(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109844748 B
(45)授权公告日 2023.01.06

(21)申请号 201780064096.X
(22)申请日 2017.10.16
(65)同一申请的已公布的文献号
申请公布号 CN 109844748 A
(43)申请公布日 2019.06.04
(30)优先权数据
15/333,573 2016.10.25 US
(85)PCT国际申请进入国家阶段日
2019.04.17
(86)PCT国际申请的申请数据
PCT/US2017/056703 2017.10.16
(87)PCT国际申请的公布数据
WO2018/080814 EN 2018.05.03
(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 M·E·皮尔逊 T·阿卡 R·弗玛
(74)专利代理机构 北京市金杜律师事务所 11256
专利代理师 王茂华 彭梦晔
(51)Int.Cl.
G06F 21/53(2006.01)

(56)对比文件
US 2013152047 A1,2013.06.13
US 2007230706 A1,2007.10.04
CN 104982005 A,2015.10.14
CN 102208000 A,2011.10.05
CN 104756127 A,2015.07.01
CN 105493099 A,2016.04.13
JP 2009175945 A,2009.08.06
US 2009172781 A1,2009.07.02
US 2010082991 A1,2010.04.01
CN 104486307 A,2015.04.01
US 2015074764 A1,2015.03.12
US 2012266209 A1,2012.10.18
王栋博.网格服务中虚拟计算环境的可信保证机制.《微计算机信息》.2008,(第03期),
祝凯捷等.密钥安全及其在虚拟化技术下的新发展.《密码学报》.2016,(第01期),
M. Ku, D. Min and E. Choi.Analysis of virtual machine creation characteristics on virtualized computing environment.《The 7th International Conference on Networked Computing and Advanced Information Management》.2011,

审查员 赵喆

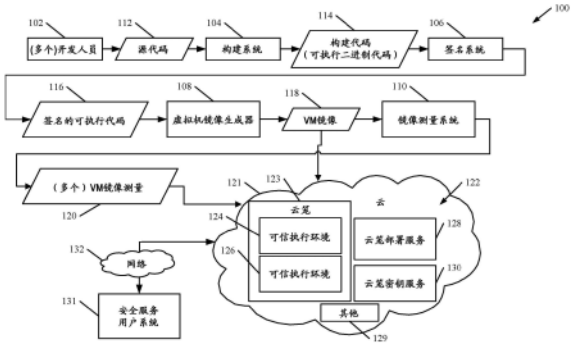
权利要求书3页 说明书11页 附图6页

(54)发明名称

托管在虚拟安全环境中的安全服务的计算系统及方法

(57)摘要

执行环境具有所部署的虚拟机镜像。虚拟机镜像提供由角色标识的服务。执行环境生成虚拟机镜像的测量并且将其提供给密钥服务以请求启用执行环境中的虚拟机镜像的操作的角色密钥。密钥服务确定虚拟机镜像是否被映射到角色,并且如果是,则将角色密钥返回给请求执行环境。



CN 109844748 B

1.一种计算系统,包括:

至少一个处理器;以及

存储器,所述存储器存储由所述至少一个处理器可执行的指令,其中所述指令当被执行时,提供:

策略引擎,所述策略引擎被配置为:

接收角色标识符,所述角色标识符标识角色,所述角色表示要由执行环境托管的服务,

接收虚拟机VM镜像测量,所述VM镜像测量指示被部署在所述执行环境中的VM镜像,

基于测量到角色映射来确定所述VM镜像测量是否被映射到所述角色,以及

生成指示所述确定的评估信号;

密钥包装密码引擎,所述密钥包装密码引擎被配置为:

基于指示所述VM镜像测量被映射到所述角色的所述评估信号,来包装一组角色密钥,所述角色密钥:

对应于所述角色,以及

支持所述执行环境执行所述服务;以及

密钥服务,所述密钥服务被配置为为所述执行环境提供经包装的所述一组角色密钥。

2.根据权利要求1所述的计算系统,其中所述策略引擎被配置为接收所述角色标识符、所述VM镜像测量和来自请求执行环境的执行环境标识符,所述执行环境标识符标识所述请求执行环境。

3.根据权利要求2所述的计算系统,其中所述策略引擎被配置为基于所述执行环境标识符来确定所述请求执行环境是否被映射到所述VM镜像测量,并且基于所述确定来生成所述评估信号。

4.根据权利要求2所述的计算系统,其中所述策略引擎被配置为:

访问一组测量到角色映射,所述一组测量到角色映射将多个不同组角色中的每个角色映射到不同的VM镜像测量;以及

基于所述一组测量到角色映射来确定所述VM镜像测量是否被映射到所述角色。

5.根据权利要求4所述的计算系统,其中所述指令提供:

角色密钥储存器/生成器,所述角色密钥储存器/生成器被配置为向所述密钥包装密码引擎提供所述一组角色密钥;以及

一组密钥包装器密钥,每个密钥包装器密钥被映射到给定角色,

其中所述密钥包装密码引擎被配置为:

标识被映射到由所述角色标识符标识的所述角色的一个或多个密钥包装器密钥,以及

利用所标识的所述一个或多个密钥包装器密钥来加密所述角色密钥。

6.根据权利要求1所述的计算系统,其中所述指令提供:

部署引擎,所述部署引擎被配置为:

接收所述角色标识符,

基于所述角色标识符来获取所述VM镜像,以及

将所述VM镜像部署到所述执行环境。

7.根据权利要求6所述的计算系统,其中所述指令提供:

一组角色到镜像映射,每个角色到镜像映射将角色映射到VM镜像,

其中所述部署引擎被配置为访问所述一组角色到镜像映射以标识所述VM镜像。

8.根据权利要求7所述的计算系统,其中所述指令提供:

VM镜像存储库,所述VM镜像存储库被配置为:

存储所述VM镜像,

其中所述部署引擎被配置为从所述VM镜像存储库获取所述VM镜像以用于部署。

9.根据权利要求6所述的计算系统,其中所述执行环境包括:

测量系统,所述测量系统被配置为生成所述VM镜像测量并且向所述密钥服务提供所述VM镜像测量。

10.根据权利要求9所述的计算系统,其中所述测量系统被配置为对所述VM镜像执行散列函数以获取包括所述VM镜像测量的散列值。

11.一种由计算系统执行的方法,所述方法包括:

标识与执行环境相关联的服务,所述执行环境被配置为执行所述服务;

标识虚拟机VM镜像测量,所述VM镜像测量指示被部署在所述执行环境中的VM镜像;

基于测量到角色映射来确定所述VM镜像测量是否被映射到所述服务;

生成指示所述确定的评估信号;

响应于所述评估信号指示所述VM镜像测量被映射到所述服务,获取一组角色密钥,所述角色密钥:

对应于所述服务,以及

支持所述执行环境执行所述服务;

加密所述一组角色密钥中的所述角色密钥;以及

为所述执行环境提供经加密的所述一组角色密钥。

12.根据权利要求11所述的方法,还包括:

接收标识所述服务的角色标识符;

接收所述VM镜像测量;以及

从所述执行环境接收执行环境标识符,所述执行环境标识符标识所述执行环境,并且其中确定所述VM镜像测量是否被映射到所述服务包括基于所述执行环境标识符来确定所述执行环境是否被映射到所述VM镜像测量,并且生成所述评估信号包括基于所述确定来生成所述评估信号。

13.根据权利要求12所述的方法,其中确定所述VM镜像测量是否被映射到所述服务包括:

通过访问将多个不同组的角色中的每个角色映射到不同的VM镜像测量的测量到角色映射的资产来确定所述VM镜像测量是否被映射到所述角色。

14.根据权利要求13所述的方法,其中加密所述角色密钥包括:

标识被映射到所述角色的一个或多个密钥包装器密钥;以及

利用所标识的所述一个或多个密钥包装器密钥来加密所述角色密钥。

15.根据权利要求11所述的方法,还包括:

在部署系统处接收所述角色;

通过访问一组角色到镜像映射来基于所述角色在所述部署系统处获取所述VM镜像,所述一组角色到镜像映射将所述角色映射到所述VM镜像;以及

将所述VM镜像部署到所述执行环境。

16.根据权利要求15所述的方法,还包括:

利用所述执行环境中的测量系统生成所述VM镜像测量;以及

向密钥服务提供所述VM镜像测量。

17.根据权利要求16所述的方法,其中生成所述VM镜像测量包括:

利用所述测量系统,对所述VM镜像执行散列函数,以获取包括所述VM镜像测量的散列值。

18.一种计算系统,包括:

至少一个处理器;以及

存储器,所述存储器存储由所述至少一个处理器可执行的指令,其中所述指令当被执行时将所述计算系统配置为:

执行由所部署的虚拟机VM镜像表示的并且由角色标识的服务;

将散列函数应用于所述VM镜像以生成VM镜像测量;

向密钥服务提供所述角色和所述VM镜像测量以请求一组角色密钥;

从所述密钥服务接收经包装的一组角色密钥;

解密经包装的所述一组角色密钥以获取所请求的所述一组角色密钥;以及

使用所请求的所述角色密钥来执行所述服务。

19.根据权利要求18所述的计算系统,其中所述指令将所述计算系统配置为:

从执行环境接收所述角色和所述VM镜像测量,所述角色标识所述服务,所述VM镜像测量指示被部署在所述执行环境中的所述VM镜像;

确定所述VM镜像测量被映射到所述角色;生成指示所述确定的评估信号;

基于指示所述VM镜像测量被映射到所述角色的所述评估信号,包装所述一组角色密钥;以及

为所述执行环境提供经包装的所述一组角色密钥。

20.根据权利要求19所述的计算系统,其中所述指令将所述计算系统配置为:

访问一组角色到镜像映射,所述一组角色到镜像映射将所述角色映射到所述VM镜像;

通过基于所述角色访问所述角色到镜像映射来从VM镜像存储库获取所述VM镜像以用于部署;以及

将所述VM镜像部署到所述执行环境。

托管在虚拟安全环境中的安全服务的计算系统及方法

技术领域

[0001] 本公开的实施例涉及计算机领域，并且更具体地，涉及托管在虚拟安全环境中的安全服务的计算系统及方法。

背景技术

[0002] 计算机系统目前广泛使用。一些这样的计算机系统部署在它们托管服务的远程服务器环境中(诸如在云中)。

[0003] 所托管的服务可以是安全性很重要的服务。例如，所托管的一些服务可以是支付服务、信用卡处理服务、银行服务或处理机密信息的各种其他服务。

[0004] 这些类型的系统具有通常托管在离散系统上的基础设施。作为示例，所托管的每个服务可以托管在单独的或分立的物理机器上。这些机器可以部署在物理笼式环境中以提供物理安全性。此外，为这些类型的系统编写代码的开发人员或其他程序员经常可以使用相对隔离的网络来进入安全或笼式物理设施，以再次提高与部署在这样的服务上的开发代码相关的安全性。

[0005] 这可能导致针对诸如服务等的很多缺点。作为示例，由于每个服务通常部署在专用物理机器(或服务器)上并且不涉及虚拟化，因此可扩展性可能非常困难。为了扩展这样的服务，必须为其他服务或服务实例添加其他物理机器。此外，由于开发人员或程序员需要在物理安全且严格控制的环境中生成代码，所以这可能导致刚性，因为很难进行更改。

[0006] 以上讨论仅仅是为了一般背景信息而提供的，并不旨在用于帮助确定所要求保护的主题的范围。

发明内容

[0007] 执行环境具有所部署的虚拟机镜像。虚拟机镜像提供由角色标识的服务。执行环境生成虚拟机镜像的测量并且将其提供给密钥服务以请求启用执行环境中的虚拟机镜像的操作的角色密钥。密钥服务确定虚拟机镜像是否被映射到角色，并且如果是，则将角色密钥返回给请求执行环境。

[0008] 提供本“发明内容”是为了以简化的形式介绍一些概念，这些概念将在下面的“具体实施方式”中进一步描述。本“发明内容”不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。所要求保护的主题不限于解决背景技术中提到的任何或所有缺点的实现。

附图说明

[0009] 图1是示出用于开发服务和生成与服务相对应的虚拟机镜像的开发通道的一个示例的流程图。

[0010] 图2是云笼架构的一个示例的框图。

[0011] 图3是示出部署服务的操作的一个示例的流程图。

[0012] 图4是示出执行环境的操作的一个示例的流程图。

[0013] 图5是示出在向执行环境提供所请求的角色密钥时密钥服务的操作的一个示例的流程图。

[0014] 图6是示出可以在图1所示的架构中使用的计算环境的一个示例的框图。

具体实施方式

[0015] 图1是示出开发通道100的操作的一个示例的流程图。开发通道 100说明性地包括开发人员102、构建系统104、签名系统106、虚拟机镜像生成器108和镜像测量系统110。图1还示出了开发通道100 可以耦合到云架构122，云架构122包括云笼123(其本身包括可信执行环境124和126)、云笼部署服务128和云笼密钥服务130，并且云架构122可以包括其他项目129。图1还示出了一个或多个安全服务用户系统131可以通过网络132访问架构122。

[0016] 在图1所示的示例中，开发人员102说明性地开发源代码112，源代码112是要在所托管的安全服务中(诸如在可信执行环境124-126 中)运行的代码。这样的服务可以是支付服务、银行服务、信用卡处理服务或各种其他服务中的任何一种。

[0017] 构建系统104接收源代码112并且将代码构建成可执行二进制代码(或其他构建代码)114。代码114是说明性地编译的可执行代码，其可以包括脚本和各种数据文件。它说明性地被提供给签名系统106。签名系统106说明性地对代码114进行签名以生成签名的可执行代码 116。因为代码116被签名，所以这可以确保其在签名发生之后不被修改。签名还可以指示代码签名者(或签名系统106的身份)。

[0018] 然后，虚拟机镜像生成器108通过组合适当的操作系统镜像和签名的可执行代码116来生成虚拟机镜像。所得到的虚拟机(VM)镜像118可以包括一个或多个服务以及可以被部署以在执行环境中实现这些服务的数据库。在一个示例中，虚拟机镜像生成器108可以使用虚拟硬盘驱动器格式作为虚拟机的硬盘。这可以允许多个操作系统驻留在单个机器上。

[0019] 然后，镜像测量系统110基于虚拟机镜像118生成一个或多个虚拟机镜像测量120。测量120说明性地包括表示每个镜像118的可重新计算的强身份。在一个示例中，每个测量120可以是在对应的VM 镜像118上计算的密码散列值。然后，可以将VM镜像118及其对应的测量120提供给云环境(或云架构)122，在云环境122中，VM镜像118及其对应的测量120可以由一个或多个可信执行环境124-126 的虚拟机执行。

[0020] 可以将VM镜像118以及角色到VM镜像映射提供给云笼部署服务128，角色到VM镜像映射将VM镜像118映射到与其将执行的服务相对应的特定角色。可以将VM测量120以及测量到角色映射提供给云笼密钥服务130，测量到角色映射将VM镜像118的特定测量也映射到角色。另外，用于执行VM镜像118之一的特定可信执行环境 124-126可以向云笼密钥服务130发送可信执行环境标识符，该可信执行环境标识符标识将部署由VM镜像测量120表示的VM镜像118 的特定可信执行环境。

[0021] 简而言之，在操作中，云笼部署服务128可以将特定VM镜像部署到可信执行环境124-126。然后，环境124-126可以从云笼密钥服务130请求角色密钥。云笼密钥服务130标识特定VM镜像是否适合于特定角色和请求执行环境，并且如果是，则向请求执行环境返回加密的角色密钥以便它可以操作以执行其服务。

[0022] 图1还示出了一旦将服务(诸如支付服务或其他安全服务)部署到可信执行环境

124-126中，支付(或其他安全服务)用户系统131 就可以通过网络132和云121在可信执行环境之一中访问服务。作为示例，如果安全服务是信用卡处理服务，则用户系统131可以是需要信用卡处理的信用卡公司处的系统。如果它是银行服务，则系统131 可以部署在银行处。这些仅是示例。

[0023] 网络132可以是各种网络中的任何一种，诸如广域网、局域网、或各种其他有线或无线网络或网络组合中的任何一种。为了举例，下面列出了一些。

[0024] 图2是更详细地示出部署在云121中的云笼架构122的一个示例的框图。图2所示的一些项目与图1所示的项目相似，并且它们的编号相似。

[0025] 在描述图2所示的架构122的整体操作之前，首先提供图2中的一些项目及其操作的简要描述。在图2所示的示例中，云笼123可以包括一个或多个处理器或服务器136、可信执行环境124-126，并且还可以包括其他项目。可信执行环境124可以包括管理程序138和一个或多个虚拟机140以及解密系统141和测量系统142。它还可以包括其他项目144。可信执行环境126还可以包括管理程序146，或者管理程序138和146可以实现为用于生成虚拟机140-148的单个管理程序。执行环境126还可以包括描述系统149和测量系统150以及各种其他项目152。可信执行环境124-126可以是相似的或不同的。出于本描述的目的，将假定它们是相似的，并且因此本文中将仅提供可信执行环境124的操作。

[0026] 虚拟机140说明性地从云笼部署服务128(其在下面更详细地描述)接收虚拟机镜像并且执行该镜像。测量系统142可以测量部署在虚拟机140上的镜像。可以通过将密码散列函数应用于镜像来生成测量。例如，在镜像由虚拟硬盘镜像表示的情况下，可以通过将SHA-256 散列应用于该镜像来生成测量。这仅是一个示例，并且也可以使用用于生成虚拟机镜像的测量的各种其他方式。在执行由VM镜像表示的服务时，可信执行环境124可以公开用户系统131可以与之交互以使用服务的应用程序编程接口(API)151。

[0027] 为了将虚拟机镜像部署到可信执行环境124，可以使用云笼部署服务128。在一个示例中，服务128可以包括一个或多个处理器或服务器154、部署引擎156、虚拟机镜像存储库158、角色到虚拟机镜像映射160，并且可以包括其他项目162。可信执行环境124说明性地向部署引擎156提供角色(其表示其要执行的服务)。然后，部署引擎156访问角色到VM镜像映射160以标识与该角色相对应的特定 VM镜像，并且从VM镜像存储库158获取该镜像。然后，它在请求可信执行环境124中在虚拟机140上部署该VM镜像。这将在下面参考图3更详细地描述。

