

身份验证及账户信息变更方法和装置

技术领域

[01] 本说明书涉及风险控制技术领域，尤其涉及身份验证及账户信息变更方法和装置。

背景技术

- 5 [02] 在实际应用中，常常需要对用户进行身份验证。例如，当用户执行账户信息变更时，需要先验证执行账户信息变更操作的当前操作者是否账户所有者，然后才对账户信息进行变更，以免使用户的账户遭受损失。因此，有必要对身份验证方式进行改进。

发明内容

[03] 基于此，本说明书提供了身份验证及账户信息变更方法和装置。

- 10 [04] 根据本说明书实施例的第一方面，提供一种身份验证方法，所述方法包括：在接收到账户信息变更请求之后，获取当前操作者的个人信息和网络环境信息；分别对所述个人信息和网络环境信息进行风险识别，对应获取第一风险识别结果和第二风险识别结果；其中，所述第一风险识别结果于表征当前操作者与账户所有者不一致的风险，所述第二风险识别结果用于表征当前操作者所处的网络环境存在安全隐患的风险；根据所述第一
- 15 风险识别结果和第二风险识别结果选择身份验证方式，并根据所述身份验证方式对所述当前操作者进行身份验证。

[05] 可选地，对所述网络环境信息进行风险识别的步骤包括：对所述网络环境信息进行特征提取；将提取到的特征输入风控模型，以对所述网络环境信息进行风险识别。

[06] 可选地，所述个人信息包括当前操作者的生物信息和待变更账户的账户信息。

- 20 [07] 可选地，所述账户信息包括所述账户的历史交易信息、对所述账户执行的历史操作信息，和/或与所述账户绑定的网络身份识别信息。

- [08] 可选地，对所述个人信息进行风险识别，获取第一风险识别结果的步骤包括：获取当前操作者输入的历史交易信息，若输入的历史交易信息与实际历史交易信息不一致，判定所述第一风险识别结果为存在风险；和/或对所述历史操作信息进行特征提取，若提
- 25 取到存在风险的特征，判定所述第一风险识别结果为存在风险；和/或获取当前操作者输入的网络身份识别信息，若输入的网络身份识别信息与预存的网络身份识别信息不一致，

判定所述第一风险识别结果为存在风险。

[09]可选地，对所述个人信息进行风险识别，获取第一风险识别结果的步骤包括：获取当前操作者的生物信息；若输入的生物信息与预存的生物信息不一致，判定所述第一风险识别结果为存在风险。

5 [10]可选地，根据所述第一风险识别结果和第二风险识别结果选择身份验证方式的步骤包括：根据所述第一风险识别结果中账户信息对应的风险识别结果计算第一风险分值；根据所述第一风险识别结果中生物信息对应的风险识别结果计算第二风险分值；根据所述第二风险识别结果计算第三风险分值；根据所述第一风险分值、第二风险分值和第三风险分值选择身份验证方式。

10 [11]可选地，所述生物信息包括虹膜信息、指纹信息、声纹信息和/或人脸特征信息。

[12]可选地，根据所述身份验证方式对所述当前操作者进行身份验证的步骤包括：将所述第一风险识别结果和第二风险识别结果输入预存的机器学习模型，获取所述当前操作者的身份验证结果，所述身份验证结果用于表征当前操作者与账户所有者相同的概率。

[13]根据本说明书实施例的第二方面，提供一种账户信息变更方法，所述方法包括：根据任一实施例的身份验证方法对执行账户变更操作的当前操作者进行身份验证；若身份验证通过，对所述账户信息进行变更。

[14]根据本说明书实施例的第三方面，提供一种身份验证装置，所述装置包括：获取模块，用于在接收到账户信息变更请求之后，获取当前操作者的个人信息和网络环境信息；风险识别模块，用于分别对所述个人信息和网络环境信息进行风险识别，对应获取第一风险识别结果和第二风险识别结果；其中，所述第一风险识别结果用于表征当前操作者与账户所有者不一致的风险，所述第二风险识别结果用于表征当前操作者所处的网络环境存在安全隐患的风险；身份验证模块，用于根据所述第一风险识别结果和第二风险识别结果选择身份验证方式，并根据所述身份验证方式对所述当前操作者进行身份验证。

