

(12) 发明专利申请

(10) 申请公布号 CN 102823195 A

(43) 申请公布日 2012. 12. 12

(21) 申请号 201180015119. 0

代理人 吕俊刚 孙海龙

(22) 申请日 2011. 03. 01

(51) Int. Cl.

(30) 优先权数据

H04L 12/24 (2006. 01)

61/316, 498 2010. 03. 23 US

G06F 11/36 (2006. 01)

12/879, 204 2010. 09. 10 US

G06F 9/445 (2006. 01)

(85) PCT申请进入国家阶段日

2012. 09. 21

(86) PCT申请的申请数据

PCT/US2011/026576 2011. 03. 01

(87) PCT申请的公布数据

W02011/119299 EN 2011. 09. 29

(71) 申请人 富士通株式会社

地址 日本神奈川县川崎市

(72) 发明人 小谷诚刚 铃木雅人

(74) 专利代理机构 北京三友知识产权代理有限公司 11127

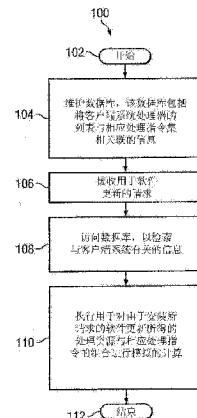
权利要求书 3 页 说明书 12 页 附图 7 页

(54) 发明名称

利用由虚拟机进行的软件测试远程维护电子网络中的客户端系统的系统和方法

(57) 摘要

一种用于在对被配置为服务多个客户端的电子网络执行远程维护的系统可以包括客户端(20)、数据库和虚拟机(22)。所述客户端包括多个处理资源。所述多个处理资源中的每一个可以具有存储在各自关联的计算机可读存储器上的相应处理指令集。所述数据库可以包括将处理资源的列表与相应处理指令集相关的信息(104)。所述虚拟机可以可操作为访问所述数据库(108)并在许可为客户端请求的软件更新之前执行模拟所提出的处理资源及其相应组处理指令的组合的计算(110)。



1. 一种用于在被配置为服务多个客户端的电子网络中执行远程维护的系统，所述系统包括：

客户端，所述客户端包括多个节点；

所述多个节点中的每一个节点具有存储在各自关联的计算机可读存储器上的相应处理指令集；

数据库，所述数据库与所述电子网络关联，所述数据库包括用于将节点的列表与相应处理指令集相关联的信息；以及

虚拟机，所述虚拟机能够操作以访问所述数据库并在许可为所述客户端请求的软件更新之前执行用于模拟所提出的节点及其相应处理指令集的组合的计算。

2. 根据权利要求 1 所述的系统，其中，所述虚拟机包括：

操作系统；以及

被编码在计算机可读存储器中的处理指令，所述处理指令在由处理资源执行时能够操作以执行包括以下操作的操作：

接收向所述客户端提供软件更新的请求；

向所述数据库查询与所述客户端关联的信息；

模拟所述客户端的所述多个节点与所请求的软件更新的组合；

将所述模拟的结果与一个或更多个兼容性规则进行比较；以及

如果所述结果符合所述一个或更多个兼容性规则，则许可所请求的软件更新。

3. 根据权利要求 1 所述的系统，其中，所述客户端是汽车。

4. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机被构造为通过受信任平台模块接收与所述客户端的当前状态相关的数据。

5. 根据权利要求 1 所述的系统，其中，所述客户端包括与汽车关联的 FlexRay 系统。

6. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以基于一个或更多个安全因子执行针对所请求的软件更新的风险分析。

7. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以至少基于高速性能指标执行针对所请求的软件更新的风险分析。

8. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以至少基于环境阻抗性能指标执行针对所请求的软件更新的风险分析。

9. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以创建与为所述客户端请求的所述软件更新相关的报告。

10. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以创建与为所述客户端请求的所述软件更新相关的报告，所述报告包括与所述客户端相关的操作信息的摘要。

11. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以创建与为所述客户端请求的所述软件更新相关的报告，所述报告包括由受信任平台模块计算出的散列值。

12. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以创建与为所述客户端请求的所述软件更新相关的报告，所述报告包括时间戳。

13. 根据权利要求 1 所述的系统，所述系统还包括所述虚拟机能够操作以创建与为所

述客户端请求的所述软件更新相关的报告,所述报告由与所述电子网络关联的计算机可读存储器存储。

14. 根据权利要求 1 所述的系统,所述系统还包括所述虚拟机能够操作以在所请求的软件更新不符合兼容性规则的情况下建议另选的软件更新。

15. 一种用于在由电子网络服务的客户端系统中执行远程维护的方法,所述方法包括以下步骤:

维护数据库,所述数据库包括用于将客户端系统节点的列表与相应处理指令集相关联的信息;

接收针对软件更新的请求,所述请求包括与特定客户端系统以及特定处理指令集对应的标识符;

访问所述数据库,以检索与和所述客户端系统关联的节点以及与所关联的处理器相关的相应处理指令集相关的信息;以及

执行用于模拟由于安装所请求的软件更新而导致的节点与相应处理指令的组合的计算。

16. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:将所模拟的计算的结果与一个或更多个兼容性规则进行比较。

17. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:如果所模拟的计算的结果符合所述一个或更多个兼容性规则,则许可所请求的软件更新。

18. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:通过受信任平台模块接收与所述客户端的当前状态相关的数据。

19. 根据权利要求 15 所述的方法,其中,所述客户端包括与汽车关联的 FlexRay 系统。

20. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:基于一个或更多个安全因子执行针对所请求的软件更新的风险分析。

21. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:至少基于高速性能指标执行针对所请求的软件更新的风险分析。

22. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:至少基于环境阻抗性能指标执行针对所请求的软件更新的风险分析。

23. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:创建与为所述客户端系统请求的所述软件更新相关的报告。

24. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:创建与为所述客户端系统请求的所述软件更新相关的报告,所述报告包括与所述客户端相关的操作信息的摘要。

25. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:创建与为所述客户端系统请求的所述软件更新相关的报告,所述报告包括由受信任平台模块计算的散列值。

26. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:创建与为所述客户端系统请求的所述软件更新相关的报告,所述报告包括时间戳。

27. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:创建与为所述客户端请求的所述软件更新相关的报告,所述报告由与所述电子网络关联的计算机可读存储器存储。

28. 根据权利要求 15 所述的方法,所述方法还包括以下步骤:在所请求的软件更新不

符合兼容性规则的情况下，建议另选的软件更新。

## 利用由虚拟机进行的软件测试远程维护电子网络中的客户 端系统的系统和方法

### 技术领域

[0001] 本发明总体上涉及信息交换，并且更具体地说，涉及用于以改进的安全性和保密性远程维护信息处理系统的方法和系统。

### 背景技术

[0002] 分布式通信网络包括从专用内部网络到不安全的互联网的宽范围的系统。在任何通信网络中，电子内容从网络中的一个点流向另一个点。关于这点，电子内容可以包括电子文档、可执行文件、数据文件等。在一些通信网络中，对该电子内容的访问可能被限制和/或限于特定的用户和/或客户端。存在多种方法来验证尝试获得对电子内容的访问的用户的标识，诸如用户名和密码组合、公用/专用密钥组合和/或生物特征(biometrics)。在一些网络中，中心服务器可以在向进行请求的用户和/或客户端分发电子内容之前采用这些方法。

[0003] 服务提供方与客户端之间的软件交换可以通过认证所交换的数据的内容和安全性来改进。用于认证的一些系统由于各种原因而难以实现。例如，其难以保护操作系统内的扫描和报告代理程序。作为另一示例，客户端系统的大小可能由于大小而需要过多时间来完成扫描和/或发送报告。作为另一示例，一些系统可能无法提供生物特征传感器与报告代理程序之间的安全连接。改进的认证方法和系统可以改进服务提供方与客户端之间的软件交换的安全性、速度和/或效率。

### 发明内容

[0004] 本公开提供了一种基本上消除或减少了与先前方法和系统关联的至少一些缺点和问题的用于分发电子内容的方法和系统。

[0005] 根据一种实施方式，一种用于对被配置为在服务多个客户端的电子网络中执行远程维护的系统可以包括客户端、数据库和虚拟机。所述客户端包括多个处理资源。所述多个处理资源中的每一个可以具有存储在各自的关联的计算机可读存储器上的相应处理指令集。所述数据库可以包括用于将处理资源的列表与相应处理指令集相关联的信息。所述虚拟机可以操作为访问所述数据库并在许可为客户端请求的软件更新之前执行模拟所提出的处理资源及其相应处理指令集的组合的计算。

[0006] 根据另一实施方式，一种用于在由电子网络服务的客户端系统中执行远程维护的方法可以包括以下步骤：维护数据库；接收针对软件更新的请求；访问所述数据库；以及执行计算。所述数据库可以包括用于将客户端系统节点的列表与相应处理指令集相关的信息。所述请求可以包括与特定客户端系统以及特定处理指令集对应的标识符。访问所述数据库可以包括以下步骤：检索与和所述客户端系统关联的节点以及与所述关联处理器相关的相应处理指令集相关的信息。所述计算可以模拟由于安装所请求的软件更新而导致的节点与相应处理指令的组合。

[0007] 本文公开的方法和系统可以包括使用以下讨论的虚拟机(VM)的技术。本公开的特定实施方式的技术优势包括远程维护中的增加的安全性和 / 或可靠性,该远程维护包括以无线方式从服务多个客户端系统的外部数据中心传送电子内容。根据以下附图、描述以及权利要求书,本领域技术人员将容易明白其它技术优点。而且,虽然上面已经列举了具体优点,但是各种实施方式可以包括全部或一些所列举的优点或者不包括所列举的优点。

## 附图说明

[0008] 为了更完整地理解本发明及其优点,现在结合附图对以下描述进行说明,附图中:

[0009] 图 1 示出了根据本公开的教导的、包括客户端系统和外部数据中心的示例通信网络;

[0010] 图 2 示出了根据本公开的教导的、包括示例客户端系统和外部数据中心的示例通信网络;

[0011] 图 3 示出了根据本公开的教导的、包括客户端系统的细节的示例通信网络;以及

[0012] 图 4-11 示出了说明用于以改进的安全性和保密性对信息处理系统进行远程维护的各种方法的流程图。

## 具体实施方式

[0013] 优选实施方式和它们的优点通过参照图 1 到图 11 来最佳地理解,附图中,相同的数字用于指示相同和对应的部分。图 1 示出了根据本公开的教导的、示例电子网络 1 的简化表示。电子网络 1 可以包括数据中心 10 和客户端系统 20。电子网络 1 的一些实施方式可以包括多个客户端和它们的相应客户端系统。在图 1-3 中,为清楚起见,示出并讨论了单个客户端及其客户端系统 20。

[0014] 数据中心 10 可以被配置为向各个客户端和 / 或客户端系统 20 提供维护。这种维护可以包括管理软件和 / 或固件的更新和 / 或状态。在具有许多客户端系统 20 的复杂电子网络中,如果必须认证和 / 或验证报告,则对向各个客户端系统 20 的电子内容传递进行管理可能更加困难。

[0015] 出于公开的目的,“电子内容”、“内容”、“软件”和 / 或“软件更新”可以包括任何文件、文件、目标代码、可执行代码、数据记录或者电子网络的客户端可能希望访问的任何其它电子记录的数据结构。例示性示例可以包括文本文件、电子表格、电子邮件、医疗记录、图像和其它电子数据以及网页、专用网络、字处理程序、文件管理系统和其它程序。另外,“客户端”可以指充当终端用户的人,或者指由这种人用来接入通信网络的装置或多个装置,诸如个人计算机、信息站(kiosk)或移动计算装置。

[0016] 受信任计算(Trusted Computing)和 TrustCube 可以向服务提供方(例如,数据中心 10)提供与客户端系统 20 有关的可认证报告。可认证报告可能难以保护与客户端系统 20 关联的扫描和 / 或报告代理程序。另外,完成扫描和发送大的关联报告所需的时间可能太大。作为另一示例,可能难以实现针对客户端系统 20 的生物特征传感器及其报告代理程序。

[0017] 在本发明的一些实施方式中,虚拟机(VM)技术和受信任计算技术的组合可以提供

超过其它方法的优点。例如,利用具有针对生成报告的有限目的的最小操作系统(OS)的第一 VM 可以向客户端系统 20 的其余部分提供针对外部访问的保护。作为另一示例,因为第一 VM 使用较少数量的文件,并且这些文件较小,所以可以减小发送给数据中心 10 的报告的大小。这些优点可以通过利用虚拟硬盘映像和虚拟存储器映像代替硬盘分区中的单个文件来增加。作为另一示例,有限目的 OS 可以重复使用相同的文件和 / 或存储器映像,并且可以丢弃和 / 或删除针对那些文件和映像的改变。

[0018] 在一些实施方式中,VM 技术可以与文件存储技术(例如, mbox)组合。例如,可以将文件以纯文本格式存储在单个文件中。这些技术可以允许文本处理工具容易地用于这些内容。

[0019] 虚拟机管理器(VMM)可以创建、运行、监测和 / 或终止各种 VM。VMM 可以起作用以截取 VM 之间的中断和 / 或故障,和 / 或控制应用对硬件装置和 / 或已安装软件的访问。VMM 还可以通过在应用和 / 或 VM 在其中运行的各个线程之间共享时间来管理针对处理器的多任务。VMM 的使用可以扩展上述 VM 的功能。

[0020] 作为另一示例,生物特征传感器可以通过 VMM 利用独立的 VM 并入并连接至第一 VM。数据中心 10 可以结合生物特征数据使用可认证报告技术,以评估客户端系统 20 的状态和 / 或生物特征数据的可信赖性。

[0021] 数据中心 10 可以包括处理器 12、存储资源 14 以及通信总线 16。处理器 12 可以包括可操作为解释和 / 或执行程序指令和 / 或处理数据的任何系统、装置或设备,并且可以不受限制地包括被配置为解释和 / 或执行程序指令和 / 或处理数据的微处理器、微控制器、数字信号处理器(DSP)、专用集成电路(ASIC)或者任何其它数字或模拟电路。在一些实施方式中,处理器 104 可以解释和 / 或执行存储在存储资源 14 和 / 或数据中心 10 的另一组件中的程序指令和 / 或处理数据。

[0022] 数据中心 10 可以代表管理安全策略和认证属性的受信任的专用服务器。数据中心 10 可以包含数据库,该数据库包含限定一组属性值的多个策略(在客户端系统 20 被准许访问电子内容和 / 或软件之前,这些策略必须被满足)。数据中心 10 可以接收来自客户端系统 20 的属性报告,属性报告标识与客户端系统 20 关联的一个或更多个属性。在认证这些属性之后,数据中心 10 可以确定是否向客户端系统 20 提供所请求的服务。应用这种属性报告和认证也可以被称为“基于策略的管理”。该语境的数据可以包括表示客户端系统 20 的数据,诸如客户端系统 20 的物理位置(例如,IP 地址)、安装在进行请求的机器上的特定软件(例如,严格防病毒软件)、生物特征标识符或任何其它合适的背景属性。

[0023] 存储资源 14 可以可通信地耦接至处理器 12,并且可以包括可操作为在一时段内保持程序指令或数据的任何系统、装置或设备(例如,计算机可读介质)。存储资源 14 可以包括随机存取存储器(RAM)、电可擦除可编程只读存储器(EEPROM)、PCMCIA 卡、闪速存储器、磁存储器、光磁存储器或在存储资源 12 的电力断开之后保持数据的非易失性存储器或易失性存储器的任何合适选择结果和 / 或集合。

[0024] 存储资源 14 可以包括硬件和软件的任何组合(包括控制逻辑)。例如,存储资源 14 可以包括文档(诸如医疗记录)的集中式储存库。作为另一示例,存储资源 14 可以表示通过网络提供针对特定应用、软件或其它介质的访问的应用服务提供方。这些应用、软件或介质可以包括文档阅读器、网络浏览器或文档编辑软件等。作为另一示例,存储资源 14 可以与

在线联网网站或电子邮件提供方关联。

[0025] 为描述清楚起见,图1将处理器12和存储资源14描述为独立组件。在一些实施方式中,处理器12和存储单元14可以包括存储在计算机可读介质上并可由一个或更多个计算机和/或服务器关联的一个或更多个处理器执行的独立软件程序。然而,处理器12和存储单元14还可以包括大型软件程序的硬编码到计算机可读介质中的组件或子例程和/或被配置为执行期望功能的任何硬件或软件模块。

[0026] 通信总线16可以是可操作为用作数据中心10与网络18之间的接口的任何合适的系统、设备或装置。通信总线16可以使得数据中心10能够利用任何合适的传输协议和/或标准来通过网络18进行通信,该传输协议和/或标准包括但不限于以下针对网络18的讨论列举的所有传输协议和/或标准。在一些实施方式中,网络18可以是封闭网络(例如,网络18仅可由授权客户端接入)。

[0027] 如所示,网络18可以包括能够发送音频和/或视频电信信号、数据和/或消息的任何网络。一些示例可以包括无线电接入网络、公共交换电话网(PSTN)、公用或专用数据网络、局域网(LAN)、城域网(MAN)、广域网(WAN)、诸如互联网的局部性、地区性或全球性通信或计算机网络、有线或无线网络、企业内部网或者以上的任何组合中的全部或一部分。

[0028] 在操作中,网络18可以利用任何合适的通信协议来提供耦接至网络18的组件之间的连接性。为实现所述通信能力,网络18可以包括路由器、集线器、交换机、网关、呼叫控制器和/或任何合适的形式或布置的任何其它合适的组件。另外,网络18可以包括被配置为按照数据的分组、单元、帧、区段或其它部分的形式对信息进行通信的任何硬件和/或软件。尽管网络18被例示为单个网络,但是通信网络18可以包括任何数量或配置的网络。而且,通信网络1的特定实施方式可以包括任何数量或配置的网络18。

[0029] 在一些实施方式中,网络18可以包括虚拟专用网络(VPN)。与开放的和/或公用的网络相比,VPN提供增加的安全性。一般来说,VPN分离和/或封装数据传递,使得数据可以相对于共享中间网络(例如,LAN或WAN)的其它装置保持私密和/或安全性。在操作中,VPN可以允许多个客户端20与数据中心10相互作用,就像直接和/或专门连接一样。

[0030] 客户端20可以包括至少部分地由数据中心10维护的电子网络1的任何系统和/或组件。客户端20可以包括多个处理器、相关软件和/或固件、传感器等。例如,客户端20可以包括汽车及其内部网络。作为另一示例,客户端20可以包括具有处理器和软件标识模块(SIM)卡的便携式电话。在本公开的上下文中,客户端20可能是针对具体实施方式来描述的,但是本教导并不因而受限。在一些实施方式中,与客户端20关联的各个处理器和存储资源可能由多个厂商和/或服务提供方来提供。在那些实施方式中,对各个处理器及其关联软件和/或固件的维护可能因需要针对所有多个厂商和/或服务提供方协调数据而变复杂。本公开的教导可以实现使各个资源彼此分离的虚拟划分,而不是允许无拘束地访问整个客户端系统20。

