(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113811873 B
(45)授权公告日 2025.03.14

(21)申请号 202080035161.8
(22)申请日 2020.06.24
(65)同一申请的已公布的文献号
申请公布号 CN 113811873 A
(43)申请公布日 2021.12.17
(30)优先权数据
16/455,168 2019.06.27 US
(85)PCT国际申请进入国家阶段日
2021.11.11
(86)PCT国际申请的申请数据
PCT/IB2020/055961 2020.06.24
(87)PCT国际申请的公布数据
WO2020/261134 EN 2020.12.30

(73)专利权人 国际商业机器公司
地址 美国纽约阿芒克
(72)发明人 M·萨巴斯 J·J·B·卢姆
M·斯坦德 D·皮特纳
(74)专利代理机构 北京市金杜律师事务所 11256
专利代理师 马明月

(51)Int.Cl.
G06F 21/31(2006.01)
(56)对比文件
US 2012174198 A1,2012.07.05
US 2018101850 A1,2018.04.12
审查员 王洋

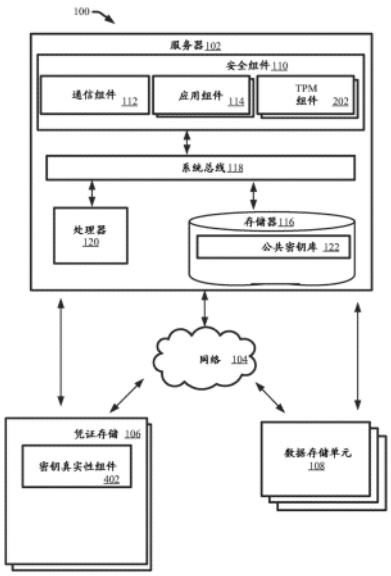
权利要求书2页 说明书19页 附图11页

(54)发明名称

安全凭证的分配

(57)摘要

提供了关于使用描述计算机应用的数字身份令牌以基于一个或多个策略获得对机密数据的授权的技术。例如,在此描述的一个或多个实施例可以包括一种系统,该系统可以包括可以存储计算机可执行组件的存储器。该系统还可包括处理器,其可操作地耦合到存储器,并且可执行存储在存储器中的计算机可执行组件。计算机可执行组件可包括受信平台模块组件,该受信平台模块组件可生成绑定到计算机应用进程的数字身份令牌。计算机可执行组件还可包括可将数字身份令牌与安全密钥进行比较以取回安全凭证的密钥真实性组件。



CN 113811873 B

1.一种用于分发安全凭证的系统,所述系统包括:

存储器,其存储计算机可执行组件;

处理器,其可操作地耦合到所述存储器,并且执行存储在所述存储器中的所述计算机可执行组件,其中所述计算机可执行组件包括:

受信平台模块组件,其可操作用于生成绑定到计算机应用进程的数字身份令牌;以及

密钥真实性组件,其可操作以将所述数字身份令牌与安全密钥进行比较以取回安全凭证,其中所述数字身份令牌包括描述所述计算机应用进程的工作负载的测量,其中所述计算机应用进程生成共同位于网荚内的多个容器,所述网荚支配所述多个容器如何被计算机应用进程运行,并且描述所述计算机应用进程的所述工作负载。

2.如权利要求1所述的系统,进一步包括:

策略真实性组件,所述策略真实性组件可操作用于执行所述数字身份令牌与支配所述计算机应用进程的经定义的策略的比较,其中所述安全凭证的取回进一步基于所述比较。

3.如权利要求1所述的系统,其中所述数字身份令牌由源自硬件的信任链来签名。

4.如权利要求1所述的系统,进一步包括:

应用组件,用于使用所述安全凭证通过从数据库检索数据来执行所述计算机应用进程。

5.如权利要求1所述的系统,其中所述数字身份令牌可操作用于在经定义的时间量之后到期,并且其中所述数字身份令牌的报头包括有效载荷,所述有效载荷指示与运行所述计算机应用进程的一个或多个组件相关联的地理区域的数据。

6.一种用于分发安全凭证的计算机实现的方法,所述方法包括:

通过操作地耦合到处理器的系统生成绑定到计算机应用进程的数字身份令牌;以及

由所述系统将所述数字身份令牌与安全密钥进行比较以取回安全凭证,其中所述数字身份令牌包括描述所述计算机应用进程的工作负载的测量;以及

由所述系统生成共同位于网荚内的多个容器,其中所述网荚支配所述多个容器如何被计算机应用进程运行,并且其中所述多个容器收集关于所述计算机应用进程的一个或多个声明并且描述所述计算机应用进程的所述工作负载。

7.如权利要求6所述的计算机实现的方法,进一步包括:

由所述系统将所述数字身份令牌与支配所述计算机应用进程的经定义的策略进行比较,其中对所述安全凭证的取回进一步基于所述将所述数字身份令牌与所述经定义的策略进行比较。

8.如权利要求6所述的计算机实现的方法,其中所述数字身份令牌由源自硬件的信任链来签名。

9.如权利要求6所述的计算机实现的方法,进一步包括:

由所述系统通过使用所述安全凭证从数据库检索数据来执行所述计算机应用进程。

10.如权利要求6所述的计算机实现的方法,其中所述数字身份令牌在经定义的时间量之后到期。

11.一种用于分发安全凭证的计算机程序产品,所述计算机程序产品包括:

计算机可读存储介质,所述计算机可读存储介质可由处理电路读取并且存储用于由所述处理电路执行以执行如权利要求6至10中任一项所述的方法的指令。

12.一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被加载到数字计算机的内部存储器中,所述计算机程序包括软件代码部分,当所述计算机程序在计算机上运行时,所述软件代码部分用于执行如权利要求6至10中任一项所述的方法。

安全凭证的分配

技术领域

[0001] 本公开涉及数据安全凭证的分配,并且更具体地,涉及可基于一个或多个计算机应用工作负载的授权来限制经由凭证发布系统对服务提供商管理员的安全凭证的访问的一个或多个数据安全过程。

背景技术

[0002] 一些云计算客户需要服务提供商不能访问客户数据的云。为达到该目标而实施的常规技术可以包括安全密钥传输协议、受信平台模块和/或主机起源和完整性。然而,常规技术可能由于忽略的和/或恶意的管理员和/或冒充管理员的实体而受损。

[0003] 因此,在本领域中需要解决上述问题。

发明内容

[0004] 从第一方面来看,本发明提供了一种用于分发安全凭证的系统,该系统包括:存储器,其存储计算机可执行组件;处理器,其可操作地耦合到该存储器,并且执行该存储器中存储的计算机可执行组件,其中该计算机可执行组件包括:受信平台模块组件,其可操作用于生成绑定到计算机应用进程的数字身份令牌;以及可操作用于向安全密钥解析所述数字身份令牌以取回(retrieve)安全凭证的真实性组件。

[0005] 从又一方面来看,本发明提供一种用于分发安全凭证的计算机实现的方法,所述方法包括:由可操作地耦合到处理器的系统生成绑定到计算机应用进程的数字身份令牌;以及由所述系统向安全密钥解析所述数字身份令牌以取回安全凭证。

[0006] 从又一方面来看,本发明提供一种系统,包括:存储器,其存储计算机可执行组件;处理器,其可操作地耦合到所述存储器,并且执行存储在所述存储器中的所述计算机可执行组件,其中,所述计算机可执行组件包括:受信平台模块组件,其生成绑定到计算机应用进程的数字身份令牌;以及密钥真实性组件,其将数字身份令牌与安全密钥进行比较以取回安全凭证。

[0007] 从又一方面来看,本发明提供一种系统,包括:存储器,其存储计算机可执行组件;处理器,其可操作地耦合到所述存储器,并且执行存储在所述存储器中的所述计算机可执行组件,其中所述计算机可执行组件包括:受信平台模块组件,其生成绑定到计算机应用进程的数字身份令牌;以及策略真实性组件,其将所述数字身份令牌与支配所述计算机应用进程的定义的策略进行比较以取回安全凭证。

[0008] 从又一方面来看,本发明提供一种计算机实现的方法,包括:由操作地耦合到处理器的系统生成绑定到计算机应用进程的数字身份令牌;以及由所述系统将所述数字身份令牌与安全密钥进行比较以取回安全凭证。

[0009] 一种计算机实现的方法,包括:由可操作地耦合到处理器的系统生成绑定到计算机应用进程的数字身份令牌;以及由所述系统将所述数字身份令牌与支配所述计算机应用进程的定义的策略进行比较以取回安全凭证。

[0010] 从又一方面来看,本发明提供了一种用于分发安全凭证的计算机程序产品,该计算机程序产品包括计算机可读存储介质,该计算机可读存储介质具有体现在其中的程序指令,该程序指令可由处理器执行以使该处理器:由操作地耦合到该处理器的系统生成绑定到计算机应用进程的数字身份令牌;以及由所述系统将所述数字身份令牌与安全密钥进行比较以取回所述安全凭证。

[0011] 从另一方面来看,本发明提供了一种用于分发安全凭证的计算机程序产品,该计算机程序产品包括可由处理电路读取并且存储用于由该处理电路执行以便执行用于执行本发明的步骤的方法的指令的计算机可读存储介质。

[0012] 从另一方面来看,本发明提供一种存储在计算机可读介质上并且可加载到数字计算机的内部存储器中的计算机程序,该计算机程序包括当所述程序在计算机上运行时用于执行本发明的步骤的软件代码部分。

[0013] 以下呈现发明内容以提供对本发明的一个或多个实施例的基本理解。本发明内容并不旨在识别关键或重要的元素,或描绘特定实施例的任何范围或权利要求的任何范围。其唯一的目的是以简化的形式呈现概念,作为稍后呈现的更详细描述的序言。在此描述的一个或多个实施例中,描述了可以促进数字安全凭证的管理的系统、计算机实现的方法、装置和/或计算机程序产品。

[0014] 根据实施例,提供了一种系统。该系统可以包括存储器,该存储器可以存储计算机可执行组件。该系统还可包括处理器,其可操作地耦合到存储器,并且可执行存储在存储器中的计算机可执行组件。计算机可执行组件可包括受信平台模块组件,该受信平台模块组件可生成绑定到计算机应用进程的数字身份令牌。计算机可执行组件还可包括可将数字身份令牌与安全密钥进行比较以取回安全凭证的密钥真实性组件。

[0015] 根据实施例,提供了一种系统。该系统可以包括存储器,该存储器可以存储计算机可执行组件。该系统还可包括处理器,其可操作地耦合到存储器,并且可执行存储在存储器中的计算机可执行组件。计算机可执行组件可包括受信平台模块组件,该受信平台模块组件可生成绑定到计算机应用进程的数字身份令牌。计算机可执行组件还可包括策略真实性组件,该策略真实性组件可将数字身份令牌与支配计算机应用进程的定义的策略进行比较以取回安全凭证。

[0016] 根据实施例,提供了一种计算机实现的方法。该计算机实现的方法可包括由操作地耦合到处理器的系统生成绑定到计算机应用进程的数字身份令牌。该计算机实现的方法还可包括由该系统将该数字身份令牌与安全密钥进行比较以取回安全凭证。

[0017] 根据实施例,提供了一种计算机实现的方法。该计算机实现的方法可包括由操作地耦合到处理器的系统生成绑定到计算机应用进程的数字身份令牌。该计算机实现的方法还可包括由该系统将该数字身份令牌与支配该计算机应用进程以取回安全凭证的定义的策略进行比较。

[0018] 根据实施例,提供了一种用于分发安全凭证的计算机程序产品。该计算机程序产品可以包括计算机可读存储介质,该计算机可读存储介质具有体现在其上的程序指令。所述程序指令可由处理器执行以致使所述处理器通过可操作地耦合到处理器的系统产生绑定到计算机应用进程的数字身份令牌。程序指令还可由处理器执行以由系统比较数字身份令牌与安全密钥以取回安全凭证。

附图说明

[0019] 现在将参考如在以下附图中所示出的优选实施例仅通过实例的方式来描述本发明：

[0020] 图1示出了根据本文描述的一个或多个实施例的可以管理安全凭证以执行一个或多个计算机应用的示例非限制性系统的框图。

[0021] 图2示出了根据本文描述的一个或多个实施例的示例非限制性系统的框图，该系统可以基于一个或多个计算机应用工作负载的授权来限制经由凭证发布系统对服务提供商管理员的一个或多个安全凭证的访问。

[0022] 图3示出了根据本文所述的一个或多个实施例的可促进一个或多个数据安全系统中的安全凭证的管理的示例非限制性数字身份令牌的图。

[0023] 图4示出了根据本文所述的一个或多个实施例的可基于一个或多个数字身份令牌与公共可用的数字密钥的比较来实现一个或多个身份可靠性机制的示例非限制性系统的图。

[0024] 图5示出了根据本文所述的一个或多个实施例的可基于一个或多个数字身份令牌与管理策略的比较来实现一个或多个身份可靠性机制的示例非限制性系统的图。

[0025] 图6示出了根据本文描述的一个或多个实施例的可由一个或多个系统执行的示例非限制性计算机应用进程的图，该系统可基于对一个或多个计算机应用工作负载的授权来限制经由凭证发布系统对服务提供商管理员的一个或多个安全凭证的访问。

[0026] 图7示出了根据本文描述的一个或多个实施例的可以基于一个或多个计算机应用工作负载的授权经由凭证发布系统来限制对服务提供商管理员的一个或多个安全凭证的访问的示例非限制性系统的框图。

[0027] 图8示出了根据本文描述的一个或多个实施例的可促进基于一个或多个计算机应用工作负载的授权经由凭证释放系统限制对服务提供商管理员的凭证的访问的示例非限制性方法的流程图。

[0028] 图9示出了根据本文描述的一个或多个实施例的可促进基于一个或多个计算机应用工作负载的授权经由凭证释放系统限制对服务提供者管理员的凭证的访问的示例非限制性方法的流程图。

[0029] 图10描绘了根据本文描述的一个或多个实施例的云计算环境。

[0030] 图11描绘了根据本文描述的一个或多个实施例的抽象模型层。

[0031] 图12示出了其中可促进本文所述的一个或多个实施例的示例非限制性操作环境的框图。

具体实施方式

[0032] 以下详细说明仅是说明性的并且不旨在限制实施例和/或实施例的应用或使用。此外，无意受在先前背景或发明内容部分或具体实施方式部分中呈现的任何明确或隐含的信息的约束。

