(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110825548 B
(45)授权公告日 2022.11.08

(21)申请号 201911018935.1

(22)申请日 2019.10.24

(65)同一申请的已公布的文献号
申请公布号 CN 110825548 A

(43)申请公布日 2020.02.21

(73)专利权人 新华三信息安全技术有限公司
地址 230000 安徽省合肥市高新区创新大道2800号创新产业园二期H2栋541室

(72)发明人 孙尚勇

(74)专利代理机构 北京超成律师事务所 11646
专利代理师 孔默

(51)Int.Cl.
G06F 11/07(2006.01)

(56)对比文件
CN 110188360 A,2019.08.30
US 2018234443 A1,2018.08.16
CN 109948669 A,2019.06.28
CN 109120632 A,2019.01.01
CN 109213616 A,2019.01.15
CN 108021932 A,2018.05.11
US 2010153315 A1,2010.06.17
程凡.基于排序学习的信息检索模型研究.《万方数据》.2013,
韩凯等.基于日志分析的虚拟机智能运维.《信息与电脑(理论版)》.2018,(第20期),
蔡飞等.基于用户相关反馈的排序学习算法研究.《国防科技大学学报》.2013,(第02期),

审查员 岳孟果

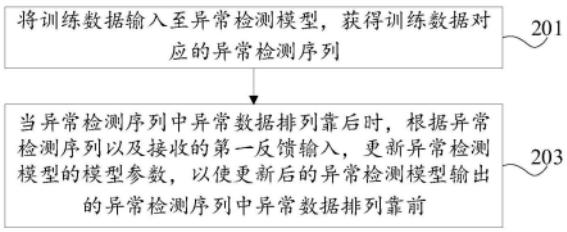
权利要求书2页 说明书9页 附图5页

(54)发明名称

异常检测方法、模型训练方法及相关装置

(57)摘要

本申请提出一种异常检测方法、模型训练方法及相关装置，涉及异常检测技术领域，通过将训练数据输入至异常检测模型，以获得训练数据对应的异常检测序列，并当异常检测序列中异常数据排列靠后时，根据该异常检测序列以及接收的第一反馈输入，更新该异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前，相比于现有技术，能够使异常数据在异常检测序列中处于靠前位置，从而使运维人员能够快速在异常检测序列排查到异常数据，提升异常检测效率。



CN 110825548 B

1.一种异常检测模型训练方法,其特征在于,所述方法包括:

将训练数据输入至异常检测模型,获得所述训练数据对应的异常检测序列;

当所述异常检测序列中异常数据排列靠后时,根据所述异常检测序列以及接收的第一反馈输入,更新所述异常检测模型的模型参数,以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前;

其中,所述第一反馈输入表征所述异常检测序列中异常数据排列靠后。

2.如权利要求1所述的方法,其特征在于,根据所述异常检测序列以及接收的第一反馈输入,更新所述异常检测模型的模型参数的步骤,包括:

根据所述异常检测序列及所述第一反馈输入计算损失函数值;

增大所述损失函数值,并利用所述增大后的损失函数值更新所述异常检测模型的模型参数。

3.如权利要求2所述的方法,其特征在于,更新所述异常检测模型的模型参数的计算公式满足如下:

$loss' = -y_t SCORE(x_n; w_n)$

式中,$loss'$表示所述增大后的损失函数值,y_t表示所述第一反馈输入,SCORE函数表示对所述异常检测序列的异常分数计算函数,x_n表示所述异常检测序列,w_n表示所述更新后的模型参数。

4.如权利要求2所述的方法,其特征在于,所述损失函数值的计算公式满足如下:

$loss = SCORE(x_n; w_{n-1}) - y_t$

式中,loss表示所述损失函数值,SCORE函数表示对所述异常检测序列的异常分数计算函数,x_n表示所述异常检测序列,w_{n-1}表示所述异常检测模型的模型参数,y_t表示所述第一反馈输入。

5.一种异常检测方法,其特征在于,所述方法包括:

接收待检测数据;

将所述待检测数据输入至利用如权利要求1-4任一项所述方法训练完成的异常检测模型,得到所述待检测数据对应的异常检测序列。

6.一种异常检测模型训练装置,其特征在于,所述装置包括:

预处理模块,用于将训练数据输入至异常检测模型,获得所述训练数据对应的异常检测序列;

更新模块,用于当所述异常检测序列中异常数据排列靠后时,根据所述异常检测序列以及接收的第一反馈输入,更新所述异常检测模型的模型参数,以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前;

其中,所述第一反馈输入表征所述异常检测序列中异常数据排列靠后。

7.如权利要求6所述的装置,其特征在于,所述更新模块在根据所述异常检测序列以及接收的第一反馈输入,更新所述异常检测模型的模型参数时,具体用于:

根据所述异常检测序列及所述第一反馈输入计算损失函数值;

增大所述损失函数值,并利用所述增大后的损失函数值更新所述异常检测模型的模型参数。

8.一种异常检测装置,其特征在于,所述装置包括:

接收模块，用于接收待检测数据；

检测模块，用于将所述待检测数据输入至利用如权利要求1-4任一项所述方法训练完成的异常检测模型，得到所述待检测数据对应的异常检测序列。

9.一种电子设备，其特征在于，包括：

存储器，用于存储一个或多个程序；

处理器；

当所述一个或多个程序被所述处理器执行时，实现如权利要求1-5中任一项所述的方法。

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，该计算机程序被处理器执行时实现如权利要求1-5中任一项所述的方法。

异常检测方法、模型训练方法及相关装置

技术领域

[0001] 本申请涉及异常检测技术领域，具体而言，涉及一种异常检测方法、模型训练方法及相关装置。

背景技术

[0002] 为了保障服务器的稳定运行，一般需要运维人员通过监控各种各样的关键性能指标(比如CPU、内存、访问量等)来判断服务器是否有稳定运行，因为相关指标如果发生异常，往往意味着与其相关的应用发生了问题。

[0003] 运维人员监控的关键性能指标一般分为两种类型：服务指标和机器指标。服务指标是指能够反映服务器的规模、质量的性能指标，例如，网页响应时间，网页访问量，连接错误数量等；机器指标是指能够反映设备(服务器、路由器、交换机)健康状态的性能指标，例如，CPU使用率，内存使用率，磁盘IO，网卡吞吐率等。运维人员可以通过算法分析各种指标的时间序列数据，从而对服务器的各项指标进行异常检测，进而判断服务器是否出现异常行为。运维人员利用算法分析异常数据指标，可以得到异常检测序列，然后对异常检测序列中的各个数据进行排查，判断异常检测序列中的各个数据是否异常，从而确定服务器是否出现异常。

[0004] 然而，在例如前述的异常检测方案中，正常数据比异常数据往往在异常检测序列中排列更靠前，使得运维人员往往需要花费较多时间才能在异常检测序列排查到异常数据，异常检测效率较低。

发明内容

[0005] 本申请的目的在于提供一种异常检测方法、模型训练方法及相关装置，使运维人员能够快速在异常检测序列排查到异常数据，提升异常检测效率。

[0006] 为了实现上述目的，本申请实施例采用的技术方案如下：

[0007] 第一方面，本申请实施例提供一种异常检测模型训练方法，所述方法包括：

[0008] 将训练数据输入至异常检测模型，获得所述训练数据对应的异常检测序列；

[0009] 当所述异常检测序列中异常数据排列靠后时，根据所述异常检测序列以及接收的第一反馈输入，更新所述异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前；

[0010] 其中，所述第一反馈输入表征所述异常检测序列中异常数据排列靠后。

[0011] 第二方面，本申请实施例提供一种异常检测方法，所述方法包括：

[0012] 接收待检测数据；

[0013] 将所述待检测数据输入至利用上述第一方面提供的异常检测模型训练方法训练完成的异常检测模型，得到所述待检测数据对应的异常检测序列。

[0014] 第三方面，本申请实施例提供一种异常检测模型训练装置，所述装置方法包括：

[0015] 预处理模块，用于将训练数据输入至异常检测模型，获得所述训练数据对应的异

常检测序列；

[0016] 更新模块，用于当所述异常检测序列中异常数据排列靠后时，根据所述异常检测序列以及接收的第一反馈输入，更新所述异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前；

[0017] 其中，所述第一反馈输入表征所述异常检测序列中异常数据排列靠后。

[0018] 第四方面，本申请实施例提供一种异常检测装置，所述装置包括：

[0019] 接收模块，用于接收待检测数据；

[0020] 检测模块，用于将所述待检测数据输入至利用上述第一方面提供的异常检测模型训练方法训练完成的异常检测模型，得到所述待检测数据对应的异常检测序列。

[0021] 第五方面，本申请实施例提供一种电子设备，所述电子设备包括存储器，用于存储一个或多个程序；处理器；当所述一个或多个程序被所述处理器执行时，实现上述的异常检测模型训练方法或异常检测方法。

[0022] 第六方面，本申请实施例提供一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述的异常检测模型训练方法或异常检测方法。

[0023] 本申请实施例提供的一种异常检测方法、模型训练方法及相关装置，通过将训练数据输入至异常检测模型，以获得训练数据对应的异常检测序列，并当异常检测序列中异常数据排列靠后时，根据该异常检测序列以及接收的第一反馈输入，更新该异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前，相比于现有技术，能够使异常数据在异常检测序列中处于靠前位置，从而使运维人员能够快速在异常检测序列排查到异常数据，提升异常检测效率。

