(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 2020/258505 A1

(51) 国际专利分类号:
H04L 12/26 (2006.01)

(21) 国际申请号: PCT/CN2019/103646

(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:
201910578479.X 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 2020/258505 A1

(54) **Title:** NETWORK ACCESS SECURITY DETERMINATION METHOD AND APPARATUS

(54) 发明名称: 网络访问的安全判定方法和装置

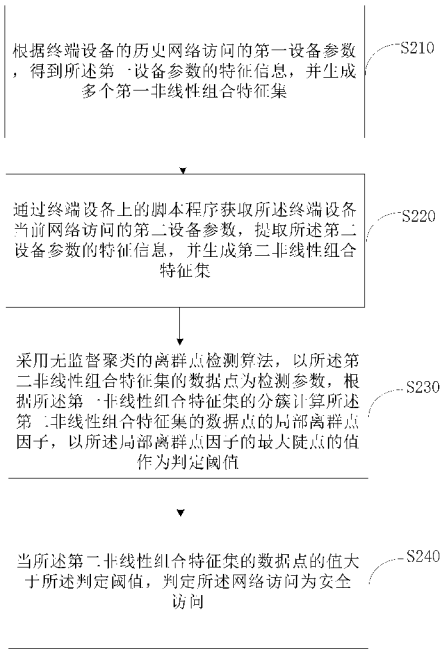

图 2

S210 Obtain, according to first device parameters of historical network access of a terminal device, feature information of the first device parameters, and generate a plurality of first non-linear combination feature sets

S220 Acquire, by means of a script program on the terminal device, second device parameters of current network access of the terminal device, extract feature information of the second device parameters, and generate a second non-linear combination feature set

S230 Calculate, according to clustering of the first non-linear combination feature sets and by using data points of the second non-linear combination feature set as detection parameters, a local outlier factor of the data points of the second non-linear combination feature set by using an unsupervised clustering outlier detection algorithm, and use a value of a maximum steep point of the local outlier factor as a determination threshold

S240 Determine that the network access is a secure access when the value of the data points of the second non-linear combination feature set is greater than the determination threshold

(57) **Abstract:** The present application relates to the field of security detection technology, and provides a network access security determination method and apparatus. Said method comprises: obtaining, according to first device parameters of historical network access of a terminal device, feature information thereof to generate a plurality of first non-linear combination feature sets; acquiring, by means of a script program on the terminal device, second device parameters of the current network access of the terminal device, and extracting corresponding feature information to generate a second non-linear combination feature set; calculating, according to

[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))。

clustering of the first non-linear combination feature sets, a local outlier factor of data points of the second non-linear combination feature set by using an unsupervised clustering outlier detection algorithm, and using the value of a maximum steep point of the local outlier factor as a determination threshold; and determining that the network access is a secure access when the value of the local outlier factor of the data points of the second non-linear combination feature set is greater than the determination threshold. Said method facilitates improvement of the security detection capability of the terminal device for a current network access.

(57) 摘要：本申请为安全检测技术领域，本申请提供一种网络访问的安全判定方法和装置，所述方法包括根据终端设备的历史网络访问的第一设备参数，得到其特征信息生成多个第一非线性组合特征集；通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取对应的特征信息生成第二非线性组合特征集；采用无监督聚类的离群点检测算法，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问。该方法有利于提高对终端设备当前网络访问的安全检测能力。

网络访问的安全判定方法和装置

本申请要求于 2019 年 6 月 28 日提交中国专利局、申请号为 201910578479.X，发明名称为“网络访问的安全判定方法和装置”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安全判定方法和装置。

背景技术

随着网络技术的广泛应用，网络安全也同样得到重视。网络安全的其中一个体现是网站安全容易受到威胁。在目前威胁网站安全的主要手段之一是通过网络爬虫访问网站，导致网站不能正确辨别正常的网络访问。针对这个问题，目前的方法是通过采集网络访问中的终端设备所产生的点击和拖动轨迹的操作数据，判断该网络访问是否安全。发明人意识到，该方法并不能完全准确辨认安全的网络访问，容易将安全的网络访问辨认为非安全网络访问，影响用户的体验。

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，用户的使用痕迹数据不能完全辨认安全的网络访问的问题，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安全判定方法，包括以下步骤：

根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

为解决上述技术问题，本申请还提供一种网络访问的安全判定装置，其包括：

第一生成模块，用于根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

第二生成模块，用于通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

计算模块，用于采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

判定模块，用于当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

为解决上述问题，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上述实施例所述的网络访问的安全判定方法，其中，所述网络访问的安全判定方法，包括：

根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

为解决上述问题，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上述实施例所述的网络访问的安全判定方法，其中，所述网络访问的安全判定方法，包括：

根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

本申请所提供的一种网络访问的安全判定方法和装置，对所述历史采集的终端设备的生成多个第一非线性组合特征集的数据点与终端设备当前网络访问生成的第二非线性组合特征集的数据点的空间位置得到对应的局部离群点因子，并根据所述局部离群点因子与多个局部离群点因子所得到的曲线的最大陡点的值进行比较，得到所述终端设备当前网络访问是否为异常访问的判定结果。

