



(12) 发明专利申请

(10) 申请公布号 CN 105408913 A

(43) 申请公布日 2016. 03. 16

(21) 申请号 201380078406. 5

G06F 15/16(2006. 01)

(22) 申请日 2013. 08. 21

(85) PCT国际申请进入国家阶段日

2016. 01. 21

(86) PCT国际申请的申请数据

PCT/US2013/055915 2013. 08. 21

(87) PCT国际申请的公布数据

W02015/026336 EN 2015. 02. 26

(71) 申请人 英特尔公司

地址 美国加利福尼亚州

(72) 发明人 M · D · 雅维斯 J · 波尔特

S · K · 加吉 李宏

(74) 专利代理机构 上海专利商标事务所有限公司 31100

代理人 张东梅

(51) Int. Cl.

G06F 21/62(2006. 01)

G06F 21/30(2006. 01)

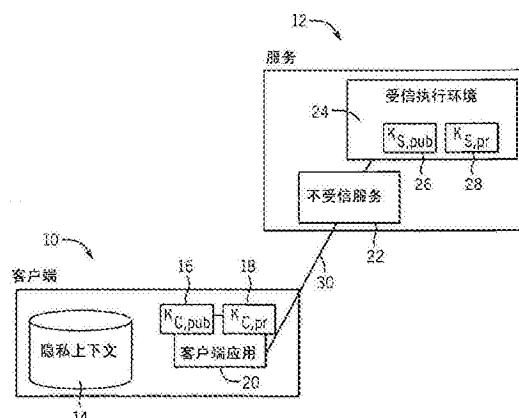
权利要求书1页 说明书7页 附图8页

(54) 发明名称

在云中隐私地处理数据

(57) 摘要

尽管云服务可提供来自个人设备的处理或来自多个源的合成数据，但是许多用户更喜欢对他们的数据保持隐私。根据某些实施例，隐私用户数据可在云中处理而不向云服务提供商暴露用户身份。仅用户或用户的授权代理和服务的硬件平台可访问某些密钥。服务应用软件和操作系统仅可访问加密数据。



1. 一种方法，包括：

经由不受信云服务提供商在云中与受信方建立安全通道；

与所述受信方交换公钥而不将所述密钥暴露给所述提供商；

经由所述安全通道通过所述提供商发送经加密的数据以便由所述受信方与所述提供商分离地处理；以及

经由所述安全通道通过所述提供商从所述受信方接收所述处理的经加密的结果。

2. 如权利要求 1 所述的方法，包括从所述受信方接收公钥。

3. 如权利要求 2 所述的方法，包括在将所述数据发送到所述受信方之前使用所述公钥加密所述数据。

4. 如权利要求 3 所述的方法，包括将经加密的客户端公钥发送到所述方。

5. 如权利要求 4 所述的方法，包括接收用所述客户端公钥加密的结果。

6. 如权利要求 1 所述的方法，其中，所述受信方是第三方。

7. 如权利要求 1 所述的方法，其中，所述受信方是受信环境。

8. 如权利要求 1 所述的方法，包括将带有所述方的公钥的隐私数据用所述客户端的公钥和会话密钥加密并与用所述会话密钥加密的随机值一起提供给所述受信方。

9. 至少一种机器可读介质，包括多个指令，响应于在计算设备上被执行，所述指令致使所述计算设备执行根据权利要求 1 至 9 中任一项所述的方法。

10. 一种装置，被安排成用于执行如权利要求 1 至 9 中任一项所述的方法。

11. 如权利要求 10 所述的装置，包括用于通过企业服务器建立到所述受信方的安全通道的企业客户端设备。

12. 一种方法，包括：

经由不受信云服务提供商与客户端建立安全通道；

与所述客户端交换密钥；

经由所述安全通道接收经加密的数据；

处理所述经加密的数据；以及

经由所述安全通道通过所述不受信云服务提供商发送所述处理的经加密的结果。

13. 如权利要求 12 所述的方法，包括从所述客户端接收公钥。

14. 如权利要求 13 所述的方法，包括在将所述数据发送到所述客户端之前使用所述公钥加密所述数据。

15. 如权利要求 14 所述的方法，包括将经加密的服务器公钥发送到所述客户端。

16. 如权利要求 15 所述的方法，包括发送用所述客户端公钥加密的结果。

17. 至少一种机器可读介质，包括多个指令，响应于在计算设备上被执行，所述指令致使所述计算设备执行根据权利要求 12 至 16 中任一项所述的方法。

18. 一种装置，被安排成用于执行如权利要求 12 至 16 中任一项所述的方法。

## 在云中隐私地处理数据

[0001] 背景

[0002] 本发明总体上涉及在云中处理数据。

[0003] 云基本上是为客户端（诸如移动电话、膝上计算机、个人计算机以及实际上可通过有线或无线网络与服务器通信的任何基于处理器的设备）提供存储或处理服务的任何服务器。云计算是用于使得能够对可以用最小的管理努力或服务提供商交互快速供应并释放的可配置计算资源共享池（例如，网络、服务器、存储、应用以及服务）进行无处不在的、方便的、按需的网络访问的模型。

[0004] 通常，从客户端到服务器提供各种任务。结合苹果 iPhone 的常见任务是使用 Siri 语音识别服务。用户可说出问题并且该信息可由服务器处理，然后该服务器提供答案。

[0005] 某些人更喜欢云服务提供商不访问正在被处理的数据。该数据可包括用户的语音、任何其他用户隐私数据以及用户正在提供的实际内容。然而，用户在许多情况下具有很少的选择，因为电话提供商也是提供云服务的提供商。

[0006] 附图简要说明

[0007] 参照以下附图描述一些实施例：

[0008] 图 1 是根据一个实施例的客户端服务器的架构图；

[0009] 图 2 是根据一个实施例的通信流；

[0010] 图 3 是在一个实施例中有用的分组格式的图；

[0011] 图 4 是根据一个实施例的受信执行环境的图；

[0012] 图 5 是根据一个实施例的使用第三方受信服务提供商的架构的图；

[0013] 图 6 是来自企业内的受信服务提供商的架构图；

[0014] 图 7 是客户端处的一个实施例的流程图；

[0015] 图 8 是服务器处的一个实施例的流程图；以及

[0016] 图 9 是一个实施例的系统图。

[0017] 详细描述

[0018] 尽管云服务可提供来自个人设备的处理或来自多个源的合成数据，但是许多用户喜欢对他们的数据保持隐私。根据某些实施例，隐私用户数据可在云中处理而不向云服务提供商暴露用户身份。仅用户或用户的授权代理和服务的硬件平台能访问某些密钥并因此访问未经加密的数据。服务应用软件和操作系统仅能访问加密数据。

[0019] 根据一个实施例，云服务中的受信计算库使得服务能够隐私地处理用户数据。数据可仅以加密格式存储并传输。明文数据的处理可仅在云服务中的受信硬件组件中发生。云服务操作系统应用软件仅能访问经加密的数据。