[0031] 客户端20可以包括具有用于与数据中心10进行无线通信的功能的计算机和/或计算装置。例如,客户端20可以包括台式计算机、膝上型计算机、个人数字助理(PDA)、智能电话,蜂窝或移动电话、车内或车外导航系统和/或移动游戏装置。客户端20可以操作一个或更多个客户端应用(例如,网络浏览器、文本编辑器等)。

[0032] 图1示出了示例客户端系统20,该示例客户端系统20包括处理模块21、多个VM

22、VMM 24、受信任平台模块(TPM) 26、资源列表 28、客户端网络系统 30、节点 32 以及 GPS 接口 40。一些实施方式可以通过创建多个 VM 22 并且利用 VMM 24 控制这些 VM 22 之间的信息流来为 VM 22 提供经增加的安全性。

[0033] 客户端系统 20 可以比图 1 所示的简化客户端网络系统 30 明显地更加复杂。例如，汽车可以包括客户端网络系统 30(例如，FlexRay)，该客户端网络系统 30 包括多个处理器，在一些示例中，包括几百个处理器。在图 1 中，节点 32 表示与客户端网络系统 30 关联的单个处理器和 / 或其它资源。

[0034] VM 22 可以包括与客户端网络系统 30 对应的和 / 或与和客户端网络系统 30 关联的单个处理对应的虚拟机。多个 VM 22 可以运行多个操作系统(OS)。在这种布置中，各个 VM 22 可以使用单个目的 OS，并且通过 VMM 24 对客户端系统 20 和 / 或处理模块 21 的任何所需的处理资源进行时间共享。

[0035] 受信任平台模块 26 可以包括被配置为生成密钥的资源(例如，硬件伪随机数生成器)。在一些实施方式中，TPM 26 可以包括远程证明和 / 或密封存储器(sealed storage)。在一些实施方式中，TPM 26 包括至少一个专用处理器，该专用处理器具有被分配给处理器芯片并在制造期间烧制到处理器芯片中的唯一且秘密的 RSA 密钥。在 TPM 26 中使用唯一 RSA 密钥可以允许数据中心 10 验证客户端系统 20 实际上为客户端。

[0036] 例如，TPM 26 可以采用包括客户端系统 20 的硬件和软件配置的摘要的散列密钥。散列密钥可以使得客户端系统 20 能够测试任何进入的软件包和 / 或更新，以验证它们没有被改变。一个示例验证方法包括基于在处理器制造期间对于该处理器唯一的 TPM 背书(endorsement)密钥和 / 或与该背书密钥有关的另一受信任密钥的绑定、加密。另一示例验证方法包括密封，其可以对 TPM 26 的条件施加附加状态需求。

[0037] 资源列表 28 可以包括实体的列表和 / 或登记。在一些实施方式中，资源列表 28 可以包括经准许访问和 / 或识别的实体的白名单。白名单可以包括 TPM 26 可以准许访问客户端系统 20 的任何数据中心 10 实体。在一些实施方式中，资源列表 28 可以包括被拒绝访问的实体的黑名单。

[0038] 客户端网络 30 可以包括特定客户端内的网络系统，其包括多个处理器和 / 或存储资源。例如，客户端网络 30 可以包括与汽车关联的 FlexRay 网络系统。FlexRay 是针对管理汽车系统中的多个处理器开发的网络通信协议的具体实施方式。作为另一示例，控制器区域网络(CAN 或 CAN 总线)是被设计成使得微控制器与装置能够在不需要主计算机的情况下彼此通信的通信协议标准的具体实施方式。附加示例包括时间触发协议(TTP)和航空电子设备全双工交换以太网(AFDX)。

[0039] 客户端系统 20 中的节点 32 可以包括客户端系统 20 的任何特定资源。例如，节点 32 可以包括处理器和 / 或它们的关联软件、固件和 / 或有关于处理器的处理指令。例如，汽车可以具有包括多个 CPU 的非常复杂的网络系统。各个 CPU 可以具有用于其由厂商提供的操作的软件和 / 或固件。客户端系统 30 可以负责各个节点 32 的操作和 / 或维护，这包括管理与客户端系统 20 中的各个节点 32 关联的软件和 / 或固件的版本和 / 或更新状态。

[0040] 全球定位系统接口 40 可以包括与全球定位系统(GPS)的任何接口。GPS 包括提供可靠的位置和时间信息的基于空间的全球导航卫星系统。GPS 可被具有 GPS 接收机的任何人和 / 或任何系统访问。使用特定且准确的位置和 / 或定时信息可以使得客户端处理模块

21能够管理信息请求、下载和 / 或其它内容。

[0041] 图 2 示出了根据本公开的教导的、包括示例客户端系统 20 和外部数据中心 10a 和 10b 的示例通信网络 2。数据中心 10 可以包括可由客户端系统 20 访问的任何外部数据库。仅出于例示的目的,与图 2 有关地描述了一个示例客户端系统 20,其中客户端系统 20 包括移动导航系统。本公开的教导可以用于任何合适的客户端系统 20。

[0042] 通信网络 2 可以包括互联网 42、外部数据中心 10 以及客户端移动导航系统 20。客户端系统 20 可以通过专用基础设施 44 (例如,用户家中的基于家庭的互联网连接) 与互联网 42 进行通信。数据中心 10a 和 10b 可以通过网络 18 与客户端系统 20 进行通信。网络 18 可以提供如本公开所述的安全通信。

[0043] 数据中心 10a 可以包括在客户端系统 20 中有用的电子内容的数据库。例如,如果客户端系统 20 包括移动导航系统,则数据中心 10a 可以包括与移动导航系统有关的地图、针对用户的更新接口以及其它内容。数据中心 10a 还可以经由 ISP 与互联网 42 进行通信。

[0044] 数据中心 10b 可以包括针对与移动导航系统 20 的操作有关的固件、维护以及软件的数据库。例如,数据中心 10b 可以提供针对移动导航系统 20 中的各个处理器的固件的最新版本的列表。

[0045] 客户端系统 20 可以操作模块 21 中的多个 VM 22,以与各个独立数据源连接。例如,VM 22a 可以包括用于与互联网 42 交互的通用浏览器和 / 或网络 OS。作为另一示例,VM 22b 和 22c 可以包括用于分别与数据中心 10a 和 10b 交互的专门应用和虚拟 OS。作为另一示例,VM 22d 可以包括用于与用户的汽车 32 中的各个系统交互的专门应用和虚拟 OS。

[0046] 各个 VM 22 可以通过 VMM 24 仅与另一 VM 22 进行通信。VMM 24 可以与 TPM 合作地管理这些通信,以增加各个 VM 22 的安全性。例如,从互联网 42 接收到的内容可能不被安装至节点 32,除非通过在此描述的各种方法中的任一种方法被 VMM 24 许可。

[0047] 图 3 示出了根据本公开的教导的、包括客户端系统 20 的细节的示例通信网络 2 的细节。图 3 示出了 VMM 24 负责各个 VM 22 的环境管理。各个 VM 22 可以包括由 OS 46 操作的关联应用 44。VMM 24 可以在适当时候向各个 VM 22 提供存储资源 48。VMM 24 可以与各个 VM 22 关联地操作一个或更多个程序 50。VMM 24 还可以与 TPM 26 和 / 或资源列表 28 协作,以提供加密、确认密钥、白名单和 / 或黑名单。

[0048] 图 4 例示了根据本公开的特定实施方式的、用于执行被配置为服务于多个客户端系统 20 的电子网络中的远程维护的示例方法 60 的流程图。方法 60 可以包括多个步骤,并且可以由电子网络 1 的各个组件(包括数据中心 10 和 / 或其它资源)来执行。方法 60 可以在 62 开始。在一些实施方式中,客户端系统 20 可以包括汽车和 / 或与汽车关联的 FlexRay 系统。

[0049] 步骤 64 可以包括操作具有与客户端系统中的各个处理器和资源关联的软件的数据库的数据中心 10。例如,步骤 64 可以包括维护与客户端系统 20 关联的处理器的列表以及针对使用客户端系统 20 的处理器而提供的任何当前软件和 / 或固件。

[0050] 步骤 66 可以包括与由客户端系统 20 的处理模块 21 托管的第一虚拟机 22b 进行通信。第一虚拟机 22b 可以处理与数据中心 10 关联的第一数据集。如以上讨论的,第一虚拟机 22b 可以由 VMM 24 来管理。第一虚拟机 22b 可以被配置为监测处理器的列表和它们的由数据中心 10 维护的关联软件和 / 或固件。

[0051] 步骤 68 可以包括接收来自第一虚拟机 22b 的、标识用于传送至客户端系统 20 的软件更新的请求。例如，数据中心 10 可以通过网络 18 接收来自第一虚拟机 22b 的这种请求。

[0052] 步骤 70 可以包括执行验证客户端系统 20 的标识的证明处理。证明处理可以包括上面讨论的验证处理中的任一个。在一些实施方式中，证明处理可以包括接收、测试和 / 或验证一个或更多个生物特征指示符。在一些实施方式中，数据中心 10 可以执行证明处理以验证客户端系统 20 的标识。

[0053] 步骤 72 可以包括利用网络 18 向第一虚拟机 22b 发送所标识的软件更新。网络 18 可以是如上讨论的封闭网络。在一些实施方式中，数据中心 10 可以执行步骤 72。在一些实施方式中，所标识的软件更新可以无线地发送。

[0054] 步骤 74 可以包括授权第一虚拟机 22b 利用与客户端系统关联的第二虚拟机 22c 将所标识的软件更新安装在客户端系统 20 上。在一些实施方式中，数据中心 10 可以执行步骤 74。在其它实施方式中，VMM 26 可以执行步骤 74。方法 60 可以在 76 结束。

