

阈值确定及核身方法、装置、电子设备及存储介质

技术领域

[01]本公开涉及计算机技术领域，具体涉及一种阈值确定及核身方法、装置、电子设备及存储介质。

5 背景技术

[02]现代风控体系对系统的安全性和用户的体验都提出了更高的要求。核身作为风控决策的重要手段和依据已成为风控的重要组成部分。常用的核身装置通常有多种产品支持，包括短信验证、身份证号、银行卡绑卡、KBA 问答、生物核身等。从核身的管控强度上来说，各种校验方式有强弱之分，另外，在金融领域为保证用户安全通常还会使用叠加方式进行多重多次核身。

[03]核身就像是一把双刃剑，强度较高的校验方式将行为异常的用户拒之门外的同时也给正常的用户造成了一定的打扰，低强度的校验会造成风险的蔓延，并使得部分用户觉得缺乏安全感。目前的多数改密核身都采用单一的核身强度进行校验，未考虑到用户的个人差异造成的对核身需求的多元化。比如，有的用户不喜欢被强校验，对于总是被强校验体验不好最终可能导致用户流失；有的用户不喜欢被弱校验，因为用户会觉得这种弱校验方式容易导致黑客侵入个人账户，没有安全感。以修改密码的场景为例，当用户忘记了账户密码时，系统通常通过核身验证当前是本人在操作时才可以让用户重置密码或获取原密码。

发明内容

[04]本公开实施例提供一种阈值确定及核身方法、装置、电子设备及计算机可读存储介质。

[05]第一方面，本公开实施例中提供了一种阈值确定方法，包括：

[06]获取多个核身识别模型分别对应的预设目标值；其中，所述预设目标值用于表示所述核身识别模型被期望达到的目标识别能力；

[07]根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值；其中，所述用户业务变量值用于划分活跃用户和不活跃用户，所述核身阈值被

所述核身识别模型用于从所述不活跃用户中剔除需要强校验的用户。

[08]进一步地, 根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值, 包括:

5 [09]将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标, 通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值。

10 [10]进一步地, 将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标, 通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值, 包括:

[11]利用所述用户业务变量值、多个所述核身识别模型分别对应的所述核身阈值构建解向量;

15 [12]以所述用户业务变量值所划分的不活跃用户的范围最大化作为所述优化算法的约束条件, 分别以多个所述核身识别模型对应的所述核身阈值小于其对应的所述预设目标值作为所述优化算法的目标函数, 对所述解向量进行求解。

[13]进一步地, 所述核身识别模型包括: 盗用风险识别模型、安全感识别模型和/或篡改动机异常识别模型; 其中, 所述盗用风险识别模型用于识别账户被盗用的可能性; 所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度; 所述篡改动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

20 [14]第二方面, 本公开实施例中提供了一种核身方法, 包括:

[15]响应于核身请求, 根据用户业务变量值确定待核身用户是否为不活跃用户;

[16]在所述待核身用户为不活跃用户时, 确定多个核身识别模型中的至少一个对所述待核身用户的识别结果;

25 [17]根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式; 其中, 所述核身方式包括弱校验核身方式和强校验核身方式; 所述用户业务变量值以及所述核身阈值采用上述阈值确定方法得到;

[18]采用所述核身方式对所述待核身用户进行核身。

[19]进一步地, 所述核身识别模型包括: 盗用风险识别模型、安全感识别模型和/或篡改

动机异常识别模型；其中，所述盗用风险识别模型用于识别账户被盗用的可能性；所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

5 [20]进一步地，根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式，包括：

[21]根据第一识别结果以及所述盗用风险识别模型对应的所述核身阈值确定所述待核身用户的第一核身方式，根据第二识别结果以及所述安全感识别模型对应的所述核身阈值确定所述待核身用户的第二核身方式，并根据第三识别模型以及所述改密动机异常识别模型对应的所述核身阈值确定所述待核身用户的第三核身方式；其中，所述第一识别结果、第二识别结果和第三识别结果分别为所述盗用风险识别模型、安全感识别模型和改密动机异常识别模型对所述待核身用户的识别结果；

10

[22]在所述第一核身方式、第二核身方式以及第三核身方式均为弱校验核身方式时，确定所述待核身用户的核身方式为弱校验核身方式。

[23]进一步地，根据所述识别结果以及对应的所述核身阈值确定所述待核身用户的核身方式，还包括：

15

[24]在所述第一核身方式、第二核身方式以及第三核身方式中的至少一个为强校验核身方式时，确定所述待核身用户的核身方式为强校验核身方式。

[25]第三方面，本公开实施例提供了一种阈值确定装置，包括：

[26]获取模块，被配置为获取多个核身识别模型分别对应的预设目标值；其中，所述预设目标值用于表示所述核身识别模型被期望达到的目标识别能力；

20

[27]第一确定模块，被配置为根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值；其中，所述用户业务变量值用于划分活跃用户和不活跃用户，所述核身阈值被所述核身识别模型用于从所述不活跃用户中剔除需要强校验的用户。

25 [28]进一步地，所述第一确定模块，包括：

[29]优化子模块，被配置为将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标，通过优化算法确定所述用户业务变量值以及所述核身识别模型

对应的所述核身阈值。

[30]进一步地，所述优化子模块，包括：

[31]构建子模块，被配置为利用所述用户业务变量值、多个所述核身识别模型分别对应的所述核身阈值构建解向量；

- 5 [32]求解子模块，被配置为以所述用户业务变量值所划分的不活跃用户的范围最大化作为所述优化算法的约束条件，分别以多个所述核身识别模型对应的所述核身阈值小于其对应的所述预设目标值作为所述优化算法的目标函数，对所述解向量进行求解。

- [33]进一步地，所述核身识别模型包括：盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型；其中，所述盗用风险识别模型用于识别账户被盗用的可能性；所述
10 安全感识别模型用于识别用户对于账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

[34]所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。

- [35]在一个可能的设计中，阈值确定装置的结构中包括存储器和处理器，所述存储器用于存储一条或多条支持阈值确定装置执行上述第一方面中阈值确定方法的计算机指令，
15 所述处理器被配置为用于执行所述存储器中存储的计算机指令。所述阈值确定装置还可以包括通信接口，用于阈值确定装置与其他设备或通信网络通信。

[36]第四方面，本公开实施例中提供了一种核身装置，包括：

- [37]第二确定模块，被配置为响应于核身请求，根据用户业务变量值确定待核身用户是
20 否为不活跃用户；

[38]第三确定模块，被配置为在所述待核身用户为不活跃用户时，确定多个核身识别模型中的至少一个对所述待核身用户的识别结果；

- [39]第四确定模块，被配置为根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式；其中，所述核身方式包括弱校验
25 核身方式和强校验核身方式；所述用户业务变量值以及所述核身阈值采用上述阈值确定装置得到；

[40]核身模块，被配置为采用所述核身方式对所述待核身用户进行核身。

[41]进一步地，所述核身识别模型包括：盗用风险识别模型、安全感识别模型和/或改密

动机异常识别模型；其中，所述盗用风险识别模型用于识别账户被盗用的可能性；所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

[42]进一步地，所述第四确定模块，包括：

- 5 [43]第一确定子模块，被配置为根据第一识别结果以及所述盗用风险识别模型对应的所述核身阈值确定所述待核身用户的第一核身方式，根据第二识别结果以及所述安全感识别模型对应的所述核身阈值确定所述待核身用户的第二核身方式，并根据第三识别模型以及所述改密动机异常识别模型对应的所述核身阈值确定所述待核身用户的第三核身方式；其中，所述第一识别结果、第二识别结果和第三识别结果分别为所述盗用风险识别模型、安全感识别模型和改密动机异常识别模型对所述待核身用户的识别结果；

[44]第二确定子模块，被配置为在所述第一核身方式、第二核身方式以及第三核身方式均为弱校验核身方式时，确定所述待核身用户的核身方式为弱校验核身方式。

[45]进一步地，所述第四确定模块，还包括：

- 15 [46]第三确定子模块，被配置为在所述第一核身方式、第二核身方式以及第三核身方式中的至少一个为强校验核身方式时，确定所述待核身用户的核身方式为强校验核身方式。

[47]所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。

- 20 [48]在一个可能的设计中，核身装置的结构中包括存储器和处理器，所述存储器用于存储一条或多条支持核身装置执行上述第二方面中核身方法的计算机指令，所述处理器被配置为用于执行所述存储器中存储的计算机指令。所述核身装置还可以包括通信接口，用于核身装置与其他设备或通信网络通信。

