



(12)发明专利申请

(10)申请公布号 CN 108377240 A

(43)申请公布日 2018.08.07

(21)申请号 201810124338.6

(22)申请日 2018.02.07

(71)申请人 平安科技(深圳)有限公司

地址 518052 广东省深圳市福田区八卦岭
八卦三路平安大厦六楼

(72)发明人 王元铭

(74)专利代理机构 广州华进联合专利商标代理
有限公司 44224

代理人 李文渊

(51)Int.Cl.

H04L 29/06(2006.01)

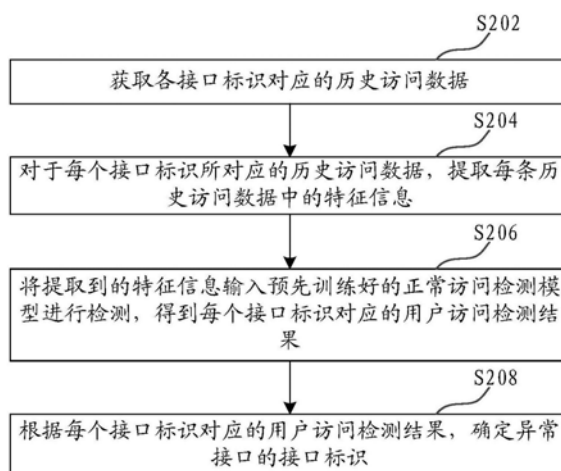
权利要求书2页 说明书12页 附图5页

(54)发明名称

异常接口检测方法、装置、计算机设备和存储介质

(57)摘要

本申请涉及一种异常接口检测方法、装置、计算机设备和存储介质。所述方法包括:获取各接口标识对应的历史访问数据;对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果;根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。采用本方法能够根据正常访问检测模型对历史访问数据进行检测,提高了用户访问检测结果的准确率。直接根据准确率较高的各接口标识分别对应的用户访问检测结果,确定异常接口的接口标识,提高了异常接口的检测准确率。



1. 一种异常接口检测方法,所述方法包括:
获取各接口标识对应的历史访问数据;
对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;
将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果;
根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。
2. 根据权利要求1所述的方法,其特征在于,所述对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息,包括:
对于每个接口标识所对应的历史访问数据,读取每条历史访问数据;
根据预设特征信息标识从读取到的历史访问数据中提取特征信息。
3. 根据权利要求2所述的方法,其特征在于,所述将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果,包括:
将提取到的特征信息输入到预先训练好的正常访问检测模型,得到所述读取到的历史访问数据是否为正常用户访问数据的检测结果;
根据得到的检测结果统计所述每个接口标识对应的正常用户访问量和异常访问量,以统计到正常用户访问量和异常用户访问量作为所述每个接口标识对应的用户访问检测结果。
4. 根据权利要求3所述的方法,其特征在于,所述根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识,包括:
根据所述每个接口标识对应的用户访问检测结果,统计所述每个接口标识分别对应的正常访问比例;
确定低于预设比例阈值的正常访问比例所对应的接口标识,以确定的接口标识对应的接口为异常接口。
5. 根据权利要求1所述的方法,其特征在于,所述根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,还包括:
定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量;
根据统计到的正常访问量和异常访问量生成检测报告。
6. 根据权利要求1所述的方法,其特征在于,所述根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,还包括:
根据所述每个接口标识对应的用户访问检测结果,从所述历史访问数据中提取正常用户访问数据;
统计提取到的正常用户访问数据量;
将统计到的正常用户访问数据量减去预设训练样本数据量,得到样本数据量差;
若所述样本数据量差大于预设数据量差,以提取到正常用户访问数据作为训练样本重新训练正常访问检测模型;
将预先训练好的正常访问检测模型替换为重新训练的正常访问检测模型。
7. 根据权利要求1所述的方法,其特征在于,所述预先训练好的正常访问检测模型的生成过程包括:

- 获取模型训练指令；
根据所述模型训练指令从数据库中获取模型样本数据；
提取所述模型样本数据中每条正常用户访问数据中的特征信息；
以提取到的特征信息作为输入，以正常用户访问作为输出训练正常访问检测模型，得到预先训练好的正常访问检测模型。
8. 一种异常接口检测装置，其特征在于，所述装置包括：
历史数据获取模块，用于获取各接口标识对应的历史访问数据；
特征信息提取模块，用于对于每个接口标识所对应的历史访问数据，提取每条历史访问数据中的特征信息；
检测结果得到模块，用于将提取到的特征信息输入预先训练好的正常访问检测模型进行检测，得到所述每个接口标识对应的用户访问检测结果；
异常接口确定模块，用于根据所述每个接口标识对应的用户访问检测结果，确定异常接口的接口标识。
9. 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，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中任一项所述方法的步骤。
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中任一项所述的方法的步骤。

异常接口检测方法、装置、计算机设备和存储介质

技术领域

[0001] 本申请涉及网络数据处理技术领域,特别是涉及一种异常接口检测方法、装置、计算机设备和存储介质。

背景技术

[0002] 随着网络技术的发展,各种网络安全方面的问题也不断的凸显出来。为了保证网络安全,需要对网络访问过程中的访问接口进行检测,以检测是否存在异常的网络访问情况。

[0003] 传统的网络访问检测,大都是通过对网络访问请求中的各中参数的检测,且传统的检测方式,都是人工预设检测方式。随着网络安全的需求越来越高,需要对异常接口进行检测,由于现在异常接口的隐蔽性也越来越强,使得根据人工预设检测方式对异常接口的检测效果越来越差,降低了异常接口的检测准确率。

发明内容

[0004] 基于此,有必要针对上述技术问题,提供一种能够提高异常接口的检测准确率的异常接口检测方法、装置、计算机设备和存储介质。

[0005] 一种异常接口检测方法,所述方法包括:

[0006] 获取各接口标识对应的历史访问数据;

[0007] 对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;

[0008] 将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果;

[0009] 根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。

[0010] 在其中一个实施例中,所述对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息,包括:

[0011] 对于每个接口标识所对应的历史访问数据,读取每条历史访问数据;

[0012] 根据预设特征信息标识从读取到的历史访问数据中提取特征信息。

[0013] 在其中一个实施例中,所述将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果,包括:

[0014] 将提取到的特征信息输入到预先训练好的正常访问检测模型,得到所述读取到的历史访问数据是否为正常用户访问数据的检测结果;

[0015] 根据得到的检测结果统计所述每个接口标识对应的正常用户访问量和异常访问量,以统计到正常用户访问量和异常用户访问量作为所述每个接口标识对应的用户访问检测结果。

[0016] 在其中一个实施例中,所述根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识,包括:

[0017] 根据所述每个接口标识对应的用户访问检测结果,统计所述每个接口标识分别对应的正常访问比例;

[0018] 确定低于预设比例阈值的正常访问比例所对应的接口标识,以确定的接口标识对应的接口为异常接口。

[0019] 在其中一个实施例中,所述根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,还包括:

[0020] 定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量;

[0021] 根据统计到的正常访问量和异常访问量生成检测报告。

[0022] 在其中一个实施例中,所述根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,还包括:

[0023] 根据所述每个接口标识对应的用户访问检测结果,从所述历史访问数据中提取正常用户访问数据;

[0024] 统计提取到的正常用户访问数据量;

[0025] 将统计到的正常用户访问数据量减去预设训练样本数据量,得到样本数据量差;

[0026] 若所述样本数据量差大于预设数据量差,以提取到正常用户访问数据作为训练样本重新训练正常访问检测模型;

[0027] 将预先训练好的正常访问检测模型替换为重新训练的正常访问检测模型。

[0028] 在其中一个实施例中,所述预先训练好的正常访问检测模型的生成过程包括:

[0029] 获取模型训练指令;

[0030] 根据所述模型训练指令从数据库中获取模型样本数据;

[0031] 提取所述模型样本数据中每条正常用户访问数据中的特征信息;

[0032] 以提取到的特征信息作为输入,以正常用户访问作为输出训练正常访问检测模型,得到预先训练好的正常访问检测模型。

[0033] 一种异常接口检测装置,所述装置包括:

[0034] 历史数据获取模块,用于获取各接口标识对应的历史访问数据;

[0035] 特征信息提取模块,用于对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;

[0036] 检测结果得到模块,用于将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果;

[0037] 异常接口确定模块,用于根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。

[0038] 一种计算机设备,包括存储器和处理器,所述存储器存储有计算机程序,所述处理器执行所述计算机程序时实现以下步骤:

[0039] 获取各接口标识对应的历史访问数据;

[0040] 对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;

[0041] 将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果;

- [0042] 根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。
- [0043] 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以下步骤:
- [0044] 获取各接口标识对应的历史访问数据;
- [0045] 对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;
- [0046] 将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到所述每个接口标识对应的用户访问检测结果;
- [0047] 根据所述每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。
- [0048] 上述异常接口检测方法、装置、计算机设备和存储介质,获取各接口标识对应的历史访问数据,对于每个接口标识对应的历史访问数据,提取每条历史访问数据中的特征信息,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到各接口标识分别对应的用户访问检测结果,根据正常访问检测模型对历史访问数据进行检测,提高了用户访问检测结果的准确率。直接根据准确率较高的各接口标识分别对应的用户访问检测结果,确定异常接口的接口标识,提高了异常接口的检测准确率。

附图说明

- [0049] 图1为一个实施例中异常接口检测方法的应用场景图;
- [0050] 图2为一个实施例中异常接口检测方法的流程示意图;
- [0051] 图3为另一个实施例中异常接口检测方法的流程示意图;
- [0052] 图4为一个实施例中生成检测报告的步骤的流程示意图;
- [0053] 图5为一个实施例中替换正常访问检测模型的步骤的流程示意图;
- [0054] 图6为一个实施例中生成正常访问检测模型的步骤的流程示意图;
- [0055] 图7为一个实施例中异常接口检测装置的结构框图;
- [0056] 图8为另一个实施例中异常接口检测装置的结构框图;
- [0057] 图9为再一个实施例中异常接口检测装置的结构框图;
- [0058] 图10为一个实施例中计算机设备的内部结构图。

具体实施方式

- [0059] 为了使本申请的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本申请进行进一步详细说明。应当理解,此处描述的具体实施例仅仅用以解释本申请,并不用于限定本申请。
- [0060] 本申请提供的异常接口检测方法,可以应用于如图1所示的应用环境中。其中,终端102通过网络与服务器104通过网络进行通信。其中,终端102可以但不限于各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备,服务器104可以用独立的服务器或者是多个服务器组成的服务器集群来实现。
- [0061] 在一个实施例中,如图2所示,提供了一种异常接口检测方法,以该方法应用于图1中的服务器为例进行说明,包括以下步骤:
- [0062] S202,获取各接口标识对应的历史访问数据。

[0063] 具体地,服务器对接口进行扫描,通过扫描获取各接口对应的接口标识,根据获取到的各接口标识,从数据库中查询各接口标识分别对应的历史访问数据,提取查询到的历史访问数据。

[0064] 在一个实施例中,服务器在接收到接口访问请求后,提取接口访问请求中的接口标识和接口访问请求中的接口访问数据,将提取到的接口访问数据与接口标识对应存储到数据库中,得到提取到的接口标识对应的历史访问数据。

[0065] S204,对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息。

[0066] 具体地,服务器对于每个接口标识对应的历史访问数据按访问时间进行排序,按照访问时间的顺序读取每条历史访问数据中,对读取到的历史访问数据进行解析,通过解析从读取到的历史访问数据中提取特征信息。

[0067] 其中,特征信息具体包括用户账号、终端网络地址、浏览器种类和终端设备类型中的至少一种。

[0068] 在一个实施例中,S204具体还包括以下内容:对于每个接口标识所对应的历史访问数据,读取每条历史访问数据;根据预设特征信息标识从读取到的历史访问数据中提取特征信息。

[0069] 具体地,服务器在数据库中对于每个接口标识都设置有一张对应的历史访问数据表。服务器在获取到接口标识对应的用户访问数据后,按照访问时间将用户访问数据添加到相应的历史访问数据表中。服务器按照每个接口标识对应的历史访问数据表中的排列顺序,逐条读取历史访问数据。服务器根据预设特征信息标识从读取到的历史访问数据中提取特征信息。例如,服务器从读取到的历史访问数据中提取用户账号、终端网络地址、浏览器类型和终端类型中的至少一种。

[0070] S206,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到每个接口标识对应的用户访问检测结果。

