(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 111104242 A
(43)申请公布日 2020.05.05

(21)申请号 201911329739.6

(22)申请日 2019.12.20

(71)申请人 青岛海尔科技有限公司
地址 266101 山东省青岛市崂山区海尔路1号海尔工业园

(72)发明人 刘超 尹德帅 徐志方 马成东 钱学文

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 王晓婷

(51)Int.Cl.
G06F 11/07(2006.01)
G06K 9/62(2006.01)
G06N 20/00(2019.01)

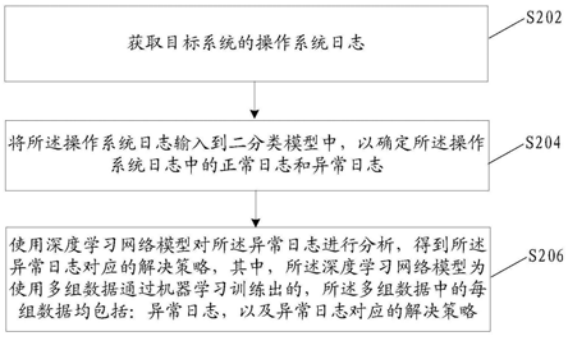
权利要求书1页 说明书8页 附图3页

(54)发明名称

基于深度学习的操作系统的异常日志的处理方法及装置

(57)摘要

本发明提供了一种基于深度学习的操作系统的异常日志的处理方法及装置，上述方法包括：获取目标系统的操作系统日志；将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志；使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略，采用上述技术方案，解决了相关技术中，解决操作系统故障的过程，耗时耗力，效率低下等问题，进而能够省时高效的确认操作系统的故障。



CN 111104242 A

1.一种基于深度学习的操作系统的异常日志的处理方法,其特征在于,包括:

获取目标系统的操作系统日志;

将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志;

使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,其中,所述深度学习网络模型为使用多组数据通过机器学习训练出的,所述多组数据中的每组数据均包括:异常日志,以及异常日志对应的解决策略。

2.根据权利要求1所述的方法,其特征在于,将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志之前,所述方法还包括:

将所述操作系统日志转换为词向量;

将转换后的词向量输入到所述二分类模型中。

3.根据权利要求1所述的方法,其特征在于,将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志之后,所述方法还包括:

对所述异常日志进行聚类处理,分成K类,其中,K为大于1的整数;

将K类异常日志输入到所述深度学习网络模型中。

4.根据权利要求1所述的方法,其特征在于,使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,包括:

对异常日志进行标签,得到目标异常日志;

使用深度学习网络模型对所述异常日志进行分析,得到所述目标异常日志对应的解决策略。

5.根据权利要求1所述的方法,其特征在于,使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略之后,所述方法还包括:

使用确定得到的解决策略对所述目标系统进行预处理。

6.一种基于深度学习的操作系统的异常日志的处理装置,其特征在于,包括:

获取模块,用于获取目标系统的操作系统日志;

输入模块,用于将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志;

确定模块,用于使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,其中,所述深度学习网络模型为使用多组数据通过机器学习训练出的,所述多组数据中的每组数据均包括:异常日志,以及异常日志对应的解决策略。

7.根据权利要求6所述的装置,其特征在于,所述装置还包括:处理模块,所述处理模块,用于将所述操作系统日志转换为词向量;将转换后的词向量输入到所述二分类模型中。

8.根据权利要求6所述的装置,其特征在于,所述确定模块,还用于对所述异常日志进行聚类处理,分成K类,其中,K为大于1的整数;将K类异常日志输入到所述深度学习网络模型中。

9.一种计算机可读的存储介质,其特征在于,所述存储介质中存储有计算机程序,其中,所述计算机程序被设置为运行时执行所述权利要求1至5任一项中所述的方法。

10.一种电子装置,包括存储器和处理器,其特征在于,所述存储器中存储有计算机程序,所述处理器被设置为运行所述计算机程序以执行所述权利要求1至5任一项中所述的方法。

基于深度学习的操作系统的异常日志的处理方法及装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种基于深度学习的操作系统的异常日志的处理方法及装置。