[49]第五方面，本公开实施例提供了一种电子设备，包括存储器和处理器；其中，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行以实现第一方面或第二方面所述的方法步骤。

- 25 [50]第六方面，本公开实施例提供了一种计算机可读存储介质，用于存储阈值确定装置或核身装置所用的计算机指令，其包含用于执行上述第一方面中阈值确定方法或第二方面中核身方法所涉及的计算机指令。

[51]本公开实施例提供的技术方案可以包括以下有益效果：

[52]本公开实施例在核身过程中，为了平衡多种不同核身识别模型对用户核身方式的识别结果，通过获取多个不同核身识别模型所要达到的目标识别能力，并根据该目标识别能力确定用于划分活跃用户和不活跃用户的用户业务变量值以及核身识别模型的核身阈值，以便将不活跃用户的范围最大化的同时，能够从不活跃用户中识别出具有风险的

5 用户，也即这样既能满足不活跃用户的弱校验核身需求，又能从中识别出需采用强校验核身的用户，能够实现用户体验和风险控制的平衡。

[53]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

10 [54]结合附图，通过以下非限制性实施方式的详细描述，本公开的其它特征、目的和优点将变得更加明显。在附图中：

[55]图 1 示出根据本公开一实施方式的阈值确定方法的流程图；

[56]图 2 示出根据本公开一实施方式的阈值确定方法中优化算法的流程图；

[57]图 3 示出根据本公开一实施方式的核身方法的流程图；

15 [58]图 4 示出根据图 3 所示实施方式的步骤 303 的流程图；

[59]图 5 示出根据本公开一实施方式的阈值确定装置的结构框图；

[60]图 6 示出根据本公开一实施方式的阈值确定装置中优化算法的结构框图；

[61]图 7 示出根据本公开一实施方式的核身装置的结构框图；

[62]图 8 示出根据图 7 所示实施方式的第四确定模块 703 的结构框图；

20 [63]图 9 是适于用来实现根据本公开一实施方式的阈值确定方法的电子设备的结构示意图。

具体实施方式

[64]下文中，将参考附图详细描述本公开的示例性实施方式，以使本领域技术人员可容易地实现它们。此外，为了清楚起见，在附图中省略了与描述示例性实施方式无关的部分。

25

[65]在本公开中，应理解，诸如“包括”或“具有”等的术语旨在指示本说明书中所公

开的特征、数字、步骤、行为、部件、部分或其组合的存在，并且不欲排除一个或多个其他特征、数字、步骤、行为、部件、部分或其组合存在或被添加的可能性。

[66]另外还需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本公开。

- 5 [67]对于核身强弱的把握，主要有三个问题需要解决。第一，希望给什么样的用户体验优先；比如为了拉动新用户使用产品，希望对新用户或者不太活跃的用户进行高体验核身，因此这部分用户将被给予单因子核身；第二，当前采取简单核身的这部分用户是否具有风险；比如希望只对当前账户识别为安全的进行单因子弱校验，比如要求改密用户提供身份证号或者手机短信验证码即可方便地通过验证，对于不确定安全的进行多因子
- 10 强校验，比如在用户提供短信验证码之外，额外需通过人脸校验；第三，在给定的风险范围内，如何最大化体验优先用户的比例，换言之，如何通过提高用户体验更好地为用户服务这个目标。本公开实施例提出了一种阈值确定方法，可以通过一定条件的约束，可以自动调整单因子核身等弱校验用户的比例，实现用户体验和风险控制的平衡。例如，在同样的案件浓度约束条件下，已有的方案可能只能让 5%的用户享受简单便捷的单因
- 15 子核身等弱校验体验，但是经过本公开实施例提出的区域确定方法得到的用户业务变量和核身阈值，能够使得 10%的用户单因子核身。

[68]图 1 示出根据本公开一实施方式的阈值确定方法的流程图。如图 1 所示，所述阈值确定方法包括以下步骤 S101-S102:

- [69]在步骤 S101 中，获取多个核身识别模型分别对应的预设目标值；其中，所述预设
- 20 目标值用于表示所述核身识别模型被期望达到的目标识别能力；

[70]在步骤 S102 中，根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值；其中，所述用户业务变量值用于划分活跃用户和不活跃用户，所述核身阈值被所述核身识别模型用于从所述不活跃用户中剔除需要强校验的用户。

- [71]本实施例中，核身识别模型可以基于用户的特征和/或账户的特征识别该用户的账户
- 25 是否存在核身风险，如果存在则采用强校验核身，否则采用弱校验核身；也即核身识别模型用于识别该用户的账户采用强校验还是弱校验进行核身。强校验核身是指在核实用户身份时，采用多重因子进行校验的方式，而弱校验核身是指采用单个或者少数几个因子对用户身份进行核实校验的方式，弱校验核身采用的因子数量少于强校验核身采用的因子数量，且弱校验核身采用的校验强度小于强校验核身。例如，弱校验核身采用身份

证号或者手机短信验证码等因子进行校验；而强校验核身采用的因子除了身份证号和/或手机短信验证码等之外，还采用人脸等强因子。

[72]多个核身识别模型可以从多个不同方面对用户账户进行识别，也即不同的核身识别模型可以基于用户和/或账户的不同特征识别账户的不同核身风险。例如，识别账户是否
5 被盗的模型、识别用户安全感强弱的模型（如果用户安全感特强，则存在核身风险）、识别用户改密动机异常的模型等。核身识别模型可以基于用户和/或账户的特征对用户账户进行打分，并根据打分的高低来判断账户所存在的风险。

[73]预设目标值可以是预先设定好的、与所述核身识别模型所要达到的目标识别能力相关的值，也即预设目标值可以认为是对于核身识别模型识别准确率或识别错误率的一个
10 期望值。在一实施例中，预设目标值可以是期望核身识别模型能够从众多用户中识别出风险用户的准确率。在另一实施例中，预设目标值可以是期望核身识别模型无法从众多用户中识别出风险用户的错误率。无论是目标识别准确率还是目标识别错误率，预设目标值都是用于表示核身识别模型的识别能力所要达到的目标期望值。预设目标值可以基于业务经验以及业务需求等预先设置，例如，当前业务涉及金融等安全级别较高的账户
15 时，可以设置一预设目标值，使得核身识别模型的识别能力较高，而如果当前业务仅涉及论坛等安全级别较低的账户时，可以设置另一预设目标值使得核身识别模型的识别能力较低。

[74]本实施例中，用户业务变量值可以用于衡量用户的活跃程度，通过用户业务变量值可以将当前业务系统中的用户划分为活跃用户和不活跃用户。活跃用户可以为经常在当前业务系统中执行一些操作的用户，例如浏览、发文章、购物、支付等操作行为，而不
20 活跃用户可以为从来未在当前业务系统执行过任何操作或者最近一段时间内执行操作的次数较低的用户。例如，对于第三方支付系统，用户业务变量值可以设置为用户的支付次数，在所述用户业务变量值较大时，被划分成不活跃用户的占比较高，在所述用户业务变量值较小时，被划分为不活跃用户的占比较低。

[75]本实施例中，核身阈值是核身识别模型所输出的模型分值的阈值，例如，在核身阈值确定了的情况下，利用核实识别模型对用户进行识别时，如果输出的模型分值小于（或大于）该核身阈值，则认为该用户不是风险用户，可以采用弱校验核身方式；而如果输出的模型分值大于或等于（或小于或等于）核身阈值，则认为该用户是风险用户，
25 可以采用强校验核身方式。核身阈值的大小与被核身识别模型识别为风险用户的比例相关，也与核身模型识别模型的识别错误率或识别准确率相关，在核身阈值较大时，被识
30

别为风险用户比例会较低（或较高），但是识别错误率较高（或者识别错误率较低）；而在核身阈值较小时，被识别为风险用户的比例会较高（或较低），但是识别错误率较低（或者识别错误率较高）。核身阈值与被核身识别模型识别为风险用户的比例呈正比还是呈反比，或者说核身阈值与核身识别模型的识别错误率（或者识别准确率）呈正比还是呈反比，可以根据实际情况设置，对此不做限制。

