一种调整风险参数的方法、风险识别方法及装置

技术领域

本申请涉及信息技术领域，尤其涉及一种调整风险参数的方法、风险识别方法及装置。

背景技术

随着线上支付、线上转账等电子交易方式的普及，确保交易安全，及时准确识别交易风险，至关重要。

一般而言，用户可以在提供电子交易服务的客户端（如手机上安装的电子交易应用、电子交易网站对应的浏览器页面等）上注册账号和设置交易密码，并将账号与本人的银行卡绑定。当用户登录客户端，在客户端中输入交易密码请求支付时，客户端向控制服务器发送支付请求，控制服务器将对接收到的支付请求进行风险识别，如果风控识别的结果是安全的，即当前交易是用户本人操作的或用户本人授权他人操作的，则控制服务器根据该支付请求对用户的银行卡进行相应的扣款操作；如果风控识别的结果是不安全的，即当前交易有较大概率是不法分子盗用用户的账号和密码进行操作的，则控制服务器可以采取诸如指示客户端将当前交易冻结、向账号绑定的手机号码及邮箱发送风险提示短信等措施。

现有的风险识别方法有两种：方法一，根据已知风险，人为定义各种风险识别规则，由控制服务器根据风险识别规则对交易进行风险识别。方法二，在控制服务器上布设人工智能的风险识别系统，预先使用诸如随机森林、逻辑回归、神经网络等机器学习算法，向风险识别系统提供海量的历史操作数据（包含安全的操作数据和不安全的操作数据），对风险识别系统进行训练，使得风险识别系统根据已知风险总结出风险识别规则，在面对新的交易时，能够在一定程度上识别出该交易的风险。

实际上，人为定义的或者通过机器学习总结出的风险识别规则，对已知风

险的依赖性太强。不法分子往往会频繁得尝试破解风险识别规则，不断研究出新的线上财产盗用手段，使得风险识别系统总是面对不可控的未知风险。在现有的风险识别方法中，为了应对频繁出现的新的财产盗用手段，需要对风险识别规则进行频繁更新。

在现有的风险识别方法中，不论是人力维护风险识别规则，还是通过机器学习更新风险识别规则，都只是风险识别规则被破解后的补救措施，也就是说，在不法分子采用新的财产盗用手段绕过风险识别规则给用户造成难以估量的损失后，才能通过人工补防或风险识别系统的重训来完成对风险识别规则的更新。

尤其是，一方面人工补防成本太高，且难免出现工作的疏忽和遗漏；另一方面，风险识别系统的重训往往需要离线进行，且耗时可达数月。可见，现有的调整风险识别规则的方法存在成本过高和延时性过大的问题。

发明内容

本申请实施例提供一种调整风险参数的方法、风险识别方法及装置，以解决现有的风险识别方法存在的成本过高和延时性过大的问题。

为解决上述技术问题，本申请实施例是这样实现的：

本申请实施例提供的一种调整风险参数的方法，包括：

接收支付请求，所述支付请求中包含用户标识和通过所述用户标识在当前交易中产生的操作数据；

根据所述操作数据，确定在所述当前交易中产生的至少一个操作跳转序列，所述操作跳转序列中包含至少一个操作跳转事件；

从所述用户标识对应的风险参数集合中，获取与所述操作跳转序列中包含的所述操作跳转事件对应的风险参数，所述风险参数集合中包含的风险参数是根据所述用户标识对应的上一次交易产生的操作数据，对在上一次交易中进行风险识别所使用的风险参数进行调整后得到的；

根据所述至少一个操作跳转序列，调整获取到的所述风险参数。

本申请实施例提供的一种风险识别方法，包括：

接收支付请求，所述支付请求中包含在当前交易中产生的至少一个维度的操作数据；

针对每个维度，根据该维度的操作数据，确定所述当前交易的风险度；

在得到各维度对应的所述当前交易的风险度时，根据得到的不同的风险度，对所述当前交易进行风险识别。

本申请实施例提供的一种调整风险参数的装置，包括：

接收模块，接收支付请求，所述支付请求中包含用户标识和通过所述用户标识在当前交易中产生的操作数据；

确定模块，根据所述操作数据，确定在所述当前交易中产生的至少一个操作跳转序列，所述操作跳转序列中包含至少一个操作跳转事件；

获取模块，从所述用户标识对应的风险参数集合中，获取与所述操作跳转序列中包含的所述操作跳转事件对应的风险参数，所述风险参数集合中包含的风险参数是根据所述用户标识对应的上一次交易产生的操作数据，对在上一次交易中进行风险识别所使用的风险参数进行调整后得到的；

调整模块，根据所述至少一个操作跳转序列，调整获取到的所述风险参数。

本申请实施例提供的另一种风险识别装置，包括：

接收模块，接收支付请求，所述支付请求中包含在当前交易中产生的至少一个维度的操作数据；

确定模块，针对每个维度，根据该维度的操作数据，确定当前交易的风险度；

识别模块，在得到各维度对应的所述当前交易的风险度时，根据得到的不同的风险度，对所述当前交易进行风险识别。

本申请实施例提供的一种风险识别系统，包括：

智能模块，接收交易请求，获取通过用户标识在当前交易中产生的操作数

据，根据所述操作数据进行风险分析，并将风险分析结果发送给风险识别模块；所述风险分析结果通过上述风险识别方法得到；

风险识别模块，根据接收到的风险分析结果，进行风险识别。

由以上本申请实施例提供的技术方案可见，在本申请实施例中，一方面，将一次交易涉及的操作数据转化为至少一个操作跳转序列，每个操作跳转序列又包含至少一个操作跳转事件，每个操作跳转事件都对应有一个风险参数，那么，一次交易涉及的操作数据实际上被离散化为若干个独立的操作跳转事件；另一方面，针对在提供电子交易服务的客户端上注册的各用户标识，设置与各用户标识一一对应的各风险参数集合，并支持对各风险参数进行在线实时更新。如此以来，一旦不法分子盗用了用户的用户标识，通过用户标识在客户端上向控制服务器发起支付请求，即使不法分子暂时骗过了风险识别系统，造成了用户的财产损失，控制服务器也可以及时根据支付请求中包含的操作数据，对通过所述用户标识发起的这次交易所涉及的各操作跳转事件对应的风险参数进行在线动态更新，而无需待人工补防或风险识别系统离线重训。通过本申请所要求保护的风险识别方法，一方面可以避免人工补防的高成本，另一方面也无需等待风险识别系统长达数月的重训，就能实现对风险参数的在线动态更新，及时对风险识别系统完成补防。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术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申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例提供的一种调整风险参数的方法流程图；

图 2 是本申请实施例提供的一种风险识别方法流程图；

图 3 是本申请实施例提供的一种调整风险参数的装置示意图；

图 4 是本申请实施例提供的一种风险识别装置示意图；

图 5 是本申请实施例提供的一种风险识别系统示意图；

图 6（a）、图 6（b）、图 6（c）和图 6（d）分别是本申请实施例提供的一种风险识别系统的详细示意图。

具体实施方式

为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

在在线风险识别的技术领域，通常采用如背景技术所述的方法一和方法二的结合进行在线风险识别。即一方面通过向风险识别系统提供海量的历史操作数据，利用机器学习的方法，对风险识别系统进行训练，使风险识别系统总结出风险识别规则，另一方面再人工将专家的业务经验加入到风险识别规则中。但是，这种基于方法一和方法二结合的风险识别方法，依然存在成本过高和延时性大的缺陷。

