(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 102882855 B
(45)授权公告日 2016.06.29

(21)申请号 201210326881.7

(22)申请日 2012.09.06

(30)优先权数据
13/226223 2011.09.06 US

(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 G. 迪亚斯 - 克拉 S. 伊斯金
J.P.C. 科罗内尔门多扎
S.B. 格雷厄姆 N.D. 伍德

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李亚非 汪扬

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 1633084 A,2005.06.29,

审查员 裴广坤

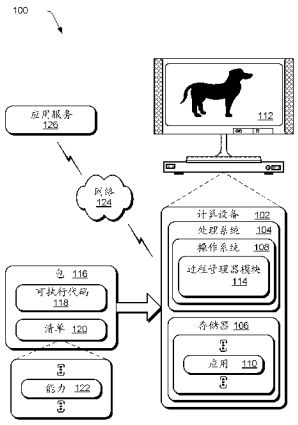
权利要求书1页 说明书9页 附图8页

(54)发明名称

按过程的连网能力的管理方法及设备

(57)摘要

描述了按过程的连网能力技术。在一个或多个实施方式中,基于与在计算设备上执行的过程相关的标记,确定关于是否允许该过程访问网络能力。该标记具有一个或多个安全标识符,其引用在清单中描述的一个或多个网络能力。基于该确定来管理对网络能力的访问。



CN 102882855 B

1.一种通过计算设备实现的方法，该方法包括：

由在计算设备本地执行的过程请求对包括来自或去往远程计算设备的相应的向内或向外连接的计算设备的防火墙类型网络能力的访问；

响应于过程的执行，由计算设备创建与过程相关联的标记，该标记包括一个或多个安全标识符，该安全标识符对应于作为可执行代码的安装的一部分在本地存储的清单中定义的一个或多个网络能力，可执行代码当被执行时，实现该过程；

由计算设备通过将该过程请求的访问与响应于该过程的执行创建的标记进行比较来确定是否允许该过程访问；以及

基于该确定由计算设备来管理对网络能力的访问(504)。

2.如权利要求1所述的方法，其中清单由所述可执行代码的开发者生成以描述所述可执行代码被允许访问哪些网络能力。

3.如权利要求2所述的方法，其中清单存储在防篡改的位置中作为计算设备上的可执行代码的安装部分。

4.如权利要求1所述的方法，其中通过访问在所述过程不能访问的计算设备的防篡改位置中存储的能力的描述来形成标记。

5.如权利要求1所述的方法，其中清单中描述的至少一个所述网络能力指示是否允许通过过程的回路。

6.如权利要求1所述的方法，其中清单中描述的至少一个所述网络能力指示是否允许通过网络的向外连接供所述过程使用。

7.如权利要求1所述的方法，其中清单中描述的至少一个所述网络能力指示是否允许通过网络的向内和向外连接供所述过程使用。

8.如权利要求7所述的方法，其中向内连接允许所述过程接受未经同意的连接。

9.如权利要求1所述的方法，其中清单中描述的至少一个所述网络能力指示是否允许私有网络访问供所述过程使用。

10.一种计算设备，该设备包括：

适于由在计算设备本地执行的过程请求对包括来自或去往远程计算设备的相应的输入或输出连接的计算设备的防火墙类型网络能力的访问的单元；

适配来响应于过程的执行，由计算设备创建与过程相关联的标记的单元，该标记包括一个或多个安全标识符，该安全标识符对应于作为可执行代码的安装的一部分在本地存储的清单中定义的一个或多个网络能力，可执行代码当被执行时，实现该过程；

由计算设备通过将该过程请求的访问与响应于该过程的执行创建的标记进行比较来确定是否允许该过程访问的单元；

以及

适于基于该确定来管理对网络能力的访问的单元。

按过程的连网能力的管理方法及设备

背景技术

[0001] 用户可以获得用于由计算设备来执行的可执行代码(例如,软件)的方式在不断增加。例如,用户传统上敢于去“实体”商店来查找(locate)并购买应用,所述应用随后由用户来手动安装。因此,由于商店自身的声誉以及软件开发者的声誉,用户通常能信任该软件。

[0002] 然而,随着应用卖场(marketplace)的出现,用户可以从成百甚至上千个不同开发者获得数以千计的不同类型的应用。因此,用户可以在计算设备上安装来自广泛的源的众多应用,其中一些源可以甚至导致一个应用危害另一应用。因此,用户甚至卖场自身难以确定这些应用是否是可信赖的,并且因而应该被允许访问用户的计算设备的功能。该困难可能被恶意方进一步加剧,该恶意方可以攻击应用以访问应用所支持的功能,例如访问甚至是用于源自可信赖源的应用的敏感数据。

发明内容

[0003] 描述了按过程的连网能力技术。在一个或多个实施方式中,基于与在计算设备上执行的过程相关的标记,确定关于是否允许该过程访问网络能力。该标记具有一个或多个安全标识符,其引用一个或多个在清单(manifest)中描述的网络能力。基于该确定来管理对网络能力的访问。

[0004] 在一个或多个实施方式中,网络被探测以识别代理服务器、子网或远程可访问网络。基于代理服务器或子网的识别以及对与在计算设备上执行的过程相关的标记的审查来管理该过程对网络的网络能力的访问。标记具有一个或多个安全标识符,其引用允许该过程所使用的、在清单中描述的网络能力。这可以以安全的方式来执行,该安全的方式没有被配置为受该过程影响。

[0005] 在一个或多个实施方式中,一个或多个计算机可读存储介质包括存储在其上的指令,响应于在计算设备上的执行,该指令使得计算设备执行操作系统以形成具有一个或多个安全标识符的标记,所述一个或多个安全标识符引用清单中描述的网络能力,该清单对应于通过由计算设备对执行代码的执行来形成的过程,所述执行代码和清单从包(package)被安装在计算设备上,标记可由操作系统使用来管理过程对网络能力的访问。

[0006] 提供此发明内容来以简要形式介绍一些概念选集,其将在以下具体实施例中进一步介绍。此发明内容不旨在标识要求保护主题的关键特征或必要特征,也不旨在用来帮助确定要求保护主题的范围。

附图说明

[0007] 参考附图来描述具体实施例。在图中,附图标记的最左边的一个或多个数字标识该附图标记首次出现在哪个图中。说明书和附图中的不同实例中使用的相同附图标记指示相似或相同的项。

[0008] 图1是可用于执行按过程连网能力技术的示例实施方式中的环境的图示。

[0009] 图2是示出按过程连网能力技术的示例实施方式的示例实施方式中的系统的图

示。

[0010] 图3是示出按过程连网能力技术的示例实施方式的示例实施方式中的系统的另一图示。

[0011] 图4是描绘具有可执行代码的包和清单被安装在计算设备上并用以响应于发起执行代码的执行来形成标记的示例实施方式中的过程的流程图。

[0012] 图5是描绘计算设备使用在图4中形成的标记来管理对能力的访问的示例实施方式中的过程的流程图。

[0013] 图6是描绘探测连同标记被一起使用来管理对网络能力的按过程访问的示例实施方式中的过程的流程图。

[0014] 图7图示了包括如参考图1所述的计算设备的示例系统。

[0015] 图8图示了示例设备的各种组件，该示例设备可以实现为如参考图1-3和7所述的任意类型的计算设备以实现本文中描述的技术的实施例。

具体实施例

[0016] 概览

[0017] 传统上，执行在计算设备上的应用被允许访问计算设备的大多数(如果不是全部的话)功能，甚至不管是否期望该访问。这可以包括对网络的不受约束的访问。然而，在一些实例中，这些同样的应用可能被恶意方所利用。这些恶意方因而可以使用不受约束的访问来访问互联网上的资源、接收未经同意的连接、访问联网功能等等。因此，给予这些应用的宽泛的访问现在可能给用户的计算设备以及计算设备可访问的设备呈现显著的风险。

