(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 8 月 20 日 (20.08.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/164274 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/117939

(22) 国际申请日: 2019 年 11 月 13 日 (13.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910115365.1 2019年2月13日 (13.02.2019) 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: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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,

WO 2020/164274 A1

(54) **Title:** NETWORK VERIFICATION DATA SENDING METHOD AND APPARATUS, AND STORAGE MEDIUM AND SERVER

(54) **发明名称:** 网络验证数据的发送方法、装置、存储介质和服务器

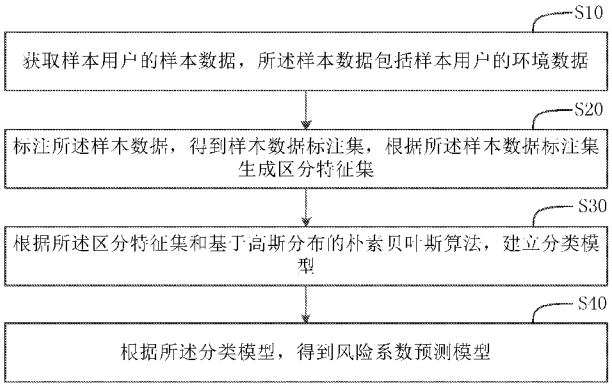

图 1

S10 Acquire sample data of a sample user, the sample data comprising environmental data of the sample user

S20 Label the sample data to obtain a sample data labeled set, and generate a distinguishing feature set according to the sample data labeled set

S30 Establish a classification model according to the distinguishing feature set and a Gaussian-distribution-based naive Bayes algorithm

S40 Obtain a risk coefficient prediction model according to the classification model

(57) **Abstract:** Provided are a network verification data sending method and apparatus, and a storage medium and a server. The network verification data sending method comprises: receiving a verification request of a target user; acquiring environmental data of a terminal device of the target user; obtaining a risk coefficient of the terminal device of the target user according to the environmental data; if the risk coefficient is lower than a preset risk threshold, sending perception-free verification data to the target user; and if the risk coefficient is not lower than the preset risk threshold, sending intelligence verification data to the target user. In the present application, relatively

[见续页]

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))。

simple perception-free verification data can be sent to a terminal device with a low risk coefficient, such that difficulty in verification is reduced for a normal user, and intelligence verification data is sent to a terminal device with a high risk coefficient, such that the capability of a server resisting a malicious attack is improved.

(57) 摘要：本申请提供一种网络验证数据的发送方法、装置、存储介质和服务器，所述网络验证数据的发送方法，包括：接收目标用户的验证请求；获取目标用户终端设备的环境数据；根据所述环境数据，得到目标用户终端设备的风险系数；若风险系数低于预设风险阈值，向目标用户发送无感知验证数据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据。本申请可达到向风险系数低的终端设备发送较为简单的无感知验证数据，降低正常用户的验证难度，同时，向风险系数高的终端设备发送智力验证数据，提高了服务器对抗恶意攻击的能力。

网络验证数据的发送方法、装置、存储介质和服务器

本申请要求于 2019 年 02 月 13 日提交中国专利局、申请号为201910115365.1、申请名称为“网络验证数据的发送方法、装置、存储介质和服务器”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

本申请涉及计算机技术领域，具体而言，本申请涉及一种网络验证数据的发送方法、装置、存储介质和服务器。

背景技术

当用户进行登录操作或浏览部分网页时，为了避免机器操作占用服务器资源或遭受恶意攻击，app 或网页的客户端会要求用户进行行为验证，以确认当前操作的用户为非机器用户，以及避免恶意登录或恶意攻击。在现有的网络验证方式中，对所有用户来说，不管其是否为机器账户、或是账户登录的软硬件环境等因素如何，一般均采用一种网络验证方式。为了保证非机器用户的用户体验，一般验证方式不宜过于复杂，但简单的验证方式又容易被部分风险系数高的用户破解，从而无法达到保护正常用户权益的目的；但设定过于复杂的验证方式，对于一些风险系数低的用户来说，验证方式又存在验证时间长、操作复杂的问题，用户体验很差。

发明内容

本申请针对现有方式的缺点，提出一种网络验证数据的发送方法、装置、存储介质和服务器，用以解决现有技术中存在的的问题。

所述网络验证数据的发送方法，包括：

接收目标用户的验证请求；

获取目标用户终端设备的环境数据；

根据所述环境数据，得到目标用户终端设备的风险系数；

若风险系数低于预设风险阈值，向目标用户发送无感知验证数据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据。

本申请还提出一种网络验证数据的发送装置，该装置包括：

验证请求接收模块，用于接收目标用户的验证请求；

环境数据获取模块，用于获取目标用户终端设备的环境数据；

风险系数计算模块，用于根据所述环境数据，得到目标用户终端设备的风险系数；

验证数据发送模块，用于当风险系数低于预设风险阈值时，向目标用户发送无感知验证数据；当风险系数不低于所述预设风险阈值时，向目标用户发送智力验证数据。

本申请还提出一种计算机非易失性可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现前述任意一项所述的网络验证数据的发送方法。

本申请还提出一种服务器，所述服务器包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现前述任意一项所述的网络验证数据的发送方法

本申请具有以下有益效果：

本申请可达到向风险系数低的终端设备发送较为简单的无感知验证数据，降低正常用户的验证难度，提高用户体验的目的；同时，本申请可向风险系数高的终端设备发送智力验证数据，防止机器用户通过验证请求的方式向服务器发起恶意攻击，从而达到了过滤非正常验证请求的目的，提高了服务器对抗恶意攻击的能力。

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 为本申请建立风险系数预测模型实施例的流程示意图；

图 2 为本申请网络验证数据的发送方法第二实施例的流程示意图；

图 3 为本申请网络验证数据的发送装置实施例的模块结构示意图；

图 4 为本申请服务器实施例的结构示意图。

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。

本技术领域技术人员可以理解，这里所使用的服务器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，云由基于云计算（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。

本申请实施例提供的方案可以应用在网页服务器或应用程序服务器中，通过本申请实施例提供的方案，服务器可判断访问网页或应用程序的用户所在的终端应用环境的风险系数，并根据所述风险系数确定用户的验证方式，从而减少非正常用户对服务器的干扰或攻击。本申请实施例提供的方案可以应用在多种用户验证的场景中，本申请并不对此做出限定。

本申请实施例提供的技术方案分两部分构成：第一部分利用样本用户的区分特征集进行分类模型训练，以建立风险系数预测模型；第二部分利用训练好的风险系数预测模型判断目标用户的风险系数与预设风险阈值的高低，以便发送对应的验证数据。

