(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107016291 B
(45)授权公告日 2022.01.25

(21)申请号 201611166779.X

(22)申请日 2016.12.16

(65)同一申请的已公布的文献号
申请公布号 CN 107016291 A

(43)申请公布日 2017.08.04

(30)优先权数据
14/971806 2015.12.16 US

(73)专利权人 弗兰克公司
地址 美国华盛顿州

(72)发明人 J.P.希特尔 C.J.伍顿

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 毕铮 张涛

(51)Int.Cl.
G06F 21/60(2013.01)

(56)对比文件
WO 2014145168 A1,2014.09.18
CN 101174262 A,2008.05.07

审查员 王邦吉

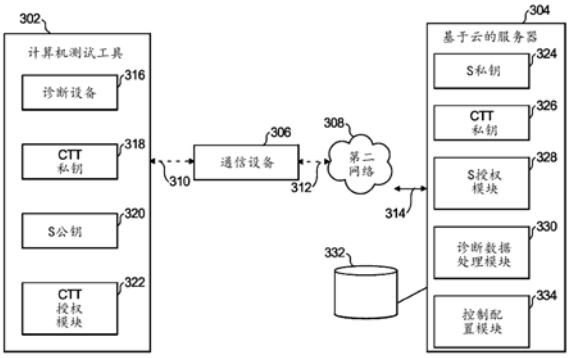
权利要求书3页 说明书12页 附图9页

(54)发明名称

计算机测试工具和基于云服务器间安全通信的系统和方法

(57)摘要

提供了用于计算机测试工具和基于云的服务器之间的安全通信的系统和方法。本发明提供了一种用于提供数据通信的系统。所述系统包括被配置为在计算机网络上执行一个或多个诊断测试的至少一个计算机测试工具。所述系统还包括至少一个通信设备，所述通信设备被配置为耦接到所述至少一个计算机测试工具，以便从所述至少一个计算机测试工具接收并缓存测试数据以及无线耦接到通信网络。另外，所述系统包括基于云的服务器，所述基于云的服务器被配置为耦接到所述通信网络以接收从所述至少一个通信设备传输的测试数据，其中所述测试数据在所述至少一个计算机测试工具中被加密并且在所述基于云的服务器中被解密。



CN 107016291 B

1.一种用于提供数据通信的系统,包括:

至少一个计算机测试工具,所述计算机测试工具被配置为在计算机网络上执行一个或多个诊断测试,并生成相关联的测试数据;

多个通信设备,每个通信设备经由对应通信信道与所述至少一个计算机测试工具通信,并与不同于所述计算机网络且不同于所述对应通信信道的通信网络无线通信;以及

基于云的服务器,所述基于云的服务器与所述通信网络通信,

其中所述至少一个计算机测试工具包括处理器,所述处理器执行计算机指令以:

加密所述测试数据并将所述测试数据的未加密的识别标签附加到加密的测试数据;

通过所述对应通信信道将具有所述识别标签的所述加密的测试数据的副本提供到所述多个通信设备中的每个;以及

当所述基于云的服务器接收到了所述加密的测试数据时向所述计算机测试工具发出确认,响应于从所述基于云的服务器接收到所述确认,而向所述多个通信设备中的每个提供指令以删除具有所述识别标签的所述加密的测试数据;

其中所述多个通信设备中的每个对应通信设备包括处理器,所述处理器执行计算机指令以:

确定所述对应通信设备是否通过所述通信网络与所述基于云的服务器通信;

响应于由所述对应通信设备确定所述对应通信设备与所述基于云的服务器通信,而将所述加密的测试数据从所述对应通信设备发送到所述基于云的服务器;以及

响应于由所述对应通信设备从所述至少一个计算机测试工具接收到所述指令,而删除具有所述识别标签的所述加密的测试数据,使得所述对应通信设备不再将所述加密的测试数据发送到所述基于云的服务器;并且

其中所述基于云的服务器包括处理器,所述处理器执行计算机指令以:

解密从所述多个通信设备中的一个接收到的所述加密的测试数据;以及

向所述至少一个计算机测试工具提供所述确认。

2.根据权利要求1所述的系统,其中利用与所述至少一个计算机测试工具相关联的私钥将所述测试数据加密,并且在所述基于云的服务器中利用与所述至少一个计算机测试工具相关联的公钥将所述测试数据解密。

3.根据权利要求1所述的系统,其中所述基于云的服务器的处理器执行另外的计算机指令以发送加密的测试数据,所述加密的测试数据经由所述通信网络和所述多个通信设备中的至少一个在所述至少一个计算机测试工具中被接收。

4.根据权利要求3所述的系统,其中所述至少一个计算机测试工具的处理器执行另外的计算机指令以解密从所述基于云的服务器发送的所述加密的测试数据。

5.根据权利要求4所述的系统,其中利用与所述基于云的服务器相关联的私钥将从所述基于云的服务器发送的所述数据加密,并且在所述至少一个计算机测试工具中利用与所述基于云的服务器相关联的公钥将所述数据解密。

6.根据权利要求1所述的系统,其中所述至少一个计算机测试工具的处理器执行另外的计算机指令以缓存从一个或多个诊断测试得到的测试数据,直到所述至少一个计算机测试工具与所述多个通信设备中的至少一个通信设备建立数据通信。

7.根据权利要求6所述的系统,其中所述至少一个计算机测试工具根据选自以下之一

的通信协议来与所述至少一个通信设备建立数据通信:BLUETOOTH®、WiFi、USB耦接以及NFC。

8.根据权利要求1所述的系统,其中所述多个通信设备中的每个对应通信设备的处理器执行另外的计算机指令以缓存从所述至少一个计算机测试工具接收的加密的测试数据,直到在所述对应通信设备和所述基于云的服务器之间建立起通信。

9.根据权利要求1所述的系统,其中所述多个通信设备选自由智能电话设备和平板设备所构成的组。

10.根据权利要求3所述的系统,其中:

所述基于云的服务器的处理器执行另外的计算机指令以向所述多个通信设备中的每个传输控制或配置数据的副本,每个副本与识别所述相关联的控制或配置数据的相同识别标签相关联;

所述计算机测试工具的处理器执行另外的计算机指令以响应于接收到所述控制或配置数据,而向所述基于云的服务器发送对所述控制或配置数据的接收确认;以及

所述基于云的服务器的处理器执行另外的计算机指令以响应于接收到所述接收确认,而向所述多个通信设备中的每个传输消息,所述消息含有删除具有与所述控制或配置数据相关联的所述识别标签的所述控制或配置数据的所有副本的指令。

11.根据权利要求1所述的系统,其中:

所述至少一个计算机测试工具的处理器执行另外的计算机指令以将到期时间附加到所述加密的测试数据,所述到期时间指示在其之后,指定删除由所述多个通信设备中的任一个所存储的所述加密的测试数据的任何副本;以及

所述基于云的服务器的处理器执行另外的计算机指令以将经由所述多个通信设备发送到所述至少一个计算机测试工具的控制或配置数据附加到过期时间,所述过期时间指示在其之后,指定删除由所述多个通信设备中的任一个存储的所述控制或配置数据的任何副本。

12.根据权利要求11所述的系统,其中所述至少一个计算机测试工具、所述多个通信设备和所述基于云的服务器删除相关联的到期时间在当前时间之后的所存储或所接收的数据的任何副本。

13.一种用于传送测试数据的计算机测试工具,包括:

被配置为存储可执行指令的存储器;以及

被设置为与所述存储器通信的处理器,其中所述处理器在执行所述指令时执行动作,所述动作包括:

在计算机网络上执行一个或多个诊断测试并生成相关联的测试数据;

缓存所述测试数据;

加密所述测试数据;

将未加密的识别标签附加到加密的测试数据,其中所述未加密的识别标签识别所述测试数据;

通过不同于被测试的所述计算机网络的通信链路将所述加密的测试数据的副本传输到多个通信设备,其中所传输的加密测试数据被配置为由基于云的服务器解密,所述基于云的服务器通过不同于所述计算机测试工具与通信设备之间的通信链路且不同于被测试

的所述计算机网络的无线网络与通信设备通信;以及

响应于从所述基于云的服务器接收到所述基于云的服务器接收到了所述加密的测试数据而向所述计算机测试工具发出的确认,而向所述多个通信设备中的每个提供指令以删除具有所述识别标签的所述加密的测试数据,使得所述多个通信设备不再将所述加密的测试数据传输到所述基于云的服务器。

14.根据权利要求13所述的计算机测试工具,其中所述计算机测试工具经由所述多个通信设备中的至少一个从所述基于云的服务器接收加密的测试数据。

15.根据权利要求14所述的计算机测试工具,其中所述计算机测试工具的处理器执行另外的指令以将从所述基于云的服务器接收的所述加密的测试数据解密。

16.根据权利要求15所述的计算机测试工具,其中利用与所述基于云的服务器相关联的私钥将从所述基于云的服务器接收的所述加密的测试数据加密,并且所述计算机测试工具利用与所述基于云的服务器相关联的公钥将所述加密的测试数据解密。

17.根据权利要求13所述的计算机测试工具,其中所述计算机测试工具缓存所述测试数据,直到所述计算机测试工具与所述多个通信设备中的至少一个建立通信链路。

18.一种用于提供数据通信的基于云的服务器,包括:

被配置为存储可执行指令的存储器;以及

被设置为与所述存储器通信的处理器,其中所述处理器在执行所述指令时执行动作,所述动作包括:

加密与计算机测试设备在计算机网络上执行诊断测试的操作相关联的控制或配置数据;

