

(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)



(10) 国际公布号
WO 2020/258670 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/118378

(22) 国际申请日: 2019 年 11 月 14 日 (14.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910580047.2 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, Liguì); 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: 深圳市世纪恒程知识产权代理事务所(CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区粤海街道高新技术产业园北区松坪山路 3 号奥特讯电力大厦 201, Guangdong 518057 (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,

(54) Title: NETWORK ACCESS ABNORMALITY DETERMINATION METHOD AND APPARATUS, SERVER, AND STORAGE MEDIUM

(54) 发明名称: 网络访问的异常判定方法、装置、服务器和存储介质

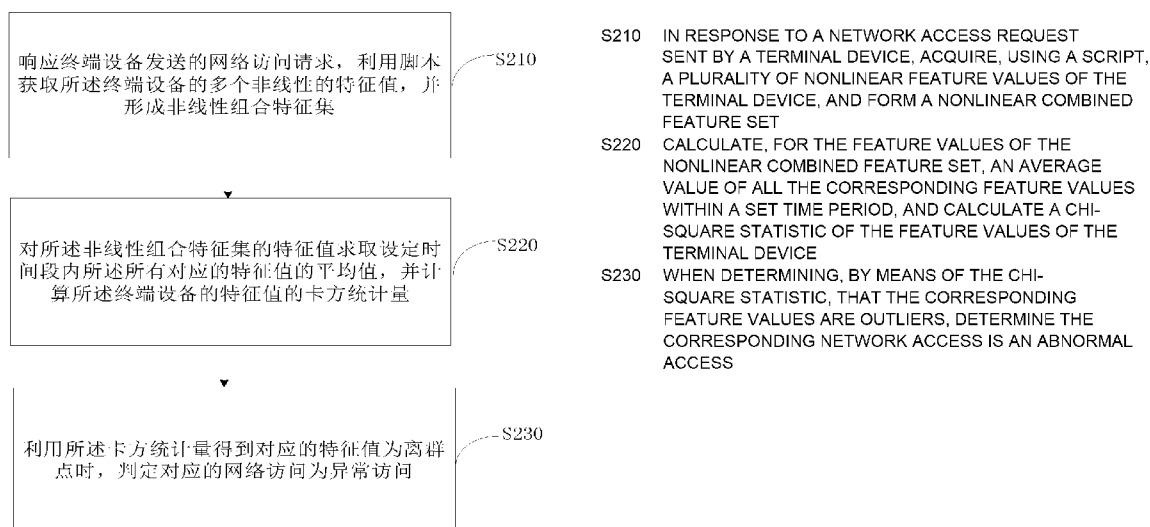


图 2

(57) Abstract: The present application relates to the field of security detection technology. The present application provides a network access abnormality determination method and apparatus, a server and a storage medium. Said method comprises: in response to a network access request sent by a terminal device, acquiring, using a script, a plurality of nonlinear feature values of the terminal device, and forming a nonlinear combined feature set; calculating, for the feature values of the nonlinear combined feature set, an average value of all the corresponding feature values within a set time period, and calculating a Chi-square statistic of the feature values of the terminal device; when the Chi-square statistic of the feature values of the terminal device is greater than a corresponding determination

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
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)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

threshold, determining the corresponding feature values as outliers; and performing determination, according to the feature values of the obtained outliers, to obtain that the network access is an abnormal access. The present application is beneficial to improving the effect of network access abnormality determination.

(57) 摘要: 本申请涉及安全检测技术领域, 本申请提供一种网络访问的异常判定方法、装置、服务器及存储介质, 所述方法包括响应终端设备发送的网络访问请求, 利用脚本获取所述终端设备的多个非线性的特征值, 并形成非线性组合特征集; 对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值, 并计算所述终端设备的特征值的卡方统计量; 当所述终端设备的特征值的卡方统计量大于对应的判断阈值时, 确定对应的特征值为离群点; 根据得到的离群点的特征值, 判定得到所述网络访问为异常访问。本申请有利于提高对网络访问的异常判定效果。

网络访问的异常判定方法、装置、服务器和存储介质

本申请要求于 2019 年 6 月 28 日提交中国专利局、申请号为 201910580047.2、发明名称为“终端设备网络访问的异常判定方法和装置”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

本申请涉及安全检测技术领域，具体而言，本申请涉及一种网络访问的异常判定方法、装置、服务器及存储介质。

背景技术

在目前网络访问中，威胁网站安全的主要手段之一是通过网络爬虫访问网站，导致网站不能做出正确的判断，从而容易造成反应错误。针对该问题，目前的方法是通过采集用户验证过程中的点击时间、鼠标拖动轨迹等数据，针对此行为数据判别用户种类，此类方法错误率较高，容易将真实用户判别为异常用户，准确性低。

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，本申请提供一种网络访问的异常判定方法，其包括以下步骤：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

第二方面，本申请还提供一种网络访问的异常判定装置，其包括：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

第三方面，本申请还提供一种服务器，其包括：

一个或多个处理器；

存储器；

一个或多个计算机可读指令，

其中所述一个或多个计算机可读指令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可读指令被执行时实现以下步骤：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

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

计算机可读指令，所述计算机可读指令被处理器执行时实现以下步骤：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

