(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108351937 A
(43)申请公布日 2018.07.31

(21)申请号 201680067500.4

(22)申请日 2016.11.16

(30)优先权数据
62/269,666 2015.12.18 US
15/060,844 2016.03.04 US

(85)PCT国际申请进入国家阶段日
2018.05.18

(86)PCT国际申请的申请数据
PCT/US2016/062139 2016.11.16

(87)PCT国际申请的公布数据
WO2017/105733 EN 2017.06.22

(71)申请人 英特尔公司
地址 美国加利福尼亚

(72)发明人 Y·拉古拉姆 S·M·巴勒 N·T·库克 K·索德

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 21/53(2006.01)
G06F 21/57(2006.01)

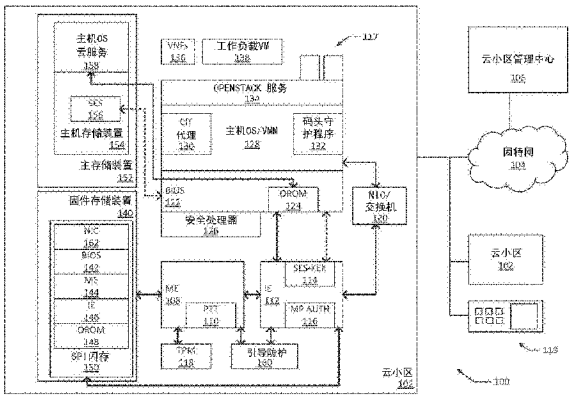
权利要求书2页 说明书15页 附图9页

(54)发明名称

计算设备

(57)摘要

本文公开了与云环境中的安全性有关的实施例。在一些实施例中，例如，计算设备(例如，微云)可以包括：可信执行环境；基本输入/输出系统(BIOS)，用于从可信执行环境请求密钥加密密钥(KEK)；以及与KEK相关联的自加密存储装置(SES)；其中所述可信执行环境验证所述BIOS并且在验证所述BIOS之后将所述KEK提供给所述BIOS，并且所述BIOS将所述KEK提供给所述SES以对所述SES解锁以由所述可信执行环境访问。



CN 108351937 A

1.一种计算设备,包括:

可信执行环境;

基本输入/输出系统(BIOS),其用于从所述可信执行环境请求密钥加密密钥(KEK);以及

与所述KEK相关联的自加密存储装置(SES);

其中,所述可信执行环境用于验证所述BIOS并且在验证所述BIOS之后将所述KEK提供给所述BIOS,并且所述BIOS将所述KEK提供给所述SES以对所述SES解锁以由所述可信执行环境访问。

2.如权利要求1所述的计算设备,其中,所述可信执行环境是用于所述计算设备的信任根。

3.如权利要求1所述的计算设备,其中,所述可信执行环境包括处理资源,所述处理资源是与所述计算设备上的操作系统的执行相隔离的硬件和软件。

4.如权利要求1所述的计算设备,其中,所述计算设备是微云。

5.如权利要求1-4中任一项所述的计算设备,其中,所述可信执行环境用于与远程管理计算设备通信以接收更新。

6.如权利要求5所述的计算设备,其中,所述可信执行环境包括生命周期管理器,其用于通过RESTful接口与所述远程管理计算设备进行通信。

7.如权利要求6所述的计算设备,其中,所述生命周期管理器用于模拟将配置参数公开给另一计算设备的只读设备。

8.如权利要求6所述的计算设备,其中,所述生命周期管理器用于模拟将日志或诊断信息公开给另一计算设备的只读设备。

9.如权利要求1-4中任一项所述的计算设备,还包括虚拟化网络功能(VNF)逻辑。

10.如权利要求1-4中任一项所述的计算设备,还包括虚拟机(VM)逻辑。

11.一种联网计算系统,包括:

微云,包括:

可信执行环境,

基本输入/输出系统(BIOS),其用于从所述可信执行环境请求密钥加密密钥(KEK),以及

与所述KEK相关联的自加密存储装置(SES),

其中,所述可信执行环境将所述KEK提供给所述BIOS,并且所述BIOS将所述KEK提供给所述SES以对所述SES解锁以由所述可信执行环境访问;以及

微云管理中心,其远离所述微云、与所述可信执行环境通信。

12.如权利要求11所述的联网计算系统,其中,所述联网计算系统是移动边缘计算(MEC)系统。

13.如权利要求11所述的联网计算系统,其中,所述联网计算系统是第五代移动网络(5G)系统。

14.如权利要求11所述的联网计算系统,还包括与所述微云管理中心通信的多个微云。

15.如权利要求11-14中任一项所述的联网计算系统,其中,所述可信执行环境是运营商信任根。

16.如权利要求11-14中任一项所述的联网计算系统，其中，所述可信执行环境是制造商信任根。

17.如权利要求11-14中任一项所述的联网计算系统，其中，所述可信执行环境在所述微云的操作系统继续执行的同时从所述微云管理中心接收更新映像。

18.一种用于安全存储访问的方法，包括：

由计算设备的可信执行环境来验证所述计算设备的基本输入/输出系统(BIOS)；

响应于验证所述BIOS，由所述可信执行环境向所述BIOS提供用于所述计算设备的自加密存储装置(SES)的密钥加密密钥(KEK)；以及

由所述BIOS向所述SES提供所述KEK以对所述SES解锁。

19.如权利要求18所述的方法，其中，所述SES包括硬盘驱动器。

20.如权利要求18-19中任一项所述的方法，其中，平台固件被存储在所述SES中。

21.一个或多个具有存储于其上的指令的非暂时性计算机可读介质，所述指令响应于由计算设备的基本输入/输出系统(BIOS)执行而使所述计算设备用于：

请求用于所述计算设备的自加密存储装置(SES)的密钥加密密钥(KEK)；

响应于对所述BIOS的验证，从所述计算设备的可信执行环境接收所述KEK；以及

提供所述KEK以对所述SES解锁。

22.如权利要求21所述的一个或多个非暂时性计算机可读介质，其中，所述SES被分区，并且提供所述密钥以对所述SES解锁包括提供所述密钥以对与所述KEK相关联的所述SES的分区解锁。

23.如权利要求21所述的一种或多种非暂时性计算机可读介质，其中，固件配置信息被存储在所述SES中。

24.如权利要求21-23中任一项所述的一个或多个非暂时性计算机可读介质，其中，所述SES使用所述KEK来对媒体加密密钥(MEK)解锁，并且所述MEK对存储在所述SES中的数据进行加密。

25.如权利要求21-23中任一项所述的一个或多个非暂时性计算机可读介质，其中，所述计算设备是移动边缘计算(MEC)网络中的边缘服务器。

计算设备

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年12月18日提交的题为“SECURITY IN CLOUDLET ENVIRONMENTS”的美国临时专利申请第62/269,666号和于2016年3月4日提交的题为“COMPUTING DEVICES”的美国非临时专利申请第15/060,844号的优先权的利益,所述申请的全部内容均通过引用并入本文。

背景技术

[0003] 经由集中在房间或建筑物大小的远程数据中心中的处理和存储资源向终端用户提供许多计算应用。这些数据中心针对这些资源提供物理安全性,保护它们免受物理篡改或盗窃。

附图说明

[0004] 通过以下结合附图的详细描述将容易理解实施例。为了便于说明,相同的附图标记表示相同的结构元件。在附图的图中通过举例而非限制的方式来示出实施例。

[0005] 图1是根据各种实施例的包括一个或多个微云的联网计算系统的框图。

[0006] 图2是根据各种实施例的包括一个或多个微云中的微云生命周期管理器的联网计算系统的框图。

[0007] 图3是根据各种实施例的用于包括微云的移动边缘计算(MEC)的联网计算系统的框图。

[0008] 图4是根据各种实施例的用于包括微云的网络功能虚拟化(NFV)的联网计算系统的框图。

[0009] 图5示出了根据各种实施例的可信引导过程的第一阶段。

[0010] 图6示出了根据各种实施例的可信引导过程的第二阶段。

[0011] 图7示出了根据各种实施例的包括信任根测量的可信引导过程的第一阶段。

[0012] 图8示出了根据各种实施例的包括信任根测量的可信引导过程的第二阶段。

[0013] 图9是根据各种实施例的可用于实现本文公开的联网计算系统的各种组件的计算设备的框图。

具体实施方式

[0014] 传统的云计算系统通常将存储和处理资源定位在远离引导这些资源的用户设备的集中式数据中心中。这种安排的结果通常是跨网络的高延迟和大流量。但是,如果将这些存储和处理资源从集中式数据中心中取出,并移动靠近网络的“边缘”(用户设备所在的位置),则不再受到集中式数据中心的物理保护和监视,并且这些资源遭受实际损害的风险增加。特别是,这些资源可能会被窃取和/或被篡改,导致它们以不易于检测的不期望的方式进行表现。例如,“远程”处理资源可以经由因特网从远程站点下载受损的云平台固件、操作系统(OS)、软件虚拟化网络功能(VNF)更新和/或补丁,并且这种损害可能未被发现。在另一

个示例中，黑客可能获得对竞争资源的物理访问并篡改它，使其运行在受损状态。常规计算系统不能信任运行在远程计算资源上的软件(例如，固件、OS等)没有受到损害。

[0015] 本文公开了用于在物理安全性不能保证的环境中针对微云(cloudlet)提供耐篡改或防篡改安全性的方法和装置。本文公开的微云可以提供“盒中云系统，其提供云计算系统功能而不需要连接回到传统云环境的硬连接并且其满足服务提供商期望的其常规基于数据中心的云资源的安全性要求”。本文公开的各种实施例可涉及整个操作平台的硬件实施的引导完整性方案和信任链的创建。

[0016] 在一些实施例中，本文公开的微云可以使得网络功能虚拟化(NFV)和软件定义网络(SDN)运营商能够将他们的云服务的基础结构扩展到更接近其订户，实现性能和延迟方面的改进而不损害安全性和可靠性。本文公开的各种实施例在移动边缘计算(MEC)(例如，欧洲电信标准协会(ETSI)MEC)、雾计算和云边缘计算应用中可能是特别有利的。例如，本文公开的微云可以支持第五代移动网络(5G)和MEC能力的安全实现及其相关的使用场景。

[0017] 在下面的详细描述中，参考构成其一部分的附图，其中类似的附图标记始终表示类似的部分，并且其中通过示例的方式示出了可以实践的实施例。应该理解，在不脱离本公开的范围的情况下可以利用其他实施例并且可以进行结构或逻辑改变。因此，下面的详细描述不是限制性的。

[0018] 各种操作可以以最有助于理解要求保护的主题的方式依次描述为多个离散的动作或操作。然而，描述的顺序不应被解释为暗示这些操作必须依赖于顺序。特别是，这些操作可以不按照所呈现的顺序执行。所描述的操作可以以与所描述的实施例不同的顺序来执行。可以执行各种附加操作，并且/或者在附加实施例中可以省略所描述的操作。

[0019] 为了本公开的目的，短语“A和/或B”意指(A)、(B)或(A和B)。为了本公开的目的，短语“A、B和/或C”意指(A)、(B)、(C)、(A和B)、(A和C)、(B和C)、或(A，B和C)。该描述使用短语“在一个实施例中”或“在实施例中”，其可以分别指代相同或不同的实施例中的一个或多个。此外，关于本公开的实施例使用的术语“包括”、“包含”、“具有”等是同义的。附图不一定按比例绘制。