进一步地，本申请所提供的技术方案运用了采用无监督聚类的离群点检测算法，得到判定依据的值并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；而且该方案使相应数据实现可视化，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安全判定方法和装置的判定效果。

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

图 1 是本申请中的实施例执行网络访问的安全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安全判定方法的流程图；

图 3 是本申请中的另一个实施例的网络访问的安全判定方法的流程图；

图 4 为本申请中的一个实施例的网络访问的安全判定装置的示意图；

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

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。

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安全判定。

为了解决目前安全判定方法不容易辨认安全的网络访问的问题，本申请提供了一种网络访问的安全判定方法。可参考图 2，图 2 是一个实施例的网络访问的安全判定方法的流程图，该方法包括以下步骤：

S210、根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集。

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，服务器从终端设备所发出的历史网络访问的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生成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网络访问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，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集。

为了可实时判定所述终端设备的网络访问是否安全状态，根据判定需要，对所述终端设备当前每一次访问的状态进行判定。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网络访问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，根据所述特征信息得到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、采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值。

在本申请提供的一种网络访问的安全判定方法，所述第二非线性组合特征集在该网络访问的安全判定方法作为待检样本，在采用无监督聚类的离群点检测算法构建对应的检测模型的过程中，以所述第二非线性组合特征集的数据点为检测参数。

所述第二非线性组合特征集的数据点是离散的，相对于所述第一设备参数的特征信息的数据点而言，可能有部分靠近所述第一设备参数的特征信息的大部分数据点在空间上形成的集合，相比较而言，有部分会远离所述集合形成离群点。根据所述计算得到对应第二非线性组合特征集的数据

点的局部离群点因子，以便通过作为检测样本的所述第二非线性组合特征集得到与所述第一非线性组合特征集的数据点的空间位置关系，从而可根据相关空间位置关系得到的数值对所述终端设备发起网络访问是否为安全状态。在本实施例中，相关空间位置关系以所述局部离群点因子的最大陡点的值进行表征，以所述最大陡点的值作为判定对应终端设备当前发起的网络请求是否属于正常状态。

S240、当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问。

在该步骤中，根据步骤 S230 得到的所述将所述第二非线性组合特征集的数据点的局部离群点因子的值与最大陡点的值进行比较，根据比较结果，判定对应终端设备当前发起的网络请求是否属于正常状态。

如果所述第二非线性组合特征集的数据点的值大于所述判定阈值，则判定所述终端设备当前发起的网络访问为安全访问；否则，为非安全访问。

本申请提供的一种网络访问的安全判定方法，通过将终端设备当前发起的网络访问得到的第二非线性组合特征集的数据点与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的分簇的空间位置，及计算所述数据点的局部离群点因子，并以单个局部离群点因子与所有的局部离群点因子形成的最大陡点的值作为判定阈值进行比较，得到所述终端设备发起的网络访问是否为安全访问的判定结果。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，并根据计算得到的局部离群点因子为依据，对所述终端设备发起的网络访问是否为异常访问进行判定，这样，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等终端设备的数据作为安全检测的依据所造成容易将真实用户判别为安全用户的问题，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安全检测的结果，有利于提高网络访问的安全检测的效率。

参考图 3，图 3 是另一个实施例的网络访问的安全判定方法的流程图，在上述方案描述的基础上，步骤 S230 可包括：

S231、采用无监督聚类的离群点检测算法，将所述第一非线性组合特征集划为大簇和小簇；

S232、根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子；

其中，所述大簇和小簇是根据包含数据点的个数，并按照设定比例值进行划分。

根据采用无监督聚类的离群点检测算法的无监督聚类，将所述第一非线性组合特征集划分为大簇和小簇。其中，具体地分簇方法根据所述第一非线性组合特征集中的不同的类别分为若干个簇，每个簇有各自的中心点。在分簇后，按照各个簇的包含数据点的个数进行降序排列，并按照针对数据点个数所设定比例值进行大簇和小簇的划分。在本实施例中，所述设定比例值为 90%，即将集中所有数据点个数的 90%的数据点所形成的簇设定为大簇，其余的根据数据点的空间分布设定为小簇。

利用上述对所述第一非线性组合特征集分簇，对从步骤 S230 得到的作为待检样本的所述第二非线性组合特征集的数据点进行局部离群点因子的计算。根据所述第二非线性组合特征集的数据点分别与上述将所述第一非线性组合特征集划分得到的大簇和小簇的空间位置关系，得到相应的大簇的第一局部离群点因子或对应数据点的小簇的第二局部离群点因子。对于上述的步骤 S232，在本实施例中可具体包括以下步骤：

A1、根据所述第二非线性组合特征集的数据点，分别得到所述数据点与所述大簇的第一距离和所述小簇的第二距离；

A2、若所述第一距离小于所述第二距离，求取所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子，其中，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子为所述大簇的大小值与所述数据点与所述大簇的相似性的乘积；

A3、若所述第一距离大于所述第二距离，求取所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子，其中，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子为所述小簇的大小值与所述数据点与最接近的所述大簇的相似性的乘积。

