(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115664839 B
(45)授权公告日 2023.04.11

(21)申请号 202211420547.8

(22)申请日 2022.11.15

(65)同一申请的已公布的文献号
申请公布号 CN 115664839 A

(43)申请公布日 2023.01.31

(73)专利权人 富算科技(上海)有限公司
地址 200135 上海市浦东新区自由贸易试验区浦东大道1200号2层A区

(72)发明人 尤志强 卞阳

(74)专利代理机构 上海弼兴律师事务所 31283
专利代理师 罗朗 林嵩

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 112395642 A,2021.02.23
CN 113282960 A,2021.08.20
CN 114650179 A,2022.06.21
CN 115296859 A,2022.11.04
US 2011219423 A1,2011.09.08

审查员 姜云杰

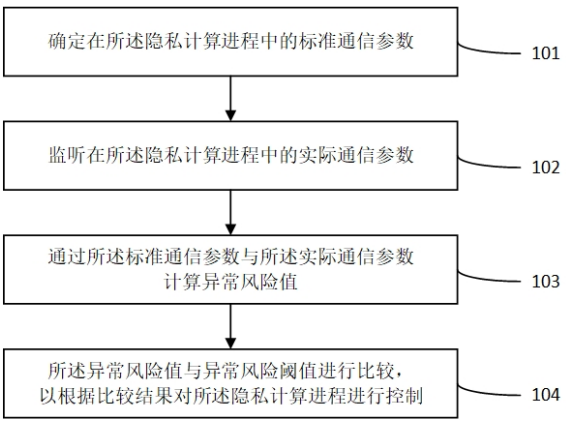
权利要求书2页 说明书9页 附图4页

(54)发明名称

隐私计算进程的安全监控方法、装置、设备、介质

(57)摘要

本公开为隐私计算进程的安全监控方法、装置、设备、介质。适用于多方安全计算中多个参与节点中的任一参与节点，其中方法包括：确定在所述隐私计算进程中的标准通信参数；监听在所述隐私计算进程中的实际通信参数；通过所述标准通信参数与所述实际通信参数计算异常风险值；所述异常风险值与异常风险阈值进行比较，以根据比较结果对所述隐私计算进程进行控制。本公开实现了对隐私计算进程的安全监控。有效地对隐私计算进程的安全性进行监测，并且能在监测到异常情况的第一时间处理。



CN 115664839 B

1.一种隐私计算进程的安全监控方法,适用于多方安全计算中多个参与节点中的任一参与节点,其特征在于,所述安全监控方法包括:

确定在所述隐私计算进程中的标准通信参数;

监听在所述隐私计算进程中的实际通信参数;

通过所述标准通信参数与所述实际通信参数计算异常风险值;

所述异常风险值与异常风险阈值进行比较,以根据比较结果对所述隐私计算进程进行控制。

2.根据权利要求1所述的隐私计算进程的安全监控方法,其特征在于,所述多个参与节点中的任一参与节点部署有相同的隐私计算的任务脚本;所述确定在所述隐私计算进程中的标准通信参数包括:

解析部署于本地的所述任务脚本以获取所述任务脚本的算法逻辑;

对所述任务脚本中的实际执行的所述算法逻辑进行所述标准通信参数的计算。

3.根据权利要求1所述的隐私计算进程的安全监控方法,其特征在于,所述实际通信参数为与其他参与节点之间交互的通信活动信息。

4.根据权利要求1所述的隐私计算进程的安全监控方法,其特征在于,所述计算异常风险值包括:

计算所述标准通信参数与所述实际通信参数的偏移量,并将所述偏移量确定为所述异常风险值;

和/或,通过预先训练的预警模型计算所述异常风险值。

5.根据权利要求4所述的隐私计算进程的安全监控方法,其特征在于,所述计算所述标准通信参数与所述实际通信参数的偏移量包括:

识别所述标准通信参数与所述实际通信参数的类型;

将同类型的所述标准通信参数与所述实际通信参数进行所述偏移量的计算。

6.根据权利要求4所述的隐私计算进程的安全监控方法,其特征在于,所述通过预先训练的预警模型计算所述异常风险值包括:

获取所述实际通信参数;

将所述实际通信参数输入所述预警模型,其中,所述预警模型预先采用正负样本数据进行训练;

经所述预警模型对输入的实际通信参数进行预警判断,获取所述实际通信参数的所述异常风险值。

7.根据权利要求1-6中任一项所述的隐私计算进程的安全监控方法,其特征在于,所述异常风险值与异常风险阈值进行比较,以根据比较结果对所述隐私计算进程进行控制包括:

若所述异常风险值不超出所述异常风险阈值,则判定为正常情况,所述隐私计算进程继续运行;

若所述异常风险值超出所述异常风险阈值,则判定为异常情况,终止所述隐私计算进程。

8.一种隐私计算进程的安全监控装置,其特征在于,包括:

初始模块,用于确定在所述隐私计算进程中的标准通信参数;

监听模块，用于监听在所述隐私计算进程中的实际通信参数；

识别模块，用于通过所述标准通信参数与所述实际通信参数计算异常风险值；

控制模块，用于所述异常风险值与异常风险阈值进行比较，以根据比较结果对所述隐私计算进程进行控制。

9.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至7任一项所述的隐私计算进程的安全监控方法。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至7任一项所述的隐私计算进程的安全监控方法。