[15]根据本说明书实施例的第四方面，提供一种账户信息变更装置，所述装置包括：任一实施例的身份验证装置；以及信息变更模块，用于若所述身份验证装置的身份验证结果为验证通过，对所述账户信息进行变更。

[16]根据本说明书实施例的第五方面，提供一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现任一实施例的方法。

[17]根据本说明书实施例的第六方面，提供一种计算机设备，包括存储器、处理器及存

储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现任一实施例的方法。

[18]应用本说明书实施例方案，通过获取当前操作者的个人信息和网络环境信息，一方面能够识别出当前操作者与账户所有者不一致的风险，另一方面能够识别出当前操作者所处的网络环境存在安全隐患的风险，将两种风险识别结果共同作为判断当前操作者身份的依据，能够提高识别准确率，降低账户被盗用的风险，提高安全性。同时，上述身份识别方式实时性较高，能够减少用户不必要的操作。

[19]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，并不能限制本说明书。

10 附图说明

[20]此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书一起用于解释本说明书的原理。

[21]图 1 是一个实施例的身份验证流程图。

[22]图 2 是本说明书一个实施例的身份验证方法流程图。

15 [23]图 3 是本说明书一个实施例的身份验证系统的分层架构图。

[24]图 4 是本说明书一个实施例的身份验证方法的总体流程图。

[25]图 5 是本说明书一个实施例的账户信息变更方法流程图。

[26]图 6 是本说明书一个实施例的身份验证装置的框图。

[27]图 7 是本说明书一个实施例的账户信息变更装置的框图。

20 [28]图 8 是本说明书一个实施例的用于实施本说明书实施例方法的计算机设备的示意图。

具体实施方式

[29]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[30]在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。

在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

5 [31]应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

10 [32]如图 1 所示，是一个实施例的身份验证流程图。身份验证过程可由客户端触发，例如，在用户需要执行账户信息变更操作时，可以先进行身份验证。其中，账户信息变更是指用户对账户基本信息（例如，密码、绑定手机号、邮箱等）的增加、删除、更改等操作的统称。在服务器接收到客户端发送的账户信息变更请求之后，服务器可以请求客户端提供用于证明当前操作者身份的身份信息。客户端提交身份信息之后，服务器可以对身份信息进行验证。如果验证通过，则允许客户端更改账户信息。客户端可以将变更后的账户信息发送至服务器。

[33]基于此，本说明书实施例提供了一种身份验证方法，如图 2 所示，所述方法可包括：

[34]步骤 202：在接收到账户信息变更请求之后，获取当前操作者的个人信息和网络环境信息；

20 [35]步骤 204：分别对所述个人信息和网络环境信息进行风险识别，对应获取第一风险识别结果和第二风险识别结果；其中，所述第一风险识别结果于表征当前操作者与账户所有者不一致的风险，所述第二风险识别结果用于表征当前操作者所处的网络环境存在安全隐患的风险；

[36]步骤 206：根据所述第一风险识别结果和第二风险识别结果选择身份验证方式，并根据所述身份验证方式对所述当前操作者进行身份验证。

25 [37]本实施例可由服务器执行。在步骤 202 中，当前操作者是指当前向服务器发送账户信息变更请求的用户。其中，当前操作者的个人信息可以用于确定当前操作者的身份，当前操作者的网络环境信息可以用于表征，当前操作者的网络环境的安全性。

[38]在步骤 204 中，第一风险识别结果和第二风险识别结果可以采用布尔值（1 或者 0）来表示，其中，取值为 1 可表示存在风险；取值为 0 可表示不存在风险。第一风险识别

结果和第二风险识别结果也可以采用分值来表示,例如,大于 80 分表示存在高危风险,大于 60 分且小于或等于 80 分表示存在一定风险,大于 40 分且小于或等于 60 分表示风险值较小,小于 40 分表示不存在风险。