[0028] 一旦VM镜像部署在虚拟机140上，可信执行环境124说明性地仍然需要它将使用的角色密钥以便执行已经部署的特定服务(或角色)。也就是说，所部署的虚拟机镜像可以包括表示一个或多个服务和数据库的代码，但是它还没有执行其操作所需要的密钥。因此，可信执行环境124生成部署在虚拟机140上的VM镜像的测量，并且将其与角色(对应于服务)一起提供给云笼密钥服务130以便获取其需要操作的角色密钥。

[0029] 云笼密钥服务130可以包括一个或多个处理器或服务器164、虚拟可信执行环境(VTEE)密钥服务166、策略引擎168、密钥包装密码引擎170、VM镜像测量储存器172、测量到角色映射174、角色密钥储存器/生成器176、密钥包装器密钥178，并且还可以包括各种其他项目180。VTEE密钥服务166向策略引擎168提供请求(虚拟机镜像测量和对应角色以及请求可信执行环境124的身份)。策略引擎 168访问VM镜像测量172以验证请求可信执行环境是

用于执行由 VM镜像表示的特定角色的适当环境。引擎168还访问测量到角色映射174以标识由可信执行环境124提供的VM镜像测量是否被映射到由可信执行环境124在其对密钥的请求中标识的角色。如果策略引擎 168肯定地评估，则这指示请求密钥的可信执行环境是用于执行所标识的角色的适当环境。它还指示部署在可信执行环境124中的VM镜像中的代码(例如，操作系统、代码、数据库等)的测量映射到由可信执行环境124标识的角色。因此，这指示可信执行环境124是适当的，并且代码尚未被改变并且映射到所标识的角色。

[0030] 在这种情况下，VTEE密钥服务166请求密钥包装密码引擎从角色密钥储存器/生成器176获取所标识的角色的角色密钥，并且用一个或多个密钥包装器密钥178包装这些密钥或对它们进行加密。然后，将包装的密钥提供回VTEE密钥服务166，VTEE密钥服务166将它们返回到请求可信执行环境124。在那里，它们可以由解密系统141 解密并且用于在该环境中执行服务(或角色)。

[0031] 图3是更详细地示出云笼部署服务128的操作的一个示例的流程图。部署引擎156首先接收标识要被部署到可信执行环境124中的角色的角色标识符。这由图3中的框190指示。角色说明性地对应于要由可信执行环境124托管的安全服务，诸如支付服务、信用卡服务等。这由框192指示。角色标识符可以是任意字符串194或其他表示196。

[0032] 然后，部署引擎156访问角色到VM镜像映射160以标识与角色相对应的特定VM镜像。访问角色到VM镜像映射由框198指示，并且基于这些映射来标识角色被映射到的VM镜像由框200指示。在一个示例中，映射被表示为如下面的等式1所示，其中“IMAGE(图像)”以虚拟镜像格式表示，并且“H”是密码散列函数。

[0033] $$\emptyset: Role \rightarrow H(IMAGE)$$ 等式 1

[0034] 角色映射Φ可以用角色映射签名密钥K_{Φ}签名，并且部署引擎 156可以向安装在可信执行环境124中的部署机器上(例如，安装在 VM 140上)的公钥证书机构验证签名。验证角色映射签名由框202 指示。再次，VM镜像可以是与适当操作系统的镜像组合的签名代码，如框204所示。VM镜像可以表示一个或多个服务和数据库，如框206 所示，并且VM镜像也可以以其他方式标识，如框208所示。

[0035] 然后，部署引擎156从VM镜像存储库158获取所标识的VM镜像。这由框210指示。然后，它将所标识的VM镜像部署到基于云的可信执行环境124。这由框212指示。

[0036] 图4是示出可信执行环境124在从云笼密钥服务130请求角色密钥并且接收这些密钥并且使用它们来执行其工作时的操作的一个示例的流程图。首先假定表示要在环境124中执行的服务的VM镜像已经由部署服务128在可信执行环境124中部署。这由框218指示。然后，可信执行环境124确定表示其要执行的服务的角色的角色密钥需要执行操作。这由图4的流程图中的框220指示。

[0037] 然后，测量系统142生成部署在虚拟机140上的部署的VM镜像的VM镜像测量。这由框222指示。再次，如上面简要描述的，可以通过向VM镜像应用散列函数来获取VM镜像测量。这由框224指示。它也可以以其他方式获取，如框226所示。

[0038] 然后，可信执行环境124将VM镜像测量和标识角色的角色标识符发送到云笼密钥服务130以获取角色的角色密钥，使得可信执行环境124可以执行其操作。这由框228指示。

[0039] 然后，云笼密钥服务130操作以验证角色适合于请求可信执行环境并且密钥适合

于角色。如果是，则服务130将包装的(或加密的) 角色密钥返回到云笼123中的请求可信执行环境124。下面参考图5 更详细地描述云笼密钥服务130的操作，并且在可信执行环境124处获取包装或加密的角色密钥由图4的流程图中的框230指示。

[0040] 然后，可信执行环境124中的解密系统141解包(或解密)所接收的角色密钥并且使用它们来以其正在执行的角色(或服务)来执行工作。这由图3的流程图中的框232和234指示。要在可信执行环境中执行的特定工作将有很大不同，这取决于它托管或执行的特定服务。例如，角色密钥可以用于解密信用卡信息，如框236所示。它们可以用于执行支付处理，如框238所示。它们当然也可以以各种其他方式使用，并且这由框240指示。

[0041] 图5是更详细地示出云笼密钥服务130的操作的一个示例的流程图。VTEE密钥服务166首先从请求角色密钥的执行环境(诸如可信执行环境124)接收引用(quote)。这由图5的流程图中的框250指示。如上面简要讨论的，引用可以包括标识由请求执行环境执行的特定角色的角色标识符252。它还说明性地包括由该环境生成的VM测量。这由框254指示。它可以包括标识正在发出请求的特定可信执行环境的可信执行环境标识符256。该请求也可以包括其他项目258。

[0042] 然后将该请求提供给策略引擎168，在策略引擎168中对其进行评估以确定引用(或请求)是否来自适当的可信执行环境以及它是否具有用于所标识的角色的正确的操作系统、代码等。这由图5的流程图中的框260指示。在一个示例中，策略引擎168访问VM镜像测量储存器172以标识请求可信执行环境是否对应于在请求中接收的VM 镜像测量。例如，它可以确定该VM镜像是否已经适当地部署在适当的可信执行环境中。这由框262指示。

[0043] 策略引擎168还可以访问测量到角色映射174以确定部署在请求可信执行环境上(并且由VM镜像测量表示)的VM镜像是否被映射到所标识的角色。这由框264指示。因此，给定VM镜像测量，策略引擎168通过访问将VM镜像映射到一组角色的映射174来生成一组角色，如下：

[0044] $\theta: h \rightarrow S_R$

[0045] $$S_R = \{Role | \emptyset(Role) = h\}$$

[0046] 其中

[0047] h＝H(IMAGE) 等式2

[0048] 从上面的等式2，可以看出，映射Θ将镜像h(其等于上面的等式1中所示的H(IMAGE)(H(镜像)))映射到一组角色S_R。该组角色S_R是通过映射Φ而映射到VM镜像测量的那些角色。该组角色由角色组成，其中给定该角色到镜像测量h的映射。

[0049] 如果策略引擎168确定请求可信执行环境不是运行由VM镜像测量标识的VM镜像的适当环境，或者如果它确定VM镜像测量未映射到请求可信执行环境的角色，则VTEE密钥服务166确定策略引擎168 尚未肯定地评估引用。这由图5中的框270指示。因此，VTEE密钥服务166拒绝对角色密钥的请求，如框272所示。它可以响应于该否定评估而发送通知或警报或其他消息或者执行其他操作。这由框274 指示。

[0050] 然而，假定策略引擎168确定请求可信执行环境124是执行角色的适当环境，并且假定由请求可信执行环境提供的VM镜像测量映射到所标识的角色，则VTEE密钥服务166在框270处确定策略引擎评估是肯定的或有利的。在这种情况下，VTEE密钥服务166与密钥包

装密码引擎交互以获取角色密钥，使得它可以将它们提供给请求可信执行环境124。

[0051] 为此，VTEE密钥服务166向密钥包装密码引擎170提供角色标识符。引擎170访问角色密钥储存器/生成器176以获取或生成所标识的角色的角色密钥。这由图5的流程图中的框276指示。然后，引擎 170访问密钥包装器密钥178，并且用一个或多个密钥包装器密钥178 包装(或加密)该组角色密钥。这由图5的流程图中的框278指示。角色密钥可以单独地或作为一组进行包装。密钥包装器密钥可以是公共密钥，如框280所示，并且包装角色密钥也可以以其他方式执行，并且这由框282指示。

[0052] 角色密钥可以是任意密码密钥类型，并且包装密钥说明性地是该特定角色的公钥。在获取包装器密钥时，引擎170可以访问将给定角色映射到包装公钥Pu_r的映射Ψ，如下面的等式3所示：