[0055] 方法 60 可以对客户端系统 20 有用，其中，第一虚拟机 22b 和第二虚拟机 22c 通过 VMM 24 通信。使用 VMM 24 可以保护客户端系统 20 不被数据中心 10 直接访问，和 / 或另外增加客户端系统 20 的组件的安全性。在方法 60 的一些实施方式中，第一虚拟机 22b 可以询问第二虚拟机 22c，以验证客户端系统 20 已经成功安装软件更新。

[0056] 在具有大量节点 32 的客户端系统 20 中，传统维护方法需要在安全维护位置维修客户端系统 20。通过无线电传输和 / 或另一空中系统的远程维护在那些传统方法下可能降低安全性。

[0057] 相反，采用方法 60 的电子网络 1 可以允许在不降低安全性的情况下使用远程维护。电子网络 1 的特定实施方式可以通过利用 VMM 24 管理 VM 22 来增加任何特定 VM 22 的安全性，其中，各个 VM 22 之间的数据交换可以由 VMM 24 来操作和 / 或控制。

[0058] 图 5 例示了根据本公开的特定实施方式的、用于客户端系统 20 请求并接收来自远程服务器的软件更新的示例方法 80 的流程图。方法 80 可以包括多个步骤，并且可以由电子网络 1 的各个组件(包括客户端系统 20 的处理器模块 21 和 / 或其它资源)来执行。在一些实施方式中，客户端系统 20 可以包括汽车和 / 或与汽车关联的 FlexRay 系统。方法 80 可以在 82 开始。

[0059] 步骤 84 可以包括托管与客户端系统 20 关联的两个 VM 22。第一 VM 22b 可以处理与客户端系统 20 关联的第一数据集。第二 VM 22c 可以处理与外部数据中心 10 关联的第二数据集。

[0060] 步骤 86 可以包括操作被配置为管理两个虚拟机 22 之间的通信的 VMM 24。使用 VMM 24 可以保护客户端系统 20 不被数据中心 10 直接访问和 / 或另外增加客户端系统 20 的组件的安全性。

[0061] 步骤 88 可以包括识别第一数据集与第二数据集相比已经过期。步骤 88 可以由 VM 22 执行。例如，第二 VM 22b 可以询问第一 VM 22c 以检查任何处理器和 / 或它们的相应软件和 / 或固件的状态、版本和 / 或配置。例如，第二 VM 22b 可以与数据中心 10 中的更新数据比较特定处理器和 / 或其相应软件和 / 或固件的状态、版本和 / 或配置。

[0062] 步骤 90 可以包括标识用于传送至客户端系统 20 的软件更新。步骤 90 可以由

VM22、数据中心 10 和 / 或电子网络 1 的其它组件来执行。在一些实施方式中，VM 22 可以经由安全机构(例如，经由 TPM/TNC)向数据中心 10 发送与客户端系统 20 有关的数据。

[0063] 步骤 92 可以包括执行验证数据中心 10 的标识的证明处理。证明处理可以包括上面讨论的验证处理中的任一个。在一些实施方式中，证明处理可以包括接收、测试和 / 或验证一个或更多个生物特征指示符。在一些实施方式中，客户端系统 20 可以利用第二 VM 22b、TPM 24 和 / 或资源列表 28 来执行证明处理以验证数据中心 10 的标识。

[0064] 步骤 94 可以包括请求来自外部数据中心 10 的所标识的软件更新。在一些实施方式中，第二 VM 22b 可以执行步骤 94。所标识的软件更新可以包括与客户端系统 20 的一个或更多个节点 32 (例如，CPU) 有关的各个软件和 / 或固件。

[0065] 步骤 96 可以包括接收从外部数据中心 10 到客户端系统 20 的所标识的软件更新。在一些实施方式中，第二 VM 22b 将执行步骤 96。所标识的软件更新可以通过网络 18 发送。在一些实施方式中，VMM 24 可以在执行步骤 98 之前检查所接收的软件更新的完整性。

[0066] 步骤 98 可以包括通过第一虚拟机 22b 将所发送的软件更新安装在客户端系统 20 上。在方法 80 的一些实施方式中，第二虚拟机 22b 可以询问第一虚拟机 22c，以验证客户端系统 20 已经成功安装软件更新。在一些实施方式中，客户端系统 20 可以创建和 / 或维护针对接收和 / 或安装软件更新的日志。在一些实施方式中，数据中心 10 可以创建和 / 或维护针对发送和 / 或安装软件更新的日志。该日志可以包括时间戳。

[0067] 方法 80 可以在 99 结束。

[0068] 在具有大量节点 32 的客户端系统 20 中，传统维护方法需要在安全维护位置维修客户端系统 20。通过无线电传输和 / 或另一空中系统进行的远程维护在那些传统方法下可能降低安全性。

[0069] 相反，采用方法 80 的电子网络 1 可以允许在不降低安全性的情况下使用远程维护。电子网络 1 的特定实施方式可以通过利用 VMM 24 管理 VM 22 来增加任何特定 VM 22 的安全性，其中，各个 VM 22 之间的数据交换可以由 VMM 24 来操作和 / 或控制。

[0070] 图 6 例示了根据本公开的特定实施方式的、用于在由电子网络提供服务的客户端系统中执行远程维护的示例方法 100 的流程图。方法 100 可以包括多个步骤，并且可以由电子网络 1 的各个组件(包括数据中心 10 和 / 或其它资源)来执行。在一些实施方式中，客户端系统 20 可以包括汽车和 / 或与汽车关联的 FlexRay 系统。方法 100 可以在 102 开始。

[0071] 步骤 104 可以包括维护数据库，所述数据库包括将客户端系统节点 32 的列表与相应处理指令集关联的信息。数据中心 10 可以单独或者结合其它资源来执行步骤 104。例如，个体可以负责随着新信息变得可用而更新数据库。作为另一示例，与客户端系统节点 32 关联的各个厂商和 / 或提供方可以通过电子方式向数据中心 10 传送更新软件和 / 或固件包。

[0072] 步骤 106 可以包括接收针对软件更新的请求，该请求包括与特定客户端系统 20 以及特定处理指令集对应的标识符。数据中心 10 可以执行步骤 106。数据中心可以通过网络 18 接收该请求。

[0073] 步骤 108 可以包括访问该数据库以检索与客户端系统节点 32 以及与关联的节点 32 相关的相应处理指令集有关的信息。数据中心 10 可以基于所接收的请求来执行步骤 108。

[0074] 步骤 110 可以包括执行用于模拟节点 32 与由安装所请求的软件更新导致的相应处理指令的组合的计算。数据中心 10 可以执行步骤 110。

[0075] 方法 100 可以在 112 结束。

[0076] 在一些实施方式中,客户端系统 20 可以包括具有多个节点 32 (例如, CPU 和 / 或处理资源)的复杂网络系统。各个节点 32 可以包括由厂商提供的关联软件和 / 或固件。随着任何特定节点 32 接收到来自其相应厂商的更新软件和 / 或固件,存在用于客户端系统 20 的软件和 / 或固件的新组合。可能的组合的数量可能非常大。软件和 / 或固件的无效的和 / 或不合适的组合可能影响客户端系统 20 的操作。在一些实施方式中,数据中心 10 可以维护节点 32 及其相应软件的数据库。

[0077] 方法 100 可以使得数据中心 10 和 / 或电子网络 1 的附加组件能够在向客户端系统 20 传送任何电子内容之前,模拟所提出的节点 32 和 / 或它们的相应软件和 / 或固件的组合。针对操作完整性、兼容性和 / 或任何其它合适标准测试所提出的组合可增加客户端系统 20 的可靠性和 / 或稳定性。

[0078] 图 7 例示了根据本公开的特定实施方式的、用于执行针对由服务多个客户端 20 的电子网络 1 提供服务的客户端系统 20 的远程维护的示例方法 120 的流程图。方法 120 可以包括多个步骤,并且可以由电子网络 1 的各个组件(包括客户端系统 20 和 / 或其它资源)来执行。在一些实施方式中,客户端系统 20 可以包括汽车和 / 或与汽车关联的 FlexRay 系统。方法 120 可以在 122 开始。

[0079] 步骤 124 可以包括接收可用于传送至多个客户端系统 20 的更新的软件模块的列表。这些更新的软件模块可以托管在多个服务器上。步骤 124 可以由客户端系统 20 执行。例如,第一 VM 22b 可以向数据中心 10 查询该列表,并接着接收该列表。

[0080] 步骤 126 可以包括至少部分地基于与客户端系统 20 关联的多个节点 32 的标识,来确定是否请求该列表上的任何更新的软件模块。在一些实施方式中,第一 VM 22b 可以考虑客户端系统 20 中的处理器的列表,并且比较该列表与可用模块的列表。例如,如果客户端系统 20 是汽车和 / 或与汽车关联的 FlexRay 系统,则第一 VM 22b 可以基于该汽车的品牌、型号和 / 或年份来确定是否请求更新。

[0081] 步骤 128 可以包括请求更新软件模块。在一些实施方式中,步骤 128 可以是空中和 / 或远程通信。客户端系统 20 可以执行步骤 128。例如,第一 VM 22b 可以向数据中心 10 请求所述更新软件模块。

[0082] 步骤 130 可以包括接收所请求的更新的软件模块。在一些实施方式中,更新的软件模块可以托管在多个服务器上。在这种实施方式中,客户端系统 20 可以从托管所请求的模块的特定服务器接收所请求的模块。在这些实施方式中,更新的软件模块的列表可以包括标识各个模块的位置的统一资源定位符。

[0083] 步骤 132 可以包括将所接收的更新的软件模块安装在客户端系统上。更新的软件模块可以通过空中方式和 / 或通过另一远程通信系统来传送。方法 120 可以在 134 结束。

[0084] 图 8 例示了根据本公开的特定实施方式的、用于执行在被配置为服务于多个客户端系统 20 的电子网络 1 中的远程维护的示例方法 140 的流程图。方法 140 可以包括多个步骤,并且可以由电子网络 1 的各个组件(包括数据中心 10 和 / 或其它资源)来执行。在一些实施方式中,客户端 20 可以包括移动电话。方法 140 可以在 142 开始。