[0020] 参照图 1，客户端 10 可通过通信路径 30 与服务或服务器 12 通信。通信路径 30 可以是任何有线或无线通信路径。客户端 10 可以是任何基于处理器的设备，包括平板计算机、蜂窝电话、膝上计算机或个人计算机。其还可以是电视接收器、打印机游戏设备或可穿戴设备。客户端 10 包括隐私上下文 14，该隐私上下文可包括用户更喜欢保持机密的信息和应用。其还可以包括多个客户端应用 20，每个客户端应用具有其自身所分配的公钥 16 和私

钥 18。

[0021] 在一个实施例中,通信路径 30 可例如结合超文本传输协议安全 (HTTPS) 协议实现传输层安全 (TLS) 连接。客户端可建立到服务 12 内的受信执行环境 24 的 TLS 连接。例如,在一个实施例中,通过 TLS 连接 30 的通信可依赖于向客户端保证受信执行环境是特定的受信执行环境的证书交换。客户端可存储被受信接受的执行环境列表。例如,Verisign 证书可向客户端提供充分的信息:客户端可确信受信执行环境的身份。然后,客户端仅需检查数据库以便确定受信执行环境是否是客户端可信任的那个。

[0022] 证书可由服务(诸如 Verisign)生成,该证书向用户确保正在与其通信的实体是实体所说的实体。

[0023] 服务 12 可包括不受信服务 22,路径 30 通过该不受信服务 22 到达受信执行环境 24。然而,不受信服务仅可访问经加密的数据。仅受信执行环境 24 具有将用户数据隐私地从客户端 10 传送到受信执行环境 24 所需的公钥 26 和私钥 28。不受信服务可以例如是互联网服务提供商或蜂窝电话服务提供商,作为两个示例。

[0024] 因此,参照图 2,客户端 10 可通过不受信服务 22 与受信执行环境 24 通信。客户端 10 包括公钥和私钥并且使用 TLS 通道 30 验证受信执行环境的身份。具体地,信任请求 32 被发布到受信执行环境。受信执行环境用其公钥做出响应,如箭头 34 所示。然后,客户端基于预定的受信执行环境列表确定受信执行环境是否是客户端能够信任的环境。可确信受信执行环境的身份,因为这个身份由 TLS 通道确认。

[0025] 然后,如果客户端 10 选择由受信执行环境 24 处理隐私数据,其发送包括用服务器的公钥和客户端的公钥加密的会话密钥以及用会话密钥加密的隐私数据和随机值,如箭头 36 所示。然后,受信执行环境 24 具有客户端的公钥并且可处理隐私数据。其将如 38 处所示的结果发送到客户端 10。使用第二会话密钥对这些结果和随机值进行加密。也使用客户端的公钥对会话密钥进行加密。

[0026] 服务从客户端接收隐私数据并且在受信执行环境执行处理。仅受信执行环境具有解密数据的密钥,该数据曾以其他方式在存储器中并且在盘上加密。一旦处理完成,使用第二会话密钥对这些结果进行加密。由客户端公钥加密的第二会话密钥、这些结果以及由第二会话密钥加密的随机值被返回客户端。

[0027] 图 3 示出了一种可能的分组格式。公钥 40 与有效载荷加密密钥 44 一起用于加密签名 48。因此,有效载荷 46 被加密并且然后头 42 可被提供。也就是,使用如 50 处所示的有效载荷加密密钥 44 对有效载荷进行加密。然后,如 52 处所示,可用头、加密密钥 44 和有效载荷 46 对签名进行散列。

[0028] 图 4 中示出的受信执行环境是服务器进行安全处理的关键。从客户端接收的所有数据以加密形式存储在存储器 66 中和存储 70 上。受信执行环境包含用于解密数据的秘密密钥和用于处理的存储器 66。经解密的数据仅在处理期间可用,并且在其被处理之后永不在存储器中或盘上可用。

[0029] 因此,中央处理单元 (CPU) 或其他处理器 54 包括作为公私钥对或对称密钥的秘密 56。可用于在数据 62 中提供指令 60 的解密单元 58 中进行解密。读写链路 64 将存储器 66 和 CPU 54 链接起来。存储器 66 可存储也可从如 72 中所指示的存储 70 加载的经加密的信息 68。

[0030] 至此为止,数据已经用算法或不用算法(例如,个人上下文作为经加密的文本文件)从客户端传输以便在驻留在服务器上的数据上操作。在另一个实施例中,客户端传送数据和指令两者以便在服务器上执行。在这种情况下,客户端能够控制对数据的访问以及在数据上发生的处理。处理指令与图2中被标记为“隐私数据”和在图3中被标记为“经加密的有效载荷”的块中的数据一起被传输。可或者通过要求对指令进行签名或者要求在沙盒(例如,Java虚拟机)中对指令进行解释来保护服务器,该沙盒在受信执行环境或两者中运行。

[0031] 在至此所描述的示例中,存在其服务器具有受信执行环境的最终用户和单个服务提供商。以下描述两个扩展。

[0032] 在某些情况下,用户可与用户不信任的服务提供商交互,即使该服务提供商具有含受信执行环境的硬件。在这种情况下,如图5所示,可使用受信第三方。用户与受信第三方的硬件建立关系而不是与不受信服务提供商。第三方受信硬件中发生计算并且仅经加密的请求和结果数据通过不受信服务提供商传输。

[0033] 因此,在图5中,客户端设备74包括公钥和私钥78和80、客户端应用82和隐私上下文76。设备74通过路径84通信,该路径可以是有线或无线并且可通常是TLS连接。其与具有不受信服务90的不受信服务提供商88通信。不受信服务提供商和受信服务提供商92两者都在云86中。受信服务提供商92包括不受信服务94、公钥和私钥98和100以及受信执行环境96。

[0034] 在另一个示例中,如图6所示,客户端可以是企业环境中的设备。在本示例中,企业102可能希望访问未经加密的数据。此外,企业可能希望设置有关可处理什么数据以及该数据可由什么外部服务提供商访问的策略。在这种情况下,企业客户端设备106通过企业服务或服务器112或可能企业所提供的代理与受信服务提供商124通信。企业服务112包含适当的安全策略114并且与信任执行环境128协商受信关系和密钥。因此,企业客户端设备106包括企业数据108和经由路径116在企业102内与企业服务器112通信的客户端应用110。企业服务器112具有用于用公钥和私钥120和122对数据和企业服务118进行云处理的安全策略。受信执行环境128还包括云104中的公钥和私钥130和132。

[0035] 因此,企业客户端设备106通过路径116与企业102内的企业服务器112通信。其还通过路径116经由不受信服务124与云104和受信执行环境128通信。

[0036] 在某些实施例中,会话密钥可以是随机数并且随机值可以是另一个随机数。会话密钥可以例如是对称密钥。

[0037] 在某些实施例中,可以用保留其隐私性的方式在云中处理数据。服务提供商可能永远都不知道客户端设备的所有者的身份或者甚至正在提供的数据。数据执行可与不受信服务提供商分离。