[0053] $$\Psi: Role \rightarrow P_{U_R} \qquad \text{等式 3}$$

[0054] S_{kr}是用包装公钥Pu_R的角色密钥加密的一组包装的角色密钥$E_{P_{U_R}}(K_R)$，如下所示：

[0055] $$S_{K_R} = \left\{ E_{P_{U_R}}(K_R) | \Psi(\text{Role}) = K_{Pu_R} \right\} \qquad \text{等式 4}$$

[0056] 一旦密钥包装密码引擎170获取角色密钥并且用适当的密钥包装器密钥178包装它们，它就将包装的角色密钥返回给VTEE密钥服务 166，VTEE密钥服务166将它们返回到请求可信执行环境124。这通过图5的流程图中的框284指示。

[0057] 因此，应当理解，云笼将多个支付服务视为角色，并且将这些角色映射到如上定义的VM镜像。在云笼可信执行环境中运行的角色或服务的一些示例可以是虚拟硬件安全模块(或密码服务)、汇款代理服务、汇款代理数据库等。

[0058] 在上述架构中，在一个示例中，每个服务器硬件说明性地具有高保证密码处理器、相对少量的密钥存储、密钥对、以及测量由云笼部署服务128中的可信硬件加载的二进制镜像的能力。高保证密码处理器可以具有带有可验证证书的公钥。它还可以包括硬件中的用于由该硬件生成的密钥的证明能力。这将密钥完整性绑定到特定密钥证书。另外，如上所述，可以对角色到VM镜像映射进行签名。签名密钥保密性及其公钥完整性可以由单独的系统来验证，或者这些系统可以是云笼架构的一部分。角色密钥和包装密钥依赖于上面讨论的映射Φ和Ψ。角色定义代码和数据可以被签名并且向证书机构验证，证书机构可以是外部机构。

[0059] 因此，可以看出，即使没有围绕开发和部署资源的物理笼安全性，本系统也能够确保安全性。它确保了部署在可信执行环境中的虚拟机镜像尚未改变。它还确保了在获取角色密钥之前，虚拟机镜像是用于获取这些密钥的适当的虚拟机镜像，并且可信执行环境是用于运行该虚拟机镜像的适当的环境。角色密钥在返回到可信执行环境时会被包装或加密，以便它可以执行其操作。

[0060] 应当注意，上述讨论已经描述了各种不同的系统、组件和/或逻辑。应当理解，这样的系统、组件和/或逻辑可以包括执行与这些系统、组件和/或逻辑相关联的功能的硬件项

目(诸如处理器和相关联的存储器、或其他处理组件,其中的一些在下面描述)。另外,系统、组件和/或逻辑可以包括加载到存储器中并且随后由处理器或服务器或其他计算组件执行的软件,如下所述。系统、组件和/或逻辑还可以包括硬件、软件、固件等的不同组合,其一些示例在下面描述。这些仅是可以用于形成上述系统、组件和/或逻辑的不同结构的一些示例。也可以使用其他结构。

[0061] 本讨论已经提到了处理器和服务器。在一个实施例中,处理器和服务器包括具有相关联的存储器和定时电路的计算机处理器(未单独示出)。它们是它们所属的以及激活它们的系统或设备的功能部分,并且支持这些系统中的其他组件或项目的功能。

[0062] 此外,已经讨论了很多用户界面显示。它们可以采用各种不同的形式,并且可以具有设置在其上的各种不同的用户可致动输入机制。例如,用户可致动的输入机制可以是文本框、复选框、图标、链接、下拉菜单、搜索框等。它们也可以以各种不同的方式被致动。例如,可以使用点击设备(诸如跟踪球或鼠标)来致动它们。可以使用硬件按钮、开关、操纵杆或键盘、拇指开关或拇指垫等来致动它们。也可以使用虚拟键盘或其他虚拟致动器来致动它们。另外,在显示它们的屏幕是触敏屏幕的情况下,可以使用触摸手势来致动它们。而且,在显示它们的设备具有语音识别组件的情况下,可以使用语音命令来致动它们。

[0063] 还讨论了很多数据储存器。应当注意,它们每个可以分成多个数据储存器。所有这些都可以是访问它们的系统的本地的,所有这些都可以是远程的,或者一些可以是本地的,而另一些是远程的。所有这些配置都在本文中考虑。

[0064] 此外,附图示出了具有归于每个框的功能的多个框。应当注意,可以使用更少的框,因此功能由更少的组件执行。此外,可以使用更多框,其中功能分布在更多组件之间。

[0065] 本文中将架构122描述为云计算架构。云计算提供计算、软件、数据访问和存储服务,这些服务不需要终端用户了解提供服务的系统的物理位置或配置。在各种实施例中,云计算使用适当的协议在诸如因特网等广域网上提供服务。例如,云计算提供商通过广域网提供应用,并且可以通过web浏览器或任何其他计算组件来访问它们。架构 122的软件或组件以及对应的数据可以存储在远程位置处的服务器上。云计算环境中的计算资源可以在远程数据中心位置处合并,或者可以是分散的。云计算基础设施可以通过共享数据中心提供服务,即使它们呈现为用户的单一访问点。因此,本文中描述的组件和功能可以使用云计算架构从远程位置处的服务提供商提供。替代地,它们可以从传统服务器提供,或者它们可以直接或以其他方式安装在客户端设备上。

[0066] 本描述旨在包括公共云计算和私有云计算两者。云计算(公共和私有两者)提供了大量无缝的资源池,并且减少了对管理和配置底层硬件基础设施的需求。

[0067] 公共云由供应商管理,并且通常使用相同的基础设施支持多个消费者。此外,与私有云相反,公共云可以无需终端用户管理硬件。私有云可以由组织本身管理,并且基础设施通常不与其他组织共享。组织仍然在某种程度上维护硬件,诸如安装和维修等。

[0068] 图6是可以部署架构100或其一部分(例如)的计算环境的一个示例。参考图6,用于实现一些实施例的示例系统包括计算机810形式的通用计算设备。计算机810的组件可以包括但不限于处理单元 820(其可以包括处理器或服务器136、154或164)、系统存储器830 和系统总线821,系统总线821将包括系统存储器在内的各种系统组件耦合到处理单元820。系统总线821可以是若干类型的总线结构中的任何一种,其包括使用各种总线架构中的任何

一种的存储器总线或存储器控制器、外围总线和本地总线。作为示例而非限制，这样的架构包括工业标准架构(ISA)总线、微通道架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)本地总线和外围组件互连(PCI)总线(也称夹层总线)。关于图1描述的存储器和程序可以部署在图6的对应部分中。

[0069] 计算机810通常包括各种计算机可读介质。计算机可读介质可以是可以由计算机810访问的任何可用介质，并且包括易失性和非易失性介质、可移除和不可移除介质。作为示例而非限制，计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质不同于并且不包括调制数据信号或载波。它包括硬件存储介质，硬件存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等信息的任何方法或技术实现的易失性和非易失性的可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储技术、CD-ROM、数字通用盘(DVD)或其他光盘存储装置、磁带盒、磁带、磁盘存储装置或其他磁存储设备、或者可以用于存储期望的信息并且可以由计算机810访问的任何其他介质。通信介质通常在传输机制中包含计算机可读指令、数据结构、程序模块或其他数据，并且包括任何信息传递介质。术语“调制数据信号”表示以在信号中对信息进行编码的方式设置或改变其一个或多个特征的信号。作为示例而非限制，通信介质包括诸如有线网络或直接有线连接等有线介质以及诸如声学、RF、红外和其他无线介质等无线介质。任何上述的组合也应当被包括在计算机可读介质的范围内。

[0070] 系统存储器830包括易失性和/或非易失性存储器形式的计算机存储介质，诸如只读存储器(ROM)831和随机存取存储器(RAM) 832。包含有助于在计算机810内的元件之间传送信息的基本例程(例如在启动期间)的基本输入/输出系统833(BIOS)通常存储在ROM 831中。RAM 832通常包含立即可访问和/或当前正在由处理单元820 操作的数据和/或程序模块。作为示例而非限制，图6示出了操作系统 834、应用程序835、其他程序模块836和程序数据837。

[0071] 计算机810还可以包括其他可移除/不可移除的易失性/非易失性计算机存储介质。仅作为示例，图6示出了从不可移除的非易失性磁介质读取或向其写入的硬盘驱动器841、以及从诸如CD ROM或其他光学介质等可移除的非易失性光盘856读取或向其写入的光盘驱动器 855。可以在示例性操作环境中使用的其他可移除/不可移除的易失性/ 非易失性计算机存储介质包括但不限于磁带盒、闪存卡、数字通用盘、数字录像带、固态RAM、固态ROM等。硬盘驱动器841通常通过诸如接口840等不可移除存储器接口连接到系统总线821，并且光盘驱动器855通常通过诸如接口850等可移除存储器接口连接到系统总线 821。

[0072] 替代地或另外地，本文中描述的功能可以至少部分地由一个或多个硬件逻辑组件执行。例如而非限制，可以使用的说明性类型的硬件逻辑组件包括现场可编程门阵列(FPGA)、程序专用集成电路 (ASIC)、程序专用标准产品(ASSP)、片上系统(SOC)、复杂可编程逻辑器件(CPLD)等。

