(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 10 月 14 日 (14.10.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/204086 A1

(51) 国际专利分类号:
G06F 21/32 (2013.01) *G06F 21/31* (2013.01)
G06N 3/08 (2006.01)

(21) 国际申请号: PCT/CN2021/085319

(22) 国际申请日: 2021 年 4 月 2 日 (02.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010262293.6 2020年4月6日 (06.04.2020) CN

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 陈栋 (**CHEN, Dong**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李基 (**LI, Ji**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (**LONGSUN LEAD IP LTD.**); 中国北京市海淀区北清路68号院3号楼101, Beijing 100094 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** IDENTITY AUTHENTICATION METHOD, AND METHOD AND DEVICE FOR TRAINING IDENTITY AUTHENTICATION MODEL

(54) **发明名称:** 身份认证的方法、身份认证模型的训练方法及装置

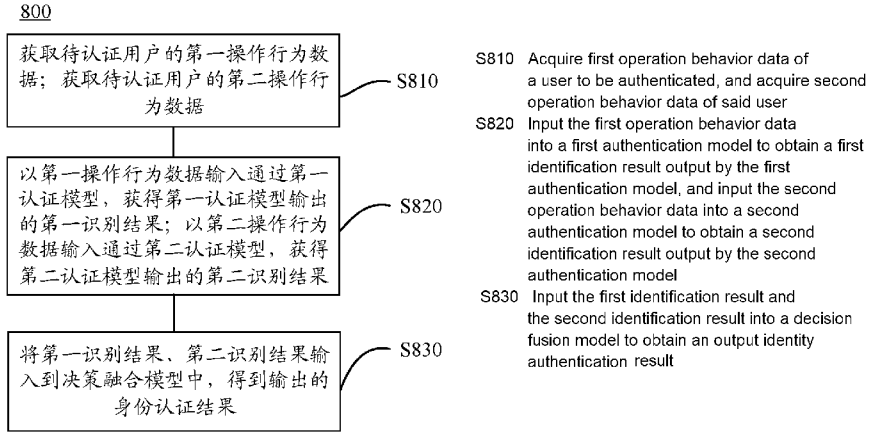


图 8

(57) **Abstract:** Disclosed are an identity authentication method, a method and device for training an identity authentication model, and a computer-readable medium, which belong to the field of artificial intelligence (AI). The identity authentication method comprises: acquiring first operation behavior data and second operation behavior data of a user to be authenticated; inputting the first operation behavior data into a first authentication model to obtain a first identification result output by the first authentication model, and inputting the second operation behavior data into a second authentication model to obtain a second identification result output by the second authentication model, wherein the first authentication model and the second authentication model are an anomaly detection model and a classification model, respectively; and inputting the first identification result and the second identification result into a decision fusion model to obtain an output identity authentication result. In the method of the present application, decision fusion is carried out on the basis of at least two identification results, such that the accuracy of identity authentication can be improved.

WO 2021/204086 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请公开了人工智能(AI)领域中的一种身份认证的方法、身份认证模型的训练方法、装置及计算机可读介质。该身份认证的方法包括：获取待认证用户的第一操作行为数据和第二操作行为数据；以第一操作行为数据输入至第一认证模型，获得第一认证模型输出的第一识别结果；以第二操作行为数据输入至第二认证模型，获得第二认证模型输出的第二识别结果；第一、第二认证模型分别为异常检测模型和分类模型；将第一识别结果和第二识别结果输入到决策融合模型中，得到输出的身份认证结果。本申请的方法基于至少两个识别结果进行决策融合，能够提高身份认证的准确性。

身份认证的方法、身份认证模型的训练方法及装置

本申请要求于2020年04月06日提交中国专利局、申请号为202010262293.6、申请名称为“身份认证的方法、身份认证模型的训练方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及人工智能领域，并且更具体地，涉及一种身份认证的方法、身份认证模型的训练方法及装置。

