(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109446789 A
(43)申请公布日 2019.03.08

(21)申请号 201811233085.2

(22)申请日 2018.10.22

(71)申请人 武汉极意网络科技有限公司
地址 430000 湖北省武汉市东湖开发区大学园路武汉大学科技园内兴业楼2单元2楼204室-020号

(72)发明人 张振宇 汪智勇

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/55(2013.01)
G06K 9/62(2006.01)

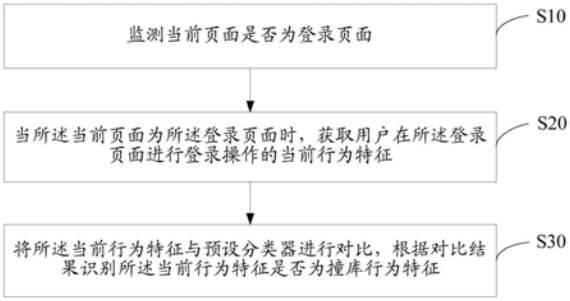
权利要求书2页 说明书11页 附图5页

(54)发明名称

基于人工智能的防撞库方法、设备、存储介质及装置

(57)摘要

本发明公开了一种基于人工智能的防撞库方法、设备、存储介质及装置，所述方法包括：监测当前页面是否为登录页面，当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征，将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。本发明中通过预设行为采集代码采集用户登录页面进行操作的行为特征数据，从所述行为特征数据中提取出当前行为特征，通过预设分类器对所述当前行为特征进行分类，从而识别出所述当前行为特征是否为撞库行为特征，能够在撞库攻击者登录成功之前识别出撞库攻击行为，有效防止撞库攻击，保障真实用户的网络安全。



CN 109446789 A

1.一种基于人工智能的防撞库方法,其特征在于,所述基于人工智能的防撞库方法包括以下步骤:

监测当前页面是否为登录页面;

当所述当前页面为所述登录页面时,获取用户在所述登录页面进行登录操作的当前行为特征;

将所述当前行为特征与预设分类器进行对比,根据对比结果识别所述当前行为特征是否为撞库行为特征。

2.如权利要求1所述的基于人工智能的防撞库方法,其特征在于,所述监测当前页面是否为登录页面之前,所述基于人工智能的防撞库方法还包括:

获取样本数据,所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性;

建立基础分类器,根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练,生成预设分类器。

3.如权利要求2所述的基于人工智能的防撞库方法,其特征在于,所述建立基础分类器,根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练,生成预设分类器,具体包括:

建立基础分类器,将所述样本行为特征输入至所述基础分类器中,以使所述基础分类器输出预测正负性;

当所述预测正负性与所述样本正负性不一致时,对所述基础分类器的参数进行调整,以生成预设分类器。

4.如权利要求1-3中任一项所述的基于人工智能的防撞库方法,其特征在于,所述当前行为特征包括:重复登录次数、登录信息的当前输入速度和鼠标光标的当前移动特征;

相应地,所述当所述当前页面为所述登录页面时,获取用户在所述登录页面进行登录操作的当前行为特征,具体包括:

当所述当前页面为所述登录页面时,检测单位时段内所述登录页面的重复登录次数;

检测用户在所述登录页面中输入登录信息时的当前输入速度;

检测鼠标光标在所述登录页面的当前移动特征。

5.如权利要求4所述的基于人工智能的防撞库方法,其特征在于,所述当前移动特征包括:鼠标光标在所述登录页面的当前移动速度、当前移动加速度和当前移动轨迹。

6.如权利要求1-3中任一项所述的基于人工智能的防撞库方法,其特征在于,所述将所述当前行为特征与预设分类器进行对比,根据对比结果识别所述当前行为特征是否为撞库行为特征之后,所述基于人工智能的防撞库方法还包括:

当所述当前行为特征为撞库行为特征时,展示预设验证码。

7.如权利要求6所述的基于人工智能的防撞库方法,其特征在于,所述当所述当前行为特征为撞库行为特征时,展示预设验证码之后,所述基于人工智能的防撞库方法还包括:

根据所述当前行为特征生成撞库风险报告;

将所述撞库风险报告发送至所述登录页面对应的目标网站,以使所述目标网站执行保护措施。

8.一种基于人工智能的防撞库设备,其特征在于,所述基于人工智能的防撞库设备包

括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于人工智能的防撞库程序,所述基于人工智能的防撞库程序被所述处理器执行时实现如权利要求1至7中任一项所述的基于人工智能的防撞库方法的步骤。

9.一种存储介质,其特征在于,所述存储介质上存储有基于人工智能的防撞库程序,所述基于人工智能的防撞库程序被处理器执行时实现如权利要求1至7中任一项所述的基于人工智能的防撞库方法的步骤。

10.一种基于人工智能的防撞库装置,其特征在于,所述基于人工智能的防撞库装置包括:

页面监测模块,用于监测当前页面是否为登录页面;

特征获取模块,用于当所述当前页面为所述登录页面时,获取用户在所述登录页面进行登录操作的当前行为特征;

行为识别模块,用于将所述当前行为特征与预设分类器进行对比,根据对比结果识别所述当前行为特征是否为撞库行为特征。

基于人工智能的防撞库方法、设备、存储介质及装置

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种基于人工智能的防撞库方法、设备、存储介质及装置。

背景技术

[0002] 随着人们越来越频繁地浏览网站，网站的登录安全与使用安全也受到了人们的关注。由于不少用户在不同网站上都会注册账号，为了方便记忆，一般这些账号与密码皆为相同，或者密码不同但存在明显规律，因此，出现一种黑客攻击网站的技术手段，撞库，即黑客通过已收集到的某网站的账号信息和密码信息去攻击其他网站，并且一般为批量登录，以达到增加攻击频次与成功率的作用。

