

(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



(10) 国际公布号

WO 2020/258657 A1

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

(51) 国际专利分类号:
G06F 21/50 (2013.01)

安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(21) 国际申请号: PCT/CN2019/117607

(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)。

(22) 国际申请日: 2019 年 11 月 12 日 (12.11.2019)

(25) 申请语言: 中文

(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)。

(26) 公布语言: 中文

(30) 优先权:
201910575550.9 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

(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,

(54) Title: ABNORMALITY DETECTION METHOD AND APPARATUS, COMPUTER DEVICE AND STORAGE MEDIUM

(54) 发明名称: 异常检测方法、装置、计算机设备及存储介质

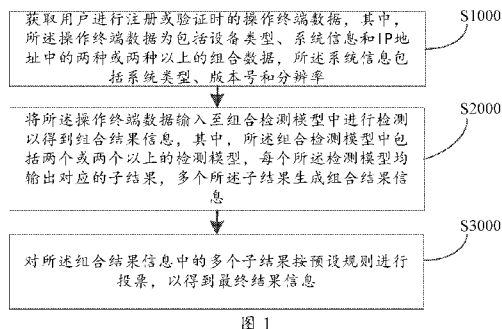


图 1

S1000 Acquire operation terminal data when a user performs registration or verification, wherein the operation terminal data is combined data comprising two or more of a device type, system information and an IP address, and the system information comprises a system type, a version number and a resolution
S2000 Input the operation terminal data into a combined detection model for detection, so as to obtain combined result information, wherein the combined detection model comprises two or more detection models, each detection model outputs a corresponding sub-result, and the combined result information is generated from a plurality of sub-results
S3000 Vote, according to a preset rule, on the plurality of sub-results in the combined result information, so as to obtain final result information

(57) Abstract: An abnormality detection method, comprising: acquiring operation terminal data when a user performs registration or verification, wherein the operation terminal data is combined data comprising two or more of a device type, system information and an IP address; inputting the operation terminal data into a combined detection model for detection, so as to obtain combined result information, wherein the combined detection model comprises two or more detection models, each detection model outputs a corresponding sub-result, and the combined result information is generated from a plurality of sub-results; and voting on the combined result information to obtain final result information. According to the method, a feature conversion method is used to convert, in conjunction with a sample distribution condition, a plurality of pieces of unreadable attribute data into 0-1 two-valued combined features, a distinguishing combined feature set is generated, a detection model is built under a Bagging policy, and whether the user who performs registration or verification is abnormal is determined more comprehensively, thereby improving the accuracy of abnormality detection.

(57) 摘要: 一种异常检测方法, 包括: 获取用户进行注册或验证时的操作终端数据, 其中, 操作终端数据为包括设备类型、系统信息和 IP 地址中的两种或两种以上的组合数据; 将操作终端数据输入至组合检测模型中进行检测以得到组合结果信息, 其中, 组合检测模型中包括两个或两个以上的检测模型, 每个检测模型均输出对应的子结果, 多个子结果生成组合结果信息; 对组合结果信息进行投票, 以得到最终结果信息。该方法采用特征转化方法, 将难以理解的多个属性数据结合样本分布情况, 转化为 0-1 二值的组合特征, 生成具有区分性的组合特征集合, 构建 Bagging 策略下的检测模型, 较为全面的判断注册、验证用户是否异常, 提高了异常检测的准确率。

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, 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))。

异常检测方法、装置、计算机设备及存储介质

- [1] 本申请要求于2019年6月28日提交中国专利局、申请号为201910575550.9、发明名称为“异常检测方法、装置、计算机设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在申请中。
- [2] 技术领域
- [3] 本发明涉及计算机应用技术领域，具体而言，本发明涉及一种异常检测方法、装置、计算机设备及存储介质。
- [4] 背景技术
- [5] 用户异常行为是指违反社会文明准则或成群体行为习惯和标准的“反常”行为。特别是随着人们对公共安全意识、网络安全意识的提高，因此对人群场景、网络等环境中的异常行为检测的关注度越来越高。
- [6] 目前对用户行为异常检测，通常依据个体异常行为的特征进行匹配检测，或依据个体正常行为的特征进行对比检测。但由于样本的属性基本为标称属性，仅分辨率等少量属性为数值型。复杂的文本型设备数据和难以理解的标称属性数据，难以挖掘有效分类特征，进而不能得到好的异常检测模型，导致了异常检测的准确率很低。
- [7] 发明内容
- [8] 本发明的目的旨在至少能解决上述的技术缺陷之一，公开一种异常检测方法、装置、计算机设备及存储介质，能够全面地获取光标的触发数据，以精确地识别异常的光标触发数据。
- [9] 为了达到上述目的，本发明公开一种异常检测方法，包括：
- [10] 获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据；
- [11] 将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；

- [12] 对所述组合结果信息进行投票，以得到最终结果信息。
- [13] 另一方面，本申请公开一种异常检测装置，包括：
- [14] 获取模块：被配置为执行获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；
- [15] 处理模块：被配置为执行将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；
- [16] 执行模块：被配置为执行对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。
- [17] 另一方面，本申请公开一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行上述任一项所述的异常检测方法的步骤。
- [18] 另一方面，本申请公开一种存储有计算机可读指令的存储介质，所述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上述任一项所述的异常检测方法的步骤。
- [19] 本发明的有益效果是：在本申请中公开的异常检测方法及装置，通过分解复杂的文本型设备数据，采用有效的特征转化方法，将难以理解的多个标称属性数据结合样本分布情况，转化为0-1二值的组合特征，生成具有区分性的组合特征集合，挖掘出有效的分类特征集，即可利用此特征集进行模型训练，得到更好的异常检测模型，同时，采用五种算法构建Bagging策略下的检测模型，根据Bagging策略，构建多模型用于异常检测，Naive Bayes从样本整体分布上给出一个综合概率，OneClassSVM和孤立森林分别从正常、异常方面给出样本的检测结果，利用五者的判定结果，能够较为全面的判断注册、验证用户是否异常，有效的避免了只利用数据量较多的正常样本训练出单一检测模型的片面性问题可在一定程度上避免由于样本不均衡导致Naive Bayes分类不准确的问题，提高了异常检测的准确率。

