说　明　书

风控方法、设备及存储介质

技术领域

本说明书涉及互联网技术领域，尤其涉及一种风控方法、设备及存储介质。

背景技术

随着互联网技术的快速发展，越来越多的人们通过服务平台享受更便捷的服务。一些不法分子通过钓鱼邮件（不法分子伪装成被人们信任的个人或者机构，向服务平台的合法使用者发送含有恶意链接或者附件的电子邮件，诱使合法使用者泄露信息，例如账户、密码等）等非法手段盗用服务平台的合法使用者的账户，并通过盗用的账户进行一些违法活动。这对服务平台和服务平台的合法使用者带来一定的风险。因此如何防控被盗账户带来的风险是服务平台在风控过程中亟需解决的问题。

背景技术部分的内容仅仅是发明人个人所知晓的信息，并不代表上述信息在本公开申请日之前已经进入公共领域，也不代表其可以成为本公开的现有技术。

发明内容

本说明书提供一种风控方法、设备及存储介质，能够准确识别被盗账户，并对被盗账户发起的事件进行风险防控，并且，还能增加不法分子绕过风控策略的难度和成本，提升风控的有效性。

第一方面，本说明书提供一种风控方法，包括：响应于检测到目标账户触发或者即将触发目标事件，获得所述目标账户对应的用户行为数据，所述用户行为数据表征所述目标账户的当前使用者在发起所述目标事件之前的历史时段内通过交互页面执行的行为序列；基于所述用户行为数据确定所述目标账户为被盗账户的概率；以及基于所述概率确定所述目标事件的风险识别结果。

第二方面，本说明书还提供一种电子设备，包括：至少一个存储介质，存储有至少一个指令集，用于风控；以及至少一个处理器，同所述至少一个存储介质通信连接，其中，所述至少一个处理器运行时读取所述至少一个指令集，并且根据所述至少一个

指令集的指示：响应于检测到目标账户触发或者即将触发目标事件，获得所述目标账户对应的用户行为数据，所述用户行为数据表征所述目标账户的当前使用者在发起所述目标事件之前的历史时段内通过交互页面执行的行为序列，基于所述用户行为数据确定所述目标账户为被盗账户的概率，以及基于所述概率确定所述目标事件的风险识别结果。

第三方面，本说明书提供一种计算机可读非暂时性存储介质，其中，所述计算机可读非暂时性存储介质中存储有至少一个指令集，所述至少一个指令集被至少一个处理器执行时，实现如第一方面所述的风控方法。

本说明书提供的风控方法、设备及存储介质的其他功能将在以下说明中部分列出。本说明书提供的风控方法、设备及存储介质的创造性方面可以通过实践或使用下面详细示例中所述的方法、装置和组合得到充分解释。

附图说明

为了更清楚地说明本说明书实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 示出了根据本说明书的实施例提供的风控应用场景的示意图；

图 2 示出了根据本说明书的实施例提供的一种电子设备的硬件结构图；

图 3 示出了根据本说明书的实施例提供的一种风控方法的流程图；

图 4 示出了根据本说明书的实施例提供的目标模型的训练方法的流程图；

图 5 示出了根据本说明书的实施例提供的风控方法的一执行方式的示意图；

图 6 示出了根据本说明书的实施例提供的风控方法的另一执行方式的示意图；

图 7 示出了根据本说明书的实施例提供的风控方法的又一执行方式的示意图；以及

图 8 示出了根据本说明书的实施例提供的确定最终风险识别结果的示意图。

具体实施方式

以下描述提供了本说明书的特定应用场景和要求，目的是使本领域技术人员能够制造和使用本说明书中的内容。对于本领域技术人员来说，对所公开的实施例的各种局部修改是显而易见的，并且在不脱离本说明书的精神和范围的情况下，可以将这里定义的一般原理应用于其他实施例和应用。因此，本说明书不限于所示的实施例，而是与权利要求一致的最宽范围。

这里使用的术语仅用于描述特定示例实施例的目的，而不是限制性的。比如，除非上下文另有明确说明，这里所使用的，单数形式“一”，“一个”和“该”也可以包括复数形式。当在本说明书中使用时，术语“包括”、“包含”和/或“含有”意思是指所关联的整数，步骤、操作、元素和/或组件存在，但不排除一个或多个其他特征、整数、步骤、操作、元素、组件和/或组的存在或在该系统/方法中可以添加其他特征、整数、步骤、操作、元素、组件和/或组。

考虑到以下描述，本说明书的这些特征和其他特征、以及结构的相关元件的操作和功能、以及部件的组合和制造的经济性可以得到明显提高。参考附图，所有这些形成本说明书的一部分。然而，应该清楚地理解，附图仅用于说明和描述的目的，并不旨在限制本说明书的范围。还应理解，附图未按比例绘制。

本说明书中使用的流程图示出了根据本说明书中的一些实施例的系统实现的操作。应该清楚地理解，流程图的操作可以不按顺序实现。相反，操作可以以反转顺序或同时实现。此外，可以向流程图添加一个或多个其他操作。可以从流程图中移除一个或多个操作。

通常情况下，在目标账户发起目标事件时，服务平台可以获得目标事件的事件信息，并基于事件信息和预设的风险识别规则确定目标事件的风险识别结果。

例如，目标事件为支付事件。支付平台检测到目标账户发起支付事件时，可以获得支付事件的事件信息。所述事件信息包括但不限于：支付金额，支付设备，目标账户的 x 日内支付次数等。支付平台预设的风险识别规则包括但不限于以下至少一项：支付金额大于或等于金额阈值，支付设备不是目标账户的常用设备，目标账户的 x 日内支付次数大于或等于频次阈值。

若基于所述事件信息确定上述至少一项风险识别规则被满足，则支付平台确定目标事件的风险识别结果为有风险；或者，若基于事件信息确定上述风险识别规则都不被满足，则支付平台确定目标事件的风险识别结果为没有风险。支付平台确定目标事

件的风险识别结果后，可以针对目标事件执行所述风险识别结果对应的风控策略。其中，不同的风险识别结果可以对应不同的风控策略。

综上，当前的风控识别规则大多都是基于事件信息设置，风险识别逻辑比较简单。不法分子可以通过有限次数的测试推算出部分识别规则。例如，不法分子可以通过多次测试发现风控识别规则中的金额阈值、频次阈值等。从而后续不法分子通过盗用的账户执行违法事件时，可以绕开上述风控识别规则，使得风控失效，对服务平台以及被盗用账户的合法使用者不利。