经由对应第一通信连接将所述控制或配置数据的副本传输到多个通信设备中的每个以经由第二通信连接转发到所述计算机测试设备,其中所述第一通信连接和所述第二通信连接不同于被所述计算机测试设备测试的所述计算机网络;响应于接收到所述计算机测试设备接收到了所述控制或配置数据的确认,而向所述多个通信设备中的每个提供指令以删除所述控制或配置数据的副本,使得所述多个通信设备不再将加密的测试数据传输到所述基于云的服务器;

在所述多个通信设备中的至少一个通信设备与所述基于云的服务器经由对应第一通信连接建立通信之后,从所述多个通信设备中的所述至少一个通信设备接收加密的测试数据,其中所述测试数据在由所述计算机测试设备在所述计算机网络上执行的所述诊断测试期间被捕获,在所述计算机测试设备中缓存和加密以在所述基于云的服务器中解密,并且在所述多个通信设备和所述计算机测试设备之间建立对应第二通信连接之后被所述计算机测试设备传输到所述多个通信设备;以及

解密所述加密的测试数据。

计算机测试工具和基于云服务器间安全通信的系统和方法

技术领域

[0001] 本发明所公开的实施例整体涉及用于监测测试设备的系统和方法，并且更具体地讲，涉及用于计算机测试工具和基于云的服务器之间的通信的安全系统和方法。

背景技术

[0002] 相关领域的说明

[0003] 测试设备(例如，计算机测试工具)可能够与基于云的(也称为云端)服务器通信。在一些配置中，计算机测试工具和服务器必须同时耦接到网络以便交换数据。然而，计算机测试工具在需要数据交换的关键时刻可能无法访问用于交换数据的网络连接。

[0004] 为了能够访问网络，移动设备(诸如，移动电话、平板电脑或膝上型计算机)可被耦接到计算机测试工具，以收集和存储来自计算机测试工具的数据，并随后将数据传输到服务器。然而，入侵者可冒充计算机测试工具或通信设备，并向服务器发送虚假或伪造的诊断数据。在另一种情况下，入侵者可冒充服务器或通信设备，并向计算机测试工具发送虚假或伪造的控制或配置数据。

发明内容

[0005] 以下描述的图示实施例的目的和优点将在下面的具体实施方式中示出并且是显而易见的。图示实施例的附加优点将通过书面具体实施方式和本文的权利要求书以及附图中具体指出的设备、系统和方法来实现和获得。

[0006] 为了实现这些及其他优点并且根据图示实施例的目的，在一个方面，描述了一种用于提供数据通信的系统。该系统包括被配置为在计算机网络上执行一个或多个诊断测试的至少一个计算机测试工具。该系统还包括至少一个通信设备，该通信设备被配置为耦接到至少一个计算机测试工具，以便从所述至少一个计算机测试工具接收并缓存测试数据以及无线耦接到通信网络。另外，该系统包括基于云的服务器，该基于云的服务器被配置为耦接到通信网络，以便接收从至少一个通信设备传输的测试数据，其中测试数据在所述至少一个计算机测试工具中被加密并且在基于云的服务器被解密。

[0007] 在实施例中，可利用与所述至少一个计算机测试工具相关联的私钥将测试数据加密，并且在基于云的服务器中利用与所述至少一个计算机测试工具相关联的公钥将此数据解密。所述基于云的服务器可还被配置为发送将被所述至少一个计算机测试工具经由通信网络和所述至少一个通信设备所接收的加密数据。

[0008] 此外，在实施例中，该至少一个计算机测试工具还被配置为将从基于云的服务器发送的加密数据解密。可利用与基于云的服务器相关联的私钥将从基于云的服务器发送的数据加密，并且在所述至少一个计算机测试工具中利用与基于云的服务器相关联的公钥将此数据解密。所述至少一个计算机测试工具可还被配置为缓存从一个或多个诊断测试得到的测试数据，直到该至少一个计算机测试工具与所述至少一个通信设备建立数据通信。所述至少一个计算机测试工具可根据选自以下之一的通信协议与所述至少一个通信设备建

立数据通信:蓝牙、WiFi、USB耦接以及NFC。

[0009] 另外,在实施例中,所述至少一个通信设备可还被配置为缓存从所述至少一个计算机测试工具接收的加密的测试数据,直到在所述至少一个通信设备和基于云的服务器之间建立起通信。该至少一个通信设备可选自智能电话设备和平板设备。

[0010] 在实施例中,计算机测试工具可向所述至少一个通信设备传输测试数据的多个副本,每个副本与识别相关联的测试数据的相同识别标签相关联。响应于接收到测试数据的副本,基于云的服务器可向所述计算机测试工具发送对接收到所识别的测试数据的确认。响应于接收到此接收确认,所述计算机测试工具可向所述至少一个通信设备传输消息,该消息含有删除关联有该识别标签的测试数据的所有副本的指令。

[0011] 此外,在实施例中,基于云的服务器可向所述至少一个通信设备传输控制或配置数据的多个副本,每个副本与识别相关联的控制或配置数据的相同识别标签相关联。响应于接收到测试数据副本,所述计算机测试工具可向基于云的服务器发送对接收到所识别的控制或配置数据的确认。响应于接收到此接收确认,基于云的服务器可向所述至少一个通信设备传输消息,该消息含有删除关联有识别标签的控制或配置数据的所有副本的指令。

[0012] 另外,在实施例中,所述至少一个计算机测试工具和基于云的服务器还可被配置为使要与所述至少一个通信设备交换的数据与相关联的到期时间相关联,该到期时间指示在该时间之后,指定删除由所述至少一个计算机测试工具、所述至少一个通信设备或基于云的服务器中的任一者所存储的诊断数据的任何副本。所述至少一个计算机测试工具、所述至少一个通信设备和基于云的服务器可还被配置为删除相关联的到期时间在当前时间之后的所存储或所接收的数据的任何副本。

[0013] 在另外的可选方面,描述了一种用于传送测试数据的计算机测试工具。该计算机测试工具包括被配置为存储可执行指令的存储器和被设置为与该存储器通信的处理器,其中所述处理器在执行指令时被配置为在计算机网络上执行一个或多个诊断测试并输出相关联的测试数据、缓存测试数据、加密测试数据并将加密的测试数据传输到通信设备,其中被传输的加密测试数据被配置为由耦接到通信设备的基于云的服务器解密。

[0014] 在实施例中,计算机测试工具可经由通信网络和所述至少一个通信设备从基于云的服务器接收加密数据。所述计算机测试工具可还被配置为将从基于云的服务器接收的加密数据解密。可利用与基于云的服务器相关联的私钥将从基于云的服务器接收的数据加密,并且可在计算机测试工具中利用与基于云的服务器相关联的公钥将此数据解密。计算机测试工具可缓存测试数据,直到所述计算机测试工具与至少一个通信设备建立数据通信。

[0015] 在另外的可选方面,描述了一种用于提供数据通信的基于云的服务器。该基于云的服务器包括被配置为存储可执行指令的存储器和被设置为与该存储器通信的处理器,其中该处理器在执行指令时被配置为在通信设备与基于云的服务器之间经由通信网络建立通信之后,从通信设备接收加密的测试数据,其中所述测试数据在计算机测试设备中执行诊断测试期间被捕获,在计算机测试设备中缓存和加密,被配置为在基于云的服务器中解密,并在通信设备和计算机测试设备之间建立通信之后被传输到通信设备。该处理器还被配置为在执行指令时将加密的测试数据解密。

附图说明

[0016] 附带的附录和/或附图示出了根据本公开的各种非限制性、示例性、创造性方面：

[0017] 图1示出了示例性通信网络；

[0018] 图2示出了示例性网络设备/节点；

[0019] 图3是示出根据本公开的云辅助诊断系统的流程图；

[0020] 图4是示出根据本公开的由计算机测试工具执行以安全传输诊断数据的方法的流程图；

[0021] 图5是示出根据本公开的由计算机测试工具执行以安全地接收控制与配置数据的方法的流程图；

[0022] 图6是示出根据本公开的由通信设备执行以与计算机测试工具或服务器安全地交换数据的方法的流程图；

[0023] 图7是示出根据本公开的由服务器执行以安全地接收诊断数据的方法的流程图；

[0024] 图8是示出根据本公开的由服务器执行以安全地传输控制和配置数据的方法的流程图；以及

[0025] 图9是示出根据本公开的具有多个通信设备的云辅助诊断系统的流程图。

具体实施方式

[0026] 现在参照附图更全面地描述图示实施例，其中类似的附图标记表示类似的结构/功能特征结构。图示实施例不以任何方式限于所示内容，因为下面所描述的图示实施例仅仅是示例性的，如本领域技术人员所理解的那样，其能够以各种形式实施。因此，应当理解，本文所公开的任何结构和功能细节不应被解释为限制，而仅仅是作为权利要求书的基础，并作为用于教导本领域技术人员以各种方式采用所讨论实施例的表示。此外，本文所使用的术语和短语不旨在是限制性的，而是提供所示实施例的可理解描述。

[0027] 除非另有定义，否则本文所用的所有技术术语和科学术语都具有与本发明所属领域的普通技术人员通常理解的相同含义。但是与本文所述的那些类似或等同的任何方法和材料也可用于所示实施例的实践或测试，现在描述示例性方法和材料。

[0028] 必须注意，如本文和所附权利要求所用，单数形式“一个”和“该”包括复数指示物，除非上下文另有明确指示。因此，例如，对“一个激励”的引用包括多个这样的激励，并且对“该信号”的引用包括对一个或多个信号以及本领域技术人员已知的其等同物的引用，以此类推。