具体而言，线上风险如同对弈，风控人员维护的风险识别系统所依赖的风险识别规则总是基于已知风险确定的，而不法分子盗用了用户的用户标识之后，总是会不断尝试破解风险识别规则，研究出新的财产盗用手段。倘若不法分子一旦得手，风控人员可以及时对风险识别系统进行补防，及时遏制了这种新的财产盗用手段危害的扩大，那么，不法分子的偶尔得手并不会造成很大的线上风险。

但是实际上，现有的风险识别方法是通过人工补防或系统重训补防的，而人工补防除了存在成本过高的问题外，一种新的财产盗用手段在不造成足以引起风控人员重视的较大面积危害之前，风控人员是不会对风险识别规则进行更

新的，人工补防也在一定程度上存在延时性大的问题；对系统重训而言，延时性大的问题更加严重，因为风险识别系统的重训需要采用离线学习的方式，且周期往往长达数月，而数月之后，新的财产盗用手段又会被不法分子研究出来，系统重训的价值也大打折扣。可见，由于现有的风险识别方法应对新的线上风险具有很大的延时性，因此导致现有的风险识别系统总是被不法分子“牵着鼻子走”，非常被动，也往往不能及时阻止线上风险的扩大。

而本申请所要求保护的风险识别方法，可以实现在线上风险的博弈中，响应于不法分子对风险识别系统的每次挑战，及时地、在线地对各风险参数进行动态调整，相当于在实战中利用不法分子不知疲倦地尝试，来对风险识别系统进行线上训练。其中，每个风险参数对应于一个操作跳转事件，风险操作系统根据风险参数集合分析每次交易涉及到的操作跳转事件的风险，综合地对这次交易进行风险识别。也就是说，所述风险参数是风险识别规则的一种具体形式，调整了风险参数，也就实现了对风险识别规则的更新。

现实中，即使不法分子偶尔得手，风险识别系统也可以随后及时（最长需要一天）通过调整风险参数完成补防，不法分子采用偶尔得手所采用的新的财产盗用手段在下一次非法交易中就会被识别出来。此外，由于风险参数总是可以得到在线动态调整，对不法分子而言，风险识别系统的也越来越难以被破解。

本申请的核心思想在于，将一次交易离散化为一系列可被独立进行发生可能性评价的操作跳转事件（对操作跳转事件的解释详见后文），由于不论是用户本人还是不法分子通过用户的用户标识登录客户端后进行的操作都可以被离散化一系列最基本的操作跳转事件，因此，可以通过对一次交易涉及的各操作跳转事件分别进行发生可能性的评价，来总体上实现对当前交易的发生可能性的评价，也就实现了对当前交易的风险识别，同时，可以通过对预设的每个用户标识对应的操作跳转事件集中的指定的至少一个操作跳转事件对应的风险参数进行调整，也就能对指定的操作跳转事件的发生可能性的预期进行调整，从而实现了风险识别系统的风险识别规则的逻辑或策略进行调整。

而在现有的风险识别方法中，由于人为设置的或机器学习总结的风险识别规则的逻辑是封闭的，不能对风险识别规则进行调整，只能在风险识别系统离线的情况下，新增或替换风险识别规则，这样就具有很大的延时性，也耗费较大的成本。

总之，本申请所要求保护的风险识别方法，通过根据每次交易的操作数据动态调整风险参数，可以对线上风险进行实时的记忆，风险识别系统能够自适应地学习，更少依赖人力，并且，风险识别系统总是保持与不法分子“对弈”的状态，风险参数集合中的各风险参数的准确性也久经考验，逐渐地，风险识别系统总是可以更加准确地识别风险，甚至可以在一定程度上实现对线上风险的预测。

以下结合附图，详细说明本申请各实施例提供的技术方案。

图 1 是本申请实施例提供的一种调整风险参数的方法流程图，包括以下步骤：

S101：接收支付请求。

本方法的执行主体可以是提供电子交易服务的服务商的控制服务器，所述控制服务器与安装于各用户的终端设备上的客户端进行交互，接收客户端发送的支付请求，向客户端发送指令，如冻结交易后向客户端发送指令，指令客户端在终端设备屏幕上显示消息“交易已冻结”。

在本申请实施例中，所述控制服务器上可以部署有风险识别系统，所述风险识别系统用于根据支付请求进行风险识别。所述风险识别系统除了可以进行线上自学习，自主调整风险参数外，还支持风控人员对风险参数进行手动更新，也支持离线训练。

在本申请实施例中，所述支付请求中包含用户标识和通过所述用户标识在当前交易中产生的操作数据。其中，所述用户标识可以是登录客户端的用户标识（用户的账号）。所述操作数据可以包含如下数据:通过所述用户标识进行当前交易的人执行的操作、当前交易的时间、当前交易涉及的商户信息、物流信

息、待付款金额、当前交易中使用的终端设备与外界交互产生的数据等。总之，凡是当前交易涉及的，可被客户端获取的数据，都可以是本申请所述的操作数据。

本申请实施例中所述支付涉及的技术载体，例如可以包括近场通信（Near Field Communication，NFC）、WIFI、3G/4G/5G、POS 机刷卡技术、二维码扫码技术、条形码扫码技术、蓝牙、红外、短消息（Short Message Service，SMS）、多媒体消息（Multimedia Message Service，MMS）等。

S102：根据所述操作数据，确定在所述当前交易中产生的至少一个操作跳转序列。

在本申请实施例中，所述操作跳转序列可以是包含至少一个操作跳转事件序列，操作跳转序列包含的各操作跳转事件之间有逻辑联系。例如，操作跳转序列包含操作跳转事件 T1、T2、T3，而在一次交易中，T1、T2、T3 相继发生，T1 发生后，才可能发生 T2，T2 发生后，才可能发生 T3。

而一个操作跳转事件可以是一个行为的发生，也可以是两个状态之间发生转移的事件。例如，“在客户端中点击了链接”就是一个操作跳转事件，该操作跳转事件可以是“发生了点击链接的行为”，也可以是“从链接未被点击的状态转移到链接被点击的状态”。为了描述的方便，以下以操作跳转事件为两个状态之间发生转移的事件为例说明。

假设小明打开客户端，点击了客户端中的购买链接，并在弹出的付款页面中点击了“支付”按钮，那么控制服务器会接收到这一支付请求，该支付请求包含小明的用户标识和通过小明的用户标识在当前交易中产生的操作数据，假设所述操作数据为“小明使用小丽的苹果手机（出厂号 f2154）在客户端上登录自己的账号，于 2016 年 1 月 5 日 17 点 20 分点击了耐克专卖店的购买链接，并于 2016 年 1 月 5 日 18 点 05 分请求支付 500 元购买一双耐克专卖店的球鞋”，那么，根据该操作数据，可以确定至少一个操作跳转序列，操作跳转序列实际上可以反映当前使用小明账号的人有多大概率是小明本人。例如，可以确定三

个操作跳转序列，分别涉及通过小明的账号如何操作、通过小明的账号在何时操作、苹果手机 f2154 每天登录账号的次数这三个方面，可以从这三个方面考察当前使用小明账号的人有多大概率是小明本人。具体而言，操作跳转序列 1，包含的操作跳转事件为：小明点击了耐克专卖店的购买链接，小明点击了一双球鞋的支付按钮；操作跳转序列 2，包含的操作跳转事件为：小明于 2016 年 1 月 5 日 17 点 20 分点击了购买链接，小明于 2016 年 1 月 5 日 18 点 05 分点击了支付按钮；跳转序列 3，包含的操作跳转事件为：苹果手机 f2154 上退出了小丽的账号，苹果手机 f2154 上登录了小明的账号。