鉴于此，本说明书提供一种风控方法、设备及存储介质，通过当前账户对应的用户行为数据确定目标账户被盗用的概率，进而基于概率确定由目标账户触发的目标事件的风险识别结果。本说明书提供的风控方案可以提高不法分子通过测试绕过风险识别策略的门槛，提升风控的有效性。

下面结合图 1 对本说明书提供的风控应用场景进行介绍。

图 1 示出了根据本说明书的实施例提供的风控应用场景的示意图。如图 1 所示，场景 001 可以包括：操作人员 100，终端设备 200，服务器 300、网络 400，风控设备 500。

操作人员 100 可以通过终端设备 200 执行相关事件。例如，终端设备 200 安装有一个或多个服务平台的客户端，所述客户端能够为操作人员 100 提供执行相关事件的能力。所述服务平台包括但不限于：网页浏览器类平台、搜索类平台、聊天类平台、购物类平台、服务类平台、视频类平台、理财类平台、支付类平台等。比如，终端设备 200 可以向操作人员 100 呈现交互界面，以便操作人员 100 通过该交互界面执行支付事件。操作人员 100 可能是服务平台的合法使用者，也可能是盗用合法使用者的账户的不法分子。

在一些实施例中，终端设备 200 可以执行本说明书描述的风控方法。终端设备 200 可以存储有用于实现风控方法的数据和指令，并可以执行或用于执行所述数据和指令。在一些实施例中，终端设备 200 可以包括具有数据信息处理功能的硬件设备和驱动该硬件设备工作所需必要的程序。

示例性的，终端设备 200 响应于检测到目标账户触发或者即将触发目标事件，获得目标账户对应的用户行为数据，基于用户行为数据确定目标账户为被盗账户的概率，进而基于概率确定目标事件的风险识别结果。该示例中各步骤的实现以及涉及的相关术语在后文方法 P100 中详细介绍。

终端设备 200 可以包括移动设备、平板电脑、笔记本电脑、机动车辆的内置设备或类似内容，或其任意组合。在一些实施例中，所述移动设备可包括智能家居设备、智能移动设备、虚拟现实设备、增强现实设备或类似设备，或其任意组合。在一些实施例中，所述智能家居装置可包括智能电视、台式电脑等，或任意组合。在一些实施例中，所述智能移动设备可包括智能手机、个人数字辅助、游戏设备、导航设备等，或其任意组合。在一些实施例中，所述虚拟现实设备或增强现实设备可能包括虚拟现实头盔、虚拟现实眼镜、虚拟现实补丁、增强现实头盔、增强现实眼镜、增强现实补丁或类似内容，或其中的任何组合。例如，所述虚拟现实设备或所述增强现实设备可能包括 AR 眼镜、头戴式显示器、VR 等。在一些实施例中，所述机动车中的内置装置可包括车载计算机、车载电视等。在一些实施例中，终端设备 200 可以是具有定位技术的设备，用于定位终端设备 200 的位置。

如图 1 所示，终端设备 200 可以与服务器 300 进行通信连接。服务器 300 可以是提供各种服务的服务器，例如对终端设备 200 提供支付服务的后台服务器。

在一些实施例中，服务器 300 可以执行本说明书描述的风控方法。服务器 300 可以存储有用于实现风控方法的数据和指令，并可以执行或用于执行所述数据和指令。在一些实施例中，服务器 300 可以包括具有数据信息处理功能的硬件设备和驱动该硬件设备工作所需必要的程序。

示例性的，服务器 300 响应于检测到目标账户触发或者即将触发目标事件，从本地或者终端设备 200 获得目标账户对应的用户行为数据，并基于用户行为数据确定目标账户为被盗账户的概率，进而基于概率确定目标事件的风险识别结果。该示例中各步骤的实现以及涉及的相关术语在后文方法 P100 中详细介绍。

网络 400 用以在终端设备 200、服务器 300 和风控设备 500 之间提供通信连接的介质。网络 400 可以促进信息或数据的交换。在一些实施例中，网络 400 可以是任何类型的有线或无线网络，也可以是其组合。比如，网络 400 可以包括电缆网络，有线网络、光纤网络、电信通信网络、内联网、互联网、局域网（LAN）、广域网（WAN）、无线局域网（WLAN）、大都市市区网（MAN）、公用电话交换网（PSTN）、蓝牙网络、ZigBee 网络、近场通信（NFC）网络或类似网络。在一些实施例中，网络 400 可以包括一个或多个网络接入点。例如，网络 400 可以包括有线或无线网络接入点，如基站或互联网交换点，通过该接入点，终端设备 200、服务器 300 和风控设备 500 的一个或多个组件可以连接到网络 400 以交换数据或信息。

风控设备 500 是具有一定计算能力的计算设备。例如，风控设备 500 可以是向服务器 300 提供风控能力的计算设备。风控设备 500 也可以称为风控系统。风控设备 500 可以对应单个计算设备，也可以对应由多个计算设备组成的计算集群。

在一些实施例中，风控设备 500 可以执行本说明书描述的风控方法。风控设备 500 可以存储有用于实现风控方法的数据和指令，并可以执行或用于执行所述数据和指令。在一些实施例中，风控设备 500 可以包括具有数据信息处理功能的硬件设备和驱动该硬件设备工作所需必要的程序。

示例性的，风控设备 500 与服务器 300 通过网络 400 通信连接。在终端设备 200 或者服务器 300 检测到目标账户触发或者即将触发目标事件后，向风控设备 500 发送检测到目标账户触发或者即将触发目标事件的指示信息。风控设备 500 响应于该指示信息，向终端设备 200 或者服务器 300 获得目标账户对应的用户行为数据，并基于用户行为数据确定目标账户为被盗账户的概率，进而基于概率确定目标事件的风险识别结果。或者，风控设备 500 确定目标账户为被盗账户的概率后，将概率发送给终端设备 200 或者服务器 300，终端设备 200 或者服务器 300 基于概率确定目标事件的风险识别结果。

应该理解，图 1 中的终端设备 200、服务器 300、网络 400 和风控设备 500 的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备 200、服务器 300、网络 400 和风控设备 500。