[20] 本发明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，或通过本发明的实践了解到。

[21] 附图说明

[22] 本发明上述的和/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：

[23] 图1为本发明一种异常检测方法示意图；

[24] 图2为本发明组合检测模型的训练方法的流程图；

[25] 图3为本发明获取样本数据以构造组合特征集的方法流程图；

[26] 图4为本发明对得到最终结果信息的方法流程图；

[27] 图5为本发明一种异常检测装置的结构示意图；

[28] 图6为本发明计算机设备基本结构框图。

[29] 具体实施方式

[30] 下面详细描述本发明的实施例，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，仅用于解释本发明，而不能解释为对本发明的限制。

[31] 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，本发明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。

[32] 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），具有与本发明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。

[33] 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。

[34] 具体的，请参阅图1，本发明公开一种异常检测方法，包括：

[35] S1000、获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；

[36] 本申请的技术方案主要用于验证用户操作异常行为的检测，尤其是在监控用户在注册新账号或者登陆时进行验证过程中的异常操作。

[37] 在获取用户通过客户端发送注册信息至服务器端的数据中，包括用户注册的账号信息、身份信息，同时还会携带客户端所在设备的IP地址，进一步的通过设置获取参数，还可以进一步获取得到关于客户端所在设备的设备类型以及系统信息。这里的设备类型包括设备的硬件支持，比如手机、平板、电脑终端或者其他设备，而系统信息为这些硬件支持的软件，比如IOS系统、OS系统、WINDO

WS系统、Andriod系统，进一步的，系统信息还包括具体的系统版本号信息以及系统的分辨率等信息。在本申请中，所述操作终端数据至少包括设备类型、系统信息和IP地址中的两种或两种以上的组合信息。例如，其组合信息可以为设备类型、系统类型、IP地址这三种数据，可以是设备类型、系统类型、版本号、IP地址这四种数据，也可以是设备类型、系统类型、版本号、分辨率、IP地址这五个，还可以是其他的数据，以及这些数据的任意组合。

[38] S2000、将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；

[39] 通过步骤S1000可知，获取的操作终端数据为组合信息，该组合信息至少包括设备类型、系统信息和IP地址中的两种或两种以上，将这些组合信息输入至组合检测模型中进行检测，即可得到对应的组合结果信息。在本申请中，组合检测模型包括至少两个检测模型，每个检测模型输出结果都相互独立，因此针对组合信息会输出至少两组结果信息。例如，组合信息为设备类型、系统类型和IP地址这三种，而组合检测模型中包括A、B、C、D和E五种，每个检测模型都相互独立，因此可得到五组针对设备类型、系统类型和IP地址的组合信息的结果信息，比如结果信息分别为（A1、A2、A3）、（B1、B2、B3）、（C1、C2、C3）、（D1、D2、D3）以及（E1、E2、E3），标号1表示设备类型的检测结果信息，标号2表示系统类型的检测结果，标号3表示IP地址的检测结果。

[40] S3000、对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。

[41] 组合检测模块中的多个检测模型分别针对同样的操作终端数据输出对应的子结果后生成组合结果信息，随后，对组合结果信息中的子结果按照一定的规则进行投票以得最终结果信息。这里公开的一定的规则包括但不限于选取子结果相同的数量最多的作为最终结果。

[42] 本申请通过获取用户的操作终端数据，并从中提取多个数据作为组合数据进行识别，通过组合数据使判断结果更准确，此外识别组合数据的检测模型也是组合检测模型，通过多种训练方式训练出来的不同的检测模型对统一组合数据进行

行识别，以投票的方式来获取最终的结果信息，全面地判断注册、验证用户是否异常，有效的避免了只利用数据量较多的正常样训练出单一检测模型的片面性问题，同时降低了由于样本不均衡导致单一的检测模型的不准确性，提高了异常检测的准确率。

[43] 在一实施例中，所述组合检测模型中的检测模型包括：Naive Bayes检测模型、正类的OneClassSVM检测模型、负类的OneClassSVM检测模型、正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型。

[44] Naive Bayes（朴素贝叶斯模型）检测模型是一种分类算法，且借助了贝叶斯定理。另外，它是一种生成模型（generative model），采用直接对联合概率 $P(x,c)$ 建模，以获得目标概率值的方法。贝叶斯定理描述了一个事件的可能性，这个可能性是基于了预先对于一些与该事件相关的情况的知识，用数学公式来表述贝叶斯定理：

[45] 用数学公式来表述贝叶斯定理：

[46] $P(c|x)=P(x) P(x|c)/ P(c)= P(x,c)/P(x)$

[47] c 表示的是随机事件发生的一种情况。 x 表示的就是证据（evidence）\状况(condition)，泛指与随机事件相关的因素。

[48] $P(c|x)$ ：在 x 的条件下，随机事件出现 c 情况的概率（后验概率）。

[49] $P(c)$ ：（不考虑相关因素）随机事件出现 c 情况的概率（先验概率）。

[50] $P(x|c)$ ：在已知事件出现 c 情况的条件下，条件 x 出现的概率（后验概率）。

[51] $P(x)$ ： x 出现的概率（先验概率）。

[52] OneClassSVM检测模型是指在训练数据中只有正样本和负样本，符合要求的为正样本，所有其他不符合要求的则为负样本，利用One-Class SVM，它有能力捕获数据集的形状,因此对于强非高斯数据有更加优秀的效果，例如两个截然分开的数据集。严格来说，一分类的SVM并不是一个异常点监测算法，而是一个奇异点检测算法：它的训练集不能包含异常样本，否则的话，可能在训练时影响边界的选取。本申请中，OneClassSVM检测模型包括正类的OneClassSVM检测模型、负类的OneClassSVM检测模型，其中，正类的OneClassSVM检测模型只给定正样本进行训练，而负类的OneClassSVM检测模型只给定负样本进行训练

