(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 12 月 30 日 (30.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/258509 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/103663

(22) 国际申请日: 2019 年 8 月 30 日 (30.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910580052.3 2019年6月28日 (28.06.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 黎立桂 (LI, Ligui); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 北京市立方律师事务所 (LIFANG & PARTNERS); 中国北京市东城区香河园街1号院信德京汇中心12层, Beijing 100028 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

WO 2020/258509 A1

(54) **Title:** METHOD AND DEVICE FOR ISOLATING ABNORMAL ACCESS OF TERMINAL DEVICE

(54) 发明名称: 终端设备异常访问的隔离方法和装置

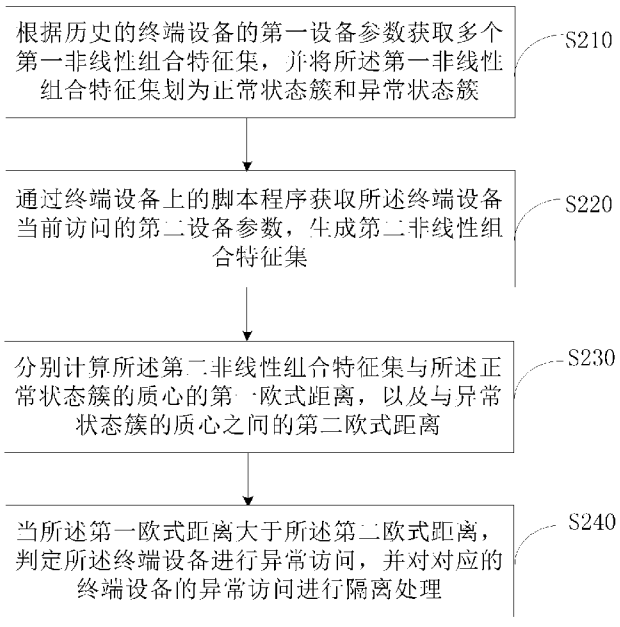


图 2

(57) **Abstract:** A method and a device for isolating an abnormal access of a terminal device, applied to the technical field of security detection, wherein the method comprises acquiring a plurality of first non-linear combined feature sets according to a historical first device parameter of the terminal device, and dividing the first non-linear combined feature sets into a normal state cluster and an abnormal state cluster (S210); acquiring a second device parameter currently accessed by the terminal device through a script program on the terminal device, and generating a second non-linear combined feature set (S220); respectively calculating a first Euclidean

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明：
— 发明人资格(细则4.17(iv))

本国际公布：
— 包括国际检索报告(条约第21条(3))。

distance between the second non-linear combined feature set and the centroid of the normal state cluster, and a second Euclidean distance between the second non-linear combined feature set and the centroid of the abnormal state cluster (S230); and when the first Euclidean distance is greater than the second Euclidean distance, determining that the terminal device performs an abnormal access, and isolating the abnormal access to a corresponding terminal device (S240). The method is beneficial to improve the isolation capability of abnormal access to the current terminal device by the terminal device.

(57) 摘要：一种终端设备异常访问的隔离方法和装置，应用于安全检测技术领域，所述方法包括根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇(S210)；通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集(S220)；分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离(S230)；当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理(S240)。该方法有利于提高对终端设备当前终端设备异常访问的隔离能力。

终端设备异常访问的隔离方法和装置

本申请要求于 2019 年 6 月 28 日提交中国专利局、申请号为 201910580052.3，发明名称为“终端设备异常访问的隔离方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及网络检测技术领域，具体而言，本申请涉及一种终端设备异常访问的隔离方法和装置。

背景技术

在终端设备网络访问时，提供网络连接的服务器可以获取终端设备发送的访问请求终端设备的点击和拖动轨迹的数据。发明人意识到，目前判断该终端设备是否为正常的终端设备，通常可通过终端设备的点击和拖动轨迹的数据检测该发起访问请求的终端设备属于正常的终端设备还是网络爬虫。但是，由于该检测方法不容易区分正常访问的终端设备和网络爬虫，导致检测的错误率较高，容易将正常访问的终端设备检测判定为异常访问，影响正常的用户访问，导致不容易对网络爬虫进行隔离处理。

发明内容

为克服以上技术问题，特别是现有技术中通过终端设备登录网络时，根据用户的使用痕迹数据容易将真实用户判别为异常用户的问题，特提出以下技术方案：

第一方面，本申请提供一种终端设备异常访问的隔离方法，包括以下步骤：

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备

参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

第二方面，本申请还提供一种终端设备异常访问的隔离装置，包括：

获取模块，用于根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；

生成模块，用于通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；

计算模块，用于分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

隔离模块，用于当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

第三方面，本申请还提供一种服务器，包括：

一个或多个处理器；

存储器；

一个或多个计算机程序，其中所述一个或多个计算机程序被存储在所述存储器中并被配置为由所述一个或多个处理器执行，所述一个或多个计算机程序配置用于执行一种终端设备异常访问的隔离方法，所述终端设备异常访问的隔离方法包括以下步骤：

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

第四方面，本申请还提供一种计算机可读存储介质，所述计算机可读

存储介质上存储有计算机程序，该计算机程序被处理器执行时实现一种终端设备异常访问的隔离方法，所述终端设备异常访问的隔离方法包括以下步骤：

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

本申请所提供的技术方案更容易对正常访问的终端设备和网络爬虫进行区分，降低网络爬虫访问入侵网站的概率，有效对网络爬虫进行隔离。

附图说明

图 1 是本申请中的实施例执行终端设备异常访问的隔离方案的应用环境图；

图 2 是本申请中的一个实施例的终端设备异常访问的隔离方法的流程图；

图 3 是本申请中的另一个实施例的终端设备异常访问的隔离方法的流程图；

图 4 为本申请中的一个实施例的终端设备异常访问的隔离装置的示意图；

图 5 为本申请中的一个实施例的服务器的结构示意图。

具体实施方式

本技术领域技术人员可以理解，这里所使用的“终端”、“终端设备”既包括无线信号接收器的设备，其仅具备无发射能力的无线信号接收器的设备，又包括接收和发射硬件的设备，其具有能够在双向通信链路上，执行双向通信的接收和发射硬件的设备。这种设备可以包括：蜂窝或其他通信设备，其具有单线路显示器或多线路显示器或没有多线路显示器的蜂窝或其他通信设备；PCS（Personal Communications Service，个人通信系统），其可以组合语音、数据处理、传真和/或数据通信能力；PDA（Personal Digital Assistant，个人数字助理），其可以包括射频接收器、寻呼机、

