(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111859379 A
(43)申请公布日 2020.10.30

(21)申请号 202010764827.5
(22)申请日 2020.07.31
(71)申请人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号
申请人 工银科技有限公司
(72)发明人 郭铮铮 李佳宸
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 刘丽丽
(51)Int.Cl.
G06F 21/55(2013.01)
G06F 21/57(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)

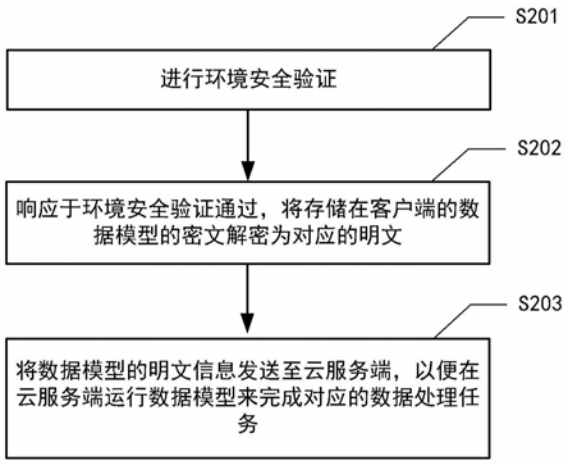
权利要求书2页 说明书16页 附图8页

(54)发明名称

保护数据模型的处理方法和装置

(57)摘要

本公开提供了一种保护数据模型的处理方法，涉及云计算、信息安全等技术领域。该方法包括：进行环境安全验证；响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文；以及将数据模型的明文信息发送至云服务端，以便在云服务端运行数据模型来完成对应的数据处理任务。本公开还提供了一种保护数据模型的处理装置、一种电子设备以及一种计算机可读存储介质。



CN 111859379 A

1.一种保护数据模型的处理方法,包括:

进行环境安全验证;

响应于环境安全验证通过,将存储在客户端的数据模型的密文解密为对应的明文;以及

将所述数据模型的明文信息发送至云服务端,以便在所述云服务端运行所述数据模型来完成对应的数据处理任务。

2.根据权利要求1所述的方法,还包括:在将所述数据模型的明文信息发送至所述云服务端之后,或者在所述云服务端开始运行所述数据模型之后,

将保存在所述客户端的所述数据模型的明文信息清除。

3.根据权利要求2所述的方法,其中,所述将保存在所述客户端的所述数据模型的明文信息清除,包括以下至少之一:

将保存在所述客户端的所述数据模型的明文本身清除;

将所述客户端用于存储所述数据模型的明文信息的文件清除;

将所述客户端用于存储所述数据模型的明文信息的内存空间清空。

4.根据权利要求1至3中任一项所述的方法,其中,所述进行环境安全验证,包括以下至少之一:

对所述客户端进行环境安全验证;

对所述云服务端进行环境安全验证;

对所述客户端与所述云服务端之间的通信信道进行环境安全验证。

5.根据权利要求4所述的方法,其中,所述对所述客户端进行环境安全验证,包括:

验证针对所述客户端的系统侦测操作是否已被禁止。

6.根据权利要求5所述的方法,其中,所述验证针对所述客户端的系统侦测操作是否已被禁止,包括:

通过配置文件或者配置文件的哈希值验证针对所述客户端的系统侦测操作是否已被禁止。

7.根据权利要求4所述的方法,其中,所述对所述云服务端进行环境安全验证,包括以下至少之一:

验证所述云服务端针对所述数据模型的日志生成功能是否已被关闭;

验证所述云服务端是否已针对所述数据模型设置有日志加密操作。

8.根据权利要求4所述的方法,其中,所述对所述客户端与所述云服务端之间的通信信道进行环境安全验证,包括:

验证所述客户端与所述云服务端之间的通信信道是否已被加密。

9.根据权利要求1所述的方法,还包括:在所述云服务端运行所述数据模型的过程中,

定期进行环境安全验证。

10.一种保护数据模型的处理装置,包括:

验证模块,用于进行环境安全验证;

解密模块,用于响应于环境安全验证通过,将存储在客户端的数据模型的密文解密为对应的明文;以及

发送模块,用于将所述数据模型的明文信息发送至云服务端,以便在所述云服务端运

行所述数据模型来完成对应的数据处理任务。

11.一种电子设备,包括:

一个或多个处理器;

存储器,用于存储一个或多个程序,

其中,当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器实现权利要求1至9中任一项所述的方法。

12.一种计算机可读存储介质,存储有计算机可执行指令,所述指令在被执行时用于实现权利要求1至9中任一项所述的方法。

保护数据模型的处理方法和装置

技术领域

[0001] 本公开涉及云计算、信息安全等技术领域，特别是涉及一种保护数据模型的处理方法和装置。

背景技术

[0002] 随着云计算的快速发展，金融、政务等领域中，越来越多的业务应用被迁移到云环境中运行。不管是公有云、专有云、还是私有云，其云环境与传统运行环境不同。传统运行环境的主机是由企业或者机构自己维护的，可以通过设置网络及主机访问权限，有效地通过连接阻断来保证存储在主机文件系统中的业务应用、数据模型以及其他敏感信息等的安全。但是云环境的主机是由第三方维护的，随着金融、政务等领域的业务应用被迁移到第三方云环境中运行，用户对金融、政务等领域的业务应用、数据模型以及其他敏感信息等的访问权限是由第三方控制的。由此导致运行在云环境中的业务应用、数据模型以及其他敏感信息等可能被泄露或者被复制，进而可能给金融、政务等机构造成损失。

发明内容

[0003] 本公开的一个方面提供了一种保护数据模型的处理方法，包括：进行环境安全验证；响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文；以及将上述数据模型的明文信息发送至云服务端，以便在上述云服务端运行上述数据模型来完成对应的数据处理任务。

[0004] 可选地，还包括：在将上述数据模型的明文信息发送至上述云服务端之后，或者在上述云服务端开始运行上述上述数据模型之后，将保存在上述客户端的上述数据模型的明文信息清除。

[0005] 可选地，上述将保存在上述客户端的上述数据模型的明文信息清除，包括以下至少之一：将保存在上述客户端的上述数据模型的明文本身清除；将上述客户端用于存储上述数据模型的明文信息的文件清除；将上述客户端用于存储上述数据模型的明文信息的内存空间清空。

[0006] 可选地，上述进行环境安全验证，包括以下至少之一：对上述客户端进行环境安全验证；对上述云服务端进行环境安全验证；对上述客户端与上述云服务端之间的通信信道进行环境安全验证。

[0007] 可选地，上述对上述客户端进行环境安全验证，包括：验证针对上述客户端的系统侦测操作是否已被禁止。

[0008] 可选地，上述验证针对上述客户端的系统侦测操作是否已被禁止，包括：通过配置文件或者配置文件的哈希值验证针对上述客户端的系统侦测操作是否已被禁止。

[0009] 可选地，上述对上述云服务端进行环境安全验证，包括以下至少之一：验证上述云服务端针对上述数据模型的日志生成功能是否已被关闭；验证上述云服务端是否已针对上述数据模型设置有日志加密操作。

[0010] 可选地，上述对上述客户端与上述云服务端之间的通信信道进行环境安全验证，包括：验证上述客户端与上述云服务端之间的通信信道是否已被加密。

[0011] 可选地，还包括：在上述云服务端运行上述数据模型的过程中，定期进行环境安全验证。

[0012] 本公开的另一个方面提供了一种保护数据模型的处理装置，包括：验证模块，用于进行环境安全验证；解密模块，用于响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文；以及发送模块，用于将上述数据模型的明文信息发送至云服务端，以便在上述云服务端运行上述数据模型来完成对应的数据处理任务。

[0013] 本公开的另一方面提供了一种电子设备，包括：一个或多个处理器；存储器，用于存储一个或多个程序，其中，当上述一个或多个程序被上述一个或多个处理器执行时，使得上述一个或多个处理器实现本公开实施例的方法。

[0014] 本公开的另一方面提供了一种计算机可读存储介质，存储有计算机可执行指令，上述指令在被执行时用于实现本公开实施例的方法。

[0015] 本公开的另一方面提供了一种计算机程序，上述计算机程序包括计算机可执行指令，上述指令在被执行时用于实现本公开实施例的方法。

附图说明

[0016] 为了更完整地理解本公开及其优势，现在将参考结合附图的以下描述，其中：

[0017] 图1A示意性示出了根据本公开实施例的适于保护数据模型的处理方法和装置的系统架构；

[0018] 图1B示意性示出了根据图1A所示的客户端的系统结构图；

[0019] 图1C示意性示出了根据图1A所示的云服务端的系统结构图；

[0020] 图2示意性示出了根据本公开实施例的保护数据模型的处理方法的流程图；

[0021] 图3示意性示出了根据本公开又一实施例的保护数据模型的处理方法的流程图；

[0022] 图4A示意性示出了根据本公开实施例的进行环境安全验证的示意图；

[0023] 图4B示意性示出了根据本公开实施例的进行环境安全验证的逻辑图；

[0024] 图5示意性示出了根据本公开又一实施例的保护数据模型的处理方法的流程图；

[0025] 图6示意性示出了根据本公开实施例的保护数据模型的处理装置的框图；以及

[0026] 图7示意性示出了根据本公开实施例的电子设备的框图。

具体实施方式

[0027] 以下，将参照附图来描述本公开的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本公开的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本公开实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本公开的概念。

[0028] 在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本公开。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

[0029] 在此使用的所有术语(包括技术和科学术语)具有本领域技术人员通常所理解的含义,除非另外定义。应注意,这里使用的术语应解释为具有与本说明书的上下文相一致的含义,而不应以理想化或过于刻板的方式来解释。

[0030] 在使用类似于“A、B和C等中至少一个”这样的表述的情况下,一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释(例如,“具有A、B和C中至少一个的系统”应包括但不限于单独具有A、单独具有B、单独具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B、C的系统等)。

