(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 108140098 B
(45)授权公告日 2022.04.05

(21)申请号 201680059130.X
(22)申请日 2016.09.16
(65)同一申请的已公布的文献号
申请公布号 CN 108140098 A
(43)申请公布日 2018.06.08
(30)优先权数据
62/245,534 2015.10.23 US
15/267,044 2016.09.15 US
(85)PCT国际申请进入国家阶段日
2018.04.03
(86)PCT国际申请的申请数据
PCT/US2016/052139 2016.09.16
(87)PCT国际申请的公布数据
WO2017/069879 EN 2017.04.27
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 M·阿米尔 A·U·瑞曼
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 边海梅
(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/53(2013.01)
G06F 21/44(2013.01)
G06F 9/455(2006.01)
H04W 12/06(2021.01)
H04L 9/40(2022.01)
(56)对比文件
CN 1906886 A,2007.01.31
US 2007130462 A1,2007.06.07
US 2009323941 A1,2009.12.31
US 2014245025 A1,2014.08.28
US 2014282833 A1,2014.09.18
审查员 赵鼎新

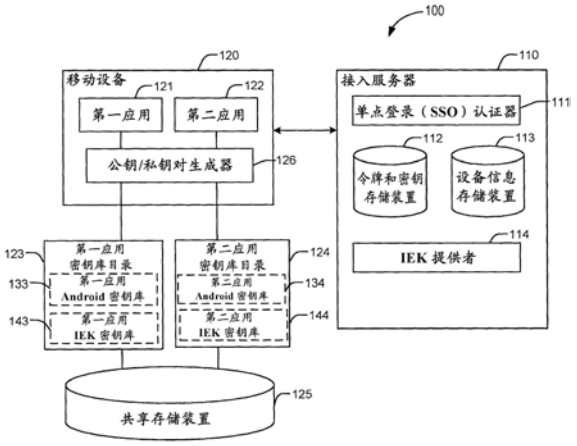
权利要求书4页 说明书20页 附图9页

(54)发明名称

建立容器之间的信任

(57)摘要

提供了用于在容器化应用之间建立数据的安全交换的技术。一种方法能够包括:由设备向接入服务器注册该设备上的第一容器化应用,由该设备向接入服务器注册该设备上的第二容器化应用,验证第一容器化应用和第二容器化应用被配置为交换数据,以及在向接入服务器注册的第一容器化应用与第二容器化应用之间交换数据。



CN 108140098 B

1.一种计算机实现的方法,包括:

由设备向接入服务器注册所述设备上的第一容器化应用,其中向所述接入服务器注册所述第一容器化应用包括:

生成第一公钥/私钥,并将所述第一公钥/私钥存储在所述设备上的所述第一容器化应用的第一密钥库中;

将来自所述接入服务器的意图加密密钥IEK存储在所述设备上的所述第一容器化应用的第二密钥库中,其中所述第一容器化应用的所述第二密钥库不同于所述第一容器化应用的所述第一密钥库;

使用所生成的第一公钥/私钥中的公钥,对所述第一容器化应用的所述第二密钥库进行加密;

其中,所述第一密钥库和所述第二密钥库仅能够被所述第一容器化应用访问;

由所述设备向所述接入服务器注册所述设备上的第二容器化应用;

验证所述第一容器化应用和所述第二容器化应用被配置为交换数据;以及

在向所述接入服务器注册的所述第一容器化应用和所述第二容器化应用之间交换数据。

2.如权利要求1所述的计算机实现的方法,还包括从所述接入服务器接收意图加密密钥(IEK)、根密钥和会话令牌。

3.如权利要求2所述的计算机实现的方法,其中向所述接入服务器注册所述第一容器化应用还包括:

创建共享应用列表并将所述第一容器化应用的标识信息添加到所述共享应用列表;以及

加密所述共享应用列表。

4.如权利要求3所述的计算机实现的方法,其中所述共享应用列表是使用来自所述接入服务器的所述根密钥进行加密的。

5.如权利要求3所述的计算机实现的方法,其中向所述接入服务器注册所述第二容器化应用包括:

生成第二公钥/私钥,并将所述第二公钥/私钥存储在所述第二容器化应用的第一密钥库中;

将来自所述接入服务器的所述IEK存储在所述第二容器化应用的第二密钥库中;

使用所生成的第二公钥/私钥中的第二公钥对所述第二容器化应用的第二密钥库进行加密;以及

解密所述共享应用列表,并将所述第二容器化应用的标识信息添加到所述共享应用列表。

6.如权利要求3、4或5中任一项所述的计算机实现的方法,其中所述接入服务器是移动安全接入服务器(MSAS)。

7.如权利要求3、4或5中任一项所述的计算机实现的方法,其中所述第一容器化应用的标识信息包括所述第一容器化应用的签名和包名称。

8.如权利要求5所述的计算机实现的方法,其中所述第二容器化应用的标识信息包括所述第二容器化应用的签名和包名称。

9.如权利要求5所述的计算机实现的方法,其中验证所述第一容器化应用和所述第二容器化应用被配置为交换数据包括:由所述第一容器化应用确定所述第二容器化应用的签名和包名称在所述共享应用列表上。

10.如权利要求1所述的计算机实现的方法,其中在所述第一容器化应用与所述第二容器化应用之间交换数据包括:

由所述第一容器化应用向所述第二容器化应用发送经加密的意图;以及

由所述第二容器化应用使用所述IEK来解密所述经加密的意图。

11.如权利要求10所述的计算机实现的方法,其中所述经加密的意图是用根密钥和会话令牌加密的意图。

12.如权利要求11所述的计算机实现的方法,其中所述意图包括指示针对动作或主题的描述的消息包。

13.如权利要求5所述的计算机实现的方法,其中使用所述根密钥来解密所述共享应用列表。

14.如权利要求5所述的计算机实现的方法,还包括:

从所述接入服务器接收经更新的IEK;

向所述接入服务器认证所述第一容器化应用;以及

由所述第一容器化应用接收所述经更新的IEK。

15.一种存储能够由一个或多个处理器执行以使所述一个或多个处理器执行操作的多条指令的非瞬态计算机可读存储介质,所述操作包括:

由设备向接入服务器注册所述设备上的第一容器化应用,其中向所述接入服务器注册所述第一容器化应用包括:

生成第一公钥/私钥,并将所述第一公钥/私钥存储在所述设备上的所述第一容器化应用的第一密钥库中;

将来自所述接入服务器的意图加密密钥IEK存储在所述设备上的所述第一容器化应用的第二密钥库中,其中所述第一容器化应用的所述第二密钥库不同于所述第一容器化应用的所述第一密钥库;

使用所生成的第一公钥/私钥中的公钥,对所述第一容器化应用的所述第二密钥库进行加密;

其中,所述第一密钥库和所述第二密钥库仅能够被所述第一容器化应用访问;

由所述设备向所述接入服务器注册所述设备上的第二容器化应用;

验证所述第一容器化应用和所述第二容器化应用被配置为交换数据;以及

在向所述接入服务器注册的所述第一容器化应用和所述第二容器化应用之间交换数据。

16.如权利要求15所述的非瞬态计算机可读存储介质,还包括从所述接入服务器接收意图加密密钥(IEK)、根密钥和会话令牌。

17.如权利要求16所述的非瞬态计算机可读存储介质,其中向所述接入服务器注册所述第一容器化应用还包括:

创建共享应用列表,并将所述第一容器化应用的标识信息添加到所述共享应用列表;以及

加密所述共享应用列表。

18.如权利要求17所述的非瞬态计算机可读存储介质，其中所述共享应用列表是使用来自所述接入服务器的所述根密钥进行加密的。

19.如权利要求17所述的非瞬态计算机可读存储介质，其中向所述接入服务器注册所述第二容器化应用包括：

生成第二公钥/私钥，并将所述第二公钥/私钥存储在所述第二容器化应用的第一密钥库中；

将来自所述接入服务器的所述IEK存储在所述第二容器化应用的第二密钥库中；

使用所生成的第二公钥/私钥中的第二公钥，对所述第二容器化应用的第二密钥库进行加密；以及

解密所述共享应用列表，并将所述第二容器化应用的标识信息添加到所述共享应用列表。

20.一种计算系统，包括：

存储器；以及

一个或多个处理器，耦合到所述存储器，并被配置为：

向接入服务器注册设备上的第一容器化应用，其中向所述接入服务器注册所述第一容器化应用包括：

生成第一公钥/私钥，并将所述第一公钥/私钥存储在所述设备上的所述第一容器化应用的第一密钥库中；

将来自所述接入服务器的意图加密密钥IEK存储在所述设备上的所述第一容器化应用的第二密钥库中，其中所述第一容器化应用的所述第二密钥库不同于所述第一容器化应用的所述第一密钥库；

使用所生成的第一公钥/私钥中的公钥，对所述第一容器化应用的所述第二密钥库进行加密；

其中，所述第一密钥库和所述第二密钥库仅能够被所述第一容器化应用访问；

向所述接入服务器注册所述设备上的第二容器化应用；

验证所述第一容器化应用和所述第二容器化应用被配置为交换数据；以及

在向所述接入服务器注册的所述第一容器化应用和所述第二容器化应用之间交换数据。

21.一种计算设备，包括：

用于向接入服务器注册第一容器化应用的装置，其中向所述接入服务器注册所述第一容器化应用包括：

生成第一公钥/私钥，并将所述第一公钥/私钥存储在所述设备上的所述第一容器化应用的第一密钥库中；

将来自所述接入服务器的意图加密密钥IEK存储在所述设备上的所述第一容器化应用的第二密钥库中，其中所述第一容器化应用的所述第二密钥库不同于所述第一容器化应用的所述第一密钥库；

使用所生成的第一公钥/私钥中的公钥，对所述第一容器化应用的所述第二密钥库进行加密；

其中,所述第一密钥库和所述第二密钥库仅能够被所述第一容器化应用访问;

用于向所述接入服务器注册第二容器化应用的装置;

用于验证所述第一容器化应用和所述第二容器化应用被配置为交换数据的装置;以及

用于在向所述接入服务器注册的所述第一容器化应用和所述第二容器化应用之间交换数据的装置。

建立容器之间的信任

[0001] 对相关申请的交叉引用

[0002] 本PCT申请要求于2016年9月15日提交的标题为“ESTABLISHING TRUST BETWEEN CONTAINERS”的美国非临时申请No.15/267,044的权益和优先权,并且还要求于2015年10月23日提交的标题为“METHOD OF TRUST BETWEEN CONTAINERS”的美国临时申请No.62/245,534(美国非临时申请No.15/267,044也要求美国临时申请No.62/245,534的优先权)。上面提到的15/267,044和62/245,534申请的全部内容通过引用并入本文,用于所有目的。

背景技术

[0003] 本公开一般而言涉及在容器化应用之间建立数据的安全交换。具体而言,本公开涉及在同一设备上运行并且注册到同一接入服务器(诸如Oracle移动安全接入服务器)的容器化应用之间的数据的安全交换。

[0004] 当应用(诸如容器化应用)被安装在设备(诸如移动设备)上时,该应用被启动。设备的用户将被要求向接入服务器认证他们自己,以确定他们是否是授权用户。如果用户通过认证,那么他们将被允许访问应用及其数据。如果另一个应用(诸如容器化应用)安装在该设备上并向同一接入服务器注册,并且该应用是经认证的并持有会话令牌和数据加密密钥(根密钥),那么单点登录(single sign-on,SSO)可以在应用之间被执行。

[0005] SSO是让用户输入相同的ID和密码以便登录到企业内的多个应用的能力。访问管理器可以通过实现SSO系统来管理对一个或多个资源的访问。SSO系统可以提供使经认证的应用能够访问该应用有权访问的受保护资源的SSO会话。

[0006] 通过使用意图(intent)和广播(broadcast),可以在应用之间共享数据。意图或邮包(parcel)是消息包,它可以提供用于在不同应用中的代码之间执行后期运行时绑定(late runtime binding)的设施。意图可以被用于例如起动活动(activity)、起动服务(service)和/或输送广播。意图可以是持有动作(action)或主题(topic)的抽象描述的被动数据结构。例如,意图可以包含消息。广播可以是应用可以接收的消息。系统可以为系统事件输送各种类型的广播。

[0007] 意图和广播可以注册在动作(诸如自定义动作)上。自定义动作例如可以由开发人员定义。动作是要执行的一般动作。动作可以包括例如显示信息、编辑信息等等。当应用在动作上启动意图和广播时,监听该动作的其它应用可以接收该意图,该意图包含在该动作上广播的消息。

[0008] 然而,如果流氓应用或未经授权的应用也将自己注册在相同的动作上,那么该流氓应用可以接收意图和广播并且将能够访问该意图中存在的所有数据。因此,关于意图和广播的数据需要被保护远离流氓应用。

[0009] 应用之间的消息交换可以通过使用签名级保护来保证。签名级保护在例如**Android®**应用中被使用。通过使用签名级保护,只有当第二应用由同一个签名者签名或者第二应用具有与第一应用相同的签名证书时,才可以允许第二应用与第一应用通信。

[0010] 然而,相同的签名者信息可能是不可能的。例如,用于移动应用管理系统的容器化

工具(诸如Oracle移动安全套件(OMSS)容器化工具)可以被用于将任何第三方应用容器化。然后,容器化应用可以被上传到应用商店并由用户使用。因此,这些容器化应用将具有与其它应用不同的签名者信息。因此,消息交换在应用之间将不起作用,因为这些应用不会有相同的签名者信息。

发明内容

[0011] 示例性实施例提供了用于在容器化应用之间建立数据的安全交换的技术。

[0012] 在示例实施例中,一种方法可以包括由设备将该设备上的第一容器化应用向接入服务器注册,由该设备将该设备上的第二容器化应用向接入服务器注册,验证第一容器化应用和第二容器化应用被配置为交换数据,以及在向接入服务器注册的第一容器化应用与第二容器化应用之间交换数据。