本申请所提供的技术方案运用了采用卡方统计量的检测算法，得到判定依据的值与临界值进行对比后得到相应的判定结果，且不需要对终端设备发起网络访问的特征信息数据进行标注，节省了后期统计和分析的工作

量；而且该方案分析的过程简单，结果直观，可容易得到准确率较高的判定结果，最终提高所述终端设备网络访问的异常判定效果。

本申请附加的方面和优点将在下面的描述中部分给出，这些将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

本申请上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 是本申请中的实施例执行网络访问的异常判定方案的应用环境图；

图 2 是本申请中的一个实施例的网络访问的异常判定方法的流程图；

图 3 为本申请中的一个实施例的网络访问的异常判定装置的示意图；

图 4 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

下面详细描述本申请的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本申请，而不能解释为对本申请的限制。

本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本申请的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解，当我们称元件被“连接”或“耦接”到另一元件时，它可以直接连接或耦接到其他元件，或者也可以存在中间元件。此外，这里使用的“连接”或“耦接”可以包括无线连接或无线耦接。这里使用的措辞“和/或”包括一个或更多个相关联的列出项的全部或任一单元和全部组合。

本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语（包括技术术语和科学术语），具有与本申请所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术

语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样被特定定义，否则不会用理想化或过于正式的含义来解释。

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讯链路上，执行双向通讯的接收和发射硬件的设备。这种设备可以包括：蜂窝或其他通讯设备，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讯设备；PCS（Personal Communications Service，个人通讯系统），其可以组合语音、数据处理、传真和/或数据通讯能力；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”还可以是通讯终端、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。

本技术领域技术人员可以理解，这里所使用的远端网络设备，其包括但不限于计算机、网络主机、单个网络服务器、多个网络服务器集或多个服务器构成的云。在此，云是基于云计算（Cloud Computing）的大量计算机或网络服务器构成，其中，云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。本申请的实施例中，远端网络设备、终端设备与 WNS 服务器之间可通过任何通讯方式实现通讯，包括但不限于，基于 3GPP、LTE、WIMAX 的移动通讯、基于 TCP/IP、UDP 协议的计算机网络通讯以及基于蓝牙、红外传输标准的近距无线传输方式。

参考图 1 所示，图 1 是本申请实施例执行网络访问的异常判定方案的应用环境图；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判定。

为了解决目前判定异常数据容易将真实用户判别为异常用户的问题,本申请提供了一种网络访问的异常判定方法。可参考图 2,图 2 是一个实施例的网络访问的异常判定方法的流程图,该方法包括以下步骤:

S210、响应终端设备发送的网络访问请求,利用脚本获取所述终端设备的多个非线性的特征值,并形成非线性组合特征集。

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,用户通过发送注册、验证请求,前端利用 JavaScript 脚本获取终端设备的相关的特征值,包括设备类型(IPone、Mac、Andriod)、系统信息(OS 类型、版本、分辨率)、IP 等的多个特征值,所述特征值之间相互为非线性关系。所述多个特征值形成了关于所述终端设备关于网络访问请求的非线性组合特征集。

在本实施例中,所述特征值可以具体包括通过前端获取设备的特征值 user_agent、分辨率、像素比、触屏事件(支持触屏事件的最大点数、是否支持可触控)。通过解析 user_agent 中的字符串信息,获取设备的类型、品牌、型号、操作系统版本号,通过上述解析的当前发出网络访问请求的终端设备的品牌及型号关联基础库中相同的设备品牌及型号的分辨率、像素比、触屏事件信息。其中,基础库是通过权威网站获取的所有设备型号的分辨率、像素比、触屏事件的真实信息。

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、对所述非线性组合特征集的特征值求取设定时间段内所述所有对应的特征值的平均值,并计算所述终端设备的特征值的卡方统计量。

在该步骤中,根据从步骤 S210 得到的所述非线性组合特征集,并对应提取相应的特征值,并根据所述特征值得到的其他关联值,计算得到与

所述特征值对应的卡方统计量，得到所述终端设备在发起网络访问请求时所形成的特征值分布。

其中，对于所述卡方统计量，可以进一步通过求取设定时间段内所述所有对应的特征值的平均值，并计算所述终端设备的所述特征值的卡方统计量。

具体地，所述终端设备发起网络访问请求时，在一定连续时长内，正常的情况下，一般会发出多次网络访问请求。所述终端设备每发起一次网络访问请求，所形成的一组特征值便形成一组所述非线性组合特征集。为了能通过其中的若干项的特征值进行异常访问的判定，根据需要从所述非线性组合特征集提取相应的特征值。

进一步地，求取在上述设定时间段内由所述终端设备发起网络访问请求时所形成的所有对应的特征值的平均值，计算得到所述终端设备的所述特征值的卡方统计量。

计算所述卡方统计量的具体计算过程如下：

$$\chi^2 = \sum_{i=1}^n \frac{(o_i - E_i)^2}{E_i} \quad (1)$$

其中， o_i 为所述终端设备在某一检测时间点所发起网络访问请求时所形成的第*i*个特征的值， E_i 为设定时间段内所述终端设备所发起网络访问请求所形成的所有第*i*个特征的平均值，*n*是在设定时间段内所述终端设备所发起网络访问请求所形成的所有第*i*个特征的特征总数。

