



(12) 发明专利

(10) 授权公告号 CN 107438081 B

(45) 授权公告日 2021.08.06

(21) 申请号 201710770819.X

(22) 申请日 2012.10.18

(65) 同一申请的已公布的文献号  
申请公布号 CN 107438081 A

(43) 申请公布日 2017.12.05

(30) 优先权数据  
13/284,475 2011.10.28 US

(62) 分案原申请数据  
201280064750.4 2012.10.18

(73) 专利权人 谷歌有限责任公司  
地址 美国加利福尼亚州

(72) 发明人 殷莉 帕兰姆·雷达帕加里  
马尤尔·卡马特 左正平 张宏

(74) 专利代理机构 中原信达知识产权代理有限  
责任公司 11219

代理人 周亚荣 安翔

(51) Int.Cl.  
H04L 29/06 (2006.01)  
G06F 21/57 (2013.01)  
G06F 21/62 (2013.01)

(56) 对比文件  
CN 1901475 A, 2007.01.24  
CN 100568212 C, 2009.12.09  
CN 101069157 A, 2007.11.07  
CN 101488138 A, 2009.07.22  
US 2003135755 A1, 2003.07.17

审查员 刘耀瑞

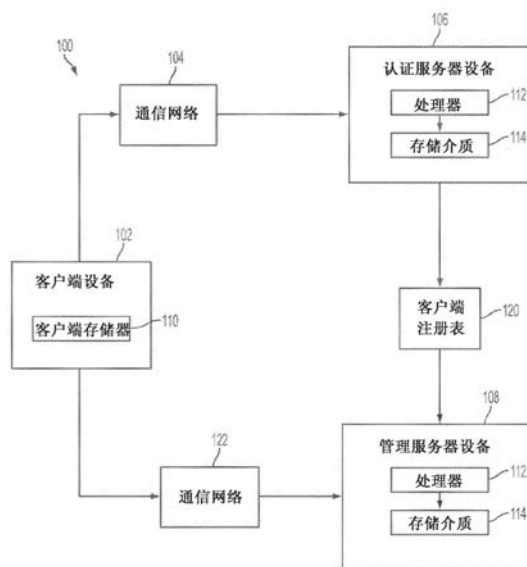
权利要求书5页 说明书7页 附图6页

(54) 发明名称

客户端设备的策略执行

(57) 摘要

本申请涉及客户端设备的策略执行。一种方法可包括由客户端设备向认证服务器设备发送访问请求。该访问请求可包括用以访问被管理资源的请求。该方法可包括响应于客户端设备不遵守与被管理资源相关联的管理策略而从认证服务器设备接收关于安装客户端应用的一个或多个指令，由客户端设备根据该指令来接收客户端应用，并将客户端应用安装在客户端设备上。



1. 一种用于认证服务器设备的策略执行的方法,包括:

从客户端设备接收对于被管理资源的第一访问请求,所述被管理资源服从控制对所述被管理资源的访问的管理策略,所述第一访问请求包括所述客户端设备的唯一标识符;

至少部分地基于所述唯一标识符和客户端注册表来确定所述客户端设备是否遵守所述管理策略,其中,所述客户端注册表包括多个客户端设备的唯一标识符以及与所述多个客户端设备中的每个客户端设备的相应唯一标识符相关联的指示客户端设备是否遵守所述管理策略的状态,其中,只要所述客户端设备按响应时间或在所述响应时间之后的某个时间段内发送通信、在一时间段内发送一定数目的通信或一定百分比的通信、或者发送一定数目的连续通信,所述状态即被保持为遵守所述管理策略;

响应于确定所述客户端设备不遵守所述管理策略,使得所述客户端设备安装客户端应用,所述客户端应用被配置来将所述管理策略应用于所述客户端设备;

从所述客户端设备接收对于所述被管理资源的第二访问请求,所述第二访问请求包括所述客户端设备的所述唯一标识符和登录信息;

基于所述第二访问请求中所包括的所述唯一标识符和所述登录信息以及存储在所述客户端注册表中的与所述唯一标识符相关联的所述状态来确定所述客户端设备是否遵守所述管理策略;以及

响应于确定所述客户端设备遵守所述管理策略,向所述客户端设备发送提供对所述被管理资源的访问的令牌。

2. 根据权利要求1所述的方法,其中,使得所述客户端设备安装客户端应用包括:

向所述客户端设备发送包括在所述客户端设备处安装所述客户端应用的指令的一个或多个指令;

从所述客户端设备接收获得所述客户端应用的请求;以及

向所述客户端设备发送所述客户端应用。

3. 根据权利要求1所述的方法,进一步包括:

向所述客户端设备发送包括在所述客户端设备处安装所述客户端应用的指令的一个或多个指令;以及

从在所述客户端设备处执行的所述客户端应用接收所述客户端设备的注册信息,所述注册信息包括以下中的一个或多个:所述客户端设备的所述唯一标识符、所述客户端设备的电话号码、所述客户端设备的用户的名称、或者所述客户端设备的所述用户的地址。

4. 根据权利要求1所述的方法,其中,所述客户端应用被配置来将一个或多个数据安全策略应用于所述客户端设备,所述一个或多个数据安全策略包括以下中的一个或多个:

需要密码来访问所述客户端设备;

需要所述密码来满足一个或多个格式要求;

针对所述客户端设备迫使密码重置;

响应于所述客户端设备在空闲模式下操作一段时间而自动地锁定所述客户端设备;或者

防止所述客户端设备在空闲模式下操作。

5. 根据权利要求1所述的方法,其中,确定所述客户端设备是否遵守所述管理策略包括:

确定所述唯一标识符是否存储在所述客户端注册表中;以及

响应于确定所述唯一标识符存储在所述客户端注册表中,基于存储在所述客户端注册表中的与所述唯一标识符相关联的所述状态来确定所述客户端设备是否遵守所述管理策略。

6. 根据权利要求1所述的方法,其中,确定所述客户端设备是否遵守所述管理策略包括:

确定所述唯一标识符是否存储在所述客户端注册表中;以及

响应于确定所述唯一标识符没有存储在所述客户端注册表中,确定所述客户端设备不遵守所述管理策略。

7. 根据权利要求1所述的方法,进一步包括:

响应于确定所述客户端设备遵守所述管理策略,更新所述客户端注册表以指示所述客户端设备遵守所述管理策略。

8. 一种用于认证服务器设备的策略执行的计算系统,包括:

一个或多个处理器;

一个或多个通信端口;

存储器,存储客户端注册表和指令,所述指令在被执行时使得所述一个或多个处理器:

经由所述一个或多个通信端口从客户端设备接收对于被管理资源的第一访问请求,所述被管理资源服从控制对所述被管理资源的访问的管理策略,所述第一访问请求包括所述客户端设备的唯一标识符;