[0071] 其中,正常访问检测模型用于检测提取到的特征信息所对应的历史访问数据是否为正常用户在访问接口时产生的历史访问数据。

[0072] 具体地,服务器将提取到的特征信息作为输入,将提取到的特征信息输入至预先训练好的正常访问检测模型进行检测,获取预先训练好的正常访问检测模型输出的与提取到的特征信息对应的检测结果。其中,检测结果为检测提取到的特征信息所对应的历史访问数据是否为正常用户在访问接口时产生的历史访问数据。服务器将获取到的检测结果与相应的接口标识对应存储,得到每个接口标识对应的用户访问检测结果。

[0073] S208,根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。

[0074] 其中,用户访问检测结果中包括正常用户访问量,还可以包括异常用户访问量和用户访问总量中的至少一种。

[0075] 具体地,服务器从存储的用户访问检测接口中,获取每个接口标识对应的用户访问检测结果。服务器从每个接口标识对应的用户访问检测结果中统计每个接口标识对应的异常用户访问量,将统计到的异常用户访问量与预设异常访问量阈值比较。服务器确定大于预设异常访问量阈值的异常用户访问量,查询确定的异常用户访问量对应的接口标识,查询到的接口标识为异常接口的接口标识。

[0076] 在一个实施例中,服务器从每个接口标识对应的用户访问检测接口中统计每个接口标识对应的正常用户访问量,将统计到的正常用户访问量与预设正常访问量阈值比较。服务器确定小于预设正常访问量阈值的正常用户访问量,查询确定的正常用户访问量对应的接口标识,查询到的接口标识为异常接口的接口标识。服务器将检测到的异常接口关闭,或者拒绝异常接口的访问请求。

[0077] 本实施例中,获取各接口标识对应的历史访问数据,对于每个接口标识对应的历史访问数据,提取每条历史访问数据中的特征信息,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到各接口标识分别对应的用户访问检测结果,根据正常访问检测模型对历史访问数据进行检测,提高了用户访问检测结果的准确率。直接根据准确率较高的各接口标识分别对应的用户访问检测结果,确定异常接口的接口标识,提高了异常接口的检测准确率。

[0078] 在另一个实施例中,如图3所示,提供了一种异常接口检测方法,该方法包括以下内容:

[0079] S302,获取各接口标识对应的历史访问数据。

[0080] 具体地,服务器中存储着各接口标识分别对应的历史访问数据表。服务器从存储的历史访问数据表中读取各接口标识对应的历史访问数据。

[0081] S304,对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息。

[0082] 具体地,服务器对于每个接口标识所对应的历史访问数据中,逐条读取历史访问数据,并从读取到的历史访问数据中提取每个字段对应的信息作为特征信息。

[0083] S306,将提取到的特征信息输入到预先训练好的正常访问检测模型,得到读取到的历史访问数据是否为正常用户访问数据的检测结果。

[0084] 具体地,服务器将提取到的特征信息进行处理,通过处理将提取到的特征向量转换为特征向量,将转换得到的特征向量输入到预先训练好的正常访问检测模型,得到正常访问检测模型输出的与读取到的历史访问数据对应的检测结果。检测结果中包括判定读取到的历史访问数据是否为正常用户访问数据的内容,例如,读取到的历史访问数据的检测结果为真实用户访问接口产生的访问数据。

[0085] S308,根据得到的检测结果统计每个接口标识对应的正常用户访问量和异常访问量,以统计到正常用户访问量和异常用户访问量作为每个接口标识对应的用户访问检测结果。

[0086] 具体地,服务器将检测结果对应于接口标识存储。服务器根据每条历史访问数据对应的检测结果,统计每个接口标识对应的被判定为正常用户访问数据的条数和被判定为异常用户访问数据条数,以统计到的正常用户访问数据的条数作为正常用户访问量,同时以统计到的异常用户访问数据的条数作为异常用户访问量,以正常用户访问量和异常用户访问量作为用户访问检测结果。

[0087] S310,根据每个接口标识对应的用户访问检测结果,统计每个接口标识分别对应的正常访问比例。

[0088] 具体地,服务器提取每个接口标识对应的用户访问检测结果中的正常用户访问量和异常用户访问量,将提取到的正常用户访问量和异常用户访问量相加得到用户访问总

量,以正常用户访问量除以用户访问总量得到正常访问比例,得到每个接口标识分别对应的正常访问比例。

[0089] S312,确定低于预设比例阈值的正常访问比例所对应的接口标识,以确定的接口标识对应的接口为异常接口。

[0090] 具体地,服务器将每个接口标识对应的正常访问比例与预设比例阈值进行比较,从所有的接口标识中筛选低于预设比例阈值的正常访问比例所对应的接口标识,则判定筛选到的接口标识对应的接口为异常接口。

[0091] 在一个实施例中,服务器以异常访问量除以用户访问总量得到异常访问比例。服务器将每个接口标识对应的异常访问比例与预设比例阈值进行比较,通过比较从接口标识中筛选到异常访问比例高于预设比例阈值的接口标识,则判定筛选到的接口标识对应的接口为异常接口。

[0092] 本实施例中,通过预先训练好的正常访问检测模型对每条历史访问数据进行检测,以检测每条历史访问数据对应的用户是否为真实用户,根据每个接口标识对应历史访问数据的检测结果,统计每个接口标识对应的正常访问比例来确定异常接口的标识,即根据每个接口标识对应的真实用户访问量,来确定接口是否异常,从而提高了对异常接口的检测准确率。

[0093] 在一个实施例中,如图4所示,S208之后具体还包括生成检测报告的步骤,该步骤具体包括以下内容:

[0094] S402,定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量。

[0095] 具体地,服务器定期获取各接口标识对应的用户访问检测结果,对于每个接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量。

[0096] S404,根据统计到的正常访问量和异常访问量生成检测报告。

[0097] 具体地,服务器根据统计到的正常访问量和异常访问量相加得到用户访问总量,将统计到的正常访问量除以用户访问总量得到正常访问比例,将统计到的异常访问量除以用户访问总量得到异常访问比例,根据统计时间、接口标识、正常访问量、异常访问量、用户访问总量、正常访问比例和异常访问比例生成检测报告,将生成的检测报告与相应的接口标识对应存储。