[0013] 在实施例的一方面,一种方法可以包括从接入服务器接收意图加密密钥(IEK)、根密钥和会话令牌。

[0014] 在实施例的一方面,向接入服务器注册第一容器化应用可以包括生成第一公钥/私钥并将第一公钥/私钥存储在第一容器化应用的第一密钥库中,将来自接入服务器的IEK存储在容器化应用的第二密钥库中,使用所生成的公钥/私钥中的公钥对第一容器化应用的第二密钥库进行加密,创建共享应用列表并将第一容器化应用的标识信息添加到共享应用列表,以及加密共享应用列表。

[0015] 在实施例的一方面,使用来自接入服务器的根密钥来加密共享应用列表。

[0016] 在实施例的一方面,向接入服务器注册第二容器化应用包括生成第二公钥/私钥并将第二公钥/私钥存储在第二容器化应用的第一密钥库中,将来自接入服务器的IEK存储在第二容器化应用的第二密钥库中,使用所生成的第二公钥/私钥中的第二公钥对第二容器化应用的第二密钥库进行加密,以及解密共享应用列表并将第二容器化应用的标识信息添加到共享应用列表。

[0017] 在实施例的一方面,接入服务器是移动安全接入服务器(MSAS)。

[0018] 在实施例的一方面,第一容器化应用的标识信息可以包括第一容器化应用的签名和包名称。

[0019] 在实施例的一方面,第二容器化应用的标识信息可以包括第二容器化应用的签名和包名称。

[0020] 在实施例的一方面,验证第一容器化应用和第二容器化应用被配置为交换数据包括由第一容器化应用确定第二容器化应用的签名和包名称在共享应用列表上。

[0021] 在实施例的一方面,在第一容器化应用与第二容器化应用之间交换数据包括由第一容器化应用向第二容器化应用发送经加密的意图,以及由第二容器化应用使用IEK来解密该经加密的意图。

[0022] 在实施例的一方面,经加密的意图是用根密钥和会话令牌进行加密的意图。

[0023] 在实施例的一方面,意图包括指示针对动作或主题的描述的消息包。

[0024] 在实施例的一方面,使用根密钥来解密共享应用列表。

[0025] 在实施例的一方面,一种方法还可以包括从接入服务器接收经更新的IEK,向接入服务器认证第一容器化应用,以及由第一容器化应用接收经更新的IEK。

[0026] 在示例实施例中，存储可由一个或多个处理器执行以使这一个或多个处理器执行操作的多条指令的非瞬态计算机可读存储介质，其中操作可以包括：由设备将该设备上的第一容器化应用向接入服务器注册，由设备将该设备上的第二容器化应用向接入服务器注册，验证第一容器化应用和第二容器化应用被配置为交换数据，以及在向接入服务器注册的第一容器化应用与第二容器化应用之间交换数据。

[0027] 在示例实施例中，一种系统可以包括存储器以及耦合到存储器的一个或多个处理器，这一个或多个处理器被配置为将设备上的第一容器化应用向接入服务器注册，将该设备的第二容器化应用向接入服务器注册，验证第一容器化应用和第二容器化应用被配置为交换数据，以及在向接入服务器注册的第一容器化应用和第二容器化应用之间交换数据。

[0028] 其它实施例针对与本文描述的方法相关联的系统、便携式消费设备和计算机可读介质。

[0029] 参考以下详细描述和附图可以更好地理解示例性实施例的本质和优点。

附图说明

[0030] 结合附图通过以下详细描述将容易理解本公开，附图中相同的标号表示相同的元件，并且其中：

[0031] 图1示出根据一些实施例的、用于在容器化应用之间建立数据的安全交换的系统。

[0032] 图2示出根据一些实施例的、向接入服务器注册第一容器化应用的序列图。

[0033] 图3示出根据一些实施例的、向接入服务器注册第二容器化应用的序列图。

[0034] 图4示出根据一些实施例的、启动经注册的容器化应用的序列图。

[0035] 图5示出根据一些实施例的、刷新和/或改变意图加密密钥(IEK)的序列图。

[0036] 图6示出根据一些实施例的、在容器化应用之间建立数据的安全交换的流程图。

[0037] 图7绘出了用于实现一些实施例的分布式系统的简化图。

[0038] 图8示出根据一些实施例的、在其中服务可以作为云服务被提供的系统环境的一个或多个部件的简化框图。

[0039] 图9示出根据一些实施例的、可以被用于实现某些元件的示例性计算机系统。

具体实施方式

[0040] 在以下描述中，为了解释的目的而阐述了具体细节，以便提供对示例性实施例的透彻理解。然而，将清楚的是，各种实施例可以在没有这些具体细节的情况下实践。例如，电路、系统、算法、结构、技术、网络、处理和其它部件可以以框图形式示为组成部分，以免用不必要的细节混淆实施例。附图和描述不旨在是限制性的。

[0041] 示例性实施例提供了用于在容器化应用之间建立数据的安全交换的技术。容器化应用可以是使用容器化技术(也称为应用沙箱)而配置的应用。容器化应用可以是封装在具有其自己的操作环境的容器中的应用。容器化应用可以是电子邮件应用、文档编辑器、业务应用等等。当容器化应用被启动时，应用类被初始化。由于所有初始化/生命周期方法都已被重命名，因此那些代码不会被执行。相反，(由容器化装置注入的)虚拟方法(dummy method)被执行。在应用类初始化之后，内容提供者被初始化，并且(由容器化装置注入的)用于内容提供者的包装类(wrapper class)将被初始化。

[0042] 容器化是针对软件开发和移动应用管理(MAM)的、限制某些代码可以在其中执行的环境的方法。因此,可以将容器化应用配置为使得其被限制在设备上的容器或沙箱中执行。容器化应用可以被配置用于在与其它应用隔离的环境中执行。

[0043] “容器化装置”应用可以以本地未修改的应用作为输入,并且输出容器化的经修改的应用。例如,用于Google **Android®**(谷歌安卓)计算机应用的ApplicationManifest.XML文件和Google **Dalvik®**可执行文件(DEX)字节代码文件是从Google **Android®**应用包(APK)文件中提取的。为应用、内容提供者和活动创建包装类和虚拟生命周期方法。一个目的是创建虚拟生命周期,使得在完成认证之前不执行原始代码。一旦认证成功完成,就在实际应用代码被执行之前获取并应用策略。

[0044] 示例性实施例提供了容器化应用之间的安全机制。该安全机制可以实现用于在容器化应用之间授予权限的技术。根据示例性实施例的安全机制可以包括两级安全机制,其包括两步验证处理。验证的第一步是在接入服务器级执行的,并且验证的第二步是在设备级执行的。因此,为了例如以非授权方式获得在设备上的两个容器化应用之间交换的信息,服务器和设备二者都必须被破坏。例如,服务器和设备二者都需要被入侵。

[0045] 具体而言,为了获得意图加密密钥(IEK),需要入侵设备。如果设备被入侵,那么容器化应用可能无法工作并且用户无法向接入服务器进行认证。然而,即使可以从接入服务器获得IEK,黑客还将另外需要用户的密码,以获得用于对共享应用列表进行加密的根密钥。

[0046] 因此,在赋予不同的应用供应商独立性的同时,可以向容器化应用增加安全性。第三方应用供应商可以将他们的容器化应用上传到例如应用商店,并且最终用户可以在维持安全性的同时从应用商店安装容器化应用。

[0047] 图1示出根据一些实施例的、用于在容器化应用之间建立数据的安全交换的系统100。

[0048] 系统100可以包括便携式设备,诸如可以与接入服务器110通信的移动设备120。虽然示出了单个移动设备,但是一个或多个移动设备可以与接入服务器110通信。接入服务器110是服务器计算机。接入服务器110可以是例如移动安全接入服务器(MSAS)或接入网关。移动设备120可以是例如基于Google **Android®**操作系统(OS)的设备(诸如移动电话)。虽然公开了**Android®**操作系统,但是示例性实施例可以用在不同的操作系统(诸如**iOS®**)中,并且不限于**Android®**操作系统。系统100可以用在例如用于容器化应用的工作空间(诸如Oracle移动安全套件)中。

[0049] 移动设备120可以包括一个或多个应用。应用可以是容器化应用。如图1中所示,移动设备120包括第一应用121和第二应用122。虽然在图中示出了两个应用,但是移动设备可以包括多于两个或少于两个应用。

[0050] 移动设备120可以包括公钥/私钥生成器126。公钥/私钥生成器126可以用于为第一应用121和第二应用122生成公钥/私钥对。

[0051] 每个应用可以具有对应的密钥库。密钥库可以是例如安全证书(诸如授权证书或公钥证书)的储存库。第一应用121可以包括第一应用密钥库目录123,而第二应用122可以包括第二应用密钥库目录124。第一应用密钥库目录123和第二应用密钥库目录124可以包

括一个或多个密钥库。**Android®**密钥库是由Android系统提供的密钥库。每个应用可以存储密钥对，其只能由存储该密钥对的应用访问。例如，第一应用密钥库目录123中的密钥库可以是只能由第一应用121访问的第一应用**Android®**密钥库133(例如，用于第一应用的第一密钥库)。另外，第二应用密钥库目录124中的密钥库可以是只能由第二应用122访问的第二应用**Android®**密钥库134(例如，用于第二应用的第一密钥库)。**Android®**密钥库133和134可以存储例如由公钥/私钥对生成器126生成的公钥/私钥对。虽然描述了**Android®**密钥库，但这仅仅是示例，并且密钥库可以针对不同的操作系统。

[0052] 此外，第一应用密钥库目录123中的密钥库可以包括只能由第一应用121访问的第一应用IEK密钥库143(例如，用于第一应用的第二密钥库)。用于第一应用的第二密钥库可以存储在共享文件中，并且可以使用根密钥来加密该共享文件。另外，第二应用密钥库目录124中的密钥库可以包括只能由第二应用122访问的第二应用IEK密钥库144(例如，用于第二应用的第二密钥库)。

[0053] 在应用向接入服务器注册之后，应用可以将它们的包名称和签名存储在共享应用列表中。共享应用列表可以由移动设备上经认证和经注册的应用共享。共享应用列表可以存储在共享存储装置125上。共享存储装置125可以位于移动设备外部并且可以被一个或多个应用访问。

[0054] 接入服务器110可以是例如移动安全接入服务器(MSAS)。接入服务器可以提供对一个或多个资源的访问。接入服务器110可以包括或通信地耦合到可以实现SSO服务的访问管理系统(诸如Oracle访问管理器)。在一些实施例中，接入服务器110可以包括单点登录认证器111，单点登录认证器111可以建立SSO会话以提供对一个或多个资源的SSO访问。接入服务器110使得工作空间中的所有容器化应用都能够在用户的局域网(LAN)内通话。例如，接入服务器110可以呼叫互联网上的实体。系统中的所有应用都可以与接入服务器110通信。

[0055] 接入服务器110还可以包括令牌和密钥存储装置112以及设备信息存储装置113。令牌和密钥存储装置112可以存储例如会话令牌和根密钥。设备信息存储装置113可以存储例如设备的序列号(诸如用于移动设备120的序列号)。

[0056] 接入服务器110还可以包括IEK提供者114。IEK可以是用于意图的加密密钥。意图提供了用于在不同应用中的代码之间执行后期运行时绑定的设施。另外，意图可以被用于启动活动。意图可以是持有动作的描述的被动数据结构。意图是可以被用于请求来自另一个应用部件的动作的消息对象。意图可以以多种方式促进部件之间的通信。IEK提供者114可以提供用于意图的IEK。

[0057] A.第一容器化应用的注册

[0058] 图2示出根据一些实施例的、向接入服务器注册第一容器化应用的序列图。

[0059] 序列200可以由例如作为容器化应用的第一应用220、接入服务器210和经认证的应用240执行。图2的元件可以与上面关于图1描述的那些元件相似。例如，接入服务器210可以与例如图1中所述的接入服务器110对应。第一应用220和经认证的应用240可以存储在移动设备(诸如移动设备120)上。经认证的应用240可以包括该移动设备上的已经由接入服务器210认证的其它应用。可以存在先前已经由接入服务器210认证的应用(例如，经认证的应

用240)，并且可以没有任何先前经认证的应用。因此，可以没有任何先前经认证的应用240。

[0060] 图2中所示的元件仅仅是示例，并且可以有多于一个经认证的应用。另外，虽然应用被称为第一应用和第二应用，但这并不指示任何次序，并且第二应用可以是第一应用。

[0061] 在步骤221处，启动存储在移动设备上的第一应用220。当第一应用220在移动设备上被启动时，移动设备将请求移动设备的用户向接入服务器210认证他们自己。例如，用户将被要求在移动设备的用户界面上输入用户名和密码。如果用户通过认证，那么用户可以访问第一应用和第一应用中的数据。当第一应用220被启动时，它将在步骤222处向已经由接入服务器210认证和注册的应用发送广播消息。例如，如果在移动设备上存在经认证的应用240，那么第一应用220可以向经认证的应用240发送广播消息。

[0062] 广播消息是关于特定动作或主题的消息。因此，对该主题感兴趣的应用可以监听该消息。主题可以包括例如无线电台标识符FM 100或FM 89.1。广播消息可以是向已向接入服务器210认证的任何应用索要会话令牌和根密钥的消息。

[0063] 在步骤241处，经认证的应用240将在共享文件中检查第一应用220的签名和包名称。经认证的应用240可以接收广播，因为它在相同的自定义动作上注册。如果经认证的应用240未在相同的自定义动作上注册，那么经认证的应用240将不会接收来自第一应用220的广播。如果经认证的应用240在相同的自定义动作上注册，那么经认证的应用240可以对广播做出响应。

[0064] 经认证的应用240将确定第一应用220的签名和包名称是否存在于存储在共享位置中的先前创建的文件中。该文件可以存储在例如共享存储装置125中。如果第一应用220的签名和包名称不存在于该文件中，那么经认证的应用将不会向第一应用220发送响应，如步骤242所示。