下面按照建立风险系数预测模型、根据所述风险系数预测模型发送验证数据的顺序对本申请实施例进行详细介绍。

在进行本申请所述网络验证数据的发送方法之前，可先建立风险系数预测模型，如图 1 所示，所述建立风险系数预测模型包括如下步骤：

步骤 S10：获取样本用户的样本数据，所述样本数据包括样本用户的环境数据；

步骤 S20：标注所述样本数据，得到样本数据标注集，根据所述样本数据标注集生成区分特征集；

步骤 S30：根据所述区分特征集和基于高斯分布的朴素贝叶斯算法，建立

分类模型；

步骤 S40：根据所述分类模型，得到风险系数预测模型。

其中，每个步骤具体解释如下：

步骤 S10：获取样本用户的样本数据，所述样本数据包括样本用户的环境数据。

当需要根据样本数据中的环境因素预测用户的风险系数时，所述样本数据需包括多种不同的环境数据，以及对应于不同环境数据的风险系数。故，所述风险系数既包括高风险系数，亦包括低风险系数。为了得到高风险系数对应的环境数据，可采用自动化设备模拟非正常用户的异常行为，以得到对应于该异常行为的验证请求数据与对应的环境数据。当然，在实际应用中，亦可将真实的非正常用户的攻击行为作为样本数据，以不断丰富样本数据的多样性。在大部分的访问中，一般用户均为正常用户的数据，故可将实际应用中正常用户的验证请求数据和对应的环境数据作为样本数据，亦可通过自动化设备模拟正常用户的验证请求，以多种不同的正常样本数据。当样本数据中的环境数据较难获取时，可通过爬虫算法获取终端设备的环境数据。故在本申请的部分实施例中，所述获取样本用户的样本数据，可包括：

通过样本用户发送的验证请求、自动化验证设备和爬虫算法，获取样本用户的样本数据。

在本申请的部分实施例中，可根据爬虫算法和自动化验证设备获取异常的样本数据，将用户正常的验证请求对应的数据作为正常的样本数据。所述样本数据包括样本用户的环境数据和请求数据，所述爬虫算法可通过网页插件或应用程序运行于终端设备上，以将终端的环境数据发送至服务器。所述请求数据可包括用户注册请求和/或验证请求，以在用户注册或验证身份时触发该验证请求。所述环境数据可通过爬虫算法、自动化验证设备和正常验证等途径获取。

在本申请的另一实施例中，所述通过样本用户发送的验证请求、自动化验证设备和爬虫算法，获取样本用户的样本数据，包括：

获取样本用户的正常请求数据，根据所述正常请求数据得到样本用户的环境数据，将所述正常请求数据和环境数据作为正常的样本数据；

通过自动化验证设备模拟异常样本用户的验证请求，获取对应于异常样本

用户的样本请求数据；通过爬虫算法获取所述自动化验证设备的环境数据，得到对应于异常样本用户的环境数据，将所述异常样本用户的样本请求数据和环境数据作为异常的样本数据。

本申请中所述的环境数据可包括：设备类型、硬件型号数据、像素比数据、颜色深度数据、屏幕分辨率数据、可用屏幕分辨率数据、操作系统数据、时间数据、触控数据、特定插件字数、软件安装数据、浏览器数据、堆栈指纹数据中的一个或多个。所述设备类型包括安卓手机、平板电脑、电脑类型等终端类型。所述操作系统数据包括 IOS 类型、版本、分辨率等，终点 IP 地址等。在获取的样本数据中，可能包括部分来源不确定的样本数据，可不将此种数据采用训练样本数据。

步骤 S20：标注所述样本数据，得到样本数据标注集，根据所述样本数据标注集生成区分特征集。

当样本数据为已知数据值时，可根据已知的样本数据信息标注通过所述多种途径获取的样本数据，以获得准确的样本数据标注集。所述样本数据标注集亦可包括正常的样本数据标注集和异常的的样本数据标注集。标注时，可根据已知的终端设备实际数据与通过验证请求等方式获取的样本数据是否一致来判定该样本数据是正常的样本数据还是异常的样本数据。例如：通过终端设备的 user_agent 解析设备为手机，而实际的终端设备为电脑，则将该样本数据标注为异常的样本数据；通过 JavaScript 脚本获取到终端设备不支持多点触控，而真实的终端设备是支持多点触控的，则将该样本数据标注为异常的样本数据。

在部分标注方式中，还可将样本数据与通过正常验证方式获取的正常样本数据的相似度进行标注，将与正常样本数据相似度高的标注为正常样本数据，将与正常样本数据相似度低的标注为异常样本数据。例如：通过终端设备在 1 分钟之内的访问频次或某固定 IP 地址在 1 分钟之内的访问频次标注样本数据；如果终端设备在 1 分钟之内的访问频次或某固定 IP 地址在 1 分钟之内的访问频次超过 10 次，则将该样本数据标注为异常样本数据。又例如：根据 1 个用户的操作系统种类数、设备种类数、IP 地址种类数等因素进行标注，若 1 个用户的操作系统种类数或设备种类数或 IP 地址种类数很多，则将该样本数据标注为异常样本数据。

得到样本数据标注集之后，再根据所述样本数据标注集生成区分特征集。所述区分特征集中的特征均从所述环境数据中确定，其具体特征可包括如下特征中的一个或多个：浏览器语言、终端设备的像素比、终端设备的颜色深度、X 方向屏幕分辨率、Y 方向屏幕分辨率、X 方向可用屏幕分辨率、Y 方向可用屏幕分辨率、X 方向与 Y 方向的屏幕分辨率乘积 resolution_multi、X 方向与 Y 方向的可用屏幕分辨率的乘积 available_resolution_multi、上述两个乘积的差值等。其中，所述两个乘积的差值可用于生成基于分辨率的非线性组合特征，以及用于发掘所述乘积的正常取值范围，尤其是终端设备的分辨率过低时，可根据该差值确定终端设备是否为低端设备，从而为该终端设备配置低端的爬虫算法。所述区分特征集中的具体特征还可以包括如下特征中的一个或多个：获取的 24 小时特征（例如在凌晨 2 点-5 点之间的样本数据可能为异常的样本数据）、月份特征、节假日特征（春节、国庆假期等）、工作日特征、星期特征、终端设备可触控的点的个数、终端设备是否支持可触控、终端设备可触控的点数与操作系统是否一致、终端设备可触控的点数与是否支持可触控是否一致等。其中，终端设备可触控的点数与是否支持可触控是否一致可用于根据终端设备的可触控点数检测操作系统的变化，且不支持触控操作的终端设备常用于爬虫运行而正常用户使用的终端设备一般为可触控的终端设备，故可将终端设备是否支持触控操作作为判断风险系数的特征之一。

