



(12) 发明专利

(10) 授权公告号 CN 118414806 B

(45) 授权公告日 2025. 04. 25

(21) 申请号 202280083482.4

(22) 申请日 2022.10.05

(65) 同一申请的已公布的文献号
申请公布号 CN 118414806 A

(43) 申请公布日 2024.07.30

(30) 优先权数据
17/523,789 2021.11.10 US

(85) PCT国际申请进入国家阶段日
2024.06.17

(86) PCT国际申请的申请数据
PCT/US2022/077605 2022.10.05

(87) PCT国际申请的公布数据
W02023/086712 EN 2023.05.19

(73) 专利权人 甲骨文国际公司
地址 美国

(72) 发明人 B·S·佩恩

(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 冯薇

(51) Int.Cl.
H04L 9/40 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
G06F 9/4401 (2006.01)
G06F 21/57 (2006.01)
G06F 21/64 (2006.01)

(56) 对比文件
CN 108781227 A, 2018.11.09
US 2004039946 A1, 2004.02.26

审查员 孙志玲

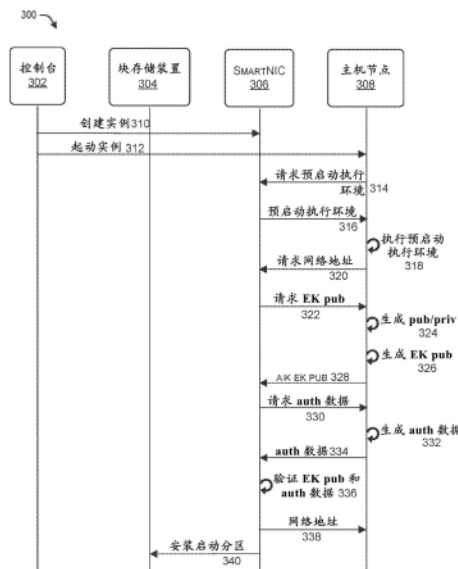
权利要求书5页 说明书20页 附图10页

(54) 发明名称

用于云基础设施系统中计算节点授权的边缘证明的方法、系统和非暂态计算机可读介质

(57) 摘要

本实施例涉及主机节点访问云基础设施环境的边缘证明。可以从控制台获得认证数据集合,用于对主机节点进行授权。该认证数据集合可以包括第一背书密钥和识别主机节点的特性的认证策略。主机节点可以发送对用以连接到云基础设施环境的网络地址的请求。主机节点可以生成第二背书密钥和认证数据,该第二背书密钥和认证数据可以被核实为与从控制台接收到的认证数据集合对应。响应于对第二背书密钥和接收到的主机节点认证数据的验证,可以将网络地址提供给主机节点,该主机节点可以用于使用该网络地址连接到云基础设施环境。



1. 一种在云基础设施环境的边缘节点处执行边缘证明的方法,所述方法包括:
在云基础设施环境的边缘节点处从与所述云基础设施环境相关联的控制台接收第一请求,
其中第一请求包括创建用于主机节点的主机实例的第一指令,
其中第一请求包括用于边缘证明处理的认证数据集合,
其中所述认证数据集合包括第一背书密钥和第一状态数据集合,
其中第一状态数据集合指示所述主机节点的参考状态;
在所述边缘节点处从所述主机节点接收第二请求,
其中第二请求包括将所述主机节点连接到所述云基础设施环境的第二指令;
至少部分地经由所述边缘节点执行所述边缘证明处理,其中所述边缘证明处理包括:
在所述边缘节点处从所述主机节点接收第二背书密钥;
至少通过将第二背书密钥与第一背书密钥进行比较来验证第二背书密钥;
在所述边缘节点处接收第二状态数据集合,其中第二状态数据集合指示所述主机节点的状态;
至少通过将第二状态数据集合与第一状态数据集合进行比较来验证第二状态数据集合;以及
响应于验证第二背书密钥和第二状态数据集合,
从所述边缘节点向所述主机节点发送与所述云基础设施环境的资源对应的网络地址,
其中所述主机节点使用所述网络地址访问所述资源。
2. 如权利要求1所述的方法,其中第一背书密钥包括第一公共证明身份密钥的第一公共密钥组件;或者其中第二背书密钥包括第二公共证明身份密钥的第二公共密钥组件。
3. 如权利要求1所述的方法,其中所述边缘节点是智能网络接口控制器的组件。
4. 如权利要求1所述的方法,其中至少通过将第二背书密钥与第一背书密钥进行比较来验证第二背书密钥包括:
确定第二背书密钥的至少一个值与第一背书密钥的对应值匹配。
5. 如权利要求1所述的方法,其中所述方法还包括:
在从所述主机节点接收第二请求之前:
从所述主机节点接收对预启动执行环境客户端的预启动请求;以及
将所述预启动执行环境客户端发送到所述主机节点,
其中,所述主机节点使用所述预启动执行环境客户端来执行启动过程。
6. 如权利要求1所述的方法,其中所述方法还包括:
将启动分区安装到存储模块,
其中所述启动分区特定于所述主机节点,并且其中所述网络地址对应于所述启动分区。
7. 如权利要求1所述的方法,其中第二请求包括对所述网络地址的请求,其中第二请求是响应于所述主机节点连接到数据中心环境而从所述主机节点发送的,所述数据中心环境包括实现所述云基础设施环境的一个或多个计算设备。
8. 一种用于在云基础设施环境的边缘节点处执行边缘证明的系统,所述系统包括:
至少一个硬件处理器;

所述系统被配置为使用所述至少一个硬件处理器来执行操作,所述操作包括:

在云基础设施环境的边缘节点处从与所述云基础设施环境相关联的控制台接收第一请求,

其中第一请求包括创建用于主机节点的主机实例的第一指令,

其中第一请求包括用于边缘证明处理的认证数据集合,

其中所述认证数据集合包括第一背书密钥和第一状态数据集合,

其中第一状态数据集合指示所述主机节点的参考状态;

在所述边缘节点处从所述主机节点接收第二请求,

其中第二请求包括将所述主机节点连接到所述云基础设施环境的第二指令;

至少部分地经由所述边缘节点执行所述边缘证明处理,其中所述边缘证明处理包括:

在所述边缘节点处从所述主机节点接收第二背书密钥;

至少通过将第二背书密钥与第一背书密钥进行比较来验证第二背书密钥;

在所述边缘节点处接收第二状态数据集合,其中第二状态数据集合指示所述主机节点的状态;

至少通过将第二状态数据集合与第一状态数据集合进行比较来验证第二状态数据集合;以及

响应于验证第二背书密钥和第二状态数据集合,

从所述边缘节点向所述主机节点发送与所述云基础设施环境的资源对应的网络地址,

其中所述主机节点使用所述网络地址访问所述资源。

9. 如权利要求8所述的系统,其中第二背书密钥包括公共证明身份密钥的公共密钥组件。

10. 如权利要求8所述的系统,其中至少通过将第二背书密钥与第一背书密钥进行比较来验证第二背书密钥包括:

确定第二背书密钥的至少一个值与第一背书密钥的对应值匹配。

11. 如权利要求8所述的系统,其中所述操作还包括:

在从所述主机节点接收第二请求之前:

从所述主机节点接收对预启动执行环境客户端的预启动请求;以及

将所述预启动执行环境客户端发送到所述主机节点,

其中,所述主机节点使用所述预启动执行环境客户端来执行启动过程。

12. 如权利要求8所述的系统,其中至少通过将第二状态数据集合与第一状态数据集合进行比较来验证第二状态数据集合包括:

识别被包括在第一状态数据集合中的第一平台配置寄存器值;

识别被包括在第一状态数据集合中的第二平台配置寄存器值;以及

确定第一平台配置寄存器值与第二平台配置寄存器值匹配。

13. 如权利要求8所述的系统,其中所述操作还包括:

将启动分区安装到存储模块,

其中所述启动分区特定于所述主机节点,并且其中所述网络地址对应于所述启动分区。

14. 如权利要求8所述的系统,其中第二请求包括对所述网络地址的请求,其中第二请

求是响应于所述主机节点连接到数据中心环境而从所述主机节点发送的,所述数据中心环境包括实现所述云基础设施环境的一个或多个计算设备。

15. 一种非暂态计算机可读介质,包括指令,所述指令在由一个或多个硬件处理器执行时,使得执行操作,所述操作包括:

在云基础设施环境的边缘节点处从与所述云基础设施环境相关联的控制台接收第一请求,

其中第一请求包括创建用于主机节点的主机实例的第一指令,

其中第一请求包括用于边缘证明处理的认证数据集合,

其中所述认证数据集合包括第一背书密钥和第一状态数据集合,

其中第一状态数据集合指示所述主机节点的参考状态;

在所述边缘节点处从所述主机节点接收第二请求,

其中第二请求包括将所述主机节点连接到所述云基础设施环境的第二指令;

至少部分地经由所述边缘节点执行所述边缘证明处理,其中所述边缘证明处理包括:

在所述边缘节点处从所述主机节点接收第二背书密钥;

至少通过将第二背书密钥与第一背书密钥进行比较来验证第二背书密钥;

在所述边缘节点处接收第二状态数据集合,其中第二状态数据集合指示所述主机节点的状态;

至少通过将第二状态数据集合与第一状态数据集合进行比较来验证第二状态数据集合;以及

响应于验证第二背书密钥和第二状态数据集合,

从所述边缘节点向所述主机节点发送与所述云基础设施环境的资源对应的网络地址,

其中所述主机节点使用所述网络地址访问所述资源。

16. 如权利要求15所述的非暂态计算机可读介质,其中第二背书密钥包括公共证明身份密钥的公共密钥组件。

17. 如权利要求15所述的非暂态计算机可读介质,其中至少通过将第二背书密钥与第一背书密钥进行比较来验证第二背书密钥包括:

确定第二背书密钥中的至少一个值与第一背书密钥中的对应值匹配。

18. 如权利要求15所述的非暂态计算机可读介质,其中至少通过将第二状态数据集合与第一状态数据集合进行比较来验证第二状态数据集合包括:

识别被包括在第一状态数据集合中的第一平台配置寄存器值;

识别被包括在第一状态数据集合中的第二平台配置寄存器值;以及

确定第一平台配置寄存器值与第二平台配置寄存器值匹配。

19. 如权利要求15所述的非暂态计算机可读介质,其中所述操作还包括:

将启动分区安装到存储模块,

其中所述启动分区特定于所述主机节点,并且其中所述网络地址对应于所述启动分区。

20. 如权利要求15所述的非暂态计算机可读介质,其中第二请求包括对所述网络地址的请求,其中第二请求是响应于所述主机节点连接到数据中心环境而从所述主机节点发送的,所述数据中心环境包括实现所述云基础设施环境的一个或多个计算设备。

21. 如权利要求16所述的非暂态计算机可读介质,其中第一背书密钥包括由可信平台模块生成的密钥。
22. 如权利要求21所述的非暂态计算机可读介质,其中第一背书密钥识别所述主机节点。
23. 如权利要求15所述的非暂态计算机可读介质,其中所述操作还包括:
在从所述主机节点接收第二请求之前:
从所述主机节点接收预启动请求,
其中所述预启动请求用于所述边缘节点向所述主机节点发送第一预启动执行环境客户端;以及
将第一预启动执行环境客户端发送到所述主机节点,
其中,所述主机节点使用第一预启动执行环境客户端来执行启动过程。
24. 如权利要求23所述的非暂态计算机可读介质,其中第二状态数据集合包括一个或多个散列寄存器值,所述一个或多个散列寄存器指示由执行所述启动过程的至少一部分产生的主机节点的状态。
25. 如权利要求23所述的非暂态计算机可读介质,其中第二状态数据集合包括平台配置寄存器值,其中所述平台配置寄存器值包括多个散列寄存器值,其中所述多个散列寄存器值中的每个散列寄存器值指示在所述启动过程期间的主机节点的特定状态。
26. 如权利要求25所述的非暂态计算机可读介质,其中所述多个散列寄存器值的每个散列寄存器值指示由所述主机节点发起的特定服务或特定组件。
27. 如权利要求23所述的非暂态计算机可读介质,其中所述操作还包括:
在将第一预启动执行环境客户端发送到所述主机节点之后:
执行第二预启动执行环境;
在所述主机节点使用第一预启动执行环境客户端执行所述启动过程时,将与第二预启动执行环境相关联的信息发送到所述主机节点,
其中,与第二预启动执行环境相关联的所述信息包括操作系统信息,所述操作系统信息对应于与第二预启动执行环境相关联地执行的操作系统。
28. 如权利要求27所述的非暂态计算机可读介质,其中所述操作系统安装在所述云基础设施环境的计算设备上。
29. 如权利要求27所述的非暂态计算机可读介质,其中所述边缘节点是智能网络接口控制器的组件,并且其中所述操作系统安装在所述智能网络接口控制器上。
30. 如权利要求27所述的非暂态计算机可读介质,其中与第二预启动执行环境相关联的所述信息允许所述主机节点执行所述启动过程,而无需在所述主机节点上安装所述操作系统。
31. 如权利要求23所述的非暂态计算机可读介质,其中所述主机节点在所述启动过程期间生成第二状态数据集合的至少一部分。
32. 如权利要求15所述的非暂态计算机可读介质,其中所述边缘证明处理还包括:
从所述边缘节点向所述主机节点发送第三请求,
其中第三请求用于所述边缘节点提供第二背书密钥,
其中,所述主机节点接收第三请求,并且响应于接收到第三请求,所述主机节点生成第