[0033] 现在参考附图描述一个或多个实施例，其中相同的附图标记在全文中用于指代相同的元件。在以下描述中，出于解释的目的，阐述了许多具体细节以便提供对一个或多个实施例的更透彻理解。然而，明显的是，在各种情况下，可以在没有这些具体细节的情况下实

践一个或多个实施例。

[0034] 本发明的各个实施例可涉及促进高效、有效和自治(例如,没有直接的人类引导)数据安全过程的计算机处理系统、计算机实现的方法、装置和/或计算机程序产品,所述数据安全过程可基于对一个或多个计算机应用工作负载的授权来限制经由凭证发布系统对服务提供商管理员的凭证的访问。例如,一个或多个实施例可包括自主生成一个或多个数字身份令牌,该数字身份令牌可被绑定到计算机应用进程和/或由源自一个或多个硬件设备的信任链来签名。一个或多个数字身份令牌可进一步与一个或多个公钥和/或策略进行比较,以促进认证计算机应用进程和取回安全凭证以用于计算机应用进程的提取。例如,该一个或多个数字身份令牌可描述主题计算机应用和/或可用于基于一个或多个用户定义的策略来获得对机密数据的授权。

[0035] 计算机处理系统、计算机实现的方法、装置和/或计算机程序产品采用硬件和/或软件来解决本质上高度技术(例如,限制对安全凭证的访问)、不抽象并且不能由人作为一组精神行为来执行的问题。本文描述的不同实施例通过限制安全凭证对一个或多个人的访问来实现增强的数据安全措施,由此减少由忽视的或恶意的人类动作引起的数据安全漏洞的可能性。

[0036] 图1示出了可以基于一个或多个计算机应用工作负载的授权来限制对服务提供商管理员的一个或多个安全凭证的访问的示例非限制性系统100的框图。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。本发明的各个实施例中的系统(例如,系统100等)、装置或过程的方面可以构成体现在一个或多个机器内(例如,体现在与一个或多个机器相关联的一个或多个计算机可读介质(或媒质)中)的一个或多个机器可执行组件。这样的组件在由一个或多个机器(例如,计算机、计算设备、虚拟机等)执行时可使得机器执行所描述的操作。

[0037] 如图1所示,系统100可以包括一个或多个服务器102、一个或多个网络104、凭证存储106和/或数据存储单元108。服务器102可以包括安全组件110。安全组件110还可以包括一个或多个通信组件112和/或应用组件114。此外,服务器102可以包括至少一个存储器116或者以其他方式与至少一个存储器116相关联。服务器102还可以包括系统总线118,系统总线118可以耦合到不同组件,例如但不限于安全组件110和相关联的组件、存储器116和/或处理器120。虽然在图1中示出了服务器102,但是在其他实施方式中,各种类型的多个设备可以与图1中示出的特征相关联或包括图1中示出的特征。进一步,服务器102可与一个或多个云计算环境通信。

[0038] 一个或多个网络104可包括有线和无线网络,包括但不限于蜂窝网络、广域网(WAN)(例如,互联网)或局域网(LAN)。例如,服务器302可使用几乎任何期望的有线或无线技术与一个或多个凭证存储106和/或数据存储单元108通信(反之亦然),该有线或无线技术包括例如但不限于:蜂窝、WAN、无线保真(Wi-Fi)、Wi-Max、WLAN、蓝牙技术、其组合和/或类似物。进一步,尽管在所示实施例中,安全组件110可设置在一个或多个服务器102上,但应当理解,系统100的架构不限于此。例如,安全组件110或安全组件110的一个或多个组件可位于另一计算机设备(诸如另一服务器设备、客户端设备等)处。

[0039] 一个或多个凭证存储106可存储、访问和/或分发一个或多个动态安全凭证。在各个实施例中,由一个或多个凭证存储106存储、访问和/或分发的动态安全凭证可以是用于

一个或多个应用和/或计算系统的秘密。示例安全凭证可以包括但不限于:令牌、口令、证书、加密密钥、应用程序接口(“API”)密钥、安全壳(“SSH”)凭证、秘密、其组合和/或类似物。在各个实施例中,一个或多个凭证存储106可加密和/或存储一个或多个安全凭证。进一步,一个或多个安全凭证可以是短暂的(例如,访问时以编程方式生成,在读取之前不存在)。

[0040] 一个或多个数据存储单元108可以包括机密信息的一个或多个数据库。在不同实施例中,一个或多个数据存储单元108可以是能够促进一个或多个数据库的创建和/或访问的一个或多个数据库管理系统。进一步,一个或多个数据库可存储在一个或多个云计算环境内,其中一个或多个数据存储单元108可管理对一个或多个数据库的访问。此外,一个或多个数据库可包括以一种或多种编程语言(诸如JavaScript对象表示法(“JSON”)和/或结构化查询语言(“SQL”))存储的数据。示例数据存储单元108可以包括但不限于:一个或多个数据库、云对象存储(“COS”)、其组合等。

[0041] 一个或多个通信组件112可以与服务器的一个或多个其他组件(例如,与安全组件110相关联的一个或多个其他组件)共享由服务器102接收的数据。此外,一个或多个通信组件112可利用一个或多个凭证存储106和/或数据存储单元108来发送安全组件110的一个或多个输出。在一个或多个实施例中,一个或多个通信组件112可经由直接电气连接和/或一个或多个网络104发送和/或接收数据。

[0042] 一个或多个应用组件114可以运行一个或多个计算机应用。例如,一个或多个应用组件114可以是执行一个或多个应用和/或程序的一个或多个物理和/或虚拟机。进一步,在一个或多个应用组件114上运行的一个或多个应用可以由一个或多个容器组成,其中一个或多个应用组件114可以利用一个或多个容器编排平台。主题应用可由紧密耦合和/或共享资源的单个容器或多个共同定位的容器组成。例如,容器可共享资源和/或依赖性,彼此通信,和/或协调容器何时和/或如何终止。另外,一个或多个容器可由一个或多个网荚(pod)封装,其可控制一个或多个容器可如何由一个或多个应用组件114运行。

[0043] 在不同实施例中,一个或多个应用组件114可以生成关于一个或多个应用的一个或多个边车(sidecar)容器。如本文中所使用的,术语“边车容器”和/或“多个边车容器”可以指与一个或多个应用程序共同位于网荚内的一个或多个容器,其中,一个或多个边车容器可以耦接到一个或多个应用程序并且与一个或多个应用程序共享资源。该一个或多个边车容器可以分析该一个或多个应用程序。在一个或多个实施方式中,所述一个或多个应用和边车容器可一起封装在网荚内以形成单个可管理实体。另外,所述一个或多个边车容器可以分析所述网荚内的所述一个或多个应用程序以收集一个或多个声明,所述一个或多个声明可以是描述所述一个或多个应用程序的一个或多个工作负载的一个或多个测量值。

[0044] 图2示出了根据本文描述的一个或多个实施例的示例非限制性系统100的框图,该系统100进一步包括一个或多个受信平台模块(“TPM”)组件202。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。一个或多个TPM组件202可包括可生成一个或多个数字身份令牌的硬件。例如,一个或多个数字身份令牌可以统一资源定位符(“URL”)编码格式表示一个或多个声明,其中,可以对一个或多个声明进行数字签名和/或加密。例如,所述一个或多个数字身份令牌可以是JSON网络令牌(“JWT”),其中,所述一个或多个声明可被编码为一个或多个JSON对象;从而使得能够对所述一个或多个声明进行数字签名和/或加密。

[0045] 在不同实施例中,一个或多个TPM组件202可基于由一个或多个应用组件114生成的一个或多个边车容器所收集的一个或多个声明来生成一个或多个数字身份令牌。例如,一个或多个TPM组件202可基于一个或多个声明利用一个或多个私钥来生成一个或多个数字身份令牌。进一步,一个或多个私有密钥可以由一个或多个TPM组件202信任地保持。例如,私有密钥可以保持拥有一个或多个应用程序、边车容器、系统100的管理员、系统100的其他组件、和/或其他第三方不可访问的一个或多个TPM组件202。在一个或多个实施例中,每个应用组件114可以与相应的TPM组件202相关联。可替代地,应用组件114的一个或多个集群可以与相同的TPM组件202相关联。

[0046] 在一个或多个实施例中,一个或多个私钥以及因此一个或多个数字身份令牌可与一个或多个公共密钥库122内包括的一个或多个公钥相关。如图2所示,一个或多个公共密钥库122可被存储在一个或多个存储器116内,和/或一个或多个公共密钥库122可被存储在服务器102外部(例如,在第二服务器102、外部存储器单元和/或云计算环境内)。一个或多个公钥可由系统100的一个或多个组件和/或管理员读取。然而,一个或多个公共密钥库122的管理可被保留给受信系统100管理员。由此,系统100的不同组件和/或系统100的外部方可读取一个或多个公钥,但不能修改一个或多个公共密钥库122(例如,不能更改公钥、从公共密钥库122移除公钥和/或向公共密钥库122添加公钥)。

[0047] 一个或多个TPM组件202可利用声明中所包括的数据来生成绑定到主题应用的执行的一个或多个数字身份令牌。此外,一个或多个TPM组件202可使用一个或多个私钥来建立由包括在一个或多个数字身份令牌内的签名表示的信任链。此外,一个或多个TPM组件202可定义一个或多个数字身份令牌的期满日期。例如,一个或多个数字身份令牌可在定义的时间量(例如,几分之一秒、几秒、几分钟、几小时、几天等)之后过期。

[0048] 图3示出了根据本文描述的一个或多个实施例的可以由一个或多个TPM组件202生成的一个或多个数字身份令牌的示例非限制性结构300的图。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。如图3所示,一个或多个数字身份令牌可包括报头、有效载荷和签名。

[0049] 报头可包括主题数字身份令牌的参考标题和/或可描述一个或多个密码操作。例如,在一个或多个数字身份令牌是JWT的情况下,报头可以是JSON网络签名(“JWS”)报头或JSON网络加密(“JWE”)报头。所述有效载荷可包括包含在所述一个或多个声明内的数据。在一个或多个声明内和/或一个或多个数字身份令牌的有效载荷内包括的示例数据可包括但不限于:与运行主题应用的一个或多个应用组件114相关联的地理区域(例如,在图3中由“集群区域”表示),与运行该主题应用的一个或多个应用组件114相关联的引用名称(例如,在图3中由关于应用组件114的集群的“集群名称”和/或关于该集群内的特定应用组件114的“机器码”表示),与封装应用的主题容器的网荚相关联的引用名称(例如,在图3中由“网荚”表示)、一个或多个容器的工作负载(例如,在图3中由“图像”表示),数字身份令牌的到期日期(例如,在图3中由“exp”表示)、数字身份令牌的发起日期(例如,在图3中由“iat”表示),主题应用的发布者(例如,在FG.3中由“iss”表示)、命名空间(例如,在图3中由“命名空间”表示)、符合性扫描结果、漏洞、特定版本信息,当前网络配置和/或信息、开放端口、其组合等。进一步,签名可包括来自由数字身份令牌使用一个或多个私钥生成的一个或多个TPM组件202的签名。

[0050] 图4示出了根据本文描述的一个或多个实施例的示例性非限制性系统100的图，该系统100还包括密钥真实性组件402。为了简洁起见，省略对在此描述的其他实施例中采用的相似元件的重复描述。如图4所示，一个或多个密钥真实性组件402可以包括在一个或多个凭证存储106内。

[0051] 在各个实施例中，凭证存储106可基于一个或多个数字身份令牌来确定在一个或多个应用组件114上运行的一个或多个应用是否被授权来接收一个或多个安全凭证。例如，密钥真实性组件402可利用该一个或多个数字身份令牌来认证该一个或多个应用。在一个或多个实施例中，密钥真实性组件402可将数字身份令牌与包括在一个或多个公共密钥库122内的一个或多个公钥进行比较。在一个或多个实施例中，密钥真实性组件402可将数字身份令牌与证书链和/或中间证书授权机构进行比较。响应于将一个或多个数字身份令牌与一个或多个公钥进行比较，密钥真实性组件402可确定主题应用被授权接收一个或多个安全凭证。

[0052] 图5示出了根据本文所述的一个或多个实施例的示例非限制性系统100的图，该系统100进一步包括策略真实性组件502和/或策略库504。为了简洁起见，省略对在此描述的其他实施例中采用的相似元件的重复描述。如图5所示，一个或多个策略真实性组件502和/或策略库504可包括在一个或多个凭证存储106内。

[0053] 在各个实施例中，凭证存储106可进一步基于一个或多个支配策略和/或数字身份令牌来确定将哪些安全凭证分配给该一个或多个应用。例如，策略真实性组件502可将包括在所述一个或多个数字身份令牌的所述有效载荷内的数据与包括在一个或多个策略库504内的一个或多个支配策略进行比较。该一个或多个支配策略可以描绘可以访问由该一个或多个数据存储单元108管理的哪些数据、可以访问的数据量、和/或可以访问该数据的环境。例如，一个或多个支配策略可以向不同的应用提供对由一个或多个数据存储单元108管理的数据的不同级别的访问。在另一个示例中，一个或多个支配策略可以根据应用的执行的上下文(例如，哪些应用组件114正在运行应用，和/或应用组件114如何运行应用)向同一应用提供对由一个或多个数据存储单元108管理的数据的不同级别的访问。在一个或多个实施例中，一个或多个支配策略可以由一个或多个数据存储单元108管理的数据的一个或多个所有者来定义。

[0054] 基于该一个或多个数字身份令牌与支配策略之间的比较，策略真实性组件502可确定哪些限制(如果有的话)可应用于该一个或多个应用的主体执行。因此，密钥真实性组件402可以判定主题应用是否被授权访问由一个或多个数据存储单元108管理的数据，和/或策略真实性组件502可以判定任何数据访问限制是否应用于该应用的主体执行。在一个或多个实施例中，凭证存储器106可基于密钥真实性组件402和策略真实性组件502的确定将一个或多个安全凭证分配给经授权的应用程序。在一些实施例中，凭证存储器106可基于密钥真实性组件402或策略真实性组件502的确定将一个或多个安全凭证分配给经授权的应用程序。安全凭证可以使应用能够访问由一个或多个数据存储单元108管理的数据。此外，一个或多个安全凭证可以基于应用和/或根据一个或多个支配策略(例如，其可以由数据的所有者定义)执行应用来限制访问的量和/或级别。