在计算计算对应的数据点的大簇的第一局部离群点因子或对应数据点的小簇的第二局部离群点因子之前，先判断所述数据点所靠近的分簇，

并根据其所靠近的分簇的相关参数计算对应的簇的局部离群因子。

具体地，根据所述第二非线性组合特征集的数据点，分别得到其与所述大簇的第一距离和所述小簇的第二距离，该距离为所述第二非线性组合特征集的数据点与所述大簇和所述小簇的中心的距离。

当所述第一距离小于所述第二距离时，即所述第二非线性组合特征集的数据点跟靠近所述大簇，求取所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子。所述第一局部离群点因子为大簇的大小值与所述第二非线性组合特征集的数据点与所述大簇的相似性的乘积。

当所述第一距离大于所述第二距离时，即所述第二非线性组合特征集的数据点跟靠近所述小簇，求取所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子。所述第二局部离群点因子第一局部离群点因子。

对于上述关于所述第一局部离群点因子和所述第二局部离群点因子的计算中，其中，所述分簇的大小，即所述大簇的大小值或所述小簇的大小值可以通过对应所述多个第一非线性组合特征集的数据点个数进行衡量。例如，可以直接取对应分簇的数据点个数作为对应分簇的大小值，或者，也可以其对应分簇的数据点个数在所有第一非线性组合特征集的数据点中的占比。

同时，所述大簇的相似性可以通过所述第二非线性组合特征集的数据点与所述大簇的中心的距离进行衡量。例如直接以所述第二非线性组合特征集的数据点与所述大簇的中心的距离作为该大簇的相似性。

通过对所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子和所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子的计算，得到判定所述第二非线性组合特征集的数据点对应的终端设备对应网络访问是否安全访问的依据。

对于步骤 S230 中的以所述局部离群点因子的最大陡点的值作为判定阈值的步骤，可进一步为：

通过选取所有所述数据点的局部离群点因子中斜率最大的局部离群点因子的值作为最大陡点的值，并以所述最大陡点的值作为判定阈值。

根据上述得到的关于所有所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子和所述第二非线性组合特征集的数据点的小簇

的第二局部离群点因子，分别形成对应的曲线，得到各自曲线对应的最大陡点，而该最大陡点为关于对应第一或第二局部离群点因子的曲线的斜拉最大的局部离群点因子，并以所述最大的局部离群点因子的值作为所述最大陡点的值，以所述最大陡点的值作为判定所述第二非线性组合特征集的数据点所对应终端设备网络访问是否安全访问的判定阈值。

在上述基础上，步骤 S240 包括：

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子的值大于所述第一局部离群点因子对应的判定阈值时；或，

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子的值大于所述第二局部离群点因子对应的判定阈值时，判定所述网络访问为安全访问。

具体地，对于靠近所述大簇的所述第二非线性组合特征集的数据点，其对应的第一距离小于第二距离时，若所述得到的第二非线性组合特征集的数据点的大簇的第一局部离群点因子的值大于所述第一局部离群点因子形成曲线得到的判定阈值，则判定所述终端设备对应的网络访问为安全访问。

对于靠近所述小簇的所述第二非线性组合特征集的数据点，其对应的第一距离大于第二距离时，若所述得到的第二非线性组合特征集的数据点的小簇的第二局部离群点因子的值大于所述第二局部离群点因子形成曲线得到的判定阈值，则判定所述终端设备对应的网络访问为安全访问。

对于终端设备当前发起的网络请求被判定为安全访问请求，直接响应请求。否则，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。

对于上述提到的所述第一非线性组合特征集或所述第二非线性组合特征集分别包括：

通过对所述第一非线性组合特征集或所述第二非线性组合特征集的数据点进行度量数据散布计算得到的识别离群点的有效衍生特征信息。

具体地，所述第一非线性组合特征集或所述第二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安全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安全判定装置，如图 4 所示，包括：

第一生成模块 410，用于根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

第二生成模块 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网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

计算模块 430，用于采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

判定模块 440，用于当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问。

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

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 实现一种网络访问的

安全判定方法，处理器 510 能实现图 4 所示实施例中的一种网络访问的安全判定装置中的第一生成模块 410、第二生成模块 420、计算模块 430 和判定模型 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 执行一种网络访问的安全判定方法。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计算机可读存储介质，存储有计算机可读指令，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：根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

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安全判定方法和装置，对所述历史采集的终端设备的生成多个第一非线性组合特征集的数据点与终端设备当前网络访问生成的第二非线性组合特征集的数据点的空间位置得到对应的局部离群点因子，并根据所述局部离群点因子与多个局部离群点因子所得到的曲线的最大陡点的值进行比较，得到所述终端设备当前网络访问是

否为安全访问的判定结果。

本申请所提供的技术方案运用了采用无监督聚类的离群点检测算法，得到判定依据的值并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；而且该方案使相应数据实现可视化，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安全判定方法和装置的判定效果。

综上，本申请通过网络访问的安全判定方法和装置，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，并得到判定是否为安全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辨认为安全用户的问题，提高了对终端设备安全访问的判定能力。