需要说明的是，所述风控方法可以完全在终端设备 200 上执行，也可以完全在服务器 300 上执行，也可以完全在风控设备 500 上执行，也可以部分在服务器 300 上执行、部分在风控设备 500 上执行，也可以部分在终端设备 200 上执行、部分在服务器 300 上执行，或者还可以有其他未列举的执行方式，本说明书实施例对此不做限制。

图 2 示出了根据本说明书的实施例提供的一种电子设备 600 的硬件结构图。电子设备 600 可以作为图 1 中的终端设备 200 或者服务器 300，也可以作为图 1 中的风控设备 500。

如图 2 所示，电子设备 600 可以包括至少一个存储介质 630 和至少一个处理器 620。在一些实施例中，电子设备 600 还可以包括通信端口 650 和内部通信总线 610。此外，电子设备 600 还可以包括 I/O 组件 660。

内部通信总线 610 可以连接不同的系统组件。例如，内部通信总线 610 可以连接存储介质 630、处理器 620、通信端口 650 和 I/O 组件 660。

I/O 组件 660 支持电子设备 600 和其他组件之间的输入/输出。

通信端口 650 用于电子设备 600 同外界的数据通信。比如，通信端口 650 可以用于电子设备 600 同网络 400 之间的数据通信。通信端口 650 可以是有线通信端口也可以是无线通信端口。

存储介质 630 可以包括数据存储装置。所述数据存储装置可以是非暂时性存储介质，也可以是暂时性存储介质。比如，所述数据存储装置可以包括磁盘 632、只读存储介质（ROM）634 或随机存取存储介质（RAM）636 中的一种或多种。存储介质 630 还包括存储在所述数据存储装置中的至少一个指令集。所述指令集可以包括计算机程序代码，所述计算机程序代码可以包括执行本说明书提供的风控方法的程序、例程、对象、组件、数据结构、过程、模块等等。

处理器 620 可以同存储介质 630 通信连接。处理器 620 用以执行上述至少一个指令集。当电子设备 600 运行时，处理器 620 读取所述至少一个指令集，并且根据所述至少一个指令集的指示，执行本说明书提供的风控方法。

处理器 620 可以是一个或多个处理器的形式。在一些实施例中，处理器 620 可以包括一个或多个硬件处理器。例如微控制器，微处理器，精简指令集计算机（RISC），专用集成电路（ASIC），特定于应用的指令集处理器（ASIP），中心处理单元（CPU），图形处理单元（GPU），物理处理单元（PPU），微控制器单元，数字信号处理器（DSP），现场可编程门阵列（FPGA），高级 RISC 机器（ARM），可编程逻辑器件（PLD），能够执行一个或多个功能的任何电路或处理器等，或其任何组合。

为了说明问题，在附图中电子设备 600 中仅示出一个处理器 620。然而，应当注意，本说明书中电子设备 600 还可以包括多个处理器。因此，本说明书中披露的操作和/或方法步骤可以由一个处理器执行，也可以由多个处理器联合执行。例如，如果电子设备 600 的处理器 620 执行步骤 A 和步骤 B，则应该理解，步骤 A 和步骤 B 也可以由两个不同处理器 620 联合或分开执行（例如，第一处理器执行步骤 A，第二处理器执行步骤 B，或者第一和第二处理器共同执行步骤 A 和 B）。

图 3 示出了根据本说明书的实施例提供的一种风控方法 P100 的流程图。如前，电子设备 600 可以执行风控方法 P100。具体地，电子设备 600 中的处理器可以读取存储在其本地存储介质中的指令集，然后根据指令集的规定，执行风控方法 P100。

风控方法 P100 可以应用于需要风控的任何服务平台。如图 3 所示，风控方法 P100 可以包括如下步骤。

S110：响应于检测到目标账户触发或者即将触发目标事件，获得目标账户对应的用户行为数据。所述用户行为数据表征目标账户的当前使用者在发起目标事件之前的历史时段内通过交互页面执行的行为序列。

所述目标账户可以是一个，也可以是多个，本说明书实施例对此不做限制。当所述目标账户是多个时，电子设备 600 可以针对多个目标账户并行或者依次执行方法 P100，本说明书实施例对此不做限制。后文主要以一个目标账户为例，介绍电子设备 600 的执行过程。

目标账户为服务平台的合法使用者在所述服务平台注册或者申请的账户。若方法 P100 应用于目标服务平台，则目标事件可以是当前使用者在目标服务平台触发的，或者，也可以是当前使用者在其他服务平台触发的，本说明书实施例对此不做限制。所述目标事件例如支付事件，所述支付事件可以是当前使用者在支付平台触发的，也可以是当前使用者在支付平台之外的其他交易平台触发的。

所述用户行为数据可以表征：目标账户的当前使用者在发起目标事件之前的历史时段内通过目标服务平台提供的交互页面执行的行为序列，或者，目标账户的当前使用者在发起目标事件之前的历史时段内通过目标服务平台和其他服务平台提供的交互页面执行的行为序列。

“检测到目标账户触发目标事件”可以理解为：检测到目标账户的当前使用者通过交互页面执行了触发操作，所述触发操作用于发起/执行目标事件。当前使用者为当下使用所述目标账户的人，可能是不法分子，也可能是目标账户的合法使用者或者合法拥有着。例如目标事件为支付事件，若检测到当前使用者点击“支付”按钮（触发操作的举例），则可以认为检测到目标账号触发支付事件。

“检测到目标账户即将触发目标事件”可以理解为：检测到目标账户的当前使用者执行了预设交互操作。所述预设交互操作不是用于发起/执行目标事件的操作，但是却表征了当前使用者接下来大概率会执行用于发起/执行目标事件的触发操作，或者说，当前使用者接下来在较短的时间内会执行用于发起/执行目标事件的触发操作。例如目标事件为支付事件，上述预设交互操作可以为点击“结算”按钮，或者点击“提交订单”按钮，等。也就是说，若检测到当前使用者在购物车页面点击“结算”按钮（预设交互操作的举例），或者在订单页面点击“提交订单”按钮（预设交互操作的举例），则可以认为检测到目标账户即将触发支付事件。