[0029] 应当理解，下面讨论的图示实施例优选地为驻留在计算机可用介质上的软件算法、程序或代码，该计算机可用介质具有用于启用具有计算机处理器的机器的执行的控制逻辑。机器通常包括被配置用于提供来自计算机算法或程序执行的输出的记忆存储。

[0030] 如本文所用，术语“软件”是指与可在主计算机处理器中的任何代码或程序同义，而不考虑其实施是在硬件、固件中还是作为在盘上可用的计算机软件产品、记忆存储设备或者用于从远程机器下载。本文所述的实施例包括这种软件，以实施上述公式、关系和算法。本领域技术人员将基于上述实施例来理解图示实施例的其他特征和优点。因此，除了由所附权利要求所指示的之外，图示实施例不限于已经具体示出和描述的内容。

[0031] 现在描述性地转到附图，其中在所有若干视图中类似的参考特征表示类似的元

件。图1描绘了其中可实现以下所示实施例的示例性通信网络100。

[0032] 应当理解，通信网络100是通过通信链路互连的节点和用于在端节点之间传输数据的段的地域上分布的集合，诸如，个人计算机、工作站、智能电话设备、平板电脑、电视机、传感器和/或其他设备(诸如汽车等)。可获得许多类型的网络，其类型范围从局域网(LAN)到广域网(WAN)。LAN通常通过位于相同的一般物理位置(诸如，建筑物或校园)处的专用私人通信链路来连接节点。另一方面，WAN通常通过长距离通信链路，诸如，公共载波电话线、光学光路、同步光网络(SONET)、同步数字体系(SDH)链路或电力线通信(PLC)等来连接地域上分散的节点。

[0033] 图1是示例性通信网络100的示意性框图，该图示例性地包括通过各种通信方法经由链路109互连的节点/设备101-108(例如，传感器102、客户端计算设备103、智能电话设备105、网络服务器106、路由器107、交换机108等)。例如，链路109可以是有线链路或者可包括无线通信介质，其中某些节点与其他节点通信，例如，基于距离、信号强度、当前操作状态、位置等。此外，在适当的时候，每个设备可使用本领域技术人员将理解的预定义的网络通信协议(诸如，各种有线协议和无线协议等)向其他设备传送数据包(或帧)142。在该上下文中，协议由定义节点如何相互交互的一组规则组成。本领域技术人员将理解，计算机网络中可使用任何数量的节点、设备、链路等，并且本文所示的视图是出于简便目的。此外，虽然本文结合一般的网络云示出了实施例，但是本文的具体实施方式不限于此，并且可被应用于硬连线的网络。

[0034] 如本领域技术人员将理解的那样，本发明的各个方面可被体现为系统、方法或计算机程序产品。因此，本发明的各个方面可采取完全硬件实施例、完全软件实施例(包括固件、驻留软件、微代码等)或者组合软件和硬件方面的实施例的形式，在本文中这些实施例可全部被称为“电路”、“模块”或“系统”。此外，本发明的各个方面可采取计算机程序产品的形式，该计算机程序产品在其上体现计算机可读程序代码的一种或多种计算机可读介质中体现。

[0035] 可采用一种或多种计算机可读介质的任意组合。计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可以是，例如但不限于电子、磁、光学、电磁、红外或半导体系统、装置或设备或前述项的任意合适组合。计算机可读存储介质的更具体的例子(非穷尽列表)将包括下列项：具有一条或多条线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存)、光纤、便携式光盘只读存储器(CD-ROM)、光存储设备、磁存储设备或前述项的任意合适组合。在本文的语境中，计算机可读存储介质可以是可包含或存储供指令执行系统、设备或装置使用或与指令执行系统、设备或装置结合使用的程序的任何有形介质。

[0036] 计算机可读信号介质可包括其中体现计算机可读程序代码的传播数据信号，例如，在基带中或作为载波的一部分。这种传播信号可采取多种形式中的任何一种，包括但不限于电磁、光学或其任何合适的组合。计算机可读信号介质可以是满足以下条件的任何计算机可读介质，该计算机可读介质并非计算机可读存储介质，并且可传送、传播或传输供指令执行系统、装置或设备使用或与其结合的程序。

[0037] 可使用任何合适的介质传输体现在计算机可读介质上的程序代码，包括但不限于无线、有线、光纤电缆、RF等，或上述介质的任意合适组合。

[0038] 用于执行本发明各个方面的操作的计算机程序代码可通过一种或多种编程语言的任意组合来编写，该编程语言包括面向对象的编程语言(诸如，Java、Smalltalk、C++等)和常规的程序化编程语言，诸如，“C”编程语言或类似的编程语言。程序代码可全部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、部分在用户计算机上执行且部分在远程计算机上执行，或者全部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)连接到用户的计算机，或者可连接到外部计算机(例如，通过使用因特网服务提供商的因特网)。

[0039] 下面描述了根据本发明实施例的参考方法、装置(系统)和计算机程序产品的流程图和/或框图的本发明的各方面。应当理解，流程图和/或框图中的每个框以及流程图和/或框图中的框的组合可通过计算机程序指令来实施。可将这些计算机程序指令提供给通用计算机、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，使得经由计算机处理器或其他可编程数据处理装置执行的指令创建用于实施流程图和/或框图中一个或多个框中指定的功能/动作的方法。

[0040] 还可将这些计算机程序指令存储在计算机可读介质中，该计算机可读介质可指示计算机、其他可编程数据处理装置或其他设备以特定方式工作，使得存储在计算机可读介质中的指令产生制品，该制品包括实施流程图和/或框图中一个或多个框中指定的功能/动作的指令。

[0041] 还可将计算机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，以使得在计算机、其他可编程装置或其他设备上进行一系列操作步骤，以产生计算机实施的过程，使得在计算机或其他可编程装置上执行的指令提供用于实施流程图和/或框图中一个或多个框中指定的功能/动作的方法。

[0042] 图2是可与本文所述的一个或多个实施例(或其组件)，例如，作为网络100中所示的节点之一，一起使用的示例性网络计算设备200(例如，客户端计算设备103、服务器106等)的示意性框图。如上所述，在不同的实施例中，这些各种设备被配置为以任何合适方式彼此通信，诸如，经由通信网络100进行通信。

[0043] 设备200旨在表示能够执行本发明各种实施例的教导内容的任何类型的计算机系统。设备200仅是合适系统的一个例子，并且旨在不对本文所述的本发明实施例的使用范围或功能进行任何限制。无论如何，计算设备200能够实施和/或执行本文所示的任何功能。

[0044] 计算设备200与许多其他通用或专用计算系统环境或配置一起操作。可适于与计算设备200一起使用的熟知的计算系统、环境和/或配置的例子包括但不限于个人计算机系统、服务器计算机系统、瘦客户端、厚客户端、手持式设备或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、小型计算机系统以及包括任一上述系统或设备的分布式数据处理环境等。

[0045] 可在通过计算机系统执行的计算机系统可执行指令(诸如，程序模块)的一般上下文中描述计算设备200。通常，程序模块可包括执行特定任务或实施特定抽象数据类型的例程、程序、对象、组件、逻辑、数据结构等。计算设备200可在分布式数据处理环境中操作，其中任务由通过通信网络链接的远程处理设备执行。在分布式数据处理环境中，程序模块可位于包含记忆存储设备的本地和远程计算机系统存储介质中。

[0046] 图2以通用计算设备的形式示出了设备200。设备200的组件可包括但不限于一个

或多个处理器或处理单元216、系统存储器228和总线218，该总线将包括系统存储器228的各种系统组件耦接到处理器216。

[0047] 总线218表示任何几类总线结构中的一种或多种，包括存储器总线或存储器控制器、外围总线、加速图形端口，以及使用多种总线架构中任一种的处理器或局域总线。举例来说，而非限制，这种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)局域总线和外围组件互连(PCI)总线。

[0048] 计算设备200通常包括多种计算机系统可读介质。此类介质可以是设备200可访问的任何可用介质，并且其包括易失性和非易失性介质、可移动和不可移动介质。

[0049] 系统存储器228可包括易失性存储器(诸如，随机存取存储器(RAM) 230和/或高速缓冲存储器232)形式的计算机系统可读介质。计算设备200还可包括其他可移动/不可移动、易失性/非易失性计算机系统存储介质。仅举例来说，存储系统234可从不可移动、非易失性磁介质(未示出，并且通常被称为“硬盘驱动器”)的读取以及向该磁介质写入。虽然未示出，但是可提供用于从可移动非易失性磁盘(例如，“软盘”)读取和向其写入的磁盘驱动器，以及用于从可移动非易失性光盘(诸如，CD-ROM、DVD-ROM或其他光学介质)读取和向其写入的光盘驱动器。在这种情况下，每者都可通过一个或多个数据介质接口连接到总线218。如下面将进一步描绘和描述的那样，存储器228可包括至少一个程序产品，该程序产品具有被配置为执行本发明实施例功能的一组(例如，至少一个)程序模块。

[0050] 具有一组(至少一个)程序模块215(诸如，承保模块)的程序/实用程序240能够以举例的方式而非限制地存储在存储器228以及操作系统、一个或多个应用程序、其他程序模块和程序数据中。操作系统、一个或多个应用程序、其他程序模块和程序数据或它们的某种组合中的每一者都可包括联网环境的实施。程序模块215通常执行如本文所述的本发明实施例的功能和/或方法。