例如，对操作跳转序列 1 包含的操作跳转事件“小明点击了一双球鞋的支付按钮”而言，该操作跳转事件对应了两个状态间的转移，即状态 1“支付按钮未被点击”->状态 2“支付按钮被点击”。又如，对操作跳转序列 3 包含的操作跳转事件“苹果手机 f2154 上退出了小丽的账号”而言，该操作跳转事件对应了两个状态间的转移，即状态 1“苹果手机 f2154 上登录有小丽的账号”->“苹果手机 f2154 不登录有小丽的账号”。

类似地，对于操作跳转序列中的每个操作跳转事件，都可以对应如上的两个状态间的转移，不再赘述。

综上可见，操作数据、操作跳转序列、操作跳转事件（一个状态转移到另一个状态）之间的关系已经明了，即针对通过某个用户标识发起的当前交易而言，可以根据当前交易涉及的操作数据确定当前交易涉及的至少一个操作跳转序列，然后根据当前交易涉及的每个操作跳转序列，确定该操作跳转序列包含的操作跳转事件。

实际上，本申请所要求保护的技术方案的核心思想在于，一方面，将一次交易涉及的操作数据转化为至少一个操作跳转序列，每个操作跳转序列又包含至少一个操作跳转事件，每个操作跳转事件都对应有一个风险参数，那么，一次交易涉及的操作数据实际上被离散化为若干个独立的操作跳转事件；另一方面，针对在提供电子交易服务的客户端上注册的各用户标识，设置与各用户标

识一一对应的各风险参数集合，并支持对各风险参数进行在线实时更新。如此以来，一旦不法分子盗用了用户的用户标识，通过用户标识在客户端上向控制服务器发起支付请求，即使不法分子暂时骗过了风险识别系统，造成了用户的财产损失，控制服务器也可以及时根据支付请求中包含的操作数据，对通过所述用户标识发起的这次交易所涉及的各操作跳转事件对应的风险参数进行在线动态更新，而无需待人工补防或风险识别系统离线重训。

可见，在本申请实施例中，根据通过所述用户标识在当前交易中产生的操作数据来确定相应的至少一个操作跳转序列，进而确定当前交易涉及的所有操作跳转事件，是对当前交易进行风险识别和调整风险参数的必经步骤。

本申请实施例实际上借鉴了增强学习理论中的"将一次大事件视为至少一个操作转移序列，即将一次大事件离散为若干个操作跳转事件"的思想，从需要分析的大事件的操作数据中提炼出若干个操作跳转事件，机器通过不断试错，确定出每个操作跳转事件对应的发生概率，也就可以根据各操作跳转事件的发生概率，对一次大事件进行决策。

而在本申请所要求保护的技术方案提供的一种实施例中，正是受到增强学习理论的启发，将交易中可能发生的各种事件拆散为一系列操作跳转事件，初始化各操作跳转事件分别对应的发生概率，作为初始化的风险参数，这样以来，当一笔交易发生时，风险识别系统可以首先分析出这笔交易涉及的各操作跳转序列，也就确定了涉及的各操作跳转事件，在设置的各发生概率中，查询这笔交易涉及的各操作跳转事件分别对应的发生概率，对这笔交易涉及的各操作跳转事件分别对应的发生概率综合考虑，就可以确定这笔交易是否合理，也就识别了这笔交易的风险。

S103：从所述用户标识对应的风险参数集合中，获取与所述操作跳转序列中包含的所述操作跳转事件对应的风险参数。

在本申请实施例中，所述风险参数可以是机器增强学习方法中使用的发生概率，也可以是风控人员为了防止风险参数被破解，使用某种加密算法对风险

概率进行加密所得的参数。总之，凡是可以用来分析操作跳转事件的发生可能性的参数，都可以是本申请所述的风险参数。值得说明的是，调整了所述风险参数，也就意味着调整了风险识别系统所依赖的风险识别规则。

在本申请实施例中，在步骤 S101 之前，可以对控制服务器上部署的风险识别系统进行初始化，针对注册的每个用户标识，确定该用户标识对应的操作跳转事件集，并为该用户标识对应的每个操作跳转事件对应的风险参数赋予一个初始值。

具体而言，可以定义不同的节点（也就是不同的状态），遍历不同节点两两之间发生的操作跳转（也就是不同状态两两之间的转移），得到多个操作跳转事件，将多个操作跳转事件归入到操作跳转事件集。值得说明的是，每个用户标识都对应有一个操作跳转事件集。

然后，可以为操作跳转事件集中的每个操作事件对应的风险参数随机赋予一个初始值，这样，在风险识别系统日积月累地更新各风险参数的过程中，各操作事件对应的风险参数会越来越与使用对应的用户标识的用户的个性贴合。

当然，也可以根据使用用户标识的用户的个性来确定各风险参数的初始值。具体而言，可以获取通过所述用户标识产生的的历史操作数据；针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：根据所述历史操作数据，确定该操作跳转事件的发生概率；将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

对于所述历史操作数据中未涉及的操作跳转事件而言，可以为这些操作跳转事件的发生概率赋予基准值。随着本风险识别方法的执行，这些发生概率也会被逐渐调整到贴合用户的个性的程度。

当无法获取通过所述用户标识产生的的历史操作数据时，获取设定数量的其他用户标识产生的历史操作数据；针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：根据所述历史操作数据，确定该操作跳转事件的发生概率；将所述发生概率作为该操作跳转事件对应的风险参数的初始

值。

也就是说，对于新注册的用户标识，由于无法获取该用户标识对应的历史操作数据，因此，可以将注册的其他用户标识所对应的历史操作数据作为该用户标识对应的历史操作数据，在根据所述历史操作数据确定该用户标识对应的跳转事件集中的每个跳转事件的发生概率。

值得强调的是，在对风险操作系统中的风险参数集合进行初始化后，在日后针对历次交易的风险识别中，所述风险参数集合中包含的风险参数可以是根据所述用户标识对应的上一次交易产生的操作数据，对在上一次交易中进行风险识别所使用的风险参数进行调整后得到的。

也就是说，在对当前交易执行的一次风险识别方法中，进行风险识别所依据的风险参数集合是对上一次交易执行风险识别后对风险参数集合调整后得到的最新的风险参数集合。调整后的风险参数集合用于进行下一次交易的风险识别。

S104：根据所述至少一个操作跳转序列，调整获取到的所述风险参数。

在本申请实施例中，当通过对当前交易进行分析，确定了当前交易涉及的操作跳转序列时，也就确定了当前交易涉及的操作跳转事件。那么，如前所述，既然风险参数集合中已经尽可能穷尽了各操作跳转事件分别对应的风险参数，那么，就可以在风险参数集合中查询当前交易涉及的各操作跳转事件分别对应的风险参数，然后根据当前交易涉及的各操作跳转事件分别对应的风险参数（可以是发生概率），确定该操作跳转序列的风险值。在确定了当前交易的各操作跳转序列的风险值之后，就可以确定最终当前交易的风险度了。

在本申请实施例中，之所以要先根据操作数据确定至少一个操作跳转序列，然后确定每个操作跳转序列的风险值，最后根据各操作跳转序列的风险值确定当前交易的风险度，而不是直接根据操作数据涉及的所有操作跳转事件来确定风险度，是因为，操作跳转序列可以体现当前交易的操作数据反映的交易逻辑性，而单个操作跳转事件是不能反映当前交易的交易逻辑性的，操作跳转

事件按一定顺序组成的操作跳转序列才具有交易逻辑性。对当前交易的分析实际上就是对当前交易逻辑的分析，对当前交易的风险识别，实际上就是对当前交易逻辑是否合理进行判断。因此，即使是包含同样的操作跳转事件的两个操作跳转序列，也可能由于各自包含的操作跳转事件的发生顺序不同而对应不同的风险值。

在本申请实施例中，获取到的所述风险参数就是当前交易涉及的操作跳转事件分别对应的风险参数。所述风险度可以是数值，该数值有当前交易涉及的各操作跳转序列的风险值汇总而成，也可以是等级，该等级根据当前交易涉及的各操作跳转序列的风险值汇总后评定。