- 。
- [53] 孤立森林分类与检测模型 (Isolation Forest) 是一个基于Ensemble的快速异常检测方法, 具有线性时间复杂度和高精准度, 是符合大数据处理要求的state-of-the-art算法。适用与连续数据 (Continuous numerical data) 的异常检测, 将异常定义为“容易被孤立的离群点 (more likely to be separated)”——可以理解为分布稀疏且离密度高的群体较远的点。用统计学来解释, 在数据空间里面, 分布稀疏的区域表示数据发生在此区域的概率很低, 因而可以认为落在这些区域里的数据是异常的。在本申请中孤立森林分类与检测模型也包括正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型, 其中正类的孤立森林分类与检测模型通过正样本训练, 负类的孤立森林分类与检测模型通过负样本训练。
- [54] 在一实施例中, 请参阅图2, 上述五种检测模型构成的组合检测模型的训练方法包括:
- [55] S2100、获取样本数据以构造组合特征集, 其中, 所述组合特征集包括正样本和负样本;
- [56] 上述公开的正样本为根据可能的识别目的, 选取的符合该目的数据信息, 这些数据信息的表现形式可以是文字、数字、字符串, 也可以是图片、声音等。本申请的面对是用户检测用户异常输入行为, 其是通过用户客户端的设备类型、系统信息以及IP地址等信息来判断的, 因此在本申请中, 该正样本是指合法的设备类型、系统信息和IP地址, 比如合法的设备类型包括手机端、PC端、平板端和电脑端, 当识别出登录和注册信息是来自于上述公开的设备类型时, 则为正样本, 当识别出的登录和注册信息是不是属于手机、PC端、平板和电脑端的任何一种, 而是通过智能手环等一些未被认定为合法设备类型的终端时, 则该智能手环的设备数据为负样本。这些样本数据通过收集而得到。
- [57] 在一实施例中, 请参阅图3, 所述获取样本数据以构造组合特征集的方法包括:
- [58] S2110、将通过至少两种获取方式而获取的用户注册或验证时的操作终端数据作为样本数据, 其中, 所述获取方式包括通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取;

[59] 在一实施例中，样本数据来源于不同的获取方式，比如，通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取。通过爬虫算法获取为通过编译一段爬虫代码以对用户的登录进行监控，获取用户在注册或者验证时的所有操作终端数据，此过程采集的数据，除了最终的注册信息以及验证信息外，还包括中间信息，比如在传输过程中是否被截取等。设备检测为通过客户端自身识别到的数据，即在客户端，当通过输入工具输入注册信息或者验证信息之后，在最终发送之前，由客户端上自身的输入工具监测到的注册信息或验证信息；而用户发送的注册或验证信息为用户通过客户端发送，且通过后端服务器端接收到的注册或验证信息的。可以说，通过设备检测获得的数据为用户输入的原始数据，而通过爬虫算法获取的数据为原始数据从客户端发送到服务器端过程中的数据，而从用户发送的数据为服务器端接收到的原始数据，从数据输入、传输到接收三个阶段对同一数据进行监控，可以确保数据的一致性。只要任何一个环节中，对比得到的数据不一致，则表示用户注册或验证的数据有异常。

[60] S2120、计算每一种获取方式所获取的样本数据的支持度和置信度；

[61] 这里的支持度揭示了上述几种方式获取的数据同时出现的概率，置信度为表示上述各种方式获取的数据的可信度，通过验证可以得出各种获取样本数据的准确度，根据准确度来对各种方式设置一个数值，以代表其置信度，阈值越高，代表这种方式获取的数据越可信，每种方式都有一个数值来表示其置信度，例如，在上述实施例中，通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中三种方式获取用户注册或验证的数据，通过前期的数据对比和测算，可对三种方式分别设置一个置信度，比如通过爬虫算法获取的数据置信度为A，通过设备检测方式获取的数据置信度为B，通过用户发送的注册或验证信息的方式置信度为C，当通过步骤S2110方式获取了数据后，则根据数据的来源，匹配对应的置信度。

[62] S2130、选取所述支持度和置信度最大的操作终端数据的组合作为基准数据；

[63] 支持度(Support)的公式是： $\text{Support}(A \rightarrow B) = P(A \cup B)$ 。支持度揭示了A与B同时出现的概率。如果A与B同时出现的概率小，说明A与B的关系不大；如果A与B

同时出现的非常频繁，则说明A与B总是相关的。

- [64] 置信度(Confidence)的公式式： $\text{Confidence}(A \rightarrow B) = P(A | B)$ 。置信度揭示了A出现时，B是否也会出现或有多大概率出现。如果置信度为100%，则A和B可以捆绑销售了。如果置信度太低，则说明A的出现与B是否出现关系不大。
- [65] 在本申请中，由于上述的操作终端数据来自于不同的获取方式，因此可以获得多组操作终端数据，每一组操作终端数据的每一个数据都会按照支持度和置信度的公式计算得到对应的数值，选取对应的项目下支持度和置信度都最大的数据，组合起来作为本次计算的基准数据。
- [66] S2140、将每一种所述获取方式所获取的操作终端数据与所述基准数据的比对结果按照第一规则进行标记，构成特征集。
- [67] 由于可以从多种途径下获取到操作终端数据，将操作终端数据与基准数据进行对比，按照第一规则进行标记，则可得到一组特征数据，这组特征数据为特征集。
- [68] 在一实施例中，所述第一规则为，所述操作终端数据中与基准数据相同的数据标记为1，作为正样本，与所述基准数据不同的标记为0，作为负样本。这样，上述多组操作终端数据则构成了由0或1组成的特征集。
- [69] S2200、所述Naive Bayes检测模型同时学习正样本和负样本的识别；所述正类的OneClassSVM检测模型和所述正类的孤立森林分类与检测模型学习正样本的识别；所述负类的OneClassSVM检测模型和负类的孤立森林分类与检测模型学习负样本的识别。
- [70] Naive Bayes检测模型为一种分类算法，对其分别进行正样本和负样本的识别，例如，当输入需要识别的数据时，输出是正类或负类，其中，与正样本一样时，为正类，输出1，与负样本一样时，为负类，输出-1。由于在Naive Bayes检测模型中既进行了正样本的训练，又进行了负样本的训练，因此能够较为准确地得到正类输出和负类输出。正类的OneClassSVM检测模型主要通过正样本进行训练，因此对于正类的输出较为准确，负类的OneClassSVM检测模型主要通过负样本进行训练，因此对于负类的输出较为准确，同样，正类的孤立森林分类与检测模型主要对于正类的输出较为准确，负类的孤立森林分类与检测模型对