[0055] 图6示出了根据本文所述的一个或多个实施例的可由系统100实现的示例、非限制性计算机应用进程600的图。为了简洁起见，省略对在此描述的其他实施例中采用的相似元

件的重复描述。在不同实施例中,一个或多个网络104可以促进关于图6描述和/或描述的通信。如图6所示,在计算机应用处理600期间,一个或多个应用组件114(例如,两个应用组件114的集群)可以促进应用的执行。例如,如本文所描述的,一个或多个应用组件114可以生成一个或多个边车容器。

[0056] 在602,一个或多个边车容器可以收集关于应用的一个或多个声明并将声明发送到一个或多个TPM组件202。例如,声明可以描述应用的一个或多个工作负载。在604,一个或多个TPM组件202可基于声明以及由一个或多个TPM组件202确信地保持的一个或多个私钥来生成一个或多个数字身份令牌。进一步,一个或多个TPM组件202可将一个或多个数字身份令牌发送到一个或多个边车容器。在606处,所述一个或多个边车容器可与所述一个或多个应用共享所述一个或多个数字身份令牌。在各实施例中,应用程序可保持不知道如何形成一个或多个数字身份令牌和/或什么形成了一个或多个数字身份令牌。因此,系统100不需要安全组件110存储用于利用一个或多个凭证存储装置进行认证的一个或多个安全凭证;相反,安全组件(例如,经由应用组件114和/或TPM组件202)可提供用于认证的一个或多个数字身份令牌,该一个或多个数字身份令牌可基于由一个或多个边车容器(例如,经由应用组件114)所收集的一个或多个声明来动态地生成(例如,经由TPM组件202)。

[0057] 在608,应用可将一个或多个数字身份令牌发送到一个或多个凭证存储106以获取一个或多个安全凭证。在610处,密钥真实性组件402可将一个或多个数字身份令牌与包括在一个或多个公共密钥库122内的一个或多个公钥进行比较。在各个实施例中,一个或多个公共密钥库122可以由一个或多个受信系统100管理员来管理。在一个或多个实施例中,一个或多个公共密钥库122可由存储在一个或多个数据存储单元108内的机密数据的一个或多个所有者定义的一个或多个实体和/或系统管理。一个或多个公共库122的受信管理可实现对试图从一个或多个凭证存储106获得授权的伪造数字身份令牌的识别。响应于将一个或多个数字身份令牌与一个或多个公钥匹配,密钥真实性组件402可确定该应用被授权接收一个或多个安全凭证。相反,密钥真实性组件402可响应于无法将该一个或多个数字身份令牌与一个或多个公钥匹配,确定该应用未被授权接收一个或多个安全凭证。

[0058] 在密钥真实性组件402确定该应用是经授权的应用的情况下,策略真实性组件502还可将该一个或多个数字身份令牌与包括在一个或多个策略库504内的一个或多个策略进行比较。一个或多个策略可以描绘可应用于应用和/或应用的主题执行(例如,如本文所描述的)的一个或多个数据访问限制。基于612处的比较,策略真实性组件502可以确定哪些数据访问限制(如果有的话)可应用于应用的主体执行。在614处,凭证存储106可以基于密钥真实性组件402和/或策略真实性组件502的确定将一个或多个安全凭证分配给应用。例如,可以响应于应用被授权访问由一个或多个数据存储单元108管理的数据而分配一个或多个安全凭证,和/或安全凭证可以规定向应用授权的数据访问的量和/或级别。

[0059] 在616,应用可使用一个或多个分配的安全凭证来访问一个或多个数据存储单元108和/或根据由一个或多个安全凭证规定的任何数据访问限制来检索所存储的数据。应用随后可利用检索到的数据来执行一个或多个任务和/或完成计算机应用进程600。

[0060] 图7示出了根据本文描述的一个或多个实施方式的包括多个服务器102的示例非限制性系统100的示图,多个服务器102可促进在多个位置执行应用。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。如图7所示,系统100可包括例如:第

一服务器702、第二服务器704、第三服务器706和/或第四服务器708。第一服务器702、第二服务器704、第三服务器706、和/或第四服务器708可以各自:包括本文关于服务器102所描述的各种组件中的一个或多个,被定位在不同的位置中,和/或经由一个或多个网络104(例如,经由云计算环境)进行通信。例如,第一服务器702可位于伦敦,第二服务器704可位于达拉斯,第三服务器706可位于柏林,和/或第四服务器708可位于华盛顿特区。

[0061] 为了例示系统100的一个或多个能力,以下示例场景考虑具有在达拉斯和柏林的位置的跨国公司。公司可利用系统100来执行一个或多个计算机应用进程600和/或定义关于存储在一个或多个数据存储单元108内的员工数据的以下管理策略。第一策略可以描绘存在两级数据访问:全数据访问,其可以包括关于公司雇员的以下信息:名字、姓氏、排名、社会保险号和/或电话号码;和/或有限的数据访问,它可以仅包括名字、姓氏和排名信息。第二策略可以描绘仅源自柏林公司的服务器的请求并使用特定的、受信的、签名的容器的应用可被授权完全数据访问;否则,可以授予源自柏林公司服务器的请求的应用程序有限的数据访问。第三个政策可以描述位于华盛顿特区的审计公司可以临时获得完整的数据访问以进行税务审计。第四策略可以描绘源自达拉斯公司的服务器的请求的应用可以被授予有限的数据访问。此外,第五策略可以描绘源自除了达拉斯和/或柏林以外的地理位置的请求的应用未被授权访问雇员数据。

[0062] 第一服务器702、第二服务器704、第三服务器706和/或第四服务器708可以各自经由一个或多个计算机应用进程600运行相同的应用,但是实现对一个或多个数据存储单元108的不同的可访问性。例如,至少由于每个服务器102的地理位置不同,在各个服务器102上生成的数字身份令牌可以是不同的。进一步,凭证存储106可基于以上定义的(例如,存储在一个或多个策略库504中的)数字身份令牌和/或策略的不同内容来达成关于应用在多个服务器102上的执行的不同确定。

[0063] 例如,凭证存储106可至少因为安全凭证请求源自伦敦(例如,如由第一服务器702的TPM组件202生成的数字身份令牌描绘的),所以根据第五策略,确定应用在第一服务器702上执行时未被分配安全凭证。在另一实例中,凭证存储106可确定该应用在第二服务器704上被执行时被分配根据第四策略来提供受限数据访问的安全凭证,这至少因为安全凭证请求源自达拉斯的授权应用(例如,如由第二服务器704的TPM组件202生成的数字身份令牌描绘的)。在另一实例中,凭证存储106可确定该应用在第三服务器706上执行时可被分配安全凭证,该安全凭证在满足第二策略的细节时提供完全的数据访问,和/或分配安全凭证,该安全凭证在至少因为安全凭证请求源自柏林中的授权应用(例如,由第三服务器706的TPM组件202生成的数字身份令牌所描绘)而未满足第二策略的细节时提供受限的数据访问。在另一实例中,凭证存储106可确定该应用在第四服务器708上执行时被分配有根据第三策略提供完整数据访问的安全凭证,至少因为安全凭证请求源自华盛顿特区的授权应用。(例如,如由第四服务器708的TPM组件202生成的数字身份令牌所描绘的)。

[0064] 图8示出了根据本文描述的一个或多个实施例的可促进基于一个或多个计算机应用工作负载的授权经由凭证发布系统100来限制对服务提供者管理员的凭证的访问的示例非限制性方法800的流程图。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。

[0065] 在802,方法800可包括(例如,经由TPM组件202)通过可操作地耦合到一个或多个

处理器120的系统100来生成可绑定到计算机应用进程(例如,根据示例性计算机应用进程600)的一个或多个数字身份令牌。进一步,在各个实施例中,一个或多个数字身份令牌可由可源自硬件(例如,TPM组件202)的信任链来签名。例如,如本文所描述的,可基于从主题应用收集的一个或多个声明和/或一个或多个私钥来生成该一个或多个数字身份令牌。例如,(例如经由应用组件114生成的)一个或多个边车容器可以分析一个或多个主题应用和/或收集描述应用的一个或多个工作负载的一个或多个测量。在各个实施例中,一个或多个数字身份令牌可由本文描述的示例性结构300来表征(例如,一个或多个数字身份令牌可以是JWT)。此外,在一个或多个实施例中,一个或多个数字身份令牌可被设置(例如,经由TPM组件202)为在所定义的时间段(例如,几分之一秒、几秒、几分钟等)之后过期。

[0066] 在804处,方法800可包括由系统100将一个或多个数字身份令牌与一个或多个安全密钥进行比较(例如,经由密钥真实性组件402),以取回一个或多个安全凭证(例如,用于执行计算机应用进程)。如本文所描述的,一个或多个安全密钥可以是被包括在由系统100的一个或多个受信管理员管理的一个或多个公共库122内的公共密钥。进一步,一个或多个公钥可与用于生成一个或多个数字身份令牌的一个或多个私钥相关,和/或可由此促进认证一个或多个数字身份令牌。

[0067] 例如,在804处的比较可包括确定一个或多个数字身份令牌是否匹配公钥中的一个或多个公钥或以其他方式与公钥中的一个或多个公钥相关。基于804处的比较,系统100(例如,经由密钥真实性组件402)可确定所分析的数字身份令牌是否是真实的(例如,由系统100生成)和/或主题计算机应用进程是否被授权接收一个或多个安全凭证。例如,系统100(例如,经由密钥真实性组件402)可经由804处的比较(例如,由于数字身份令牌与可用公钥之间的不一致性)来识别包括捏造数据(例如,虚构有效载荷)和/或改变数据(例如,改变的有效载荷)的数字身份令牌。在另一示例中,未经授权接收安全凭证的一个或多个应用可通过在804处的比较来识别(例如,由于数字身份令牌和可用公钥之间的不一致性)。

[0068] 在806处,方法800可进一步包括由系统100将一个或多个数字身份令牌与可支配主体计算机应用进程(例如,根据示例性计算机应用进程600)的一个或多个定义的策略进行比较(例如,经由策略真实性组件502),其中取回一个或多个安全凭证可进一步基于806处的比较。如本文所描述的,一个或多个策略可被包括在一个或多个策略库504内和/或可由经由安全凭证的分布来管理的一个或多个数据所有者来定义。在806处的比较可以促进识别适用于计算机应用进程的任何数据可访问性限制。

[0069] 例如,806处的比较可确定应用访问保密数据的授权是否受到一个或多个限制。例如,分配给主题计算机应用进程的一个或多个安全凭证可以进一步基于主题应用的一个或多个工作负载。因此,在各个实施例中,系统100可基于下列项将一个或多个安全凭证分配给主题应用以促进计算机应用进程的执行:主题应用的授权状态、一个或多个数字身份令牌的真实性和/或由一个或多个支配策略定义的一个或多个数据访问限制。

[0070] 图9示出了根据本文描述的一个或多个实施例的可促进基于一个或多个计算机应用工作负载的授权经由凭证发布系统100来限制对服务提供者管理员的凭证的访问的示例非限制性方法900的流程图。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。

[0071] 在902,方法900可以包括(例如,经由应用组件114)通过可操作地耦合到一个或多

个处理器120的系统100来生成可以收集关于应用的一项或多项声明的一个或多个边车容器。例如,该一个或多个边车容器可以收集描述应用的一个或多个工作负载的一个或多个测量。在不同实施例中,该一个或多个应用可以由封装在具有一个或多个边车容器的一个或多个网荚内的一个或多个容器组成。

[0072] 在904,方法900可包括由系统100生成(例如,经由TPM组件202)可绑定至计算机应用进程(例如,根据示例性计算机应用进程600)的一个或多个数字身份令牌。进一步,在各个实施例中,一个或多个数字身份令牌可由可源自硬件(例如,TPM组件202)的信任链来签名。例如,如本文所描述的,所述一个或多个数字身份令牌可基于由所述一个或多个边车容器和/或一个或多个私钥收集的一个或多个声明来生成。在各个实施例中,一个或多个数字身份令牌可由本文描述的示例性结构300来表征(例如,一个或多个数字身份令牌可以是JWT)。此外,在一个或多个实施例中,一个或多个数字身份令牌可被设置(例如,经由TPM组件202)为在所定义的时间段(例如,几分之一秒、几秒、几分钟等)之后过期。

[0073] 在906处,方法900可包括由系统100将该一个或多个数字身份令牌与一个或多个安全密钥进行比较(例如,经由密钥真实性组件402),以促进取回一个或多个安全凭证(例如,用于执行计算机应用进程)。如本文所描述的,一个或多个安全密钥可以是被包括在由系统100的一个或多个受信管理员管理的一个或多个公共库122内的公共密钥。进一步,一个或多个公钥可与用于生成一个或多个数字身份令牌的一个或多个私钥相关,和/或可由此促进认证一个或多个数字身份令牌。

[0074] 例如,906处的比较可包括确定一个或多个数字身份令牌是否匹配公钥中的一个或多个公钥或以其他方式与公钥中的一个或多个公钥相关。基于906处的比较,系统100(例如,经由密钥真实性组件402)可确定所分析的数字身份令牌是否是真实的(例如,由系统100生成)和/或主题计算机应用进程是否被授权接收一个或多个安全凭证。例如,系统100(例如,经由密钥真实性组件402)可经由906处的比较(例如,由于数字身份令牌与可用公钥之间的不一致性)来识别包括捏造数据(例如,虚构有效载荷)和/或改变数据(例如,改变的有效载荷)的数字身份令牌。在另一示例中,未经授权接收安全凭证的一个或多个应用可通过在906处的比较来识别(例如,由于数字身份令牌和可用公钥之间的不一致性)。