二背书密钥并将第二背书密钥发送到所述边缘节点。

33. 如权利要求32所述的非暂态计算机可读介质，
其中，所述主机节点生成密钥对，以及

其中第二背书密钥是由所述主机节点基于所述密钥对生成的。

34. 如权利要求33所述的非暂态计算机可读介质，其中所述密钥对包括公共证明身份密钥。

35. 如权利要求15所述的非暂态计算机可读介质，其中所述边缘证明处理还包括：
从所述边缘节点向所述主机节点发送第三请求，

其中第三请求用于所述边缘节点提供第二状态数据集合，

其中，所述主机节点接收第三请求，并且响应于接收到第三请求，所述主机节点生成第二状态数据集合并将第二状态数据集合发送到所述边缘节点。

36. 如权利要求35所述的非暂态计算机可读介质，其中，第三请求是响应于验证第二背书密钥而从所述边缘节点发送到所述主机节点的。

用于云基础设施系统中计算节点授权的边缘证明的方法、系统和非暂态计算机可读介质

[0001] 相关申请的交叉引用

[0002] 本申请要求于2021年11月10日提交的标题为“Edge Attestation for Authorization of a Computing Node in a Cloud Infrastructure System”的编号为17/523,789的美国专利申请的优先权,其公开内容出于所有目的通过引用全文并入本文。

技术领域

[0003] 所公开的技术涉及云计算认证。更具体而言,所公开的技术涉及例如在向新加入云计算环境的主机节点授予网络访问权限之前,利用该环境的边缘组件对该新主机节点进行认证。

背景技术

[0004] 在数据中心环境中,可以添加新组件(例如,服务器)作为新主机设备。可以将新组件添加到云计算环境中以增加云环境中的计算资源或为在云环境中的组件上执行的应用/服务提供附加功能。新组件可以物理连接到数据中心环境中的其他设备,从而连接实现云计算环境的多个设备。例如,主机托管中心(colocation center)可以提供容纳实现云计算环境的组件的数据中心环境。

[0005] 但是,在许多情况下,数据中心环境(例如,主机托管中心)可以容纳其他实体的计算设备/数据中心。在这种情况下,另一个实体可以访问容纳实现云计算环境的组件的数据中心环境附近的区域。例如,另一个实体可以在未经授权的情况下恶意地将设备连接到数据中心环境。在不需要任何核实处理的情况下,连接的设备就可以访问云计算环境中私有维护的数据和/或服务。

发明内容

[0006] 本实施例涉及主机节点访问云基础设施环境的边缘证明。第一示例性实施例提供了一种用于主机节点访问云基础设施环境的证明的方法。该方法可以包括从控制台获得用于对主机节点进行授权的认证数据集合。该认证数据集合可以包括第一背书密钥和识别主机节点的特性的认证策略。认证策略可以包括第一平台配置寄存器(PCR)值。

[0007] 该方法还可以包括从主机节点获得对用以连接到云基础设施环境的网络地址的请求。该方法还可以包括从主机节点接收第二背书密钥。该方法还可以包括将第二背书密钥与在认证数据集合中接收到的第一背书密钥进行比较,以验证第二背书密钥。

[0008] 该方法还可以包括从主机节点接收主机节点认证数据集合。该主机节点认证数据集合可以包括第二PCR值,该第二PCR值包括主机节点的启动过程期间的散列寄存器值。该方法还可以包括将接收到的主机节点认证数据与在认证数据集合中接收到的认证策略进行比较,以通过确定第一PCR值是否与第二PCR值匹配来验证接收到的主机节点认证数据。该方法还可以包括响应于验证第二背书密钥和接收到的主机节点认证数据,向主机节点提

供网络地址。主机节点可以被配置为使用网络地址连接到云基础设施环境。

[0009] 第二示例性实施例涉及一种云基础设施节点。该云基础设施节点可以包括处理器和非暂态计算机可读介质。非暂态计算机可读介质可以包括指令,该指令在由处理器执行时,使得处理器从控制台获得用于对主机节点进行授权的认证数据集合。该认证数据集合包括第一背书密钥和识别主机节点的特性的认证策略。该指令还可以使得处理器从主机节点获得对用以连接到云基础设施环境的网络地址的请求。

[0010] 该指令还可以使得处理器向主机节点发送对第二背书密钥的请求。该指令还可以使得处理器从主机节点接收第二背书密钥。该指令还可以使得处理器将第二背书密钥与在认证数据集合中接收到的第一背书密钥进行比较,以验证第二背书密钥。该指令还可以使得处理器向主机节点发送对主机节点认证数据的请求。该指令还可以使得处理器从主机节点接收主机节点认证数据。

[0011] 该指令还可以使得处理器将接收到的主机节点认证数据与在认证数据集合中接收到的认证策略进行比较,以验证接收到的主机节点认证数据。该指令还可以使得处理器响应于验证第二背书密钥和接收到的主机节点认证数据,向主机节点提供网络地址。主机节点可以被配置为使用网络地址连接到云基础设施环境。

[0012] 第三示例性实施例涉及一种非暂态计算机可读介质。该非暂态计算机可读介质可以包括存储在其上的指令序列,该指令序列在由处理器执行时,使得处理器执行处理。该处理可以包括从控制台获得用于对主机节点进行授权的认证数据集合。该认证数据集合包括第一背书密钥和识别主机节点的特性的认证策略。该处理还可以包括从主机节点获得对用以连接到云基础设施环境的网络地址的请求。

[0013] 该处理还可以包括从主机节点接收对预启动执行环境客户端的请求。该处理还可以包括向主机节点提供预启动执行环境客户端,其中主机节点被配置为使用预启动执行环境客户端来执行启动过程。

[0014] 该处理还可以包括从主机节点接收第二背书密钥。该处理还可以包括将第二背书密钥与在认证数据集合中接收到的第一背书密钥进行比较,以验证第二背书密钥。该处理还可以包括从主机节点接收使用预启动执行环境客户端在启动过程期间导出的主机节点认证数据集合。

[0015] 该处理还可以包括将接收到的主机节点认证数据与在认证数据集合中接收到的认证策略进行比较,以验证接收到的主机节点认证数据。该处理还可以包括响应于验证第二背书密钥和接收到的主机节点认证数据,向主机节点提供网络地址。主机节点可以被配置为使用网络地址连接到云基础设施环境。

附图说明

[0016] 图1是根据至少一个实施例的示例网络环境的框图。

[0017] 图2是根据至少一个实施例的示例云基础设施系统的框图。

[0018] 图3是图示根据至少一个实施例的示例边缘证明处理的信令处理。

[0019] 图4是图示根据至少一个实施例的由SmartNIC执行的用于执行边缘证明处理的示例方法的框图。

[0020] 图5是图示根据至少一个实施例的由要使用边缘证明处理来验证的主机节点执行

的示例方法的框图。

[0021] 图6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个模式的框图。

[0022] 图7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个模式的框图。

[0023] 图8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个模式的框图。

[0024] 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另一个模式的框图。

[0025] 图10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

[0026] 在许多情况下,多个计算设备(例如,服务器)和在多个计算设备上执行的应用/服务可以实现云计算基础设施。此外,可以将新主机节点添加到多个计算设备,以增加云计算基础设施的计算资源或功能。在这种情况下,可以通过核实新计算设备的身份和安全特征来管理新主机节点。这种核实可以通过远程证明来执行,远程证明可以包括计算设备提供密码可核实的信息以核实每个计算设备的身份和配置。远程证明过程可以用于管理网络中设备的安全性并识别例如计算设备的状态。

[0027] 代替实现中央化服务以在云基础设施中集中实现远程证明,可以由云基础设施环境中靠近主机节点的边缘节点执行核实服务。证明核实服务可以被包括作为云基础设施中的线路插件(bump-in-the-wire)节点(例如,智能网络接口控制器(SmartNIC))的一部分。在SmartNIC处实现证明核实服务可以从云基础设施的中央组件卸载处理任务,从而提高云基础设施的数据处理效率。此外,在证明核实服务发生故障的情况下,可能只影响少数设备/应用,因为证明核实服务是在云基础设施边缘上的SmartNIC上执行的。

[0028] 本实施例涉及一种用于网络环境中主机节点的认证和授权的边缘证明服务。在允许新主机节点访问网络之前,可以执行认证处理。例如,控制台可以与云基础设施中的边缘组件(例如,smartNIC)交互,以获得用于验证新主机节点的认证数据集合(例如,公共背书密钥、租赁认证数据)。

[0029] 在一些情况下,SmartNIC可以向主机节点提供预启动(pre-boot)执行环境(例如,iPXE),以便主机节点执行启动过程,而无需在主机节点上预先安装OS。例如,可以向主机节点提供iPXE客户端,以允许在主机节点上执行的iPXE客户端与在SmartNIC上执行的iPXE环境之间的通信。

[0030] SmartNIC可以向主机节点发送对背书(endorsement)密钥的请求,并且作为响应,主机节点可以(例如,基于生成的公钥/私钥对)生成背书密钥。SmartNIC可以获得背书密钥并将其与在认证数据集合中接收到的公共背书密钥进行比较,并核实从主机节点获得的背书密钥是否与在认证数据集合中接收到的公共背书密钥对应(例如,匹配)。核实接收到的背书密钥可以核实主机节点的身份。

[0031] SmartNIC可以向主机节点发送对认证数据的请求。认证数据可以包括对主机节点进行认证的数据,诸如固件配置、设备配置、平台配置寄存器(PCR)值等。主机节点可以生成

认证数据,并且可以将生成的认证数据提供给SmartNIC。可以将接收到的认证数据与在认证数据集合中接收到的认证策略进行比较,以验证接收到的认证数据(例如,通过将主机节点生成的PCR值与认证数据集合中提供的对应PCR值进行匹配)。

[0032] SmartNIC可以响应于验证从主机节点接收到的认证数据和接收到的背书密钥而向主机节点提供网络地址。向主机节点提供网络地址(例如,互联网协议(IP)地址)可以允许主机节点访问云基础设施中的组件/应用/服务。这可以允许在提供对云基础设施的访问时提高安全性。

[0033] A. 系统概述

[0034] 图1是示例网络环境100的框图。网络环境100可以允许使用一个或多个网络(例如,互联网)在环境中的设备之间进行数据通信。如图1中所示,网络环境100可以包括控制台102、云基础设施(CI)系统104(以及对应的计算设备106a-c)和主机节点108中的任何一个。

[0035] 控制台102可以包括能够与CI系统104通信的计算设备(例如,膝上型计算机)。例如,控制台102可以向CI系统104提供用于创建主机节点108的实例(例如,包括认证数据集合)的指令。作为另一个示例,控制台102可以指示主机节点108从CI系统104获取预启动执行环境客户端(例如,iPXE)或发起主机节点108与SmartNIC 110之间的会话。

[0036] 如本文所述,CI系统104可以包括实现一个或多个云应用或服务的一个或多个互连计算设备。例如,CI系统104可以存储数据库数据并提供(例如,经由数据库查询)对数据库数据的访问。CI系统104中包括的计算设备(例如,106a-106c)可以位于一个或多个数据中心环境中(例如,主机托管中心)。

[0037] 如图1中所示,计算设备106c可以实现SmartNIC 110。SmartNIC 110可以位于CI系统104中的边缘组件(例如,计算设备106c)上。例如,SmartNIC 110可以驻留在数据中心中部署的服务器上,该服务器充当对CI系统104的边缘接入点。SmartNIC 110可以执行如本文所述的远程证明服务。

[0038] 主机节点108可以包括被引入到CI系统104的计算设备(例如,服务器)或一系列计算设备。例如,主机节点可以包括连接到数据中心环境(例如,主机托管中心)处的CI系统104并请求访问CI系统104的服务器。主机节点108可以被配置为执行各种处理任务或实现一个或多个应用/服务。如本文所述,主机节点108可以请求用于访问CI系统104的网络地址,并响应于SmartNIC 110分别验证由控制台102和主机节点108提供的背书密钥和认证数据而接收网络地址。

[0039] 图2是示例云基础设施系统104的框图。如上所述,CI系统104可以包括实现各种应用/服务的一个或多个互连计算设备。CI系统104可以包括实现CI系统104的核心功能的一个或多个中央计算设备和维护SmartNIC 110的边缘设备。SmartNIC 110可以与主机节点(例如,108)交互以获得认证数据并验证认证数据,如本文所描述的。