[0073] 上面讨论并且在图6中示出的驱动器及其相关联的计算机存储介质为计算机810提供计算机可读指令、数据结构、程序模块和其他数据的存储。例如，在图6中，硬盘驱动器841被示出为存储操作系统 844、应用程序845、其他程序模块846和程序数据847。注意，这些组件可以与操作系统834、应用程序835、其他程序模块836和程序数据837相同或不同。操作系统844、应用程序845、其他程序模块 846和程序数据847在这里被给予不同的数字以说

明它们至少是不同的副本。

[0074] 用户可以通过诸如键盘862、麦克风863和诸如鼠标、轨迹球或触摸板等指示设备861等输入设备向计算机810中输入命令和信息。其他输入设备(未示出)可以包括操纵杆、游戏手柄、圆盘式卫星天线、扫描仪等。这些和其他输入设备通常通过耦合到系统总线的用户输入接口860连接到处理单元820,但是可以通过诸如并行端口、游戏端口或通用串行总线(USB)等其他接口和总线结构连接。视觉显示器891或其他类型的显示设备也经由诸如视频接口890等接口连接到系统总线821。除了显示器之外,计算机还可以包括可以通过输出外围接口895连接的其他外围输出设备,诸如扬声器897和打印机 896。

[0075] 计算机810使用到诸如远程计算机880等一个或多个远程计算机的逻辑连接在网络环境中操作。远程计算机880可以是个人计算机、手持设备、服务器、路由器、网络PC、对等设备或其他公共网络节点,并且通常包括上面关于计算机810描述的很多或所有元件。图6中描绘的逻辑连接包括局域网(LAN)871和广域网(WAN)873,但是也可以包括其他网络。这种网络环境在办公室、企业范围的计算机网络、内联网和因特网中很常见。

[0076] 当在LAN网络环境中使用时,计算机810通过网络接口或适配器870连接到LAN 871。当在WAN网络环境中使用时,计算机810 通常包括调制解调器872或用于通过诸如因特网等WAN 873建立通信的其他装置。可以是内部的或外部的调制解调器872可以经由用户输入接口860或其他适当的机制连接到系统总线821。在网络环境中,相对于计算机810或其部分描述的程序模块可以存储在远程存储器存储设备中。作为示例而非限制,图6将远程应用程序885示出为驻留在远程计算机880上。可以理解,所示出的网络连接是示例性的,并且可以使用在计算机之间建立通信链路的其他手段。

[0077] 还应当注意,本文中描述的不同实施例可以以不同方式组合。也就是说,一个或多个实施例的部分可以与一个或多个其他实施例的部分组合。所有这些都在本文中考虑。

[0078] 示例1是一种计算系统,包括:

[0079] 策略引擎,策略引擎接收角色和虚拟机(VM)镜像测量,角色标识服务,VM镜像测量指示部署在执行环境中的虚拟机镜像,并且策略引擎确定VM镜像测量是否被映射到角色,并且生成指示确定的评估信号;

[0080] 密钥包装密码引擎,密钥包装密码引擎基于指示VM镜像测量被映射到角色的评估信号,获取并且包装一组角色密钥,角色密钥对应于角色并且使得执行环境能够执行服务;以及

[0081] 密钥服务,密钥服务为执行环境提供一组包装的角色密钥。

[0082] 示例2是根据任何或所有先前示例所述的计算系统,其中策略引擎被配置为接收角色,接收VM镜像测量并且从请求执行环境接收执行环境标识符,执行环境标识符标识请求执行环境。

[0083] 示例3是根据任何或所有先前示例所述的计算系统,其中策略引擎被配置为基于执行环境标识符来确定请求执行环境是否被映射到 VM镜像测量,并且基于确定来生成评估信号。

[0084] 示例4是根据任何或所有先前示例所述的计算系统,还包括:

[0085] 一组测量到角色映射,一组测量到角色映射将多个不同组角色中的每个角色映射到不同的VM镜像测量,策略引擎通过访问测量到角色映射来确定VM镜像测量是否被映射到

角色。

[0086] 示例5是根据任何或所有先前示例所述的计算系统,还包括:

[0087] 角色密钥储存器/生成器,角色密钥储存器/生成器被配置为向密钥包装密码引擎提供一组角色密钥;以及一组密钥包装器密钥,每个密钥包装器密钥被映射到给定角色,密钥包装密码引擎标识被映射到角色的一个或多个密钥包装器密钥,并且用所标识的一个或多个密钥包装器密钥来加密角色密钥。

[0088] 示例6是根据任何或所有先前示例所述的计算系统,还包括:

[0089] 部署引擎,部署引擎被配置为接收角色并且基于角色获取VM镜像,并且将VM镜像部署到执行环境。

[0090] 示例7是根据任何或所有先前示例所述的计算系统,还包括:

[0091] 一组角色到镜像映射,一组角色到镜像映射将角色映射到VM镜像,部署引擎访问一组角色到镜像映射以标识VM镜像。

[0092] 示例8是根据任何或所有先前示例所述的计算系统,还包括:

[0093] VM镜像存储库,VM镜像存储库存储VM镜像,部署引擎从VM 镜像存储库获取VM镜像以进行部署。

[0094] 示例9是根据任何或所有先前示例所述的计算系统,其中执行环境包括:

[0095] 测量系统,测量系统被配置为生成VM镜像测量并且将VM镜像测量提供给密钥服务。

[0096] 示例10是根据任何或所有先前示例所述的计算系统,其中测量系统对VM镜像执行散列函数以获取包括VM镜像测量的散列值。

[0097] 示例11是一种计算机实现的方法,包括:

[0098] 在密钥服务处标识执行环境服务和指示部署在执行环境中的虚拟机镜像的虚拟机(VM)镜像测量;

[0099] 确定VM镜像测量是否被映射到执行环境服务;

[0100] 生成指示确定的评估信号;

[0101] 响应于评估信号指示VM镜像测量被映射到执行环境服务,获取一组角色密钥,角色密钥对应于执行环境服务并且使得执行环境能够执行执行环境服务;

[0102] 加密一组角色密钥中的角色密钥;以及

[0103] 为执行环境提供一组加密的角色密钥。

[0104] 示例12是根据任何或所有先前示例所述的计算机实现的方法,还包括:

[0105] 接收标识执行环境服务的角色;

[0106] 接收VM镜像测量;以及

[0107] 从请求执行环境接收执行环境标识符,执行环境标识符标识请求执行环境,并且其中确定VM镜像测量是否被映射到执行环境服务包括基于执行环境标识符来确定请求执行环境是否被映射到VM镜像测量,并且生成评估信号包括基于确定来生成评估信号。

[0108] 示例13是根据任何或所有先前示例所述的计算机实现的方法,其中确定VM镜像测量是否被映射到执行环境服务包括:

[0109] 通过访问将多个不同组的角色中的每个角色映射到不同的VM镜像测量的一组测量到角色映射的资产来确定VM镜像测量是否被映射到角色。

[0110] 示例14是根据任何或所有先前示例所述的计算机实现的方法,其中加密角色密钥包括:

[0111] 标识被映射到角色的一个或多个密钥包装器密钥;以及

[0112] 用所标识的一个或多个密钥包装器密钥来加密角色密钥。

[0113] 示例15是根据任何或所有先前示例所述的计算机实现的方法,还包括:

[0114] 在部署系统处接收角色;

[0115] 通过访问将角色映射到VM镜像的一组角色到镜像映射来在部署系统处基于角色来获取VM镜像;以及

[0116] 将VM镜像部署到执行环境。

[0117] 示例16是根据任何或所有先前示例所述的计算机实现的方法,还包括:

[0118] 在执行环境中利用测量系统生成VM镜像测量;以及

[0119] 将VM镜像测量提供给密钥服务。

[0120] 示例17是根据任何或所有先前示例所述的计算机实现的方法,其中生成VM镜像测量包括:

[0121] 利用测量系统对VM镜像执行散列函数以获取包括VM镜像测量的散列值。

[0122] 示例18是一种计算系统,包括:

[0123] 执行环境,执行环境执行由所部署的虚拟机(VM)镜像表示的并且由角色标识的服务;

[0124] 测量系统,测量系统被配置为将散列函数应用于VM镜像以生成 VM镜像测量并且将VM镜像测量提供给密钥服务,执行环境将角色和VM镜像测量提供给密钥服务以请求一组角色密钥;以及

[0125] 解密系统,解密系统从密钥服务接收一组包装的角色密钥,并且解密一组包装的角色密钥以获取所请求的一组角色密钥,执行环境使用所请求的角色密钥来执行服务。

[0126] 示例19是根据任何或所有先前示例所述的计算系统,其中密钥服务包括:

[0127] 策略引擎,策略引擎从执行环境接收角色,标识服务和指示部署在执行环境中的虚拟机镜像的VM镜像测量,并且确定VM镜像测量是否被映射到角色,并且生成指示确定的评估信号;以及