[0075] 在908,方法900可进一步包括由系统100将一个或多个数字身份令牌与可支配主题计算机应用进程(例如,根据示例性计算机应用进程600)的一个或多个定义的策略进行比较(例如,经由策略真实性组件502),其中取回一个或多个安全凭证可进一步基于806处的比较。如本文所描述的,一个或多个策略可被包括在一个或多个策略库504内和/或可由经由安全凭证的分布来管理的一个或多个数据所有者来定义。908处的比较可以促进识别适用于计算机应用进程的任何数据可访问性限制。

[0076] 例如,908处的比较可确定应用访问保密数据的授权是否受到一个或多个限制。例如,分配给主题计算机应用进程的一个或多个安全凭证可以进一步基于主题应用的一个或多个工作负载。因此,在各个实施例中,系统100可基于下列项将一个或多个安全凭证分配给主题应用以促进计算机应用进程的执行:主题应用的授权状态、一个或多个数字身份令牌的真实性和/或由一个或多个支配策略定义的一个或多个数据访问限制。

[0077] 在910处,方法900还可以包括由系统100通过使用所分配的一个或多个安全凭证从(例如,由一个或多个数据存储单元108管理的)一个或多个数据库中检索数据来执行(例

如,经由应用组件114)计算机应用进程。例如,一个或多个主题应用可根据由一个或多个安全凭证指定的一个或多个可访问性限制来从一个或多个数据存储单元108检索数据。

[0078] 应当理解,虽然本公开包括关于云计算的详细描述,但是本文所引用的教导的实现不限于云计算环境。相反,本发明的实施例能够结合现在已知的或以后开发的任何其他类型的计算环境来实现。

[0079] 云计算是服务交付的模型,用于使得能够方便地、按需地网络访问可配置计算资源(例如,网络、网络带宽、服务器、处理、存储器、存储、应用、虚拟机和服务)的共享池,所述可配置计算资源可以以最小的管理努力或与所述服务的提供者的交互来快速供应和释放。该云模型可以包括至少五个特性、至少三个服务模型和至少四个部署模型。

[0080] 特性如下:

[0081] 按需自助服务:云消费者可以单方面地根据需要自动地提供计算能力,诸如服务器时间和网络存储,而不需要与服务的提供者的人类交互。广泛的网络接入:能力可通过网络获得并且通过标准机制接入,该标准机制促进异构瘦客户机平台或厚客户机平台(例如,移动电话、膝上型计算机和PDA)的使用。

[0082] 资源池:提供者的计算资源被池化以使用多租户模型来服务于多个消费者,其中不同的物理和虚拟资源根据需要动态地指派和重新指派。存在位置独立性的感觉,因为消费者通常不具有对所提供的资源的确切位置的控制或了解,但可能能够以较高抽象级别(例如,国家、州或数据中心)指定位置。

[0083] 快速弹性:能够快速和弹性地提供能力,在一些情况下自动地快速缩小和快速释放以快速放大。对于消费者而言,可用于供应的能力通常显得不受限制并且可以在任何时间以任何数量购买。

[0084] 测量的服务:云系统通过在适合于服务类型(例如,存储、处理、带宽和活动用户账户)的某个抽象级别处利用计量能力来自动控制和优化资源使用。可以监视、控制和报告资源使用,为所利用的服务的提供者和消费者提供透明度。

[0085] 服务模型如下:

[0086] 软件即服务(SaaS):提供给消费者的能力是使用在云基础设施上运行的提供者的应用。可通过诸如web浏览器(例如,基于web的电子邮件)之类的瘦客户端接口从不同客户端设备访问应用。消费者不管理或控制包括网络、服务器、操作系统、存储或甚至单独的应用能力的底层云基础设施,可能的例外是有限的用户特定应用配置设置。平台即服务(PaaS):提供给消费者的能力是将消费者创建的或获取的使用由提供商支持的编程语言和工具创建的应用部署到云基础设施上。消费者不管理或控制包括网络、服务器、操作系统或存储的底层云基础设施,但是对所部署的应用和可能的应用托管环境配置具有控制。

[0087] 基础设施即服务(IaaS):提供给消费者的能力是提供处理、存储、网络和消费者能够部署和运行任意软件的其他基本计算资源,所述软件可以包括操作系统和应用。消费者不管理或控制底层云基础设施,而是具有对操作系统、存储、所部署的应用的控制以及对所选联网组件(例如,主机防火墙)的可能受限的控制。

[0088] 部署模型如下:

[0089] 私有云:云基础架构仅为组织运作。它可以由组织或第三方管理,并且可以存在于场所内或场所外。

[0090] 社区云:云基础架构被若干组织共享并支持共享了关注(例如,任务、安全要求、策略、和合规性考虑)的特定社区。它可以由组织或第三方管理,并且可以存在于场所内或场所外。

[0091] 公共云:使云基础架构对公众或大型行业组可用,并且由出售云服务的组织拥有。

[0092] 混合云:云基础架构是两个或更多个云(私有、社区或公共)的组合,这些云保持唯一实体但通过使数据和应用能够移植的标准化或专有技术(例如,云突发以用于云之间的负载平衡)绑定在一起。

[0093] 云计算环境是面向服务的,集中于无状态、低耦合、模块化和语义互操作性。云计算的核心是包括互连节点网络的基础设施。

[0094] 现在参见图10,描述了说明性云计算环境1000。如图所示,云计算环境1000包括云消费者使用的本地计算设备可以与其通信的一个或多个云计算节点1002,本地计算设备诸如例如个人数字助理(PDA)或蜂窝电话1004、台式计算机1006、膝上型计算机1008和/或汽车计算机系统1010。节点1002可以彼此通信。它们可以物理地或虚拟地分组(未示出)在一个或多个网络中,诸如如上所述的私有云、社区云、公共云或混合云、或其组合。这允许云计算环境1000提供基础设施、平台和/或软件作为云消费者不需要为其维护本地计算设备上的资源的服务。应当理解,图10中所示的计算设备1004-1010的类型旨在仅是说明性的,并且计算节点1002和云计算环境1000可以通过任何类型的网络和/或网络可寻址连接(例如,使用网络浏览器)与任何类型的计算机化设备通信。

[0095] 现在参见图11,示出了由云计算环境1000(图10)提供的一组功能抽象层。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。应提前理解,图11中所示的组件、层和功能旨在仅是说明性的,并且本发明的实施例不限于此。如所描述,提供以下层和对应功能。

[0096] 硬件和软件层1102包括硬件和软件组件。硬件组件的示例包括:大型机1104;基于RISC(精简指令集计算机)架构的服务器1106;服务器1108;刀片式服务器1110;存储设备1112;以及网络和联网组件1114。在一些实施例中,软件组件包括网络应用服务器软件1116和数据库软件1118。

[0097] 虚拟化层1120提供抽象层,从该抽象层可以提供虚拟实体的以下示例:虚拟服务器1122;虚拟存储1124;虚拟网络1126,包括虚拟专用网络;虚拟应用和操作系统1128;以及虚拟客户端1130。

[0098] 在一个示例中,管理层1132可以提供以下描述的功能。资源供应1134提供计算资源和用于在云计算环境内执行任务的其他资源的动态采购。计量和定价1136在云计算环境内利用资源时提供成本跟踪,并为这些资源的消费开账单或发票。在一个示例中,这些资源可以包括应用软件许可证。安全性为云消费者和任务提供身份验证,以及为数据和其他资源提供保护。用户门户1138为消费者和系统管理员提供对云计算环境的访问。服务水平管理1140提供云计算资源分配和管理,使得满足所需的服务水平。服务水平协议(SLA)规划和履行1142为云计算资源提供预安排和采购,根据该SLA预期该云计算资源的未来要求。

[0099] 工作负载层1144提供可以利用云计算环境的功能的示例。可以从该层提供的工作负载和功能的示例包括:地图和导航1146;软件开发和生命周期管理1148;虚拟教室教育传递1150;数据分析处理1152;事务处理1154;以及安全凭证管理1156。本发明的各个实施例

可利用参见图10和图11描述的云计算环境来促进一个或多个安全凭证的支付以促进一个或多个计算机应用进程的执行。

[0100] 本发明可以是任何可能的技术细节集成度的系统、方法和/或计算机程序产品。计算机程序产品可包括其上具有用于使处理器执行本发明的各方面的计算机可读程序指令的计算机可读存储介质(或多个媒质)。计算机可读存储介质可为可保留和存储供指令执行装置使用的指令的有形装置。计算机可读存储介质可以是,例如但不限于,电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备、或者上述的任意合适的组合。计算机可读存储介质的更具体示例的非穷尽列表包括以下各项:便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式紧凑盘只读存储器(CD-ROM)、数字通用盘(DVD)、记忆棒、软盘、诸如穿孔卡之类的机械编码设备或具有记录在其上的指令的槽中的凸出结构、以及上述各项的任何合适的组合。如本文所使用的计算机可读存储介质不应被解释为暂时性信号本身,例如无线电波或其他自由传播的电磁波、通过波导或其他传输媒体传播的电磁波(例如,穿过光纤电缆的光脉冲)或通过电线发射的电信号。

[0101] 本文中所描述的计算机可读程序指令可以经由网络(例如,互联网、局域网、广域网和/或无线网络)从计算机可读存储介质下载到相应的计算/处理设备,或者下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输纤维、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配器卡或网络接口接收来自网络的计算机可读程序指令,并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。

[0102] 用于执行本发明的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据、或以一种或多种程序设计语言的任何组合编写的源代码或目标代码,这些程序设计语言包括面向对象的程序设计语言(诸如Smalltalk、C++等)和过程程序设计语言(诸如“C”程序设计语言或类似程序设计语言)。计算机可读程序指令可以完全地在用户计算机上执行、部分在用户计算机上执行、作为独立软件包执行、部分在用户计算机上部分在远程计算机上执行或者完全在远程计算机或服务器上执行。在后一种情况下,远程计算机可通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接至用户计算机,或者可连接至外部计算机(例如,使用互联网服务提供商通过互联网)。在一些实施例中,包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息来使电子电路个性化来执行计算机可读程序指令,以便执行本发明的各方面。

[0103] 下面将参照根据本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明。应当理解,流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合,都可以由计算机可读程序指令实现。

[0104] 这些计算机可读程序指令可被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以产生机器,使得经由计算机或其他可编程数据处理装置的处理器执行的指令创建用于实现在流程图和/或框图的或多个框中指定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中,这些指令使得计算机、可编程数

据处理装置、和/或其他设备以特定方式工作,从而,其中存储有指令的计算机可读存储介质包括包含实现流程图和/或框图中的或多个方框中规定的功能/动作的方面的指令的制造品。

[0105] 也可以把计算机可读程序指令加载到计算机、其他可编程数据处理装置、或其他设备上,使得在计算机、其他可编程装置或其他设备上执行一系列操作步骤,以产生计算机实现的处理,使得在计算机、其他可编程装置或其他设备上执行的指令实现流程图和/或框图中的或多个方框中规定的功能/动作。

[0106] 附图中的流程图和框图示出了根据本发明的不同实施例的系统、方法和计算机程序产品的可能实现方式的架构、功能和操作。对此,流程图或框图中的每个框可表示指令的模块、段或部分,其包括用于实现指定的逻辑功能的一个或多个可执行指令。在一些备选实现中,框中标注的功能可以不按照图中标注的顺序发生。例如,取决于所涉及的功能,连续示出的两个块实际上可以基本上同时执行,或者这些块有时可以以相反的顺序执行。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作或执行专用硬件与计算机指令的组合的基于专用硬件的系统来实现。

[0107] 为了提供用于所公开的主题的各方面的上下文,图12以及以下讨论旨在提供对其中可实现所公开的主题的各方面的合适环境的一般描述。图12示出了其中可促进本文所述的一个或多个实施例的示例非限制性操作环境的框图。为了简洁起见,省略对在此描述的其他实施例中采用的相似元件的重复描述。参考图12,用于实现本公开的各个方面的合适的操作环境1200可包括计算机1212。计算机1212还可以包括处理单元1214、系统存储器1216以及系统总线1218。系统总线1218可以可操作地将包括但不限于系统存储器1216的系统组件耦合至处理单元1214。处理单元1214可以是不同可用处理器中的任何处理器。双微处理器和其他多处理器架构也可以用作处理单元1214。系统总线1218可以是若干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、外围总线或外部总线、和/或使用任何各种可用总线架构的局部总线,包括但不限于工业标准架构(ISA)、微通道架构(MSA)、扩展ISA(EISA)、智能驱动电子器件(IDE)、VESA局部总线(VLB)、外围组件互连(PCI)、卡总线、通用串行总线(USB)、高级图形端口(AGP)、火线、和小型计算机系统接口(SCSI)。系统存储器1216还可包括易失性存储器1220和非易失性存储器1222。基本输入/输出系统(BIOS)(包含诸如在启动期间在计算机1212内的元件之间传输信息的基本例程)可以存储在非易失性存储器1222中。作为示例而非限制,非易失性存储器1222可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)、闪存、或非易失性随机存取存储器(RAM)(例如,铁电RAM(FeRAM))。易失性存储器1220还可包含充当外部高速缓冲存储器的随机存取存储器(RAM)。作为说明而非限制,RAM可以以许多形式获得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双倍数据速率SDRAM(DDR SDRAM)、增强型SDRAM(ESDRAM)、同步链接DRAM(SLDRAM)、直接Rambus RAM(DRRAM)、直接Rambus动态RAM(DRDRAM)和Rambus动态RAM。

[0108] 计算机1212还可以包括可移动/不可移动、易失性/非易失性计算机存储介质。图12示出了例如磁盘存储器1224。磁盘存储器1224还可以包括但不限于像磁盘驱动器、软盘驱动器、磁带驱动器、Jaz驱动器、Zip驱动器、LS-100驱动器、闪存卡、或记忆棒的装置。磁盘