[0051] 设备200还可与一个或多个外部设备214通信，诸如，键盘、指示设备、显示器224等；使用户能够与计算设备200交互的一个或多个设备；和/或使计算设备200能够与一个或多个其他计算设备通信的任何设备(例如，网卡、调制解调器等)。这种通信可经由输入/输出(I/O)接口222进行。但设备200还可经由网络适配器220与一个或多个网络通信，诸如局域网(LAN)、通用广域网(WAN)和/或公共网络(例如，因特网)。如图所示，网络适配器220经由总线218与计算设备200的其他组件通信。应当理解，尽管未示出，但是可结合设备200使用其他硬件和/或软件组件。其例子包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动器阵列、RAID系统、磁带驱动器和数据归档存储系统等。

[0052] 在下面的描述中，可参考由一个或多个计算设备(诸如，图2中的计算系统环境200)进行的操作的动作和符号表示来描述某些实施例。因此，应当理解，这种动作和操作(有时被称为由计算机执行的)包括计算机处理器对以结构化形式表示数据的电信号的操纵。这种操纵转换数据或使其保持在计算机存储器系统中的位置，这样以本领域技术人员所理解的方式重新配置或以其他方式改变计算机的操作。保持数据的数据结构是具有由数据格式定义的特定属性的存储器的物理位置。然而，虽然在前述上下文中描述了一个实施例，但是其并不旨在限制，因为本领域技术人员将理解，下文中描述的动作和操作也可在硬件中实施。

[0053] 图1和图2旨在对其中可实现下文描述的本发明实施例的说明性和/或合适的示例

性环境进行简要一般描述。图1和图2是合适环境的示例，并且不旨在对本发明的实施例的结构、使用范围或功能性进行任何限制。特定环境不应被解释为具有与示例性操作环境中示出的任一部件或部件组合有关的任何相关性或需求。例如，在某些情况下，环境的一个或多个元件可被认为是不必要的并被省略。在其他情况下，一个或多个其他元件可被认为是必要的并被添加。

[0054] 上文中总体上示出并讨论了示例性通信网络100(图1)和计算设备200(图2)，现在将描述本发明的某些图示实施例。现在参考图3至图5，总体上示出了云辅助诊断系统300，其中计算机测试工具302经由通信设备306与基于云的服务器304间接通信，其中计算机测试工具302和服务器304之间的通信受保护以防止通信设备304访问通信内容，并且还防止伪造消息被发送到计算机测试工具302和/或服务器304。

[0055] 计算机测试工具302和通信设备306可各自为计算机系统，每个计算机系统用作可类似于图1所示的通信网络100那样配置的第一网络的节点(例如，节点101至105、107或108)。计算机测试工具302和通信设备306经由至少一个第一通信链路308彼此通信。类似地，服务器304是用作节点(例如，节点106)的计算机系统，并且通信设备306用作第二网络308的节点(例如，节点101至105、107或108)，该第二网络可类似于通信网络100那样进行配置。

[0056] 因此，公钥加密使用非对称密钥算法，其中一个设备用来执行加密或解密的密钥与另一个设备在对应操作中使用的密钥不相同。涉及利用公钥加密的双向通信的每一个设备均具有一对加密密钥：公共加密密钥和私有解密密钥。公钥可被广泛传播，而私钥只有其所有者才知道。密钥是在数学上相关的，但是通过选择参数使得无法从公钥计算出私钥。

[0057] 计算机测试工具302、通信设备306和服务器304可各自被配置为类似于图2所示的网络计算设备200，例如被配置为包括处理单元216、网络适配器220、I/O接口222和存储器228。第一通信链路310、第二通信链路312和第三通信链路314可各自包括单个或多个有线和/或无线链路。在实施例中，这些链路中的一些使用近场通信，诸如射频识别(RFID)、蓝牙、红外通信等。在实施例中，第二网络308包括因特网。

[0058] 计算机测试工具302可以是包括诊断设备316的移动或固定设备，该诊断设备包括一个或多个传感器以测量物理实体的特性，诸如信号或电源的电特性、温度、施加的力等。诊断设备316根据需要结合模数(A/D)转换来输出指示与测量相关联的至少一个值的诊断数据。

[0059] 由诊断设备302输出的诊断数据被存储在存储设备诸如存储器228中。例如，所输出的诊断数据在被提交至通信设备306之前可被缓存或存储(例如，在高速缓冲存储器232或存储系统234中)。另外，计算机测试工具302(例如，在存储器228中)存储计算机测试工具(CTT)私钥318，该私钥用于加密由计算机测试工具302传输(例如传输到客户端306)的诊断数据。计算机测试工具302还存储与服务器304相关联的服务器(S)公钥320，该公钥用于将从服务器304接收的消息解密。下文更详细地讨论了CTT私钥318和S公钥320。

[0060] 根据请求和/或在建立通信链路310之后，计算机测试工具302可向经由通信链路310耦接到计算机测试工具302的通信设备306传输(例如，经由网络适配器220)诊断数据。

[0061] 计算机测试工具302包括处理与通信设备306交换(例如，从其接收或向其发送)的消息的认证模块322(例如，由服务器304的存储器228存储的程序模块215)，通过处理来认

证所接收的消息由计算机测试工具304发送，以及传输到服务器304的消息由计算机测试工具302发送。

[0062] 通信设备306可以是用作促进计算机测试工具302和服务器304之间的消息交换的中间设备的固定或便携式设备(例如，电话、平板电脑或膝上型计算机)。在一个实施例中，通信设备306可用作向计算机测试工具302提供WiFi服务的热点，允许计算机测试工具302经由WiFi与服务器304通信。在该实施例中，传输到计算机测试工具302或从其传输的数据通过通信设备306朝目的地路由。本实施例中的通信设备306包括能够使其用作热点的硬件和/或/软件(例如，程序模块215)。

[0063] 在另一个实施例中，计算机测试工具302被连接到通信设备306，其中通信链路310是包括例如电缆(例如，USB或以太网)或无线近场通信的固定链路。通信设备306充当计算机测试工具302和服务器324之间的中间设备，包括经由通信链路310与计算机测试工具302交换数据，以及经由通信312和因特网与服务器304交换数据。本实施例中的通信设备306包括硬件和/或/软件(例如，程序模块215)，该硬件和/或/软件能够使该通信设备在通信链路310可操作时从计算机测试工具302接收并存储诊断数据，并且当通信链路312可操作时将所存储的诊断数据传输到服务器304。在一个实施例中，当通信链路310和通信链路312都可操作时，通信设备306可放弃存储诊断数据。

[0064] 服务器304是经由通信链路314耦接(例如，经由网络适配器220)到第二网络308来与一个或多个通信设备306通信的网络服务器。通信链路314可以是有线、无线或者其组合，它在与通信设备306中的一者通信的操作期间可以是稳定的并且可随时提供。另外，服务器304可随时与通信设备306通信，从而接收、处理和/或存储诊断数据，并且向计算机测试工具302发送消息，例如控制或配置(corc)消息。操作时间可包括例如一天或一周的指定时间，或者一天或一周(24/7)的除了存在故障或定期维护的时间之外的任何时间。

[0065] 服务器304(例如，在存储器228中)存储S私钥324，该私钥用于加密由服务器304传输(例如传输到客户端306)的诊断数据。服务器304还存储与相应的一个或多个计算机测试工具302相关联的至少一个CTT公钥326，该公钥用于解密从计算机测试工具302接收的消息。服务器304包括处理与通信设备306交换的消息的认证模块328(例如，由服务器304的存储器228存储的程序模块215)，通过处理来认证所接收的消息由计算机测试工具302发送，以及传输到计算机测试工具302的消息由服务器304发送。

[0066] 服务器304还包括处理诊断数据和/或将诊断数据存储在存储设备332中的诊断数据处理模块330(例如，由服务器304的存储器228存储的程序模块215)。存储设备332可包括在服务器304中或作为其外围设备。服务器304还包括生成控制和/或配置数据从而控制和配置计算机测试工具302的控制和配置模块334(例如，由服务器304的存储器228存储的程序模块215)。

[0067] 在操作中，通信设备306使用第二通信链路310与第二网络308进行通信，而服务器304使用第三通信链路312与第二网络308通信。如虚线所指出的那样，通信链路310可以是间歇的，使得计算机测试工具302和通信设备306可选择性地断开，来使得链路310断开，在断开之后可重新建立连接。类似地，如虚线所指出的那样，通信链路312可以是间歇的，使得通信设备306可选择性地断开与第二网络308的通信，来使得链路312断开，在断开之后可重新建立连接。

[0068] 在一个示例性实施例中，所述第一通信链路是单个近场通信链路或有线通信链路，诸如使用蓝牙通信或USB电缆，其中所述第一网络仅包括链接的计算机测试工具302和通信设备306。计算机测试工具302执行诊断测试，并且在时间t1之前将相关联的诊断数据存储在计算机测试工具302的本地存储器中。在时间t2，计算机测试工具302和通信设备306可经由第一通信链路310耦接。通信设备306是可在时间t3耦接到第二网络308以与服务器304通信的移动电话、平板电脑或笔记本电脑。服务器304经由稳定连接耦接到第二网络308，从而使其可用于向一个或多个计算机测试工具302提供服务。在一个实施例中，t1、t2和/或t3可按时间顺序间隔排列(即，在时间上彼此间隔开)。

[0069] 换句话讲，计算机测试工具302可执行一个或多个诊断测试并将相关联的诊断测试数据存储在本地存储器中，所有这些都发生在时间t1之前。持有通信设备306的用户可在随后的时间t2接近计算机测试工具302，从而使用近场通信将通信设备306耦接到计算机测试工具302。诊断数据或者其副本可在时间t2被传送到通信设备306，并且由通信设备306临时存储。在随后的时间t3，通信设备306可耦接到第二网络308并且将诊断数据传送到服务器304。在一个实施例中，计算机测试工具302可在时间t1经由第一网络(第一通信链路310)耦接到通信设备306，这样t1和t2可几乎在同一时刻。在一个实施例中，通信设备306可在时间t2耦接到第二网络308，这样t2和t3可几乎在同一时刻。