于负类的输出较为准确。

[71] 当通过上述步骤S2000获取了组合结果信息后，则对所述组合结果信息进行投票，以得到最终结果信息，具体的，请参阅图4，对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息的方法包括：

[72] S3100、将获取的组合结果信息中的多个子结果根据Bagging策略进行投票；

[73] S3200、选取标记数量最多的结果信息作为最终结果。

[74] 在本申请中，操作终端数据是通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取，获取的方式有多种，每一种方式获取的数据可能相同也可能不同，这就导致了操作终端数据的多样性，而操作终端数据输入至组合检测模型中进行检测后，得到组合结果信息，其中组合检测模型的检测结果是相互独立的，不同的检测模型其训练的原理不同，训练的数据也可能不一样，每个检测模型都有自己的特点，因此得到的组合结果信息也可能不一样，将不同的检测模型得到的检测结果组合起来就得到了组合结果信息。将获取的组合结果信息根据Bagging策略进行投票。

[75] Bagging（装袋）又叫自助聚集，是一种根据均匀概率分布从数据中重复抽样（有放回）的技术。每个抽样生成的自助样本集上，训练一个基分类器；对训练过的分类器进行投票，将测试样本指派到得票最高的类中。每个自助样本集都和原数据一样大。有放回抽样，一些样本可能在同一训练集中出现多次，一些可能被忽略。

[76] 通过对组合结果信息进行对比，选取相同数据最多的作为最终结果。例如，在一实施例中，假设获取的操作终端数据为：设备类型、系统类型、版本号、分辨率、IP地址，在构建组合特征集步骤中，通过

[77] 假设采用Naive Bayes检测模型、正类和负类的OneClassSVM检测模型、正类和负类的孤立森林分类与检测模型五种检测模型得到的组合结果信息如下：

[表1]

	数据1	数据2	数据3	数据4	数据5
Naive Bayes 检测模型	1	1	0	0	1
正类OneClassSVM检测 模型	1	0	1	0	1
负类OneClassSVM检测 模型	1	1	0	1	1
正类的孤立 森林分	0	0	0	0	1
类与检测模 型					
负类的孤立 森林分类与 检测模型	1	1	0	1	0
最终结果	1	1	0	0	1

[78] 上述示例中，五种检测模型分别输出五组数据，由于每组数据都是对操作终端数据的输出结果与基准数据进行对比后，按照第一规则进行标记后构成的数据，因此，每组数据都具有统一性，即被归纳为0或1的数据，这样方便进行对比投票，从上述五组数据种，可以看出，对于数据1，出现“1”数量最多，因此数据1的最终结果为“1”，数据2的最终结果为“1”，数据3的最终结果为“0”，数据4的最终结果为“0”，数据5的最终结果为“1”，因此最终结果为“1、1、0、0、1”。

[79] 本申请的技术方案中，通过分解复杂的文本型设备数据，采用有效的特征转化方法，将难以理解的多个标称属性数据结合样本分布情况，转化为0-1二值的组

合特征，生成具有区分性的组合特征集合，挖掘出有效的分类特征集，即可利用此特征集进行模型训练，得到更好的异常检测模型，同时，采用五种算法构建Bagging策略下的检测模型，根据Bagging策略，构建多模型用于异常检测，Naive Bayes从样本整体分布上给出一个综合概率，OneClassSVM和孤立森林分别从正常、异常方面给出样本的检测结果，利用五者的判定结果，能够较为全面的判断注册、验证用户是否异常，有效的避免了只利用数据量较多的正常样训练出单一检测模型的片面性问题，同时降低了由于样本不均衡导致Naive Bayes分类的不准性，提高了异常检测的准确率。

[80] 另一方面，请参阅图5，本申请公开一种异常检测装置，包括：

[81] 获取模块1000：被配置为执行通过获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；处理模块2000：被配置为执行将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；执行模块3000：被配置为执行对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。

[82] 可选的，所述组合检测模型中的检测模型包括：Naive Bayes检测模型、正类的OneClassSVM检测模型、负类的OneClassSVM检测模型、正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型，所述Naive Bayes检测模型同时学习正样本和负样本的识别；所述正类的OneClassSVM检测模型和所述正类的孤立森林分类与检测模型学习正样本的识别；所述负类的OneClassSVM检测模型和负类的孤立森林分类与检测模型学习负样本的识别。

[83] 可选的，所述处理模块中还包括：特征集构建模块：被配置为获取样本数据以构造组合特征集，其中，所述组合特征集包括正样本和负样本。

[84] 可选的，所述特征集构建模块还包括：样本获取模块：被配置为执行将通过至少两种获取方式而获取的用户注册或验证时的操作终端数据作为样本数据，其中，所述获取方式包括通过爬虫算法获取、设备检测获得以及从用户发送的注

册或验证信息中获取；计算模块：被配置为执行计算每一种获取方式所获取的样本数据的支持度和置信度；第一选取模块：被配置为执行选取所述支持度和置信度最大的操作终端数据的组合作为基准数据；标记模块：被配置为执将每一种所述获取方式所获取的操作终端数据与所述基准数据的比对结果按照第一规则进行标记，构成特征集。

[85] 可选的，所述获取所述用户进行注册或验证时的操作终端数据的方法包括：通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取。