存储器1224也可以单独地或与其他存储介质组合地包括存储介质,包括但不限于光盘驱动器,如光盘ROM设备(CD-ROM)、CD可记录驱动器(CD-R驱动器)、CD可重写驱动器(CD-RW驱动器)或数字通用磁盘ROM驱动器(DVD-ROM)。为了促进磁盘存储器1224到系统总线1218的连接,可以使用可移除或不可移除接口,诸如接口1226。图12还描绘了可充当用户与在合适的操作环境1200中描述的基本计算机资源之间的中介的软件。这样的软件还可以包括例如操作系统1228。可存储在磁盘存储器1224上的操作系统1228用于控制和分配计算机1212的资源。系统应用1230可以利用操作系统1228通过例如存储在系统存储器1216或磁盘存储器1224上的程序模块1232和程序数据1234对资源的管理。应当理解,本公开可用不同操作系统或操作系统的组合来实现。用户通过一个或多个输入装置1236将命令或信息输入到计算机1212中。输入设备1236可以包括但不限于诸如鼠标、轨迹球、指示笔、触摸板、键盘、麦克风、操纵杆、游戏板、圆盘式卫星天线、扫描仪、TV调谐器卡、数码相机、数码摄像机、网络相机等定点设备。这些和其他输入设备可以经由一个或多个接口端口1238通过系统总线1218连接至处理单元1214。一个或多个接口端口1238可包括例如串行端口、并行端口、游戏端口和通用串行总线(USB)。一个或多个输出设备1240可以使用与输入设备1236相同类型的端口中的一些。因此,例如,USB端口可以用于向计算机1212提供输入,并且从计算机1212向输出装置1240输出信息。可提供输出适配器1242以示出除了需要特殊适配器的其他输出设备1240之外,还存在一些输出设备1240如监视器、扬声器和打印机。作为说明而非限制,输出适配器1242可包含提供输出装置1240与系统总线1218之间的连接装置的视频和声卡。应当注意,其他设备和/或设备的系统提供输入和输出能力两者,诸如一个或多个远程计算机1244。

[0109] 计算机1212可以使用到一个或多个远程计算机(如远程计算机1244)的逻辑连接在联网环境中操作。远程计算机1244可以是计算机、服务器、路由器、网络PC、工作站、基于微处理器的电器、对等设备或其他公共网络节点等,并且通常还可以包括相对于计算机1212所描述的许多或所有元件。为了简洁的目的,仅以远程计算机1244说明存储器存储装置1246。远程计算机1244可以通过网络接口1248在逻辑上连接到计算机1212并且然后经由通信连接1250在物理上连接。进一步,操作可跨多个(本地和远程)系统分布。网络接口1248可包括有线和/或无线通信网络,诸如局域网(LAN)、广域网(WAN)、蜂窝网络等。LAN技术包括光纤分布式数据接口(FDDI)、铜线分布式数据接口(CDDI)、以太网、令牌环等。WAN技术包括但不限于点对点链路、电路交换网络(如综合业务数字网(ISDN))及其变型、分组交换网络和数字用户线路(DSL)。一个或多个通信连接1250是指用于将网络接口1248连接至系统总线1218的硬件/软件。尽管为了清楚起见在计算机1212内部示出了通信连接1250,但它也可以在计算机1212外部。仅出于示例性目的,用于连接到网络接口1248的硬件/软件还可包括内部和外部技术,例如调制解调器,包括常规电话级调制解调器、电缆调制解调器和DSL调制解调器、ISDN适配器和以太网卡。

[0110] 本发明的实施例可以是处于任何可能的技术细节集成度的系统、方法、装置和/或计算机程序产品。计算机程序产品可包括其上具有用于使处理器执行本发明的各方面的计算机可读程序指令的计算机可读存储介质(或多个介质)。计算机可读存储介质可为可保留和存储供指令执行装置使用的指令的有形装置。计算机可读存储介质可以是,例如但不限于,电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备、或者上述的

任意合适的组合。计算机可读存储介质的更具体示例的非穷尽列表还可以包括以下各项：便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式紧凑盘只读存储器(CD-ROM)、数字通用盘(DVD)、记忆棒、软盘、诸如穿孔卡之类的机械编码设备或具有记录在其上的指令的槽中的凸出结构、以及上述各项的任何合适的组合。如本文所使用的计算机可读存储介质不应被解释为暂时性信号本身，例如无线电波或其他自由传播的电磁波、通过波导或其他传输介质传播的电磁波(例如，穿过光纤电缆的光脉冲)或通过电线发射的电信号。

[0111] 本文中所描述的计算机可读程序指令可以经由网络(例如，互联网、局域网、广域网和/或无线网络)从计算机可读存储介质下载到相应的计算/处理设备，或者下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输纤维、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配器卡或网络接口接收来自网络的计算机可读程序指令，并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。用于执行本发明的各个方面的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据、或者以一种或多种编程语言的任何组合编写的源代码或者目标代码，该一种或多种编程语言包括面向对象的编程语言(诸如Smalltalk、C++等)和过程编程语言(诸如“C”编程语言或类似编程语言)。计算机可读程序指令可以完全地在用户计算机上执行、部分在用户计算机上执行、作为独立软件包执行、部分在用户计算机上部分在远程计算机上执行或者完全在远程计算机或服务器上执行。在后一种情况下，远程计算机可通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接至用户计算机，或者可连接至外部计算机(例如，使用互联网服务提供商通过互联网)。在一些实施例中，包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息来定制该电子电路来执行计算机可读程序指令，以便执行本发明的多个方面。

[0112] 下面将参照根据本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令实现。这些计算机可读程序指令可被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以产生机器，使得经由计算机或其他可编程数据处理装置的处理器执行的指令创建用于实现在流程图和/或框图的或多个框中指定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这些指令使得计算机、可编程数据处理装置、和/或其他设备以特定方式工作，从而，其中存储有指令的计算机可读存储介质包括包含实现流程图和/或框图中的或多个方框中规定的功能/动作的方面的指令的制造品。也可以把计算机可读程序指令加载到计算机、其他可编程数据处理装置、或其他设备上，使得在计算机、其他可编程装置或其他设备上执行一系列操作动作，以产生计算机实现的处理，使得在计算机、其他可编程装置或其他设备上执行的指令实现在流程图和/或框图的或多个框中指定的功能/动作。

[0113] 附图中的流程图和框图示出了根据本发明的不同实施例的系统、方法和计算机程序产品的可能实现方式的架构、功能和操作。对此，流程图或框图中的每个框可表示指令的模块、段或部分，其包括用于实现指定的逻辑功能的一个或多个可执行指令。在一些备选实

现中,框中标注的功能可以不按照图中标注的顺序发生。例如,取决于所涉及的功能,连续示出的两个块实际上可以基本上同时执行,或者这些块有时可以以相反的顺序执行。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作或执行专用硬件与计算机指令的组合的专用的基于硬件的系统来实现。

[0114] 虽然上文已经在运行在计算机和/或计算机上的计算机程序产品的计算机可执行指令的一般上下文中描述了主题,但本领域技术人员将认识到,本公开还可或与其他程序模块组合实现。通常,程序模块包括执行特定任务和/或实现特定抽象数据类型的例程、程序、组件、数据结构等。此外,本领域的技术人员将认识到,本发明的计算机实现的方法可以用其他计算机系统配置来实践,包括单处理器或多处理器计算机系统、小型计算设备、大型计算机、以及计算机、手持式计算设备(例如,PDA、电话)、基于微处理器或可编程的消费者或工业电子产品等。所示出的方面还可以在分布式计算环境中实现,其中,任务由通过通信网络链接的远程处理设备来执行。然而,本发明的一些(如果不是全部的话)方面可在独立计算机上实践。在分布式计算环境中,程序模块可以位于本地和远程存储器存储设备两者中。

[0115] 如在本申请中所使用的,术语“组件”、“系统”、“平台”、“接口”等可以指和/或可以包括计算机相关实体或与具有一个或多个特定功能的操作机器相关的实体。本文公开的实体可以是硬件、硬件和软件的组合、软件或执行中的软件。例如,组件可以是但不限于在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。作为说明,在服务器上运行的应用和服务器两者都可以是组件。一个或多个组件可以驻留在进程和/或执行的线程内,并且组件可以位于一个计算机上和/或分布在两个或更多个计算机之间。在另一实例中,相应组件可从具有存储于其上的不同数据结构的不同计算机可读媒体执行。组件可以经由本地和/或远程进程通信,诸如根据具有一个或多个数据分组的信号(例如,来自与本地系统、分布式系统中的另一组件进行交互的一个组件的数据,和/或经由该信号跨诸如互联网之类的网络与其他系统进行交互的一个组件的数据)。作为另一示例,组件可以是具有由电气或电子电路操作的机械部件提供的特定功能的装置,该电气或电子电路由处理器执行的软件或固件应用操作。在这样的情况下,处理器可以在装置的内部或外部,并且可以执行软件或固件应用的至少一部分。作为又一示例,组件可以是通过没有机械部件的电子组件来提供特定功能的装置,其中电子组件可以包括处理器或用于执行至少部分地赋予电子组件的功能的软件或固件的其他装置。在一方面中,组件可经由例如云计算系统内的虚拟机来仿真电子组件。

[0116] 此外,术语“或”旨在意指包括性的“或”而不是排他性的“或”。也就是说,除非另外指明,或从上下文清楚,“X采用A或B”旨在意指任何自然的包含性排列。即,如果X采用A;X采用B;或X采用A和B两者,则在任何前述情况下满足“X采用A或B”。此外,如主题说明书和附图中所使用的冠词“一个(a)”和“一种(an)”通常应被解释为意指“一个或多个”,除非另外说明或从上下文清楚指向单数形式。如本文所使用的,术语“实例”和/或“示例性”用于表示用作实例、例子或例证。为了避免疑问,在此披露的主题不受此类实例的限制。此外,本文中描述为“实例”和/或“示例性”的任何方面或设计不一定被解释为优于或优于其他方面或设计,也不意味着排除本领域普通技术人员已知的等效的示例性结构和技术。

[0117] 如在本说明书中所采用的,术语“处理器”可以指基本上任何计算处理单元或装置,包括但不限于单核处理器;具有软件多线程执行能力的单处理器;多核处理器;具有软件多线程执行能力的多核处理器;具有硬件多线程技术的多核处理器;并行平台;以及具有分布式共享存储器的并行平台。另外,处理器可指代经设计以执行本文中所描述的功能的集成电路、专用集成电路(ASIC)、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、可编程逻辑控制器(PLC)、复杂可编程逻辑装置(CPLD)、离散门或晶体管逻辑、离散硬件组件或其任何组合。进一步,处理器可以利用纳米级架构,诸如但不限于基于分子和量子点的晶体管、开关和门,以便优化空间使用或增强用户设备的性能。处理器还可以被实现为计算处理单元的组合。在本公开中,诸如与组件的操作和功能相关的“保存”、“存储”、“数据保存”、“数据存储”、“数据库”和实质上任何其他信息存储组件的术语用于指“存储器组件”、体现在“存储器”中的实体、或包括存储器的组件。应当理解,本文所描述的存储器和/或存储器组件可以是易失性存储器或非易失性存储器,或者可以包括易失性存储器和非易失性存储器两者。作为示例而非限制,非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除ROM(EEPROM)、闪存、或非易失性随机存取存储器(RAM)(例如,铁电RAM(FeRAM))。易失性存储器可包括例如可充当外部高速缓冲存储器的RAM。作为说明而非限制,RAM可以以许多形式获得,诸如同步RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双倍数据速率SDRAM(DDRSDRAM)、增强SDRAM(ESDRAM)、同步链接DRAM(SLDRAM)、直接Rambus RAM(DRRAM)、直接Rambus动态RAM(DRDRAM)和Rambus动态RAM(RDRAM)。另外,本文所揭示的系统或计算机实施的方法的存储器组件旨在包含(但不限于)这些和任何其他合适类型的存储器。

[0118] 以上已经描述的内容仅包括系统、计算机程序产品和计算机实现的方法的示例。当然,为了描述本公开的目的,不可能描述组件、产品和/或计算机实现方法的每个可想象的组合,但是本领域普通技术人员可以认识到,本公开的许多进一步的组合和置换是可能的。此外,就在详细描述、权利要求书、附录和附图中使用术语“包括”、“具有”、“拥有”等来说,这些术语旨在以与术语“包含”在权利要求书中用作过渡词时所解释的类似的方式为包含性的。已经出于说明的目的呈现了不同实施例的描述,但并不旨在是详尽的或限于所公开的实施例。在不脱离所描述的实施例的范围的情况下,许多修改和变化对于本领域普通技术人员来说是显而易见的。这里使用的术语被选择来最好地解释实施例的原理、实际应用或对在市场中找到的技术的技术改进,或者使得本领域普通技术人员能够理解这里公开的实施例。