互联网/内联网访问、网络浏览器、记事本、日历和/或 GPS（Global Positioning System，全球定位系统）接收器；常规膝上型和/或掌上型计算机或其他设备，其具有和/或包括射频接收器的常规膝上型和/或掌上型计算机或其他设备。这里所使用的“终端”、“终端设备”可以是便携式、可运输、安装在交通工具（航空、海运和/或陆地）中的，或者适合于和/或配置为在本地运行，和/或以分布形式，运行在地球和/或空间的任何其他位置运行。这里所使用的“终端”、“终端设备”还可以是通信终端、上网终端、音乐/视频播放终端，例如可以是 PDA、MID（Mobile Internet Device，移动互联网设备）和/或具有音乐/视频播放功能的移动电话，也可以是智能电视、机顶盒等设备。

参考图 1 所示，图 1 是本申请实施例方案的应用环境图；该实施例中，本申请技术方案可以基于服务器上实现，如图 1 中，终端设备 110 和 120 可以通过 internet 网络访问服务器 130，终端设备 110 和/或 120 向服务器 130 发出的网络请求，服务器 130 根据网络请求进行数据交互。在进行数据交互时，服务器 130 根据终端设备 110 和/或 120 的请求信息获取终端设备 110 和/或 120 的访问数据和属性数据，并根据该数据对该终端设备进行异常检测。

为了解决目前检测异常数据容易将真实用户判别为异常用户的问题，本申请提供了一种终端设备异常访问的隔离方法。可参考图 2，图 2 是一个实施例的终端设备异常访问的隔离方法的流程图，该方法包括以下步骤：

S210、根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇。

服务器与终端设备进行数据交互的时候，根据终端设备发出的网络请求，获取该终端设备的相关参数。在该步骤中，服务器从历史的终端设备所发出的网络请求中得到第一设备参数，服务器对该第一设备参数进行解析，并根据解析的结果获取多个第一非线性组合特征集。

所述第一非线性组合特征集是与服务器进行过数据交互的终端设备一个访问记录生成的特征集，该第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据。例如属性数据可包括终端设备的型号、终端设备的屏幕分辨率 x*y 或浏览器的可用屏幕分辨率 X*Y，访问数据可包括终端设备向服务器发出请求的频率等。

所述第一非线性组合特征集对应的特征信息，在本实施例中，该特征信息具体为对应的特征值。设定对应的坐标，并在坐标上标注历史的终端设备每一次的访问记录生成的特征集或一个 n 维数据点。关于不同访问记录形成的特征集在坐标上形成对应的正常状态簇和异常状态簇。根据正常情况绝对大于异常情况的考虑，大簇是正常状态簇，小簇是异常状态簇。

进一步地，为了消除变量间的量纲关系，从而使数据具有可比性，在

对特征值标注之前，对各个特征集中的特征信息值进行标准化。例如，在得到的每一次访问记录的特征集中可能包括百分制的变量与一个 5 分值的变量，只有将所有的数据标准化，才能够在同一标准中进行比较。

S220、通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集。

为了可实时检测所述终端设备的网络访问是否处理异常状态，根据检测需要，对所述终端设备当前每一次访问的状态进行检测。在本步骤中，所述服务器通过网络连接，向所述终端设备提供脚本程序，以获取所述终端设备当前每一次访问的第二设备参数。所述第二设备参数与所述第一设备参数的性质相同。所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据。

服务器根据所述第二设备参数进行解析，提取得到所述第二设备参数的特征信息，根据所述特征信息生成关于当前向服务器发出网络请求的终端设备的第二非线性组合特征集。

所述第二非线性组合特征集所包括的特征信息至少与所述第一非线性组合特征集种的特征信息对应，以便后续进行对比。

S230、分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离。

在该步骤中，通过与历史的终端设备的网络访问的正常状态进行比较，得到当前访问服务器的终端设备的网络访问是否为异常状态。

在标注所述第一非线性组合特征集的特征信息的坐标上，标注从步骤 S220 生成的并经过标准化处理得到所述第二非线性组合特征集的特征信息，得到相应的数据点。

在利用所述坐标，分别计算所述第二非线性组合特征集得到的数据点至所述与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离，得到所述第二非线性组合特征集分别与正常状态簇和与异常状态簇的实际距离。

S240、当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。根据步骤 S230 得到的第一欧式距离和第二欧式距离，并进行比较。若比较的结果为所述第一欧式距离大于所述第二欧式距离，即表示当前终端设备向服务器发起网络访问请求更接近异常状态，这时，判定所述当前终端设备向服务器发起网络访问请求为异常访问状态。

对于终端设备当前发起的网络请求被判定为异常访问请求，服务器直接对该网络请求进行隔离处理，即拒绝响应该异常访问请求，并重新要求所述终端设备进行访问验证；若终端设备当前发起的网络请求被判定为正常访问请求，则直接响应请求。