[0018] 描述了按过程网络能力技术。在一个或多个实施方式中，使用能力模型来确保应用能够访问开发者限定的网络资源，而不能访问开发者没有限定的其他网络资源。因而，该能力模型可以防止被利用的应用利用通常不被该应用所使用的网络资源。通过此方式，模型可以用来确保被盗用(compromised)的应用被限制于访问限定的网络能力并且限制利用被开发者限定为应用不可访问的网络能力。还设想了各种其他示例，可以参考以下章节找到对于这些示例的进一步讨论。

[0019] 在以下讨论中，首先描述可以采用本文中描述的网络能力技术的示例环境。随后，描述可以在示例环境和其他环境中执行的示例过程。因此，执行所述示例过程不限于示例环境并且示例环境不限于执行示例过程。

[0020] 示例环境

[0021] 图1图示了根据一个或多个实施例的操作环境，通常在100处。环境100包括计算设备102，其具有可以包括一个或多个处理器的处理系统104、示出为存储器106的计算机可读存储介质的示例、操作系统108和一个或多个应用108。计算设备102可以体现为任意合适的计算设备，例如，以示例而非限制的方式，桌面计算机、便携式计算机、诸如个人数字助理(PDA)的手持计算机、移动电话、平板计算机等等。下面在图6和7中示出和描述了计算设备102的不同示例。

[0022] 计算设备102还包括操作系统108，其被图示为在处理系统104上执行并且可以存储在存储器106中。计算设备102进一步包括应用110，其被图示为存储在存储器106中并且也可以在处理系统104上执行。操作系统108代表计算设备102的功能，该功能可以抽象底层

的硬件和软件资源以供应用110使用。例如，操作系统108可以抽象数据如何显示在显示设备112上的功能，而应用110不必“知晓”如何实现该显示。还设想了各种其他示例，例如抽象计算设备102的处理系统104和存储器106资源、网络资源等。

[0023] 计算设备102还被图示为包括过程管理器模块114。过程管理器模块114代表计算设备102管理可执行代码访问计算设备102的能力的功能。例如，计算设备102可以接收具有可执行代码118(例如，应用)的包116以用于安装在计算设备102上。包116还可以包括由可执行代码118的开发者生成的清单120，其描述了计算设备102的一个或多个能力122，所述一个或多个能力122可以包括计算设备102访问网络124的能力。因而，该描述可以描述允许和/或不允许通过执行可执行代码118形成的过程访问计算设备102的哪些能力。例如，清单120可以列出将使得过程可以访问的能力和/或可以列出将使得该过程不可以访问的能力。通过这样的方式，可执行代码118的开发者可以在清单120中指定能力以有助于降低或甚至消除恶意方盗用应用来访问可执行代码118通常不访问的能力的本领(ability)。

[0024] 过程管理器模块114例如可以将防火墙功能利用为该模块自身的一部分，或者与另一模块，例如专用防火墙模块进行通信。该功能可以用来允许或拒绝访问网络124，如包116的清单所指定的那样。因而，可执行代码118可以如代码的开发者设想的那样工作，并从而有助于降低恶意方盗用代码的机会。

[0025] 可以从各种不同的源接收包116以用于安装在计算设备102上。例如，应用服务126(例如，应用商店)可由计算设备102经由网络124(例如，因特网)来访问。在购买时，包括可执行代码118和清单120的包116可以经由网络124传输以用于安装在计算设备102上。在另一示例中，用户可以获取包含包116的计算机可读存储介质(例如，光盘)。可以参考图2找到对于在计算设备上安装包括可执行代码118和清单的包116的进一步讨论。

[0026] 通常，本文中描述的任意功能都可以使用软件、固件、硬件(例如，固定的逻辑电路)或这些实施方式的组合来实现。本文中使用的术语“模块”、“功能”和“逻辑”通常代表软件、固件、硬件或其组合。在软件实施方式的情况下，模块、功能或逻辑代表在处理器(如一个或多个CPU)上被执行时执行指定任务的程序代码。该程序代码可以存储在一个或多个计算机可读存储器设备中。下述技术的特征是平台独立的，意指该技术可以实现在具有各种处理器的各种商业计算平台上。

[0027] 例如，计算设备102还可以包括这样的实体(例如，软件)，其使得计算设备102的硬件执行操作，例如处理器、功能块等。例如，计算设备102可以包括这样的计算机可读媒介，其被配置为维护使得计算设备，更具体地计算设备102的硬件来执行操作的指令。因而，所述指令工作以配置硬件来执行操作，并且通过这样的方式导致变换硬件来执行功能。计算机可读媒介可以通过各种不同的配置来将指令提供给计算设备102。

[0028] 一种这样的计算机可读媒介的配置为信号承载媒介，并因而被配置为比如经由网络将指令(例如作为载波)发送到计算设备的硬件。计算机可读媒介还可以被配置为计算机可读存储媒介，并因而不是信号承载媒介。计算机可读存储媒介的示例包括随机存取存储器(RAM)、只读存储器(ROM)、光盘、快闪存储器、硬盘存储器以及可以使用磁、光学和其他技术来存储指令和其他数据的其他存储器设备。

[0029] 图2是示例实施方式中的系统200的图示，该示例实施方式示出包116安装在计算设备102上和形成管理过程对计算设备的网络能力的访问的标记。如前所述，当开发者创建

可执行代码118时，还可以创建清单120，其包含被声明用于通过执行代码实现的过程的能力122的集合。这些能力122可以在安装期间注册，这被图示为图2中的包部署202。

[0030] 例如，可以经由应用目录204安装可执行代码118以用于使用。清单中描述的能力122可以安装在能力存储装置206中并且与包116和/或可执行代码118本身的身份相关。在一个或多个实施方式中，能力存储装置206被配置为防篡改的(例如物理和/或电子地)，使得恶意方不能访问或修改其中描述的能力122，以便防止过程自身的访问。

[0031] 在源自于执行可执行代码118的过程创建208期间，获取可由过程管理器模块114使用的标识符来定位针对过程210描述的能力，例如，上述包116、可执行代码118等的标识符。这些能力122随后被用作过程创建208的部分以形成标记212，过程管理器模块114可以使用该标记212来控制对计算设备102的能力的访问。

[0032] 标记212例如可以包括一个或多个安全标识符214，其对应于针对该过程在能力存储装置206中描述的能力212的一个或多个。换言之，标记212被填充有与包116关联的相关能力，作为安全标识符214。因而，过程管理器模块114可以使用标记212在过程210请求访问能力时确定是否将允许该过程210的访问。

[0033] 在一个或多个实施方式中，过程210不能操纵标记212。标记212还可以允许过程210参与针对能力(例如资源的ACL)的访问使用验证检查。进一步地，过程管理器模块114还可以实现这些技术，其中包括在授权访问能力之前基于能力(或能力组合)的存在的决定。因为过程210不能直接访问标记，所以过程管理器模块114可以充当代理，其利用标记212的不变性来确保适当的访问被授权给过程210。

[0034] 安全标识符214可以引用各种不同的能力122。另外，安全标识符214可以以各种方式来引用这些能力。例如，开发者可以创建可执行代码118(例如应用)和清单120，该清单120包含针对包116中的每个过程声明的能力的集合，该过程通过执行可执行代码118来实现。该包116还可以具有“强身份”，其中在安装包116时使用该身份将网络能力注册到操作系统108。

[0035] 因此，当后续启动过程210(其将包身份包括作为过程创建参数)时，标记212填充有过程身份和网络能力，它们可以被填充为安全标识符214。进一步地，操作系统108可以防止过程210修改标记212。在一个或多个实施方式中，子过程可以继承身份和网络能力的子集，其中该子集由父过程定义。

[0036] 可以通过清单120来指定各种不同的能力122以用于管理过程210的访问使用，例如，从预定义的网络能力到丰富的防火墙类型规则。例如，可以定义“互联网-客户端”能力来管理过程210对网络124(例如，互联网)的向外连接的访问。在另一示例中，可以定义“互联网客户端/服务器”能力来允许向内(incoming)和向外(outgoing)的网络124连接。该能力例如可以用来允许过程接受来自因特网的未经同意的连接，以及通过防火墙发送和接收数据。在进一步的示例中，可以定义“私有网络客户端服务器(PrivateNetworkClientServer)”能力来允许在同样定义的网络124(例如，家庭网络、工作网络、内部网等等)上与计算设备来回通信。还设想了各种其他示例，以使得可以创建丰富的引用能力的防火墙规则，这些能力可以变得甚至更加特定和丰富，例如访问特定的端口。通过这样的方式，使用标记212中的安全标识符214可以允许过程管理器模块114管理过程210对网络能力的访问，其示例参考下图描述。