[0024] 为使本申请的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

[0025] 为了更清楚地说明本申请实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它相关的附图。

[0026] 图1A示出聚类分析方法的一种示意图；

[0027] 图1B示出利用聚类分析方法进行异常检测的示意图；

[0028] 图2示出一种异常检测序列示意图；

[0029] 图3示出本申请实施例提供的电子设备的一种示意性结构框图；

[0030] 图4示出本申请实施例提供的异常检测模型训练方法的一种示意性流程图；

[0031] 图5示出另一种异常检测序列示意图；

[0032] 图6示出图4中步骤203的子步骤的一种示意性流程图；

[0033] 图7示出本申请实施例提供的异常检测方法的一种示意性流程图；

[0034] 图8示出本申请实施例提供的异常检测模型训练装置的一种示意性结构框图；

[0035] 图9示出本申请实施例提供的异常检测装置的一种示意性结构框图。

[0036] 图中：100-电子设备；101-存储器；102-处理器；103-通信接口；400-异常检测模型

训练装置;401-预处理模块;402-更新模块;500-异常检测装置;501-接收模块;502-检测模块。

具体实施方式

[0037] 为使本申请实施例的目的、技术方案和优点更加清楚,下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本申请一部分实施例,而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。

[0038] 因此,以下对在附图中提供的本申请的实施例的详细描述并非旨在限制要求保护的本申请的范围,而是仅仅表示本申请的选定实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0039] 应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步定义和解释。同时,在本申请的描述中,术语“第一”、“第二”等仅用于区分描述,而不能理解为指示或暗示相对重要性。

[0040] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0041] 下面结合附图,对本申请的一些实施方式作详细说明。在不冲突的情况下,下述的实施例及实施例中的特征可以相互组合。

[0042] 如上所述,运维人员可以结合一些算法方案分析异常数据指标,从而实现对异常数据的检测。

[0043] 以BCC-KNN模型等基于固定阈值和聚类算法的检测方案为例,结合图1A和图1B所示,该检测方案通过分析异常数据,并将异常数据进行聚类分析后归为多个类别,并计算每一类别异常数据的聚类中心,以及通过计算归属于每一类的所有实例距离聚类中心的均值计算每一类别的半径。

[0044] 当存在新的待检测数据时,通过计算该待检测数据与每个聚类中心的距离,选择与该待检测数据距离最小的聚类中心所属的类别作为该待检测数据的临时归属类;然后判断该待检测数据与该临时归属类的聚类中心的聚类是否小于该临时归属类对应的半径;若小于,则将该待检测数据确定为异常数据,并将该待检测数据归为该临时归属类且更新该临时归属类的聚类中心和半径;反之,若大于或等于,则将该待检测数据确定为正常数据。

[0045] 另外,对于得到的异常检测序列,往往还需要运维人员进行检测排查,从而确定服务器是否出现异常。然而,在实际的异常检测场景中,往往是批量数据一并进行异常检测;在例如前述的异常检测方案进行异常检测时,输出的检测结果往往没有考虑正常数据与异常数据之间的排列数据;比如BCC-KNN模型输出的异常检测序列可以如图2所示,假定图2中

空白圆圈表示正常数据，黑色表示异常数据，在如图2所示的排列结果中，异常数据处于异常检测序列的排列靠后位置，即正常数据比异常数据在异常检测序列中排列更靠前，使得运维人员在排查各个数据时，需要花费较多时间才能在异常检测序列排查到异常数据，异常检测效率较低。

[0046] 为此，基于上述缺陷，本申请实施例提供的一种可能的实现方式为：通过将训练数据输入至异常检测模型，以获得训练数据对应的异常检测序列，并当异常检测序列中异常数据排列靠后时，根据该异常检测序列以及接收的第一反馈输入，更新该异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前，进而使运维人员能够快速在异常检测序列排查到异常数据，提升异常检测效率。

[0047] 请参阅图3，图3示出本申请实施例提供的电子设备100的一种示意性结构框图。该电子设备100可以作为训练异常检测模型，以实现本申请实施例提供的异常检测模型训练方法的设备，或者是运行训练完成的异常检测模型，以实现本申请实施例提供的异常检测方法的设备，比如个人电脑(personal computer，PC)、平板电脑、服务器等等。

[0048] 电子设备100包括存储器101、处理器102和通信接口103，该存储器101、处理器102和通信接口103相互之间直接或间接地电性连接，以实现数据的传输或交互。例如，这些元件相互之间可通过一条或多条通讯总线或信号线实现电性连接。

[0049] 存储器101可用于存储软件程序及模块，如本申请实施例提供的异常检测模型训练装置400或者是异常检测装置500对应的程序指令/模块，处理器102通过执行存储在存储器101内的软件程序及模块，从而执行各种功能应用以及数据处理。该通信接口103可用于与其他节点设备进行信令或数据的通信。

[0050] 其中，存储器101可以是但不限于，随机存取存储器(Random Access Memory，RAM)，只读存储器(Read Only Memory，ROM)，可编程只读存储器(Programmable Read-Only Memory，PROM)，可擦除只读存储器(Erasable Programmable Read-Only Memory，EPROM)，电可擦除可编程只读存储器(Electric Erasable Programmable Read-Only Memory，EEPROM)等。

[0051] 处理器102可以是一种集成电路芯片，具有信号处理能力。该处理器102可以是通用处理器，包括中央处理器(Central Processing Unit，CPU)、网络处理器(Network Processor，NP)等；还可以是数字信号处理器(Digital Signal Processing，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现场可编程门阵列(Field－Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0052] 可以理解，图3所示的结构仅为示意，电子设备100还可以包括比图3中所示更多或者更少的组件，或者具有与图3所示不同的配置。图3中所示的各组件可以采用硬件、软件或其组合实现。