隐私计算进程的安全监控方法、装置、设备、介质

技术领域

[0001] 本公开涉及隐私计算领域，尤其涉及一种隐私计算进程的安全监控方法、装置、设备、介质。

背景技术

[0002] 隐私计算是用于保护数据本身不对外泄露的前提下实现数据分析计算的技术集合，达到对数据“可用不可见”的目的。隐私计算的加密机制能够增强对于数据的保护、降低数据泄露风险。虽然隐私计算技术是应数据保护需求所产生的，但如何能够确保隐私计算技术确实达到了保护数据的目的，是目前业内的难题。但不管是哪种隐私计算方案，都会面临安全性监控的现实需求。

[0003] 当前业内采用的方式主要是事先理论论证和事后数据检测两种方案。前者是在执行隐私计算任务之前进行严格的安全原理论证，从原理上证明隐私计算技术达到了可证明安全的目标。然而理论论证不能保证真实执行的隐私计算任务是严格按照理论所规定的算法流程执行的；另一方面，后者是隐私计算任务执行之后的数据检测方式，也并不能达到保护数据不泄露的目的。当计算进程中存在恶意行为时由于是滞后处理，实际的数据泄露已经产生。因此这两类方案都不能有效地对隐私计算进程的安全性进行监测，也不能在监测到异常情况的第一时间处理。

发明内容

[0004] 本公开要解决的问题是为了克服现有技术中不能有效地对隐私计算进程的安全性进行监测，也不能在监测到异常情况的第一时间处理的缺陷，提供一种隐私计算进程的安全监控方法、装置、设备、介质。

[0005] 本公开是通过下述技术方案来解决上述技术问题：

[0006] 第一方面，提供一种隐私计算进程的安全监控方法，适用于多方安全计算中多个参与节点中的任一参与节点，所述安全监控方法包括：

[0007] 确定在所述隐私计算进程中的标准通信参数；

[0008] 监听在所述隐私计算进程中的实际通信参数；

[0009] 通过所述标准通信参数与所述实际通信参数计算异常风险值；

[0010] 所述异常风险值与异常风险阈值进行比较，以根据比较结果对所述隐私计算进程进行控制。

[0011] 可选地，所述多个参与节点中的任一参与节点部署有相同的隐私计算的任务脚本；所述确定在所述隐私计算进程中的标准通信参数包括：

[0012] 解析部署于本地的所述任务脚本以获取所述任务脚本的算法逻辑；

[0013] 对所述任务脚本中的实际执行的所述算法逻辑进行所述标准通信参数的计算。

[0014] 可选地，所述实际通信参数为与其他参与节点之间交互的通信活动信息。

[0015] 可选地，所述计算异常风险值包括：

[0016] 计算所述标准通信参数与所述实际通信参数的偏移量，并将所述偏移量确定为所述异常风险值；

[0017] 和/或

[0018] 通过预先训练的预警模型计算所述异常风险值。

[0019] 可选地，所述计算所述标准通信参数与所述实际通信参数的偏移量包括：

[0020] 识别所述标准通信参数与所述实际通信参数的类型；

[0021] 将同类型的所述标准通信参数与所述实际通信参数进行所述偏移量的计算。

[0022] 可选地，所述通过预先训练的预警模型计算所述异常风险值包括：

[0023] 获取所述实际通信参数；

[0024] 将所述实际通信参数输入所述预警模型，其中，所述预警模型预先采用正负样本数据进行训练；

[0025] 经所述预警模型对输入的实际通信参数进行预警判断，获取所述实际通信参数的所述异常风险值。

[0026] 可选地，所述异常风险值与异常风险阈值进行比较，以根据比较结果对所述隐私计算进程进行控制包括:

[0027] 若所述异常风险值不超出所述异常风险阈值，则判定为正常情况，所述隐私计算进程继续运行；

[0028] 若所述异常风险值超出所述异常风险阈值，则判定为异常情况，终止所述隐私计算进程。

[0029] 第二方面，提供一种隐私计算进程的安全监控装置，包括：

[0030] 初始模块，用于确定在所述隐私计算进程中的标准通信参数；

[0031] 监听模块，用于监听在所述隐私计算进程中的实际通信参数；

[0032] 识别模块，用于通过所述标准通信参数与所述实际通信参数计算异常风险值；

[0033] 控制模块，用于所述异常风险值与异常风险阈值进行比较，以根据比较结果对所述隐私计算进程进行控制。

[0034] 第三方面，提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述任一项所述的隐私计算进程的安全监控方法。

[0035] 第四方面，提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述任一项所述的隐私计算进程的安全监控方法。

[0036] 本公开的积极进步效果在于：

[0037] 本公开的安全监控方法实现了对隐私计算进程的安全监控。有效地对隐私计算进程的安全性进行监测，并且能在监测到异常情况的第一时间处理。

附图说明

[0038] 图1为本公开一示例性实施例提供的一种隐私计算进程的安全监控方法流程图；

[0039] 图2为本公开一示例性实施例提供的一种隐私计算加法算子的流程图；

[0040] 图3为本公开另一个示例性实施例提供的一种隐私计算进程的安全监控方法流程图；

[0041] 图4为本公开一示例性实施例提供的一种隐私计算进程的安全监控装置的模块示意图；

[0042] 图5为本公开一示例性实施例提供的一种电子设备的结构示意图。

具体实施方式

[0043] 以下结合附图对本公开的示范性实施例做出说明，其中包括本公开实施例的各种细节以助于理解，应当将它们认为仅仅是示范性的。因此，本领域普通技术人员应当认识到，可以对这里描述的实施例做出各种改变和修改，而不会背离本公开的范围和精神。同样，为了清楚和简明，以下的描述中省略了对公知功能和结构的描述。