[0037] 图3描绘了示例实施方式中的系统，其示出通过图1的过程管理器模块来管理过程对网络能力的访问。当过程210请求访问网络124时，过程管理器模块114验证应用身份(例如，包ID 302)，并确保由标记212指定的网络能力304、306是能力存储装置206中的在安装时注册的网络能力的子集。如果剩余的能力对于网络通信是足够的，则允许通信。否则，阻塞通信。因而，过程管理器模块114可以充当防火墙的一部分来允许和/或拒绝访问计算设备102的网络能力。

[0038] 在一个或多个实施方式中，可以允许应用访问在能力存储装置206中注册的能力的全集。然而，过程210还可能创建子过程，其中该子过程不具有父过程可用的访问权限的全集。

[0039] 如前所述，可以声明各种不同的能力。进一步地，这些能力可以组合来给予过程210对于出站连接(例如客户端)或入站(inbound)和出站(outbound)连接(例如客户端&服务器)的互联网和内部网(例如，私有网络)访问。

[0040] 互联网能力还可以允许访问HTTP代理。例如，过程管理器模块114可以主动地探测网络来确定是否存在代理服务器或子网，因此绑定到私有网络(例如内部网)或互联网的连网能力可以被正确地利用。如果活动目录(Active Directory)服务器包含有关子网定义的特定信息，则过程管理器模块114还可以利用该信息来帮助确定子网的边缘(edge)。还可以采用这样的机制，其中通过行政(administrative)管理工具预先定义子网和代理，并因而不涉及探测。在没有这样的通过探测和/或使用行政管理工具规定的情况下，可能会给一些设备分配不正确的网络类型，并且因而过程管理器模块114可能会不正确地允许或拒绝访问。因而，过程管理器模块114可以基于该标识(例如，经由内部网或因特网是否可用)来正确地管理能力。

[0041] 在一个或多个实施方式中，被认为是至关重要的端口被阻塞未经同意的入站访问来防止使用相同机制的常见攻击向量。这些设置也可以经由策略(policy)人工地配置。也可以保护回路(例如，使用127.0.0.1的到同一机器的连接)，从而防止过程210“绕过”(working around)对该过程所限定的能力。例如，回路可以绑定到上述“私有网络客户端服务器”能力，但是明显的是，在另一示例中，可以使用模型将其指定为单独的能力。

[0042] 因而，这些技术还可以用来支持按过程限制网络访问和提供如上所述的不同程度的粒度的机制。如上所述，按过程连网能力可以绑定到过程的强身份。该身份还可以由子过程继承，这确保过程不能绕过已由父过程授权该过程的连网能力。与防火墙规则具有相同灵活性的高保真度连网能力还可以由过程管理器模块114来支持。连网能力例如可以在安装时注册到防火墙，并且可以具有针对防火墙规则找到的灵活性，其可以包括网络类型、连接类型和入站/出站连接。流量方向还可以与防火墙所定义的网络简档相关。

[0043] 进一步地，声明的连网能力还可以组合来提供作为不同能力的联合(union)的访问。例如，可以针对过程210组合网络能力来提供不同网络访问的组合，例如私有网络(例如，内部网)访问以及出站互联网访问。还设想了各种其他示例，可以参考以下过程找到对于它们的进一步讨论。

[0044] 再进一步地，用来强制实施能力的防火墙规则可以例如由“高度正直”的系统在运行时动态地修改或强制实施或微调，以提供可以具有增加的有用性的能力。所限定的能力可以与系统中的其他防火墙组件隔离和/或被传递给所述其他防火墙组件，以进一步地正

确管理网络中的应用。

[0045] 示例过程

[0046] 以下讨论描述了可以使用前述系统和设备实现的按过程连网能力技术。过程的每一个的各方面可以在硬件、固件或软件或其组合中实现。该过程被示出为指定通过一个或多个设备执行的操作的框的集合，并且不必限于所示出的顺序来执行各个框的操作。在以下讨论的各部分中，将分别参考图1的环境100和图2和3的系统200、300。

[0047] 图4描绘了示例实施方式中的过程400，其中具有可执行代码和清单的包被安装在计算设备上并用来形成标记。在计算设备处接收包括可执行代码和清单的包，该清单描述了可执行代码的能力(框402)。包116例如可以存储在计算机可读存储介质上，通过网络124从应用服务126下载等等。如前所述，清单120可以描述计算设备102在执行代码期间所使用的网络能力，如可执行代码122的开发者所设想的那样。

[0048] 可执行代码安装在用于执行的计算设备上(框404)。可执行代码122例如可以被配置为要被安装在计算设备上以用于通过应用目录、第三方插件模块等访问的应用。

[0049] 由清单针对可执行代码描述的网络能力被保存在计算设备上的能力存储装置中，所保存的能力可用以形成标记来管理(通过执行可执行代码形成的)一个或多个过程对计算设备的能力的访问(框406)。能力存储装置206例如可以被配置为防篡改的，例如物理地和/或电子地。通过这样的方式，其中描述的能力不能被未授权的实体所访问，不能被在计算设备102上执行的过程所访问，等等。因而，能力的描述可以被认为是“可信赖的”并因此用以形成可以用来通过过程管理访问的标记。

[0050] 随后，可以接收输入以发起安装在计算设备上的可执行代码的执行(框408)。该输入例如可以通过用户对代码的表示(例如图标、区块(tile)等)的选择来接收。该输入也可以源自代码自身(例如，以预定的时间间隔唤醒)，源自在计算设备102上执行的其他代码，等等。

[0051] 形成具有一个或多个安全标识符的标记，所述一个或多个安全标识符引用针对可执行代码的在清单中描述的网络能力(框410)。如前所述，安全标识符122可以枚举在能力存储装置206中描述的能力。标记212例如可以包括与可执行代码118和/或包116的标识符相匹配的标识符，可以在请求对能力的访问时由可执行代码118自身来传递(例如标记自身和/或可用来找到标记212的标识符)，等等。随后，标记212可以用来管理过程210对计算设备102的一个或多个网络能力的访问，可以参考下图来找到其示例。

[0052] 图5描绘了示例实施方式中的过程500，其中计算设备使用图4中形成的标记来管理对网络能力的访问。基于与过程相关的标记 确定是否允许在计算设备上执行的过程访问网络能力，该标记具有引用清单中描述的一个或多个网络能力的一个或多个安全标识符(502)。例如，过程管理器模块114可以从过程接收请求。过程210可以由计算设备102通过执行可执行代码118来实现，如前所述。

[0053] 随后，过程管理器模块114可以例如使用如前所述的包116标识符、“强类型”等来定位标记212。可以形成标记212来描述所允许的访问(例如引用所允许的能力)和/或描述所不允许的访问，例如引用不允许相应的过程210所访问的能力。

[0054] 基于所述确定来管理对网络能力的访问(框504)。过程管理器模块114例如可以接收来自过程210的访问网络能力的请求，例如请求使用向外网络连接。随后，过程管理器模

块114可以审查标记212来确定是否允许该网络访问，例如定位引用向外网络连接的安全标识符。因而，过程管理器模块114可以轻易地确定什么访问被允许并相应地达到。如前所述，还设想了各种其他示例，例如确定基于通过标记212的枚举来确定允许哪个访问。

[0055] 图6描绘了示例实施方式的过程600，其中探测网络来识别代理服务器或子网，该过程用来辅助管理给予过程的网络能力访问。网络被探测来识别代理服务器或子网(框602)。这可以通过形成一个或多个将被发送到服务器的传输、检测网络设置等来执行。

