(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118575448 A
(43)申请公布日 2024.08.30

(21)申请号 202280087816.5
(22)申请日 2022.11.10
(30)优先权数据
17/571,346 2022.01.07 US
(85)PCT国际申请进入国家阶段日
2024.07.05
(86)PCT国际申请的申请数据
PCT/US2022/079655 2022.11.10
(87)PCT国际申请的公布数据
WO2023/132997 EN 2023.07.13
(71)申请人 甲骨文国际公司
地址 美国
(72)发明人 D·L·斯塔斯卡尔 D·M·沃格
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 边海梅
(51)Int.Cl.
H04L 9/40(2006.01)

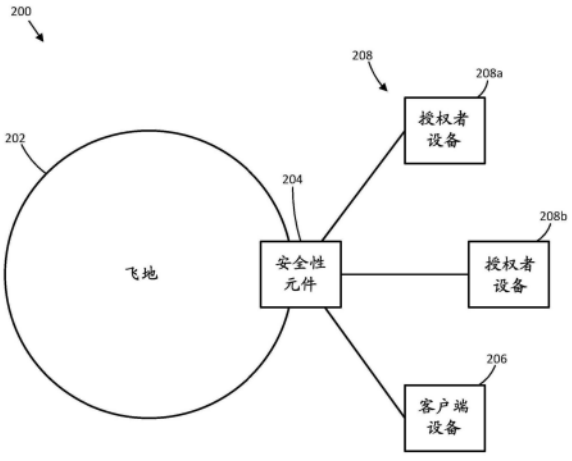
权利要求书3页 说明书32页 附图13页

(54)发明名称

基于法定人数的授权

(57)摘要

公开了一种用于管理用计算系统执行针对动作的授权的框架。例如,用于执行用户和/或客户端访问由云服务提供商(CSP)提供的基础设施服务的授权和/或用于用基础设施服务执行动作的技术包括:接收对基础设施服务要执行的动作的请求;识别要从其接收针对动作的授权的一个或多个授权者;确定要由云基础设施服务执行以完成动作的一个或多个操作;经由椭圆曲线数字签名算法签署所述一个或多个操作;存储所签署的一个或多个操作;以及至少部分地基于从所述一个或多个授权者接收的响应来发起针对动作的授权的查询过程。



CN 118575448 A

1.一种或多种其上存储有指令的非暂态计算机可以读介质,其中指令在由计算系统执行时使得计算系统:

接收对要由计算系统执行的动作的请求,该请求是从客户端设备接收的;

识别要从其接收针对动作的授权的一个或多个授权者,该授权与针对客户端设备的对动作的执行对应;

序列化与动作对应的一个或多个操作;

经由椭圆曲线数字签名算法签署序列化的一个或多个操作;

发起从所述一个或多个授权者中的每个授权者针对动作的授权的查询过程,以确定所述一个或多个操作是否被授权执行。

2.如权利要求1所述的一种或多种非暂态计算机可以读介质,其中指令在由计算系统执行时还使得计算系统:

确定已从所述一个或多个授权者中的每个授权者接收到针对动作的授权;

至少部分地基于通过签署序列化的一个或多个操作所产生的签名来核实序列化的一个或多个操作未被篡改;以及

至少部分地基于已接收到针对动作的授权的确定来执行所述一个或多个操作。

3.如权利要求1或权利要求2所述的一种或多种非暂态计算机可以读介质,其中签署序列化的一个或多个操作包括生成签名,并且其中指令在由计算系统执行时还使得计算系统向客户端设备提供签名。

4.如前述权利要求中的任一项所述的一种或多种非暂态计算机可以读介质,其中发起查询过程包括:

向所述一个或多个授权者中的每个授权者传输至少一个授权请求;以及

监视来自所述一个或多个授权者中的每个授权者对所述至少一个授权请求的响应。

5.如前述权利要求中的任一项所述的一种或多种非暂态计算机可以读介质,其中计算系统包括云基础设施服务,并且其中云基础设施服务被配置为在云基础设施服务的飞地的边缘处接收对动作的请求。

6.如权利要求5所述的一种或多种非暂态计算机可以读介质,其中云基础设施服务被配置为在飞地的防火墙之外接收对动作的请求。

7.如前述权利要求中的任一项所述的一种或多种非暂态计算机可以读介质,其中动作包括生成负载平衡器,并且其中指令在由计算系统执行时还使得计算系统:

确定已从所述一个或多个授权者中的每个授权者收到针对动作的授权;以及

生成负载平衡器。

8.如权利要求7所述的一种或多种非暂态计算机可以读介质,其中计算系统是云基础设施服务,并且其中云基础设施服务被配置为在云基础设施服务的飞地的边缘处创建负载平衡器。

9.一种确定用于云基础设施服务的针对动作的授权的方法,包括:

由安全性元件接收对要由云基础设施服务执行的动作的请求;

由安全性元件识别要从其接收针对动作的授权的一个或多个授权者,该授权与针对客户端设备的对动作的执行对应;

由安全性元件确定云基础设施服务为了完成该动作而要执行的一个或多个操作;

由安全性元件经由椭圆曲线数字签名算法签署一个或多个操作;

由安全性元件存储所签署的一个或多个操作;以及

由安全性元件至少部分地基于从所述一个或多个授权者接收到的响应来发起用于针对动作的授权的查询过程。

10.如权利要求9所述的方法,还包括由安全性元件序列化所述一个或多个操作,其中所述一个或多个操作的签署包括签署序列化的一个或多个操作。

11.如权利要求9或权利要求10所述的方法,还包括:

由安全性元件确定已从所述一个或多个授权者中的每个授权者接收到针对动作的授权;

由安全性元件至少部分地基于通过签署所述一个或多个操作所产生的签名核实所述一个或多个操作未被篡改;以及

由安全性元件至少部分地基于确定已经接收到针对动作的授权而使得执行所述一个或多个操作。

12.如权利要求9至11中的任一项所述的方法,其中安全性元件在云基础设施服务的飞地的边缘处实现。

13.如权利要求12所述的方法,其中安全性元件在飞地的防火墙之外实现。

14.如权利要求12或权利要求13所述的方法,其中安全性元件包括云基础设施服务的代理或守护进程。

15.如权利要求9至14中的任一项所述的方法,其中发起查询过程包括:

由安全性元件向所述一个或多个授权者传输至少一个授权请求;以及

由安全性元件监视从所述一个或多个授权者接收的对所述至少一个授权请求的响应,其中所述一个或多个操作是否要由云基础设施服务执行至少部分地基于该响应。

16.如权利要求9至15中的任一项所述的方法,其中云基础设施服务是第一云基础设施服务,其中请求是从第二云基础设施服务接收的,并且其中该方法还包括:在接收到从所述一个或多个授权者接收的响应之前,由安全性元件阻止与第一云基础设施服务相关的安全信息被提供给第二云基础设施服务。

17.一种计算系统,包括:

存储器,用于存储由计算系统执行的操作;以及

一个或多个处理器,耦合到存储器,所述一个或多个处理器:

识别对要由计算系统执行的动作的请求,该请求是从客户端设备接收的;

识别要从其接收针对动作的授权的一个或多个授权者,该授权与针对客户端设备的对动作的执行对应;

确定计算系统为了完成该动作而要执行的一个或多个操作;

序列化所述一个或多个操作;

经由椭圆曲线数字签名算法签署序列化的一个或多个操作;

将所签署的、序列化的一个或多个操作存储在存储器中;以及

发起从所述一个或多个授权者针对动作的授权的查询过程。

18.如权利要求17所述的计算系统,其中所述一个或多个处理器还:

确定已从所述一个或多个授权者中的每个授权者收到针对动作的授权;

从存储器中检索所签署的、序列化的一个或多个操作;以及

至少部分地基于授权和从存储器中检索到的所签署的、序列化的一个或多个操作来执行所述一个或多个操作。

19.如权利要求18所述的计算系统,其中所述一个或多个处理器还至少部分地基于通过签署序列化的一个或多个操作而产生的签名来核实所签署的、序列化的一个或多个操作未被篡改,并且其中所述一个或多个操作至少部分地基于对所签署的、序列化的一个或多个操作未被篡改的核实被执行。

20.如权利要求17至19中的任一项所述的计算系统,其中计算系统包括云基础设施服务,其中所述一个或多个处理器还在云基础设施服务的飞地的边缘处实现安全性元件,并且其中安全性元件用于识别对动作的请求。

基于法定人数的授权

[0001] 相关申请的交叉引用

[0002] 本申请要求于2022年1月7日提交的标题为“Quorum-based Authorization”的美国非临时申请No.17/571,346的优先权,该申请的公开内容通过引用整体并入本文以用于所有目的。

技术领域

[0003] 本公开涉及用于确定对云服务提供商的基础设施服务的访问授权的框架。

背景技术

[0004] 云服务提供商(CSP)使用不同的系统和基础设施服务按需向用户或客户端提供各种服务。CSP提供基础设施服务,客户端可以使用这些服务构建自己的网络并部署客户资源。为了确保CSP的基础设施服务的安全性和持续可用性,可以寻求用户和/或客户端使用和用基础设施服务执行针对动作的授权,以防止不良行为者访问未经授权的数据和/或攻击基础设施服务的某些部分。

[0005] 寻求用户和/或客户端使用和用CSP基础设施服务执行针对动作的授权的遗留方法常常导致与用户和/或客户端共享敏感信息,而这些信息可以被第三方用于未经授权访问系统和/或执行未经授权的动作。遗留方法还要求预先批准执行针对动作的授权,其中用户和/或客户端在请求执行动作之前要求获得执行针对动作的授权,以便被允许执行该动作。

发明内容

[0006] 本公开一般而言涉及一种用于管理用计算系统(诸如云基础设施服务)执行针对动作的授权的框架。本文描述了各种实施例,包括方法、系统、存储可由一个或多个处理器执行的程序、代码或指令的非暂态计算机可读存储介质等。提及这些说明性实施例并非为了限制或定义本公开,而是为了提供示例以帮助理解本公开。在详细描述部分中讨论了附加实施例,并在其中提供了进一步的描述。

[0007] 本公开的一方面针对一种或多种非暂态计算机可读介质,该介质上存储有指令,其中指令当被计算系统执行时可以使计算系统接收对计算系统执行动作的请求,该请求是从客户端设备接收的。指令当被计算系统执行时还可以使计算系统识别要从其接收针对动作的授权的一个或多个授权者,该授权与针对客户端设备的对动作的执行对应。当指令被计算系统执行时还可以使计算系统进一步序列化与动作对应的一个或多个操作,并经由椭圆曲线数字签名算法签署序列化的一个或多个操作。另外,指令当被计算系统执行时可以使计算系统发起来自一个或多个授权者中的每个授权者的针对动作的授权的查询过程,以确定是否授权执行一个或多个操作。

[0008] 本公开的一方面针对一种确定云基础设施服务的针对动作的授权的方法,包括:由安全性元件接收云基础设施服务对要执行的动作的请求,以及由安全性元件识别要从其

接收针对动作的授权的一个或多个授权者,该授权与动作的执行对应。该方法还可以包括:由安全性元件确定云基础设施服务为了完成动作要执行的一个或多个操作,由安全性元件经由椭圆曲线数字签名算法签署一个或多个操作,以及由安全性元件存储签署的一个或多个操作。该方法还可以包括:由安全性元件至少部分地基于从一个或多个授权者接收的响应来发起针对动作的授权的查询过程。

[0009] 本公开的一方面针对一种计算系统,包括用于存储由计算系统执行的操作的存储器,以及耦合到该存储器的一个或多个处理器,一个或多个处理器用于识别要由计算系统执行的操作的请求,该请求是从客户端设备接收的,以及识别要从其接收操作授权的一个或多个授权者,该授权与针对客户端设备的对动作的执行对应。一个或多个处理器还可以确定计算系统为了完成动作要执行的一个或多个操作,序列化一个或多个操作,以及经由椭圆曲线数字签名算法签署序列化的一个或多个操作。另外,一个或多个处理器可以将签署的、序列化的一个或多个操作存储在存储器中,并发起从一个或多个授权者授权动作的查询过程。

[0010] 参考以下说明书、权利要求书和附图,前述内容以及其他特征和实施例将变得更加明显。

附图说明

[0011] 当参考附图阅读以下具体实施方式时,可以更好地理解本公开的特征、实施例和优点。

[0012] 图1图示了根据一些实施例的示例基础设施服务布置。

[0013] 图2图示了根据一些实施例的示例授权布置。

[0014] 图3图示了根据一些实施例的可以为授权实现的示例数据过渡流程。

[0015] 图4图示了根据一些实施例的另一个示例授权布置。

[0016] 图5图示了根据一些实施例的用于授权客户端执行动作的示例过程。

[0017] 图6图示了根据一些实施例的用于授权客户端执行动作的另一个示例过程。

[0018] 图7图示了根据一些实施例的用于授权客户端执行动作的另一个示例过程的第一部分。

[0019] 图8图示了根据一些实施例的图7的示例过程的第二部分。

[0020] 图9是图示根据至少一个实施例的用于实现云基础设施即服务系统的一种模式的框图。

[0021] 图10是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0022] 图11是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0023] 图12是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0024] 图13是图示根据至少一个实施例的示例计算机系统的框图。

具体实施方式

[0025] 在下面的描述中,出于解释的目的,阐述了具体细节以便提供对某些实施例的透彻理解。但是,明显的是可以在没有这些具体细节的情况下实践各种实施例。附图和描述并非旨在是限制性的。本文中“示例性”一词被用于表示“用作示例、实例或说明”。本文中描述为“示例性”的任何实施例或设计不一定被解释为比其它实施例或设计优选或有利。

[0026] 本公开描述了对用户和/或客户端(在本公开中统称为“客户端”)执行授权的技术,以访问由云服务提供商(CSP)提供的基础设施服务(诸如云基础设施服务,例如图9的云基础设施、图10的云基础设施、图11的云基础设施和/或图12的云基础设施)和/或用基础设施服务执行动作。更特别地,可以提供实时授权,其中基础设施服务可以响应于从客户端接收执行动作的请求而寻求对客户端的授权,而不是在授权请求之前要求授权。基础设施服务可以序列化一个或多个操作以执行动作,并且可以经由椭圆曲线数字签名算法(ECDSA)签署序列化的操作。基础设施服务可以存储序列化的操作,并且可以一旦接收到客户端正在执行的针对动作的授权就解冻(thaw)并执行操作。

[0027] CSP可以使用不同的系统和基础设施服务(本文中称为云基础设施服务)按需向客户端提供各种服务。在某些实施例中,CSP可以在基础设施即服务(IaaS)模型下提供服务,其中CSP提供基础设施服务,客户可以使用这些服务构建自己的网络并部署客户资源。CSP提供的基础设施可以包括互连的高性能计算机资源,包括各种主机机器(也称为主机)、存储器资源和网络资源,这些资源形成物理网络,称为基础网络或底层网络。CSP提供的基础设施可以散布在一个或多个数据中心上,这些数据中心在地理上可以散布在一个或多个区域上。

[0028] CSP的物理网络(可以包括各种主机机器、存储器资源和/或网络资源)可以为在物理网络之上创建一个或多个虚拟或覆盖网络提供底层基础。这些虚拟或覆盖网络(也称为基于软件或软件定义的网络)可以使用软件虚拟化技术来实现,以创建可以在物理网络之上运行的网络抽象的层。覆盖网络可以采用多种形式。覆盖网络可以使用层3IP寻址,其中端点由其虚拟IP地址指定。这种覆盖联网方法常常被称为虚拟层3联网。

[0029] 当客户端订阅或注册由CSP提供的IaaS服务时,可以为那个客户端创建租赁,该租赁是CSP的基础设施服务内安全且隔离的分区,客户端可以在其中创建、组织和管理其云资源。例如,客户端可以使用由CSP提供的资源在客户端的租赁内构建一个或多个可自定义的且私有的虚拟网络(称为虚拟云网络(VCN))。可以在这些客户端VCN上部署一个或多个客户端资源,诸如计算实例(例如,虚拟机、裸机实例等)。

[0030] 当客户端尝试访问基础设施服务以建立租赁或执行另一个动作时,客户端可以向基础设施服务传输请求建立租赁或执行另一个动作的请求。基础设施服务可以接收请求并确定客户端正在请求基础设施服务执行动作。基于动作和/或客户端,基础设施服务可以确定要求一个或多个授权者的授权来授权客户端要执行的动作。基础设施服务可以基于客户端和/或动作识别用于提供授权的一个或多个授权者,其中授权者可以是预定义的。基础设施服务可以向每个确定的授权者提供一个或多个授权客户端执行动作的请求。基础设施服务可以监视来自授权者的响应,并基于来自授权者的响应确定客户端是否被授权执行动作。

[0031] 基于客户端请求的动作,基础设施服务可以确定基础设施服务为了完成该动作要

执行的一个或多个操作。在一些实施例中,客户端可以是有状态的,而基础设施服务可以是无状态的。为了促进有状态客户端与无状态基础设施服务之间的这种接口,与该动作相关联的状态可以被序列化并以可以一旦基础设施服务做出授权确定就被解冻和验证的方式存储。例如,基础设施服务可以序列化与动作相关联的操作。基础设施服务可以经由椭圆曲线数字签名算法(ECDSA)签署序列化的操作并存储签署的序列化的操作。与将相同数据密码保护到相同级别的遗留方法相比,使用ECDSA进行签名可以使用更少的时钟周期用于密码保护数据。另外,使用ECDSA可以使加密的数据具有后量子安全性。

[0032] 如果基础设施服务确定该动作被授权为客户端执行,那么基础设施服务可以检索签署的序列化的操作。基础设施服务可以基于通过签署序列化操作进行而产生的签名来核实序列化的操作未被篡改。例如,基础设施服务可以核实从存储装置中检索到的签署的序列化操作对应的签名与签署序列化的操作时产生的签名相匹配。如果基础设施服务核实序列化的操作未被篡改,那么基础设施服务可以执行序列化的操作。例如,基础设施服务可以根据由有状态客户端定义的状态执行操作。

[0033] 图1图示了根据一些实施例的示例基础设施服务布置100。特别地,基础设施服务布置100图示了基础设施服务的一部分,该基础设施服务可以实现贯穿本公开所描述的用于确定授权的方法中的一种或多种。在一些实施例中,基础设施服务可以包括图9的云基础设施、图10的云基础设施、图11的云基础设施和/或图12的云基础设施的特征中的一个或多个。基础设施服务可以包括计算系统。在一些实施例中,基础设施服务可以包括云计算系统。基础设施服务可以包括可为客户端提供服务的基础设施的硬件和/或软件。

[0034] 基础设施服务可以包括一个或多个设备102,这些设备102被通信地耦合以提供基础设施服务的一部分。例如,在所示实施例中,基础设施服务布置100包括第一设备102a、第二设备102b和第三设备102c。设备102可以包括计算设备,诸如计算机终端、服务器、其它计算机设备或其某种组合。设备102可以彼此通信以形成基础设施服务的一部分,其中基础设施服务可以提供基础设施服务,诸如云基础设施服务。

[0035] 设备102可以被分组到不同的飞地(enclave)。例如,第一设备102a、第二设备102b和第三设备102c可以形成基础设施服务的飞地104的一部分。飞地104可以执行特定操作。例如,飞地104可以包括提供管理操作的管理飞地、提供服务操作的服务飞地或向客户端提供客户操作的客户飞地。飞地104可以实现软件定义的边界(SDP)安全性模型以创建受保护的IaaS实例。飞地104可以具有唯一的通信简档,该简档可以与基础设施服务中不同飞地的其它通信简档不同。可以控制、监视和/或策略驱动进入和离开飞地104的访问。例如,对飞地104的访问可以基于授权,其中对飞地104的访问可以仅限于授权的客户端。飞地104可能以要求客户端从一个或多个授权者处接收授权,以提供对飞地104的访问。飞地104可以具有定义的SDP,其包括一个或多个设备(诸如第一设备102a、第二设备102b和第三设备102c)和/或某些软件,其中飞地104的边缘由设备和/或软件与飞地104外部的元素的分离来定义。

[0036] 飞地104可以具有防火墙106,用于防范恶意网络流量。例如,飞地104可以具有基于软件的防火墙106,其监视与飞地104的网络流量并防范恶意网络流量。防火墙106可以位于飞地104的边缘内,并且可以保护飞地104的至少一部分设备和/或软件。

[0037] 基础设施服务可以包括一个或多个安全性元件,诸如安全性元件108。安全性元件

108可以包括设备、软件或其某种组合。安全性元件108可以位于飞地104的边缘处。另外,安全性元件108可以位于飞地104的防火墙106之外。例如,安全性元件108可以位于飞地104的边缘处和/或防火墙106之外,以允许在无需访问飞地104的安全部分的情况下与安全性元件108进行通信。

[0038] 安全性元件108可以确定尝试访问飞地104和/或基础设施服务的客户端是否被授权访问飞地104和/或基础设施服务。例如,客户端可以传输请求飞地104和/或基础设施服务执行一个或多个动作的请求。安全性元件108可以接收该请求并确定客户端是否已接收到执行一个或多个针对动作的授权。如果安全性元件108确定客户端已获得访问飞地104和/或基础设施服务的授权,那么安全性元件108可以使飞地104和/或基础设施服务执行客户端请求的一个或多个动作。