在本申请中，所述第一非线性组合特征集和所述第二非线性组合特征集各自是由多个特征值集合而成的。每一次访问所形成的非线性组合特征

集的多个特征值形成对应的维度向量。因此，在本申请中，每个访问所产生的所述第一非线性特征集和所述第一非线性特征集均以其维度向量进行衡量。而对于所述第一非线性特征集的正常状态簇和异常状态簇，是由对应的多个所述第一非线性特征集的维度向量所形成的状态簇。因此，在本申请的技术方案中的欧式距离的计算是对对应的非线性特征集的维度向量之间的空间距离的计算。

本申请提供的一种终端设备异常访问的隔离方法，通过历史的终端设备发起网络访问的第一非线性组合特征集的数据点划为正常状态簇和异常状态簇，并将当前终端设备向服务器发起网络访问请求得到的第二非线性组合特征集分别与正常状态簇和异常状态簇进行欧式距离计算，并根据距离间的对比，得到当前终端设备所发起的网络访问请求是否为异常状态。本申请将所述终端设备网络访问所产生数据形成第一、第二非线性组合特征集，并在坐标上标注将从第一、第二非线性组合特征集得到的数据点。本申请的技术方案将终端设备发起的网络访问请求所产生的数据进行处理后直接进行对比，避免现有技术中仅对用户使用终端设备的所产生的使用记录如用户验证过程中的点击时间和拖动轨迹等数据作为异常检测的依据所造成容易将真实用户判别为异常用户的问题，更为准确地反应当前终端设备向服务器发起的网络访问请求的状态，并以更为简单、直观的数据对比方式得到异常检测的结果，有利于对异常检测对应的异常访问进行隔离处理。在上述方案描述的基础上，步骤 S230 之前，即在分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离与异常状态簇的质心之间的第二欧式距离之前，还包括：

分别对所述第一非线性组合特征集的正常状态簇和异常状态簇预设初始质心。

在该步骤中，特别是对于从未与所述第二非线性组合特征集进行欧式距离的计算的情况下，分别根据正常状态簇和异常状态簇的维度向量求取对应质心的位置，得到对应的初始质心。所述质心是对应状态簇的质量中心，其会根据状态簇的维度向量的集中状态的变化而改变。

当初次计算所述第二非线性组合特征集与所述正常状态簇和异常状态簇的欧式距离时，只需计算所述第二非线性组合特征集与所述初始质心的距离便可。

若需继续计算后续终端设备发出网络请求所产生的所述第二非线性组合特征集与正常状态簇和异常状态簇的距离，只需根据之前新产生的所述第二非线性组合特征集的数据点的位置的值直接与所述初始质心的位置的值便可求得新的质心的位置的值，避免每次新增了历史的终端设备的网络请求后，需重新根据所有正常状态簇和异常状态簇的数据点计算质心。这样，有利于控制后续异常检测的运算量，以便保持终端设备异常访问的隔离效率。

根据一般的正常用户的登录网络的使用习惯，对于一个终端设备在短

时间段内向服务器发出网络请求一般情况下会多于一次，因此，就同一终端设备可在短时间段内可能会向服务器发出多于一次的网络请求。

对此，对应的步骤 S230 可包括：

S231、分别计算在设定时间段内每一次访问的所述第二非线性组合特征集与正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

S232、就同一终端设备在设定时间段内获取排序在前的设定个数所述第一欧式距离的集合和所述第二欧式距离的集合，并分别得到所述第一欧式距离的集合和所述第二欧式距离的集合的众数值；

S233、并分别以所述第一欧式距离的集合和所述第二欧式距离的集合的众数值作为所述同一终端设备在设定时间段内所述第一欧式距离和所述第二欧式距离。

具体地，同一终端设备每向服务器发出一次网络请求，就会形成一对对应的第一欧式距离和第二欧式距离。

在设定时间段内，获取同一终端设备每一次发出网络请求时的第二非线性组合特征集，并根据该第二非线性组合特征集中的多个特征值得到对应的维度向量。在本实施例中，根据第二非线性组合特征集的维度向量分别与所述正常状态簇的质心和所述异常状态簇的质心对应求取同一终端设备每一次网络请求的所述第一欧式距离和第二欧式距离。在设定时间段内，分别根据同一终端设备多次发出网络请求所得到的多个第一欧式距离和多个第二欧式距离中距离值的大小获取排序在前的设定个数的所述第一欧式距离的集合和所述第二欧式距离的集合，如分所述设定的个数为 100，并分别就该 100 个所述第一欧式距离所组成的集合和所述第二欧式距离所组成的集合中得到各自的众数值，即在这设定个数中出现个数最多的距离值。并以该得到的所述第一欧式距离的集合和所述第二欧式距离的集合对应的众数值作为对应同一终端设备在设定时间段内的所述第一欧式距离和所述第二欧式距离。这样，可简化同一终端设备在短时间段内所产生的待处理数据，尽量排除因偶然因素所造成的异常数据影响相关欧式距离值的结果。

对于步骤 S220，包括：

A1、通过终端设备上的脚本程序获取当前访问的第二设备参数，生成第二非线性组合特征集，并从所述第二非线性组合特征集中获取终端设备的用户代理；

A2、通过对用户代理进行解析，获取所述终端设备的型号。

在步骤 A1-A2 中，服务器通过终端设备的检测脚本获取当前的第二设备参数，得到关于发出网络请求的终端设备当前的第二非线性组合特征集，并从该第二非线性组合特征集中获取该终端设备的用户代理。通过对该用户代理进行解析，获得对应所述终端设备的型号。

在此基础上，通过在步骤 S220 之后，还可以包括：

A3、根据所述终端设备的型号，得到所述终端设备的第二非线性组合特征集的各个特征数值的正常范围；

A4、将所述第二非线性组合特征集的特征数值与所述正常范围进行比较；

A5、得到所述正常范围以外的特征数值对应非线性组合特征集作为第二非线性组合特征集。

根据上述步骤 A2 得到的终端设备的型号，对所述终端设备的第二非线性组合特征集的各个特征数值分别限定正常范围值。

将获取所述终端设备的第二非线性组合特征集的各个特征数值，与上述得到的对应型号的正常范围值进行对比，根据对比的结果预测对应地终端设备是否处于异常状态，以此作为对网络爬虫进行隔离的依据。