[0065] 如果未从任何经认证的应用接收到响应，那么在步骤223处将执行认证。向移动设备的用户呈现认证屏幕，并且可以请求用户在移动设备的用户界面上输入用户名和密码。

[0066] 在第一应用220被接入服务器210认证之后，在步骤224处，将执行注册。当第一应用220在接入服务器210上注册它自己时，第一应用220将向接入服务器210提供其设备序列号。设备序列号可以是例如可以用于将该设备与其它设备区分开的唯一数字信息。

[0067] 在步骤211处，接入服务器210确定是否存在来自该移动设备的任何其它应用。例如，接入服务器可以根据设备序列号来确定是否存在来自该移动设备的任何其它应用。如果设备序列号存在于接入服务器210上，那么在步骤212处，接入服务器210将发送用于该设备的意图加密密钥(IEK)。如果设备序列号不存在，那么接入服务器210将首先生成用于该设备的IEK，然后在步骤212处发送所生成的IEK。IEK可以是诸如256位加密密钥之类的密钥。

[0068] 在步骤212处，除IEK之外，接入服务器210还发送根密钥和会话令牌。会话令牌可以是由接入服务器210提供的令牌(诸如认证cookie)。另外，会话令牌可以包括签名、用户名、ID、日期等等。而且，会话令牌可以包括随机文本串。根密钥可以是用于对应用的密钥库进行加密的主密钥。根密钥或主密钥可以用于对密钥库进行加密。

[0069] 当第一应用220接收到IEK、根密钥和会话令牌时，在步骤225处，第一应用220可以生成公钥/私钥对，并且生成的公钥/私钥对被存储在用于第一应用的第一密钥库中(诸如存储在第一应用**Android®**密钥库133中)。用于第一应用的第一密钥库(例如，第一应用

Android®密钥库133)可以只能由第一应用访问。每个应用可以具有其自己的Android®密钥库。当应用安装在例如Android®设备上时,将在设备上从存储装置为该应用指定只有该应用才能访问的私有区域。指定的私有区域可以是第一应用Android®密钥库133。

[0070] 在步骤226处,生成用于第一应用220的第二密钥库(例如,第一应用IEK密钥库143)。在步骤227处,使用在步骤225生成的公钥来加密从接入服务器210接收的IEK。然后,将经加密的IEK存储在第一应用220的第二密钥库(例如,第一应用IEK密钥库143)中。第一应用的第二密钥库(例如,第一应用IEK密钥库143)可以只能由第一应用220访问。

[0071] 然后,在步骤228处将包括经加密的IEK的第二密钥库存储在文件目录中。该文件目录可以只能由第一应用220访问并且是第一应用220私有的。

[0072] 在步骤229处,可以在共享位置创建文件(诸如共享应用列表)并对其进行加密。该文件可以包括包名称(例如,Gmail)和签名(例如,数据签名)。可以使用在步骤212处接收的根密钥对该文件进行加密。

[0073] 附加的应用可以存储在移动设备上。附加的应用可以与先前经认证并向接入服务器注册的应用进行通信。然而,在应用可以与设备上的其它经认证的应用通信之前,该应用应当也向接入服务器注册。

[0074] B.第二容器化应用的注册

[0075] 图3示出根据一些实施例的、向接入服务器310注册第二容器化应用330的序列图。

[0076] 序列300可以由例如第一应用320、第二应用330、接入服务器310和经认证的应用340执行。第一应用320、第二应用330和经认证的应用340可以存储在移动设备(诸如移动设备120)上。第一应用320和第二应用330是容器化应用。第一应用320先前已如关于图2所描述的那样被认证并注册。因此,第一应用320是经认证的应用。经认证的应用340可以包括该移动设备上的已经由接入服务器310认证的其它应用。可以存在先前已经由接入服务器310认证的应用(例如,经认证的应用340),并且例如除第一应用330以外可以没有任何先前被认证的应用。图3中所示的元件仅仅是示例,并且可以存在一个或多个经认证的应用。

[0077] 在步骤331处,启动存储在移动设备上的第二应用330。当第二应用330在移动设备上被启动时,移动设备将请求移动设备的用户向接入服务器310认证他们自己。如果用户通过认证,那么用户可以访问第二应用和第二应用中的数据。当第二应用330被启动时,它将在步骤321处向已经由接入服务器310认证和注册的应用发送广播消息。例如,第二应用330可以向第一应用320和经认证的应用340发送广播消息。广播消息可以是向已向接入服务器310认证的任何应用索要会话令牌和根密钥的消息。

[0078] 在步骤341处和步骤322处,经认证的应用340和第一应用320将检查第二应用330的签名和包名称。在图3所示的示例中,第一应用320和经认证的应用340可以接收广播,因为它们在相同的自定义动作上注册。如果第一应用320和经认证的应用340未在相同的自定义动作上注册,那么第一应用320和经认证的应用340将不接收来自第二应用330的广播。

[0079] 第一应用320和经认证的应用340将确定第二应用330的签名和包名称是否存在于在共享位置中创建并存储的文件(例如,共享应用列表)中。在共享位置中创建并存储的文件可以与例如在图2的步骤229中创建的文件对应。共享位置可以是例如共享存储装置125。

如果第二应用330的签名和包名称不存在于共享存储装置中的文件中，那么第一应用320和/或经认证的应用340将不向第二应用330发送响应，如步骤342和步骤323所示。例如，如果第二应用330的签名和包名称不存在于共享存储装置中的、在图2的步骤229中创建的文件中，那么第一应用320将不向第二应用330发送响应，如步骤323所示。如果第二应用330在相同的自定义动作上注册，那么第一应用320和/或经认证的应用340可以能够对广播做出响应。

[0080] 如果未从任何经认证的应用(诸如经认证的应用340和第一应用320)接收到响应，那么在步骤333处将执行认证。将向移动设备的用户呈现认证屏幕。例如，可以请求用户输入用户名和密码。

[0081] 在第二应用330向接入服务器310认证之后，在步骤334处，将执行注册。当第二应用330在接入服务器310上注册其自己时，第二应用330将向接入服务器310提供其设备序列号。设备序列号可以是例如可以用于将该设备与其它设备区分开的唯一数字信息。

[0082] 在步骤311处，接入服务器310确定是否存在来自该设备的任何其它应用。例如，接入服务器可以根据设备序列号来确定是否存在来自该移动设备的任何其它应用。如果设备序列号存在于接入服务器310上，那么在步骤312处，接入服务器310将发送用于该设备的意图加密密钥(IEK)。如果设备序列号不存在，那么接入服务器310将首先生成用于该设备的IEK，并且然后在步骤312处发送所生成的IEK。在步骤312处，接入服务器310除了IEK之外还发送根密钥和会话令牌。

[0083] 当第二应用330接收到IEK、根密钥和会话令牌时，在步骤335处，第二应用330可以生成公钥/私钥对，并将生成的公钥/私钥对存储在用于第二应用的第一密钥库中(例如，第二应用**Android®**密钥库134)。用于第二应用的第一密钥库(例如，第二应用**Android®**密钥库134)可以只能由第二应用访问。每个应用可以具有其自己的**Android®**密钥库。

[0084] 在步骤336处，生成用于第二应用330的第二密钥库(例如，第二应用IEK密钥库144)。在步骤337处，使用在步骤335处生成的公钥，对从接入服务器310接收到的IEK进行加密。然后将经加密的IEK存储在第二应用330的第二密钥库(例如，第二应用IEK密钥库144)中。第二应用IEK密钥库144可以只能由第二应用330访问。

[0085] 然后，在步骤338处，将包括经加密的IEK的密钥库(例如，第二应用IEK密钥库144)存储在目录(诸如文件目录)中。该目录可以只能由第二应用330访问。

[0086] 在步骤339处，可以由第二应用取回文件(诸如先前(例如，图2的步骤229)创建的共享应用列表)。第二应用可以使用在步骤312处接收的根密钥来解密该文件，并且第二应用可以将其包名称和签名信息添加到共享应用列表。然后第二应用可以使用根密钥对共享应用列表进行加密。

[0087] 因此，在第一应用和第二应用之间共享的任何消息将使用IEK来加密。另外，接收消息的第一应用或第二应用可以使用IEK来解密该消息。

[0088] 根据示例性实施例，最初执行用于获取IEK的认证。在用于获取IEK的认证之后，任何进一步的认证都可以触发经认证的应用之间(诸如第一应用和第二应用之间)的单点登录(SSO)。由于这两个应用都注册到相同的接入服务器，并且其中至少一个应用是经认证的

并持有会话令牌和意图加密密钥(IEK),因此可以在应用之间执行SSO。

[0089] C.启动经注册的容器化应用

[0090] 图4示出根据一些实施例的、启动经注册的容器化应用的序列图。

[0091] 序列400可以由例如第一应用420、第二应用430和接入服务器410执行。第一应用420和第二应用430是容器化应用。另外,第一应用420和第二应用430可以被存储在移动设备(诸如移动设备120)上。第一应用420和第二应用430已经如关于图2和图3所描述的那样被认证并注册。因此,第一应用420和第二应用430是经认证的应用。虽然第一应用420和第二应用430被示为经认证的应用,但是移动设备上可以存在其它经认证的应用。因此,可以存在先前已经由接入服务器310认证的附加应用。图4中所示的元件仅仅是示例。

[0092] 在步骤421处,启动存储在移动设备上的第一应用420。在第一应用420被启动之后,在步骤422处,第一应用420将向已经由接入服务器410认证并注册的应用发送广播消息。例如,第一应用420可以向第二应用430发送广播消息。第二应用430可以如图3中所描述的那样被认证。

[0093] 广播消息可以是向已向接入服务器410认证的任何应用索要会话令牌和根密钥的消息。

[0094] 如果在步骤432处未从任何经认证的应用(诸如从第二应用430)接收到响应,那么在步骤423处将执行认证。将向移动设备的用户呈现认证屏幕。例如,可以提示用户在设备的用户界面上输入用户名和密码。在认证之后,从接入服务器获取IEK、会话令牌和根密钥。

[0095] 如果在步骤433处启动第二应用430,那么在步骤434处,第二应用将向已经由接入服务器410认证的应用发送广播消息。例如,第二应用430可以向第一应用420发送广播消息。第一应用420可以如图2中所描述的那样被认证。

[0096] 广播消息可以是向已向接入服务器410认证的任何应用索要会话令牌和根密钥的消息。

[0097] 在步骤424处,第一应用可以检查用于第二应用430的包名称和签名。第一应用可以通过使用根密钥对共享文件或共享应用列表进行解密来检查用于第二应用430的包名称和签名。

[0098] 在步骤425处,第一应用420可以验证第二应用430是可信应用。在验证第二应用430是可信应用之后,第一应用420可以准备意图连同由IEK加密的会话令牌和根密钥。在步骤426处,意图、根密钥和会话令牌可以向第二应用430广播。

[0099] 在第二应用430接收到意图之后,在步骤431处,第二应用430从第二应用430的第一密钥库(例如,第二应用**Android®**密钥库134)中取回其生成的公钥/私钥对。**Android®**密钥库可以是系统提供的、由硬件支持的密钥库。因此,密钥安全性可以在硬件级得到保证。因此,它们不需要被解密,因为一个应用的密钥不能被另一个应用的密钥访问。

[0100] 在步骤432处,第二应用430通过使用从第二应用430的第一密钥库(例如,第二应用**Android®**密钥库134)取回的公钥/私钥对来解密具有IEK的第二应用430的第二密钥库(例如,第二应用IEK密钥库144)。在解密第二应用430的第二密钥库(例如,第二应用IEK密钥库144)之后,第二应用430可以然后从第二密钥库(例如,第二应用IEK密钥库144)取回

IEK。

[0101] 在步骤433处，第二应用430使用IEK解密从意图中解密会话令牌和根密钥。因此，第二应用430可以访问意图中的信息，并且信息可以在应用之间交换。

[0102] D.更新意图加密密钥(IEK)

[0103] 图5示出根据一些实施例的、刷新和/或改变IEK的序列图。

[0104] 序列500可以由例如第一应用520、第二应用530和接入服务器510执行。第一应用520和第二应用530是容器化应用。另外，第一应用520和第二应用530可以被存储在移动设备(诸如移动设备120)上。第一应用520和第二应用530已经如关于图2和图3所描述的那样被认证并注册。因此，第一应用520和第二应用530是经认证的应用。虽然第一应用520和第二应用530被示为经认证的应用，但是移动设备上可以存在其它经认证的应用。因此，可以存在先前已经由接入服务器510认证的附加应用，并且可以没有任何先前认证的应用。图5中所示的元件仅仅是示例。

[0105] 可以在接入服务器510处改变IEK。例如，如果IEK已经被破坏并且例如不再安全，那么可以改变IEK。可替代地，作为附加的安全措施，可以例行地更新IEK。因此，可以例如每周或每两周更新IEK。

[0106] 如果IEK被改变，那么接入服务器510可以将新的IEK传送到系统上经认证且经注册的容器化应用。例如，接入服务器510可以将新的IEK传送到第一应用520，第一应用520随后可以将新的IEK提供给第二应用530。

[0107] 在步骤511处，接入服务器510可以更新IEK。在步骤521处，第一应用可以向接入服务器510认证它自己。在成功认证之后，在步骤522处，第一应用520可以从接入服务器510接收IEK。从接入服务器接收的IEK可以是经更新的IEK。

[0108] 在步骤523处，第一应用将比较从接入服务器接收的IEK与当前存储在第一应用的第二密钥库(例如，第一应用IEK密钥库143)中的IEK。如果从接入服务器510接收的IEK不同于当前存储在第一应用的第二密钥库(例如，第一应用IEK密钥库143)中的IEK，那么在步骤524处，可以更新存储在第二密钥库中的IEK。然而，如果从接入服务器510接收的IEK与当前存储在第一应用的第二密钥库中的IEK相同，那么可以不更新IEK。