所述区分特征集中的具体特征还可以包括如下特征中的一个或多个：CPU 的类型是否可知、浏览器插件是否缺失、使用 JS/CSS 检测到的字体列表是否缺失、操作系统是否为 unknown、WebGL 供应商信息是否缺失、浏览器类型是否为 robot，浏览器生产厂商是否为 other、操作系统生产厂商是否为 other、浏览器插件、浏览器插件总数、使用 JS/CSS 检测到的字体总数、操作系统和系统平台是否一致、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、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、操作系统和系统平台是否一致等。其中，WebGL 供应商信息是否缺失可用于判断用户使用设备的异常，进而根据供应商信息的缺失程度判断用户的有效性，达到分级评判用户有效性的目的；例如

缺失程度分别为高中低时，用户有效性对应为低中高。其中，浏览器类型是否为 robot 可用于根据浏览器的篡改程度评判终端设备是否异常，或者用于根据浏览器类型判断是否为爬虫模型浏览器行为。其中，使用 JS/CSS 检测到的字体总数可用于判断是否有特定的有助于爬虫实现网页数据解析的插件，以及根据字体总数定量判断系统或浏览器是否被爬虫程序篡改。其中，操作系统和系统平台是否一致可用于检测终端设备的系统是否可以被篡改，以及标记样本数据时，用于确认操作系统和系统平台的一致性。

故，本申请还提出一种建立风险系数预测模型的实施例：所述样本用户的环境数据包括：设备类型、硬件型号数据、像素比数据、颜色深度数据、屏幕分辨率数据、可用屏幕分辨率数据、操作系统数据、时间数据、触控数据、特定插件字数、软件安装数据、浏览器数据、堆栈指纹数据中的一个或多个，以从所述环境数据中确定所述区分特征集中的特征。

本申请还可根据前述区分特征集中的数值类型特征计算各数值的极差、四分位数、四分位数极差、五数概括（按次序最小值、上四分位、中位数、下四分位数、最大值），以得到识别离群点的衍生特征。若样本数据中的所述离群点为需要的异常样本数据，则可将该离群点对应的样本数据作为异常的样本数据；若所述离群点对应的样本数据是需要过滤掉的样本数据，则从全部样本数据中去处该离群点对应的样本数据。故在本申请的又一具体实施例中，所述操作系统数据包括用户可用的逻辑处理器总数，所述字体数据包括终端设备的字体总数，所述可用屏幕分辨率数据包括终端设备的 X 方向与 Y 方向的可用屏幕分辨率的乘积，所述浏览器数据包括浏览器安装的插件总数；

所述根据所述样本数据标注集生成区分特征集之前，还包括：

计算所述用户可用的逻辑处理器总数、设备终端的字体总数、可用屏幕分辨率的乘积、插件总数的极差、四分位数、四分位数极差和五数概括；

根据所述极差、四分位数、四分位数极差和五数概括得到识别离群点的衍生特征；

根据所述衍生特征过滤所述样本数据标注集。

本实施例可达到过滤所述样本数据标注集的目的，从而提高风险系数预测模型的准确性。对于不具有数值的特征，可将其映射转化为具体的数值特征；

对于布尔类型特征，由于只有两个值，则不计算其极差、四分位数、四分位数极差、五数概括。

步骤 S30：根据所述区分特征集和基于高斯分布的朴素贝叶斯算法，建立分类模型；

选择基于高斯分布的朴素贝叶斯算法作为有监督异常验证请求的分类模型，可通过贝叶斯分类算法同时学习正、负样本的特征，以得到每一个样本是否异常的综合评估概率，即每个样本数据是否异常的概率。基于高斯分布的朴素贝叶斯算法是现有的概率模型，通过假定原有的数据服从高斯分布、一个特征值在给定类上的影响独立于其他特征的值，学习不同特征取值的特征，通过先验概率和后验概率来计算一个样例属于特定类的概率。其算法模型的数学表达式和算法模型亦为公知技术，在此不再赘述。

步骤 S40：根据所述分类模型，得到风险系数预测模型。

根据所述分类模型可得到每个样本数据是否异常的概率，再设定所述概率与风险系数之间的映射函数或对应关系，即可得到风险系数预测模型。例如，将所述概率与预设阈值相乘，可得到与所述概率正相关或负相关的风险系数。在一些实施例中，所述选定阈值ε 可用为固定系数，所述选定阈值ε 亦可为阶梯系数，以得到对应于不同数值范围的阶梯型风险系数。

本申请通过建立所述风险系数预测模型，可得到对应于不同环境数据的风险系数，以便服务器根据所述风险系数确定验证图片的发送数据。所述验证图片可包括适用于风险系数低的无感知验证图片，例如带有数字或文字的静态图片等，还可包括适用于风险系数高的需要用户参与的智力验证图片，例如滑动拼图、智力问答等。

例如，本申请建立的风险系数预测模型，可检测出正常验证的时间点和请求频率有差异的攻击性验证请求；跟进一步地示例可以为：正常情况下，用户很少在凌晨 2 点-5 点大量频繁地发送验证请求，或是正常情况下，用户不可能在短时间内动态地频繁切换 IP 地址。所以，本申请的风险系数预测模型可根据验证请求的时间特点，快速将终端设备的风险系数标记为高风险，以使用户发送适用于风险系数高的验证数据。

在本申请的一个建立风险系数预测模型的实施例中，所述通过样本用户发

送的验证请求、自动化验证设备和爬虫算法，获取样本用户的样本数据，包括：

获取样本用户的正常请求数据，根据所述正常请求数据得到样本用户的环境数据，将所述正常请求数据和环境数据作为正常的样本数据；

通过自动化验证设备模拟异常样本用户的验证请求，获取对应于异常样本用户的样本请求数据；通过爬虫算法获取所述自动化验证设备的环境数据，得到对应于异常样本用户的环境数据，将所述异常样本用户的样本请求数据和环境数据作为异常的样本数据；

所述标注所述样本数据，得到样本数据标注集；根据所述样本数据标注集生成区分特征集，包括：

分别标注所述正常的样本数据和异常的样本数据，得到正常的样本数据标注集和异常的样本数据标注集；

根据所述正常的样本数据标注集和异常的样本数据标注集生成区分特征集。

本实施例将通过自动化验证设备模拟异常样本用户的验证请求，可快速得到大量的样本数据，以提高建立风险系数预测模型的速度。所述正常请求数据为该验证请求是正常的，若正常的样本用户发出异常的验证请求，则该验证请求不是所述正常请求数据。所述异常样本用户表示风险系数可能较高的样本用户，其验证请求可能是正常的，亦有可能是异常的；通过本申请的所述风险系数预测模型，即可区分出正常的验证请求和异常的验证请求，即所述异常样本用户的风险系数为低或是高。