背景技术

[0002] 操作系统日志反映了系统运行状态，记录着系统中特定事件的活动信息，基于系统日志检测系统异常，对维护系统安全稳定有重要的意义。传统的系统故障处理思路是在系统故障发出告警后，人工分析故障原因，而经研究发现通过分析系统日志可以更敏锐的探测出系统隐患和异常以及可能出现的故障。

[0003] 在相关技术中，提供了一种基于linux操作系统信息自动分析故障的方法，该方法首先获取linux操作系统信息，并根据不同故障类别及故障部件形成故障规则库；根据故障规则库中的故障规则对操作系统信息进行自动分析，当匹配到对应故障规则后，给出问题描述及故障解决办法，并保存分析结果。该基于linux操作系统信息自动分析故障的方法，获取linux操作系统信息并根据日常故障的规律及处理办法形成一个故障规则库，当linux操作系统出现故障时，查看故障规则库中的信息即可找到相应的解决办法，但现有技术中，根据故障类别和故障部件建立故障规则库，通过匹配故障规则确定解决方案的方式，基于操作系统已经产生的故障类型和故障部件匹配解决方案，需要人工分析故障原因制定解决方案的方式，需要分析大量数据，这种方式效率低下、耗时耗力。

[0004] 由于各种操作系统组件相对比较复杂，操作系统产生故障的原因可能是多种多样，并且操作系统日志信息数量巨大，当操作系统出现故障时，需要技术人员通过查看大量的系统日志进行故障分析，找到相应的故障原因，再根据找到的故障原因制定故障解决方案，使得解决操作系统故障的过程，耗时耗力，效率低下。

[0005] 针对相关技术中，解决操作系统故障的过程，耗时耗力，效率低下等问题，尚未提出有效的技术方案。

发明内容

[0006] 本发明实施例提供了一种基于深度学习的操作系统的异常日志的处理方法及装置，以至少解决相关技术中，解决操作系统故障的过程，耗时耗力，效率低下等问题。

[0007] 根据本发明的一个实施例，提供了一种基于深度学习的操作系统的异常日志的处理方法，包括：获取目标系统的操作系统日志；将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志；使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略。

[0008] 在本发明实施例中，将操作系统日志输入到二分类模型中，以确定操作系统日志中的正常日志和异常日志之前，上述方法还包括：将操作系统日志转换为词向量；将转换后

的词向量输入到二分类模型中。

[0009] 在本发明实施例中，将操作系统日志输入到二分类模型中，以确定操作系统日志中的正常日志和异常日志之后，上述方法还包括：对异常日志进行聚类处理，分成K类，其中，K为大于1的整数；将K类异常日志输入到深度学习网络模型中。

[0010] 在本发明实施例中，使用深度学习网络模型对异常日志进行分析，得到异常日志对应的解决策略，上述方法还包括：对异常日志进行标签，得到目标异常日志；使用深度学习网络模型对异常日志进行分析，得到目标异常日志对应的解决策略。

[0011] 在本发明实施例中，使用深度学习网络模型对异常日志进行分析，得到异常日志对应的解决策略之后，上述方法还包括：使用确定得到的解决策略对目标系统进行预处理。

[0012] 根据本发明的另一个实施例，提供了一种基于深度学习的操作系统的异常日志的处理装置，包括：获取模块，用于获取目标系统的操作系统日志；输入模块，用于将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志；确定模块，用于使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略。

[0013] 在本发明实施例中，上述装置还包括：处理模块，处理模块用于将操作系统日志转换为词向量；将转换后的词向量输入到二分类模型中。

[0014] 在本发明实施例中，上述确定模块还用于对异常日志进行聚类处理，分成K类，其中，K为大于1的整数；将K类异常日志输入到深度学习网络模型中。

[0015] 在本发明实施例中，上述确定模块还用于对异常日志进行标签，得到目标异常日志；使用深度学习网络模型对所述异常日志进行分析，得到所述目标异常日志对应的解决策略。

[0016] 在本发明实施例中，上述装置还包括：预处理模块，预处理模块用于使用确定得到的解决策略对目标系统进行预处理。

[0017] 根据本发明的又一个实施例，还提供了一种存储介质，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0018] 根据本发明的又一个实施例，还提供了一种电子装置，包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器被设置为运行所述计算机程序以执行上述任一项方法实施例中的步骤。