如果对应的终端设备的某一特征值不在其型号的正常范围值内，则所述终端设备可能处于异常状态，很可能被利用进行爬虫部署访问网络。

将该可能处于异常状态的终端设备的非线性组合特征集作为所述第二非线性组合特征集，以便通过对待比较的数据进行预先筛选，减少后期进行欧式距离的求取和数据对比等数据处理工作。

对于将获取所述终端设备的第二非线性组合特征集的各个特征数值，与上述得到的对应型号的正常范围值进行对比的过程，可以包括终端设备的像素比、关于分辨率的参数或者是验证时间和验证次数的综合情况。

具体地，可以参考以下例子：

（1）像素比与终端设备的系统平台是否一致的组合特征：

windows 系统电脑的真实像素比一般为 1 左右，如果服务器所获取终端设备的 windows 系统电脑的像素比大于等于 2，那么有可能是电脑模拟手机的官方模拟器进行攻击验证码，很有可能是异常的终端设备；

苹果手机的真实像素比一般为 2-3 左右，如果服务器所获取的苹果手机的像素比为 1，那么很有可能是爬虫或自动化设备或官方模拟器等攻击验证码，那么对应的终端设备很可能是异常的终端设备；

苹果 mac 电脑的像素比一般为 1-2 左右，如果服务器所获取的 mac 电脑的像素比为 3，那么对应的终端设备很可能是异常的终端设备。

（2）生成基于分辨率的非线性组合特征与系统平台是否一致的组合特征：

浏览器可用屏幕分辨率 x,y 乘积 xy 与终端设备屏幕分辨率 x1,y1 乘积 x1y1 的差值 x1y1 - xy 与系统平台是否一致的组合特征：

比如正常情况下通过前端获取的电脑端 chrome 浏览器的 xy-x1y1 不为 0，也就是正常情况下电脑端 chrome 浏览器通过服务器所获取终端设备的屏幕分辨率和浏览器可用分辨率有一定的差值，而电脑模拟手机时通过服务器所获取终端设备的屏幕分辨率和浏览器可用分辨率完全相同或差异很大（比如 x1y1 - xy 大于 150000），那么对应的终端设备很可能是异常的终端设备。

（3）分辨率 X*Y 取值正常范围与系统平台是否一致的组合特征；

尤其是分辨率过低时，对应低端设备用于爬虫部署）。

对于步骤 S210，可具体为：

获取历史采集的终端设备的第一设备参数，提取所述第一设备参数的特征信息，根据所述特征信息生成多个第一非线性组合特征集。

针对历史采集的关于终端设备的第一设备参数，服务器针对所述第一设备参数提取相关的特征信息，如像素比、分辨率或验证时间和频率等特征信息，并针对每个特征信息生成各自的第一非线性组合特征集，并综合同一终端设备每一次的发起网络请求所生成的所有第一非线性组合特征集，可形成一个多维向量的数据点，并可在对应的坐标上进行标注，以便进行后续的数据分析和统计。

在步骤 S210 之后，还可以包括：

B1、根据历史的终端设备的访问量得到网络访问的闲时段；

B2、获取在同一所述网络访问闲时段内同一终端设备的闲时访问频率；

B3、将所述闲时访问频率与预设值进行对比；

B4、若所述闲时访问频率大于预设值，获取对应终端设备的第二非线性组合特征集。

依据上述步骤 B1-B4，根据历史的终端设备的访问数量得到网络访问闲时段。并根据所述网络访问闲时段获取同一终端设备的闲时访问频率。将就同一终端设备的显示访问频率与预设值进行对比。在本实施例中，所述预设值可以通过获取历史的终端设备在所述网络访问闲时段的访问量统计得到。

如果所述终端设备的访问频率大于预设值，则将该终端设备设定为监控对象，并获取其第二非线性组合特征集。通过获得的第二非线性组合特征集提取其他特征信息，进行进一步的监控、对比分析，以便网络访问异常检测更具针对性，提高异常情况的捕获效率，提升对网络爬虫造成的异常访问进行隔离的效果。

基于与上述终端设备异常访问的隔离方法相同的发明构思，本申请实施例还提供了一种终端设备异常访问的隔离装置，如图 4 所示，包括：

获取模块 410，用于根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

生成模块 420，用于通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

计算模块 430，用于分别计算所述第二非线性组合特征集与所述正常

状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

隔离模块 440，用于当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

请参考图 5，图 5 为一个实施例中服务器的内部结构示意图。如图 4 所示，该服务器包括通过系统总线连接的处理器 510、存储介质 520、存储器 530 和网络接口 540。其中，该服务器的存储介质 520 存储有操作系统、数据库和计算机可读指令，数据库中可存储有控件信息序列，该计算机可读指令被处理器 510 执行时，可使得处理器 510 实现一种终端设备异常访问的隔离方法，处理器 510 能实现图 4 所示实施例中的一种终端设备异常访问的隔离装置中的获取模块 410、生成模块 420、计算模块 430 和隔离模型 440 的功能。该服务器的处理器 510 用于提供计算和控制能力，支撑整个服务器的运行。该服务器的存储器 530 中可存储有计算机可读指令，该计算机可读指令被处理器 510 执行时，可使得处理器 510 执行一种终端设备异常访问的隔离方法。该服务器的网络接口 540 用于与终端连接通信。本领域技术人员可以理解，图 5 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服务器的限定，具体的服务器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。

在一个实施例中，本申请还提出了一种非易失性存储有计算机可读指令的存储介质，该计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