[0003] 目前，当前网站运营者们所采用的防撞库安全措施，一般为一段时间内，若同一个IP(Internet Protocol)地址，密码错误次数超过阈值，则认为该当前登录行为是撞库行为，对该IP地址一段时间禁止登录、校验手机短信或者回答密保问题之后才能登录。然而，由于代理IP相当廉价，撞库攻击者可以购买大量代理IP进行撞库，从IP层面识别撞库行为收效甚微。因此，现有技术存在不能较好地判别撞库行为的技术问题。

[0004] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0005] 本发明的主要目的在于提供一种基于人工智能的防撞库方法、设备、存储介质及装置，旨在解决现有技术中不能较好地判别撞库行为的技术问题。

[0006] 为实现上述目的，本发明提供一种基于人工智能的防撞库方法，所述方法包括以下步骤：

[0007] 监测当前页面是否为登录页面；

[0008] 当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征；

[0009] 将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。

[0010] 优选地，所述监测当前页面是否为登录页面之前，所述基于人工智能的防撞库方法还包括：

[0011] 获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性；

[0012] 建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器。

[0013] 优选地，所述建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器，具体包括：

[0014] 建立基础分类器，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性；

[0015] 当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。

[0016] 优选地，所述当前行为特征包括：重复登录次数、登录信息的当前输入速度和鼠标光标的当前移动特征；

[0017] 相应地，所述当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征，具体包括：

[0018] 当所述当前页面为所述登录页面时，检测单位时段内所述登录页面的重复登录次数；

[0019] 检测用户在所述登录页面中输入登录信息时的当前输入速度；

[0020] 检测鼠标光标在所述登录页面的当前移动特征。

[0021] 优选地，所述当前移动特征包括：鼠标光标在所述登录页面的当前移动速度、当前移动加速度和当前移动轨迹。

[0022] 优选地，所述将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征之后，所述基于人工智能的防撞库方法还包括：

[0023] 当所述当前行为特征为撞库行为特征时，展示预设验证码。

[0024] 优选地，所述当所述当前行为特征为撞库行为特征时，展示预设验证码之后，所述基于人工智能的防撞库方法还包括：

[0025] 根据所述当前行为特征生成撞库风险报告；

[0026] 将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施。

[0027] 此外，为实现上述目的，本发明还提供一种基于人工智能的防撞库设备，所述基于人工智能的防撞库设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于人工智能的防撞库程序，所述基于人工智能的防撞库程序被所述处理器执行时实现如上文所述基于人工智能的防撞库方法的步骤。

[0028] 此外，为实现上述目的，本发明还提供一种存储介质，所述存储介质上存储有基于人工智能的防撞库程序，所述基于人工智能的防撞库程序被处理器执行时实现如上文所述基于人工智能的防撞库方法的步骤。

[0029] 此外，为实现上述目的，本发明还提供一种基于人工智能的防撞库装置，所述基于人工智能的防撞库装置包括：

[0030] 页面监测模块，用于监测当前页面是否为登录页面；

[0031] 特征获取模块，用于当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征；

[0032] 行为识别模块，用于将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。

[0033] 在本发明中，通过监测当前页面是否为登录页面，当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征，将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。由于通过

预设行为采集代码采集用户登录页面进行操作的行为特征数据，从所述行为特征数据中提取出当前行为特征，通过预设分类器对所述当前行为特征进行分类，从而识别出所述当前行为特征是否为撞库行为特征，能够在撞库攻击者登录成功之前识别出撞库攻击行为，有效防止撞库攻击，保障真实用户的网络安全。

附图说明

[0034] 图1是本发明实施例方案涉及的硬件运行环境的基于人工智能的防撞库设备结构示意图；

[0035] 图2为本发明基于人工智能的防撞库方法第一实施例的流程示意图；

[0036] 图3为本发明基于人工智能的防撞库方法第二实施例的流程示意图；

[0037] 图4为本发明基于人工智能的防撞库方法第三实施例的流程示意图；

[0038] 图5为本发明基于人工智能的防撞库方法第四实施例的流程示意图；

[0039] 图6为本发明基于人工智能的防撞库装置第一实施例的功能模块图。

[0040] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0041] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0042] 参照图1，图1为本发明实施例方案涉及的硬件运行环境的基于人工智能的防撞库设备结构示意图。

[0043] 如图1所示，所述基于人工智能的防撞库设备可以包括：处理器1001，例如CPU，通信总线1002、用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0044] 本领域技术人员可以理解，图1中示出的结构并不构成对所述基于人工智能的防撞库设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0045] 如图1所示，作为一种存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及基于人工智能的防撞库程序。

[0046] 在图1所示的基于人工智能的防撞库设备中，网络接口1004主要用于连接后台服务器，与所述后台服务器进行数据通信；用户接口1003主要用于连接外设；所述基于人工智能的防撞库设备通过处理器1001调用存储器1005中存储的基于人工智能的防撞库程序，并执行本发明实施例提供的基于人工智能的防撞库方法。

[0047] 所述基于人工智能的防撞库设备通过处理器1001调用存储器1005中存储的基于人工智能的防撞库程序，并执行以下操作：

[0048] 监测当前页面是否为登录页面；

[0049] 当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当

前行为特征；

[0050] 将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。

[0051] 进一步地，处理器1001可以调用存储器1005中存储的基于人工智能的防撞库程序，还执行以下操作：

[0052] 获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性；

[0053] 建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器。

[0054] 进一步地，处理器1001可以调用存储器1005中存储的基于人工智能的防撞库程序，还执行以下操作：

[0055] 建立基础分类器，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性；

[0056] 当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。

[0057] 进一步地，处理器1001可以调用存储器1005中存储的基于人工智能的防撞库程序，还执行以下操作：

[0058] 当所述当前页面为所述登录页面时，检测单位时段内所述登录页面的重复登录次数；

[0059] 检测用户在所述登录页面中输入登录信息时的当前输入速度；

[0060] 检测鼠标光标在所述登录页面的当前移动特征。

[0061] 进一步地，处理器1001可以调用存储器1005中存储的基于人工智能的防撞库程序，还执行以下操作：

[0062] 当所述当前行为特征为撞库行为特征时，展示预设验证码。

[0063] 进一步地，处理器1001可以调用存储器1005中存储的基于人工智能的防撞库程序，还执行以下操作：

[0064] 根据所述当前行为特征生成撞库风险报告；

[0065] 将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施。

[0066] 在本实施例中，通过监测当前页面是否为登录页面，当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征，将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。由于通过预设行为采集代码采集用户登录页面进行操作的行为特征数据，从所述行为特征数据中提取出当前行为特征，通过预设分类器对所述当前行为特征进行分类，从而识别出所述当前行为特征是否为撞库行为特征，能够在撞库攻击者登录成功之前识别出撞库攻击行为，有效防止撞库攻击，保障真实用户的网络安全。