[0019] 通过本发明，获取目标系统的操作系统日志；将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志；使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略，采用上述技术方案，解决了相关技术中，解决操作系统故障的过程，耗时耗力，效率低下等问题，进而能够省时高效的确认操作系统的故障。

附图说明

[0020] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0021] 图1是本发明实施例的一种基于深度学习的操作系统的异常日志的处理方法的计算机终端的硬件结构框图；

[0022] 图2是根据本发明实施例的基于深度学习的操作系统的异常日志的处理方法的流程图；

[0023] 图3是根据本发明可选实施例的基于深度学习的操作系统的异常日志的处理方法的系统流程框图；

[0024] 图4是根据本发明可选实施例深度神经网络模型的结构示意图；

[0025] 图5是根据本发明可选实施例的线上预测的流程图；

[0026] 图6是根据本发明实施例的基于深度学习的操作系统的异常日志的处理装置的结构框图。

具体实施方式

[0027] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0028] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

[0029] 本申请实施例所提供的方法实施例可以在计算机终端或者类似的运算装置中执行。以运行在计算机终端上为例，图1是本发明实施例的一种基于深度学习的操作系统的异常日志的处理方法的计算机终端的硬件结构框图。如图1所示，计算机终端可以包括一个或多个(图1中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)和用于存储数据的存储器104，可选地，上述计算机终端还可以包括用于通信功能的传输设备106以及输入输出设备108。本领域普通技术人员可以理解，图1所示的结构仅为示意，其并不对上述计算机终端的结构造成限定。例如，计算机终端还可包括比图1中所示更多或者更少的组件，或者具有与图1所示等同功能或比图1所示功能更多的不同的配置。

[0030] 存储器104可用于存储计算机程序，例如，应用软件的软件程序以及模块，如本发明实施例中的基于深度学习的操作系统的异常日志的处理方法对应的计算机程序，处理器102通过运行存储在存储器104内的计算机程序，从而执行各种功能应用以及数据处理，即实现上述的方法。存储器104可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器104可进一步包括相对于处理器102远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0031] 传输装置106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端的通信供应商提供的无线网络。在一个实例中，传输装置106包括一个网络适配器(Network Interface Controller，简称为NIC)，其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置106可以为射频(Radio Frequency，简称为RF)模块，其用于通过无线方式与互联网进行通讯。

[0032] 在本实施例中提供了一种基于深度学习的操作系统的异常日志的处理方法，图2是根据本发明实施例的基于深度学习的操作系统的异常日志的处理方法的流程图，如图2

所示，该流程包括如下步骤：

[0033] 步骤202，获取目标系统的操作系统日志；

[0034] 步骤204，将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志；

[0035] 步骤206，使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略。

[0036] 通过上述步骤，获取目标系统的操作系统日志；将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志；使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略，采用上述技术方案，解决了相关技术中，解决操作系统故障的过程，耗时耗力，效率低下等问题，进而能够省时高效的确认操作系统的故障。

[0037] 在本发明实施例中，将操作系统日志输入到二分类模型中，以确定操作系统日志中的正常日志和异常日志之前，上述方法还包括：将操作系统日志转换为词向量；将转换后的词向量输入到二分类模型中，此外，需要说明的是，操作系统日志通常包含一些无用数据，比如系统日志中的位置固定的无关项的词语。所以在获取大批量操作系统日志后，需要先对操作系统日志进行预处理，清洗无用数据以加重有用数据的比重。在对操作系统日志预处理后，将处理后的操作系统日志转换成词向量，将转换后的词向量输入到二分类模型中。

[0038] 在本发明实施例中，将操作系统日志输入到二分类模型中，以确定操作系统日志中的正常日志和异常日志之后，上述方法还包括：对异常日志进行聚类处理，分成K类，其中，K为大于1的整数；将K类异常日志输入到深度学习网络模型中，即通过二分类模型对操作系统日志进行分类后，对于异常日志进行聚类处理，因为需要根据异常日志的类别设置与异常日志类别相对应的处理方案，相当于将异常日志中存在相同的异常问题的异常日志进行聚类，方便输入到深度学习网络模型中进行深度学习分析。