至少部分地基于所述唯一标识符和所述客户端注册表来确定所述客户端设备是否遵守所述管理策略,其中,所述客户端注册表包括多个客户端设备的唯一标识符以及与所述多个客户端设备中的每个客户端设备的相应唯一标识符相关联的指示客户端设备是否遵守所述管理策略的状态,其中,只要所述客户端设备按响应时间或在所述响应时间之后的某个时间段内发送通信、在一时间段内发送一定数目的通信或一定百分比的通信、或者发送一定数目的连续通信,所述状态即被保持为遵守所述管理策略;

响应于确定所述客户端设备不遵守所述管理策略,使得所述客户端设备安装客户端应用,所述客户端应用被配置来将所述管理策略应用于所述客户端设备;

经由所述一个或多个通信端口从所述客户端设备接收对于所述被管理资源的第二访问请求,所述第二访问请求包括所述客户端设备的所述唯一标识符和登录信息;

基于所述第二访问请求中所包括的所述唯一标识符和所述登录信息以及存储在所述客户端注册表中的与所述唯一标识符相关联的所述状态来确定所述客户端设备是否遵守所述管理策略;以及

响应于确定所述客户端设备遵守所述管理策略,经由所述一个或多个通信端口向所述客户端设备发送提供对所述被管理资源的访问的令牌。

9. 根据权利要求8所述的计算系统,其中,所述指令进一步使得所述一个或多个处理器:

经由所述一个或多个通信端口向所述客户端设备发送包括在所述客户端设备处安装所述客户端应用的指令的一个或多个指令;

经由所述一个或多个通信端口从所述客户端设备接收获得所述客户端应用的请求;以

及

经由所述一个或多个通信端口向所述客户端设备发送所述客户端应用。

10. 根据权利要求8所述的计算系统, 其中, 所述指令进一步使得所述一个或多个处理器:

经由所述一个或多个通信端口向所述客户端设备发送包括在所述客户端设备处安装所述客户端应用的指令的一个或多个指令; 以及

经由所述一个或多个通信端口从在所述客户端设备处执行的所述客户端应用接收所述客户端设备的注册信息, 所述注册信息包括以下中的一个或多个: 所述客户端设备的所述唯一标识符、所述客户端设备的电话号码、所述客户端设备的用户的名称、或者所述客户端设备的所述用户的地址。

11. 根据权利要求8所述的计算系统, 其中, 所述客户端应用被配置来将一个或多个数据安全策略应用于所述客户端设备, 所述一个或多个数据安全策略包括以下中的一个或多个:

需要密码来访问所述客户端设备;

需要所述密码来满足一个或多个格式要求;

针对所述客户端设备迫使密码重置;

响应于所述客户端设备在空闲模式下操作一段时间而自动地锁定所述客户端设备; 或者

防止所述客户端设备在空闲模式下操作。

12. 根据权利要求8所述的计算系统, 其中, 所述指令进一步使得所述一个或多个处理器:

确定所述唯一标识符是否存储在所述客户端注册表中; 以及

响应于确定所述唯一标识符存储在所述客户端注册表中, 基于存储在所述客户端注册表中的与所述唯一标识符相关联的所述状态来确定所述客户端设备是否遵守所述管理策略。

13. 根据权利要求8所述的计算系统, 其中, 所述指令进一步使得所述一个或多个处理器:

确定所述唯一标识符是否存储在所述客户端注册表中; 以及

响应于确定所述唯一标识符没有存储在所述客户端注册表中, 确定所述客户端设备不遵守所述管理策略。

14. 根据权利要求8所述的计算系统, 其中, 所述指令进一步使得所述一个或多个处理器:

响应于确定所述客户端设备遵守所述管理策略, 更新所述客户端注册表以指示所述客户端设备遵守所述管理策略。

15. 一种编码有指令的非暂时性计算机可读存储介质, 所述指令在被执行时使得计算系统的一个或多个处理器执行用于认证服务器设备的策略执行的方法, 所述方法包括:

从客户端设备接收对于被管理资源的第一访问请求, 所述被管理资源服从控制对所述被管理资源的访问的管理策略, 所述第一访问请求包括所述客户端设备的唯一标识符;

至少部分地基于所述唯一标识符和客户端注册表来确定所述客户端设备是否遵守所

述管理策略,其中,所述客户端注册表包括多个客户端设备的唯一标识符以及与所述多个客户端设备中的每个客户端设备的相应唯一标识符相关联的指示客户端设备是否遵守所述管理策略的状态,其中,只要所述客户端设备按响应时间或在所述响应时间之后的某个时间段内发送通信、在一时间段内发送一定数目的通信或一定百分比的通信、或者发送一定数目的连续通信,所述状态即被保持为遵守所述管理策略;

响应于确定所述客户端设备不遵守所述管理策略,使得所述客户端设备安装客户端应用,所述客户端应用被配置来将所述管理策略应用于所述客户端设备;

从所述客户端设备接收对于所述被管理资源的第二访问请求,所述第二访问请求包括所述客户端设备的所述唯一标识符和登录信息;

基于所述第二访问请求中所包括的所述唯一标识符和所述登录信息以及存储在所述客户端注册表中的与所述唯一标识符相关联的所述状态来确定所述客户端设备是否遵守所述管理策略;以及

响应于确定所述客户端设备遵守所述管理策略,向所述客户端设备发送提供对所述被管理资源的访问的令牌。

16. 根据权利要求15所述的非暂时性计算机可读存储介质,其中,所述方法进一步包括:

向所述客户端设备发送包括在所述客户端设备处安装所述客户端应用的指令的一个或多个指令;

从所述客户端设备接收获得所述客户端应用的请求;以及

向所述客户端设备发送所述客户端应用。

17. 根据权利要求15所述的非暂时性计算机可读存储介质,其中,所述方法进一步包括:

向所述客户端设备发送包括在所述客户端设备处安装所述客户端应用的指令的一个或多个指令;以及

从在所述客户端设备处执行的所述客户端应用接收所述客户端设备的注册信息,所述注册信息包括以下中的一个或多个:所述客户端设备的所述唯一标识符、所述客户端设备的电话号码、所述客户端设备的用户的名称、或者所述客户端设备的所述用户的地址。

18. 根据权利要求15所述的非暂时性计算机可读存储介质,其中,所述方法进一步包括:

确定所述唯一标识符是否存储在所述客户端注册表中;以及

响应于确定所述唯一标识符存储在所述客户端注册表中,基于存储在所述客户端注册表中的与所述唯一标识符相关联的所述状态来确定所述客户端设备是否遵守所述管理策略。

19. 根据权利要求15所述的非暂时性计算机可读存储介质,其中,所述方法进一步包括:

确定所述唯一标识符是否存储在所述客户端注册表中;以及

响应于确定所述唯一标识符没有存储在所述客户端注册表中,确定所述客户端设备不遵守所述管理策略。

20. 根据权利要求15所述的非暂时性计算机可读存储介质,其中,所述方法进一步包

括：

响应于确定所述客户端设备遵守所述管理策略，更新所述客户端注册表以指示所述客户端设备遵守所述管理策略。

## 客户端设备的策略执行

### [0001] 分案说明

[0002] 本申请属于申请日为2012年10月18日的中国发明专利申请No.201280064750.4的分案申请。

### 背景技术

[0003] 手持式移动设备已变成用于访问计算机网络上的信息的有效工具。雇员越来越多地使用其移动设备来远程地访问公司信息、应用及其他资源。然而,如果雇员的移动设备未至少如雇主策略那样严格地遵守数据安全策略或访问策略,则敏感的公司信息可能易受到未授权访问。例如,如果雇员丢失其移动设备并且该移动设备未被密码保护,则发现该移动设备的任何人可以能够使用该移动设备来访问公司信息。

### 发明内容

[0004] 在一个实施例中,一种方法可以包括由客户端设备向认证服务器设备发送访问请求。该访问请求可以包括用以访问被管理资源的请求。该方法可以包括响应于客户端设备未遵守与被管理资源相关联的管理策略而从认证服务器设备接收关于安装客户端应用的一个或多个指令,由客户端设备根据该指令来接收客户端应用,并将客户端应用程序安装在客户端设备上。

[0005] 在一个实施例中,一种方法可以包括从客户端设备接收对被管理资源的访问请求,确定客户端设备是否遵守与被管理资源相关联的管理策略,响应于客户端设备遵守管理策略,向客户端设备发送令牌,并且响应于客户端设备不遵守管理策略,向客户端设备发送命令客户端设备如何遵守管理策略的一个或多个指令。

[0006] 在一个实施例中,一种方法可以包括从客户端设备接收用以访问客户端应用的请求。可将客户端应用配置成对客户端设备应用管理策略。该方法可以包括向客户端设备发送客户端应用并用指示客户端设备遵守管理策略的信息来更新客户端注册表。

[0007] 在一个实施例中,一种系统可以包括与客户端设备通信的认证服务器设备。可将认证服务器设备配置成确定客户端设备是否被允许访问一个或多个被管理资源。该系统可以包括与客户端设备和认证服务器设备通信的管理服务器设备。可将该管理服务器设备配置成确定客户端设备是否遵守控制客户端设备访问一个或多个被管理资源的能力的管理策略。

### 附图说明

[0008] 图1图示了根据一个实施例的用于对客户端设备进行认证和/或对客户端设备应用管理策略的系统。

[0009] 图2-4图示了根据某些实施例的对客户端设备进行认证和/或对客户端设备应用管理策略的方法。

[0010] 图5图示了根据一个实施例的可在客户端设备上显示的关于客户端应用的信息。

[0011] 图6图示了根据一个实施例的可用来包含或实现程序指令的内部硬件的框图。

### 具体实施方式

[0012] 本公开不限于所述的特定系统、设备和方法,因为这些可改变。在本描述中所使用的术语仅仅用于描述特定版本或实施例的目的,并且并不意图限制范围。

[0013] 在本文中所使用的单数形式“一”、“一个”和“该”意图也包括复数引用,除非上下文另外明确地指示。除非另外定义,本文所使用的所有技术和科学术语具有与本领域的技术人员一般理解的相同的意义。不应将本公开中的任何内容理解为在本公开中所述的实施例没有资格借助于现有发明使此类公开提前发生的许可。在本文中所用的术语“包括”意指“包括但不限于”。

[0014] 出于本申请的目的,以下术语应具有下面所阐述的相应意义:

[0015] “计算设备”指的是根据一个或多个编程指令来执行一个或多个操作的电子设备。

[0016] “客户端设备”指的是被配置成通过网络来访问一个或多个被管理资源的计算设备。客户端设备可以是便携式或移动电子设备。客户端设备可在没有限制的情况下包括计算机、因特网信息亭、个人数字助理、蜂窝电话、游戏设备、台式计算机、膝上型计算机、平板计算机等。

[0017] “认证服务器设备”指的是被配置成确定客户端设备是否遵守管理策略的计算设备。认证服务器设备可在没有限制的情况下包括服务器、主机计算机、联网计算机、基于处理器的设备、虚拟机等。

[0018] “管理服务器设备”指的是被配置成对客户端设备应用管理策略的计算设备。管理策略设备可在没有限制的情况下包括服务器、主机计算机、联网计算机、基于处理器的设备、虚拟机等。

[0019] “管理策略”指的是控制客户端设备对一个或多个被管理资源的访问的一个或多个规则、策略、方针等。

[0020] “被管理资源”指的是由管理员管理的一个或多个应用程序。

[0021] “客户端应用”指的是被配置成命令客户端设备执行一个或多个任务的应用程序。

[0022] 图1图示了根据一个实施例的用于对客户端设备进行认证和/或对客户端设备应用管理策略的系统100。在实施例中,可将一个或多个客户端设备102连接到一个或多个通信网络104、122。在一个实施例中,客户端设备102可包括客户端存储器110。可将通信网络104连接到认证服务器设备106。在一个实施例中,可将通信网络122连接到管理服务器设备108。

[0023] 在一个实施例中,通信网络104、122可以是局域网(LAN)、广域网(WAN)等。例如,通信网络104、122可以是外部网、内部网、因特网等。在一个实施例中,通信网络104、122可提供客户端设备102、认证服务器设备106和/或管理服务器设备108之间的通信能力。

[0024] 在一个实施例中,通信网络104、122可使用超文本传输协议(HTTP)或使用传输控制协议/网际协议(TCP/IP)来传送信息。HTTP可允许客户端设备102访问经由通信网络104、122可用的资源。

[0025] 在一个实施例中,认证服务器设备106可包括与计算机可读存储介质114通信的处理器112。认证服务器设备106可与一个或多个客户端设备102和/或管理服务器设备108通



信。虽然被描述为单个计算机系统,但可将认证服务器设备106实现为计算机处理器网络。

[0026] 在一个实施例中,管理服务器设备108可包括与计算机可读存储介质114通信的处理器112。管理服务器设备108可与一个或多个客户端设备102和/或认证服务器设备106通信。虽然被描述为单个计算机系统,但可将管理服务器设备108实现为计算机处理器网络。管理服务器设备108的示例可包括服务器、主机计算机、联网计算机、基于处理器的设备等。

[0027] 在一个实施例中,认证服务器设备106和/或管理服务器设备108可与客户端注册表120通信。客户端注册表可包括与客户端是否遵守管理策略相关联的信息。在一个实施例中,客户端注册表可以是数据库或其他计算机可读存储介质。可将客户端注册表120存储在认证服务器设备106、管理服务器设备108和/或另一计算设备上。