[0067] 基于上述硬件结构，提出本发明基于人工智能的防撞库方法的实施例。

[0068] 参照图2，图2为本发明基于人工智能的防撞库方法第一实施例的流程示意图。

[0069] 在第一实施例中，所述基于人工智能的防撞库方法包括以下步骤：

[0070] 步骤S10:监测当前页面是否为登录页面。

[0071] 需要说明的是,本实施例的执行主体是基于人工智能的防撞库设备,所述基于人工智能的防撞库设备可以是个人电脑、服务器等电子设备,本实施例对此不加以限制。本实施例的应用场景是,当用户在登录页面进行登录时,通过采集当前行为特征,并基于预设分类器对该当前行为特征进行分类,以判断发起该当前行为特征的用户是真实用户还是撞库攻击者,从而在用户为撞库攻击者时采取防御措施。

[0072] 可以理解的是,为了采集用户在登录页面进行操作的当前行为特征,将预先监测当前页面是否为登录页面,当且仅当所述当前页面为登录页面时,对当前行为特征进行采集。

[0073] 步骤S20:当所述当前页面为所述登录页面时,获取用户在所述登录页面进行登录操作的当前行为特征。

[0074] 可以理解的是,所述登录页面中嵌有预设行为采集代码,用于对登录页面的行为特征数据进行采集,通过获取所述预设行为采集代码采集的行为特征数据,从所述行为特征数据中提取出当前行为特征,以实现通过所述当前行为特征判断所述用户是否为撞库攻击者。

[0075] 在具体实现中,通过行间事件的方式将所述预设行为采集代码嵌入所述登录页面中,具体嵌入方式为:<input type＝"button"name＝""onclick＝"alert('预设行为采集代码');">,当所述登录页面嵌入所述预设行为采集代码后,所述预设行为采集代码将采集用户在所述登录页面进行操作时的点击事件(onclick)、鼠标移入事件(mouseover)以及鼠标移出事件(mouseout)等。

[0076] 步骤S30:将所述当前行为特征与预设分类器进行对比,根据对比结果识别所述当前行为特征是否为撞库行为特征。

[0077] 需要说明的是,在已有样本数据的基础上构造出分类模型,即分类器(Classifier),该分类器能够把数据库中的数据纪录映射到给定类别中的某一个,从而可以应用于数据预测。本实施例中的预设分类器采用支持向量机(Support Vector Machine,SVM)算法构建,是一种二分类的分类器,主要用于将行为特征分类为正常登录行为特征和撞库行为特征。

[0078] 在具体实现中,将所述当前行为特征与预设分类器进行对比,即将所述当前行为特征输入至所述预设分类器中,以使所述预设分类器对所述当前行为特征的所属类别进行预测,输出分类结果,从而识别所述当前行为特征是否为撞库行为特征,以在所述当前行为特征为撞库行为特征时采取防御措施。

[0079] 在本实施例中,通过监测当前页面是否为登录页面,当所述当前页面为所述登录页面时,获取用户在所述登录页面进行登录操作的当前行为特征,将所述当前行为特征与预设分类器进行对比,根据对比结果识别所述当前行为特征是否为撞库行为特征。由于通过预设行为采集代码采集用户登录页面进行操作的行为特征数据,从所述行为特征数据中提取出当前行为特征,通过预设分类器对所述当前行为特征进行分类,从而识别出所述当前行为特征是否为撞库行为特征,能够在撞库攻击者登录成功之前识别出撞库攻击行为,有效防止撞库攻击,保障真实用户的网络安全。

[0080] 参照图3,图3为本发明基于人工智能的防撞库方法第二实施例的流程示意图,基

于上述图2所示的实施例，提出本发明基于人工智能的防撞库方法的第二实施例。

[0081] 在第二实施例中，所述步骤S10之前，所述基于人工智能的防撞库方法还包括：

[0082] 步骤S01：获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性。

[0083] 需要说明的是，所述样本数据用于构建所述预设分类器，而所述预设分类器用于将行为特征分类为正常登录行为特征和撞库行为特征，因此，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性，也即所述样本数据包含正样本行为特征和负样本行为特征，所述正样本行为特征为正常登录行为特征，所述负样本行为特征为撞库登录行为特征。

[0084] 步骤S02：建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器。

[0085] 可以理解的是，所述基础分类器为基于支持向量机算法构建的分类器，通过所述正样本行为特征和所述负样本行为特征对所述基础分类器进行训练并测试，在所述基础分类器的预测准确率达到阈值时，将其作为预设分类器。

[0086] 进一步地，所述步骤S02，具体包括：

[0087] 建立基础分类器，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性；

[0088] 当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。

[0089] 需要说明的是，通过所述样本行为特征对所述基础分类器进行训练的具体过程为，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性，当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。

[0090] 在具体实现中，将所述正样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性，当所述预测正负性为正时，所述基础分类器将输出“1”，判定所述基础分类器预测正确，正向调整所述基础分类器的参数；当所述预测正负性为负时，所述基础分类器将输出“-1”，判定所述基础分类器预测错误，反向调整所述基础分类器的参数。将所述负样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性，当所述预测正负性为正时，所述基础分类器将输出“1”，判定所述基础分类器预测错误，反向调整所述基础分类器的参数；当所述预测正负性为负时，所述基础分类器将输出“-1”，判定所述基础分类器预测正确，正向调整所述基础分类器的参数。从而通过大量正样本行为特征和负样本行为特征对所述基础分类器进行训练，逐步调整基础分类器的参数，在所述基础分类器的预测准确率达到阈值时，将其作为预设分类器。