[0098] 本实施例中,定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量,根据正常访问量和异常访问量生成相应的检测报告,以通过检测报告了解各接口标识对应的接口的访问情况。

[0099] 在一个实施例中,如图5所示,S208之后具体还包括替换正常访问检测模型的步骤,该步骤具体包括以下内容:

[0100] S502,根据每个接口标识对应的用户访问检测结果,从历史访问数据中提取正常用户访问数据。

[0101] 具体地,服务器获取每个接口标识对应的用户访问检测结果,根据用户访问检测结果,从历史访问数据中提取被判定为正常用户访问数据的历史访问数据。

[0102] 在一个实施例中,服务器将判定为正常用户访问数据的历史访问数据添加标记,服务器直接从历史访问数据中提取添加有标记的历史访问数据,提取到的历史访问数据为

被判定为正常用户访问数据的历史访问数据。

[0103] S504,统计提取到的正常用户访问数据量。

[0104] 具体地,服务器提取到正常用户访问数据后,对提取到的正常用户访问数据的数据量进行统计,经过统计得到正常用户访问数据量。

[0105] S506,将统计到的正常用户访问数据量减去预设训练样本数据量,得到样本数据量差。

[0106] 其中,预设训练样本数据量为预先训练正常访问检测模型所用到的训练样本的数据量。

[0107] 具体地,服务器将统计到的正常用户访问数据量减去预设训练数据量,以所得到的数据量差为样本数据量差。

[0108] S508,若样本数据量差大于预设数据量差,以提取到正常用户访问数据作为训练样本重新训练正常访问检测模型。

[0109] 具体地,服务器将计算得到的样本数据量差与预设数据量差进行比较,若样本数据量差大于预设数据量差,则以提取到的正常用户访问数据作为训练样本,提取训练样本中每条用户访问数据中的特征信息,以提取到的特征信息作为输入,以判定为正常用户访问数据作为输出,重新训练正常访问检测模型。

[0110] 在一个实施例中,服务器在重新训练正常访问检测模型后,将预设样本数据量更改为统计到的正常用户访问数据量。使得后续用来训练正常访问检测模型的样本数据量越来越大。

[0111] S510,将预先训练好的正常访问检测模型替换为重新训练的正常访问检测模型。

[0112] 具体地,服务器将预先训练好的正常访问检测模型进行替换,替换为重新训练的正常访问检测模型。当服务器再次获取到各接口标识对应的历史访问数据后,提取每条历史访问数据中的特征信息,将提取到的特征信息输入重新训练的正常访问检测模型,得到每个接口标识对应的用户访问检测结果。

[0113] 本实施例中,当历史访问数据中被判定为正常用户访问数据的数据量,超出预设训练样本数据量的差值大于预设数据量差时,以被判定为正常用户访问数据作为训练样本重新训练正常访问检测模型,将预先训练好的正常访问检测模型更新为重新训练的正常访问检测模型,从而提高了正常访问检测模型的检测准确性。

[0114] 在一个实施例中,如图6所示,异常接口检测方法还包括生成正常访问检测模型的步骤,具体包括以下内容:

[0115] S602,获取模型训练指令。

[0116] 具体地,终端检测到模型训练页面中的模型训练按钮被点击时,触发模型训练指令,将模型训练指令发送至服务器。服务器接收终端发送的模型训练指令。其中,模型训练指令用于指示服务器开始训练正常访问检测模型的指令。

[0117] S604,根据模型训练指令从数据库中获取模型样本数据。

[0118] 具体地,服务器提取模型训练指令中的样本数据存储地址,根据样本数据存储地址从数据库中提取模型样本数据。其中,模型样本数据中包括被标记为正常用户访问数据的访问数据。

[0119] S606,提取模型样本数据中每条正常用户访问数据中的特征信息。

[0120] 具体地,服务器逐条读取模型样本数据中的正常用户访问数据,对读取到的正常用户访问数据进行解析,通过解析提取正常用户访问数据中的特征信息。

[0121] S608,以提取到的特征信息作为输入,以正常用户访问作为输出训练正常访问检测模型,得到预先训练好的正常访问检测模型。

[0122] 具体地,服务器以从每条正常用户访问数据中提取到的特征信息作为输入,以正常用户访问作为输出训练正常访问检测模型,以训练得到的正常访问检测模型作为预先训练好的正常访问检测模型。

[0123] 本实施例中,根据模型训练指令从数据库中获取模型样本数据,根据模型样本数据训练正常访问检测模型,以通过正常访问检测模型来检测各接口标识对应历史访问数据,提高了历史访问数据的检测效率,从而提高了检测异常接口的效率。

[0124] 应该理解的是,虽然图1-6的流程图中的各个步骤按照箭头的指示依次显示,但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明,这些步骤的执行并没有严格的顺序限制,这些步骤可以以其它的顺序执行。而且,图1-6中的至少一部分步骤可以包括多个子步骤或者多个阶段,这些子步骤或者阶段并不必然是在同一时刻执行完成,而是可以在不同的时刻执行,这些子步骤或者阶段的执行顺序也不必然是依次进行,而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0125] 在一个实施例中,如图7所示,提供了一种异常接口检测装置700,包括:历史数据获取模块702、特征信息提取模块704、检测结果得到模块706和异常接口确定模块708,其中:

[0126] 历史数据获取模块702,用于获取各接口标识对应的历史访问数据。

[0127] 特征信息提取模块704,用于对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息。

[0128] 检测结果得到模块706,用于将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到每个接口标识对应的用户访问检测结果。

[0129] 异常接口确定模块708,用于根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。

[0130] 本实施例中,获取各接口标识对应的历史访问数据,对于每个接口标识对应的历史访问数据,提取每条历史访问数据中的特征信息,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到各接口标识分别对应的用户访问检测结果,根据正常访问检测模型对历史访问数据进行检测,提高了用户访问检测结果的准确率。直接根据准确率较高的各接口标识分别对应的用户访问检测结果,确定异常接口的接口标识,提高了异常接口的检测准确率。

[0131] 在一个实施例中,特征信息提取模块704还用于对于每个接口标识所对应的历史访问数据,读取每条历史访问数据;根据预设特征信息标识从读取到的历史访问数据中提取特征信息。

[0132] 检测结果得到模块706还用于将提取到的特征信息输入到预先训练好的正常访问检测模型,得到读取到的历史访问数据是否为正常用户访问数据的检测结果;根据得到的检测结果统计每个接口标识对应的正常用户访问量和异常访问量,以统计到正常用户访问