本申请提出一种网络验证数据的发送方法，如图 2 所示，用于兼顾用户验证方式的复杂性和提高用户体验，其包括如下步骤：

步骤 S1：接收目标用户的验证请求；

步骤 S2：获取目标用户终端设备的环境数据；

步骤 S3：根据所述环境数据，得到目标用户终端设备的风险系数；

步骤 S4：若风险系数低于预设风险阈值，向目标用户发送无感知验证数据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据。

当接收到目标用户的验证请求时，服务器获取目标用户终端设备的环境数据。所述环境数据可通过插件程序、爬虫算法等方法得到，或与所述验证请求

一同发送至服务器;服务器根据所述环境数据计算出目标用户终端设备的风险系数,从而根据所述风险系数的高低向终端设备发送对应的验证数据。本申请可达到向风险系数低的终端设备发送较为简单的无感知验证数据,降低正常用户的验证难度,提高用户体验的目的;同时,本申请可风险系数高的终端设备发送智力验证数据,防止机器用户通过验证请求的方式向服务器发起恶意攻击,从而达到了过滤非正常验证请求的目的,提高了服务器对抗恶意攻击的能力。

在本申请网络验证数据的发送方法的另一实施例中,所述若风险系数不低于所述预设风险阈值,向目标用户发送智力验证数据,包括:

若风险系数不低于所述预设风险阈值,且不高于预设高风险阈值,向目标用户发送第一智力验证数据;所述预设高风险阈值大于所述预设风险阈值;

若风险系数高于所述预设高风险阈值,向目标用户发送第二智力验证数据。

本实施例将所述风险系数分为三个等级,并对风险系数较高的两个等级分别发送第一智力验证数据和第二智力验证数据,例如向中等风险系数的终端设备发送第一智力验证数据,向高等风险系数的终端设备发送第二智力验证数据,从而进一步细化了环境数据与验证数据之间的对应关系,进一步优化了用户体验。

在本申请网络验证数据的发送方法的另一实施例中,所述根据所述环境数据,得到目标用户终端设备的风险系数,包括:

将所述环境数据输入所述风险系数预测模型,得到目标用户终端设备的风险系数;

所述风险系数预测模型通过以下方法建立:

获取样本用户的样本数据,所述样本数据包括样本用户的环境数据;

标注所述样本数据,得到样本数据标注集;

根据所述样本数据标注集生成区分特征集;

根据所述区分特征集和基于高斯分布的朴素贝叶斯算法,建立分类模型;

根据所述分类模型,得到风险系数预测模型。

本实施例中的风险系数预测模型可在服务器中建立,亦可来源于其它设备或网络,具有可移植性,提高了网络验证数据的发送方法的适用范围。

进一步地,若风险系数低于预设风险阈值,向目标用户发送无感知验证数

据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据，可具体采用如下方式：

设定风险阈值的方式：例如，设定风险阈值为 50%；当所述分类模型输出的概率值大于 50%，则为异常；当小于 50%为正常；也可以直接输出 1 和-1，其中 1 表示正常，-1 表示异常；根据正常和异常的结果，分别发送不同的验证数据。

设定风险级别的方式：例如，设定所述分类模型输出的概率值为 0-40%时，对应为低风险 L1 级别；输出的概率值为 40%-60%时，对应为中风险 L2 级别；输出的概率值为 60%-100%时，对应为高风险 L3 级别；根据所述级别，分别发送不同的验证数据。例如：对于 L1 级别可以加载智能无感知验证方式，对于 L2 级别可以随机加载滑动拼图验证方式或在背景图片识别文字的验证方式，对于 L3 级别可以加载语音验证方式。

本申请还提出一种网络验证数据的发送装置，如图 3 所示，该装置包括：

验证请求接收模块 1，用于接收目标用户的验证请求；

环境数据获取模块 2，用于获取目标用户终端设备的环境数据；

风险系数计算模块 3，用于根据所述环境数据，得到目标用户终端设备的风险系数；

验证数据发送模块 4，用于当风险系数低于预设风险阈值时，向目标用户发送无感知验证数据；当风险系数不低于所述预设风险阈值时，向目标用户发送智力验证数据。

本申请实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述任意一项所述的网络验证数据的发送方法。其中，所述存储介质包括但不限于任何类型的盘（包括软盘、硬盘、光盘、CD-ROM、和磁光盘）、ROM（Read-Only Memory，只读存储器）、RAM（Random AcceSS Memory，随即存储器）、EPROM（EraSable Programmable Read-Only Memory，可擦写可编程只读存储器）、EEPROM（Electrically EraSable Programmable Read-Only Memory，电可擦可编程只读存储器）、闪存、磁性卡片或光线卡片。也就是，存储介质包括由设备（例如，计算机）以能够读的形式存储或传输信息的任何介质。可以是只读存储器，磁盘或光盘等。

本申请实施例还提供一种服务器，所述服务器包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现上述任意一项所述的网络验证数据的发送方法。

图 4 为本申请服务器的结构示意图，包括处理器 320、存储装置 330、输入单元 340 以及显示单元 350 等器件。本领域技术人员可以理解，图 4 示出的结构器件并不构成对所有服务器的限定，可以包括比图示更多或更少的部件，或者组合某些部件。存储装置 330 可用于存储应用程序 310 以及各功能模块，处理器 320 运行存储在存储装置 330 的应用程序 310，从而执行设备的各种功能应用以及数据处理。存储装置 330 可以是内存储器或外存储器，或者包括内存储器和外存储器两者。内存储器可以包括只读存储器、可编程 ROM(PROM)、电可编程 ROM(EPROM)、电可擦写可编程 ROM(EEPROM)、快闪存储器、或者随机存储器。外存储器可以包括硬盘、软盘、ZIP 盘、U 盘、磁带等。本申请所公开的存储装置包括但不限于这些类型的存储装置。本申请所公开的存储装置 330 只作为例子而非作为限定。