[0020] 图1是根据各种实施例的包括一个或多个微云102的联网计算系统100的框图。如本文所使用的，“微云”可以指包含在单个外壳(或少量外壳)中以提供数据存储、处理和/或分发功能的计算资源(例如，存储器、处理器和联网设备)。在一些实施例中，微云可以充当小规模数据中心。在一些实施例中，如上所述，微云102可以在盒中提供基本全功能的云系统，而不需要连接回完整的云环境。系统100中的各种微云102可以部署在无法确保微云102的物理安全性的远程环境中(例如，在公共公园、街角、购物商场中)。系统100可以包括单个微云102或多个微云102(例如，数十个或数百个微云102)。以下参照图9讨论微云的示例实施例。

[0021] 通常，微云102可以运行虚拟功能、应用、工作负载以及数据存储和收集过程。在一些实施例中，微云102中的一个或多个可以运行一个或多个虚拟化网络功能(VNF)136。例如，VNF 136可以包括由长期演进(LTE)通信运营商提供的一个或多个VNF，诸如虚拟演进分组核心(vEPC)或虚拟客户终端设备(vCPE)。在一些实施例中，微云102中的一个或多个可以运行一个或多个工作负载虚拟机(VM)138。如本领域所知，每个工作负载VM 138可以提供操作系统(OS)以及运行在操作系统之上的应用的独立实例化。运行在工作负载VM138中的应

用可以是任何合适的应用，例如视频高速缓存、转码等。VNF 136和工作负载VM 138可以利用在主机OS/虚拟机管理器(VMM)128上运行的一组OpenStack服务134，并且主机OS/VMM 128可以包括码头守护程序132(例如，用于容器管理)，如本领域中已知的。一个或多个容器117也可以运行在微云102上，提供操作系统级虚拟化，如本领域所知(例如，用于高性能计算应用)。本文公开的安全技术可以在没有集中式数据中心的物理安全性的情况下安全地启用微云102的这些能力(通过例如使用密钥和密文)。

[0022] 微云102可以包括多个安全组件。例如，微云102可以包括可管理性引擎(ME)108。例如，ME 108可以包括融合安全性和可管理性引擎(CSME)。ME 108可以是独立的可信执行环境并且可以充当微云102的制造商的信任根(例如，针对制造商控制的引导过程提供安全环境)。例如，可信执行环境可以提供可以以比主机OS/VMM 128提供的安全级别更高安全级别来执行代码的一个或多个处理器和存储器设备。在一些实施例中，可信执行环境可以与主机OS/VMM 128的操作硬件和/或软件隔离(例如，通过加密)，并且因此可以与作为主机OS/VMM 128的一部分执行的代码隔离地执行代码。在一些实施例中，可信执行环境可以是微云102中的安全处理器126的安全区域，并且在可信执行环境中执行的代码可以安全地免受在主机OS/VMM 128中执行的代码的篡改。

[0023] 在一些实施例中，ME 108可以是运行制造商可信和主机独立OS的安全服务处理器。ME 108可以利用各种平台协议和硅功能(如智能平台管理接口(IPM I)、平台环境控制接口(PECI)和主机嵌入式控制器接口(HECI))将外部管理系统连接到平台。在一些实施例中，ME 108可以经由安全结构(例如，Intel片上系统结构(IOSF))与各种硬件组件连接。ME 108可以包括平台信任技术(PTT)组件110并且可以与可信平台模块(TPM)118通信。如本领域所知，TPM 118可以包括如下芯片(具有处理设备)，其可以安全地存储用于认证微云102的平台的数据。如本领域所知，PTT 110可以提供凭证存储和密钥管理功能，并且可以充当提供TPM功能作为ME 108上的应用的固件TPM(fTPM)。

[0024] 微云102可以包括创新引擎(IE)112。IE 112可以与ME 108进行通信，并且可以是单独的独立可信执行环境。具体而言，IE 112可以充当微云102(例如，电信设备制造商(TEM))的运营商(平台所有者)的信任根。IE 112可以按照运营商的特定固件来供应。在一些实施例中，IE 112可以包括运行由运营商信任的主机独立的OS的安全带外(OOB)服务处理器。IE 112可以包含来自运营商的引导映像和认证凭证(存储在例如熔丝和清单中)，并且可以存储用于执行IE 112内的特定应用或小应用的运营商授权方案。IE 112可以利用各种平台协议和硅功能(如IPM I、PECI和HECI)将外部管理系统连接到平台。在一些实施例中，IE 112可以经由安全架构(例如，IOSF)与各种硬件组件连接。IE 112可以将OOB可管理性接入点提供微云102的平台，并且可以可选地包括fTPM。在一些实施例中，IE 112可具有ME 108可能不具有的联网能力；例如，以太网接口和相关联网访问。IE 112还可以访问专用平台加速器，诸如现场可编程门阵列(FPGA)。

[0025] IE 112可以包括多方授权(MPA)组件116。在使用中，IE 112本身可以用签名的映像和签名的配置参数来安全引导，并且如上所述，可以充当针对运营商基础设施的硬件信任根(持有IE 112的OS和应用的安全凭证)。MPA组件116可以针对安全应用(例如，NFV运营商访问、遥测、监视、更新等)在IE 112内运行实现访问控制和显式授权。IE 112还可以负责验证使用平台凭证的任何UEFI/BIOS签名(存储在例如熔丝中)。IE 112可以存储用于自加

密存储(SES)156的密钥加密密钥(KEK)；该KEK在图1中表示为SES-KEK 114。在下面进一步详细讨论SES 156。ME 108和IE 112可以包括它们自己的处理器、加密运算核心、静态随机存取存储器(SRAM)等等。

[0026] 微云102可以包括引导防护组件160。引导防护组件160可以提供基于硬件的引导完整性保护以防止未经授权的软件和恶意软件接管微云102的引导块。在一些实施例中，引导防护组件160可以包含在认证代码模块(ACM)中。ACM是被配置为调用适当的CPU指令来执行引导防护测量和验证的固件。ACM代码可以是由制造商或另一可信实体签名的特权代码。在一些实施例中，ACM可以是下面讨论的安全处理器126的一部分。引导防护组件160可以提供测量的引导，其中初始引导块被测量到TPM 118或PTT 110中，或者提供验证的引导，其中使用引导策略密钥来对初始引导块进行密码验证。引导防护组件160可由微云102的中央处理单元(CPU)利用以在引导期间引导并触发签署和验证过程。在CPU启动开始之前，ME 108和IE 112可以由硬件验证。

[0027] 微云102可以包括安全处理器126。安全处理器126可以是安全增强的通用处理器。在一些实施例中，安全处理器126可以包括软件防护扩展(SGX)组件(未示出)以向安全处理器126提供一组指令，这组指令可以由应用用于将代码和数据的私有区域留在“安全飞地”。在一些实施例中，安全处理器126可以包括可信测量服务以执行证明以确保所有系统组件都被授权。例如，安全处理器126可以包括可信执行技术(TXT)组件(未示出)以针对微云102的每个经批准的启动启用组件创建加密的唯一标识符，并且然后提供基于硬件的强制机制以阻止启动与批准代码不匹配的代码。例如，TXT组件可以由ACM来实现。在一些实施例中，安全处理器126可以是x86处理器。

[0028] 微云102可以包括基本输入/输出系统(BIOS)122，BIOS 122继而可以包括选项只读存储器(OROM)124。BIOS 122可以是统一可扩展固件接口(UEFI)BIOS，并且OROM 124可以是UEFI OROM。如下面所讨论的，OROM 124可以被实现为由BIOS 122加载的固件，并且可以由BIOS 122使用以使得ME 108和IE 112能够读取SES 156中的数据。BIOS 122可以由ME 108认证。在一些实施例中，BIOS 122可以实现OROM 124(例如，UEFI OROM)的签名验证，以及用于微云102中的OS引导加载程序和OS映像。例如，UEFI安全引导过程可以由微云102的运营商在引导时提供OS引导加载程序和OS签名和验证，并且UEFI认证变量(例如，平台密钥(PK)、KEK、签名数据库(DB)和禁止签名数据库(DBX))可以存储在主机存储装置154的安全部分(例如，嵌入式多媒体卡(eMMC)或通用闪存装置(UFS)中的防回滚分区)中。在一些实施例中，OROM 124可以是由IE 112控制并存储在SPI闪存150中的UEFI可加载模块。在一些实施例中，OROM 124的有效载荷可以负责主要的主机存储管理和/或更新。

[0029] BIOS 122可使用由运营商供应给微云102的密钥(例如，SES-KEK 114)作为其认证变量的一部分。在一些实施例中，BIOS 122可将经认证的变量存储在SES 156的单独分区中。在一些实施例中，BIOS 122可将经认证的变量存储在主存储装置152的安全存储分区中(如下所述)，仅通过平台信任根(例如，ME 108)访问。

[0030] 主机OS/VMM 128可以包括云完整性技术(CIT)代理130。CIT代理130可以与安全处理器126的可信测量服务(例如，TXT)交互以启用BIOS 122、主机OS/VMM 128的OS和VMM，以及启动的任何VNF 136、VM 138或容器117的启动时间测量。在一些实施例中，引导防护160、CIT代理130和安全处理器126的可信测量服务(例如，TXT)可一起提供可信的、经验证和测

量的引导，一直到在微云102上运行的应用或服务。

[0031] 在一些实施例中，如以下参考图5-图8详细讨论的，微云102可以执行安全且可信的引导过程。该引导过程可以包括将SES-KEK 114释放到SES 156以完成引导过程。本文讨论的安全组件中的多个可以在该引导过程期间被利用，如下面详细讨论的，所述安全组件包括引导防护组件160、BIOS 122和主机OS/VMM 128的OS。

[0032] 微云102可以包括一个或多个网络接口控制器(NIC)/交换机120。NIC/交换机120可以与主机OS/VMM 128和IE 112通信，并且可以将数据路由到微云102/路由来自微云102的数据。在一些实施例中，安装到NIC/交换机120的所有固件和配置信息可以由ME 108、IE 112和/或安全处理器126的可信测量服务(例如，SGX)验证。这些固件和配置元素可以存储在SES 156中。在一些实施例中，NIC/交换机120可以是微云102的主处理器的一部分(例如，在中央处理单元(CPU)北部复合体中)或者芯片组(例如，平台控制器集线器(PCH)或南部复合体)中。在一些实施例中，NIC/交换机120可以在FPGA可编程逻辑模块中实现。在一些实施例中，NIC/交换机120可以位于微云102外部，并位于快速外围组件互连(PCIe)、光学或其他高速总线上。在一些实施例中，NIC/交换机120和微云102可以由不同的制造商制造。

[0033] 微云102可以包括固件存储装置140和主存储装置152。在一些实施例中，固件存储装置140可以包括串行外围接口(SPI)闪存150，但是可替代地或附加地包括例如eMMC。SPI闪存150可以包括BIOS固件存储装置142(用于BIOS 122)、ME固件存储装置144(用于ME 108)、IE固件存储装置146(用于IE 112)、NIC固件存储装置162(用于NIC/交换机120)和OROM固件存储装置148(用于OROM 124)。SPI闪存150可以为针对主平台存储装置提供存储(例如，存储UEFI平台配置参数)。

[0034] 主存储装置152可以包括用于主机OS云服务的存储装置158和用于主机的存储装置154。主存储装置152可以存储主机OS的映像，并且可以以加密方式存储存储在主存储装置152中的所有映像。主存储装置154可以包括一个或多个SES 156；尽管以单数形式提到，但SES 156可以包括一个或多个SES设备。SES 156可以包括存储器设备(例如，硬盘驱动器)和在数据被写入存储器设备或从存储器设备写入时对数据进行加密/解密的硬件电路。存储器设备中的数据的加密/解密使用媒体加密密钥(MEK)来执行，其本身由KEK加密。例如，用于SES 156的KEK是IE 112中的SES-KEK114。SES 156可以用于OS。尽管在图1中分开示出，但是在一些实施例中，SES 156可以用于平台固件。在一些实施例中，主存储装置152可以具有双重冗余分区，使得如果分区失败，则微云102可以恢复到其冗余分区。