量和异常用户访问量作为每个接口标识对应的用户访问检测结果。

[0133] 异常接口确定模块708还用于根据每个接口标识对应的用户访问检测结果,统计每个接口标识分别对应的正常访问比例;确定低于预设比例阈值的正常访问比例所对应的接口标识,以确定的接口标识对应的接口为异常接口。

[0134] 本实施例中,通过预先训练好的正常访问检测模型对每条历史访问数据进行检测,以检测每条历史访问数据对应的用户是否为真实用户,根据每个接口标识对应历史访问数据的检测结果,统计每个接口标识对应的正常访问比例来确定异常接口的标识,即根据每个接口标识对应的真实用户访问量,来确定接口是否异常,从而提高了对异常接口的检测准确率。

[0135] 在一个实施例中,异常接口检测装置700具体还包括检测报告生成模块。

[0136] 检测报告生成模块还用于定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量;根据统计到的正常访问量和异常访问量生成检测报告。

[0137] 本实施例中,定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量,根据正常访问量和异常访问量生成相应的检测报告,以通过检测报告了解各接口标识对应的接口的访问情况。

[0138] 在一个实施例中,如图8所示,异常接口检测装置700具体还包括:访问数据提取模块710、数据量统计模块712、数据量差得到模块714、模型重新训练模块716和检测模型替换模块718。

[0139] 访问数据提取模块710,用于根据每个接口标识对应的用户访问检测结果,从历史访问数据中提取正常用户访问数据。

[0140] 数据量统计模块712,用于统计提取到的正常用户访问数据量。

[0141] 数据量差得到模块714,用于将统计到的正常用户访问数据量减去预设训练样本数据量,得到样本数据量差。

[0142] 模型重新训练模块716,用于若样本数据量差大于预设数据量差,以提取到正常用户访问数据作为训练样本重新训练正常访问检测模型。

[0143] 检测模型替换模块718,用于将预先训练好的正常访问检测模型替换为重新训练的正常访问检测模型。

[0144] 实施例中,当历史访问数据中被判定为正常用户访问数据的数据量,超出预设训练样本数据量的差值大于预设数据量差时,以被判定为正常用户访问数据作为训练样本重新训练正常访问检测模型,将预先训练好的正常访问检测模型更新为重新训练的正常访问检测模型,从而提高了正常访问检测模型的检测准确性。

[0145] 在一个实施例中,如图9所示,异常接口检测装置700具体还包括以下内容:训练指令获取模块720、样本数据获取模块722、特征信息提取模块724和检测模型训练模块726。

[0146] 训练指令获取模块720,用于获取模型训练指令。

[0147] 样本数据获取模块722,用于根据模型训练指令从数据库中获取模型样本数据。

[0148] 特征信息提取模块724,用于提取模型样本数据中每条正常用户访问数据中的特征信息。

[0149] 检测模型训练模块726,用于以提取到的特征信息作为输入,以正常用户访问作为

输出训练正常访问检测模型,得到预先训练好的正常访问检测模型。

[0150] 本实施例中,根据模型训练指令从数据库中获取模型样本数据,根据模型样本数据训练正常访问检测模型,以通过正常访问检测模型来检测各接口标识对应历史访问数据,提高了历史访问数据的检测效率,从而提高了检测异常接口的效率。

[0151] 关于异常接口检测装置的具体限定可以参见上文中对于异常接口检测方法的限定,在此不再赘述。上述异常接口检测装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中,也可以以软件形式存储于计算机设备中的存储器中,以便于处理器调用执行以上各个模块对应的操作。

[0152] 在一个实施例中,提供了一种计算机设备,该计算机设备可以是服务器,其内部结构图可以如图10所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中,该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储各接口标识对应的历史访问数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种异常接口检测方法。

[0153] 本领域技术人员可以理解,图10中示出的结构,仅仅是与本申请方案相关的部分结构的框图,并不构成对本申请方案所应用于其上的计算机设备的限定,具体的计算机设备可以包括比图中所示更多或更少的部件,或者组合某些部件,或者具有不同的部件布置。

[0154] 在一个实施例中,提供了一种计算机设备,包括存储器和处理器,所述存储器存储有计算机程序,处理器执行计算机程序时实现以下步骤:获取各接口标识对应的历史访问数据;对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到每个接口标识对应的用户访问检测结果;根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。

[0155] 在一个实施例中,对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息,包括:对于每个接口标识所对应的历史访问数据,读取每条历史访问数据;根据预设特征信息标识从读取到的历史访问数据中提取特征信息。

[0156] 在一个实施例中,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到每个接口标识对应的用户访问检测结果,包括:将提取到的特征信息输入到预先训练好的正常访问检测模型,得到读取到的历史访问数据是否为正常用户访问数据的检测结果;根据得到的检测结果统计每个接口标识对应的正常用户访问量和异常访问量,以统计到正常用户访问量和异常用户访问量作为每个接口标识对应的用户访问检测结果。

[0157] 在一个实施例中,根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识,包括:根据每个接口标识对应的用户访问检测结果,统计每个接口标识分别对应的正常访问比例;确定低于预设比例阈值的正常访问比例所对应的接口标识,以确定的接口标识对应的接口为异常接口。

[0158] 在一个实施例中,根据每个接口标识对应的用户访问检测结果,确定异常接口的

接口标识之后,处理器执行计算机程序时还实现以下步骤:定期根据各接口标识对应的用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量;根据统计到的正常访问量和异常访问量生成检测报告。

[0159] 在一个实施例中,根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,处理器执行计算机程序时还实现以下步骤:根据每个接口标识对应的用户访问检测结果,从历史访问数据中提取正常用户访问数据;统计提取到的正常用户访问数据量;将统计到的正常用户访问数据量减去预设训练样本数据量,得到样本数据量差;若样本数据量差大于预设数据量差,以提取到正常用户访问数据作为训练样本重新训练正常访问检测模型;将预先训练好的正常访问检测模型替换为重新训练的正常访问检测模型。

[0160] 在一个实施例中,处理器执行计算机程序时还实现以下步骤:获取模型训练指令;根据模型训练指令从数据库中获取模型样本数据;提取模型样本数据中每条正常用户访问数据中的特征信息;以提取到的特征信息作为输入,以正常用户访问作为输出训练正常访问检测模型,得到预先训练好的正常访问检测模型。