[0109] 如果在步骤531处第二应用530被启动，那么第二应用530可以从第一应用520接收意图、会话令牌和根密钥。第二应用530可以从第一应用520接收会话令牌和根密钥，这是因为第二应用530位于可信应用的共享列表中。然而，第二应用530将不能够解密意图，因为已经使用经更新的IEK对该意图进行了加密。因此，在步骤532处解密将失败。

[0110] 在解密失败之后，在步骤526处，将在第二应用530上提供认证屏幕。当第二应用530执行认证时，第二应用530可以取回经更新的IEK，并且可以在步骤533处将经更新的IEK存储在第二应用530中的第二密钥库中。因此，第二应用530于是将具有经更新的IEK。

[0111] E.注册和启动应用的方法

[0112] 图6示出根据一些实施例的、用于在容器化应用之间建立数据的安全交换的方法600的流程图。

[0113] 在步骤610处，可以向接入服务器注册第一容器化应用。如上面所讨论的，在第一容器化应用可以与移动设备上的其它应用交换信息之前，向接入服务器注册第一容器化应用。

[0114] 另外，为了让添加到设备的任何应用与当前经认证并向设备注册的应用进行通信，添加到设备的这些应用也应当向接入服务器认证并注册。因此，在步骤620处，例如可以向接入服务器注册第二容器化应用。

[0115] 在步骤630处，可以启动经注册的应用(诸如第一应用和第二应用)。数据(诸如意图)可以在已经向接入服务器认证的应用之间交换。

[0116] 在步骤640处，可以更新意图加密密钥(IEK)。例如，如果因为IEK已被破坏而改变IEK，或者如果因为例行更新而改变IEK，那么可以在经认证的应用之间共享经更新的IEK。

[0117] F.计算机系统

[0118] 图7绘出了用于实现一些实施例的分布式系统700的简化图。在所示实施例中，分布式系统700包括一个或多个客户端计算设备702、704、706和708，这些客户端计算设备被配置为通过(一个或多个)网络710执行和操作客户端应用(诸如web浏览器、专有客户端(例如，Oracle Forms)等等)。服务器712可以经由网络710与远程客户端计算设备702、704、706和708通信地耦合。

[0119] 在各种实施例中，服务器712可以适于运行一个或多个服务或软件应用(诸如提供消息输送服务的服务和应用)。在某些实施例中，服务器712还可以提供其它服务，或者软件应用可以包括非虚拟环境和虚拟环境。在一些实施例中，这些服务可以作为基于web的服务或云服务或者在软件即服务(SaaS)模型下提供给客户端计算设备702、704、706和/或708的用户。操作客户端计算设备702、704、706和/或708的用户可以进而利用一个或多个客户端应用与服务器712交互，以利用由这些部件提供的服务。

[0120] 在图7所绘出的配置中，系统700的软件部件718、720和722被示为在服务器712上实现。在其它实施例中，系统700的一个或多个部件和/或由这些部件提供的服务也可以由客户端计算设备702、704、706和/或708中的一个或多个实现。操作客户端计算设备的用户然后可以利用一个或多个客户端应用来使用由这些部件提供的服务。这些部件可以用硬件、固件、软件或其组合实现。应当理解的是，各种不同的系统配置是可能的，其可以与分布式系统700不同。因此，图7中所示的实施例是用于实现实施例系统的分布式系统的一个示例，并且不旨在进行限制。

[0121] 客户端计算设备702、704、706和/或708可以包括各种类型的计算系统。例如，客户端设备可以包括便携式手持设备(例如，**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理(PDA))或可穿戴设备(例如，Google **Glass®**头戴式显示器)，其运行诸如Microsoft Windows **Mobile®**之类的软件和/或诸如iOS、Windows Phone、Android、BlackBerry 10，Palm OS之类的各种移动操作系统。设备可以支持各种应用(诸如各种互联网相关的应用、电子邮件、短消息服务(SMS)应用)，并且可以使用各种其它通信协议。客户端计算设备还可以包括通用个人计算机，作为示例，其包括运行各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统的个人计算机和/或膝上型计算机。客户端计算设备可以是运行任何各种商用的**UNIX®**或类UNIX操作系统(包括但不限于诸如例如Google Chrome OS的各种GNU/Linux操作系统)的工作站计算机。客户端计算设备还可以包括能够通过(一个或多个)网络710进行通信的电子设备(诸如瘦客户端计算

机、启用互联网的游戏系统(例如,具有或不具有**Kinect®**手势输入设备的Microsoft **Xbox®**游戏控制台)和/或个人消息传送设备)。

[0122] 虽然图7中的分布式系统700被示为具有四个客户端计算设备,但是可以支持任何数量的客户端计算设备。其它设备(诸如具有传感器的设备等)可以与服务器712交互。

[0123] 分布式系统700中的(一个或多个)网络710可以是对本领域技术人员熟悉的可以利用任何各种可用协议支持数据通信的任何类型的网络,其中这些协议包括但不限于TCP/IP(传输控制协议/互联网协议)、SNA(系统网络体系架构)、IPX(互联网分组交换)、AppleTalk等。仅仅作为示例,(一个或多个)网络710可以是局域网(LAN)、基于以太网的网络、令牌环、广域网、互联网、虚拟网络、虚拟专用网络(VPN)、内联网、外联网、公共交换电话网络(PSTN)、红外网络、无线网络(例如,在任何电气和电子协会(IEEE)1002.11协议套件、**Bluetooth®**、和/或任何其它无线协议下操作的网络)和/或这些网络和/或其它网络的任意组合。

[0124] 服务器712可以由一个或多个通用计算机、专用服务器计算机(作为示例,包括PC(个人计算机)服务器、**UNIX®**服务器、中档服务器、大型计算机、机架安装的服务器等)、服务器场、服务器集群或任何其它适当的布置和/或组合组成。服务器712可以包括运行虚拟操作系统的一个或多个虚拟机,或涉及虚拟化的其它计算体系架构。一个或多个灵活的逻辑存储设备池可以被虚拟化,以维护用于服务器的虚拟存储设备。虚拟网络可以由服务器712利用软件定义的联网来控制。在各种实施例中,服务器712可以适于运行在前述公开中描述的一个或多个服务或软件应用。例如,服务器712可以与根据本公开一些实施例的用于执行如上所述的处理的服务器对应。

[0125] 服务器712可以运行包括以上讨论的任何操作系统的操作系统,以及任何商用的服务器操作系统。服务器712还可以运行任何各种附加的服务器应用和/或中间层应用,包括HTTP(超文本传输协议)服务器、FTP(文件传输协议)服务器、CGI(公共网关接口)服务器、**JAVA®**服务器、数据库服务器等。示例性数据库服务器包括但不限于可从Oracle、Microsoft、Sybase、IBM(国际商业机器)等商业获得的数据库服务器。

[0126] 在一些实现中,服务器712可以包括一个或多个应用,以分析和整合从客户端计算设备702、704、706和708的用户接收到的数据馈送和/或事件更新。作为示例,数据馈送和/或事件更新可以包括但不限于从一个或多个第三方信息源和连续数据流接收到的**Twitter®**馈送、**Facebook®**更新或实时更新,连续数据流可以包括与传感器数据应用、金融报价机、网络性能测量工具(例如,网络监视和流量管理应用)、点击流分析工具、汽车流量监视等相关的实时事件。服务器712还可以包括经由客户端计算设备702、704、706和708的一个或多个显示设备显示数据馈送和/或实时事件的一个或多个应用。

[0127] 分布式系统700还可以包括一个或多个数据库714和716。这些数据库可以提供用于存储信息(诸如库存信息和由示例实施例使用的其它信息)的机制。数据库714和716可以驻留在各种位置中。作为示例,数据库714和716中的一个或多个可以驻留在服务器712本地(和/或驻留在其中)的非瞬态存储介质上。可替代地,数据库714和716可以远离服务器712,并且经由基于网络的连接或专用的连接与服务器712通信。在一组实施例中,数据库714和

716可以驻留在存储区域网络(SAN)中。类似地,用于执行服务器712所具有的功能的任何必要的文件可以适当地本地存储在服务器712上和/或远程存储。在一组实施例中,数据库714和716可以包括关系数据库(诸如由Oracle提供的数据库),其适于响应于SQL格式的命令而存储、更新和检索数据。

[0128] 在一些实施例中,上述消息输送服务可以经由云环境作为服务提供。图8示出根据一些实施例的、在其中服务可以作为云服务被提供的系统环境的一个或多个部件的简化框图。

[0129] 在图8所示的实施例中,系统环境800包括一个或多个客户端计算设备804、806和808,这一个或多个客户端计算设备804、806和808可以被用户用来与提供云服务(包括用于响应于使用模式而动态修改文档(例如,网页)的服务)的云基础设施系统802交互。云基础设施系统802可以包括一个或多个计算机和/或服务器,这一个或多个计算机和/或服务器可以包括上面针对服务器712所描述的那些计算机和/或服务器。

[0130] 应当认识到的是,图8中所绘出的云基础设施系统802可以具有除所绘出的那些部件之外的其它部件。另外,图8中所示的实施例仅仅是可以结合其中一些实施例的云基础设施系统的一个示例。在一些其它实施例中,云基础设施系统802可以具有比图中所示出的更多或更少的部件、可以组合两个或更多个部件、或者可以具有不同的部件配置或布置。

[0131] 客户端计算设备804、806和808可以是与上面针对702、704、706和708所描述的那些设备相似的设备。客户端计算设备804、806和808可以被配置为操作客户端应用(诸如web浏览器、专有客户端应用(例如,Oracle Forms)或可以被客户端计算设备的用户使用以与云基础设施系统1302交互来使用由云基础设施系统802提供的服务的一些其它应用)。虽然示例性系统环境800被示为具有三个客户端计算设备,但是可以支持任何数量的客户端计算设备。其它设备(诸如具有传感器的设备等)可以与云基础设施系统802交互。

[0132] (一个或多个)网络810可以促进客户端804、806和808与云基础设施系统802之间的数据通信和交换。每个网络可以是对本领域技术人员熟悉的、可以利用任何各种商用的协议支持数据通信的任何类型的网络,其中这些协议包括以上针对(一个或多个)网络710所描述的那些协议。

[0133] 在某些实施例中,由云基础设施系统802提供的服务可以包括对云基础设施系统的用户按需可用的一系列服务。除了与账户管理相关的服务之外,也可以提供各种其它服务,包括但不限于在线数据存储和备份解决方案、基于Web的电子邮件服务、托管的办公套件和文档协作服务、数据库处理、受管理的技术支持服务等。由云基础设施系统提供的服务可以动态扩展,以满足其用户的需求。

[0134] 在某些实施例中,由云基础设施系统802提供的服务的具体实例化在本文中可以被称为“服务实例”。一般而言,经由通信网络(诸如互联网)从云服务提供者的系统使得对用户可用的任何服务被称为“云服务”。通常,在公共云环境中,构成云服务提供者的系统的服务器和系统与客户自己的本地服务器和系统不同。例如,云服务提供者的系统可以托管应用,并且用户可以经由诸如互联网的通信网络按需订购和使用应用。

[0135] 在一些示例中,计算机网络云基础设施中的服务可以包括对由云供应商向用户或者如本领域中另外已知方式提供的存储装置、托管的数据库、托管的web服务器、软件应用或者其它服务的受保护的计算机网络访问。例如,服务可以包括通过互联网对云上的远程

存储装置的受密码保护的访问。作为另一个示例，服务可以包括基于web服务的托管的关系数据库和脚本语言中间件引擎，用于由联网的开发人员专门使用。作为另一个示例，服务可以包括对在云供应商的web站点上托管的电子邮件软件应用的访问。

[0136] 在某些实施例中，云基础设施系统802可以包括以自助服务、基于订阅、弹性可扩展、可靠、高度可用和安全的方式交付给客户的应用套件、中间件和数据库服务产品。这种云基础设施系统的示例是由本受让人提供的Oracle Public Cloud(Oracle公共云)。

[0137] 云基础设施系统802还可以提供与“大数据”相关的计算和分析服务。术语“大数据”一般用来指可由分析员和研究者存储和操纵以可视化大量数据、检测趋势和/或以其它方式与数据交互的极大数据集。这种大数据和相关应用可以在许多级别和不同规模上由基础设施系统托管和/或操纵。并行链接的数十个、数百个或数千个处理器可以作用于这种数据，以便呈现该数据、或者模拟对数据或数据所表示的内容的外力。这些数据集可以涉及结构化数据(诸如在数据库中组织或以其它方式根据结构化模型组织的数据)和/或非结构化数据(例如，电子邮件、图像、数据blob(二进制大对象)、web页面、复杂事件处理)。通过利用一些实施例相对快速地将更多(或更少)的计算资源聚焦在目标上的能力，云基础设施系统可以更好地用于基于来自企业、政府机构、研究组织、私人个人、一群志同道合的个人或组织或其它实体的需求来在大数据集上实施任务。

[0138] 在各种实施例中，云基础设施系统802可以适于自动地供应、管理和跟踪客户对由云基础设施系统802提供的服务的订阅。云基础设施系统802可以经由不同的部署模型来提供云服务。例如，服务可以在公共云模型下提供，其中云基础设施系统802由销售云服务的组织拥有(例如，由Oracle公司拥有)并且使服务对一般公众或不同的工业企业可用。作为另一个示例，服务可以在私有云模型下提供，其中云基础设施系统802仅针对单个组织操作，并且可以为组织内的一个或多个实体提供服务。云服务还可以在社区云模型下提供，其中云基础设施系统802和由云基础设施系统802提供的服务由相关社区中的若干个组织共享。云服务还可以在混合云模型下提供，混合云模型是两个或更多个不同模型的组合。

[0139] 在一些实施例中，由云基础设施系统802提供的服务可以包括在软件即服务(SaaS)类别、平台即服务(PaaS)类别、基础设施即服务(IaaS)类别、或包括混合服务的其它服务类别下提供的一个或多个服务。客户经由订阅订单可以订购由云基础设施系统802提供的一个或多个服务。云基础设施系统802然后执行处理，以提供客户的订阅订单中的服务。