[0040] CI系统104可以包括预启动执行环境204。预启动执行环境204可以包括被配置为向主机节点提供客户端的环境(例如,iPXE),允许主机节点在主机节点上未安装操作系统(OS)的情况下执行预启动执行环境。例如,主机节点可以从SmartNIC检索iPXE客户端,并通过与在CI系统104中执行的预启动执行环境204交互来执行iPXE客户端。

[0041] CI系统104可以包括存储模块206。存储模块206可以跨CI系统104中的设备存储各

种数据类型(例如,用于验证的主机节点的已安装的启动分区)。

[0042] CI系统104可以包括控制台认证数据208。控制台认证数据208可以包括从控制台获得的认证数据集中用于新主机节点的边缘证明的数据。控制台认证数据208可以包括第一背书密钥(EK) 210a和租赁授权策略212。在一些情况下,控制台认证数据208可以存储获得的引入到CI系统104的多个主机节点的认证数据。

[0043] 第一EK 210a可以包括由控制台提供的识别主机节点的密钥(例如,可信平台模块(TPM)RSA密钥)。租赁授权策略212可以包括主机节点的特性,诸如固件版本、配置设置、PCR值等。

[0044] CI系统104还可以包括主机认证数据214。主机认证数据214可以包括从主机节点获得的信息,诸如第二EK 210b和认证数据(或“auth数据”) 216。主机认证数据214中的数据可以与控制台认证数据208进行比较,以识别和验证主机节点,如本文所描述的。

[0045] CI系统104可以包括认证数据检索模块218。认证数据检索模块218可以从主机节点获得认证数据(例如,控制台认证数据208)并接收主机认证数据(例如,214),如本文所描述的。在一些情况下,认证数据检索模块218可以响应于向主机节点提供预启动执行环境客户端和/或从十个主机节点接收对网络地址的请求而请求主机认证数据(例如,214)。

[0046] CI系统104可以包括密钥核实模块220。密钥核实模块220可以从主机节点获得密钥,并使用控制台102提供的密钥来核实上述密钥。核实密钥可以包括确定接收到的密钥是否与控制台提供的密钥匹配/对应(例如,包括多个相似之处)。

[0047] CI系统104可以包括认证(auth)数据核实模块222。auth数据核实模块222可以获得/识别auth数据并将接收到的auth数据与从控制台接收到的auth策略进行比较。例如,auth数据可以指定固件版本、主机节点配置、PCR值(例如,响应于在启动过程期间识别/激活的组件而添加的一系列散列值)等。在这个示例中,可以将auth数据与租赁auth策略进行比较以匹配特定于主机节点的值、固件版本、数据类型等。响应于密钥和auth数据被核实,可以核实主机节点并且(例如,通过向主机节点提供网络地址)允许其访问云基础设施。

[0048] B. 用于执行边缘证明过程的示例方法

[0049] 图3是图示示例边缘证明处理的信令处理300。如图3中所示,控制台302和主机节点308可以与(例如,在CI系统中的边缘计算设备上执行的)SmartNIC 306交互。

[0050] 在310处,控制台302可以向SmartNIC 306发送创建新主机实例的请求。创建新主机实例的请求可以识别新主机节点,并且可以包括第一背书密钥和用于核实主机节点的租赁auth策略。

[0051] 在312处,控制台302可以向主机节点308发送启动(start)主机节点实例的请求。主机节点308接收到的请求可以包括连接到SmartNIC 306并发起启动过程的指令。

[0052] 在314处,主机节点308可以向SmartNIC 306发送对预启动执行环境(例如,iPXE客户端)的请求。该请求可以包括来自SmartNIC 306的对iPXE客户端的请求。如本文所描述的,iPXE客户端可以允许主机节点308执行启动过程,而无需在主机节点308上加载操作系统。

[0053] 在316处,SmartNIC 306可以向主机节点提供预启动执行环境(例如,iPXE客户端)。在318处,主机节点308可以(例如,通过iPXE客户端与和在边缘设备上执行的SmartNIC 306相关联的iPXE实例交互)执行预启动执行环境。执行预启动执行环境可以执行启动过

程,其包括运行启动过程、发起服务/应用和组件等。

[0054] 在一些情况下,在启动过程期间,可以计算PCR值。PCR值可以包括一系列散列值,其指示主机节点308发起的每个组件/服务。PCR值可以指示启动过程之后主机节点308的状态。

[0055] 在320处,主机节点308可以从SmartNIC 306请求网络地址。网络地址(例如,IP地址)可以允许连接到CI系统。SmartNIC 306可以仅响应于验证主机节点而给出网络地址,如本文所描述的。

[0056] 在322处,SmartNIC 306可以从主机节点308请求公共背书密钥(EK)。在324处,主机节点308可以生成公钥/私钥对。在326处,主机节点308可以从密钥对生成公共背书密钥。在328处,主机节点308可以将公共背书密钥发送到SmartNIC 306。可以将公共背书密钥与(例如,在310处)控制台提供的创建实例请求期间提供的密钥进行比较。

[0057] 在330处,SmartNIC 306可以从主机节点308请求auth数据集合。在332处,主机节点308可以生成所请求的auth数据集合(例如,与主机节点相关的详细信息、固件版本、配置设置、PCR值),如对auth数据集合的请求中所指定的。在334处,主机节点308可以将该auth数据集合发送到SmartNIC 306以核实auth数据。

[0058] 在336处,SmartNIC可以验证接收到的公共背书密钥和auth数据集合。这可以包括将从主机节点308接收到的数据与(例如,在310处)在创建实例的请求中从控制台302获得的数据进行比较。

[0059] 响应于验证接收到的数据,在338处,SmartNIC 306可以向主机节点308发送网络地址。该网络地址可以允许主机节点308和CI系统之间的连接和数据通信。在340处,SmartNIC 306可以在块存储装置304处安装特定于主机节点的启动分区。

[0060] 图4是图示由SmartNIC执行的用于执行边缘证明处理的示例方法的框图400。在402处,SmartNIC可以从控制台获得用于对主机节点进行授权的认证数据集合。该认证数据集合可以包括第一背书密钥和识别主机节点的特性的认证策略。

[0061] 在404处,SmartNIC提供预启动执行环境(例如,iPXE客户端)。SmartNIC可以从主机节点接收对预启动执行环境客户端的请求。SmartNIC可以向主机节点提供预启动执行环境客户端。主机节点可以被配置为使用预启动执行环境客户端来执行启动过程。

[0062] 在406处,SmartNIC可以从主机节点获得对用于连接到云基础设施环境的网络地址的请求。在一些情况下,响应于主机节点连接到包括实现云基础设施环境的一个或多个计算设备的数据中心环境,从主机节点获得对网络地址的请求。

[0063] 在408处,SmartNIC可以向主机节点发送对第二背书密钥的请求。在410处,SmartNIC可以从主机节点接收第二背书密钥。第二背书密钥可以包括公共证明身份密钥(AIK)。

[0064] 在412处,SmartNIC可以将第二背书密钥与在认证数据集合中接收到的第一背书密钥进行比较以验证第二背书密钥。这可以包括确定第二背书密钥中的至少一个值与第一背书密钥中的对应值匹配。

[0065] 在414处,SmartNIC可以向主机节点发送对主机节点认证数据的请求。在416处,SmartNIC可以从主机节点接收主机节点认证数据。

[0066] 在418处,SmartNIC可以将接收到的主机节点认证数据与在认证数据集合中接收

到的认证策略进行比较,以验证接收到的主机节点认证数据。这可以包括识别认证策略中包括的第一平台配置寄存器 (PCR) 值和接收到的主机节点认证数据中提供的第二PCR值 (例如,其在启动过程期间生成)。第二PCR值可以包括主机节点的启动过程期间的散列寄存器值,其指示启动过程之后主机节点的状态。这还可以包括确定第一PCR值是否与第二PCR值匹配。响应于确定第一PCR值与第二PCR值匹配,可以验证接收到的主机节点认证数据。

[0067] 在420处,SmartNIC可以向主机节点提供网络地址。主机节点可以被配置为使用网络地址连接到云基础设施环境。这可以响应于验证第二背书密钥和接收到的主机节点认证数据来执行。

[0068] 图5是图示由要使用边缘证明处理进行验证的主机节点执行的示例方法的框图500。在502处,主机节点可以从控制台接收启动实例的请求。启动实例的请求可以包括与SmartNIC通信的指令和实现启动过程的指令。

[0069] 在504处,主机节点可以从SmartNIC请求预启动执行环境。在506处,主机节点可以从SmartNIC接收预启动执行环境。在508处,主机节点可以执行预启动执行环境。预启动执行环境可以包括iPXE客户端,该客户端能够通过SmartNIC处的iPXE实例交互来执行启动过程,而无需使用主机节点上的操作系统。

[0070] 在510处,主机节点可以从SmartNIC发送对网络地址 (例如,IP地址) 的请求。在512处,主机节点可以从SmartNIC接收对公共背书密钥 (EK pub) 的请求。在514处,主机节点可以生成EK pub。EK pub可以从主机节点生成的公钥/私钥对生成。在516处,主机节点可以将生成的EK pub发送到SmartNIC。SmartNIC可以通过将接收到的EK pub与控制台接收到的密钥进行比较来验证接收到的EK pub (例如,或第二背书密钥)。

[0071] 在518处,主机节点可以接收对auth数据 (例如,主机节点认证数据) 的请求。在520处,主机节点可以生成auth数据 (例如,基于启动过程的第二PCR值)。在522处,主机节点可以将生成的auth数据发送到SmartNIC。SmartNIC可以通过将接收到的auth数据与认证策略进行比较来验证auth数据。

[0072] 在524处,主机节点可以从SmartNIC接收网络地址。该网络地址可以允许使用该网络地址与云基础设施进行连接/数据传输。响应于SmartNIC验证auth数据,可以接收该网络地址。

[0073] C. IaaS概述

[0074] 如上所述,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、日志记录、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。

[0075] 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堆栈的剩余元素。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该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。

[0076] 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。

[0077] 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(例如,服务器、存储装置、网络硬件和虚拟化)之下。因此,客户可以负责处理(OS)、中间件和/或(例如,在(例如可以按需启动的)自助服务虚拟机上的)应用部署等。

[0078] 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。

[0079] 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合存在最初的挑战。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。

[0080] 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/出站业务组规则以定义将如何设置网络的入站/出站业务以及一个或多个虚拟机(VM)。也可以供给其它基础设施元素,诸如负载均衡器、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。

[0081] 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来部署基础设施代码。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,需要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。

[0082] 图6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600。服务运营商602可以通信地耦合到可以包括虚拟云网络(VCN)606和安全主机子网608的安全主机租赁604。在一些示例中,服务运营商602可以使用一个或多个客户端计算设备(客户端计算设备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))中的任何操作系统的工作站计算机。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 606和/或互联网的网络进行通信的个人消息传递设备。

[0083] VCN 606可以包括本地对等网关(LPG) 610,该VCN 606可以经由包含在安全壳(SSH)VCN 612中的LPG 610通信地耦合到SSH VCN 612。SSH VCN 612可以包括SSH子网614,并且SSH VCN 612可以经由包含在控制平面VCN 616中的LPG 610通信地耦合到控制平面VCN 616。此外,SSH VCN 612可以经由LPG 610通信地耦合到数据平面VCN 618。控制平面VCN 616和数据平面VCN 618可以包含在可以由IaaS提供商拥有和/或操作的服务租赁619中。

[0084] 控制平面VCN 616可以包括充当外围网络(例如,公司内部网络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620。基于DMZ的服务器可以承担有限责任并有助于控制违规。此外,DMZ层620可以包括一个或多个负载平衡器(LB)子网622、可以包括(一个或多个)应用(app)子网626的控制平面应用层624、可以包括(一个或多个)数据库(DB)子网630(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628。包含在控制平面DMZ层620中的(一个或多个)LB子网622可以通信地耦合到包含在控制平面应用层624中的(一个或多个)应用子网626和可以包含在控制平面VCN 616中的互联网网关634,并且(一个或多个)应用子网626可以通信地耦合到包含在控制平面数据层628中的(一个或多个)DB子网630以及服务网关636和网络地址转换(NAT)网关638。控制平面VCN 616可以包括服务网关636和NAT网关638。

[0085] 控制平面VCN 616可以包括数据平面镜像应用层640,其可以包括(一个或多个)应用子网626。包含在数据平面镜像应用层640中的(一个或多个)应用子网626可以包括可以执行计算实例644的虚拟网络接口控制器(VNIC) 642。计算实例644可以将数据平面镜像应用层640的(一个或多个)应用子网626通信地耦合到可以包含在数据平面应用层646中的(一个或多个)应用子网626。