[0128] 密钥包装密码引擎,密钥包装密码引擎基于指示VM镜像测量被映射到角色的评估信号,获取并且包装一组角色密钥,密钥服务向执行环境提供一组包装的角色密钥。

[0129] 示例20是根据任何或所有先前示例所述的计算系统,还包括:

[0130] 部署系统,部署系统包括将角色映射到VM镜像的一组角色到镜像映射以及存储VM镜像的VM镜像存储库,并且部署引擎被配置为通过基于角色访问角色到镜像映射来从VM镜像存储库获取VM镜像以用于部署,并且被配置为将VM镜像部署到执行环境。

[0131] 尽管用结构特征和/或方法动作专用的语言描述了本主题,但是应当理解,所附权利要求书中定义的主题不必限于上述具体特征或动作。而是,上述具体特征和动作被公开作为实现权利要求的示例形式。

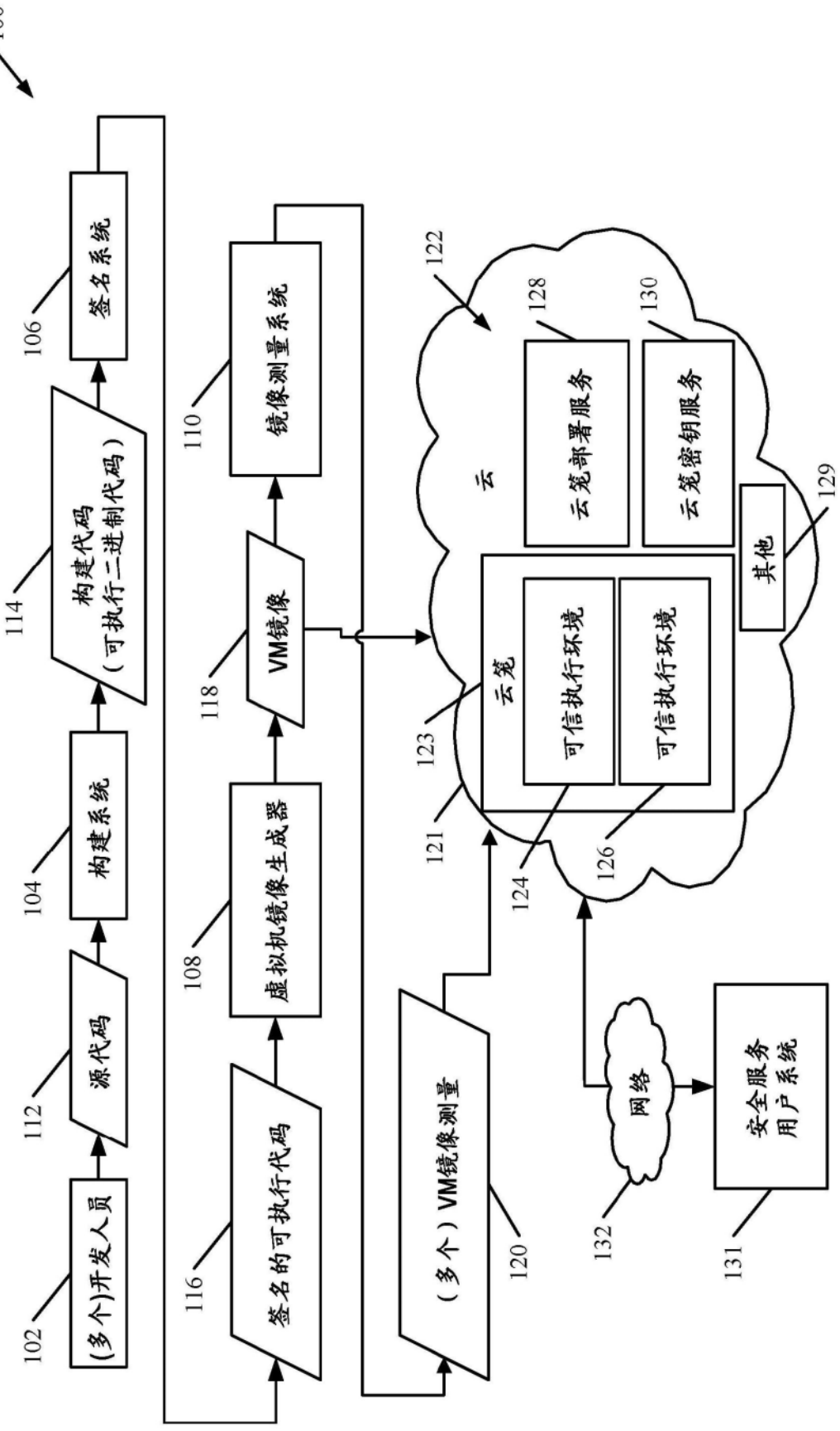

100
(多个)开发人员
102
源代码
112
构建系统
104
构建代码
(可执行二进制代码)
114
签名系统
106
签名的可执行代码
116
虚拟机镜像生成器
108
VM镜像
118
镜像测量系统
110
(多个)VM镜像测量
120
云
122
云笼
123
可信执行环境
可信执行环境
121
云笼部署服务
128
云笼密钥服务
130
其他
129
124
126
网络
132
安全服务
用户系统
131

图1

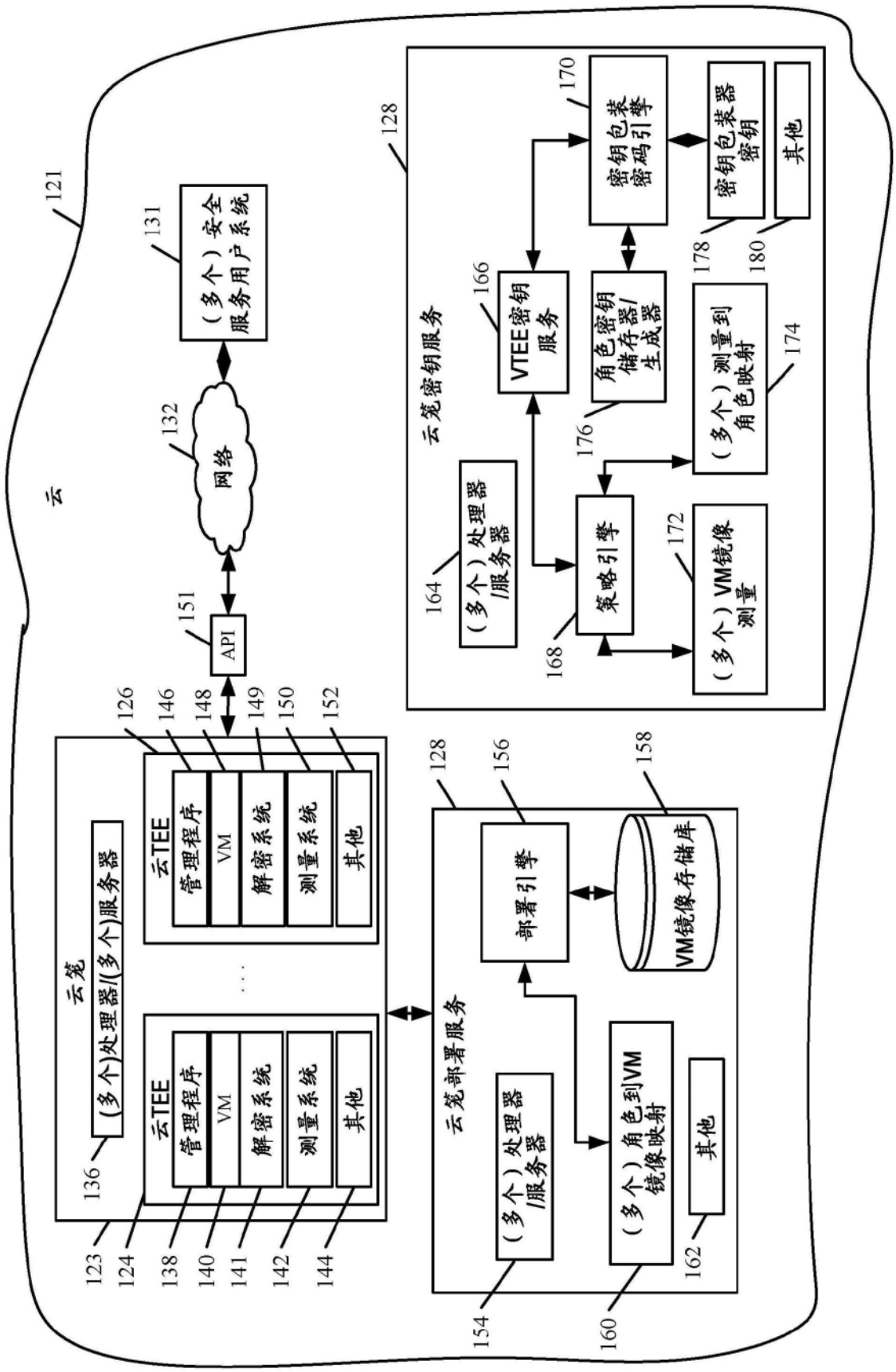

云
121
(多个)安全用户系统
131
网络
132
API
151
云TEE
管理程序
VM
解密系统
测量系统
其他
126
146
148
149
150
152
云笼
(多个)处理器/服务器
136
123
124
138
140
141
142
144
云笼部署服务
128
部署引擎
156
VM镜像存储库
158
(多个)处理器/服务器
154
(多个)角色到VM镜像映射
160
其他
162
云笼密钥服务
128
密钥包装密码引擎
170
密钥包装器密钥
178
其他
180
VTEE密钥服务
166
角色密钥储存器/生成器
176
(多个)测量到角色映射
174
(多个)处理器/服务器
164
策略引擎
168
(多个)VM镜像测量
172