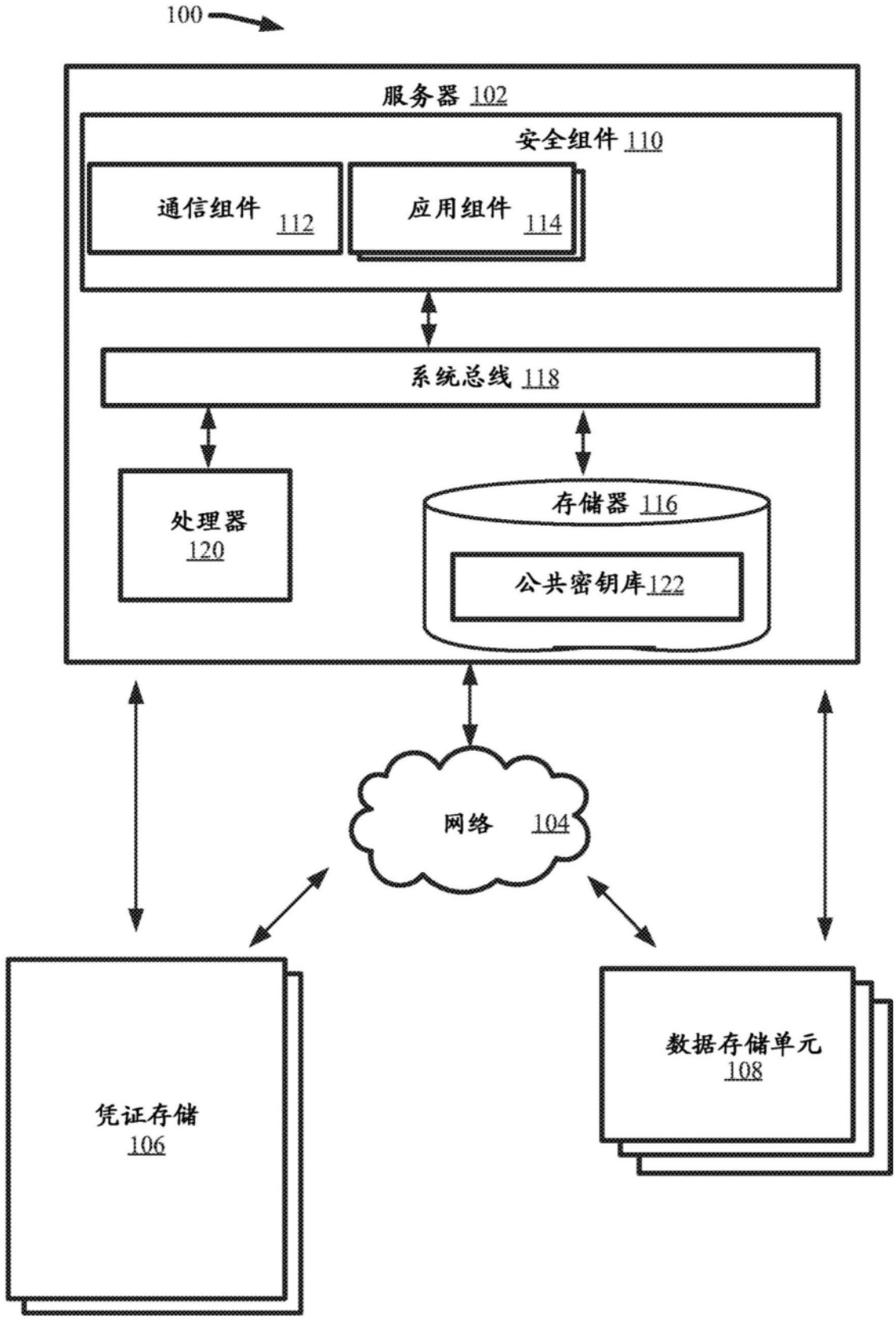

100
服务器 102
安全组件 110
通信组件 112
应用组件 114
系统总线 118
处理器 120
存储器 116
公共密钥库 122
网络 104
凭证存储 106
数据存储单元 108

图1

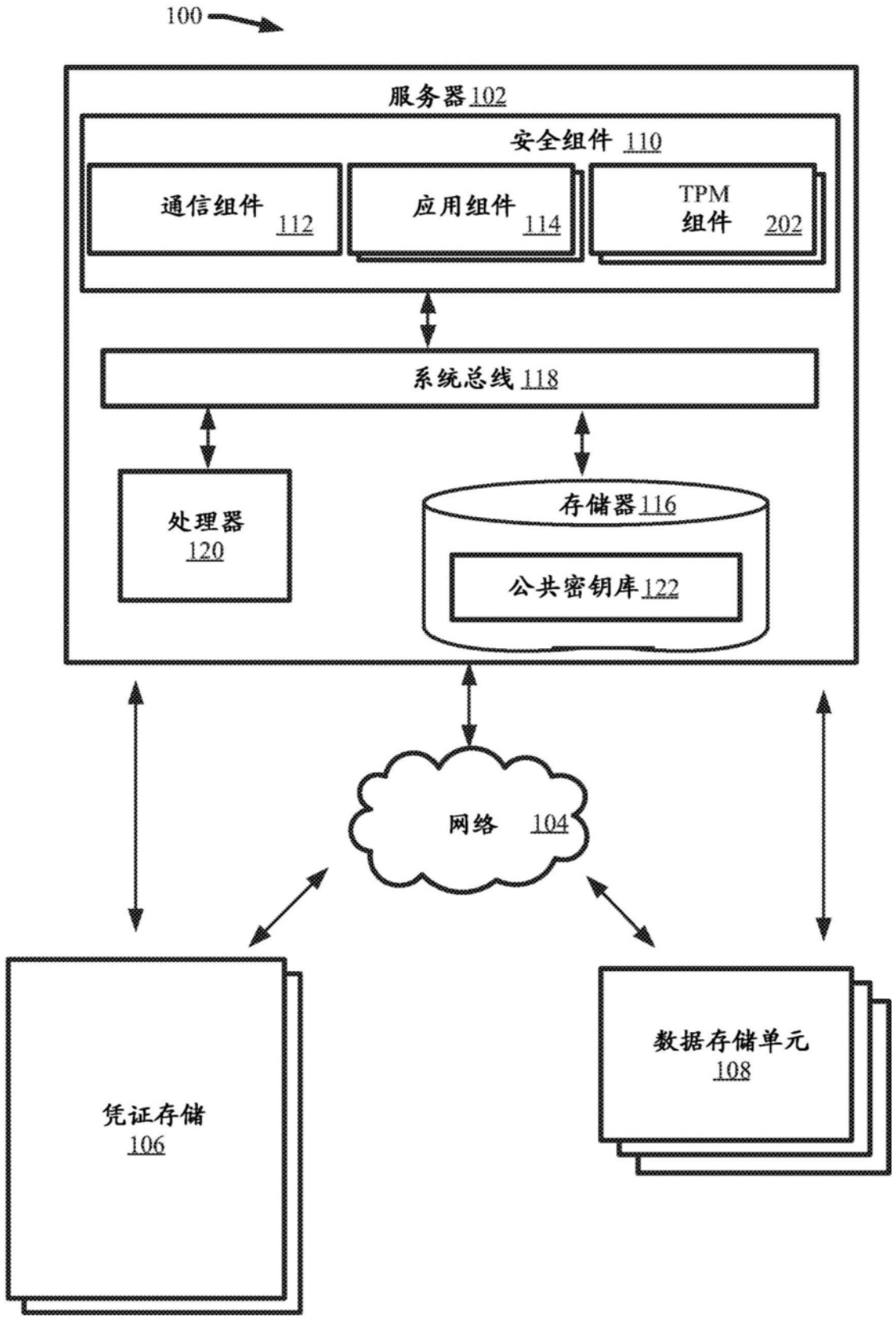

100
服务器102
安全组件 110
通信组件 112
应用组件 114
TPM 组件 202
系统总线 118
处理器 120
存储器116
公共密钥库122
网络 104
凭证存储 106
数据存储单元 108

图2

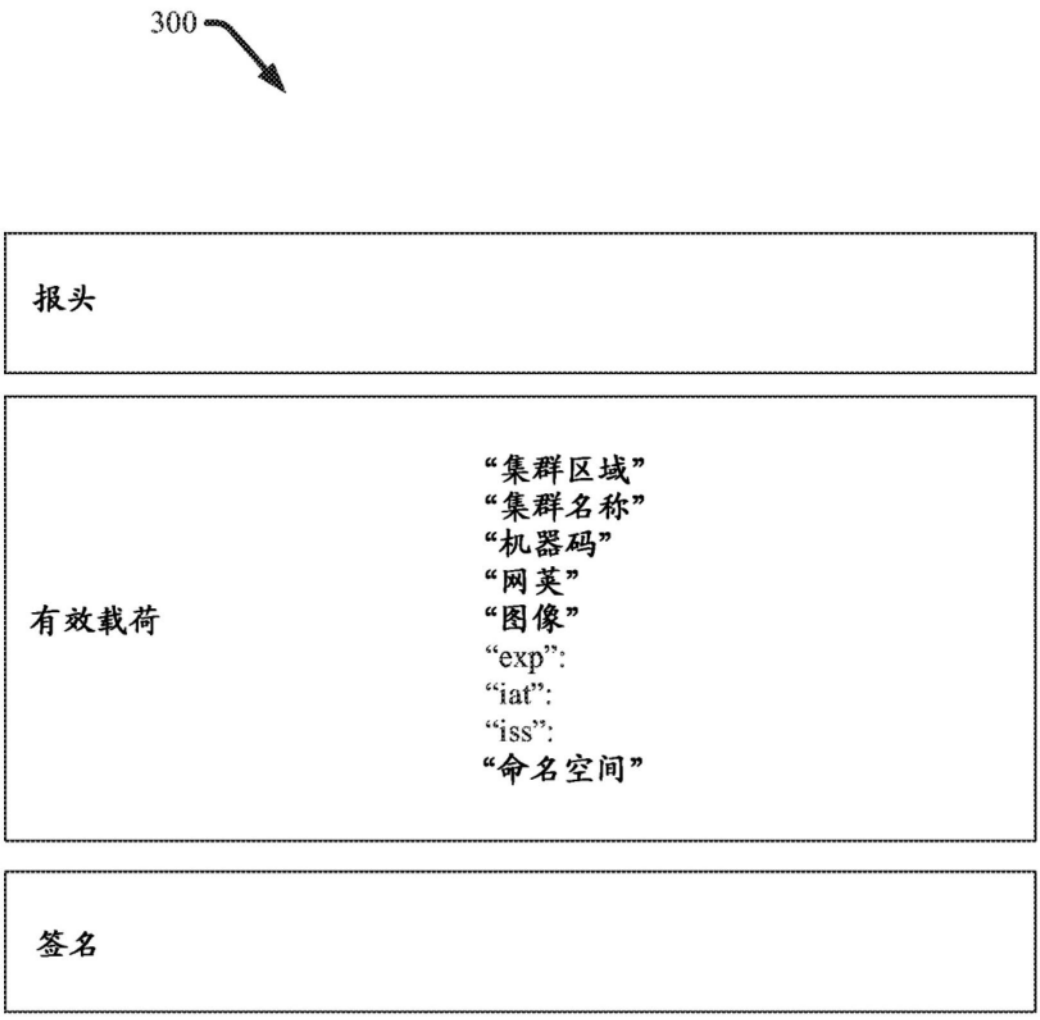


图3

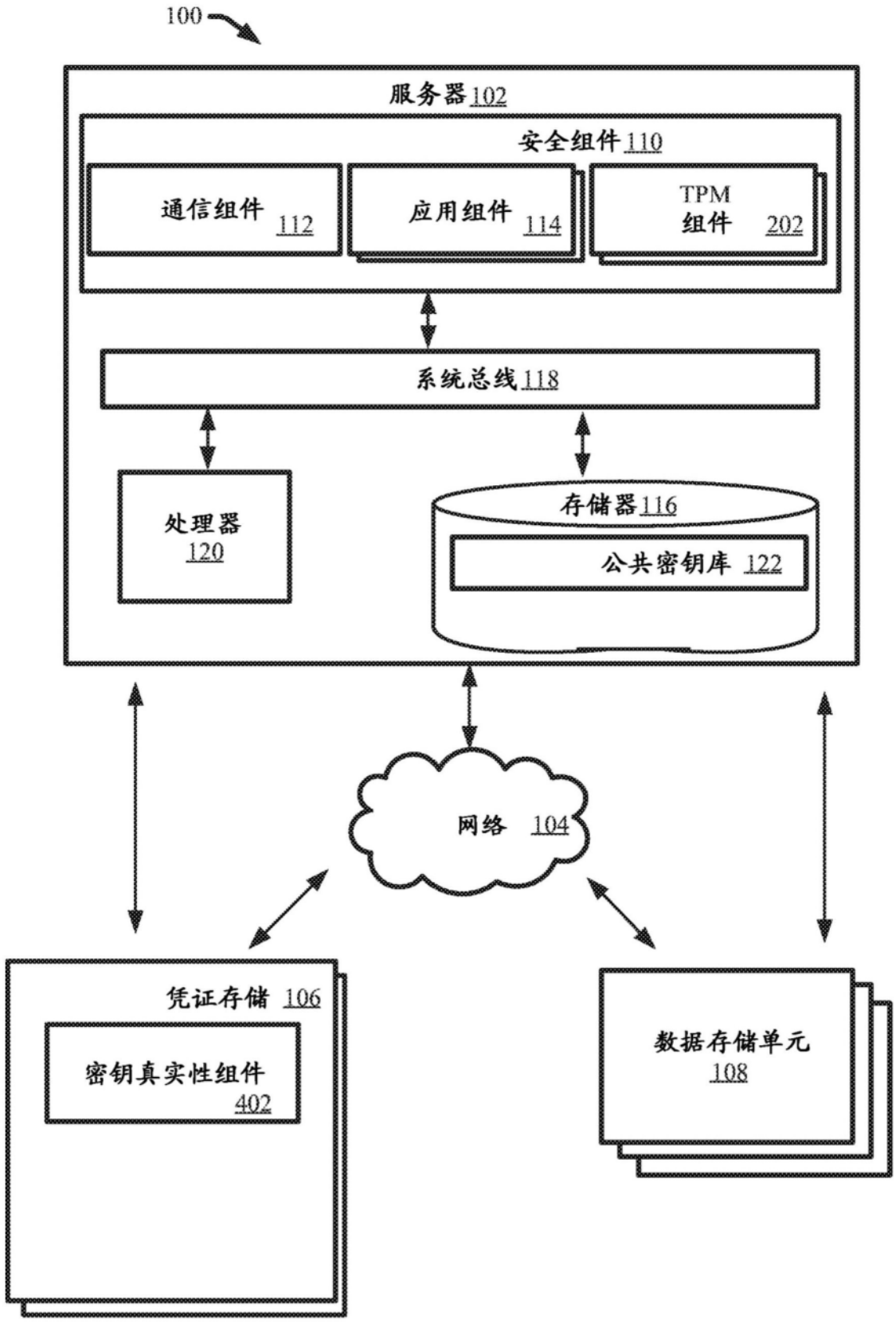

100
服务器102
安全组件110
通信组件 112
应用组件 114
TPM 组件 202
系统总线118
处理器 120
存储器116
公共密钥库 122
网络 104
凭证存储 106
密钥真实性组件 402
数据存储单元 108