[0053] 下面以图3所示的电子设备100作为示意性执行主体为例，对本申请实施例提供的异常检测模型训练方法进行示例性说明。

[0054] 请参阅图4，图4示出本申请实施例提供的异常检测模型训练方法的一种示意性流程图，可以包括以下步骤：

[0055] 步骤201，将训练数据输入至异常检测模型，获得训练数据对应的异常检测序列；

[0056] 步骤203，当异常检测序列中异常数据排列靠后时，根据异常检测序列以及接收的第一反馈输入，更新异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前。

[0057] 在本申请实施例中，可以采用孤立森林(Isolation Forest)作为异常检测模型，在对该异常检测模型进行训练时，首先将训练数据输入至该异常检测模型，从而由异常检测模型输出以获得该训练数据对应的异常检测序列；其中，输入至该异常检测模型的训练数据可以包括有多个数据，异常检测模型输出的异常检测序列即为对该多个数据进行的排列，比如该异常检测序列可以如图2所示。

[0058] 需要说明的是，异常检测模型输出的异常检测序列中既包括正常数据也包括异常数据。

[0059] 另外，可以定义第一反馈输入和第二反馈输入，第一反馈输入表征异常检测序列中异常数据排列靠后；而第二反馈输入表征异常检测序列中异常数据排列靠前。

[0060] 然后，电子设备根据异常数据在异常检测序列中的排列情况，当异常检测序列中异常数据排列靠后时，电子设备可以根据异常检测序列以及接收的第一反馈输入，计算损失函数值，进而由计算得到的损失函数值更新该异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前。

[0061] 以上述的孤立森林作为异常检测模型为例，假定电子设备执行步骤201后获得的异常检测序列如图2所示；如上所述，图2中异常数据在该异常检测序列中排列靠后；然后可以由运维人员向电子设备输入表征异常检测序列中异常数据排列靠后的第一反馈输入，进而由电子设备则执行步骤203，根据该异常检测序列以及接收的第一反馈输入，更新该孤立森林的模型参数，从而使孤立森林输出的异常检测序列中异常数据如图5所示，排列在异常检测序列的靠前位置，从而使运维人员能够快速排查到异常检测序列中的异常数据，提升异常检测效率。

[0062] 其中，需要说明的是，在本申请实施例中，排列靠前可以是指对应数据排列在异常检测序列中顺数的设定的序列中，比如前5位，或者是所有数据的前10％位，例如总的有100个数据，若排列在前10(100*10％＝10)位即为排列靠前；相对地，排列靠后则可以是指倒数的设定的序列中，比如末尾5位，或者是所有数据的末尾10％位，例如总的有100个数据，若排列在末尾的10(100*10％＝10)位即为排列靠后。

[0063] 另外，在本申请实施例提供的上述实现方案中，当异常检测序列中异常数据排列靠前时，比如异常检测序列的排列结果如图5所示，则说明此时异常检测模型的性能较为优秀，能够将异常数据排列在异常检测序列的靠前位置，此时可以选择不计算损失函数值即不更新异常检测模型的模型参数，也可以计算损失函数值以更新异常检测模型的模型参数，从而使异常检测模型的性能更加优秀，本申请实施例对异常检测序列中异常数据排列靠前时的操作方式不进行限定。

[0064] 可见，基于上述设计，本申请实施例提供的一种异常检测模型训练方法，通过将训练数据输入至异常检测模型，以获得训练数据对应的异常检测序列，并当异常检测序列中异常数据排列靠后时，根据该异常检测序列以及接收的第一反馈输入，更新该异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前，相比于现有技术，能够使异常数据在异常检测序列中处于靠前位置，从而使运维人员能够快

速在异常检测序列排查到异常数据，提升异常检测效率。

[0065] 其中，在执行步骤203更新异常检测模型的模型参数时，可以采用利用计算得到的损失函数值直接更新异常检测模型的模型参数的方案。

[0066] 另外，为加快异常检测模型的训练速度，请参阅图6，图6示出图4中步骤203的子步骤的一种示意性流程图，作为一种可能的实现方式，在对异常检测模型的模型参数进行更新时，步骤203可以包括以下子步骤：

[0067] 步骤203-1，根据异常检测序列及第一反馈输入计算损失函数值；

[0068] 步骤203-2，增大损失函数值，并利用增大后的损失函数值更新异常检测模型的模型参数。

[0069] 在本申请实施例中，电子设备在执行步骤203以更新异常检测模型的模型参数时，可以先由异常检测序列及第一反馈输入计算损失函数值。

[0070] 比如，示例性地，损失函数值的计算公式可以满足如下：

[0071] $loss=SCORE(x_n;w_{n-1})-y_t$

[0072] 式中，loss表示损失函数值，SCORE函数表示对异常检测序列的异常分数计算函数，x_n表示异常检测序列，w_{n-1}表示异常检测模型的模型参数，y_t表示第一反馈输入。