[0039] 如果安全性元件108确定客户端之前未获得执行一个或多个针对动作的授权,那么安全性元件108可以发起确定是否授予客户端执行一个或多个针对动作的授权的过程。例如,安全性元件108可以识别可以向客户端提供执行一个或多个针对动作的授权的一个或多个授权者。授权者可以包括能够向客户端授予执行一个或多个针对动作的授权的一个或多个个人和/或设备。授权者可以能够向客户端授予对基础设施服务和/或飞地104、执行一个或多个动作或其某种组合的授权。授权者可以是预定义的,或者可以在请求时定义。

[0040] 基于安全性元件108确定客户端之前未获得执行一个或多个针对动作的授权,安全性元件108最初不会执行一个或多个动作。特别地,安全性元件108可以存储一个或多个动作,直到从授权者接收到授权、从授权者接收授权的时间已到期或授权者指示客户端未被授权执行一个或多个动作。安全性元件108可以将一个或多个动作转换成一个或多个操作以供存储,其中将执行一个或多个操作以完成一个或多个动作。操作可以采用基础设施服务可以执行的格式,而动作可以采用不同的格式。

[0041] 客户端可以是有状态的,而基础设施服务可以是无状态的。为了正确执行操作,基础设施服务可以在执行操作时考虑操作的状态。为了确保在执行操作时考虑状态,可以以某种格式存储操作以维护基础设施服务操作的状态。例如,安全性元件108可以将操作序列化以进行存储。例如,安全性元件108可以将操作翻译成可以存储并且可以在以后重构的格式。操作的序列化可以允许基础设施服务在由无状态基础设施服务执行操作时维护操作的状态。

[0042] 安全性元件108可以进一步签署操作。例如,安全性元件108可以签署序列化的操作。安全性元件108可以经由椭圆曲线数字签名算法(ECDSA)签署操作。例如,安全性元件108可以利用ECDSA和密钥来生成用于签署操作的签名。安全性元件108可以基于密钥产生签名,该签名与签署的操作相关联。安全性元件108可以在飞地104内维护密钥,同时安全性元件108可以与请求动作的客户端共享签名。然后,安全性元件108可以将签署的序列化的操作存储在基础设施服务的存储器中。使用ECDSA签署操作可以提供后量子安全性。例如,量子计算机破解ECDSA所需的资源成本将比ECDSA为后量子安全性保护的数据更昂贵。另外,使用ECDSA可以比遗留方法更快,诸如与遗留方法相比,ECDSA使用更少的时钟周期来将数据保护到相同的级别。

[0043] 安全性元件108可以发起从一个或多个授权者中的每个授权者的针对动作的授权的查询过程,以确定是否授权执行一个或多个操作。例如,安全性元件108可以向每个授权

者传输一个或多个授权请求,其中授权请求可以向每个授权者请求客户端是否被授权执行客户端请求的一个或多个动作的响应。安全性元件108可以将授权请求作为文本消息、电子邮件、推送消息和/或授权者可以为响应提供的其它消息传输。授权请求可以允许每个授权者进行响应以指示客户端被授权或未被授权执行动作。安全性元件108可以监视来自一个或多个授权者中的每个授权者对授权请求的响应。

[0044] 安全性元件108可以基于从授权者接收到的响应或未接收到响应来确定客户端是否具有执行一个或多个针对动作的授权。例如,安全性元件108可以响应于安全性元件108先前提供的授权请求而接收来自授权者的响应。在一些实施例中,在执行客户端是否具有执行一个或多个针对动作的授权的确定之前,安全性元件108可以等待,直到从所有授权者收到响应。安全性元件108可以确定来自授权者的每个响应是否指示客户端具有执行一个或多个针对动作的授权或未获得执行一个或多个针对动作的授权。安全性元件108可以基于指示客户端具有执行一个或多个针对动作的授权的每个响应来确定客户端具有执行一个或多个针对动作的授权。相比之下,安全性元件108可以基于指示客户端未被授权执行一个或多个动作的任何响应来确定客户端没有执行的授权。

[0045] 在其它实例中,安全性元件108可以基于一定百分比的响应指示客户端具有执行一个或多个针对动作的授权或者与某些授权者对应的响应指示客户端具有执行一个或多个针对动作的授权来确定客户端具有授权。例如,在一些实例中,安全性元件108可以基于比指示客户端没有授权执行一个或多个动作的响应的数量更多的指示客户端具有执行一个或多个针对动作的授权的响应的数量来确定客户端具有授权。在一些实例中,可以存在某些授权者和/或某组授权者,无论其他授权者的响应如何,都可以为客户端提供执行一个或多个针对动作的授权。例如,在授权请求的授权者中,安全性元件108可以确定预定义的授权者或预定义的授权者组指示客户端具有执行一个或多个针对动作的授权,并可以基于预定义的授权者或预定义的授权者组指示客户端被授权执行一个或多个动作来确定客户端具有执行一个或多个针对动作的授权。在一些实例中,其中一个或多个授权者可以选择性地授予授权,使得如果授权者组中的任何一个指示客户端具有执行一个或多个针对动作的授权,那么安全性元件108可以确定客户端具有执行一个或多个针对动作的授权。

[0046] 在一些实例中,安全性元件108可以实现用于来自授权者的响应的定时器,以确定客户端是否具有执行一个或多个操作的授权。例如,如果安全性元件108确定在定时器定义的时间段内未接收到授权者为向客户端提供一个或多个操作的授权而提供的足够响应,那么安全性元件108可以确定客户端不具有执行一个或多个针对动作的授权。

[0047] 如果安全性元件108基于来自授权者的响应确定客户端没有执行一个或多个针对动作的授权,那么安全性元件108可以不执行与一个或多个动作相关联的操作。安全性元件108还可以基于确定客户端没有执行一个或多个针对动作的授权而从存储器中移除存储的操作。

[0048] 如果安全性元件108基于来自授权者的响应确定客户端具有执行一个或多个针对动作的授权,那么安全性元件108可以执行操作。例如,安全性元件108可以从存储器中检索签署的序列化的操作。安全性元件108可以检查签署的序列化的操作的签名以确定操作是否已被篡改。例如,安全性元件108可以将检索时的签署的序列化的操作的签名与签署序列化的操作时产生的签名进行比较。如果签名匹配,那么安全性元件108可以确定操作未被篡

改。如果签名不匹配,那么安全性元件108可以确定操作已被篡改。

[0049] 如果安全性元件108确定操作已被篡改,那么即使安全性元件108确定客户端具有执行一个或多个针对动作的授权,安全性元件108也可以阻止操作被执行。如果安全性元件108确定操作未被篡改,那么安全性元件108可以继续使得序列化的操作被执行。例如,安全性元件108可以使得基础设施服务执行序列化的操作,其中操作的序列化使得在执行操作时考虑状态。

[0050] 虽然基础设施服务布置100图示了基础设施服务的一部分的实施例,但应当理解的是,具有基础设施服务布置100的特征的基础设施服务的其他实施例也应被本公开所涵盖。例如,飞地(诸如飞地104)可以由一个或多个设备形成,和/或一个或多个设备可以包括在多个飞地内。另外,基础设施服务可以包括多个飞地,而不是所示的单个飞地。每个飞地还可以包括多个安全性元件,其中每个安全性元件可以由任何客户端访问,每个安全性元件可以专用于对应的客户端使得对应的客户端可以访问对应的安全性元件,或其组合。

[0051] 图2图示了根据一些实施例的示例授权布置200。例如,授权布置200图示了用于说明根据一些实施例的基于法定人数的授权方法的设备的示例布局。应当理解的是,授权布置200是用于说明该方法的单个实施例,并且该方法的实施方式不限于所示的示例布局。

[0052] 授权安排200可以包括飞地202。飞地202可以包括飞地104(图1)的一个或多个特征。飞地202可以包括基础设施服务或其一部分,诸如关于图1描述的基础设施服务。在一些实施例中,基础设施服务可以包括计算系统,诸如云计算系统。飞地202可以包括一个或多个安全性元件,诸如所示的安全性元件204。安全性元件204可以包括安全性元件108(图1)的特征中的一个或多个。

[0053] 授权布置200可以包括客户端设备206。客户端设备206可以包括单个设备、另一个基础设施服务或云计算系统。在一些实施例中,客户端设备206可以由与飞地202分离的操作者维护。客户端设备206可以经由网络(诸如经由互联网)与飞地202通信。在一些实施例中,客户端设备206或使用客户端设备206的用户(其中客户端设备206和用户可以被称为客户端)可以与飞地202(或包括飞地202的基础设施服务)提供的接口服务的订户相关联,其中飞地202可以向客户端设备206提供服务。在一些实施例中,订户可以包括组织,该组织可以包括多个用户和/或客户端设备。在一些实施例中,接口服务可以包括云计算服务。客户端设备206可以能够请求由飞地202提供的服务。用户可以访问客户端设备206并利用客户端设备206向飞地202请求服务。例如,用户可以是可以登录到客户端设备206的个人,其中登录到客户端设备206的用户可以核实用户的身份。

[0054] 当客户端设备206从飞地202请求动作和/或服务时,飞地202可以执行授权过程,以确定客户端设备206和/或使用客户端设备206的用户是否被授权执行动作和/或服务。例如,客户端设备206可以向飞地202传输请求飞地202或包括飞地202的基础设施服务执行一个或多个动作的请求。安全性元件204可以接收来自客户端设备206的请求,并可以确定客户端设备206正在请求飞地202或包括飞地202的基础设施服务执行一个或多个动作。

[0055] 基于从客户端设备206接收到的请求,安全性元件204可以确定客户端设备206和/或使用客户端设备206的用户的身份以传输请求。例如,从客户端设备206接收到的请求可以包括与客户端设备206对应的标识符、与使用客户端设备206的用户对应的标识符或两者。安全性元件204可以确定客户端设备206和/或使用客户端设备206的用户是否先前已被

授予执行所请求的针对动作的授权。例如,客户端设备206可以先前已被提供未来执行各种类型针对动作的授权。安全性元件204可以确定请求中请求的动作是否属于客户端设备206和/或使用客户端设备206的用户先前已获得执行授权的任何类型的操作。如果安全性元件204确定先前已经向客户端设备206和/或使用客户端设备206的用户提供了针对这些针对动作的授权,那么安全性元件204可以使飞地202和/或基础设施服务执行这些动作。

[0056] 如果安全性元件204确定先前未向客户端设备206和/或使用客户端设备206的用户呈现针对动作的授权,那么安全性元件204可以执行过程以确定客户端设备206和/或使用客户端设备206的用户是否要基于请求接收针对动作的授权。例如,安全性元件204可以识别一个或多个授权者,这些授权者可以为客户端设备206和/或使用客户端设备206的用户提供执行针对动作的授权。授权者可以是能够向客户端设备206和/或使用客户端设备206的用户授予执行针对动作的授权的个人、设备或其某种组合。授权者可以预定义或在请求时定义。授权者可以与和客户端设备206和/或使用客户端设备206的用户相同的订户相关联,或者可以由订户指派。如果安全性元件204确定尚未为客户端设备206和/或使用客户端设备206的用户指派授权者以执行动作,那么安全性元件204可以确定飞地202和/或基础设施服务不执行动作。如果安全性元件204识别出为客户端设备206和/或使用客户端设备206的用户指派的一个或多个授权者以执行动作,那么安全性元件204可以继续确定客户端设备206和/或使用客户端设备206的用户是否要接收针对动作的授权。

[0057] 由于在接收到请求与从授权者接收到授权之间可以存在延迟,因此安全性元件204可以存储动作以供将来执行。客户端设备206可以是有状态的,而飞地202和/或基础设施服务可以是无状态的。为了正确执行动作,可能需要考虑动作的状态。因而,安全性元件204可以以某种方式存储动作以维持与动作对应的状态。例如,安全性元件204可以确定飞地202和/或基础设施服务为了完成所请求的操作而要执行的一个或多个操作。安全性元件204可以以某种格式存储操作以维持与操作对应的状态。例如,安全性元件204可以序列化操作以供存储。安全性元件204可以将操作翻译成可以存储并且可以在以后重构的格式。操作的序列化可以允许飞地202和/或基础设施服务在由无状态飞地202和/或基础设施服务执行时维持操作的状态。

[0058] 安全性元件204可以进一步签署操作以供存储。操作的签署可以被用于核实操作在由飞地202和/或基础设施服务执行之前未被篡改。安全性元件204可以经由ECDSA签署操作。例如,安全性元件204可以利用ECDSA和密钥签署操作。由ECDSA和密钥产生的签名可以与操作相关联。安全性元件204可以在飞地202内维护密钥,而安全性元件204可以与传输请求的客户端设备206共享签名。然后,安全性元件204可以将签署的序列化的操作存储在诸如安全性元件204、飞地202和/或基础设施服务的存储器中。使用ECDSA用于签名可以提供后量子安全性,并且与遗留方法相比,可以使用更少的时钟周期。

[0059] 安全性元件204可以发起查询过程,以确定客户端设备206和/或使用客户端设备206的用户是否将接收执行针对动作的授权。安全性元件204可以识别被识别为用于向客户端设备206和/或使用客户端设备206的用户提供授权的授权者的账户(诸如电子邮件账户、消息传递账户、社交媒体账户或可以向授权者提供消息的其他账户)、电话号码、设备或其某种组合。安全性元件204可以向每个授权者传输请求指示客户端设备206和/或使用客户端设备206的用户是否将被授予执行操作的授权的响应的一个或多个请求。请求可以包括

客户端设备206和/或客户端设备206的用户寻求执行针对动作的授权的指示。安全性元件204可以将请求传输到每个授权者的一个或多个账户、电话号码、设备或其某种组合。请求可以请求授权者用客户端设备206和/或使用客户端设备206的用户是否应被提供针对动作的授权的指示做出响应。在一些实例中,安全性元件204可以在初始请求之后发送请求是否应向客户端设备206和/或客户端设备206的用户授予针对动作的授权的指示的一个或多个后续请求。

[0060] 授权布置200可以包括一个或多个授权者设备208,诸如第一授权者设备208a和第二授权者设备208b。授权者设备208可以与一个或多个授权者对应。例如,每个授权者设备208可以包括一个设备,一个或多个授权者可以在该设备中访问账户、电话号码和/或由安全性元件204向其传输请求的设备。基于识别出的授权者,安全性元件204可以识别与识别出的授权者相关联的授权者设备208,并且在一些实例中将请求传输到授权者设备208。在一些实例中,授权者设备208可以包括输入设备,该输入设备允许授权者输入是否要向客户端设备206和/或使用客户端设备206的用户提供针对动作的授权的指示。

[0061] 安全性元件204可以向每个授权者设备208提供请求。例如,安全性元件204可以将请求直接传输到每个授权者设备208、可以经由授权者设备208访问的账户、与授权者设备208相关联的电话号码或其某种组合。在所示实施例中,安全性元件204可以向第一授权者设备208a传输一个或多个请求以寻求来自第一授权者的指示,并可以向第二授权者设备208b传输一个或多个请求以寻求来自第二授权者的指示。在一些实例中,第一授权者设备208a和/或第二授权者设备208b可以在设备上显示用户界面,该用户界面从对应的授权者请求对客户端设备206和/或使用客户端设备206的用户的授权的指示。每个授权者设备208可以检测来自对应授权者的客户端设备206和/或使用客户端设备206的用户是否应获得针对动作的授权的指示。基于从授权者接收到的指示,授权者设备208可以传输客户端设备206和/或客户端设备206的用户是否应被授予针对动作的授权的指示。在一些实例中,授权者可以不向一个或多个授权者设备208提供指示,在这种情况下,未接收到指示的一个或多个授权者设备可以不向安全性元件204提供响应。

[0062] 安全性元件204可以监视来自授权者设备208的响应,并可以接收来自授权者设备208的响应。例如,在所示实施例中,安全性元件204可以接收来自与第一授权者对应的第一授权者设备208a的第一响应以及来自与第二授权者对应的第二授权者设备208b的第二响应。安全性元件204可以确定是否要向客户端设备206和/或客户端设备206的用户授予针对动作的授权。在一些实施例中,安全性元件204可以等待,直到从所有向其传输请求的授权者接收到响应,然后再确定是否要向客户端设备206和/或客户端设备206的用户授予针对动作的授权。如果安全性元件204确定所有授权者都指示客户端设备206和/或使用客户端设备206的用户应被授权执行这些动作,那么安全性元件204可以确定客户端设备206和/或使用客户端设备206的用户应被授权执行这些动作。如果任何授权者指示客户端设备206和/或使用客户端设备206的用户不应被授权执行这些动作,那么安全性元件204可以确定客户端设备206和/或使用客户端设备206的用户不应被授权执行这些动作。

[0063] 在一些实例中,安全性元件204可以不要求授权者一致指示客户端设备206和/或使用客户端设备206的用户将被授予授权以确定客户端设备206和/或使用客户端设备206的用户被授权执行动作。在这些实例中,安全性元件204可以基于一定百分比的响应指示客

户端具有执行针对动作的授权,或者与某些授权者对应的响应指示客户端具有执行针对动作的授权来确定客户端具有执行针对动作的授权。

[0064] 在一些实例中,安全性元件204可以实现用于来自授权者的响应的定时器,以确定客户端是否具有执行针对动作的授权。例如,如果安全性元件204确定在定时器定义的时间段内未接收到来自授权者的用于向客户端设备206和/或使用客户端设备206的用户提供执行针对动作的授权的足够响应,那么安全性元件204可以确定客户端设备206和/或使用客户端设备206的用户不具有执行针对动作的授权。

[0065] 如果安全性元件204基于来自授权者的响应确定客户端没有执行针对动作的授权,那么安全性元件204可以不执行与动作相关联的操作。安全性元件204还可以基于确定客户端没有执行针对动作的授权而从存储器中移除所存储的操作。

[0066] 如果安全性元件204基于来自授权者的响应确定客户端具有执行针对动作的授权,那么安全性元件204可以执行动作。例如,安全性元件204可以从存储器中检索签署的序列化的操作。安全性元件204可以检查签署的序列化的操作的签名以确定操作是否已被篡改。例如,安全性元件204可以将检索时的签署的序列化的操作的签名与序列化的操作被签署时产生的签名进行比较。如果签名匹配,那么安全性元件204可以确定操作未被篡改。如果签名不匹配,那么安全性元件204可以确定操作已被篡改。

[0067] 如果安全性元件204确定操作已被篡改,那么安全性元件204可以阻止执行操作。如果安全性元件204确定操作未被篡改,那么安全性元件204可以继续使得执行序列化的操作。例如,安全性元件204可使飞地202和/或基础设施服务执行序列化的操作,其中操作的序列化使得在执行操作时考虑状态。

[0068] 图3图示了根据一些实施例可以为授权实现的示例数据过渡流程300。例如,在一些实施例中,安全性元件(诸如安全性元件108(图1)和/或安全性元件204(图2))可以用从客户端设备(诸如客户端设备206(图2))接收的动作来执行一个或多个过渡。数据过渡流程300中所示的过渡和数据结构可以促进将有状态系统的操作存储在无状态系统中,以便由无状态系统稍后执行。

[0069] 数据过渡流程300可以由动作302发起。例如,安全性实体可以从客户端设备接收动作302,该动作指示飞地(诸如飞地104(图1)和/或飞地202(图2))和/或与安全实体对应的接口为客户端设备执行的动作。安全性实体可以确定动作302将被存储以供稍后执行。

[0070] 数据过渡流程300可以包括将动作302转换成一个或多个操作304。例如,安全性元件可以将从客户端设备接收的动作302转换成一个或多个操作304。一个或多个操作304可以由飞地和/或接口执行以完成动作302。例如,动作302可以采用飞地和/或基础设施服务无法执行的格式,并且安全性元件可以将动作302转换成可以由飞地和/或基础设施服务执行以完成动作302的一个或多个操作304。在其他实例中,由客户端设备提供的动作302可以采用飞地和/或基础设施服务可以执行的格式,并且动作302可以被用作一个或多个操作304。在这些实例中,可以省略转换。

[0071] 数据过渡流程300可以包括序列化一个或多个操作304。例如,安全性元件可以序列化一个或多个操作304以产生序列化的操作306。安全性元件可以将操作翻译成可以存储并在稍后重构的序列化的操作306。操作的序列化可以维护与操作对应的状态。因而,飞地和/或基础设施服务可以在稍后执行操作时考虑操作的状态。在一些实例中,可以省略序列

化。

[0072] 数据过渡流程300可以包括签署序列化的操作306。例如,安全性元件可以通过ECDSA签署序列化的操作。安全性元件可以具有密钥,并用ECDSA和密钥产生签名308。安全性元件可以用签名308签署序列化的操作306,以生成签署的序列化的操作310。在一些实例中,安全性元件可以将签名308提供给客户端设备。

[0073] 数据过渡流程300可以包括解冻签署的序列化的操作。例如,安全性元件可以解冻签署的序列化的操作,以供飞地和/或基础设施服务执行。解冻签署的序列化的操作可以包括核实签署的序列化的操作的签名308,以核实在序列化的操作被签署的时间与解冻签署的序列化的操作的时间之间操作未被篡改。解冻签署的序列化的操作还可以包括反序列化操作以产生可以由飞地和/或基础设施服务执行的一个或多个操作312。例如,安全性元件可以将序列化的操作转换成可以由飞地和/或基础设施服务执行的格式。然后,安全性元件可以使飞地和/或基础设施服务执行一个或多个操作312。