[0044] 本公开的技术方案适用于多方安全计算中多个参与节点中的任一参与节点。本公开一示例性实施例提供一种隐私计算进程的安全监控方法，如图1和图3所示，该方法包括以下步骤：

[0045] 步骤101、确定在隐私计算进程中的标准通信参数。

[0046] 多个参与节点中的任一参与节点部署有相同的隐私计算的任务脚本。参与节点会解析部署于本地的任务脚本以获取任务脚本的算法逻辑，进而对任务脚本中的实际执行的算法逻辑进行标准通信参数的计算。

[0047] 对于任一隐私计算任务，在任务进程的初始阶段，各参与节点会同步任务脚本执行所需的数据元信息描述，其中数据元信息包括：数据类型、数据的shape大小。另外，各参与节点会对任务脚本进行解析，解析任务中所涉及的各类隐私计算的算子，其中算子包括：加法算子、矩阵乘法算子、中位数计算算子、比较算子、排序算子。基于算子理论值计算公式，生成对应的标准通信参数，其中标准通信参数包括：各个阶段的通信量、通信次数、通信数据shape大小、以及对应的阶段累积通信参数信息。

[0048] 其中，对于脚本的同步，是各参与节点对自己参与的执行内容进行同步。例如，一个隐私计算的任务脚本包含下述5各部分，且有A、B、C三个节点参与计算：

[0049] 001:A执行部分；

[0050] 002:B执行部分；

[0051] 003:C执行部分；

[0052] 004:C执行部分；

[0053] 005:A执行部分。

[0054] 同步后，ABC三方同步的内容分别为：

[0055] A:001,005；

[0056] B:002；

[0057] C:003,004。

[0058] A、B、C三个节点分别对各自同步的内容，通过算子理论值计算规则，计算出对应的标准通信参数。即当一个算子逻辑确定的时候，其通信次数等信息就可以被确定，这些确定的信息就是标准通信参数。

[0059] 图2所示是一种隐私计算的加法算子的流程图，在一个实施例中，参与节点为A方和B方，实现的是A方数据x和B方数据y的安全求和操作。假设x和y的数据类型都是int64，且x和y的shape大小都为(100,5)，其中(100,5)表示行列分别为100行和5列的矩阵数据。步骤

包括：

[0060] 步骤201、A方将本地数据x拆分为x1和x2两个分片数据，x1一般使用随机数生成，x2则通过x-x1生成。

[0061] 其中，若本地数据的shape大小确定，则其他分片数据shape大小也可以确定。例如x的数据shape大小为(100,5)，则生成的随机矩阵x1的shape大小也同样是(100,5)，通过x-x1得到的x2的shape大小也是(100,5)。其中，数据的类型确定，则数据占用内存大小也可以确定。例如x1的随机数生成数据类型选择为int64，则表示采用64bit来表示一个数，x1和x2的数据占用内存大小为100 * 5 * 8 = 4000字节，其中公式中的8表示的是8字节，也表示64bit。同理，y1和y2的shape大小同样为(100,5)，内存占用量也分别为4000字节。

[0062] 步骤202、A方向B方通信发送x2分片，B方向A方通信发送y1分片。根据步骤201所述，x2和y1的内存占用量分别为4000字节，则本步骤的通信次数为2次，总通信量为:4000字节 + 4000字节 = 8000字节。

[0063] 另外也可以通过分析日志的_Recv事件，获取标准通信参数。例如，如下表所示本步骤的两次通信对应了两次_Recv事件

[0064]

A	B	op逻辑说明
Mul		A方进行分片处理
Cast		
RandomUniformInt		
Sub		
	Mul	B方进行分片处理
	Cast	
	RandomUniformInt	
	Sub	
_Recv	_Send	加法算子
AddV2		
_Send	_Recv	
	AddV2	

[0065] 步骤203、在A、B两方各自执行计算结束后，产生分片数据z1和分片数据z2，二者进入数据恢复阶段。将A方的z1与B方z2发送给结果使用方R，例如z1和z2的数据shape大小同样为(100,5)，占用内存分别都为4000字节，本步骤涉及两次通信分别为:A方的z1发送到R方、B方的z2发送到R方，则本步骤的通信次数为2次，总通信量为8000字节。

[0066] 在本实施例中，加法算子的隐私计算进程中，发生4次通信，步骤202中通信两次，总通信量为8000字节，步骤203中通信两次，总通信量为8000字节，则整个隐私计算进程共产生16000字节的通信量，且每次通信数据shape大小都为(100,5)。以上参数为理想状态下的标准通信参数。

[0067] 因此当任一参与节点在隐私计算进程中，若想要获取额外信息，或窃取非任务本身所必需的额外数据，则会引起实际通信参数的变化与标准通信参数产生差异包括:通信

次数、通信量、通信数据shape大小产生差异波动。例如需要额外的通信次数获取更多信息；例如窃取的数据大小不符合正常任务本身限定的标准；例如数据通信量/网络流量超过了标准通信参数所设计的量级。

[0068] 步骤102、监听在隐私计算进程中的实际通信参数。

[0069] 本步骤中，监听针对隐私计算进程中的一切通信活动信息，包括实际通信参数，实际通信参数为与其他参与节点之间交互的通信活动信息。其中通信活动信息包括：如参与节点之间的通信量、通信次数、通信数据shape大小、通信的目标对象节点。