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非易失性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

1.一种网络访问的安全判定方法，包括以下步骤：

根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

2.根据权利要求 1 所述的方法，所述采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数值点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子的步骤，包括：

采用无监督聚类的离群点检测算法，将所述第一非线性组合特征集划为大簇和小簇；

根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子；

其中，所述大簇和小簇是根据包含数据点的个数，并按照设定比例值进行划分。

3.根据权利要求 2 所述的方法，所述根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子的步骤，包括：

根据所述第二非线性组合特征集的数据点，分别得到所述数据点与所述大簇的第一距离和所述小簇的第二距离；

若所述第一距离小于所述第二距离，求取所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子，其中，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子为所述大簇的大小值与所述数据点与所述大簇的相似性的乘积；

若所述第一距离大于所述第二距离，求取所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子，其中，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子为所述小簇的大小值与所述数据点与最接近的所述大簇的相似性的乘积。

4.根据权利要求 3 所述的方法，所述大簇的大小值或所述小簇的大小值通过对应所述多个第一非线性组合特征集的数据点个数进行衡量；

所述大簇的相似性通过所述第二非线性组合特征集的数据点与所述大簇的中心的距离进行衡量。

5.根据权利要求 4 所述的方法，所述以所述局部离群点因子的最大陡点的值作为判定阈值的步骤，包括：

通过选取所有所述第二非线性组合特征集的数据点的局部离群点因子中斜率最大的局部离群点因子的值作为最大陡点的值，并以所述最大陡点的值作为判定阈值。

6.根据权利要求 5 所述的方法，所述当所述第二非线性组合特征集的数据点的值大于所述判定阈值，判定所述网络访问为安全访问的步骤，包括：

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子的值大于所述第一局部离群点因子对应的判定阈值时；或，

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点

的小簇的第二局部离群点因子的值大于所述第二局部离群点因子对应的判定阈值时，判定所述网络访问为安全访问。

7.根据权利要求 1 所述的方法，所述第一非线性组合特征集或所述第二非线性组合特征集分别包括：

通过对所述第一非线性组合特征集或所述第二非线性组合特征集的数据点进行度量数据散布计算得到的识别离群点的有效衍生特征信息。

8.一种网络访问的安全判定装置，包括：

第一生成模块，用于根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

第二生成模块，用于通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

计算模块，用于采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

判定模块，用于当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

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上述网络访问的安全判定方法，其中，所述网络访问的安全判定方法，包括：

根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集；

通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

10.根据权利要求 9 所述的服务器，所述采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数值点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子的步骤，包括：

采用无监督聚类的离群点检测算法，将所述第一非线性组合特征集划为大簇和小簇；

根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子；

其中，所述大簇和小簇是根据包含数据点的个数，并按照设定比例值进行划分。

11.根据权利要求 10 所述的服务器，所述根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子的步骤，包括：

根据所述第二非线性组合特征集的数据点，分别得到所述数据点与所

述大簇的第一距离和所述小簇的第二距离；

若所述第一距离小于所述第二距离，求取所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子，其中，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子为所述大簇的大小值与所述数据点与所述大簇的相似性的乘积；

若所述第一距离大于所述第二距离，求取所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子，其中，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子为所述小簇的大小值与所述数据点与最接近的所述大簇的相似性的乘积。

12.根据权利要求 11 所述的服务器，所述大簇的大小值或所述小簇的大小值通过对应所述多个第一非线性组合特征集的数据点个数进行衡量；

所述大簇的相似性通过所述第二非线性组合特征集的数据点与所述大簇的中心的距离进行衡量。

13.根据权利要求 12 所述的服务器，所述以所述局部离群点因子的最大陡点的值作为判定阈值的步骤，包括：

通过选取所有所述第二非线性组合特征集的数据点的局部离群点因子中斜率最大的局部离群点因子的值作为最大陡点的值，并以所述最大陡点的值作为判定阈值。

14.根据权利要求 13 所述的服务器，所述当所述第二非线性组合特征集的数据点的值大于所述判定阈值，判定所述网络访问为安全访问的步骤，包括：

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子的值大于所述第一局部离群点因子对应的判定阈值时；或，

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子的值大于所述第二局部离群点因子对应的判定阈值时，判定所述网络访问为安全访问。

15.一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上述网络访问的安全判定方法，其中，所述网络访问的安全判定方法，包括：

根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参

数的特征信息，并生成多个第一非线性组合特征集；

通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集；

采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值；

当所述第二非线性组合特征集的数据点的局部离群点因子的值大于所述判定阈值，判定所述网络访问为安全访问；

其中，所述第一非线性组合特征集为历史网络访问获取的终端设备的非线性特征信息；所述第二非线性组合特征集为当前网络方法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；该特征信息包括终端设备的属性数据和访问数据。

16.根据权利要求 15 所述的非易失性计算机可读存储介质，所述采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数值点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子的步骤，包括：

采用无监督聚类的离群点检测算法，将所述第一非线性组合特征集划为大簇和小簇；

根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子；

其中，所述大簇和小簇是根据包含数据点的个数，并按照设定比例值进行划分。

17.根据权利要求 16 所述的非易失性计算机可读存储介质，所述根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子的步骤，包括：