[0039] 在本发明实施例中，使用深度学习网络模型对异常日志进行分析，得到异常日志对应的解决策略，上述方法还包括：对异常日志进行标签，得到目标异常日志；使用深度学习网络模型对异常日志进行分析，得到目标异常日志对应的解决策略，通过深度学习网络模型根据聚类结果确定异常类别对异常日志添加标签方便区分，并根据深度学习网络模型对基于深度学习的操作系统的异常日志的处理分析，进一步得到异常日志对应的解决策略。

[0040] 在本发明实施例中，使用深度学习网络模型对异常日志进行分析，得到异常日志对应的解决策略之后，上述方法还包括：使用确定得到的解决策略对目标系统进行预处理。通过深度学习网络模型对异常日志进行分析输出对应的异常日志对应的解决策略，并对目标系统中产生异常日志的异常进行预处理，通过上述实施例，在操作系统最终出现故障前进行一定的预处理，尽可能的减少了操作系统故障的产生，降低系统故障发生概率。

[0041] 以下结合一示例对上述的基于深度学习的操作系统的异常日志的处理方法的技术方案进行解释说明，但不用于限定本发明实施例的技术方案。

[0042] 本发明可选实施例，通过对系统日志处理分析，检测出异常日志，基于异常日志预测处理方案，实现检测出系统异常，以及在最终操作系统故障前进行一定的预处理，尽可能减少操作系统故障的产生。图3为基于深度学习的操作系统的异常日志的处理方法的系统流程框图。

[0043] 步骤一，操作系统日志预处理，由于操作系统日志通常是些非结构化文本数据，例如：

[0044] Thu Mar 26 12:46:50 2015tread_id:0x979798

[0045] Thu Mar 26 12:46:50 2015Socket Buffers:

[0046] Thu Mar 26 12:46:50 2015TCPv4_CLIENT link local

[0047] Thu Mar 26 12:46:50 2015TLS:Initial packet from

[0048] Thu Mar 124.129.172.46:1194,sid＝8ad7ba9c 43791f63

[0049] Thu Mar 26 12:46:51 2015VERIFY OK:,

[0050] Thu Mar 26 12:46:51 2015Data Channel Encrypt:Cipher。

[0051] 操作系统日志通常包含一些无用数据，比如：上述系统日志中的位置固定的无关项“Thu Mar”。所以在获取大批量操作系统日志后，需要先对操作系统日志进行预处理，清洗无用数据以加重有用数据的比重。在对操作系统日志预处理后，将处理后的操作系统日志转换成词向量，具体采用word2vec工具将操作系统日志向量化，构建训练聚类模型的样本集，样本集中包含异常日志和正常日志。

[0052] 步骤二，通过二分类模型进行操作系统日志二分类，由于想要分析出系统异常，就需要先从大量的系统日志中找出异常日志，以方便之后分析异常日志确定处理方案。所以，在本发明实施例中，将获取到的大批量操作系统日志转换成词向量后，先通过LightGBM(Light Gradient Boosting Machine，简称LightGBM)算法训练二分类模型，对操作系统日志进行二分类，即，分为异常日志和正常日志。

[0053] 步骤三，通过聚类模型对异常日志聚类，对通过步骤二检测出的异常日志，采用无监督的学习方法，将异常日志进行聚类，即，将表征异常日志的词向量X＝{x1,x2,…,xi,…,xn}分成K类，其中聚类中心表达为C＝{c1,c2,…,cj,…,ck}，则聚类函数表达式为：$J=\sum_{j=1}^{k}\sqrt{\left(\sum_{i,i\in c_j}\left|x_i-c_j\right|^2\right)}$，其中，$c_j$为第j个聚类中心(j＝1,2,3,…k)。聚类模型训练过程即为找到使得J最小时的c_j的值的过程。

[0054] 步骤四，确定异常类别及处理方案，人工审核分析通过步骤三得到聚类结果确定异常类别，并且根据分好的异常类别，设置与异常类别对应的处理方案，相当于给异常类别添加标签，构建异常类-处理方案的训练集D＝{d1,d2,…,di,…,dn}。聚类后可能会有一些极端类别，比如离大部分类别很远的点或类，这些要看成特殊类，需要人工单独分析，如果通过分析确定是有效问题，则也需要作为一类异常，如果是不关键信息，可以忽略。