[86] 可选的，所述第一规则为：所述操作终端数据中与基准数据相同的数据标记为1，作为正样本，与所述基准数据不同的标记为0，作为负样本。

[87] 可选的，所述执行模块包括：投票模块：被配置为执行将获取的组合结果信息中的多个子结果根据Bagging策略进行投票；第二选取模块：被配置为执行选取标记数量最多的结果信息作为最终结果。

[88] 由于上述的异常检测装置是异常检测方法一一对应的装置，其功能和执行原理一样，此处不再赘述。

[89] 本发明实施例提供计算机设备基本结构框图请参阅图5。

[90] 该计算机设备包括通过系统总线连接的处理器、非易失性存储介质、存储器和网络接口。其中，该计算机设备的非易失性存储介质存储有操作系统、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执行时，可使得处理器实现一种异常检测方法。该计算机设备的处理器用于提供计算和控制能力，支撑整个计算机设备的运行。该计算机设备的存储器中可存储有计算机可读指令，该计算机可读指令被处理器执行时，可使得处理器执行一种异常检测方法。该计算机设备的网络接口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。

[91] 计算机设备通过接收关联的客户端发送的提示行为的状态信息，即关联终端是否开启提示以及贷款人是否关闭该提示任务。通过验证上述任务条件是否达成

，进而向关联终端发送对应的预设指令，以使关联终端能够根据该预设指令执行相应的操作，从而实现了关联终端的有效监管。同时，在提示信息状态与预设的状态指令不相同，服务器端控制关联终端持续进行响铃，以防止关联终端的提示任务在执行一段时间后自动终止的问题。

[92] 本发明还提供一种存储有计算机可读指令的存储介质，所述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上述任一实施例所述的异常检测方法。

[93] 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）等非易失性存储介质，或随机存储记忆体（Random Access Memory，RAM）等。

[94] 应该理解的是，虽然附图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，其可以以其他的顺序执行。而且，附图的流程图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，其执行顺序也不必然是依次进行，而是可以与其他步骤或者其他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。

[95] 以上所述仅是本发明的部分实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权利要求书

- [权利要求 1] 一种异常检测方法，其特征在于，包括：
- 获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；
- 将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；
- 对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。
- [权利要求 2] 根据权利要求1所述的异常检测方法，其特征在于，所述组合检测模型中的检测模型包括：Naive Bayes检测模型、正类的OneClassSVM检测模型、负类的OneClassSVM检测模型、正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型。
- [权利要求 3] 根据权利要求2所述的异常检测方法，其特征在于，所述组合检测模型的训练方法包括：
- 获取样本数据以构造组合特征集，其中，所述组合特征集包括正样本和负样本；
- 所述Naive Bayes检测模型同时学习正样本和负样本的识别；
- 所述正类的OneClassSVM检测模型和所述正类的孤立森林分类与检测模型学习正样本的识别；
- 所述负类的OneClassSVM检测模型和负类的孤立森林分类与检测模型学习负样本的识别。
- [权利要求 4] 根据权利要求3所述的异常检测方法，其特征在于，所述获取样本数据以构造组合特征集的方法包括：
- 将通过至少两种获取方式而获取的用户注册或验证时的操作终端数据作为样本数据，其中，所述获取方式包括通过爬虫算法获取、设备检

测获得以及从用户发送的注册或验证信息中获取；
计算每一种获取方式所获取的样本数据的支持度和置信度；
选取所述支持度和置信度最大的操作终端数据的组合作为基准数据；
将每一种所述获取方式所获取的操作终端数据与所述基准数据的比对结果按照第一规则进行标记，构成特征集。

[权利要求 5] 根据权利要求4所述的异常检测方法，其特征在于，所述第一规则为：
所述操作终端数据中与基准数据相同的数据标记为1，作为正样本，与所述基准数据不同的标记为0，作为负样本。

[权利要求 6] 根据权利要求4所述的异常检测方法，其特征在于，所述对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息的方法包括：
将获取的组合结果信息中的多个子结果根据Bagging策略进行投票；
选取标记数量最多的结果信息作为最终结果。

[权利要求 7] 一种异常检测装置，其特征在于，包括：
获取模块：被配置为执行通过获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；
处理模块：被配置为执行将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；
执行模块：被配置为执行对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。

[权利要求 8] 根据权利要求7所述的异常检测装置，其特征在于，所述组合检测模型中的检测模型包括：Naive Bayes检测模型、正类的OneClassSVM检测模型、负类的OneClassSVM检测模型、正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型。

- [权利要求 9] 根据权利要求8所述的异常检测装置，其特征在于，所述处理模块中还包括：
- 特征集构建模块：被配置为获取样本数据以构造组合特征集，其中，所述组合特征集包括正样本和负样本；
- 所述Naive Bayes检测模型同时学习正样本和负样本的识别；所述正类的OneClassSVM检测模型和所述正类的孤立森林分类与检测模型学习正样本的识别；所述负类的OneClassSVM检测模型和负类的孤立森林分类与检测模型学习负样本的识别。
- [权利要求 10] 根据权利要求9所述的异常检测装置，其特征在于，所述特征集构建模块还包括：
- 样本获取模块：被配置为执行将通过至少两种获取方式而获取的用户注册或验证时的操作终端数据作为样本数据，其中，所述获取方式包括通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取；
- 计算模块：被配置为执行计算每一种获取方式所获取的样本数据的支持度和置信度；
- 第一选取模块：被配置为执行选取所述支持度和置信度最大的操作终端数据的组合作为基准数据；
- 标记模块：被配置为执将每一种所述获取方式所获取的操作终端数据与所述基准数据的比对结果按照第一规则进行标记，构成特征集。
- [权利要求 11] 根据权利要求10所述的异常检测装置，其特征在于，所述第一规则为：
- 所述操作终端数据中与基准数据相同的数据标记为1，作为正样本，与所述基准数据不同的标记为0，作为负样本。
- [权利要求 12] 根据权利要求10所述的异常检测装置，其特征在于，所述执行模块包括：
- 投票模块：被配置为执行将获取的组合结果信息中的多个子结果根据Bagging策略进行投票；
- 第二选取模块：被配置为执行选取标记数量最多的结果信息作为最终