[76]用户业务变量值用于划分活跃用户和不活跃用户。核身方式可以包括强校验核身和弱校验核身，而为了给用户更好地体验，通常较为简单的做法就是对于不活跃用户采用弱校验，对于活跃用户采用强校验。但是这样一刀切的做法可能会存在一些隐患，以修改密码为例，不活跃用户的账号可能存在盗号风险，如果不活跃用户全部采用弱校验核身方式，很有可能出现盗号风险。因此，本公开实施例通过用户业务变量值筛选出不活跃用户（例如设置用户业务变量值为用户在一段时间内的支付次数，如果支付次数少于设定值，则可以被认为是不活跃用户），之后再利用核身识别模型及其对应的核身阈值从不活跃用户中剔除风险用户（也即识别不活跃用户是否存在风险，如果存在风险则采用强校验方式），最终对剩下的不活跃用户进行弱校验。

[77]在已有技术中，通过经验或者测试等方式单独确定不同核身识别模型的核身阈值以及用户业务变量值，且各个不同的核身识别模型对于用户的识别是各自独立的，相互不受影响。而本公开实施例为了给更多地用户提供弱校验这种高体验服务，同时又能够将风险降到最低，而采取了预先设置各个核身识别模型所要达到的预设目标值，并采用这些预设目标值确定用户业务变量值以及各个核身识别模型的核身阈值，使得各个核身识别模型的识别能力能够满足预设目标值的同时，将采用弱校验核身方式的不活跃用户范围最大化。本公开实施例通过预设目标值确定用户业务变量以及核身阈值，不但综合考虑了多种核身识别模型以及用户业务变量对风险用户的划分，并且还在各个核身识别模型间达到了一定的平衡，能够提高用户体验。

[78]本公开实施例在核身过程中，为了平衡多种不同核身识别模型对用户核身方式的识别结果，通过获取多个不同核身识别模型所要达到的目标识别能力，并根据该目标识别能力确定核身识别模型的核身阈值以及用于划分活跃用户和不活跃用户的用户业务变量值，以便将不活跃用户的范围最大化的同时，能够从不活跃用户中识别出具有风险的用户，这样既能满足不活跃用户的弱校验核身需求，又能从中识别出需采用强校验核身的用户，能够实现用户体验和风险控制的平衡。

[79]在本实施例的一个可选实现方式中，所述步骤 S103，即根据所述预设目标值确定用

户业务变量值以及多个所述核身识别模型分别对应的核身阈值的步骤，进一步包括以下步骤：

[80]将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标，
5 通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值。

[81]该可选的实现方式中，基于让更多的用户享受弱校验核身的高体验服务，同时又能够尽量保证享受弱校验核身服务的用户为无风险用户（无风险用户可以理解为应该采用强校验的用户，比如盗用他人账户的用户、缺乏安全感需要强校验的用户等）。为了达到用户的高体验和低风险两者之间的平衡，本公开实施例预先设定各个核身识别模型的
10 预设目标值，预设目标值用于表示期望核身识别模型能够达到的识别能力，而训练好的核身识别模型的识别能力可以通过核身阈值调整，核身识别模型通过对用户的特征和/或用户账户的特征进行识别，会得出一个模型分数，而模型分数的高低与该用户的风险高低相关，核身阈值可以设置为介于模型分数最大值和最小值中间，模型分数越高代表用户风险越高的情况下，核身阈值设置越大，则核身识别模型的识别能力越弱（模型分
15 数越高代表用户风险越低的情况下，核身阈值设置越小，则核身识别模型的识别能力越弱）；相反地，核身阈值设置越小，则核身识别模型的识别能力越强。因此可以为核身识别模型找到一个最优的核身阈值，能够使得核身识别模型的识别能力尽量靠近预设目标识别值。由于本公开使用多个核身识别模型对不活跃用户进行识别，同时还希望能够给更多的不活跃用户弱校验核身的服务体验，因此并非简单地将核身识别模型的核身阈
20 值设置为预设目标值，也没有通过经验或者统计等方式直接设置用户业务变量值，而是采用优化算法同时优化用户业务变量值以及多个核身识别模型分别对应的多个核身阈值，并且优化得到的用户业务变量值以及多个核身阈值能够兼顾用户体验以及用户低风险两个问题，达到两者之间的平衡。

[82]本公开实施例在优化用户业务变量以及多个核身识别模型分别对应的多个核身阈值
25 的过程中，将核身阈值与对应的预设目标值之间的差距最小、根据用户业务变量值所划分的不活跃用户的范围最大化作为优化算法的目标，通过优化算法优化得到用户业务变量值以及核身阈值。在一实施例中，优化算法可以采用 PSO（粒子群优化算法，Particle Swarm Optimization）。PSO 优化算法是一种基于种群的随机优化技术，其通过模仿昆虫、兽群、鸟群和鱼群等的群集行为，这些群体按照一种合作的方式寻找食物，群体中的
30 每个成员通过学习它自身的经验和其他成员的经验来不断改变其搜索模式，也即本公

开采用 PSO 算法, 将用户业务变量值以及各个核身阈值构成的目标函数的不同取值作为一个种群中的粒子, 通过不断迭代优化各个粒子在目标空间中的最优取值, 每次迭代的过程中粒子都从群体和个体角度出发找到自身的最优值, 最终找到粒子在目标空间中从群体和个体角度出发都最优的一个取值。通过这种算法优化得到的用户业务变量值、
5 各个核身阈值能够使得采用弱校验核身的不活跃用户的范围最大化, 同时还能够从中识别出具有风险的用户, 在用户体验和账户风险之间达到了一定的平衡。

[83]在其他实施例, 还可以采用其他解决类似问题的优化算法, 例如 ACO(蚁群算法)、Defferential Evolution (差分进化算法) 等, 具体可根据实际情况选择使用, 在此不做限制。

10 [84]在本实施例的一个可选实现方式中, 如图 2 所示, 所述将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标, 通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值的步骤, 进一步包括以下步骤 S201-S202:

15 [85]在步骤 S201 中, 利用所述用户业务变量值、多个所述核身识别模型分别对应的所述核身阈值构建解向量;

[86]在步骤 S202 中, 以所述用户业务变量值所划分的不活跃用户的范围最大化作为所述优化算法的约束条件, 分别以多个所述核身识别模型对应的所述核身阈值小于其对应的所述预设目标值作为所述优化算法的目标函数, 对所述解向量进行求解。

20 [87]该可选的实现方式中, 可以将用户业务变量值、各个核身识别模型对应的核身阈值作为变量构建一解向量。例如, 用户业务变量值用户 C 表示, 核身识别模型 i 的核身阈值用 Y_i ($i \geq 1$) 表示, 解向量可表示为 $S=[C, Y_1, Y_2, \dots, Y_i, \dots]$ 。在选定优化算法以后, 可以将用户业务变量值所划分的不活跃用户的范围最大化作为优化算法的约束条件, 并分别以多个核身阈值小于对应的预设目标值为目标函数, 执行优化算法确定用
25 户业务变量值和核身阈值。优化算法在执行过程中, 会在保证用户业务变量值最大化(用户业务变量值越大不活跃用户的划分范围越大的情况, 相反, 如果用户变量值越小, 不活跃用户的划分范围越小的情况下要以用户业务变量值最小化为约束条件) 的前提下, 使得各个核身阈值小于预设目标值, 且无限接近于预设目标值。例如, 采用 PSO 优化算法优化时, 假如构建的向量为 $S=[C, Y_1, Y_2, \dots, Y_i, \dots]$, 则适应性值函数可以
30 构建为 $p=C-(Y_1-y_1)-(Y_2-y_2)-\dots-(Y_i-y_i)-\dots$ (仅用于举例, 实际应用中可以

根据实际情况构建), y_1 、 y_2 、...、 y_i 、... 分别为核身识别模型 1、2、...、 i 、... 的预设目标值; PSO 优化算法通过寻找 p 的取值, 使得该取值在群体和个体中都是最优, 并采用更新函数对 p 进行更新后, 迭代执行上述步骤, 直到达到迭代终止条件 (例如迭代次数达到预设阈值) 为止。最终得到的 p 对应的 C 和 Y_i 就是用户业务变量值和核身阈值的最优解。