[0070] 当通信设备306被用作热点或被固定时，经由通信链路310、通信链路312进行数据交换可容易受到渗透的侵扰，诸如被冒充成通信设备306传输虚假或伪造数据的设备渗透。诊断系统300尤其容易受到传输虚假或伪造数据的威胁，因为传输到计算机测试工具302或服务器304的数据可由通信设备306存储。计算机测试工具302包括CTT认证模块322，该模块验证从通信设备306接收的数据源自服务器304，并且认证从计算机测试工具302发送的数据。类似地，服务器304包括S认证模块328(下文详述)，该模块验证从通信设备306接收的数据源自计算机测试工具302，并且认证从服务器304发送的数据。

[0071] 现在参考图4至图8，示出了展示各种示例性实施例的实施的流程图。需注意，图4至图8中示出的操作顺序并非必须，因此原则上可不按照所示顺序执行各个操作。也可跳过某些操作，可添加或替换不同操作，或者可遵循本文所描述的实施例在单独应用中进行所选操作或操作组。

[0072] 图4示出了当从计算机测试工具302向通信设备306传输诊断数据时，根据本公开的方法执行的操作的流程图。在操作401处，存储CTT私钥318。在操作402处，诊断装置316测量与物理实体相关联的特性并输出诊断数据。在操作404处，由诊断设备316输出的诊断数据由计算机测试工具302存储(例如，存储在高速缓冲存储器232或存储系统234中)。在操作406处，执行等待循环直到发生触发，其中所述触发可包括例如经由通信链路310在计算机测试工具302和通信设备306之间建立耦接。所述触发可还包括或需要例如由计算机测试工具302和通信设备306中的任一者或者其组合提交的请求。在操作408处，CTT认证模块322使用CTT私钥318来加密将要传送的所存储的诊断数据。在操作410处，加密的诊断数据被传输至与其耦接的通信设备306，以便经由通信设备306将加密的诊断数据传输到服务器304，其中通信设备306无法对数据进行解密，但服务器304存储能够使服务器304解密数据的解密密钥(例如，CTT公钥)。

[0073] 图5示出了当通过计算机测试工具302从服务器304接收控制和/或配置数据时，根

据本公开的方法执行的操作的流程图。在操作501处，存储S公钥318。在操作502处，执行等待循环直到发生触发，其中所述触发可包括例如经由通信链路310在计算机测试工具302和通信设备306之间建立耦接。所述触发可还包括或需要例如由计算机测试工具302和通信设备306中的任一者或者其组合提交的请求。在操作504处，从耦接的通信设备306接收加密的控制和/或配置数据，其中所述加密的控制和/或配置数据从服务器304传输到通信设备306，并且通信设备306不具有用于将所述加密的控制和/或配置数据解密的密钥。在操作506处，CTT认证模块322使用S公钥320对加密的控制和/或配置数据进行解密。在操作508处，对控制和/或配置数据进行处理以控制或配置(例如，布防(禁用)、撤防(重新启用、更新))计算机测试工具302。

[0074] 图6示出了在使用通信设备306与计算机测试工具302或服务器304交换数据时，根据本公开的方法执行的操作的流程图。在操作602处，执行等待循环直到发生触发，其中所述触发可包括例如经由通信链路310建立与计算机测试工具302和通信设备306中的一者的耦接，或者经由通信链路312建立与通信设备306和服务器304的耦接。所述触发可还包括或需要例如由计算机测试工具302、服务器304和通信设备306中的任一者或者其组合提交的请求。在操作604处，从计算机测试工具302或者从服务器304接收加密的数据(诊断数据或控制和/或配置数据)。通信设备306无法对所接收的数据进行解密。

[0075] 在操作606处，执行等待循环直到发生触发，其中所述触发可包括例如经由通信链路310建立与计算机测试工具302和通信设备306中的另一者的耦接，或者经由通信链路312建立通信设备306和服务器304的耦接。所述触发可还包括或需要例如由计算机测试工具302、服务器304和通信设备306中的任一者或者其组合提交的请求。在操作608处，所接收的数据被传输至已建立耦接的计算机测试工具302和服务器304中的另一者。可由接收数据的计算机测试工具302或服务器304使用为该设备所存储的公钥将此数据解密。

[0076] 图7示出了当通过服务器304使用通信设备306接收诊断数据时，根据本公开的方法执行的操作的流程图。在操作701处，存储CTT公钥318。在操作702处，执行等待循环直到发生触发，其中所述触发可包括例如经由通信链路312在通信设备306和服务器304之间建立耦接。所述触发可还包括或需要例如由服务器304和通信设备306中的任一者或者其组合提交的请求。在操作704处，接收加密的诊断数据。所述加密的诊断数据由通信设备306传输到服务器304，其中通信设备306无法将所述加密的诊断数据解密(例如，没有公钥)。在操作706处，S认证模块328使用CTT公钥320来解密诊断数据。在操作708处，所述解密的诊断数据由诊断数据处理模块330处理和/或存储在存储设备332中。

[0077] 图8示出了当由服务器304经由通信设备306向计算机测试工具302传输控制和/或配置数据时，根据本公开的方法执行的操作的流程图。在操作801处，存储S私钥324。在操作802处，执行等待循环直到发生触发，其中所述触发可包括例如经由通信链路312在通信设备306和服务器304之间建立耦接。所述触发可还包括或需要例如由服务器304和通信设备306中的任一者或者其组合提交的请求。在操作804处，控制和/或配置数据(例如由控制和配置模块334生成)由S认证模块328使用S私钥324进行加密。在操作804处，将加密的控制和/或配置数据传输到通信设备306，其中通信设备306无法将所述加密的控制和/或配置数据解密，但是计算机测试工具302存储有能够使计算机测试工具302将所述加密的控制和/或配置数据解密的解密密钥(例如，S公钥)。

[0078] 图9示出了本公开的另一个实施例的流程图，其中提供了多个通信设备306a至306n。通信设备306a至306n通过各自的通信链路310a至310n耦接到计算机测试工具202，并且经由各自的通信链路312a至312n耦接到服务器304。

[0079] 在操作中，当CTT认证模块322或S认证模块328加密数据消息时，其将未加密的识别标签(例如，数字字母混合的标签)附加到该消息。所述消息的多个副本可被传输到通信设备306a至306n中的多个设备。在一个实施例中，当服务器304接收到所述消息副本中的一个时，服务器304可解密、处理和/或存储这多个消息中的仅一个，而其他副本可被忽略和/或删除。在一个实施例中，当服务器304接收到所述消息的第一副本时，服务器304可向计算机测试工具302发送加密的确认。例如，响应于此确认，服务器304和/或计算机测试工具302可向计算机测试工具302能够与其耦接的通信设备306a至306n发送未加密的“删除所有副本”(DAD)消息。DAD消息指示通信设备306a至306n删除ID为正在存储或处理的数据消息的任何副本。因此，响应于DAD消息的通信设备306a至306n将不再存储或传输已经由服务器304接收的消息的副本。

[0080] 类似地，在一个实施例中，当计算机测试工具302接收到消息的副本中的一个时，该计算机测试工具302可解密、处理和/或存储多个消息中的仅一个，而其他副本可被忽略和/或删除。在一个实施例中，当计算机测试工具302接收到消息的第一副本时，该计算机测试工具302可向服务器304发送加密的确认。响应于该确认，服务器304向所选择的通信设备306a至306n发送未加密的DAD消息，这些选择的通信设备具有与计算机测试工具耦接的跟踪历史。响应于接收到DAD消息，所选择的通信设备306a至306n删除ID由该设备306存储或正在处理的数据消息的任何副本。因此，所选择的通信设备306a至306n将不再存储或传输已经由计算机测试工具302接收的消息的副本。在该实施例中，服务器304可跟踪并存储具有与计算机测试工具302交换数据消息的历史的通信设备306的标识。

[0081] 在一个实施例中，当计算机测试工具302或服务器306加密数据时，它向数据消息添加一次性指示符。该一次性指示符向解密数据的模块(例如，CTT认证模块322或S认证模块328)表明该数据只能被解密或处理一次。

[0082] **例如，服务器306可向计算机测试工具302发送一次性消息以执行特殊功能、打开、关闭或为自身布防，直到接收到后续消息。一次性消息通过序列号加密，从而使得这些一次性消息不能被重复使用，例如，以打开或关闭计算机测试工具302。所述加密的序列号防止存储和重复使用单个合法的一次性消息。例如，当用户购买一周的特定特殊特征的使用权时，服务器306可向计算机测试工具302发送通过序列号加密的一次性“打开此特征消息”。当该周结束时，计算机测试工具302自动关闭该特征。序列号防止用户重复使用原始消息(例如，重放原始消息至计算机测试工具302)以再使用一周的特殊功能。

[0083] 在一个实施例中，CTT认证模块322和S认证模块328将“生存时间”(TTL)信息附加到由计算机测试工具302和服务器304交换的数据消息。TTL信息指示过期日期。当与数据消息相关联的过期日期已过时，正在存储或处理消息的任何通信设备306a至306n删除该消息。使用TTL信息来限制消息寿命可减少可经由不同路径通过通信链路310a至310n和/或312a至312n不止一次地发送相同消息的机会。