[0035] 在一些实施例中，SES 156可以被划分成分区，并且IE 112和/或ME 108可以根据需要递增地解锁这些分区(例如，使用不同的KEK)。KEK(例如，SES-KEK114)可以总是在IE 112和/或ME 108(或其他可信环境)内被保护，并且根据需要被编程到SES 156中。在一些实施例中，每个存储分区可以具有其自己的唯一加密KEK。在一些实施例中，KEK(例如，SES-KEK114)可以由IE 112和/或ME 108安全地包装，并被传递到运营商的安全命令中心或微云102的基础设施所有者。例如，安全命令中心可以使用包装的KEK进行审计和托管。

[0036] 主存储装置152和/或固件存储装置140可以是安全存储装置，诸如安全回滚保护的eMMC和/或安全闪存分区。例如，该安全存储装置可用于存储平台固件、OS引导加载程序和OS组件。在一些实施例中，微云102的安全存储装置可以用于存储可用于检查正确版本是否到位的平台固件、OS引导加载程序和/或OS识别信息。此类OS识别信息的示例包括版本、

安全版本、OS的组成(例如,Openstack映像、存储和联网服务)、授权签名者以及认证变量等等。“版本”可以指区分软件的不同版本的账面价值。“安全版本”可以指在软件、固件或其他相关组件中检测到安全策略违规时更改的值。例如,软件可以具有为1的安全版本,直到发现安全问题,此时安全版本可能会更新为2(并且在此新安全版本之前的所有安全版本可能被视为易受攻击)。“认证变量”可以指安全签名数据库变量,例如签名密钥、授权数据库、密钥分层结构、更新日志等。当BIOS 122是UEFI BIOS时,这些认证变量由UEFI定义。在一些实施例中,可以将安全存储装置以密码方式绑定到平台硬件信任根(例如,ME 108、IE 112和/或安全处理器126的可信测量服务(例如,SGX))。安全存储装置可以绑定到微云102的平台,并且在一些实施例中,任何物理篡改都可能使平台无法引导。在一些实施例中,微云102的平台不可以在没有安全存储装置的情况下引导。

[0037] 如图1所示,微云102可以与一个或多个另外的微云102通信。可以根据上面讨论的任何实施例来配置这些另外的微云102。在一些实施例中,微云102可能不与任何其他微云102通信。微云102还可以经由因特网104与微云管理中心106(其也可以被称为微云控制中心)进行通信。因特网104可以由网络设备、因特网连接、骨干光纤或将微云102耦合到微云管理中心106的任何其他网络硬件组成。在一些实施例中,一个或多个微云102可以与一个或多个网络基础设施组件119(例如,架顶式交换机或路由器)进行通信。

[0038] 微云管理中心106可以提供用于管理系统100中的微云102的基础架构即服务(IAAS)。使用微云管理中心106来管理微云102可以允许系统100以较低的总拥有成本(TCO)和大规模部署能力实施。在一些实施例中,微云管理中心106可以包括安装和配置管理电路以向微云102提供适当的软件和配置信息。当在微云102上运行的主机OS或应用将被更新时,微云管理中心106中的远程管理和遥测电路可以使用专用的带外机制来与微云102进行通信。例如,NIC/交换机120的一个端口可以被指派为作为该带外机制来操作,并且可以在微云102和微云管理中心106之间提供安全和可靠的通道。包括更新的新映像可以由微云管理中心106下推到微云102,并且IE 112可以调用OROM 124以提供IE 112对主存储装置152中的SES 156的存取以存储新映像。当经由带外机制将新映像下推到微云102时,主机OS/VMM 128可以继续运行,从而使得由更新引起的停机时间最小化。在其他实施例中,在IE 112和主存储装置152之间,和/或在ME 108和主存储装置152之间可以存在直接连接(例如,主存储装置152可以包括用于与IE 112及ME 108通信的多个头)。以这种方式,用于主存储装置152的控制器可以使得主机OS/VMM 128、IE 112和/或ME 108充当不同的“代理”以连接到主存储装置152并且将其用于读/写。

[0039] 在一些实施例中,系统100中包括的微云102中的多个上的OS映像可以是相同的,并且微云102的身份可以由托管在安全伪通用串行总线(USB)(或伪PCIe)设备上的配置文件来确定。伪设备可以提供一组类似设备的操作,而无需通常与这种设备相关联的硬件,来增强现有设备的功能或访问微云102的子系统。在一些实施例中,伪设备可以由伪设备驱动程序实现,该伪设备驱动程序可以是如下内核的一部分,其充当设备驱动程序但不对应于微云102中的任何“实际”设备硬件。特别地,安全且可信的引导过程(诸如下面参考图5-图8所讨论的过程)可以被构建为将配置信息作为USB(或PCIe)总线上的伪设备公开,并且使IE 112安全地更新关于设备的信息。在一些实施例中,这样的实施例可以包括使OROM 124将相关存储装置安装为USB或PCIe设备,并且在IE 112中具有USB或PCIe重定向控制器。加密的

静态存储装置的存在可以限制物理攻击的风险。

[0040] 图2是根据各种实施例的包括一个或多个微云102中的微云生命周期管理器170的联网计算系统100的框图。微云生命周期管理器170可以嵌入在微云102中。在一些实施例中，微云102的微云生命周期管理器170可以位于IE 112中。如图2所示，每个微云102可以与微云管理中心106通信。特别地，微云生命周期管理器170可以与微云管理中心106的安装和配置管理电路以及远程管理和遥测电路进行通信，如上文讨论的。在操作期间，微云102的平台遥测电路可以与包括在ME 108中的遥测集线器(其如本文所讨论的可以包括固件TPM 118)通信，并且ME 108可以与IE 112中的微云生命周期管理器进行通信。每个微云102还可以与由电信公司或其他服务提供商提供的云系统174进行通信以执行NFV和SDN操作。云系统174可以具有其自己的数据中心176，其可以采用传统的云计算数据中心形式。每个微云102还可以与云应用分发设备172通信，云应用分发设备172可以将用于特定应用的软件提供给微云102。

[0041] 微云生命周期管理器170可以与微云管理中心106交互，以允许在微云102和微云管理中心106之间的安全交换，而不存在中间人或欺骗安排的可能性。例如，在一些实施例中，微云生命周期管理器170可以模拟只读设备并且可以将该模拟的只读设备公开给主服务器(例如，系统100中的微云管理中心106或微云102)。该模拟的设备可以包括配置参数，其可以作为主服务器上的操作应用软件已知的文件或其他数据形式来公开。微云生命周期管理器170可以将应用编程接口(API)公开给微云管理中心106以允许对模拟设备的内容进行安全更新。微云生命周期管理器170因此可以提供节点配置伪设备。

[0042] 在另一个示例中，在一些实施例中，微云生命周期管理器170可以模拟日志记录设备并且可以将该模拟的只读设备公开给主服务器。写入该设备的信息可以作为记录器诊断信息由微云生命周期管理器170安全地呈现给微云管理中心106。微云生命周期管理器170可以基于来自微云管理中心106的配置或策略设置来过滤发送到微云管理中心106的日志信息。

[0043] 在另一个示例中，一旦微云102的平台已经被完全验证，则微云102可以将带外证明级别公开给外部系统。该带外证明级别可以代表微云102的测量的安全性。例如，“五星”证明级别可以表示微云102的固件、OS引导、密钥和配置如预期那样。“四星级”证明级别可以表示微云102大部分但并非完全如预期的那样(例如，固件是落后的版本)。“0星”证明级别可能表示完全失败(例如，测量的引导与期望值不匹配)。

[0044] 在一些实施例中，微云生命周期管理器170可以经由RESTful接口与微云管理中心106的远程管理和遥测电路进行通信。该接口可以使用JavaScript对象符号(JSON)数据格式，并且在一些实施例中，可以是安全超文本传输协议(HTTPS)接口(例如，根据用于客户端/服务器认证的X.509标准)。

[0045] 如上所述，在一些实施例中，本文公开的微云102可以被包括在MEC布置中。图3是根据各种实施例的用于包括微云102的移动边缘计算(MEC)的联网计算系统100的框图。在图3的系统100中，用户设备178可以表示任何终端设备，诸如智能电话、其他个人计算设备、物联网(IoT)设备、车辆或传感器。示出单个用户设备178以便于说明，并且系统100可以包括多个用户设备178。小型小区180可以与用户设备178进行通信，并且可以表示小型无线网络集线器(例如，Wi-Fi集线器、第三代合作伙伴计划(3GPP)天线等)。根据本文公开的任何

实施例，小型小区180可以耦合到MEC平台182，而MEC平台182可以包括微云102。可以在MEC平台182处执行端接，并且微云102可以提供VNF 136以用于手机端接、信令、数据平面和应用。MEC平台182可以与可以具有MEC核心节点186的移动核心184通信。MEC平台182和移动核心184之间的通信可以包括回程链路、路由器、交换机以及任何其它合适的硬件，如本领域所知的。移动核心184可以包括例如LTE骨干网络。MEC核心节点186然后可以与因特网104通信，因特网104继而可以与诸如内容递送、内容分析、车辆监视、其他传感器的监视、紧急服务等的多种服务(未示出)中的任何服务耦合。该架构可以与传统移动网络形成对比，在传统移动网络中小型小区180经由不具有用于提供云计算服务的能力的eNB耦合到移动核心184。

[0046] 图4是根据各种实施例的用于包括微云102的网络功能虚拟化(NFV)的联网计算系统100的框图。在图4的系统100中，微云102可以担当NFV基础设施(NFV)的角色，并且微云管理中心106可以被包括在NFV管理和编排(NFV MANO)组件中。在一些实施例中，图1的微云102的所有组件可以被包括在NFVI中，除了OpenStack服务134、VNF136、工作负载VM138和容器117之外。

[0047] 如上所述，在一些实施例中，微云102可以执行安全且可信的引导过程。该引导过程可以包括将SES-KEK 114释放到SES 156以完成引导过程。图5和图6分别示出了可信引导过程的第一实施例的第一阶段和第二阶段，而图7和图8分别示出了可信引导过程的第二实施例的第一阶段和第二阶段。

[0048] 在图5-图8的可信引导过程中，与SES 156相关联的SES-KEK114受到ME 108和IE 112的保护，并且在适用时可以传递给BIOS 122。一旦成功认证和授权，SES-KEK114可以提供给SES 156用于自我解密和解锁。在接收SES-KEK 114之前，BIOS 122可能必须通过源自ME 108和/或IE 112的签名验证检查以及测量检查。BIOS 122可以包括用于对SES 156访问和解锁的机制。在一些实施例中，上述BIOS操作可以通过基于UEFI BIOS系统管理中断(SMI)的系统管理模式(SMM)模式来执行。在一些这样的实施例中，在SMM中执行的代码可以由ME 108和/或IE 112信任和验证为信任根。

[0049] 转到图5，示出了根据各种实施例的可信引导过程的第一阶段500。如下所讨论的，第一阶段500可以是用于硬件和BIOS的测量和验证阶段。在系统上电之后，在502处，微码可以验证并测量引导保护(BtG)160的认证代码模块(ACM)。结果可以被写入平台配置寄存器(PC)。在504处，引导防护160的ACM可以验证BIOS 122，并且可以将结果写入PCR。在506处，ACM可证实并测量BIOS 122的初始化代码。结果可被写入PCR;如果证实失败，则该过程可能会中止。在508处，可以初始化安全处理器126的可信测量服务(例如，TXT)及其存储器，并且可以加载SMM。在510处，可以测量SMM和其他可信代码并将结果写入PCR。在512处，可信测量服务(例如，TXT)及其存储器的配置可以通过提供ENTERACCS:LockConfig指令来锁定。在514处，可以执行非关键代码。在516处，BIOS 122可以与IE 112通信以获得用于锁定的SES 156的SES-KEK 114。