[0056] 基于对代理服务器或子网的识别以及与在计算设备上执行的过程相关的标记的审查来管理该过程对网络的网络能力的访问，所述标记具有一个或多个安全标识符，该一个或多个安全标识符引用在清单中描述的允许过程使用的网络能力(框604)。如前，过程管理器模块114可以通过使用标记来管理访问，该标记“指明”允许与该标记相关的过程访问哪些能力。进一步地，该标记可以用来确保对网络的访问与该枚举相一致，例如该访问准确地反映处设备是否经由子网或因特网等可访问的。还设想了各种其他示例。

[0057] 示例系统和设备

[0058] 图7示出了包括如参考图1描述的计算设备102的示例系统700。当在个人计算机(PC)、电视设备和/或移动设备上运行应用时，示例系统700实现了用于无缝用户体验过的普适环境。当使用应用、播放视频游戏、观看视频等等时，服务和应用在所有三个环境中运行基本类似以用于在从一个设备转变到下一个设备时的共同的用户体验。

[0059] 在示例系统700中，多个设备通过中央计算设备互连。该中央计算设备可以是多个设备本地的，或者可以远离所述多个设备。在一个实施例中，中央计算设备可以是一个或多个服务器计算机的云，其通过网络、因特网或其他数据通信链路连接到多个设备。在一个实施例中，该互连架构使得功能能够跨多个设备递送来向多个设备的用户提供共同的和无缝的体验。多个设备的每一个可以具有不同的物理要求和能力，并且中央计算设备使用平台来实现对设备的体验的递送，该体验既对该设备是定制的又对所有设备是共同的。在一个实施例中，创建一类目标设备并且对设备通用类定制体验。一类设备可以由设备的物理特征、使用类型或其他共同特征来定义。

[0060] 在各种实施方式中，计算设备102可以采取各种不同的配置，例如以用于计算机702、移动装置704和电视706。这些配置的每一个包括可以具有一般不同的构造和能力的设备，并且因而计算设备102可以根据不同设备类的一个或多个来配置。例如，计算设备102可以实现为设备的计算机702类，其包括个人计算机、桌面计算机、多屏幕计算机、膝上计算机、上网本、等等。

[0061] 计算设备102还可以被实现为设备的移动装置704类，其包括诸如移动电话、便携式音乐播放器、便携式游戏设备、平板计算机、多屏幕计算机等的移动设备。计算设备102还可以实现为设备的电视706类，其包括具有或连接到随意查看环境中的通常较大的屏幕的设备。这些设备包括电视、机顶盒、游戏机、等等。本文中描述的技术可以得到计算设备102的这些各种配置的支持并且不限于本文中描述的技术的特定示例。

[0062] 云708包括和/或代表用于内容服务712的平台710。该平台710抽象云708的硬件(例如服务器)和软件资源的底层功能。内容服务712可以包括可以被使用的应用和/或数据，同时计算机处理在远离计算设备102的服务器上执行。内容服务712可以被提供为通过因特网和/或用户网络(例如蜂窝网络或Wi-Fi网络)的服务。

[0063] 平台710可以抽象资源和功能来将计算设备102与其他计算设备相连接。平台710还可以用来抽象资源的缩放(scaling)以提供对于所遇到的经由平台710实现的内容服务712的需求的相应规模(scale)等级。相应地，在互连的设备实施例中，对于本文中描述的功能的功能实现可以遍及系统700分布。例如，功能可以部分实现在计算设备102上以及部分经由抽象云708的功能的平台710实现。

[0064] 图8示出示例设备800的各种组件，该示例设备800可以实现为如参考图1、2和7所述的任意类型的计算设备以实现本文中描述的技术的实施例。设备800包括通信设备802，其使得能够有线和/或无线地传输设备数据804(例如，已接收的数据，正在被接收的数据、计划用于广播的数据、数据的数据分组等)。设备数据804或其他设备内容可以包括设备的配置设置、存储在设备上的媒体内容和/或与设备的用户相关的信息。存储在设备800上的媒体内容可以包括任意类型的音频、视频和/或图像数据。设备800包括一个或多个数据输入806，经由其可以接收任意类型的数据、媒体内容和/或输入，例如用户可选的输入、消息、音乐、电视媒体内容、记录的视频内容和从任意内容和/或数据源接收的任意其他类型的音频、视频和/或图像数据。

[0065] 设备800还包括通信接口808，其可以实现为串行和/或并行接口、无线接口、任意类型的网络接口、调制解调器的任意一个或多个，或实现为任意其他类型的通信接口。通信接口808提供了设备800和通信网络之间的连接和/或通信链路，其他电子、计算和通信设备通过该连接和/或通信链路与设备800进行通信。

[0066] 设备800包括一个或多个处理器810(例如，任意微处理器、控制器等)，其处理各种计算机可执行指令来控制设备800的操作并实现本文中描述的技术的实施例。可替换地或附加地，设备800可以用硬件、固件或固定逻辑电路的任意一个或组合来实现，该固定逻辑电路通常与在812处标识的处理和控制电路相连接。虽然未示出，但是设备800可以包括耦接设备中各种组件的系统总线或数据传送系统。系统总线可以包括不同总线结构的任意一个或组合，例如存储器总线或存储器控制器、外围总线、通用串行总线和/或使用任意各种架构的处理器或局部总线。

[0067] 设备800还包括计算机可读介质814，例如一个或多个存储器组件，其示例包括随机存取存储器(RAM)、非易失性存储器(例如，只读存储器(ROM)、闪存存储器、EPROM、EEPROM等的任意一个或多个)以及磁盘存储设备。磁盘存储设备可以实现为任意类型的磁或光学存储设备，例如硬盘驱动器、可记录和/或可重写光盘(CD)、任意类型的数字化通用盘(DVD)，等等。设备800还可以包括大规模存储介质设备816。

[0068] 计算机可读介质814提供数据存储机制来存储设备数据804，以及各种设备应用818和任意其他类型的与设备800的操作方面相关的信息和/或数据。例如，操作系统820可以被维护为具有计算机可读介质814的计算机应用并在处理器810上执行。设备应用818可以包括设备管理器(例如控制应用、软件应用、信号处理和控制模块、特定设备本地的代码、特定设备的硬件抽象层等)。设备应用818还包括任意系统组件或模块来实现本文中描述的技术的实施例。在此示例中，设备应用818包括接口应用822和输入/输出模块824，它们被示出为软件模块和/或计算机应用。输入/输出模块824代表用来向被配置为捕获输入的设备(例如触摸屏、跟踪板、摄像头、麦克风等)提供接口的软件。可替换地或附加地，接口应用822和输入/输出模块824可以实现为硬件、软件、固件或其任意组合。另外，输入/输出模块

824可以被配置为支持多个输入设备，例如单独的设备来分别捕获视觉和音频输入。

[0069] 设备800还包括音频和/或视频输入-输出系统826，其向音频系统828提供音频数据和/或向显示系统830提供视频数据。音频系统828和/或显示系统830可以包括处理、显示和/或用其他方式再现音频、视频和图像数据的任意设备。视频信号和音频信号可以经由RF(射频)链路、S-视频链路、混合视频链路、分量视频链路、DVI(数字视频接口)、模拟视频连接或其他类似的通信链路从设备800传输到音频设备和/或显示设备。在实施例中，音频系统828和/或显示系统830被实现为设备800的外部组件。可替换地，音频系统828和/或显示系统830被实现为示例设备800的集成组件。

[0070] 结论

[0071] 虽然以特定于结构化特征和/或方法学上的行为的语言描述本发明，但是要理解的是，所附权利要求中限定的本发明不必限于所描述的具体特征和行为。相反，这些具体特征和行为以实现所要求保护的发明的示例形式来公开。