[0074] 图4图示了根据一些实施例的另一个示例授权布置400。例如,授权布置400图示了客户端设备402请求生成负载平衡器404的示例。基于法定人数的授权方法可以在授权布置400中实现。

[0075] 授权布置400可以包括客户端设备402。客户端设备402可以包括客户端设备206(图2)的特征中的一个或多个。在所示实施例中,客户端设备402可以请求由飞地406和/或基础设施服务(诸如关于图1描述的基础设施服务、图9的云基础设施、图10的云基础设施、图11的云基础设施和/或图12的云基础设施)生成负载平衡器404。负载平衡器404可以被用于将由客户端设备402传输的数据指引到飞地406和/或基础设施服务。例如,负载平衡器404可以被用于指引由客户端设备402或飞地406和/或基础设施服务内的其他设备请求的动作。

[0076] 授权布置400可以包括飞地406。飞地406可以包括飞地104(图1)和/或飞地202(图2)的特征中的一个或多个。飞地406可以包括基础设施服务或其一部分,诸如关于图1描述的基础设施服务。在一些实施例中,基础设施服务可以包括计算系统,诸如云计算系统。飞地406可以包括安全性元件408。安全性元件408可以包括安全性元件108(图1)和/或安全性元件204(图2)的特征中的一个或多个。客户端设备402可以经由网络(诸如经由互联网)与飞地406耦合,并且可以与飞地406通信。在所示实施例中,客户端设备402或利用客户端设备402的用户可以向飞地406传输请求生成负载平衡器404或包括生成负载平衡器404的另一个动作的请求。飞地406的安全性元件408可以接收该请求,并可以确定客户端设备402和/或利用客户端设备402的用户是否具有生成负载平衡器404或使得执行包括生成负载平衡器404的针对动作的授权。如果安全性元件408确定客户端设备402和/或利用客户端设备402的用户先前已被授予生成负载平衡器404或使得执行该针对动作的授权,那么安全性元件408可以使得飞地406和/或基础设施服务生成负载平衡器404。

[0077] 如果安全性元件408确定客户端设备402和/或利用客户端设备402的用户先前未被授予生成负载平衡器404或使得执行该针对动作的授权,那么安全性元件408可以执行过程以确定客户端设备402和/或利用客户端设备402的用户是否要接收生成负载平衡器404和/或执行生成负载平衡器404的针对动作的授权。例如,安全性元件408可以识别一个或多个授权者,这些授权者可以为客户端设备402和/或利用客户端设备402的用户提供生成负

载平衡器404和/或执行生成负载平衡器404的针对动作的授权。授权者可以预定义或在请求时定义。授权者可以与和客户端设备402和/或利用客户端设备402的用户相同的订阅者相关联,或者可以由订阅者指派。

[0078] 安全性元件408可以存储用于生成负载平衡器404和/或生成负载平衡器404的动作的操作以供将来执行。这些操作可以与负载平衡器404的生成和/或动作对应,使得执行这些操作的飞地406和/或基础设施服务将导致负载平衡器404的生成和/或动作的执行。由于客户端设备402可以是有状态的,而飞地406和/或基础设施服务可以是无状态的,因此飞地406和/或基础设施服务可以在未来执行期间考虑与这些操作对应的状态,以正确生成负载平衡器404和/或执行动作。因而,安全性元件408可以将操作存储在特定状态以维持与操作对应的状态。例如,安全性元件408可以序列化操作以供存储以维持与操作对应的状态。操作的序列化可以提供由安全性元件408以可以在稍后重构以供飞地406和/或基础设施服务执行的格式存储的操作。

[0079] 安全性元件408还可以签署操作以供存储。操作的签署可以被用于核实操作在由飞地406和/或基础设施服务执行之前未被篡改。安全性元件408可以经由ECDSA签署操作。例如,安全性元件408可以使用ECDSA和密钥签署操作。由ECDSA和密钥产生的签名可以与操作相关联。安全性元件408可以在飞地406内维护密钥,而安全性元件408可以与客户端设备402共享签名。然后,安全性元件408可以将签署的序列化的操作存储在诸如安全性元件408、飞地406和/或基础设施服务的存储器中。使用ECDSA用于签名可以提供后量子安全性,并且与遗留方法相比,可以利用更少的时钟周期。

[0080] 安全性元件408可以发起查询过程,以确定客户端设备402和/或利用客户端设备402的用户是否将接收生成负载平衡器404和/或执行针对动作的授权。安全性元件408可以识别被识别为用于向客户端设备402和/或利用客户端设备402的用户提供授权的授权者的账户(诸如电子邮件账户、消息传递账户、社交媒体账户或可以向授权者提供消息的其他账户)、电话号码、设备或其某种组合。安全性元件408可以向每个授权者传输请求指示客户端设备402和/或利用客户端设备402的用户是否将被授予生成负载平衡器404和/或针对动作的授权的响应的一个或多个请求。请求可以包括客户端设备402和/或客户端设备402的用户寻求授权以生成负载平衡器404和/或动作的指示。安全性元件408可以将请求传输到每个授权者的账户、电话号码、设备或其某种组合中的一个或多个。请求可以请求授权者用客户端设备402和/或利用客户端设备402的用户是否将被授予生成负载平衡器404和/或针对动作的授权的指示进行响应。在一些实例中,安全性元件408可以在请求是否将向客户端设备402和/或客户端设备402的用户授予生成负载平衡器404和/或针对动作的授权的指示的初始请求之后发送一个或多个后续请求。

[0081] 授权布置400可以包括一个或多个授权者设备410,诸如第一授权者设备410a和第二授权者设备410b。授权者设备410可以与一个或多个授权者对应。例如,每个授权者设备410可以包括设备,一个或多个授权者可以在该设备中访问账户、电话号码和/或由安全性元件408向其传输请求的设备。基于识别出的授权者,安全性元件408可以识别与识别出的授权者相关联的授权者设备410,并且在一些实例中将请求传输到授权者设备410。在一些实例中,授权者设备410可以包括输入设备,该输入设备允许授权者输入是否向客户端设备402和/或利用客户端设备402的用户提供生成负载平衡器404和/或执行针对动作的授权的

指示。

[0082] 安全性元件408可以向每个授权者设备410提供请求。例如,安全性元件408可以将请求直接传输到每个授权者设备410、可以经由授权者设备410访问的账户、与授权者设备410相关联的电话号码或其某种组合。在所示实施例中,安全性元件408可以向第一授权者设备410a传输一个或多个请求以寻求来自第一授权者的指示,并可以向第二授权者设备410b传输一个或多个请求以寻求来自第二授权者的指示。在一些实例中,第一授权者设备410a和/或第二授权者设备410b可以在设备上显示用户界面,该用户界面从对应的授权者请求对客户端设备402和/或利用客户端设备402的用户的授权的指示。每个授权者设备410可以检测来自对应授权者的是否应向客户端设备402和/或利用客户端设备402的用户提供生成负载平衡器404和/或执行针对动作的授权的指示。基于从授权者接收到的指示,授权者设备410可以传输是否应向客户端设备402和/或客户端设备402的用户授予生成负载平衡器404和/或针对动作的授权的指示。在一些实例中,授权者可能未向一个或多个授权者设备410提供指示,在这种情况下,未接收到指示的一个或多个授权者设备可以不向安全性元件408提供响应。

[0083] 安全性元件408可以监视来自授权者设备410的响应,并可以接收来自授权者设备410的响应。例如,在所示实施例中,安全性元件408可以接收来自与第一授权者对应的第一授权者设备410a的第一响应以及来自与第二授权者对应的第二授权者设备410b的第二响应。安全性元件408可以确定是否要向客户端设备402和/或客户端设备402的用户授予生成负载平衡器404和/或针对动作的授权。在一些实施例中,安全性元件408在确定是否要向客户端设备402和/或客户端设备402的用户授予生成负载平衡器和/或针对动作的授权之前可以等待,直到从所有向其传输请求的授权者接收到响应。如果安全性元件408确定所有授权者都指示客户端设备402和/或利用客户端设备402的用户应被授权生成负载平衡器404和/或执行动作,那么安全性元件408可以确定客户端设备402和/或利用客户端设备402的用户应被授权生成负载平衡器404和/或执行动作。如果任何授权者指示客户端设备402和/或利用客户端设备402的用户不应被授权生成负载平衡器404和/或执行动作,那么安全性元件408可以确定客户端设备402和/或利用客户端设备402的用户不应被授权生成负载平衡器404和/或执行动作。

[0084] 在一些实例中,安全性元件408可以不要求授权者一致指示客户端设备402和/或利用客户端设备402的用户将被授予授权的,以确定客户端设备402和/或利用客户端设备402的用户被授权生成负载平衡器404和/或执行动作。在这些实例中,安全性元件408可以基于一定百分比的指示客户端具有生成负载平衡器404和/或执行针对动作的授权的响应或者与某些授权者对应的响应指示客户端具有生成负载平衡器404和/或执行针对动作的授权来确定客户端具有授权。

[0085] 在一些实例中,安全性元件408可以实现用于来自授权者的用于确定客户端是否具有生成负载平衡器404和/或执行针对动作的授权的响应的定时器。例如,如果安全性元件408确定在定时器定义的时间段内未接收到来自授权者的为客户端设备402和/或利用客户端设备402的用户提供生成负载平衡器404和/或执行针对动作的授权的足够响应,那么安全性元件408可以确定客户端设备402和/或利用客户端设备402的用户不具有生成负载平衡器404和/或执行针对动作的授权。

[0086] 如果安全性元件408基于来自授权者的响应确定客户端没有生成负载平衡器404和/或执行针对动作的授权,那么安全性元件408可以不执行与生成负载平衡器404和/或动作相关联的操作。安全性元件408还可以基于确定客户端没有生成负载平衡器404和/或执行针对动作的授权而从存储器中移除所存储的操作。

[0087] 如果安全性元件408基于来自授权者的响应确定客户端具有生成负载平衡器404和/或执行针对动作的授权,那么安全性元件408可以执行操作。例如,安全性元件408可以从存储器中检索签署的序列化的操作。安全性元件408可以检查签署的序列化的操作的签名以确定操作是否已被篡改。例如,安全性元件408可以将检索时的签署的序列化的操作的签名与序列化的操作被签署时产生的签名进行比较。如果签名匹配,那么安全性元件408可以确定操作未被篡改。如果签名不匹配,那么安全性元件408可以确定操作已被篡改。

[0088] 如果安全性元件408确定操作已被篡改,那么安全性元件408可以阻止执行操作。如果安全性元件408确定操作未被篡改,那么安全性元件204可以继续使得执行序列化的操作。例如,安全性元件408可以使飞地406和/或基础设施服务执行序列化的操作,其中操作的序列化使得在执行操作时考虑状态。操作的执行可以导致负载平衡器404的生成。在所示实施例中,负载平衡器404可以在飞地406中生成。在其他实施例中,负载平衡器404可以在基础设施服务的另一部分中生成。在一些实施例中,安全性元件408可以在飞地406的边缘处生成负载平衡器404。负载平衡器404可以位于飞地406的防火墙内部或外部。

[0089] 图5图示了根据一些实施例的授权客户端执行动作的示例过程500。过程500可由基础设施服务(诸如关于图1描述的基础设施服务、图9的云基础设施、图10的云基础设施、图11的云基础设施和/或图12的云基础设施,其可以包括计算系统和/或云计算系统)、飞地(诸如飞地104(图1)、飞地202(图2)和/或飞地406(图4))、安全性元件(例如,安全性元件108(图1)、安全性元件204(图2)和/或安全性元件408(图4))或其某种组合执行。可以执行过程500以确定客户端设备(诸如客户端设备206(图2)和/或客户端设备402(图4))是否被授权执行动作(诸如生成负载平衡器(诸如负载平衡器404(图4))。

[0090] 为简洁起见,本文将过程500描述为由计算系统执行,但应当理解的是,过程500可以由基础设施服务、飞地、安全性元件或其某种组合执行。在一些实施例中,计算系统可以包括云基础设施服务。

[0091] 在502中,计算系统可以接收对要执行的动作的请求。例如,安全性元件可以接收对要由计算系统执行的操作的请求,该请求是从客户端设备接收的。在一些实施例中,计算系统可以包括云基础设施服务。在一些实施例中,云基础设施服务可以在飞地的边缘(例如,飞地104(图1)的边缘)处接收对动作的请求。在这些实施例中的一些实施例中,云基础设施服务可以在飞地的防火墙之外接收对动作的请求。在一些实施例中,动作可以包括生成负载平衡器(诸如负载平衡器404(图4))。

[0092] 在504中,计算系统可以识别一个或多个授权者。例如,计算系统可以识别要从其接收针对动作的授权的一个或多个授权者。授权可以与针对客户端设备的对动作的执行对应。授权者可以包括贯穿本公开描述的授权者的特征中的一个或多个。可以基于客户端设备、客户端设备的用户、所请求的动作或其某种组合来识别授权者。在一些实施例中,客户端设备和/或客户端设备的用户可以与计算系统的订户相关联,其中授权者可以与和客户端设备和/或客户端设备的用户相同的订户相关联。计算系统可以基于确定客户端设备和/

或客户端设备的用户先前未被授予执行针对动作的授权来识别一个或多个授权者。

[0093] 在506中,计算系统可以序列化一个或多个操作。例如,计算系统可以序列化与请求执行的动作对应的一个或多个操作。一个或多个操作的序列化可以包括贯穿本公开描述的序列化操作的特征中的一个或多个,诸如序列化的操作306(图3)。序列化一个或多个操作的计算系统可以维持与对应操作的状态,使得可以在稍后解冻操作以执行操作。

[0094] 在508中,计算系统可以签署一个或多个序列化的操作。例如,计算系统可以经由ECDSA签署一个或多个序列化的操作。经由ECDSA签署一个或多个序列化的操作可以包括贯穿本公开描述的经由ECDSA签署操作的特征中的一个或多个,诸如签署的序列化的操作306(图3)。例如,计算系统可以利用密钥和ECDSA来生成用于签署一个或多个序列化的操作的签名。计算系统可以用签名签署一个或多个序列化的操作。

[0095] 在510中,计算系统可以向客户端设备提供签名。例如,计算系统可以与客户端设备共享签名,同时在计算系统、飞地(诸如飞地104、飞地202和/或飞地406)和/或基础设施服务中维护用于生成签名的密钥。在计算系统、飞地和/或基础设施服务中维护密钥可以提供针对不良行为者的安全性,而共享签名可以提供对客户端设备的识别。在一些实施例中,可以省略510。

[0096] 在512中,计算系统可以发起查询过程。例如,计算机系统可以发起针对来自一个或多个授权者中的每一个针对动作的授权的查询过程,以确定是否授权执行一个或多个操作。查询过程可以包括贯穿本公开描述的用于授权者的查询过程的特征中的一个或多个。在一些实施例中,查询过程可以包括向一个或多个授权者中的每一个传输至少一个授权请求。计算系统还可以监视一个或多个授权者中的每一个对至少一个授权请求的响应。

[0097] 在514中,计算系统可以确定已接收到授权。例如,计算系统可以确定已经从一个或多个授权者中的每一个接收到针对该针对动作的授权。特别地,计算系统可以确定客户端设备和/或使用客户端设备的用户具有执行该针对动作的授权。计算系统可以根据本文描述的用于确定已从授权者接收到授权的方法来确定已接收到授权,诸如所有授权者指示将授予授权、授权者的某一部分指示将授予授权或授权者的某个组指示将授予授权。在一些实例中,动作可以是生成负载平衡器,其中授权者可以指示客户端设备和/或利用客户端设备的用户被授权生成负载平衡器。在一些实施例中,可以省略514。

[0098] 在516中,计算系统可以核实序列化的一个或多个操作未被篡改。例如,计算系统可以至少部分地基于通过序列化的一个或多个操作的签署产生的签名来核实序列化的一个或多个操作未被篡改。计算系统可以基于在检索时来自签署的序列化的操作的签名与签署序列化的操作时的签名相同来核实一个或多个操作未被篡改。在一些实施例中,可以省略516。

[0099] 在518中,计算系统可以执行一个或多个操作。例如,计算系统可以至少部分地基于已接收到针对动作的授权的确定来执行一个或多个操作。执行一个或多个操作的计算系统可以导致执行客户端设备请求的动作。在一些实施例中,动作可以是生成负载平衡器,其中一个或多个操作导致计算系统生成负载平衡器。在计算系统是云基础设施服务的实施例中,云基础设施服务可以被配置为在云基础设施服务的飞地末端创建负载平衡器。在一些实施例中,可以省略518。

[0100] 图6图示了根据一些实施例的授权客户端执行动作的另一个示例过程600。过程

600可以以由基础设施服务(诸如关于图1描述的基础设施服务、图9的云基础设施、图10的云基础设施、图11的云基础设施和/或图12的云基础设施,其可以以包括计算系统和/或云计算系统)、飞地(诸如飞地104(图1)、飞地202(图2)和/或飞地406(图4))、安全性元件(诸如安全性元件108(图1)、安全性元件204(图2)和/或安全性元件408(图4))或其某种组合执行。可以执行过程600来确定客户端设备(诸如客户端设备206(图2)和/或客户端设备402(图4))是否被授权执行动作(诸如生成负载平衡器(诸如负载平衡器404(图4))。

[0101] 为简洁起见,本文将过程600描述为由安全性元件执行,但应当理解的是,过程600可以由基础设施服务、飞地、计算系统或其某种组合执行。在一些实施例中,安全性元件可以是云基础设施服务的一部分。

[0102] 在602中,安全性元件可以接收对要执行的动作的请求。例如,安全性元件可以接收要由云基础设施服务执行的动作的请求。安全性元件可以从客户端设备(诸如客户端设备206和/或客户端设备402)接收请求。在一些实施例中,安全性元件可以在云基础设施服务的飞地(诸如飞地104、飞地202和/或飞地406)的边缘处实现。另外,在一些实施例中,安全性元件可以实现在飞地的防火墙之外。在一些实施例中,安全性元件可以包括云基础设施服务的代理或守护进程。

[0103] 在604中,安全性元件可以防止提供安全信息。例如,在一些实施例中,云基础设施服务可以是第一云基础设施服务,并且请求可以从第二云基础设施服务接收,其中客户端设备可以是第二云基础设施服务或其某些部分。安全性元件可以防止将与第一云基础设施服务相关的安全信息提供给第二云基础设施服务。在一些实施例中,安全性元件可以在接收到来自一个或多个授权者接收的响应之前防止将安全信息提供给第二云基础设施服务。在其他实施例中,安全性元件可以防止在整个过程600中和/或在第一云基础设施服务与第二云基础设施服务之间的整个交互中将安全信息提供给第二云基础设施服务。在一些实施例中,可以省略604。

[0104] 在606中,安全性元件可以识别一个或多个授权者。例如,安全性元件可以识别要从其接收针对动作的授权的一个或多个授权者,该授权与动作的执行对应。识别出的授权者可以是可以为客户端设备和/或利用客户端设备的用户提供执行针对动作的授权的授权者。授权者可以包括贯穿本公开描述的一个或多个授权者的特征,诸如与客户端设备和/或利用客户端设备的用户与云基础设施服务的同一订户相关联的授权者。

[0105] 在608中,安全性元件可以确定一个或多个操作。例如,安全性元件可以确定云基础设施服务为了完成动作而要执行的一个或多个操作。云基础设施服务可以能够执行一个或多个操作以完成客户端设备请求的动作。安全性元件可以根据贯穿本公开描述的用于动作的操作的确定来确定一个或多个操作。

[0106] 在610中,安全性元件可以序列化一个或多个操作。例如,安全性元件可以序列化与请求执行的动作对应的一个或多个操作。一个或多个操作的序列化可以包括贯穿本公开描述的序列化操作的特征中的一个或多个,诸如序列化的操作306(图3)。序列化一个或多个操作的计算系统可以维持与对应操作的状态,使得操作可以在稍后解冻以执行操作。在一些实施例中,可以省略610。

[0107] 在612中,安全性元件可以签署一个或多个操作。例如,安全性元件可以经由ECDSA签署一个或多个操作。经由ECDSA签署一个或多个序列化的操作可以包括贯穿本公开描述

的经由ECDSA签署操作的特征中的一个或多个,诸如签署的序列化的操作306(图3)。例如,安全性元件可以利用密钥和ECDSA来生成用于签署一个或多个操作的签名。安全性元件可以用签名签署一个或多个操作。在操作被序列化的实施例中,安全性元件可以签署序列化的一个或多个操作。

[0108] 在614中,安全性元件可以存储签署的一个或多个操作。例如,安全性元件可以将签署的一个或多个操作存储在安全性元件的存储器、飞地的存储器、云基础设施服务的存储器或其某种组合中。在操作已被序列化的实施例中,安全性元件可以存储签署的、序列化的一个或多个操作。

[0109] 在616中,安全性元件可以发起查询过程。例如,安全性元件可以至少部分地基于从一个或多个授权者接收到的响应来发起用于授权动作的查询过程。查询过程可以包括贯穿本公开描述的授权者查询过程的特征中的一个或多个。在一些实施例中,查询过程可以包括向一个或多个授权者传输至少一个授权请求。安全性元件可以监视从一个或多个授权者接收到的对至少一个授权请求的响应。