S230、用所述卡方统计量得到对应的特征值为离群点时，判定对应的网络访问为异常访问。

根据上述步骤 S220 根据关于终端设备在发起网络访问请求时所形成的特征值计算得到的卡方统计量，体现了检测时间点对应的特征值分布情况。根据所述特征值的分别情况，得到对应特征值的离群点，根据该离群点的位置，得到对应的网络访问为异常访问的判定结果。

本申请提供的一种网络访问的异常判定方法，通过所述终端设备发起的网络访问请求获得多个非线性的特征值，根据上述特征值极端得到对应

的卡方统计量，利用卡方统计量得到对应的特征值为离群点的情况下，得到该终端设备当前为网络访问为异常访问的判定结果。

本申请的技术方案将终端设备发起的网络访问请求得到为离群点对应的特征值，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和拖动轨迹的数据作为异常判定的依据，从而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访问的判定结果，有利于提高终端设备网络访问的异常判定的效率。

对于上述求取在上述设定时间段内由所述终端设备发起网络访问请求时所形成的所有对应的特征值的平均值，计算得到所述终端设备的所述特征值的卡方统计量的步骤，可进一步包括：

A221、根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的一特定的必要特征值，求取所述必要特征值的第一平均值；

A222、根据所述必要特征值和所述第一平均值，计算得到所述终端设备的对应必要特征值的第一卡方统计量。

在步骤 A221-A222 的实施例，是以其中一项特征值对所述终端设备的网络访问进行异常判定。针对所进行异常判定的事项，在设定时间段内的所形成的所述非线性组合特征集中提取一特定的必要特征值，并对在该设定时间段内的每一次网络访问请求所产生的同一必要特征的值求取第一平均值。

其中，该必要特征值是所述终端设备发起网络访问请求所产生的必要特征值，能够通过所述基础库能找到相应的真实信息，以便后续作为参照。如分辨率、像素比、系统对用户代理可用的逻辑处理器总数等可以数值的形式来衡量的信息。

具体地，如在 7PM-9PM 的设定时间段，获取该期间的每一次网络访问请求所产生的非线性组合特征集的如分辨率的特定的必要特征值，并求其在该设定时间段内每一次网络访问请求所产生的分辨率的平均值，并以该平均值作为该必要特征值分辨率的第一平均值。根据上述的公式（1），计算得到该必要特征值的第一卡方统计量。

可进一步地,计算在设定时间段内对应特征值的所有第一卡方统计量,并对所述第一卡方统计量求取其平均值,并以该平均值做进一步判定的依据,避免因偶然的异常情况引起的数据异常影响整体的判定结果。

在此基础上,在步骤 S230 之前,即在对所述网络访问的异常访问的判定之前,还包括:

根据所述设定时间段内所得到的第一卡方统计量,计算得到所述第一卡方统计量的四分位距的上限值作为所述特征值对应的第一判断阈值。

在该步骤,针对上述特征值在所述设定时间段内所有得到的对应的第一卡方统计量,并此作为统计的对应形成一数组,并按照所形成的时间进行排列。根据排列好的数组,分别计算其下四分位数 $Q1$ 、中位数 $Q2$ 和上四分位数 $Q3$,得到对应的四分位距 $IQR=Q3-Q1$,最后计算得到对应的四分位距的上限值,并以该四分位距的上限值作为所述特征值的第一判定阈值。

所述第一判定阈值也可以是根据针对所述特征值所获取的历史数据得到的临界值,并根据所述临界值为依据设定对应的第一判定阈值。

上述步骤 S220,可形成另一实施例,其进一步包括:

B221、根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的多个特征值,得到对应的非线性组合特征集的多个特征值的维度向量作为所述非线性组合特征集的特征值;

B222、根据所有所述非线性组合特征集的特征值,求取对应的第二平均值;

B223、根据所述非线性组合特征集的特征值和所述第二平均值,并计算得到所述终端设备的所述非线性组合特征集的特征值的第二卡方统计量。

在步骤 B221-B223 的实施例,是以所述非线性组合特征集的多个特征值、甚至是全部的特征值作为一整体对所述终端设备的网络访问进行异常访问的判定。

具体地,根据评估的需要,在设定时间段内针对所述终端设备在每一次发起的网络访问请求所形成的非线性组合特征集提取多个特征值。如确认对所述终端设备的 IP 地址是否为 IDC (Internet Data Center, 互联网数据中心) 或者是机房服务器,则可以对其中的特征值 user agent、分辨率、

像素比、触屏事件的各个特征值作为一个维度的值，并得到所述多个特征值对应的维度向量进行评估。并以该维度向量作为所述非线性组合特征集的特征值。

根据设定时间段内的每一次网络访问请求对应所述非线性组合特征集的特征值，求取对应的第二平均值。

根据所述非线性组合特征集的特征值和对应的所述第二平均值，利用上述的公式（1），计算得到所述终端设备的所述非线性组合特征集的第二卡方统计量，得到关于 IP 地址相关特征值的数据分布。

进一步地，计算在设定时间段内对应特征值的所有第二卡方统计量，并对所述第二卡方统计量求取其平均值，并以该平均值做进一步判定的依据，避免因偶然的异常情况引起的数据异常影响整体的判定结果。