[0038] 可在本文的实施例中使用具有公/私钥对的任何客户端应用。通常,客户端必须具有公/私钥对以及验证其能够并且应当信任的身份的某种方式。因此,在某些实施例中,任何人可与任何受信实体使用这个序列。

[0039] 参照图7,可在客户端中实现、可在软件、固件和/或硬件中实现序列134。在软件和固件实施例中,它可由一个或多个非瞬态计算机可读介质(如磁、光学、或半导体存储)执行。

[0040] 程序代码或指令可被存储在例如易失性和 / 或非易失性存储器中, 诸如存储设备和 / 或相关联的机器可读或机器可访问介质, 包括但不限于固态存储器、硬盘驱动器、软盘、光存储、磁带、闪存、存储器棒、数字视频盘、数字通用盘 (DVD) 等等, 以及更独特的介质, 诸如机器可访问生物状态保存存储。机器可读介质可包括用于以机器可读的形式存储、传输或接收信息的任何机制, 并且该介质可包括程序代码可通过其传递的介质, 诸如天线、光纤、通信接口等等。程序代码可被以分组、串行数据、并行数据等形式传输, 并且可以用压缩或加密格式使用。

[0041] 如框 136 中所示的, 序列 134 可通过与受信执行环境或其他受信实体建立 TLS 通道开始。然后, 发送信任请求, 如框 138 中所示。信任请求可包括客户端设备的公钥。服务器从客户端设备接收公钥, 如框 140 中所示。如框 142 中所示的, 服务器通过经由不受信服务向受信实体发送经加密的服务器公钥、会话密钥、客户端公钥、隐私数据和随机值来做出响应。然后, 客户端接收经加密的客户端公钥、会话密钥、结果和随机值, 如框 144 中所示。

[0042] 序列 146 在图 8 中指示服务器中的相应的活动。序列 146 可在软件、固件和 / 或硬件中实现。在软件和固件实施例中, 它可由存储在一个或多个非瞬态计算机可读介质 (如磁、光学、或半导体存储) 中计算机执行指令实现。

[0043] 序列 146 可通过接收对客户端设备的 TLS 请求开始, 如框 148 中所示。然后, 服务器可发送其公钥, 如框 150 中所示。接下来, 服务器接收经加密的数据、服务器和客户端公钥以及随机值, 如框 152 中所示。服务器处理隐私数据, 如框 154 中所示。然后, 服务器返回经加密的客户端公钥、会话密钥、结果和随机值, 如框 156 中所示。

[0044] 实施例可在许多不同的系统类型中实现。现在参照图 9, 示出了根据可在桌上计算机、膝上计算机、移动互联网设备、移动计算节点、智能电话、蜂窝电话、无线电、固定计算节点等等中发现的实施例的系统的框图。多处理器系统 200 是点到点互连系统, 并包括经由点到点互连 250 耦合的第一处理器 270 和第二处理器 280。处理器 270 和 280 中的每一个都可以是多核处理器。术语“处理器”可指代任何设备或处理来自寄存器和 / 或存储器的电子数据以便将该电子数据转换成可存储在寄存器和 / 或存储器中的其他电子数据的设备的一部分。第一处理器 270 可包括存储器控制器中枢 (MCH) 和点到点 (P-P) 接口。类似地, 第二处理器 280 可包括 MCH 和 P-P 接口。MCH 可将处理器耦合到对应的存储器, 即, 存储器 232 和存储器 234, 这些存储器可以是本地地附接到对应的处理器的主存储器 (例如, 动态随机存取存储器 (DRAM)) 的多个部分。第一处理器 270 和第二处理器 280 可分别经由 P-P 互连耦合到芯片组 290。芯片组 290 可包括 P-P 接口。此外, 芯片组 290 可经由接口耦合至第一总线 216。各种输入 / 输出 (I/O) 设备 214 可以连同总线桥 218 耦合到第一总线 216, 总线桥 218 将第一总线 216 耦合至第二总线 220。在一个实施例中, 各种设备可耦合到第二总线 220, 包括例如键盘 / 鼠标 222、通信设备 226 和数据存储单元 228, 诸如可包括代码 230 的磁盘驱动器或其他大容量存储设备。代码可存储在一个或多个存储器中, 包括存储器 228、232、234、经由网络耦合到系统 200 的存储器等等。而且, 音频 I/O 224 可耦合到第二总线 220。

[0045] 实施例可在代码中实现并且可存储在其上存储有可用于对系统进行编程的指令以便执行这些指令的至少一个存储介质上。存储介质可包括但不限于任何类型的盘, 包括软盘、光盘、固态驱动器 (SSD)、致密盘只读存储 (CD-ROM)、致密盘可重写 (CD-RW)、以及

磁光盘、半导体器件,诸如只读存储器 (ROM)、随机存取存储器 (RAM),诸如 DRAM、动态和静态 RAM、可擦可编程只读存储器 (EPROM)、电可擦可编程只读存储器 (EEPROM)、闪存、磁或光卡、或任何其他类型的适合用于存储电子指令的介质。

[0046] 在此参照数据 (诸如指令、功能、过程、数据结构、应用程序、配置设置、代码等等) 描述了各实施例。这种指令包括在例如图 7 和图 8 中并且可存储在 (或分布在) 各种位置,诸如位置 232、231、235、236、230 和 / 或 228 等等。当该数据由机器访问时,该机器可通过执行任务、定义抽象数据类型、建立低级硬件上下文和 / 或执行其他操作来做出响应,如在此更详细描述的。该数据可存储在易失性和 / 或非易失性数据存储中。术语“代码”或“程序”覆盖广泛范围的组件和构造,包括应用、驱动程序、进程、例程、方法、模块和子程序,并且可指代当由处理系统执行时执行所期望的操作的任何指令集合。此外,替代实施例可包括使用比所有公开的操作更少的进程、使用附加操作的进程、使用不同序列中的相同操作的进程以及在此公开的单独操作在其中组合、细分或以其他方式更改的进程。

[0047] 在一个实施例中,使用术语控制逻辑包括硬件 (诸如晶体管、寄存器或其他硬件 (诸如可编程逻辑器件 (235)))。然而,在另一个实施例中,逻辑还包括软件或代码 (231)。这种逻辑可与硬件 (诸如固件或微代码 (236)) 集成。处理器或控制器可包括旨在表示本领域已知的各种各种的控制逻辑中的任一种,并且这样可很好地被实现为微处理器、微控制器、现场可编程门阵列 (FPGA)、专用集成电路 (FPGA)、可编程逻辑器件 (FPGA) 等等。