[0110] 在618中,安全性元件可以确定已接收到授权。例如,安全性元件可以确定已从一个或多个授权者中的每一个接收到针对动作的授权。特别地,安全性元件可以确定客户端设备和/或利用客户端设备的用户具有执行针对动作的授权。计算系统可以根据本文描述的用于确定已从授权者接收到授权的方法来确定已接收到授权,诸如所有授权者指示要授予授权、授权者的某一部分指示要授予授权、或授权者的某一组指示要授予授权。在一些实施例中,可以省略618。

[0111] 在620中,安全性元件可以核实一个或多个操作未被篡改。例如,安全性元件可以至少部分地基于通过签署一个或多个操作所产生的签名来核实一个或多个操作未被篡改。计算系统可以基于在检索时来自签署的操作的签名与签署操作时的签名相同来核实一个或多个操作未被篡改。在一些实施例中,可以省略620。

[0112] 在622中,安全性元件可以使得执行一个或多个操作。例如,安全性元件可以至少部分地基于确定已接收到针对动作的授权而使得执行一个或多个操作。使得执行一个或多个操作的安全性元件可以使得执行客户端设备所请求的操作。在一些实施例中,可以省略622。

[0113] 图7图示了根据一些实施例的授权客户端执行动作的另一个示例过程700的第一部分。图8图示了根据一些实施例的示例过程700的第二部分。过程700可以由基础设施服务(诸如关于图1描述的基础设施服务、图9的云基础设施、图10的云基础设施、图11的云基础设施和/或图12的云基础设施,其可以包括计算系统和/或云计算系统)、飞地(诸如飞地104(图1)、飞地202(图2)和/或飞地406(图4))、安全性元件(诸如安全性元件108(图1)、安全性元件204(图2)和/或安全性元件408(图4))或其某种组合执行。可以执行过程700来确定客户端设备(诸如客户端设备206(图2)和/或客户端设备402(图4))是否被授权执行动作(诸如生成负载平衡器(诸如负载平衡器404(图4))。

[0114] 为简洁起见,本文将过程700描述为由计算系统执行,但应当理解的是,过程700可以由基础设施服务、飞地、安全性元件或其某种组合执行。在一些实施例中,安全性元件可以是云基础设施服务的一部分。

[0115] 在702中,计算系统可以实现安全性元件。例如,计算系统可以包括云基础设施服

务,其中云基础设施服务将在云基础设施服务的飞地的边缘处实现安全性元件。安全性元件可以包括安全性元件108、安全性元件204和/或安全性元件408的特征中的一个或多个。在一些实施例中,可以省略702。

[0116] 在704中,计算系统可以识别对要执行的动作的请求。例如,计算系统可以识别对要由计算系统执行的动作的请求,该请求从客户端设备(诸如客户端设备206和/或客户端设备402)接收。在一些实施例中,计算系统可以包括云基础设施服务,在一些实施例中,该云基础设施服务可以在云基础设施服务的飞地的边缘接收对动作的请求。在这些实施例中的一些实施例中,云基础设施服务可以在飞地的防火墙外接收对动作的请求。在计算系统实现安全性元件的一些实施例中,安全性元件可以识别对动作的请求。

[0117] 在706中,计算系统可以识别一个或多个授权者。例如,计算系统可以识别要从其接收针对动作的授权的一个或多个授权者,该授权与针对客户端设备的对动作的执行对应。授权者可以包括贯穿本公开描述的授权者的特征中的一个或多个。可以基于客户端设备、客户端设备的用户、所请求的动作或其某种组合来识别授权者。在一些实施例中,客户端设备和/或客户端设备的用户可以与计算系统的订户相关联,其中授权者可以与和客户端设备和/或客户端设备的用户相同的订户相关联。计算系统可以基于确定客户端设备和/或客户端设备的用户先前未被授予执行针对动作的授权来识别一个或多个授权者。

[0118] 在708中,计算系统可以确定要执行的一个或多个操作。例如,计算系统可以确定计算系统为了完成动作而要执行的一个或多个操作。计算系统可以能够执行一个或多个操作以完成客户端设备请求的动作。计算系统可以根据贯穿本公开描述的用于动作的操作确定来确定一个或多个操作。

[0119] 在710中,计算系统可以序列化一个或多个操作。一个或多个操作的序列化可以包括贯穿本公开描述的序列化操作的特征中的一个或多个,诸如序列化的操作306(图3)。序列化一个或多个操作的计算系统可以维持与对应操作的状态,使得操作可以在稍后解冻以执行操作。

[0120] 在712中,计算系统可以签署序列化的一个或多个操作。例如,计算系统可以经由ECDSA签署序列化的一个或多个操作。经由ECDSA签署一个或多个序列化的操作可以包括贯穿本公开描述的经由ECDSA签署操作的特征中的一个或多个,诸如签署的序列化的操作306(图3)。例如,计算系统可以利用密钥和ECDSA来生成用于签署一个或多个序列化的操作的签名。计算系统可以用签名签署一个或多个序列化的操作。

[0121] 在714中,计算系统可以存储签署的、序列化的一个或多个操作。例如,计算系统可以将签署的、序列化的一个或多个操作存储在存储器中。存储器可以是计算系统的存储器、安全性元件的存储器、基础设施服务的存储器,或其某种组合。过程700可以从图7的716进行到图8的716。

[0122] 在802中,计算系统可以发起查询过程。例如,计算系统可以发起用于来自一个或多个授权者的针对动作的授权的查询过程。查询过程可以包括贯穿本公开描述的针对授权者的查询过程的特征中的一个或多个。在一些实施例中,查询过程可以包括向一个或多个授权者中的每一个传输至少一个授权请求。计算系统还可以监视一个或多个授权者中的每一个对至少一个授权请求的响应。

[0123] 在804中,计算系统可以确定已接收到授权。例如,计算系统可以确定已从一个或

多个授权者中的每一个接收到针对动作的授权。特别地,计算系统可以确定客户端设备和/或利用客户端设备的用户具有执行针对动作的授权。计算系统可以根据本文描述的确定已从授权者接收到授权的方法来确定已接收到授权,诸如所有授权者指示要授予授权、授权者的某一部分指示要授予授权、或授权者的某一组指示要授予授权。在一些实施例中,可以省略804。

[0124] 在806中,计算系统可以检索签署的、序列化的一个或多个操作。例如,计算系统可以从存储器中检索签署的、序列化的一个或多个操作。计算系统可以基于已接收到授权的确定来检索签署的、序列化的一个或多个操作。在一些实施例中,可以省略806。

[0125] 在808中,计算系统可以核实签署的、序列化的一个或多个操作未被篡改。例如,计算系统可以至少部分地基于通过签署序列化的一个或多个操作而进行核实。计算系统可以基于在检索时来自签署的、序列化的操作的签名与签署序列化的操作时的签名相同来核实一个或多个操作未被篡改。在一些实施例中,可以省略808。

[0126] 在810中,计算系统可以执行一个或多个操作。例如,计算系统可以至少部分地基于授权和从存储器检索到的签署的、序列化的一个或多个操作来执行一个或多个操作。在一些实施例中,计算系统还可以至少部分地基于对签署的、序列化的一个或多个操作未被篡改的核实来执行一个或多个操作。执行一个或多个操作的计算系统可以使得执行客户端设备请求的操作。在一些实施例中,可以省略810。

[0127] 如以上所指出的,基础设施即服务(IaaS)是一种特定类型的云计算。IaaS可以被配置为通过公共网络(例如,互联网)提供虚拟化计算资源。在IaaS模型中,云计算提供商可以托管基础设施组件(例如,服务器、存储设备、网络节点(例如,硬件)、部署软件、平台虚拟化(例如,管理程序层)等)。在一些情况下,IaaS提供商还可以提供各种服务来伴随这些基础设施组件(例如,计费、监视、记载、负载平衡和聚类等)。因此,由于这些服务可能是策略驱动的,因此IaaS用户可以能够实现策略来驱动负载平衡,以维持应用的可用性和性能。

[0128] 在一些情况下,IaaS客户可以通过诸如互联网之类的广域网(WAN)访问资源和服务,并且可以使用云提供商的服务来安装应用栈的剩余元素。例如,用户可以登录到IaaS平台以创建虚拟机(VM)、在每个VM上安装操作系统(OS)、部署诸如数据库之类的中间件、为工作负载和备份创建存储桶,甚至将企业软件安装到那个VM中。然后,客户可以使用提供商的服务来执行各种功能,包括平衡网络流量、解决应用问题、监视性能、管理灾难恢复等。

[0129] 在大多数情况下,云计算模型将需要云提供商的参与。云提供商可以但不一定是专门提供(例如,供应、出租、销售)IaaS的第三方服务。实体也可能选择部署私有云,从而成为其自己的基础设施服务提供商。

[0130] 在一些示例中,IaaS部署是将新应用或应用的新版本放置到准备好的应用服务器等上的处理。它还可以包括准备服务器(例如,安装库、守护进程等)的处理。这通常由云提供商管理,位于管理程序层之下(例如,服务器、存储装置、网络硬件和虚拟化)。因此,客户可以负责处理(OS)、中间件和/或应用部署(例如,在(例如,可以按需启动的)自助服务虚拟机等上)。

[0131] 在一些示例中,IaaS供给可以指获取计算机或虚拟主机以供使用,甚至在它们上安装所需的库或服务。大多数情况下,部署不包括供给,并且供给可能需要被首先执行。

[0132] 在一些情况下,IaaS供给存在两个不同的挑战。首先,在任何东西运行之前供给初

始基础设施集存在最初的挑战。其次,一旦所有东西已被供给,就存在演进现有基础设施(例如,添加新服务、更改服务、移除服务等)的挑战。在一些情况下,可以通过启用以声明方式定义基础设施的配置来解决这两个挑战。换句话说,基础设施(例如,需要哪些组件以及它们如何交互)可以由一个或多个配置文件来定义。因此,基础设施的总体拓扑(例如,哪些资源依赖于哪些资源,以及它们如何协同工作)可以以声明的方式描述。在一些情况下,一旦定义了拓扑,就可以生成创建和/或管理配置文件中描述的不同组件的工作流。

[0133] 在一些示例中,基础设施可以具有许多互连的元素。例如,可能存在一个或多个虚拟私有云(VPC)(例如,可配置和/或共享计算资源的潜在按需池),也称为核心网络。在一些示例中,还可以供给一个或多个入站/出站流量组规则以定义如何设置网络的入站/出站流量以及一个或多个虚拟机(VM)。也可以供给其它基础设施元素,诸如负载平衡器、数据库等。随着期望和/或添加越来越多的基础设施元素,基础设施可以逐步演进。

[0134] 在一些情况下,可以采用连续部署技术来使得能够跨各种虚拟计算环境部署基础设施代码。此外,所描述的技术可以使得能够在这些环境内进行基础设施管理。在一些示例中,服务团队可以编写期望部署到一个或多个但通常是许多不同的生产环境(例如,跨各种不同的地理位置,有时跨越整个世界)的代码。但是,在一些示例中,必须首先设置将在其上部署代码的基础设施。在一些情况下,供给可以手动完成,可以利用供给工具来供给资源,和/或一旦供给基础设施就可以利用部署工具来部署代码。

[0135] 图9是图示根据至少一个实施例的IaaS体系架构的示例模式的框图900。服务运营商902可以通信地耦合到可以包括虚拟云网络(VCN)906和安全主机子网908的安全主机租赁904。在一些示例中,服务运营商902可以使用一个或多个客户端计算设备,其可以是便携式手持设备(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)、运行软件(诸如Microsoft Windows **Mobile®**)和/或各种移动操作系统(诸如iOS、Windows Phone、Android、BlackBerry 8、Palm OS等),并且支持互联网、电子邮件、短消息服务(SMS)、**Blackberry®**或其它通信协议。可替代地,客户端计算设备可以是通用个人计算机,包括例如运行各种版本的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各种商业上可获得的**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统(诸如例如Google Chrome OS)中的任何一种)的工作站计算机。替代地或附加地,客户端计算设备可以是任何其它电子设备,诸如瘦客户端计算机、支持互联网的游戏系统(例如,具有或不具有**Kinect®**手势输入设备的Microsoft Xbox游戏控制台),和/或能够通过可以访问VCN 906和/或互联网的网络进行通信的个人消息传递设备。

[0136] VCN 906可以包括本地对等网关(LPG)910,其可以经由包含在SSH VCN 912中的LPG 910通信地耦合到安全壳(SSH)VCN 912。SSH VCN 912可以包括SSH子网914,并且SSH VCN 912可以经由包含在控制平面VCN 916中的LPG 910通信地耦合到控制平面VCN 916。此外,SSH VCN 912可以经由LPG 910通信地耦合到数据平面VCN 918。控制平面VCN 916和数据平面VCN 918可以包含在可以由IaaS提供商拥有和/或操作的服务租赁919中。

[0137] 控制平面VCN 916可以包括充当外围网络(例如,公司内部网和外部网络之间的公

司网络的部分)的控制平面非军事区(DMZ)层920。基于DMZ的服务器可以承担有限责任并有助于控制漏洞。此外,DMZ层920可以包括一个或多个负载平衡器(LB)子网922、可以包括(一个或多个)应用子网926的控制平面应用层924、可以包括(一个或多个)数据库(DB)子网930(例如,(一个或多个)前端DB子网和/或(一个或多个)后端DB子网)的控制平面数据层928。包含在控制平面DMZ层920中的(一个或多个)LB子网922可以通信地耦合到包含在控制平面应用层924中的(一个或多个)应用子网926和可以包含在控制平面VCN 916中的互联网网关934,并且(一个或多个)应用子网926可以通信地耦合到包含在控制平面数据层928中的(一个或多个)DB子网930以及服务网关936和网络地址转换(NAT)网关938。控制平面VCN916可以包括服务网关936和NAT网关938。

[0138] 控制平面VCN 916可以包括数据平面镜像应用层940,其可以包括(一个或多个)应用子网926。包含在数据平面镜像应用层940中的(一个或多个)应用子网926可以包括可以执行计算实例944的虚拟网络接口控制器(VNIC)942。计算实例944可以将数据平面镜像应用层940的(一个或多个)应用子网926通信地耦合到可以包含在数据平面应用层946中的(一个或多个)应用子网926。

[0139] 数据平面VCN 918可以包括数据平面应用层946、数据平面DMZ层948和数据平面数据层950。数据平面DMZ层948可以包括(一个或多个)LB子网922,其可以通信地耦合到数据平面应用层946的(一个或多个)应用子网926和数据平面VCN 918的互联网网关934。(一个或多个)应用子网926可以通信地耦合到数据平面VCN 918的服务网关936和数据平面VCN918的NAT网关938。数据平面数据层950还可以包括可以通信地耦合到数据平面应用层946的(一个或多个)应用子网926的(一个或多个)DB子网930。

[0140] 控制平面VCN 916和数据平面VCN 918的互联网网关934可以通信地耦合到元数据管理服务952,元数据管理服务952可以通信地耦合到公共互联网954。公共互联网954可以通信地耦合到控制平面VCN 916和数据平面VCN 918的NAT网关938。控制平面VCN 916和数据平面VCN 918的服务网关936可以通信地耦合到云服务956。

[0141] 在一些示例中,控制平面VCN 916或数据平面VCN 918的服务网关936可以对云服务956进行应用编程接口(API)调用,而无需通过公共互联网954。从服务网关936到云服务956的API调用可以是单向的:服务网关936可以对云服务956进行API调用,并且云服务956可以将请求的数据发送到服务网关936。但是,云服务956可以不发起对服务网关936的API调用。

[0142] 在一些示例中,安全主机租赁904可以直接连接到服务租赁919,服务租赁919否则可以被隔离。安全主机子网908可以通过LPG 910与SSH子网914通信,LPG 910可以使得能够在否则隔离的系统上进行双向通信。将安全主机子网908连接到SSH子网914可以使安全主机子网908访问服务租赁919内的其它实体。

[0143] 控制平面VCN 916可以允许服务租赁919的用户设置或以其它方式供给期望的资源。在控制平面VCN 916中供给的期望资源可以在数据平面VCN 918中部署或以其它方式使用。在一些示例中,控制平面VCN 916可以与数据平面VCN 918隔离,并且控制平面VCN 916的数据平面镜像应用层940可以经由VNIC 942与数据平面VCN 918的数据平面应用层946通信,VNIC 942可以包含在数据平面镜像应用层940和数据平面应用层946中。

[0144] 在一些示例中,系统的用户或客户可以通过可以将请求传送到元数据管理服务

952的公共互联网954来做出请求,例如创建、读取、更新或删除(CRUD)操作。元数据管理服务952可以通过互联网网关934将请求传送到控制平面VCN 916。请求可以被包含在控制平面DMZ层920中的(一个或多个)LB子网922接收。(一个或多个)LB子网922可以确定请求是有效的,并且响应于该确定,(一个或多个)LB子网922可以将请求传输到包含在控制平面应用层924中的(一个或多个)应用子网926。如果请求被验证并且需要对公共互联网954的调用,那么对公共互联网954的调用可以被传输到可以对公共互联网954进行调用的NAT网关938。该请求可能期望被存储的存储器可以存储在(一个或多个)DB子网930中。

[0145] 在一些示例中,数据平面镜像应用层940可以促进控制平面VCN 916和数据平面VCN 918之间的直接通信。例如,可能期望对包含在数据平面VCN 918中的资源应用对配置的更改、更新或其它适当的修改。经由VNIC 942,控制平面VCN 916可以直接与包含在数据平面VCN 918中的资源通信,并且从而可以执行对配置的更改、更新或其它适当的修改。

[0146] 在一些实施例中,控制平面VCN 916和数据平面VCN 918可以包含在服务租赁919中。在这种情况下,系统的用户或客户可能不拥有或操作控制平面VCN 916或数据平面VCN918。替代地,IaaS提供商可以拥有或操作控制平面VCN 916和数据平面VCN 918,这两者平面都可以包含在服务租赁919中。该实施例可以使得能够隔离可能阻止用户或客户与其它用户或其它客户的资源交互的网络。此外,该实施例可以允许系统的用户或客户私自存储数据库,而无需依赖可能不具有期望威胁预防级别的公共互联网954进行存储。

[0147] 在其它实施例中,包含在控制平面VCN 916中的(一个或多个)LB子网922可以被配置为从服务网关936接收信号。在这个实施例中,控制平面VCN 916和数据平面VCN 918可以被配置为由IaaS提供商的客户调用而无需调用公共互联网954。IaaS提供商的客户可能期望这个实施例,因为客户使用的(一个或多个)数据库可以由IaaS提供商控制并且可以存储在服务租赁919上,服务租赁919可能与公共互联网954隔离。

[0148] 图10是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1000。服务运营商1002(例如,图9的服务运营商902)可以通信地耦合到安全主机租赁1004(例如,图9的安全主机租赁904),该安全主机租赁1004可以包括虚拟云网络(VCN)1006(例如,图9的VCN 906)和安全主机子网1008(例如,图9的安全主机子网908)。VCN 1006可以包括本地对等网关(LPG)1010(例如,图9的LPG 910),其可以经由包含在SSH VCN 1012中的LPG 910通信地耦合到安全壳(SSH)VCN 1012(例如,图9的SSH VCN 912)。SSH VCN 1012可以包括SSH子网1014(例如,图9的SSH子网914),并且SSH VCN 1012可以经由包含在控制平面VCN1016中的LPG 1010通信地耦合到控制平面VCN 1016(例如,图9的控制平面VCN 916)。控制平面VCN 1016可以包含在服务租赁1019(例如,图9的服务租赁919)中,并且数据平面VCN1018(例如,图9的数据平面VCN 918)可以包含在可能由系统的用户或客户拥有或操作的客户租赁1021中。

[0149] 控制平面VCN 1016可以包括控制平面DMZ层1020(例如,图9的控制平面DMZ层920),其可以包括(一个或多个)LB子网1022(例如,图9的(一个或多个)LB子网922)、可以包括(一个或多个)应用子网1026(例如,图9的(一个或多个)应用子网926)的控制平面应用层1024(例如,图9的控制平面应用层924)、可以包括(一个或多个)数据库(DB)子网1030(例如,类似于图9的(一个或多个)DB子网930)的控制平面数据层1028(例如,图9的控制平面数据层928)。包含在控制平面DMZ层1020中的(一个或多个)LB子网1022可以通信地耦合到包

含在控制平面应用层1024中的(一个或多个)应用子网1026和可以包含在控制平面VCN1016中的互联网网关1034(例如,图9的互联网网关934),并且(一个或多个)应用子网1026可以通信地耦合到包含在控制平面数据层1028中的(一个或多个)DB子网1030以及服务网关1036(例如,图9的服务网关636)和网络地址转换(NAT)网关1038(例如,图9的NAT网关938)。控制平面VCN 1016可以包括服务网关1036和NAT网关1038。