[0085] 步骤 144 可以包括操作具有与客户端系统中的各个节点 32 关联的软件的数据库的数据中心 10。在客户端系统 20 包括移动电话的实施方式中,节点 32 可以包括各种软件标识符模块(SIM)。数据中心 10 可以执行步骤 144。

[0086] 步骤 146 可以包括与由客户端系统 20 托管的第一虚拟机 22b 进行通信。第一虚拟机 22b 可以处理与数据中心 10 关联的第一数据集。例如,第一虚拟机 22b 可以被配置为访问与客户端系统 20 的各个节点 32 有关的各种配置、修订号等的列表。数据中心 10 可以利用网络 18 执行步骤 146。数据中心 10 可以将与第一 VM 22b 关联的数据集与现行版本和 / 或更新状态的列表进行比较,并标记标识中的任何变化。

[0087] 步骤 148 可以包括接收第一虚拟机 22b 标识用于传送至客户端系统 20 中的各种节点 32 中的一个节点的软件更新的请求。例如,第一 VM 22b 可以请求针对移动电话中的特定 SIM 的软件更新。数据中心 10 可以执行步骤 148。

[0088] 步骤 150 可以包括执行验证客户端系统 20 的标识的证明处理。数据中心 10 可以执行步骤 150。证明处理可以包括上面讨论的验证处理中的任一个。在一些实施方式中,证明处理可以包括接收、测试和 / 或验证一个或更多个生物特征指示符。在一些实施方式中,客户端系统 20 可以利用第二 VM 22b、TPM 24 和 / 或资源列表 28 来执行用于验证数据中心 10 的标识的证明处理。

[0089] 步骤 152 可以包括利用网络向第一虚拟机发送所标识的软件更新。在一些实施方式中,数据中心 10 可以通过网络 18 发送所标识的软件。在一些实施方式中,步骤 152 可以通过无线方式和 / 或空中方式发送所标识的软件更新来执行。

[0090] 步骤 154 可以包括授权第一 VM 22b 利用与各个节点 32 中的所述一个节点关联的第二 VM 22c 将所接收的软件更新安装在客户端系统 20 上。第一 VM 22b 与第二 VM 22c 可以通过 VMM 24 进行通信。在一些实施方式中,客户端系统 20 可以在接受来自数据中心 10 的所接收的软件之前,执行验证所接收的软件的完整性和 / 或安全性的证明处理。方法 140 可以在 156 结束。证明可以在安装所接收的软件更新之前和 / 或之后进行。

[0091] 在一些实施方式中,第一 VM 22b 可以询问第二 VM 22c 以验证客户端系统 20 已经接收到该软件更新。在一些客户端系统 20 中,多个节点 32 中的每一个可以利用唯一操作系统来操作。例如,在具有多个 SIM 卡的移动电话中,各个 SIM 卡可以对其自己的 OS 进行操作。多个 SIM 卡之间和 / 或客户端系统 20 的各个 VM 22 之间的数据交换可能因 OS 的变化而变复杂。在一些实施方式中,特定 SIM 卡可能具有比另一 SIM 卡及其 OS 低级别的安全性需求。在这些实施方式中,传统维护需要在安全维护位置维修客户端系统 20。

[0092] 使用方法 140 和本公开的教导可以允许通过空中方式和 / 或无线方式维护客户端系统 20。在具有通过 VMM 24 链接的多个 VM 22 的客户端系统中,数据中心 10 与客户端系统 20 之间的数据交换可以由 TPM 26 来支持,并且提供增加的安全性和 / 或可靠性。

[0093] 图 9 例示了根据本公开的特定实施方式的、用于客户端系统 20 请求并接收来自远程服务器 10 的软件更新的示例方法 160 的流程图。方法 160 可以包括多个步骤,并且可以由电子网络 1 的各组件(包括客户端系统 20 和 / 或其它资源)来执行。在一些实施方式中,客户端 20 可以包括移动电话。节点 32 可以包括用户标识模块(SIM)卡。方法 160 可以在 162 开始。

[0094] 步骤 144 可以包括托管与客户端系统 20 关联的两个虚拟机 22。第一 VM 22b 可以

处理与外部数据中心 10 关联的第一数据集。第二 VM 22c 可以处理与客户端系统 20 中的节点 32 关联的第二数据集。第一 VM 22b 与第二 VM 22c 可以通过 VMM 24 进行通信, 以维护各个 VM 22 的数据完整性和 / 或可靠性。

[0095] 步骤 146 可以包括操作被配置为管理两个 VM 之间的通信的 VMM 24。客户端系统 20 可以与 TPM 26 结合执行步骤 146。

[0096] 步骤 148 可以包括识别第一数据集与第二数据集相比标识已过期。数据中心 10、VM 22b 或 22c 和 / 或 VMM 24 可以执行步骤 148。

[0097] 步骤 150 可以包括标识用于传送至节点 32 的软件更新, 该软件更新被配置为恢复第一数据集与第二数据集之间的标识。

[0098] 步骤 152 可以包括执行验证客户端系统的标识、验证数据中心 10 的标识和 / 或所标识出的软件更新的可靠性和 / 或安全性的证明处理。电子网络 1 的某一部分可以执行该证明处理。例如, VMM 24 可以结合 TPM 26 进行操作, 以确认软件包和 / 或数据中心 10 的标识。

[0099] 步骤 154 可以包括请求来自外部数据中心 10 的所标识的软件更新。第一 VM 22b 可以执行步骤 154。

[0100] 步骤 156 可以包括接收从外部数据中心 10 至第一 VM 22b 的所标识的软件更新。

[0101] 步骤 158 可以包括通过第二 VM 22c 将所发送的软件更新安装在节点 32 上。在一些实施方式中, 第一 VM 22b 可以询问第二 VM 22c 以验证节点 32 已经接收到该软件更新。

[0102] 在一些客户端系统 20 中, 多个节点 32 中的每一个可以利用唯一操作系统进行操作。例如, 在具有多个 SIM 卡的移动电话中, 各个 SIM 卡可以以其自己的 OS 进行操作。多个 SIM 卡之间和 / 或客户端系统 20 的各个 VM 22 之间的数据交换可能因 OS 的差别而变复杂。在一些实施方式中, 特定 SIM 卡可以具有比另一 SIM 卡及其 OS 低级别的安全性需求。在这些实施方式中, 传统维护需要在安全维护位置维修客户端系统 20。

[0103] 方法 160 的使用和本公开的教导可以使得能够通过空中方式和 / 或无线方式维护客户端系统 20。在具有通过 VMM 24 链接的多个 VM 22 的客户端系统中, 数据中心 10 与客户端系统 20 之间的数据交换可以由 TPM 26 来支持, 并且提供增加的安全性和 / 或可靠性。

[0104] 图 10 例示了根据本公开的特定实施方式的、用于验证电子软件代码完整性的示例方法 182 的流程图。方法 182 可以包括多个步骤, 并且可以由电子网络 1 的各个组件(包括客户端系统 20 和 / 或其它资源)来执行。方法 182 可以在 184 开始。

[0105] 步骤 186 可以包括向客户端系统 20 提供多个加密密钥, 所述多个加密密钥中的每一个与相应时间因子相关。该时间因子可以至少部分地取决于在传送软件代码包时生成的控制因子和时间戳、该软件代码包的更新定时或者与该客户端关联的受信任协议模块的更新定时。

[0106] 步骤 188 可以包括基于与软件代码包有关的时间因子利用所述多个加密密钥中的一个来对该软件代码包进行加密。

[0107] 步骤 190 可以包括向客户端系统 20 传送加密的软件代码包。

[0108] 步骤 192 可以包括向客户端 20 通知基于与客户端 20 接收软件代码包的时间关联的时间因子来选择解密密钥。方法 182 可以在 194 结束。

[0109] 传统软件代码的完整性可以利用电子签名(例如, 公用密钥基础设施(PKI)认证方

法)来检查。然而,与本公开的方法相比,使用电子签名可能不可靠。例如,电子签名可以并入到期日期,在该到期日期之后,签名失效。可以在执行电子签名确认处理之前和 / 或之后替换和 / 或改变代码。

[0110] 根据本公开的教导,代码完整性可以通过包括更新定时 / 密钥控制来实质改进。该加密密钥可以基于时间因子而改变。例如,该时间因子可以至少部分地取决于与发送和 / 或传送电子内容有关的时间戳。作为另一示例,时间因子可以至少部分地取决于 TPM 26 和 / 或 VM 22 的更新定时。在任何情况下,该时间因子还可以取决于预先设置的控制因子  $\alpha$ 。可以通过与 TPM 26 关联的资源列表 28 存储多个加密密钥。利用合适的加密密钥,TPM 26 还可以利用其电子签名日期来检查电子内容的到期时间。

[0111] 图 11 例示了根据本公开的特定实施方式的、用于验证电子软件代码的完整性的示例方法 200 的流程图。方法 200 可以包括多个步骤,并且可以由电子网络 1 的各个组件(包括客户端系统 20 和 / 或其它资源)来执行。方法 200 可以在 202 开始。

[0112] 根据本公开的教导,代码完整性可以通过包括更新定时 / 密钥控制来实质改进。该加密密钥可以基于时间因子而改变。例如,该时间因子可以至少部分地取决于与发送和 / 或传送电子内容相关的时间戳。作为另一示例,时间因子可以至少部分地取决于 TPM 26 和 / 或 VM 22 的更新定时。在任何情况下,该时间因子还可以取决于预先设置的控制因子  $\alpha$ 。可以通过与 TPM 26 关联的资源列表 28 存储多个加密密钥。利用合适的加密密钥,TPM 26 还可以利用其电子签名日期来检查电子内容的到期时间。