[0050] 图6中所示的第二阶段600可以是各种其他组件(例如，信任引导(TBOOT)、OS、码头引擎等)的测量阶段。例如，TBOOT可以是可以调用TXT指令来测量OS或VM的“预内核”组件。转到图6，在602处，BIOS 122可将SES-KEK 114提供给SES 156。在604处，SES 156可使用SES-KEK114来对SES 156的MEK解密，从而对SES 156解锁。如果SES 156的解锁失败，该过程

可以中止。在606处，可以加载SINIT和OS代码，并且可以提供SENTER指令(作为本领域中已知的TXT过程的一部分)。在608处，微码可以证实606的SINIT，并且可以将结果写入PCR。在610，SINIT可以测量TBOOT，并且可以将结果写入PCR。在612，SINIT可以测量OS内核initrd++，并且可以将结果写入PCR。在614处，Tboot-xm可以测量应用、配置数据、码头守护程序和/或其他OS组件，并且可以将结果写入PCR。在614处测量的组件可以是可配置的。在616，OS可以被启动。

[0051] 在图5和图6中示出的可信任引导过程可以提供对微云102的平台的远程安全访问，该访问包括使得ME 108和/或IE 112能够对SES 156解锁的授权凭证。SES-KEK 114对于受保护的固件永不可见，或在正常情况下被提取。在一些实施例中，为了运营商合规性，微云102的KEK可以使用高度特权的授权来取回。例如，IE 112和/或ME 108可以预先被提供有授权凭证，所述授权凭证可用于将KEK安全地递送到管理实体(例如，如图4所示的NFV虚拟化基础设施管理器)。

[0052] 图7和图8分别示出了可信引导过程的第二实施例的第一阶段和第二阶段。在图7和图8所示的可信引导过程中，还测量了信任根(例如ME 108和IE 112)。这可以适用于安全审计和合规性，以确保微云102的平台以已知的一组信任根固件/OS和已知的信任根配置来引导。

[0053] 如下所述，第一阶段700可以是针对硬件和BIOS的测量和验证阶段。转向图7的第一阶段700，在系统上电之后，在702处，可以执行ME ROM引导(例如，ME 108)和硬件初始化，并且可以将测量存储在内部SRAM中(例如，当TPM 118尚未准备好时)。在704处，可以执行IE ROM引导(例如，IE 112)和多方授权(例如，多方授权组件116)，并且可以将测量存储在内部SRAM中(例如，当TPM 118尚未准备好时)。在706处，微码可证实并测量BIOS 122的ACM，并且可将结果写入PCR。在708，ACM可证实并测量BIOS 122的初始化代码。结果可被写入PCR；如果证实失败，则该过程可以中止。在710处，可以初始化安全处理器126的可信测量服务(例如，TXT)及其存储器，并且可以加载系统管理模式(SMM)。如本领域中已知的，SMM可以是其中OS执行被挂起并且可信固件被执行的模式。在712处，可以测量SMM和其他可信代码，并将结果写入PCR。在714处，可信测量服务(例如，TXT)及其存储器的配置可以被锁定，并且可以提供ENTERACCS:LockConfig指令。在716，可以执行非关键代码。在718处，BIOS 122可以与IE 112通信以获得用于锁定的SES 156的SES-KEK 114。

[0054] 图8中所示的第二阶段800可以是各种其他组件(例如，TBOOT、OS、码头引擎等)的测量阶段。转到图8，在802处，BIOS 122可将SES-KEK114提供给SES 156。在804，SES 156可使用SES-KEK114来对SES 156的MEK解密，并且从而解锁SES 156。如果SES 156的解锁失败，该过程可以中止。在806，可以加载SINIT和OS代码，并且可以提供SENTER指令。在808处，微码可以验证806的SINIT，并且可以将结果写入PCR。在810处，SINIT可以测量TBOOT，并且可以将结果写入PCR。在812处，SINIT可以测量OS内核initrd++，并且可以将结果写入PCR。在814处，Tboot-xm可以测量应用、配置和码头数据，并且可以将结果写入PCR。在814处测量的组件可以是可配置的。在816，可以启动OS。

[0055] 图9是根据各种实施例的可用于实现本文公开的联网计算系统的各种组件的计算设备900的框图。例如，计算设备900的组件中的一些或全部可以被包括在微云102、微云管理中心106、用户设备178或云应用分发设备172中。多个元件在图9中示出为包括在计算设

备900中，但是这些元件中的任何一个或多个可以在适用于应用时而被省略或复制。

[0056] 另外，在各种实施例中，计算设备900可以不包括图9中所示的元件中的一个或多个，但是计算设备900可以包括用于耦合到一个或多个元件的接口电路。例如，计算设备900可以不包括显示设备906，但是可以包括显示设备906可以耦合到的显示设备接口电路(例如，连接器和驱动器电路)。在另一组示例中，计算设备900可以不包括音频输入设备924或音频输出设备908，但可以包括音频输入设备924或音频输出设备908可以被耦合到的音频输入或输出设备接口电路(例如，连接器和支持电路)。

[0057] 计算设备900可以包括处理设备902(例如，一个或多个处理设备)。如本文所使用的，术语“处理设备”或“处理器”可以指处理来自寄存器和/或存储器的电子数据以将该电子数据转换为可以存储在寄存器和/或存储器中的其他电子数据的任何设备或设备的一部分。处理设备902可以包括一个或多个数字信号处理器(DSP)、专用集成电路(ASIC)、中央处理单元(CPU)、图形处理单元(GPU)、密码处理器、服务器处理器或任何其他合适的处理设备。例如，处理设备902可以包括安全处理器126以及包括在微云102的ME 108和IE 112中的单独的处理器。计算设备900可以包括存储器904，存储器904本身可以包括一个或多个存储器设备，如易失性存储器(例如，动态随机存取存储器(DRAM))、非易失性存储器(例如，只读存储器(ROM))、闪存、固态存储器、SES和/或硬盘驱动器。例如，存储器904可以包括微云102的固件存储装置140和主存储装置152。

[0058] 在一些实施例中，计算设备900可以包括通信芯片912(例如，一个或多个通信芯片)。例如，通信芯片912可以被包括在微云102的NIC/交换机120中。例如，通信芯片912可以被配置用于管理用于向计算设备900传输数据和从计算设备900传输数据的无线通信。术语“无线”及其派生词可用于描述可通过使用经过非固体介质的调制电磁辐射来传送数据的电路、设备、系统、方法、技术、通信信道等。该术语并不意味着相关联的设备不包含任何线路，尽管在一些实施例中它们可能不包含线路。

[0059] 通信芯片912可以实现多种无线标准或协议中的任何一种，包括但不限于包括Wi-Fi(IEEE 802.11族)、IEEE 802.16标准(例如，IEEE 802.16-2005修正案)的电气和电子工程师协会(IEEE)标准、长期演进(LTE)项目以及任何修改、更新和/或修订(例如，高级LTE项目、超移动宽带(UMB)项目(也被称为“3GPP2”)等)。IEEE 802.16兼容宽带无线接入(BWA)网络通常被称为WiMAX网络，这是代表全球微波接入互操作性的首字母缩写，它是通过IEEE 802.16标准的符合性和互操作性测试的产品的认证标志。通信芯片912可以根据全球移动通信系统(GSM)、通用分组无线电服务(GPRS)、通用移动电信系统(UMTS)、高速分组接入(HSPA)、演进的HSPA(E-HSPA)或LTE网络来进行操作。通信芯片912可以根据增强型数据GSM演进(EDGE)、GSM EDGE无线电接入网络(GERAN)、通用陆地无线电接入网络(UTRAN)或演进型UTRAN(E-UTRAN)进行操作。通信芯片912可以根据码分多址(CDMA)、时分多址(TDMA)、数字增强无绳通信(DECT)、演进数据优化(EV-DO)及其派生物以及被指定为3G、4G、5G及以上的任何其他无线协议来进行操作。在其他实施例中，通信芯片912可以根据其他无线协议进行操作。计算设备900可以包括天线922以促进无线通信和/或接收其他无线通信(诸如AM或FM无线电传输)。

[0060] 在一些实施例中，通信芯片912可以管理诸如电气、光学或任何其他合适的通信协议(例如以太网)之类的有线通信。如上所述，通信芯片912可以包括多个通信芯片。例如，第

一通信芯片912可以专用于诸如Wi-Fi或蓝牙之类的较短距离无线通信，并且第二通信芯片912可以专用于诸如全球定位系统(GPS)、EDGE、GPRS、CDMA、WiMAX、LTE、EV-DO或其他之类的较远距离无线通信。在一些实施例中，第一通信芯片912可以专用于无线通信，并且第二通信芯片912可以专用于有线通信。

[0061] 计算设备900可以包括电池/电力电路914。电池/电力电路914可以包括用于将计算设备900的元件耦合到与计算设备900分离的能量源的一个或多个能量存储设备(例如电池或电容器)和/或电路(例如，AC线路电力)。

[0062] 计算设备900可以包括显示设备906(或者如上所述的相对应的接口电路)。例如，显示设备906可以包括任何视觉指示器，诸如平视显示器、计算机监视器、投影仪、触摸屏显示器、液晶显示器(LCD)、发光二极管显示器或平板显示器。

[0063] 计算设备900可以包括音频输出设备908(或者如上所述的相对应的接口电路)。例如，音频输出设备908可以包括生成可听指示符的任何设备，诸如扬声器、头戴式耳机或耳塞。

[0064] 计算设备900可以包括音频输入设备924(或者如上所述的相对应的接口电路)。音频输入设备924可以包括产生表示声音的信号的任何设备，诸如麦克风、麦克风阵列或数字乐器(例如具有乐器数字接口(MIDI)输出的乐器)。

[0065] 计算设备900可以包括全球定位系统(GPS)设备918(或者如上所述的相对应的接口电路)。如本领域所知，GPS设备918可以与基于卫星的系统通信并且可以接收计算设备900的位置。

[0066] 计算设备900可以包括其他输出设备910(或者如上所述的相对应的接口电路)。其他输出设备910的示例可以包括音频编解码器、视频编解码器、打印机、用于向其他设备提供信息的有线或无线发射器或附加存储设备。

[0067] 计算设备900可以包括其他输入设备920(或者如上所述的相对应的接口电路)。其他输入设备920的示例可以包括加速度计、陀螺仪、图像捕获设备、键盘、诸如鼠标之类的光标控制设备、指示笔、触摸板、条形码读取器、快速响应(QR)码读取器、任何传感器或射频识别(RFID)读取器。

[0068] 尽管本文讨论了可信执行环境的特定示例(例如ME 108和IE 112)，但这仅仅是为了说明的目的，并且可以使用任何期望的可信分区或环境(例如，SGX或SMM模式)来实现本文公开的实施例。

[0069] 在微云102的一些实施例中，ME 108、IE 112、安全处理器126(例如使用SGX和/或TXT)、SES 156、引导防护组件160和CIT代理130可以被一起使用以确保微云102的平台的固件和针对微云102的OS引导程序操作受到保护(例如，由ME 108和IE 112)并且SES-KEK 114(以及任何其他KEK)被存储和保护(例如，由ME 108和IE 112)。其结果是受信任和经验证的引导以及受硬件保护的经过认证的密钥访问。