- [88]在本实施例的一个可选实现方式中, 所述核身识别模型包括: 盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型; 其中, 所述盗用风险识别模型用于识别账户被盗用的可能性; 所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度; 所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。
- 10 [89]本实施例中, 盗用风险识别模型可以是实时识别模型, 主要用于对用户当前的改密行为进行风险识别。若识别有风险, 则对改密用户进行强校验核身。安全感识别模型可以是离线识别模型, 通过 $T+1$ 的方式 (例如采用当前识别时间之前的一些用户特征对该用户进行识别) 对用户进行识别。用户若被识别为高危, 则表明该用户有安全感的诉求, 需要用强校验核身来提高用户的安全感。改密动机异常识别模型可以实时识别当前改密
- 15 行为是否合理改密, 比如当用户其实是在当天有过通过密码支付的情况下再进行改密, 则动机不合理, 应该给予强校验核身。盗用风险识别模型和安全感识别模型均可以通过有监督学习构建, 如 GBDT、RandomForest、Logistic Regression 等模型; 而改密动机异常识别模型可以为无监督学习模型, 通过刻画行为的异常来识别风险, 如 One Class SVM 等。通过上述三个核身识别模型中的一个或多个的组合, 能够从不活跃用户中剔除具有
- 20 风险的用户, 在兼顾了让更多的不活跃用户享受弱校验服务的同时, 降低了弱校验核身带来的风险问题。

- [90]盗用风险识别模型通过用户的盗用风险特征对用户进行识别, 盗用风险特征用于刻画账户盗用风险的模型变量, 比如设备维度、环境维度、用户操作维度等多方面刻画异常。
- 25 [91]安全感识别模型通过安全感风险特征对用户进行识别, 安全感风险特征用于刻画用户对安全感的诉求, 可以包括两类, 一类是文本类特征, 例如用户历史上的来电反馈或文本反馈; 另一类是行为类特征, 例如用户历史上是否有过周期性改密的习惯, 是否绑卡后会解绑等。

- [92]改密动机异常识别模型通过改密动机特征对用户进行识别, 改密动机特征针对用户
- 30 当前改密是否真的是忘记密码这一点进行特征刻画, 例如可以包括是否当前改密之前短

时间内有过密码支付、同设备上有过多个账号进行改密等行为的特征。

[93] 用户业务变量、上述各个核身识别模型对用户进行核身识别所需要的特征都可以从以下数据中提取得到：

[94] 用户信息数据：包括用户信息，如用户 ID，用户注册时间、用户身份证所等。

5 [95] 历史交易数据：包括用户历史上的交易，包含用户 ID 对于的交易号、交易时间以及金额，同时也可以通过底层的关联获取交易时刻的交易设备、IP、WIFI 等详细信息。

[96] 历史案件信息：包含用户对盗用案件以及安全感问卷等信息。账户盗用是指账户由非本人进行操作并进行支付，本人发现后进行投诉或报案。该部分数据通常在建模过程中当做样本标签进行有监督学习。安全感问卷是为了获取用户安全感诉求而进行的某种抽样或定向数据调查。目的同盗用报案信息一样通常在建模过程中当做为样本的标签进行有监督学习。

10

[97] 舆情信息：包含历史上出现舆情的主要用户以及用户的舆情的特征，比如用户的来电反馈，或者在该段期间用户的行为数据，比如尝试改密码，解绑银行卡、删除好友等特征。

15 [98] 图 3 示出根据本公开一实施方式的核身方法的流程图。如图 3 所示，所述核身方法包括以下步骤 S301-S304：

[99] 在步骤 S301 中，响应于核身请求，根据用户业务变量值确定待核身用户是否为不活跃用户；

[100] 在步骤 S302 中，在所述待核身用户为不活跃用户时，确定多个核身识别模型中的至少一个对所述待核身用户的识别结果；

20

[101] 在步骤 S303 中，根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式；其中，所述核身方式包括弱校验核身方式和强校验核身方式；所述用户业务变量值以及所述核身阈值采用上述阈值确定方法得到；

25 [102] 在步骤 S304 中，采用所述核身方式对所述待核身用户进行核身。

[103] 本实施例中，在利用上述阈值确定方法得到了用户业务变量值、核身识别模型的核身阈值后，如果接收到需要对用户账户进行核身的请求，首先可以利用用户业务变量值确定待核身用户是否为不活跃用户；如果是不活跃用户，那么再利用核身识别模型

对用户进行识别，确定该用户是否为不活跃用户当中具有风险的用户，例如以改密行为为例，确定当前请求改密的用户是否正在盗取该账户；再例如，当前待核身用户是否为安全感诉求较高，不希望进行弱校验的用户等。核身识别模型会针对待核身用户对应的相应特征对用户进行打分，通过比较分值和该核身识别模型对应的核身阈值后，确定该待核身用户是否具有风险，如果有风险则采强校验核身方式；如果所要使用的一个或多个核身识别模型对该待核身用户的识别结果均为无风险用户时，采用弱校验核身方式。

[104] 本实施例的一些技术细节可参考上述阈值确定方法中的描述，在此不再赘述。

[105] 本公开实施例利用阈值确定方法优化得到的用户业务变量值、核身阈值以及核身识别模型对用户进行识别，以确定对用户采用强校验核身方式还是采用弱校验核身方式。通过这种方法，可以将不活跃用户的范围最大化的同时，能够从不活跃用户中识别出具有风险的用户，也即这样既能满足不活跃用户的弱校验核身需求，又能从中识别出需采用强校验核身的用户，能够实现用户体验和风险控制的平衡。

[106] 在本实施例的一个可选实现方式中，所述核身识别模型包括：盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型；其中，所述盗用风险识别模型用于识别账户被盗用的可能性；所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

[107] 该可选的实现方式中，盗用风险识别模型可以是实时识别模型，主要用于对用户当前的改密行为进行风险识别。若识别有风险，则对改密用户进行强校验核身。安全感识别模型可以是离线识别模型，通过 T+1 的方式（例如采用当前识别时间之前的一些用户特征对该用户进行识别）对用户进行识别。用户若被识别为高危，则表明该用户有安全感的诉求，需要用强校验核身来提高用户的安全感。改密动机异常识别模型可以实时识别当前改密行为是否合理改密，比如当用户其实是在当天有过通过密码支付的情况下再进行改密，则动机不合理，应该给予强校验核身。

[108] 该可选的实现方式中的其他细节可参考上述阈值确定方法中的描述，在此不再赘述。

[109] 在本实施例的一个可选实现方式中，如图 4 所示，所述步骤 S303 即根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式的步骤，进一步包括以下步骤 S401-S402：

[110] 在步骤 S401 中，根据第一识别结果以及所述盗用风险识别模型对应的所述核身

阈值确定所述待核身用户的第一核身方式,根据第二识别结果以及所述安全感识别模型对应的所述核身阈值确定所述待核身用户的第二核身方式,并根据第三识别模型以及所述改密动机异常识别模型对应的所述核身阈值确定所述待核身用户的第三核身方式;其中,所述第一识别结果、第二识别结果和第三识别结果分别为所述盗用风险识别模型、安全感识别模型和改密动机异常识别模型对所述待核身用户的识别结果;

[111] 在步骤 S402 中,在所述第一核身方式、第二核身方式以及第三核身方式均为弱校验核身方式时,确定所述待核身用户的核身方式为弱校验核身方式。

[112] 该可选的实现方式中,采用盗用风险识别模型、安全感识别模型和改密动机异常识别模型对不活跃用户进行识别,并在上述三个识别模型的识别结果均为待核身用户无风险,可以采用弱校验核身方式时,才对该待核身用户采用弱校验。弱校验核身方式可以是单因子核身方式,也即采用手机验证码、身份证号等单个因素进行校验的方式,而强校验核身方式可以是多因子核身方式,例如采用身份证号和/或手机验证码对用户识别后,还采用人脸识别等方式,强校验核身方式的校验强度高于弱校验核身方式,采用的校验因子较为可靠,步骤较为繁琐。通过本实施例这种方式,既可以将不活跃用户的范围最大化,同时还能够从不活跃用户中剔除有盗用账户风险的用户、安全感诉求较高的用户以及改密动机有异常的用户,而剩下的不活跃用户都可以采用弱校验的方式。

[113] 如上述所述,安全感诉求识别模型为离线识别模式,可以定期对用户的安全感诉求进行识别,并保存其识别结果。因此,在响应于针对该用户的核身请求时,可以利用盗用风险识别模型以及改密动机识别模型对该用户进行在线识别,而安全感识别模型的识别结果可以直接获取,也即从相应存储位置处获取之前利用安全感识别模型对该用户的识别结果。

[114] 可以理解的是,盗用风险识别模型和安全感识别模型不一定在用户请求修改密码时对用户进行核身识别,在其他需要的场景下也可以对用户进行核身识别,具体可以根据实际情况进行选择,对此不做限制。