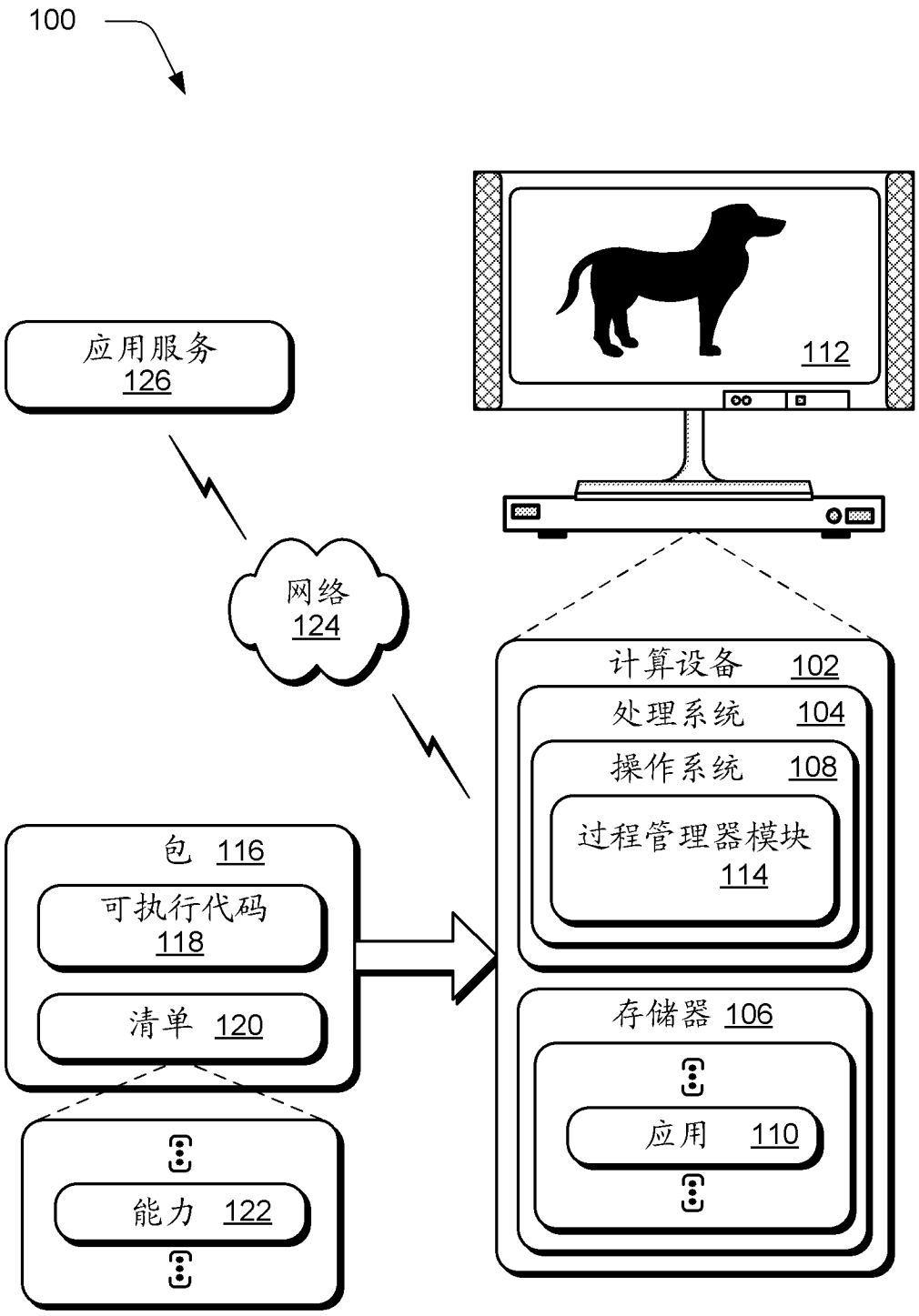

100
112
应用服务
126
网络
124
计算设备 102
处理系统 104
操作系统 108
过程管理器模块
114
包 116
可执行代码
118
清单 120
能力 122
存储器 106
应用 110

图 1

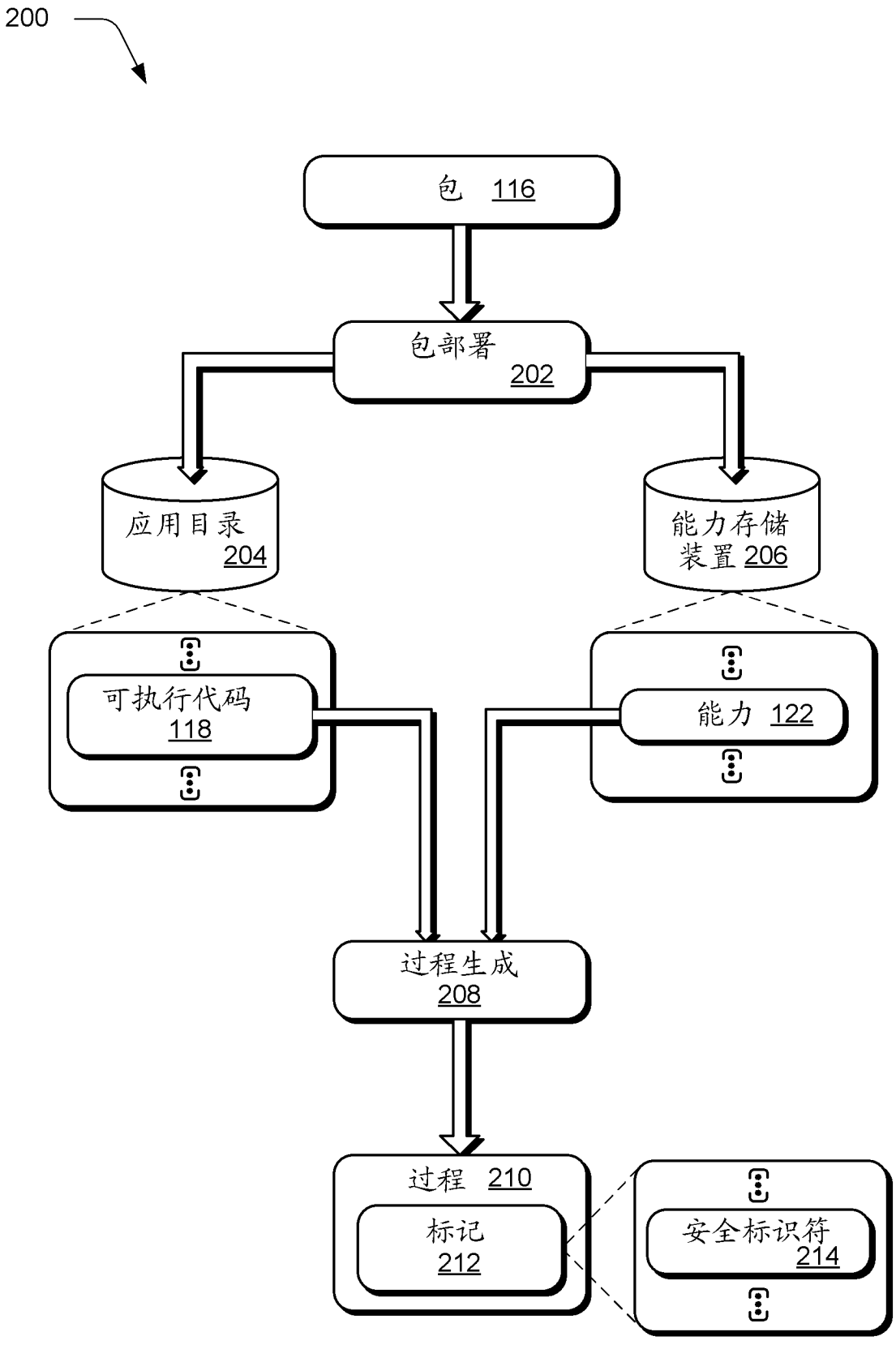

200
包 116
包部署
202
应用目录
204
能力存储
装置 206
可执行代码
118
能力 122
过程生成
208
过程 210
标记
212
安全标识符
214