[0048] 本领域技术人员将理解的是总体上在此并且尤其在所附权利要求书 (例如,所附权利要求书的主体) 中使用的术语通常旨在是“开放式”术语 (例如,术语“包括 (including)”应当被解释为“包括但不限于 (including but not limited to)”,术语“具有 (having)”应当被解释为“至少具有 (having at least)”,术语“包括 (includes)”应当被解释为“包括但不限于 (includes but is not limited to)”)。本领域技术人员将进一步理解的是如果预期所引入的权利要求引用的特定编号,这种意图将明确地在该权利要求中引用并且在不存在这种引用时不存在这种意图。例如,作为对理解的辅助,以下所附权利要求书可包含引入性短语“至少一个”和“一个或多个”的使用以便引入权利要求引用。然而,这种短语的使用不应当被解释为暗指通过不定冠词“a(一种)”或“an(一种)”对权利要求引用的引入将包含这种引入权利要求引用的任何特定的权利要求限制为仅包含一个这种引用的发明,即使当相同的权利要求包括引入性短语“一个或多个”或“至少一个”以及不定冠词诸如“a(一种)”或“an(一种)”(例如,应当通常被解释为“至少一个”或“一个或多个”);用于引入权利要求引用的定冠词的使用也如此。此外,即使明确引用了引入权利要求引用的特定编号,本领域技术人员将认识到这种引用应当通常被解释为意指至少该引用编号 (例如,仅引用“两个引用”而没有其他修饰符通常意指至少两个引用或两个或更多个引用)。在使用类似于“A、B 或 C 等等中的至少一项”的惯例的情形中,通常,这种构造的含义为本领域技术人员将理解的该惯例 (例如,“系统具有 A、B 或 C 中的至少一项”将包括但不限于仅具有 A、仅具有 B、仅具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C 和 / 或具有 A、B 和 C 等等的系统)。本领域技术人员将进一步理解的是实际上无论在说明书、权利要求书还是附图中呈现两个或更多个替代术语的任何分隔词和 / 或短语应当被理解为考虑包括这些术语之一、这些术语中的任一项或这两个术语的可能性。例如,短语“A 或 B”将被理解为包括“A”或“B”或“A 和 B”的可能性。

[0049] 也可相对于在此所描述的方法或过程实现以上所描述的装置的全部可选特征。尽管已经针对有限数量的实施例描述了本发明，本领域技术人员将认识到从其延伸的多种修改和变形。旨在所附权利要求书涵盖所有这种修改和变形，落入本发明的真实精神和范围内。

[0050] 以下子句和 / 或示例涉及进一步的实施例：

[0051] 至少一个机器可读介质，包括指令，当由处理器执行时，该指令执行序列，该序列包括：经由不受信云服务提供商在云中与受信方建立安全通道；与该受信方交换公钥而不将该密钥暴露给该提供商；经由该安全通道通过该提供商发送经加密的数据以便由该受信方与该提供商分离地处理；以及经由该安全通道通过该提供商从该受信方接收该处理的经加密的结果。该介质可进一步存储用于从该受信方接收公钥的指令。该介质可进一步存储用于在将所述数据发送到所述受信方之前使用所述公钥加密所述数据的指令。该介质可包括将经加密的客户端公钥发送到所述方。该介质可包括接收用所述客户端公钥加密的结果。该介质可包括该受信方是第三方。该介质可包括至少一个介质，其中，该受信方是受信环境。该介质可包括将带有该方的公钥的隐私数据用该客户端的公钥和会话密钥加密并用会话密钥加密的随机值一起提供给该受信方。

[0052] 在另一个示例实施例中，至少一个机器可读介质包括指令，当由处理器执行时，该指令执行序列，该序列包括：经由不受信云服务提供商与客户端建立安全通道；与该客户端交换密钥；经由该安全通道接收经加密的数据；处理该经加密的数据；以及经由所述安全通道通过该不受信云服务提供商发送所述处理的经加密的结果。该至少一个介质可进一步存储用于从该客户端接收公钥的指令。该至少一个介质可进一步存储用于在将所述数据发送到所述客户端之前使用所述公钥加密所述数据的指令。该至少一个介质包括将经加密的服务器公钥发送到所述客户端。该至少一个介质包括发送用所述客户端公钥加密的结果。

[0053] 另一个示例实施例可以是一种装置，该装置包括处理器和耦合到所述处理器的存储，该处理器用于：经由不受信云服务提供商在云中给予受信方建立安全通道；与该受信方交换密钥；经由该安全通道发送经加密的数据以便由该受信方处理；以及经由所述安全通道从该受信方接收所述处理的经加密的结果。该装置可包括所述处理器从该受信方接收公钥。该装置可包括所述处理器在将所述数据发送到所述受信方之前使用所述公钥加密所述数据。该装置可包括所述处理器将经加密的客户端公钥发送到所述方。该装置可包括所述处理器接收用所述客户端公钥加密的结果。

[0054] 在又一个示例实施例中，可以是一种装置，该装置包括处理器和耦合到所述装置存储，该处理器用于：经由不受信云服务提供商与客户端建立安全通道；与该客户端交换密钥；经由该安全通道接收经加密的数据；处理该经加密的数据；以及经由所述安全通道通过该不受信云服务提供商发送所述处理的经加密的结果。该装置可包括所述处理器从该客户端接收公钥。该装置可包括所述处理器在将所述数据发送到所述客户端之前使用所述公钥加密所述数据。该装置可包括所述处理器将经加密的服务器公钥发送到所述客户端。该装置可包括所述处理器发送用所述客户端公钥加密的结果。该装置可包括云服务器。该装置可包括受信执行环境。该装置可包括所述服务器相对于所述客户端是第三方并且在云中相对于所述客户端是服务提供商。

[0055] 贯穿本说明书对“一个实施例”或“一种实施例”的引用是指在此结合实施例所述的特定特征、结构或特性包括在本公开中所包含的至少一种实现方式中。因此，短语“一个实施例”或“在实施例中”的出现无需指代相同的实施例。此外，特定的特征、结构或特性可被设置为其他合适的形式而不是所展示的特定实施例，并且所有这种形式可包含在本申请的权利要求书中。