[115] 在本实施例的一个可选实现方式中,所述步骤 S303 即根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式的步骤,进一步还包括以下步骤:

[116] 在所述第一核身方式、第二核身方式以及第三核身方式中的至少一个为强校验核身方式时,确定所述待核身用户的核身方式为强校验核身方式。

[117] 该可选的实现方式中, 如果盗用风险识别模型、安全感识别模型和改密动机异常识别模型中的任一个的识别结果表明, 当前待核身用户为具有风险的用户, 需要采用强校验核身方式, 那么最终采用强校验核身方式对该用户进行核身。也就是说, 待核身用户只要存在其中之一的任意一种风险或异常, 则对该用户采用强校验核身方式。通过这种方式, 可以尽可能地降低用户账户风险。

[118] 下述为本公开装置实施例, 可以用于执行本公开方法实施例。

[119] 图 5 示出根据本公开一实施方式的阈值确定装置的结构框图, 该装置可以通过软件、硬件或者两者的结合实现成为电子设备的部分或者全部。如图 5 所示, 所述阈值确定装置包括获取模块 501 和第一确定模块 502:

10 [120] 获取模块 501, 被配置为获取多个核身识别模型分别对应的预设目标值; 其中, 所述预设目标值用于表示所述核身识别模型被期望达到的目标识别能力;

[121] 第一确定模块 502, 被配置为根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值; 其中, 所述用户业务变量值用于划分活跃用户和不活跃用户, 所述核身阈值被所述核身识别模型用于从所述不活跃用户中剔除需要强
15 校验的用户。

[122] 本实施例中, 核身识别模型可以基于用户的特征和/或账户的特征识别该用户的账户是否存在核身风险, 如果存在则采用强校验核身, 否则采用弱校验核身; 也即核身识别模型用于识别该用户的账户采用强校验还是弱校验进行核身。强校验核身是指在核实用户身份时, 采用多重因子进行校验的方式, 而弱校验核身是指采用单个或者少数几个因子对用户身份进行核实校验的方式, 弱校验核身采用的因子数量少于强校验核身采用的因子数量, 且弱校验核身采用的校验强度小于强校验核身。例如, 弱校验核身采用身份证号或者手机短信验证码等因子进行校验; 而强校验核身采用的因子除了身份证号和/或手机短信验证码等之外, 还采用人脸等强因子。

25 [123] 多个核身识别模型可以从多个不同方面对用户账户进行识别, 也即不同的核身识别模型可以基于用户和/或账户的不同特征识别账户的不同核身风险。例如, 识别账户是否被盗的模型、识别用户安全感强弱的模型(如果用户安全感特强, 则存在核身风险)、识别用户改密动机异常的模型等。核身识别模型可以基于用户和/或账户的特征对用户账户进行打分, 并根据打分的高低来判断账户所存在的风险。

[124] 预设目标值可以是预先设定好的、与所述核身识别模型所要达到的目标识别能

- 力相关的值,也即预设目标值可以认为是对于核身识别模型识别准确率或识别错误率的一个期望值。在一实施例中,预设目标值可以是期望核身识别模型能够从众多用户中识别出风险用户的准确率。在另一实施例中,预设目标值可以是期望核身识别模型无法从众多用户中识别出风险用户的错误率。无论是目标识别准确率还是目标识别错误率,预设目标值都是用于表示核身识别模型的识别能力所要达到的目标期望值。预设目标值可以基于业务经验以及业务需求等预先设置,例如,当前业务涉及金融等安全级别较高的账户时,可以设置一预设目标值,使得核身识别模型的识别能力较高,而如果当前业务仅涉及论坛等安全级别较低的账户时,可以设置另一预设目标值使得核身识别模型的识别能力较低。
- 10 [125] 本实施例中,用户业务变量值可以用于衡量用户的活跃程度,通过用户业务变量值可以将当前业务系统中的用户划分为活跃用户和不活跃用户。活跃用户可以为经常在当前业务系统中执行一些操作的用户,例如浏览、发文章、购物、支付等操作行为,而不活跃用户可以为从来未在当前业务系统执行过任何操作或者最近一段时间内执行操作的次数较低的用户。例如,对于第三方支付系统,用户业务变量值可以设置为用户的支付次数,在所述用户业务变量值较大时,被划分成不活跃用户的占比较高,在所述用户业务变量值较小时,被划分为不活跃用户的占比较低。
- 15 [126] 本实施例中,核身阈值是核身识别模型所输出的模型分值的阈值,例如,在核身阈值确定了的情况下,利用核身识别模型对用户进行识别时,如果输出的模型分值小于(或大于)该核身阈值,则认为该用户不是风险用户,可以采用弱校验核身方式;而
- 20 而如果输出的模型分值大于或等于(或小于或等于)核身阈值,则认为该用户是风险用户,可以采用强校验核身方式。核身阈值的大小与被核身识别模型识别为风险用户的比例相关,也与核身模型识别模型的识别错误率或识别准确率相关,在核身阈值较大时,被识别为风险用户比例会较低(或较高),但是识别错误率较高(或者识别错误率较低);而在核身阈值较小时,被识别为风险用户的比例会较高(或较低),但是识别错误率较低(或者识别错误率较高)。核身阈值与被核身识别模型识别为风险用户的比例呈正比还是呈反比,或者说核身阈值与核身识别模型的识别错误率(或者识别准确率)呈正比还是呈反比,可以根据实际情况设置,对此不做限制。
- 25 [127] 用户业务变量值用于划分活跃用户和不活跃用户。核身方式可以包括强校验核身和弱校验核身,而为了给用户更好地体验,通常较为简单的做法就是对于不活跃用户
- 30 采用弱校验,对于活跃用户采用强校验。但是这样一刀切的做法可能会存在一些隐患,

以修改密码为例，不活跃用户的账号可能存在盗号风险，如果不活跃用户全部采用弱校验核身方式，很有可能出现盗号风险。因此，本公开实施例中通过用户业务变量值筛选出不活跃用户（例如设置用户业务变量值为用户在一段时间内的支付次数，如果支付次数少于设定值，则可以被认为是不活跃用户），之后再利用核身识别模型及其对应的核身阈值从不活跃用户中剔除风险用户（也即识别不活跃用户是否存在风险，如果存在风险则采用强校验方式），最终对剩下的不活跃用户进行弱校验。

[128] 在已有技术中，通过经验或者测试等方式单独确定不同核身识别模型的核身阈值以及用户业务变量值，且各个不同的核身识别模型对于用户的识别是各自独立的，相互不受影响。而本公开实施例为了给更多地用户提供弱校验这种高体验服务，同时又能将风险降到最低，而采取了预先设置各个核身识别模型所要达到的预设目标值，并采用这些预设目标值确定用户业务变量值以及各个核身识别模型的核身阈值，使得各个核身识别模型的识别能力能够满足预设目标值的同时，将采用弱校验核身方式的不活跃用户范围最大化。本公开实施例通过预设目标值确定用户业务变量以及核身阈值，不但综合考虑了多种核身识别模型以及用户业务变量对风险用户的划分，并且还在各个核身识别模型间达到了一定的平衡，能够提高用户体验。

[129] 本公开实施例在核身过程中，为了平衡多种不同核身识别模型对用户核身方式的识别结果，通过获取多个不同核身识别模型所要达到的目标识别能力，并根据该目标识别能力确定核身识别模型的核身阈值以及用于划分活跃用户和不活跃用户的用户业务变量值，以便将不活跃用户的范围最大化的同时，能够从不活跃用户中识别出具有风险的用户，这样既能满足不活跃用户的弱校验核身需求，又能从中识别出需采用强校验核身的用户，能够实现用户体验和风险控制的平衡。

[130] 在本实施例的一个可选实现方式中，所述第一确定模块 502，包括：

[131] 优化子模块，被配置为将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标，通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值。

[132] 该可选的实现方式中，基于让更多的用户享受弱校验核身的高体验服务，同时又能够尽量保证享受弱校验核身服务的用户为无风险用户（无风险用户可以理解为应该采用强校验的用户，比如盗用他人账户的用户、缺乏安全感需要强校验的用户等）。为了达到用户的高体验和低风险两者之间的平衡，本公开实施例预先设定各个核身识别模