输入单元 340 用于接收信号的输入，以及接收目标用户在第一统计日期的用户属性信息以及对指定目标的访问信息。输入单元 340 可包括触控面板以及其它输入设备。触控面板可收集用户在其上或附近的触摸操作（比如用户使用手指、触笔等任何适合的物体或附件在触控面板上或在触控面板附近的操作），并根据预先设定的程序驱动相应的连接装置；其它输入设备可以包括但不限于物理键盘、功能键（比如播放控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。显示单元 350 可用于显示用户输入的信息或提供给用户的信息以及计算机设备的各种菜单。显示单元 350 可采用液晶显示器、有机发光二极管等形式。处理器 320 是计算机设备的控制中心，利用各种接口和线路连接整个电脑的各个部分，通过运行或执行存储在存储装置 330 内的软件程序和/或模块，以及调用存储在存储装置内的数据，执行各种功能和处理数据。

在一实施方式中，服务器包括一个或多个处理器 320，以及一个或多个存储装置 330，一个或多个应用程序 310，其中所述一个或多个应用程序 310 被

存储在存储装置 330 中并被配置为由所述一个或多个处理器 320 执行，所述一个或多个应用程序 310 配置用于执行以上实施例所述的流失用户预警方法。

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。

应该理解的是，在本申请各实施例中的各功能单元可集成在一个处理模块中，也可以各个单元单独物理存在，也可以两个或两个以上单元集成于一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

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

权利要求

1、一种网络验证数据的发送方法，其特征在于，包括步骤：

接收目标用户的验证请求；

获取目标用户终端设备的环境数据；

根据所述环境数据，得到目标用户终端设备的风险系数；

若风险系数低于预设风险阈值，向目标用户发送无感知验证数据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据。

2、根据权利要求 1 所述的方法，其特征在于，所述若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据，包括：

若风险系数不低于所述预设风险阈值，且不高于预设高风险阈值，向目标用户发送第一智力验证数据；所述预设高风险阈值大于所述预设风险阈值；

若风险系数高于所述预设高风险阈值，向目标用户发送第二智力验证数据。

3、根据权利要求 1 所述的方法，其特征在于，所述根据所述环境数据，得到目标用户终端设备的风险系数之前，还包括建立风险系数预测模型，所述建立风险系数预测模型包括如下步骤：

获取样本用户的样本数据，所述样本数据包括样本用户的环境数据；

标注所述样本数据，得到样本数据标注集，根据所述样本数据标注集生成区分特征集；

根据所述区分特征集和基于高斯分布的朴素贝叶斯算法，建立分类模型；

根据所述分类模型，得到风险系数预测模型；

所述根据所述环境数据，得到目标用户终端设备的风险系数，包括：

将所述环境数据输入所述风险系数预测模型，得到目标用户终端设备的风险系数。

4、根据权利要求 3 所述的方法，其特征在于，所述获取样本用户的样本数据，包括：

获取样本用户的正常请求数据，根据所述正常请求数据得到样本用户的环境数据，将所述正常请求数据和环境数据作为正常的样本数据；

通过自动化验证设备模拟异常样本用户的验证请求，获取对应于异常样本用户的样本请求数据；通过爬虫算法获取所述自动化验证设备的环境数据，得

到对应于异常样本用户的环境数据，将所述异常样本用户的样本请求数据和环境数据作为异常的样本数据；

所述标注所述样本数据，得到样本数据标注集；根据所述样本数据标注集生成区分特征集，包括：

分别标注所述正常的样本数据和异常的样本数据，得到正常的样本数据标注集和异常的样本数据标注集；

根据所述正常的样本数据标注集和异常的样本数据标注集生成区分特征集。

5、根据权利要求 3 所述的方法，其特征在于，所述样本用户的环境数据包括：设备类型、硬件型号数据、像素比数据、颜色深度数据、屏幕分辨率数据、可用屏幕分辨率数据、操作系统数据、时间数据、触控数据、特定插件字数、软件安装数据、浏览器数据、堆栈指纹数据中的一个或多个。

6、根据权利要求 5 所述的方法，其特征在于，所述操作系统数据包括用户可用的逻辑处理器总数，所述字体数据包括终端设备的字体总数，所述可用屏幕分辨率数据包括终端设备的 X 方向与 Y 方向的可用屏幕分辨率的乘积，所述浏览器数据包括浏览器安装的插件总数；

所述根据所述样本数据标注集生成区分特征集之前，还包括：

计算所述用户可用的逻辑处理器总数、终端设备的字体总数、可用屏幕分辨率的乘积、插件总数的极差、四分位数、四分位数极差和五数概括；

根据所述极差、四分位数、四分位数极差和五数概括得到识别离群点的衍生特征；

根据所述衍生特征过滤所述样本数据标注集。

7、根据权利要求 3 所述的方法，其特征在于，所述区分特征集中的特征包括以下任一项或多项：浏览器语言、终端设备的像素比、终端设备的颜色深度、X 方向屏幕分辨率、Y 方向屏幕分辨率、X 方向可用屏幕分辨率、Y 方向可用屏幕分辨率、X 方向与 Y 方向的屏幕分辨率的第一乘积、X 方向与 Y 方向的可用屏幕分辨率的第二乘积、所述第一乘积和所述第二乘积的差值、CPU 的类型是否可知、浏览器插件是否缺失、使用 JS/CSS 检测到的字体列表是否缺失、操作系统是否为 unknown、WebGL 供应商信息是否缺失、浏览器类型

是否为 robot、浏览器生产厂商是否为 other、操作系统生产厂商是否为 other、浏览器插件、浏览器插件总数、使用 JS/CSS 检测到的字体总数、操作系统和系统平台是否一致、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、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、操作系统和系统平台是否一致。

8、一种网络验证数据的发送装置，其特征在于，包括：

验证请求接收模块，用于接收目标用户的验证请求；

环境数据获取模块，用于获取目标用户终端设备的环境数据；

风险系数计算模块，用于根据所述环境数据，得到目标用户终端设备的风险系数；

验证数据发送模块，用于当风险系数低于预设风险阈值时，向目标用户发送无感知验证数据；当风险系数不低于所述预设风险阈值时，向目标用户发送智力验证数据。

9、根据权利要求 8 所述的装置，其特征在于，所述验证数据发送模块在当风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据时，具体用于：