综合上述实施例可知，本申请最大的有益效果在于：

本申请所提供的一种终端设备异常访问的隔离方法和装置，分别对所述历史采集的终端设备的网络访问和当前的网络访问分别生成多个第一非线性组合特征集和对应的第二非线性组合特征集，并将所述多个第一非线性组合特征集的数据点分为正常状态簇和异常状态簇，分别计算得到所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及

与异常状态簇的质心之间的第二欧式距离；根据所述第一欧式距离与所述第二欧式距离的比较结果，判定所述网络访问是否为异常访问，并对异常访问对应的请求进行隔离处理。

本申请所提供的技术方案将所述终端设备在发起网络访问请求时所生成的特征信息转化为相应的数据点，并根据数据点相互之间的空间位置关系，并以此得到判定结果。这样，可以将终端设备终端网络访问得到的特性信息以通过相关间的距离参数的比较结果，直观地反映所述终端设备网络访问是否为异常访问，使得更容易判断所述终端设备是否通过网络爬虫访问入侵网站，提高对终端设备的异常访问的隔离效果。

综上，本申请通过终端设备异常访问的隔离方法和装置，通过将终端设备网络访问所生成的特征信息数据进行可视化的距离对比，并得到判定是否为异常访问的判定结果的技术方案，解决了现有技术中通过终端设备登录网络时用户的使用痕迹数据容易将真实用户判别为异常用户的问题，提高了对终端设备异常访问的检测能力。

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，该计算机程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，前述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）等存储介质，或随机存储记忆体（Random Access Memory，RAM）等。

以上所述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。

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本申请专利范围的限制。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。

权 利 要 求 书

1. 一种终端设备异常访问的隔离方法，包括以下步骤：

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

2. 根据权利要求 1 所述的方法，在所述分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离的步骤之前，还包括：

分别对所述第一非线性组合特征集的正常状态簇和异常状态簇预设初始质心。

3. 根据权利要求 1 或 2 所述的方法，所述分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离的步骤包括：

分别计算在设定时间段内每一次访问的所述第二非线性组合特征集与正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

就同一终端设备在设定时间段内获取排序在前的设定个数所述第一欧式距离的集合和所述第二欧式距离的集合，并分别得到所述第一欧式距离的集合和所述第二欧式距离的集合的众数值；

并分别以所述第一欧式距离的集合和所述第二欧式距离的集合的众数值作为所述同一终端设备在设定时间段内所述第一欧式距离和所述第二欧式距离。

4. 根据权利要求 1 所述的方法，所述通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集的步骤包括：

通过终端设备上的脚本程序获取当前访问的第二设备参数，生成第二非线性组合特征集，并从所述第二非线性组合特征集中获取终端设备的用户代理；

通过对用户代理进行解析，获取所述终端设备的型号。

5. 根据权利要求 4 所述的方法，在所述通过对用户代理进行解析，获取所述终端设备的型号的步骤之后，还包括：

根据所述终端设备的型号，得到所述终端设备的第二非线性组合特征集的各个特征数值的正常范围；

将所述第二非线性组合特征集的特征数值与所述正常范围进行比较；

得到所述正常范围以外的特征数值对应终端设备的非线性组合特征集作为第二非线性组合特征集。

6. 根据权利要求 1 所述的方法，所述根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集的步骤包括：

获取历史采集的终端设备的第一设备参数，提取所述第一设备参数的特征信息，根据所述特征信息生成多个第一非线性组合特征集。

7. 根据权利要求 1 所述的方法，所述根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集的步骤之后，还包括：

根据历史的终端设备的访问量得到网络访问闲时段；

获取在同一所述网络访问闲时段内同一终端设备的闲时访问频率；

将所述闲时访问频率与预设值进行对比；

若所述闲时访问频率大于预设值，获取对应终端设备的第二非线性组合特征集。

8. 一种终端设备异常访问的隔离装置，包括：

获取模块，用于根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；

生成模块，用于通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；

计算模块，用于分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

隔离模块，用于当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

9. 一种服务器，包括：

一个或多个处理器；

存储器；

一个或多个计算机程序，其中所述一个或多个计算机程序被存储在所述存储器中并被配置为由所述一个或多个处理器执行，所述一个或多个计算机程序配置用于执行一种终端设备异常访问的隔离方法，所述终端设备异常访问的隔离方法包括以下步骤：

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征

集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

10. 根据权利要求 9 所述的服务器，在所述分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离的步骤之前，还包括：

分别对所述第一非线性组合特征集的正常状态簇和异常状态簇预设初始质心。

11. 根据权利要求 9 或 10 所述的服务器，所述分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离的步骤包括：

分别计算在设定时间段内每一次访问的所述第二非线性组合特征集与正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

就同一终端设备在设定时间段内获取排序在前的设定个数所述第一欧式距离的集合和所述第二欧式距离的集合，并分别得到所述第一欧式距离的集合和所述第二欧式距离的集合的众数值；

并分别以所述第一欧式距离的集合和所述第二欧式距离的集合的众数值作为所述同一终端设备在设定时间段内所述第一欧式距离和所述第二欧式距离。

12. 根据权利要求 9 所述的服务器，所述通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集的步骤包括：

通过终端设备上的脚本程序获取当前访问的第二设备参数，生成第二非线性组合特征集，并从所述第二非线性组合特征集中获取终端设备的用户代理；

通过对用户代理进行解析，获取所述终端设备的型号。

13. 根据权利要求 12 所述的服务器，在所述通过对用户代理进行解析，获取所述终端设备的型号的步骤之后，还包括：

根据所述终端设备的型号，得到所述终端设备的第二非线性组合特征集的各个特征数值的正常范围；

将所述第二非线性组合特征集的特征数值与所述正常范围进行比较；

得到所述正常范围以外的特征数值对应终端设备的非线性组合特征集作为第二非线性组合特征集。

14. 根据权利要求 9 所述的服务器，所述根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集的步骤包括：