[0073] 其中，SCORE函数可以为孤立森林中用于计算每条待测数据的异常分数(Anomaly Score)的公式。

[0074] 然后，增大该损失函数值，进而利用该增大后的损失函数值更新异常检测模型的模型参数；也就是说，当异常检测序列中异常数据排列靠后时，电子设备可以增大该异常检测模型的损失函数值，比如以设定的比例系数乘以该损失函数值，从而使异常检测模型的模型参数调整幅度更大，异常检测模型能够更快达到收敛条件，完成训练。

[0075] 其中，示例性地，更新所述异常检测模型的模型参数的计算公式可以满足如下：

[0076] $loss'=-y_tSCORE(x_n;w_n)$

[0077] 式中，loss′表示增大后的损失函数值，y_t表示第一反馈输入，SCORE函数表示对异常检测序列的异常分数计算函数，x_n表示异常检测序列，w_n表示更新后的模型参数；即，根据该计算公式，可以反算出异常检测模型更新后的模型参数w_n。

[0078] 可见，基于上述设计，本申请实施例提供的一种异常检测模型训练方法，根据异常检测序列及第一反馈输入计算损失函数值，然后增大该损失函数值，并利用增大后的损失函数值更新异常检测模型的模型参数，从而使异常检测模型的模型参数调整幅度更大，进而使异常检测模型能够更快达到收敛条件。

[0079] 下面以孤立森林作为异常检测模型为示例，利用本申请实施例提供的异常检测模型训练方式对该孤立森林进行第n(n为大于1的正整数)次训练为例进行说明。

[0080] 其中，孤立森林的初始模型参数可以采用模型的参数值(比如默认为1)，并预先定义$y_t=-1$表示第一反馈输入，$y_1=1$表示第二反馈输入；即：若电子设备接收的运维人员输入为1，则表示异常检测序列中异常数据排列靠前，而若电子设备接收的运维人员输入为-1，则表示异常检测序列中正常数据排列靠前。

[0081] 在训练时：

[0082] 步骤1，将训练数据I_n输入至孤立森林，由孤立森林输出异常检测序列x_n；

[0083] 步骤2，接收运维人员反馈的输入，计算损失函数值，以更新孤立森林的模型参数。

[0084] 其中，运维人员反馈的输入表征的是异常检测序列中的真实的排序情况，运维人员可以通过排查异常检测序列x_n，判断异常检测序列x_n中具体为异常数据排列靠前或是正常数据排列靠前；若是异常数据排列靠前，则运维人员可以输入1反馈给电子设备；若是正常数据排列靠前，则运维人员可以输入-1反馈给电子设备。

[0085] 其中，在执行步骤2时，损失函数值的计算公式可以为：

[0086] $loss = SCORE(x_n; w_{n-1}) - y$

[0087] 式中，loss表示损失函数值，SCORE函数表示对异常检测序列的异常分数计算函数，x_n表示异常检测序列，w_{n-1}表示孤立森林的模型参数，y表示运维人员的反馈输入。

[0088] 在该损失函数值的计算公式中，SCORE函数为归一化后的幂指数函数，其值域范围在(0,1)，即大于0小于1；而y的取值仅能为$y_1 = 1$或$y_t = -1$。

[0089] 所以当$y_1 = 1$时，损失函数的值必然大于0；而当$y_t = -1$时，损失函数的值必然小于0。

[0090] 因此，在计算获得孤立森林更新后的模型参数时，计算公式可以为：

[0091] $k \cdot loss = -y SCORE(x_n; w_n)$

[0092] 式中，k表示对应的比例系数，loss表示损失函数值，y表示运维人员的反馈输入，SCORE函数表示对异常检测序列的异常分数计算函数，x_n表示异常检测序列，w_n表示更新后的模型参数。

[0093] 其中，可以定义，当y的取值为$y_1 = 1$时，对应的k取值为0.1；当y的取值为$y_t = -1$时，对应的k取值为10。

[0094] 因此，按照上述计算公式，当运维人员的反馈输入y取值为$y_t = -1$时，电子设备计算得到的损失函数值loss会大于0，即电子设备确定孤立森林当前的异常检测序列中异常数据排列靠后，此时电子设备则以对应的比例系数10乘以损失函数的值，即调大损失函数值，加快孤立森林模型参数的调整速度；另一方面，当运维人员的反馈输入y取值为$y_1 = 1$时，电子设备计算得到的损失函数值loss会小于0，即电子设备确定孤立森林当前的异常检测序列中异常数据排列靠前，孤立森林的异常检测性能较为优秀，此时电子设备则以对应的比例系数0.1乘以损失函数的值，即缩小损失函数值，从而在较小的范围内调整孤立森林的模型参数。

[0095] 另外，基于上述异常检测模型训练方法，本申请实施例还提供一种异常检测方法，请参阅图7，该异常检测方法可以包括以下步骤：

[0096] 步骤301，接收待检测数据；

[0097] 步骤303，将待检测数据输入至训练完成的异常检测模型，得到待检测数据对应的异常检测序列。

[0098] 在利用本申请实施例提供的上述异常检测模型训练方法将异常检测模型训练完成后，可以将训练完成的异常检测模型用于异常检测，以提升运维人员检测异常数据的效率。