若风险系数不低于所述预设风险阈值，且不高于预设高风险阈值，向目标用户发送第一智力验证数据；所述预设高风险阈值大于所述预设风险阈值；

若风险系数高于所述预设高风险阈值，向目标用户发送第二智力验证数据。

10、根据权利要求 8 所述的装置，其特征在于，所述风险系数计算模块还用于建立风险系数预测模型，所述风险系数计算模块在建立风险系数预测模型时，具体用于：

获取样本用户的样本数据，所述样本数据包括样本用户的环境数据；

标注所述样本数据，得到样本数据标注集，根据所述样本数据标注集生成区分特征集；

根据所述区分特征集和基于高斯分布的朴素贝叶斯算法，建立分类模型；

根据所述分类模型，得到风险系数预测模型；

所述风险系数计算模块在根据所述环境数据，得到目标用户终端设备的风

险系数时，具体用于：

将所述环境数据输入所述风险系数预测模型，得到目标用户终端设备的风险系数。

11、根据权利要求 10 所述的装置，其特征在于，所述风险系数计算模块在获取样本用户的样本数据时，具体用于：

获取样本用户的正常请求数据，根据所述正常请求数据得到样本用户的环境数据，将所述正常请求数据和环境数据作为正常的样本数据；

通过自动化验证设备模拟异常样本用户的验证请求，获取对应于异常样本用户的样本请求数据；通过爬虫算法获取所述自动化验证设备的环境数据，得到对应于异常样本用户的环境数据，将所述异常样本用户的样本请求数据和环境数据作为异常的样本数据；

所述风险系数计算模块在标注所述样本数据，得到样本数据标注集；根据所述样本数据标注集生成区分特征集时，具体用于：

分别标注所述正常的样本数据和异常的样本数据，得到正常的样本数据标注集和异常的样本数据标注集；

根据所述正常的样本数据标注集和异常的样本数据标注集生成区分特征集。

12、根据权利要求 10 所述的装置，其特征在于，所述样本用户的环境数据包括：设备类型、硬件型号数据、像素比数据、颜色深度数据、屏幕分辨率数据、可用屏幕分辨率数据、操作系统数据、时间数据、触控数据、特定插件字数、软件安装数据、浏览器数据、堆栈指纹数据中的一个或多个。

13、根据权利要求 12 所述的装置，其特征在于，所述操作系统数据包括用户可用的逻辑处理器总数，所述字体数据包括终端设备的字体总数，所述可用屏幕分辨率数据包括终端设备的 X 方向与 Y 方向的可用屏幕分辨率的乘积，所述浏览器数据包括浏览器安装的插件总数；

所述风险系数计算模块还用于：

计算所述用户可用的逻辑处理器总数、终端设备的字体总数、可用屏幕分辨率的乘积、插件总数的极差、四分位数、四分位数极差和五数概括；

根据所述极差、四分位数、四分位数极差和五数概括得到识别离群点的衍

生特征；

根据所述衍生特征过滤所述样本数据标注集。

14、根据权利要求 10 所述的装置，其特征在于，所述区分特征集中的特征包括以下任一项或多项：浏览器语言、终端设备的像素比、终端设备的颜色深度、X 方向屏幕分辨率、Y 方向屏幕分辨率、X 方向可用屏幕分辨率、Y 方向可用屏幕分辨率、X 方向与 Y 方向的屏幕分辨率的第一乘积、X 方向与 Y 方向的可用屏幕分辨率的第二乘积、所述第一乘积和所述第二乘积的差值、CPU 的类型是否可知、浏览器插件是否缺失、使用 JS/CSS 检测到的字体列表是否缺失、操作系统是否为 unknown、WebGL 供应商信息是否缺失、浏览器类型是否为 robot、浏览器生产厂商是否为 other、操作系统生产厂商是否为 other、浏览器插件、浏览器插件总数、使用 JS/CSS 检测到的字体总数、操作系统和系统平台是否一致、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、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、操作系统和系统平台是否一致。

15、一种计算机非易失性可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求 1 至 7 中任意一项所述的网络验证数据的发送方法。

16、一种服务器，其特征在于，所述服务器包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现以下步骤：

接收目标用户的验证请求；

获取目标用户终端设备的环境数据；

根据所述环境数据，得到目标用户终端设备的风险系数；

若风险系数低于预设风险阈值，向目标用户发送无感知验证数据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据。

17、根据权利要求 16 所述的服务器，其特征在于，所述处理器在实现所

述若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据时，具体执行以下步骤：

若风险系数不低于所述预设风险阈值，且不高于预设高风险阈值，向目标用户发送第一智力验证数据；所述预设高风险阈值大于所述预设风险阈值；

若风险系数高于所述预设高风险阈值，向目标用户发送第二智力验证数据。

18、根据权利要求 16 所述的服务器，其特征在于，所述处理器在实现所述根据所述环境数据，得到目标用户终端设备的风险系数之前，还用于建立风险系数预测模型，所述处理器在实现所述建立风险系数预测模型时，具体执行以下步骤：

获取样本用户的样本数据，所述样本数据包括样本用户的环境数据；

标注所述样本数据，得到样本数据标注集，根据所述样本数据标注集生成区分特征集；

根据所述区分特征集和基于高斯分布的朴素贝叶斯算法，建立分类模型；

根据所述分类模型，得到风险系数预测模型；

所述处理器在实现所述根据所述环境数据，得到目标用户终端设备的风险系数时，具体执行以下步骤：

将所述环境数据输入所述风险系数预测模型，得到目标用户终端设备的风险系数。

19、根据权利要求 18 所述的服务器，其特征在于，所述处理器在实现所述获取样本用户的样本数据时，具体执行以下步骤：

获取样本用户的正常请求数据，根据所述正常请求数据得到样本用户的环境数据，将所述正常请求数据和环境数据作为正常的样本数据；

通过自动化验证设备模拟异常样本用户的验证请求，获取对应于异常样本用户的样本请求数据；通过爬虫算法获取所述自动化验证设备的环境数据，得到对应于异常样本用户的环境数据，将所述异常样本用户的样本请求数据和环境数据作为异常的样本数据；

所述处理器在实现所述标注所述样本数据，得到样本数据标注集；根据所述样本数据标注集生成区分特征集时，具体执行以下步骤：

分别标注所述正常的样本数据和异常的样本数据，得到正常的样本数据标

注集和异常的样本数据标注集；

根据所述正常的样本数据标注集和异常的样本数据标注集生成区分特征集。

20、根据权利要求 18 所述的服务器，其特征在于，所述操作系统数据包括用户可用的逻辑处理器总数，所述字体数据包括终端设备的字体总数，所述可用屏幕分辨率数据包括终端设备的 X 方向与 Y 方向的可用屏幕分辨率的乘积，所述浏览器数据包括浏览器安装的插件总数；