[0086] 数据平面VCN 618可以包括数据平面应用层646、数据平面DMZ层648和数据平面数据层650。数据平面DMZ层648可以包括(一个或多个)LB子网622,其可以通信地耦合到数据平面应用层646的(一个或多个)应用子网626和数据平面VCN 618的互联网网关634。(一个或多个)应用子网626可以通信地耦合到数据平面VCN 618的服务网关636和数据平面VCN 618的NAT网关638。数据平面数据层650还可以包括可以通信地耦合到数据平面应用层646的(一个或多个)应用子网626的(一个或多个)DB子网630。

[0087] 控制平面VCN 616和数据平面VCN 618的互联网网关634可以通信地耦合到元数据管理服务652,该元数据管理服务652可以通信地耦合到公共互联网654。公共互联网654可以通信地耦合到控制平面VCN 616和数据平面VCN 618的NAT网关638。控制平面VCN 616和数据平面VCN 618的服务网关636可以通信地耦合到云服务656。

[0088] 在一些示例中,控制平面VCN 616或数据平面VCN 618的服务网关636可以对云服务656进行应用编程接口(API)调用,而无需通过公共互联网654。从服务网关636到云服务656的API调用可以是单向的:服务网关636可以对云服务656进行API调用,并且云服务656

可以将请求的数据发送到服务网关636。但是,云服务656可以不发起对服务网关636的API调用。

[0089] 在一些示例中,安全主机租赁604可以直接连接到服务租赁619,服务租赁619否则可以被隔离。安全主机子网608可以通过LPG 610与SSH子网614通信,LPG 610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608连接到SSH子网614可以使安全主机子网608访问服务租赁619内的其它实体。

[0090] 控制平面VCN 616可以允许服务租赁619的用户设置或以其它方式供给期望资源。在控制平面VCN 616中供给的期望资源可以在数据平面VCN 618中部署或以其它方式使用。在一些示例中,控制平面VCN 616可以与数据平面VCN 618隔离,并且控制平面VCN 616的数据平面镜像应用层640可以经由VNIC 642与数据平面VCN 618的数据平面应用层646通信,VNIC 642可以包含在数据平面镜像应用层640和数据平面应用层646中。

[0091] 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652的公共互联网654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652可以通过互联网网关634将请求传送到控制平面VCN 616。请求可以由包含在控制平面DMZ层620中的(一个或多个)LB子网622接收。(一个或多个)LB子网622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622可以将请求传输到包含在控制平面应用层624中的(一个或多个)应用子网626。如果请求被验证并且需要对公共互联网654的调用,那么对公共互联网654的调用可以被传输到可以对公共互联网654进行调用的NAT网关638。请求可能期望存储的存储器可以存储在(一个或多个)DB子网630中。

[0092] 在一些示例中,数据平面镜像应用层640可以促进控制平面VCN 616和数据平面VCN 618之间的直接通信。例如,可能期望对包含在数据平面VCN 618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 642,控制平面VCN 616可以直接与包含在数据平面VCN 618中的资源通信,并且从而可以执行对这些资源的配置的更改、更新或其它适当的修改。

[0093] 在一些实施例中,控制平面VCN 616和数据平面VCN 618可以包含在服务租赁619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 616或数据平面VCN 618。替代地,IaaS提供商可以拥有或操作控制平面VCN 616和数据平面VCN 618,这两种平面都可以包含在服务租赁619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进行交互的网络。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的威胁防范级别的公共互联网654以进行存储。

[0094] 在其它实施例中,包含在控制平面VCN 616中的(一个或多个)LB子网622可以被配置为从服务网关636接收信号。在这个实施例中,控制平面VCN 616和数据平面VCN 618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654。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619上,服务租赁619可能与公共互联网654隔离。

[0095] 图7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700。服务运营商702(例如,图6的服务运营商602)可以通信地耦合到安全主机租赁704(例如,图6的安全主机租赁604),该安全主机租赁704可以包括虚拟云网络(VCN)706(例如,图6的VCN 606)和安全主机子网708(例如,图6的安全主机子网608)。VCN 706可以包括本地对等网关

(LPG) 710 (例如, 图6的LPG 610), 该VCN 706可以经由包含在安全壳 (SSH) VCN 712 (例如, 图6的SSH VCN 612) 中的LPG 610通信地耦合到SSH VCN 712。SSH VCN 712可以包括SSH子网714 (例如, 图6的SSH子网614), 并且SSH VCN 712可以经由包含在控制平面VCN 716 (例如, 图6的控制平面VCN 616) 中的LPG 710通信地耦合到控制平面VCN 716。控制平面VCN 716可以包含在服务租赁719 (例如, 图6的服务租赁619) 中, 并且数据平面VCN 718 (例如, 图6的数据平面VCN 618) 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721中。

[0096] 控制平面VCN 716可以包括控制平面DMZ层720 (例如, 图6的控制平面DMZ层620), 其可以包括 (一个或多个) LB子网722 (例如, 图6的 (一个或多个) LB子网622)、可以包括 (一个或多个) 应用子网726 (例如, 图6的 (一个或多个) 应用子网626) 的控制平面应用层724 (例如, 图6的控制平面应用层624)、可以包括 (一个或多个) 数据库 (DB) 子网730 (例如, 类似于图6的 (一个或多个) DB子网630) 的控制平面数据层728 (例如, 图6的控制平面数据层628)。包含在控制平面DMZ层720中的 (一个或多个) LB子网722可以通信地耦合到包含在控制平面应用层724中的 (一个或多个) 应用子网726和可以包含在控制平面VCN 716中的互联网网关734 (例如, 图6的互联网网关634), 并且 (一个或多个) 应用子网726可以通信地耦合到包含在控制平面数据层728中的 (一个或多个) DB子网730以及服务网关736 (例如, 图6的服务网关) 和网络地址转换 (NAT) 网关738 (例如, 图6的NAT网关638)。控制平面VCN 716可以包括服务网关736和NAT网关738。

[0097] 控制平面VCN 716可以包括可以包括 (一个或多个) 应用子网726的数据平面镜像应用层740 (例如, 图6的数据平面镜像应用层640)。包含在数据平面镜像应用层740中的 (一个或多个) 应用子网726可以包括可以执行计算实例744 (例如, 类似于图6的计算实例644) 的虚拟网络接口控制器 (VNIC) 742 (例如, VNIC 642)。计算实例744可以促进数据平面镜像应用层740的 (一个或多个) 应用子网726和可以包含在数据平面应用层746 (例如, 图6的数据平面应用层646) 中的 (一个或多个) 应用子网726之间的经由包含在数据平面镜像应用层740中的VNIC 742以及包含在数据平面应用层746中的VNIC 742的通信。

[0098] 包含在控制平面VCN 716中的互联网网关734可以通信地耦合到元数据管理服务752 (例如, 图6的元数据管理服务652), 该元数据管理服务752可以通信地耦合到公共互联网754 (例如, 图6的公共互联网654)。公共互联网754可以通信地耦合到包含在控制平面VCN 716中的NAT网关738。包含在控制平面VCN 716中的服务网关736可以通信地耦合到云服务756 (例如, 图6的云服务656)。

[0099] 在一些示例中, 数据平面VCN 718可以包含在客户租赁721中。在这种情况下, IaaS提供商可以为每个客户提供控制平面VCN 716, 并且IaaS提供商可以为每个客户设置包含在服务租赁719中的唯一计算实例744。每个计算实例744可以允许包含在服务租赁719中的控制平面VCN 716和包含在客户租赁721中的数据平面VCN 718之间的通信。计算实例744可以允许在包含在服务租赁719中的控制平面VCN 716中供给的资源被部署或以其它方式用于包含在客户租赁721中的数据平面VCN 718中。

[0100] 在其它示例中, IaaS提供商的客户可以具有存在于客户租赁721中的数据库。在这个示例中, 控制平面VCN 716可以包括数据平面镜像应用层740, 该数据平面镜像应用层740可以包括 (一个或多个) 应用子网726。数据平面镜像应用层740可以驻留在数据平面VCN 718中, 但数据平面镜像应用层740可能不存在于数据平面VCN 718中。换句话说, 数据平面

镜像应用层740可以访问客户租赁721,但是数据平面镜像应用层740可能不存在于数据平面VCN 718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740可以被配置为对数据平面VCN 718进行调用,但可以被配置为对包含在控制平面VCN 716中的任何实体进行调用。客户可能期望在数据平面VCN 718中部署或以其它方式使用在控制平面VCN 716中供给的资源,并且数据平面镜像应用层740可以促进客户的期望部署或资源的其它使用。

[0101] 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 718。在这个实施例中,客户可以确定数据平面VCN 718可以访问什么,并且客户可以限制从数据平面VCN 718对公共互联网754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 718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721中的数据平面VCN 718上可以帮助将数据平面VCN 718与其它客户和公共互联网754隔离开。

[0102] 在一些实施例中,云服务756可以由服务网关736调用以访问公共互联网754、控制平面VCN 716或数据平面VCN 718上可能不存在的服务。云服务756与控制平面VCN 716或数据平面VCN 718之间的连接可以不是实时的或连续的。云服务756可以存在于由IaaS提供商拥有或操作的不同网络上。云服务756可以被配置为接收来自服务网关736的调用并且可以被配置为不接收来自公共互联网754的调用。一些云服务756可以与其它云服务756隔离,并且控制平面VCN 716可以与可能与控制平面VCN 716不在同一区域的云服务756隔离。例如,控制平面VCN 716可能位于“区域1”,并且云服务“部署6”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 716中的服务网关736对部署6进行调用,那么该调用可以被传输到区域1中的部署6。在这个示例中,控制平面VCN 716或区域1中的部署6可能不与区域2中的部署6通信地耦合或以其它方式通信。

[0103] 图8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800。服务运营商802(例如,图6的服务运营商602)可以通信地耦合到安全主机租赁804(例如,图6的安全主机租赁604),该安全主机租赁804可以包括虚拟云网络(VCN) 806(例如,图6的VCN 606)和安全主机子网808(例如,图6的安全主机子网608)。VCN 806可以包括LPG 810(例如,图6的LPG 610),该VCN 806可以经由包含在SSH VCN 812(例如,图6的SSH VCN 612)中的LPG 810通信地耦合到SSH VCN 812。SSH VCN 812可以包括SSH子网814(例如,图6的SSH子网614),并且SSH VCN 812可以经由包含在控制平面VCN 816(例如,图6的控制平面VCN 616)中的LPG 810通信地耦合到控制平面VCN 816并且经由包含在数据平面VCN 818(例如,图6的数据平面618)中的LPG 810通信地耦合到数据平面VCN 818。控制平面VCN 816和数据平面VCN 818可以包含在服务租赁819(例如,图6的服务租赁619)中。

[0104] 控制平面VCN 816可以包括可以包括(一个或多个)负载均衡器(LB)子网822(例如,图6的(一个或多个)LB子网622)的控制平面DMZ层820(例如,图6的控制平面DMZ层620)、可以包括(一个或多个)应用子网826(例如,类似于图6的(一个或多个)应用子网626)的控制平面应用层824(例如,图6的控制平面应用层624)、可以包括(一个或多个)DB子网830的控制平面数据层828(例如,图6的控制平面数据层628)。包含在控制平面DMZ层820中的(一个或多个)LB子网822可以通信地耦合到包含在控制平面应用层824中的(一个或多个)应用子网826和可以包含在控制平面VCN 816中的互联网网关834(例如,图6的互联网网关634),并且(一个或多个)应用子网826可以通信地耦合到包含在控制平面数据层828中的(一个或

多个) DB子网830以及服务网关836 (例如,图6的服务网关) 和网络地址转换 (NAT) 网关838 (例如,图6的NAT网关638)。控制平面VCN 816可以包括服务网关836和NAT网关838。

[0105] 数据平面VCN 818可以包括数据平面应用层846 (例如,图6的数据平面应用层646)、数据平面DMZ层848 (例如,图6的数据平面DMZ层648)、以及数据平面数据层850 (例如,图6的数据平面数据层650)。数据平面DMZ层848可以包括可以通信地耦合到数据平面应用层846的 (一个或多个) 可信应用子网860和 (一个或多个) 不可信应用子网862以及包含在数据平面VCN 818中的互联网网关834的 (一个或多个) LB子网822。(一个或多个) 可信应用子网860可以通信地耦合到包含在数据平面VCN 818中的服务网关836、包含在数据平面VCN 818中的NAT网关838、以及包含在数据平面数据层850中的 (一个或多个) DB子网830。(一个或多个) 不可信应用子网862可以通信地耦合到包含在数据平面VCN 818中的服务网关836和包含在数据平面数据层850中的 (一个或多个) DB子网830。数据平面数据层850可以包括可以通信地耦合到包含在数据平面VCN 818中的服务网关836的 (一个或多个) DB子网830。