根据所述第二非线性组合特征集的数据点，分别得到所述数据点与所述大簇的第一距离和所述小簇的第二距离；

若所述第一距离小于所述第二距离，求取所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子，其中，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子为所述大簇的大小值与所述数据点与所述大簇的相似性的乘积；

若所述第一距离大于所述第二距离，求取所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子，其中，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子为所述小簇的大小值与所述数据点与最接近的所述大簇的相似性的乘积。

18.根据权利要求 17 所述的非易失性计算机可读存储介质，所述大簇的大小值或所述小簇的大小值通过对应所述多个第一非线性组合特征集的数据点个数进行衡量；

所述大簇的相似性通过所述第二非线性组合特征集的数据点与所述大簇的中心的距离进行衡量。

19.根据权利要求 18 所述的非易失性计算机可读存储介质，所述以所述局部离群点因子的最大陡点的值作为判定阈值的步骤，包括：

通过选取所有所述第二非线性组合特征集的数据点的局部离群点因子中斜率最大的局部离群点因子的值作为最大陡点的值，并以所述最大陡点的值作为判定阈值。

20.根据权利要求 19 所述的非易失性计算机可读存储介质，

所述当所述第二非线性组合特征集的数据点的值大于所述判定阈值，判定所述网络访问为安全访问的步骤，包括：

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的大簇的第一局部离群点因子的值大于所述第一局部离群点因子对应的判定阈值时；或，

当所述第一距离大于第二距离，所述第二非线性组合特征集的数据点的小簇的第二局部离群点因子的值大于所述第二局部离群点因子对应的判定阈值时，判定所述网络访问为安全访问。

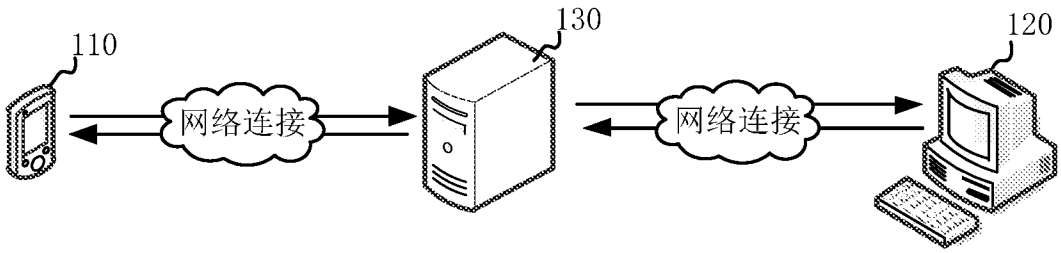
110
130
120
网络连接
网络连接

图 1

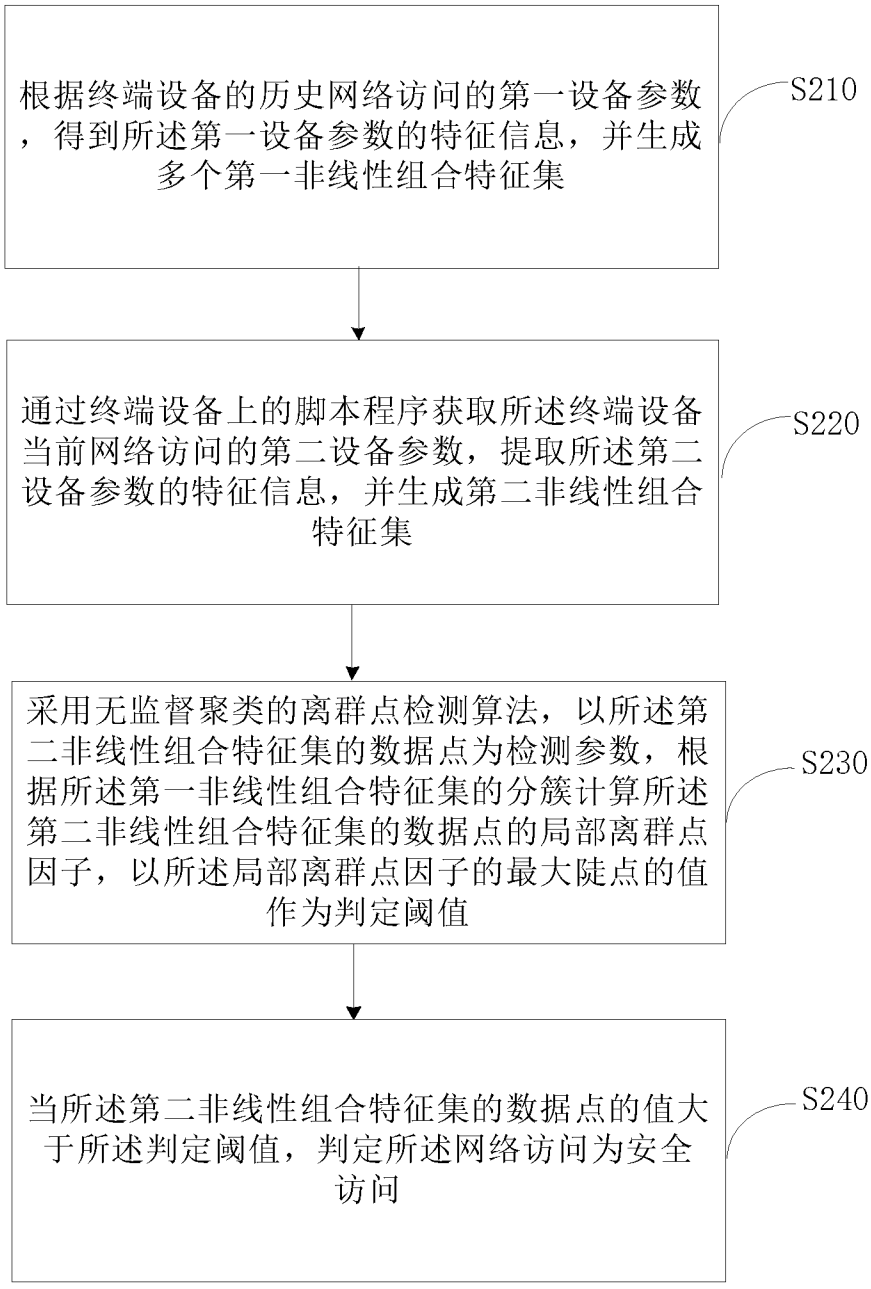
根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集
S210
通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集
S220
采用无监督聚类的离群点检测算法，以所述第二非线性组合特征集的数据点为检测参数，根据所述第一非线性组合特征集的分簇计算所述第二非线性组合特征集的数据点的局部离群点因子，以所述局部离群点因子的最大陡点的值作为判定阈值
S230
当所述第二非线性组合特征集的数据点的值大于所述判定阈值，判定所述网络访问为安全访问
S240