背景技术

人工智能（artificial intelligence, AI）是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。换句话说，人工智能是计算机科学的一个分支，它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式作出反应的智能机器。人工智能也就是研究各种智能机器的设计原理与实现方法，使机器具有感知、推理与决策的功能。人工智能领域的研究包括机器人，自然语言处理，计算机视觉，决策与推理，人机交互，推荐与搜索，AI基础理论等。

随着智能设备的普及，为了保护个人的财产和隐私安全，用户通常会设置身份认证保护措施。然而，传统身份认证方式，如密码认证、图案认证等方式，存在肩窥窃取风险；生物身份认证方式，如指纹认证或人脸认证等方式，存在仿冒攻击的风险。目前，可以通过行为身份认证方式进一步提高系统安全性。行为身份认证指的是，通过机器学习算法对用户过去的行为建模，用以识别近期行为，实现身份认证。现有的行为身份认证方式在抗攻击能力、认证用户识别率等方面无法达到预期。在实际的行为身份认证过程中，若认证用户识别能力差，则认证用户常会被误认为是非认证用户，导致用户体验差；若抗攻击能力差，则非认证用户会被误认为认证用户，身份认证形同虚设。

因此，如何提高身份认证的准确率，成为一个亟需解决的技术问题。

发明内容

本申请提供一种身份认证的方法、身份认证模型的训练方法及装置，能够提高身份认证的准确性。

第一方面，提供了一种身份认证的方法，该方法包括：获取待认证用户的第一操作行为数据；获取待认证用户的第二操作行为数据；以所述第一操作行为数据输入通过第一认证模型，获得所述第一认证模型输出的第一识别结果；以所述第二操作行为数据输入通过第二认证模型，获得所述第二认证模型输出的第二识别结果；其中，所述第一、第二认证模型分别为异常检测模型和分类模型； 将所述第一识别结果、所述第二识别结果输入到

决策融合模型中，得到输出的身份认证结果，其中，所述决策融合模型用于根据所述第一识别结果和所述第二识别结果的权重参数确定所述身份认证结果。

该身份认证模型包括第一认证模型、第二认证模型和决策融合模型。应理解，该身份认证模型可以包括多个认证模型和决策融合模型，将多个认证模型输出的识别结果输入决策融合模型中，由决策融合模型输出身份认证结果。

应理解，第一操作行为数据和第二操作行为数据可以相同，也可以不同。

可选地，第一识别结果和/或第二识别结果包括待认证用户为认证用户或待认证用户为非认证用户。

可选地，第一识别结果和/或第二识别结果包括待认证用户为认证用户的概率或待认证用户为非认证用户的概率。

例如，若第一识别结果和第二识别结果中存在一个识别结果为认证用户，则该身份认证结果为认证用户。或者，若第一识别结果和第二识别结果中存在一个识别结果为非认证用户，则该身份认证结果为非认证用户。

决策融合模型输出的身份认证结果可以包括待认证用户为认证用户或待认证用户为非认证用户。或者，决策融合模型输出的身份认证结果可以包括待认证用户为认证用户的概率或待认证用户为非认证用户的概率。

在本申请实施例中，将两个认证模型的识别结果输入决策融合模型进行决策融合，得到身份认证结果，能够提高身份认证的准确性。同时，通过用户的操作行为数据进行身份验证，不会改变用户的用机习惯，有利于实现无感验证。

此外，在采用异常检测模型实现身份认证的情况下，无法保证模型的抗攻击能力，抗攻击能力差，则非认证用户会被误认为认证用户，身份认证形同虚设；在采用分类模型实现身份认证的情况下，无法保证认证用户的识别率，认证用户识别能力差，则认证用户常会被误认为是非认证用户，导致用户体验差。本申请实施例采用异常检测模型和分类模型，一方面通过异常检测模型提高了认证用户识别率，另一方面通过分类模型提高了抗攻击能力，整体上提高了身份认证模型的识别能力。