图 2

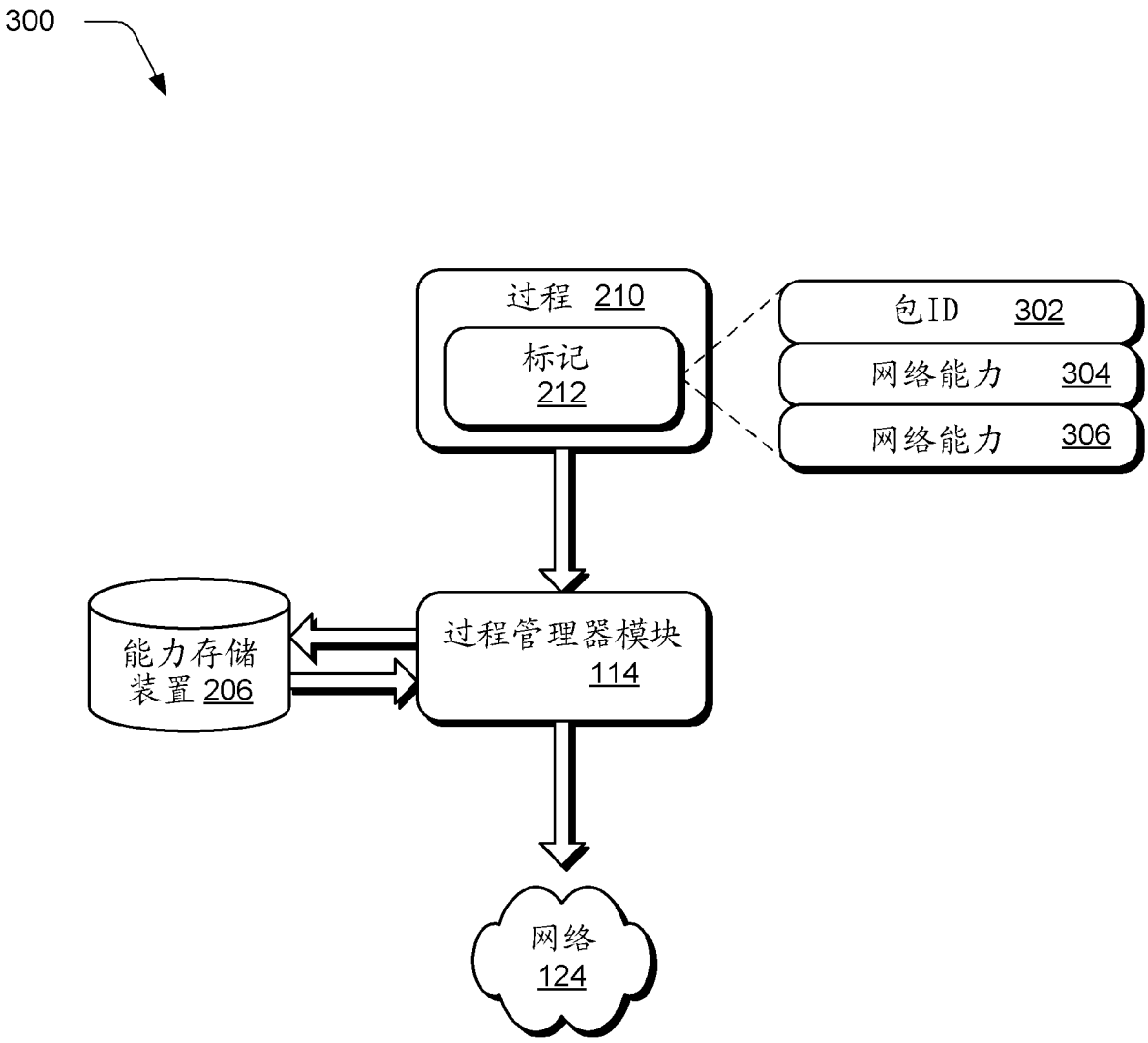

300
过程 210
标记 212
包ID 302
网络能力 304
网络能力 306
能力存储装置 206
过程管理器模块 114
网络 124

图 3

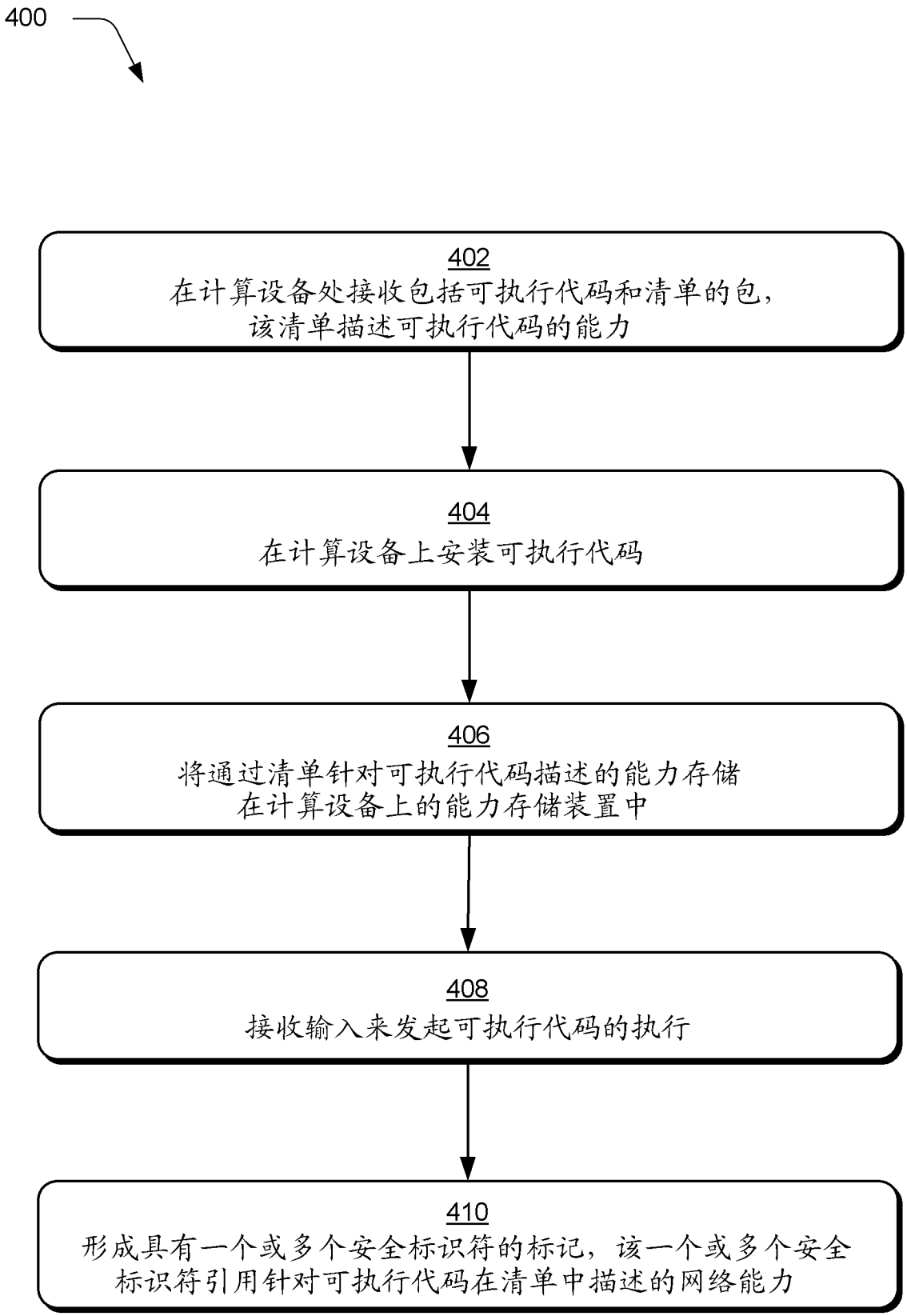

400
402
在计算设备处接收包括可执行代码和清单的包，该清单描述可执行代码的能力
404
在计算设备上安装可执行代码
406
将通过清单针对可执行代码描述的能力存储在计算设备上的能力存储装置中
408
接收输入来发起可执行代码的执行
410
形成具有一个或多个安全标识符的标记，该一个或多个安全标识符引用针对可执行代码在清单中描述的网络能力