[0106] (一个或多个) 不可信应用子网862可以包括可以通信地耦合到租户虚拟机 (VM) 866(1) - (N) 的一个或多个主VNIC 864(1) - (N)。每个租户VM 866(1) - (N) 可以通信地耦合到可以包含在相应容器出口VCN 868(1) - (N) 中的相应应用子网867(1) - (N), 该相应容器出口VCN 868(1) - (N) 可以包含在相应客户租赁870(1) - (N) 中。相应辅VNIC 872(1) - (N) 可以促进包含在数据平面VCN 818中的 (一个或多个) 不可信应用子网862与包含在容器出口VCN 868(1) - (N) 中的应用子网之间的通信。每个容器出口VCN 868(1) - (N) 可以包括NAT网关838, 该NAT网关838可以通信地耦合到公共互联网854 (例如,图6的公共互联网654)。

[0107] 包含在控制平面VCN 816中以及包含在数据平面VCN 818中的互联网网关834可以通信地耦合到元数据管理服务852 (例如,图6的元数据管理系统652), 该元数据管理服务852可以通信地耦合到公共互联网854。公共互联网854可以通信地耦合到包含在控制平面VCN 816中以及包含在数据平面VCN 818中的NAT网关838。包含在控制平面VCN 816中以及包含在数据平面VCN 818中的服务网关836可以通信地耦合到云服务856。

[0108] 在一些实施例中,数据平面VCN 818可以与客户租赁870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予IaaS提供商的代码。

[0109] 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846的功能。运行该功能的代码可以在VM 866(1) - (N) 中执行,并且该代码可以不被配置为在数据平面VCN 818上的其它任何地方运行。每个VM 866(1) - (N) 可以连接到一个客户租赁870。包含在VM 866(1) - (N) 中的相应容器871(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871(1) - (N) 运行代码,其中容器871(1) - (N) 可能至少包含在 (一个或多个) 不可信应用子网862中所包含的VM 866(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871(1) - (N) 可以通信地耦合到客户租赁870并且可以被配置为传输或接收来自客户租赁870的数据。容器871(1) - (N) 可以不被配置为从数据平面VCN 818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871(1) - (N)。

[0110] 在一些实施例中, (一个或多个) 可信应用子网860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860可以通信地耦合到 (一个或多个) DB子网830并且被配置为在 (一个或多个) DB子网830中执行CRUD操作。(一个或多个) 不可信应用子网862可以通信地耦合到 (一个或多个) DB子网830, 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830中执行读取操作。可以包含在每个客户的VM 866(1) - (N) 中并且可以运行来自客户的代码的容器871(1) - (N) 可以不与 (一个或多个) DB子网830通信地耦合。

[0111] 在其它实施例中, 控制平面VCN 816和数据平面VCN 818可以不直接通信地耦合。在这个实施例中, 控制平面VCN 816和数据平面VCN 818之间可能不存在直接通信。但是, 通信可以通过至少一个方法而间接地发生。LPG 810可以由IaaS提供商建立, 其可以促进控制平面VCN 816和数据平面VCN 818之间的通信。在另一个示例中, 控制平面VCN 816或数据平面VCN 818可以经由服务网关836对云服务856进行调用。例如, 从控制平面VCN 816对云服务856的调用可以包括对可以与数据平面VCN 818通信的服务的请求。

[0112] 图9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900。服务运营商902 (例如, 图6的服务运营商602) 可以通信地耦合到安全主机租赁904 (例如, 图6的安全主机租赁604), 该安全主机租赁904可以包括虚拟云网络 (VCN) 906 (例如, 图6的VCN 606) 和安全主机子网908 (例如, 图6的安全主机子网608)。VCN 906可以包括LPG 910 (例如, 图6的LPG 610), 该VCN 906可以经由包含在SSH VCN 912 (例如, 图6的SSH VCN 612) 中的LPG 910通信地耦合到SSH VCN 912。SSH VCN 912可以包括SSH子网914 (例如, 图6的SSH子网614), 并且SSH VCN 912可以经由包含在控制平面VCN 916 (例如, 图6的控制平面VCN 616) 中的LPG 910通信地耦合到控制平面VCN 916并且经由包含在数据平面VCN 918 (例如, 图6的数据平面618) 中的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可以包含在服务租赁919 (例如, 图6的服务租赁619) 中。

[0113] 控制平面VCN 916可以包括可以包括 (一个或多个) LB子网922 (例如, 图6的 (一个或多个) LB子网622) 的控制平面DMZ层920 (例如, 图6的控制平面DMZ层620)、可以包括 (一个或多个) 应用子网926 (例如, 图6的 (一个或多个) 应用子网626) 的控制平面应用层924 (例如, 图6的控制平面应用层624)、可以包括 (一个或多个) DB子网930 (例如, 图8的 (一个或多个) DB子网830) 的控制平面数据层928 (例如, 图6的控制平面数据层628)。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 (例如, 图6的互联网网关634), 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 (例如, 图6的服务网关) 和网络地址转换 (NAT) 网关938 (例如, 图6的NAT网关638)。控制平面VCN 916可以包括服务网关936和NAT网关938。

[0114] 数据平面VCN 918可以包括数据平面应用层946 (例如, 图6的数据平面应用层646)、数据平面DMZ层948 (例如, 图6的数据平面DMZ层648)、以及数据平面数据层950 (例如, 图6的数据平面数据层650)。数据平面DMZ层948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) 可信应用子网960 (例如, 图8的 (一个或多个) 可信应用子网860) 和

(一个或多个)不可信应用子网962(例如,图8的(一个或多个)不可信应用子网862)以及包含在数据平面VCN 918中的互联网网关934的(一个或多个)LB子网922。(一个或多个)可信应用子网960可以通信地耦合到包含在数据平面VCN 918中的服务网关936、包含在数据平面VCN 918中的NAT网关938以及包含在数据平面数据层950中的(一个或多个)DB子网930。(一个或多个)不可信应用子网962可以通信地耦合到包含在数据平面VCN 918中的服务网关936和包含在数据平面数据层950中的(一个或多个)DB子网930。数据平面数据层950可以包括可以通信地耦合到包含在数据平面VCN 918中的服务网关936的(一个或多个)DB子网930。

[0115] (一个或多个)不可信应用子网962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962内的租户虚拟机(VM) 966(1) - (N)的主VNIC 964(1) - (N)。每个租户VM 966(1) - (N)可以运行相应容器967(1) - (N)中的代码,并且可通信地耦合到可以包含在数据平面应用层946中的应用子网926,该数据平面应用层946可以包含在容器出口VCN 968中。相应辅VNIC 972(1) - (N)可以促进包含在数据平面VCN 918中的(一个或多个)不可信应用子网962和包含在容器出口VCN 968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954(例如,图6的公共互联网654)的NAT网关938。

[0116] 包含在控制平面VCN 916中以及包含在数据平面VCN 918中的互联网网关934可以通信地耦合到元数据管理服务952(例如,图6的元数据管理系统652),该元数据管理服务952可以通信地耦合到公共互联网954。公共互联网954可以通信地耦合到包含在控制平面VCN 916中以及包含在数据平面VCN 918中的NAT网关938。包含在控制平面VCN 916中以及包含在数据平面VCN 918中的服务网关936可以通信地耦合到云服务956。

[0117] 在一些示例中,图9的框图900的体系架构所示的模式可以被认为是图8的框图800的体系架构所示的模式的例外,并且在IaaS提供商不能直接与客户通信(例如,断开连接的区域)的情况下,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包含在VM 966(1) - (N)中的相应容器967(1) - (N)。容器967(1) - (N)可以被配置为对包含在数据平面应用层946的(一个或多个)应用子网926中的相应辅VNIC 972(1) - (N)进行调用,该数据平面应用层946可以包含在容器出口VCN 968中。辅VNIC 972(1) - (N)可以将调用传输到NAT网关938,该NAT网关938可以将调用传输到公共互联网954。在这个示例中,可以由客户实时访问的容器967(1) - (N)可以与控制平面VCN 916隔离,并且可以与包含在数据平面VCN 918中的其它实体隔离。容器967(1) - (N)也可以与来自其它客户的资源隔离。

[0118] 在其它示例中,客户可以使用容器967(1) - (N)来调用云服务956。在这个示例中,客户可以运行容器967(1) - (N)中的从云服务956请求服务的代码。容器967(1) - (N)可以将该请求传输到辅VNIC 972(1) - (N),该辅VNIC 972(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954。公共互联网954可以经由互联网网关934将请求传输到包含在控制平面VCN 916中的(一个或多个)LB子网922。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926,该(一个或多个)应用子网926可以经由服务网关936将请求传输到云服务956。

[0119] 应当认识到的是,各图中描绘的IaaS体系架构600、700、800、900可以具有除所描绘的组件之外的其它组件。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,或者可以具有不同的组件布置或配置。

[0120] 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、弹性可伸缩、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方提供的Oracle云基础设施(OCI)。

[0121] 图10图示了其中可以实现本公开的各种实施例的示例计算机系统1000。系统1000可以用于实现上述任何计算机系统。如图所示,计算机系统1000包括经由总线子系统1002与多个外围子系统通信的处理单元1004。这些外围子系统可以包括处理加速单元1006、I/O子系统1008、存储子系统1018和通信子系统1024。存储子系统1018包括有形计算机可读存储介质1022和系统存储器1010。

[0122] 总线子系统1002提供用于让计算机系统1000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1002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1002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。

[0123] 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1004控制计算机系统1000的操作。一个或多个处理器可以被包括在处理单元1004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1004可以被实现为一个或多个独立的处理单元1032和/或1034,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1004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。

[0124] 在各种实施例中,处理单元1004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1004中和/或存储子系统1018中。通过适当的编程,(一个或多个)处理器1004可以提供上述各种功能。计算机系统1000可以附加地包括处理加速单元1006,其可以包括数字信号处理器(DSP)、专用处理器,等等。

[0125] I/O子系统1008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去往输入设备(例如,Google **Glass®**)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。

[0126] 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、数码摄录机、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音频输入设备,诸如MIDI键盘、数字乐器等。

[0127] 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。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。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1000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。

[0128] 计算机系统1000可以包括存储子系统1018,其包括软件元素,示为当前位于系统存储器1010内。系统存储器1010可以存储可在处理单元1004上加载和执行的程序指令,以及在这些程序的执行期间生成的数据。

[0129] 取决于计算机系统1000的配置和类型,系统存储器1010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)、闪存等)。RAM通常包含数据和/或程序模块,其可立即访问处理单元1004和/或当前由处理单元1004操作和执行。在一些实施方式中,系统存储器1010可以包括多种不同类型的存储器,诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。在一些实施方式中,基本输入/输出系统(BIOS)(包含帮助在计算机系统1000内的元件之间传送信息的基本例程(诸如在启动期间))通常可以存储在ROM中。作为示例而非限制,系统存储器1010还图示了应用程序1012,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1014和操作系统1016。举例来说,操作系统1016可以包括各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种商业上可用的 **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/或移动操作系统(诸如iOS、**Windows® Phone**、**Android®OS**、**BlackBerry® 100S**和 **Palm®OS**操作系统)。

[0130] 存储子系统1018还可以提供有形的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构造。当由处理器执行时提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统1018中。这些软件模块或指令可以由处理单元1004执行。存储子系统1018还可以提供用于存储根据本公开使用的数据的储存库。

[0131] 存储子系统1000还可以包括还可以连接到计算机可读存储介质1022的计算机可读存储介质读取器1020。与系统存储器1010一起并可选地与系统存储器1010结合,计算机可读存储介质1022可以全面地表示远程、本地、固定和/或可移除存储设备加上用于临时和/或更永久地包含、存储、传输和检索计算机可读信息的存储介质。

[0132] 包含代码或代码的部分的计算机可读存储介质1022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、可移除和不可移除的介质。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)或其它光学存储装置、磁带盒、磁带、磁盘存储装置或其它磁存储设备,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,或者可以被用来传输期望信息并且可以被计算机系统1000访问的任何其它介质。

[0133] 举例来说,计算机可读存储介质1022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1022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、数字视频带等。计算机可读存储介质1022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的SSD和基于闪存存储器的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1000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。

[0134] 通信子系统1024提供到其它计算机系统和网络的接口。通信子系统1024用作用于从其它系统接收数据和从计算机系统1000向其它系统传输数据的接口。例如,通信子系统1024可以使计算机系统1000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1024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、或其任何组合)、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,通信子系统1024可以提供有线网络连接(例如,以太网),作为无线接口的附加或者替代。

[0135] 在一些实施例中,通信子系统1024也可以代表可以使用计算机系统1000的一个或多个用户接收结构化和/或非结构化的数据馈送1026、事件流1028、事件更新1030等形式的输入通信。

[0136] 举例来说,通信子系统1024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1026,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。

[0137] 此外,通信子系统1024也可以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1028和/或事件更新1030。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。

[0138] 通信子系统1024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1026、事件流1028、事件更新1030等,该一个或多个数据库可以与耦合到计算机系统1000的一个或多个流式传输数据源计算机进行通信。