[0028] 图2图示了根据一个实施例的用于对客户端设备进行认证和对客户端设备应用管理策略的方法。在一个实施例中,客户端设备可以尝试200访问一个或多个被管理资源。被管理资源可以是由不是客户端设备用户的管理员管理的软件应用。例如,电子邮件应用、文字处理应用和日历应用可以是被管理资源的示例,并且这些资源可由雇主管理员管理。在本公开的范围内可使用附加和/或替选管理员。

[0029] 在一个实施例中,客户端设备可尝试200响应于用户选择客户端设备上的被管理资源的图标、图形、链接或其他表示而访问被管理资源。在一个实施例中,客户端设备可尝试响应于客户端设备用户提供与被管理资源相关联的诸如用户名和/或密码之类的登录信息而访问被管理资源。

[0030] 在一个实施例中,客户端设备可向认证服务器设备发送202对被管理资源的访问请求。访问请求可包括与正在请求访问的客户端设备相关联的标识符。在一个实施例中,访问请求可包括客户端设备正在请求访问的一个或多个被管理资源。该访问请求可包括加密的密码或其他加密信息。

[0031] 图3图示了根据一个实施例的由认证服务器设备对客户端设备进行认证的方法。如图3所示,认证服务器设备可接收300访问请求,并且可验证302客户端设备是否服从管理策略。在一个实施例中,管理策略可包括客户端设备必须满足以便访问一个或多个被管理资源的一个或多个规则、条件等。在一个实施例中,管理策略可包括一个或多个数据安全策略。示例性数据安全策略可包括从丢失或被盗客户端设备远程地擦除数据,在一段时间的不活动之后将空闲客户端设备锁定,要求用以访问客户端设备的密码,为一个或多个客户端密码设置最小长度,要求具有某个格式的密码等。在一个实施例中,可针对一组被管理资源来管理管理策略。例如,同一组数据安全策略可应用于与雇主相关联的所有被管理资源。替选地,可使每个被管理资源与不同的管理策略相关联。例如,可使第一被管理资源与第一管理策略相关联,而可使第二被管理资源与第二管理策略相关联。

[0032] 在一个实施例中,认证服务器可通过分析客户端注册表来验证302客户端设备是否服从管理策略。客户端注册表可包括客户端的列表和与每个相关联的状态。例如,客户端注册表可包括与注册表中的每个客户端相关联的唯一标识符以及用于每个客户端的关于客户端设备是否遵守管理策略的状态。示例性唯一标识符可包括与客户端设备相关联的序号或其他唯一字母数字标识符。表1图示了根据实施例的示例性客户端注册表。

[0033]

客户端设备	标识符	遵守管理
客户端设备1	245XCY23	是

客户端设备2	871FGB10	否
客户端设备3	3JB9082NB	是

[0034] 在一个实施例中,在接收到访问请求时,认证服务器可将访问请求中接收到的信息的至少一部分与客户端注册表中的信息相比较304。例如,认证服务器可将访问请求中的客户端标识符与客户端注册表相比较304以便确定正在请求访问的客户端设备是否已服从管理策略、遵守管理策略等。

[0035] 在一个实施例中,如果在访问请求中接收到的该部分信息与来自自己认证客户端设备的列表的信息匹配并且客户端注册表指示客户端设备遵守管理策略306,则认证服务器可向客户端设备发送308令牌。例如,参考表1,认证服务器设备可响应于从客户端设备1接收到访问请求而向客户端设备1发送308令牌,因为客户端设备1被列在客户端注册表中并被客户端注册表识别为遵守管理策略。

[0036] 在一个实施例中,客户端设备可从认证服务器设备接收204令牌。在一个实施例中,客户端设备可206使用该令牌来访问一个或多个被管理资源。在一个实施例中,只有具有令牌的那些设备可被允许访问一个或多个被管理资源。

[0037] 在一个实施例中,如果在访问请求中接收到的该部分信息不与来自客户端注册表的信息匹配310,则可向管理员发送312通知。该通知可请求管理员批准或拒绝该请求。例如,可向管理员发送包括关于访问请求的信息的电子邮件。可要求管理员批准或拒绝该请求。如果该请求被拒绝,则可告知客户端用户访问已被拒绝。如果该请求被批准,则认证服务器设备可向客户端设备发送314一个或多个指令,如下所述。

[0038] 在一个实施例中,如果在访问请求中接收到的该部分信息不与来自客户端注册表310的信息匹配,或者如果该部分信息与来自客户端注册表的信息匹配但客户端注册表指示客户端不遵守管理策略318,则认证服务器可向客户端设备发送314一个或多个指令。例如,参考表1,认证服务器设备可响应于从客户端设备4接收到访问请求而向客户端设备4发送314一个或多个指令,因为与客户端设备4相关联的唯一标识符未被包括在客户端注册表中。作为另一示例,认证服务器设备可响应于从客户端设备2接收到访问请求而向客户端设备2发送314一个或多个指令,因为客户端注册表指示客户端设备2不遵守管理策略。

[0039] 在一个实施例中,所述一个或多个指令可被客户端设备接收到208。该指令可向客户端设备和/或客户端设备的用户命令210客户端设备如何能够遵守管理策略。例如,所述一个或多个指令可命令210客户端设备从某个位置将客户端应用下载到客户端设备以便对客户端设备应用管理策略。在一个实施例中,所述一个或多个指令可使得文本显示在客户端设备的显示器上。该文本可告知客户端设备的用户如何对客户端设备应用管理策略。例如,该文本可告知用户必须从某个位置下载客户端应用以便对客户端应用管理策略。

[0040] 在一个实施例中,客户端应用可向管理服务器设备发送212请求以获得客户端应用。该请求可被管理服务器设备接收400。管理服务器设备可将客户端应用存储在与管理服务器设备相关联的存储器中。在一个实施例中,客户端设备可响应于用户选择与客户端应用相关联的图标、图形、链接或其他表示而向管理服务器设备发送212请求。例如,用户可从网页、诸如应用市场等选择与客户端应用相关联的图标。在一个实施例中,可要求用户购买客户端应用。在替选实施例中,用户可免费接收客户端应用。

[0041] 在一个实施例中,管理服务器设备可向可接收214客户端应用的客户端设备发送

402客户端应用。可将该客户端应用安装216在客户端设备上并且其可与管理服务器设备通信218。例如,客户端设备可向管理服务器设备注册。在一个实施例中,客户端设备的用户可向管理服务器设备提供注册信息。注册信息可包括与客户端设备相关联的唯一标识符、与客户端设备相关联的电话号码、用户的姓名、用户的地址等。在一个实施例中,注册信息可在没有用户交互的情况下由客户端设备自动地提供。

[0042] 在一个实施例中,管理服务器设备可存储404与已接收到客户端应用的一个或多个客户端设备相关联的注册信息。在一个实施例中,管理服务器设备可将注册信息的至少一部分存储404在客户端注册表中。例如,如果未包括在客户端注册表中的客户端下载客户端应用,则管理服务器设备可向客户端注册表添加关于客户端设备的信息,诸如例如唯一标识符。管理服务器设备还可向客户端注册表添加客户端设备遵守管理策略的指示。