需要说明的是，上面是以“将预设交互操作作为目标事件即将被触发的信号”为

例，来对目标事件即将被触发进行举例说明。本领域技术人员能够理解，目标事件即将被触发还可以通过其他方式进行检测。

所述行为序列可以理解为一个或多个用户行为。所述用户行为即目标账户的当前使用者的行为。

所述历史时段是指在目标账户的当前使用者发起目标事件之前的某个时间段。在一些实施例中，所述历史时段可以基于目标事件的触发时刻与预设时长确定。例如预设时长为 X 分钟，则所述历史时段是以目标事件的触发时刻为结束时刻、时长为 X 分钟的一个时间段。在一些实施例中，所述历史时段的开始时刻和结束时刻可以均位于目标事件的触发时刻之前。

假设电子设备 600 在时刻 T1 检测到目标账号即将触发目标事件，并在时刻 T2 检测到目标账号触发目标事件，时刻 T2 晚于时刻 T1。该情况下，电子设备 600 获得的用户行为数据可以表征目标账户的当前使用者在时段[T0，T1]内通过交互页面执行的行为序列，其中时刻 T0 早于时刻 T1。或者，电子设备 600 获得的用户行为数据可以表征目标账户的当前使用者在时段[T0，T2]内通过交互页面执行的行为序列。本说明书实施例对此不做限制。

示例性的，电子设备 600 检测到以下任一种情况，则表示检测到目标账户即将触发目标事件。

情况 1：目标账户的当前使用者触发浏览预设页面，所述预设页面为用于触发目标事件的页面的前置页面。

触发浏览预设页面可以理解为：开始浏览预设页面。用于触发目标事件的页面可以理解为：用于发起/执行目标事件的页面。前置页面可以理解为：当前使用者在触发目标事件之前需要浏览的页面。

例如，用于触发目标事件的页面为支付页面，预设页面可以是购物车页面，也可以是提交订单页面。一般来说，当前使用者通过在购物车页面或者提交订单页面进行相关操作（例如点击“结算”或者“提交订单”按钮）后，购物车页面或者提交订单页面才会跳转（可以是一次跳转，也可以是多次跳转）到支付页面。当前使用者后续才可以在支付页面触发支付事件。因此购物车页面、或者提交订单页面称为支付页面的前置页面。

情况 2：目标账户的当前使用者执行预设交互操作，所述预设交互操作为执行目标事件的前置操作。

前置操作可以理解为：在触发目标事件之前，当前使用者需要执行的操作；或者，在跳转到用于触发目标事件的页面之前，当前使用者需要执行的操作等。预设交互操作的举例参考前文描述，不再赘述。

在一些实施例中，所述用户行为数据包括多个目标页面对应的浏览数据，所述多个目标页面为所述目标账户的当前使用者在所述历史时段内依次浏览的交互页面。在该实施例中，通过浏览数据刻画当前使用者的行为，后续电子设备 600 可以基于浏览数据识别被盗账户。不法分子难以感知哪些浏览行为会被识别为异常，因此采用浏览数据进行风控的方案可以提升风控的有效性。

需要说明的是，本说明书实施例中的用户行为数据除了包括浏览数据之外，还可以包括当前使用者在浏览目标页面的过程中在目标页面进行的一些操作数据（比如点击操作，选择选项操作等）。本说明书实施例主要以浏览数据为例介绍方法 P100 的实现逻辑。

下面以所述多个目标页面中的目标页面 1 为例，介绍目标页面 1 对应的浏览数据。所述多个目标页面中其他目标页面对应的浏览数据是类似的，不再赘述。

示例性的，目标页面 1 对应的浏览数据包括以下至少一项：目标页面 1 的标识信息，目标页面 1 对应的浏览时长，目标页面 1 对应的浏览时刻，以及目标页面对应的浏览时刻与当前时刻之间的时间间隔。在该示例中，通过多维度的浏览数据全面表征当前使用者的浏览行为，为后续电子设备 600 识别被盗账户提供坚实依据。

其中，目标页面 1 对应的浏览时长可以理解为：当前使用者浏览目标页面 1 的总时长。目标页面 1 对应的浏览时刻可以理解为：当前使用者开始浏览目标页面 1 的时刻，或者当前使用者触发浏览目标页面 1 的时刻，或者当前使用者结束浏览目标页面 1 的时刻，或者开始浏览时刻和结束浏览时刻之间的时刻，本说明书实施例对此不做限制。所述当前时刻是指电子设备 600 执行“获得目标账户对应的用户行为数据”这个步骤时的时刻。例如，假设电子设备在时刻 T1 检测到目标账户即将触发目标事件，并在时刻 T2 检测到目标账户触发目标事件。在 S110 中，若电子设备 600 响应于检测到目标账户即将触发目标事件而获得目标账户对应的用户行为数据，则上述当前时刻可以为时刻 T1，或者为与时刻 T1 接近的时刻；若电子设备 600 响应于检测到目标账户触发目标事件而获得目标账户对应的用户行为数据，则上述当前时刻可以为时刻 T2，或者与时刻 T2 接近的时刻。

在一些实施例中，电子设备 600 获得目标账户在所述历史时段内的埋点数据；基于埋点数据确定所述多个目标页面的浏览顺序、以及所述多个目标页面各自对应的浏览数据；进而基于多个目标页面的浏览顺序，将所述多个目标页面各自对应的浏览数据排序得到所述用户行为数据。在该实施例中，用户行为数据中的浏览数据是按顺序排列的，可以更清晰的表征当前使用者的浏览轨迹，使得后续更准确的识别被盗账户。

埋点也称为打点、或者行为追踪，可以指在服务平台的客户端的特定位置插入代码来记录服务平台的使用者与终端设备的交互行为。记录的交互行为会被终端设备或者服务器收集并存储。电子设备 600 可以从终端设备或者服务器获得目标账户在所述历史时段内的埋点数据。如果所述多个目标页面都有埋点，且所述多个目标页面是当前使用者在所述历史时段内浏览的页面，则电子设备 600 获得的所述埋点数据即所述多个目标页面各自对应的埋点数据。

示例性的，以目标页面 1 为例，目标页面 1 对应的埋点数据可以包括目标页面 1 的标识信息，以及目标页面 1 对应的浏览时刻。其他目标页面对应的埋点数据也是类似，不再赘述。

电子设备 600 获得所述多个目标页面各自对应的埋点数据后，可以基于埋点数据中的浏览时刻确定所述多个目标页面的浏览顺序，还可以基于埋点数据确定各个目标页面各自对应的浏览数据。