[0070] 在微云102的一些实施例中，ME 108、IE 112、安全处理器126(例如，使用SGX)、UEFI安全引导(其中微云102的固件检查系统引导加载程序是用由包含在固件中的数据库授权的密钥来签名的)、安全熔丝(其中引导所需的密钥(例如，公共密钥哈希的初始集合)永久地被烧入硬件中的熔丝以提供硬件信任根)、安全封装(其中使用不允许公开存储在安全熔丝中的密钥的封装技术)和安全eMMC/存储(例如，在eMMC中使用具有防回滚保护的存

储装置，例如重放保护存储器块(RPMB))可以一起使用以确保微云102的平台在可信环境中被引导并且可操作，确保作为微云102上的伪USB(或PCIe)设备公开的配置信息能够被安全地访问和更新，并且该配置信息受到ME 108和IE 112的保护。

[0071] 在微云102的一些实施例中，ME 108、IE 112、安全处理器126(例如，使用SGX和/或TXT)、引导防护组件160和CIT代理130可一起使用以提供测量的引导和信任链以确保微云102(包括ME 108、IE 112以及静态和动态信任链)的证明是安全的(例如，不会受损)，并且确保带外证明级别可以公开给外部系统。

[0072] 在微云102的一些实施例中，ME 108和IE 112可一起用于以托管嵌入式微云生命周期管理器。嵌入式微云生命周期管理器可以模拟只读设备并且可以将该模拟的设备公开给主服务器。另外地或可选地，嵌入式微云生命周期管理器可以模拟日志记录设备并且可以将该模拟的设备公开给主服务器。

[0073] 本文公开的各个实施例可以提供优于常规方法的一个或多个优点。一些实施例可以在物理安全性不能被断言的环境中提供整个操作平台的硬件强制完整性和信任链。一些实施例可以提供安全且防篡改的微云，其在其平台生命周期的各个阶段保持安全、可信和被证明，而不需要数据中心的物理安全性。一些实施例可以提供对微云的操作状态和经证明的信任级别的非可欺骗的可见性。一些实施例可以允许基于“开放平台”的NFV和SDN解决方案以安全的方式部署在远程、无人和不受保护的站点。该解决方案可以针对运营商(例如MEC和5G)实现可以受益于远程、安全、分布式、独立数据处理的许多使用案例。一些实施例可以支持5G和/或IoT。

[0074] 以下段落提供了本文公开的各种实施例的示例。

[0075] 示例1是一种计算设备，包括：可信执行环境；基本输入/输出系统(BIOS)，用于从可信执行环境请求密钥加密密钥(KEK)；以及与KEK相关联的自加密存储装置(SES)；其中所述可信执行环境用于验证所述BIOS并且在验证所述BIOS之后将所述KEK提供给所述BIOS，并且所述BIOS用于将所述KEK提供给所述SES以解锁所述SES以由所述可信执行环境访问。

[0076] 示例2可以包括示例1的主题，并且还可以指定可信执行环境是用于计算设备的信任根。

[0077] 示例3可以包括示例1-2中的任何示例的主题，并且还可以指定可信执行环境包括在所述计算设备的操作系统的执行被挂起的模式下的操作。

[0078] 示例4可以包括示例1-3中的任一个的主题，并且还可以指定该计算设备是微云。

[0079] 示例5可以包括示例1-4中的任何一个的主题，并且还可以指定可信执行环境与远程管理计算设备通信以接收更新。

[0080] 示例6可以包括示例5的主题，并且还可以指定可信执行环境包括生命周期管理器，其用于通过RESTful接口与远程管理计算设备进行通信。

[0081] 示例7可以包括示例6的主题，并且还可以指定生命周期管理器用于模拟将配置参数公开给另一个计算设备的只读设备。

[0082] 示例8可以包括示例6的主题，并且还可以指定生命周期管理器用于模拟将日志或诊断信息公开给另一个计算设备的只读设备。

[0083] 示例9可以包括示例1-8中任一示例的主题，还包括虚拟化网络功能(VNF)逻辑。

[0084] 示例10可以包括示例1-9中的任一个的主题，还包括虚拟机(VM)逻辑。

[0085] 示例11是联网计算系统，其包括：微云，包括可信执行环境，用于从可信执行环境请求密钥加密密钥(KEK)的基本输入/输出系统(BIOS)以及与KEK相关联的加密存储装置(SES)，其中可信执行环境将KEK提供给BIOS，并且BIOS将KEK提供给SES以对SES解锁以由可信执行环境访问；以及远离微云的与可信执行环境通信的微云管理中心。

[0086] 示例12可以包括示例11的主题，并且还可以指定该联网计算系统是移动边缘计算(MEC)系统。

[0087] 示例13可以包括示例11-12中的任一个的主题，并且还可以指定该联网计算系统是第五代移动网络(5G)系统。

[0088] 示例14可以包括示例11-13中的任何一个的主题，并且还可以包括与微云管理中心通信的多个微云。

[0089] 示例15可以包括示例11-14中的任一个的主题，并且还可以指定可信执行环境是运营商信任根。

[0090] 示例16可以包括示例11-15中的任一个的主题，并且还可以指定可信执行环境是制造商信任根。

[0091] 示例17可以包括示例11-16中任一项的主题，并且还可以指定可信执行环境在微云的操作系统继续执行时从微云管理中心接收更新映像。

[0092] 示例18是一种用于安全存储访问的方法，包括：通过计算设备的可信执行环境来验证计算设备的基本输入/输出系统(BIOS)；响应于验证所述BIOS，由所述可信执行环境向所述BIOS提供用于所述计算设备的自加密存储装置(SES)的密钥加密密钥(KEK)；以及通过BIOS向SES提供KEK以对SES解锁。

[0093] 示例19可以包括示例18的主题，并且还可以指定SES包括硬盘驱动器。

[0094] 示例20可以包括示例18-19中的任何一个的主题，其中平台固件被存储在SES中。

[0095] 示例21是具有存储在其上的指令的一个或多个非暂时性计算机可读介质，所述指令响应于由计算设备的基本输入/输出系统(BIOS)的执行，使计算设备执行以下操作：请求用于计算设备的自加密存储装置(SES)的密钥加密密钥(KEK)；响应于所述BIOS的验证，从所述计算设备的可信执行环境接收所述KEK；并提供KEK来对SES解锁。

[0096] 示例22可以包括示例21的主题，并且还可以指定SES被分区并且提供密钥以对SES解锁包括提供密钥以对与KEK相关联的SES的分区解密。

[0097] 示例23可以包括示例21-22中任一示例的主题，并且还可以指定固件配置信息被存储在SES中。

[0098] 示例24可以包括示例21-23中的任何一个的主题，并且还可以指定SES使用KEK来对媒体加密密钥(MEK)解锁，并且MEK对存储在SES中的数据进行加密。

[0099] 示例25可以包括示例21-24中的任一个的主题，并且还可以指定该计算设备是移动边缘计算(MEC)网络中的边缘服务器。

[0100] 示例26是一种计算设备，包括：可信执行环境；用于从可信执行环境请求KEK的BIOS；以及与KEK相关联的SES；其中所述可信执行环境用于验证所述BIOS并且在验证所述BIOS之后将所述KEK提供给所述BIOS，并且所述BIOS将所述KEK提供给所述SES以对所述SES解锁以由所述可信执行环境访问。

[0101] 示例27可以包括示例26的主题，并且还可以指定可信执行环境包括ME和/或IE。

[0102] 示例28可以包括示例26-27中的任何一个的主题，并且还可以指定可信执行环境包括SMM。

[0103] 示例29可以包括示例26-28中的任何一个的主题，并且还可以指定该计算设备是微云。

[0104] 示例30可以包括示例26-29中的任何一个的主题，并且还可以指定计算设备与微云管理中心通信。

[0105] 示例31可以包括示例26-30中的任何一个的主题，并且还可以包括生命周期管理器。

[0106] 示例32可以包括示例31的主题，并且还可以指定生命周期管理器用于模拟将配置参数公开给另一个计算设备的只读设备。

[0107] 示例33可以包括示例31-32中的任一个的主题，并且还可以指定生命周期管理器用于模拟将日志或诊断信息公开给另一个计算设备的只读设备。

[0108] 示例34可以包括示例26-33中的任一个的主题，并且还可以指定该计算设备执行一个或多个VNF。

[0109] 示例35可以包括示例26-34中的任一个的主题，并且还可以指定该计算设备包括一个或多个工作负载VM。

[0110] 示例36是包括示例26-35中的任何示例的联网计算系统。

[0111] 示例37可以包括示例36的主题，并且还可以指定该联网计算系统是MEC系统。

[0112] 示例38可以包括示例36的主题，并且还可以指定该联网计算系统是5G系统。

[0113] 示例39是一种用于安全存储访问的方法，包括：由计算设备的可信执行环境验证计算设备的BIOS；响应于验证所述BIOS，由所述可信执行环境向所述BIOS提供用于所述计算设备的SES的KEK；并由BIOS向SES提供KEK以对SES解锁。

[0114] 示例40可以包括示例39的主题，并且还可以指定该计算设备是示例1-10或示例26-35的计算设备中的任何一个。

[0115] 示例41是一种装置，包括用于执行示例18-20中的任何示例、示例39-40中的任何示例、示例43-45中的任何示例的方法或者本文公开的任何其他方法的单元的装置。

[0116] 示例42是具有存储在其上的指令的一个或多个计算机可读介质(例如，非暂时性计算机可读介质)，所述指令响应于计算设备的一个或多个处理设备的执行而使计算设备执行示例18-20中的任何示例、示例39-40中的任何示例、示例43-45中的任何示例的方法或者本文公开的任何其他方法。

[0117] 示例43是用于操作微云的方法，包括：引导远离数据中心的微云，其中微云引导不能利用由微云的操作系统执行的软件篡改；以及在微云处从个人移动计算设备接收数据。

[0118] 示例44可以包括示例43的主题，并且还可以包括：检测用于篡改微云的硬件的尝试；并且响应于检测到用于篡改微云的硬件的尝试，中断引导过程。

[0119] 示例45可以包括示例43-44中的任何示例的主题，并且还可以包括使用在微云处接收的数据由微云执行虚拟化网络功能(VNF)。

[0120] 示例46是云计算，其包括：安全处理器，与安全处理器通信的BIOS，与BIOS通信的ME和IE，以及与BIOS通信的SES，其中BIOS从IE请求密钥加密密钥(KEK)，IE用于验证BIOS并且在验证BIOS之后将KEK提供给BIOS，BIOS将KEK提供给SES以对SES解锁以由IE访问，并且