[0140] 在一些实施例中，由云基础设施系统802提供的服务可以包括但不限于应用服务、平台服务和基础设施服务。在一些示例中，应用服务可以由云基础设施系统经由SaaS平台提供。SaaS平台可以被配置为提供属于SaaS类别的云服务。例如，SaaS平台可以提供在集成的开发和部署平台上构建和交付点播应用套件的能力。SaaS平台可以管理和控制用于提供SaaS服务的底层软件和基础设施。通过利用由SaaS平台提供的服务，客户可以利用在云基础设施系统上执行的应用。客户可以获取应用服务，而无需客户购买单独的许可证和支持。可以提供各种不同的SaaS服务。示例包括但不限于为大型组织提供用于销售绩效管理、企业集成和业务灵活性的解决方案的服务。

[0141] 在一些实施例中，平台服务可以由云基础设施系统802经由PaaS平台提供。PaaS平台可以被配置为提供属于PaaS类别的云服务。平台服务的示例可以包括但不限于使组织

(诸如Oracle)能够在共享的公共体系架构上整合现有应用的服务,以及利用由平台提供的共享服务构建新应用的能力。PaaS平台可以管理和控制用于提供PaaS服务的底层软件和基础设施。客户可以获取由云基础设施系统802提供的PaaS服务,而无需客户购买单独的许可证和支持。平台服务的示例包括但不限于Oracle Java云服务(JCS)、Oracle数据库云服务(DBCS)以及其它。

[0142] 通过利用由PaaS平台提供的服务,客户可以采用由云基础设施系统支持的编程语言和工具,并且还控制所部署的服务。在一些实施例中,由云基础设施系统提供的平台服务可以包括数据库云服务、中间件云服务(例如,Oracle Fusion Middleware服务)和Java云服务。在一个实施例中,数据库云服务可以支持共享服务部署模型,其使得组织能够汇集数据库资源并且以数据库云的形式向客户提供数据库即服务。在云基础设施系统中,中间件云服务可以为客户提供开发和部署各种业务应用的平台,并且Java云服务可以为客户提供部署Java应用的平台。

[0143] 可以由云基础设施系统中的IaaS平台提供各种不同的基础设施服务。基础设施服务促进底层计算资源(诸如存储装置、网络和其它基本计算资源)的管理和控制,以便客户利用由SaaS平台和PaaS平台提供的服务。

[0144] 在某些实施例中,云基础设施系统802还可以包括基础设施资源830,用于提供用来向云基础设施系统的客户提供各种服务的资源。在一个实施例中,基础设施资源830可以包括执行由PaaS平台和SaaS平台提供的服务的硬件(诸如服务器、存储装置和联网资源)的预先集成和优化的组合,以及其它资源。

[0145] 在一些实施例中,云基础设施系统802中的资源可以由多个用户共享并且按需动态地重新分配。此外,资源可以以不同时区分配给用户。例如,云基础设施系统802可以使第一时区中的第一用户集合在指定的小时数内能够利用云基础设施系统的资源,并且然后使得能够将相同资源重新分配给位于不同时区中的另一用户集合,从而最大化资源的利用率。

[0146] 在某些实施例中,可以提供由云基础设施系统802的不同部件或模块共享的多个内部共享服务832,以使得能够由云基础设施系统802供应服务。这些内部共享服务可以包括但不限于安全和身份服务、集成服务、企业储存库服务、企业管理器服务、病毒扫描和白名单服务、高可用性、备份和恢复服务、用于启用云支持的服务、电子邮件服务、通知服务、文件传输服务等。

[0147] 在某些实施例中,云基础设施系统802可以提供对云基础设施系统中的云服务(例如,SaaS、PaaS和IaaS服务)的综合管理。在一个实施例中,云管理功能可以包括用于供应、管理和跟踪由云基础设施系统802等接收到的客户的订阅的能力。

[0148] 在一个实施例中,如图8中所绘出的,云管理功能可以由诸如订单管理模块820、订单编排模块822、订单供应模块824、订单管理和监视模块826以及身份管理模块828的一个或多个模块提供。这些模块可以包括一个或多个计算机和/或服务器,或可以利用一个或多个计算机和/或服务器来提供,该一个或多个计算机和/或服务器可以是通用计算机、专用服务器计算机、服务器场,服务器集群或任何其它适当的布置和/或组合。

[0149] 在示例性操作中,在834处,使用客户端设备(诸如客户端设备804、806或808)的客户可以通过请求由云基础设施系统802提供的一个或多个服务并且对由云基础设施系统

802提供的一个或多个服务的订阅下订单，来与云基础设施系统802交互。在某些实施例中，客户可以访问诸如云UI 812、云UI 814和/或云UI 816的云用户界面(UI)并经由这些UI下订阅订单。响应于客户下订单而由云基础设施系统802接收到的订单信息可以包括识别客户以及客户打算订阅的由云基础设施系统802提供的一个或多个服务的信息。

[0150] 在836处，从客户接收到的订单信息可以存储在订单数据库818中。如果这是新的订单，则可以为该订单创建新的记录。在一个实施例中，订单数据库818可以是由云基础设施系统818操作的若干数据库当中的一个，并且与其它系统元件结合操作。

[0151] 在838处，订单信息可以被转发到订单管理模块820，订单管理模块820可以被配置为执行与订单相关的计费和记帐功能，诸如验证订单以及在通过验证时预订订单。

[0152] 在840处，关于订单的信息可以被传送到订单编排模块822，订单编排模块822被配置为编排用于由客户下的订单的服务和资源的供应。在一些情况下，订单编排模块822可以使用订单供应模块824的服务以用于供应。在某些实施例中，订单编排模块822使得能够管理与每个订单相关联的业务过程，并且应用业务逻辑来确定订单是否应当继续供应。

[0153] 如图8中绘出的实施例所示，在842处，在接收到新订阅的订单时，订单编排模块822向订单供应模块824发送分配资源和配置履行订阅订单所需的资源的请求。订单供应模块824使得能够为由客户订购的服务分配资源。订单供应模块824提供由云基础设施系统800提供的云服务和用来供应用于提供所请求的服务的资源的物理实现层之间的抽象级别。这使得订单编排模块824能够与实现细节隔离，诸如服务和资源实际上是实时供应，还是预先供应并且仅在请求时才进行分配/指定。

[0154] 在844处，一旦供应了服务和资源，就可以向进行订阅的客户发送指示所请求的服务现在已准备好用于使用的通知。在一些情况下，可以向客户发送使得客户能够开始使用所请求的服务的信息(例如，链接)。

[0155] 在846处，可以由订单管理和监视模块826来管理和跟踪客户的订阅订单。在一些情况下，订单管理和监视模块826可以被配置为收集关于客户使用所订阅的服务的使用统计数据。例如，可以针对所使用的存储量、所传送的数据量、用户的数量以及系统启动时间和系统停机时间的量等来收集统计数据。

[0156] 在某些实施例中，云基础设施系统800可以包括身份管理模块828，其被配置为提供身份服务，诸如云基础设施系统800中的访问管理和授权服务。在一些实施例中，身份管理模块828可以控制关于希望利用由云基础设施系统802提供的服务的客户的信息。这种信息可以包括认证这些客户的身份的信息以及描述那些客户被授权相对于各种系统资源(例如，文件、目录、应用、通信端口、存储器段等)执行的动作的信息。身份管理模块828还可以包括关于每个客户的描述性信息以及关于如何和由谁来访问和修改这些描述性信息的管理。

[0157] 图9示出根据一些示例性实施例的、可以被用于实现某些元件的示例性计算机系统。在一些实施例中，计算机系统900可以被用来实现上述任何各种服务器和计算机系统。如图9所示，计算机系统900包括各种子系统，包括经由总线子系统902与多个外围子系统通信的处理单元904。这些外围子系统可以包括处理加速单元906、I/O子系统908、存储子系统918和通信子系统924。存储子系统918可以包括有形的计算机可读存储介质922和系统存储器910。

[0158] 总线子系统902提供用于让计算机系统900的各种部件和子系统按照期望彼此通信的机制。虽然总线子系统902被示意性地示为单个总线，但是总线子系统的可替代实施例可以利用多个总线。总线子系统902可以是若干种类型的总线结构中的任何一种，包括利用任何各种总线体系架构的存储器总线或存储器控制器、外围总线和局部总线。例如，此类体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围部件互连(PCI)总线，其可以实现为根据IEEE P1386.1标准制造的夹层(Mezzanine)总线，等等。

[0159] 处理子系统904控制计算机系统900的操作并且可以包括一个或多个处理单元932、934等。处理单元可以包括一个或多个处理器，其包括单核或多核处理器、处理器的一个或多个核、或其组合。在一些实施例中，处理子系统904可以包括一个或多个专用协处理器，诸如图形处理器、数字信号处理器(DSP)等。在一些实施例中，处理子系统904的处理单元中的一些或全部可以利用定制电路来实现，诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)。

[0160] 在一些实施例中，处理子系统904中的处理单元可以执行存储在系统存储器910中或计算机可读存储介质922上的指令。在各种实施例中，处理单元可以执行各种程序或代码指令，并且可以维护多个并发执行的程序或进程。在任何给定的时间，要执行的程序代码中的一些或全部可以驻留在系统存储器910中和/或计算机可读存储介质910上，潜在地包括在一个或多个存储设备上。通过适当的编程，处理子系统904可以提供上述用于响应于使用模式而动态修改文档(例如，web页面)的各种功能。

[0161] 在某些实施例中，可以提供处理加速单元906，用于执行定制的处理或用于卸载由处理子系统904执行的一些处理，以便加速由计算机系统900执行的整体处理。

[0162] I/O子系统908可以包括用于向计算机系统900输入信息和/或用于从或经由计算机系统900输出信息的设备和机制。一般而言，术语“输入设备”的使用旨在包括用于向计算机系统900输入信息的所有可能类型的设备和机制。用户接口输入设备可以包括，例如，键盘、诸如鼠标或轨迹球的指示设备、结合到显示器中的触摸板或触摸屏、滚轮、点拨轮、拨盘、按钮、开关、键板、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备也可以包括使用户能够控制输入设备并与其交互的诸如Microsoft **Kinect®**运动传感器的运动感测和/或姿势识别设备、Microsoft **Xbox®** 360游戏控制器、提供用于接收利用姿势和口语命令的输入的接口的设备。用户接口输入设备也可以包括眼睛姿势识别设备，诸如从用户检测眼睛活动(例如，当拍摄图片和/或进行菜单选择时的“眨眼”)并将眼睛姿势转换为到输入设备(例如，Google **Glass®**)中的输入的Google **Glass®**眨眼检测器。此外，用户接口输入设备可以包括使用户能够通过语音命令与语音识别系统(例如，**Siri®**导航器)交互的语音识别感测设备。

[0163] 用户接口输入设备的其它示例包括但不限于三维(3D)鼠标、操纵杆或指示杆、游戏板和图形平板、以及音频/视频设备，诸如扬声器、数字相机、数字摄像机、便携式媒体播放器、网络摄像机、图像扫描仪、指纹扫描仪、条形码读取器3D扫描仪、3D打印机、激光测距仪、以及眼睛注视跟踪设备。此外，用户接口输入设备可以包括例如医疗成像输入设备，诸如计算机断层摄影、磁共振成像、位置发射断层摄影、医疗超声检查设备。用户接口输入设

备也可以包括例如音频输入设备，诸如MIDI键盘、数字乐器等。

[0164] 用户接口输出设备可以包括显示子系统、指示器灯或诸如音频输出设备的非可视显示器等。显示子系统可以是阴极射线管(CRT)、诸如利用液晶显示器(LCD)或等离子体显示器的平板设备、投影设备、触摸屏等。一般而言，术语“输出设备”的使用旨在包括用于从计算机系统900向用户或其它计算机输出信息的所有可能类型的设备和机制。例如，用户接口输出设备可以包括但不限于，可视地传达文本、图形和音频/视频信息的各种显示设备，诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备和调制解调器。

[0165] 存储子系统918提供用于存储由计算机系统900使用的信息的储存库或数据存储。存储子系统918提供有形非瞬态计算机可读存储介质，用于存储提供一些实施例的功能的基本编程和数据结构。当由处理子系统904执行时提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统918中。软件可以由处理子系统904的一个或多个处理单元执行。存储子系统918也可以提供用于存储根据示例实施例使用的数据的储存库。

[0166] 存储子系统918可以包括一个或多个非瞬态存储器设备，包括易失性和非易失性存储器设备。如图9所示，存储子系统918包括系统存储器910和计算机可读存储介质922。系统存储器910可以包括多个存储器，包括用于在程序执行期间存储指令和数据的易失性主随机存取存储器(RAM)和其中存储固定指令的非易失性只读存储器(ROM)或闪存存储器。在一些实现中，包含帮助在诸如启动期间在计算机系统900内的元件之间传送信息的基本例程的基本输入/输出系统(BIOS)通常可以存储在ROM中。RAM通常包含当前由处理子系统904操作和执行的数据和/或程序模块。在一些实现中，系统存储器910可以包括多个不同类型的存储器，诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。

[0167] 作为示例而非限制，如在图9中所绘出的，系统存储器910可以存储应用程序912，其可以包括客户端应用、Web浏览器、中间层应用、关系数据库管理系统(RDBMS)等、程序数据914和操作系统916。作为示例，操作系统916可以包括各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种商用**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统、Google **Chrome®**OS等)和/或诸如iOS、**Windows®** Phone、**Android®**OS、**BlackBerry®** 10OS和**Palm®** OS操作系统的移动操作系统。