[0091] 在本实施例中，通过获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性；建立基础分类器，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性；当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。由于采集了大量正负样本，提高了所述预设分类器的预测准确率，从而提高对所述当前行为特征识别的准确率。

[0092] 参照图4，图4为本发明基于人工智能的防撞库方法第三实施例的流程示意图，基

于上述图3所示的实施例，提出本发明基于人工智能的防撞库方法的第三实施例。

[0093] 在第三实施例中，所述当前行为特征包括：重复登录次数、登录信息的当前输入速度和鼠标光标的当前移动特征。

[0094] 相应地，所述步骤S20，具体包括：

[0095] 步骤S201：当所述当前页面为所述登录页面时，检测单位时段内所述登录页面的重复登录次数。

[0096] 需要说明的是，当所述当前页面为所述登录页面时，将通过所述预设行为采集代码采集用户在所述登录页面进行操作时的当前行为特征，以通过所述预设分类器识别所述当前行为特征是否为撞库行为特征，其中，所述当前行为特征包括重复登录次数，由于真实用户的登录次数远远低于撞库的登录次数，因此，将重复登录次数作为识别行为特征是否为撞库行为特征的特征之一，以实现区分真实用户行为特征和撞库行为特征。在本实施例中，对所述单位时段的时长进行预设，可以是5分钟，也可以是其它时长，本实施例对此不加以限制。当所述当前页面为所述登录页面时，检测单位时段内用户在所述登录页面的重复登录次数。

[0097] 步骤S202：检测用户在所述登录页面中输入登录信息时的当前输入速度。

[0098] 可以理解的是，所述当前行为特征还包括当前输入速度，由于真实用户的输入速度一般低于撞库的输入速度，因此，将输入速度作为识别行为特征是否为撞库行为特征的特征之一，以实现区分真实用户行为特征和撞库行为特征。

[0099] 步骤S203：检测鼠标光标在所述登录页面的当前移动特征。

[0100] 需要说明的是，所述当前行为特征还包括当前移动特征，由于真实用户与撞库用户移动鼠标光标的方式具有较大的差异，真实用户的移动较为缓慢和杂乱，而撞库的鼠标移动较为快速和有序，因此，将鼠标光标的移动特征作为识别行为特征是否为撞库行为特征的特征之一，以实现区分真实用户行为特征和撞库行为特征。

[0101] 进一步地，所述当前移动特征包括：鼠标光标在所述登录页面的当前移动速度、当前移动加速度和当前移动轨迹。

[0102] 可以理解的是，由于真实用户的移动较为缓慢和杂乱，而撞库的鼠标移动较为快速和有序，因此，将鼠标光标在所述登录页面的当前移动速度、当前移动加速度和当前移动轨迹作为所述当前移动特征，以提高区分真实用户行为特征和撞库行为特征的准确性。

[0103] 在本实施例中，通过将重复登录次数、登录信息的当前输入速度和鼠标光标的当前移动特征等特征作为当前行为特征，以实现区分真实用户行为特征和撞库行为特征，并将重复登录次数、登录信息的输入速度和鼠标光标的移动特征等特征作为样本行为特征进行分类器的训练，以提高预设分类器的识别准确率。

[0104] 参照图5，图5为本发明基于人工智能的防撞库方法第四实施例的流程示意图，基于上述图3所示的实施例，提出本发明基于人工智能的防撞库方法的第四实施例。

[0105] 在第四实施例中，所述当前行为特征包括：重复登录次数、登录信息的当前输入速度和鼠标光标的当前移动特征。

[0106] 相应地，所述步骤S30之后，所述基于人工智能的防撞库方法还包括：

[0107] 步骤S40：当所述当前行为特征为撞库行为特征时，展示预设验证码。

[0108] 需要说明的是，当所述当前行为特征为撞库行为特征时，将采取防御措施阻止撞

库攻击者登录所述登录页面对应的目标网站，在本实施例中，将展示预设验证码，所述预设验证码为图形验证码或者滑动验证码等，具有较高难度，撞库攻击者难以通过机器直接进行验证。

[0109] 步骤S50：根据所述当前行为特征生成撞库风险报告。

[0110] 步骤S60：将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施。

[0111] 可以理解的是，在展示预设验证码之后，为提高防御效果，所述防御措施还包括根据所述当前行为特征生成撞库风险报告，并将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施，制止所述撞库攻击者的当前登录行为。

[0112] 在本实施例中，通过当所述当前行为特征为撞库行为特征时，展示预设验证码；根据所述当前行为特征生成撞库风险报告；将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施。由于在所述当前行为特征为撞库行为特征时，展示预设验证码和生成撞库风险报告，可以实时的阻止撞库攻击者登录所述目标网站，并通过目标网站进行后续的防御，提高所述目标网站的防御力度。