[0056] 尽管已经描述了有限数量的实施例，本领域技术人员将意识到许多修改和变化。旨在所附权利要求书涵盖落入本公开的真实精神和范围中的所有这种修改和变化。

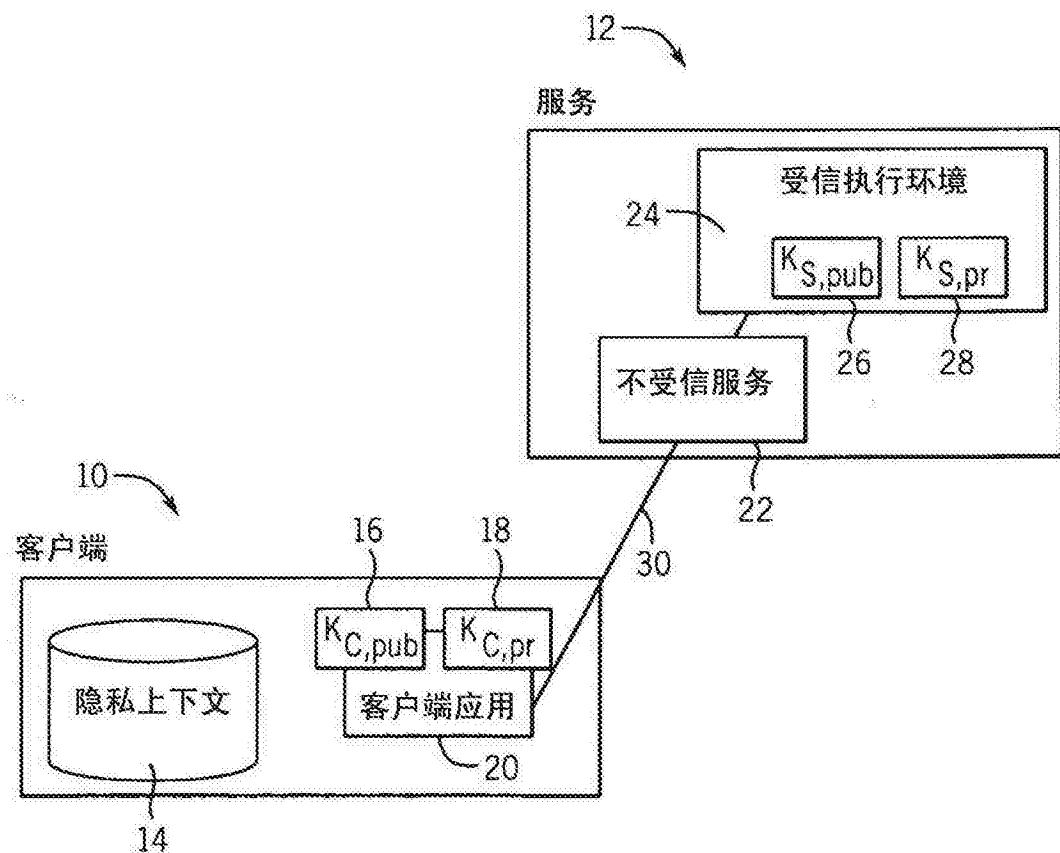


图 1