图 4

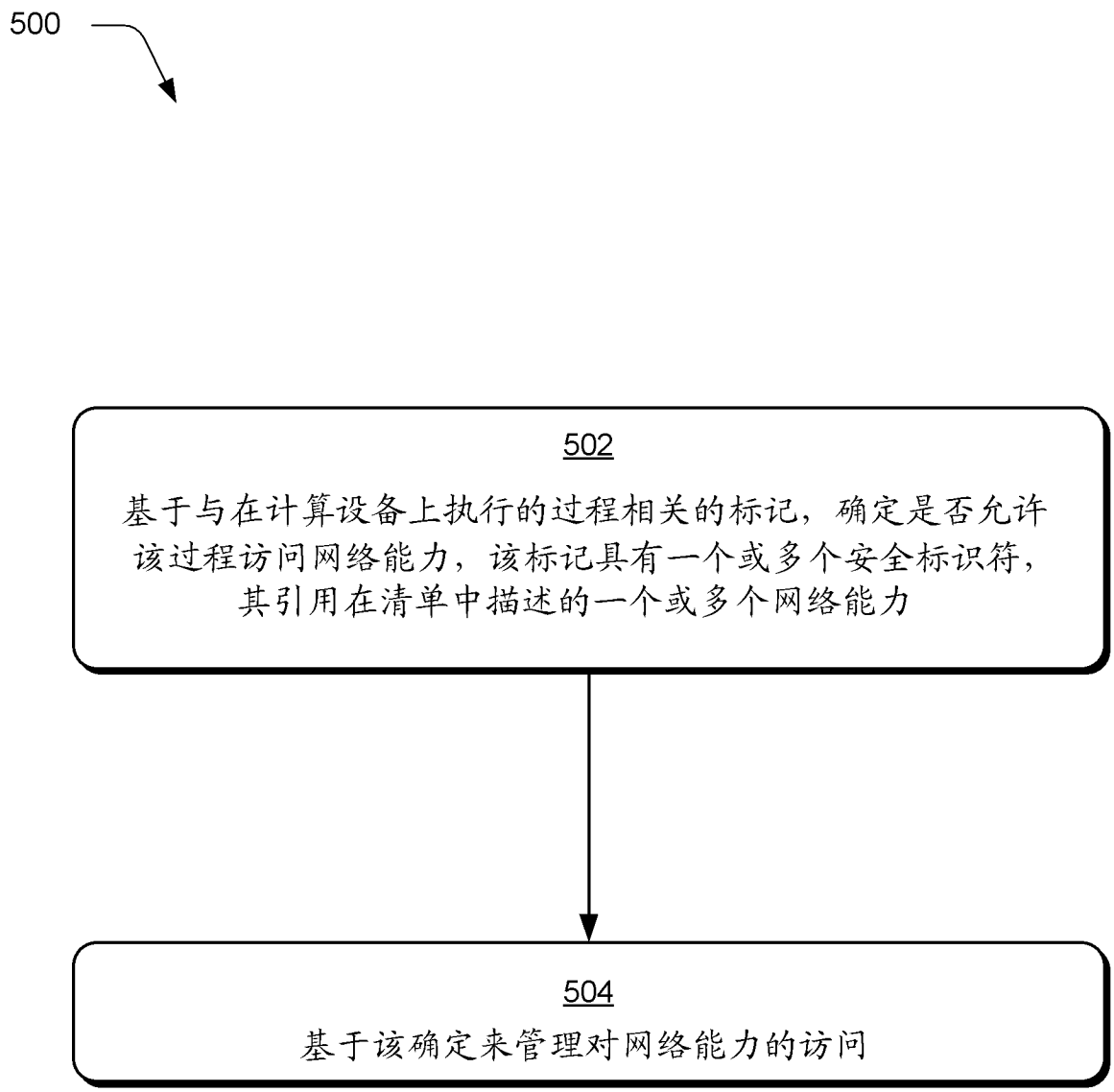

500
502
基于与在计算设备上执行的过程相关的标记，确定是否允许该过程访问网络能力，该标记具有一个或多个安全标识符，其引用在清单中描述的一个或多个网络能力
504
基于该确定来管理对网络能力的访问

图 5

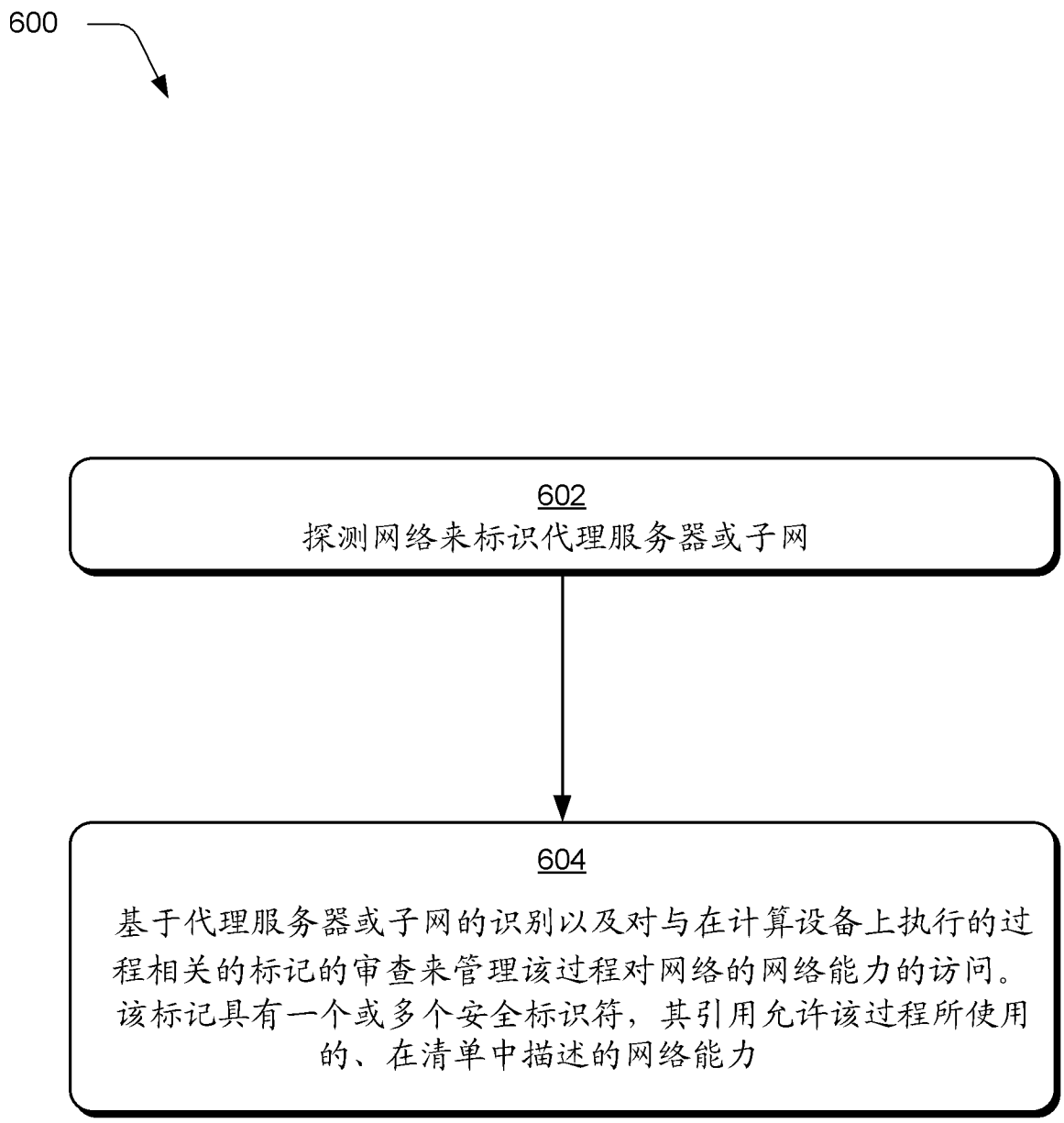

600
602
探测网络来标识代理服务器或子网
604
基于代理服务器或子网的识别以及对与在计算设备上执行的过程相关的标记的审查来管理该过程对网络的网络能力的访问。该标记具有一个或多个安全标识符，其引用允许该过程所使用的、在清单中描述的网络能力