[39]在步骤 206 中,可以根据第一风险识别结果和第二风险识别结果来综合选择身份验证方式。例如,当第一风险识别结果和第二风险识别结果均为无风险时,选择较为简单的验证方式(例如,发送短信验证码、邮箱验证码等);当第一风险识别结果和第二风险识别结果均为存在风险时,采用较为复杂或者可靠的验证方式(例如,人工验证等)。

[40]应用本说明书实施例方案,通过获取当前操作者的个人信息和网络环境信息,一方面能够识别出当前操作者与账户所有者不一致的风险,另一方面能够识别出当前操作者所处的网络环境存在安全隐患的风险,将两种风险识别结果共同作为判断当前操作者身份的依据,能够提高识别准确率,降低账户被盗用的风险,提高安全性。同时,上述身份识别方式实时性较高,能够减少用户不必要的操作。

[41]在一个实施例中,所述个人信息包括当前操作者的生物信息和待变更账户的账户信息。其中,生物信息是利用生物识别技术获取到的携带人体固有的生理特性的信息,例如:指纹信息,人脸特征信息、虹膜信息和/或声纹信息等。账户信息可以包括账户的历史交易信息、对账户执行的历史操作信息,和/或与账户绑定的网络身份识别信息。其中,历史交易信息可以是最近一笔交易发生的时间和订单地址等信息;历史操作信息可以是历史时间段内的登录、登出信息等;与账户绑定的网络身份识别信息可以是账户的关联手机号、关联邮箱、密码保护问题等。通过账户信息可以判断操作者与本账户的强弱附属关系,通过生物信息可以进一步判断操作者与账户的一致性,从而提高判断准确性。

[42]因此,在对所述个人信息进行风险识别时,可以采用以下方式:

[43]方式一:若账户信息中包括账户的历史交易信息,则可以获取当前操作者输入的历史交易信息,若输入的历史交易信息与实际历史交易信息不一致,判定所述第一风险识别结果为存在风险。例如,系统数据库中记录的账户最近一次的订单交易时间为 2018 年 7 月 1 日,订单地址为 A;但当前操作者提供的历史交易信息中,订单地址为 B,与数据库中的记录不一致,则可以判定第一风险识别结果为存在风险。

[44]方式二:若账户信息中包括对账户执行的历史操作信息,则可以对所述历史操作信息进行特征提取,若提取到存在风险的特征,判定所述第一风险识别结果为存在风险。其中,特征可以包括各种操作(例如,登录、登出、使用账户资产等)的发生次数、发

生时间、发生地点和持续时间等。存在风险的特征即与用户一般情况下的操作习惯相违背的特征。例如，账户在短时间内连续在不同的 IP 地址多次登录，或者账户在短时间内（例如，1 天）内发生上百起交易等。提取到存在风险的特征，表示账户很有可能存在被盗用的风险。

5 [45]方式三：若账户信息中包括与账户绑定的网络身份识别信息，则可以获取当前操作者输入的网络身份识别信息，若输入的网络身份识别信息与预存的网络身份识别信息不一致，判定所述第一风险识别结果为存在风险。其中，网络身份识别信息可包括账户名、账户昵称、邮箱地址及与前述有关的密码与密码保护问题和答案等。对于实名认证过的账户，还可以包括与账户绑定的个人身份信息，例如：身份证、护照或者驾驶证等。

10 [46]对于账户信息中包括前述信息中的多者的情形，对应的风险识别方式也可以采用上述三种方式的结合。例如，若账户信息中包括历史交易信息和网络身份识别信息，可以同时采用方式一和方式三来进行风险识别。

[47]此外，对于个人信息中包括生物信息的实施例，对个人信息进行风险识别进行风险识别时，可以获取当前操作者的生物信息；若输入的生物信息与预存的生物信息不一致，
15 判定所述第一风险识别结果为存在风险。获取生物信息时，可以通过客户端调用用户终端设备（例如，手机）上的相应模块，然后将获取到的生物信息上传至服务器。例如，当需要获取人脸特征信息时，可以由客户端调用手机摄像头进行拍摄，拍摄完成后再将用户的人脸照片上传至服务器。也可以由客户端先进行特征提取，再将提取到的特征信息返回至服务器。