[0055] 步骤五，神经神经网络模型(相当于本发明实施例中的深度学习网络模型)训练，将通过步骤四得到的异常类-处理方案训练集，用于训练深度神经网络模型，根据训练结果不断调优，具体选用随机梯度下降(Stochastic Gradient Descent，简称SGD)优化算法进行模型调优，最终得到训练好的深度神经网络模型。深度神经网络模型具体采用TextCNN的

神经网络结构，具体网络结构如图4所示。

[0056] (1)输入层是样本词向量矩阵，在本方案中将通过步骤一到步骤三得到异常日志的词向量输入到神经网络模型中前，先将异常日志的词向量逐行排列成矩阵，用补齐的方式统一矩阵大小，最终每段文本被表示为长为最大句长、宽为词向量维度的，假设输入的文本的长度为n，词向量的维度为m，词向量矩阵的大小为n×m。

[0057] (2)卷积层用若干可学习的卷积核与词向量矩阵进行卷积，卷积层的计算公式如下：$y_j = \tanh(\sum_{i \in n} d_i \bullet k_{ij} + b_j)$；上述计算公式中，$y_j$表示经过卷积层得到的第j个特征数据，$d_i$表示输入数据的集合D中第i个输入数据，$k_{ij}$表示在卷积层中第i个输入特征数据对应第j个输出特征数据的卷积核权值，b_j为偏置项。

[0058] (3)最大池化层是对卷积层输出的特征进行最大抽样操作，提取最大特征。

[0059] (4)输出层将所有提取的最大特征全部连接在一起，并通过Softmax函数输出单个样本对应每个类别的概率，选取概率最大的为该样本的类别，从而实现系统日志分类。

[0060] 步骤六，深度神经网络模型更新，将在实际应用中通过步骤一到步骤四中可能出现的新增的异常类别和对应处理方案添加到异常类-处理方案样本集中，对深度神经网络模型进行增量学习，不断更新模型，以提高模型决策的准确度。

[0061] 步骤七，线上预测，线上预测流程如图5所示，将训练好的深度神经网络模型用于线上对产生的系统日志的预测对应的处理方案。先将操作系统日志二分类，从大量的系统日志中检测出异常日志，可以实现对线上系统日志异常检测。对大量系统日志进行二分类，再采用聚类实现系统异常日志无监督分类，然后基于分好的异常类别设置对应的处理方案，训练深度神经网络模型，通过二分类模型和深度神经网络模型，实现对线上操作系统产生的异常日志的检测以及预测与对应的处理方案。通过对异常日志进行聚类以及训练深度神经网络模型，可以实现对检测出的异常日志预测对应处理方案。

[0062] 综上所述，本发明可选实施例通过二分类模型对线上的系统日志进行实时检测，即实时检测系统日志中的异常日志，当检测出异常日志后，将异常日志输入到深度神经网络模型中，通过深度神经网络模型输出对应的异常类-处理方案，给予技术人员更多的对操作系统异常的处理时间，降低系统故障发生概率。

[0063] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献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(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0064] 在本实施例中还提供了一种基于深度学习的操作系统的异常日志的处理装置，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0065] 图6是根据本发明实施例的基于深度学习的操作系统的异常日志的处理装置的结构框图，如图6所示，该装置包括：

[0066] (1)获取模块62,用于获取目标系统的操作系统日志;

[0067] (2)输入模块64,用于将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志;

[0068] (3)确定模块66,用于使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,其中,所述深度学习网络模型为使用多组数据通过机器学习训练出的,所述多组数据中的每组数据均包括:异常日志,以及异常日志对应的解决策略。

[0069] 通过上述装置,获取目标系统的操作系统日志;将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志;使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,其中,所述深度学习网络模型为使用多组数据通过机器学习训练出的,所述多组数据中的每组数据均包括:异常日志,以及异常日志对应的解决策略,采用上述技术方案,解决了相关技术中,解决操作系统故障的过程,耗时耗力,效率低下等问题,进而能够省时高效的确认操作系统的故障。