风险识别系统确定了当前交易的风险度后，可以根据风险度确定当前交易的风险概率，也可以根据风险度将当前交易定性为安全或不安全。总之，在本申请所要求保护的技术方案中，对风险值、风险度、风险识别的输出结果都不做具体形式的限定。

在本申请实施例中，可以在确定了当前交易的风险度之后，当确定当前交易对应的风险度高于设定阈值时，调低获取到的所述风险参数；在确定当前交易对应的风险度不高于设定阈值时，调高获取到的所述风险参数。所述设定阈值可以是预设的，风控人员认为的最大可控风险度，当前交易的风险度如果高于设定阈值，则说明当前交易的风险较大，那么当前交易涉及的操作跳转事件的发生的合理性就应当被低估，也就是说，发生概率较低的操作跳转事件是在一笔安全的交易中被风控人员认为有较低可能性出现的事件。

同理，当前交易的风险度如果低于设定阈值，则说明当前交易的风险不大，当前交易涉及的操作跳转事件的发生是合理的，符合既定预期，也就是说，当前交易涉及的操作跳转事件很可能是用户自己操作引起的，而不是不法分子引起的，那么，可以维持当前交易涉及的操作跳转事件对应的风险参数不变，或者调高当前交易涉及的操作跳转事件对应的风险参数。

当然，在本申请实施例中，也可以无需等待确定了当前交易的风险度后才

根据所述风险度调整获取到的所述风险参数。可以根据每个操作跳转序列的风险值对该操作跳转序列对应的风险参数进行调整。例如，风险值较高的操作跳转序列也可以说明将这个操作跳转序列包含的各操作跳转事件综合起来看，总体上发生的概率较低。

举例说明，假设一个操作跳转序列包含的操作跳转事件为 T1、T2、T3、T4、T5，各操作跳转事件发生的顺序为 T1、T4、T3、T5、T2，对小明而言，T1 的发生概率（风险参数）为 0.9，T4 的发生概率为 0.8，T3 的发生概率为 0.1，T4 的发生概率为 0.05，T5 发生的概率为 0.15，那么，即使 T1 和 T2 的发生概率都很高，但是 T1、T4、T3、T5、T2 按此顺序一并发生的可能性却很低，那么依然判定该操作跳转序列的风险值较高。

在本申请实施例中，可以根据用户的每次操作界定一个操作跳转事件，也可以根据交易中涉及的每两个状态的转移界定一个操作跳转事件，还可以根据除用户外的其他维度，如用户使用的终端设备的维度、当前交易指向的商户的维度、用户当前所处的位置的维度以及其他可用的维度，来界定一个操作跳转事件。例如“小明点击购买链接”或“购买链接未被点击->购买链接被点击”可以是一个操作跳转事件，“手机未扫二维码->手机扫二维码”可以是一个操作跳转事件，“耐克专卖店每分钟卖出 1 双球鞋->耐克专卖店每分钟卖出 10 双球鞋”可以是一个操作跳转事件。

总之，本申请对具体如何界定一个操作跳转事件不做限制，本申请的核心是将一次交易离散为一系列可被独立评价的操作跳转事件，以便于通过对每个操作跳转事件的风险参数的调整实现对风险识别系统的策略的调整。

基于同样的原因，本申请对具体采用何种算法或方式对各操作跳转事件的回报函数值、各操作跳转序列的风险值、当前交易的风险度进行计算和汇总，也不做限制，风控人员可以根据业务情况灵活部署。

综上，通过图 1 所示的风险识别方法，针对在提供电子交易服务的客户端上注册的各用户标识，分别设置各用户标识对应的风险参数，并支持对风险参

数进行在线实时更新。如此以来，一旦不法分子盗用了用户的用户标识，通过用户标识在客户端上向控制服务器发起支付请求，即使不法分子暂时破解了用户标识对应的风险参数，造成了用户的财产损失，控制服务器也可以及时根据支付请求中包含的操作数据，对用户标识对应的风险参数进行在线动态更新，而无需待人工补防或风险识别系统离线重训。通过本申请所要求保护的风险识别方法，一方面可以避免人工补防的高成本，另一方面也无需等待风险识别系统长达数月的重训，就能实现对风险参数的在线动态更新，及时对风险识别系统完成补防。同时，通过在线动态调整风险参数集中的风险参数，也就实现了风险识别系统的自学习。

此外，现有的风险识别方法还存在的准确性较低的问题。现有的风险识别方法存在明显的局限性，即客户端及控制服务器依赖一定的风险识别规则"一刀切"得对不同的用户所发起的交易进行风险识别。

具体而言，如背景技术所述，不论是现有的风险识别方法中的方法一还是方法二，客户端及控制服务器进行风险识别时所依据的风险识别规则是适用于所有用户的共同规则，但是，各用户除了具有风险识别规则中包含的共性外，还具有各自的特性，如，有的用户喜欢透支消费，经常一次性花费银行卡余额的 80%以上的金额，又如，有的用户虽然未满 25 岁，但是经济能力较强，单次转账金额超过 5000 元的概率很高。对这些用户而言，现有的风险识别方法是不准确的。

即便将两种方法结合，即将专家经验和历史操作数据一并提供给风险识别系统进行训练，虽然能一定程度上提升风险识别的准确性，但是背景技术中所述的问题依然存在，未能考虑用户个性的风险识别方法的准确性依然是不高的。

也就是说，虽然可以通过采集海量的各用户在历史上产生的操作数据，从操作数据中提炼出适用于各用户的风险识别规则，但是，各用户的交易习惯毕竟千差万别，每个用户的日常交易场景也不是一成不变的，一条通用于不同用

户的风险识别规则也往往是粗糙的，它势必会遗漏用户的一些个性化的交易场景。

以风险识别规则“凌晨 12 点至 7 点之间，转账 5000 以上的交易不安全”为例，根据经验，在凌晨 12 点至 7 点之间在线进行较大数额的转账是不合常理的，因此这条风险识别规则一般是准确的，但是，现代社会人与人的作息规律差异巨大，有的用户习惯昼伏夜出，在凌晨 12 点至 7 点之间进行较大数额的在线交易是完全可能的，对这些用户而言，这条风险识别规则是不准确的，倘若依照这条风险识别规则对这些用户的交易进行冻结，反而给用户造成了困扰。

为此，在本申请所要求保护的技术方案中，通过针对每个用户标识设置该用户标识对应的风险参数集，为使用提供电子交易服务的客户端的用户定制个性化的风险识别策略。由于每个用户标识对应的风险参数集都是定制化的，这一方面使得风险识别系统所依赖的风险识别规则与每个用户的个性化特征相贴合，也就在一定程度上提升了风险识别的准确性，另一方面，客观上也增加了不法分子绕过风险识别系统的难度，不法分子不仅要窃取用户的用户标识，还必须对该用户的日常交易习惯有一定的了解才可能成功进行非法交易。

值得说明的是，试验表明，倘若只考察用户个性化的交易习惯进行风险识别，即预先从用户通过对应的用户标识在客户端上进行的历史交易中分析出用户的交易习惯，作为该用户标识对应的风险识别规则，当交易者通过该用户标识进行在线交易时，可以根据本次通过该用户标识进行的交易操作判断交易者是不是用户标识对应的用户本人，那么风险识别的准确性仍然不算高。原因有以下几点：

其一，风险识别规则的个性化虽然克服了现有技术中的风险识别规则“一刀切”和较为粗糙的问题，但是带来了新的弊端，即个性化的风险识别规则稳定性较差。也就是说，现有技术中的风险识别规则是基于业务常识和统计学，对用户群体交易习惯共性的提炼，其虽然较为粗糙，难以适应用户的个性化的