[0084] 在上述某些图示实施例中，应当理解，本文所述的各种非限制性实施例可针对具体应用单独、组合或者选择性地组合使用。另外，上述非限制性实施例的各项特征中的一些

可在没有对应使用其他所描述的特征的情况下使用。以上描述应当理解为仅对本发明的原理、教导和示例性实施例进行说明而不是进行限制。

[0085] 应当理解，上述配置仅为示例性实施例的原理应用的说明。本领域的技术人员可在不脱离图示实施例的范围下设计多种修改形式和可选配置，所附权利要求旨在涵盖这些修改形式和配置。

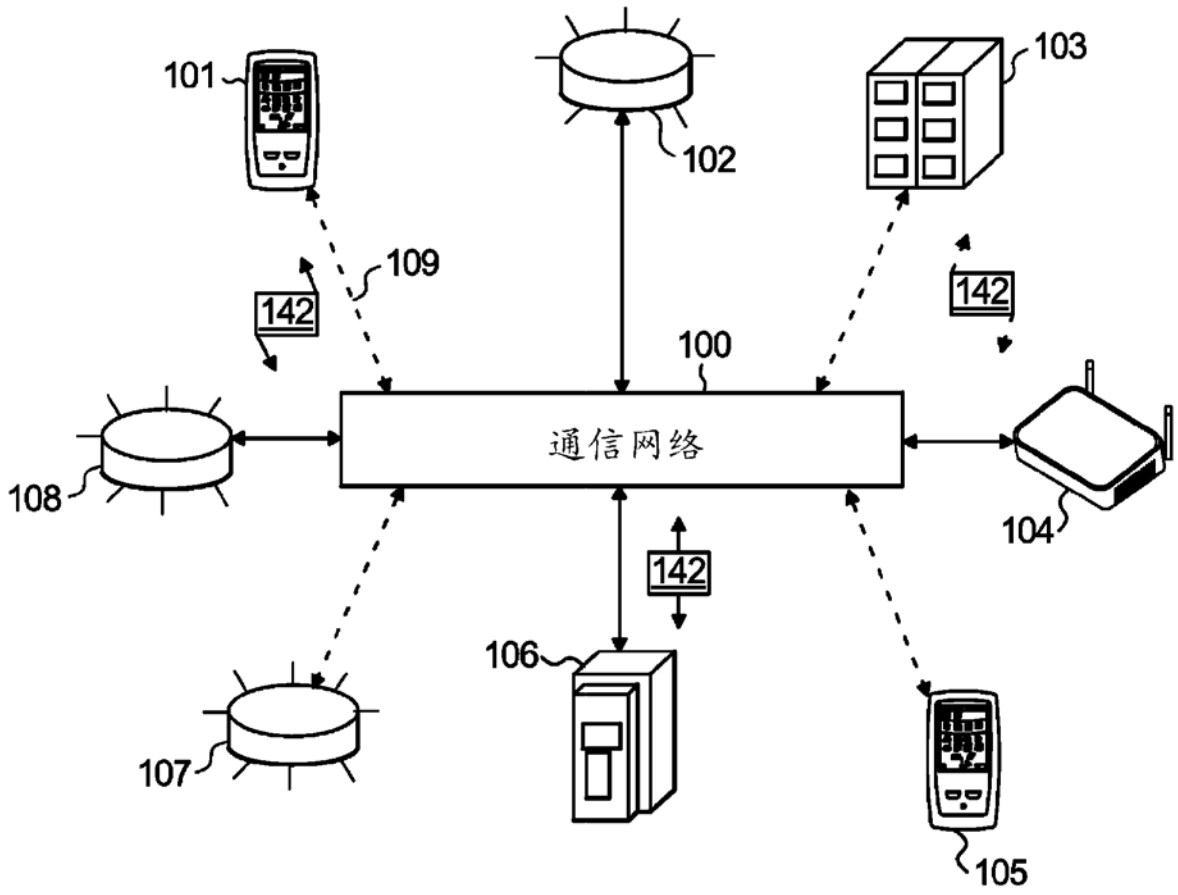


图 1

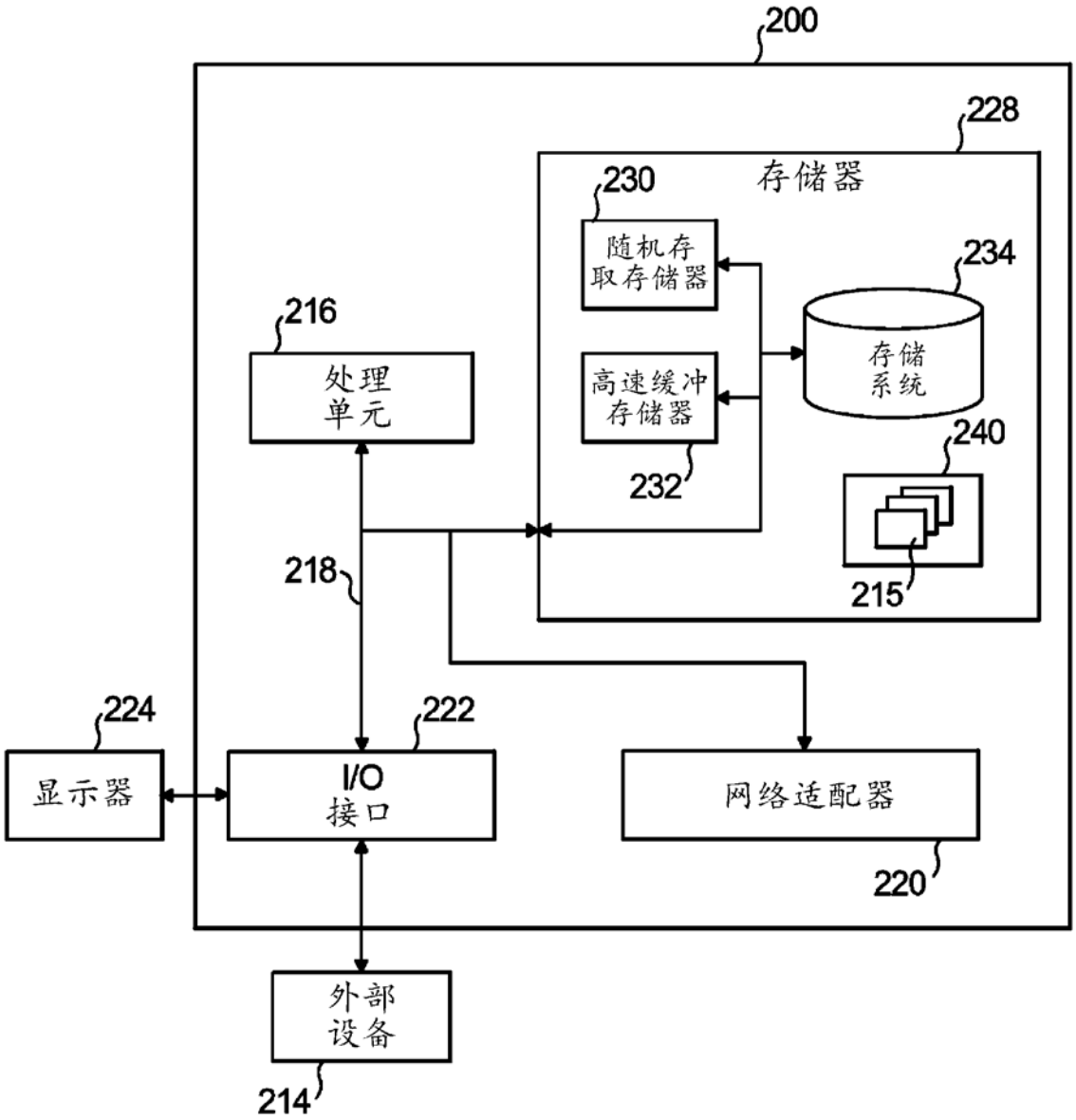

200
228
存储器
230
随机存取存储器
234
存储系统
216
处理单元
高速缓冲存储器
232
240
218
215
224
222
显示器
I/O接口
网络适配器
220
外部设备
214