在该实施例的基础上，在步骤 S230 之前，即在对所述网络访问的异常访问的判定之前，还包括：

根据设定时间段内所有网络访问请求对应的所述第二卡方统计量形成的曲线，并得到所述曲线的最大斜率对应的第二卡方统计量作为第二判断阈值。

在该步骤中，针对所述非线性组合特征集的特征值在所述设定时间段内所有得到的对应的第二卡方统计量，并对应应在坐标上标注对应的所述第二卡方统计量的值，形成对应的一曲线，并从所述曲线上的斜率最大的点所对应的第二卡方统计量作为所述第二判断阈值。

所述第二判定阈值也可以是根据针对所述非线性组合特征集的特征值所获取的历史数据得到的临界值，并根据所述临界值为依据设定对应的第二判定阈值。

对于步骤 S230，进一步包括：

S231、通过所述终端设备的第一或第二卡方统计量大于对应的判断阈值时，对应的特征值为离群点；

S232、根据得到的离群点的特征值，判定得到所述网络访问为异常访问。

将所述第一或第二卡方统计量与对应的第一或所述第二判断阈值进行对比。根据对比的结果，判定对应的所述非线性组合特征集的特征值是否

为离群点，以此判定对应的网络访问是否为异常访问。若第一或第二卡方统计量大于对应的第一或第二判断阈值时，对应的特征值为离群点，则判定得到产生对应特征值的网络访问为异常访问。

对于所述终端设备当前发起的网络请求被判定为异常访问请求，服务器直接拒绝请求或重新要求所述终端设备进行访问验证；若所述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。

其中，在上述实施例中提到的所述判断阈值是表现所述终端设备在发起正常网络访问请求的情况下，所形成的相关特征值的临界点。将所述卡方统计量与所述判断阈值进行比较，若所述卡方统计量超出了所述判断阈值的范围，则所述卡方统计量对应的特征值为在异常访问的情况下所形成的，以此得到在对应的检测时间点所述终端设备发起的网络访问是否为异常访问的判定结果。

对于上述提到的所述非线性组合特征集还可以包括原始类别的特征信息和有效衍生特征信息，其中，先利用脚本获取原始类别的特征信息，然后通过对原始类别的特征信息进行度量数据散布计算得到识别离群点的有效衍生特征信息。

具体地，所述非线性组合特征集可以包括浏览器语言、像素比、颜色深度、音频堆栈指纹是否提供、音频堆栈指纹的参数信息、系统对用户代理可用的逻辑处理器总数、浏览器生产厂商是否为 other、操作系统生产厂商是否为 other、浏览器类型是否为 robot 等原始类别的特征信息。

根据所述度量数据散布计算，可以得到识别离群点的有效衍生特征，其包括是否安装 Adblock、用户是否篡改了语言、用户是否篡改了屏幕分辨率、用户是否篡改了操作系统、浏览器生产厂商、操作系统生产厂商、访问设备类型、操作系统家族。

所述度量数据散布计算包括对应特征信息数据计算极差、四分位数、四分位数极差、五数概括，所述五数概括按次序为最小值、上四分位、中位数、下四分位数、最大值。

基于与上述网络访问的异常判定方法相同的发明构思，本申请实施例还提供了一种网络访问的异常判定装置，如图 3 所示，包括：

获取模块 310，用于响应终端设备发送的网络访问请求，利用脚本获

取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

计算模块 320，用于对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

判定模块 330，用于当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述获取模块还用于用脚本获取原始类别的特征信息的特征值，并通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

进一步的，所述卡方统计量包括第一卡方统计量，所述计算模块还用于根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的一特定的必要特征值，求取所述必要特征值的第一平均值；根据所述必要特征值和所述第一平均值，计算得到所述终端设备的对应必要特征值的第一卡方统计量。

进一步的，所述判断阈值包括第一判断阈值，所述计算模块还用于根据所述设定时间段内所得到的第一卡方统计量，计算得到所述第一卡方统计量的四分位距的上限值作为所述特征值对应的第一判断阈值。

进一步的，所述卡方统计量包括第二卡方统计量，所述计算模块还用于根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的多个特征值，得到对应的非线性组合特征集的多个特征值的维度向量作为所述非线性组合特征集的特征值；根据所有所述非线性组合特征集的特征值，求取对应的第二平均值；根据所述非线性组合特征集的特征值和所述第二平均值，并计算得到所述终端设备的所述非线性组合特征集的特征值的第二卡方统计量。

进一步的，所述判断阈值包括第二判断阈值，所述计算模块还用于根据设定时间段内所有网络访问请求对应的所述第二卡方统计量形成的曲线，并得到所述曲线的最大斜率对应的第二卡方统计量作为第二判断阈值。

请参考图 4，图 4 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 410、存储介质 420、存储器 430 和网络接口 440。其中，该服务器的存储介质 420 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 410 执行时，可使得处理器 410 实现一种网络访问的异常判定方法，处理器 410 能实现图 3 所示实施例中的一种网络访问的异常判定装置中的获取模块 310、计算模块 320 和判定模块 330 的功能。该服务器的处理器 410 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 430 中可存储有计算机可读指令，该计算机可读指令被处理器 410 执行时，可使得处理器 410 执行一种网络访问的异常判定方法。该服务器的网络接口 440 用于与终端连接通信。本领域技术人员可以理解，图 4 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存储有计算机可读指令的计算机可读存储介质，所述计算机可读存储介质可以为非易失性可读存储介质，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：响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；对所述非线性组合特征集的特征值求取设定时间段内所述所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；利用所述卡方统计量得到对应的特征值为离群点时，判定对应的网络访问为异常访问。