图2

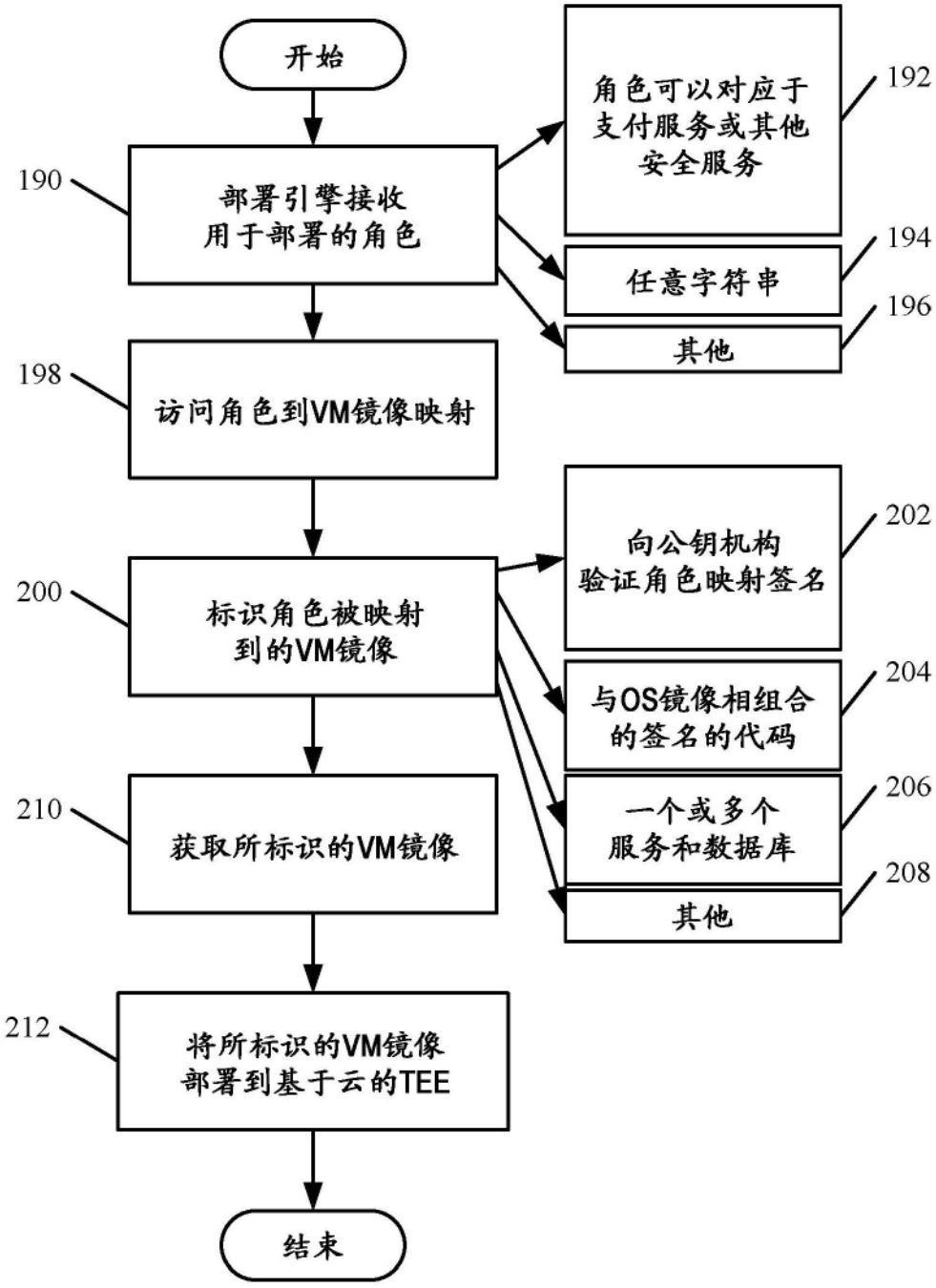

开始
190
部署引擎接收
用于部署的角色
192
角色可以对应于
支付服务或其他
安全服务
194
任意字符串
196
其他
198
访问角色到VM镜像映射
200
标识角色被映射
到的VM镜像
202
向公钥机构
验证角色映射签名
204
与OS镜像相组合
的签名的代码
206
一个或多个
服务和数据库
208
其他
210
获取所标识的VM镜像
212
将所标识的VM镜像
部署到基于云的TEE
结束

图3

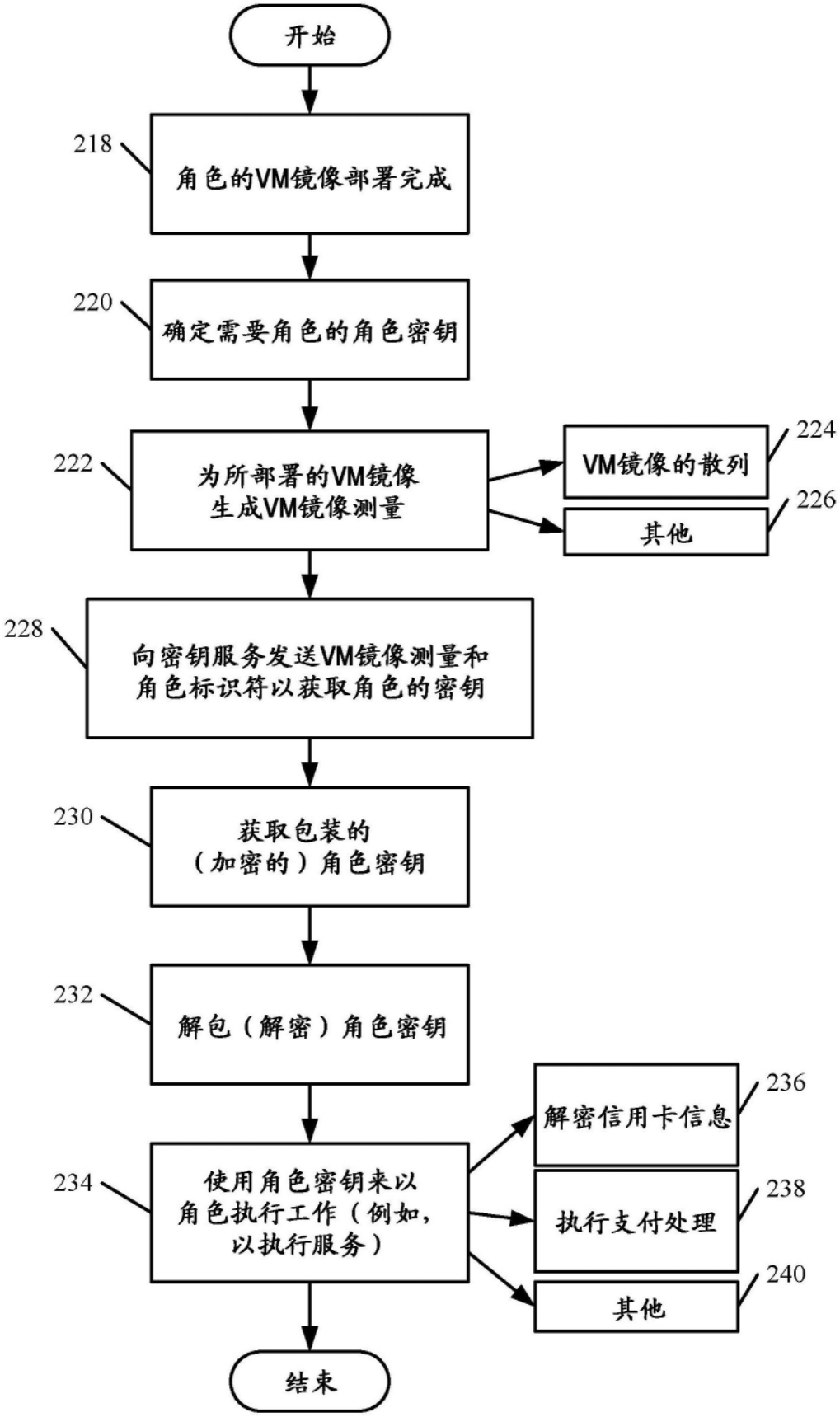

开始
218
角色的VM镜像部署完成
220
确定需要角色的角色密钥
222
为所部署的VM镜像
生成VM镜像测量
224
VM镜像的散列
226
其他
228
向密钥服务发送VM镜像测量和
角色标识符以获取角色的密钥
230
获取包装的
（加密的）角色密钥
232
解包（解密）角色密钥
234
使用角色密钥来以
角色执行工作（例如，
以执行服务）
236
解密信用卡信息
238
执行支付处理
240
其他
结束