图 2

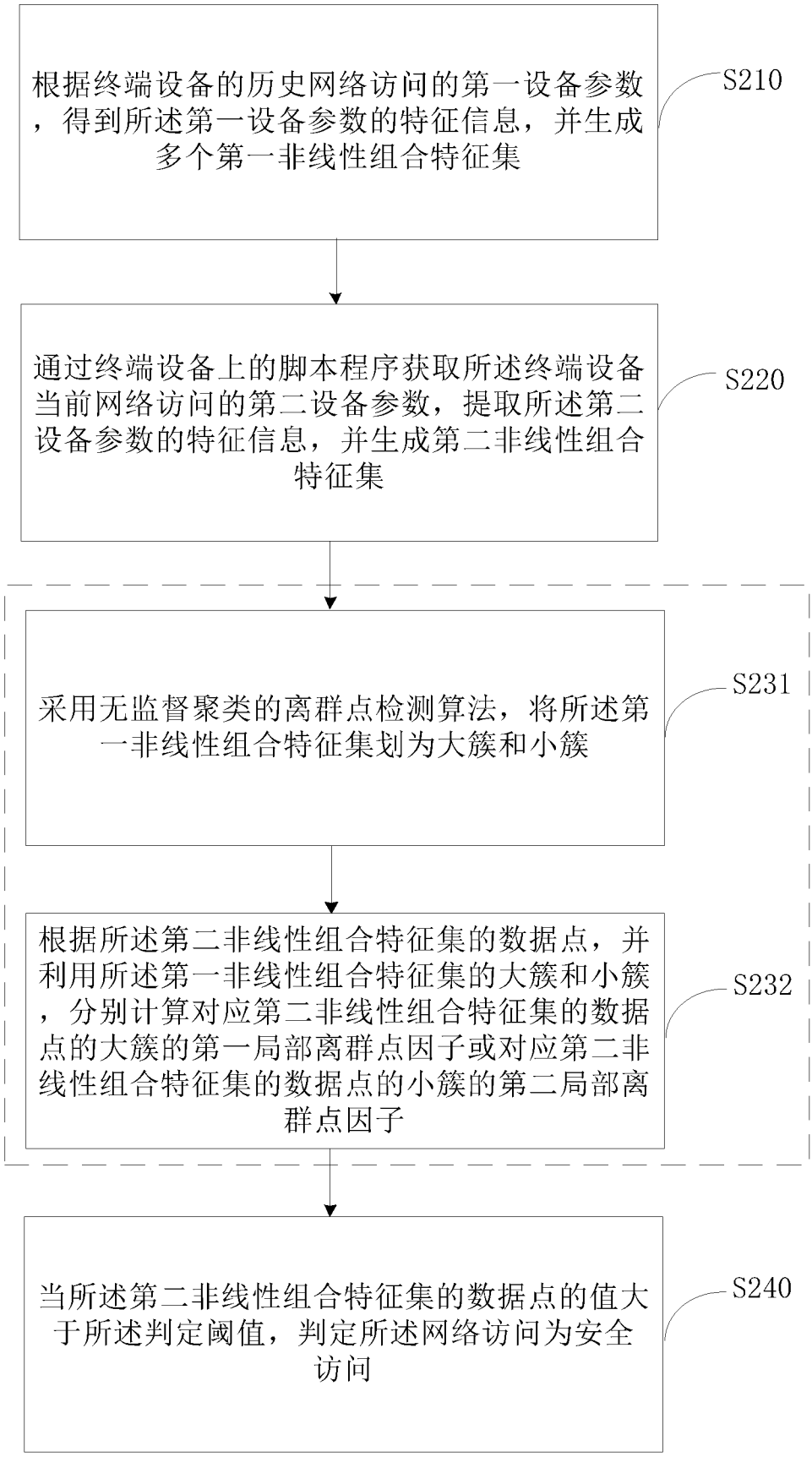
根据终端设备的历史网络访问的第一设备参数，得到所述第一设备参数的特征信息，并生成多个第一非线性组合特征集
S210
通过终端设备上的脚本程序获取所述终端设备当前网络访问的第二设备参数，提取所述第二设备参数的特征信息，并生成第二非线性组合特征集
S220
采用无监督聚类的离群点检测算法，将所述第一非线性组合特征集划为大簇和小簇
S231
根据所述第二非线性组合特征集的数据点，并利用所述第一非线性组合特征集的大簇和小簇，分别计算对应第二非线性组合特征集的数据点的大簇的第一局部离群点因子或对应第二非线性组合特征集的数据点的小簇的第二局部离群点因子
S232
当所述第二非线性组合特征集的数据点的值大于所述判定阈值，判定所述网络访问为安全访问
S240