[0099] 比如，运维人员可以将监控服务器运行的服务指标(比如CPU、内存、访问量等)作为待检测数据输入至电子设备，其中，该电子设备存储有利用上述异常检测模型训练方法训练完成的异常检测模型；电子设备将接收的待检测数据输入至该训练完成的异常检测模型，从而由该训练完成的异常检测模型输出得到该待检测数据对应的异常检测序列，例如

得到如图5所示的异常检测序列，从而辅助运维人员快速排查到异常数据，提升异常检测的效率。

[0100] 需要说明的是，本申请实施例提供的异常检测模型训练方法和异常检测方法，可以由相同的电子设备执行完成，也可以由不同的电子设备执行完成，本申请实施例对异常检测模型训练方法和异常检测方法两者的执行主体是否相同不进行限制。

[0101] 基于与上述异常检测模型训练方法相同的发明构思，请参阅图8，图8示出本申请实施例提供的异常检测模型训练装置400的一种示意性结构框图，该异常检测模型训练装置400包括预处理模块401及更新模块402。其中：

[0102] 预处理模块401用于，将训练数据输入至异常检测模型，获得训练数据对应的异常检测序列；

[0103] 更新模块402用于，当异常检测序列中异常数据排列靠后时，根据异常检测序列以及接收的第一反馈输入，更新异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前；

[0104] 其中，第一反馈输入表征异常检测序列中异常数据排列靠后。

[0105] 可选地，作为一种可能的实现方式，更新模块402在根据异常检测序列以及接收的第一反馈输入，更新异常检测模型的模型参数时，具体用于：

[0106] 根据异常检测序列及第一反馈输入计算损失函数值；

[0107] 增大损失函数值，并利用增大后的损失函数值更新异常检测模型的模型参数。

[0108] 可选地，作为一种可能的实现方式，更新异常检测模型的模型参数的计算公式可以满足如下：

[0109] $loss' = -y_t SCORE(x_n; w_n)$

[0110] 式中，$loss'$表示增大后的损失函数值，y_t表示第一反馈输入，SCORE函数表示对异常检测序列的异常分数计算函数，x_n表示异常检测序列，w_n表示更新后的模型参数。

[0111] 可选地，作为一种可能的实现方式，损失函数值的计算公式可以满足如下：

[0112] $loss = SCORE(x_n; w_{n-1}) - y_t$

[0113] 式中，loss表示损失函数值，SCORE函数表示对异常检测序列的异常分数计算函数，x_n表示异常检测序列，w_{n-1}表示异常检测模型的模型参数，y_t表示第一反馈输入。

[0114] 另外，基于与上述异常检测方法相同的发明构思，请参阅图9，图9示出本申请实施例提供的异常检测装置500的一种示意性结构框图，该异常检测装置500包括接收模块501及检测模块502。其中：

[0115] 接收模块501用于，接收待检测数据；

[0116] 检测模块502用于，将待检测数据输入至训练完成的异常检测模型，得到待检测数据对应的异常检测序列。

[0117] 在本申请所提供的实施例中，应该理解到，所揭露的装置和方法，也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，附图中的流程图和框图显示了根据本申请实施例的装置、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，所述模块、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。

[0118] 也应当注意，在有些作为替换的实现方式中，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，两个连续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。

[0119] 也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动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。

[0120] 另外，在本申请实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0121] 所述功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本申请实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

[0122] 综上所述，本申请实施例提供的一种异常检测方法、模型训练方法及相关装置，通过将训练数据输入至异常检测模型，以获得训练数据对应的异常检测序列，并当异常检测序列中异常数据排列靠后时，根据该异常检测序列以及接收的第一反馈输入，更新该异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前，相比于现有技术，能够使异常数据在异常检测序列中处于靠前位置，从而使运维人员能够快速在异常检测序列排查到异常数据，提升异常检测效率。

[0123] 并且，还根据异常检测序列及第一反馈输入计算损失函数值，然后增大该损失函数值，并利用增大后的损失函数值更新异常检测模型的模型参数，从而使异常检测模型的模型参数调整幅度更大，进而使异常检测模型能够更快达到收敛条件。

[0124] 以上所述仅为本申请的优选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

[0125] 对于本领域技术人员而言，显然本申请不限于上述示范性实施例的细节，而且在不背离本申请的精神或基本特征的情况下，能够以其它的具体形式实现本申请。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化囊括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。