[0043] 在一个实施例中,客户端应用可对客户端应用220与客户端应用相关联的管理策略的策略中的一个或多个。例如,如果对客户端设备的访问不要求密码,则客户端应用可提示用户输入用于客户端设备的密码。同样地,如果用于客户端设备的密码不满足管理策略所要求的最小长度或格式,则客户端应用可要求客户端设备用户提供满足此类要求的密码。在一个实施例中,客户端应用可迫使密码重置。该密码可被客户端设备用户重置,或者其可由管理员提供。

[0044] 在一个实施例中,客户端应用可响应于客户端在睡眠模式或其他空闲模式下操作一段时间而自动地锁定客户端设备。在一个实施例中,客户端应用可防止客户端设备在睡眠或其他空闲模式下操作。

[0045] 在一个实施例中,客户端应用可从客户端设备删除、擦除或去除信息。例如,客户端应用可在客户端设备上执行出厂重置。客户端应用可响应于从管理服务器设备接收到一个或多个指令而从客户端设备去除信息。在一个实施例中,管理服务器设备可发送客户端应用指令以在客户端设备被报告为丢失或被盗的情况下去除数据。在一个实施例中,管理服务器设备可发送客户端应用指令以在客户端设备的用户变得不隶属于管理员的情况下去除数据。例如,雇员离职、被开除或停止为雇主工作,雇主可能希望从雇员的客户端设备去除信息。这样地,前雇员可继续使用他或她的个人客户端设备,即使在他或她的雇佣已终止之后。在一个实施例中,可在不提供任何通知的情况下或者从客户端设备用户接收任何确认的情况下从客户端设备去除信息。

[0046] 图5图示了根据一个实施例的可在客户端设备上显示的关于客户端应用的示例性信息。如图5所示,该信息可包括应用于客户端设备500的一个或多个当前管理策略和/或最近管理策略更新的日期和/或时间502。

[0047] 在一个实施例中,客户端应用可向管理服务器设备通信222客户端设备的一个或多个特征。例如,客户端应用可向管理服务器设备通信222与客户端设备相关联的电话号码、与客户端设备相关联的序列号、到或来自客户端设备的呼叫是否是活动的、与呼叫客户端设备的电话相关联的电话号码、与客户端设备呼叫的电话相关联的电话号码、客户端设备的诸如GPS位置之类的位置等。在一个实施例中,客户端应用可允许诸如管理服务器设备之类的远程设备向诸如USB储存器、SD卡的客户端存储器等进行写入。在一个实施例中,管理服务器设备可监视对客户端的失败登录尝试。客户端应用可要求响应于一定数目的连续失败登录尝试而将与客户端设备相关联的密码重置。

[0048] 在一个实施例中,可将管理策略的更新提供406给客户端设备。例如,如果管理策略改变,则管理服务器设备可向客户端设备发送406已更新的管理策略。在一个替选实施例中,客户端设备可周期性地或定期地查询管理服务器设备或另一设备,以用于对管理策略的更新。

[0049] 在一个实施例中,客户端应用可命令224客户端设备在某些响应时间向管理服务器设备发送通信。例如,客户端应用可命令224客户端设备在每三个小时之后向管理服务器设备发送通信。在一个替选实施例中,客户端应用可命令224客户端设备在一个或多个时间向管理服务器设备发送通信。例如,客户端应用可命令224客户端设备在每天的12:00A.M.、6:00A.M.、12:00P.M.和6:00P.M.向管理服务器设备发送通信。在本公开的范围内可使用附加和/或替选的时间和/或时间段。

[0050] 在一个实施例中,管理服务器设备可确定406通信已被客户端设备接收到。例如,管理服务器设备可确定406通信是否已在某个时间、在某个时间段内等被客户端设备接收到。如果客户端设备未能向管理服务器发送一个或多个通信,则客户端应用可能已被从客户端设备卸载或去除,或者可能有错误。在任一种情况下,都存在客户端设备不再遵守管理策略的风险。

[0051] 在一个实施例中,管理服务器设备可将客户端设备的状态在客户端注册表中保持408为遵守管理策略,只要管理服务器设备按响应时间或在响应时间之后的某个时间段内从客户端设备接收到通信即可。例如,如果客户端设备被调度为在12:00P.M.向管理服务器设备发送通信,则如果管理服务器设备在11:58A.M.和12:02P.M.之间从客户端设备接收到通信,管理服务器设备可将客户端的状态在客户端注册表中保持408为遵守。在本公开的范围内可使用附加和/或替选的时间段。

[0052] 在一个实施例中,如果管理服务器设备未能按响应时间或在响应时间之后的时间段内从客户端设备接收到一个或多个通信,在管理服务器设备可将客户端注册表中的客户端设备的状态变成410不遵守管理策略。例如,如果管理服务器设备没有按响应时间或在响应时间之后的某个时间段内从客户端设备接收到通信,则管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。在一个实施例中,如果在一时间段内未从客户端设备接收到一定数目的通信,管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。例如,如果在24小时的时间段内没有从客户端设备接收到三个通信,则管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。在一个实施例中,如果在一时间段内没有从客户端设备接收到一定百分比的通信,则管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。例如,如果其在24小时的时间段内没有从客户端设备接收到至少90%的通信,则管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。在一个实施例中,如果没有从客户端设备接收到一定数目的连续通信,则管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。例如,如果其没有从客户端设备接收到接连的两个通信,管理服务器设备可在客户端注册表中将客户端设备的状态变成410非遵守的。

[0053] 在一个实施例中,管理服务器设备可响应于客户端设备被报告为丢失或被盗或者响应于客户端设备的用户变得不隶属于管理员而将客户端设备的状态变成410不遵守管理策略。例如,如果雇员客户端设备用户不再被雇主管理员雇佣,则管理服务器设备可在客户

端注册表中将客户端设备的状态变成非遵守的。

[0054] 在一个实施例中,在客户端应用被安装在客户端设备上之后,客户端设备可向认证服务器设备发送202对被管理资源的访问请求。认证服务器设备可验证302客户端设备是否遵守管理策略,并且如果是这样的话,可向客户端设备发送308客户端设备可用来访问所请求的被管理资源的令牌。

[0055] 图6描述了根据一个实施例的可用来包含或实现程序指令的示例性硬件的框图。总线600充当将硬件的其他所示部件互连的主信息通道。CPU 605是系统的中央处理单元,执行要执行程序所需的计算和逻辑操作。只读存储器 (ROM) 610和随机存取存储器 (RAM) 615组成示例性存储设备。

[0056] 控制器620与一个或多个可选的存储设备625对接到系统总线600。这些存储设备625可包括例如外部或内部DVD驱动器、CD ROM驱动器、硬盘驱动器、闪存存储器、USB驱动器等。如先前所指示的,这些各种驱动器和控制器是可选设备。