获取历史采集的终端设备的第一设备参数，提取所述第一设备参数的特征信息，根据所述特征信息生成多个第一非线性组合特征集。

15. 根据权利要求 9 所述的服务器，所述根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集的步骤之后，还包括：

根据历史的终端设备的访问量得到网络访问闲时段；

获取在同一所述网络访问闲时段内同一终端设备的闲时访问频率；

将所述闲时访问频率与预设值进行对比；

若所述闲时访问频率大于预设值，获取对应终端设备的第二非线性组合特征集。

16. 一种非易失性计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现一种终端设备异常访问的隔离方法，所述终端设备异常访问的隔离方法包括以下步骤：

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇；其中，所述第一非线性组合特征集为历史获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集；其中，所述第二非线性组合特征集为当前获取的终端设备的非线性特征信息，该特征信息包括终端设备的属性数据和访问数据；

分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离；

当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理。

17. 根据权利要求 16 所述的非易失性计算机可读存储介质，在所述分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离的步骤之前，还包括：

分别对所述第一非线性组合特征集的正常状态簇和异常状态簇预设初始质心。

18. 根据权利要求 16 或 17 所述的非易失性计算机可读存储介质，所述分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离的步骤包括：

分别计算在设定时间段内每一次访问的所述第二非线性组合特征集与正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第

二欧式距离；

就同一终端设备在设定时间段内获取排序在前的设定个数所述第一欧式距离的集合和所述第二欧式距离的集合，并分别得到所述第一欧式距离的集合和所述第二欧式距离的集合的众数值；

并分别以所述第一欧式距离的集合和所述第二欧式距离的集合的众数值作为所述同一终端设备在设定时间段内所述第一欧式距离和所述第二欧式距离。

19. 根据权利要求 16 所述的非易失性计算机可读存储介质，所述通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集的步骤包括：