交易场景，却具有统计学上的稳定性（绝大部分用户的交易习惯的共性可以提炼为通用的风险识别规则）；相反，个性化的风险识别规则是根据某个用户的交易习惯总结得出的，而个人的交易习惯并不如群体的交易习惯一般，有基于统计学的稳定性，个性化的风险识别规则较为具体细致，但个人时常会受情绪或意外事件的影响改变交易习惯，从而造成个性化的风险识别规则易失真，不甚稳定。

例如，小明习惯中午去公司楼下的麦当劳吃午饭并通过客户端在线支付，但是偶尔工作太忙，没有时间下楼，只能通过客户端定其他餐厅的外卖，或小明最近吃腻了西式快餐，连续几天吃中餐并通过客户端在线支付，倘若根据历史上总结出的小明进行在线交易的风险识别规则，小明连续几天吃中餐的支付行为很可能被判定为不安全的交易行为，但实际上，小明的账号并没有被盗用。

其二，相比于手机，用户在客户端上使用的账号和密码更容易失窃。现实中大量的线上财产失窃案都是由用户的账号和密码被盗用引起的。并且，一旦盗用者使用用户的账号和密码登录客户端，也可以查看用户的交易记录，模仿用户的交易习惯进行非法支付和转账，这是根据用户的交易习惯总结出的风险识别规则所难以涵盖的。

考虑到以上情况，在本申请所要求保护的技术方案提供的一个优选实施例中，可以不仅考察用户的交易习惯进行风险识别，同时还要至少增加一个维度的考察，来增强风险识别的可靠性。

一般而言，用户进行一次交易涉及的维度有以下几个：用户标识（对应于个性化的交易习惯）、终端设备（根据用户使用终端设备的习惯，总结出终端设备与外界进行数据交互的规律）、商户（当前交易的商户）、位置（进行当前交易时的位置）、物流（当前交易指定的物流地址、收货人信息等）、介质（当前的网络环境）等。

可见，本申请所要求保护的风险识别方法，还可以通过在至少两个维度上考察通过用户标识进行的当前交易的风险度，来对当前交易的风险进行综合性

地识别。由于本申请所要求保护的技术方案的一个优选地实施例通过至少两个维度分别进行了风险识别，再根据各维度所占的权重进行总体上的风险识别，因此，本方案的风险识别方法一方面既能实现个性化地风险识别，另一方面各维度的协作也能将风险识别规则的个性化所引发的误差降到最低，增强风险识别系统的稳定性，从而提升风险识别的准确性。

当然，本申请所要求保护的技术方案还可以采用其他维度对当前交易进行考察，对当前交易在上述的各维度下进行考察的方式也可以不限于上述举例。总之，本申请的实施例可以有多种，只要可以从至少两个维度上考察通过用户标识进行的当前交易的风险即可，本申请对此不做限制。下面结合附图，对另一种多维度下的风险识别方法进行说明。

图 2 是本申请实施例提供的一种风险识别方法流程图，包括以下步骤：

S201：接收支付请求。

在本申请实施例中，所述支付请求可以携带当前交易中产生的至少一个维度的操作数据，也可以携带用户标识和通过所述用户标识在当前交易中产生的操作数据。

S202：针对每个维度，根据该维度的操作数据，确定当前交易的风险度。

如前所述，用户进行一次交易涉及的维度至少有以下四个：用户标识（对应于个性化的交易习惯）、终端设备（根据用户使用终端设备的习惯，总结出终端设备与外界进行数据交互的规律）、商户（当前交易的商户）、位置（进行当前交易时的位置）、物流（当前交易指定的物流地址、收货人信息等）、介质（当前的网络环境）等。

例如，所述用户标识的至少一个维度的操作数据可以是所述用户标识在当前交易涉及的终端设备维度下的操作数据，如终端设备每天登录的账号数，也可以是当前交易涉及的用户标识维度下的操作数据，如小明每天的购买习惯、小明登录客户端后通常会进行的一系列动作习惯，还可以是当前交易涉及的商户、位置维度下的操作数据，如商户每天交易的顾客的特征、该位置附近经常

进行交易的用户的用户特征等。

用户标识（账号）维度可以反映用户的个性化的交易习惯，当不法分子贸然盗用用户的账号进行交易时，在用户标识维度商可能露出马脚，风险识别系统识别出来。但是如前所述的两点原因，只从用户标识维度进行风险识别，准确性并不高。

此外，终端设备维度可以作为一个很好的补充，以提高风险识别的准确性。由于在当代社会，用户使用终端设备，如手机，已经到了片刻不离身的地步，不易被盗，并且，即便手机被盗，不法分子也很难通过手机的密码锁屏界面，进入到手机的操作系统中的客户端进行不法支付或转账，因此，不法分子的手段往往是通过网络黑客技术盗用用户的用户标识在其他终端设备上使用。也就是说，不法分子即便可以使用盗用的用户标识在其他终端设备上模仿用户的交易习惯进行不法交易，其使用的却并非用户经常使用的终端设备，也容易露出马脚，因而在终端设备维度上被风险识别系统识别为异常。

另一方面，将终端设备维度与用户标识维度进行结合，并根据业务经验，对这两个维度赋予在风险识别中不同的权重，形成“双保险”，经测验，可以有效提升风险识别的准确性。

例如，小明使用自己的苹果手机（假设出厂号为 A）的习惯为，每天在苹果手机 A 上的客户端登录的账号数不会超过两次，由于不法分子常常使用自己的某个手机频繁的登录不同的账号进行非法交易，因此，倘若不法分子盗用了小明的账号，使用自己的苹果手机 B 登录小明的账号，模仿小明的交易习惯，在小明经常消费的商户进行消费，那么即使在用户标识维度上，风险识别系统未能识别出这笔交易的风险，但是在终端设备维度，风险识别系统可以识别出当前交易中小明的账号登录的苹果手机 B 不是小明平时使用的苹果手机 A，并且，苹果手机 B 每天登录的账号数较多，从而判断苹果手机 B 很可能是不法分子用来进行非法交易的终端设备，在终端设备维度上将这笔交易识别为高风险的交易。此外，风险识别系统可以根据不法分子当前交易的操作数据，对小

明的用户标识对应的终端设备维度的风险参数集进行调整，使得“每天在苹果手机 A 上的客户端登录的账号数不会超过两次”这一风险参数在风险识别中所占的比重提升。

另外，不法交易涉及的商户，往往是不法分子集中进行销赃的商户，这使得商户作为一个维度，可以帮助判断当前交易的商户有多大概率是不法分子进行销赃的商户。如珠宝店 A 的平均日销售额为 50 万元，但是某段时间的日销售额稳定在 200 万元，疑似有犯罪分子集中进行线上销赃，倘若小明的账号在这段时间被同一伙犯罪分子盗用，那么风险识别系统在进行风险识别时，当检测到当前交易涉及的商户为珠宝店 A 时，会在商户维度上判断小明的账号被盗用的风险较高，即在商户维度上输出较高的风险度。

同理，在物流维度下可以识别出当前交易指定的物流信息与用户平时指定的物流信息差异是否过大，在介质维度下可以识别出当前交易的网络环境是 WIFI 还是移动数据，移动数据的服务商是移动、联通还是电信，这些信息是否与用户平时的介质信息差异过大。

在本申请实施例中，可以针对上述维度中的每一个，根据该维度的操作数据，确定当前交易的风险度。具体可以采用图 1 所示的调整风险参数的方法以及进一步进行风险识别的方法来根据操作数据确定风险度，进行风险识别，即可以根据维度（设备维度、用户维度、商户维度、位置维度中的任一种）的操作数据，确定在所述当前交易中产生的至少一个设备维度的操作跳转序列，所述设备维度的操作跳转序列中包含至少一个设备维度的操作跳转事件；根据至少一个设备维度的操作跳转序列，确定与所述设备维度的操作跳转序列中包含的所述设备维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