[0070] 在本发明实施例中,上述装置还包括:处理模块,处理模块用于将操作系统日志转换为词向量;将转换后的词向量输入到二分类模型中。操作系统日志通常包含一些无用数据,比如系统日志中的位置固定的无关项的词语。所以在获取大批量操作系统日志后,需要先对操作系统日志进行预处理,清洗无用数据以加重有用数据的比重。在对操作系统日志预处理后,将处理后的操作系统日志转换成词向量,将转换后的词向量输入到二分类模型中。

[0071] 在本发明实施例中,上述确定模块还用于对异常日志进行聚类处理,分成K类,其中,K为大于1的整数;将K类异常日志输入到深度学习网络模型中。通过二分类模型对操作系统日志进行分类后,对于异常日志进行聚类处理,因为需要根据异常日志的类别设置与异常日志类别相对应的处理方案,相当于将异常日志中存在相同的异常问题的异常日志进行聚类,方便输入到深度学习网络模型中进行深度学习分析。

[0072] 在本发明实施例中,上述确定模块还用于对异常日志进行标签,得到目标异常日志;使用深度学习网络模型对所述异常日志进行分析,得到所述目标异常日志对应的解决策略。通过深度学习网络模型根据聚类结果确定异常类别对异常日志添加标签方便区分,并根据深度学习网络模型对基于深度学习的操作系统的异常日志的处理分析,进一步得到异常日志对应的解决策略。

[0073] 在本发明实施例中,上述装置还包括:预处理模块,预处理模块用于使用确定得到的解决策略对目标系统进行预处理。通过深度学习网络模型对异常日志进行分析输出对应的异常日志对应的解决策略,并对目标系统中产生异常日志的异常进行预处理,通过上述实施例,在操作系统最终出现故障前进行一定的预处理,尽可能的减少了操作系统故障的产生,降低系统故障发生概率。

[0074] 需要说明的是,上述各个模块是可以通过软件或硬件来实现的,对于后者,可以通过以下方式实现,但不限于此:上述模块均位于同一处理器中;或者,上述各个模块以任意组合的形式分别位于不同的处理器中。

[0075] 本发明的实施例还提供了一种存储介质,该存储介质中存储有计算机程序,其中,该计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0076] 可选地,在本实施例中,上述存储介质可以被设置为存储用于执行以下步骤的计

算机程序：

[0077] S1,获取目标系统的操作系统日志；

[0078] S2,将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志；

[0079] S3,使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,其中,所述深度学习网络模型为使用多组数据通过机器学习训练出的,所述多组数据中的每组数据均包括:异常日志,以及异常日志对应的解决策略。

[0080] 可选地,在本实施例中,上述存储介质可以包括但不限于:U盘、只读存储器(Read-Only Memory,简称为ROM)、随机存取存储器(Random Access Memory,简称为RAM)、移动硬盘、磁碟或者光盘等各种可以存储计算机程序的介质。

[0081] 本发明的实施例还提供了一种电子装置,包括存储器和处理器,该存储器中存储有计算机程序,该处理器被设置为运行计算机程序以执行上述任一项方法实施例中的步骤。

[0082] 可选地,上述电子装置还可以包括传输设备以及输入输出设备,其中,该传输设备和上述处理器连接,该输入输出设备和上述处理器连接。

[0083] 可选地,在本实施例中,上述处理器可以被设置为通过计算机程序执行以下步骤：

[0084] S1,获取目标系统的操作系统日志；

[0085] S2,将所述操作系统日志输入到二分类模型中,以确定所述操作系统日志中的正常日志和异常日志；

[0086] S3,使用深度学习网络模型对所述异常日志进行分析,得到所述异常日志对应的解决策略,其中,所述深度学习网络模型为使用多组数据通过机器学习训练出的,所述多组数据中的每组数据均包括:异常日志,以及异常日志对应的解决策略。