[0161] 本实施例中,获取各接口标识对应的历史访问数据,对于每个接口标识对应的历史访问数据,提取每条历史访问数据中的特征信息,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到各接口标识分别对应的用户访问检测结果,根据正常访问检测模型对历史访问数据进行检测,提高了用户访问检测结果的准确率。直接根据准确率较高的各接口标识分别对应的用户访问检测结果,确定异常接口的接口标识,提高了异常接口的检测准确率。

[0162] 在一个实施例中,提供了一种计算机可读存储介质,其上存储有计算机程序,计算机程序被处理器执行时实现以下步骤:

[0163] 获取各接口标识对应的历史访问数据;对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息;将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到每个接口标识对应的用户访问检测结果;根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识。

[0164] 在一个实施例中,对于每个接口标识所对应的历史访问数据,提取每条历史访问数据中的特征信息,包括:对于每个接口标识所对应的历史访问数据,读取每条历史访问数据;根据预设特征信息标识从读取到的历史访问数据中提取特征信息。

[0165] 在一个实施例中,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到每个接口标识对应的用户访问检测结果,包括:将提取到的特征信息输入到预先训练好的正常访问检测模型,得到读取到的历史访问数据是否为正常用户访问数据的检测结果;根据得到的检测结果统计每个接口标识对应的正常用户访问量和异常访问量,以统计到正常用户访问量和异常用户访问量作为每个接口标识对应的用户访问检测结果。

[0166] 在一个实施例中,根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识,包括:根据每个接口标识对应的用户访问检测结果,统计每个接口标识分别对应的正常访问比例;确定低于预设比例阈值的正常访问比例所对应的接口标识,以确定的接口标识对应的接口为异常接口。

[0167] 在一个实施例中,根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,计算机程序被处理器执行时还实现以下步骤:定期根据各接口标识对应的

用户访问检测结果,统计各接口标识对应的正常访问量和异常访问量;根据统计到的正常访问量和异常访问量生成检测报告。

[0168] 在一个实施例中,根据每个接口标识对应的用户访问检测结果,确定异常接口的接口标识之后,计算机程序被处理器执行时还实现以下步骤:根据每个接口标识对应的用户访问检测结果,从历史访问数据中提取正常用户访问数据;统计提取到的正常用户访问数据量;将统计到的正常用户访问数据量减去预设训练样本数据量,得到样本数据量差;若样本数据量差大于预设数据量差,以提取到正常用户访问数据作为训练样本重新训练正常访问检测模型;将预先训练好的正常访问检测模型替换为重新训练的正常访问检测模型。

[0169] 在一个实施例中,计算机程序被处理器执行时还实现以下步骤:获取模型训练指令;根据模型训练指令从数据库中获取模型样本数据;提取模型样本数据中每条正常用户访问数据中的特征信息;以提取到的特征信息作为输入,以正常用户访问作为输出训练正常访问检测模型,得到预先训练好的正常访问检测模型。

[0170] 本实施例中,获取各接口标识对应的历史访问数据,对于每个接口标识对应的历史访问数据,提取每条历史访问数据中的特征信息,将提取到的特征信息输入预先训练好的正常访问检测模型进行检测,得到各接口标识分别对应的用户访问检测结果,根据正常访问检测模型对历史访问数据进行检测,提高了用户访问检测结果的准确率。直接根据准确率较高的各接口标识分别对应的用户访问检测结果,确定异常接口的接口标识,提高了异常接口的检测准确率。

[0171] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的计算机程序可存储于一非易失性计算机可读取存储介质中,该计算机程序在执行时,可包括如上述各方法的实施例的流程。其中,本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0172] 以上实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0173] 以上所述实施例仅表达了本申请的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本申请构思的前提下,还可以做出若干变形和改进,这些都属于本申请的保护范围。因此,本申请专利的保护范围应以所附权利要求为准。