图 2

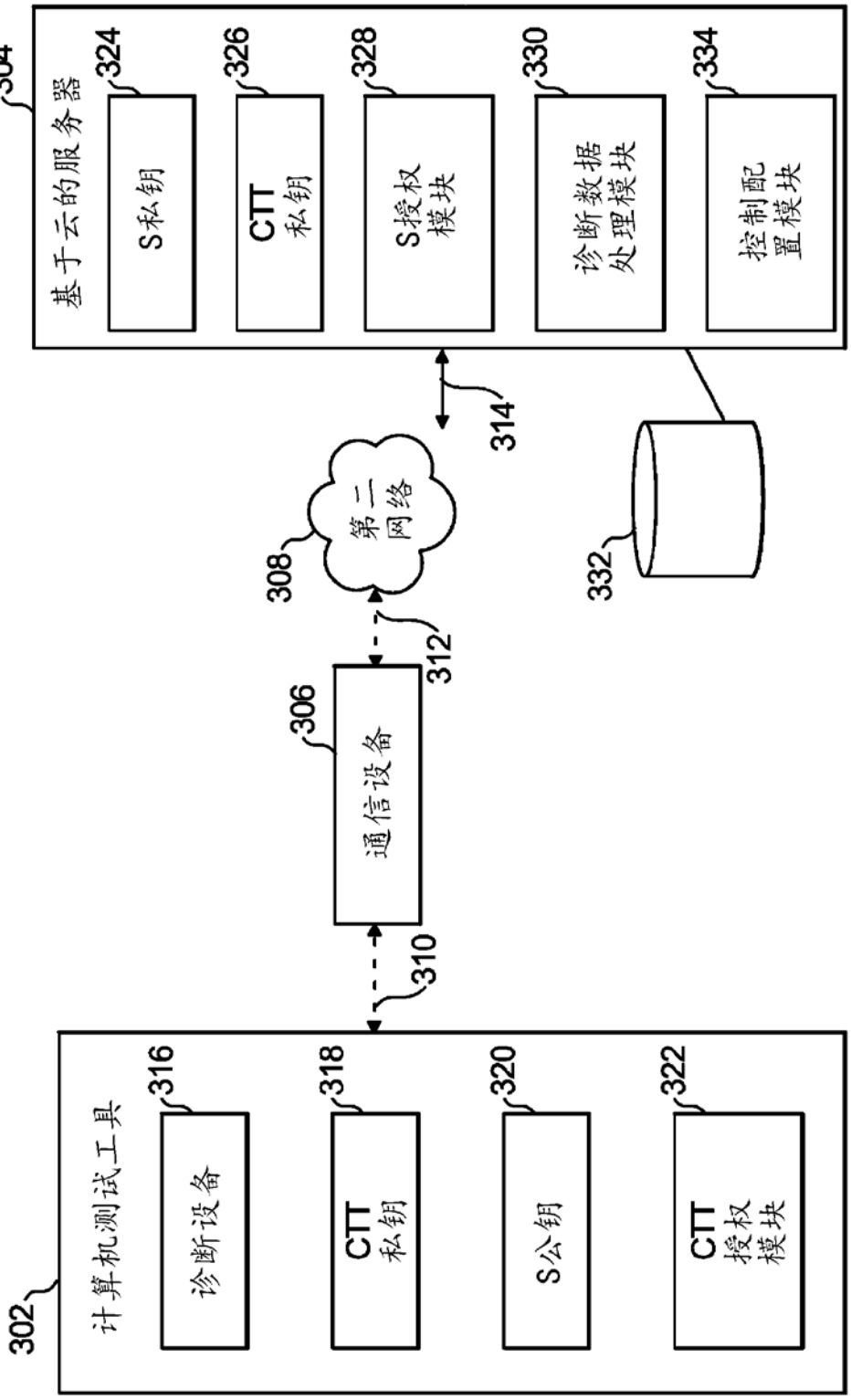

304
基于云的服务器
324
S私钥
326
CTT
私钥
328
S授权
模块
330
诊断数据
处理模块
334
控制配
置模块
314
308
第二
网络
332
312
306
通信设备
310
302
计算机测试工具
316
诊断设备
318
CTT
私钥
320
S公钥
322
CTT
授权
模块

图 3

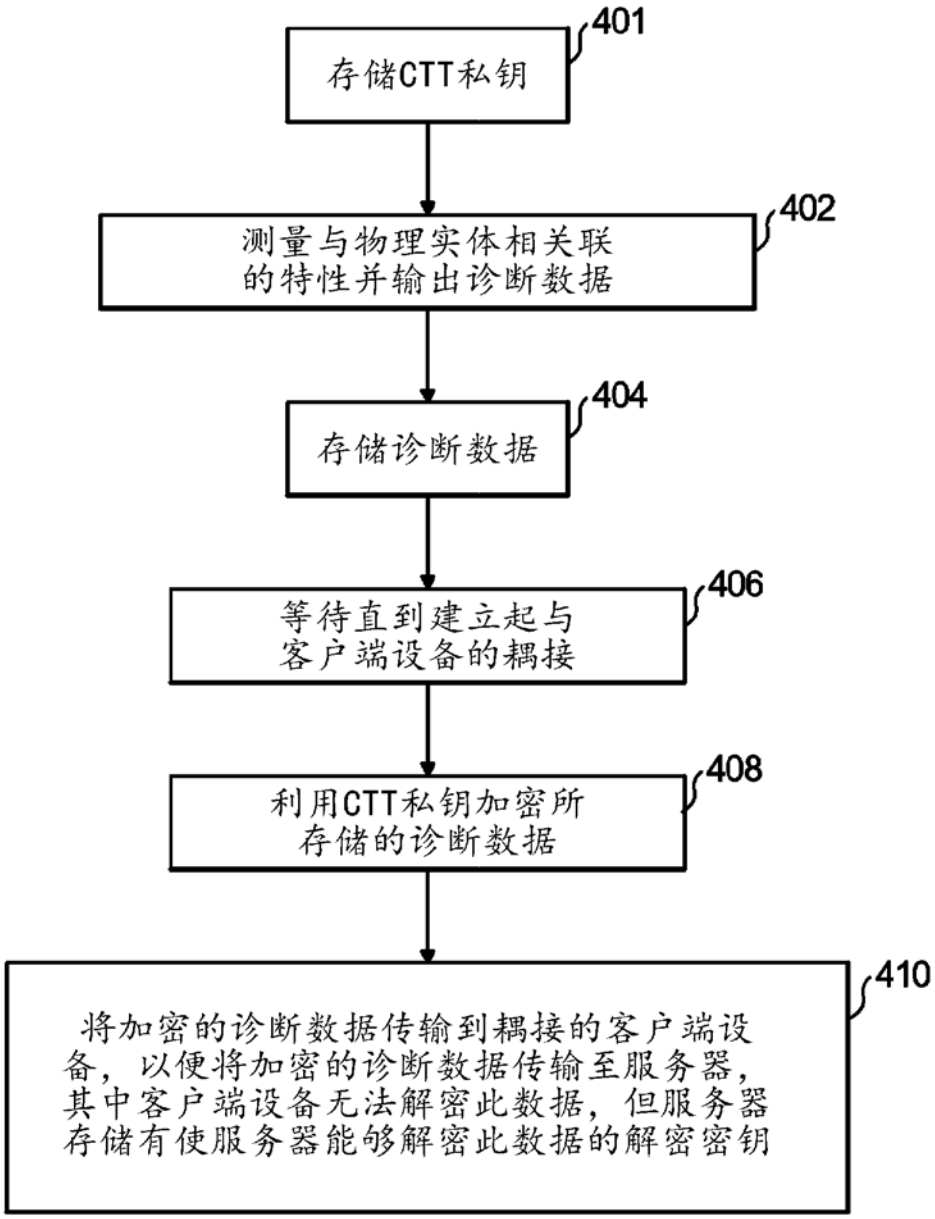

401
存储CTT私钥
402
测量与物理实体相关联的特性并输出诊断数据
404
存储诊断数据
406
等待直到建立起与客户端设备的耦接
408
利用CTT私钥加密所存储的诊断数据
410
将加密的诊断数据传输到耦接的客户端设备，以便将加密的诊断数据传输至服务器，其中客户端设备无法解密此数据，但服务器存储有使服务器能够解密此数据的解密密钥

图 4

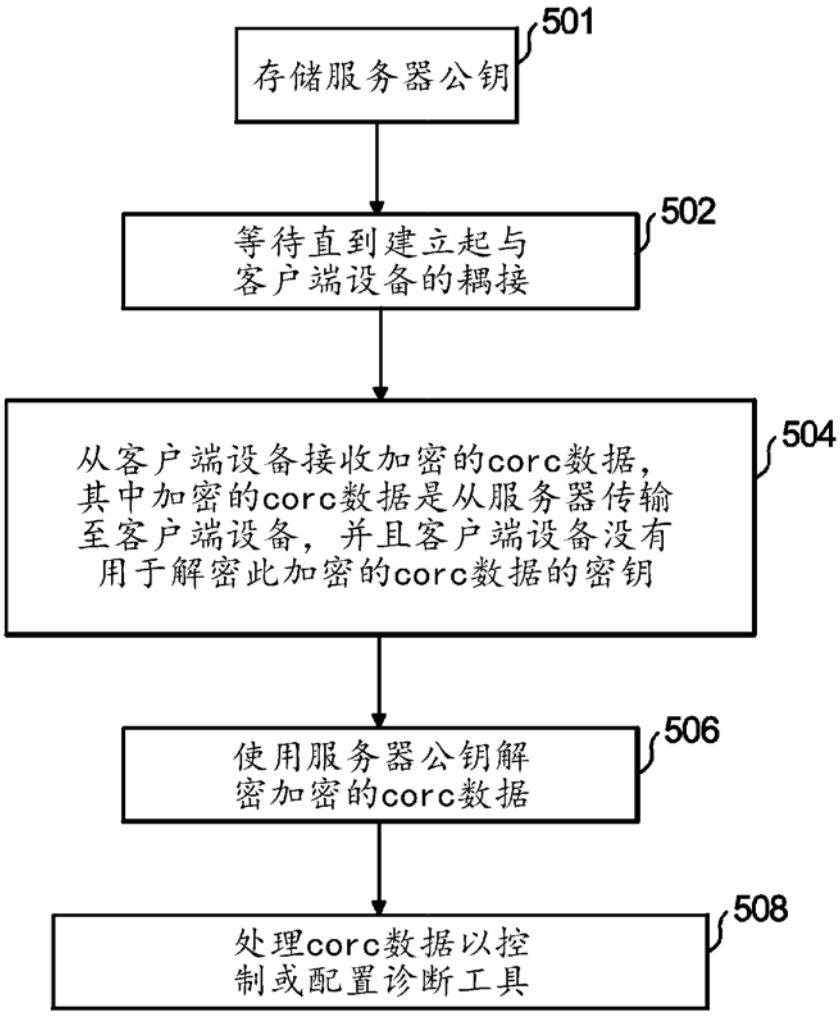

501
存储服务器公钥
502
等待直到建立起与客户端设备的耦接
504
从客户端设备接收加密的corc数据，其中加密的corc数据是从服务器传输至客户端设备，并且客户端设备没有用于解密此加密的corc数据的密钥
506
使用服务器公钥解密加密的corc数据
508
处理corc数据以控制或配置诊断工具