[0113] 步骤 204 可以包括存储来自数据中心 10 的加密密钥的列表,各个加密密钥与相应时间因子相关。该列表可以由 TPM 24 和 / 或由与 TPM 24 关联的存储资源来存储。

[0114] 步骤 206 可以包括接收来自数据中心 10 的加密软件代码包。在一些实施方式中,还可以接收电子签名。

[0115] 步骤 208 可以包括基于时间因子来选择加密密钥。在一些实施方式中,TPM 24 还可以检查随着加密软件包传送的电子签名。方法 200 可以在 210 结束。

[0116] 尽管图 4-11 表示了要针对方法 60、80、100、120、140、160、184 以及 200 采取的特定数量的步骤,但是各种方法可以比所描绘的那些步骤更多或更少的步骤来执行。利用本文公开的方法和系统,可以改进、减少或消除与维护针对电子内容的安全访问关联的特定问题。例如,本文公开的方法和系统可以针对执行客户端系统的远程维护的电子网络提供增加的安全性和 / 或可靠性。

[0117] 尽管已经利用多个实施方式描述了本发明,但是本领域技术人员可以想到各种改变和修改。本发明旨在涵盖落入所附权利要求书的范围内的这些改变和修改。本公开的教导涵盖本领域普通技术人员应当理解的、对于本文的示例实施方式的所有改变、替换、变型、更改、修改。

[0118] 在具体实施方式中,可以将一个或更多个网页与联网系统和 / 或联网服务关联。具体实施方式可能涉及检索和 / 或获得(render)由任何类型的网络可寻址资源或网站托管的结构性文档。另外,在本文使用时,“用户”可以包括个体、团体和 / 或公司实体(例如,商业和第三方应用)。