[0031] 附图中示出了一些方框图和/或流程图。应理解,方框图和/或流程图中的一些方框或其组合可以由计算机程序指令来实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器,从而这些指令在由该处理器执行时可以创建用于实现这些方框图和/或流程图中所说明的功能/操作的装置。本公开的技术可以硬件和/或软件(包括固件、微代码等)的形式来实现。另外,本公开的技术可以采取存储有指令的计算机可读存储介质上的计算机程序产品的形式,该计算机程序产品可供指令执行系统使用或者结合指令执行系统使用。

[0032] 本公开的实施例提供了一种保护数据模型的处理方法以及能够应用该方法的保护数据模型的处理装置。该方法包括进行环境安全验证;响应于环境安全验证通过,将存储在客户端的数据模型的密文解密为对应的明文;以及将上述数据模型的明文信息发送至云服务端,以便在上述云服务端运行上述数据模型来完成对应的数据处理任务。

[0033] 图1A示意性示出了根据本公开实施例的适于保护数据模型的处理方法和装置的系统架构。图1B示意性示出了根据图1A所示的客户端的系统结构图。图1C示意性示出了根据图1A所示的云服务端的系统结构图。

[0034] 需要注意的是,图1A所示仅为可以应用本公开实施例的系统架构的示例,以帮助本领域技术人员理解本公开的技术内容,但并不意味着本公开实施例不可以用于其他设备、系统、环境或场景。同样,图1B所示仅为可以应用本公开实施例的客户端系统架构的示例,以帮助本领域技术人员理解本公开的技术内容,但并不意味着本公开实施例不可以用于其他设备、系统、环境或场景。同样,图1C所示仅为可以应用本公开实施例的云服务端系统架构的示例,以帮助本领域技术人员理解本公开的技术内容,但并不意味着本公开实施例不可以用于其他设备、系统、环境或场景。

[0035] 如图1A所示,该系统架构100包括:客户端101、102、103等和云环境104。云环境104可以包括多个云服务端(如云服务器1～n)。

[0036] 在本公开实施例中,企业或者个人可以将自己的一个或者多个数据模型存储在自己的客户端中。如企业甲将其数据模型全部存储在客户端101上,企业乙将其数据模型全部存储在客户端102上,企业丙将其数据模型全部存储在客户端103上,……等等。当需要执行数据处理任务时,可以向云环境104提交任务并将对应的数据模型发送至云环境104中运行。由此企业或者个人无需重复搭建基层服务设施,而是可以直接共享云计算环境。

[0037] 应该理解,通过系统架构100,银行、政务等机构在提供大数据业务服务时,可以直接将已有的、成熟的、用于大数据处理的数据模型从客户端迁移至云环境中运行,因而可以保证业务处理的高效性和快捷性。但是,由于云环境的主机是由第三方维护的,如果直接将数据模型迁移至云环境中运行,则第三方对业务数据具有更大的访问权限,因而可能导致

运行在云环境中的数据模型存在被泄露或者被复制的风险。

[0038] 此外，应该理解，在传统的运行环境中，可以通过设置网络及主机的用户访问权限，有效地阻断相关通信连接，进而通过阻断相关通信连接来保证存储在主机文件系统中的数据模型的安全。而当数据模型被迁移至第三方云环境中后，云主机的访问权限是第三方即云基础服务提供者控制的，因此对于应用系统来说，与处理数据或者分析数据相关的具有商业价值的敏感信息即数据模型，就需要改进的保护方案。

[0039] 另外，考虑到当前大数据平台的开源License限制(如需要满足软件禁止分发以及软件修改的严格规定等)，以及考虑到当前竞争激烈的应用服务市场(如需要满足快速的交付要求以及需要满足业务运营和维护要求等)，需要提供一种较佳的、高效的处理方案。并且在大数据应用中，用于数据分析和数据处理的数据模型是基于长期的业务提炼而积累的业务资产，所以既要保证数据模型的安全，又要保证对原有应用系统适配改造最小、通用性更强。对此，本公开实施例对客户端和云服务端进行了适应性改造。

[0040] 如图1B所示，改造后的客户端101(或者客户端102、103)等包括：计算机硬件或者虚拟机平台、计算机操作系统和客户端程序。进一步，客户端程序可以包括数据模型加密模块、任务提交模块、环境安全验证模块、数据模型解密模块、数据模型管理模块和环境安全监控模块。

[0041] 具体地，数据模型加密模块用于对存储在客户端的各数据模型进行加密，即客户端存储的是数据模型的密文，由此可以防止数据模型泄露后被轻易复制。

[0042] 任务提交模块用于向服务系统发起提交服务请求的流程，包括先调用环境安全验证模块而发起环境安全验证，并接收环境安全验证模块返回的环境安全验证结果，进而基于环境安全验证结果决定是否继续后续流程。例如，如果任务提交模块接收到环境安全验证通过的结果，则确定继续后续流程；如果任务提交模块接收到环境安全验证不通过的结果，则终止服务请求提交流程。进一步，在确定继续后续流程的情况下，任务提交模块再调用数据模型解密模块。数据模型解密模块用于使用内置的密钥对数据模型的密文执行解密运算，并向任务提交模块返回解密后的数据模型的明文信息。任务提交模块在接收到数据模型的明文信息后，基于解密后的数据模型向服务端系统发起服务请求。服务请求中包括数据模型的明文信息。进一步，在数据模型的明文信息被提交后或者在云服务端开始运行被提交的数据模型后，任务提交模块再调用数据模型管理模块。数据模型管理模块用于清理解密后的数据模型的明文信息。由此可以防止由于数据模型的明文信息被泄露或者被复制而造成损失。进一步，在云服务端运行被提交的数据模型的过程中，任务提交模块还可以调用环境安全监控模块。环境安全监控模块用于定期进行环境安全验证，并定期向任务提交模块返回环境安全验证结果。任务提交模块还用于接收并基于环境安全监控模块返回的环境安全验证结果决定是否继续在云服务端运行数据模型。例如，如果任务提交模块接收到环境安全验证通过的结果，则确定继续在云服务端运行数据模型；如果任务提交模块接收到环境安全验证不通过的结果，则向服务系统发起终止服务请求的流程。

[0043] 此外，在本公开实施例中，上述计算机操作系统可以为Linux操作系统。上述客户端程序可以是基于Java语言编写的程序。进一步，为了防止客户端程序被反编译，以及防止客户端程序运行在非授权的的客户端系统中，可以使用程序加密技术对客户端程序进行加密处理，并使用授权控制技术对客户端系统进行加固处理。

[0044] 如图1C所示，改造后的云服务端1～n中的每个可以作为一个服务节点，每个服务节点可以包括：Hive server、Yarn Server、Name Node、Data Node等。具体地，每个服务节点可以包括计算机硬件或者虚拟化平台、计算机操作系统、服务端应用模块和环境安全监控模块。不同服务节点的服务端应用模块可以按照大数据平台的组网协议和应用协议进行通信，从而形成一个统一整体，共同完成数据模型的计算服务。

[0045] 具体地，云服务端接收来自客户端的服务请求，基于客户端提供的数据模型完成大数据计算后，向客户端返回计算结果。云服务端的环境安全监控模块运行在每个节点的操作系统层，可以定期基于预先配置的安全环境验证要求比对完成验证，包括验证针对数据模型生成的日志是否已经加密或者针对数据模型的日志生成功能是否已关闭。具体地，可以验证针对大数据平台(即对应的云服务节点)设置的当前配置文件是否与其预设配置文件一致。或者，通过计算云服务节点当前的配置文件的哈希值，以及其预设的配置文件的哈希值，并比较两个哈希值是否一致。如果两个哈希值一致，则判定为运行环境安全；如果两个哈希值不一致，则判定为运行环境不安全。完成云服务端环境安全验证并返回对应的验证结果。

[0046] 通过本公开实施例，克服了传统数据模型迁移到第三方云基础环境中运行时，由于主机访问权限发生转移而导致数据模型存在被泄露或者被复制的风险的问题，可以实现在迁移过程中保护数据模型的目的。

[0047] 以下将结合附图和具体实施例详细阐述本公开。

[0048] 图2示意性示出了根据本公开实施例的保护数据模型的处理方法的流程图。

[0049] 如图2所示，该方法可以包括操作S201～S203。

[0050] 在操作S201，进行环境安全验证。

[0051] 接下来，在操作S202，响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文。

[0052] 再接下来，在操作S203，将数据模型的明文信息发送至云服务端，以便在云服务端运行数据模型来完成对应的数据处理任务。

[0053] 具体地，为了防止数据模型被泄露或者被复制，可以将各数据模型进行加密处理并将其密文保存在客户端。但是，云服务端在执行数据处理和数据分析任务时需要运行解密后的数据模型。鉴于此，在需要提交数据处理和数据分析任务时，客户端需要先解密数据模型的密文，再基于解密后的数据模型的明文信息提交服务请求。

[0054] 因此，为了保证数据模型在解密过程中，或者在传输过程中，或者在运行过程中的安全，在操作S201，可以进行环境安全验证，包括验证客户端环境是否安全、云服务端环境是否安全、客户端与云服务端之间的传输通道是否安全等。其中，在所有的环境验证结果都表征环境安全的情况下(即环境安全验证通过)，执行操作S202，否则结束后续流程。

[0055] 需要说明的是，在本公开的一个实施例中，数据模型的明文信息可以包括数据模型的明文本身，此种情况下在操作S203，可以将数据模型的明文本身发送至云服务端。或者，在本公开的另一个实施例中，数据模型的明文信息可以包括存储数据模型的明文的文件路径和文件名称，此种情况下在操作S203，可以将存储数据模型的明文的文件路径和文件名称发送至云服务端。或者，在本公开的另一个实施例中，数据模型的明文信息可以包括保存数据模型的明文的内存地址，此种情况下在操作S203，可以将保存数据模型的明文的

内存地址发送至云服务端。对于前一个实施例，云服务端可以基于客户端发送的数据模型的明文本身，直接运行该数据模型以执行对应的数据任务。对于后两个实施例，云服务端可以基于客户端发送的数据模型的文件路径和文件名称、或者内存地址，先读取数据模型的明文，在运行该数据模型以执行对应的数据任务。