[0070] 监听的时机包括：隐私计算执行的过程的每次通信时、每一个时间步、算子计算阶段。

[0071] 监听的位置为数据产生和/或传输的路径上，包括：参与节点的网关、网卡端口、数据的发送和/或接收的端口。

[0072] 本步骤可以通过硬件与软件实现对实际通信参数的监听。硬件包括：通过网卡、路由器。通过对应的驱动程序，实时分析通信报文数据进行上报；软件包括：网关、抓包解析。比如采用类似wireshark软件的原理进行报文的实时解析验证。还可以通过改写HTTP/GRPC等网络协议代理，来监控并截取数据，例如，当参与节点作为请求方访问服务器时会发送一个请求，该请求先经过监听软件系统，然后再到服务器。服务器返回数据给请求方时，也会经过监听软件系统再到参与节点。由于所有的通信数据都会经过监听软件系统，因此监听软件系统能够截获这些数据，实现数据的抓包。然后基于抓包数据解析隐私计算进程的通信安全。

[0073] 步骤103、通过标准通信参数与实际通信参数计算异常风险值。

[0074] 在一个实施例中，计算标准通信参数与实际通信参数的偏移量，并将偏移量确定为异常风险值；

[0075] 在一个实施例中，通过预先训练的预警模型计算异常风险值；

[0076] 在一个实施例中，同时使用通过偏移量和预警模型所计算的异常风险值时，通过对二者的权重计算得到异常风险值。假设偏移量和预警模型计算的异常风险值分别为p1和p2，其权重分别设为a和b。其中a和b均为小于等于1的系数，且满足a+b=1。则异常风险值P的计算方式为：P=p1*a+p2*b。例如，当p1=0.7，p2=0.85，a=0.8，b=0.2时，P=0.7*0.8+0.85*0.2=0.73

[0077] 在一个实施例中，通过计算标准通信参数与实际通信参数的偏移量并将偏移量确定为异常风险值，包括：识别标准通信参数与实际通信参数的类型；将同类型的标准通信参数与实际通信参数进行偏移量的计算。

[0078] 其中标准通信参数与实际通信参数的类型包括：通信量、通信次数、通信数据shape大小、以及对应的阶段累积通信参数信息。其中偏移量的计算方式包括：

[0079] 标准通信参数与实际通信参数的绝对差，例如

$$\Delta = |\text{标准通信参数} - \text{实际通信参数}|;$$

[0080] 欧式距离计算，例如：$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$或 $d = \sqrt{\sum_{i=1}^{n}(x_i - y_i)}$；

[0081] 偏离度百分比，例如$P = |\text{标准通信参数} - \text{实际通信参数}| / \text{标准通信参数}$。

[0082] 例如，如下表所示隐私计算进程中的两次通信，关于通信量的实际通信参数和标准通信参数

[0083]

通信量	实际通信参数	标准通信参数
第1次	120M	100M
第2次	110M	100M

[0084] 则根据上述计算方法计算偏移量分别为：

[0085] 根据标准通信参数与实际通信参数的绝对差计算偏移量，

[0086] 第1次通信的偏移量为 $\Delta = |100-120| = 20M$，

[0087] 第2次通信的偏移量为 $\Delta = |100-110| = 10M$；

[0088] 根据欧式距离计算偏移量，两次通信的偏移量为，

[0089] $d = \sqrt{(100-120)^2+(100-110)^2} = \sqrt{20^2+10^2} = 22.36$；

[0090] 跟据偏离度百分比计算偏移量，

[0091] 第1次通信的偏移量为$P = |100-120|/100 = 0.2$，

[0092] 第2次通信的偏移量为$P = |100-110|/100 = 0.1$；

[0093] 在一个实施例中，通过预先训练的预警模型计算异常风险值，包括：获取实际通信参数；将实际通信参数输入预警模型，其中，预警模型预先采用正负样本数据进行训练；经预警模型对输入的实际通信参数进行预警判断，获取实际通信参数的异常风险值。

[0094] 其中，对预警模型训练所需要的训练集包括：模拟数据和现实业务中产生的真实数据。训练集在提取数据特征以后，进行训练。训练的算法包括：逻辑回归、基于树的模型、神经网络模型。预警模型训练完成以后，在进行预警判断时，预警模型的输入数据为实际通信参数，经过处理后预警模型的输出数据为异常风险值，异常风险值包括概率形式。

[0095] 标准通信参数的数据特征包括：通信次数、通信数据大小、通信量级、通信耗时、通信速率。实际通信参数的数据特征包括：通信次数、通信数据大小、通信量级、通信耗时、丢包率、通信重试次数。标准通信参数与实际通信参数的交叉特征包括：通信次数差异值、耗时比率。

[0096] 步骤104、异常风险值与异常风险阈值进行比较，以根据比较结果对隐私计算进程进行控制。

[0097] 在一个实施例中，若异常风险值不超出异常风险阈值，则判定为正常情况，隐私计算进程继续运行；若异常风险值超出异常风险阈值，则判定为异常情况，终止隐私计算进程。

[0098] 其中，异常风险阈值的设定，主要与实际通信网络环境、业务安全风险程度相关。设定的规则包括：(1)若实际通信网络环境较差，导致网络的重试次数、丢包率大于正常的情况下，异常风险阈值可以设置范围为10%-20%。反之，若在理想的通信网络环境下，则异常风险阈值可以设置在5%以内。