[0057] 可将程序指令存储在ROM 610和/或RAM 615中。可选地,可将程序指令可存储在有形计算机可读存储介质上,诸如硬盘、紧凑式磁盘、数字磁盘、闪存存储器、存储卡、USB驱动器、光盘存储介质,诸如Blu-ray™磁盘和/或其他记录介质。

[0058] 可选显示接口640可允许将信息以音频、视觉、图形或字母数字格式的信息从总线600显示在显示器635上。与外部设备的通信可使用各种通信端口640发生。示例性通信端口640可附着于通信网络,诸如因特网或内部网。

[0059] 硬件还可包括接口645,其允许从诸如键盘650之类的输入设备或其他输入设备655接收数据,其他输入设备655诸如鼠标、操纵杆、触摸屏、遥控器、指示设备、视频输入设备和/或音频输入设备。

[0060] 还将认识到的是可期望地将上文公开的变体及其他特征和功能或其备选组合成许多其他不同的系统或应用。随后可以由本领域的技术人员进行其中的各种目前未预见到或未预期的备选、修改、变更或改进,其也意图被以下权利要求涵盖。

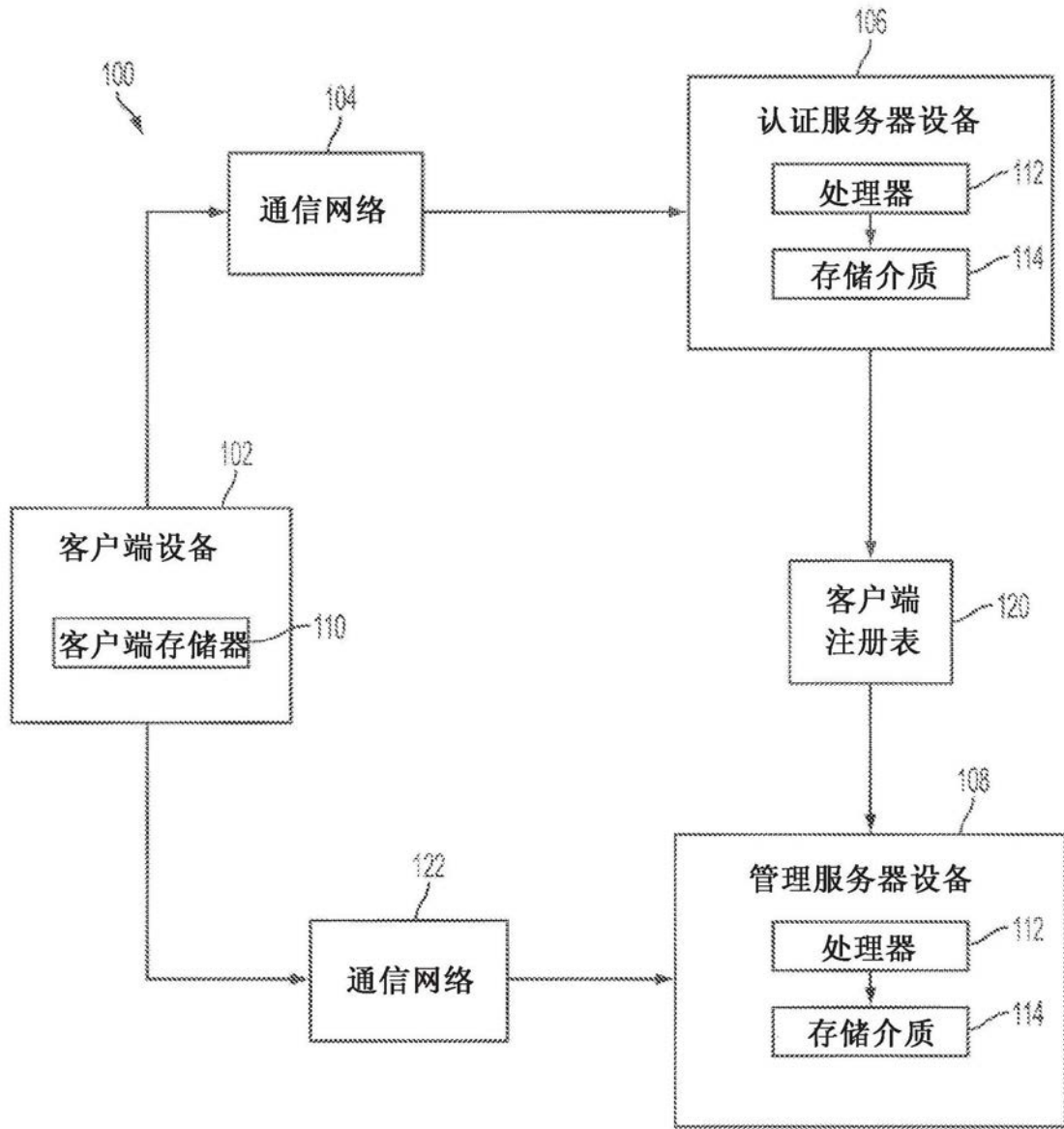