[0056] 通过本公开实施例，由于在解密数据模型、传输数据模型的明文信息以及运行数据模型之前采用了环境安全验证的技术手段，因而可以保护数据模型，防止其在解密过程中、或者传输过程中、或者运行过程中被泄露或者被复制。

[0057] 此外，在本公开实施例中，在将传统的基于数据模型的应用系统迁移到第三方云环境后，即可以实现云主机运维不受影响(继续由第三方对云主机进行维护)，又可以保护应用系统中的数据模型安全。同时在交付云服务端部署、运营的过程中，能够遵从开源软件License协议的要求。此外，本公开实施例并没有对数据模型本身的方法逻辑进行改造，因而实现了在最低成本改造的基础上，达到最优性价比的安全效果。

[0058] 作为一种可选的实施例，该方法还可以包括：在将数据模型的明文信息发送至云服务端之后，或者在云服务端开始运行数据模型之后，将数据模型保存在客户端的明文信息清除。

[0059] 具体地，在本公开实施例中，数据模型的解密流程如下：(1)，客户端的任务提交模块向数据模型解密模块发送数据模型解密请求，包括需要解密的数据模型的相关信息；(2)，数据模型解密模块向数据模型管理模块发送针对数据模型的存储环境准备消息，优选地，存储环境准备消息可以包括内存随机地址，即使用内存存储解密得到的数据模型的明文，另外存储环境准备消息可以包括随机文件路径，即使用随机文件夹存储解密得到的数据模型的明文；(3)，数据模型管理模块向数据模型解密模块发送针对数据模型的存储环境准备就绪消息，包括数据模型的存储信息；(4)，数据解密模块读取数据模型的密文信息，使用预置的秘钥对数据模型进行解密后存储；(5)，数据模型解密模块将数据模型解密结果消息(包含数据模型的明文信息的存储信息)发送至任务提交模块。

[0060] 由此可见，客户端在解密数据模型后，除了将包含数据模型的明文信息的存储信息发送至云服务端之外，还会在客户端的相应文件路径下的文件夹中或者内存中保存其明文信息。为了防止客户端保存的数据模型的明文信息和存储信息被泄露或者被复制，优选地，在将数据模型的明文信息发送至云服务端之后，或者在云服务端开始运行数据模型之后，可以将数据模型保存在客户端的明文信息清除。

[0061] 如图3所示，在本公开实施例中，该方法除了包括如图2所示的操作S201～S203之外，还可以包括操作S301。

[0062] 其中，图3所示的操作S201～S203与图2所示的操作S201～S203相同，在此不再赘述。

[0063] 在操作S301，将保存在客户端的数据模型的明文信息清除。

[0064] 具体地，本公开实施例提供的保护数据模型的处理方法除了包括环境安全验证过程、数据模型解密过程和数据模型计算过程之外，还可以包括数据模型清除过程。

[0065] 环境安全验证过程是客户端系统发起对包括客户端系统、服务端系统以及客户端系统和服务端系统之间的通信信道的环境安全验证，具体包括验证是否满足数据模型对计算环境的安全要求。

[0066] 数据模型解密过程是客户端系统在验证当前的计算环境满足数据模型对计算环境的安全要求的情况下,对于数据模型的密文进行解密的过程。

[0067] 数据模型计算过程是客户端系统使用解密后获得的数据模型的明文信息和存储信息向服务端系统发起数据模型计算请求的过程。

[0068] 数据模型清除过程是客户端系统在向服务端系统提交数据模型计算请求后,清除客户端保存的数据模型的明文信息和存储信息的过程。

[0069] 需要说明的是,数据模型解密过程返回的数据模型信息可以是数据模型的明文本身,或者可以是存放数据模型的明文的内存地址,也可以是将数据模型的明文保存为文件形式后的文件路径和文件名称等。优选的,可以使用内存存储数据模型的明文。此外,任务提交模块可以包括Hive客户端使用的提交工具beeline,因而可以通过提交工具beeline向大数据平台服务端系统提交计算服务请求。

[0070] 具体地,客户端系统的任务提交模块通过调用数据模型管理模块来清理客户端存储的数据模型的明文信息的存储空间中的存储信息(简称数据模型信息)。更具体地,任务提交模块可以将需要清理的数据模型信息包括在数据模型清理请求消息中发送给数据模型管理模块,数据模型管理模块基于接收的数据模型清理请求消息清除数据模型所处存储区中的相关信息,并向任务提交模块返回数据模型信息清理返回消息。

[0071] 在本公开实施例中,数据模型信息的清理流程可以如下:

[0072] (1),任务提交模块判断数据模型计算服务请求提交后,向数据模型管理模块发送数据模型信息清理请求。

[0073] 其中判断数据模型计算服务请求提交的方法包括接收服务端应用模块返回的信息。如果该信息显示服务端大数据平台已经基于接收到的数据模型开始数据计算过程,则认为计算服务请求已提交完成。数据模型清理请求包括需要清理的数据模型的明文的存储信息。

[0074] (2),数据模型管理模块对数据模型的明文存储空间中的信息进行清除。

[0075] 具体地,清除方法可以包括将数据模型的明文存储空间中的全部数据改写成0或者改写成1。同时回收存储空间以完成信息清理流程。完成信息清理之后,数据模型管理模块向任务提交模块发送数据模型信息清理结果的返回消息。

[0076] 进一步,作为一种可选的实施例,将保存在客户端的数据模型的明文信息清除,可以包括以下至少之一:

[0077] 将保存在客户端的数据模型的明文本身清除。

[0078] 将客户端用于存储数据模型的明文信息的文件清除。

[0079] 将客户端用于存储数据模型的明文信息的内存空间清空。

[0080] 由于数据模型解密模块向任务提交模块返回的数据模型信息,可以包括数据模型的明文本身,或者可以包括存放数据模型的明文信息的内存地址,或者可以包括将数据模型的明文信息保存为文件形式后的文件路径和文件名称等,因此任务提交模块调用数据模型管理模块清理数据模型信息时,可以基于将保存在客户端的数据模型的明文本身清除,或者将客户端用于存储数据模型的明文信息的文件清除,或者可以将客户端用于存储数据模型的明文信息的内存空间清空。

[0081] 此外,作为一种可选的实施例,进行环境安全验证,可以包括以下至少之一。对客

户端进行环境安全验证，以保证在安全的环境中对数据模型的密文执行解密操作。对云服务端进行环境安全验证，以保证在安全的环境中运行数据模型。对客户端与云服务端之间的通信信道进行环境安全验证，以保证数据模型在传输过程中不被泄露。

[0082] 具体地，环境安全验证模块负责接收任务提交模块的验证请求，对包括客户端系统、所有的服务端系统以及客户端系统与所有服务端系统之间的通信信道进行基于预设规则模板的比较验证。只有客户端系统、所有的服务端系统、以及客户端系统与所有的服务端系统之间通信信道都通过环境安全验证的情况下，才向任务提交模块返回环境安全验证通过的结果。在任意一个主机系统，或者其承载的应用程序不符合任何一项规则模板的验证的情况下，则向任务提交模块返回环境安全验证不通过的结果。

[0083] 应该理解，客户端程序发起数据处理和数据分析任务时需要调用的数据模型，可以存储在客户端系统的文件系统中。服务端系统可以包括多个应用主机系统，共同提供大数据运算处理的功能组件。多个主机系统运行大数据计算软件系统，构成大数据系统(大数据平台)。基于客户端提交的计算服务请求，大数据系统接收来自客户端的数据模型，按照数据模型提供的方法逻辑进行数据分析运算并返回对应的处理结果。为了保护数据模型，在本公开实施例中，服务端系统支持敏感日志控制设置，同时支持UI的访问控制权限。正常情况下，服务端在基于预设规则模板设定的环境下工作，在整个运算过程中，基于该预设规则模板的配置要求，不存储、打印输出与数据模型关联的信息，运算完成后向客户端程序返回运算结果。异常情况下，服务端的计算环境可能与预设规则模板的配置要求不符，这样可能导致数据模型不安全，因此需要全面监控每一个服务端节点。

[0084] 如图4A所示，环境安全验证模块包括环境安全验证主程序、环境安全验证客户端程序和环境安全验证服务端程序。其中，环境安全验证主程序运行在客户端系统中，环境安全验证客户端程序也运行客户端系统中，环境安全验证服务端程序运行在各个服务端操作系统中，即每个服务端主机运行一个环境安全验证服务端程序。

[0085] 具体地，环境安全验证主程序向环境安全验证客户端程序和环境安全验证服务端程序发送安全计算环境验证的请求消息。环境安全验证客户端程序收到请求后，按照预先配置的客户端系统规则模板执行安全计算环境验证的方法逻辑，并收集基于客户端系统客户端系统规则模板在客户端系统实际设置的配置参数，将收集的配置参数与预设的配置参数比对。如果比对结果一致，则向环境安全验证主程序发送包括客户端计算环境验证通过的消息。否则，如果比对结果不一致，则向环境安全验证主程序发送包括客户端计算环境验证不通过的消息。

[0086] 需要说明的是，在本公开实施例中，环境安全验证主程序收集整个环境包括所有环境安全验证客户端程序和所有环境安全验证服务端程序发送的安全计算环境验证结果后，判断所有的安全计算环境验证结果都为计算环境安全结果的消息(即验证通过)的情况下，向任务提交模块发送包括表征计算环境安全的安全计算环境验证返回消息。否则，向任务提交模块发送包括表征计算环境不安全的安全计算环境验证返回消息。

[0087] 具体地，在本公开实施例中，环境安全验证模块负责接收任务提交模块发起的验证请求，从预先配置的规则模板文件中提取配置信息以验证计算环境是否安全。规则模板包括客户端系统规则模板和服务端系统规则模板。客户端系统规则模板是用于验证运行客户端程序的客户端系统计算环境的安全验证标准。服务端系统规则模板是用于验证服务端