结果。

[权利要求 13] 一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；

将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；

对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。

[权利要求 14] 根据权利要求13所述的计算机设备，其特征在于，所述组合检测模型中的检测模型包括：Naive Bayes检测模型、正类的OneClassSVM检测模型、负类的OneClassSVM检测模型、正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型。

[权利要求 15] 根据权利要求14所述的计算机设备，其特征在于，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

获取样本数据以构造组合特征集，其中，所述组合特征集包括正样本和负样本；

所述Naive Bayes检测模型同时学习正样本和负样本的识别；

所述正类的OneClassSVM检测模型和所述正类的孤立森林分类与检测模型学习正样本的识别；

所述负类的OneClassSVM检测模型和负类的孤立森林分类与检测模型学习负样本的识别。

[权利要求 16] 根据权利要求15所述的计算机设备，其特征在于，所述计算机可读指令被所述处理器执行时，使得所述处理器执行以下步骤：

将通过至少两种获取方式而获取的用户注册或验证时的操作终端数据作为样本数据，其中，所述获取方式包括通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取；

计算每一种获取方式所获取的样本数据的支持度和置信度；

选取所述支持度和置信度最大的操作终端数据的组合作为基准数据；

将每一种所述获取方式所获取的操作终端数据与所述基准数据的比对结果按照第一规则进行标记，构成特征集。

[权利要求 17] 一种存储有计算机可读指令的存储介质，所述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：

获取用户进行注册或验证时的操作终端数据，其中，所述操作终端数据为包括设备类型、系统信息和IP地址中的两种或两种以上的组合数据，所述系统信息包括系统类型、版本号和分辨率；

将所述操作终端数据输入至组合检测模型中进行检测以得到组合结果信息，其中，所述组合检测模型中包括两个或两个以上的检测模型，每个所述检测模型均输出对应的子结果，多个所述子结果生成组合结果信息；

对所述组合结果信息中的多个子结果按预设规则进行投票，以得到最终结果信息。

[权利要求 18] 根据权利要求17所述的存储有计算机可读指令的存储介质，其特征在于，所述组合检测模型中的检测模型包括：Naive Bayes检测模型、正类的OneClassSVM检测模型、负类的OneClassSVM检测模型、正类的孤立森林分类与检测模型和负类的孤立森林分类与检测模型。

[权利要求 19] 根据权利要求18所述的存储有计算机可读指令的存储介质，其特征在于，所述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：

获取样本数据以构造组合特征集，其中，所述组合特征集包括正样本和负样本；

所述Naive Bayes检测模型同时学习正样本和负样本的识别；

所述正类的OneClassSVM检测模型和所述正类的孤立森林分类与检测模型学习正样本的识别；

所述负类的OneClassSVM检测模型和负类的孤立森林分类与检测模型学习负样本的识别。

[权利要求 20] 根据权利要求19所述的存储有计算机可读指令的存储介质，其特征在于，所述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：

将通过至少两种获取方式而获取的用户注册或验证时的操作终端数据作为样本数据，其中，所述获取方式包括通过爬虫算法获取、设备检测获得以及从用户发送的注册或验证信息中获取；