图4

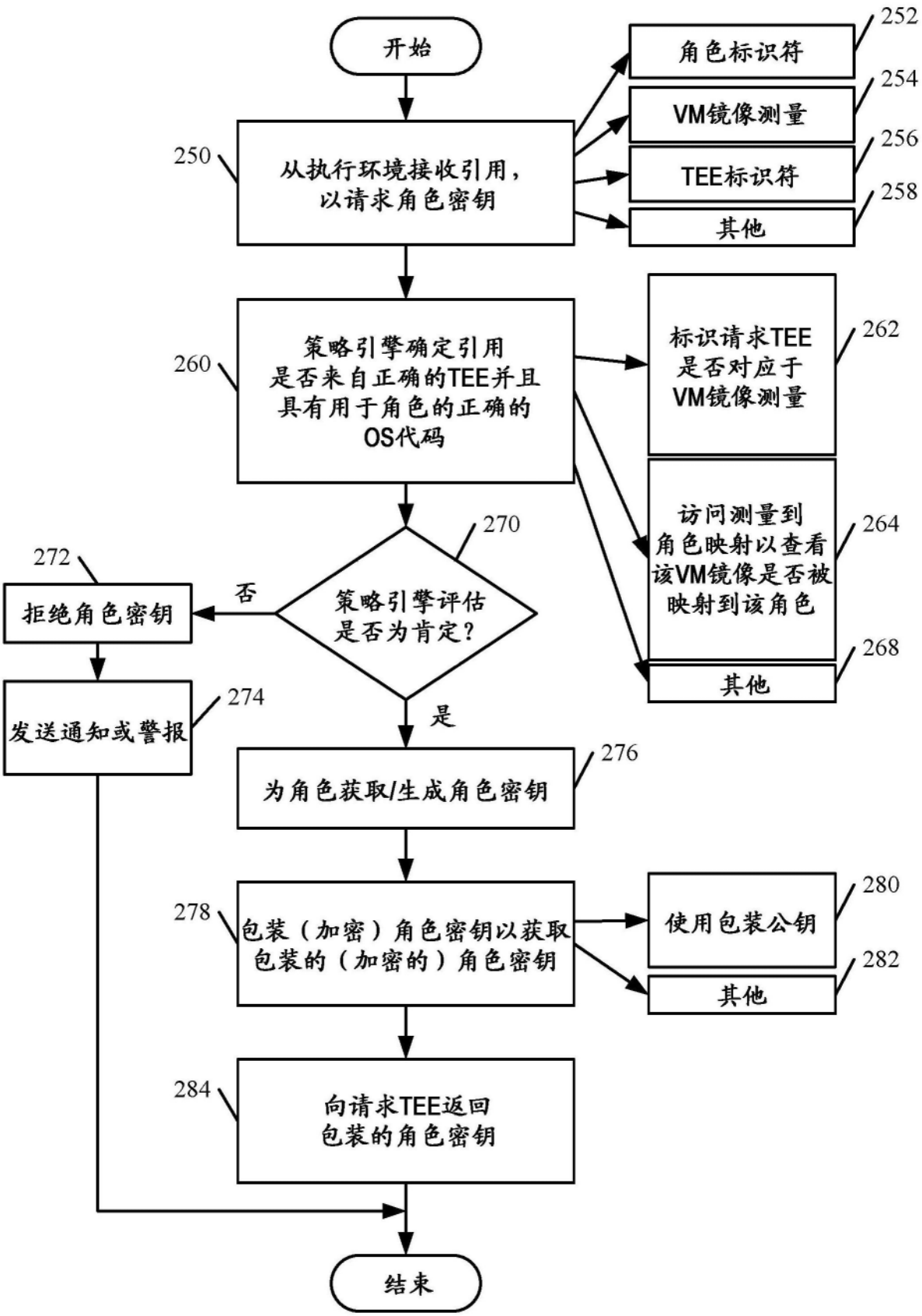

开始
从执行环境接收引用，以请求角色密钥
250
角色标识符
252
VM镜像测量
254
TEE标识符
256
其他
258
策略引擎确定引用是否来自正确的TEE并且具有用于角色的正确的OS代码
260
标识请求TEE是否对应于VM镜像测量
262
访问测量到角色映射以查看该VM镜像是否被映射到该角色
264
其他
268
策略引擎评估是否为肯定？
270
否
拒绝角色密钥
272
发送通知或警报
274
是
为角色获取/生成角色密钥
276
包装（加密）角色密钥以获取包装的（加密的）角色密钥
278
使用包装公钥
280
其他
282
向请求TEE返回包装的角色密钥
284
结束

图5

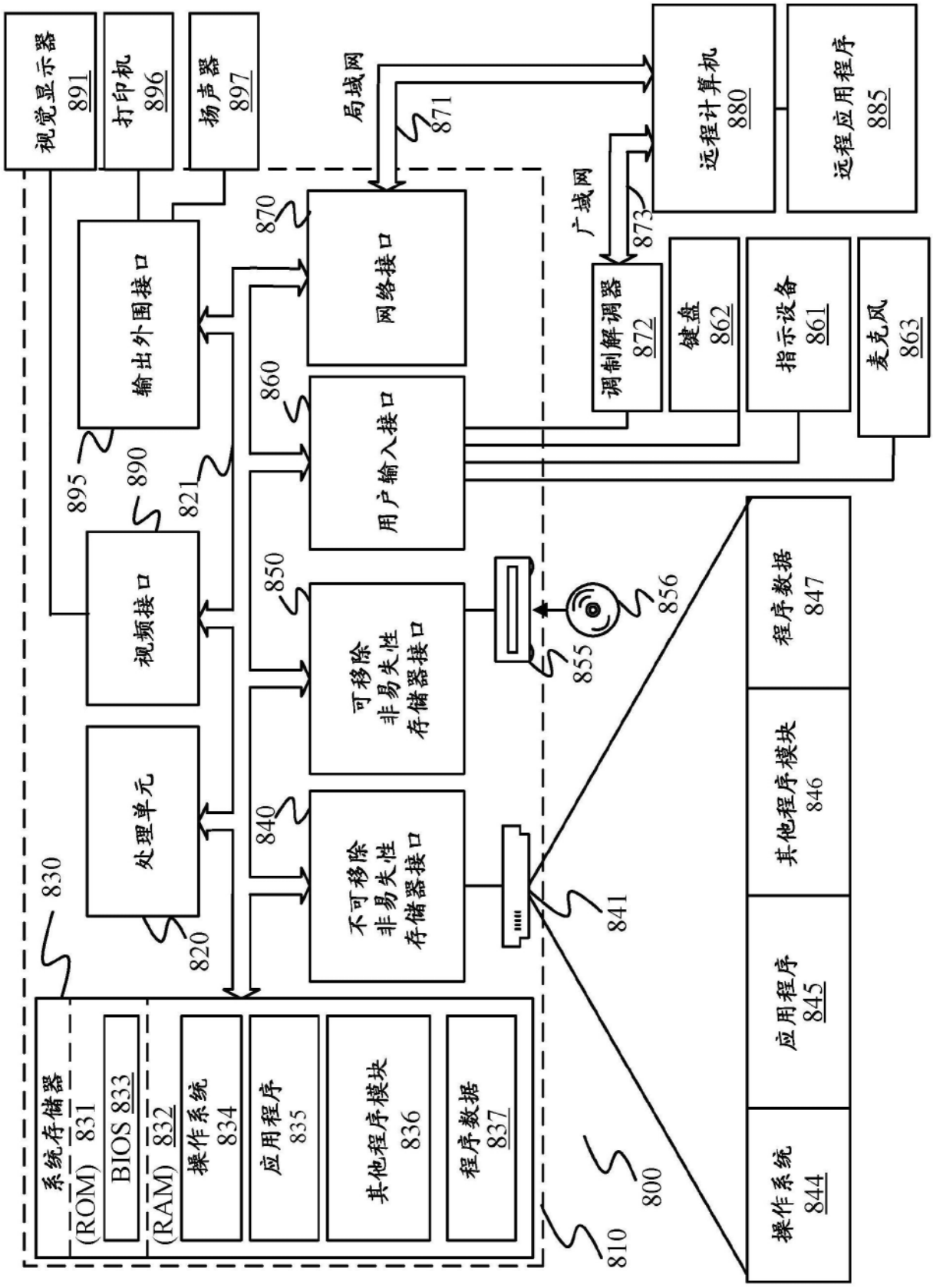

视觉显示器 891
打印机 896
扬声器 897
局域网
871
远程计算机 880
远程应用程序 885
广域网
873
870
网络接口
输出外围接口
895
890
821
860
用户输入接口
调制解调器 872
键盘 862
指示设备 861
麦克风 863
850
可移除 非易失性 存储器接口
856
855
840
不可移除 非易失性 存储器接口
841
处理单元
820
视频接口
830
系统存储器
(ROM) 831
BIOS 833
(RAM) 832
操作系统 834
应用程序 835
其他程序模块 836
程序数据 837
程序数据 847
其他程序模块 846
应用程序 845
操作系统 844
800
810

图6