[0139] 计算机系统1000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。

[0140] 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1000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applet)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。

[0141] 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。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。

[0142] 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。实施例可以仅用硬件、或仅用软件、或使用它们的组合来实现。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。因而,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、或通过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,或者同一进程对可以在不同时间使用不同的技术。

[0143] 因而,说明书和附图被认为是说明性的而不是限制性的意义。但是,在不脱离权利要求中阐述的更广泛的精神和范围的情况下,显然可以对其进行添加、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。

[0144] 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”以及类似的指称应被解释为涵盖单数和复数两者,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”和“含有”应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内、附接到或连接在一起,即使中间存在一些东西。除非本文另有指示,否则本文中的值范围的描述仅旨在用作单独引用落入该范围内的每个单独值的简略方法,并且每个单独值被并入说明书中,就好像它在本文中单独描述一样。除非本文另有指示或另外与上下文明显矛盾,否则本文描述的所有方法都可以以任何合适的顺序执行。除非另有声明,否则本文提供的任何和全部示例或示例性语言(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。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。

[0145] 除非另有明确说明,否则析取(disjunctive)语言(诸如短语“X、Y或Z中的至少一个”)旨在在上下文中被理解为用作一般地表示项目、术语等可以是X、Y或Z中的任一者或者是它们的任何组合(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。

[0146] 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。这些优选实施例的变型对于本领域普通技术人员在阅读前述的描述后将变得显而易见。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。因而,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,除非本文另有指示,否则本公开包括在其所有可能的变型中的上述元素的任何组合。

[0147] 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,就好像指示每个参考文献单独且具体地通过引用并入并且在本文中全文阐述一样。

[0148] 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环境和应用之外的任何数量的环境和应用中被使用。因而,本说明书和附图应当被认为是说明性而不是限制性的。

[0149] 另外,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,该计算机程序/指令在由处理器执行时,使得处理器执行本文公开内容中描述的任何方法/技术。