[0150] 控制平面VCN 1016可以包括:可以包括(一个或多个)应用子网1026的数据平面镜像应用层1040(例如,图9的数据平面镜像应用层940)。包含在数据平面镜像应用层1040中的(一个或多个)应用子网1026可以包括可以执行计算实例1044(例如,类似于图9的计算实例944)的虚拟网络接口控制器(VNIC)1042(例如,图9的VNIC 942)。计算实例1044可以促进数据平面镜像应用层1040的(一个或多个)应用子网1026和可以包含在数据平面应用层1046(例如,图9的数据平面应用层946)中的(一个或多个)应用子网1026之间经由包含在数据平面镜像应用层1040中的VNIC 1042和包含在数据平面应用层1046中的VNIC 1042的通信。

[0151] 包含在控制平面VCN 1016中的互联网网关1034可以通信地耦合到元数据管理服务1052(例如,图9的元数据管理服务952),该元数据管理服务1052可以通信地耦合到公共互联网1054(例如,图9的公共互联网954)。公共互联网1054可以通信地耦合到包含在控制平面VCN 1016中的NAT网关1038。包含在控制平面VCN 1016中的服务网关1036可以通信地耦合到云服务1056(例如,图9的云服务956)。

[0152] 在一些示例中,数据平面VCN 1018可以包含在客户租赁1021中。在这种情况下,IaaS提供商可以为每个客户提供控制平面VCN1016,并且IaaS提供商可以为每个客户设置包含在服务租赁1019中的唯一计算实例1044。每个计算实例1044可以允许包含在服务租赁1019中的控制平面VCN 1016和包含在客户租赁1021中的数据平面VCN 1018之间的通信。计算实例1044可以允许在包含在服务租赁1019中的控制平面VCN 1016中供给的资源被部署在包含在客户租赁1021中的数据平面VCN 1018中或以其它方式在其中使用。

[0153] 在其它示例中,IaaS提供商的客户可以具有存在于客户租赁1021中的数据库。在这个示例中,控制平面VCN 1016可以包括数据平面镜像应用层1040,其可以包括(一个或多个)应用子网1026。数据平面镜像应用层1040可以驻留在数据平面VCN 1018中,但数据平面镜像应用层1040可能不在数据平面VCN 1018中。即,数据平面镜像应用层1040可以访问客户租赁1021,但是数据平面镜像应用层1040可能不存在于数据平面VCN 1018中或者由IaaS提供商的客户拥有或操作。数据平面镜像应用层1040可以被配置为对数据平面VCN 1018进行调用,但可以不被配置为对包含在控制平面VCN 1016中的任何实体进行调用。客户可能期望在数据平面VCN 1018中部署或以其它方式使用在控制平面VCN 1016中供给的资源,并且数据平面镜像应用层1040可以促进客户的期望部署或资源的其它使用。

[0154] 在一些实施例中,IaaS提供商的客户可以将过滤器应用到数据平面VCN 1018。在这个实施例中,客户可以确定数据平面VCN 1018可以访问什么,并且客户可以限制从数据平面VCN 1018对公共互联网1054的访问。IaaS提供商可能无法应用过滤器或以其它方式控制数据平面VCN 1018对任何外部网络或数据库的访问。客户将过滤器和控制应用到包含在客户租赁1021中的数据平面VCN 1018上可以帮助将数据平面VCN 1018与其它客户和公共互联网1054隔离开。

[0155] 在一些实施例中,云服务1056可以由服务网关1036调用以访问公共互联网1054、控制平面VCN 1016或数据平面VCN 1018上可能不存在的服务。云服务1056与控制平面VCN1016或数据平面VCN 1018之间的连接可以不是实时的或连续的。云服务1056可以存在于由IaaS提供商拥有或操作的不同网络上。云服务1056可以被配置为接收来自服务网关1036的调用并且可以被配置为不接收来自公共互联网1054的调用。一些云服务1056可以与其它云服务1056隔离,并且控制平面VCN 1016可以与可能与控制平面VCN 1016不在同一区域的云服务1056隔离。例如,控制平面VCN 1016可能位于“区域1”,并且云服务“部署9”可能位于区域1和“区域2”。如果包含在位于区域1中的控制平面VCN 1016中的服务网关1036对部署9进行调用,那么该调用可以被传输到区域1中的部署9。在这个示例中,控制平面VCN 1016或区域1中的部署9可能不与区域2中的部署9通信地耦合或以其它方式与之通信。

[0156] 图11是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1100。服务运营商1102(例如,图9的服务运营商902)可以通信地耦合到安全主机租赁1104(例如,图9的安全主机租赁904),该安全主机租赁1104可以包括虚拟云网络(VCN)1106(例如,图9的VCN 906)和安全主机子网1108(例如,图9的安全主机子网908)。VCN 1106可以包括LPG1110(例如,图9的LPG 910),其可以经由包含在SSH VCN 1112中的LPG 1110通信地耦合到SSH VCN 1112(例如,图9的SSH VCN 912)。SSH VCN 1112可以包括SSH子网1114(例如,图9的SSH子网914),并且SSH VCN 1112可以经由包含在控制平面VCN 1116中的LPG 1110通信地耦合到控制平面VCN 1116(例如,图9的控制平面VCN 916)并且经由包含在数据平面VCN1118中的LPG 1110耦合到数据平面VCN 1118(例如,图9的数据平面918)。控制平面VCN1116和数据平面VCN 1118可以包含在服务租赁1119(例如,图9的服务租赁919)中。

[0157] 控制平面VCN 1116可以包括:可以包括(一个或多个)负载平衡器(LB)子网1122(例如,图9的(一个或多个)LB子网922)的控制平面DMZ层1120(例如,图9的控制平面DMZ层920)、可以包括(一个或多个)应用子网1126(例如,类似于图9的(一个或多个)应用子网926)的控制平面应用层1124(例如,图9的控制平面应用层924)、可以包括(一个或多个)DB子网1130的控制平面数据层1128(例如,图9的控制平面数据层928)。包含在控制平面DMZ层1120中的(一个或多个)LB子网1122可以通信地耦合到包含在控制平面应用层1124中的(一个或多个)应用子网1126和可以包含在控制平面VCN 1116中的互联网网关1134(例如,图9的互联网网关934),并且(一个或多个)应用子网1126可以通信地耦合到包含在控制平面数据层1128中的(一个或多个)DB子网1130以及服务网关1136(例如,图9的服务网关936)和网络地址转换(NAT)网关1138(例如,图9的NAT网关938)。控制平面VCN 1116可以包括服务网关1136和NAT网关1138。

[0158] 数据平面VCN 1118可以包括数据平面应用层1146(例如,图9的数据平面应用层946)、数据平面DMZ层1148(例如,图9的数据平面DMZ层948)、以及数据平面数据层1150(例如,图9的数据平面数据层950)。数据平面DMZ层1148可以包括可以通信地耦合到数据平面应用层1146的(一个或多个)可信应用子网1160和(一个或多个)不可信应用子网1162以及包含在数据平面VCN 1118中的互联网网关1134的(一个或多个)LB子网1122。(一个或多个)可信应用子网1160可以通信地耦合到包含在数据平面VCN 1118中的服务网关1136、包含在数据平面VCN 1118中的NAT网关1138以及包含在数据平面数据层1150中的(一个或多个)DB子网1130。(一个或多个)不可信应用子网1162可以通信地耦合到包含在数据平面VCN 1118

中的服务网关1136和包含在数据平面数据层1150中的(一个或多个)DB子网1130。数据平面数据层1150可以包括可以通信地耦合到包含在数据平面VCN 1118中的服务网关1136的(一个或多个)DB子网1130。

[0159] (一个或多个)不可信应用子网1162可以包括可以通信地耦合到租户虚拟机(VM)1166(1)-(N)的一个或多个主VNIC 1164(1)-(N)。每个租户VM 1166(1)-(N)可以通信地耦合到可以包含在相应容器出口VCN 1168(1)-(N)中的相应应用子网1167(1)-(N),相应容器出口VCN 1168(1)-(N)可以包含在相应客户租赁1170(1)-(N)中。相应的次级VNIC 1172(1)-(N)可以促进数据平面VCN 1118中包含的(一个或多个)不可信应用子网1162与容器出口VCN 1168(1)-(N)中包含的应用子网之间的通信。每个容器出口VCN 1168(1)-(N)可以包括NAT网关1138,该NAT网关1138可以通信地耦合到公共互联网1154(例如,图9的公共互联网954)。

[0160] 包含在控制平面VCN 1116中并且包含在数据平面VCN 1118中的互联网网关1134可以通信地耦合到元数据管理服务1152(例如,图9的元数据管理系统952),该元数据管理服务1152可以通信地耦合到公共互联网1154。公共互联网1154可以通信地耦合到包含在控制平面VCN 1116中并且包含在数据平面VCN 1118中的NAT网关1138。包含在控制平面VCN1116中和包含在数据平面VCN 1118中的服务网关1136可以通信地耦合到云服务1156。

[0161] 在一些实施例中,数据平面VCN 1118可以与客户租赁1170集成。在一些情况下,诸如在执行代码时可能期望支持的情况下,这种集成对于IaaS提供商的客户可能是有用的或期望的。客户可能提供可能具有破坏性、可能与其它客户资源通信或可能以其它方式导致非期望效果的代码来运行。作为对此的响应,IaaS提供商可以确定是否运行由客户给与IaaS提供商的代码。

[0162] 在一些示例中,IaaS提供商的客户可以向IaaS提供商授予临时网络访问,并请求附加到数据平面应用层1146的功能。运行该功能的代码可以在VM 1166(1)-(N)中执行,并且该代码可以不被配置为在数据平面VCN 1118上的其它任何地方运行。每个VM 1166(1)-(N)可以连接到一个客户租赁1170。包含在VM 1166(1)-(N)中的相应容器1171(1)-(N)可以被配置为运行代码。在这种情况下,可以存在双重隔离(例如,容器1171(1)-(N)运行代码,其中容器1171(1)-(N)可能至少包含在(一个或多个)不可信应用子网1162中包含的VM1166(1)-(N)中),这可以帮助防止不正确的或以其它方式非期望的代码损坏IaaS提供商的网络或损坏不同客户的网络。容器1171(1)-(N)可以通信地耦合到客户租赁1170并且可以被配置为传输或接收来自客户租赁1170的数据。容器1171(1)-(N)可以不被配置为从数据平面VCN 1118中的任何其它实体传输或接收数据。在运行代码完成后,IaaS提供商可以终止或以其它方式处置容器1171(1)-(N)。

[0163] 在一些实施例中,(一个或多个)可信应用子网1160可以运行可以由IaaS提供商拥有或操作的代码。在这个实施例中,(一个或多个)可信应用子网1160可以通信地耦合到(一个或多个)DB子网1130并且被配置为在(一个或多个)DB子网1130中执行CRUD操作。(一个或多个)不可信应用子网1162可以通信地耦合到(一个或多个)DB子网1130,但是在这个实施例中,(一个或多个)不可信应用子网可以被配置为在(一个或多个)DB子网1130中执行读取操作。可以包含在每个客户的VM 1166(1)-(N)中并且可以运行来自客户的代码的容器1171(1)-(N)可以不与(一个或多个)DB子网1130通信地耦合。

[0164] 在其它实施例中,控制平面VCN 1116和数据平面VCN 1118可以不直接通信地耦合。在这个实施例中,控制平面VCN 1116和数据平面VCN 1118之间可能没有直接通信。但是,通信可以通过至少一种方法间接发生。LPG 1110可以由IaaS提供商建立,其可以促进控制平面VCN 1116和数据平面VCN 1118之间的通信。在另一个示例中,控制平面VCN 1116或数据平面VCN 1118可以经由服务网关1136调用云服务1156。例如,从控制平面VCN 1116对云服务1156的调用可以包括对可以与数据平面VCN 1118通信的服务的请求。

[0165] 图12是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1200。服务运营商1202(例如,图9的服务运营商902)可以通信地耦合到安全主机租赁1204(例如,图9的安全主机租赁904),该安全主机租赁1204可以包括虚拟云网络(VCN)1206(例如,图9的VCN 906)和安全主机子网1208(例如,图9的安全主机子网908)。VCN 1206可以包括LPG1210(例如,图9的LPG 910),该LPG 1210可以经由包含在SSH VCN 1212(例如,图9的SSH VCN 912)中的LPG 1210通信地耦合到SSH VCN 1212。SSH VCN 1212可以包括SSH子网1214(例如,图9的SSH子网914),并且SSH VCN 1212可以经由包含在控制平面VCN 1216中的LPG1210通信地耦合到控制平面VCN 1216(例如,图9的控制平面VCN 916)并且经由包含在数据平面VCN 1218中的LPG 1210耦合到数据平面VCN 1218(例如,图9的数据平面918)。控制平面VCN 1216和数据平面VCN 1218可以包含在服务租赁1219(例如,图9的服务租赁919)中。

[0166] 控制平面VCN 1216可以包括:可以包括(一个或多个)LB子网1222(例如,图9的(一个或多个)LB子网922)的控制平面DMZ层1220(例如,图9的控制平面DMZ层920)、可以包括(一个或多个)应用子网1226(例如,图9的(一个或多个)应用子网926)的控制平面应用层1224(例如,图9的控制平面应用层924)、可以包括(一个或多个)DB子网1230(例如,图11的(一个或多个)DB子网1130)的控制平面数据层1228(例如,图9的控制平面数据层928)。包含在控制平面DMZ层1220中的(一个或多个)LB子网1222可以通信地耦合到包含在控制平面应用层1224中的(一个或多个)应用子网1226和可以包含在控制平面VCN 1216中的互联网网关1234(例如,图9的互联网网关934),并且(一个或多个)应用子网1226可以通信地耦合到包含在控制平面数据层1228中的(一个或多个)DB子网1230以及服务网关1236(例如,图9的服务网关)和网络地址转换(NAT)网关1238(例如,图9的NAT网关938)。控制平面VCN 1216可以包括服务网关1236和NAT网关1238。

[0167] 数据平面VCN 1218可以包括数据平面应用层1246(例如,图9的数据平面应用层946)、数据平面DMZ层1248(例如,图9的数据平面DMZ层948))、以及数据平面数据层1250(例如,图9的数据平面数据层950)。数据平面DMZ层1248可以包括可以通信地耦合到数据平面应用层1246的(一个或多个)可信应用子网1260(例如,图11的(一个或多个)可信应用子网1160)和(一个或多个)不可信应用子网1262(例如,图11的(一个或多个)不可信应用子网1162)以及包含在数据平面VCN 1218中的互联网网关1234的(一个或多个)LB子网1222。(一个或多个)可信应用子网1260可以通信地耦合到包含在数据平面VCN 1218中的服务网关1236、包含在数据平面VCN 1218中的NAT网关1238以及包含在数据平面数据层1250中的(一个或多个)DB子网1230。(一个或多个)不可信应用子网1262可以通信地耦合到包含在数据平面VCN 1218中的服务网关1236和包含在数据平面数据层1250中的(一个或多个)DB子网1230。数据平面数据层1250可以包括可以通信地耦合到包含在数据平面VCN 1218中的服务

网关1236的(一个或多个)DB子网1230。

[0168] (一个或多个)不可信应用子网1262可以包括可以通信地耦合到驻留在(一个或多个)不可信应用子网1262内的租户虚拟机(VM)1266(1)-(N)的主VNIC 1264(1)-(N)。每个租户VM 1266(1)-(N)可以在相应的容器1267(1)-(N)中运行代码,并且可通信地耦合到可以包含在容器出口VCN 1268中包含的数据平面应用层1246中的应用子网1226。相应的次级VNIC 1272(1)-(N)可以促进包含在数据平面VCN 1218中的(一个或多个)不可信应用子网1262和包含在容器出口VCN 1268中的应用子网之间的通信。容器出口VCN可以包括可以通信地耦合到公共互联网1254(例如,图9的公共互联网954)的NAT网关1238。

[0169] 包含在控制平面VCN 1216中和包含在数据平面VCN 1218中的互联网网关1234可以通信地耦合到元数据管理服务1252(例如,图9的元数据管理系统952),该元数据管理服务1252可以通信地耦合到公共互联网1254。公共互联网1254可以通信地耦合到包含在控制平面VCN 1216中并且包含在数据平面VCN 1218中的NAT网关1238。包含在控制平面VCN1216中并且包含在数据平面VCN 1218中的服务网关1236可以通信地耦合到云服务1256。

[0170] 在一些示例中,图12的框图1200的体系架构所示的模式可以被认为是图11的框图1100的体系架构所示的模式的例外,并且如果IaaS提供商不能直接与客户通信(例如,断开连接的区域),那么这种模式可能是IaaS提供商的客户所期望的。客户可以实时访问每个客户的VM 1266(1)-(N)中包含的相应容器1267(1)-(N)。容器1267(1)-(N)可以被配置为对包含在数据平面应用层1246的(一个或多个)应用子网1226中的相应次级VNIC 1272(1)-(N)进行调用,该数据平面应用层1246可以包含在容器出口VCN 1268中。次级VNIC 1272(1)-(N)可以将调用传输到NAT网关1238,NAT网关1238可以将调用传输到公共互联网1254。在这个示例中,可以由客户实时访问的容器1267(1)-(N)可以与控制平面VCN 1216隔离,并且可以与数据平面VCN 1218中包含的其它实体隔离。容器1267(1)-(N)也可以与来自其它客户的资源隔离。

[0171] 在其它示例中,客户可以使用容器1267(1)-(N)来调用云服务1256。在这个示例中,客户可以运行容器1267(1)-(N)中从云服务1256请求服务的代码。容器1267(1)-(N)可以将该请求传输到次级VNIC 1272(1)-(N),次级VNIC 1272(1)-(N)可以将请求传输到NAT网关,该NAT网关可以将请求传输到公共互联网1254。公共互联网1254可以经由互联网网关1234将请求传输到包含在控制平面VCN 1216中的(一个或多个)LB子网1222。响应于确定请求有效,(一个或多个)LB子网可以将请求传输到(一个或多个)应用子网1226,该(一个或多个)应用子网1226可以经由服务网关1236将请求传输到云服务1256。

[0172] 应当认识到的是,各图中描绘的IaaS体系架构900、1000、1100、1200可以具有除所描绘的那些之外的其它组件。另外,各图中所示的实施例仅仅是可以结合本公开的实施例的云基础设施系统的一些示例。在一些其它实施例中,IaaS系统可以具有比各图中所示更多或更少的组件,可以组合两个或更多个组件,或者可以具有组件的不同配置或布置。

[0173] 在某些实施例中,本文描述的IaaS系统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。此类IaaS系统的示例是本受让人提供的Oracle云基础设施(OCI)。

[0174] 图13图示了其中可以实现各种实施例的示例计算机系统1300。系统1300可以用于实现上述任何计算机系统。如图所示,计算机系统1300包括经由总线子系统1302与多个外

围子系统通信的处理单元1304。这些外围子系统可以包括处理加速单元1306、I/O子系统1308、存储子系统1318和通信子系统1324。存储子系统1318包括有形计算机可读存储介质1322和系统存储器1310。

[0175] 总线子系统1302提供用于让计算机系统1300的各种组件和子系统按意图彼此通信的机制。虽然总线子系统1302被示意性地示出为单条总线,但是总线子系统的替代实施例可以利用多条总线。总线子系统1302可以是若干种类型的总线结构中的任何一种,包括存储器总线或存储器控制器、外围总线、以及使用任何各种总线体系架构的局部总线。例如,这种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)局部总线和外围组件互连(PCI)总线,其可以被实现为按IEEE P1386.1标准制造的Mezzanine总线。

[0176] 可以被实现为一个或多个集成电路(例如,常规微处理器或微控制器)的处理单元1304控制计算机系统1300的操作。一个或多个处理器可以被包括在处理单元1304中。这些处理器可以包括单核或多核处理器。在某些实施例中,处理单元1304可以被实现为一个或多个独立的处理单元1332和/或1334,其中在每个处理单元中包括单核或多核处理器。在其它实施例中,处理单元1304也可以被实现为通过将两个双核处理器集成到单个芯片中形成的四核处理单元。

[0177] 在各种实施例中,处理单元1304可以响应于程序代码执行各种程序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,要被执行的程序代码中的一些或全部代码可以驻留在(一个或多个)处理器1304中和/或存储子系统1318中。通过适当的编程,(一个或多个)处理器1304可以提供上述各种功能。计算机系统1300可以附加地包括处理加速单元1306,其可以包括数字信号处理器(DSP)、专用处理器,等等。

[0178] I/O子系统1308可以包括用户接口输入设备和用户接口输出设备。用户接口输入设备可以包括键盘、诸如鼠标或轨迹球的定点设备、结合到显示器中的触摸板或触摸屏、滚动轮、点击轮、拨盘、按钮、开关、键盘、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。用户接口输入设备可以包括,例如,运动感测和/或手势识别设备,诸如的Microsoft **Kinect®** 运动传感器,其使得用户能够使用手势和语音命令通过自然用户接口来控制诸如的Microsoft **Xbox®360** 游戏控制器的输入设备并与之交互。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,当拍摄照片和/或做出菜单选择时的“眨眼”)并且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。

[0179] 用户接口输入设备也可以包括但不限于三维(3D)鼠标、操纵杆或指向棒、游戏面板和绘图板,以及音频/视频设备,诸如扬声器、数码相机、数码摄像机、便携式媒体播放器、网络摄像头、图像扫描仪、指纹扫描仪、条形码阅读器3D扫描仪、3D打印机、激光测距仪和视线跟踪设备。此外,用户接口输入设备可以包括,例如,医学成像输入设备,诸如计算机断层扫描、磁共振成像、正电子发射断层摄影术、医疗超声设备。用户接口输入设备也可以包括,例如,诸如MIDI键盘、数字乐器等的音频输入设备。