- 型的预设目标值,预设目标值用于表示期望核身识别模型能够达到的识别能力,而训练好的核身识别模型的识别能力可以通过核身阈值调整,核身识别模型通过对用户的特征和/或用户账户的特征进行识别,会得出一个模型分数,而模型分数的高低与该用户的风险高低相关,核身阈值可以设置为介于模型分数最大值和最小值中间,模型分数越高代表用户风险越高的情况下,核身阈值设置越大,则核身识别模型的识别能力越弱(模型分数越高代表用户风险越低的情况下,核身阈值设置越小,则核身识别模型的识别能力越强);相反地,核身阈值设置越小,则核身识别模型的识别能力越强。因此可以为核身识别模型找到一个最优的核身阈值,能够使得核身识别模型的识别能力尽量靠近预设目标识别值。由于本公开使用多个核身识别模型对不活跃用户进行识别,同时还希望能够给更多的不活跃用户弱校验核身的服务体验,因此并非简单地将核身识别模型的核身阈值设置为预设目标值,也没有通过经验或者统计等方式直接设置用户业务变量值,而是采用优化算法同时优化用户业务变量值以及多个核身识别模型分别对应的多个核身阈值,并且优化得到的用户业务变量值以及多个核身阈值能够兼顾用户体验以及用户低风险两个问题,达到两者之间的平衡。
- 15 [133] 本公开实施例在优化用户业务变量以及多个核身识别模型分别对应的多个核身阈值的过程中,将核身阈值与对应的预设目标值之间的差距最小、根据用户业务变量值所划分的不活跃用户的范围最大化作为优化算法的目标,通过优化算法优化得到用户业务变量值以及核身阈值。在一实施例中,优化算法可以采用 PSO(粒子群优化算法, Particle Swarm Optimization)。PSO 优化算法是一种基于种群的随机优化技术,其通过模仿昆虫、兽群、鸟群和鱼群等的群集行为,这些群体按照一种合作的方式寻找食物,群体中的每个成员通过学习它自身的经验和其他成员的经验来不断改变其搜索模式,也即本公开采用 PSO 算法,将用户业务变量值以及各个核身阈值构成的目标函数的不同取值作为一个种群中的粒子,通过不断迭代优化各个粒子在目标空间中的最优取值,每次迭代的过程中粒子都从群体和个体角度出发找到自身的最优值,最终找到粒子在目标空间中从群体和个体角度出发都最优的一个取值。通过这种算法优化得到的用户业务变量值、各个核身阈值能够使得采用弱校验核身的不活跃用户的范围最大化,同时还能够从中识别出具有风险的用户,在用户体验和账户风险之间达到了一定的平衡。
- 20
- 25
- 30 [134] 在其他实施例中,还可以采用其他解决类似问题的优化算法,例如 ACO(蚁群算法)、Defferential Evolution(差分进化算法)等,具体可根据实际情况选择使用,在此不做限制。

[135] 在本实施例的一个可选实现方式中,如图6所示,所述优化子模块,包括:

[136] 构建子模块601,被配置为利用所述用户业务变量值、多个所述核身识别模型分别对应的所述核身阈值构建解向量;

5 [137] 求解子模块602,被配置为以所述用户业务变量值所划分的不活跃用户的范围最大化作为所述优化算法的约束条件,分别以多个所述核身识别模型对应的所述核身阈值小于其对应的所述预设目标值作为所述优化算法的目标函数,对所述解向量进行求解。

[138] 该可选的实现方式中,可以将用户业务变量值、各个核身识别模型对应的核身阈值作为变量构建一解向量。例如,用户业务变量值用户C表示,核身识别模型i的核身阈值用 Y_i ($i \geq 1$)表示,解向量可表示为 $S=[C, Y_1, Y_2, \dots, Y_i, \dots]$ 。在选定优化算法以后,可以将用户业务变量值所划分的不活跃用户的范围最大化作为优化算法的约束条件,并分别以多个核身阈值小于对应的预设目标值为目标函数,执行优化算法确定用户业务变量值和核身阈值。优化算法在执行过程中,会在保证用户业务变量值最大化(用户业务变量值越大不活跃用户的划分范围越大的情况,相反,如果用户变量值越小,不活跃用户的划分范围越小的情况下要以用户业务变量值最小化为约束条件)的前提下,使得各个核身阈值小于预设目标值,且无限接近于预设目标值。例如,采用PSO优化算法优化时,假如构建的向量为 $S=[C, Y_1, Y_2, \dots, Y_i, \dots]$,则适应性值函数可以构建为 $p=C-(Y_1-y_1)-(Y_2-y_2)-\dots-(Y_i-y_i)-\dots$ (仅用于举例,实际应用中可以根据实际情况构建), $y_1, y_2, \dots, y_i, \dots$ 分别为核身识别模型1、2、 $\dots$ 、i、 $\dots$ 的预设目标值;PSO优化算法通过寻找一p的取值,使得该取值在群体和个体中都是最优,并采用更新函数对p进行更新后,迭代执行上述步骤,直到达到迭代终止条件(例如迭代次数达到预设阈值)为止。最终得到的p对应的C和 Y_i 就是用户业务变量值和核身阈值的最优解。

10
15
20

[139] 在本实施例的一个可选实现方式中,所述核身识别模型包括:盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型;其中,所述盗用风险识别模型用于识别账户被盗用的可能性;所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度;所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

25

[140] 本实施例中,盗用风险识别模型可以是实时识别模型,主要用于对用户当前的改密行为进行风险识别。若识别有风险,则对改密用户进行强校验核身。安全感识别模型可以是离线识别模型,通过T+1的方式(例如采用当前识别时间之前的一些用户特征对该用户进行识别)对用户进行识别。用户若被识别为高危,则表明该用户有安全感的

30

诉求，需要用强校验核身来提高用户的安全感。改密动机异常识别模型可以实时识别当前改密行为是否合理改密，比如当用户其实是在当天有过通过密码支付的情况下再进行改密，则动机不合理，应该给予强校验核身。盗用风险识别模型和安全感识别模型均可以通过有监督学习构建，如 GBDT、RandomForest、Logistic Regression 等模型；而改密动机异常识别模型可以为无监督学习模型，通过刻画行为的异常来识别风险，如 One Class SVM 等。通过上述三个核身识别模型中的一个或多个的组合，能够从不活跃用户中剔除具有风险的用户，在兼顾了让更多的不活跃用户享受弱校验服务的同时，降低了弱校验核身带来的风险问题。

[141] 盗用风险识别模型通过用户的盗用风险特征对用户进行识别，盗用风险特征用于刻画账户盗用风险的模型变量，比如设备维度、环境维度、用户操作维度等多方面刻画异常。

[142] 安全感识别模型通过安全感风险特征对用户进行识别，安全感风险特征用于刻画用户对安全感的诉求，可以包括两类，一类是文本类特征，例如用户历史上的来电反馈或文本反馈；另一类是行为类特征，例如用户历史上是否有过周期性改密的习惯，是否绑卡后会解绑等。

[143] 改密动机异常识别模型通过改密动机特征对用户进行识别，改密动机特征针对用户当前改密是否真的是忘记密码这一点进行特征刻画，例如可以包括是否当前改密之前短时间内有过密码支付、同设备上有过多个账号进行改密等行为的特征。

[144] 用户业务变量、上述各个核身识别模型对用户进行核身识别所需要的特征都可以从以下数据中提取得到：

[145] 用户信息数据：包括用户信息，如用户 ID，用户注册时间、用户身份证所等。

[146] 历史交易数据：包括用户历史上的交易，包含用户 ID 对于的交易号、交易时间以及金额，同时也可以通过底层的关联获取交易时刻的交易设备、IP、WIFI 等详细信息。

[147] 历史案件信息：包含用户对盗用案件以及安全感问卷等信息。账户盗用是指账户由非本人进行操作并进行支付，本人发现后进行投诉或报案。该部分数据通常在建模过程中当做样本标签进行有监督学习。安全问卷是为了获取用户安全感诉求而进行的某种抽样或定向数据调查。目的同盗用报案信息一样通常在建模过程中当作为样本的标签进行有监督学习。

[148] 舆情信息：包含历史上出现舆情的主要用户以及用户的舆情的特征，比如用户的来电反馈，或者在该段期间用户的行为数据，比如尝试改密码，解绑银行卡、删除好友等特征。

[149] 图7示出根据本公开一实施方式的核身装置的结构框图，该装置可以通过软件、硬件或者两者的结合实现成为电子设备的部分或者全部。如图7所示，所述核身装置包括第二确定模块701、第三确定模块702、第四确定模块703和核身模块704：