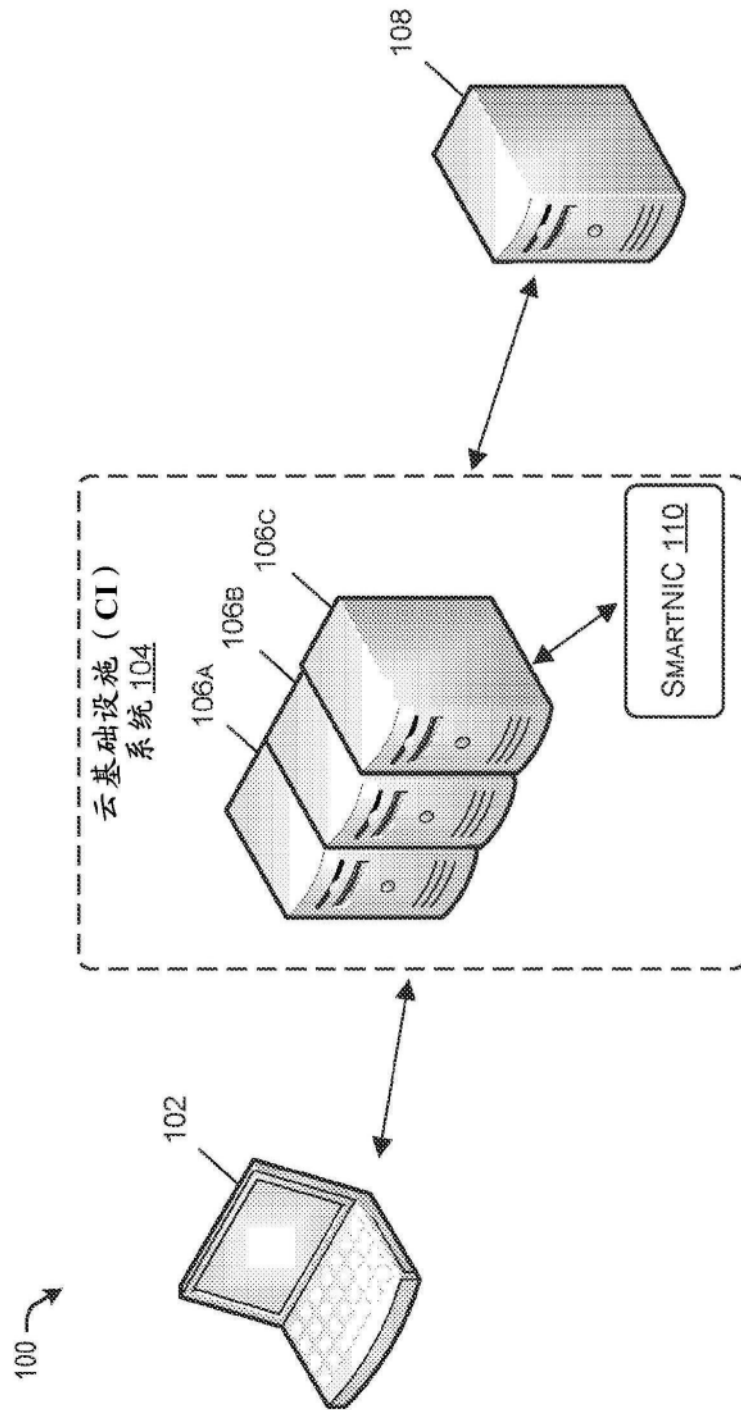


图1

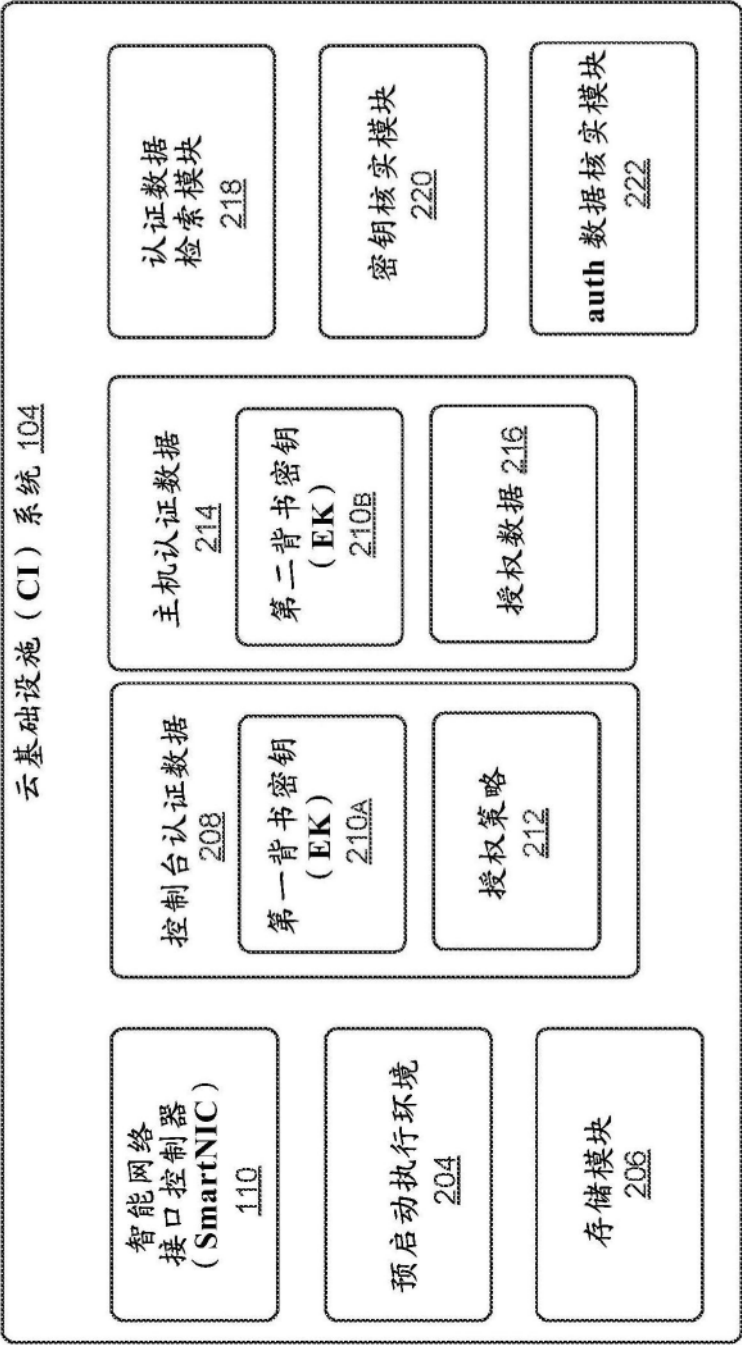


图2

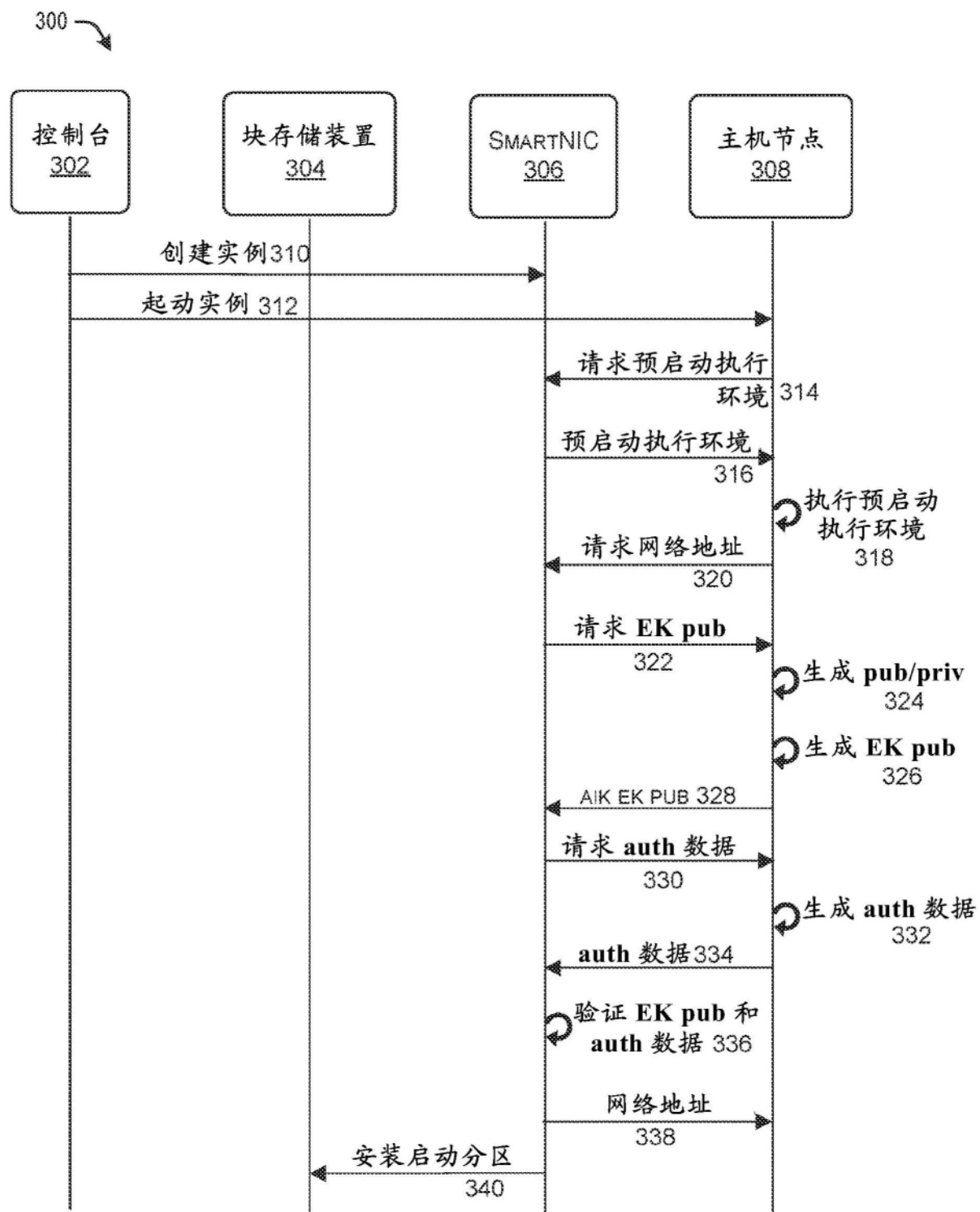


图3

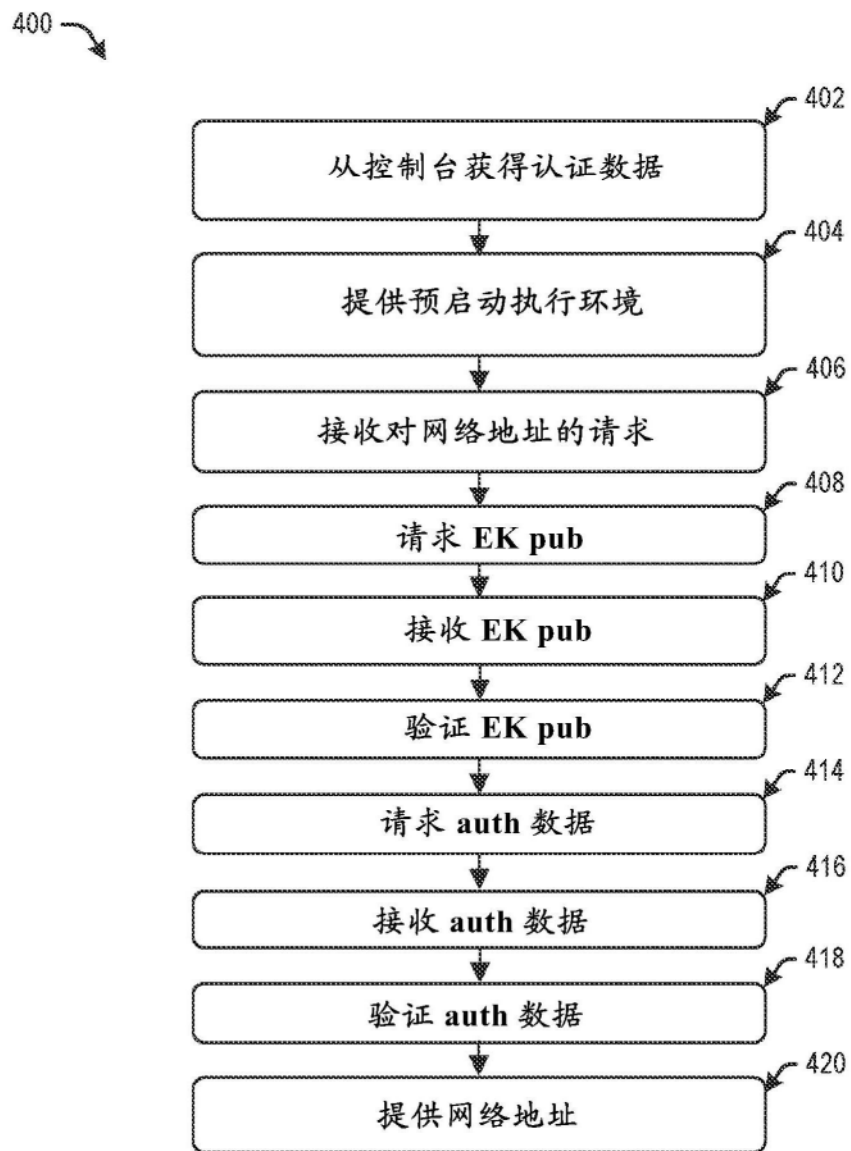


图4

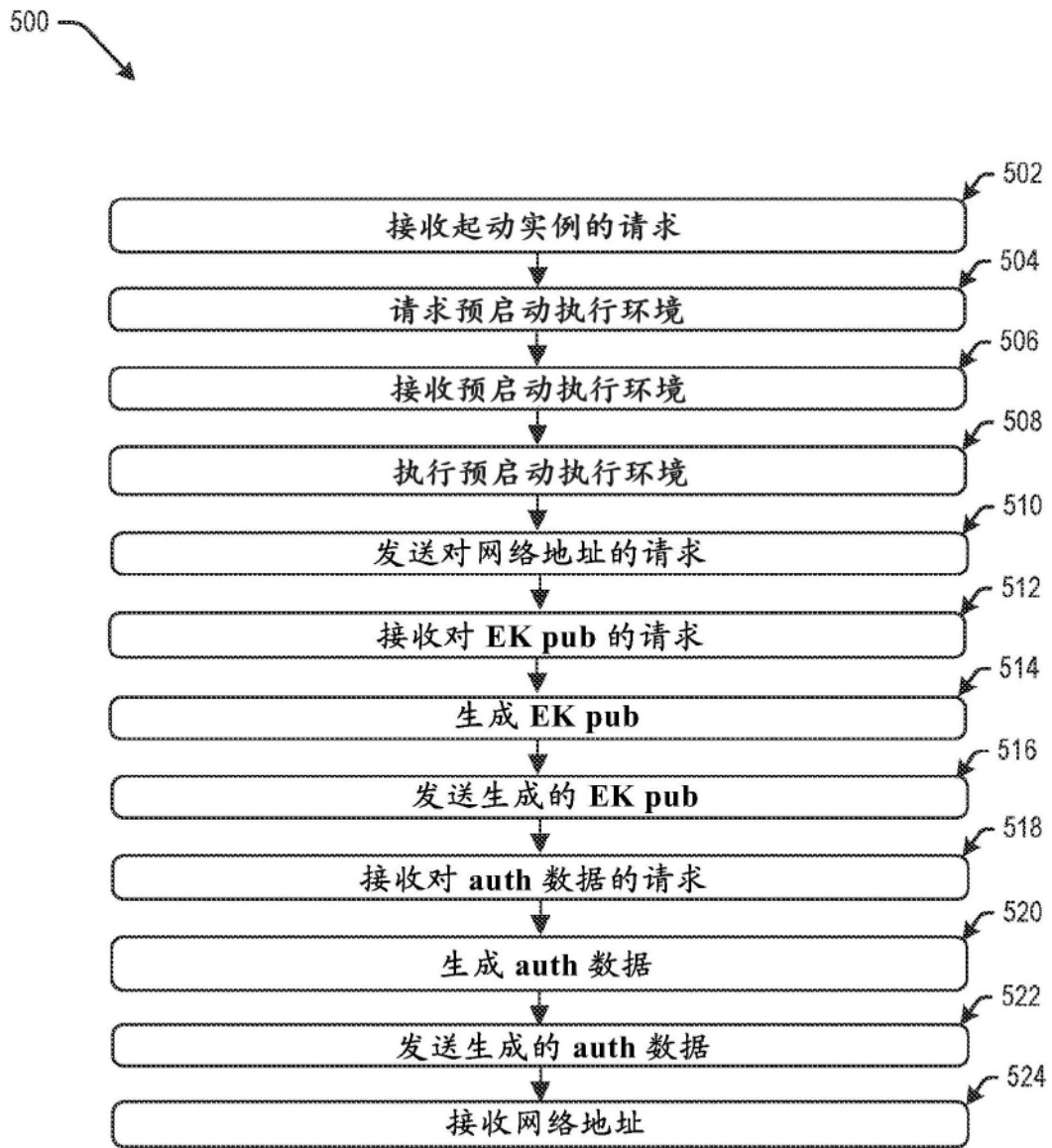


图5