[0180] 用户接口输出设备可以包括显示子系统、指示灯,或者诸如音频输出设备的非可

视显示器,等等。显示子系统可以是阴极射线管(CRT)、诸如使用液晶显示器(LCD)或等离子显示器的平板设备、投影设备、触摸屏,等等。一般而言,术语“输出设备”的使用意在包括用于从计算机系统1300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,以及调制解调器。

[0181] 计算机系统1300可以包括包含软件元件、被示为当前位于系统存储器1310中的存储子系统1318。系统存储器1310可以存储可加载并且可在处理单元1304上执行的程序指令,以及在这些程序的执行期间所产生的数据。

[0182] 取决于计算机系统1300的配置和类型,系统存储器1310可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存存储器,等等)。RAM通常包含可被处理单元1304立即访问和/或目前正被处理单元1304操作和执行的数据和/或程序模块。在一些实施方式中,系统存储器1310可以包括多种不同类型的存储器,例如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。在一些实施方式中,诸如包含有助于在启动期间在计算机系统1300的元件之间传送信息的基本例程的基本输入/输出系统(BIOS),通常可以被存储在ROM中。举例来说,但不是限制,系统存储器1310也示出了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)等的应用程序1312,程序数据1314,以及操作系统1316。举例来说,操作系统1316可以包括各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种可商业获得的**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®** OS和**Palm®** OS操作系统的移动操作系统。

[0183] 存储子系统1318也可以提供用于存储提供一些实施例的功能的基本编程和数据结构的有形计算机可读存储介质。当被处理器执行时提供上述功能的软件(程序、代码模块、指令)可以被存储在存储子系统1318中。这些软件模块或指令可以被处理单元1304执行。存储子系统1318也可以提供用于存储根据本公开被使用的数据的储存库。

[0184] 存储子系统1300也可以包括可被进一步连接到计算机可读存储介质1322的计算机可读存储介质读取器1320。与系统存储器1310一起并且,可选地,与其相结合,计算机可读存储介质1322可以全面地表示用于临时和/或更持久地包含、存储、发送和检索计算机可读信息的远程、本地、固定和/或可移除存储设备加存储介质。

[0185] 包含代码或代码的部分的计算机可读存储介质1322也可以包括本领域已知或使用的任何适当的介质,包括存储介质和通信介质,诸如但不限于,以用于信息的存储和/或传输的任何方法或技术实现的易失性和非易失性、可移除和不可移除介质。这可以包括有形的计算机可读存储介质,诸如RAM、ROM、电可擦除可编程ROM(EEPROM)、闪存存储器或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光学储存器、磁带盒、磁带、磁盘储存器或其它磁存储设备,或者其它有形的计算机可读介质。这也可以包括非有形的计算机可读介质,诸如数据信号、数据传输,或者可以被用来发送期望信息并且可以被计算系统1300访问的任何其它介质。

[0186] 举例来说,计算机可读存储介质1322可以包括从不可移除的非易失性磁介质读取或写到其的硬盘驱动器、从可移除的非易失性磁盘读取或写到其的磁盘驱动器、以及从可移除的非易失性光盘(诸如CD ROM、DVD和Blu-Ray®盘或其它光学介质)读取或写到其的光盘驱动器。计算机可读存储介质1322可以包括,但不限于,Zip®驱动器、闪存卡、通用串行总线(USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字音频带,等等。计算机可读存储介质1322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,诸如固态RAM、动态RAM、静态RAM、基于DRAM的SSD、磁阻RAM(MRAM)SSD,以及使用基于DRAM和闪存存储器的SSD的组合的混合SSD。盘驱动器及其关联的计算机可读介质可以为计算机系统1300提供计算机可读指令、数据结构、程序模块及其它数据的非易失性存储。

[0187] 通信子系统1324提供到其它计算机系统和网络的接口。通信子系统1324用作用于从其它系统接收数据和从计算机系统1300向其它系统发送数据的接口。例如,通信子系统1324可以使计算机系统1300能够经由互联网连接到一个或多个设备。在一些实施例中,通信子系统1324可以包括用于访问无线语音和/或数据网络的射频(RF)收发器组件(例如,使用蜂窝电话技术,诸如3G、4G或EDGE(用于全球演进的增强型数据速率)的先进数据网络技术,WiFi(IEEE 802.11系列标准),或其它移动通信技术,或其任意组合)、全球定位系统(GPS)接收器组件和/或其它组件。在一些实施例中,作为无线接口的附加或者替代,通信子系统1324可以提供有线网络连接(例如,以太网)。

[0188] 在一些实施例中,通信子系统1324也可以代表可以使用计算机系统1300的一个或多个用户接收结构化和/或非结构化数据馈送1326、事件流1328、事件更新1330等形式的输入通信。

[0189] 举例来说,通信子系统1324可以被配置为实时地从社交网络和/或其它通信服务的用户接收数据馈送1326,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。

[0190] 此外,通信子系统1324也可被配置为接收连续数据流形式的数据,这可以包括本质上可以是连续的或无界的没有明确终止的实时事件的事件流1328和/或事件更新1330。产生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,等等。

[0191] 通信子系统1324也可被配置为向一个或多个数据库输出结构化和/或非结构化数据馈送1326、事件流1328、事件更新1330,等等,这一个或多个数据库可以与耦合到计算机系统1300的一个或多个流式数据源计算机通信。

[0192] 计算机系统1300可以是各种类型之一,包括手持便携式设备(例如,iPhone®蜂窝电话、iPad®计算平板电脑、PDA)、可穿戴设备(例如,GoogleGlass®头戴式显示器)、PC、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。

[0193] 由于计算机和网络的不断变化的本质,在图中绘出的计算机系统1300的描述仅仅要作为具体的示例。具有比图中绘出的系统更多或更少组件的许多其它配置是可能的。例如,定制的硬件也可以被使用和/或特定的元素可以用硬件、固件、软件(包括applets)或其组合来实现。另外,也可以采用到诸如网络输入/输出设备之类的其它计算设备的连接。基

于本文提供的公开内容和示教,本领域普通技术人员将认识到实现各种实施例的其它方式和/或方法。

[0194] 虽然已经描述了具体实施例,但是各种修改、变更、替代构造和等效形式也包含在本公开的范围内。实施例不限于在某些特定数据处理环境内操作,而是可以在多个数据处理环境内自由操作。此外,虽然已经使用特定系列的事务和步骤描述了实施例,但是本领域技术人员应该清楚本公开的范围不限于所描述系列的事务和步骤。上述实施例的各种特征和方面可以单独或联合使用。

[0195] 另外,虽然已经使用硬件和软件的特定组合描述了实施例,但是应当认识到硬件和软件的其它组合也在本公开的范围内。实施例可以仅用硬件、或仅用软件、或使用其组合来实现。实施例可以通过使用计算机程序产品来实现,该计算机程序产品包括计算机程序/指令,当计算机程序/指令由处理器执行时,使处理器执行本公开中描述的任何方法。本文描述的各种处理可以以任何组合在相同的处理器或在不同的处理器上实现。相应地,在组件或模块被描述为被配置为执行某些操作的情况下,可以通过例如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,或其任何组合来完成这样的配置。处理可以使用多种技术进行通信,包括但不限于用于处理间通信的常规技术,并且不同的处理对可以使用不同的技术,或者同一对处理可以在不同时间使用不同的技术。

[0196] 相应地,说明书和附图被认为是说明性的而不是限制性的。但是,显然可以对其进行添加、减少、删除和其它修改和改变而不背离权利要求中阐述的更广泛的精神和范围。因此,虽然已经描述了具体的公开实施例,但这些并不旨在进行限制。各种修改和等效形式都在以下权利要求的范围内。

[0197] 在描述所公开的实施例的上下文中(尤其在以下权利要求的上下文中)使用术语“一”和“一个”和“该”以及类似的指称要被解释为涵盖单数和复数,除非本文另有指示或与上下文明显矛盾。除非另有说明,否则术语“包括”、“具有”、“包含(including)”和“包含(containing)”要被解释为开放式术语(即,意思是“包括但不限于”)。术语“连接”应被解释为部分或全部包含在、附加到或连接在一起,即使中间存在一些东西。除非本文另有指示,否则本文中值范围的列举仅旨在用作个别引用落入该范围内的每个单独值的速记方法,并且每个单独值被并入说明书中,就好像它在本文中个别列举一样。除非本文另有指示或与上下文明显矛盾,否则本文所述的所有方法都可以以任何合适的顺序执行。本文提供的任何和所有示例或示例性语言(例如,“诸如”)的使用仅旨在更好地阐明实施例并且不对本公开的范围构成限制,除非另有声明。说明书中的任何语言都不应被解释为指示任何未要求保护的元素对于本公开的实践是必不可少的。

[0198] 析取语言,诸如短语“X、Y或Z中的至少一个”,除非另有明确说明,否则旨在在一般用于表示项目、术语等的上下文中理解,可以是X、Y或Z,或它们的任何组合(例如,X、Y和/或Z)。因此,这种析取语言通常不旨在也不应暗示某些实施例需要X中的至少一个、Y中的至少一个或Z中的至少一个各自存在。

[0199] 本文描述了本公开的优选实施例,包括已知用于实施本公开的最佳模式。那些优选实施例的变型对于本领域普通技术人员在阅读上述描述后会变得显而易见。普通技术人员应该能够适当地采用这样的变型并且可以以不同于本文具体描述的方式来实践本公开。相应地,本公开包括在适用法律允许的情况下对所附权利要求中记载的主题的所有修改和

等效形式。此外,除非在本文中另有指示,否则本公开包括在其所有可能的变化中的上述元素的任何组合。

[0200] 本文引用的所有参考文献,包括出版物、专利申请和专利,均以相同的程度通过引用并入本文,就好像每个参考文献个别且具体地指示通过引用并入并在本文中全文阐述一样。

[0201] 在前述的说明书中,本公开的各方面参考其具体实施例进行了描述,但本领域技术人员将认识到的是,本公开不限于此。上述公开的各个特征和方面可以被单独或联合使用。此外,在不脱离本说明书的更广泛精神和范围的情况下,实施例可以在除本文所述的那些之外的任何数量的环境和应用中被使用。相应地,本说明书和附图应当被认为是说明性而不是限制性的。

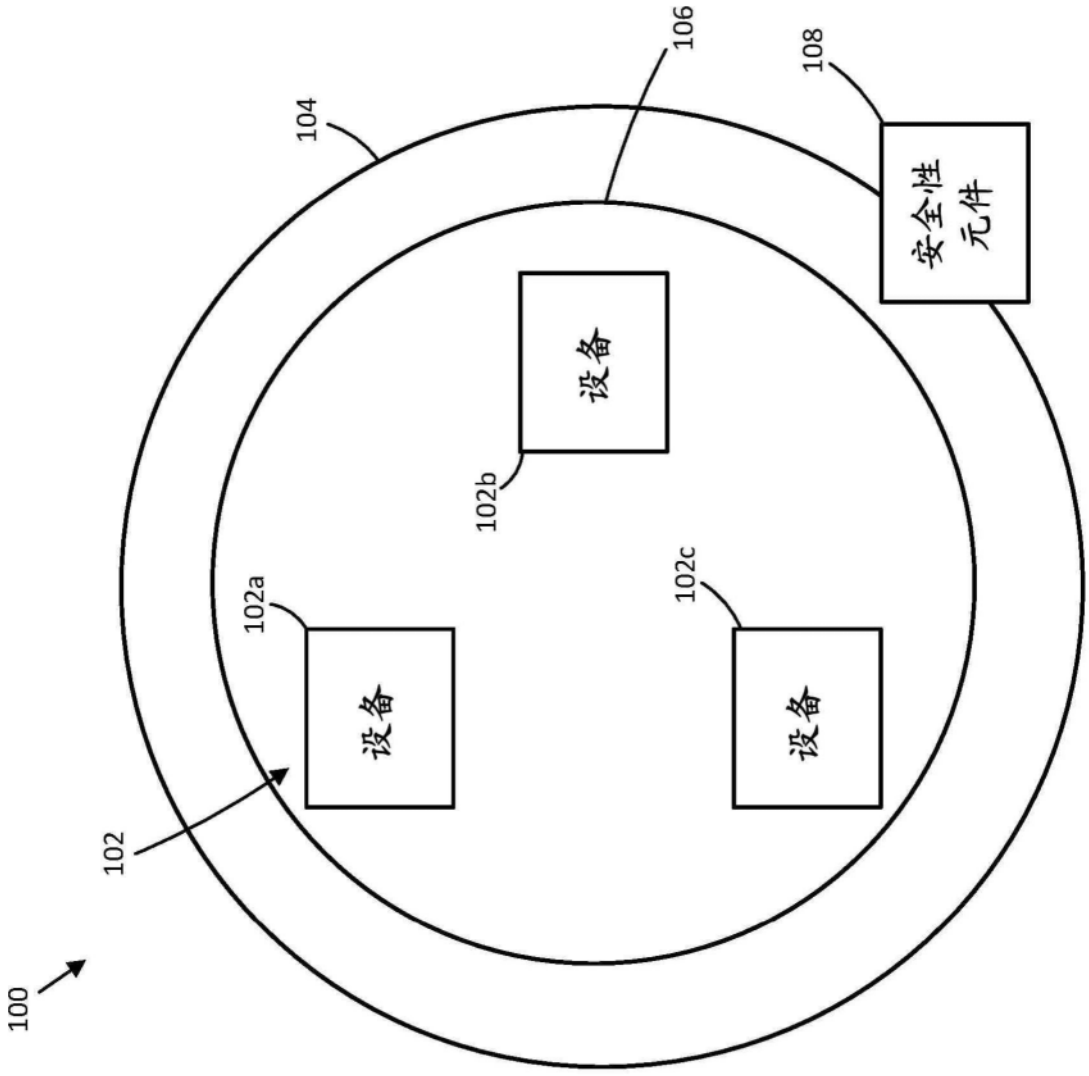


图1

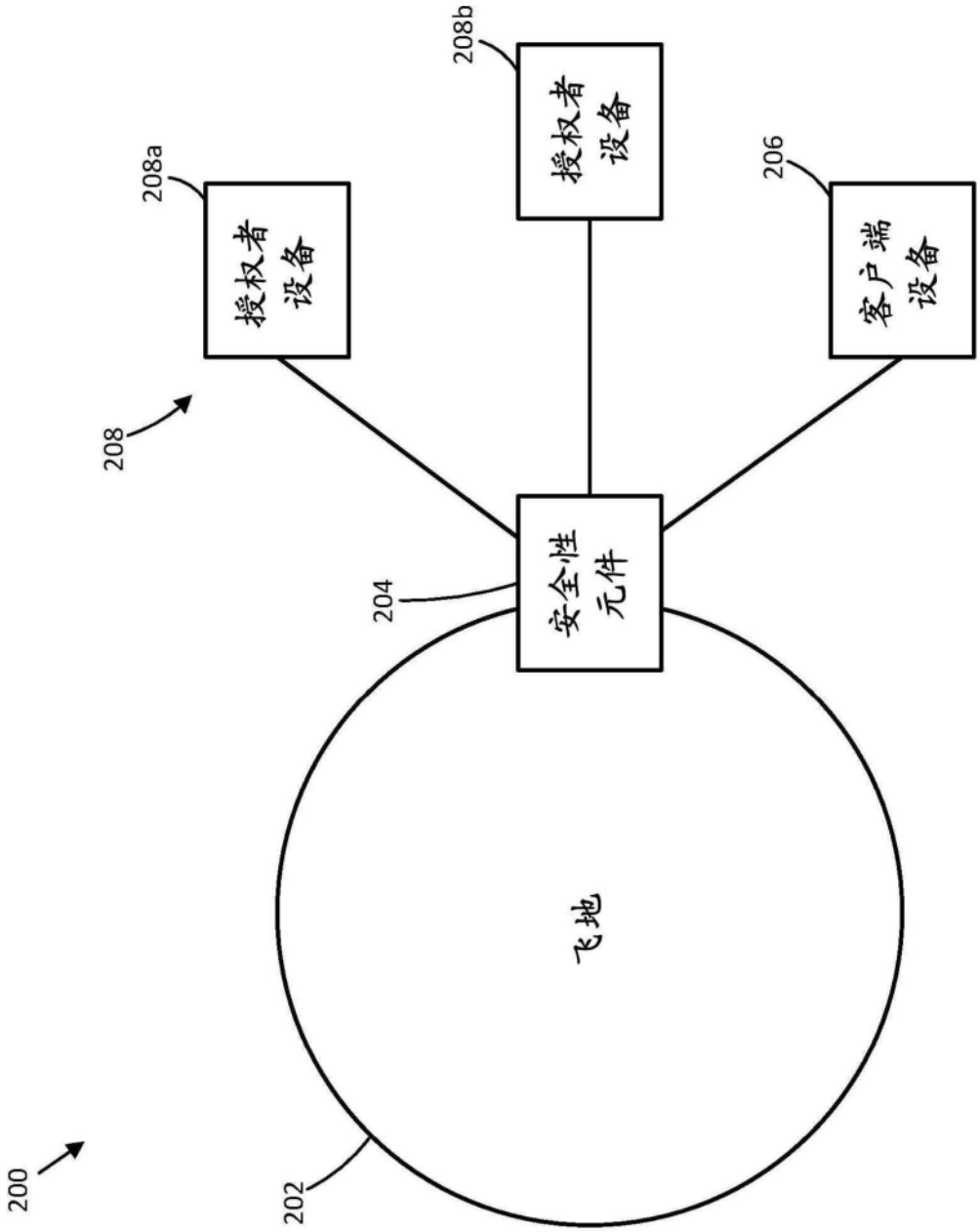


图2

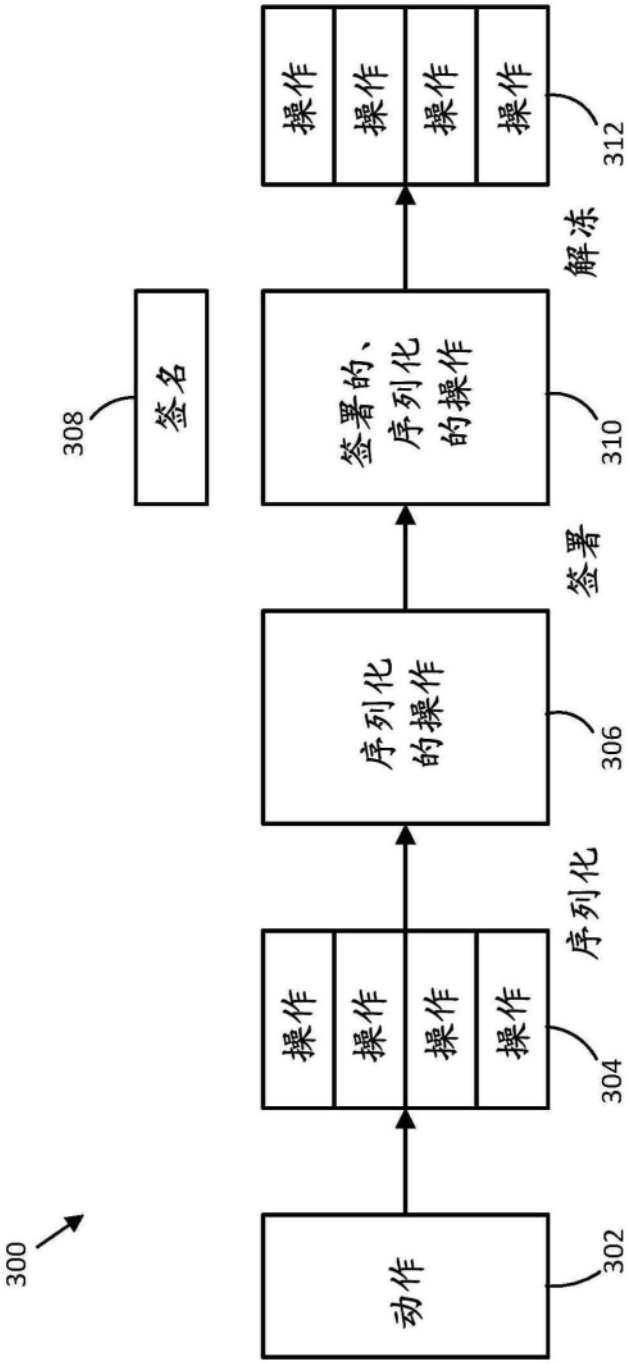

300
动作
302
操作
操作
操作
操作
304
序列化
序列化的操作
306
签署
签署的、序列化的操作
310
308
签名
解冻
操作
操作
操作
操作
312