计算每一种获取方式所获取的样本数据的支持度和置信度；

选取所述支持度和置信度最大的操作终端数据的组合作为基准数据；

将每一种所述获取方式所获取的操作终端数据与所述基准数据的比对结果按照第一规则进行标记，构成特征集。

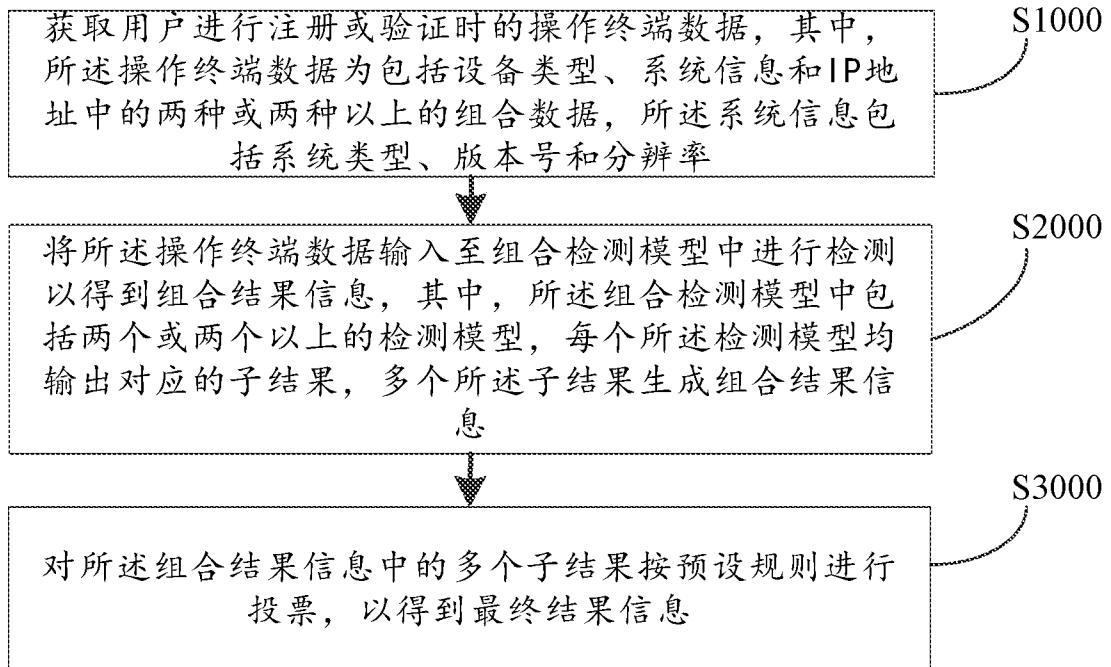


图 1

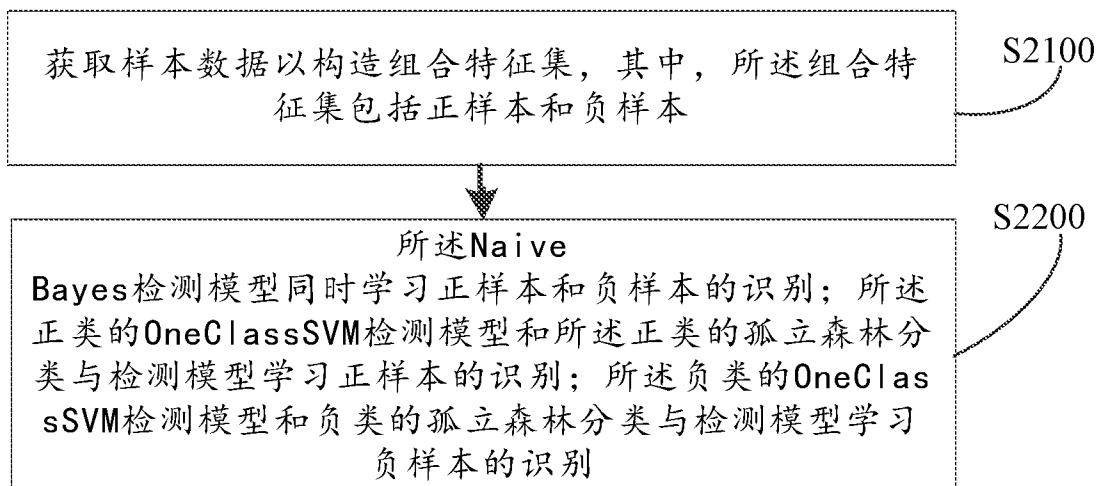


图 2

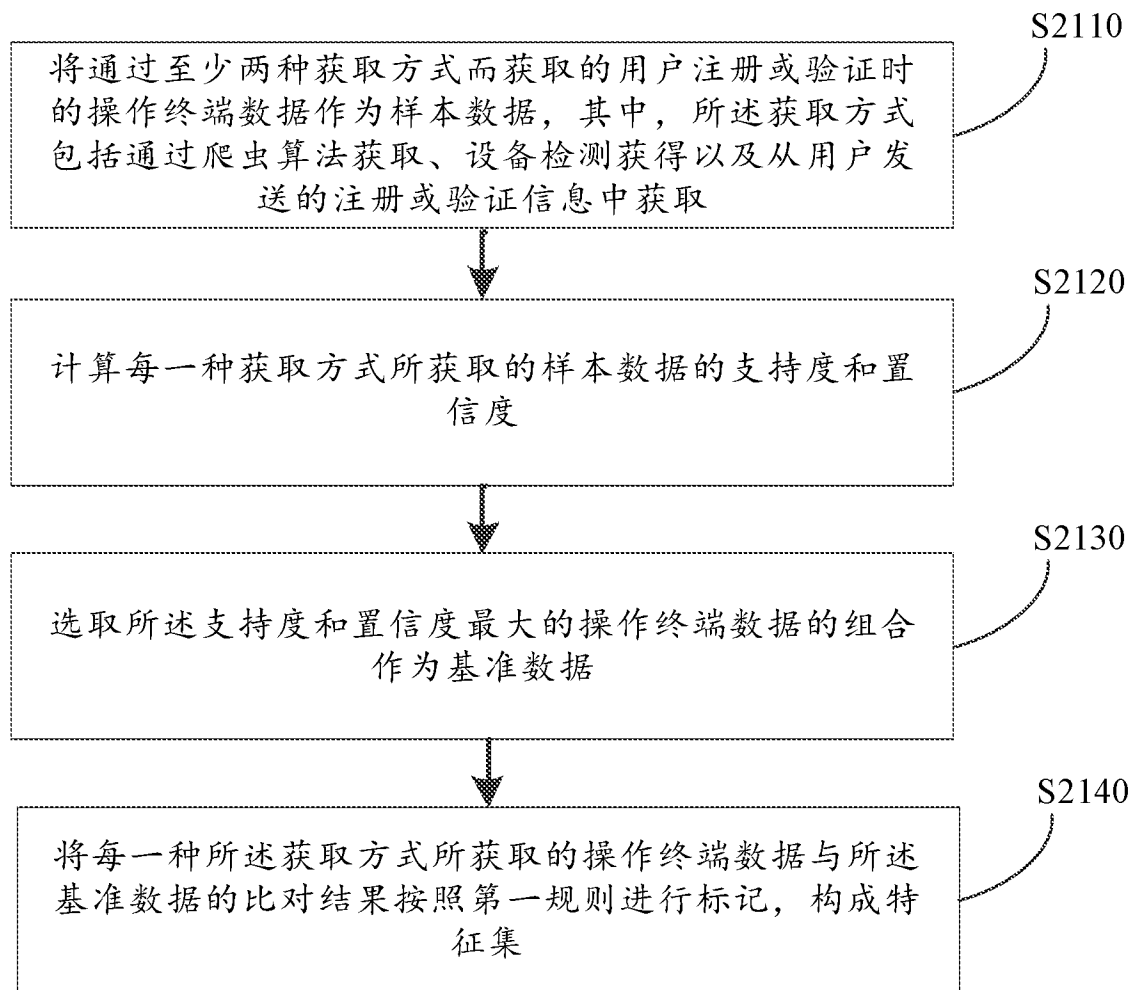


图 3

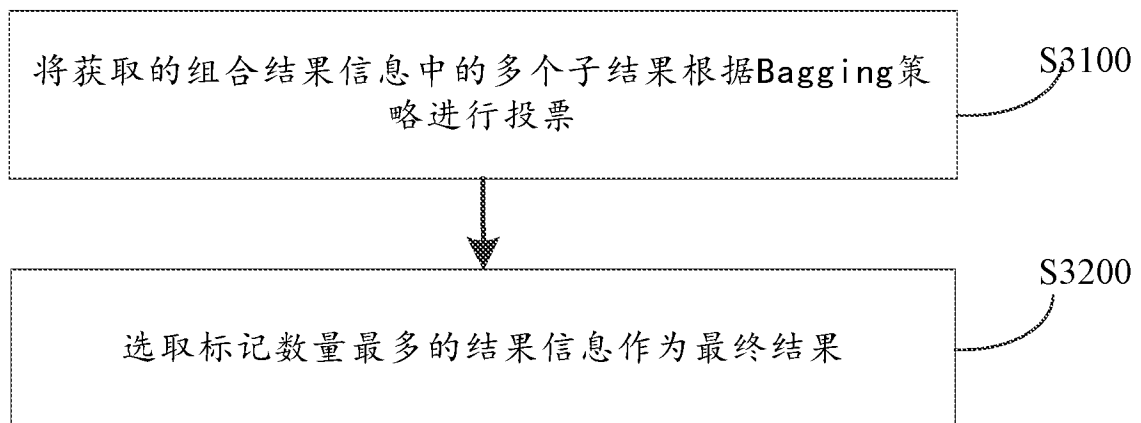


图 4

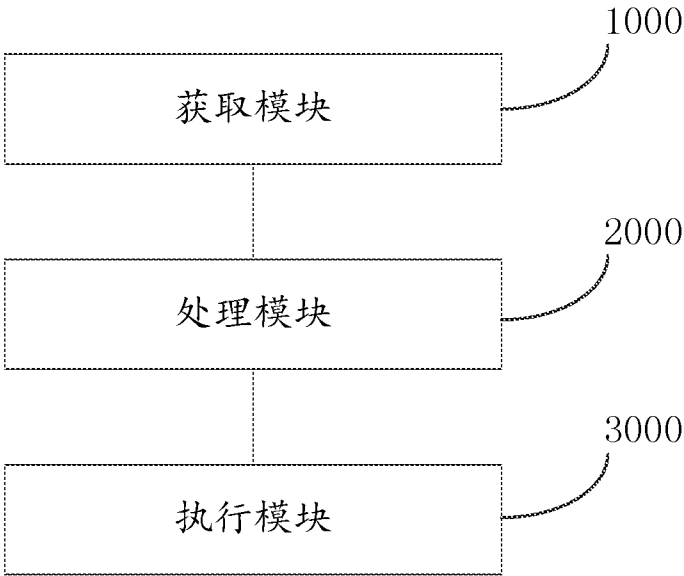


图 5

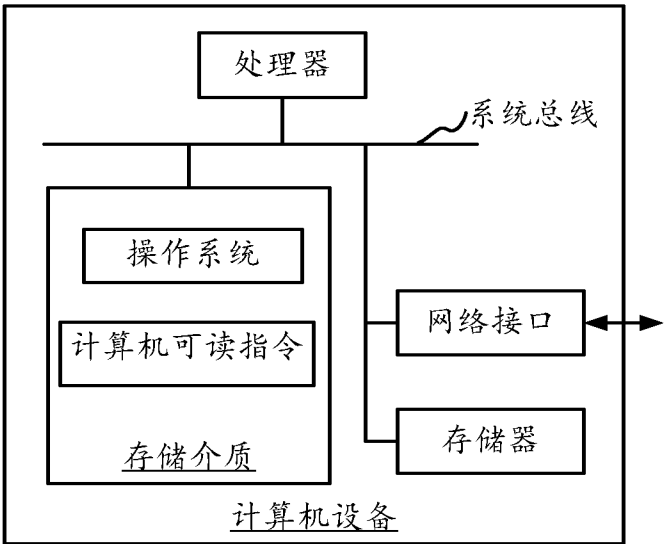


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/117607

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/50(2013.01)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)

G06F; H04L; G06K

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)

WPI; EPODOC; CNKI; CNPAT: 检测, 识别, 异常, 模型, 分类器, 投票, 用户, 注册, 登录, detect+, identify, abnorm+, model, classifier, vote, user, registration, login

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110166462 A (SHENZHEN LAUNCH TECHNOLOGY CO., LTD.) 23 August 2019 (2019-08-23) description, paragraphs [0039]-[0043] and [0070]-[0071]	1-20
X	CN 107612938 A (ZHU, Qihua) 19 January 2018 (2018-01-19) description, paragraphs [0024]-[0028]	1-20
A	CN 108881194 A (ZHENGZHOU XINDA ADVANCED TECHNOLOGY CO., LTD. et al.) 23 November 2018 (2018-11-23) entire document	1-20
A	US 2019034836 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 31 January 2019 (2019-01-31) 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

05 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