系统中各个服务应用程序计算环境的安全验证标准。

[0088] 进一步，作为一种可选的实施例，对客户端进行环境安全验证，包括：验证针对客户端的系统侦测操作是否已被禁止。

[0089] 在公开实施例中，为了保证客户端系统计算环境安全，可以禁止执行针对客户端系统的任何侦测操作。

[0090] 基于此，在验证客户端系统计算环境是否安全时，可以验证针对客户端的系统侦测操作是否已被禁止。

[0091] 更进一步，作为一种可选的实施例，验证针对客户端的系统侦测操作是否已被禁止，包括：通过配置文件或者配置文件的哈希值验证针对客户端的系统侦测操作是否已被禁止。

[0092] 此外，作为一种可选的实施例，对云服务端进行环境安全验证，包括以下至少之一：验证云服务端针对数据模型的日志生成功能是否已被关闭。验证云服务端是否已针对数据模型设置有日志加密操作。

[0093] 在公开实施例中，为了保证服务端系统计算环境安全，可以关闭云服务端的日志生成功能。或者，不关闭云服务端的日志生成功能，但是设置日志加密操作，即针对生成的日志进行加密。

[0094] 基于此，在验证服务端系统计算环境是否安全时，可以验证云服务端针对数据模型的日志生成功能是否已被关闭。或者，可以验证云服务端是否已针对数据模型设置有日志加密操作。

[0095] 具体地，云服务端接收来自客户端的服务请求，基于客户端提供的数据模型完成大数据计算后，向客户端返回计算结果。云服务端的环境安全监控模块运行在每个节点的操作系统层，可以定期基于预先配置的安全环境验证要求比对完成验证，包括验证针对数据模型生成的日志是否已经加密或者针对数据模型的日志生成功能是否已关闭。具体地，可以验证针对大数据平台(即对应的云服务节点)设置的当前配置文件是否与其预设配置文件一致。或者，通过计算云服务节点当前的配置文件的哈希值，以及其预设的配置文件的哈希值，并比较两个哈希值是否一致。如果两个哈希值一致，则判定为运行环境安全；如果两个哈希值不一致，则判定为运行环境不安全。完成云服务端环境安全验证并返回对应的验证结果。

[0096] 此外，作为一种可选的实施例，对客户端与云服务端之间的通信信道进行环境安全验证可以包括：验证客户端与云服务端之间的通信信道是否已被加密。

[0097] 在公开实施例中，为了保证客户端系统与服务端系统之间的通信环境安全，可以对客户端系统与服务端系统之间通信信道进行加密。

[0098] 基于此，在验证客户端与云服务端之间的通信环境是否安全时，可以验证客户端与云服务端之间的通信信道是否已被加密。

[0099] 示例性的，在本公开实施例中，基于数据模型的处理流程如下：(1)，任务提交模块使用客户端系统运行的大数据计算任务提交程序beeline，读取解密后的数据模型信息，向服务端系统发起数据模型计算服务请求，较优的，客户端系统通过加密通信信道向服务端应用模块发送包括数据模型的大数据计算任务；(2)，服务端应用模块通过内部组网形成的整体大数据计算服务系统，完成基于数据模型的计算任务后，向任务提交模块返回基于数

据模型的计算服务结果。

[0100] 以下结合附图并以一个具体实施例详细阐述环境安全验证的过程。如图4B所示，环境安全验证的过程如下：

[0101] 操作S401，任务提交模块向环境安全验证模块发送安全计算环境验证请求消息。具体地，可以向环境安全验证模块中的环境安全验证主程序发送安全计算环境验证请求消息。

[0102] 操作S402，环境安全验证模块中的环境安全验证主程序向环境安全验证客户端程序发送客户端安全计算环境验证请求消息。

[0103] 操作S403，环境安全验证客户端程序按照预设的客户端系统安全环境验证要求(包括客户端系统和服务端系统之间采用加密信道通信，禁止对客户端系统的操作系统执行系统侦测操作，等等)对客户端系统进行环境安全验证。如果验证表明客户端系统满足预设的安全环境验证要求，则生成表征客户端系统的计算环境安全的验证结果。否则，如果验证表明客户端系统不满足预设的安全环境验证要求，则生成表征客户端系统的计算环境不安全的验证结果。进一步，环境安全验证客户端程序向环境安全验证模块返回对应的客户端计算环境安全与否的验证结果。

[0104] 在本公开实施例中，上述提及的系统侦测操作可以包括sudo，find等操作。

[0105] 操作S404，客户端系统的环境安全监控客户端程序，可以定期执行安全计算环境验证操作，并将验证结果包括在客户端安全计算环境验证结果定期上报消息中发送给环境安全监控模块。

[0106] 需要说明的是，在本公开实施例中，环境安全监控客户端程序与前述的环境安全验证客户端程序可以是同一程序。环境安全监控模块与前述的环境安全验证模块可以是同一模块。

[0107] 操作S405，环境安全验证模块向每个环境安全验证服务端程序发送服务端安全计算环境验证请求消息。

[0108] 操作S406，环境安全验证服务端程序运行在每个服务器节点的操作系统层，接收来自环境安全验证模块的服务端安全计算环境验证请求消息，基于预先配置的安全环境验证要求比对完成验证，包括运行验证数据模型产生的日志是否已经加密，或者验证日志生成功能是否已关闭等。具体地，可以通过验证大数据平台当前的配置文件是否与预设的配置文件一致，或者通过验证各计算节点的配置文件的哈希值与预设的配置文件的哈希值是否一致，来确定日志是否已经加密或者日志生成功能是否已关闭。如果一致，则判定为计算环境安全；如果不一致，则判定为计算环境不安全。运行在每个计算节点的环境安全验证服务端程序执行同样的流程，产生安全计算环境验证结果后通过服务端安全计算环境验证结果消息向环境安全验证模块发送。

[0109] 操作S407，各服务端系统的环境安全监控客户端程序，可以定期执行安全计算环境验证操作，并将验证结果包括在服务端安全计算环境验证结果定期上报消息中发送给环境安全监控模块。

[0110] 需要说明的是，在本公开实施例中，环境安全监控服务端程序与前述的环境安全验证服务端程序可以是同一程序。

[0111] 操作S408，环境安全监控主程序，接收到来自环境安全监控客户端程序发送的客

户端系统计算环境验证结果，来自所有服务端系统节点的环境安全监控服务端程序发送的服务端系统计算环境验证结果，在确定所有计算环境验证结果均为表征计算环境安全的结果的情况下，判定为整个应用系统的计算环境安全。否则，判定为整个应用系统的计算环境不安全。

[0112] 需要说明的是，在本公开实施例中，环境安全监控主程序与前述的环境安全验证主程序可以是同一程序。

[0113] 操作S409，环境安全监控模块将应用系统计算环境验证结果包括在应用系统安全计算环境验证结果消息中向任务提交模块发送。

[0114] 需要说明的是，在本公开实施例中，环境安全监控模块与前述的环境安全验证模块可以是同一模块。

[0115] 操作S410，任务提交模块在确定应用系统计算环境安全的情况下，继续执行后续流程，在确定应用系统计算环境不安全的情况下，停止后续流程的执行。

[0116] 此外，作为一种可选的实施例，该方法还可以包括：在云服务端运行数据模型的过程中，定期进行环境安全验证。

[0117] 如图5所示，在本公开实施例中，该方法除了包括如图2所示的操作S201～S203之外，还可以包括操作S501。

[0118] 其中，图5所示的操作S201～S203与图2所示的操作S201～S203相同，在此不再赘述。

[0119] 在操作S501，在云服务端运行数据模型的过程中，定期进行环境安全验证。

[0120] 具体地，在本公开的一个实施例中，在客户端将数据模型发送至云服务端后，在云服务端运行数据模型的过程中，可以实时或者定期对云服务端进行环境安全验证。

[0121] 云服务端在运行数据模型的过程中，可能由于配置参数被修改等原因而导致计算环境变为不安全的环境，从而影响数据模型的安全。而在云服务端运行数据模型的过程中，通过定期验证计算环境是否安全，可以及时发现计算环境的变化并及时采取止损措施。

[0122] 优选地，对云服务端进行环境安全验证可以包括：定期对云服务端进行环境安全验证。与实时对云服务端进行环境安全验证相比，定期验证可以保证在及时发现计算环境的变化并及时采取止损措施的基础上，减少对云服务端计算资源的过度消耗。

[0123] 具体地，在本公开实施例中，对云服务端进行环境安全验证可以包括以下至少之一。验证云服务端针对数据模型的通信端口是否已被关闭或者已被限制；验证云服务端针对数据模型的日志生成功能是否已被关闭；验证云服务端是否已针对数据模型设置有日志加密操作；验证云服务端针对数据模型的数据保存功能是否已被关闭；验证云服务端是否已针对数据模型设置有数据加密操作；验证针对云服务端的系统侦测操作是否已被禁止。

[0124] 为了保证云服务端计算环境的安全，可以采取以下措施：

[0125] 方案1，直接关闭运行数据模型的云服务端对外的通信端口。

[0126] 显然，通过方案1可以保证日志信息、中间数据和最终数据、以及数据模型本身不被泄露或者不被非法复制。但是，是直接关闭对外通信端口也会给提交任务的客户端造成不便。