[0113] 此外，本发明实施例还提出一种存储介质，所述存储介质上存储有基于人工智能的防撞库程序，所述基于人工智能的防撞库程序被处理器执行时实现如下操作：

[0114] 监测当前页面是否为登录页面；

[0115] 当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征；

[0116] 将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。

[0117] 进一步地，所述基于人工智能的防撞库程序被处理器执行时还实现如下操作：

[0118] 获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性；

[0119] 建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器。

[0120] 进一步地，所述基于人工智能的防撞库程序被处理器执行时还实现如下操作：

[0121] 建立基础分类器，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性；

[0122] 当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。

[0123] 进一步地，所述基于人工智能的防撞库程序被处理器执行时还实现如下操作：

[0124] 当所述当前页面为所述登录页面时，检测单位时段内所述登录页面的重复登录次数；

[0125] 检测用户在所述登录页面中输入登录信息时的当前输入速度；

[0126] 检测鼠标光标在所述登录页面的当前移动特征。

[0127] 进一步地，所述基于人工智能的防撞库程序被处理器执行时还实现如下操作：

[0128] 当所述当前行为特征为撞库行为特征时，展示预设验证码。

[0129] 进一步地，所述基于人工智能的防撞库程序被处理器执行时还实现如下操作：

[0130] 根据所述当前行为特征生成撞库风险报告；

[0131] 将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施。

[0132] 在本实施例中，通过监测当前页面是否为登录页面，当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征，将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。由于通过预设行为采集代码采集用户登录页面进行操作的行为特征数据，从所述行为特征数据中提取出当前行为特征，通过预设分类器对所述当前行为特征进行分类，从而识别出所述当前行为特征是否为撞库行为特征，能够在撞库攻击者登录成功之前识别出撞库攻击行为，有效防止撞库攻击，保障真实用户的网络安全。

[0133] 参照图6，图6为本发明基于人工智能的防撞库装置第一实施例的功能模块图，基于所述基于人工智能的防撞库方法，提出本发明基于人工智能的防撞库装置的第一实施例。

[0134] 在本实施例中，所述基于人工智能的防撞库装置包括：

[0135] 页面监测模块10，用于监测当前页面是否为登录页面。

[0136] 需要说明的是，本实施例的应用场景是，当用户在登录页面进行登录时，通过采集当前行为特征，并基于预设分类器对该当前行为特征进行分类，以判断发起该当前行为特征的用户是真实用户还是撞库攻击者，从而在用户为撞库攻击者时采取防御措施。

[0137] 可以理解的是，为了采集用户在登录页面进行操作的当前行为特征，将预先监测当前页面是否为登录页面，当且仅当所述当前页面为登录页面时，对当前行为特征进行采集。

[0138] 特征获取模块20，用于当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征。

[0139] 可以理解的是，所述登录页面中嵌有预设行为采集代码，用于对登录页面的行为特征数据进行采集，通过获取所述预设行为采集代码采集的行为特征数据，从所述行为特征数据中提取出当前行为特征，以实现通过所述当前行为特征判断所述用户是否为撞库攻击者。

[0140] 在具体实现中，通过行间事件的方式将所述预设行为采集代码嵌入所述登录页面中，具体嵌入方式为：<input type＝"button"name＝""onclick＝"alert('预设行为采集代码');">，当所述登录页面嵌入所述预设行为采集代码后，所述预设行为采集代码将采集用户在所述登录页面进行操作时的点击事件(onclick)、鼠标移入事件(mouseover)以及鼠标移出事件(mouseout)等。

[0141] 行为识别模块30，用于将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。

[0142] 需要说明的是，在已有样本数据的基础上构造出分类模型，即分类器(Classifier)，该分类器能够把数据库中的数据纪录映射到给定类别中的某一个，从而可以应用于数据预测。本实施例中的预设分类器采用支持向量机(Support Vector Machine，SVM)算法构建，是一种二分类的分类器，主要用于将行为特征分类为正常登录行为特征和撞库行为特征。

[0143] 在具体实现中，将所述当前行为特征与预设分类器进行对比，即将所述当前行为特征输入至所述预设分类器中，以使所述预设分类器对所述当前行为特征的所属类别进行预测，输出分类结果，从而识别所述当前行为特征是否为撞库行为特征，以在所述当前行为特征为撞库行为特征时采取防御措施。

[0144] 在本实施例中，通过监测当前页面是否为登录页面，当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征，将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征。由于通过预设行为采集代码采集用户登录页面进行操作的行为特征数据，从所述行为特征数据中提取出当前行为特征，通过预设分类器对所述当前行为特征进行分类，从而识别出所述当前行为特征是否为撞库行为特征，能够在撞库攻击者登录成功之前识别出撞库攻击行为，有效防止撞库攻击，保障真实用户的网络安全。

[0145] 在一实施例中，所述基于人工智能的防撞库装置还包括：

[0146] 样本采集模块，用于获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性。

[0147] 模型建立模块，用于建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器。

[0148] 在一实施例中，所述模型建立模块，还用于建立基础分类器，将所述样本行为特征输入至所述基础分类器中，以使所述基础分类器输出预测正负性；

[0149] 当所述预测正负性与所述样本正负性不一致时，对所述基础分类器的参数进行调整，以生成预设分类器。

[0150] 在一实施例中，所述当前行为特征包括：重复登录次数、登录信息的当前输入速度和鼠标光标的当前移动特征；

[0151] 相应地，所述特征获取模块20，还用于当所述当前页面为所述登录页面时，检测单位时段内所述登录页面的重复登录次数；

[0152] 检测用户在所述登录页面中输入登录信息时的当前输入速度；

[0153] 检测鼠标光标在所述登录页面的当前移动特征。

[0154] 在一实施例中，所述当前移动特征包括：鼠标光标在所述登录页面的当前移动速度、当前移动加速度和当前移动轨迹。

[0155] 在一实施例中，所述基于人工智能的防撞库装置还包括：

[0156] 验证防御模块，用于当所述当前行为特征为撞库行为特征时，展示预设验证码。

[0157] 在一实施例中，所述基于人工智能的防撞库装置还包括：

[0158] 风险防御模块，用于根据所述当前行为特征生成撞库风险报告；

[0159] 将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施。

[0160] 本发明所述基于人工智能的防撞库装置的其他实施例或具体实现方式可参照上述各方法实施例，此处不再赘述。

[0161] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有

的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0162] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0163] 单词第一、第二、以及第三等的使用不表示任何顺序，可将这些单词解释为名称。

[0164] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0165] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