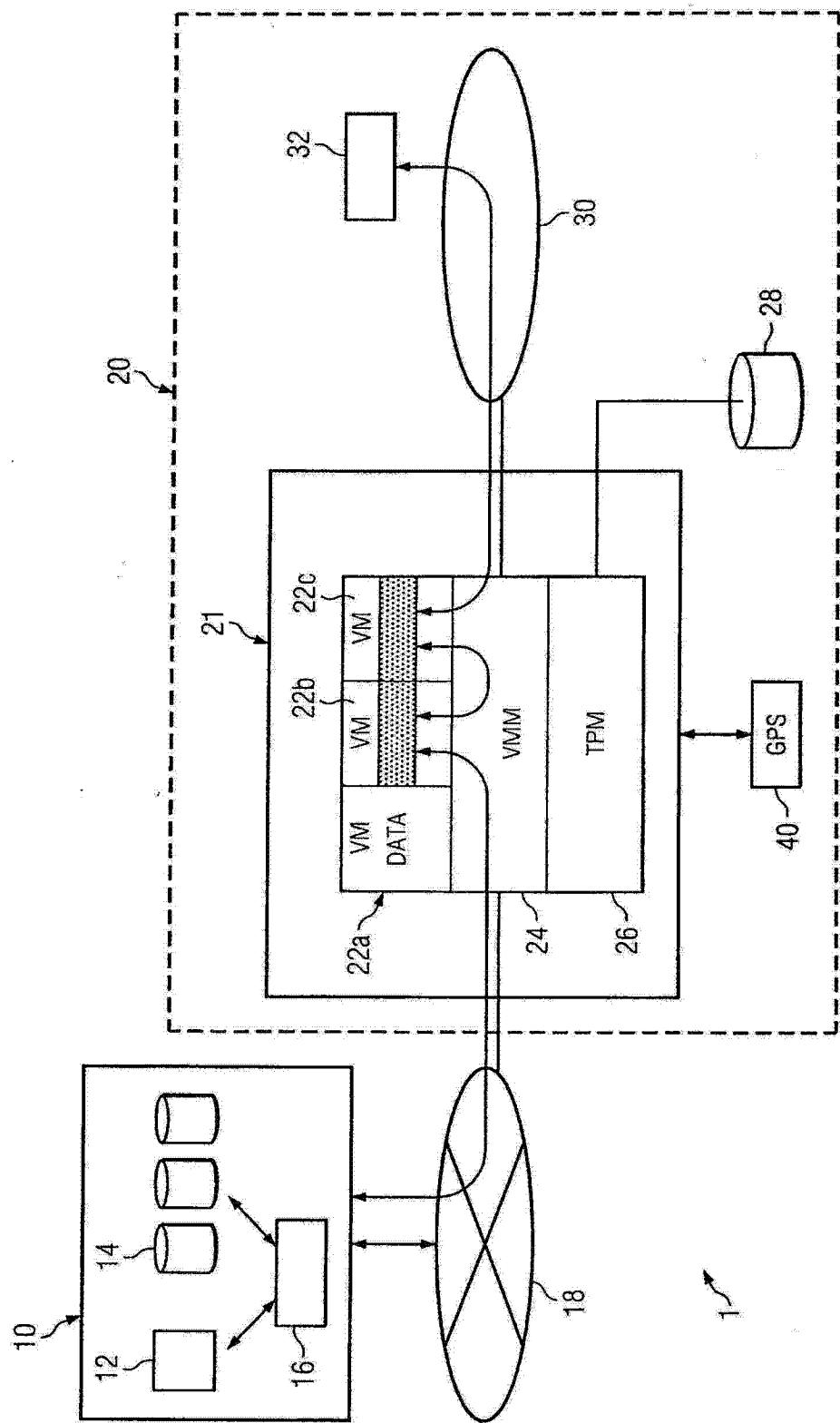


图 1

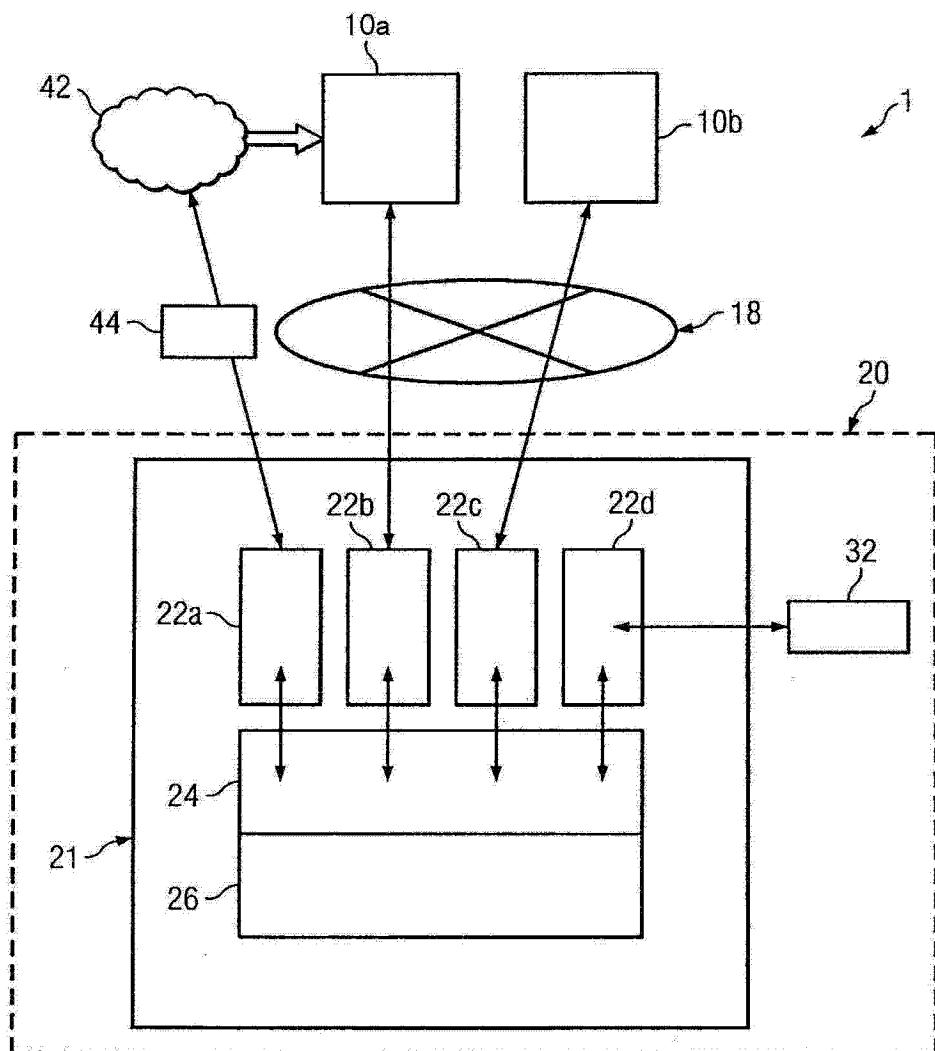


图 2

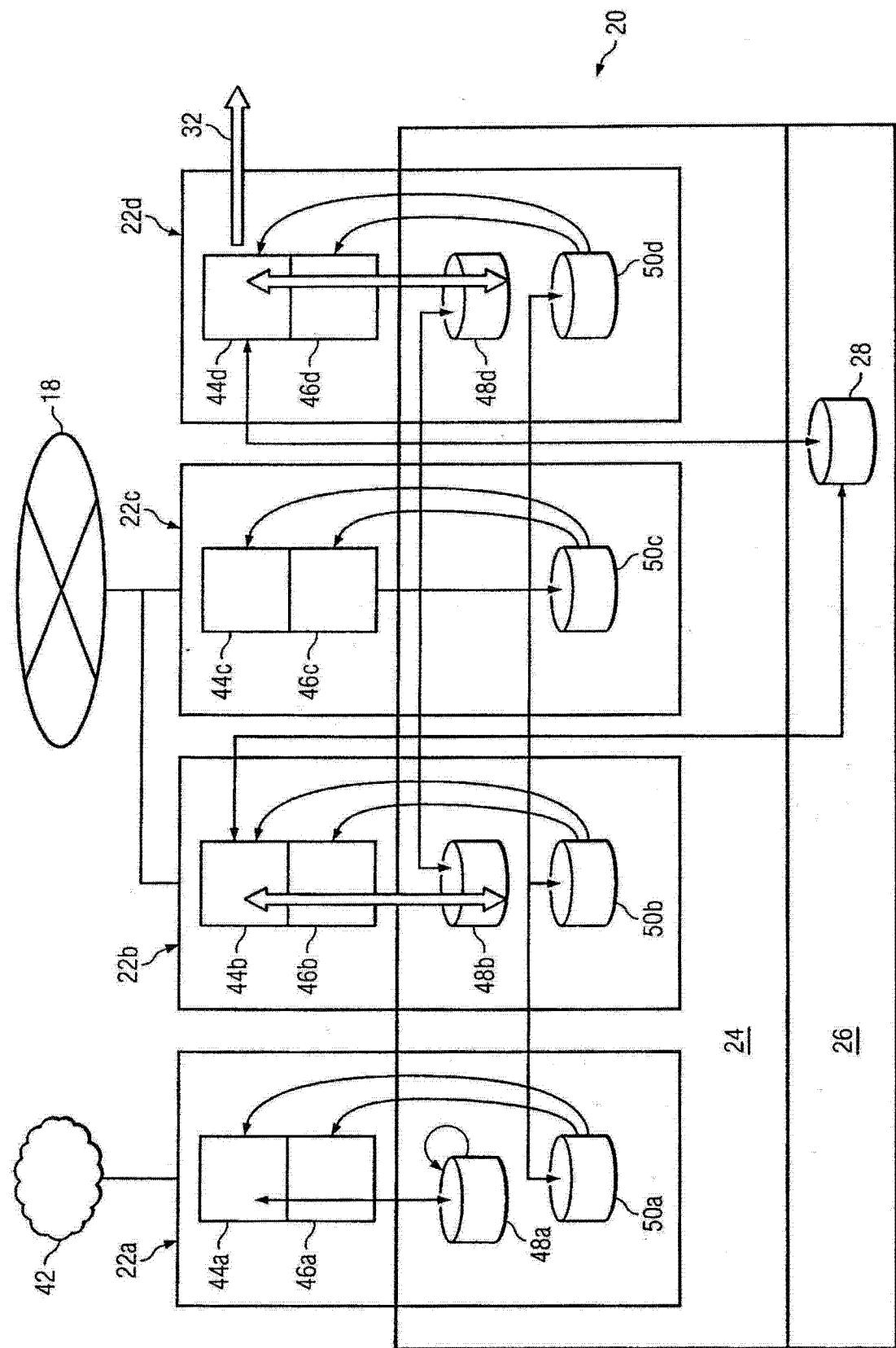
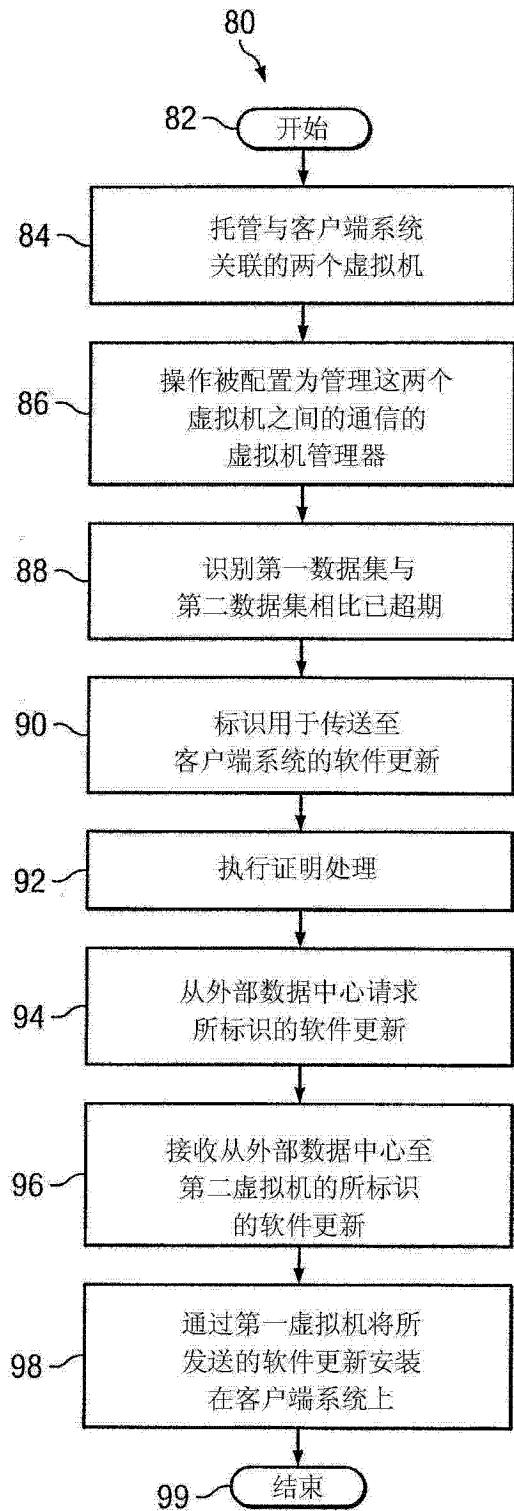
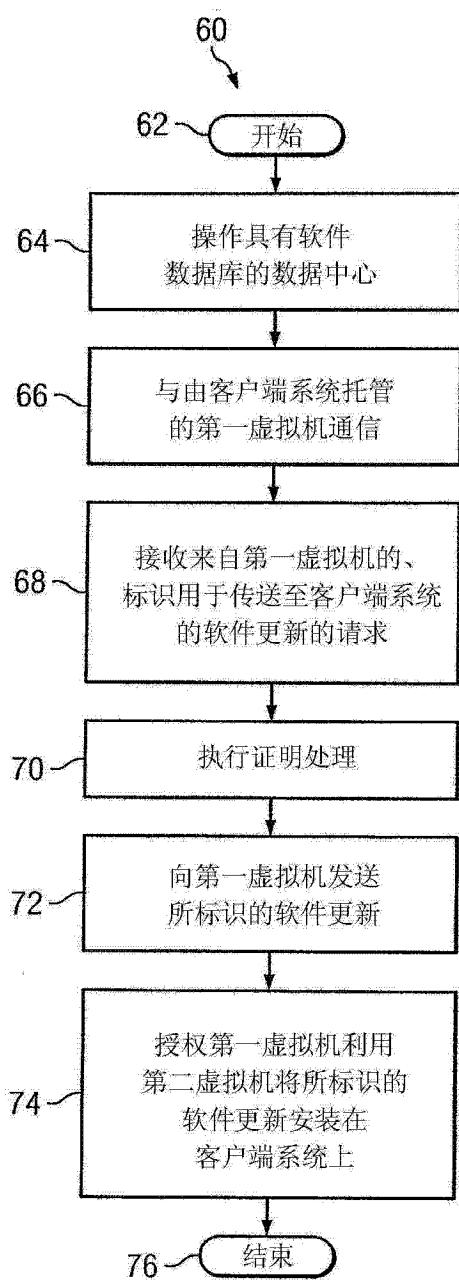


