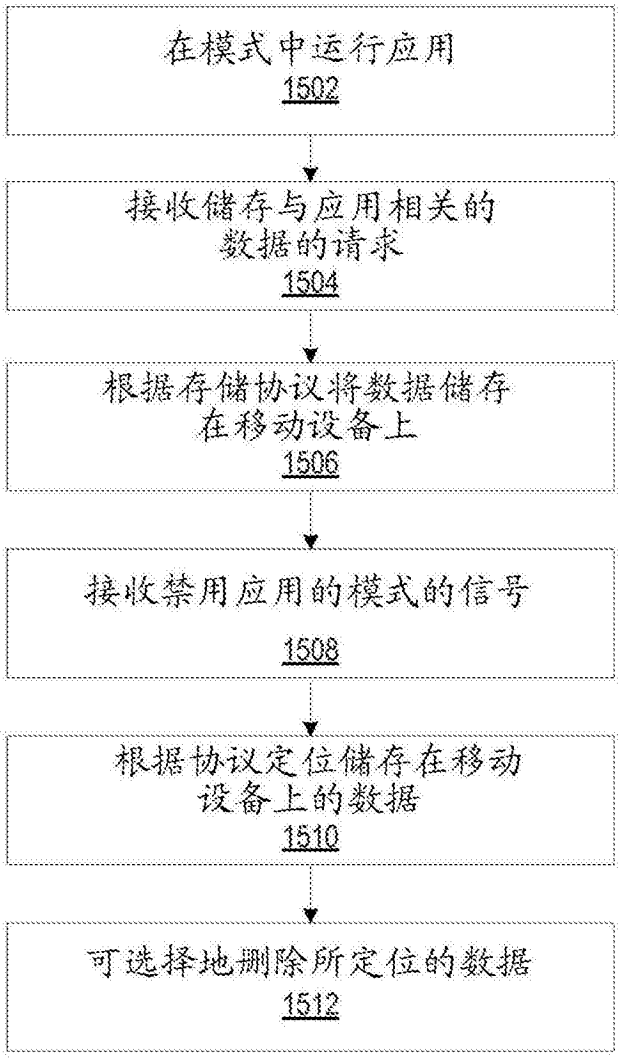

在模式中运行应用
1502
接收储存与应用相关的数据的请求
1504
根据存储协议将数据储存在移动设备上
1506
接收禁用应用的模式的信号
1508
根据协议定位储存在移动设备上的数据
1510
可选择地删除所定位的数据
1512

图15

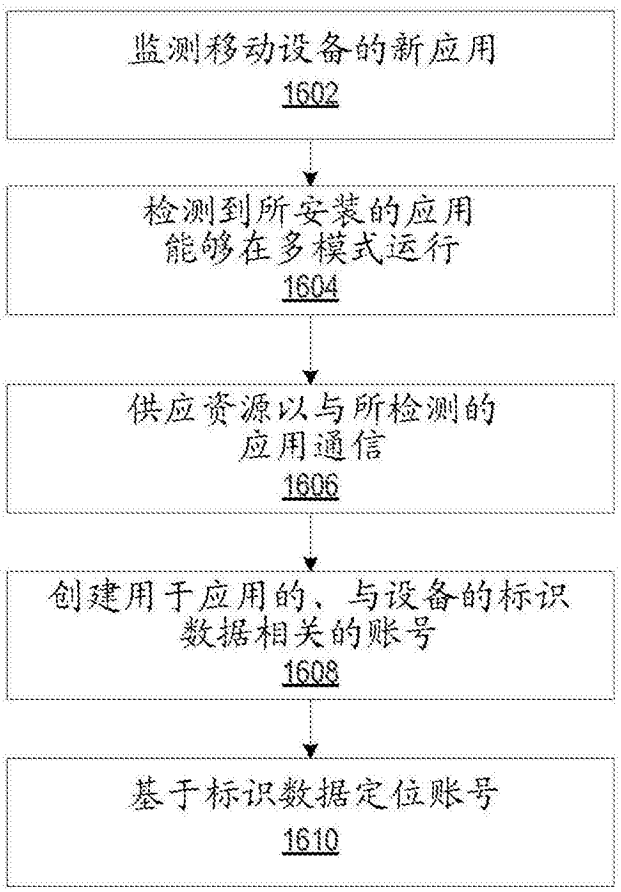

监测移动设备的新应用
1602
检测到所安装的应用
能够在多模式运行
1604
供应资源以与所检测的
应用通信
1606
创建用于应用的、与设备的标识
数据相关的账号
1608
基于标识数据定位账号
1610

图16

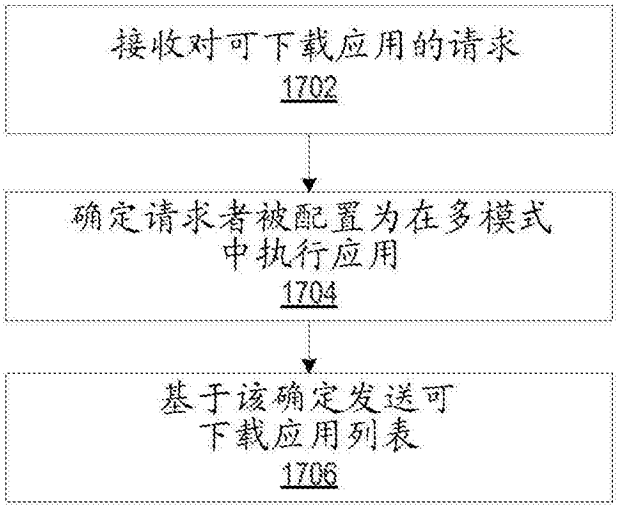

接收对可下载应用的请求
1702
确定请求者被配置为在多模式
中执行应用
1704
基于该确定发送可
下载应用列表
1706

图17