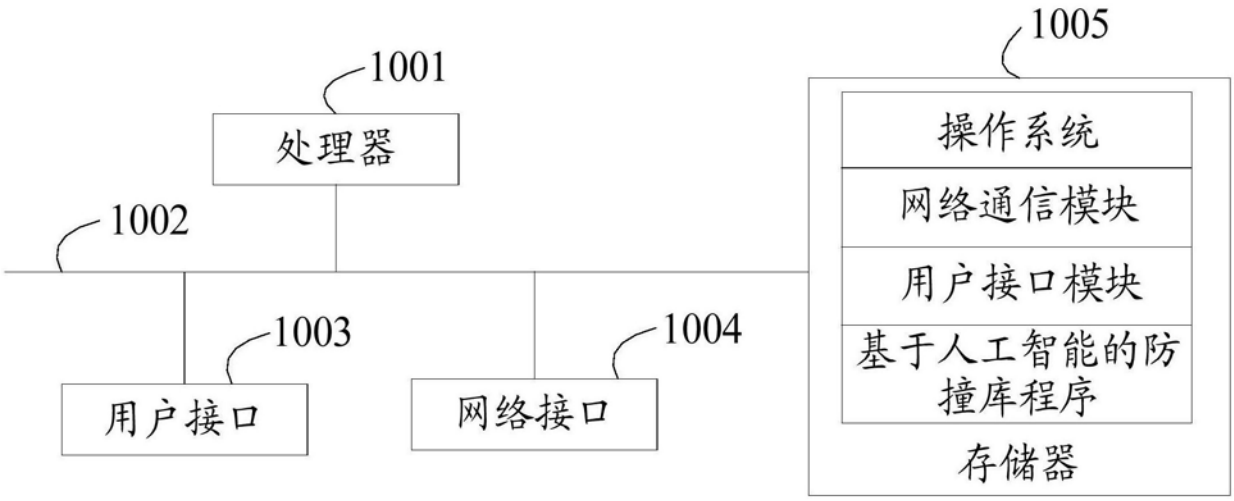

1005
1001
处理器
操作系统
网络通信模块
用户接口模块
1002
基于人工智能的防撞库程序
1003
1004
用户接口
网络接口
存储器

图1

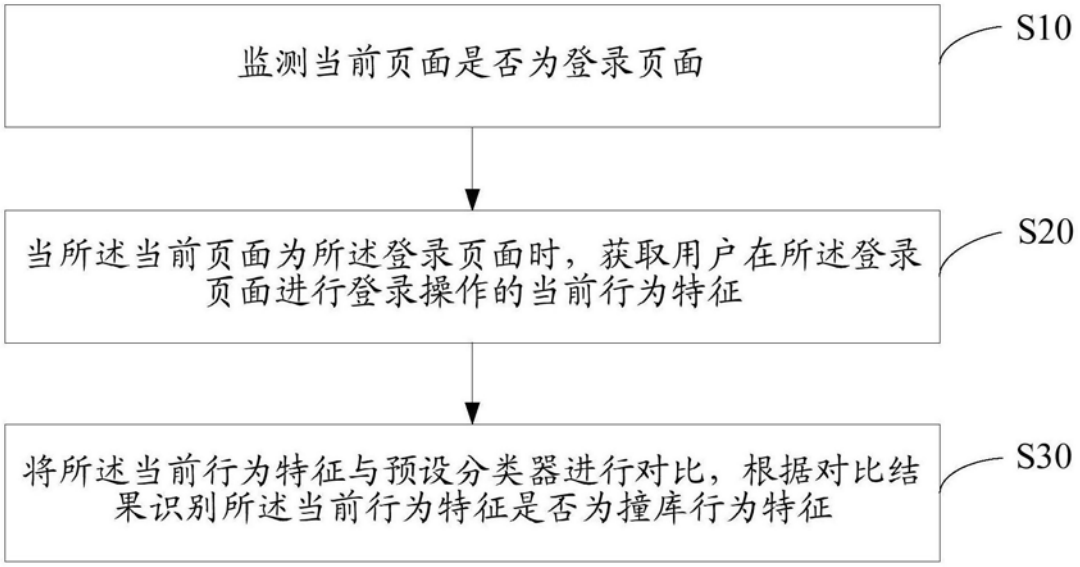

监测当前页面是否为登录页面
S10
当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征
S20
将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征
S30