所述处理器在实现所述根据所述样本数据标注集生成区分特征集之前，还用于实现以下步骤：

计算所述用户可用的逻辑处理器总数、终端设备的字体总数、可用屏幕分辨率的乘积、插件总数的极差、四分位数、四分位数极差和五数概括；

根据所述极差、四分位数、四分位数极差和五数概括得到识别离群点的衍生特征；

根据所述衍生特征过滤所述样本数据标注集。

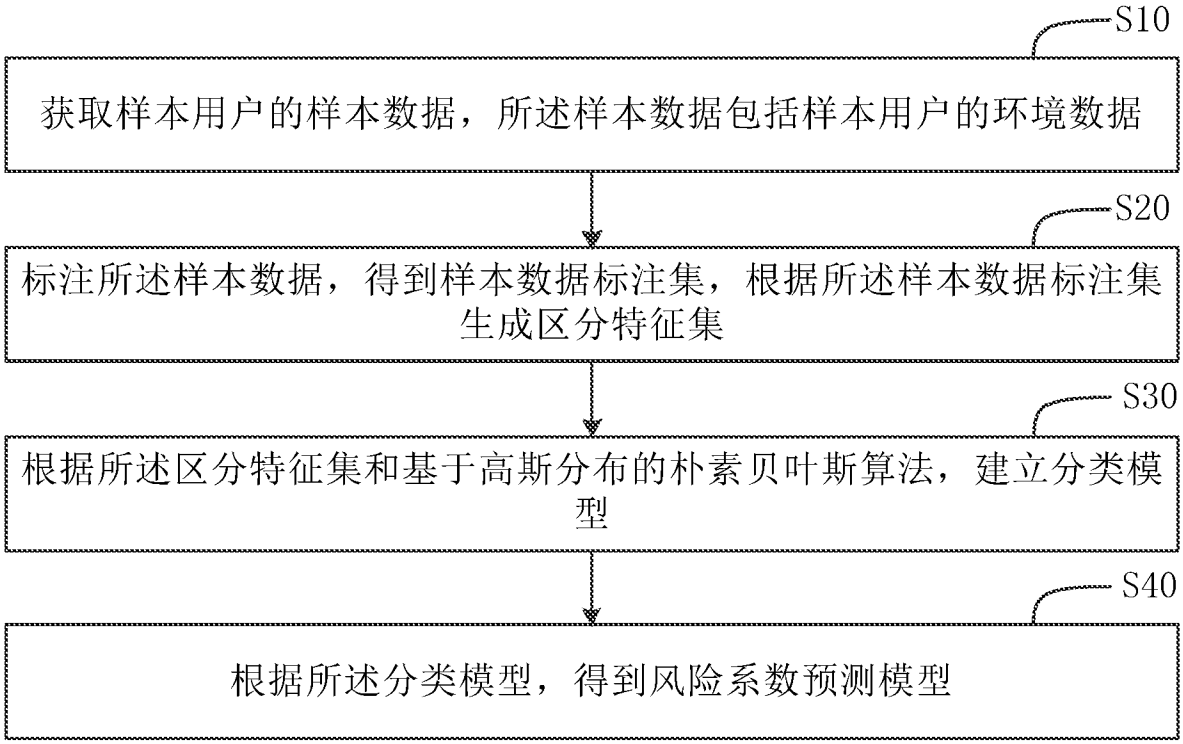
S10
获取样本用户的样本数据，所述样本数据包括样本用户的环境数据
S20
标注所述样本数据，得到样本数据标注集，根据所述样本数据标注集生成区分特征集
S30
根据所述区分特征集和基于高斯分布的朴素贝叶斯算法，建立分类模型
S40
根据所述分类模型，得到风险系数预测模型

图 1

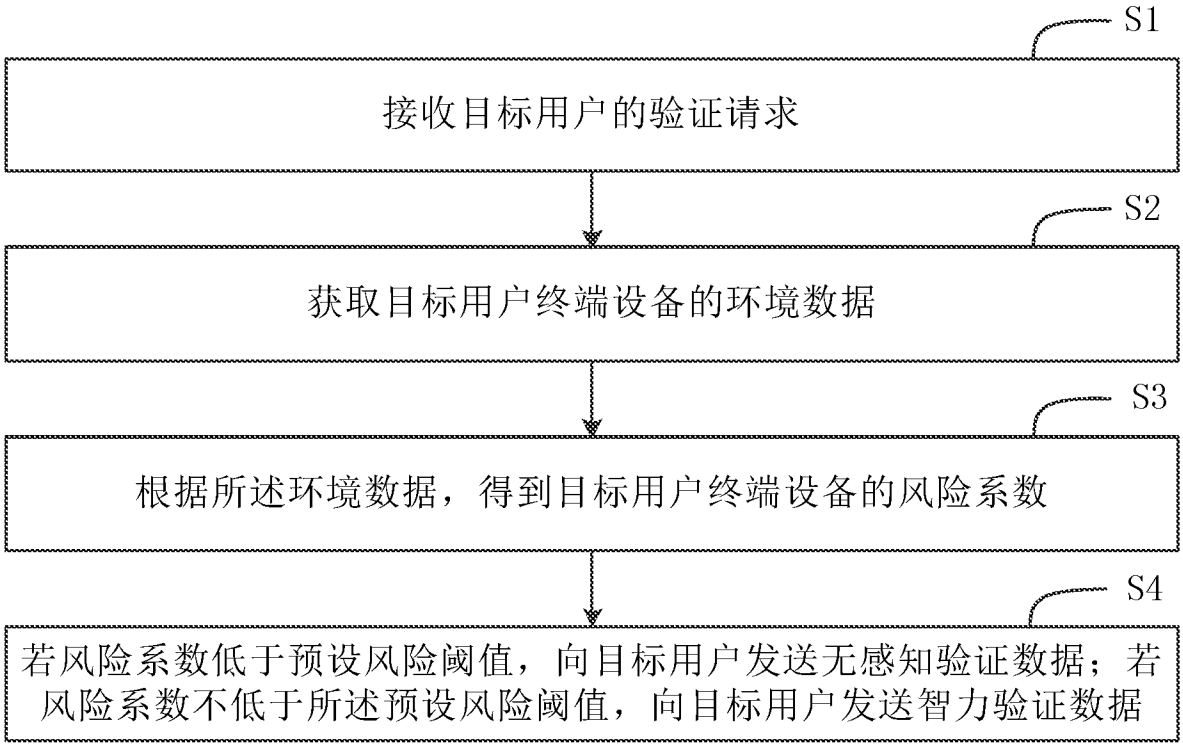
S1
接收目标用户的验证请求
S2
获取目标用户终端设备的环境数据
S3
根据所述环境数据，得到目标用户终端设备的风险系数
S4
若风险系数低于预设风险阈值，向目标用户发送无感知验证数据；若风险系数不低于所述预设风险阈值，向目标用户发送智力验证数据