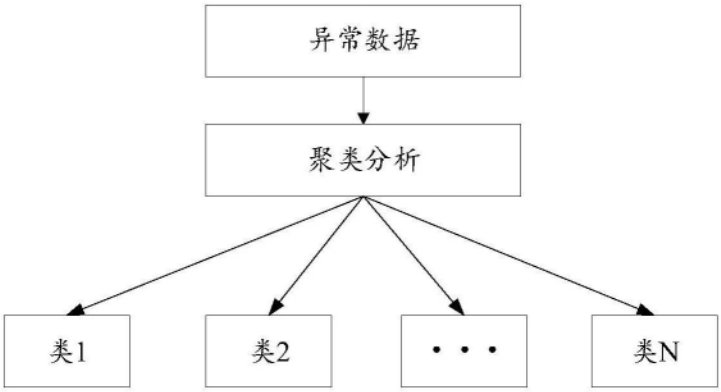


图1A

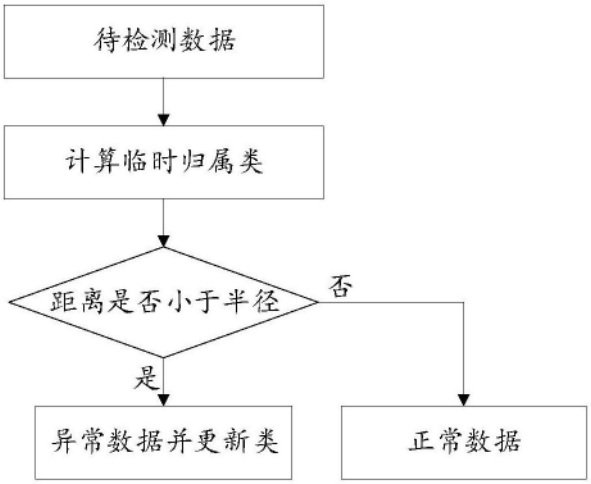


图1B

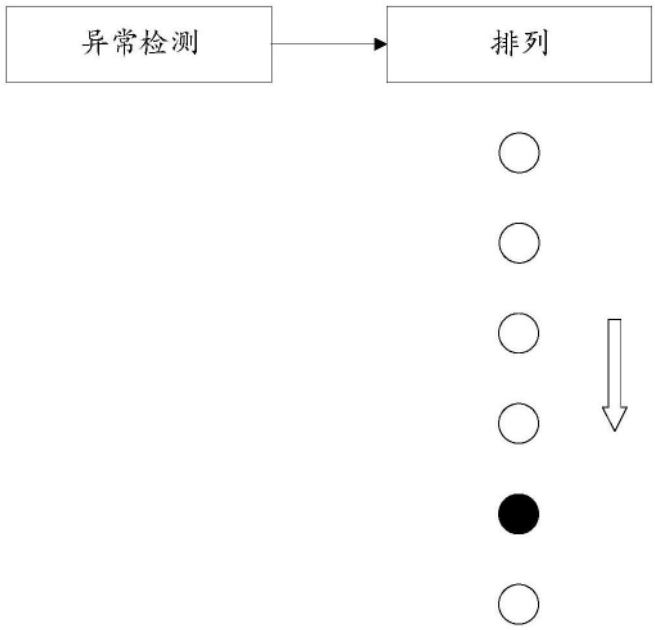


图2

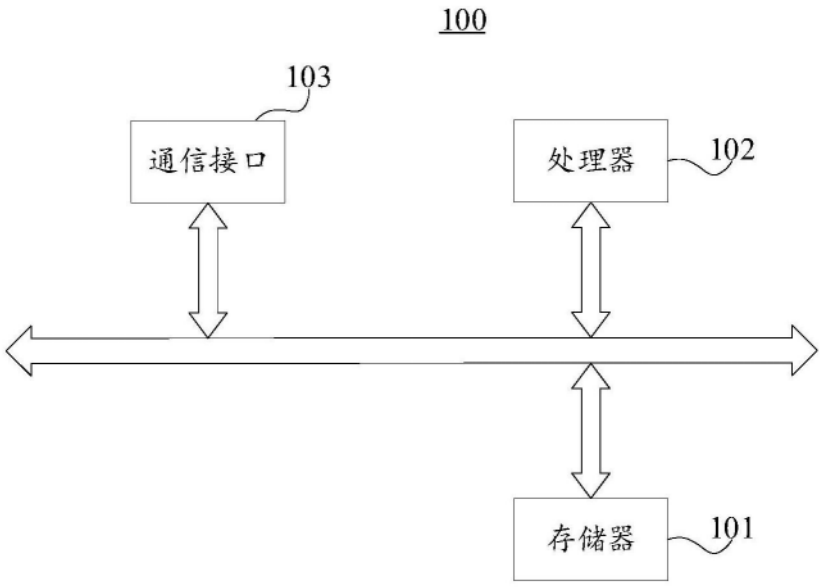


图3

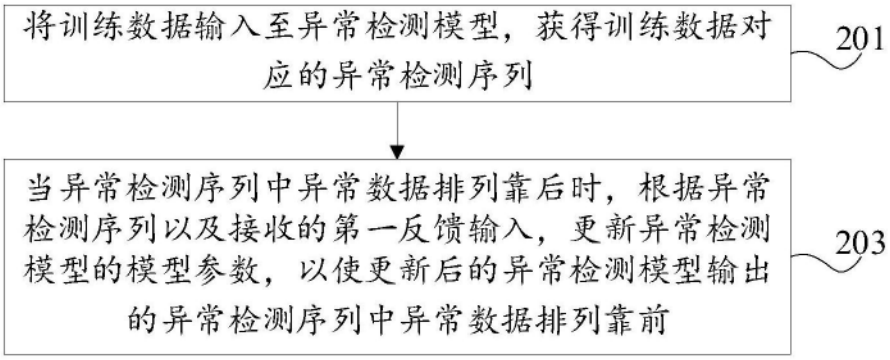

将训练数据输入至异常检测模型，获得训练数据对应的异常检测序列
201
当异常检测序列中异常数据排列靠后时，根据异常检测序列以及接收的第一反馈输入，更新异常检测模型的模型参数，以使更新后的异常检测模型输出的异常检测序列中异常数据排列靠前
203