图2

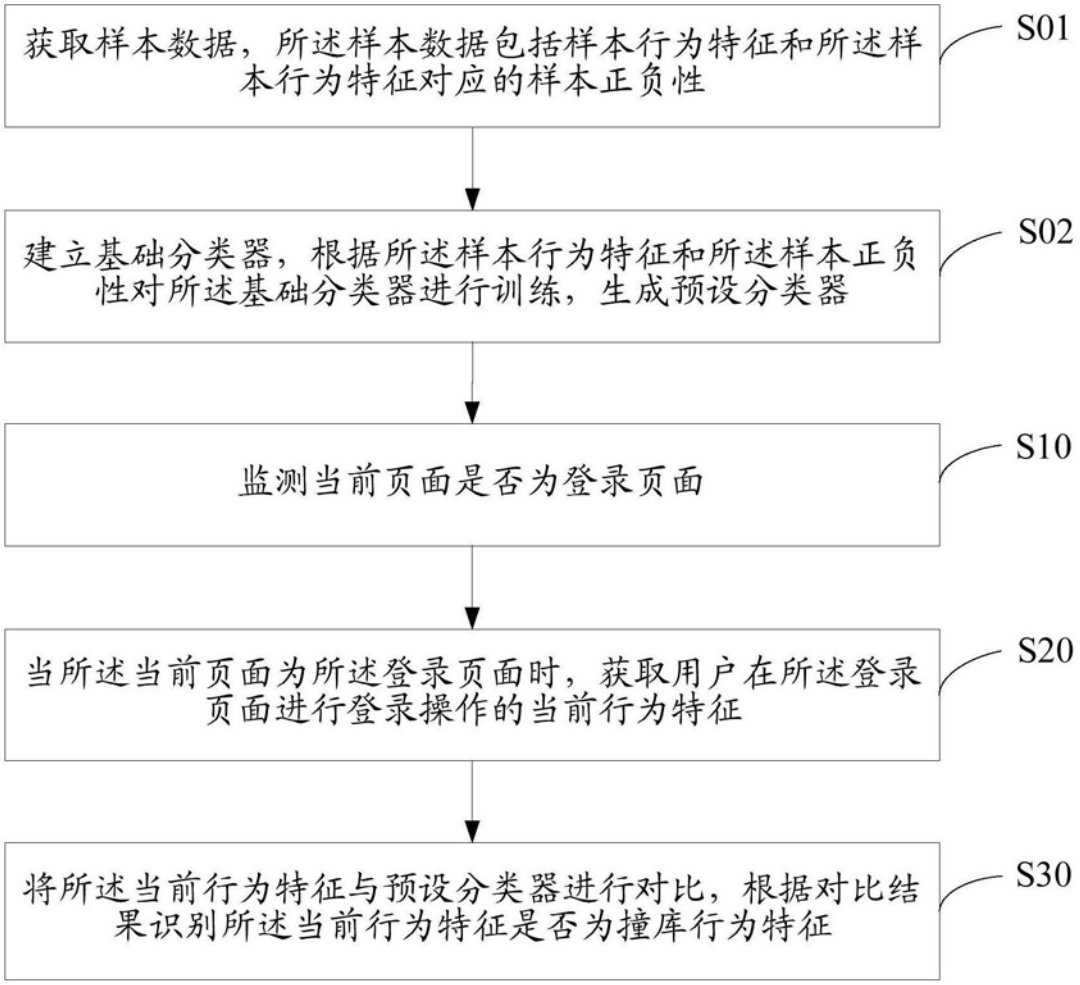

获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性
S01
建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器
S02
监测当前页面是否为登录页面
S10
当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征
S20
将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征
S30

图3

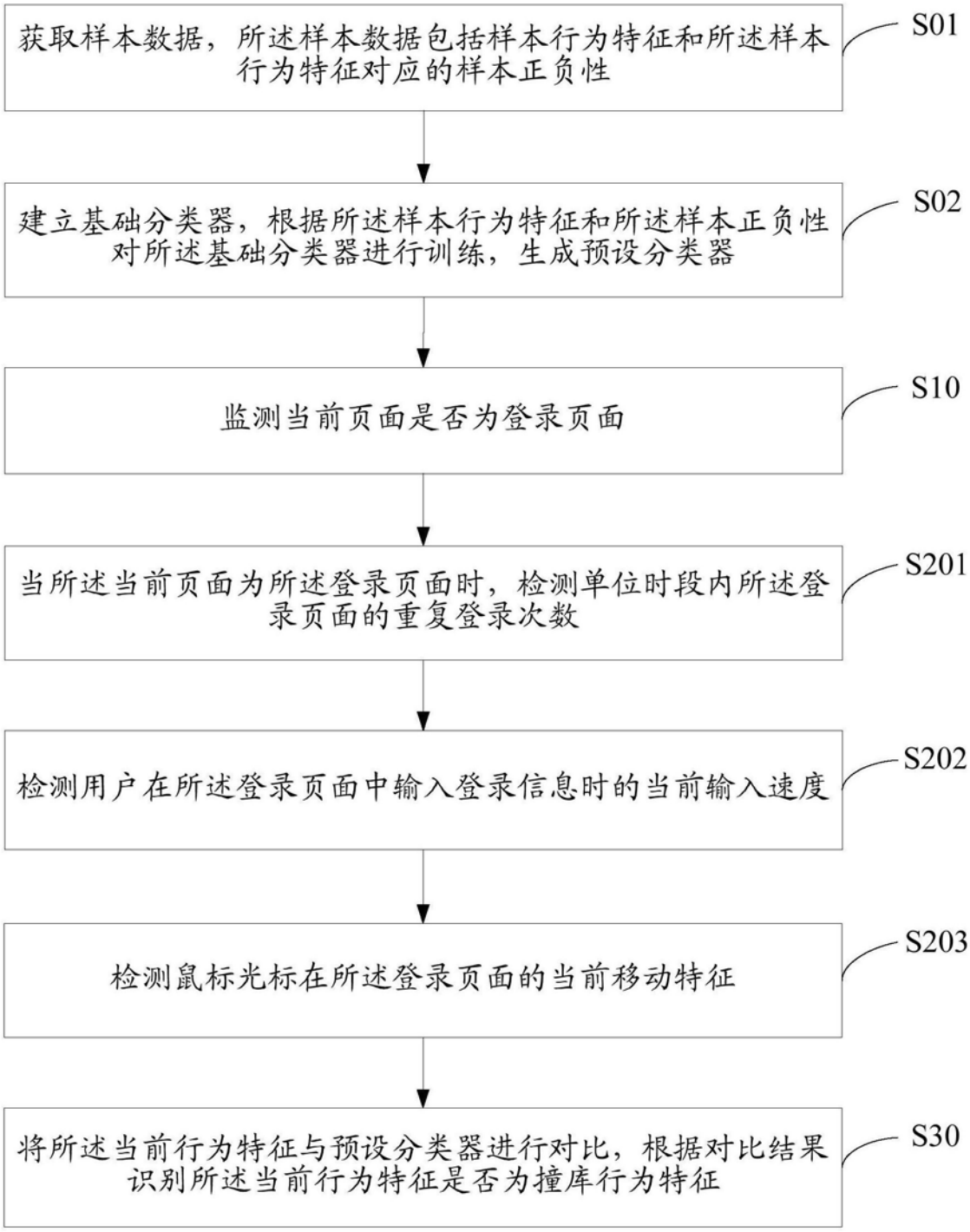

获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性
S01
建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器
S02
监测当前页面是否为登录页面
S10
当所述当前页面为所述登录页面时，检测单位时段内所述登录页面的重复登录次数
S201
检测用户在所述登录页面中输入登录信息时的当前输入速度
S202
检测鼠标光标在所述登录页面的当前移动特征
S203
将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征
S30