[0099] (2)若业务安全风险程度较高，对安全指标要求苛刻，则异常风险阈值可以设置为2-3%。反之，若安全指标要求不敏感，则异常风险阈值可以设置在20%-30%以内。

[0100] 考虑到异常风险阈值受多种因素影响，可通过权重计算设定阈值，公式如下：$t_v = \sum_i^n w_i * t_i$，其中i为实际需要考虑的因子，比如网络环境因子、业务安全风险因子等。

w为因子i所对应权重，t表示因子i在不同条件要求下对应的经验值。通过将多个条件加权求和得到最终的阈值。

[0101] 其中终止隐私计算进程包括：

[0102] 任务终止判断。判断依据异常风险值和异常风险阈值的比较，其中异常风险值通过偏移量获取或者通过通过预警模型运算获得，异常风险阈值的设定基于实验模拟的数据获得；

[0103] 任务终止执行。若任意节点的风险判断结果触发了任务终止条件，则终止隐私计算进程，包括：禁止节点之间的网关通信，或将异常状况上报给后端管理平台，由后端管理平台执行进程终止动作，或隐私计算进程的终端程序直接警告提示，并直接终止当前进程。根据风险程度不同，采取不同的任务终止执行方式；

[0104] 流程信息存证。最后将任务终止执行的流程相关信息进行存证，并生成相应分析报告，以供事后回溯核验。

[0105] 图4为本公开一示例性实施例提供的一种隐私计算进程的安全监控装置的模块示意图，该隐私计算进程的安全监控装置包括：

[0106] 初始模块41，用于确定在所述隐私计算进程中的标准通信参数；

[0107] 监听模块42，用于监听在所述隐私计算进程中的实际通信参数；

[0108] 识别模块43，用于通过所述标准通信参数与所述实际通信参数计算异常风险值；

[0109] 控制模块44，用于所述异常风险值与异常风险阈值进行比较，以根据比较结果对所述隐私计算进程进行控制。

[0110] 可选地，初始模块具体用于：

[0111] 多个参与节点中的任一参与节点部署有相同的隐私计算的任务脚本；确定在隐私计算进程中的标准通信参数包括：

[0112] 解析部署于本地的任务脚本以获取任务脚本的算法逻辑；

[0113] 对任务脚本中的实际执行的算法逻辑进行标准通信参数的计算。

[0114] 可选地，监听模块中的实际通信参数为与其他参与节点之间交互的通信活动信息。

[0115] 可选地，识别模块具体用于：

[0116] 计算异常风险值包括：

[0117] 计算标准通信参数与实际通信参数的偏移量，并将偏移量确定为异常风险值；

[0118] 和/或，通过预先训练的预警模型计算异常风险值。

[0119] 可选地，计算标准通信参数与实际通信参数的偏移量包括：

[0120] 识别标准通信参数与实际通信参数的类型；

[0121] 将同类型的标准通信参数与实际通信参数进行偏移量的计算。

[0122] 可选地，通过预先训练的预警模型计算异常风险值包括：

[0123] 获取实际通信参数；

[0124] 将实际通信参数输入预警模型，其中，预警模型预先采用正负样本数据进行训练；

[0125] 经预警模型对输入的实际通信参数进行预警判断，获取实际通信参数的异常风险值。

[0126] 可选地，控制模块具体用于：

[0127] 异常风险值与异常风险阈值进行比较，以根据比较结果对隐私计算进程进行控制包括：

[0128] 若异常风险值不超出异常风险阈值，则判定为正常情况，隐私计算进程继续运行；

[0129] 若异常风险值超出异常风险阈值，则判定为异常情况，终止隐私计算进程。

[0130] 根据本公开的实施例，本公开还提供了一种电子设备、一种可读存储介质和一种计算机程序产品。

[0131] 图5示出了可以用来实施本公开的实施例的示例电子设备800的示意性框图。电子设备旨在表示各种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例，并且不意在限制本文中描述的和/或者要求的本公开的实现。

[0132] 如图5所示，设备800包括计算单元801，其可以根据存储在只读存储器(ROM)802中的计算机程序或者从存储单元808加载到随机访问存储器(RAM)803中的计算机程序，来执行各种适当的动作和处理。在RAM 803中，还可存储设备800操作所需的各种程序和数据。计算单元801、ROM 802以及RAM 803通过总线804彼此相连。输入/输出(I/O)接口805也连接至总线804。

[0133] 设备800中的多个部件连接至I/O接口805，包括：输入单元806，例如键盘、鼠标等；输出单元807，例如各种类型的显示器、扬声器等；存储单元808，例如磁盘、光盘等；以及通信单元809，例如网卡、调制解调器、无线通信收发机等。通信单元809允许设备800通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0134] 计算单元801可以是各种具有处理和计算能力的通用和/或专用处理组件。计算单元801的一些示例包括但不限于中央处理单元(CPU)、图形处理单元(GPU)、各种专用的人工智能(AI)计算芯片、各种运行机器学习模型算法的计算单元、数字信号处理器(DSP)、以及任何适当的处理器、控制器、微控制器等。计算单元801执行上文所描述的各个方法和处理，例如隐私计算进程的安全监控方法。例如，在一些实施例中，隐私计算进程的安全监控方法可被实现为计算机软件程序，其被有形地包含于机器可读介质，例如存储单元808。在一些实施例中，计算机程序的部分或者全部可以经由ROM 802和/或通信单元809而被载入和/或安装到设备800上。当计算机程序加载到RAM 803并由计算单元801执行时，可以执行上文描述的隐私计算进程的安全监控方法的一个或多个步骤。备选地，在其他实施例中，计算单元801可以通过其他任何适当的方式(例如，借助于固件)而被配置为执行隐私计算进程的安全监控方法。