安全处理器在IE访问SES之后运行虚拟进程。

[0121] 示例47可以包括示例1-42中的任一个的主题，并且还可以指定可信执行环境包括处理资源，该处理资源是与计算设备上的操作系统的执行隔离的硬件和软件。

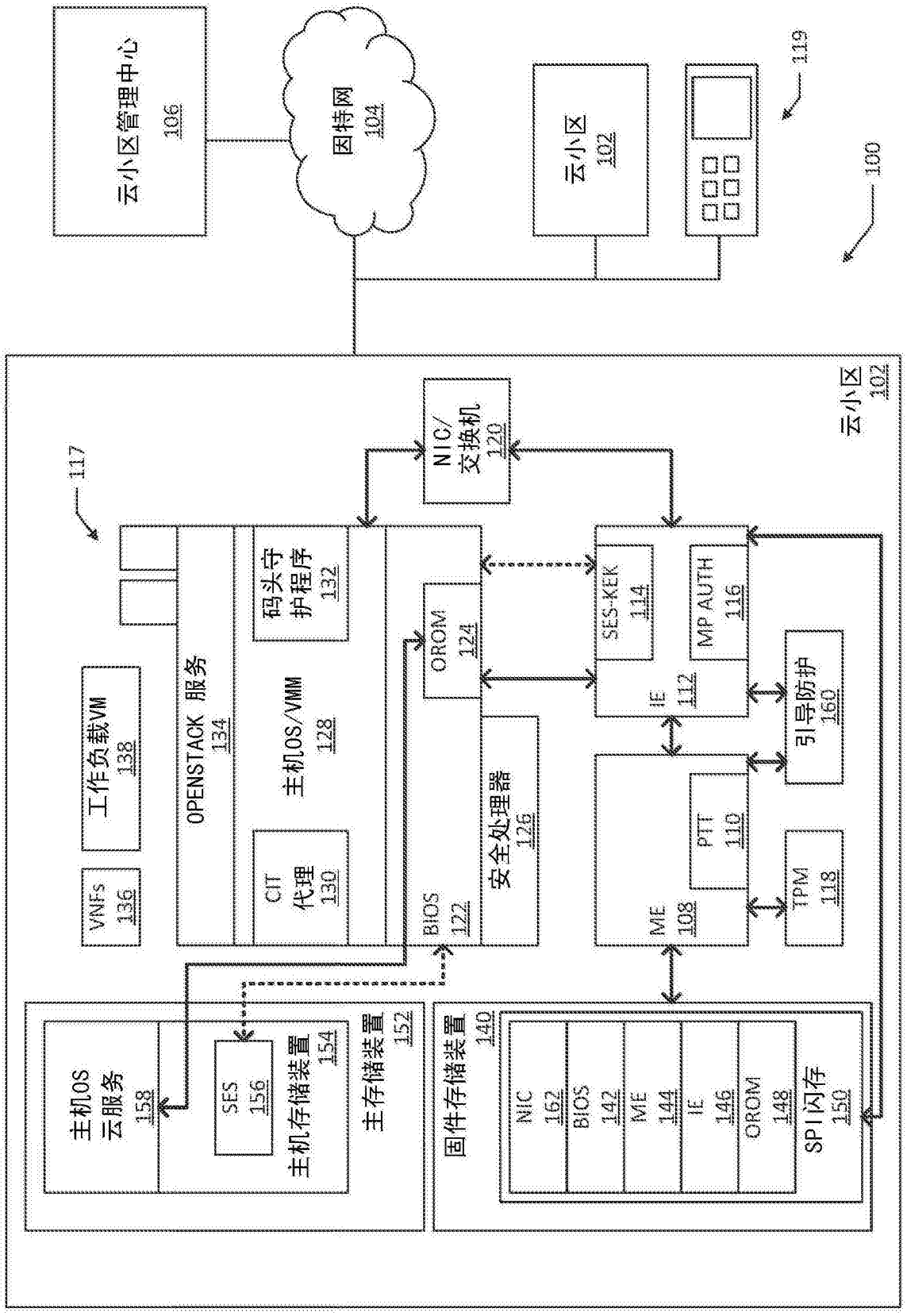

云小区管理中心
106
因特网
104
云小区
102
119
100
云小区
102
117
NIC/
交换机
120
码头守
护程序
132
OPENSTACK 服务
134
主机OS/VMM
128
OROM
124
SES-KEK
114
MP AUTH
116
IE
112
工作负载VM
138
VNFs
136
CIT
代理
130
BIOS
122
安全处理器
126
ME
108
PTT
110
TPM
118
引导防护
160
主机OS
云服务
158
SES
156
主机存储装置
154
主存储装置
152
固件存储装置
140
NIC
162
BIOS
142
ME
144
IE
146
OROM
148
SPI闪存
150

图1

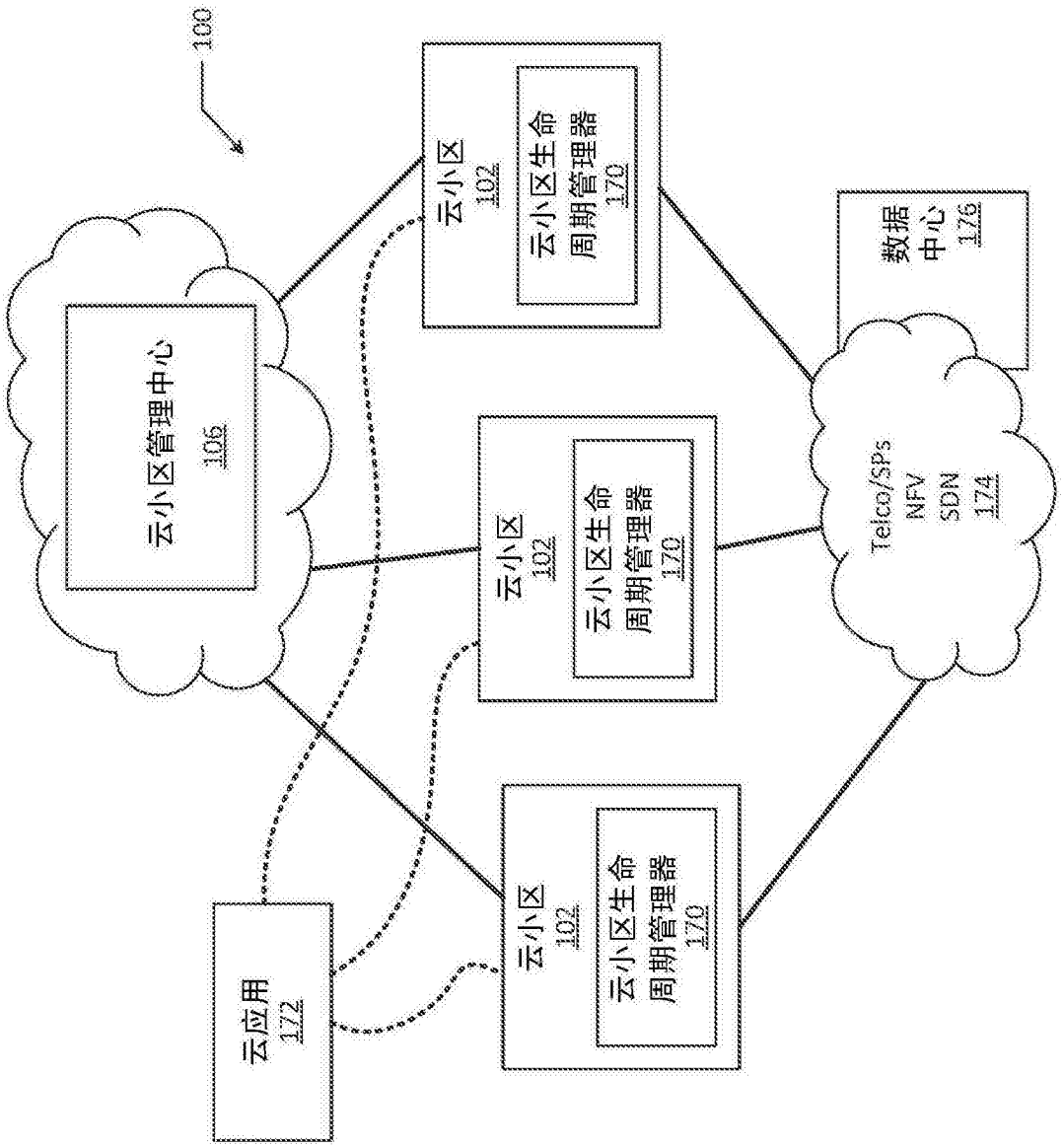

100
云小区管理中心
106
云小区
102
云小区生命
周期管理器
170
数据
中心
176
Telco/SPs
NFV
SDN
174
云小区
102
云小区生命
周期管理器
170
云小区
102
云小区生命
周期管理器
170
云应用
172

图2

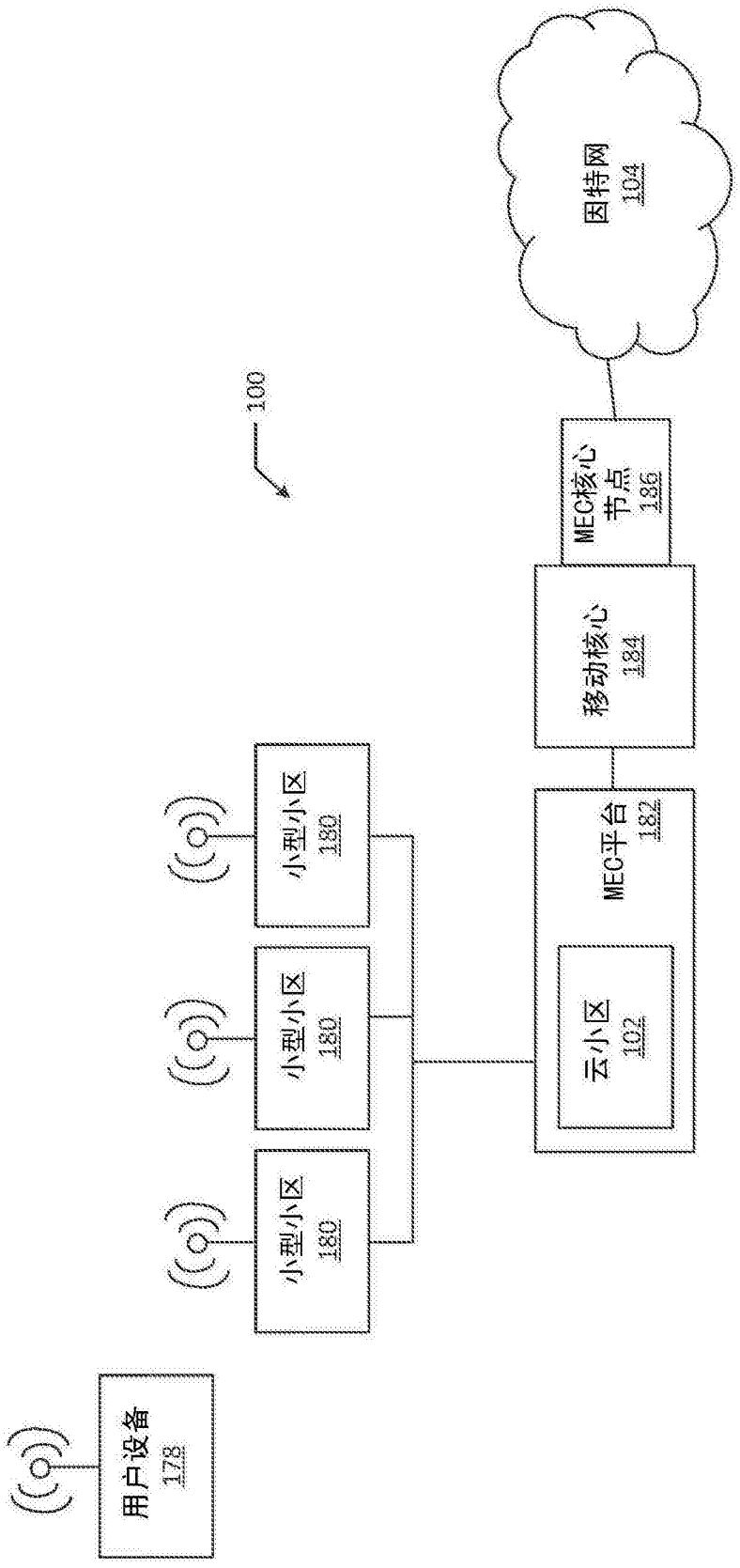

因特网
104
100
MEC核心
节点
186
移动核心
184
MEC平台
182
云小区
102
小型小区
180
小型小区
180
小型小区
180
用户设备
178