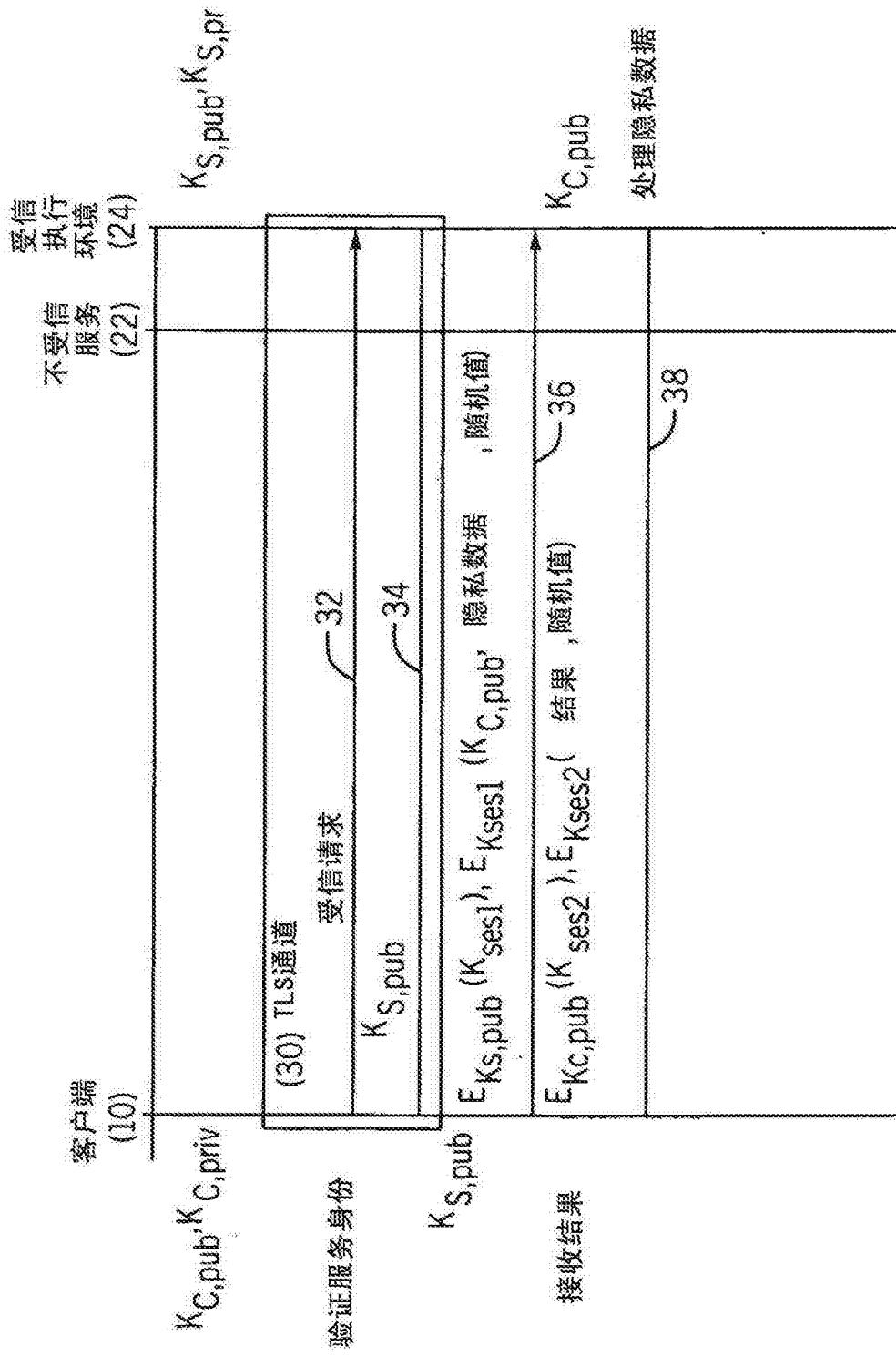


图 2

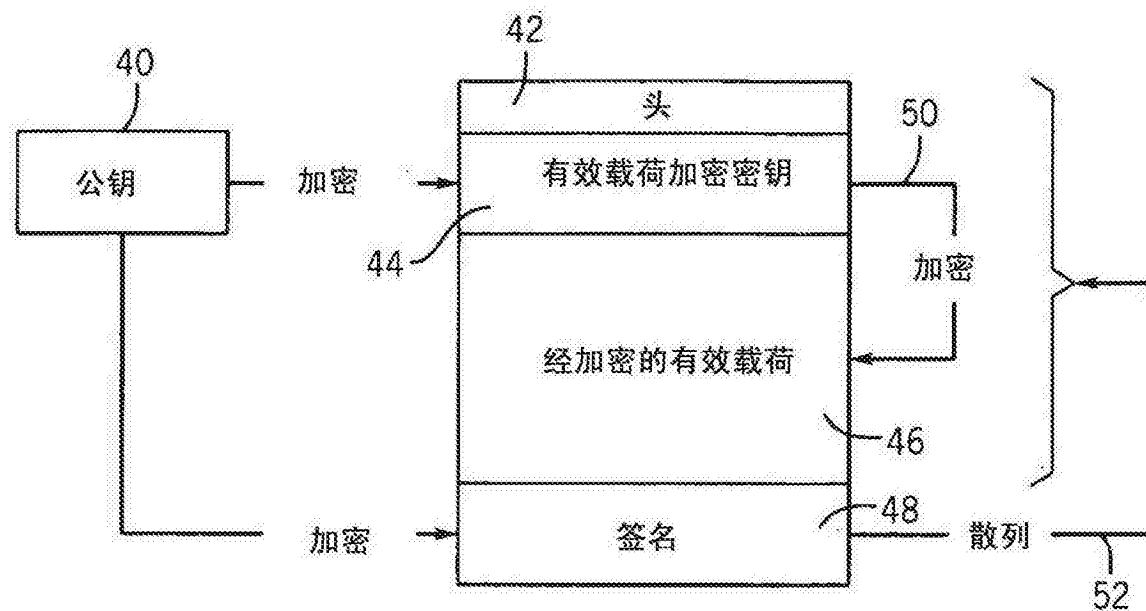


图 3

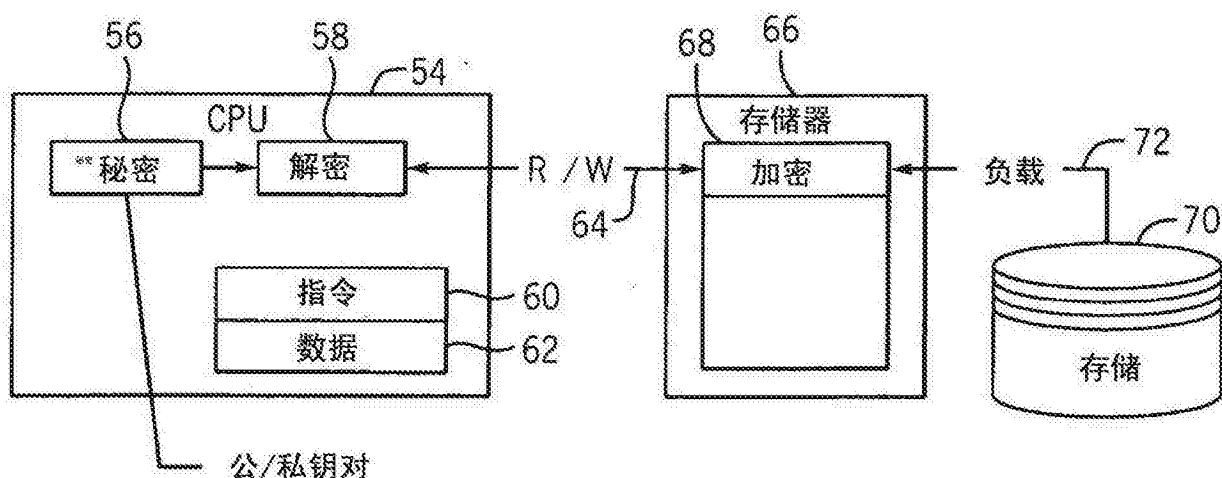