图 6

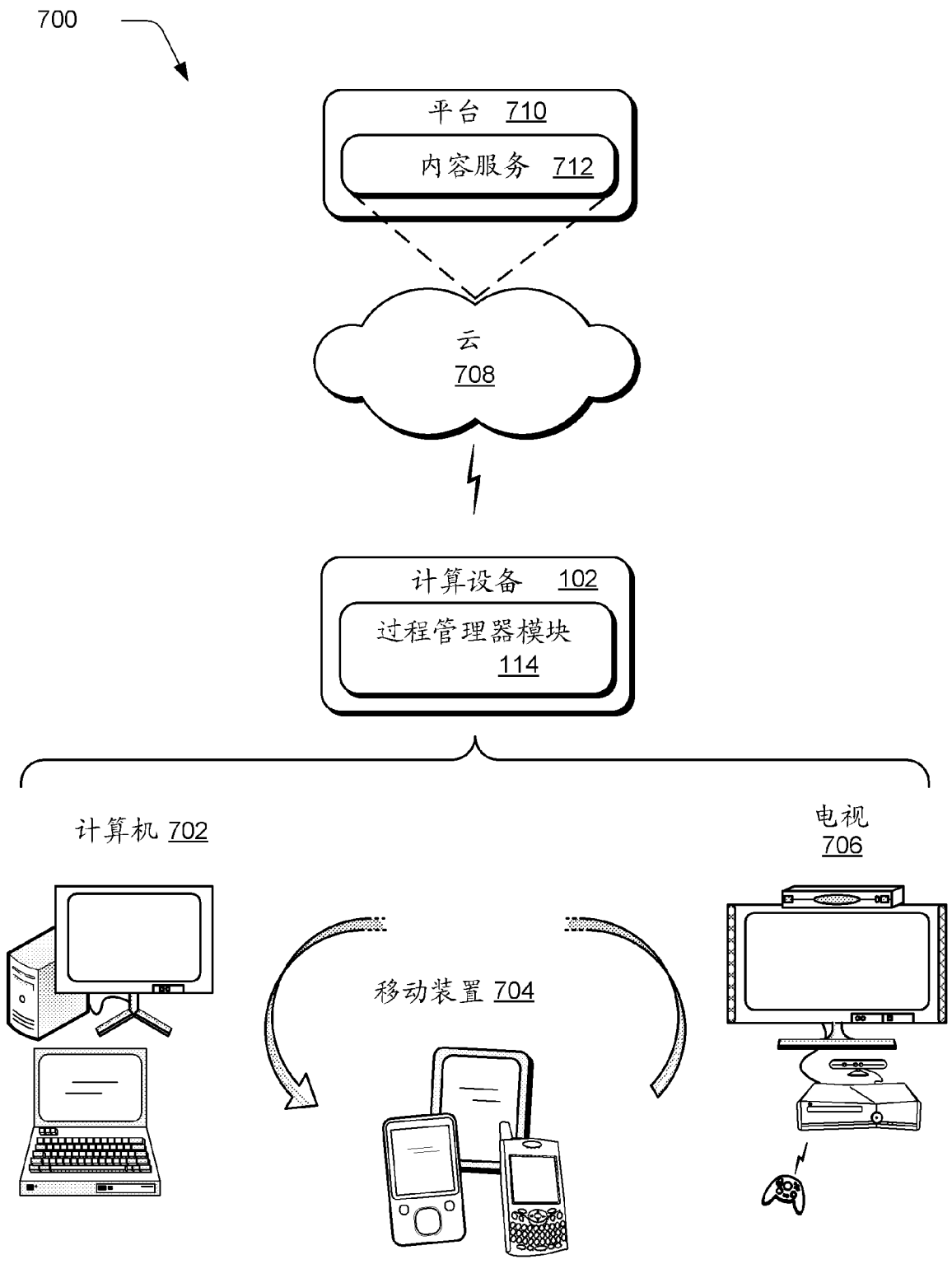

700
平台 710
内容服务 712
云
708
计算设备 102
过程管理器模块
114
计算机 702
移动装置 704
电视
706

图 7

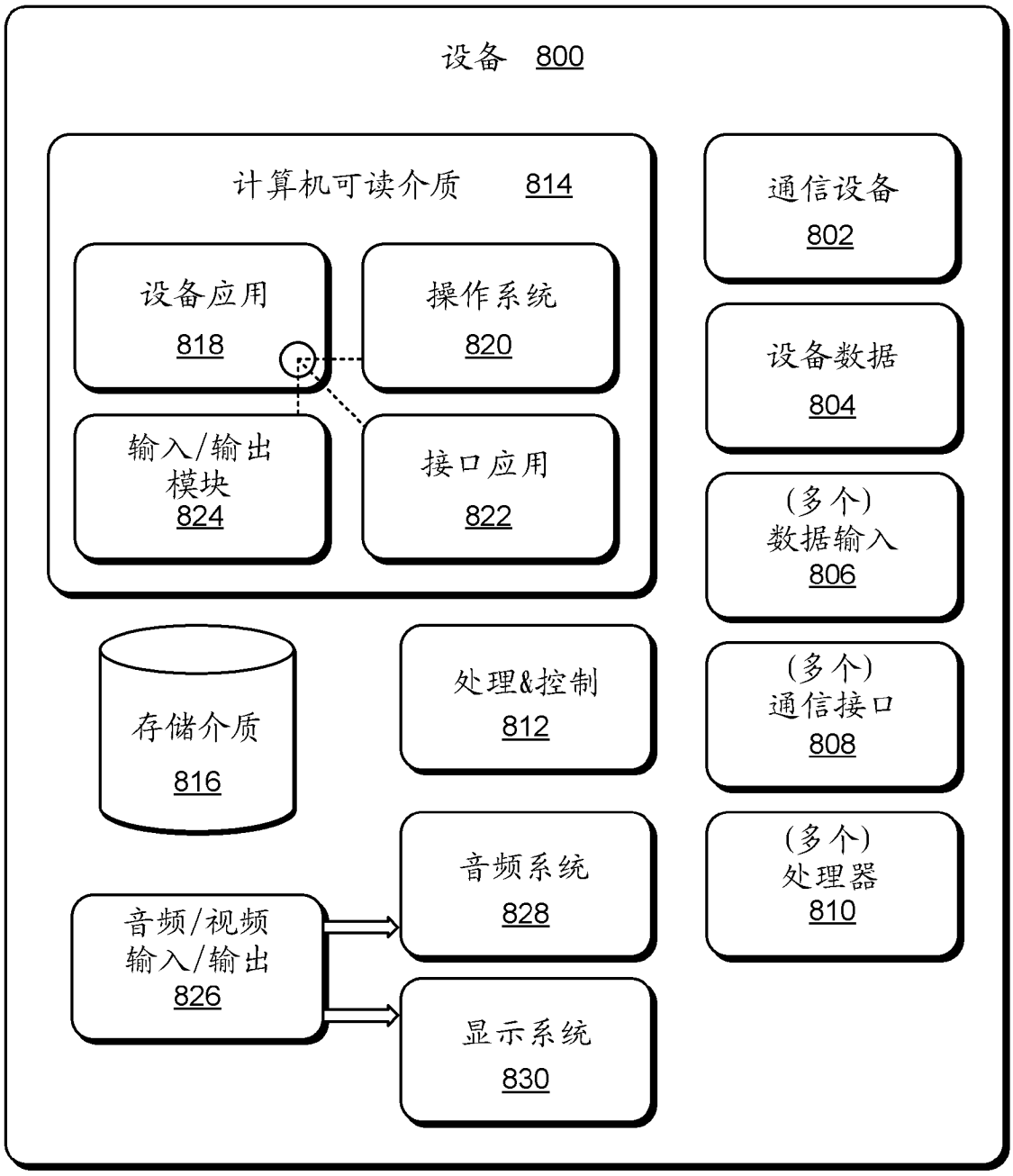

设备 800
计算机可读介质 814
设备应用 818
操作系统 820
输入/输出模块 824
接口应用 822
存储介质 816
处理&控制 812
音频/视频输入/输出 826
音频系统 828
显示系统 830
通信设备 802
设备数据 804
(多个)数据输入 806
(多个)通信接口 808
(多个)处理器 810

图 8