以目标页面 1 为例，目标页面 1 对应的标识信息和浏览时刻可以直接基于目标页面 1 对应的埋点数据得到。目标页面 1 对应的浏览时刻与当前时刻之间的时间间隔可以基于埋点数据以及前文提及的所述当前时刻计算得到。目标页面 1 对应的浏览时长可以基于目标页面 1 对应的浏览时刻与当前使用者浏览的下一个目标页面对应的埋点数据确定。比如，当前使用者浏览的下一个目标页面为目标页面 2，则电子设备 600 可以基于目标页面 1 对应的浏览时刻与目标页面 2 对应的浏览时刻之间的差值确定目标页面 1 对应的浏览时长。其他目标页面对应的浏览数据的确定方式是类似的，不再赘述。

电子设备 600 得到所述多个目标页面各自对应的浏览数据后，按照所述多个目标页面的浏览顺序将多个浏览数据排序整理得到所述用户行为数据。

S120：基于所述用户行为数据确定目标账户为被盗账户的概率。

在一些实施例中，电子设备 600 可以将所述用户行为数据展示给风控人员，风控人员基于风控经验向电子设备 600 输入目标账户为被盗账户的概率。电子设备 600 可

以基于风控人员的输入确定目标账户为被盗账户的概率。

在一些实施例中，电子设备 600 将所述用户行为数据输入目标模型，得到目标账户为被盗账户的概率，所述目标模型被训练为基于账户对应的用户行为数据预测所述账户为被盗账户的概率。在该实施例中，通过预先训练好的目标模型可以提高得到所述概率的效率，并且目标模型的预测尺度比较统一，针对不同账户对应的用户行为数据得到的概率的准确度相对比较稳定。

示例性的，所述目标模型基于多个训练样本训练得到。目标模型可以由电子设备 600 或者其他设备训练得到，后文以电子设备 600 训练为例说明。如图 4 所示，目标模型的训练方法 P200 可以包括如下步骤。

S210：获得多个训练样本。其中，一个训练样本包括样本账户关联的用户行为数据和所述样本账户对应的标注信息。所述样本账户关联的用户行为数据表征所述样本账户的使用者在发起样本事件之前通过交互页面执行的行为序列。所述标注信息表征所述使用者是否是所述样本账户的合法用户。

所述样本事件可以是已经完成的历史事件。

电子设备 600 确定 n_1 个风险样本事件和 n_2 个普通样本事件，n_1 为大于或等于 1 的整数，n_2 为大于或等于 1 的整数。风险样本事件比如不是样本账户的合法使用者完成的历史事件。普通样本事件比如由样本账户的合法使用者完成的历史事件。也就是说风险样本事件对应的样本账户为被盗账户，普通样本事件对应的样本账户不是被盗账户。

示例性的，电子设备 600 可以基于至少一个风险样本事件对应的样本账户关联的用户行为数据生成一个对应负向标注信息的训练样本。负向标注信息表征所述训练样本对应的使用者不是合法用户。比如负向标注信息为 1。电子设备 600 可以基于至少一个普通样本事件对应的样本账户关联的用户行为数据生成一个对应正向标注信息的训练样本。正向标注信息表征所述训练样本对应的使用者是合法用户。比如正向标注信息为 0。

电子设备 600 获得风险样本事件或者普通样本事件对应的样本账户关联的用户行为数据的方式，与前文电子设备 600 获得目标账户对应的用户行为数据的方式类似，不再赘述。样本账户关联的用户行为数据包括的具体内容可参考前文对目标账户对应的用户行为数据的相关描述，不再赘述。

S220：获得待训练的目标模型。

待训练的目标模型可以是神经网络模型。例如长短期记忆网络（Long Short-Term Memory，LSTM）或者其他模型，本说明书实施例对此不做限制。

S230：将所述样本账户关联的用户行为数据输入待训练的目标模型，以获得所述样本账户为被盗账户的预测概率。

S240：以最小化所述预测概率与所述标注信息之间的差异为训练目标，对所述目标模型的参数进行更新。

示例性的，将所述多个训练样本分为训练集和验证集，将训练集中的训练样本分为多个 epoch。电子设备 600 在每轮迭代训练中使用一个或者多个 epoch，如此重复进行多轮迭代训练，直到电子设备 600 基于验证集、所述目标函数确定训练得到的目标模型达到训练结束条件。

S130：基于目标账户为被盗账户的概率确定目标事件的风险识别结果。

在一些实施例中，所述风险识别结果表征目标事件是否有风险。方法 P100 还包括：

在所述风险识别结果表征目标事件有风险的情况下，电子设备 600 针对目标事件执行预设风控策略。

所述预设风控策略例如拦截目标事件，或者对当前使用者进行核身。

在一些实施例中，所述风险识别结果表征目标事件的风险等级。方法 P100 还包括：

电子设备 600 基于所述风险识别结果，针对目标事件执行与所述风险等级对应的风控策略。其中，不同风险等级对应的风控策略不同。

例如，电子设备 600 维护多个风险等级和多个风控策略的对应关系。电子设备 600 确定风险识别结果即确定目标事件对应的风险等级，进而可以基于所述对应关系确定目标风控策略，从而针对目标事件执行所述目标风控策略。比如所述概率为 0-1 之间的数字，概率越大，表示目标事件对应的风险等级越高。

在该实施例中，针对表征不同风险程度的风险等级可以预设不同的风控策略，比较灵活。在实际风控过程中可以基于风险等级选择合适的风控策略，从而针对性的对目标事件进行风控。

示例性的，当所述风险识别结果表征第一风险等级时，电子设备 600 拦截所述目标事件；当所述风险识别结果表征第二风险等级时，电子设备 600 对所述当前使用者进行核身；或者当所述风险识别结果表征第三风险等级时，电子设备 600 放行所述目标事件。其中，第一风险等级高于第二风险等级，第二风险等级高于第三风险等级。

比如，第一风险等级为概率大于或等于 0.9，所述第二风险等级为概率大于或等于

0.5、且概率小于 0.9，所述第三风险等级为概率小于 0.5。

拦截目标事件可以理解为：电子设备 600 拒绝当前使用者继续目标事件的后续流程。例如电子设备 600 拒绝当前使用者继续支付事件的后续流程，并可以向当前使用者的终端设备发送风险提示。风险提示比如“您的账户有被盗风险，请停止支付操作”。