图 4

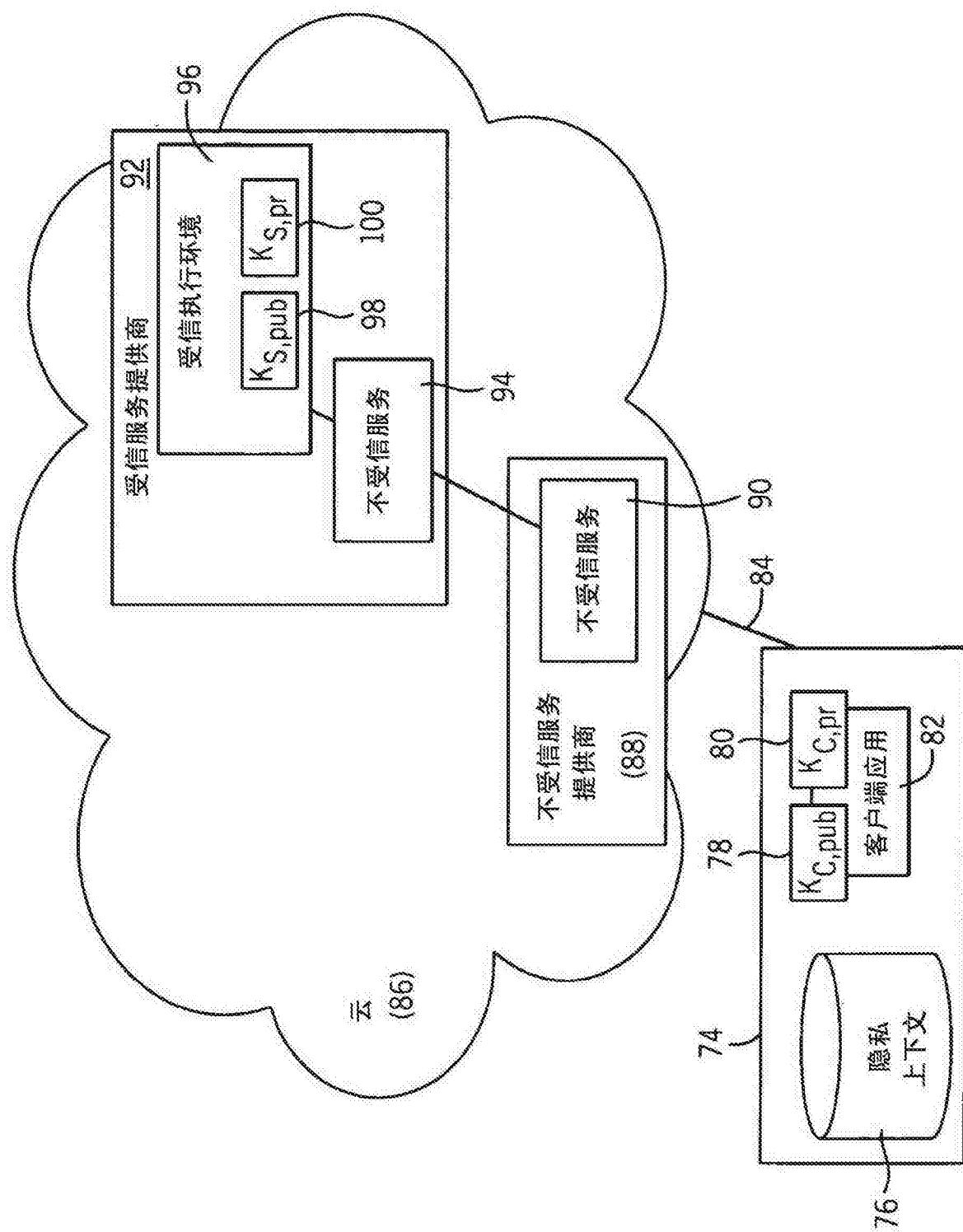


图 5

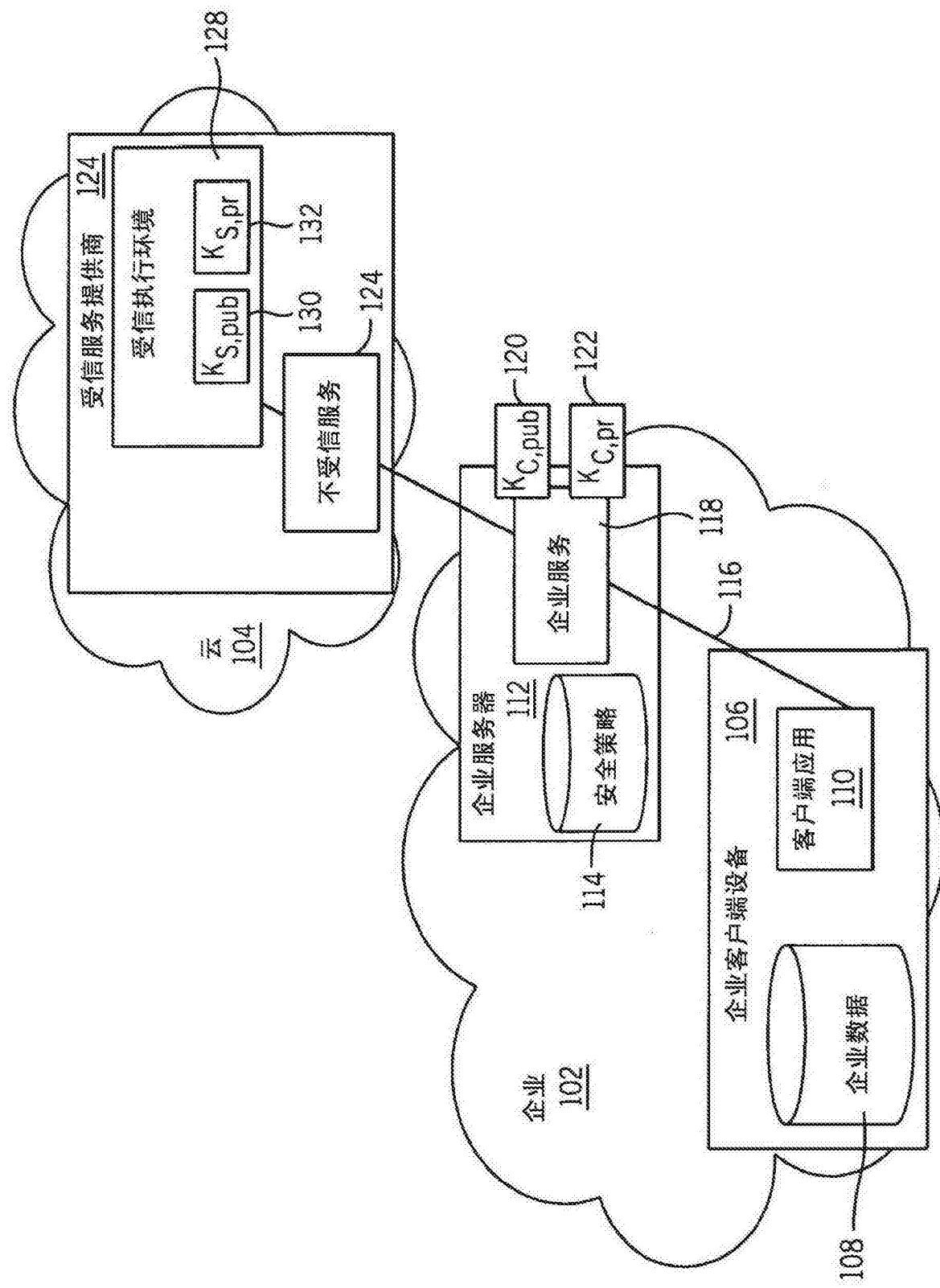


图 6