通过终端设备上的脚本程序获取当前访问的第二设备参数，生成第二非线性组合特征集，并从所述第二非线性组合特征集中获取终端设备的用户代理；

通过对用户代理进行解析，获取所述终端设备的型号。

20. 根据权利要求 19 所述的非易失性计算机可读存储介质，在所述通过对用户代理进行解析，获取所述终端设备的型号的步骤之后，还包括：

根据所述终端设备的型号，得到所述终端设备的第二非线性组合特征集的各个特征数值的正常范围；

将所述第二非线性组合特征集的特征数值与所述正常范围进行比较；

得到所述正常范围以外的特征数值对应终端设备的非线性组合特征集作为第二非线性组合特征集。

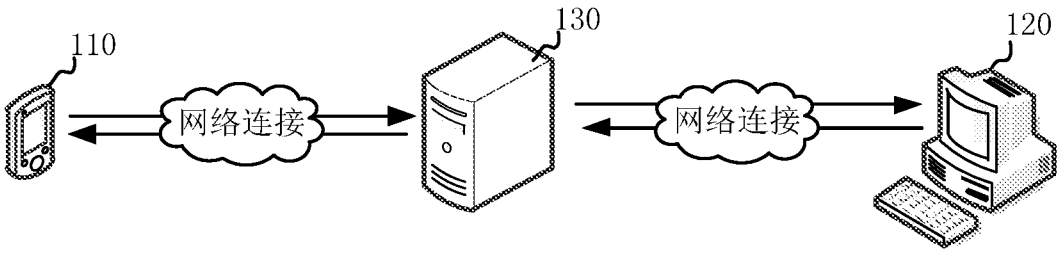

110
网络连接
130
网络连接
120

图 1

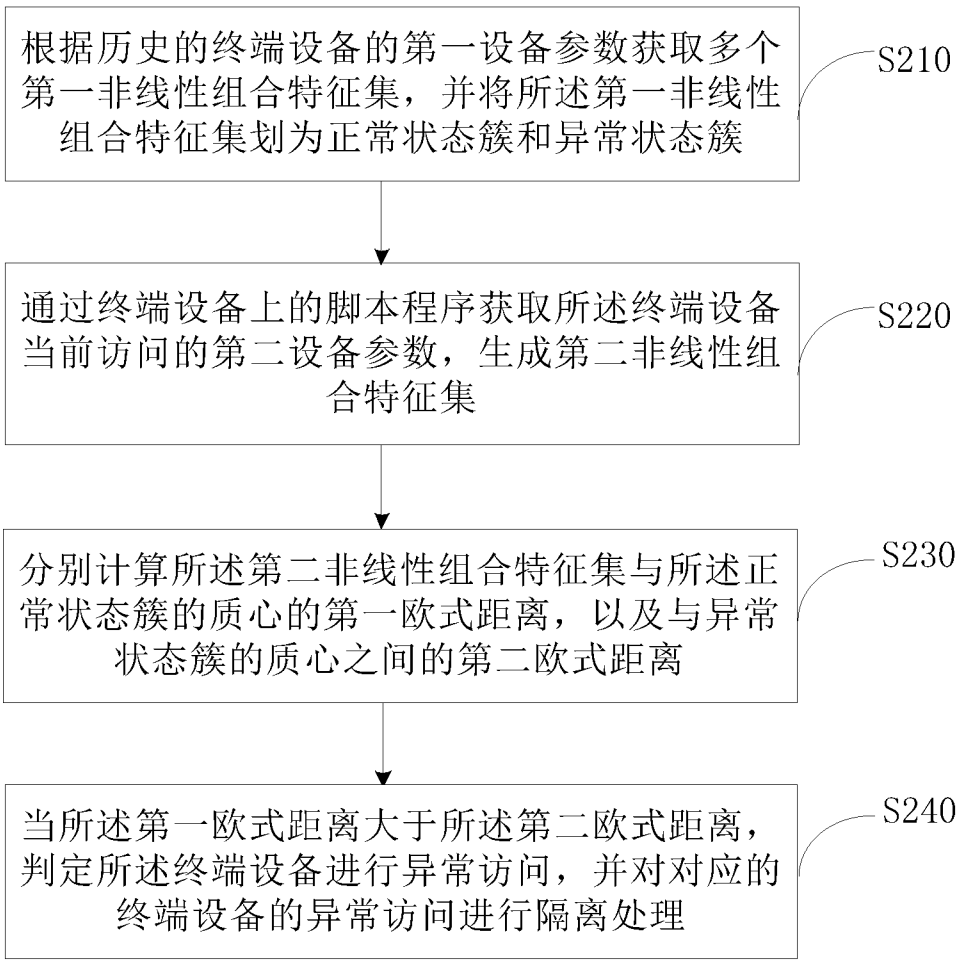

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇
S210
通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集
S220
分别计算所述第二非线性组合特征集与所述正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离
S230
当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理
S240

图 2

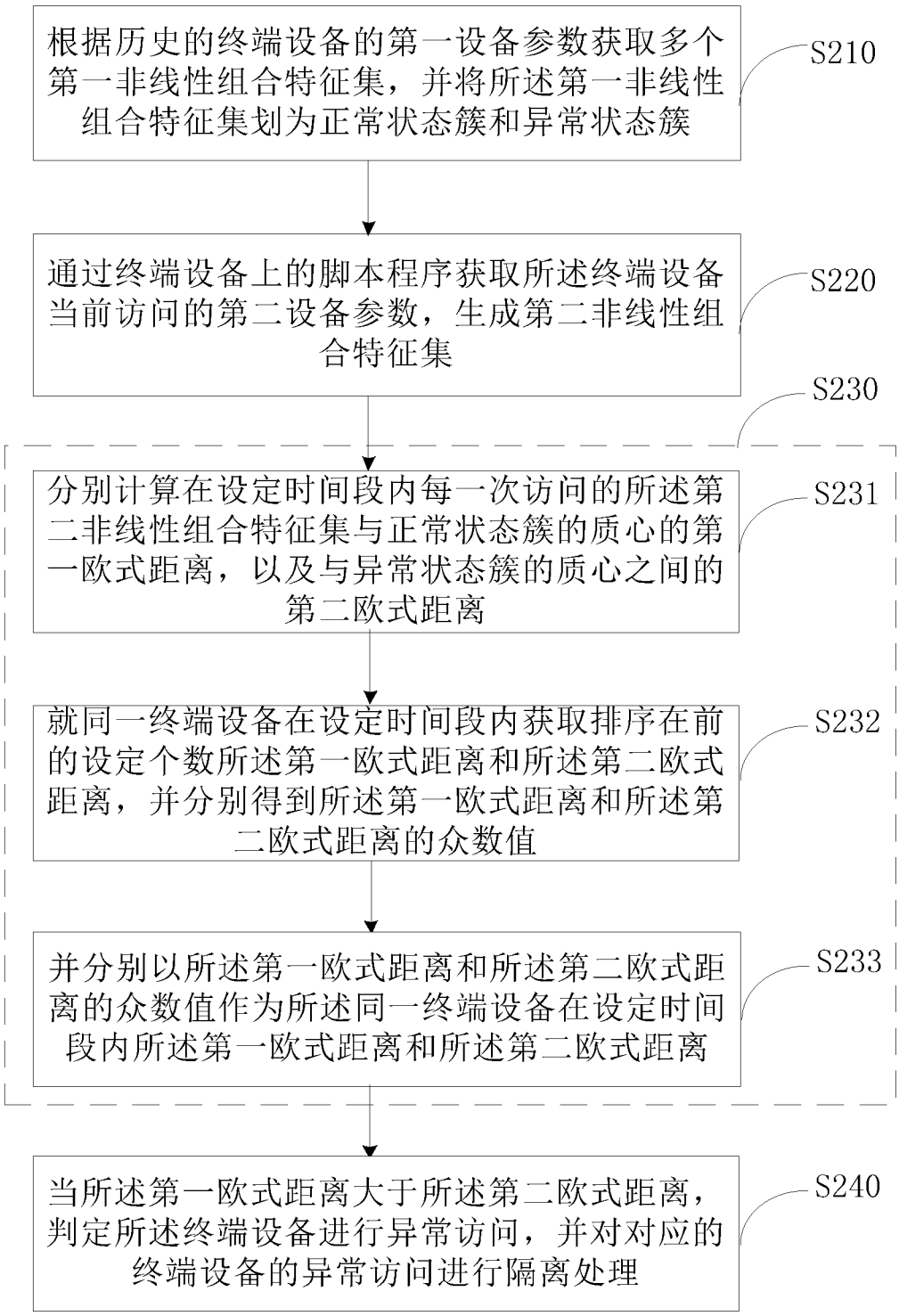

根据历史的终端设备的第一设备参数获取多个第一非线性组合特征集，并将所述第一非线性组合特征集划为正常状态簇和异常状态簇
S210
通过终端设备上的脚本程序获取所述终端设备当前访问的第二设备参数，生成第二非线性组合特征集
S220
S230
分别计算在设定时间段内每一次访问的所述第二非线性组合特征集与正常状态簇的质心的第一欧式距离，以及与异常状态簇的质心之间的第二欧式距离
S231
就同一终端设备在设定时间段内获取排序在前的设定个数所述第一欧式距离和所述第二欧式距离，并分别得到所述第一欧式距离和所述第二欧式距离的众数值
S232
并分别以所述第一欧式距离和所述第二欧式距离的众数值作为所述同一终端设备在设定时间段内所述第一欧式距离和所述第二欧式距离
S233
当所述第一欧式距离大于所述第二欧式距离，判定所述终端设备进行异常访问，并对对应的终端设备的异常访问进行隔离处理
S240