[0168] 计算机可读存储介质922可以存储提供一些实施例的功能的编程和数据构造。当由处理子系统904执行时使处理器提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统918中。作为示例，计算机可读存储介质922可以包括非易失性存储器，诸如硬盘驱动器、磁盘驱动器、诸如CD ROM、DVD、**Blu-Ray®** (蓝光)盘或其它光学介质的光盘驱动器。计算机可读存储介质922可以包括但不限于，**Zip®**驱动器、闪存存储器卡、通用串行总线(USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质922也可以包括基于非易失性存储器的固态驱动器(SSD)(诸如基于闪存存储器的SSD、企业闪存驱动器、固态ROM等)、基于易失性存储器的SSD(诸如基于固态RAM、动态RAM、静态RAM、DRAM的SSD、磁阻RAM(MRAM)SSD)，以及使用基于DRAM和基于闪存存储器的SSD的组合的混合SSD。计算机可读介质922可以为计算机系统900提供计算机可读指令、数据结构、程序模块和其它

数据的存储。

[0169] 在某些实施例中，存储子系统900也可以包括计算机可读存储介质读取器920，其可以进一步连接到计算机可读存储介质922。计算机可读存储介质922与系统存储器910一起和可选地相组合，可以全面地表示用于存储计算机可读信息的远程、本地、固定和/或可移动存储设备加上存储介质。

[0170] 在某些实施例中，计算机系统900可以提供对执行一个或多个虚拟机的支持。计算机系统900可以执行诸如管理程序之类的程序，以便促进虚拟机的配置和管理。每个虚拟机可以被分配存储器资源、计算资源(例如，处理器、内核)、I/O资源和联网资源。每个虚拟机通常运行其自己的操作系统，其可以与由计算机系统900执行的其它虚拟机执行的操作系统相同或不同。相应地，多个操作系统可以潜在地由计算机系统900并发地运行。每个虚拟机一般独立于其它虚拟机运行。

[0171] 通信子系统924提供到其它计算机系统和网络的接口。通信子系统924用作用于从计算机系统900的其它系统接收数据和向其发送数据的接口。例如，通信子系统924可以使计算机系统900能够经由互联网建立到一个或多个客户端设备的通信信道，用于从客户端设备接收信息和发送信息到客户端设备。

[0172] 通信子系统924可以支持有线和/或无线通信协议两者。例如，在某些实施例中，通信子系统924可以包括用于(例如，使用蜂窝电话技术、高级数据网络技术(诸如3G、4G或EDGE(全球演进的增强数据速率)、WiFi(IEEE 802.11族标准)、或其它移动通信技术、或其任意组合)接入无线语音和/或数据网络的射频(RF)收发器部件、全球定位系统(GPS)接收器部件和/或其它部件。在一些实施例中，作为无线接口的附加或替代，通信子系统924可以提供有线网络连接(例如，以太网)。

[0173] 通信子系统924可以以各种形式接收和发送数据。例如，在一些实施例中，通信子系统924可以以结构化和/或非结构化的数据馈送926、事件流928、事件更新930等形式接收输入通信。例如，通信子系统924可以被配置为实时地从社交媒体网络的用户和/或其它通信服务接收(或发送)数据馈送926(诸如**Twitter®**馈送、**Facebook®**更新、诸如丰富站点摘要(RSS)馈送的web馈送)和/或来自一个或多个第三方信息源的实时更新。

[0174] 在某些实施例中，通信子系统924可以被配置为以连续数据流的形式接收数据，连续数据流本质上可能是连续的或无界的没有明确结束，其中连续数据流可以包括实时事件的事件流928和/或事件更新930。生成连续数据的应用的示例可以包括例如传感器数据应用、金融报价机、网络性能测量工具(例如网络监视和流量管理应用)、点击流分析工具、汽车流量监视等。

[0175] 通信子系统924也可以被配置为向一个或多个数据库输出结构化和/或非结构化的数据馈送926、事件流928、事件更新930等，其中所述一个或多个数据库可以与耦合到计算机系统900的一个或多个流数据源计算机通信。

[0176] 计算机系统900可以是各种类型中的一种，包括手持便携式设备(例如，**iPhone®**蜂窝电话、**iPad®**计算平板、PDA)、可穿戴设备(例如，Google **Glass®**头戴式显示器)、个人计算机、工作站、大型机、信息站、服务器机架或任何其它数据处理系统。

[0177] 由于计算机和网络不断变化的性质，对图9中绘出的计算机系统900的描述旨在仅仅作为具体示例。具有比图9中所绘出的系统更多或更少部件的许多其它配置是可能的。基

于本文所提供的公开内容和教导，本领域普通技术人员将理解实现各种实施例的其它方式和/或方法。

[0178] 虽然已经描述了具体的示例实施例，但是各种修改、更改、替代构造和等效物也包含在本发明的范围之内。本发明的实施例不限于在某些特定数据处理环境内的操作，而是可以在多个数据处理环境内自由操作。此外，虽然已利用特定的一系列的事务和步骤描述了本发明的实施例，然而，对本领域技术人员应当清楚的是，本发明的范围不限于所描述的一系列的事务和步骤。上述实施例的各种特征和方面可以被单独或结合使用。

[0179] 另外，虽然已经利用硬件和软件的特定组合描述了示例实施例，但是应当认识到，硬件和软件的其它组合也在示例实施例的范围之内。示例实施例中的一些可以只用硬件、或只用软件、或利用其组合来实现。本文描述的各种过程可以在同一处理器或以任何组合的不同处理器上实现。相应地，在部件或模块被描述为被配置为执行某些操作的情况下，这种配置可以例如通过设计电子电路来执行操作、通过对可编程电子电路(诸如微处理器)进行编程来执行操作、或通过其任意组合来实现。进程可以利用各种技术来通信，包括但不限于用于进程间通信的常规技术，并且不同的进程对可以使用不同的技术，或者同一对进程可以在不同时间使用不同的技术。

[0180] 因而，说明书和附图应当在说明性而不是限制性的意义上考虑。然而，将清楚的是，在不背离权利要求中阐述的更广泛精神和范围的情况下，可以对其进行添加、减少、删除和其它修改和改变。因此，虽然已描述了具体的发明实施例，但是这些实施例不旨在进行限制。各种修改和等效物都在以下权利要求的范围之内。

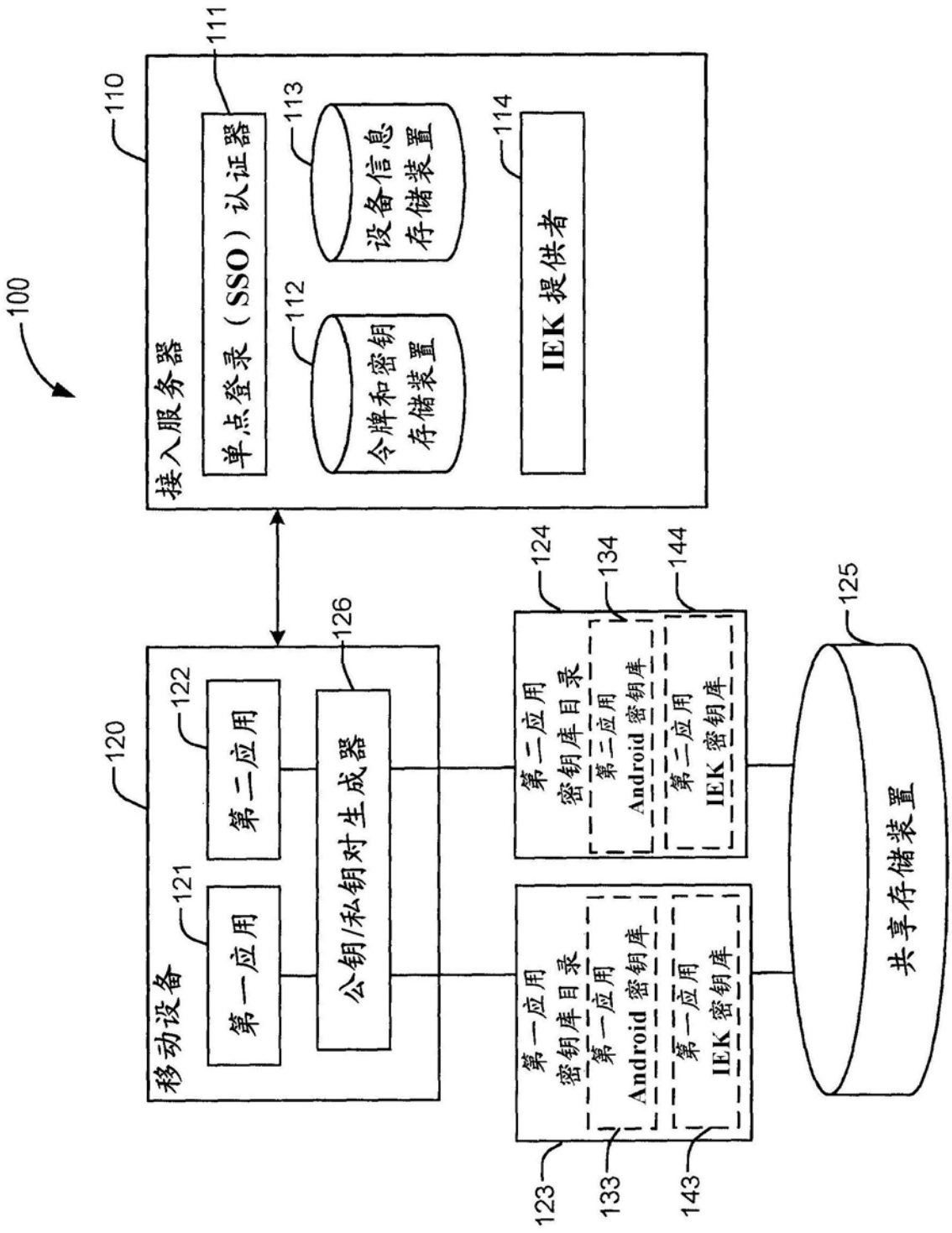

100
110
接入服务器
111
单点登录（SSO）认证器
112
令牌和密钥存储装置
113
设备信息存储装置
114
IEK 提供者
120
移动设备
121
第一应用
122
第二应用
126
公钥/私钥对生成器
123
第一应用密钥库目录
第一应用 Android 密钥库
第一应用 IEK 密钥库
124
第二应用密钥库目录
133
第二应用 Android 密钥库
143
第二应用 IEK 密钥库
144
125
共享存储装置

图1

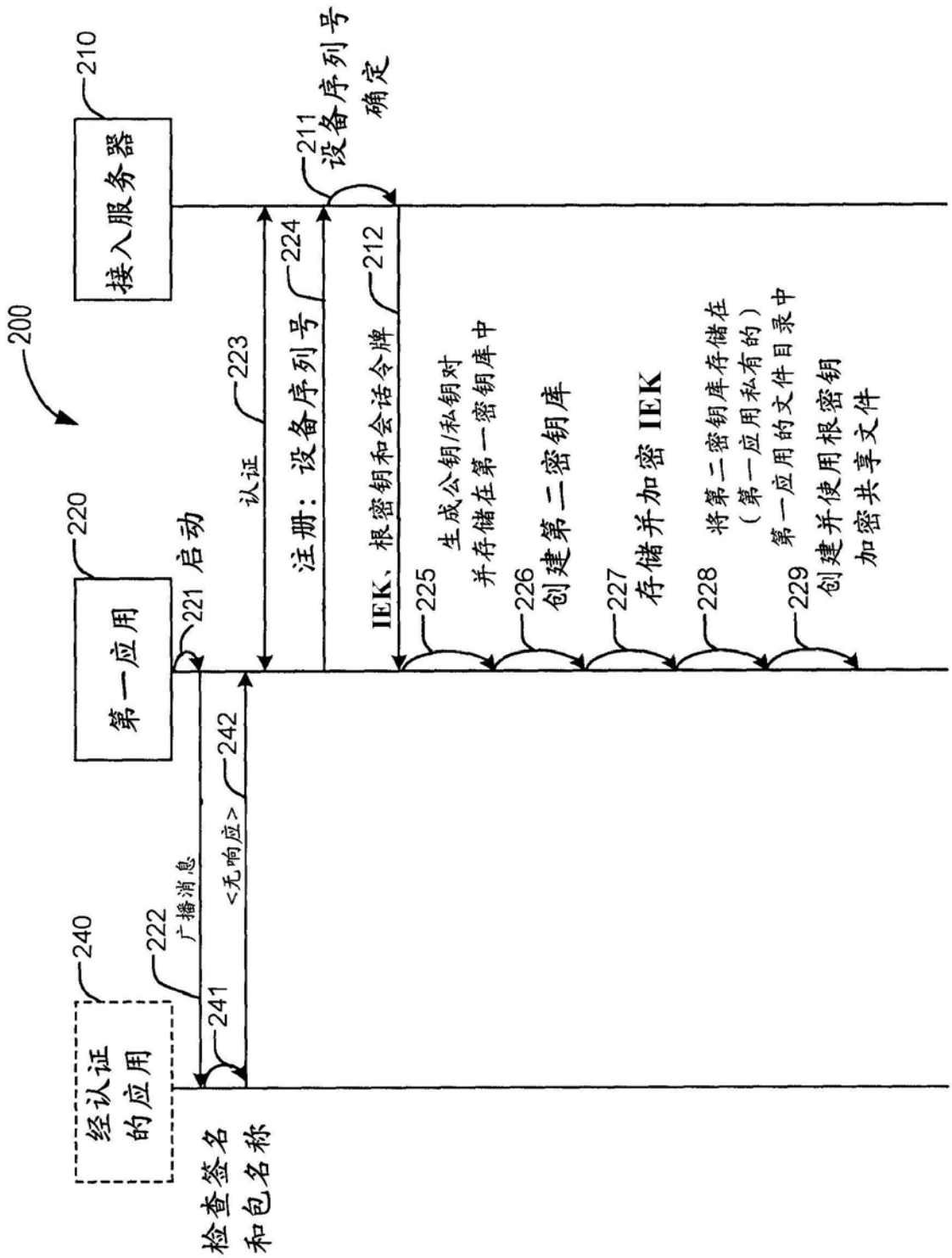

200
接入服务器
210
211 设备序列号确定
第一应用
220
221 启动
认证
223
注册：设备序列号
224
IEK、根密钥和会话令牌
212
225 生成公钥/私钥对并存储在第一密钥库中
226 创建第二密钥库
227 存储并加密 IEK
228 将第二密钥库存储在（第一应用私有的）第一应用的文件目录中
229 创建并使用根密钥加密共享文件
经认证的应用
240
222 广播消息
241
<无响应>
242
检查签名和包名称