[0135] 本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统的系统(SOC)、复杂可编程逻辑设备(CPLD)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至

少一个输出装置。

[0136] 用于实施本公开的方法的程序代码可以采用一个或多个编程语言的任何组合来编写。这些程序代码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或控制器，使得程序代码当由处理器或控制器执行时使流程图和/或框图中所规定的功能/操作被实施。程序代码可以完全在机器上执行、部分地在机器上执行，作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

[0137] 在本公开的上下文中，机器可读介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的程序。机器可读介质可以是机器可读信号介质或机器可读储存介质。机器可读介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。机器可读存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、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或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备、或上述内容的任何合适组合。

[0138] 为了提供与用户的交互，可以在计算机上实施此处描述的系统和技术，该计算机具有：用于向用户显示信息的显示装置(例如，CRT(阴极射线管)或者LCD(液晶显示器)监视器)；以及键盘和指向装置(例如，鼠标或者轨迹球)，用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈(例如，视觉反馈、听觉反馈、或者触觉反馈)；并且可以用任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户的输入。

[0139] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如，作为数据服务器)、或者包括中间件部件的计算系统(例如，应用服务器)、或者包括前端部件的计算系统(例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如，通信网络)来将系统的部件相互连接。通信网络的示例包括：局域网(LAN)、广域网(WAN)和互联网。

[0140] 计算机系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器，也可以为分布式系统的服务器，或者是结合了区块链的服务器。

[0141] 应该理解，可以使用上面所示的各种形式的流程，重新排序、增加或删除步骤。例如，本发公开中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本公开公开的技术方案所期望的结果，本文在此不进行限制。

[0142] 上述具体实施方式，并不构成对本公开保护范围的限制。本领域技术人员应该明白的是，根据设计要求和其他因素，可以进行各种修改、组合、子组合和替代。任何在本公开的精神和原则之内所作的修改、等同替换和改进等，均应包含在本公开保护范围之内。

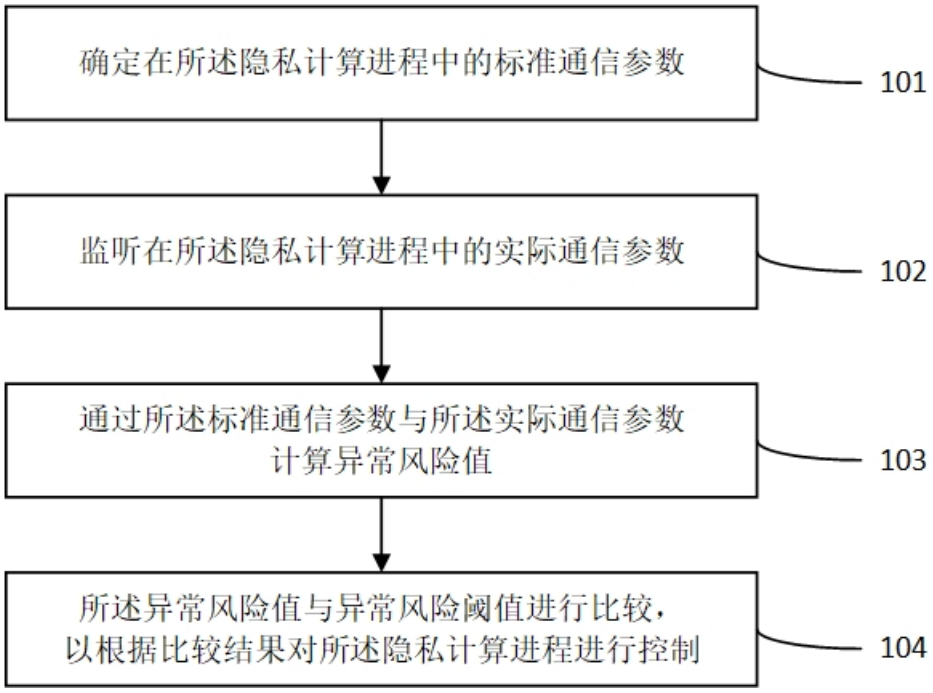

确定在所述隐私计算进程中的标准通信参数
101
监听在所述隐私计算进程中的实际通信参数
102
通过所述标准通信参数与所述实际通信参数
计算异常风险值
103
所述异常风险值与异常风险阈值进行比较，
以根据比较结果对所述隐私计算进程进行控制
104