[0127] 方案2，限制除特定客户端之外的设备访问运行数据模型的云服务端的通信端口。

[0128] 其中，特定客户端为提交本次任务的客户端。显然，通过方案2不仅可以保证日志

信息、中间数据和最终数据、以及数据模型本身不被泄露或者不被非法复制，而且也不会给提交任务的客户端造成不便。

[0129] 方案3，验证云服务端针对数据模型的日志生成功能是否已被关闭。

[0130] 显然，通过方案3不生成日志可以保证数据模型安全，使得数据模型难以被泄露或者被非法复制。

[0131] 方案4，验证云服务端是否已针对数据模型设置有日志加密操作。

[0132] 显然，通过方案4，即使运行数据模型的云服务端的通信端口对外开放，或者日志生成功能处于开启状态，也可以阻止数据模型信息被轻易泄露出去或者被轻易复制。

[0133] 方案5，验证云服务端针对数据模型的数据保存功能是否已被关闭。

[0134] 显然，与方案3类似，通过方案5不保存运行数据模型而产生的数据也可以保证数据模型安全，使得数据模型难以被泄露或者被非法复制。

[0135] 方案6，验证云服务端是否已针对数据模型设置有数据加密操作。

[0136] 显然，通过方案6，即使运行数据模型产生数据，由于产生的数据已被加密，因此也可以阻止数据模型信息被轻易泄露出去或者被轻易复制。

[0137] 方案7，验证针对云服务端的系统侦测操作是否已被禁止。统侦测操作可以包括sudo，find等操作。

[0138] 作为一种可选的实施例，验证云服务端针对数据模型的通信端口是否已被关闭可以包括如下操作。

[0139] 通过配置文件或者配置文件的哈希值验证云服务端针对数据模型的通信端口是否已被关闭或已被限制。和/或

[0140] 通过客户端访问云服务端，以验证云服务端针对数据模型的通信端口是否已被关闭或已被限制。

[0141] 具体地，在本公开实施例中，为了保证数据模型安全，在预先设定的配置文件中，可以将运行数据模型的云服务端的通信接口设置为关闭状态。基于此，在云服务端运行过程中，可以定期或者实时获取当前的配置文件并将其与预设的配置文件比较。如果两个配置文件完全一致，则认为当前的计算环境时是安全的。否则，如果两个配置文件不完全一致，则认为当前的计算环境时是不安全的。类似地，除了比较两个配置文件本身是否一致之外，还可以计算两个配置文件的哈希值，并比较两个哈希值是否一致。如果两个哈希值完全一致，则认为当前的计算环境时是安全的。否则，如果两个哈希值不完全一致，则认为当前的计算环境时是不安全的。

[0142] 作为一种可选的实施例，验证针对云服务端的系统侦测操作是否已被禁止可以包括：通过配置文件或者配置文件的哈希值验证针对云服务端的系统侦测操作是否已被禁止。

[0143] 具体地，在本公开实施例中，为了保证数据模型安全，在预先设定的配置文件中，可以将运行数据模型的云服务端的计算环境配置为禁止执行系统侦测操作的状态。基于此，在云服务端运行过程中，可以定期或者实时获取当前的配置文件并将其与预设的配置文件比较。如果两个配置文件完全一致，则认为当前的计算环境时是安全的。否则，如果两个配置文件不完全一致，则认为当前的计算环境时是不安全的。类似地，除了比较两个配置文件本身是否一致之外，还可以计算两个配置文件的哈希值，并比较两个哈希值是否一致。

如果两个哈希值完全一致，则认为当前的计算环境时是安全的。否则，如果两个哈希值不完全一致，则认为当前的计算环境时是不安全的。

[0144] 作为一种可选的实施例，验证云服务端针对数据模型的数据保存功能是否已被关闭可以包括以下至少之一：通过配置文件或者配置文件的哈希值验证云服务端针对数据模型的数据保存功能是否已被关闭；验证云服务端针对数据模型保存在数据是否为空；验证云服务端针对数据模型的数据保存量是否有增长。

[0145] 应该理解，在本公开实施例中，通过配置文件或者配置文件的哈希值验证云服务端针对数据模型的数据保存功能是否已被关闭，与前述实施例中通过配置文件或者配置文件的哈希值验证针对云服务端的系统侦测操作是否已被禁止，以及通过配置文件或者配置文件的哈希值验证云服务端针对数据模型的通信端口是否已被关闭或已被限制的方法类似，在此不再赘述。

[0146] 作为一种可选的实施例，该方法还可以包括：响应于环境安全验证未通过，向云服务端发送任务终止请求，以便停止在云服务端运行数据模型。

[0147] 具体地，在运行数据模型的过程中，如果通过监控计算环境发现存在任何不安全因素，则客户端可以直接向对应的云服务端发送终止任务的请求以便及时终止当前的数据处理任务，并停止运行当前的数据模型，达到保护数据模型安全的目的。

[0148] 图6示意性示出了根据本公开实施例的保护数据模型的处理装置的框图。

[0149] 如图6所示，保护数据模型的处理装置600包括验证模块601、解密模块602和发送模块603。该处理装置可以执行上面参考方法实施例部分描述的方法，在此不再赘述。

[0150] 具体地，验证模块601，用于进行环境安全验证。

[0151] 解密模块602，用于响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文。

[0152] 发送模块603，用于将所述数据模型的明文信息发送至云服务端，以便在所述云服务端运行所述数据模型来完成对应的数据处理任务。

[0153] 通过本公开实施例，由于在解密数据模型、传输数据模型的明文信息以及运行数据模型之前采用了环境安全验证的技术手段，因而可以保护数据模型，防止其在解密过程中、或者传输过程中、或者运行过程中被泄露或者被复制。

[0154] 此外，在本公开实施例中，在将传统的基于数据模型的应用系统迁移到第三方云环境后，即可以实现云主机运维不受影响(继续由第三方对云主机进行维护)，又可以保护应用系统中的数据模型安全。同时在交付云服务端部署、运营的过程中，能够遵从开源软件License协议的要求。此外，本公开实施例并没有对数据模型本身的方法逻辑进行改造，因而实现了在最低成本改造的基础上，达到最优性价比的安全效果。

[0155] 作为一种可选的实施例，该装置还可以包括：清除模块，用于在将所述数据模型的明文信息发送至所述云服务端之后，或者在所述云服务端开始运行所述所述数据模型之后，将保存在所述客户端的所述数据模型的明文信息清除。

[0156] 作为一种可选的实施例，上述清除模块可以用于执行以下操作中的至少之一：将保存在上述客户端的上述数据模型的明文本身清除；将上述客户端用于存储上述数据模型的明文信息的文件清除；将上述客户端用于存储上述数据模型的明文信息的内存空间清空。

[0157] 作为一种可选的实施例，上述验证模块包括以下单元中的至少之一：第一验证单元，用于对所述客户端进行环境安全验证；第二验证单元，用于对所述云服务端进行环境安全验证；第三验证单元，用于对所述客户端与所述云服务端之间的通信信道进行环境安全验证。

[0158] 作为一种可选的实施例，上述第一验证单元还用于：验证针对所述客户端的系统侦测操作是否已被禁止。

[0159] 作为一种可选的实施例，上述第一验证单元还用于：通过配置文件或者配置文件的哈希值验证针对所述客户端的系统侦测操作是否已被禁止。

[0160] 作为一种可选的实施例，上述第二验证单元还用于执行以下操作中的至少之一：验证所述云服务端针对所述数据模型的日志生成功能是否已被关闭；验证所述云服务端是否已针对所述数据模型设置有日志加密操作。

[0161] 作为一种可选的实施例，上述第三验证单元还用于：验证所述对所述客户端与所述云服务端之间的通信信道是否已被加密。

[0162] 作为一种可选的实施例，上述验证模块还用于：在所述云服务端运行所述数据模型的过程中，定期进行环境安全验证。

[0163] 具体地，上述验证模块还用于在所述云服务端运行所述数据模型的过程中，对所述云服务端进行环境安全验证。

[0164] 作为一种可选的实施例，上述验证模块还用于：定期对所述云服务端进行环境安全验证。

[0165] 作为一种可选的实施例，上述验证模块还用于执行以下操作中的至少之一：验证所述云服务端针对所述数据模型的通信端口是否已被关闭或者已被限制；验证所述云服务端针对所述数据模型的日志生成功能是否已被关闭；验证所述云服务端是否已针对所述数据模型设置有日志加密操作；验证所述云服务端针对所述数据模型的数据保存功能是否已被关闭；验证所述云服务端是否已针对所述数据模型设置有数据加密操作；验证针对所述云服务端的系统侦测操作是否已被禁止。

[0166] 作为一种可选的实施例，上述验证模块还用于：通过配置文件或者配置文件的哈希值验证所述云服务端针对所述数据模型的通信端口是否已被关闭或已被限制；和/或通过客户端访问所述云服务端，以验证所述云服务端针对所述数据模型的通信端口是否已被关闭或已被限制。

[0167] 作为一种可选的实施例，上述验证模块还用于：通过配置文件或者配置文件的哈希值验证针对所述云服务端的系统侦测操作是否已被禁止。

[0168] 作为一种可选的实施例，上述验证模块还用于执行以下操作中的至少之一：通过配置文件或者配置文件的哈希值验证所述云服务端针对所述数据模型的数据保存功能是否已被关闭；验证所述云服务端针对所述数据模型保存在数据是否为空；验证所述云服务端针对所述数据模型的数据保存量是否有增长。

[0169] 作为一种可选的实施例，上述发送模块还用于：响应于环境安全验证未通过，向所述云服务端发送任务终止请求，以便停止在所述云服务端运行所述数据模型。

[0170] 需要说明的是，本公开的装置部分的实施例与本共公开的方法部分的实施例对应类似，并且所达到的技术效果也对应类似，在此不再赘述。

[0171] 根据本公开的实施例的模块、单元中的任意多个、或其中任意多个的至少部分功能可以在一个模块中实现。根据本公开实施例的模块、单元中的任意一个或多个可以被拆分成多个模块来实现。根据本公开实施例的模块、单元中的任意一个或多个可以至少被部分地实现为硬件电路，例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC)，或可以通过对电路进行集成或封装的任何其他的合理方式的硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，根据本公开实施例的模块、单元中的一个或多个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

[0172] 例如，验证模块601、解密模块602和发送模块603中的任意多个可以合并在一个模块中实现，或者其中的任意一个模块可以被拆分成多个模块。或者，这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合，并在一个模块中实现。根据本公开的实施例，验证模块601、解密模块602和发送模块603中的至少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC)，或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者验证模块601、解密模块602和发送模块603中的至少一个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

[0173] 图7示意性示出了根据本公开实施例的电子设备的框图。图7示出的电子设备仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

[0174] 如图7所示，电子设备700包括处理器710、计算机可读存储介质720。该电子设备700可以执行根据本公开实施例的方法。

[0175] 具体地，处理器710例如可以包括通用微处理器、指令集处理器和/或相关芯片组和/或专用微处理器(例如，专用集成电路(ASIC))，等等。处理器710还可以包括用于缓存用途的板载存储器。处理器710可以是用于执行根据本公开实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