图3

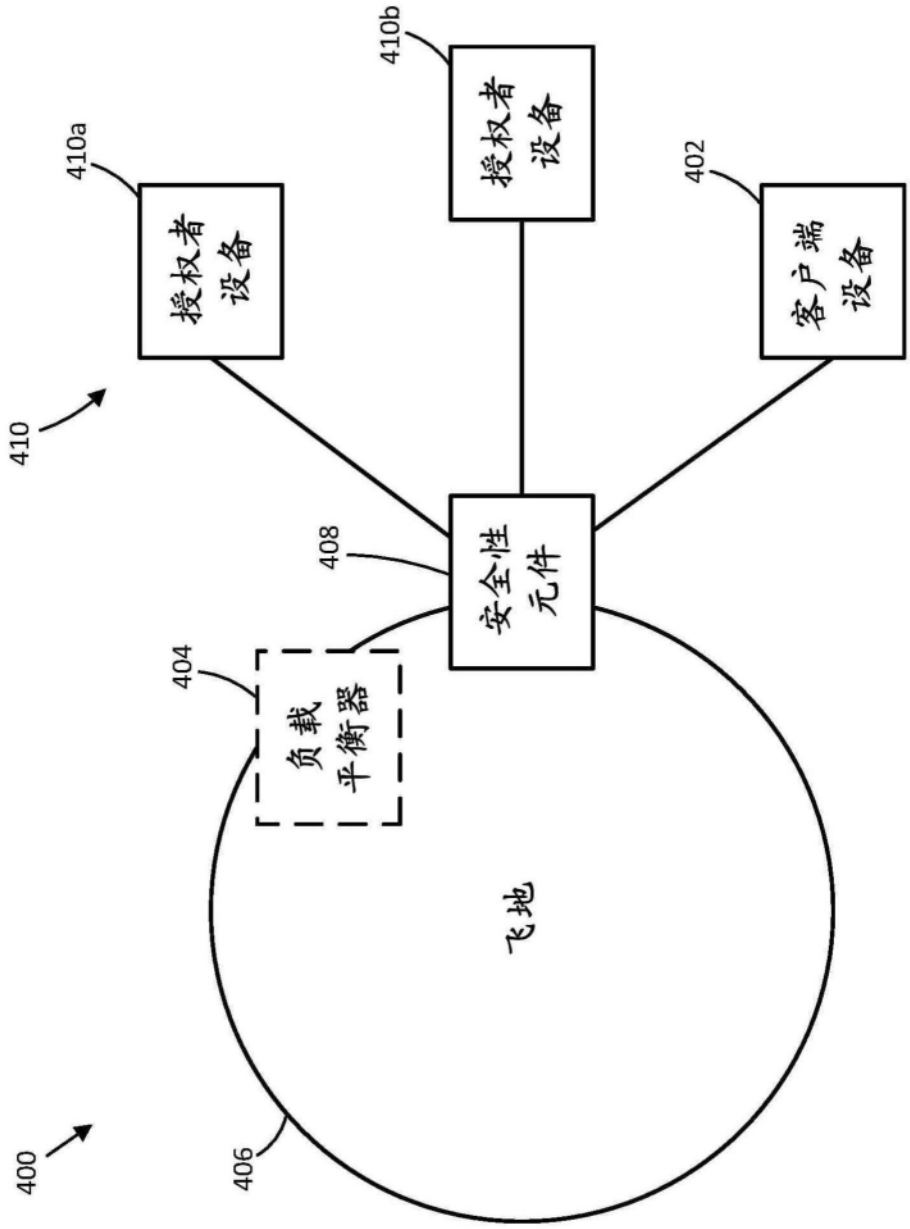

410b
授权者设备
410a
授权者设备
402
客户端设备
410
408
安全性元件
404
负载平衡器
飞地
406
400

图4

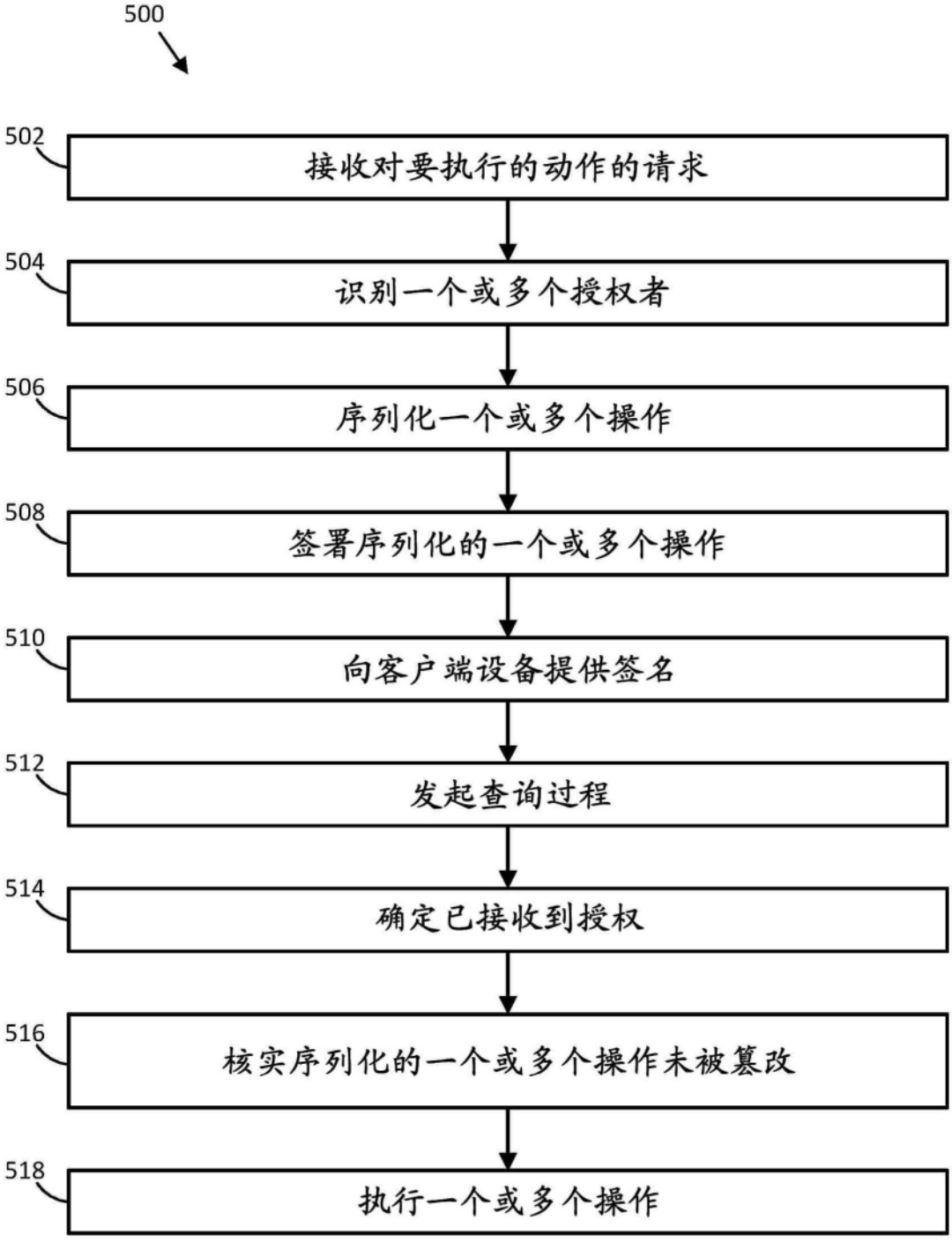

500
502
接收对要执行的动作的请求
504
识别一个或多个授权者
506
序列化一个或多个操作
508
签署序列化的一个或多个操作
510
向客户端设备提供签名
512
发起查询过程
514
确定已接收到授权
516
核实序列化的一个或多个操作未被篡改
518
执行一个或多个操作

图5

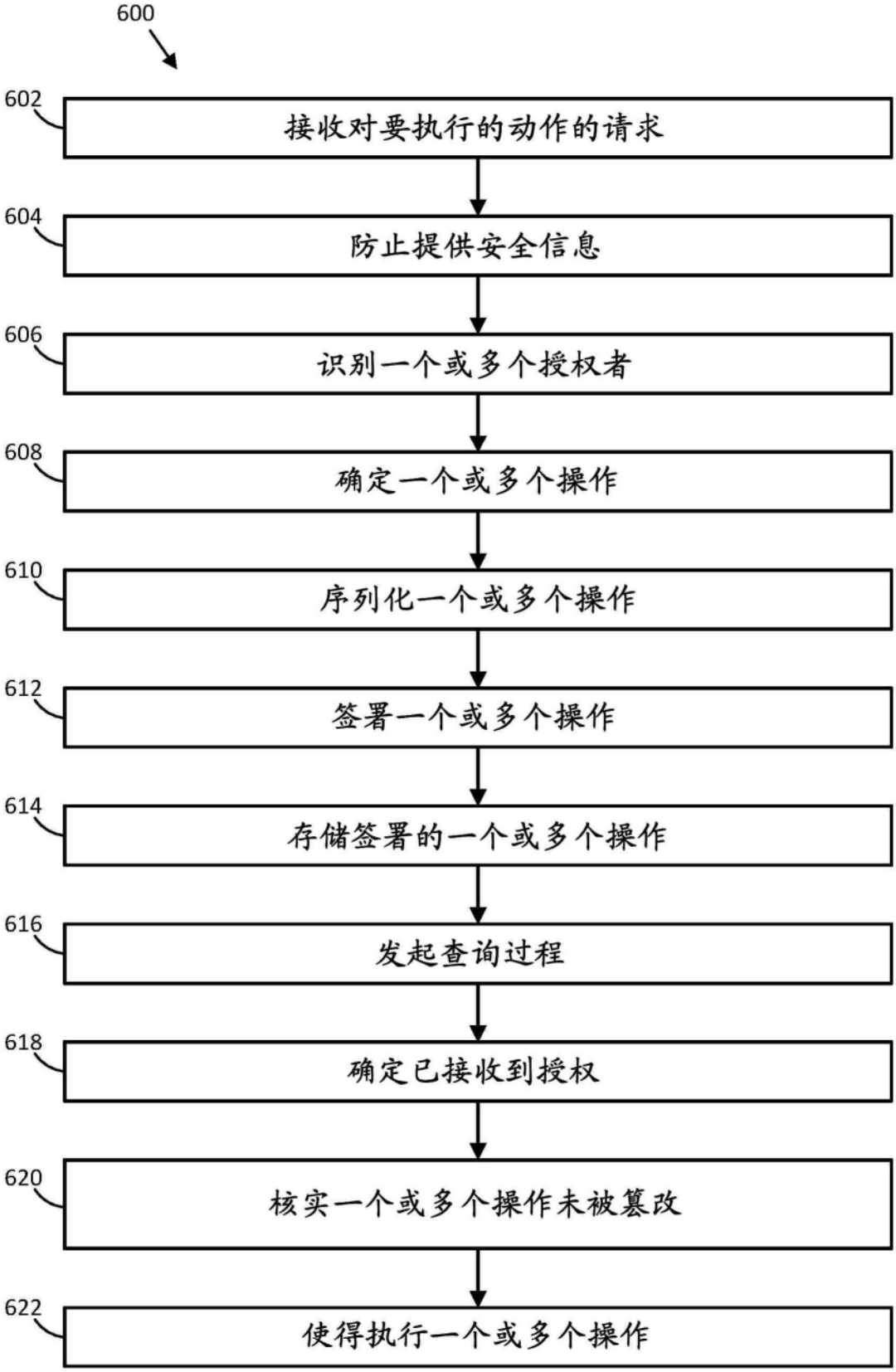

600
602
接收对要执行的动作的请求
604
防止提供安全信息
606
识别一个或多个授权者
608
确定一个或多个操作
610
序列化一个或多个操作
612
签署一个或多个操作
614
存储签署的一个或多个操作
616
发起查询过程
618
确定已接收到授权
620
核实一个或多个操作未被篡改
622
使得执行一个或多个操作

图6

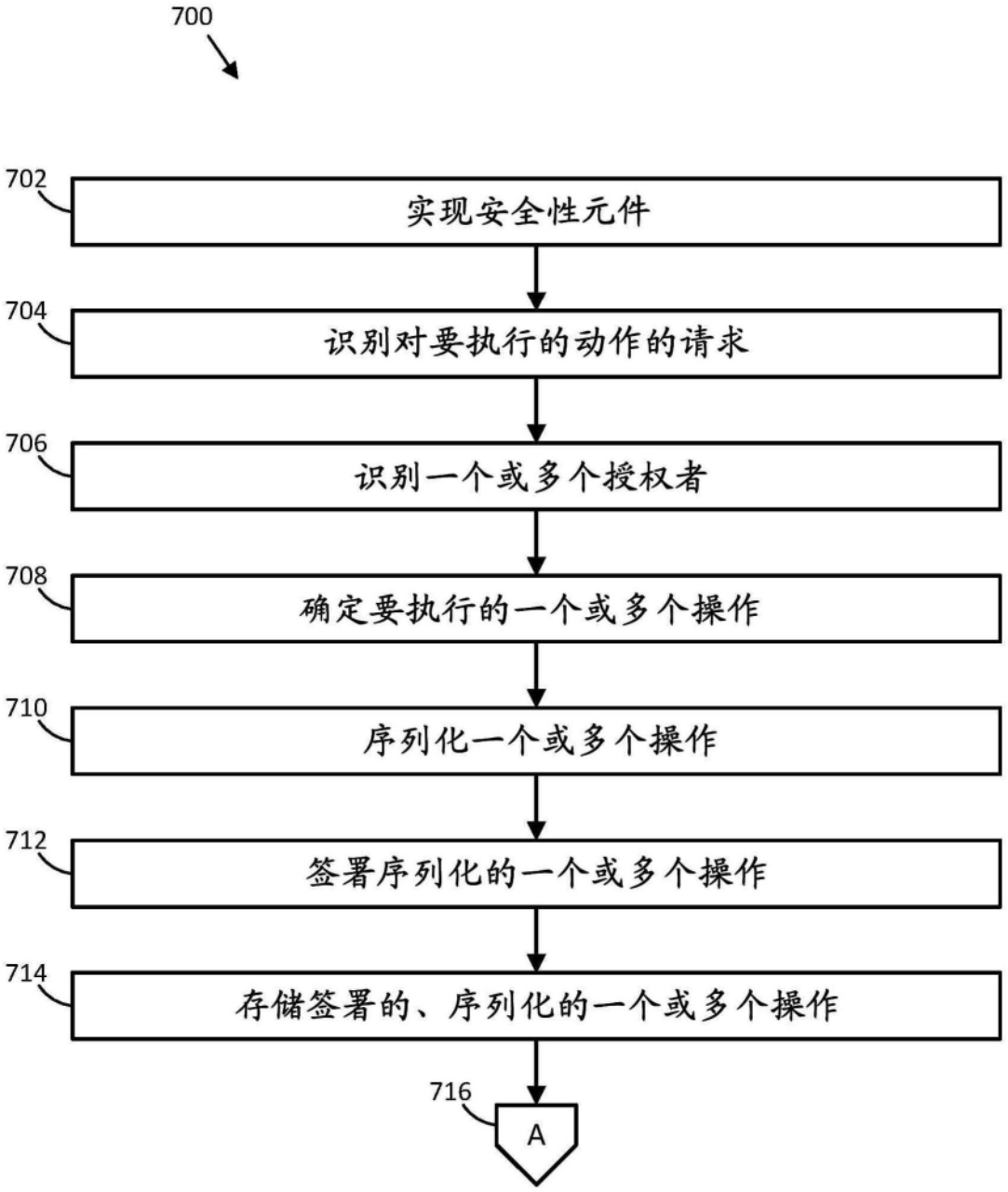

700
702
实现安全性元件
704
识别对要执行的动作的请求
706
识别一个或多个授权者
708
确定要执行的一个或多个操作
710
序列化一个或多个操作
712
签署序列化的一个或多个操作
714
存储签署的、序列化的一个或多个操作
716
A

图7

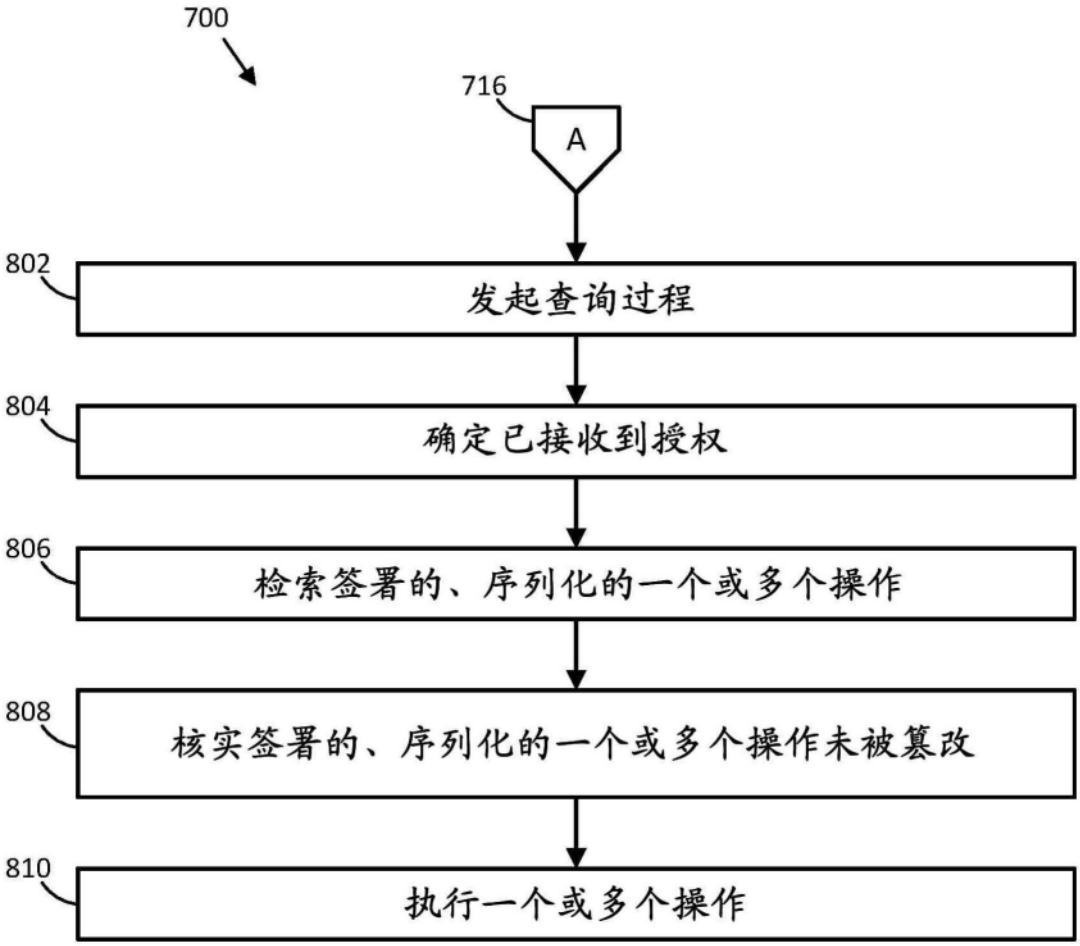

700
716
A
802
发起查询过程
804
确定已接收到授权
806
检索签署的、序列化的一个或多个操作
808
核实签署的、序列化的一个或多个操作未被篡改
810
执行一个或多个操作

图8

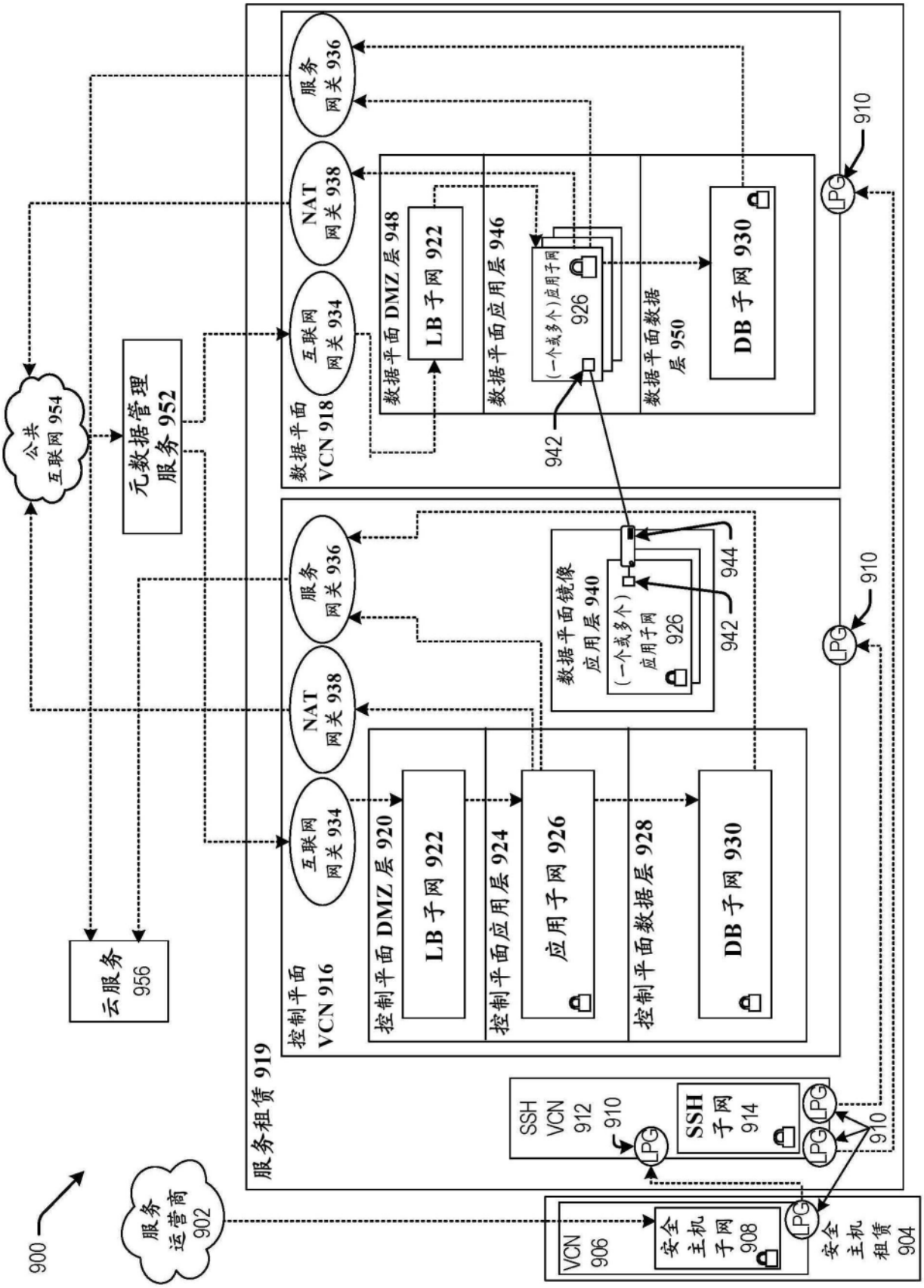

900
服务运营商 902
服务租赁 919
VCN 906
安全主机子网 908
安全主机租赁 904
SSH VCN 912
SSH 子网 914
910
LPG
控制平面 VCN 916
互联网网关 934
NAT 网关 936
服务网关 936
控制平面 DMZ 层 920
LB 子网 922
控制平面应用层 924
应用子网 926
控制平面数据层 928
DB 子网 930
数据平面镜像应用层 940
(一个或多个)应用子网 926
942
944
数据平面 VCN 918
数据平面 DMZ 层 948
数据平面应用层 946
(一个或多个)应用子网 926
数据平面数据层 950
云服务 956
元数据管理服务 952
公共互联网 954