图 3

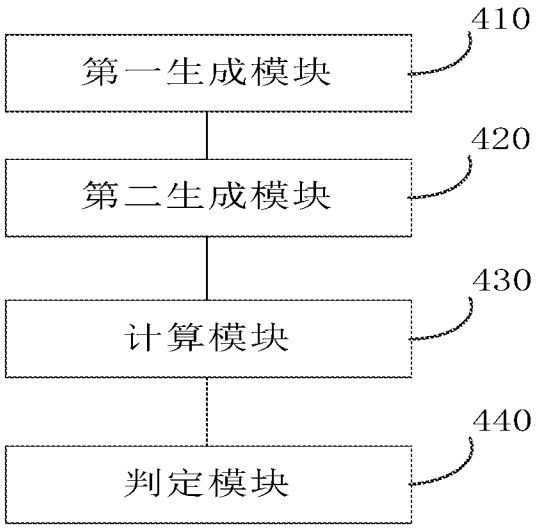
410
第一生成模块
420
第二生成模块
430
计算模块
440
判定模块

图 4

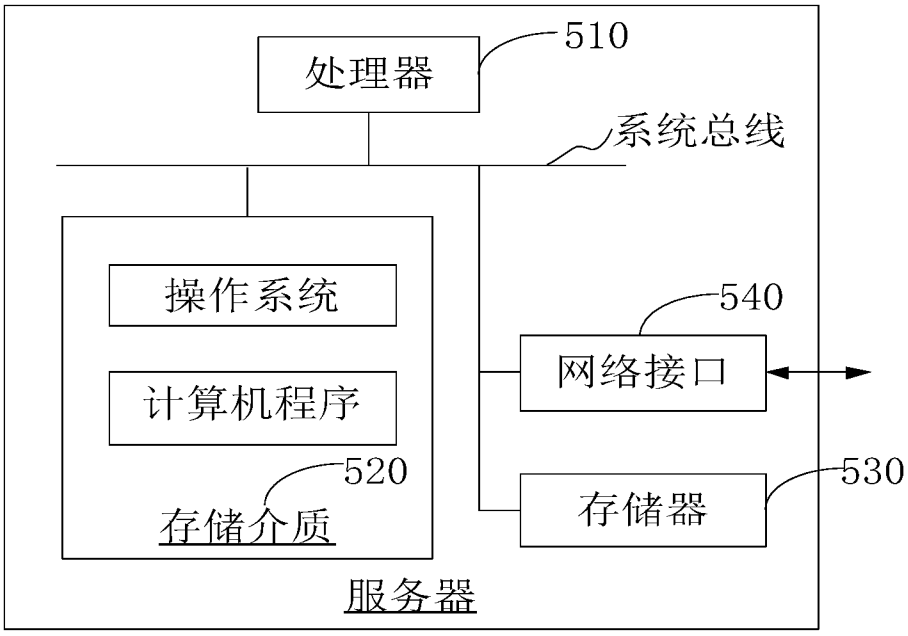
处理器
510
系统总线
操作系统
计算机程序
520
存储介质
540
网络接口
530
存储器
服务器

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/103646

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26(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, IEEE: 网络, 访问, 安全, 异常, 入侵, 检测, 聚类, 离群, 簇, 历史, 当前, network, visit, safety, abnomal, abnormal, intrusion, detection, cluster, outlier, LOF, history, current