[0087] 可选地,本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例,本实施例在此不再赘述。

[0088] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。

[0089] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

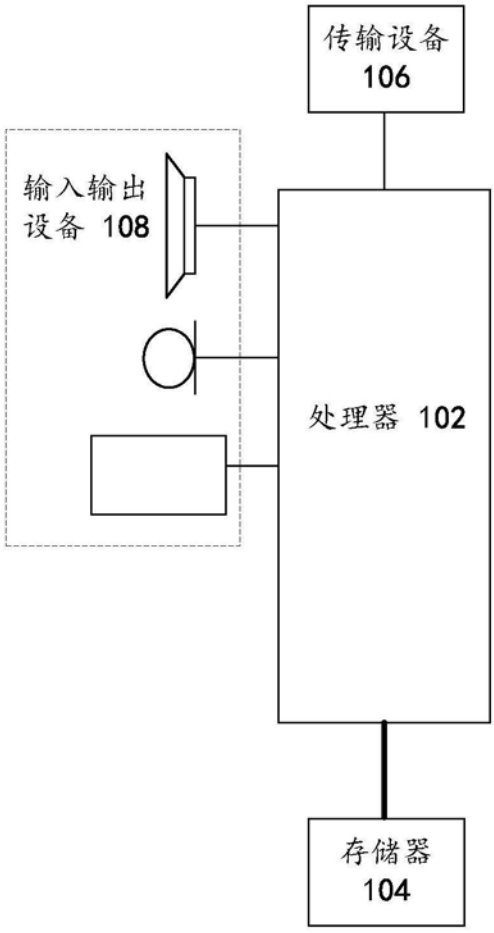

传输设备
106
输入输出
设备 108
处理器 102
存储器
104

图1

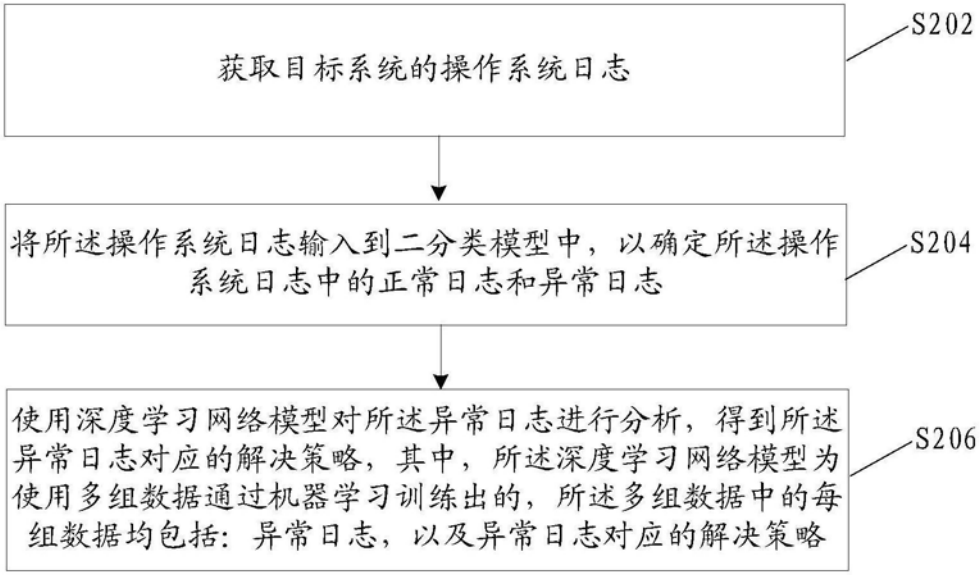

获取目标系统的操作系统日志
S202
将所述操作系统日志输入到二分类模型中，以确定所述操作系统日志中的正常日志和异常日志
S204
使用深度学习网络模型对所述异常日志进行分析，得到所述异常日志对应的解决策略，其中，所述深度学习网络模型为使用多组数据通过机器学习训练出的，所述多组数据中的每组数据均包括：异常日志，以及异常日志对应的解决策略
S206