[0176] 计算机可读存储介质720，例如可以是非易失性的计算机可读存储介质，具体示例包括但不限于：磁存储装置，如磁带或硬盘(HDD)；光存储装置，如光盘(CD-ROM)；存储器，如随机存取存储器(RAM)或闪存；等等。

[0177] 计算机可读存储介质720可以包括计算机程序721，该计算机程序721可以包括代码/计算机可执行指令，其在由处理器710执行时使得处理器710执行根据本公开实施例的方法或其任何变形。

[0178] 计算机程序721可被配置为具有例如包括计算机程序模块的计算机程序代码。例如，在示例实施例中，计算机程序721中的代码可以包括一个或多个程序模块，例如包括721A、模块721B、……。应当注意，模块的划分方式和个数并不是固定的，本领域技术人员可以根据实际情况使用合适的程序模块或程序模块组合，当这些程序模块组合被处理器710执行时，使得处理器710可以执行根据本公开实施例的方法或其任何变形。

[0179] 根据本公开的实施例，验证模块601、解密模块602和发送模块603中的至少一个可

以实现为参考图7描述的计算机程序模块，其在被处理器710执行时，可以实现上面描述的相应操作。

[0180] 本公开还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储介质承载有一个或者多个程序，当上述一个或者多个程序被执行时，实现根据本公开实施例的方法。

[0181] 附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0182] 本领域技术人员可以理解，尽管已经参照本公开的特定示例性实施例示出并描述了本公开，但是本领域技术人员应该理解，在不背离所附权利要求及其等同物限定的本公开的精神和范围的情况下，可以对本公开进行形式和细节上的多种改变。因此，本公开的范围不应该限于上述实施例，而是应该不仅由所附权利要求来进行确定，还由所附权利要求的等同物来进行限定。

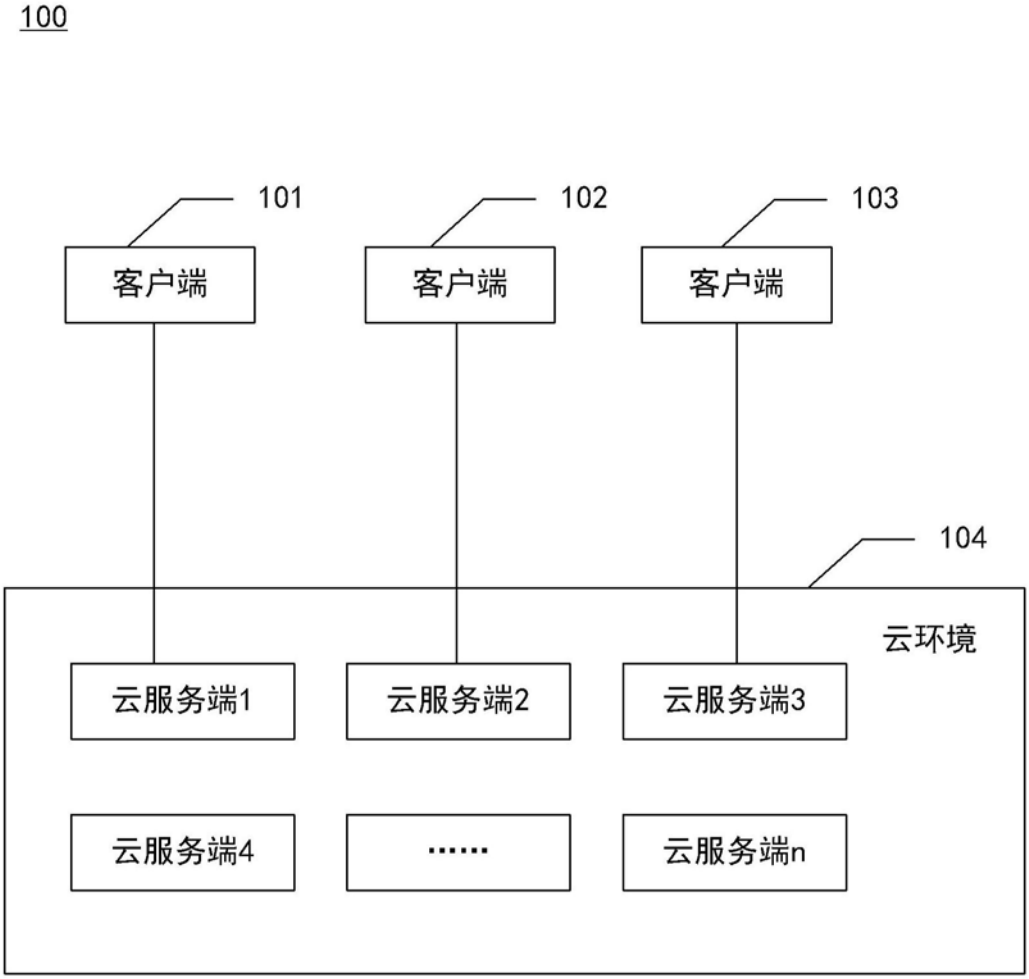

100
101
102
103
客户端
客户端
客户端
104
云环境
云服务端1
云服务端2
云服务端3
云服务端4
.....
云服务端n

图1A

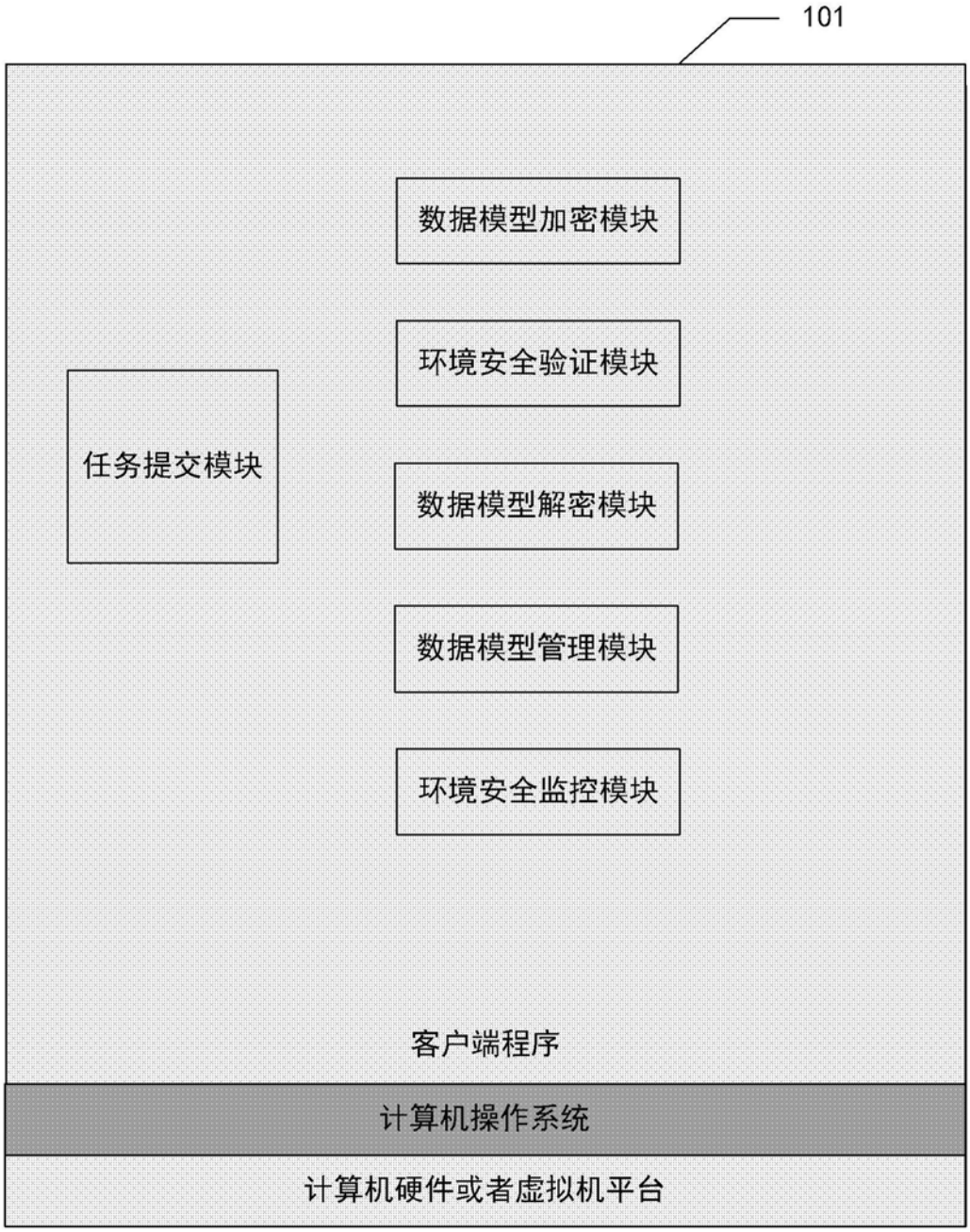

101
数据模型加密模块
环境安全验证模块
任务提交模块
数据模型解密模块
数据模型管理模块
环境安全监控模块
客户端程序
计算机操作系统
计算机硬件或者虚拟机平台