图3

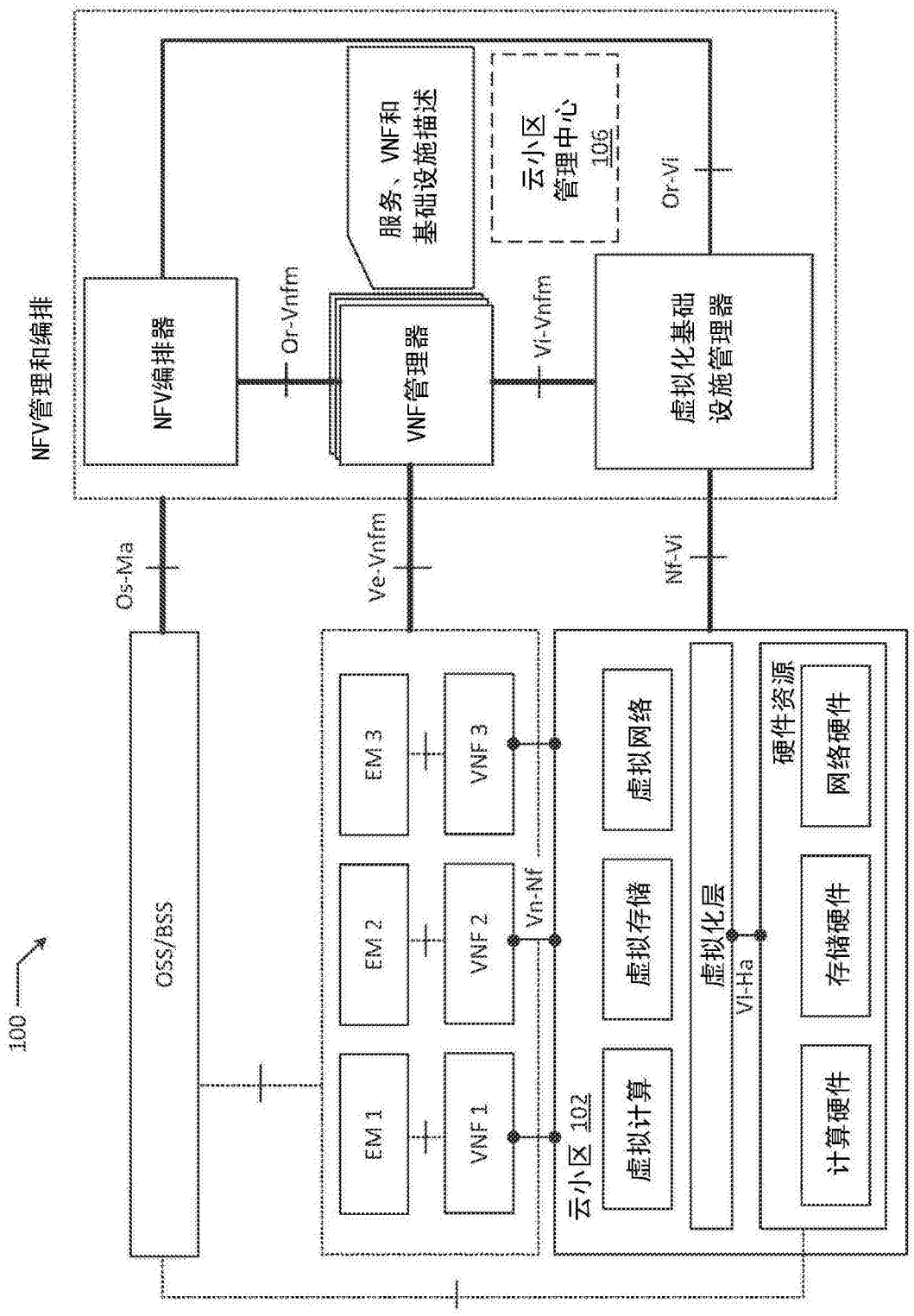

NFV管理和编排
NFV编排器
Or-Vnfm
VNF管理器
服务、VNF和
基础设施描述
云小区
管理中心
105
Vi-Vnfm
Or-Vi
虚拟化基础
设施管理器
Os-Ma
Ve-Vnfm
Nf-Vi
100
OSS/BSS
EM 3
VNF 3
EM 2
VNF 2
EM 1
VNF 1
Vn-Nf
虚拟网络
虚拟存储
虚拟计算
云小区 102
虚拟化层
Vi-Ha
硬件资源
网络硬件
存储硬件
计算硬件

图4

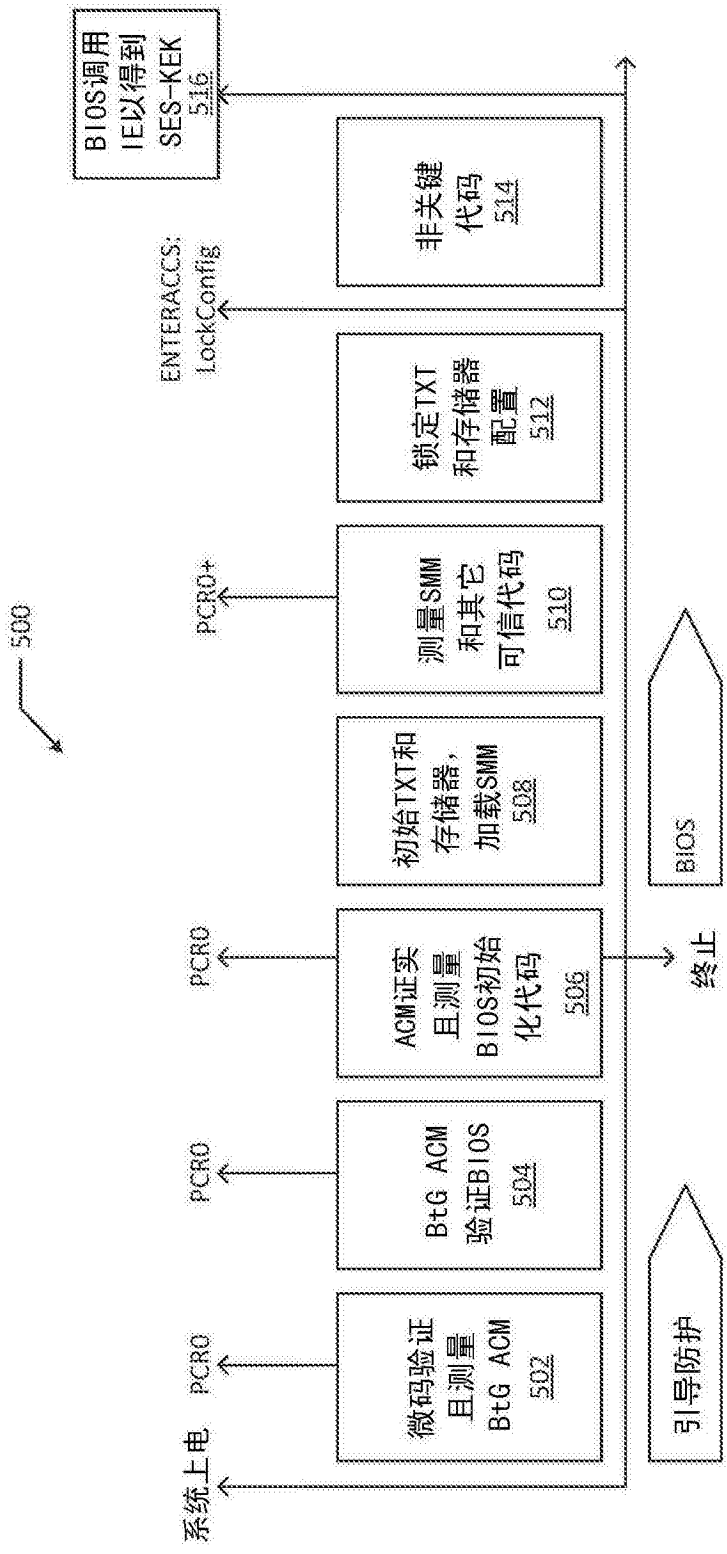

500
系统上电
PCR0
微码验证且测量BtG ACM 502
PCR0
BtG ACM验证BIOS 504
PCR0
ACM证实且测量BIOS初始化代码 506
初始TXT和存储器，加载SMM 508
PCR0+
测量SMM和其它可信代码 510
ENTERACCS: LockConfig
锁定TXT和存储器配置 512
非关键代码 514
BIOS调用IE以得到SES-KEK 516
引导防护
终止
BIOS

图5

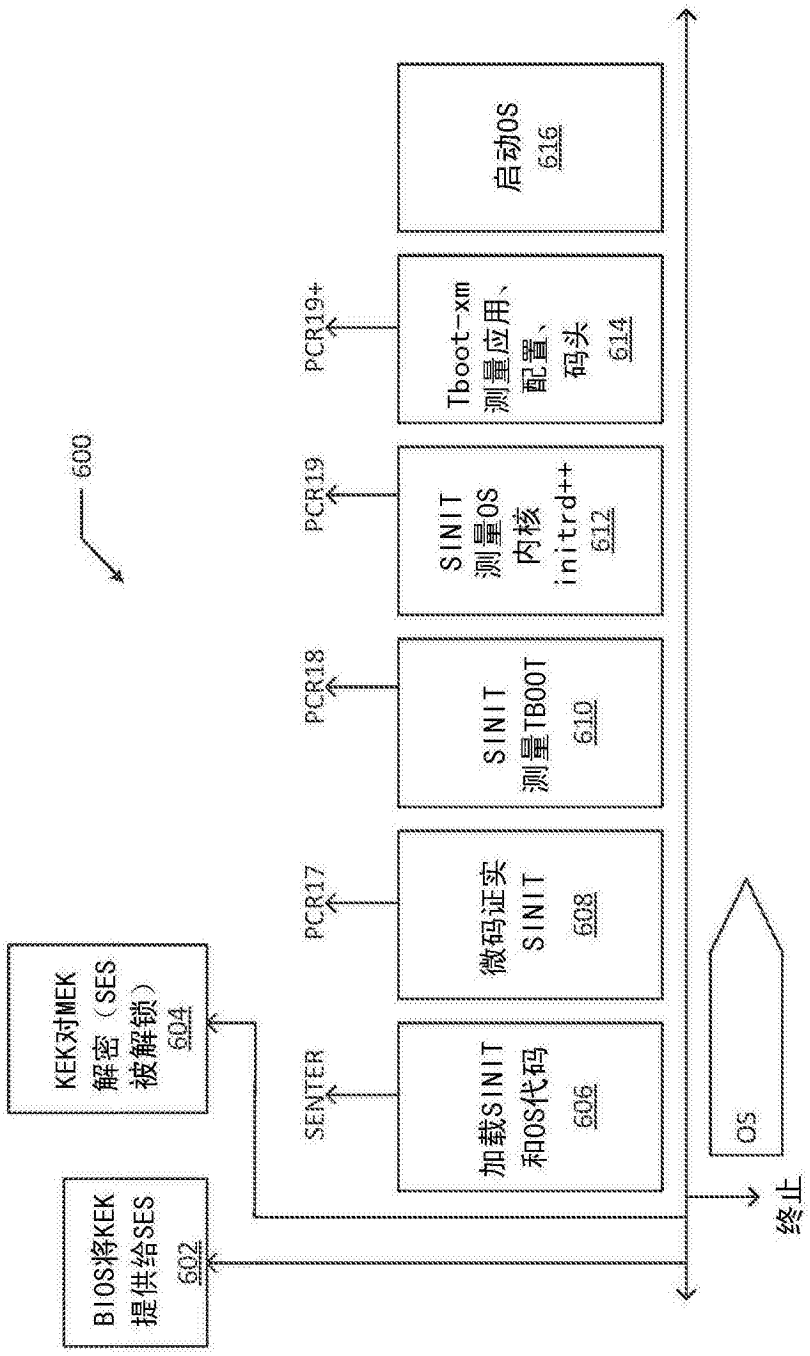

600
BIOS将KEK提供给SES 602
KEK对MEK解密（SES被解锁） 604
SENTER
加载SINIT和OS代码 606
PCR17
微码证实SINIT 608
PCR18
SINIT测量TBOOT 610
PCR19
SINIT测量OS内核initrd++ 612
PCR19+
Tboot-xm测量应用、配置、码头 614
启动OS 616
OS
终止