S203：在得到各维度对应的所述当前交易的风险度时，根据得到的不同的风险度，对所述当前交易进行风险识别。

在本申请实施例中，可以依据特定策略规则对得到的不同的风险度进行计

算，得到所述当前交易的风险系数；根据确定的所述风险系数，对所述当前交易进行风险识别。

其中，所述特定策略规则可以是对不同的风险度设定不同的权重，将各风险度进行汇总即可得到所述风险系数，也可以简单地将各风险度进行叠加处理，得到所述风险系数。总之，所述特定策略规则可以将不同的风险度进行汇总整体上反映当前交易的风险即可。

值得说明的是，由于图 2 所示的方法与图 1 所示的方法基于同样的发明构思，图 2 所示的方法中，确定每个维度上的风险度的方式，正是图 1 所示的确定当前交易的风险度的方式，只不过在图 2 所示的方法中，可以在不止一个维度上分别确定当前交易在该维度的风险度，并进一步汇总各维度的风险度来进行风险识别。

在对当前交易进行风险识别时，考察的维度越多，风险识别的准确性就越高。最后，风险操作系统可以根据确定出的各个维度的风险结果，对当前交易在总体上进行风险识别。

在图 2 所示的风险识别方法中，当服务器接收到当前交易的支付请求时，将图 1 所示的风险识别方法，在至少两个维度上分别执行一次，在各维度下分别输出该维度的风险度，最后可以根据各维度的风险度确定当前交易的风险结果（如对各维度的风险度进行归一化，确定当前交易的风险概率），从而实现对当前交易的风险识别。也可以分别根据该维度的交易特征，对该维度的风险参数进行调整。

基于图 1 所示的调整风险参数的方法，本申请实施例还对应提供了调整风险参数的装置，如图 3 所示，包括：

接收模块 301，接收支付请求，所述支付请求中包含用户标识和通过所述用户标识在当前交易中产生的操作数据；

确定模块 302，根据所述操作数据，确定在所述当前交易中产生的至少一个操作跳转序列，所述操作跳转序列中包含至少一个操作跳转事件；

获取模块 303，从所述用户标识对应的风险参数集合中，获取与所述操作跳转序列中包含的所述操作跳转事件对应的风险参数，所述风险参数集合中包含的风险参数是根据所述用户标识对应的上一次交易产生的操作数据，对在上一次交易中进行风险识别所使用的风险参数进行调整后得到的；

调整模块 304，根据所述至少一个操作跳转序列，调整获取到的所述风险参数。

所述装置还包括：识别模块 305，根据获取到的所述风险参数和所述至少一个操作跳转序列，确定当前交易的风险度；根据所述风险度，对当前交易进行风险识别。

所述调整模块 304，在确定当前交易对应的风险度高于设定阈值时，调低获取到的所述风险参数；在确定当前交易对应的风险度不高于设定阈值时，调高获取到的所述风险参数；调整后的所述风险参数用于对所述用户标识对应的下一次交易进行风险识别。

所述装置还包括：初始化模块 306，在风险识别系统进行初始化时，在接收支付请求之前，确定所述用户标识对应的操作跳转事件集以及所述操作跳转事件集中包含的各操作跳转事件对应的风险参数的初始值。

所述初始化模块 306，定义不同的节点；遍历不同所述节点之间发生的操作跳转，得到多个操作跳转事件，所述操作跳转事件中包含两个所述节点；根据所述多个操作跳转事件，得到操作跳转事件集。

所述初始化模块 306，获取通过所述用户标识产生的的历史操作数据；针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：根据所述历史操作数据，确定该操作跳转事件的发生概率；将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

所述初始化模块 306，当无法获取通过所述用户标识产生的的历史操作数据时，获取设定数量的其他用户标识产生的历史操作数据； 针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：根据所述历史操作

数据，确定该操作跳转事件的发生概率；将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

所述识别模块 305，针对各操作跳转序列，确定该操作跳转序列中包含的操作跳转事件，并根据所述操作跳转事件对应的风险参数，确定该操作跳转序列的风险值；在得到各操作跳转序列的风险值后，根据各操作跳转序列的风险值，确定当前交易的风险度。

基于图 2 所示的风险识别方法，本申请还对应提供了一种风险识别装置，如图 4 所示，包括：

接收模块 401，接收支付请求，所述支付请求中包含在当前交易中产生的至少一个维度的操作数据；

确定模块 402，针对每个维度，根据该维度的操作数据，确定当前交易的风险度；

识别模块 403，在得到各维度对应的所述当前交易的风险度时，根据得到的不同的风险度，对所述当前交易进行风险识别。

所述确定模块 402，若该维度的操作数据为设备维度的操作数据，则根据设备维度的操作数据，确定在所述当前交易中产生的至少一个设备维度的操作跳转序列，所述设备维度的操作跳转序列中包含至少一个设备维度的操作跳转事件；根据至少一个设备维度的操作跳转序列，确定与所述设备维度的操作跳转序列中包含的所述设备维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

所述确定模块 402，若该维度的操作数据为用户维度的操作数据，则根据用户维度的操作数据，确定在所述当前交易中产生的至少一个用户维度的操作跳转序列，所述用户维度的操作跳转序列中包含至少一个用户维度的操作跳转事件；根据至少一个用户维度的操作跳转序列，确定与所述用户维度的操作跳转序列中包含的所述用户维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

所述确定模块 402，若该维度的操作数据为商户维度的操作数据，则根据商户维度的操作数据，确定在所述当前交易中产生的至少一个商户维度的操作跳转序列，所述商户维度的操作跳转序列中包含至少一个商户维度的操作跳转事件；根据至少一个商户维度的操作跳转序列，确定与所述商户维度的操作跳转序列中包含的所述商户维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

所述确定模块 402，若该维度的操作数据为位置维度的操作数据，则根据位置维度的操作数据，确定在所述当前交易中产生的至少一个位置维度的操作跳转序列，所述位置维度的操作跳转序列中包含至少一个位置维度的操作跳转事件；根据至少一个位置维度的操作跳转序列，确定与所述位置维度的操作跳转序列中包含的所述位置维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

所述识别模块 403，依据特定策略规则对得到的不同的风险度进行计算，得到所述当前交易的风险系数；根据确定的所述风险系数，对所述当前交易进行风险识别。

图 5 是本申请实施例提供的一种风险识别系统的示意图，包括：

智能模块 501，获取通过用户标识在当前交易中产生的操作数据，根据所述操作数据进行风险分析，并将风险分析结果发送给风险识别模块；所述智能模块的数量为至少一个；所述风险分析结果通过上述风险识别方法得到；

风险识别模块 502，根据接收到的风险分析结果，进行风险识别。

所述智能模块 501，具体包括：

获取单元 5011，获取通过用户标识在当前交易中产生的操作数据，根据所述操作数据确定至少一个操作跳转序列，将所述至少一个操作跳转序列发送给分析单元；

分析单元 5012，根据接收到的操作跳转序列进行风险分析，并向发送单元输出风险分析结果；

发送单元5013，根据接收到的各风险分析结果，确定风险度，将所述风险度发送给风险识别模块。

图6（a）、图6（b）、图6（c）和图6（d）分别是本申请实施例提供的一种风险识别系统的详细示意图。值得强调的是，图6（a）、图6（b）、图6（c）和图6（d）所示的风险识别系统的智能模块数量最多为4，分别对应用户、终端设备、商户、位置4个维度，但是这并不构成对本申请的限制。