图1

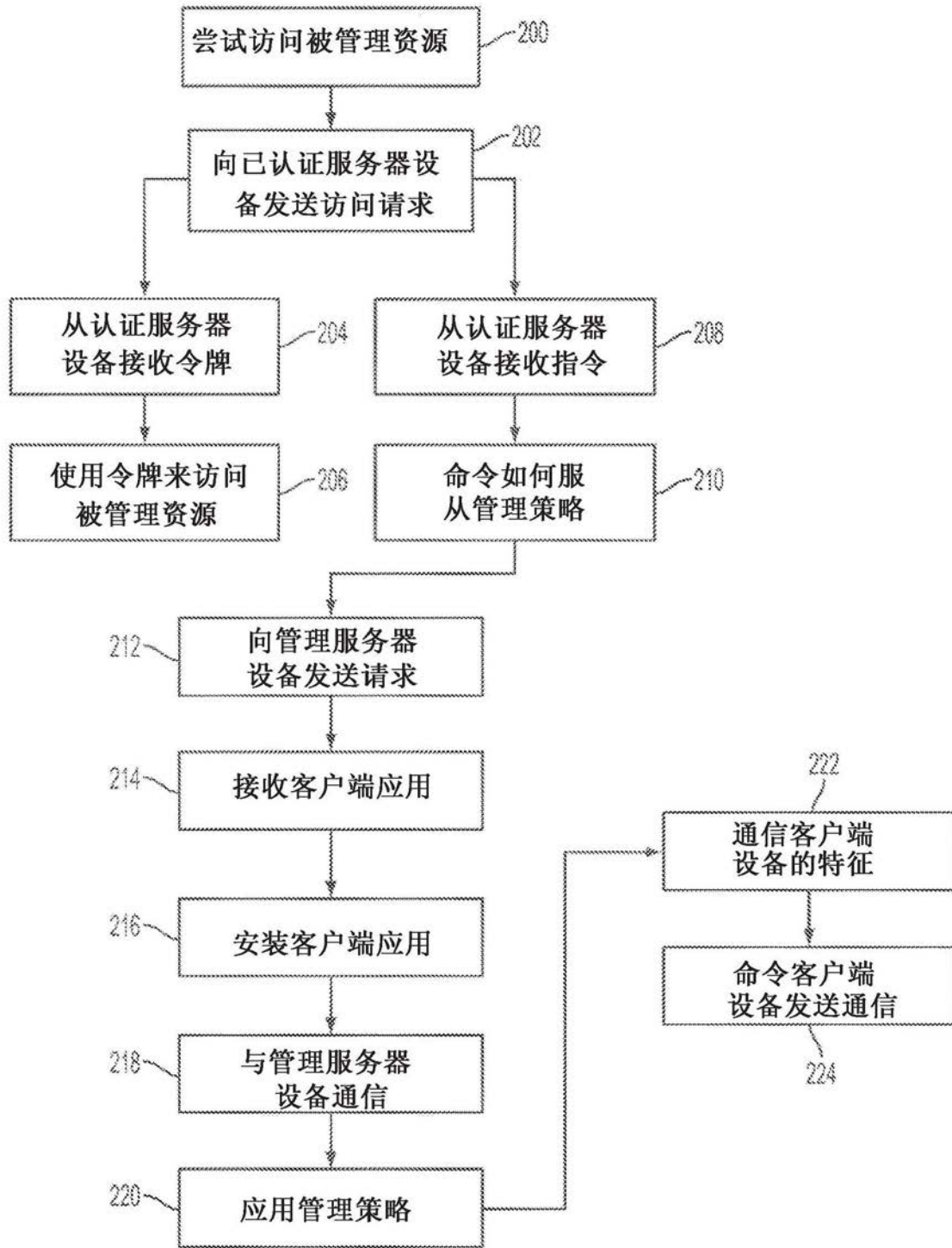


图2

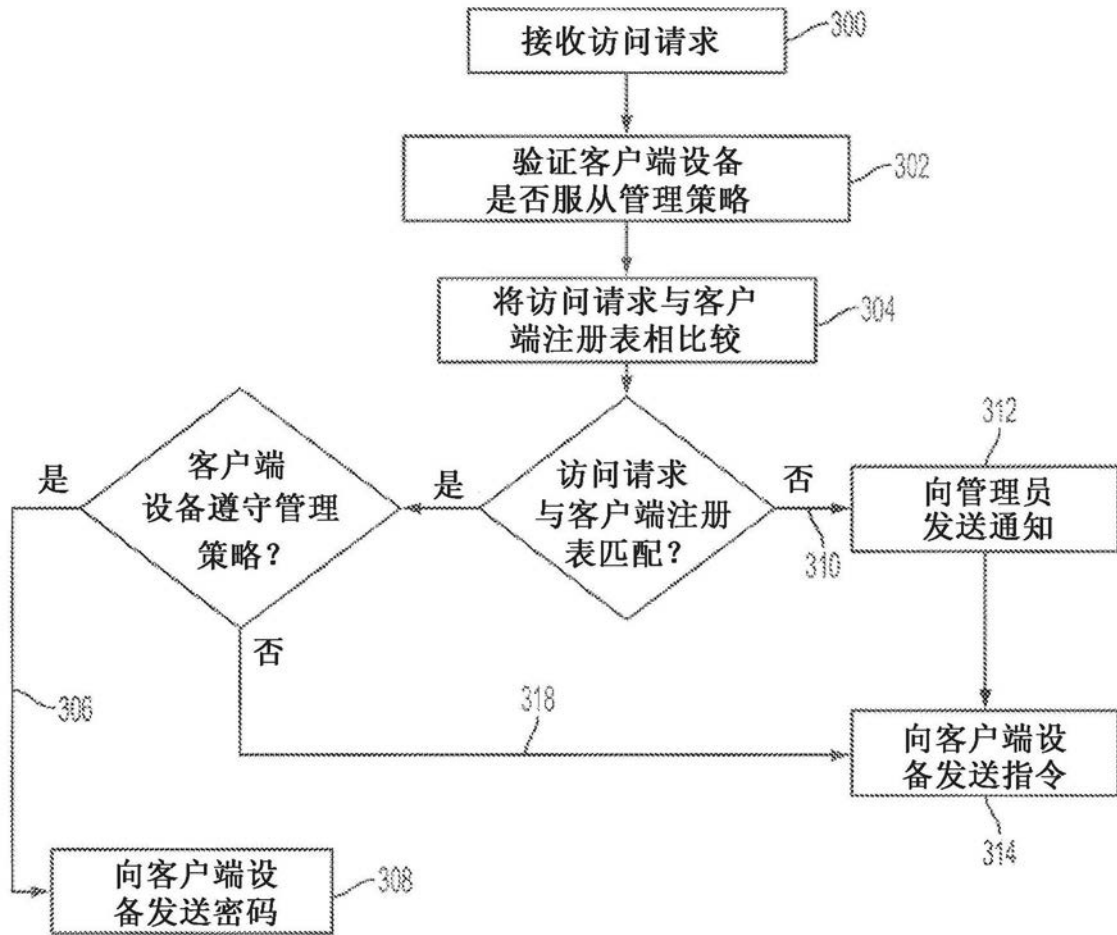


图3



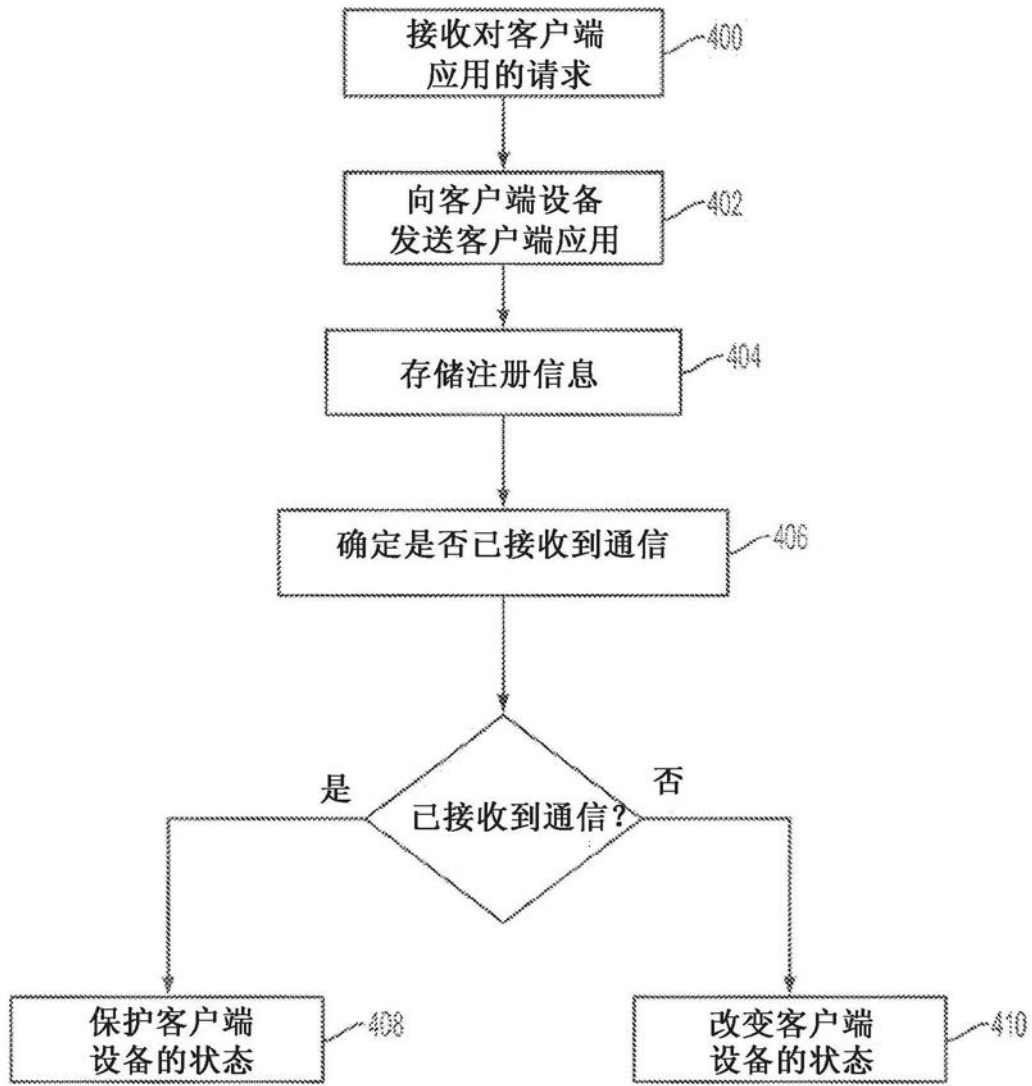


图4

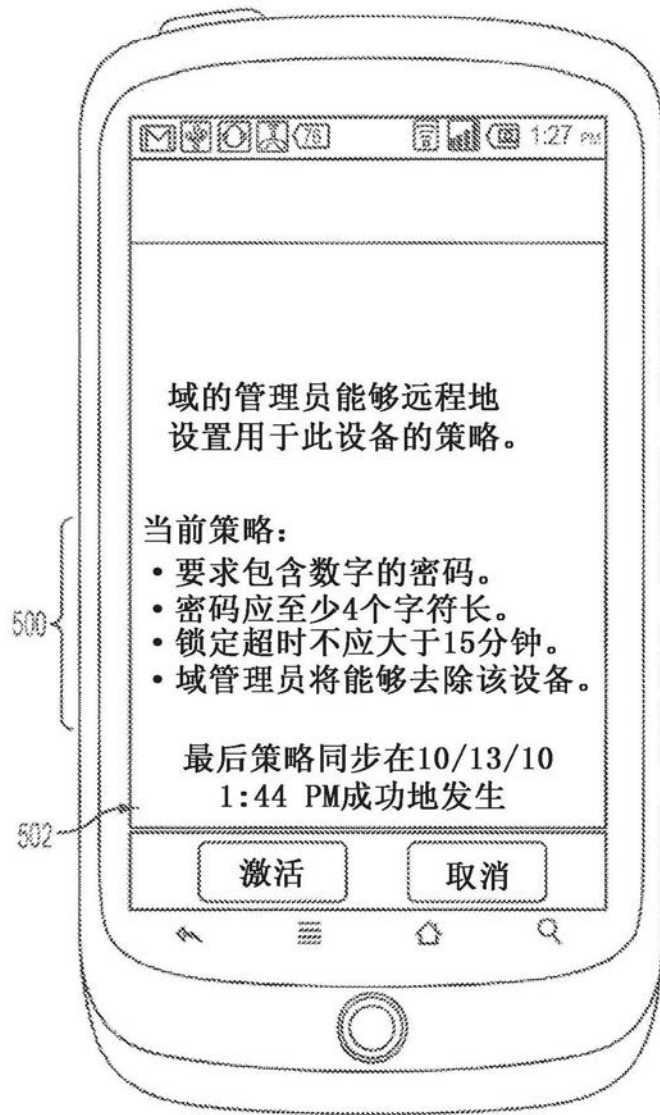


图5

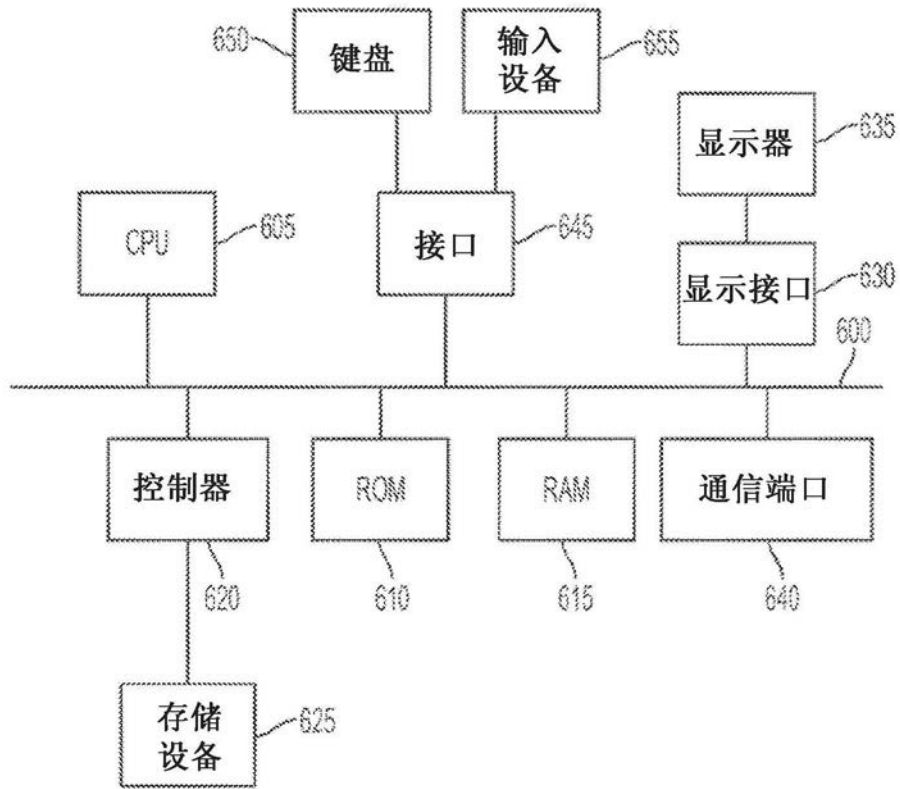


图6