图6

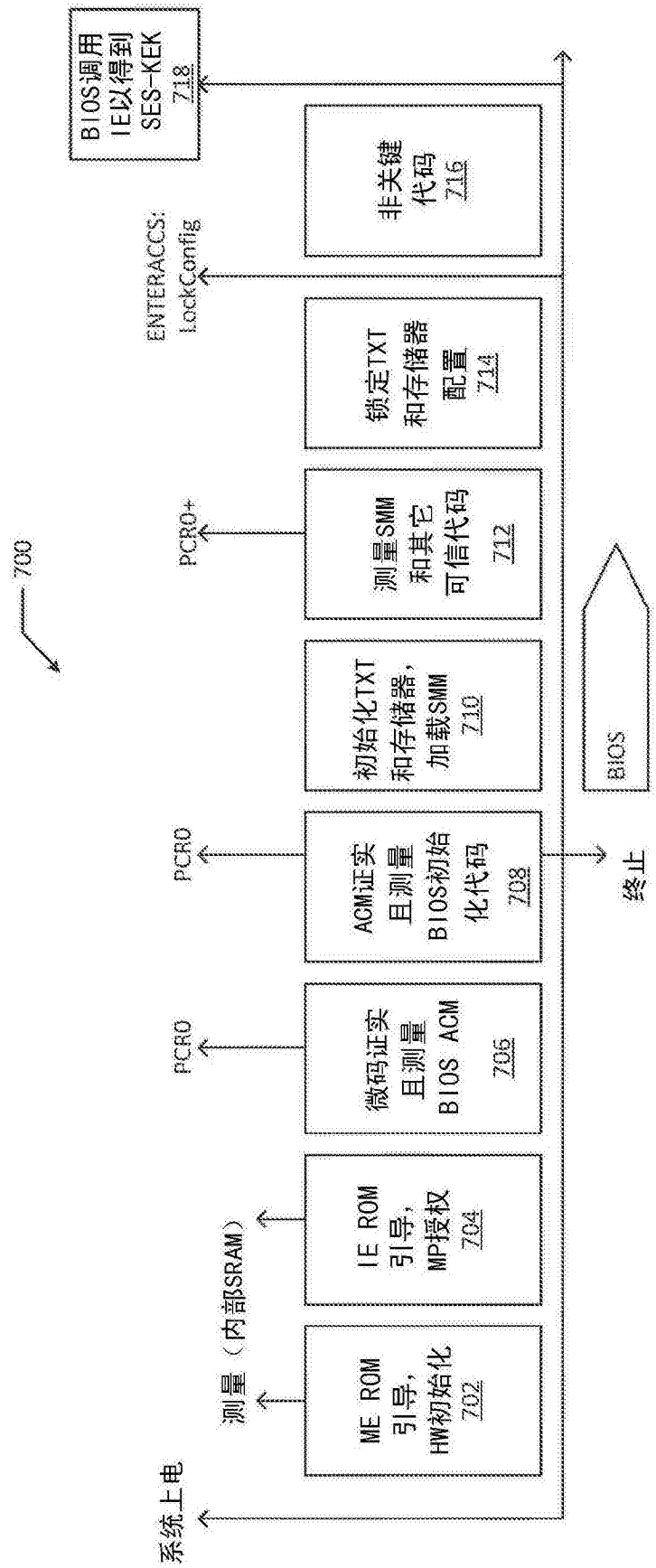

700
系统上电
测量（内部SRAM）
ME ROM
引导，
HW初始化
702
IE ROM
引导，
MP授权
704
PCR0
微码证实
且测量
BIOS ACM
706
PCR0
ACM证实
且测量
BIOS初始
化代码
708
终止
PCR0+
初始化TXT
和存储器，
加载SMM
710
测量SMM
和其它
可信代码
712
ENTERACCS:
LockConfig
锁定TXT
和存储器
配置
714
非关键
代码
716
BIOS调用
IE以得到
SES-KEK
718
BIOS

图7

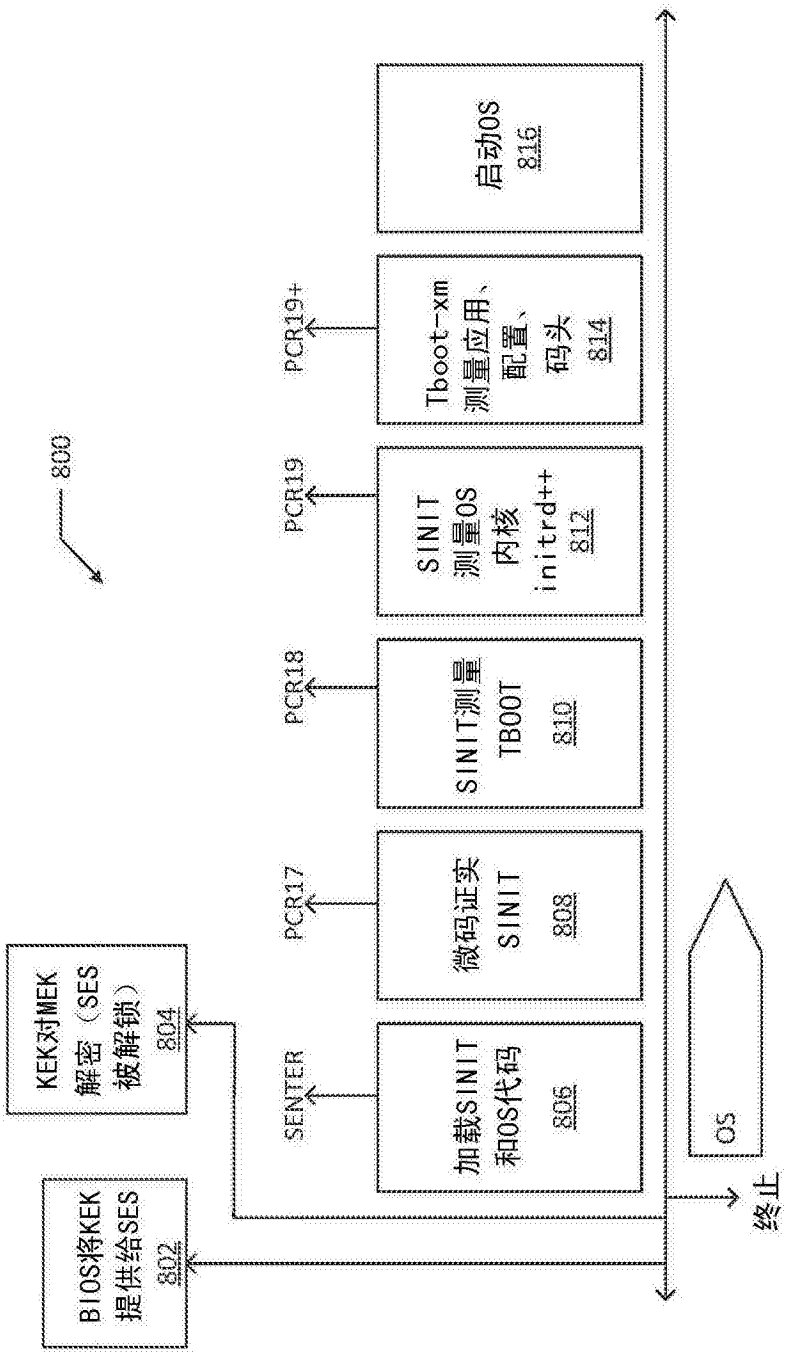

800
BIOS将KEK提供给SES 802
KEK对MEK解密（SES被解锁） 804
SENTER
加载SINIT和OS代码 805
PCR17
微码证实SINIT 808
PCR18
SINIT测量TBOOT 810
PCR19
SINIT测量OS内核initrd++ 812
PCR19+
Tboot-xm测量应用、配置、码头 814
启动OS 816
OS
终止

图8

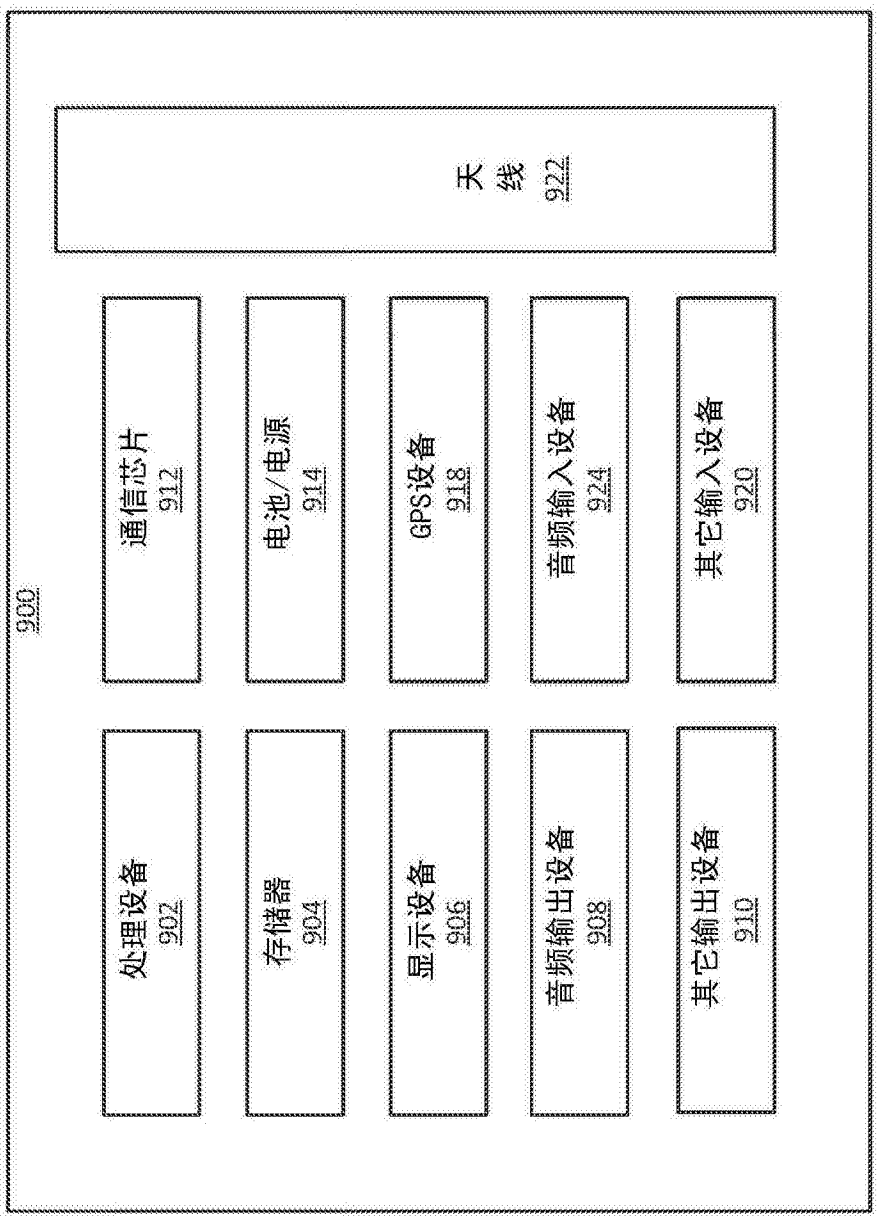

900
天线 922
通信芯片 912
电池/电源 914
GPS设备 918
音频输入设备 924
其它输入设备 920
处理设备 902
存储器 904
显示设备 906
音频输出设备 908
其它输出设备 910

图9