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网络访问的异常判定方法、装置、服务器及存储介质，根据从所述终端设备发起的网络访问请求中获取对应的多个特征值，并形成非线性组合特征集，根据异常判定需要，从所述非线性组合特征集提取相应的特征值，得到对应的卡方统计量，并由卡方统计量得到该特征值对应的离群点，从而得到对应的网络访问为异常访问的判定结果。

在此基础上，该离群点为所述终端设备的卡方统计量大于对应的判断阈值得到的，根据所述卡方统计量与判断阈值进行对比，从而得到异常的

网络访问的判定结果。

本申请所提供的技术方案运用了采用卡方统计量的检测算法，得到判定依据的值与临界值进行对比后得到相应的判定结果，且不需要对终端设备发起网络访问的特征信息数据进行标注，节省了后期统计和分析的工作量；而且该方案分析的过程简单，结果直观，可容易得到准确率较高的判定结果，最终提高所述网络访问的异常判定的判定效果。

综上，本申请通过网络访问的异常判定方法、装置、服务器及存储介质，通过无监督聚类的离群点检测算法直接对终端设备网络访问所生成的特征信息数据进行分析，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判定能力。

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

1.一种网络访问的异常判定方法，其特征在于，包括以下步骤：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

2.根据权利要求1所述的方法，其特征在于，所述卡方统计量包括第一卡方统计量，

所述对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量的步骤，包括：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的一特定的必要特征值，求取所述必要特征值的第一平均值；

根据所述必要特征值和所述第一平均值，计算得到所述终端设备的对应必要特征值的第一卡方统计量。

3.根据权利要求2所述的方法，其特征在于，所述判断阈值包括第一判断阈值，

所述当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点的步骤之前，还包括：

根据所述设定时间段内所得到的第一卡方统计量，计算得到所述第一

卡方统计量的四分位距的上限值作为所述特征值对应的第一判断阈值。

4.根据权利要求1所述的方法，其特征在于，所述卡方统计量包括第二卡方统计量，

所述对所述非线性组合特征集的特征值求取设定时间段内所述所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量的步骤包括：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的多个特征值，得到对应的非线性组合特征集的多个特征值的维度向量作为所述非线性组合特征集的特征值；

根据所有所述非线性组合特征集的特征值，求取对应的第二平均值；

根据所述非线性组合特征集的特征值和所述第二平均值，并计算得到所述终端设备的所述非线性组合特征集的特征值的第二卡方统计量。

5.根据权利要求4所述的方法，其特征在于，所述判断阈值包括第二判断阈值，

所述当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点的步骤之前，还包括：

根据设定时间段内所有网络访问请求对应的所述第二卡方统计量形成的曲线，并得到所述曲线的最大斜率对应的第二卡方统计量作为第二判断阈值。

6.一种网络访问的异常判定装置，其特征在于，包括：

获取模块，用于响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

计算模块，用于对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

判定模块，用于当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述获取模块还用于用脚本获取原始类别的特征信息的特征值，并通过对原始类别的特征信息的特征值进行度量数据散

布计算，得到识别离群点的有效衍生特征信息的特征值。

7、如权利要求 6 所述的装置，其特征在于，所述卡方统计量包括第一卡方统计量，所述计算模块还用于：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的一特定的必要特征值，求取所述必要特征值的第一平均值；

根据所述必要特征值和所述第一平均值，计算得到所述终端设备的对应必要特征值的第一卡方统计量。

8、如权利要求 7 所述的装置，其特征在于，所述判断阈值包括第一判断阈值，所述计算模块还用于：

根据所述设定时间段内所得到的第一卡方统计量，计算得到所述第一卡方统计量的四分位距的上限值作为所述特征值对应的第一判断阈值

9、如权利要求 6 所述的装置，其特征在于，所述卡方统计量包括第二卡方统计量，所述计算模块还用于：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的多个特征值，得到对应的非线性组合特征集的多个特征值的维度向量作为所述非线性组合特征集的特征值；

根据所有所述非线性组合特征集的特征值，求取对应的第二平均值；

根据所述非线性组合特征集的特征值和所述第二平均值，并计算得到所述终端设备的所述非线性组合特征集的特征值的第二卡方统计量

10、如权利要求 9 所述的装置，其特征在于，所述判断阈值包括第二判断阈值，所述计算模块还用于：

根据设定时间段内所有网络访问请求对应的所述第二卡方统计量形成的曲线，并得到所述曲线的最大斜率对应的第二卡方统计量作为第二判断阈值。

11.一种服务器，其特征在于，包括：

一个或多个处理器；

存储器；

一个或多个计算机可读指令，其中所述一个或多个计算机可读指令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可读指令被执行时实现以下步骤：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识别离群点的有效衍生特征信息的特征值。