图2

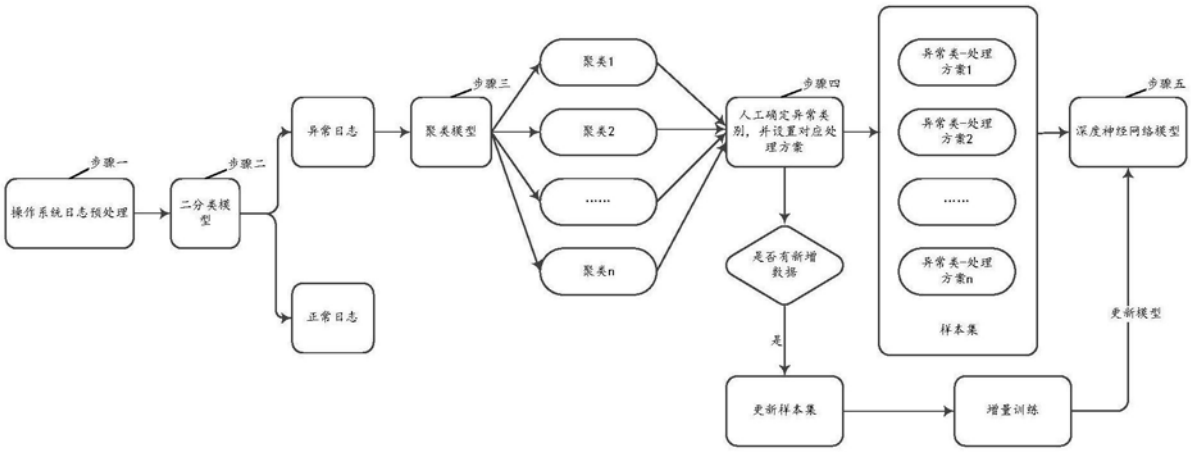

步骤一
操作系统日志预处理
步骤二
二分类模型
异常日志
正常日志
步骤三
聚类模型
聚类1
聚类2
……
聚类n
步骤四
人工确定异常类别，并设置对应处理方案
是否有新增数据
是
更新样本集
异常类-处理方案1
异常类-处理方案2
……
异常类-处理方案n
样本集
增量训练
步骤五
深度神经网络模型
更新模型

图3

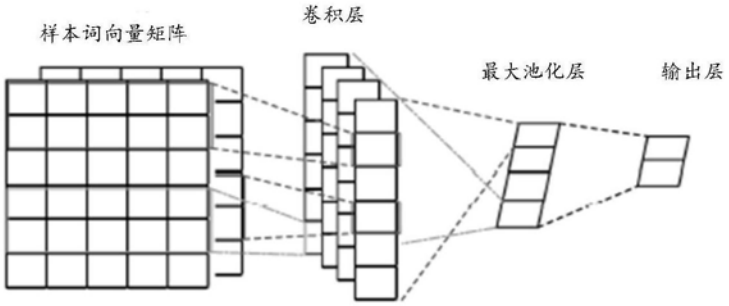

样本词向量矩阵
卷积层
最大池化层
输出层

图4

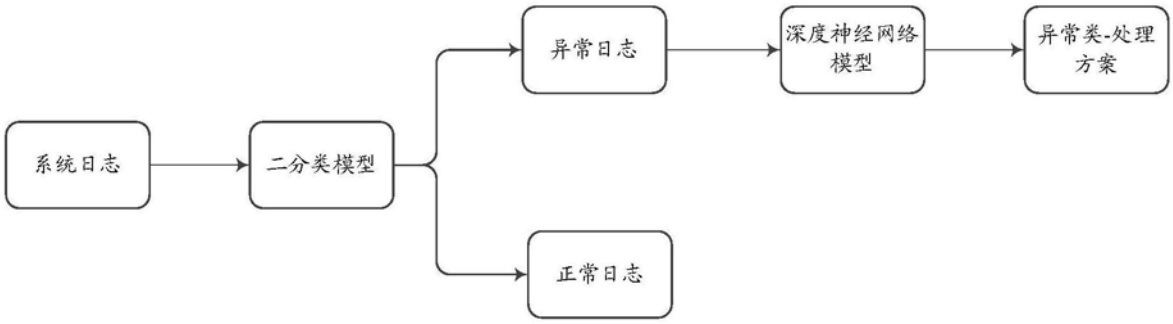

系统日志
二分类模型
异常日志
正常日志
深度神经网络模型
异常类-处理方案

图5

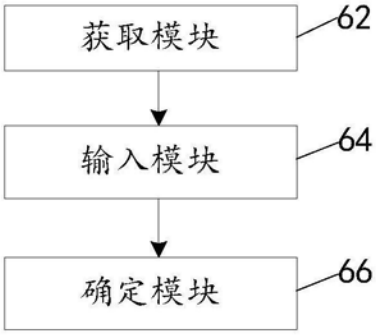


图6