图4

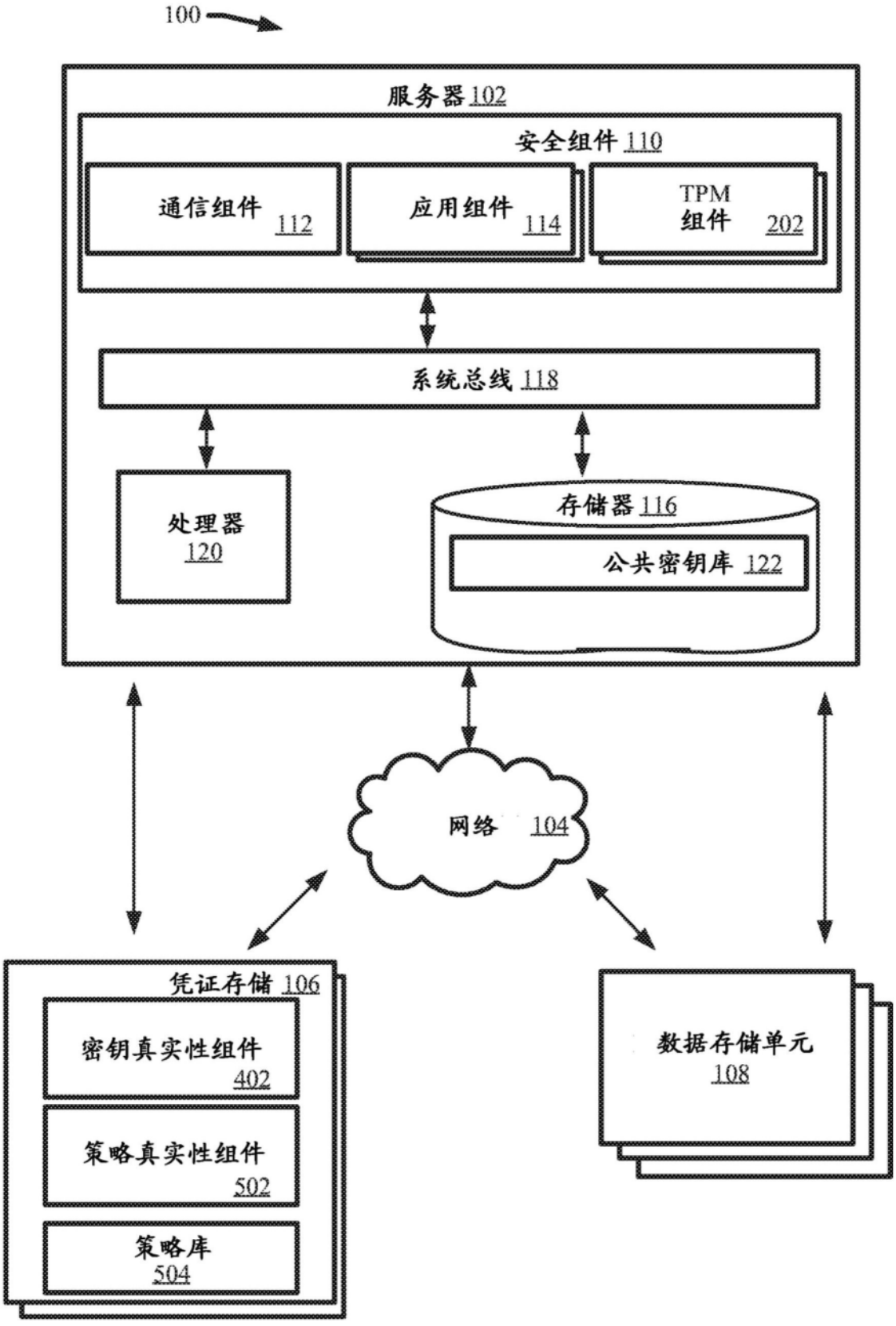

100
服务器 102
安全组件 110
通信组件 112
应用组件 114
TPM 组件 202
系统总线 118
处理器 120
存储器 116
公共密钥库 122
网络 104
凭证存储 106
密钥真实性组件 402
策略真实性组件 502
策略库 504
数据存储单元 108

图5

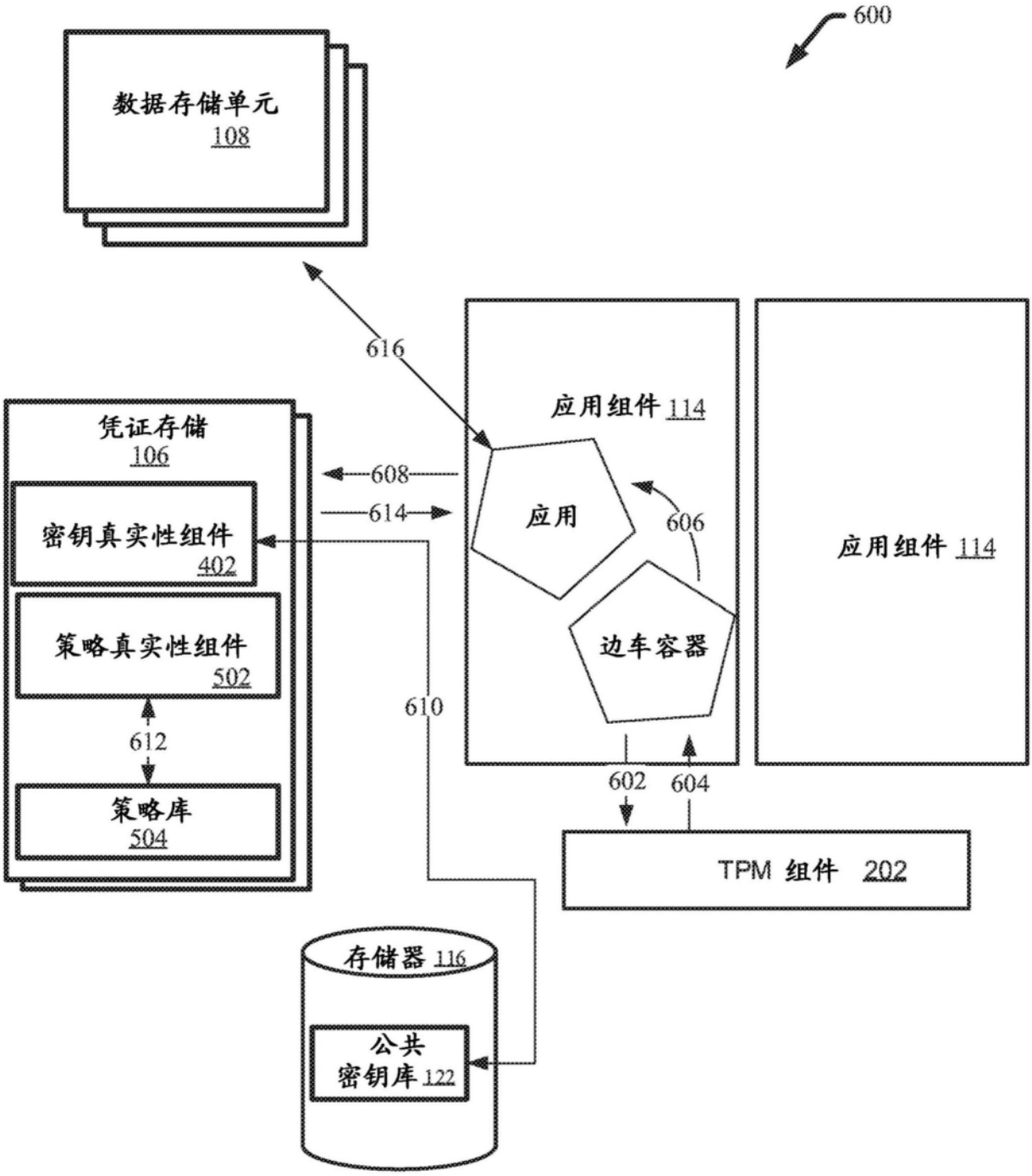

600
数据存储单元
108
616
应用组件 114
凭证存储
106
608
614
密钥真实性组件
402
应用
606
应用组件 114
策略真实性组件
502
边车容器
610
612
策略库
504
602
604
TPM 组件 202
存储器 116
公共
密钥库 122

图6

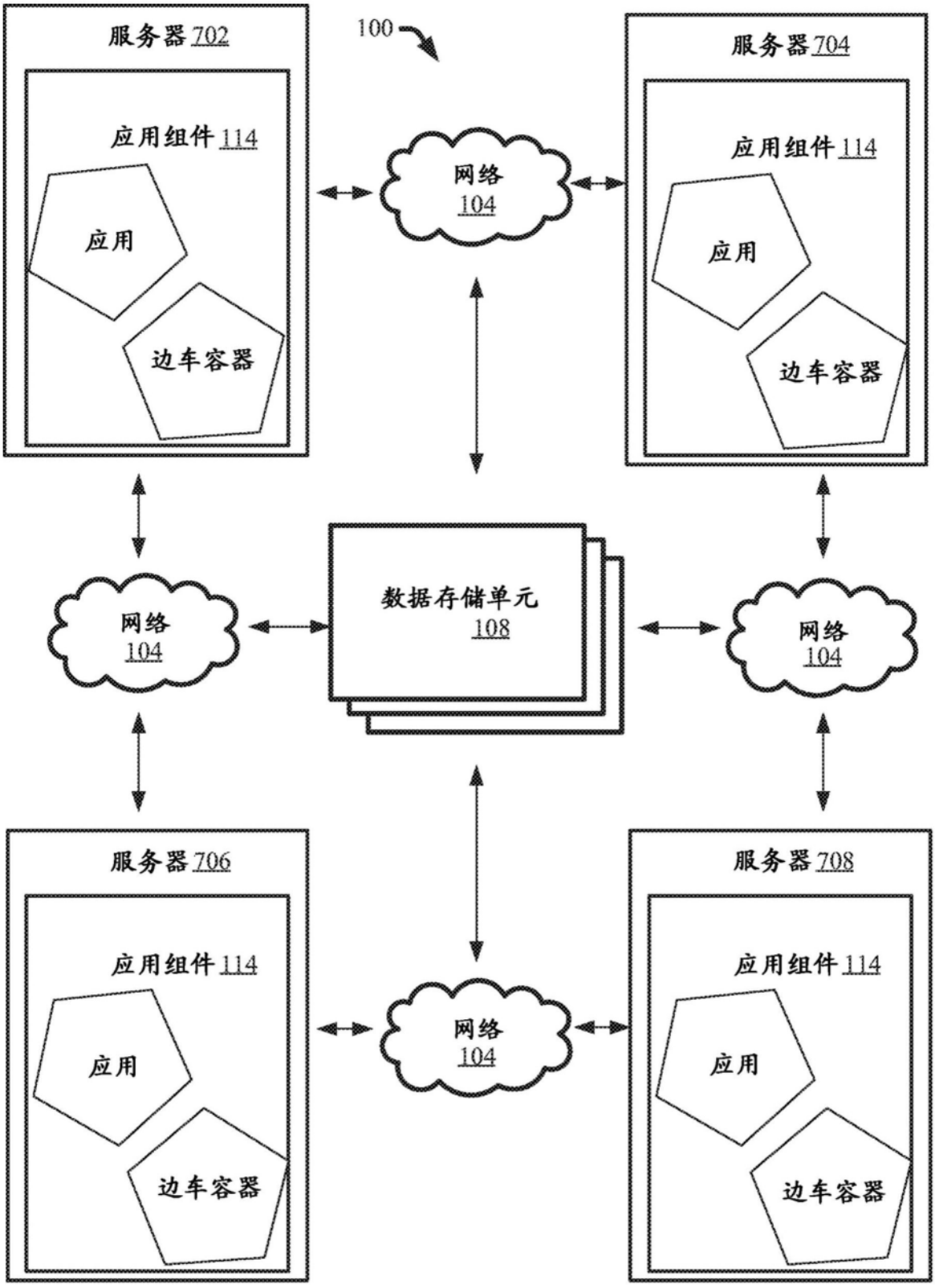

服务器 702
100
服务器 704
应用组件 114
网络
104
应用
边车容器
应用组件 114
应用
边车容器
网络
104
数据存储单元
108
网络
104
服务器 706
服务器 708
应用组件 114
网络
104
应用
边车容器
应用组件 114
应用
边车容器

图7

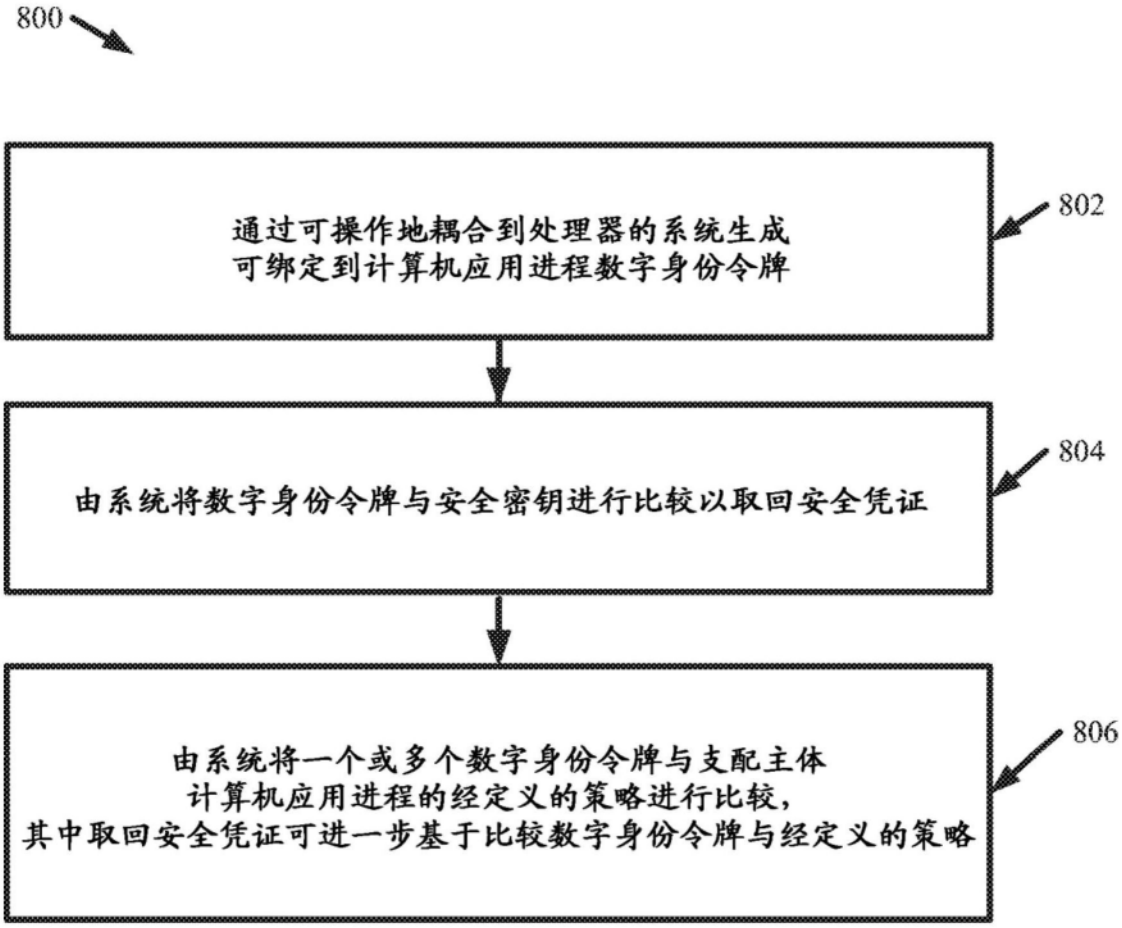

800
通过可操作地耦合到处理器的系统生成
可绑定到计算机应用进程数字身份令牌
802
由系统将数字身份令牌与安全密钥进行比较以取回安全凭证
804
由系统将一个或多个数字身份令牌与支配主体
计算机应用进程的经定义的策略进行比较，
其中取回安全凭证可进一步基于比较数字身份令牌与经定义的策略
806