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/117607

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110166462	A	23 August 2019	None			
CN	107612938	A	19 January 2018	None			
CN	108881194	A	23 November 2018	None			
US	2019034836	A1	31 January 2019	US	2017061322	A1	02 March 2017

国际检索报告

国际申请号

PCT/CN2019/117607

A. 主题的分类

G06F 21/50(2013.01)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)

G06F; H04L; G06K

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))

WPI;EPDOC;CNKI;CNPAT: 检测, 识别, 异常, 模型, 分类器, 投票, 用户, 注册, 登录, detect+, identify, abnorm+, model, classifier, vote, user, registration, login

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
PX	CN 110166462 A (深圳市元征科技股份有限公司) 2019年 8月 23日 (2019 - 08 - 23) 说明书第[0039]-[0043], [0070]-[0071]段	1-20
X	CN 107612938 A (朱秋华) 2018年 1月 19日 (2018 - 01 - 19) 说明书第[0024]-[0028]段	1-20
A	CN 108881194 A (郑州信大先进技术研究院 等) 2018年 11月 23日 (2018 - 11 - 23) 全文	1-20
A	US 2019034836 A1 (IBM) 2019年 1月 31日 (2019 - 01 - 31) 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

2020年 3月 5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

授权官员

庄湧

电话号码 86-(10)-53961296

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/117607

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	110166462	A	2019年 8月 23日	无			
CN	107612938	A	2018年 1月 19日	无			
CN	108881194	A	2018年 11月 23日	无			
US	2019034836	A1	2019年 1月 31日	US	2017061322	A1	2017年 3月 2日