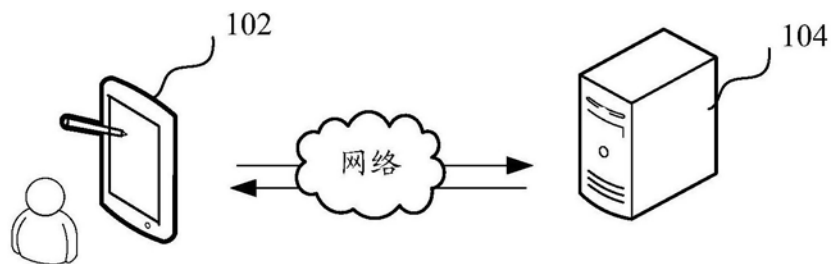


图1

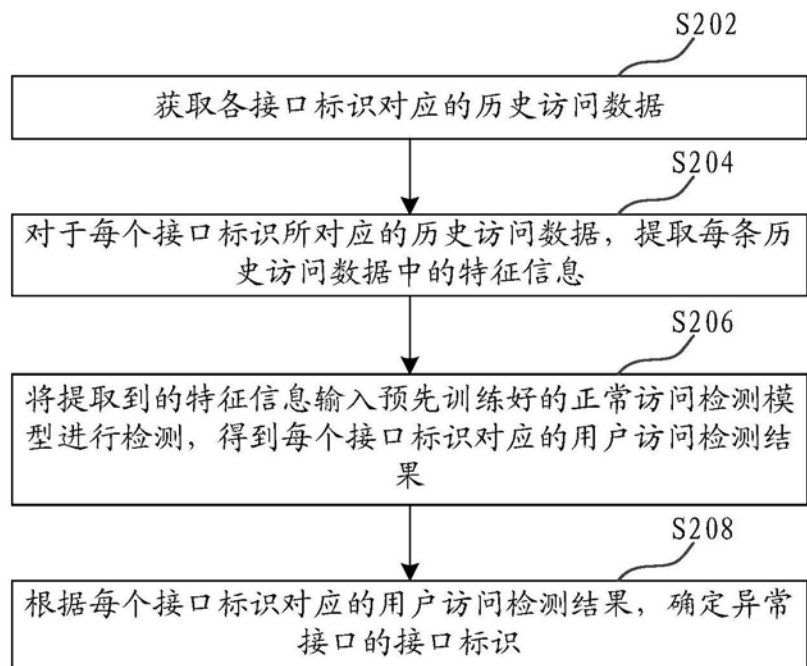


图2

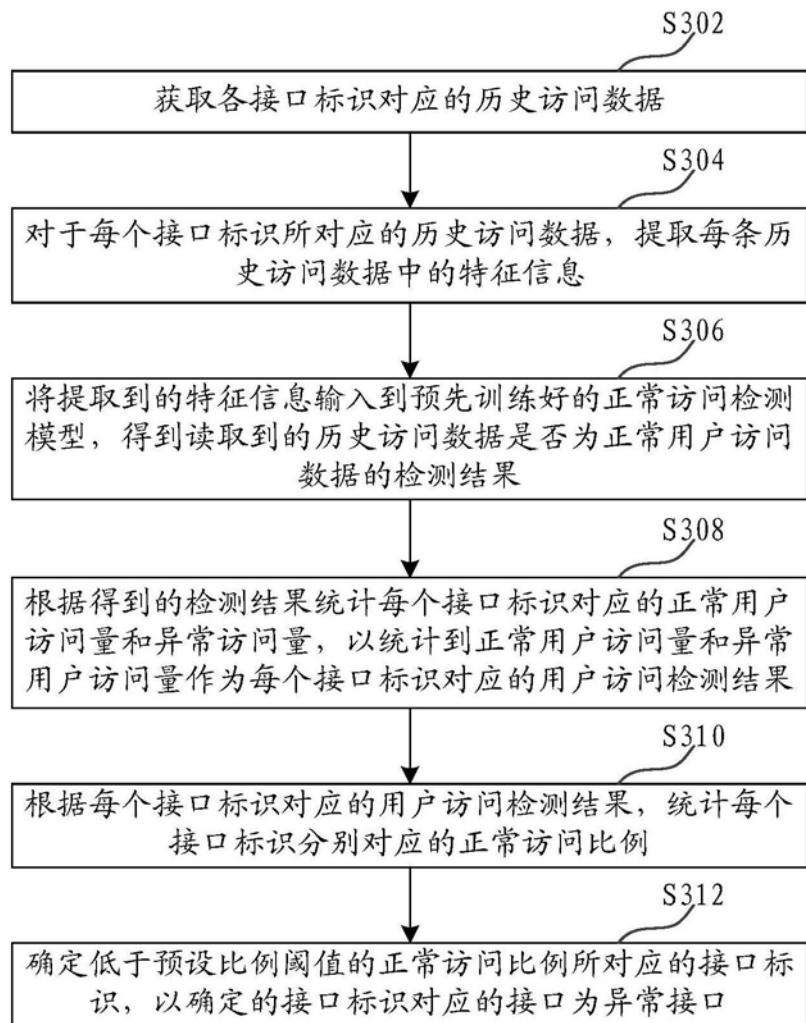


图3

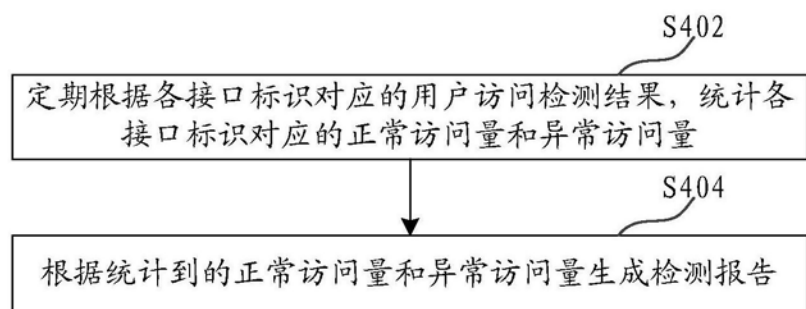


图4

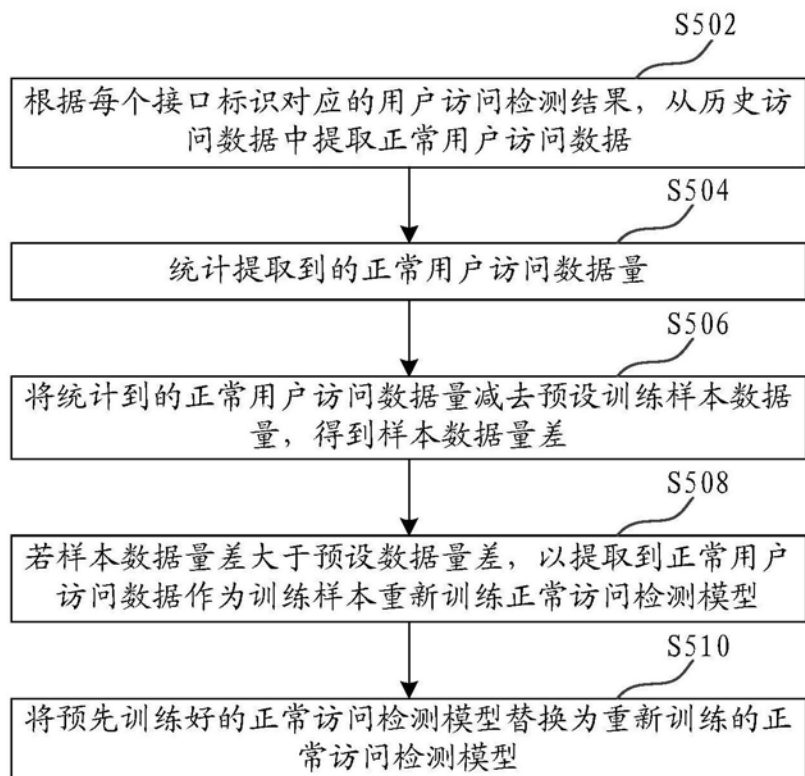


图5