对所述当前使用者进行核身可以理解为：电子设备 600 要求当前使用者输入可以证明自己是合法使用者的信息。例如电子设备 600 通过给目标账户的注册手机号发送验证码，并向当前使用者的终端设备发送提示信息。提示信息比如“您的账户有被盗风险，请输入验证码”。或者电子设备 600 要求当前使用者输入密码或者进行人脸识别等核身操作。当前使用者通过终端设备核身成功后，电子设备 600 可以引导当前使用者完成目标事件的后续流程。若当前使用者核身失败，则电子设备 600 可以拒绝当前使用者的进一步操作。

放行目标事件可以理解为：电子设备 600 对目标事件不进行额外操作，即不拦截也不要求核身。当前使用者不会感知到阻拦，可以完成目标事件。例如，电子设备 600 允许目标账户完成支付事件的后续流程，或者电子设备 600 无需对目标账户的使用者进行核身的情况下，可以允许或者引导目标账户的使用者完成支付后续流程。

可以理解，本说明书提供的风控方法的执行方式（S110、S120、S130 的执行时机）可以有多种。下面以其中 3 种为例介绍。

方式 1

例如图 5 所示，假设目标事件的触发时刻为时刻 T2。电子设备 600 在时刻 T1 检测到目标账户即将触发目标事件，时刻 T1 早于时刻 T2。该情况下，电子设备 600 可以在时刻 T1 触发执行本说明书提供的风控方法，即在时刻 T1 触发执行 S110、S120 和 S130。在这种执行方式中，历史时段可以是指时刻 T1 之前的某个时段，例如，结合图 5，历史时段可以为时刻 T0 到时刻 T1 之间的时段。

在该方式中，电子设备 600 在检测到当前使用者发起目标事件之前（即时刻 T2 之前），就可以提前预测得到目标事件的风险识别结果。从而后续在电子设备 600 检测到目标事件被触发时，可以快速基于风险识别结果进行风控，风控效率较高，可以对当前使用者快速给出反馈。

方式 2

例如图 6 所示，假设目标事件的触发时刻为 T2。电子设备 600 在时刻 T1 检测到目标账户即将触发目标事件，时刻 T1 早于时刻 T2。该情况下，电子设备 600 可以在

时刻 T1 触发执行本说明书提供的风控方法中的步骤 S110 和 S120。通过上述两个步骤的执行，电子设备 600 可以确定出目标账户为被盗账户的概率。随后，电子设备 600 在时刻 T2 检测到目标事件被触发时，触发执行步骤 S130，以确定出目标事件的风险识别结果。在这种执行方式中，历史时段可以是指时刻 T1 之前的某个时段，例如，结合图 6，历史时段可以为时刻 T0 到时刻 T1 之间的时段。

在该方式中，电子设备 600 在检测到当前使用者发起目标事件之前，可以提前收集历史时段内的用户行为数据，并基于用户行为数据确定目标账号为被盗账户的概率。从而后续在电子设备 600 检测到目标事件被触发时，可以相对快速的基于所述概率确定目标事件的风险识别结果，并基于风险识别结果进行风控，风控效率也相对较高。

方式 3

例如图 7 所示，电子设备 600 在时刻 T2 检测到目标账户触发目标事件。响应于检测到目标账户触发目标事件，电子设备 600 在时刻 T2 触发执行本说明书提供的风控方法中的 S110、S120 和 S130，从而得到目标事件的风险识别结果。在这种执行方式中，历史时段可以为时刻 T2 之前的某个时段，例如参见图 7，历史时段可以为时刻 T0 到时刻 T2 之间的时段。

在一些实施例中，如图 8 所示，电子设备 600 基于所述用户行为数据确定目标账户为被盗账户的概率，进而基于所述概率确定目标事件的第一风险识别结果。第一风险识别结果不是目标事件的最终风险识别结果，电子设备 600 还需要结合目标事件的事件信息确定所述最终风险识别结果。即方法 P100 还包括：

响应于检测到所述目标事件被触发，获得所述目标事件的事件信息。如图 8 所示，电子设备 600 基于所述事件信息确定目标事件的第二风险识别结果，进而基于第一风险识别结果和第二风险识别结果确定目标事件的最终风险识别结果。

在该实施例中，电子设备 600 从多个维度对目标事件进行了风险识别，识别较为全面，得到的最终风险识别结果较为准确，避免从单一维度（事件信息维度，或者用户行为数据维度）识别的遗漏问题。

例如，目标事件为支付事件。支付平台检测到目标账户触发支付事件时，可以获得支付事件的事件信息。所述事件信息包括但不限于：支付金额，支付设备，目标账户的 x 日内支付次数等。

电子设备 600 可以基于所述事件信息和预设的风险识别规则确定第二风险识别结果。例如，支付平台预设的风险识别规则包括但不限于以下至少一项：支付金额大于

或等于金额阈值，支付设备不是目标账户的常用设备，目标账户的 x 日内支付次数大于或等于频次阈值。

电子设备 600 基于上述风险识别规则确定所述第二风险识别结果的方式可以参考前文描述，不再赘述。

可以理解，电子设备 600 得到的最终风险识别结果可以表征目标事件的风险等级。电子设备 600 可以基于最终风险识别结果，针对目标事件执行与所述风险等级对应的风控策略。风险等级的划分、风控策略的确定和具体内容以及其他相关内容可参考上文描述，不再赘述。

电子设备 600 可以在线执行方法 P100，即在目标事件未完成前对目标事件进行风控，或者说在目标事件的执行过程中对目标事件进行风控。实时分析当前使用者的行为数据，以便确定发起目标事件的目标账户是盗用账户的可能性，从而在目标事件被触发时对目标事件及时执行风控策略。即在风险发生前进行干预，及时采取风控策略，避免给合法使用者或者服务平台造成损失或者不利影响。