图 3



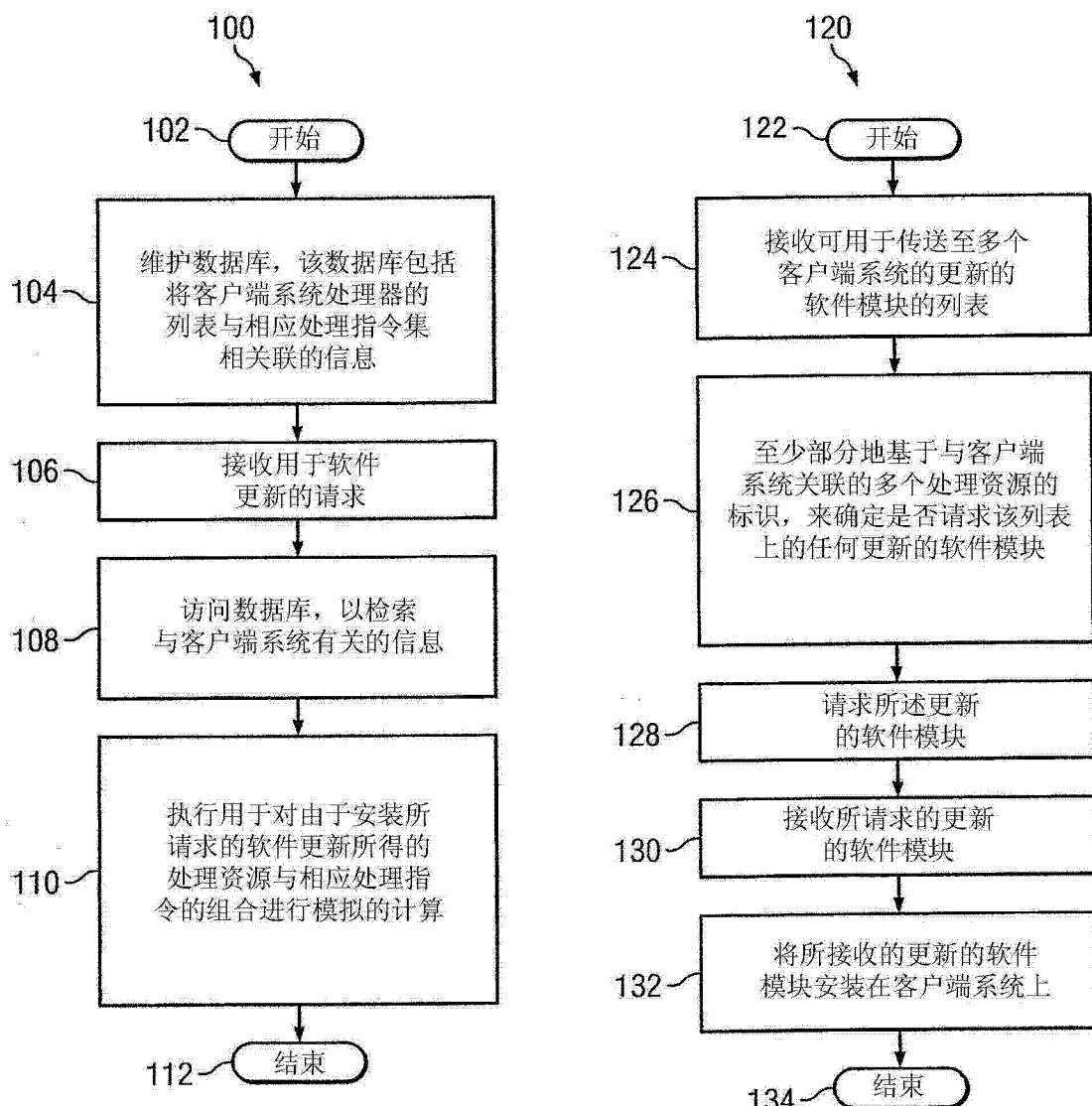


图 6

图 7

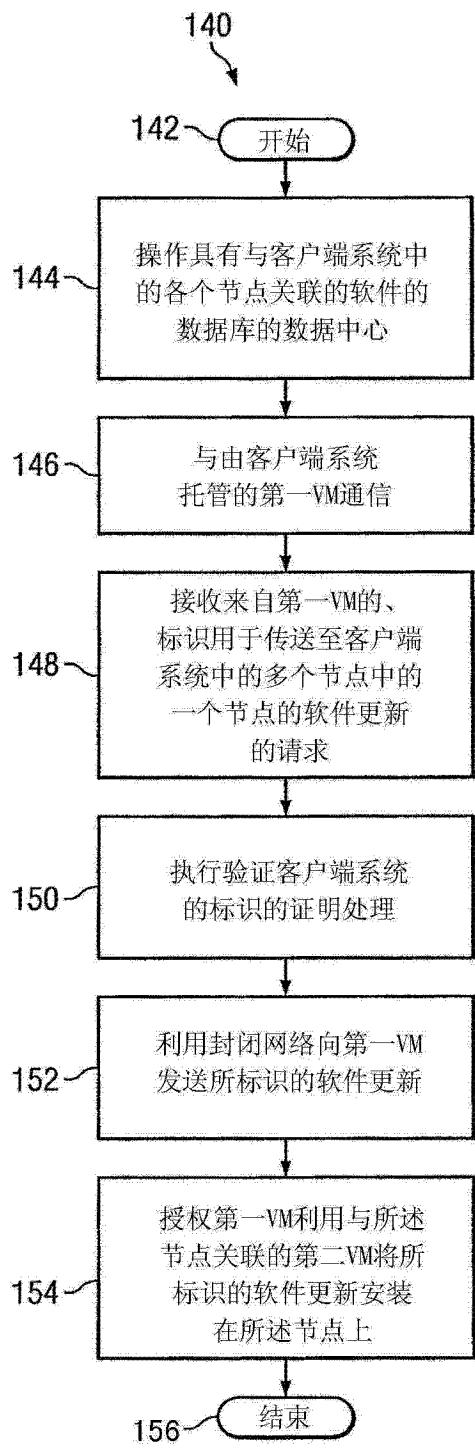


图 8

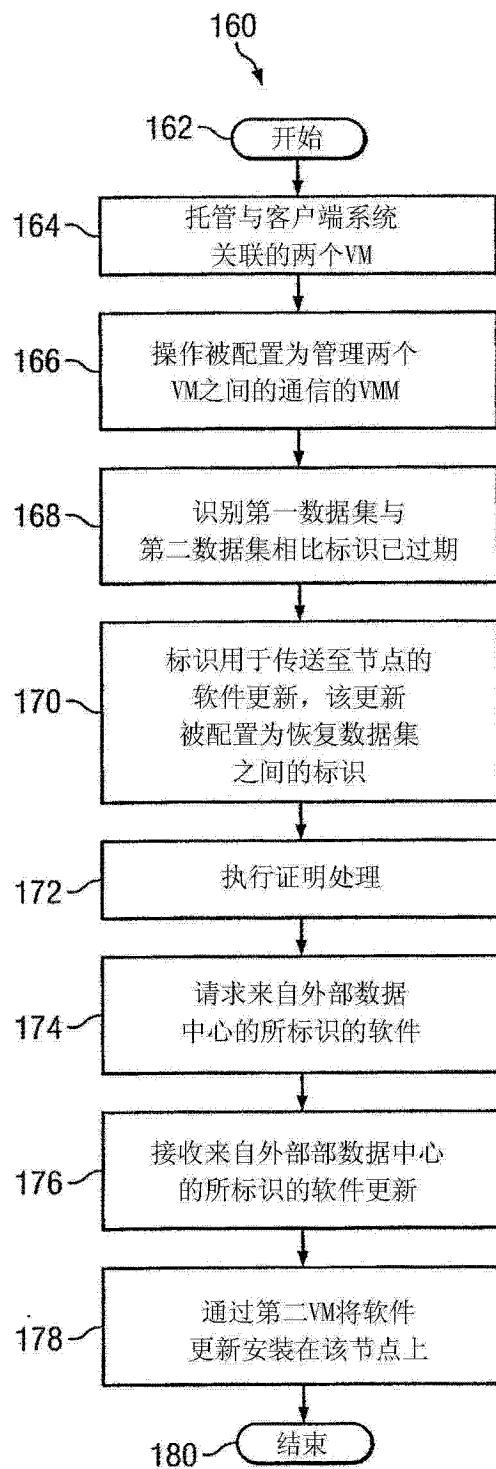


图 9

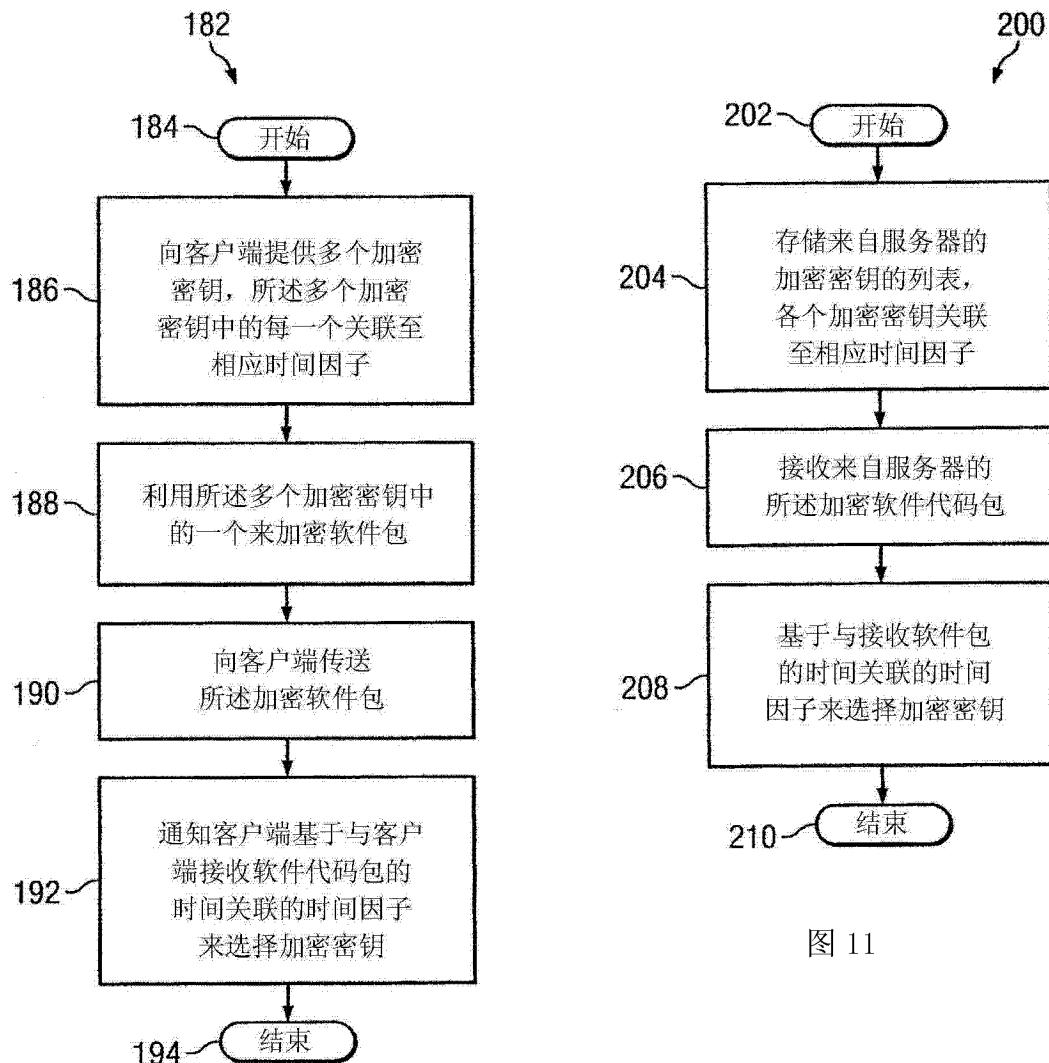


图 10

图 11