图1

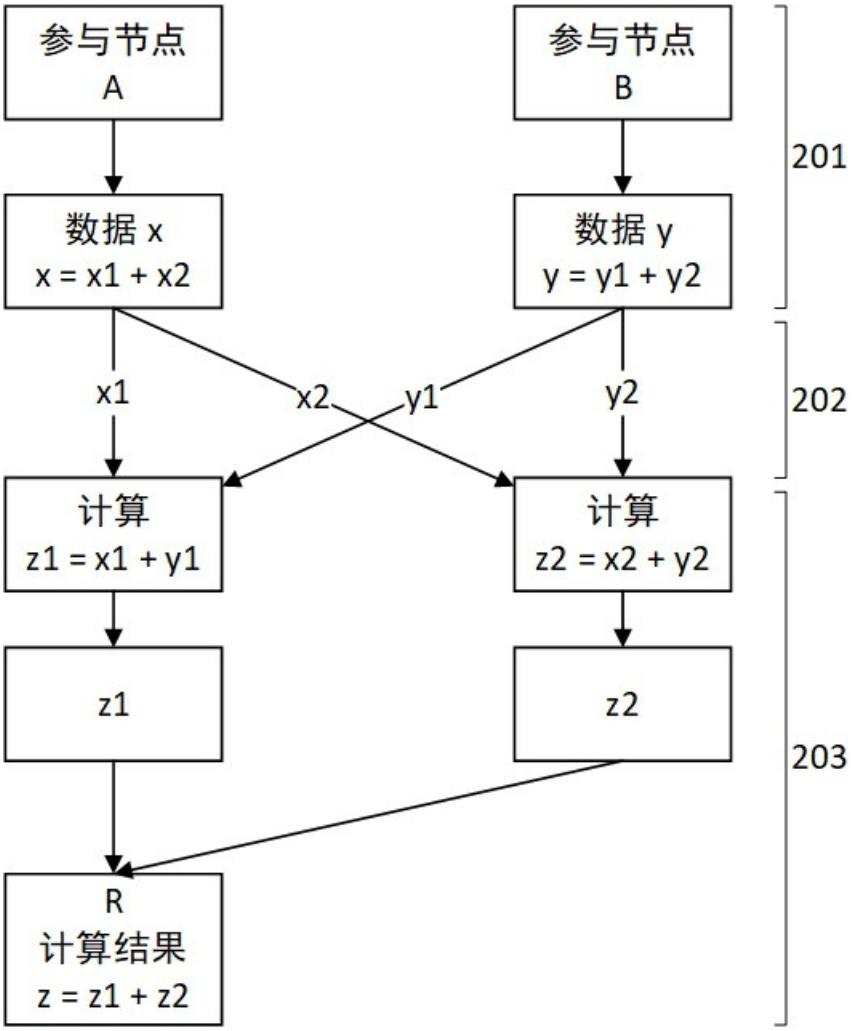

参与节点
A
参与节点
B
201
数据 x
x = x1 + x2
数据 y
y = y1 + y2
x1
x2
y1
y2
202
计算
z1 = x1 + y1
计算
z2 = x2 + y2
z1
z2
203
R
计算结果
z = z1 + z2

图2

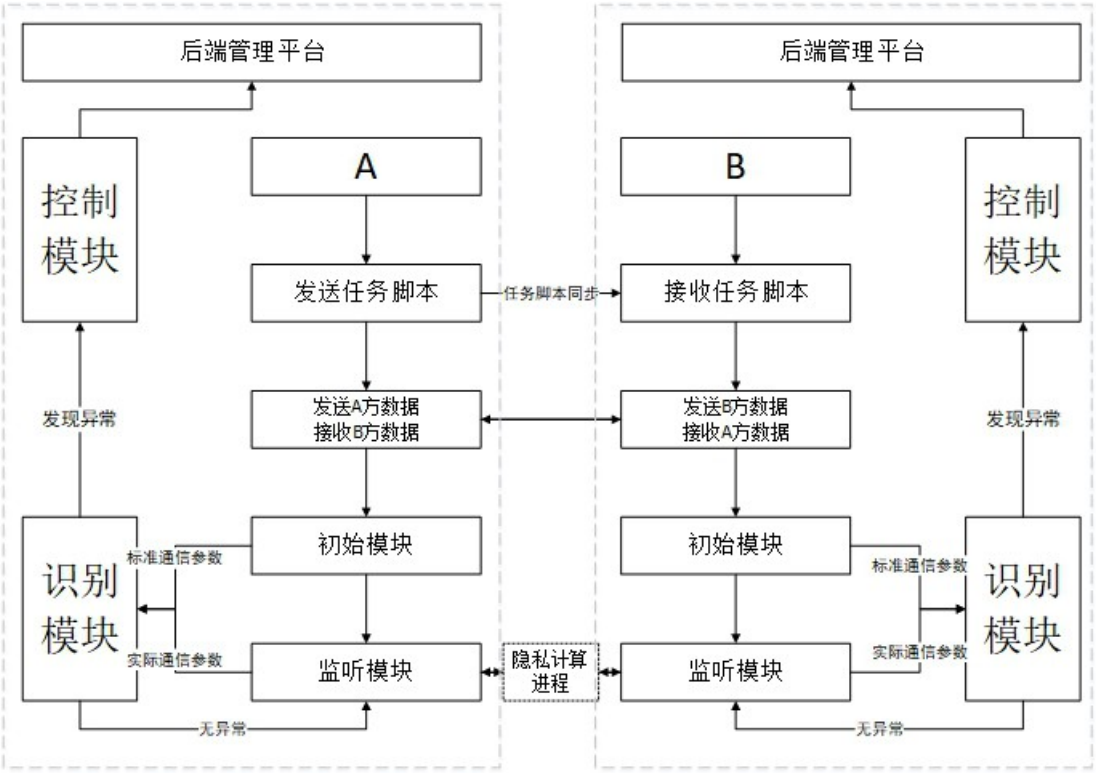

后端管理平台
后端管理平台
控制模块
A
B
控制模块
发送任务脚本
任务脚本同步
接收任务脚本
发现异常
发送A方数据
接收B方数据
发送B方数据
接收A方数据
发现异常
识别模块
标准通信参数
初始模块
初始模块
标准通信参数
识别模块
实际通信参数
监听模块
隐私计算进程
监听模块
实际通信参数
无异常
无异常