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108809745 A (CHINA MOBILE GROUP CHONGQING COMPANY LIMITED et al.) 13 November 2018 (2018-11-13) description, paragraphs 0061-0094, figure 1	1-20
A	CN 104618175 A (SHANGHAI DIANJI UNIVERSITY) 13 May 2015 (2015-05-13) entire document	1-20
A	CN 106294529 A (ALIBABA GROUP HOLDING LIMITED) 04 January 2017 (2017-01-04) entire document	1-20
A	CN 107579956 A (BEIJING QIANXIN TECHNOLOGY CO., LTD.) 12 January 2018 (2018-01-12) entire document	1-20
A	CN 106982196 A (ALIBABA GROUP HOLDING LIMITED) 25 July 2017 (2017-07-25) entire document	1-20
A	US 2017061322 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 02 March 2017 (2017-03-02) entire document	1-20
A	US 2017124478 A1 (CITRIX SYSTEMS, INC.) 04 May 2017 (2017-05-04) 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
26 February 2020	**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/CN2019/103646

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	严晓光 等 (YAN, Xiaoguang et al.). "聚类在网络入侵的异常检测中的应用 (Application to Cluster Algorithm in Anomaly Detection of Network Intrusion)" *计算机系统应用 (Computer Systems & Applications),* No. 10, 31 December 2005 (2005-12-31), pp. 34-37	1-20
A	罗敏 等 (LUO, Min et al.). "基于无监督聚类的入侵检测方法 (An Unsupervised Clustering-Based Intrusion Detection Method)" *电子学报 (Acta Electronica Sinica),* Vol. 31, No. 11, 30 November 2003 (2003-11-30), pp. 1713-1716	1-20
A	Tian Huang et al. "An LOF-based Adaptive Anomaly Detection Scheme for Cloud Computing" *2013 IEEE 37th Annual Computer Software and Applications Conference Workshops,* 31 December 2013 (2013-12-31), pp. 206-211	1-20
A	Gerhard Münz et al. "Traffic Anomaly Detection Using KMeans Clustering" *GI/ITG Workshop MMBnet,* 31 December 2007 (2007-12-31), pp. 1-8	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/103646

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108809745 A	13 November 2018	None	
CN 104618175 A	13 May 2015	None	
CN 106294529 A	04 January 2017	None	
CN 107579956 A	12 January 2018	None	
CN 106982196 A	25 July 2017	WO 2017124942 A1	27 July 2017
		TW 201730766 A	01 September 2017
US 2017061322 A1	02 March 2017	US 2019034836 A1	31 January 2019
US 2017124478 A1	04 May 2017	None	

国际检索报告

国际申请号
PCT/CN2019/103646

A. 主题的分类

H04L 12/26(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,IEEE：网络，访问，安全，异常，入侵，检测，聚类，离群，簇，历史，当前，network, visit, safety, abnomal, abnormal, intrusion, detection, cluster, outlier, LOF, history, current

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 108809745 A (中国移动通信集团重庆有限公司 等) 2018年 11月 13日 (2018-11-13) 说明书第0061-0094段，附图1	1-20
A	CN 104618175 A (上海电机学院) 2015年 5月 13日 (2015-05-13) 全文	1-20
A	CN 106294529 A (阿里巴巴集团控股有限公司) 2017年 1月 4日 (2017-01-04) 全文	1-20
A	CN 107579956 A (北京奇安信科技有限公司) 2018年 1月 12日 (2018-01-12) 全文	1-20
A	CN 106982196 A (阿里巴巴集团控股有限公司) 2017年 7月 25日 (2017-07-25) 全文	1-20
A	US 2017061322 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2017年 3月 2日 (2017-03-02) 全文	1-20
A	US 2017124478 A1 (CITRIX SYSTEMS, INC.) 2017年 5月 4日 (2017-05-04) 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 2月 26日	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 王燕花 电话号码 86-（10）-53961656

国际检索报告

国际申请号
PCT/CN2019/103646

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
A	严晓光 等. "聚类在网络入侵的异常检测中的应用" 计算机系统应用, 第10期, 2005年 12月 31日 (2005-12-31), 第34-37页	1-20
A	罗敏 等. "基于无监督聚类的入侵检测方法" 电子学报, 第31卷, 第11期, 2003年 11月 30日 (2003-11-30), 第1713-1716页	1-20
A	Tian Huang 等. "An LOF-based Adaptive Anomaly Detection Scheme for Cloud Computing" 2013 IEEE 37th Annual Computer Software and Applications Conference Workshops, 2013年 12月 31日 (2013-12-31), 第206-211页	1-20
A	Gerhard Münz 等. "Traffic Anomaly Detection Using KMeans Clustering" GI/ITG Workshop MMBnet, 2007年 12月 31日 (2007-12-31), 第1-8页	1-20

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/103646

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	108809745	A	2018年 11月 13日	无			
CN	104618175	A	2015年 5月 13日	无			
CN	106294529	A	2017年 1月 4日	无			
CN	107579956	A	2018年 1月 12日	无			
CN	106982196	A	2017年 7月 25日	WO	2017124942	A1	2017年 7月 27日
				TW	201730766	A	2017年 9月 1日
US	2017061322	A1	2017年 3月 2日	US	2019034836	A1	2019年 1月 31日
US	2017124478	A1	2017年 5月 4日	无			