20 [48]在一个实施例中，对所述网络环境信息进行风险识别的步骤包括：对所述网络环境信息进行特征提取；将提取到的特征输入风控模型，以对所述网络环境信息进行风险识别。提取到的特征可包括：用于表征网络是公共网络或者家庭网络的网络类型信息和/或用于表征网络 IP 地址是否曾被举报的信息等。提取到的特征可以输入预先训练好的风控模型（例如，二分类模型），并将该风控模型的输出结果作为对所述网络环境信息
25 进行风险识别的结果。

[49]在一个实施例中，在根据所述第一风险识别结果和第二风险识别结果选择身份验证方式时，可以根据所述第一风险识别结果中账户信息对应的风险识别结果计算第一风险分值；根据所述第一风险识别结果中生物信息对应的风险识别结果计算第二风险分值；根据所述第二风险识别结果计算第三风险分值；根据所述第一风险分值、第二风险分值
30 和第三风险分值选择身份验证方式。

- [50] 风险分值的高低可以用于表征执行账户信息变更操作时所存在的风险。分值越高，风险越大。对于个人信息包括生物信息和账户信息的实施例，可以获取上述第一风险分值和第二风险分值，并结合第三风险分值，选择身份验证方式。具体地，可以根据各个风险分值的加权平均值选择身份验证方式，也可以采用其他算法或者模型来对各个风险
- 5 分值进行综合评价，最终选择身份验证方式。对于个人信息仅包括生物信息或者账户信息的实施例，也可以仅获取上述第一风险分值或者第二风险分值，然后结合第三风险分值，选择身份验证方式。
- [51] 上述身份验证方式可以是一种身份验证策略，例如，人工验证、通过邮箱验证码或短信验证码的方式验证等；也可以是通过机器学习模型进行验证。对于后者，可以将所
- 10 述第一风险识别结果和第二风险识别结果输入预存的机器学习模型，获取所述当前操作者的身份验证结果，所述身份验证结果用于表征当前操作者与账户所有者相同的概率。
- [52] 在一个实施例中，还可以同时向用户推送多组可选的验证方式，由用户从中选择一种。只要其中一种验证方式验证通过，即认为当前操作者身份验证通过。这样可以提高用户的自主性，从而提高用户体验。
- 15 [53] 上述身份验证方法可通过图 3 所示身份验证系统实现，该系统可包括数据层、识别层和推荐层。其中，数据层可包括账户信息采集单元、生物信息采集单元和环境信息采集单元，分别用于采集账户信息、当前操作者的生物信息以及网络环境信息。识别层可包括账户信息识别模块、生物信息识别模块和环境风险识别模块。账户信息识别模块可获取账户信息采集模块发送的数据，并通过对该数据进行身份验证、交易验证和/或行为
- 20 验证的方式来进行风险识别。生物信息识别模块可以获取生物信息采集单元发送的数据，并进行人脸识别、指纹识别和/或声纹识别等生物识别。环境风险识别模块可以获取环境信息采集模块发送的数据，并根据预先存储的风险策略或者风险模型进行风险识别。推荐层收集到识别层推送的数据，通过该层各类推荐策略及推荐模型的分析，最后呈现给用户不同的校验方式。通过这种方式，可以向用户推送个性化的验证方式，一方面更加
- 25 符合实际情况，另一方面也提高了不法分子进行风险对抗的难度，提高了系统的防御鲁棒性。
- [54] 在一个实施例中，如图 4 所示，用户可以先按照普通的自助核身方式进行操作，如果能够自助核身，则通过普通的自助核身方式进行核身。如果不能自助核身（例如，无法获取验证码，或者手机、邮箱无法使用等情况），则可以通过图 3 所示的身份验证系统
- 30 进行身份验证。如果验证通过，则可完成账户信息变更操作。本实施例解决了传统的