12.如权利要求 11 所述的服务器，其特征在于，所述卡方统计量包括第一卡方统计量，

所述对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量的步骤，包括：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的一特定的必要特征值，求取所述必要特征值的第一平均值；

根据所述必要特征值和所述第一平均值，计算得到所述终端设备的对应必要特征值的第一卡方统计量。

13.如权利要求 12 所述的服务器，其特征在于，所述判断阈值包括第一判断阈值，

所述当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点的步骤之前，还包括：

根据所述设定时间段内所得到的第一卡方统计量，计算得到所述第一卡方统计量的四分位距的上限值作为所述特征值对应的第一判断阈值。

14.如权利要求 11 所述的服务器，其特征在于，所述卡方统计量包括第二卡方统计量，

所述对所述非线性组合特征集的特征值求取设定时间段内所述所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量的步骤包括：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的多个特征值，得到对应的非线性组合特征集的多个特征值的维度向量作为所述非线性组合特征集的特征值；

根据所有所述非线性组合特征集的特征值，求取对应的第二平均值；

根据所述非线性组合特征集的特征值和所述第二平均值，并计算得到所述终端设备的所述非线性组合特征集的特征值的第二卡方统计量。

15.如权利要求 14 所述的服务器，其特征在于，所述判断阈值包括第二判断阈值，

所述当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点的步骤之前，还包括：

根据设定时间段内所有网络访问请求对应的所述第二卡方统计量形成的曲线，并得到所述曲线的最大斜率对应的第二卡方统计量作为第二判断阈值。

16.一种存储介质，其特征在于，所述存储介质上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现以下步骤：

响应终端设备发送的网络访问请求，利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集；

对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量；

当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点；

根据得到的离群点的特征值，判定得到所述网络访问为异常访问；

其中，所述非线性组合特征集包括原始类别的特征信息的特征值和有效衍生特征信息的特征值，所述利用脚本获取所述终端设备的多个非线性的特征值，并形成非线性组合特征集的步骤包括：

利用脚本获取原始类别的特征信息的特征值；

通过对原始类别的特征信息的特征值进行度量数据散布计算，得到识

别离群点的有效衍生特征信息的特征值。

17.如权利要求 16 所述的存储介质，其特征在于，所述卡方统计量包括第一卡方统计量，

所述对所述非线性组合特征集的特征值求取设定时间段内所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量的步骤，包括：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的一特定的必要特征值，求取所述必要特征值的第一平均值；