图 3

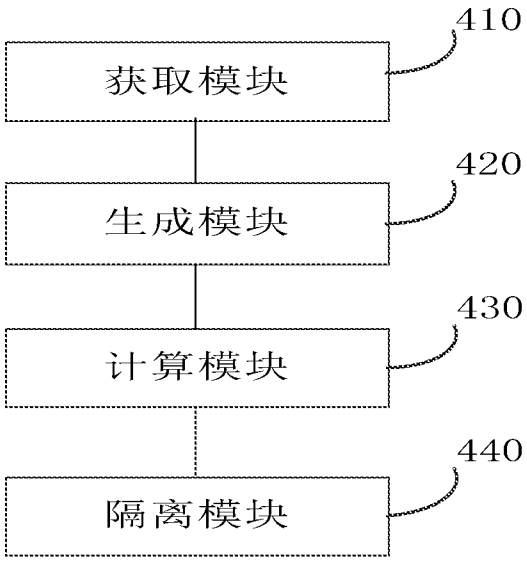

410
获取模块
420
生成模块
430
计算模块
440
隔离模块

图 4

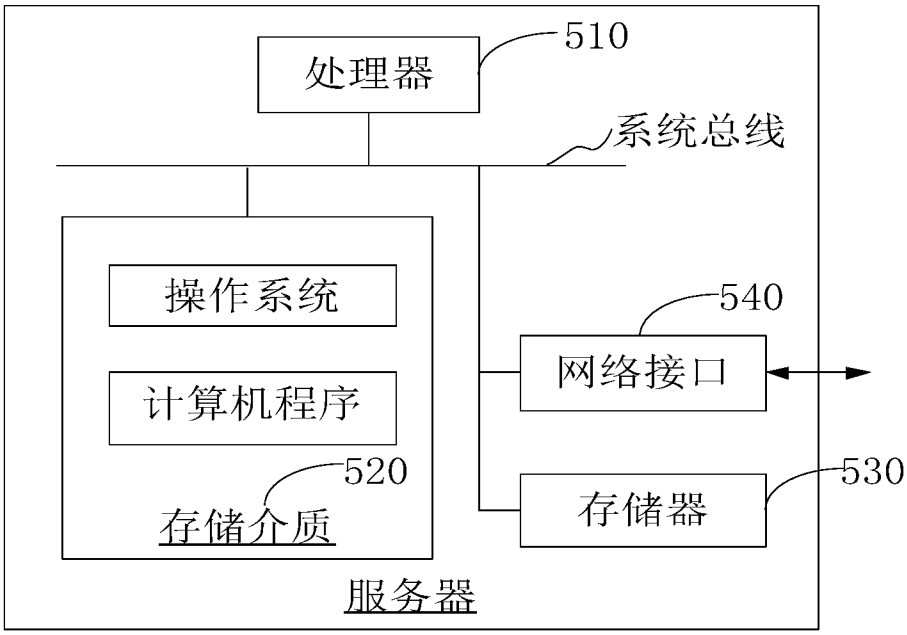

处理器
510
系统总线
操作系统
计算机程序
520
存储介质
540
网络接口
存储器
530
服务器

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/103663

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 终端设备, 异常访问, 隔离, 安全, 参数, 历史, 非线性, 特征集, 正常, 异常, 状态簇, 质心, 欧氏距离, terminal device, abnormal access, isolate+, safe, parameter, history, non-linear, feature set, normal, abnormal, state cluster, centroid, Euclidean distance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 109886290 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 14 June 2019 (2019-06-14) description, paragraphs [0005]-[0048], and figures 1-7	1-20
A	CN 109391620 A (WUHAN JIYI NETWORK TECHNOLOGY CO., LTD.) 26 February 2019 (2019-02-26) entire document	1-20
A	CN 107819631 A (NEUSOFT CORPORATION) 20 March 2018 (2018-03-20) entire document	1-20
A	US 2011016525 A1 (JEONG, C.Y. et al.) 20 January 2011 (2011-01-20) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 March 2020	**27 March 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/103663

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109886290 A	14 June 2019	None	
CN 109391620 A	26 February 2019	None	
CN 107819631 A	20 March 2018	None	
US 2011016525 A1	20 January 2011	KR 20110011935 A	09 February 2011
		KR 101219538 B1	08 January 2013

国际检索报告

国际申请号
PCT/CN2019/103663

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, CNKI, WPI, EPODOC：终端设备，异常访问，隔离，安全，参数，历史，非线性，特征集，正常，异常，状态簇，质心，欧氏距离，terminal device, abnormal access, isolate+, safe, parameter, history, non-linear, feature set, normal, abnormal, state cluster, centroid, Euclidean distance

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 109886290 A (平安科技深圳有限公司) 2019年 6月 14日 (2019-06-14) 说明书第[0005]-[0048]段，附图1-7	1-20
A	CN 109391620 A (武汉极意网络科技有限公司) 2019年 2月 26日 (2019-02-26) 全文	1-20
A	CN 107819631 A (东软集团股份有限公司) 2018年 3月 20日 (2018-03-20) 全文	1-20
A	US 2011016525 A1 (JEONG, ChiYoon等) 2011年 1月 20日 (2011-01-20) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 3月 15日	2020年 3月 27日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 白露霜 电话号码 86-(10)53961390

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/103663

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 109886290 A	2019年 6月 14日	无	
CN 109391620 A	2019年 2月 26日	无	
CN 107819631 A	2018年 3月 20日	无	
US 2011016525 A1	2011年 1月 20日	KR 20110011935 A	2011年 2月 9日
		KR 101219538 B1	2013年 1月 8日