图1B


环境安全监控模块
服务端应用模块
计算机操作系统
计算机硬件或者虚拟机平台

图1C

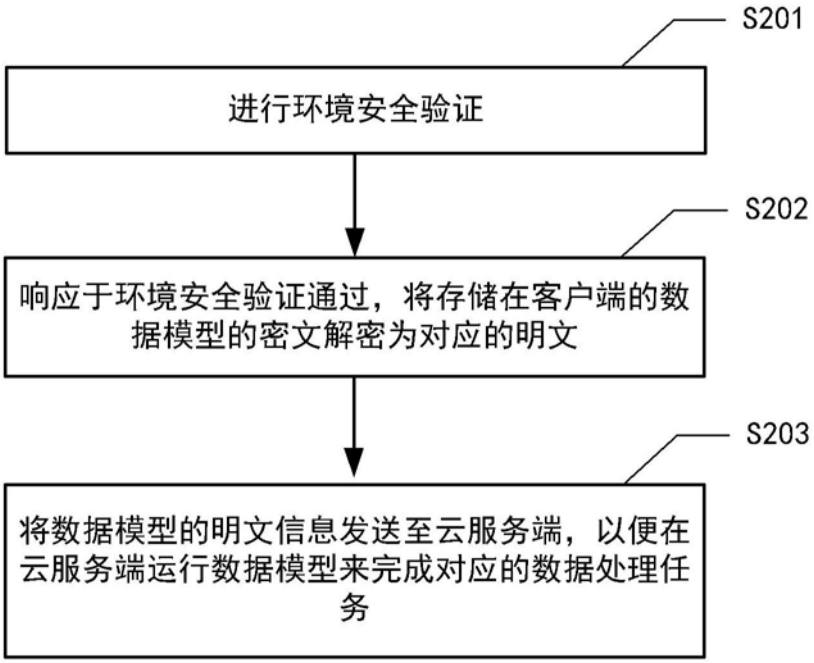

S201
进行环境安全验证
S202
响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文
S203
将数据模型的明文信息发送至云服务端，以便在云服务端运行数据模型来完成对应的数据处理任务

图2

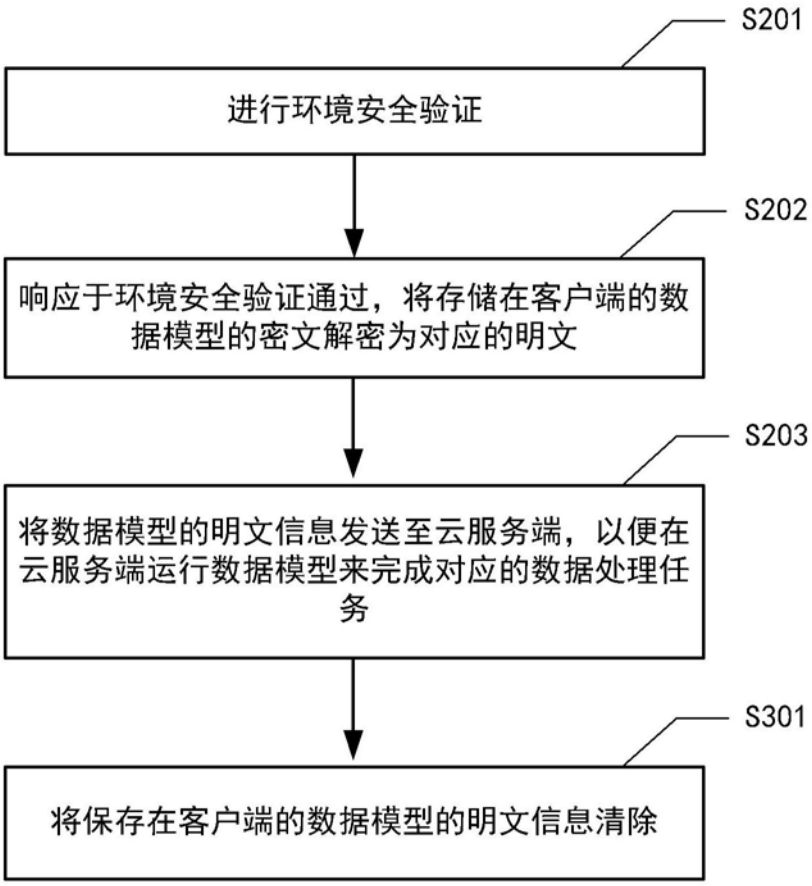

S201
进行环境安全验证
S202
响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文
S203
将数据模型的明文信息发送至云服务端，以便在云服务端运行数据模型来完成对应的数据处理任务
S301
将保存在客户端的数据模型的明文信息清除

图3

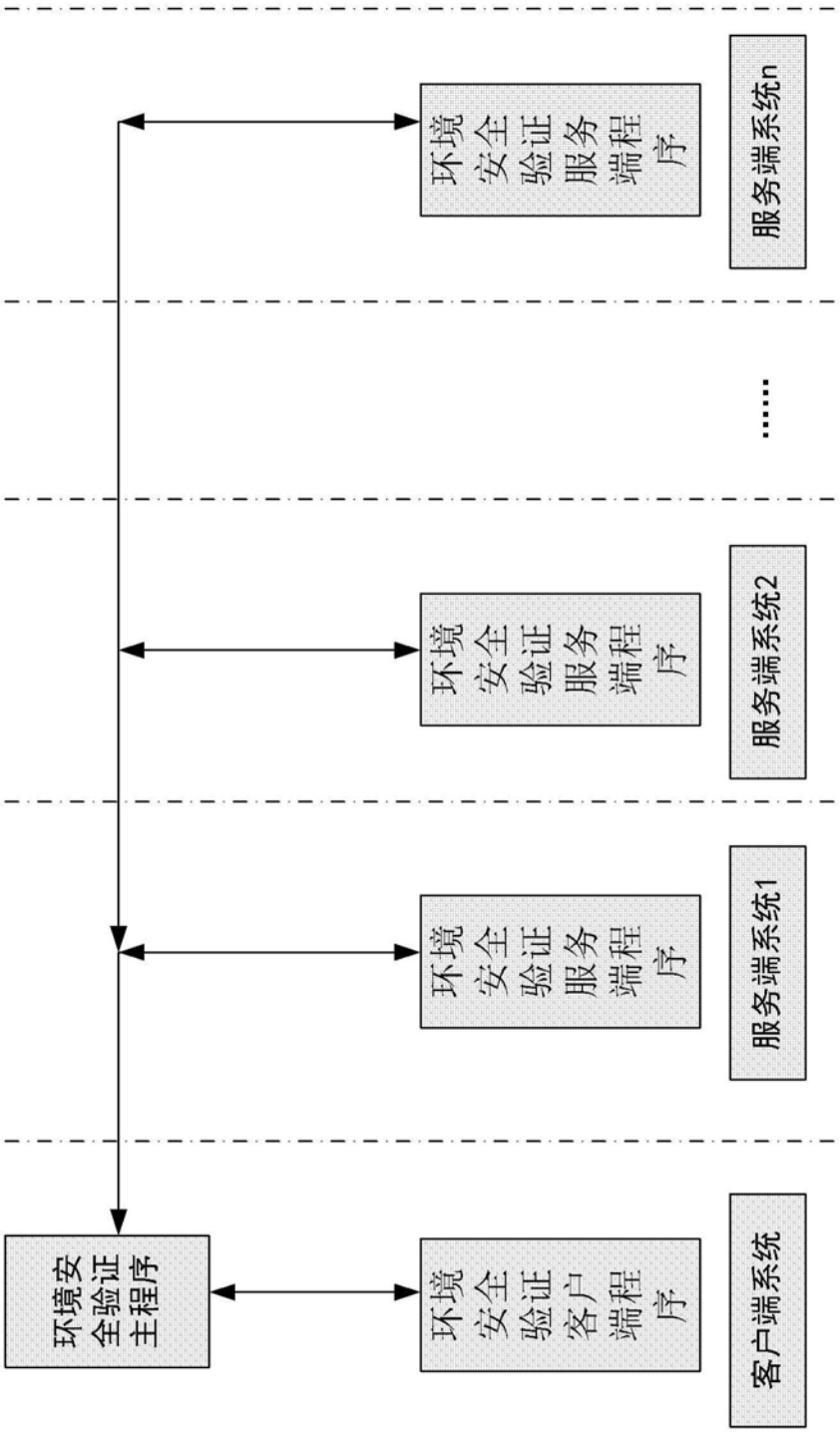

环境安全验证主程序
环境安全验证客户端程序
客户端系统
环境安全验证服务端程序
服务端系统1
环境安全验证服务端程序
服务端系统2
.....
环境安全验证服务端程序
服务端系统n