图4

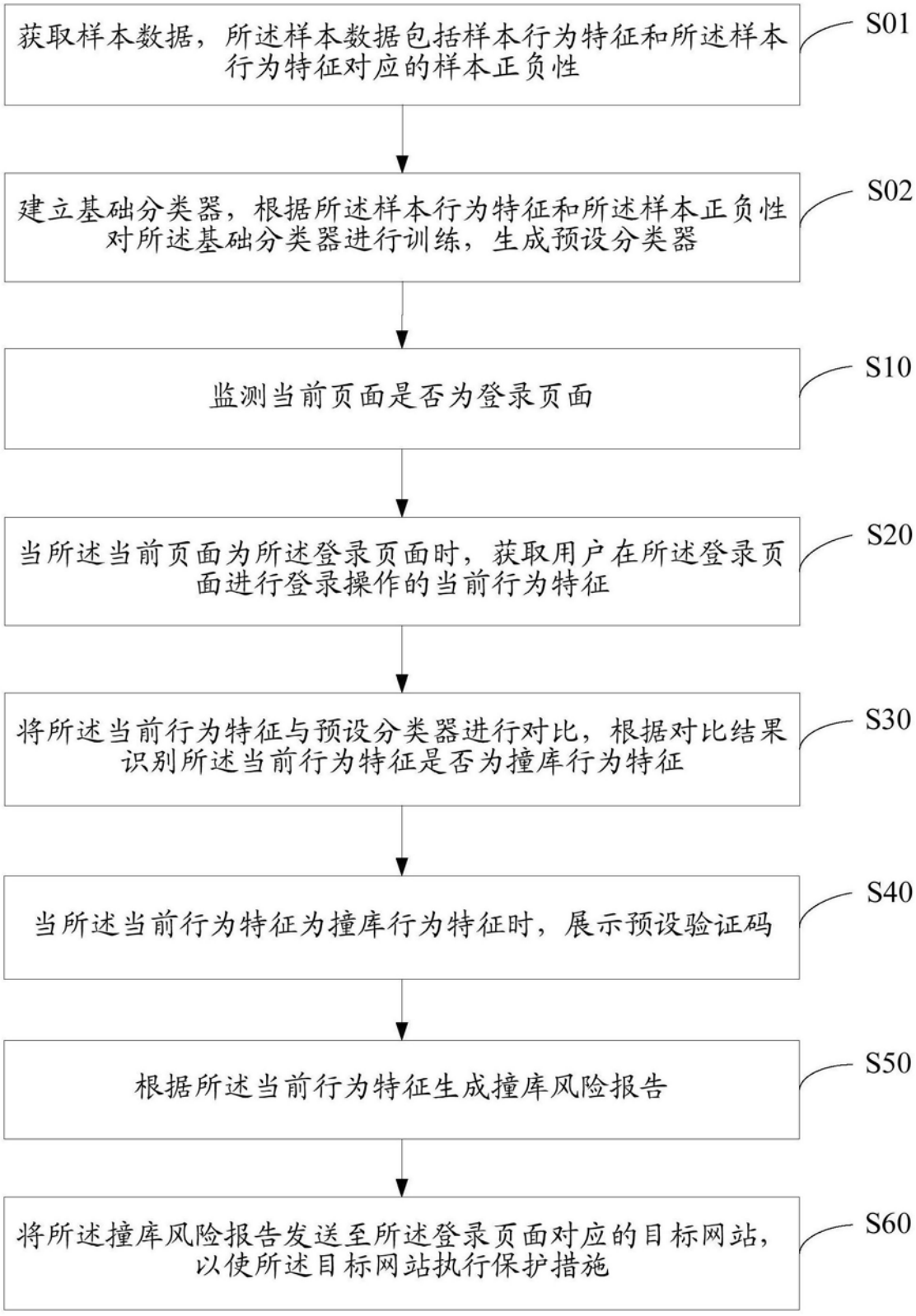

获取样本数据，所述样本数据包括样本行为特征和所述样本行为特征对应的样本正负性
S01
建立基础分类器，根据所述样本行为特征和所述样本正负性对所述基础分类器进行训练，生成预设分类器
S02
监测当前页面是否为登录页面
S10
当所述当前页面为所述登录页面时，获取用户在所述登录页面进行登录操作的当前行为特征
S20
将所述当前行为特征与预设分类器进行对比，根据对比结果识别所述当前行为特征是否为撞库行为特征
S30
当所述当前行为特征为撞库行为特征时，展示预设验证码
S40
根据所述当前行为特征生成撞库风险报告
S50
将所述撞库风险报告发送至所述登录页面对应的目标网站，以使所述目标网站执行保护措施
S60

图5

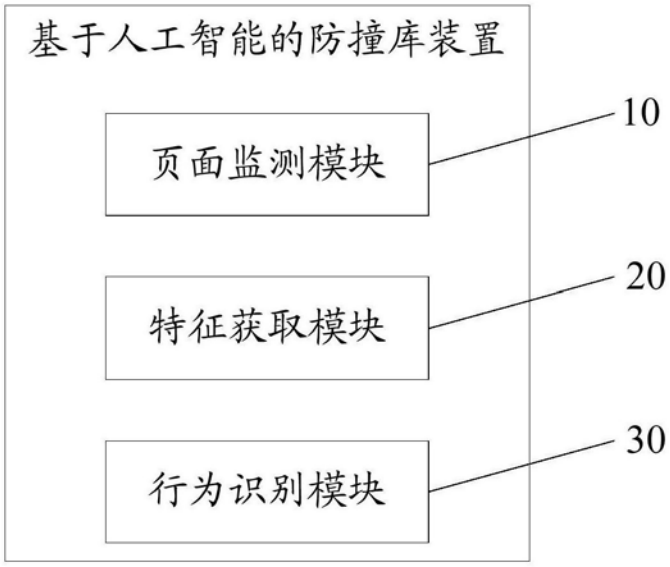


图6