除此之外，电子设备 600 还可以离线执行方法 P100。在离线执行的过程中，与在线执行有区别的是：电子设备 600 是在目标事件完成后，确定目标事件对应的风险识别结果；在离线执行过程中基于风险识别结果进行的风控策略与在线实行过程中采用的风控策略会有不同。例如，电子设备 600 在 T 日对 T-1 日发生的历史事件进行依次识别。以一个历史事件为例，电子设备 600 在预设时刻（比如 T 日 00:00），获得历史事件的触发账户（即执行完成历史事件的账户）对应的用户行为数据。所述用户行为数据表征所述触发账户的使用者在发起所述历史事件之前的历史时段内通过交互页面执行的行为序列。进而电子设备 600 基于所述用户行为数据执行 S120 和 S130 得到历史事件的风险识别结果。离线执行过程中，电子设备 600 得到风险识别结果后，也可以基于风险识别结果表征的风险等级确定针对历史事件的风控策略。比如，风险识别结果对应所述第一风险等级，则电子设备 600 可以将历史事件对应的触发账户加到风险账户列表，或者黑名单。后续电子设备 600 会拦截所述触发账户发起的事件。再比如，风险识别结果对应所述第二风险等级，则电子设备 600 可以将历史事件对应的触发账户加到加强核身名单。后续电子设备 600 对所述触发账户发起的事件，可以要求对触发账户的使用者进行核身。

除了上述列举的区别之外，离线执行过程中涉及的其他步骤以及术语等相关内容可参考前文描述，不再赘述。离线执行可以对已经发生的事件进行补充识别，以发现

潜在的被盗账户，有助于后续风控。

另外，本说明书在涉及举例时，是以支付场景进行举例说明的。本领域技术人员应当理解，除了支付场景之外，本说明书提供的技术方案还可以应用于其他需要风控的场景，在其他场景的具体实现方式和技术效果与上述支付场景是类似的，本说明书对此不作赘述。

综上所述，本说明书提供的风控方法、设备及存储介质，电子设备 600 基于目标账户对应的用户行为数据确定目标账户为被盗账户的概率，进而基于概率确定目标账户触发或者即将触发的目标事件的风险识别结果。本说明书提供的风控方案依据的用户行为数据能够刻画当前使用者在历史时段内的行为模式，从而电子设备 600 可以从识别异常行为的角度出发确定所述概率。不法分子很难通过测试获知 P100 中基于用户行为数据得到相关概率的内在逻辑，不法分子也难以感知他的哪些行为可以被认为是异常行为被捕捉并分析。因此，本说明书提供的风控方案可以提高不法分子绕过风控的门槛和成本，提升风控的有效性。

本说明书另一方面提供一种计算机可读非暂时性存储介质，存储有至少一组用来进行风控的可执行指令。当所述可执行指令被处理器执行时，所述可执行指令指导所述处理器实施本说明书所述的方法 P100 的步骤。在一些可能的实施方式中，本说明书的各个方面还可以实现为一种程序产品的形式，其包括程序代码。当所述程序产品在电子设备 600 上运行时，所述程序代码用于使电子设备 600 执行本说明书描述的方法 P100 的步骤。用于实现上述方法的程序产品可以采用便携式紧凑盘只读存储器（CD-ROM）包括程序代码，并可以在电子设备 600 上运行。然而，本说明书的程序产品不限于此，在本说明书中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统使用或者与其结合使用。所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器（CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。所述计算机可读存储介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的

组合。可读存储介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。可读存储介质上包含的程序代码可以用任何适当的介质传输，包括但不限于无线、有线、光缆、RF 等等，或者上述的任意合适的组合。可以以一种或多种程序设计语言的任意组合来编写用于执行本说明书操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在电子设备 600 上执行、部分地在电子设备 600 上执行、作为一个独立的软件包执行、部分在电子设备 600 上部分在远程计算设备上执行、或者完全在远程计算设备上执行。

本说明书提及的“多个”，如果没有特殊的声明，应当理解为两个或者两个以上。

上述对本说明书特定实施例进行了描述。其他实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者是可能有利的。

综上所述，在阅读本详细公开内容之后，本领域技术人员可以明白，前述详细公开内容可以仅以示例的方式呈现，并且可以不是限制性的。尽管这里没有明确说明，本领域技术人员可以理解本说明书需求囊括对实施例的各种合理改变，改进和修改。这些改变，改进和修改旨在由本说明书提出，并且在本说明书的示例性实施例的精神和范围内。

此外，本说明书中的某些术语已被用于描述本说明书的实施例。例如，“一个实施例”，“实施例”和/或“一些实施例”意味着结合该实施例描述的特定特征，结构或特性可以包括在本说明书的至少一个实施例中。因此，可以强调并且应当理解，在本说明书的各个部分中对“实施例”或“一个实施例”或“替代实施例”的两个或更多个引用不一定都指代相同的实施例。此外，特定特征，结构或特性可以在本说明书的一个或多个实施例中适当地组合。

应当理解，在本说明书的实施例的前述描述中，为了帮助理解一个特征，出于简化本说明书的目的，本说明书将各种特征组合在单个实施例、附图或其描述中。然而，这并不是说这些特征的组合是必须的，本领域技术人员在阅读本说明书的时候完全有

可能将其中一部分设备标注出来作为单独的实施例来理解。也就是说，本说明书中的实施例也可以理解为多个次级实施例的整合。而每个次级实施例的内容在于少于单个前述公开实施例的所有特征的时候也是成立的。

本文引用的每个专利，专利申请，专利申请的出版物和其他材料，例如文章、书籍、说明书、出版物、文件、物品等，除了与本文件不一致或相冲突的、或者对权利要求的最宽范围具有限制性影响的文件，均可以通过引用结合于此，并用于现在或以后与本文件相关联的所有目的。此外，在任何材料对相关术语的描述、定义和/或使用与本文件对相关术语的描述、定义和/或使用之间存在任何不一致或冲突时，以本文件中的术语为准。

最后，应理解，本文公开的申请的实施方案是对本说明书的实施方案的原理的说明。其他修改后的实施例也在本说明书的范围内。因此，本说明书披露的实施例仅仅作为示例而非限制。本领域技术人员可以根据本说明书中的实施例采取替代配置来实现本说明书中的申请。因此，本说明书的实施例不限于申请中被精确地描述过的实施例。

权 利 要 求 书

1. 一种风控方法，包括：

响应于检测到目标账户触发或者即将触发目标事件，获得所述目标账户对应的用户行为数据，所述用户行为数据表征所述目标账户的当前使用者在发起所述目标事件之前的历史时段内通过交互页面执行的行为序列；

基于所述用户行为数据确定所述目标账户为被盗账户的概率；以及

基于所述概率确定所述目标事件的风险识别结果。

2. 根据权利要求 1 所述的方法，其中，所述用户行为数据包括多个目标页面对应的浏览数据，所述多个目标页面为所述目标账户的当前使用者在所述历史时段内依次浏览的交互页面。