图2

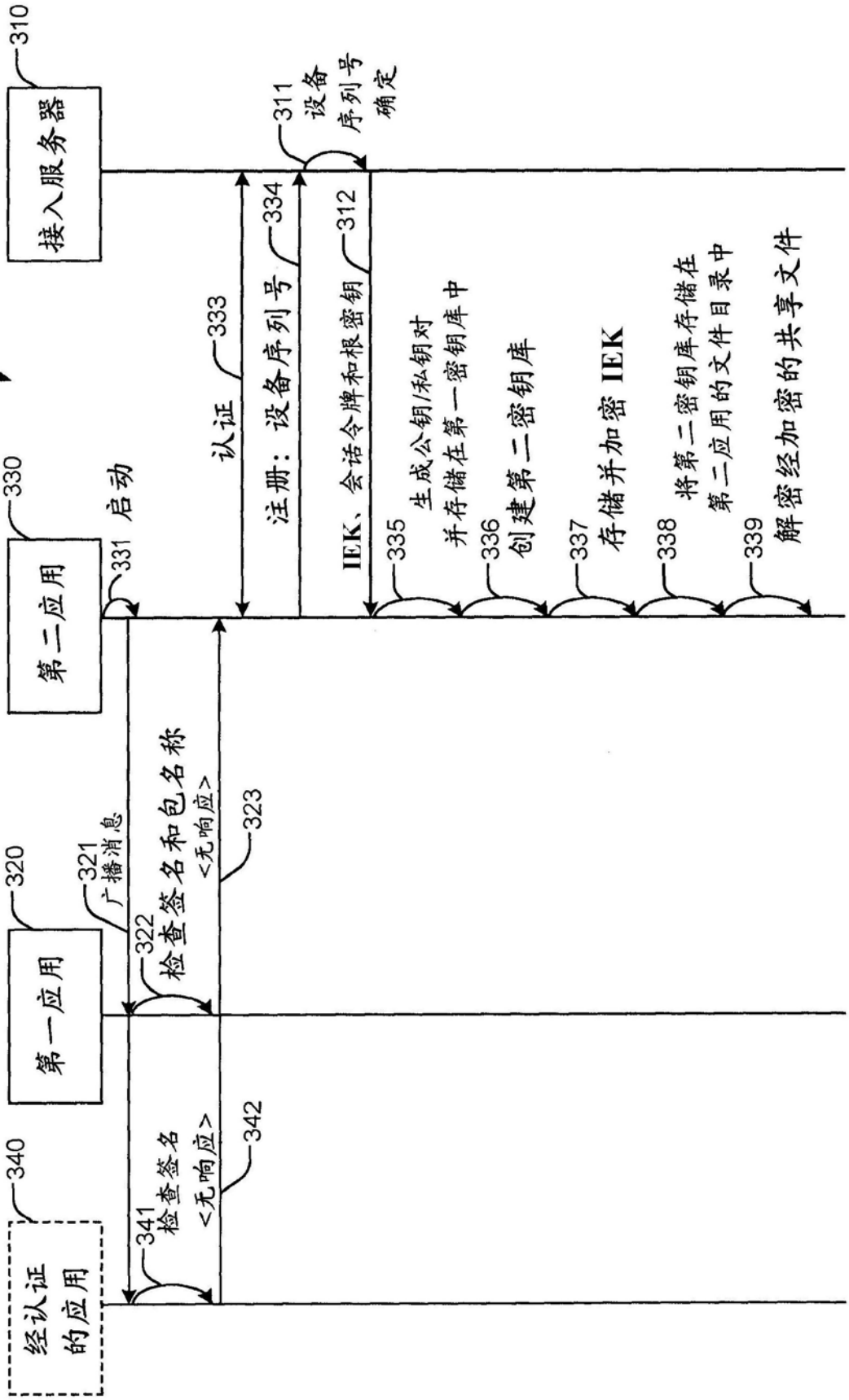

300
接入服务器
310
311
设备序列号确定
第二应用
330
331
启动
认证
333
注册：设备序列号
334
IEK、会话令牌和根密钥
312
335
生成公钥/私钥对并存储在第一密钥库中
336
创建第二密钥库
337
存储并加密 IEK
338
将第二密钥库存储在第二应用的文件目录中
339
解密经加密的共享文件
第一应用
320
321
广播消息
322
检查签名和包名称
<无响应>
323
经认证的应用
340
341
检查签名
<无响应>
342

图3

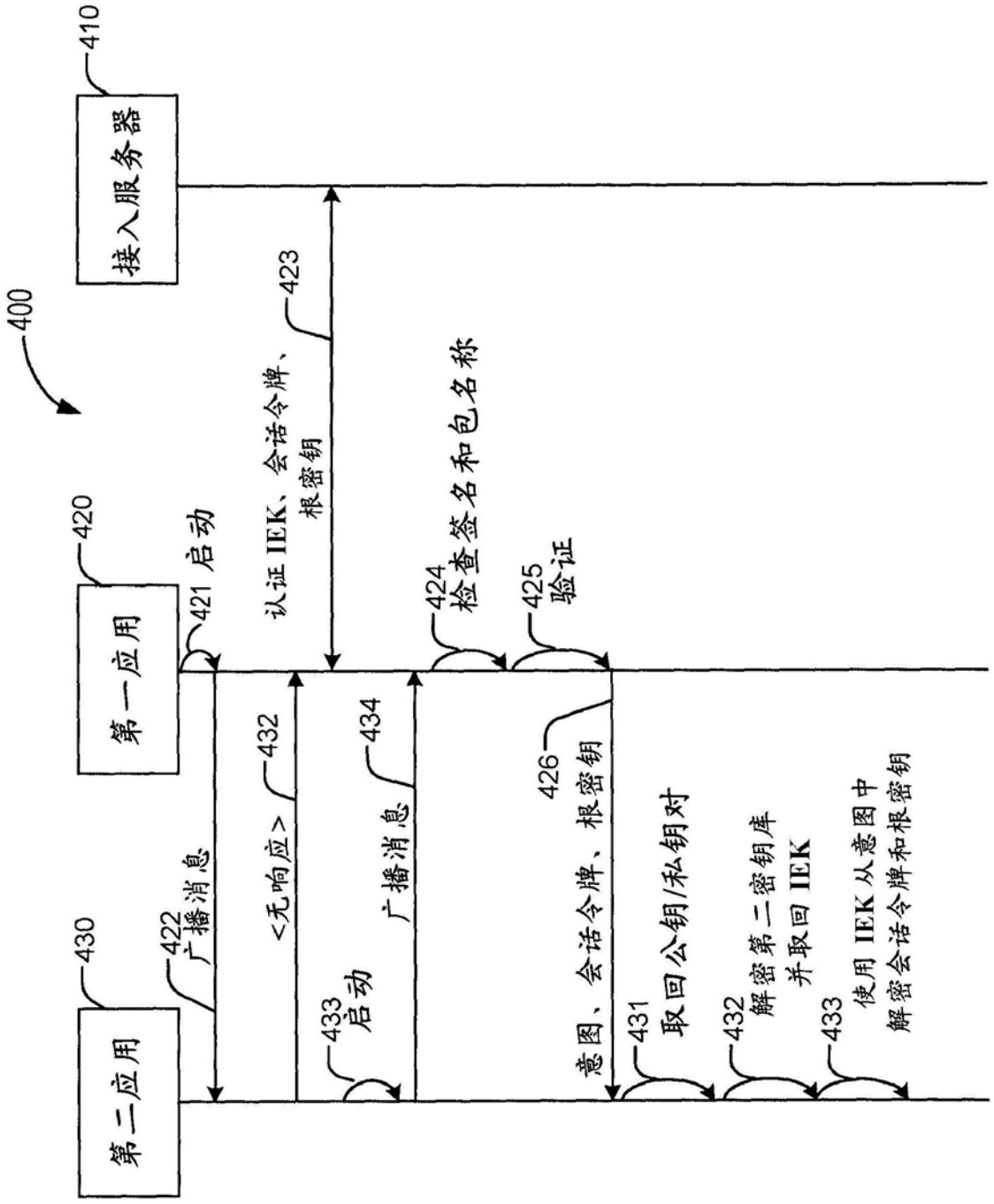

400
410
接入服务器
420
第一应用
430
第二应用
421 启动
422 广播消息
423 认证 IEK、会话令牌、根密钥
424 检查签名和包名称
425 验证
426 意图、会话令牌、根密钥
431 取回公钥/私钥对
432 解密第二密钥库并取回 IEK
433 使用 IEK 从意图中解密会话令牌和根密钥
<无响应> 432
433 启动
434 广播消息

图4

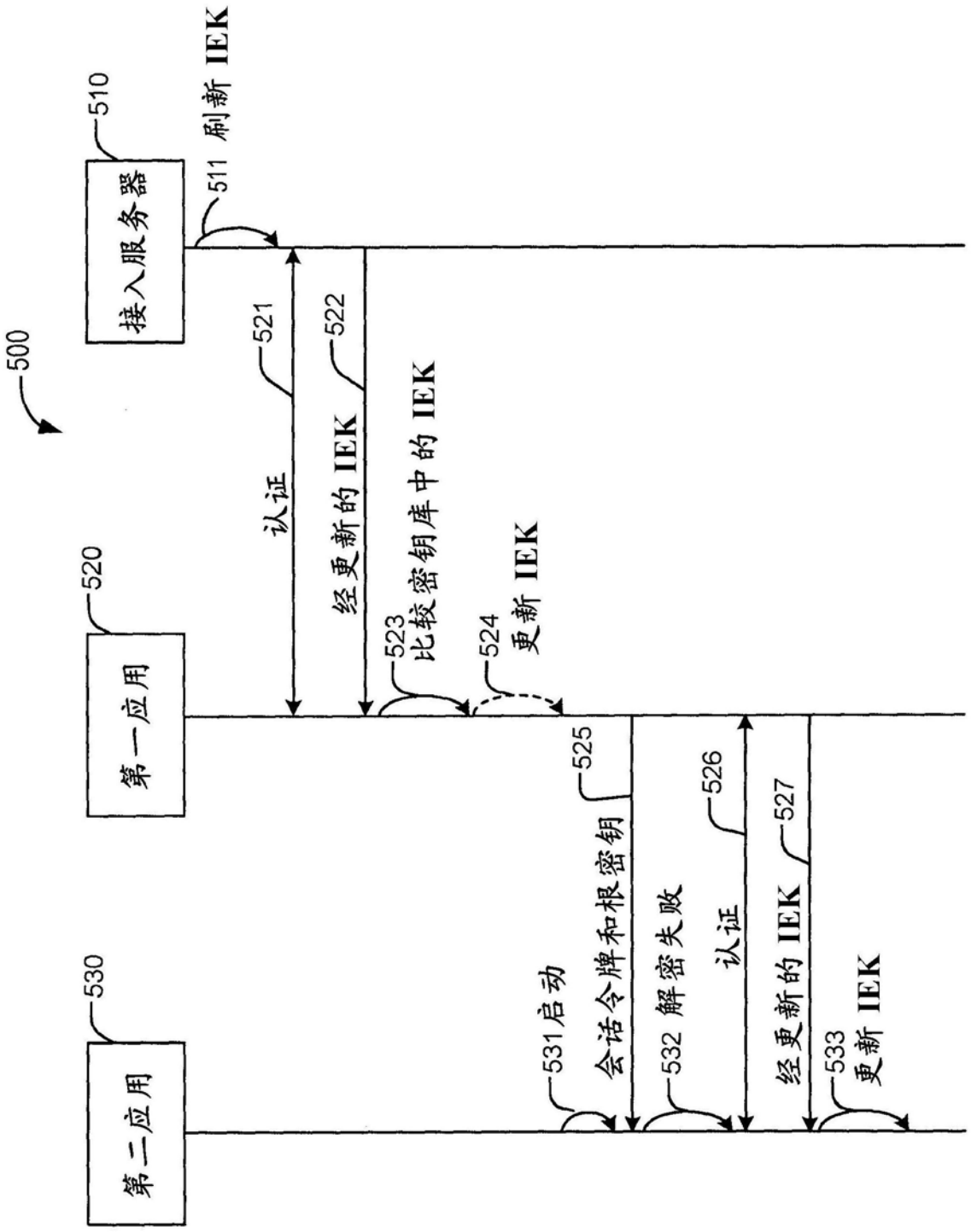

500
接入服务器
510
511 刷新 IEK
第一应用
520
521 认证
522 经更新的 IEK
523 比较密钥库中的 IEK
524 更新 IEK
第二应用
530
525
531启动
会话令牌和根密钥
526
532 解密失败
认证
527
经更新的 IEK
533
更新 IEK