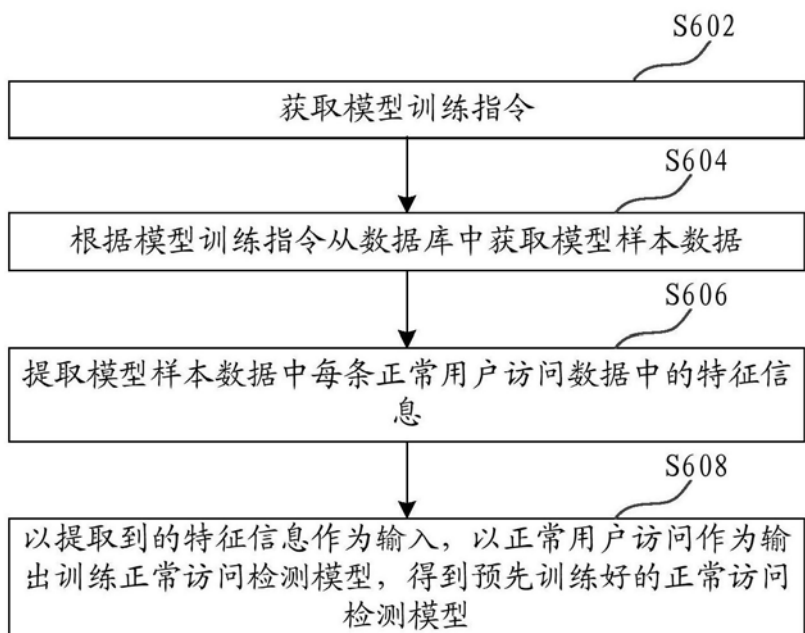


图6

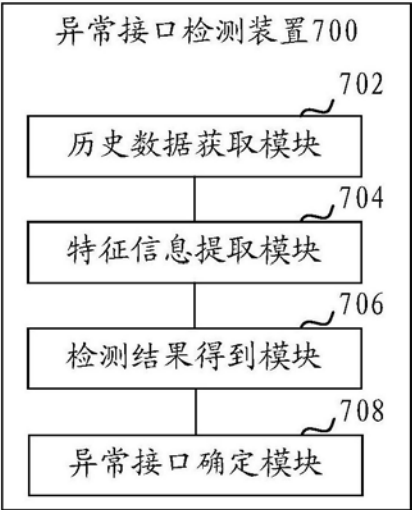


图7

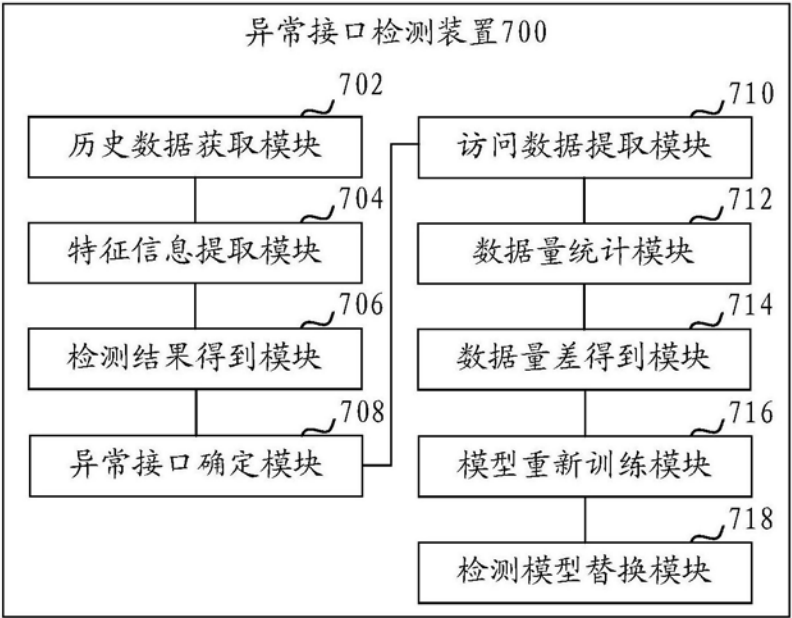


图8

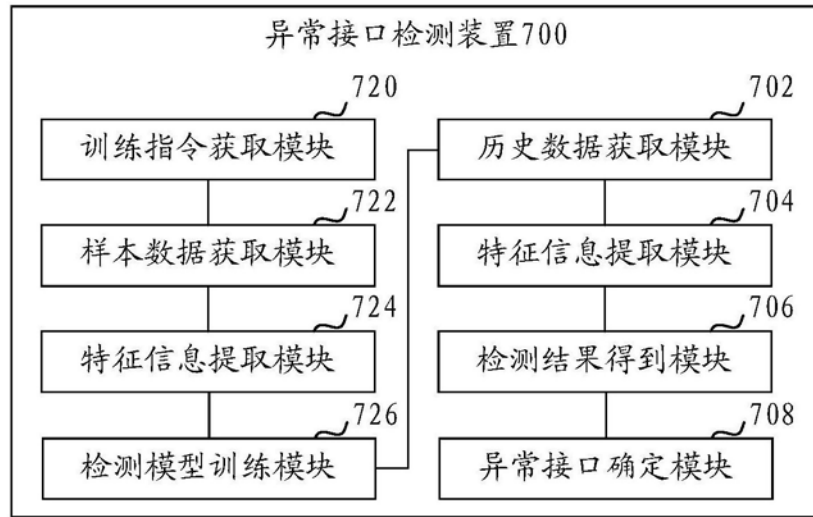


图9

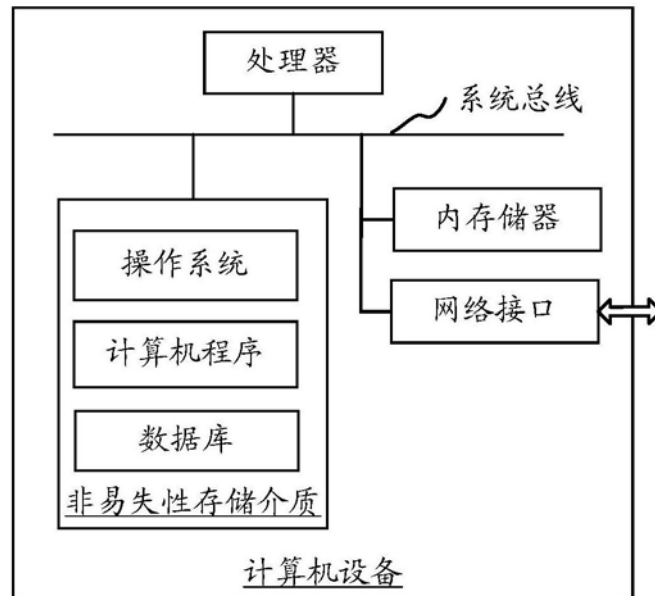


图10