图8

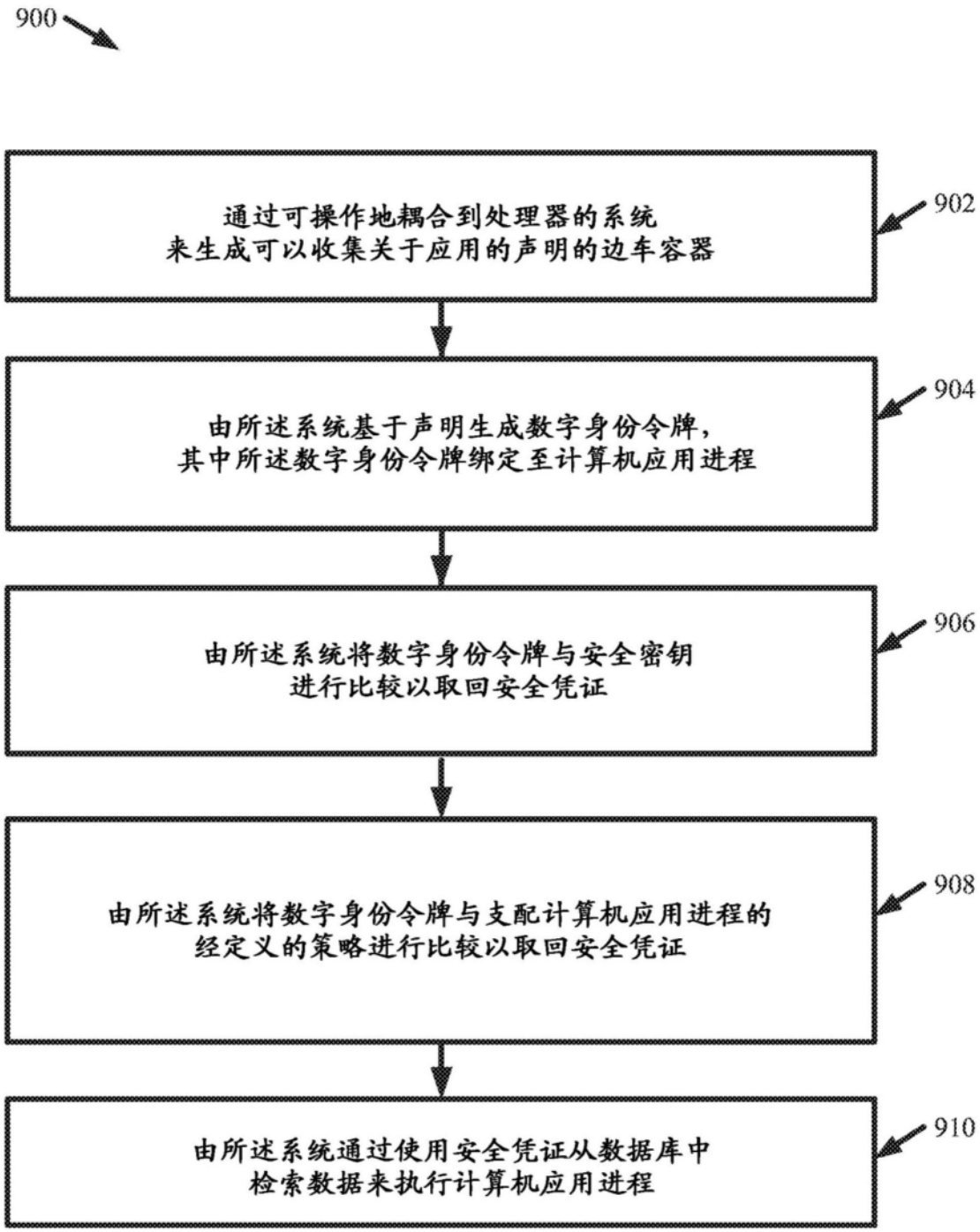

900
通过可操作地耦合到处理器的系统
来生成可以收集关于应用的声明的边车容器
902
由所述系统基于声明生成数字身份令牌，
其中所述数字身份令牌绑定至计算机应用进程
904
由所述系统将数字身份令牌与安全密钥
进行比较以取回安全凭证
906
由所述系统将数字身份令牌与支配计算机应用进程的
经定义的策略进行比较以取回安全凭证
908
由所述系统通过使用安全凭证从数据库中
检索数据来执行计算机应用进程
910

图9

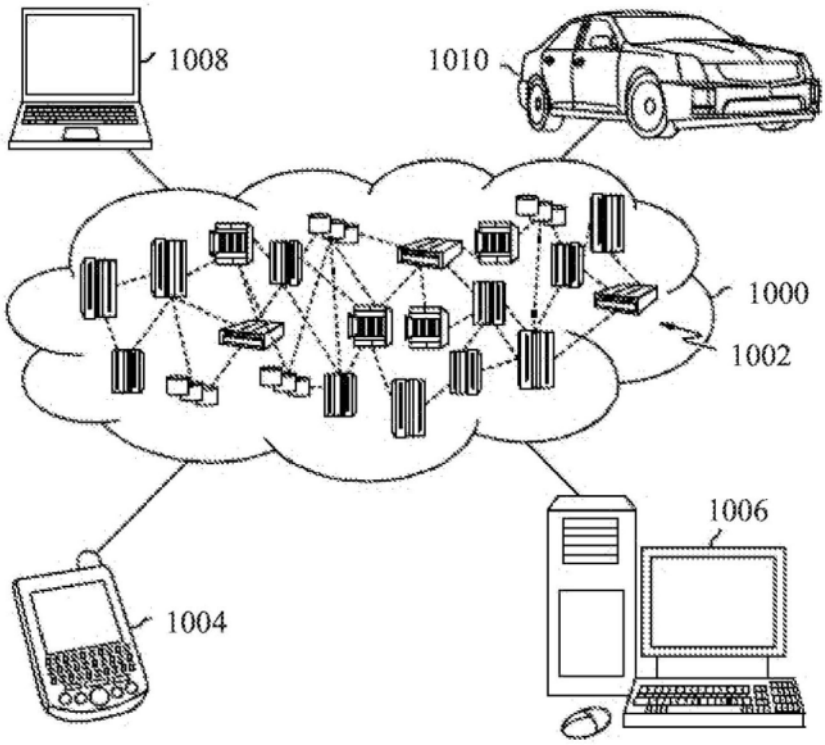

1008
1010
1000
1002
1006
1004

图10

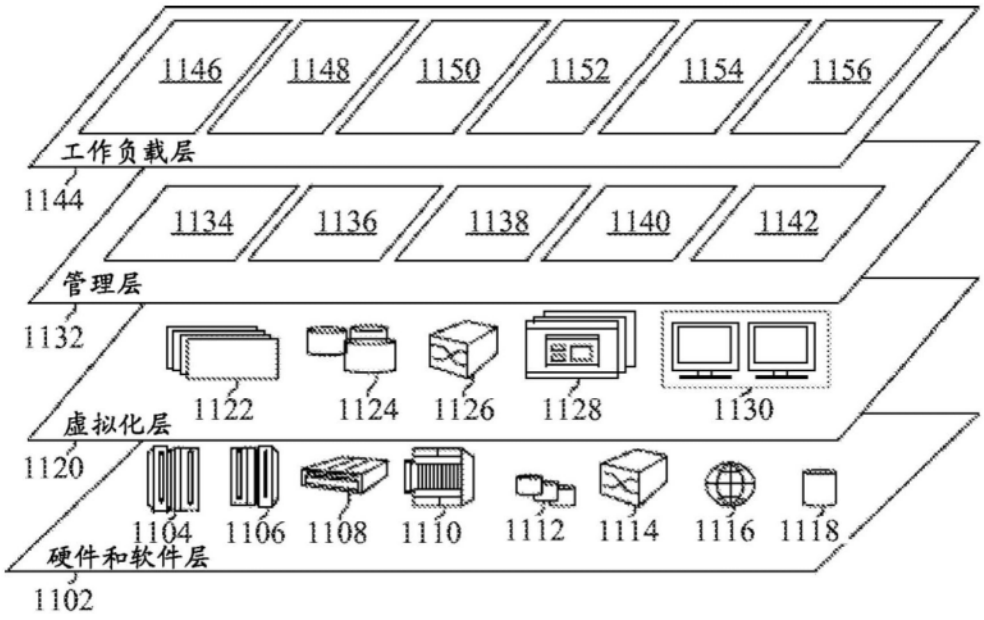

1146
1148
1150
1152
1154
1156
工作负载层
1144
1134
1136
1138
1140
1142
管理层
1132
1122
1124
1126
1128
1130
虚拟化层
1120
1104
1106
1108
1110
1112
1114
1116
1118
硬件和软件层
1102

图11

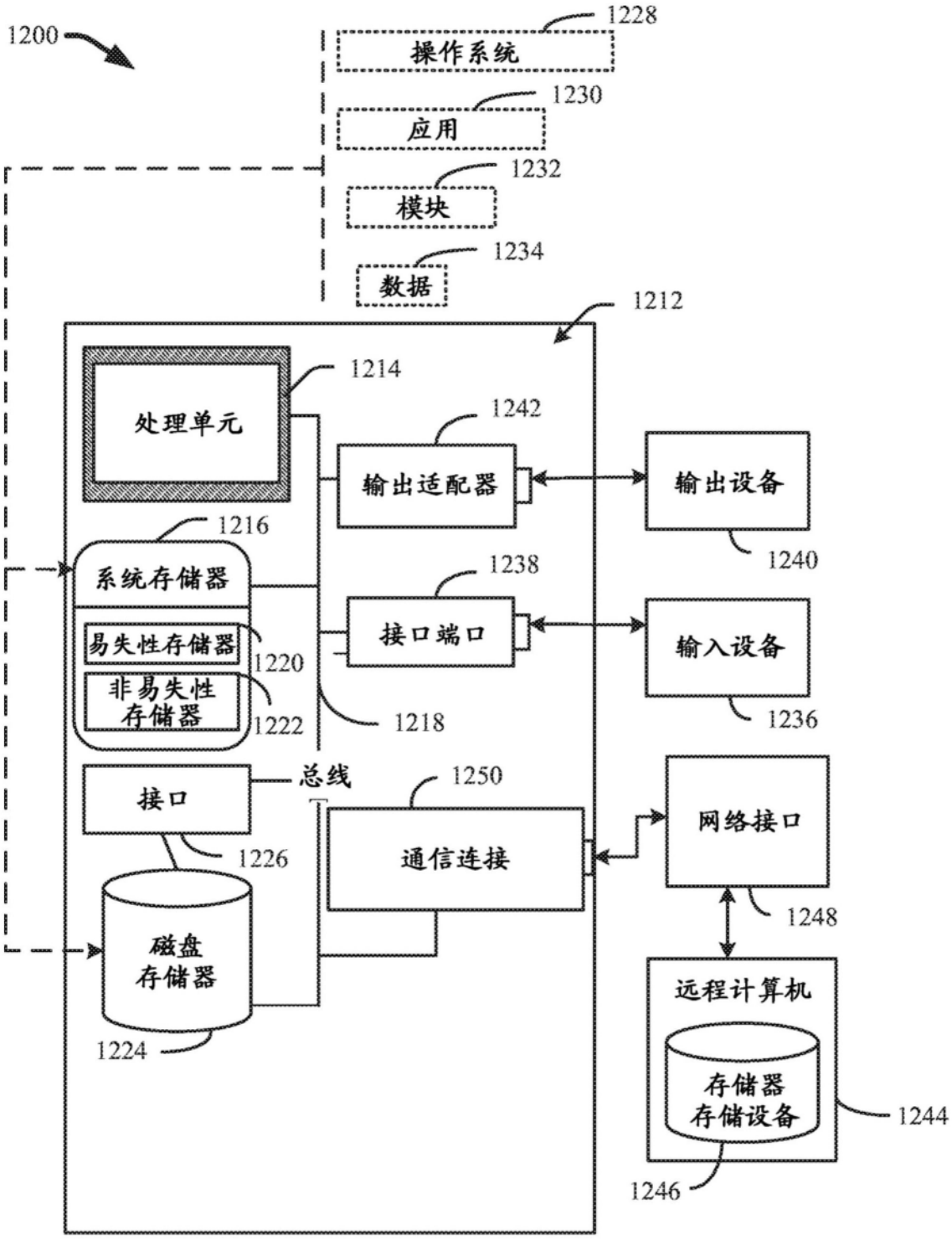

1200
1228
操作系统
1230
应用
1232
模块
1234
数据
1212
1214
处理单元
1242
输出适配器
输出设备
1240
1216
系统存储器
易失性存储器
1220
非易失性存储器
1222
1238
接口端口
输入设备
1236
1218
总线
接口
1226
1250
通信连接
网络接口
1248
磁盘存储器
1224
远程计算机
存储器存储设备
1244
1246

图12