根据所述必要特征值和所述第一平均值，计算得到所述终端设备的对应必要特征值的第一卡方统计量。

18.如权利要求 17 所述的存储介质，其特征在于，所述判断阈值包括第一判断阈值，

所述当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，确定对应的特征值为离群点的步骤之前，还包括：

根据所述设定时间段内所得到的第一卡方统计量，计算得到所述第一卡方统计量的四分位距的上限值作为所述特征值对应的第一判断阈值。

19.如权利要求 16 所述的存储介质，其特征在于，所述卡方统计量包括第二卡方统计量，

所述对所述非线性组合特征集的特征值求取设定时间段内所述所有对应的特征值的平均值，并计算所述终端设备的特征值的卡方统计量的步骤包括：

根据在设定时间段内每一次网络访问请求的所述非线性组合特征集的多个特征值，得到对应的非线性组合特征集的多个特征值的维度向量作为所述非线性组合特征集的特征值；

根据所有所述非线性组合特征集的特征值，求取对应的第二平均值；

根据所述非线性组合特征集的特征值和所述第二平均值，并计算得到所述终端设备的所述非线性组合特征集的特征值的第二卡方统计量。

20.如权利要求 19 所述的存储介质，其特征在于，所述判断阈值包括第二判断阈值，

所述当所述终端设备的特征值的卡方统计量大于对应的判断阈值时，

确定对应的特征值为离群点的步骤之前，还包括：

根据设定时间段内所有网络访问请求对应的所述第二卡方统计量形成的曲线，并得到所述曲线的最大斜率对应的第二卡方统计量作为第二判断阈值。

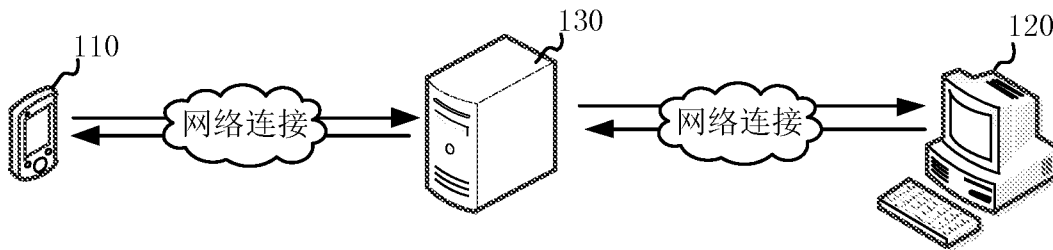


图 1

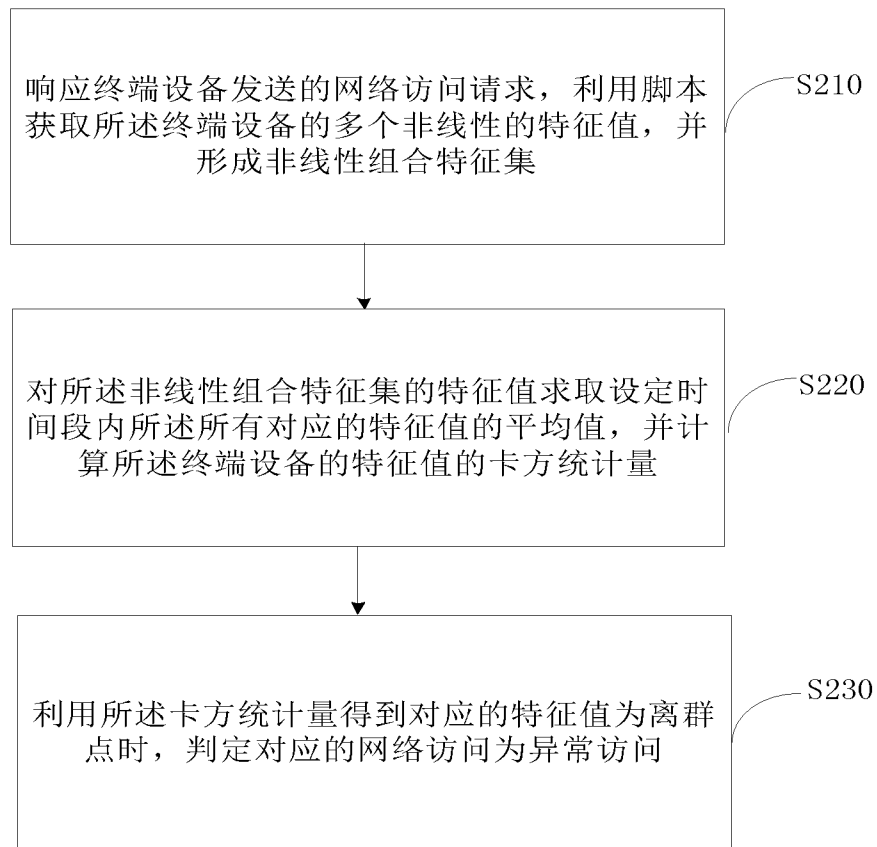


图 2

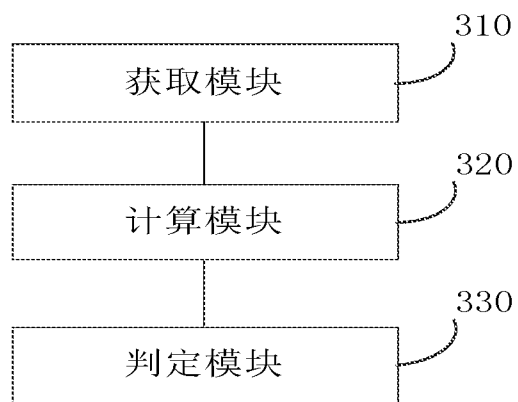


图 3

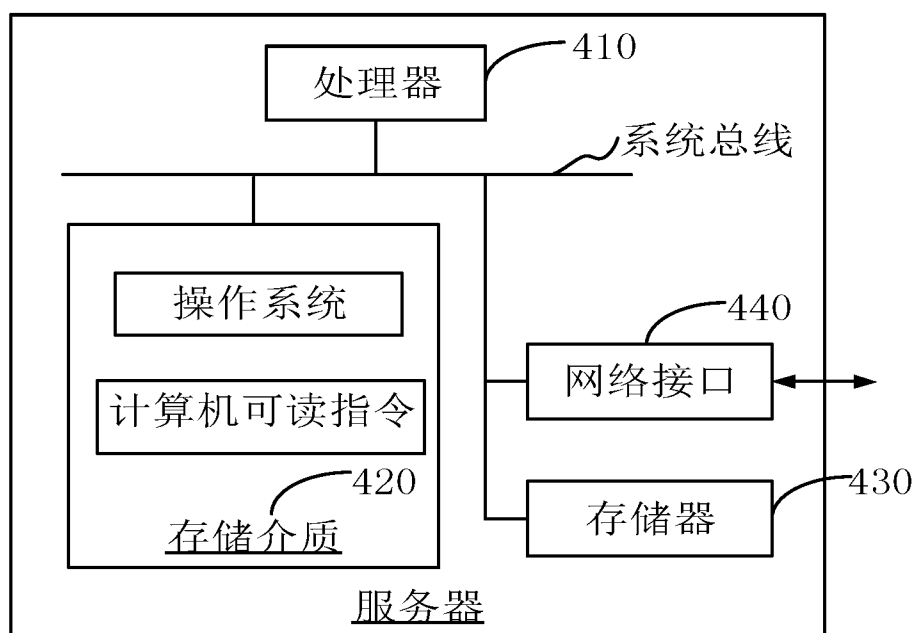


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/118378

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; H04W; H04Q

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: 噪音, noise, 离群点, outlier, 异常, anomaly, 访问, network, 特征, characteristic, 非线性, nonlinear, 卡方, chi-square, SPSS, 阈值, 门限, threshold