从图6（a）中可以看出，风险识别系统可以采集一个维度的操作数据，根据采集到的操作数据对当前交易是否存在风险进行识别。具体识别方式可以参照上述实施例中记载的内容，至于一个维度的操作数据，在图6（a）中以用户维度的操作数据为例进行说明。

从图6（b）中可以看出，风险识别系统可以采集两个维度的操作数据，根据采集到的操作数据对当前交易是否存在风险进行识别。具体识别方式可以参照上述实施例中记载的内容，至于两个维度的操作数据，在图6（b）中以用户维度的操作数据和设备维度的操作数据为例进行说明。

从图6（c）中可以看出，风险识别系统可以采集三个维度的操作数据，根据采集到的操作数据对当前交易是否存在风险进行识别。具体识别方式可以参照上述实施例中记载的内容，至于三个维度的操作数据，在图6（c）中以用户维度的操作数据、设备维度的操作数据和商户维度的操作数据为例进行说明。

从图6（d）中可以看出，风险识别系统可以采集四个维度的操作数据，根据采集到的操作数据对当前交易是否存在风险进行识别。具体识别方式可以参照上述实施例中记载的内容，至于四个维度的操作数据，在图6（d）中以用户维度的操作数据、设备维度的操作数据、商户维度的操作数据和位置维度的操作数据为例进行说明。

在图6（a）、图6（b）、图6（c）和图6（d）所示的风险识别系统中，所述分析单元针对接收到的每个操作跳转序列都会确定一个风险值，并将该风险值作为风险分析结果输出给所述发送单元，所述发送单元可以将接收到的各风

险分析结果确定风险度，并将风险度发送给所述风险识别模块进行最终决策，输出对当前交易的风险评价（如风险概率）。

在图 6（a）、图 6（b）、图 6（c）和图 6（d）所示的风险识别系统中，各智能模块可以相互联络，形成联动。例如，不法分子集中在某个商户销赃，商户维度对应的智能模块发现异常后，可以将这种新的风险告知其他智能模块，其他智能模块可以及时根据这种新的风险调整自己的风险识别策略。由于风险识别系统具有这种模块间的反馈机制，可以使得各模块的风险参数集合始终保持最新，能够更快响应于最新的线上风险，进行更为准确的风险识别。

图 6（a）、图 6（b）、图 6（c）和图 6（d）所示的风险识别系统具有较强的鲁棒性。也就是说，由于风险识别系统可以包括一个以上的智能模块，当某个智能模块发生异常时，不会对其他智能模块产生影响，风险识别模块依然可以接收到至少一个智能模块发送的风险度，进行风险识别。

此外，图 6（a）、图 6（b）、图 6（c）和图 6（d）所示的风险识别系统还可以具有对应的测试系统，即采用 A/B Test 上线模式，测试系统与所述风险识别系统拥有相同的架构，测试系统只对较少的用户标识对应的交易进行风险识别，当新的风险出现时，可以先在测试系统上进行补防，待风控人员观察测试系统的表现是否稳定后，再决定是否对所述风险识别系统进行同样的补防。

在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array, FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设

计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件

部件内的结构。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处

理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

还需要说明的是，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、商品或者设备不仅包括那些要素，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、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算

机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种调整风险参数的方法，其特征在于，包括：

接收支付请求，所述支付请求中包含用户标识和通过所述用户标识在当前交易中产生的操作数据；

根据所述操作数据，确定在所述当前交易中产生的至少一个操作跳转序列，所述操作跳转序列中包含至少一个操作跳转事件；

从所述用户标识对应的风险参数集合中，获取与所述操作跳转序列中包含的所述操作跳转事件对应的风险参数，所述风险参数集合中包含的风险参数是根据所述用户标识对应的上一次交易产生的操作数据，对在上一次交易中进行风险识别所使用的风险参数进行调整后得到的；

根据所述至少一个操作跳转序列，调整获取到的所述风险参数。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

根据获取到的所述风险参数和所述至少一个操作跳转序列，确定当前交易的风险度；

根据所述风险度，对当前交易进行风险识别。

3、根据权利要求 2 所述的方法，其特征在于，根据所述至少一个操作跳转序列，调整获取到的所述风险参数，包括：

在确定当前交易对应的风险度高于设定阈值时，调低获取到的所述风险参数；

在确定当前交易对应的风险度不高于设定阈值时，调高获取到的所述风险参数；

调整后的所述风险参数用于对所述用户标识对应的下一次交易进行风险识别。

4、根据权利要求 2 所述的方法，其特征在于，在接收支付请求之前，所述方法还包括：

在风险识别系统进行初始化时，确定所述用户标识对应的操作跳转事件集

以及所述操作跳转事件集中包含的各操作跳转事件对应的风险参数的初始值。

5、根据权利要求 4 所述的方法，其特征在于，确定操作跳转事件集，包括：

定义不同的节点；

遍历不同所述节点之间发生的操作跳转，得到多个操作跳转事件，所述操作跳转事件中包含两个所述节点；

根据所述多个操作跳转事件，得到操作跳转事件集。

6、根据权利要求 4 所述的方法，其特征在于，确定所述操作跳转事件集中包含的各操作跳转事件对应的风险参数的初始值，包括：

获取通过所述用户标识产生的的历史操作数据；

针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：

根据所述历史操作数据，确定该操作跳转事件的发生概率；

将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

7、根据权利要求 4 所述的方法，其特征在于，确定所述操作跳转事件集中包含的各操作跳转事件对应的风险参数的初始值，包括：

当无法获取通过所述用户标识产生的的历史操作数据时，获取设定数量的其他用户标识产生的历史操作数据；

针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：

根据所述历史操作数据，确定该操作跳转事件的发生概率；

将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

8、根据权利要求 6 或 7 所述的方法，其特征在于，根据获取到的所述风险参数和所述至少一个操作跳转序列，确定当前交易的风险度，包括：

针对各操作跳转序列，确定该操作跳转序列中包含的操作跳转事件，并根据所述操作跳转事件对应的风险参数，确定该操作跳转序列的风险值；

在得到各操作跳转序列的风险值后，根据各操作跳转序列的风险值，确定当前交易的风险度。

9、一种风险识别方法，其特征在于，包括：

接收支付请求，所述支付请求中包含在当前交易中产生的至少一个维度的操作数据；

针对每个维度，根据该维度的操作数据，确定所述当前交易的风险度；

在得到各维度对应的所述当前交易的风险度时，根据得到的不同的风险度，对所述当前交易进行风险识别。

10、根据权利要求9所述的方法，其特征在于，根据该维度的操作数据，确定所述当前交易的风险度，具体包括：

若该维度的操作数据为设备维度的操作数据，则根据设备维度的操作数据，确定在所述当前交易中产生的至少一个设备维度的操作跳转序列，所述设备维度的操作跳转序列中包含至少一个设备维度的操作跳转事件；

根据至少一个设备维度的操作跳转序列，确定与所述设备维度的操作跳转序列中包含的所述设备维度的操作跳转事件对应的风险参数；

根据所述风险参数，确定所述当前交易的风险度。

11、根据权利要求10所述的方法，其特征在于，根据该维度的操作数据，确定所述当前交易的风险度，具体包括：

若该维度的操作数据为用户维度的操作数据，则根据用户维度的操作数据，确定在所述当前交易中产生的至少一个用户维度的操作跳转序列，所述用户维度的操作跳转序列中包含至少一个用户维度的操作跳转事件；