[150] 第二确定模块701，被配置为响应于核身请求，根据用户业务变量值确定待核身用户是否为不活跃用户；

[151] 第三确定模块702，被配置为在所述待核身用户为不活跃用户时，确定多个核身识别模型中的至少一个对所述待核身用户的识别结果；

[152] 第四确定模块703，被配置为根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式；其中，所述核身方式包括弱校验核身方式和强校验核身方式；所述用户业务变量值以及所述核身阈值采用上述阈值确定装置得到；

[153] 核身模块704，被配置为采用所述核身方式对所述待核身用户进行核身。

[154] 本实施例中，在利用上述阈值确定装置得到了用户业务变量值、核身识别模型的核身阈值后，如果接收到需要对用户账户进行核身的请求，首先可以利用用户业务变量值确定待核身用户是否为不活跃用户；如果是不活跃用户，那么再利用核身识别模型对用户进行识别，确定该用户是否为不活跃用户当中具有风险的用户，例如以改密行为为例，确定当前请求改密的用户是否正在盗取该账户；再例如，当前待核身用户是否为安全感诉求较高，不希望进行弱校验的用户等。核身识别模型会针对待核身用户对应的相应特征对用户进行打分，通过比较分值和该核身识别模型对应的核身阈值后，确定该待核身用户是否具有风险，如果有风险则采强校验核身方式；如果所要使用的一个或多个核身识别模型对该待核身用户的识别结果均为无风险用户时，采用弱校验核身方式。

[155] 本实施例的一些技术细节可参考上述阈值确定装置中的描述，在此不再赘述。

[156] 本公开实施例利用阈值确定装置优化得到的用户业务变量值、核身阈值以及核身识别模型对用户进行识别，以确定对用户采用强校验核身方式还是采用弱校验核身方式。通过这种方式，可以将不活跃用户的范围最大化的同时，能够从不活跃用户中识别出具有风险的用户，也即这样既能满足不活跃用户的弱校验核身需求，又能从中识别出

需采用强校验核身的用户，能够实现用户体验和风险控制平衡。

[157] 在本实施例的一个可选实现方式中，所述核身识别模型包括：盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型；其中，所述盗用风险识别模型用于识别账户被盗用的可能性；所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

[158] 该可选的实现方式中，盗用风险识别模型可以是实时识别模型，主要用于对用户当前的改密行为进行风险识别。若识别有风险，则对改密用户进行强校验核身。安全感识别模型可以是离线识别模型，通过 T+1 的方式（例如采用当前识别时间之前的一些用户特征对该用户进行识别）对用户进行识别。用户若被识别为高危，则表明该用户有安全感的诉求，需要用强校验核身来提高用户的安全感。改密动机异常识别模型可以实时识别当前改密行为是否合理改密，比如当用户其实是在当天有过通过密码支付的情况下再进行改密，则动机不合理，应该给予强校验核身。

[159] 该可选的实现方式中的其他细节可参考上述阈值确定装置中的描述，在此不再赘述。

[160] 在本实施例的一个可选实现方式中，如图 8 所示，所述第四确定模块 703，包括：

[161] 第一确定子模块 801，被配置为根据第一识别结果以及所述盗用风险识别模型对应的所述核身阈值确定所述待核身用户的第一核身方式，根据第二识别结果以及所述安全感识别模型对应的所述核身阈值确定所述待核身用户的第二核身方式，并根据第三识别模型以及所述改密动机异常识别模型对应的所述核身阈值确定所述待核身用户的第三核身方式；其中，所述第一识别结果、第二识别结果和第三识别结果分别为所述盗用风险识别模型、安全感识别模型和改密动机异常识别模型对所述待核身用户的识别结果；

[162] 第二确定子模块 802，被配置为在所述第一核身方式、第二核身方式以及第三核身方式均为弱校验核身方式时，确定所述待核身用户的核身方式为弱校验核身方式。

[163] 该可选的实现方式中，采用盗用风险识别模型、安全感识别模型和改密动机异常识别模型对不活跃用户进行识别，并在上述三个识别模型的识别结果均为待核身用户无风险，可以采用弱校验核身方式时，才对该待核身用户采用弱校验。弱校验核身方式可以是单因子核身方式，也即采用手机验证码、身份证号等单个因素进行校验的方式，而强校验核身方式可以是多因子核身方式，例如采用身份证号和/或手机验证码对用户识别后，还采用人脸识别等方式，强校验核身方式的校验强度高于弱校验核身方式，采用

的校验因子较为可靠，步骤较为繁琐。通过本实施例这种方式，既可以将不活跃用户的范围最大化，同时还能够从不活跃用户中剔除有盗用账户风险的用户、安全感诉求较高的用户以及改密动机有异常的用户，而剩下的不活跃用户都可以采用弱校验的方式。

[164] 如上述所述，安全感诉求识别模型为离线识别模式，可以定期对用户的安全感诉求进行识别，并保存其识别结果。因此，在响应于针对该用户的核身请求时，可以利用盗用风险识别模型以及改密动机识别模型对该用户进行在线识别，而安全感识别模型的识别结果可以直接获取，也即从相应存储位置处获取之前利用安全感识别模型对该用户的识别结果。

[165] 可以理解的是，盗用风险识别模型和安全感识别模型不一定在用户请求修改密码时对用户进行核身识别，在其他需要的场景下也可以对用户进行核身识别，具体可以根据实际情况进行选择，对此不做限制。

[166] 在本实施例的一个可选实现方式中，所述第四确定模块 703，还包括：

[167] 第三确定子模块，被配置为在所述第一核身方式、第二核身方式以及第三核身方式中的至少一个为强校验核身方式时，确定所述待核身用户的核身方式为强校验核身方式。

[168] 该可选的实现方式中，如果盗用风险识别模型、安全感识别模型和改密动机异常识别模型中的任一个的识别结果表明，当前待核身用户为具有风险的用户，需要采用强校验核身方式，那么最终采用强校验核身方式对该用户进行核身。也就是说，待核身用户只要存在其中之一的任意一种风险或异常，则对该用户采用强校验核身方式。通过这种方式，可以尽可能地降低用户账户风险。

[169] 图 9 是适于用来实现根据本公开实施方式的阈值确定方法的电子设备的结构示意图。

[170] 如图 9 所示，电子设备 900 包括中央处理单元（CPU）901，其可以根据存储在只读存储器（ROM）902 中的程序或者从存储部分 908 加载到随机访问存储器（RAM）903 中的程序而执行上述图 1 所示的实施方式中的各种处理。在 RAM903 中，还存储有电子设备 900 操作所需的各种程序和数据。CPU901、ROM902 以及 RAM903 通过总线 904 彼此相连。输入/输出（I/O）接口 905 也连接至总线 904。

[171] 以下部件连接至 I/O 接口 905：包括键盘、鼠标等的输入部分 906；包括诸如阴极射线管（CRT）、液晶显示器（LCD）等以及扬声器等的输出部分 907；包括硬盘等

的存储部分 908; 以及包括诸如 LAN 卡、调制解调器等网络接口卡的通信部分 909。通信部分 909 经由诸如因特网的网络执行通信处理。驱动器 910 也根据需要连接至 I/O 接口 905。可拆卸介质 911, 诸如磁盘、光盘、磁光盘、半导体存储器等等, 根据需要安装在驱动器 910 上, 以便于从其上读出的计算机程序根据需要被安装入存储部分 908。

- 5 [172] 特别地, 根据本公开的实施方式, 上文参考图 1 描述的方法可以被实现为计算机软件程序。例如, 本公开的实施方式包括一种计算机程序产品, 其包括有形地包含在其可读介质上的计算机程序, 所述计算机程序包含用于执行图 1 的方法的程序代码。在这样的实施方式中, 该计算机程序可以通过通信部分 909 从网络上被下载和安装, 和/或从可拆卸介质 911 被安装。

- 10 [173] 图 9 所示的电子设备同样适于用来实现本公开实施方式的核身方法。

- [174] 附图中的流程图和框图, 图示了按照本公开各种实施方式的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上, 流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分, 所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意, 在有些作为替换的实现中, 方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如, 两个接连地表示的方框实际上可以基本并行地执行, 它们有时也可以按相反的顺序执行, 这依所涉及的功能而定。也要注意的, 框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合, 可以用执行规定的功能或操作的专用的基于硬件的系统来实现, 或者可以用专用硬件与计算机指令的组合来实现。
- 15