核身方式中，当用户无法进行自助核身时需要通过后置人工审核的方式进行核身，从而导致时效性差的问题。

[55]本说明书实施例的方案具有以下优点：

5 [56]（1）利用生物识别及智能风险策略核验当前操作者，输出梯度的个性化验证方式，不仅可以提升用户的自助操作成功率，减少用户不必要的来电，而且还能降低被盗用风险。同时，对于其他方案仅仅依赖人脸、证件的交互服务，在体验上有了质的提升及飞跃，同时提高了系统的防御鲁棒性。

[57]（2）通过生物识别+账户信息验证+线上环境风险识别+智能推荐的创新组合服务方式，能够更加精准有效的识别操作本人，防止盗用的同时提升用户的操作体验。

10 [58]（3）提供了一种替代原本需要人工电话处理且处理时长不固定，用户一次性解决问题困难的系统，从用户操作层面来看仅三步即可完成验证，大大减少了原本需要等待 1-7 个工作日的处理时长，从多维度来保障用户的安全性同时提升用户的操作体验。

15 [59]如图 5 所示，本说明书实施例还提供了一种账户信息变更方法，所述方法包括：根据任一实施例的身份验证方法对所述当前操作者进行身份验证；若身份验证通过，对所述账户信息进行变更。进一步地，若身份验证失败，还可以向客户端返回错误提示。

[60]如图 6 所示，本说明书实施例还提供一种身份验证装置 600，所述装置可包括：

[61]获取模块 602，用于在接收到账户信息变更请求之后，获取当前操作者的个人信息和网络环境信息；

20 [62]风险识别模块 604，用于分别对所述个人信息和网络环境信息进行风险识别，对应获取第一风险识别结果和第二风险识别结果；其中，所述第一风险识别结果于表征当前操作者与账户所有者不一致的风险，所述第二风险识别结果用于表征当前操作者所处的网络环境存在安全隐患的风险；

[63]身份验证模块 606，用于根据所述第一风险识别结果和第二风险识别结果选择身份验证方式，并根据所述身份验证方式对所述当前操作者进行身份验证。

25 [64]上述装置中各个模块的功能和作用的实现过程具体详情见上述身份验证方法中对应步骤的实现过程，在此不再赘述。

[65]如图 7 所示，本说明书实施例还提供一种账户信息变更装置 700，所述装置可包括：任一实施例的身份验证装置 600；以及信息变更模块 702，用于若身份验证通过，对所

述账户信息进行变更。

[66]上述装置中信息变更模块 702 的功能和作用的实现过程具体详情见上述账户信息变更方法中对应步骤的实现过程，在此不再赘述。

[67]本说明书装置的实施例可以应用在计算机设备上，例如服务器或终端设备。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，
5 作为一个逻辑意义上的装置，是通过其所在文件处理的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 8 所示，为本说明书装置所在计算机设备的一种硬件结构图，除了图 8 所示的处理器 802、内存 804、网络接口 806、以及非易失性存储器 808 之外，实施例中装置所在的服务器或电子设备，
10 通常根据该计算机设备的实际功能，还可以包括其他硬件，对此不再赘述。

[68]对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据
15 实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[69]相应地，本说明书实施例还提供一种计算机存储介质，所述存储介质中存储有程序，所述程序被处理器执行时实现上述任一实施例中的方法。

[70]相应地，本说明书实施例还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述任一实施例中的方法。
20

[71]本说明书实施例可采用在一个或多个其中包含有程序代码的存储介质（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。计算机可用存储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
25

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。

[72]本领域技术人员在考虑说明书及实践这里公开的说明书后,将容易想到本公开的其它实施方案。本公开旨在涵盖本公开的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的,本公开的真正范围和精神由下面的权利要求指出。

[73]应当理解的是,本公开并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

[74]以上所述仅为本公开的较佳实施例而已,并不用以限制本公开,凡在本公开的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本公开保护的范围之内。