图5

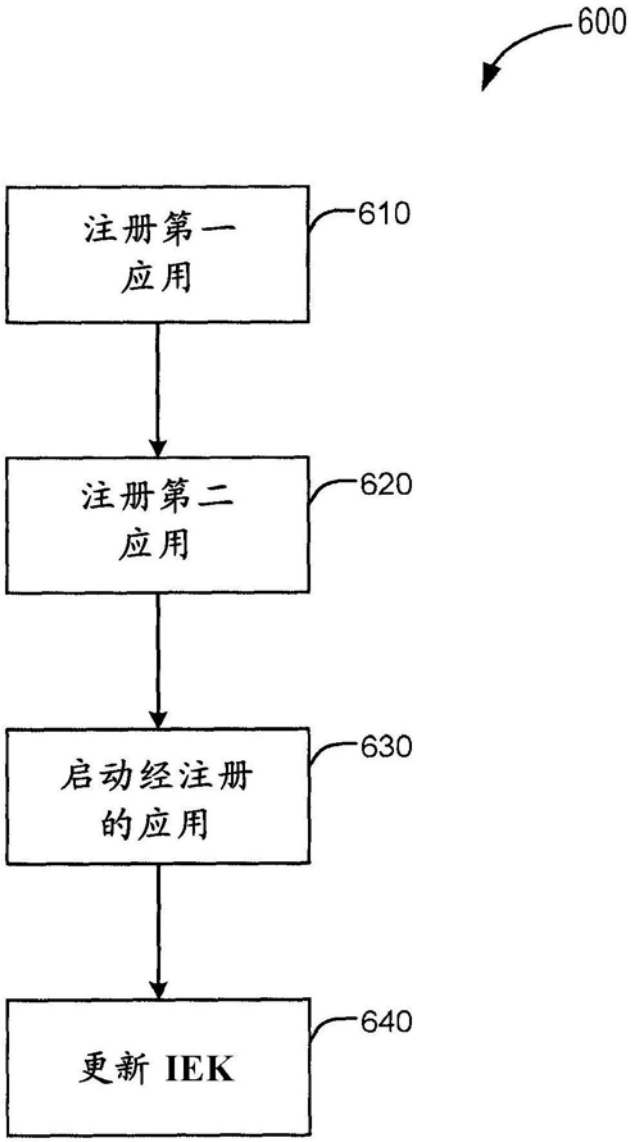


图6

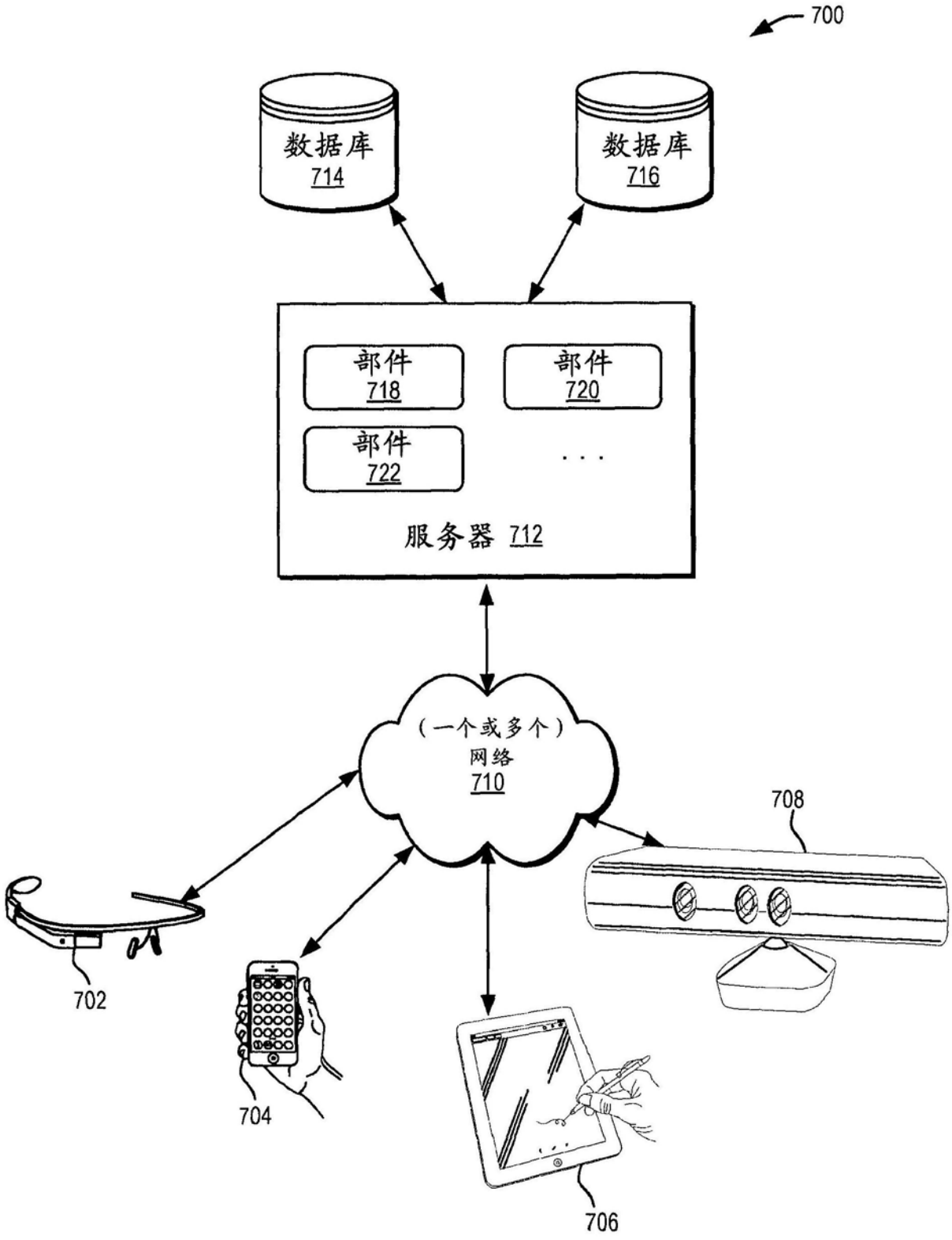

700
数据库
714
数据库
716
部件
718
部件
720
部件
722
. . .
服务器 712
（一个或多个）
网络
710
708
702
704
706

图7

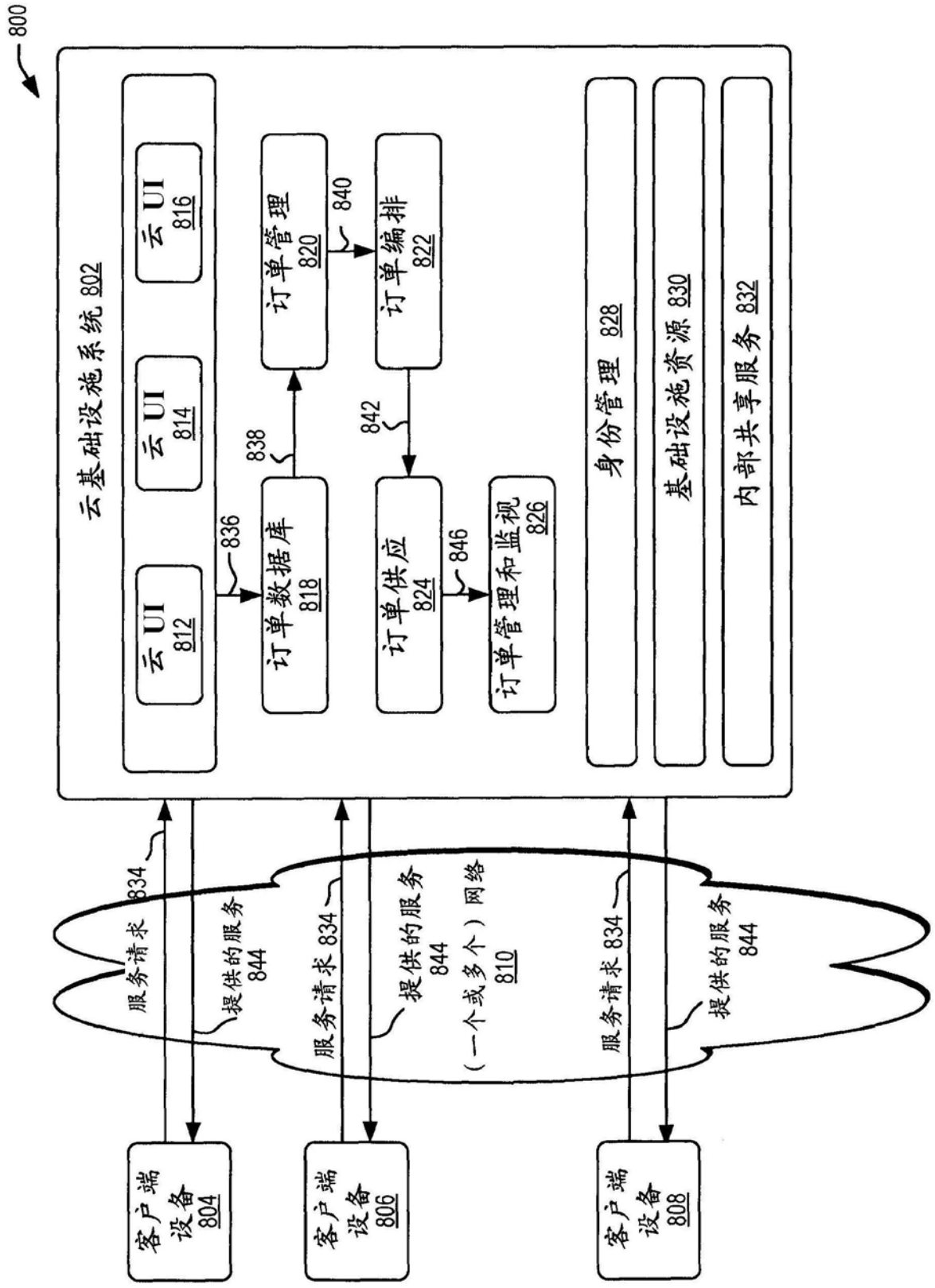

800
云基础设施系统 802
云 UI 812
云 UI 814
云 UI 816
订单数据库 818
订单管理 820
订单编排 822
订单供应 824
订单管理和监视 826
身份管理 828
基础设施资源 830
内部共享服务 832
836
838
840
842
846
服务请求 834
提供的服务 844
（一个或多个）网络 810
客户端设备 804
客户端设备 806
客户端设备 808

图8

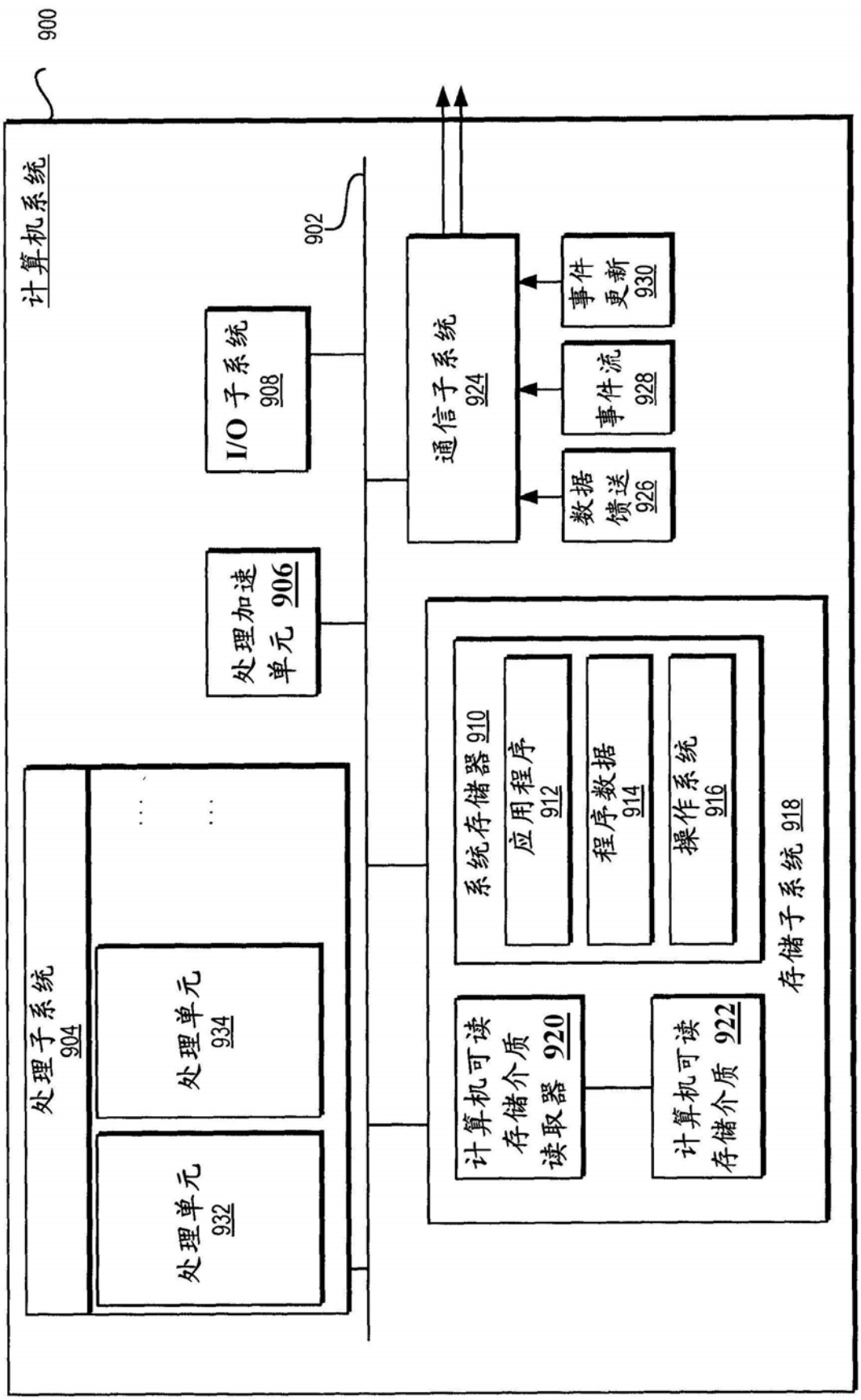

900
计算机系统
902
I/O 子系统 908
处理加速单元 906
通信子系统 924
数据馈送 926
事件流 928
事件更新 930
处理子系统 904
处理单元 932
处理单元 934
系统存储器 910
应用程序 912
程序数据 914
操作系统 916
存储子系统 918
计算机可读存储介质读取器 920
计算机可读存储介质 922

图9