根据至少一个用户维度的操作跳转序列，确定与所述用户维度的操作跳转序列中包含的所述用户维度的操作跳转事件对应的风险参数；

根据所述风险参数，确定所述当前交易的风险度。

12、根据权利要求11所述的方法，其特征在于，根据该维度的操作数据，确定所述当前交易的风险度，具体包括：

若该维度的操作数据为商户维度的操作数据，则根据商户维度的操作数据，确定在所述当前交易中产生的至少一个商户维度的操作跳转序列，所述商户维度的操作跳转序列中包含至少一个商户维度的操作跳转事件；

根据至少一个商户维度的操作跳转序列，确定与所述商户维度的操作跳转序列中包含的所述商户维度的操作跳转事件对应的风险参数；

根据所述风险参数，确定所述当前交易的风险度。

13、根据权利要求 12 所述的方法，其特征在于，根据该维度的操作数据，确定所述当前交易的风险度，具体包括：

若该维度的操作数据为位置维度的操作数据，则根据位置维度的操作数据，确定在所述当前交易中产生的至少一个位置维度的操作跳转序列，所述位置维度的操作跳转序列中包含至少一个位置维度的操作跳转事件；

根据至少一个位置维度的操作跳转序列，确定与所述位置维度的操作跳转序列中包含的所述位置维度的操作跳转事件对应的风险参数；

根据所述风险参数，确定所述当前交易的风险度。

14、根据权利要求 9 所述的方法，其特征在于，根据得到的不同的风险度，对所述当前交易进行风险识别，具体包括：

依据特定策略规则对得到的不同的风险度进行计算，得到所述当前交易的风险系数；

根据确定的所述风险系数，对所述当前交易进行风险识别。

15、一种调整风险参数的装置，其特征在于，包括：

接收模块，接收支付请求，所述支付请求中包含用户标识和通过所述用户标识在当前交易中产生的操作数据；

确定模块，根据所述操作数据，确定在所述当前交易中产生的至少一个操作跳转序列，所述操作跳转序列中包含至少一个操作跳转事件；

获取模块，从所述用户标识对应的风险参数集合中，获取与所述操作跳转序列中包含的所述操作跳转事件对应的风险参数，所述风险参数集合中包含的

风险参数是根据所述用户标识对应的上一次交易产生的操作数据，对在上一次交易中进行风险识别所使用的风险参数进行调整后得到的；

调整模块，根据所述至少一个操作跳转序列，调整获取到的所述风险参数。

16、根据权利要求 15 所述的装置，其特征在于，所述装置还包括：识别模块，其中：

所述识别模块，根据获取到的所述风险参数和所述至少一个操作跳转序列，确定当前交易的风险度；根据所述风险度，对当前交易进行风险识别。

17、根据权利要求 16 所述的装置，其特征在于，

所述调整模块，在确定当前交易对应的风险度高于设定阈值时，调低获取到的所述风险参数；在确定当前交易对应的风险度不高于设定阈值时，调高获取到的所述风险参数；调整后的所述风险参数用于对所述用户标识对应的下一次交易进行风险识别。

18、根据权利要求 16 所述的装置，其特征在于，所述装置还包括：初始化模块，其中：

所述初始化模块，在风险识别系统进行初始化时，在接收支付请求之前，确定所述用户标识对应的操作跳转事件集以及所述操作跳转事件集中包含的各操作跳转事件对应的风险参数的初始值。

19、根据权利要求 19 所述的装置，其特征在于，

所述初始化模块，定义不同的节点；遍历不同所述节点之间发生的操作跳转，得到多个操作跳转事件，所述操作跳转事件中包含两个所述节点；根据所述多个操作跳转事件，得到操作跳转事件集。

20、根据权利要求 19 所述的装置，其特征在于，

所述初始化模块，获取通过所述用户标识产生的的历史操作数据；针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：根据所述历史操作数据，确定该操作跳转事件的发生概率；将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

21、根据权利要求 19 所述的装置，其特征在于，

所述初始化模块，当无法获取通过所述用户标识产生的的历史操作数据时，获取设定数量的其他用户标识产生的历史操作数据；针对所述操作跳转事件集中包含的每个操作跳转事件，分别执行以下操作：根据所述历史操作数据，确定该操作跳转事件的发生概率；将所述发生概率作为该操作跳转事件对应的风险参数的初始值。

22、根据权利要求 19 或 20 所述的装置，其特征在于，

所述识别模块，针对各操作跳转序列，确定该操作跳转序列中包含的操作跳转事件，并根据所述操作跳转事件对应的风险参数，确定该操作跳转序列的风险值；在得到各操作跳转序列的风险值后，根据各操作跳转序列的风险值，确定当前交易的风险度。

23、一种风险识别装置，其特征在于，包括：

接收模块，接收支付请求，所述支付请求中包含在当前交易中产生的至少一个维度的操作数据；

确定模块，针对每个维度，根据该维度的操作数据，确定当前交易的风险度；

识别模块，在得到各维度对应的所述当前交易的风险度时，根据得到的不同的风险度，对所述当前交易进行风险识别。

24、根据权利要求 23 所述的装置，其特征在于，所述确定模块，若该维度的操作数据为设备维度的操作数据，则根据设备维度的操作数据，确定在所述当前交易中产生的至少一个设备维度的操作跳转序列，所述设备维度的操作跳转序列中包含至少一个设备维度的操作跳转事件；根据至少一个设备维度的操作跳转序列，确定与所述设备维度的操作跳转序列中包含的所述设备维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

25、根据权利要求 24 所述的装置，其特征在于，所述确定模块，若该维

度的操作数据为用户维度的操作数据，则根据用户维度的操作数据，确定在所述当前交易中产生的至少一个用户维度的操作跳转序列，所述用户维度的操作跳转序列中包含至少一个用户维度的操作跳转事件；根据至少一个用户维度的操作跳转序列，确定与所述用户维度的操作跳转序列中包含的所述用户维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

26、根据权利要求 25 所述的装置，其特征在于，所述确定模块，若该维度的操作数据为商户维度的操作数据，则根据商户维度的操作数据，确定在所述当前交易中产生的至少一个商户维度的操作跳转序列，所述商户维度的操作跳转序列中包含至少一个商户维度的操作跳转事件；根据至少一个商户维度的操作跳转序列，确定与所述商户维度的操作跳转序列中包含的所述商户维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

27、根据权利要求 26 所述的装置，其特征在于，所述确定模块，若该维度的操作数据为位置维度的操作数据，则根据位置维度的操作数据，确定在所述当前交易中产生的至少一个位置维度的操作跳转序列，所述位置维度的操作跳转序列中包含至少一个位置维度的操作跳转事件；根据至少一个位置维度的操作跳转序列，确定与所述位置维度的操作跳转序列中包含的所述位置维度的操作跳转事件对应的风险参数；根据所述风险参数，确定所述当前交易的风险度。

28、根据权利要求 23 所述的装置，其特征在于，所述识别模块，依据特定策略规则对得到的不同的风险度进行计算，得到所述当前交易的风险系数；根据确定的所述风险系数，对所述当前交易进行风险识别。

29、一种风险识别系统，包括：

至少一个智能模块，接收交易请求，获取通过用户标识在当前交易中产生的操作数据，根据所述操作数据进行风险分析，并将风险分析结果发送给风险

识别模块；所述风险分析结果通过权利要求 1 至 8 所述的方法得到；

风险识别模块，根据接收到的风险分析结果，进行风险识别。

30、根据权利要求 29 所述的系统，其特征在于，所述智能模块，具体包括：

获取单元，获取通过用户标识在当前交易中产生的操作数据，根据所述操作数据确定至少一个操作跳转序列，将所述至少一个操作跳转序列发送给分析单元；

分析单元，根据接收到的操作跳转序列进行风险分析，并向发送单元输出风险分析结果；

发送单元，根据接收到的各风险分析结果确定风险度，将所述风险度发送给风险识别模块。