图4A

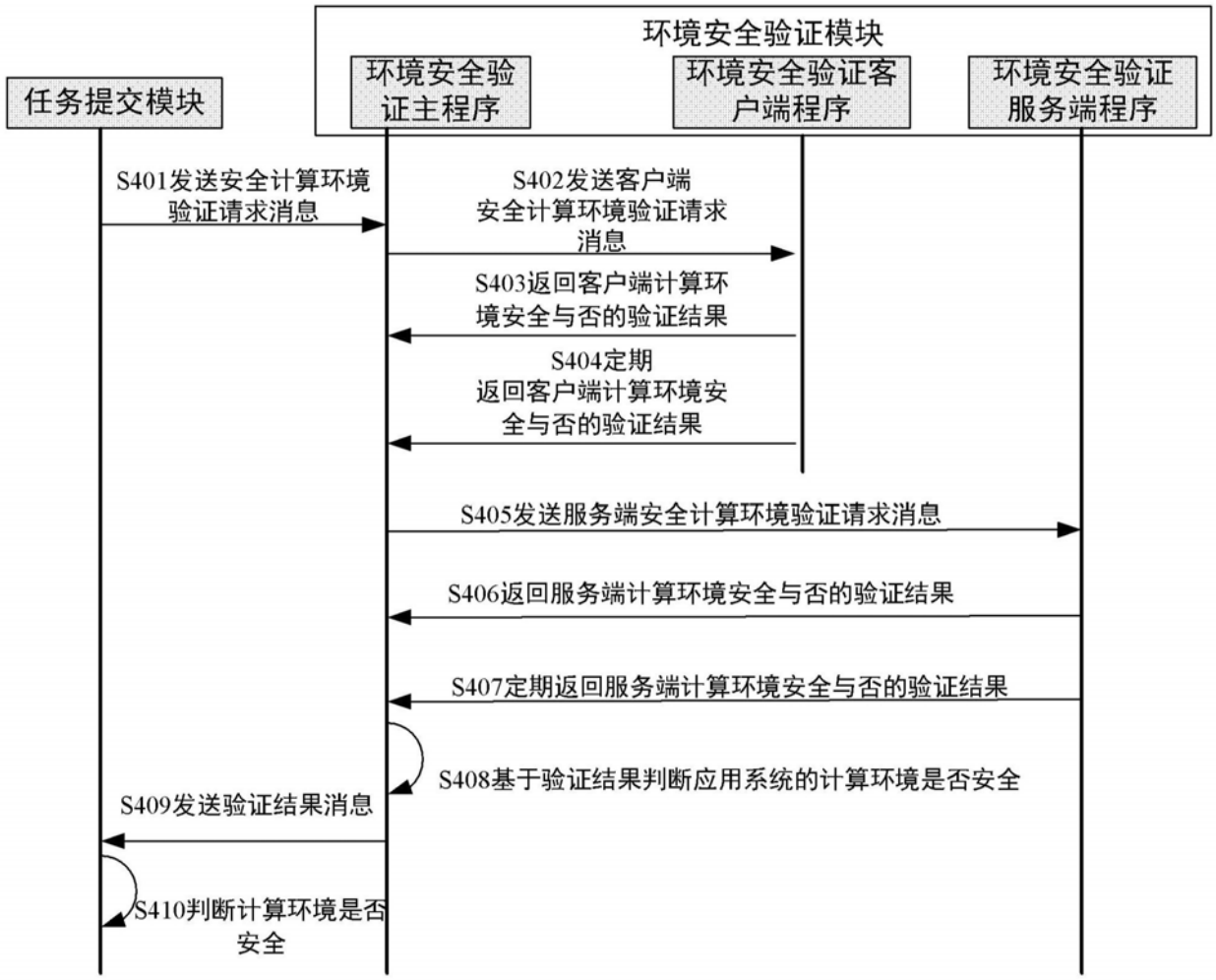

环境安全验证模块
任务提交模块
环境安全验证主程序
环境安全验证客户端程序
环境安全验证服务端程序
S401发送安全计算环境验证请求消息
S402发送客户端安全计算环境验证请求消息
S403返回客户端计算环境安全与否的验证结果
S404定期返回客户端计算环境安全与否的验证结果
S405发送服务端安全计算环境验证请求消息
S406返回服务端计算环境安全与否的验证结果
S407定期返回服务端计算环境安全与否的验证结果
S408基于验证结果判断应用系统的计算环境是否安全
S409发送验证结果消息
S410判断计算环境是否安全

图4B

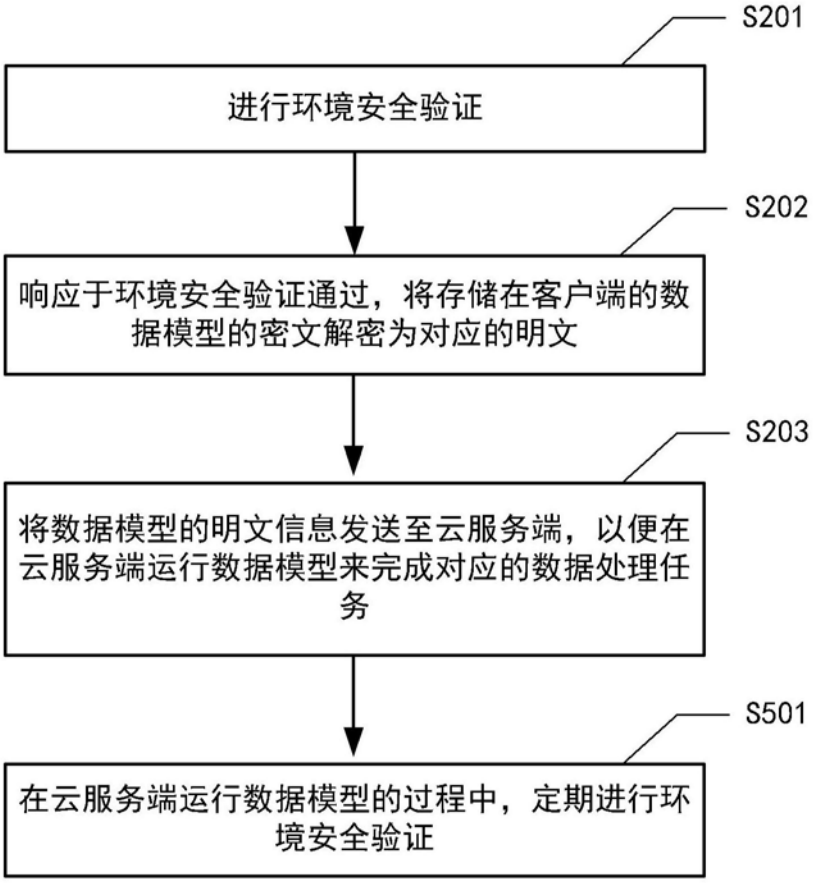

S201
进行环境安全验证
S202
响应于环境安全验证通过，将存储在客户端的数据模型的密文解密为对应的明文
S203
将数据模型的明文信息发送至云服务端，以便在云服务端运行数据模型来完成对应的数据处理任务
S501
在云服务端运行数据模型的过程中，定期进行环境安全验证

图5

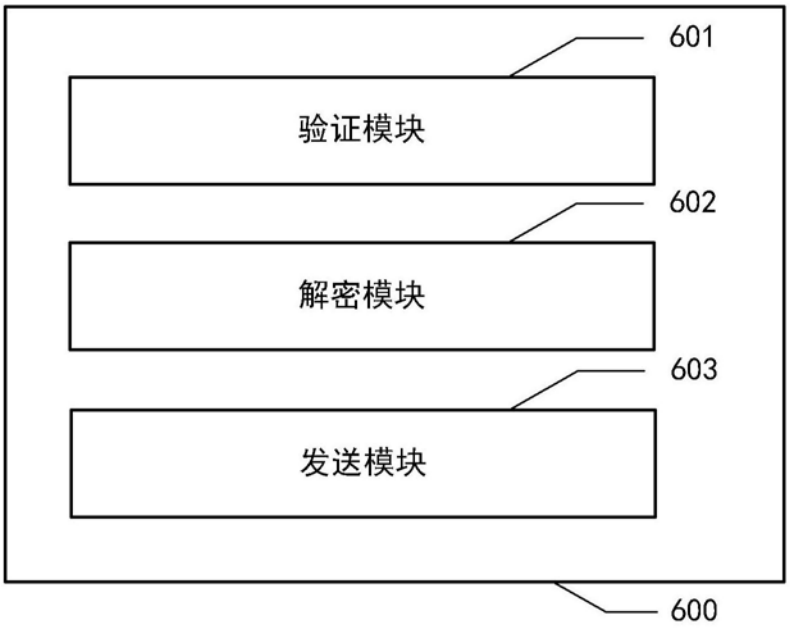

601
验证模块
602
解密模块
603
发送模块
600

图6

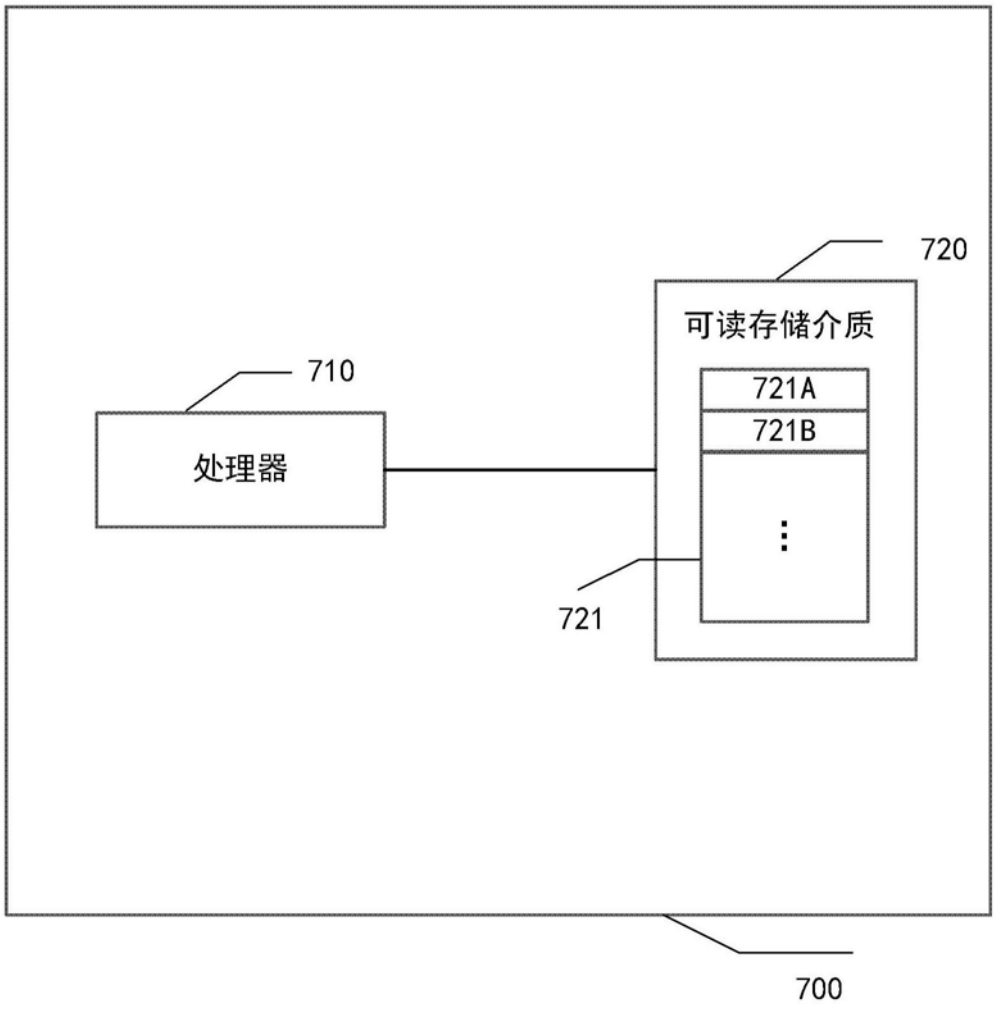


图7