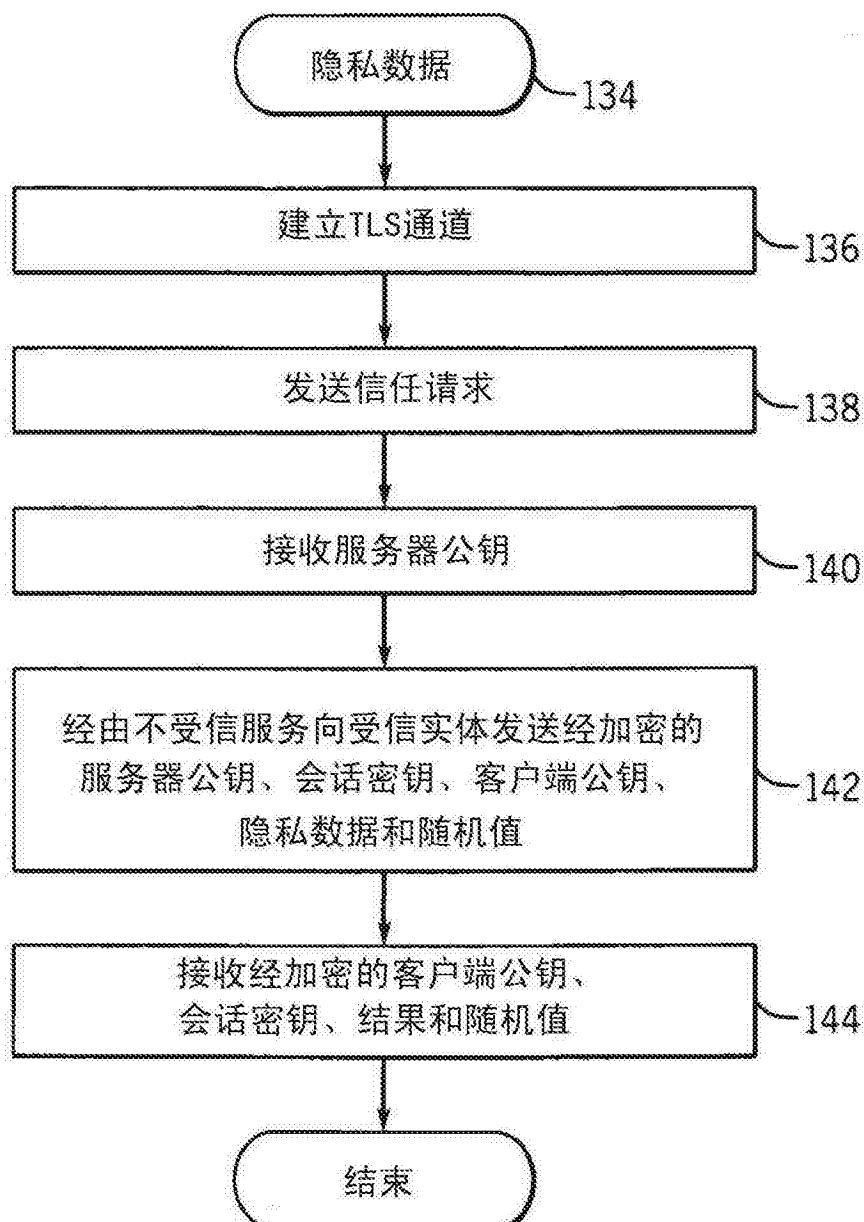


图 7

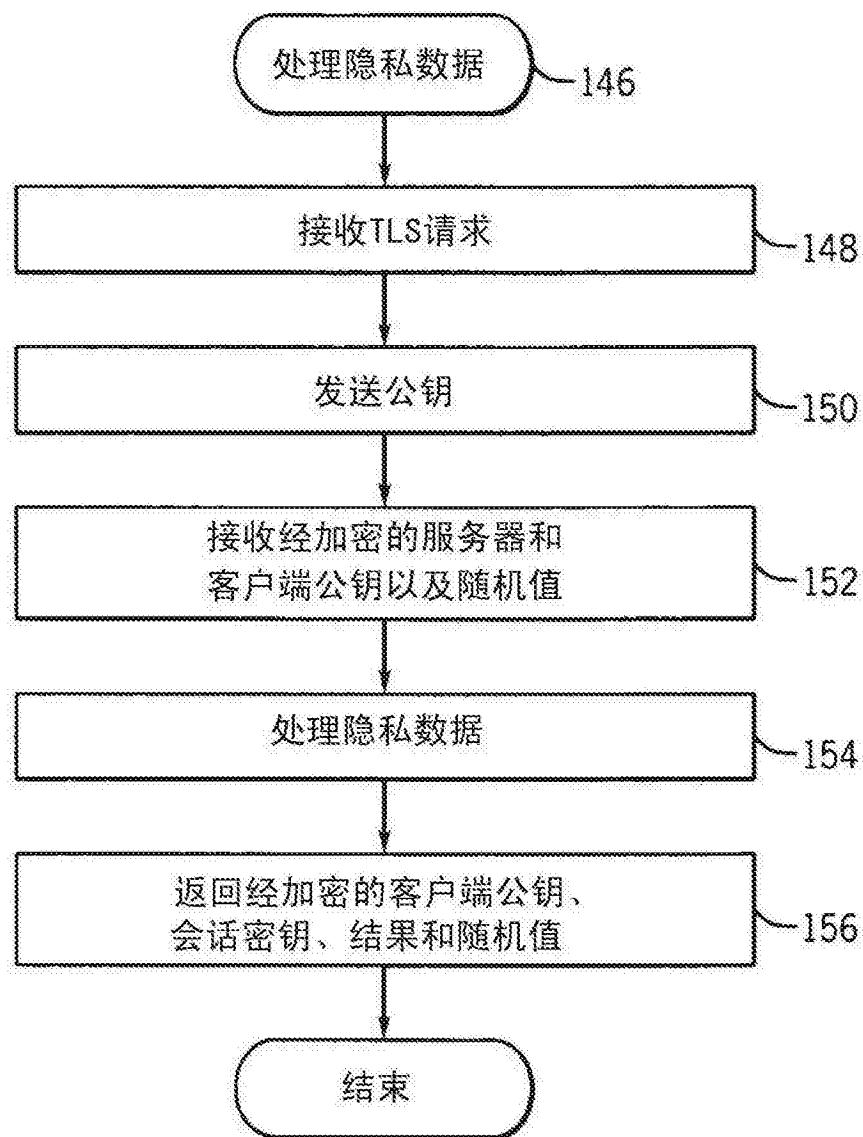


图 8

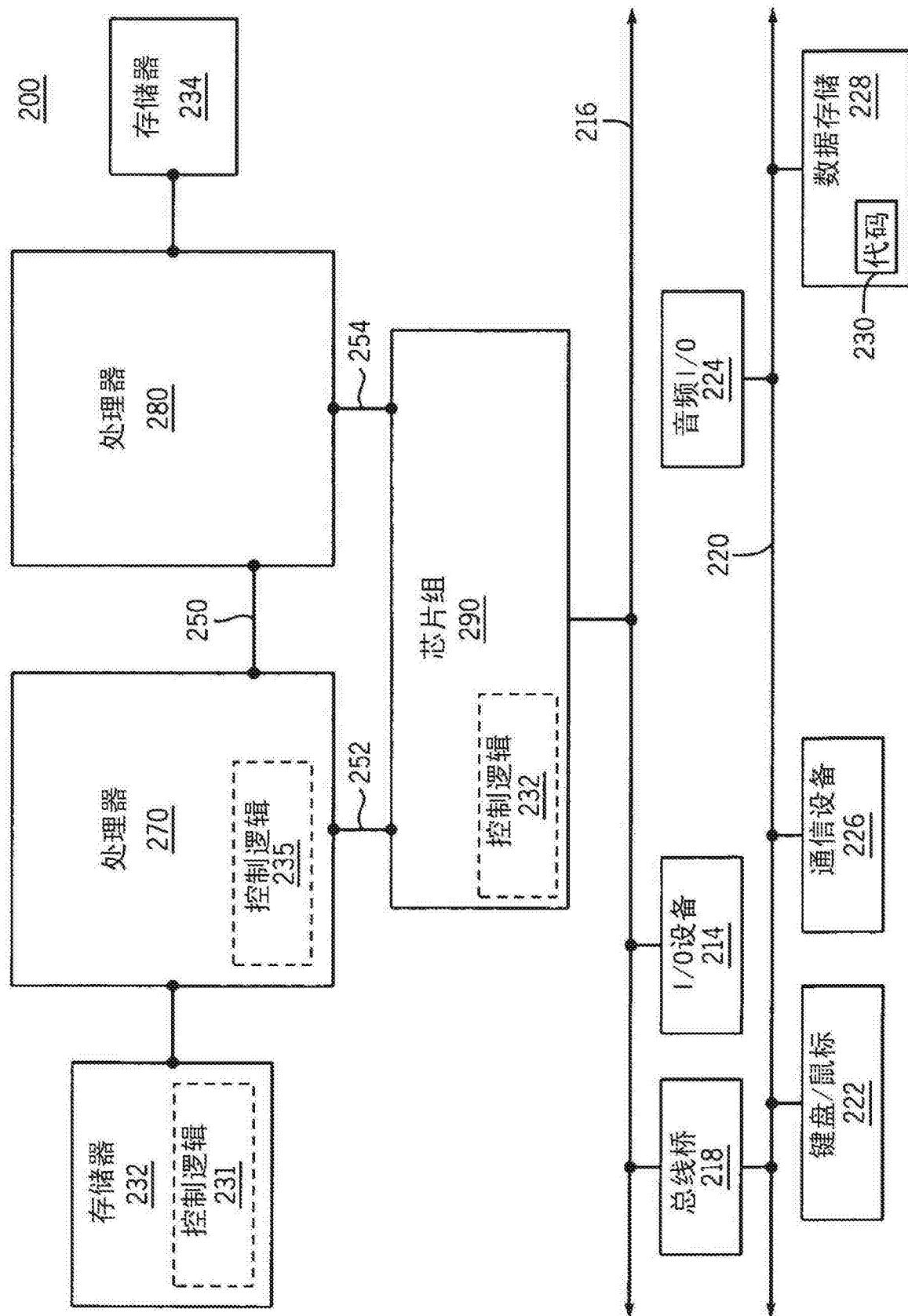


图 9