图 2

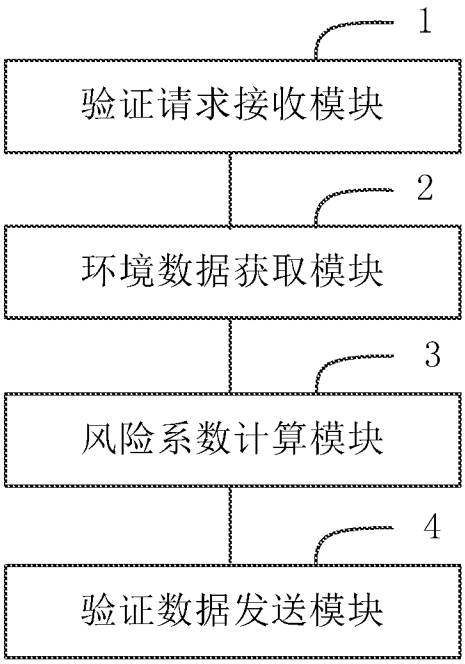
1
验证请求接收模块
2
环境数据获取模块
3
风险系数计算模块
4
验证数据发送模块

图 3

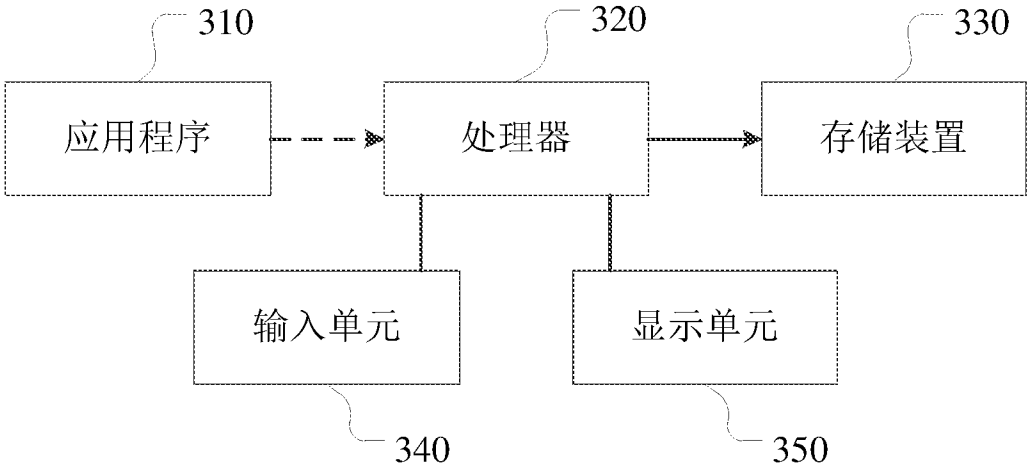
310
应用程序
320
处理器
330
存储装置
输入单元
显示单元
340
350

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/117939

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)

WPI; EPODOC; CNKI; IEEE; CNPAT: 验证, 请求, 风险, 网络, 环境, 设备信息, 阈值, 门限, 模型, authentication, verification, request, risk, network, attribute, device, threshold, model, environment

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109981567 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 05 July 2019 (2019-07-05) entire document	1-20
X	CN 107749844 A (VIVO COMMUNICATION TECHNOLOGY CO., LTD.) 02 March 2018 (2018-03-02) description, paragraphs [0024]-[0089], and figures 1 and 2	1-20
A	CN 109120629 A (NEW H3C INFORMATION SECURITY TECHNOLOGY CO., LTD.) 01 January 2019 (2019-01-01) entire document	1-20
A	CN 107256257 A (SHANGHAI CTRIP COMMERCE CO., LTD.) 17 October 2017 (2017-10-17) entire document	1-20
A	US 2018255097 A1 (ALIBABA GROUP HOLDING LTD.) 06 September 2018 (2018-09-06) 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
06 January 2020	**31 January 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
Information on patent family members

International application No.
PCT/CN2019/117939

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109981567	A	05 July 2019	None			
CN	107749844	A	02 March 2018	None			
CN	109120629	A	01 January 2019	None			
CN	107256257	A	17 October 2017	None			
US	2018255097	A1	06 September 2018	CN	106686599	A	17 May 2017
				JP	2019502192	A	24 January 2019
				SG	11201803771T	A	28 June 2018
				EP	3373626	A1	12 September 2018
				AU	2016351177	A1	14 June 2018
				SG	10201908340R	A	30 October 2019
				JP	6609047	B2	20 November 2019
				EP	3373626	A4	10 April 2019
				PH	12018500971	A1	17 December 2018
				KR	20180082504	A	18 July 2018
				WO	2017076210	A1	11 May 2017

国际检索报告

国际申请号
PCT/CN2019/117939

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））

WPI; EPODOC; CNKI; IEEE; CNPAT: 验证，请求，风险，网络，环境，设备信息，阈值，门限，模型，authentication, verification, request, risk, network, attribute, device, threshold, model, environment

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 109981567 A (平安科技深圳有限公司) 2019年 7月 5日 (2019-07-05) 全文	1-20
X	CN 107749844 A (维沃移动通信有限公司) 2018年 3月 2日 (2018-03-02) 说明书第[0024]-[0089]段，图1-2	1-20
A	CN 109120629 A (新华三信息安全技术有限公司) 2019年 1月 1日 (2019-01-01) 全文	1-20
A	CN 107256257 A (上海携程商务有限公司) 2017年 10月 17日 (2017-10-17) 全文	1-20
A	US 2018255097 A1 (ALIBABA GROUP HOLDING LTD.) 2018年 9月 6日 (2018-09-06) 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 1月 6日	2020年 1月 31日

ISA/CN的名称和邮寄地址	受权官员
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	孙国辉
传真号 (86-10)62019451	电话号码 86-10-53961753

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/117939

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	109981567	A	2019年 7月 5日	无			
CN	107749844	A	2018年 3月 2日	无			
CN	109120629	A	2019年 1月 1日	无			
CN	107256257	A	2017年 10月 17日	无			
US	2018255097	A1	2018年 9月 6日	CN	106686599	A	2017年 5月 17日
				JP	2019502192	A	2019年 1月 24日
				SG	11201803771T	A	2018年 6月 28日
				EP	3373626	A1	2018年 9月 12日
				AU	2016351177	A1	2018年 6月 14日
				SG	10201908340R	A	2019年 10月 30日
				JP	6609047	B2	2019年 11月 20日
				EP	3373626	A4	2019年 4月 10日
				PH	12018500971	A1	2018年 12月 17日
				KR	20180082504	A	2018年 7月 18日
				WO	2017076210	A1	2017年 5月 11日