图 5

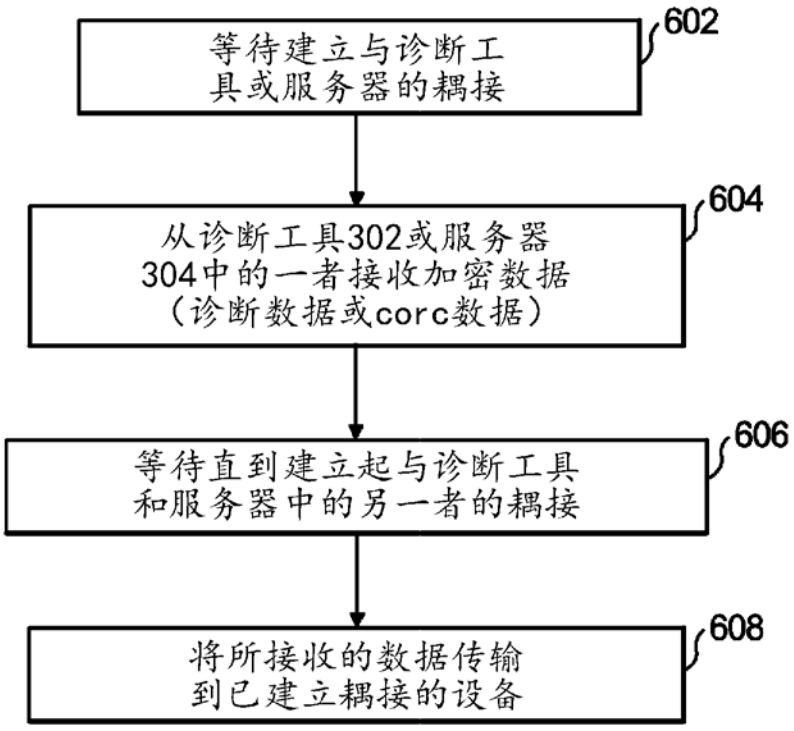

602
等待建立与诊断工具或服务器的耦接
604
从诊断工具302或服务器304中的一者接收加密数据（诊断数据或corc数据）
606
等待直到建立起与诊断工具和服务器中的另一者的耦接
608
将所接收的数据传输到已建立耦接的设备

图 6

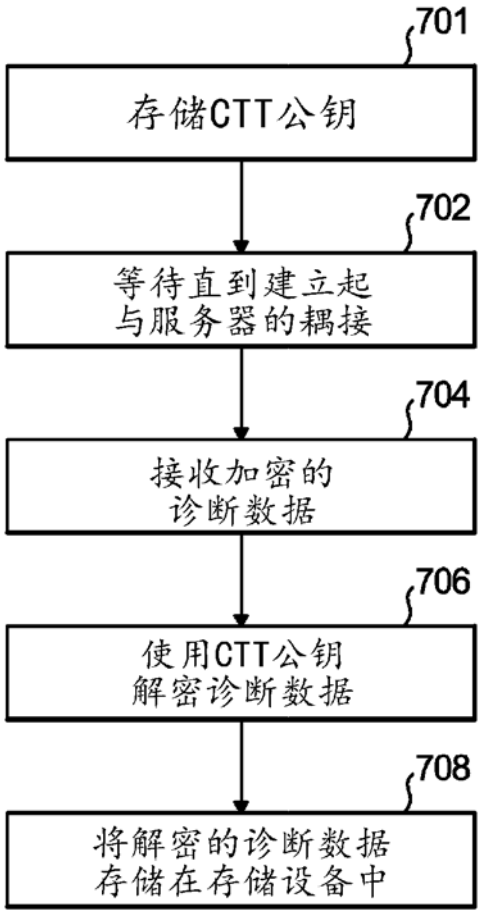

701
存储CTT公钥
702
等待直到建立起
与服务器的耦接
704
接收加密的
诊断数据
706
使用CTT公钥
解密诊断数据
708
将解密的诊断数据
存储在存储设备中

图 7

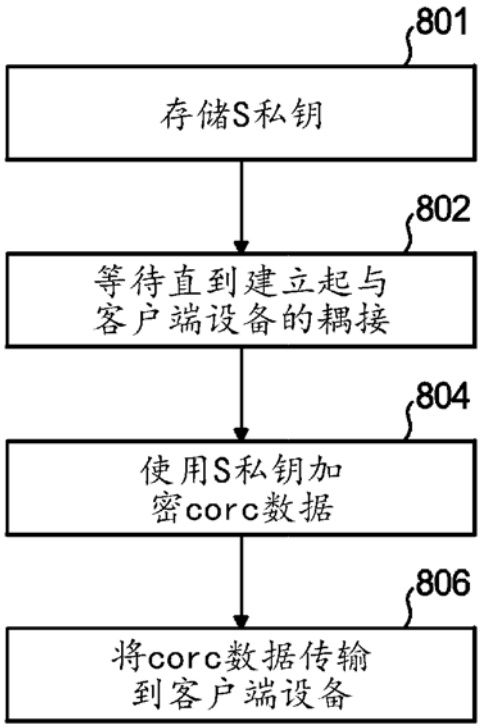

801
存储S私钥
802
等待直到建立起与
客户端设备的耦接
804
使用S私钥加
密corc数据
806
将corc数据传输
到客户端设备

图 8

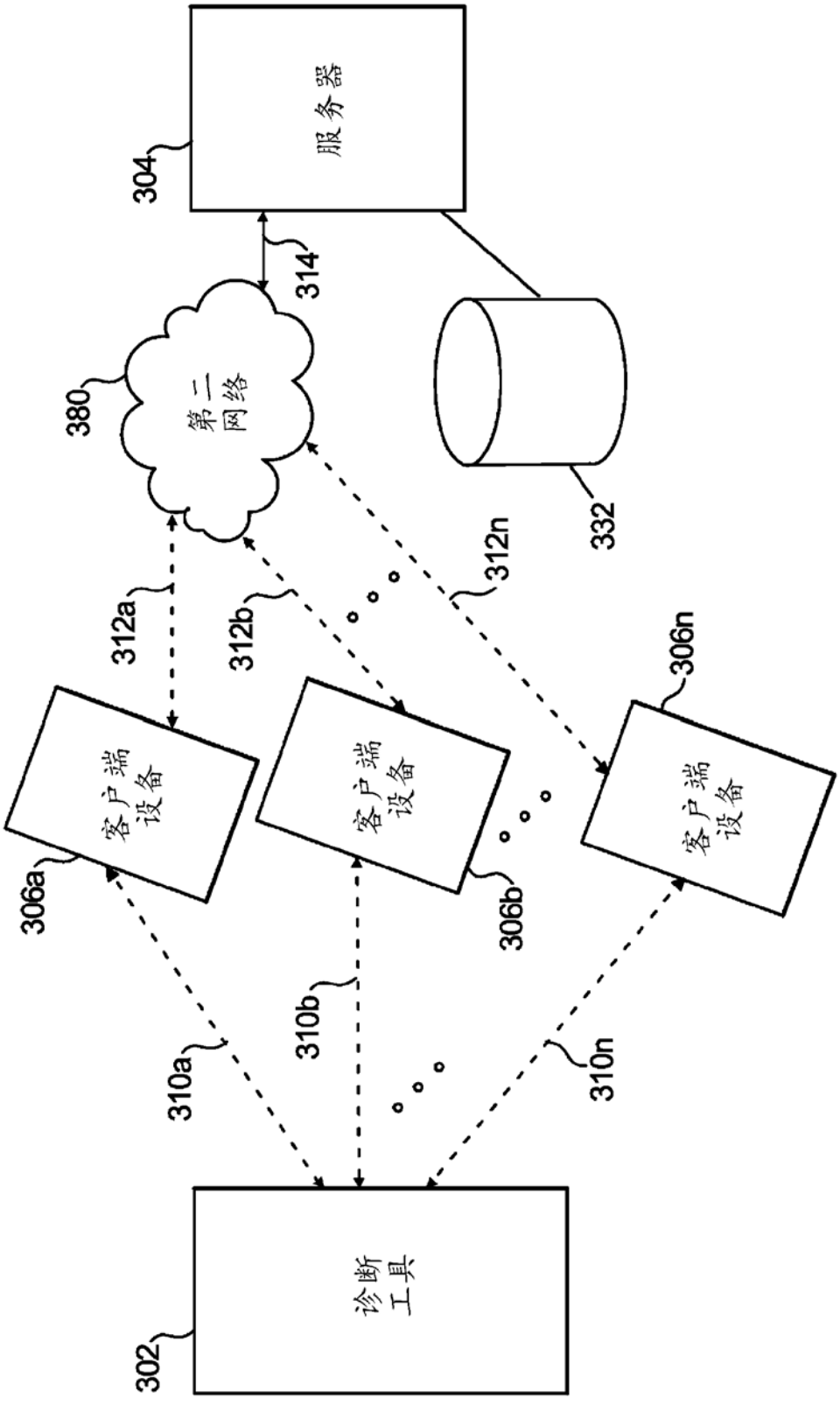

服务器
304
314
第二网络
380
332
312a
312b
312n
客户端设备
306a
客户端设备
306b
客户端设备
306n
310a
310b
310n
诊断工具
302

图 9