3. 根据权利要求 2 所述的方法，其中，一个目标页面对应的浏览数据包括以下至少一项：

所述目标页面的标识信息，

所述目标页面对应的浏览时长，

所述目标页面对应的浏览时刻，以及

所述目标页面对应的浏览时刻与当前时刻之间的时间间隔。

4. 根据权利要求 2 所述的方法，其中，所述获得目标账户对应的用户行为数据，包括：

获得所述目标账户在所述历史时段内的埋点数据；

基于所述埋点数据确定所述多个目标页面的浏览顺序、以及所述多个目标页面各自对应的浏览数据；以及

基于多个目标页面的浏览顺序，将所述多个目标页面各自对应的浏览数据排序得到所述用户行为数据。

5. 根据权利要求 1 所述的方法，其中，所述检测到目标事件即将被触发，包括下述中的一种：

检测到所述目标账户的当前使用者触发浏览预设页面，所述预设页面为用于触发所述目标事件的页面的前置页面；或者

检测到所述目标账户的当前使用者执行预设交互操作，所述预设交互操作为执行所述目标事件的前置操作。

6. 根据权利要求 5 所述的方法，其中，所述用户行为数据是响应于检测到所述目标事件即将被触发而获得的，所述基于所述概率确定所述目标事件的风险识别结果，包括：

响应于检测到所述目标事件被触发，基于所述概率确定所述目标事件的风险识别结果。

7. 根据权利要求 1 所述的方法，其中，所述基于所述用户行为数据确定所述目标账户为被盗账户的概率，包括：

将所述用户行为数据输入目标模型，得到所述目标账户为被盗账户的概率，所述目标模型被训练为基于账户对应的用户行为数据预测所述账户为被盗账户的概率。

8. 根据权利要求 7 所述的方法，其中，所述目标模型基于多个训练样本训练得到，其中，一个训练样本包括样本账户关联的用户行为数据和所述样本账户对应的标注信息，

所述样本账户关联的用户行为数据表征所述样本账户的使用者在发起样本事件之前通过交互页面执行的行为序列，

所述标注信息表征所述使用者是否是所述样本账户的合法用户。

9. 根据权利要求 1 所述的方法，其中，所述风险识别结果表征所述目标事件的风险等级，所述方法还包括：

基于所述风险识别结果，针对所述目标事件执行与所述风险等级对应的风控策略，其中，不同风险等级对应的风控策略不同。

10. 根据权利要求 9 所述的方法，其中，所述基于所述风险识别结果，针对所述目标事件执行与所述风险等级对应的风控策略，包括下述中的一种：

当所述风险识别结果表征第一风险等级时，拦截所述目标事件；

当所述风险识别结果表征第二风险等级时，对所述当前使用者进行核身；或者

当所述风险识别结果表征第三风险等级时，放行所述目标事件，其中

所述第一风险等级高于所述第二风险等级，所述第二风险等级高于所述第三风险等级。

11. 根据权利要求 1 所述的方法，其中，所述方法还包括：

响应于检测到所述目标事件被触发，获得所述目标事件的事件信息；

所述基于所述概率确定所述目标事件的风险识别结果，包括：

基于所述概率确定所述目标事件的第一风险识别结果；

基于所述事件信息确定所述目标事件的第二风险识别结果；以及

基于所述第一风险识别结果和所述第二风险识别结果确定所述目标事件的所述风险识别结果。

12. 根据权利要求 1 所述的方法，其中，所述目标事件为支付事件。

13. 一种电子设备，包括：

至少一个存储介质，存储有至少一个指令集，用于风控；以及

至少一个处理器，同所述至少一个存储介质通信连接，其中，所述至少一个处理器运行时读取所述至少一个指令集，并且根据所述至少一个指令集的指示：

响应于检测到目标账户触发或者即将触发目标事件，获得所述目标账户对应的用户行为数据，所述用户行为数据表征所述目标账户的当前使用者在发起所述目标事件之前的历史时段内通过交互页面执行的行为序列，

基于所述用户行为数据确定所述目标账户为被盗账户的概率，以及

基于所述概率确定所述目标事件的风险识别结果。

14. 根据权利要求 13 所述的电子设备，其中，所述用户行为数据包括多个目标页面对应的浏览数据，所述多个目标页面为所述目标账户的当前使用者在所述历史时段内依次浏览的交互页面。

15. 根据权利要求 14 所述的电子设备，其中，一个目标页面对应的浏览数据包括以下至少一项：

所述目标页面的标识信息，

所述目标页面对应的浏览时长，

所述目标页面对应的浏览时刻，以及

所述目标页面对应的浏览时刻与当前时刻之间的时间间隔。

16. 根据权利要求 14 所述的电子设备，其中，为了获得目标账户对应的用户行为数据，所述至少一个处理器：

获得所述目标账户在所述历史时段内的埋点数据；

基于所述埋点数据确定所述多个目标页面的浏览顺序、以及所述多个目标页面各自对应的浏览数据；以及

基于多个目标页面的浏览顺序，将所述多个目标页面各自对应的浏览数据排序得到所述用户行为数据。

17. 根据权利要求 13 所述的电子设备，其中，所述至少一个处理器：

检测到所述目标账户的当前使用者触发浏览预设页面，所述预设页面为用于触发所述目标事件的页面的前置页面；或者

检测到所述目标账户的当前使用者执行预设交互操作，所述预设交互操作为执行所述目标事件的前置操作。

18. 根据权利要求 17 所述的电子设备，其中，所述用户行为数据是响应于检测到所述目标事件即将被触发而获得的，为了确定所述目标事件的风险识别结果，所述至少一个处理器：

响应于检测到所述目标事件被触发，基于所述概率确定所述目标事件的风险识别结果。

19. 根据权利要求 13 所述的电子设备，其中，为了确定所述目标账户为被盗账户的概率，所述至少一个处理器：

将所述用户行为数据输入目标模型，得到所述目标账户为被盗账户的概率，所述目标模型被训练为基于账户对应的用户行为数据预测所述账户为被盗账户的概率。

20. 一种计算机可读非暂时性存储介质，其中，所述计算机可读非暂时性存储介质中存储有至少一个指令集，所述至少一个指令集被至少一个处理器执行时，实现如权利要求 1-12 中任一项所述的方法。