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110311909 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 08 October 2019 (2019-10-08) claims 1-10 and description, paragraphs 47-106	1-20
Y	CN 109905362 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 18 June 2019 (2019-06-18) description, paragraphs 0065-0074	1-20
Y	黄强等 CAO, Qiang et al.). "离群点识别方法研究 (An Overview of Outlier Recognition Methods)" 软件导刊 (Software Guide), Vol. 18, No. 6, 04 January 2019 (2019-01-04), pp. 35-40	1-20
A	WO 03014974 A2 (POLYVISTA INC) 20 February 2003 (2003-02-20) entire document	1-20
A	CN 109582741 A (ALIBABA GROUP HOLDING LIMITED) 05 April 2019 (2019-04-05) entire document	1-20
A	CN 105915555 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 31 August 2016 (2016-08-31) 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

12 March 2020

Date of mailing of the international search report

26 March 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/118378

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007088534 A1 (HONEYWELL INTERNATIONAL INC.) 19 April 2007 (2007-04-19) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/118378

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)	
CN	110311909	A	08 October 2019	None			
CN	109905362	A	18 June 2019	None			
WO	03014974	A2	20 February 2003	None			
CN	105915555	A	31 August 2016	None			
US	2007088534	A1	19 April 2007	EP	1946254	A2	23 July 2008
				AT	546794	T	15 March 2012
				CN	101542509	A	23 September 2009
				JP	2009512097	A	19 March 2009
				WO	2007047868	A2	26 April 2007

国际检索报告

国际申请号

PCT/CN2019/118378

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; H04W; H04Q 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, EPDOC: 噪音, noise, 离群点, outlier, 异常, anomaly, 访问, 网络, visit, network, 特征, characteristic, 非线性, nonlinear, 卡方, chi-square, SPSS, 阈值, 门限, threshold																										
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 110311909 A (平安科技深圳有限公司) 2019年 10月 8日 (2019 - 10 - 08) 权利要求1-10, 说明书第47-106段</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>CN 109905362 A (平安科技深圳有限公司) 2019年 6月 18日 (2019 - 06 - 18) 说明书第0065-0074段</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>黄强等. “离群点识别方法研究” 软件导刊, 第18卷, 第6期, 2019年 1月 4日 (2019 - 01 - 04), 第35-40页</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>W0 03014974 A2 (POLYVISTA INC) 2003年 2月 20日 (2003 - 02 - 20) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 109582741 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 105915555 A (北京奇虎科技有限公司等) 2016年 8月 31日 (2016 - 08 - 31) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2007088534 A1 (HONEYWELL INTERNATIONAL INC.) 2007年 4月 19日 (2007 - 04 - 19) 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 110311909 A (平安科技深圳有限公司) 2019年 10月 8日 (2019 - 10 - 08) 权利要求1-10, 说明书第47-106段	1-20	Y	CN 109905362 A (平安科技深圳有限公司) 2019年 6月 18日 (2019 - 06 - 18) 说明书第0065-0074段	1-20	Y	黄强等. “离群点识别方法研究” 软件导刊, 第18卷, 第6期, 2019年 1月 4日 (2019 - 01 - 04), 第35-40页	1-20	A	W0 03014974 A2 (POLYVISTA INC) 2003年 2月 20日 (2003 - 02 - 20) 全文	1-20	A	CN 109582741 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 全文	1-20	A	CN 105915555 A (北京奇虎科技有限公司等) 2016年 8月 31日 (2016 - 08 - 31) 全文	1-20	A	US 2007088534 A1 (HONEYWELL INTERNATIONAL INC.) 2007年 4月 19日 (2007 - 04 - 19) 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																								
PX	CN 110311909 A (平安科技深圳有限公司) 2019年 10月 8日 (2019 - 10 - 08) 权利要求1-10, 说明书第47-106段	1-20																								
Y	CN 109905362 A (平安科技深圳有限公司) 2019年 6月 18日 (2019 - 06 - 18) 说明书第0065-0074段	1-20																								
Y	黄强等. “离群点识别方法研究” 软件导刊, 第18卷, 第6期, 2019年 1月 4日 (2019 - 01 - 04), 第35-40页	1-20																								
A	W0 03014974 A2 (POLYVISTA INC) 2003年 2月 20日 (2003 - 02 - 20) 全文	1-20																								
A	CN 109582741 A (阿里巴巴集团控股有限公司) 2019年 4月 5日 (2019 - 04 - 05) 全文	1-20																								
A	CN 105915555 A (北京奇虎科技有限公司等) 2016年 8月 31日 (2016 - 08 - 31) 全文	1-20																								
A	US 2007088534 A1 (HONEYWELL INTERNATIONAL INC.) 2007年 4月 19日 (2007 - 04 - 19) 全文	1-20																								
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																										
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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																						
* 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 2020年 3月 12日		国际检索报告邮寄日期 2020年 3月 26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 张德珍 电话号码 86-(10)-53961658																								

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/118378

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	110311909	A	2019年 10月 8日	无			
CN	109905362	A	2019年 6月 18日	无			
WO	03014974	A2	2003年 2月 20日	无			
CN	105915555	A	2016年 8月 31日	无			
US	2007088534	A1	2007年 4月 19日	EP	1946254	A2	2008年 7月 23日
				AT	546794	T	2012年 3月 15日
				CN	101542509	A	2009年 9月 23日
				JP	2009512097	A	2009年 3月 19日
				WO	2007047868	A2	2007年 4月 26日