图4

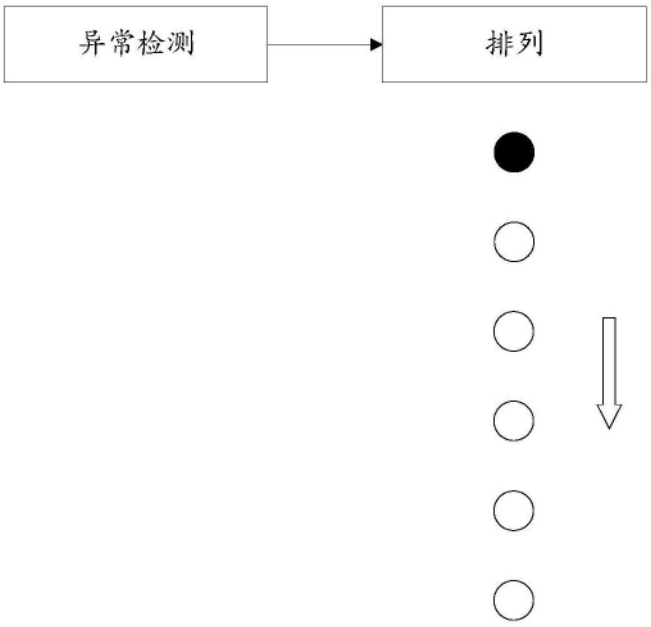

异常检测
排列

图5

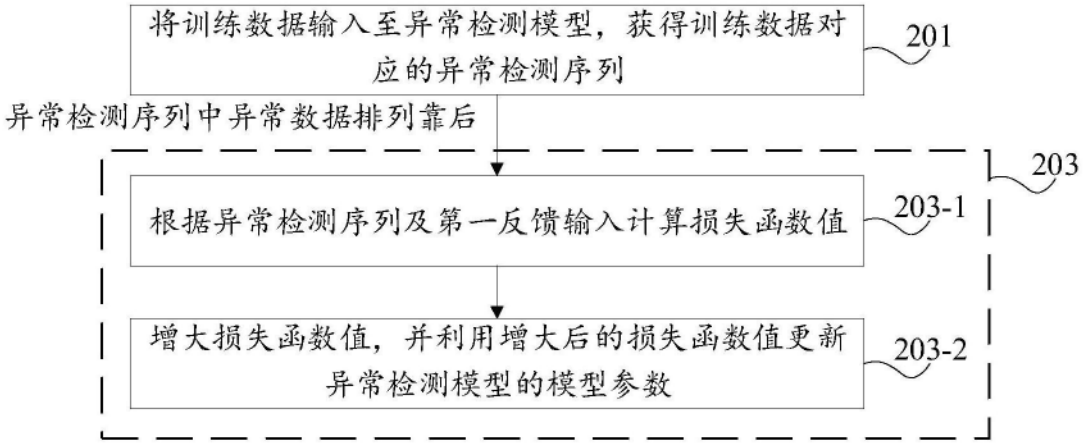

将训练数据输入至异常检测模型，获得训练数据对应的异常检测序列
201
异常检测序列中异常数据排列靠后
203
根据异常检测序列及第一反馈输入计算损失函数值
203-1
增大损失函数值，并利用增大后的损失函数值更新异常检测模型的模型参数
203-2

图6


接收待检测数据
301
将待检测数据输入至训练完成的异常检测模型，得到待检测数据对应的异常检测序列
303

图7

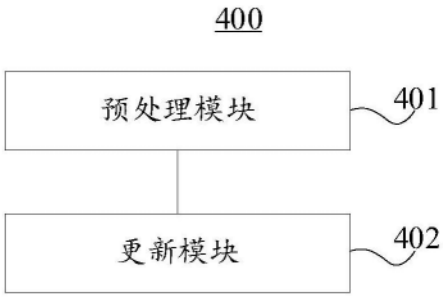

400
预处理模块
401
更新模块
402

图8

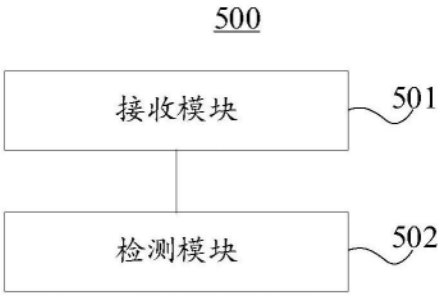


图9