图3

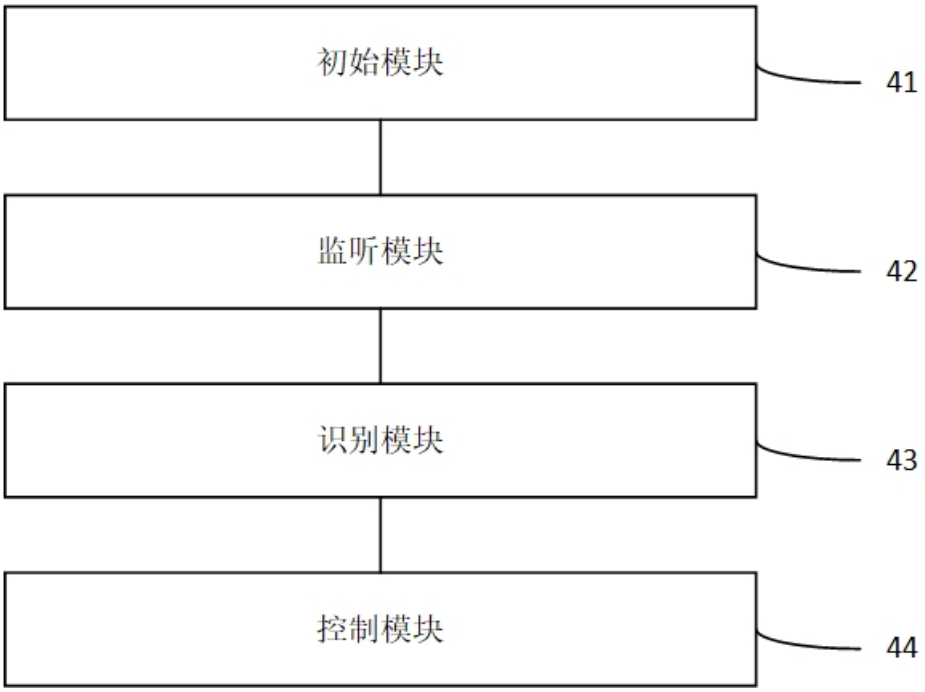

初始模块
41
监听模块
42
识别模块
43
控制模块
44

图4

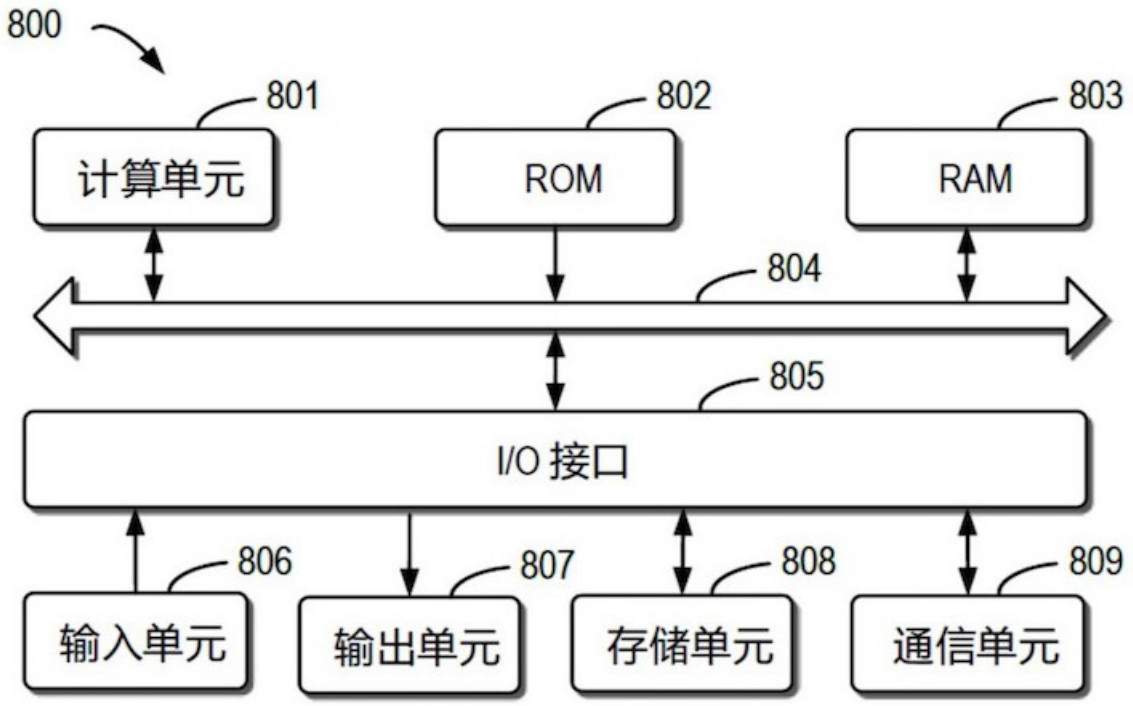

800
801
计算单元
802
ROM
803
RAM
804
805
I/O 接口
806
输入单元
807
输出单元
808
存储单元
809
通信单元

图5