- 20 [175] 描述于本公开实施方式中所涉及到的单元或模块可以通过软件的方式实现, 也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中, 这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

- [176] 作为另一方面, 本公开还提供了一种计算机可读存储介质, 该计算机可读存储介质可以是上述实施方式中所述装置中所包含的计算机可读存储介质; 也可以是单独存在, 未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序, 所述程序被一个或者一个以上的处理器用来执行描述于本公开的方法。
- 25

[177] 以上描述仅为本公开的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解, 本公开中所涉及的发明范围, 并不限于上述技术特征的特定组合而成的技术方案, 同时也应涵盖在不脱离所述发明构思的情况下, 由上述技术特征或其等同特

征进行任意组合而形成的其它技术方案。例如上述特征与本公开中公开的（但不限于）具有类似功能的技术特征进行互相替换而形成的技术方案。

权利要求书

1、一种阈值确定方法，其特征在于，包括：

获取多个核身识别模型分别对应的预设目标值；其中，所述预设目标值用于表示所述核身识别模型被期望达到的目标识别能力；

5 根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值；其中，所述用户业务变量值用于划分活跃用户和不活跃用户，所述核身阈值被所述核身识别模型用于从所述不活跃用户中剔除需要强校验的用户。

2、根据权利要求 1 所述的阈值确定方法，其特征在于，根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值，包括：

10 将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标，通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值。

3、根据权利要求 2 所述的阈值确定方法，其特征在于，将所述核身识别模型对应的所述核身阈值与所述核身识别模型对应的所述预设目标值的差距最小、以及根据所述
15 用户业务变量值所划分的不活跃用户范围最大化作为目标，通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值，包括：

利用所述用户业务变量值、多个所述核身识别模型分别对应的所述核身阈值构建解向量；

以所述用户业务变量值所划分的不活跃用户的范围最大化作为所述优化算法的约
20 束条件，分别以多个所述核身识别模型对应的所述核身阈值小于其对应的所述预设目标值作为所述优化算法的目标函数，对所述解向量进行求解。

4、根据权利要求 1-3 任一项所述的阈值确定方法，其特征在于，所述核身识别模型包括：盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型；其中，所述
25 盗用风险识别模型用于识别账户被盗用的可能性；所述安全感识别模型用于识别用户对账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

5、一种核身方法，其特征在于，包括：

响应于核身请求，根据用户业务变量值确定待核身用户是否为不活跃用户；

30 在所述待核身用户为不活跃用户时，确定多个核身识别模型中的至少一个对所述待核身用户的识别结果；

根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确

定所述待核身用户的核身方式；其中，所述核身方式包括弱校验核身方式和强校验核身方式；所述用户业务变量值以及所述核身阈值采用权利要求 1-3 任一项所述的方法得到；

采用所述核身方式对所述待核身用户进行核身。

5 6、根据权利要求 5 所述的核身方法，其特征在于，所述核身识别模型包括：盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型；其中，所述盗用风险识别模型用于识别账户被盗用的可能性；所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度；所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

10 7、根据权利要求 6 所述的核身方法，其特征在于，根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式，包括：

根据第一识别结果以及所述盗用风险识别模型对应的所述核身阈值确定所述待核身用户的第一核身方式，根据第二识别结果以及所述安全感识别模型对应的所述核身阈值确定所述待核身用户的第二核身方式，并根据第三识别模型以及所述改密动机异常识别模型对应的所述核身阈值确定所述待核身用户的第三核身方式；其中，所述第一识别
15 结果、第二识别结果和第三识别结果分别为所述盗用风险识别模型、安全感识别模型和改密动机异常识别模型对所述待核身用户的识别结果；

在所述第一核身方式、第二核身方式以及第三核身方式均为弱校验核身方式时，确定所述待核身用户的核身方式为弱校验核身方式。

20 8、根据权利要求 7 所述的核身方法，其特征在于，根据所述识别结果以及对应的所述核身阈值确定所述待核身用户的核身方式，还包括：

在所述第一核身方式、第二核身方式以及第三核身方式中的至少一个为强校验核身方式时，确定所述待核身用户的核身方式为强校验核身方式。

9、一种阈值确定装置，其特征在于，包括：

25 获取模块，被配置为获取多个核身识别模型分别对应的预设目标值；其中，所述预设目标值用于表示所述核身识别模型被期望达到的目标识别能力；

第一确定模块，被配置为根据所述预设目标值确定用户业务变量值以及多个所述核身识别模型分别对应的核身阈值；其中，所述用户业务变量值用于划分活跃用户和不活跃用户，所述核身阈值被所述核身识别模型用于从所述不活跃用户中剔除需要强校验的用户。

30 10、根据权利要求 9 所述的阈值确定装置，其特征在于，所述第一确定模块，包括：

优化子模块，被配置为将所述核身识别模型对应的所述核身阈值与所述核身识别模

型对应的所述预设目标值的差距最小、以及根据所述用户业务变量值所划分的不活跃用户范围最大化作为目标,通过优化算法确定所述用户业务变量值以及所述核身识别模型对应的所述核身阈值。

11、根据权利要求 10 所述的阈值确定装置,其特征在于,所述优化子模块,包括:

- 5 构建子模块,被配置为利用所述用户业务变量值、多个所述核身识别模型分别对应的所述核身阈值构建解向量;

求解子模块,被配置为以所述用户业务变量值所划分的不活跃用户的范围最大化作为所述优化算法的约束条件,分别以多个所述核身识别模型对应的所述核身阈值小于其对应的所述预设目标值作为所述优化算法的目标函数,对所述解向量进行求解。

- 10 12、根据权利要求 9-11 任一项所述的阈值确定装置,其特征在于,所述核身识别模型包括:盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型;其中,所述盗用风险识别模型用于识别账户被盗用的可能性;所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度;所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

- 15 13、一种核身装置,其特征在于,包括:

第二确定模块,被配置为响应于核身请求,根据用户业务变量值确定待核身用户是否为不活跃用户;

第三确定模块,被配置为在所述待核身用户为不活跃用户时,确定多个核身识别模型中的至少一个对所述待核身用户的识别结果;

- 20 第四确定模块,被配置为根据所述核身识别模型的所述识别结果以及所述核身识别模型对应的核身阈值确定所述待核身用户的核身方式;其中,所述核身方式包括弱校验核身方式和强校验核身方式;所述用户业务变量值以及所述核身阈值采用权利要求 9-11 任一项所述的装置得到;

核身模块,被配置为采用所述核身方式对所述待核身用户进行核身。

- 25 14、根据权利要求 13 所述的核身装置,其特征在于,所述核身识别模型包括:盗用风险识别模型、安全感识别模型和/或改密动机异常识别模型;其中,所述盗用风险识别模型用于识别账户被盗用的可能性;所述安全感识别模型用于识别用户对于账户安全性的高低诉求程度;所述改密动机异常识别模型用于识别所述用户修改密码的行为异常的可能性。

- 30 15、根据权利要求 14 所述的核身装置,其特征在于,所述第四确定模块,包括:

第一确定子模块,被配置为根据第一识别结果以及所述盗用风险识别模型对应的所

述核身阈值确定所述待核身用户的第一核身方式,根据第二识别结果以及所述安全感识别模型对应的所述核身阈值确定所述待核身用户的第二核身方式,并根据第三识别模型以及所述改密动机异常识别模型对应的所述核身阈值确定所述待核身用户的第三核身方式;其中,所述第一识别结果、第二识别结果和第三识别结果分别为所述盗用风险识别模型、安全感识别模型和改密动机异常识别模型对所述待核身用户的识别结果;

第二确定子模块,被配置为在所述第一核身方式、第二核身方式以及第三核身方式均为弱校验核身方式时,确定所述待核身用户的核身方式为弱校验核身方式。

16、根据权利要求 15 所述的核身装置,其特征在于,所述第四确定模块,还包括:

第三确定子模块,被配置为在所述第一核身方式、第二核身方式以及第三核身方式中的至少一个为强校验核身方式时,确定所述待核身用户的核身方式为强校验核身方式。

17、一种电子设备,其特征在于,包括存储器和处理器;其中,

所述存储器用于存储一条或多条计算机指令,其中,所述一条或多条计算机指令被所述处理器执行以实现权利要求 1-8 任一项所述的方法步骤。

18、一种计算机可读存储介质,其上存储有计算机指令,其特征在于,该计算机指令被处理器执行时实现权利要求 1-8 任一项所述的方法步骤。