图9

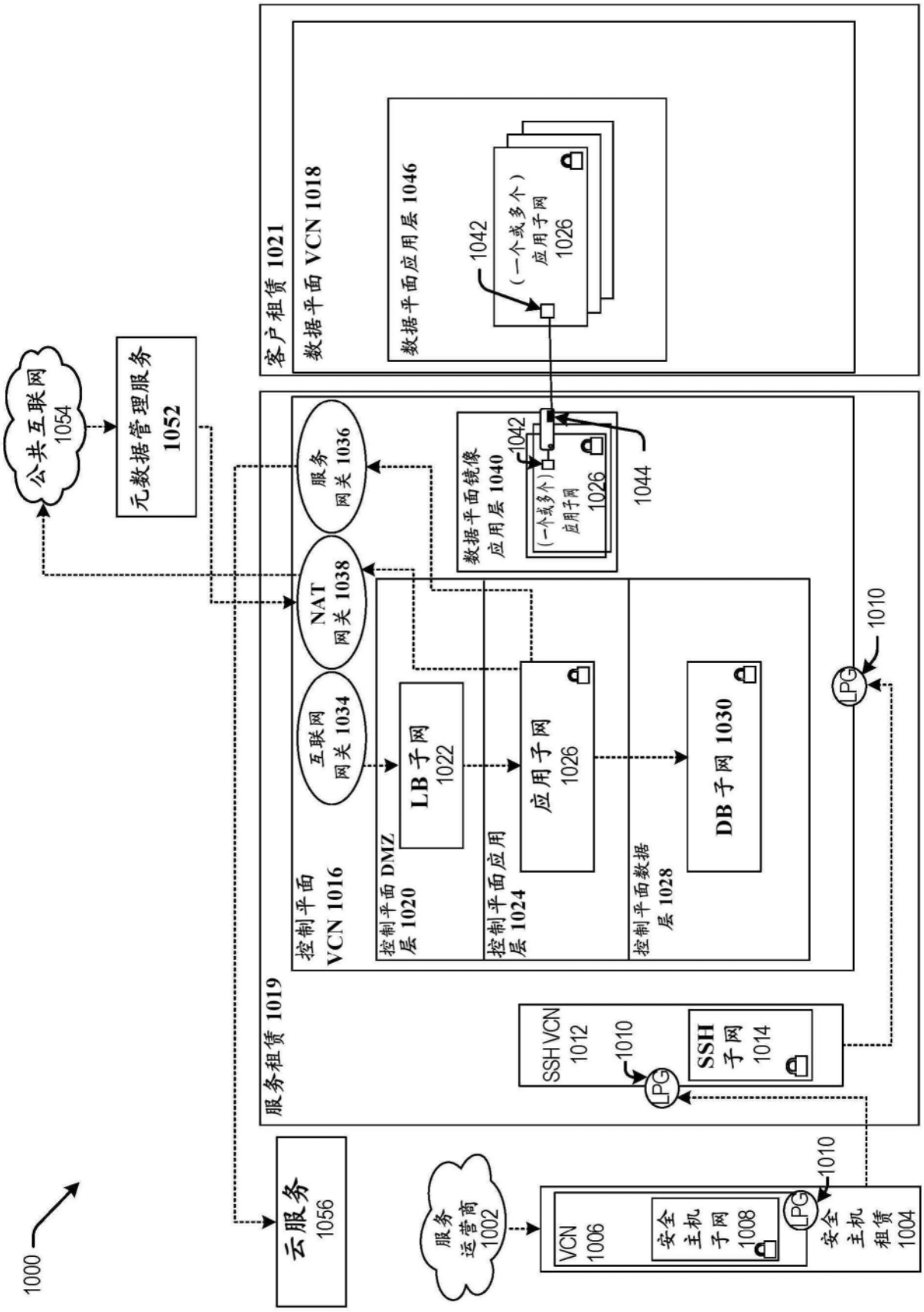

1000
公共互联网 1054
元数据管理服务 1052
云服务 1056
服务运营商 1002
客户租赁 1021
数据平面 VCN 1018
数据平面应用层 1046
1042
（一个或多个）应用子网 1026
数据平面镜像应用层 1040
1044
服务网关 1036
NAT 网关 1038
互联网网关 1034
服务租赁 1019
控制平面 VCN 1016
控制平面 DMZ 层 1020
LB 子网 1022
控制平面应用层 1024
应用子网 1026
控制平面数据层 1028
DB 子网 1030
LPG
1010
SSH VCN 1012
SSH 子网 1014
VCN 1006
安全主机子网 1008
安全主机租赁 1004

图10

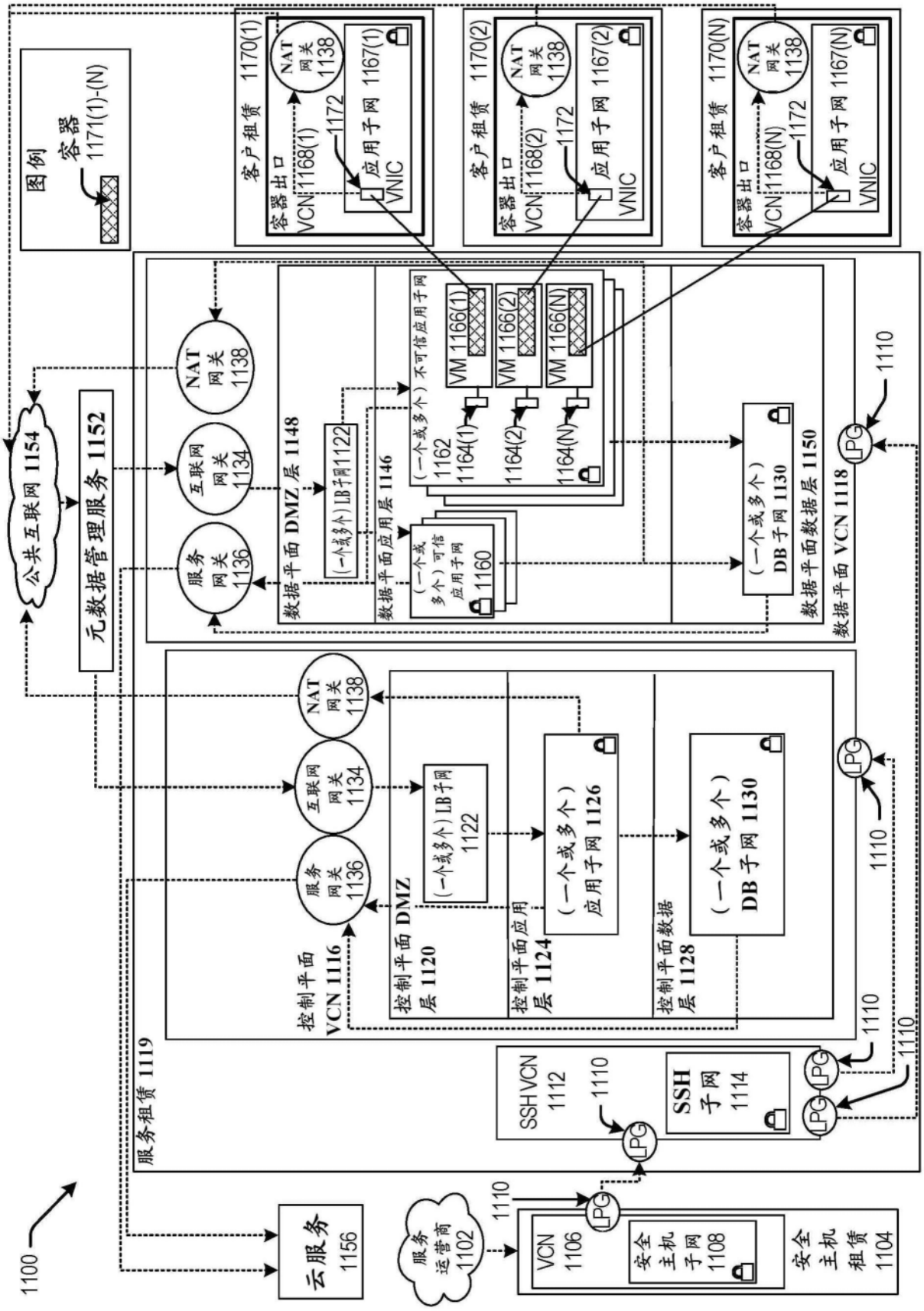

图例
容器
1171(1)-(N)
客户租赁 1170(1)
容器出口
VCN 1168(1)
NAT 网关 1138
1172
应用子网 1167(1)
VNIC
客户租赁 1170(2)
容器出口
VCN 1168(2)
NAT 网关 1138
1172
应用子网 1167(2)
VNIC
客户租赁 1170(N)
容器出口
VCN 1168(N)
NAT 网关 1138
1172
应用子网 1167(N)
VNIC
公共互联网 1154
元数据管理服务 1152
NAT 网关 1138
互联网网关 1134
服务网关 1136
数据平面 DMZ 层 1148
(一个或多个) LB子网1122
数据平面应用层 1146
(一个或多个) 可信应用子网 1160
(一个或多个) 不可信应用子网 1162
VM 1166(1)
VM 1166(2)
VM 1166(N)
1164(1)
1164(2)
1164(N)
数据平面数据层 1150
(一个或多个) DB 子网 1130
数据平面 VCN 1118
1110
服务租赁 1119
控制平面 VCN 1116
控制平面 DMZ 层 1120
(一个或多个) LB子网 1122
控制平面应用层 1124
(一个或多个) 应用子网 1126
控制平面数据层 1128
(一个或多个) DB 子网 1130
SSH VCN 1112
SSH 子网 1114
LPG
云服务 1156
服务运营商 1102
VCN 1106
安全主机子网 1108
安全主机租赁 1104
1100

图11

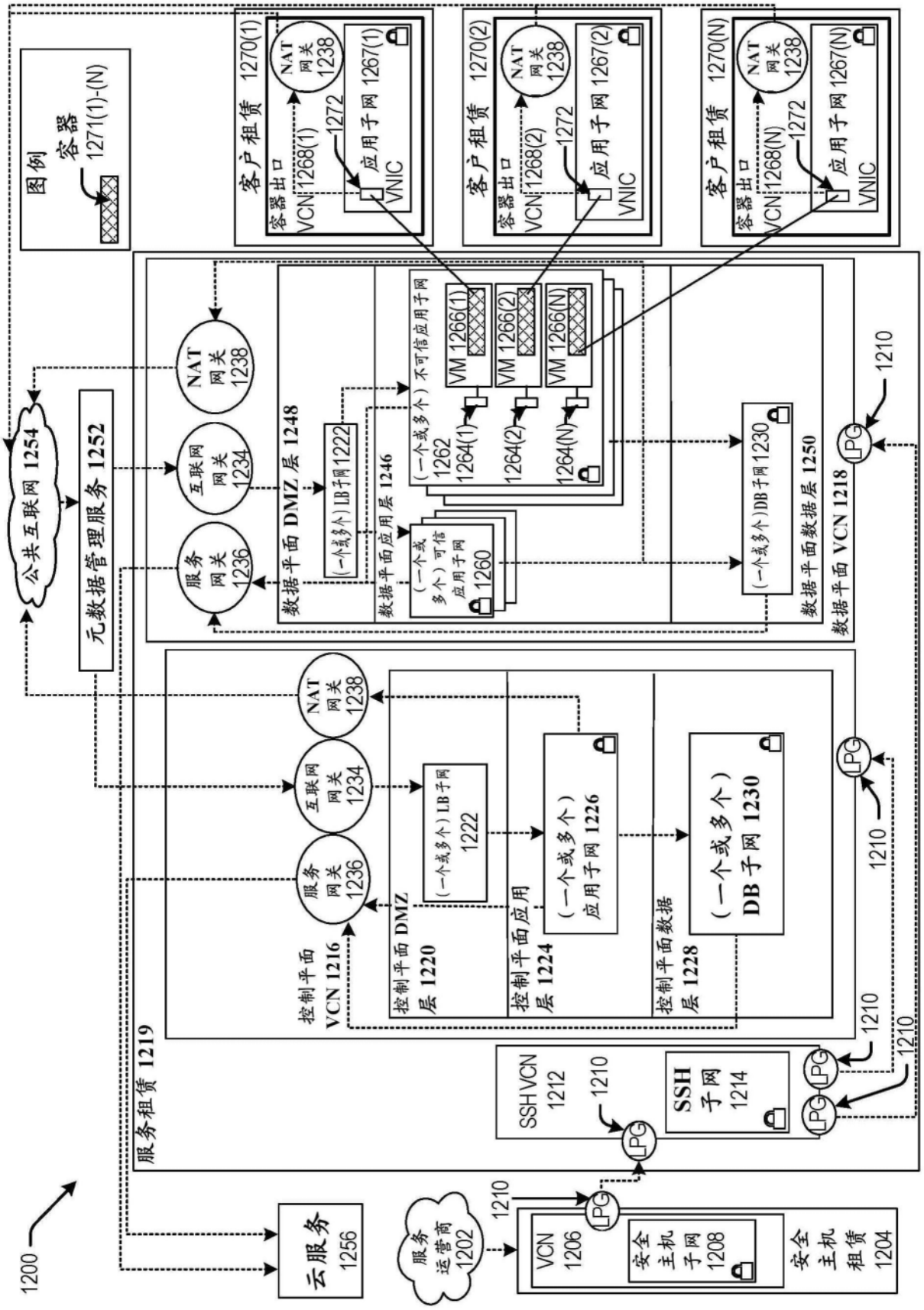

图例
容器
1271(1)-(N)
客户租赁 1270(1)
容器出口
VCN 1268(1)
NAT 网关 1238
1272
应用子网 1267(1)
VNIC
客户租赁 1270(2)
容器出口
VCN 1268(2)
NAT 网关 1238
1272
应用子网 1267(2)
VNIC
客户租赁 1270(N)
容器出口
VCN 1268(N)
NAT 网关 1238
1272
应用子网 1267(N)
VNIC
公共互联网 1254
元数据管理服务 1252
NAT 网关 1238
互联网网关 1234
服务网关 1236
数据平面 DMZ 层 1248
(一个或多个) LB子网 1222
数据平面应用层 1246
(一个或多个) 可信应用子网 1260
(一个或多个) 不可信应用子网 1262
VM 1266(1)
VM 1266(2)
VM 1266(N)
1264(1)
1264(2)
1264(N)
(一个或多个) DB子网 1230
数据平面数据层 1250
数据平面 VCN 1218
1210
服务租赁 1219
控制平面 VCN 1216
控制平面 DMZ 层 1220
(一个或多个) LB子网 1222
控制平面应用层 1224
(一个或多个) 应用子网 1226
控制平面数据层 1228
(一个或多个) DB 子网 1230
SSH VCN 1212
SSH 子网 1214
LPG
云服务 1256
服务运营商 1202
VCN 1206
安全主机子网 1208
安全主机租赁 1204
1200

图12

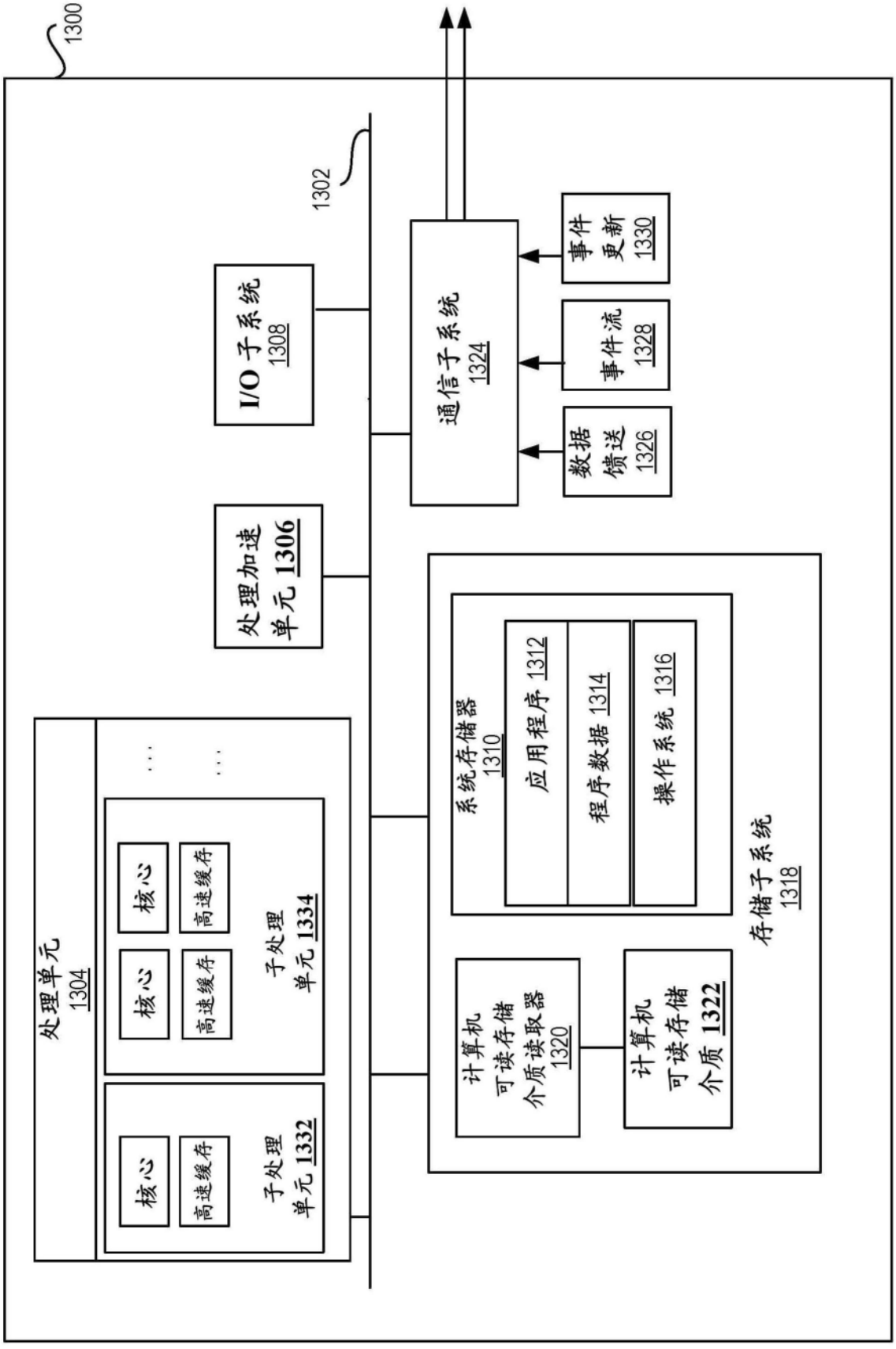

1300
1302
I/O 子系统
1308
处理加速
单元 1306
通信子系统
1324
事件
更新
1330
事件流
1328
数据
馈送
1326
处理单元
1304
核心
高速缓存
子处理
单元 1332
核心
高速缓存
核心
高速缓存
子处理
单元 1334
系统存储器
1310
应用程序 1312
程序数据 1314
操作系统 1316
存储子系统
1318
计算机
可读存储
介质读取器
1320
计算机
可读存储
介质 1322

图13