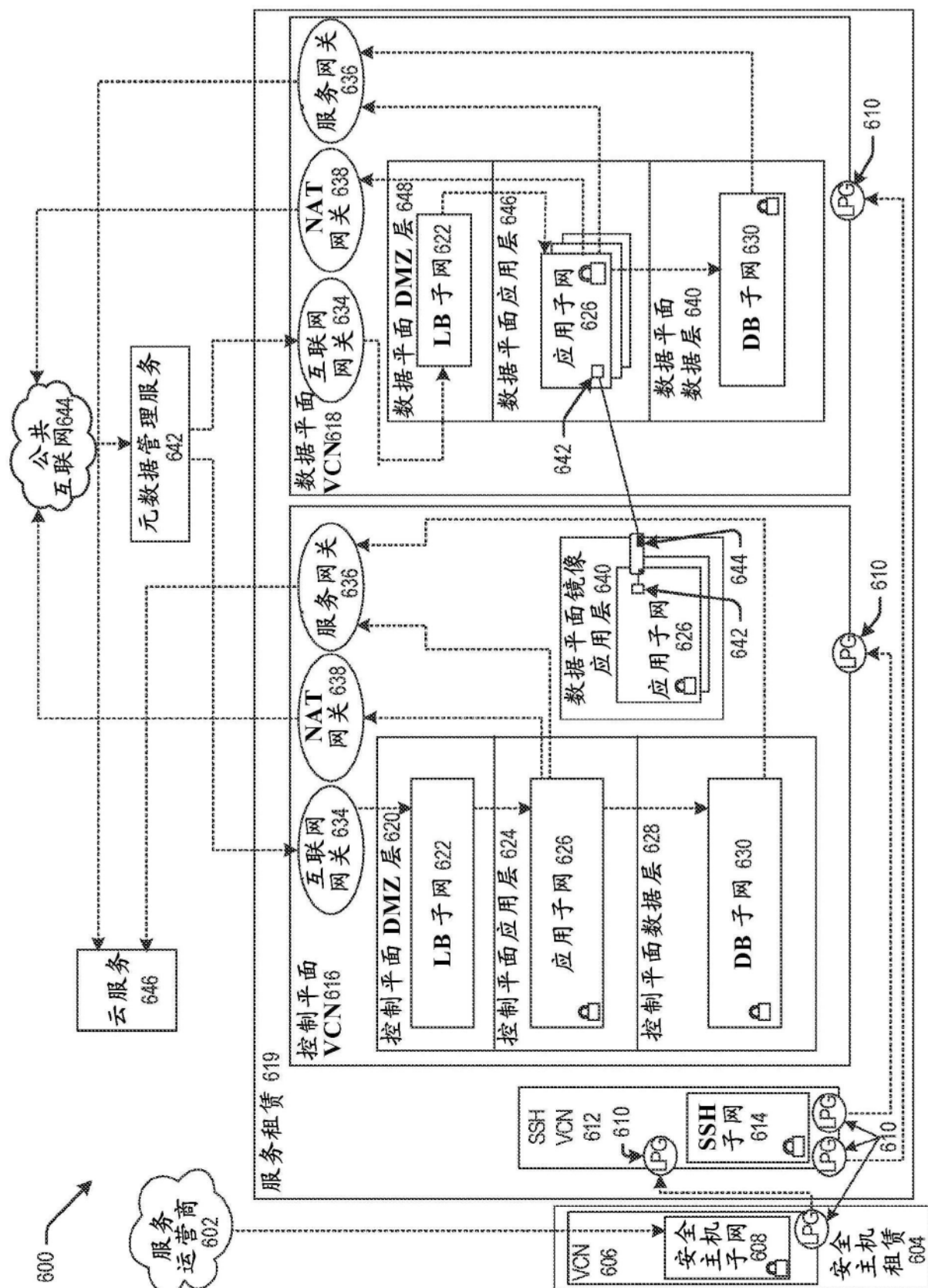


图6

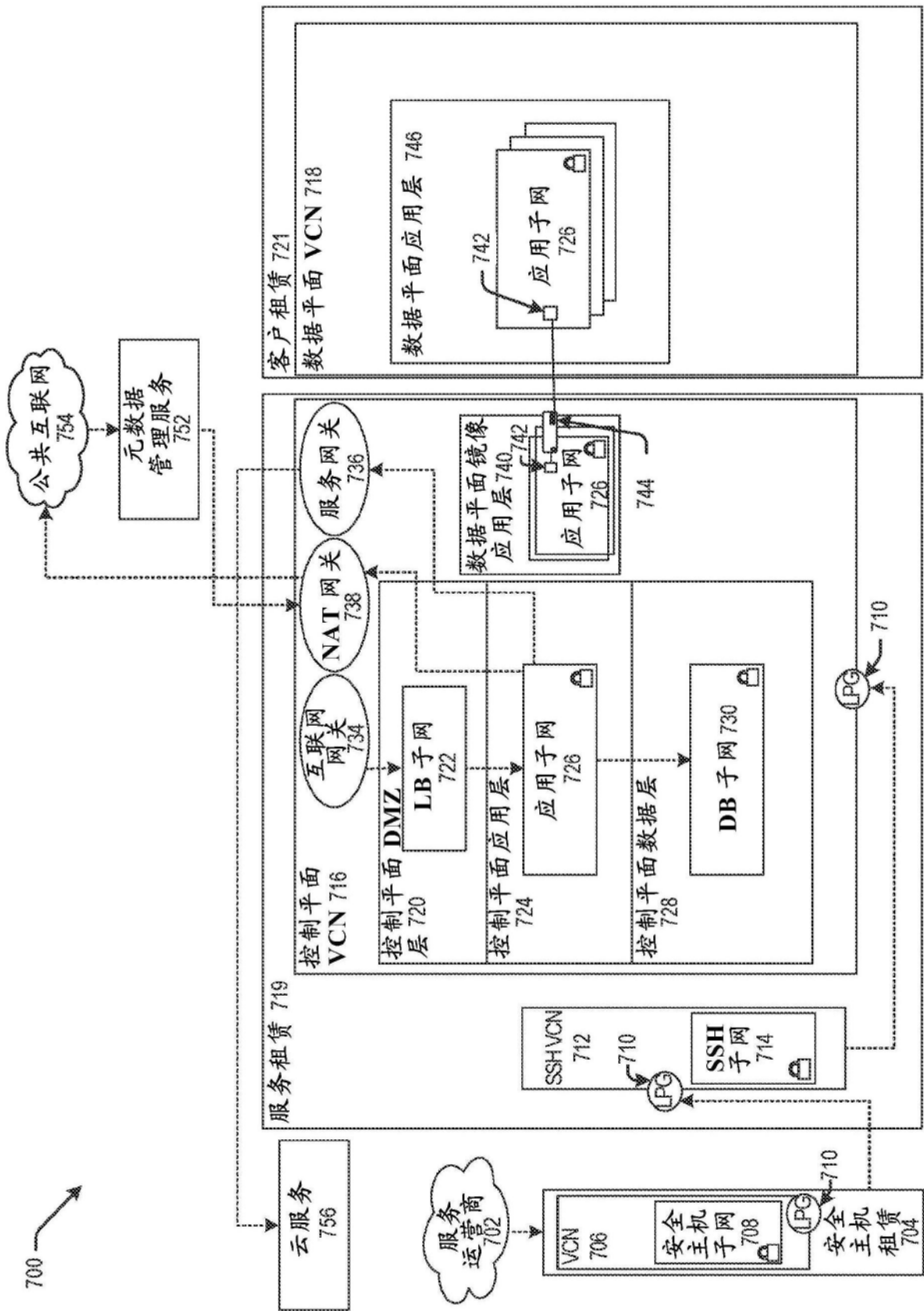


图7

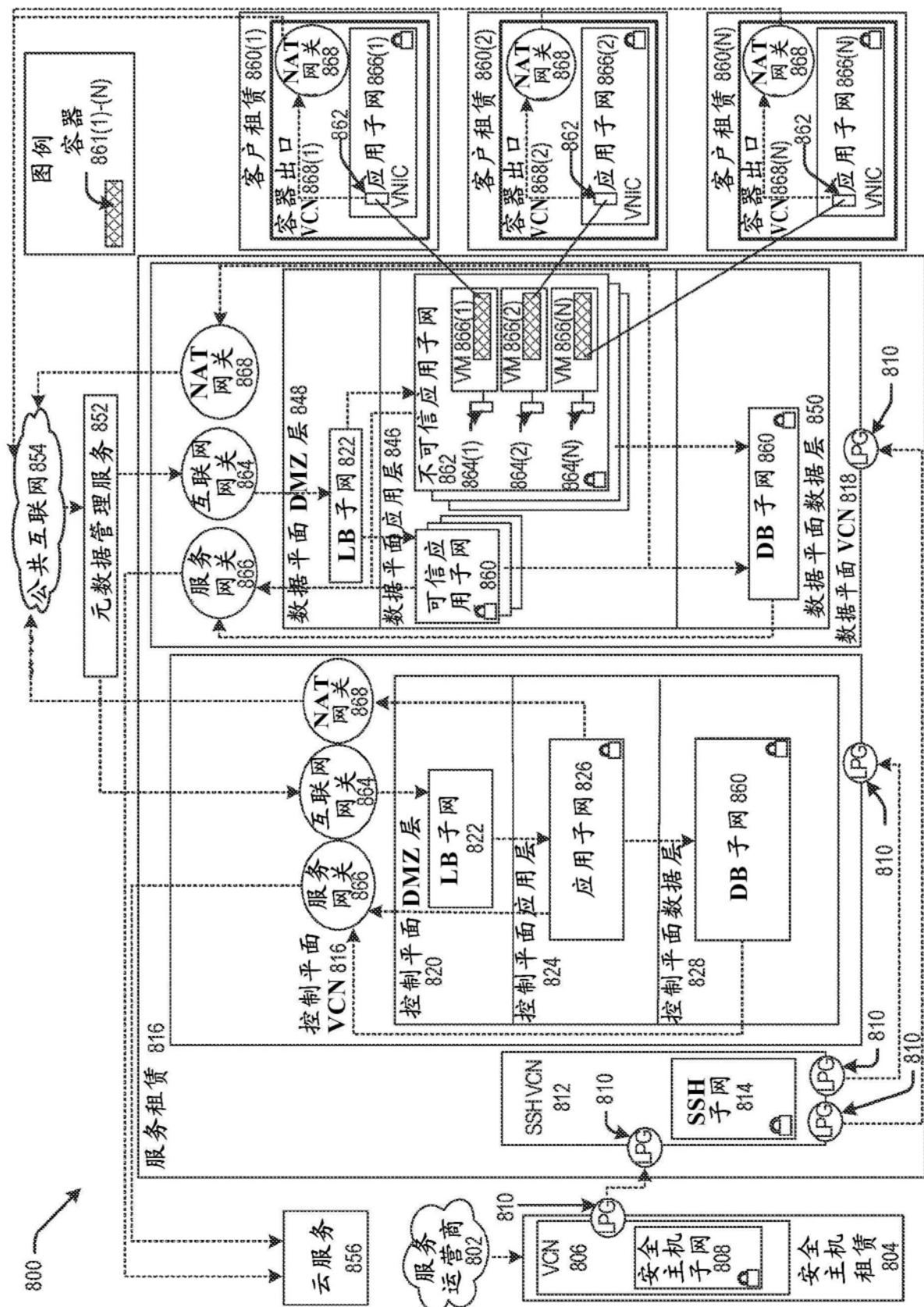


图8

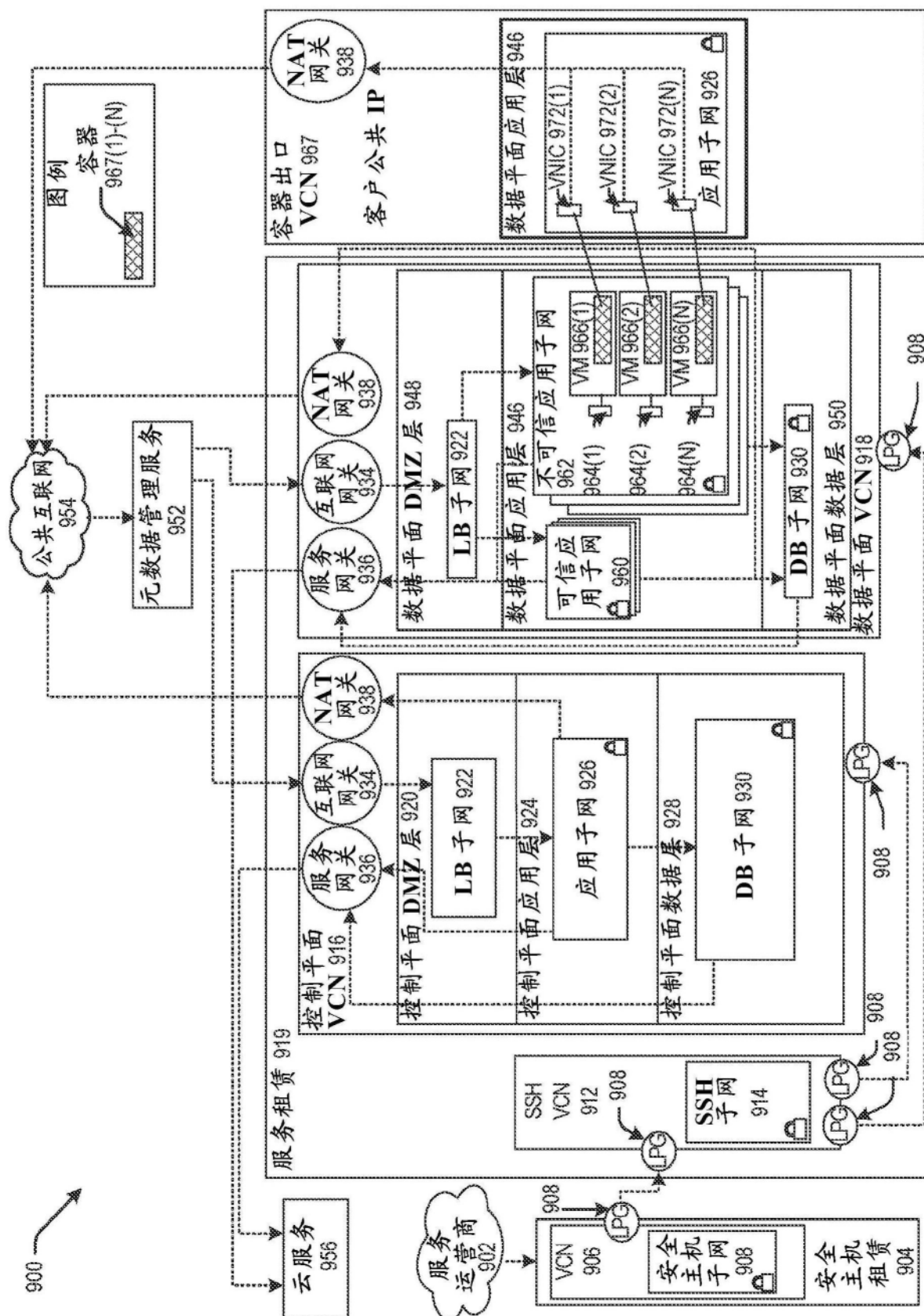


图9

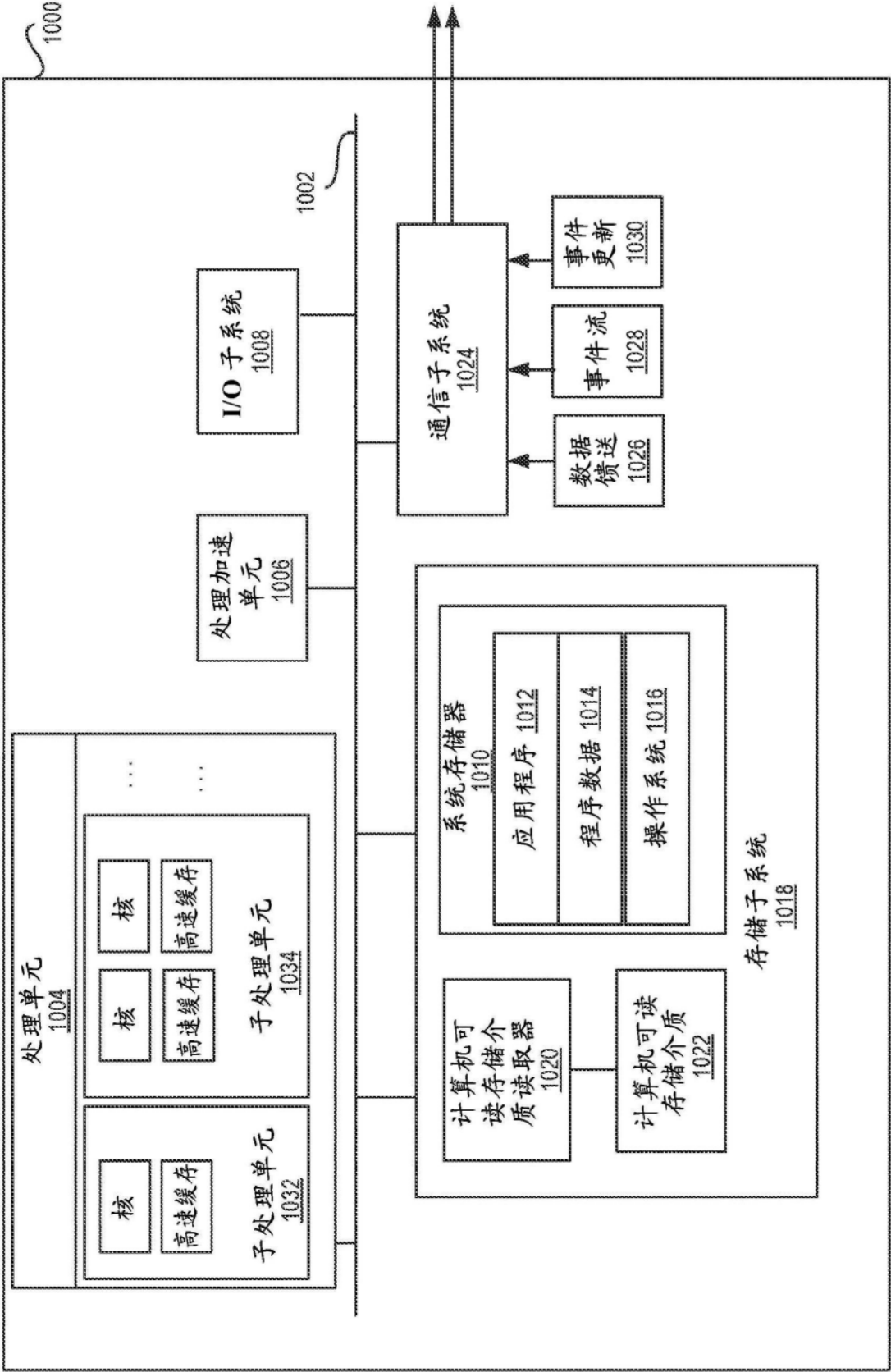


图10