结合第一方面，在第一方面的某些实现方式中，第一操作行为数据和/或第二操作行为数据是通过传感器采集的数据。

例如，传感器包括运动传感器和/或触屏传感器。

待认证用户的操作行为数据可以为对传感器采集的原始数据进行处理后得到的数据。

例如，触屏传感器采集的原始数据包括：时间戳、触摸点 X/Y 轴坐标、触摸面积、触摸压力、动作（action）和屏幕方向等。运动传感器采集的原始数据包括：时间戳、加速度 X/Y/Z 轴数据、陀螺仪 X/Y/Z 轴数据等。应理解，以上仅为示意，传感器采集的数据可以包括以上中的任一项或几项，也可以包括其他数据。

结合第一方面，在第一方面的某些实现方式中，第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括：第一操作行为样本数据和第一操作行为样本数据对应的标签，第一操作行为样本数据对应的标签用于表示第一操作行为样本数据对应的用户为认证用户或非认证用户。

第二认证模型的模型参数是基于第五样本数据训练得到的，第五样本数据包括：第五操作行为样本数据和第五操作行为样本数据对应的标签，第五操作行为样本数据对应的标

签用于表示第五操作行为样本数据对应的用户为认证用户或非认证用户。

结合第一方面，在第一方面的某些实现方式中，异常检测模型可以采用单分类支持向量机 SVM 或孤立森林等。分类模型可以采用 SVM 或神经网络等。

在本申请实施例中，异常检测模型和分类模型均可以使用小规模算法，例如，异常检测模型可以使用单分类支持向量机 SVM，分类模型可以使用二分类 SVM。这样，在身份认证过程中，算法开销小，无需额外的硬件支持，该身份认证模型可以在用户端侧进行训练，能够实现用户端侧数据安全存储，避免上传云端造成的隐私安全问题。

结合第一方面，在第一方面的某些实现方式中，决策融合模型的权重参数是通过将第二样本数据中的第二操作行为样本数据输入到所述第一认证模型和所述第二认证模型中，得到所述第一认证模型和所述第二认证模型输出的所述第二操作行为样本数据的识别结果，以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练得到的，所述第二样本数据包括所述第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户。

在本申请实施例中，通过对决策融合模型进行训练，得到更优的模型参数，例如，得到更优的认证模型的权重比例，进一步提高了身份认证的准确性。

结合第一方面，在第一方面的某些实现方式中，第一识别结果包括：第一操作行为数据对应的匹配分数和/或第一操作行为数据对应的匹配结果；第二识别结果包括第二操作行为数据对应的匹配分数和/或第二操作行为数据对应的匹配结果；其中，第一操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，第一操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，第一操作行为数据对应的匹配结果包括基于至少两个阈值和第一操作行为数据对应的匹配分数确定的至少两个匹配结果；第二操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，第二操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，第二操作行为数据对应的匹配结果包括基于至少两个阈值和第二操作行为数据对应的匹配分数确定的至少两个匹配结果。

下面举例说明第一识别结果和第二识别结果。

两个认证模型输出的识别结果分别包括：异常检测模型输出的识别结果和分类模型输出的识别结果。

异常检测模型输出的识别结果包括：由异常检测模型输出的第一操作行为数据对应的匹配分数 A 以及第一操作行为数据对应的匹配结果 A。

例如，至少两个阈值包括第一阈值 A 和第二阈值 A，第一阈值 A 大于第二阈值 A。由异常检测模型输出的第一操作行为数据对应的匹配结果 A 包括：基于第一阈值 A 确定的匹配结果和基于第二阈值 A 确定的匹配结果。当匹配分数 A 大于或等于第一阈值 A 时，基于第一阈值 A 确定的匹配结果为认证用户；当匹配分数 A 小于第一阈值 A 时，基于第一阈值 A 确定的匹配结果为非认证用户。当匹配分数 A 大于或等于第二阈值 A 时，基于第二阈值 A 确定的匹配结果为认证用户；当匹配分数 A 小于第二阈值 A 时，基于第二阈值 A 确定的匹配结果为非认证用户。

分类模型输出的识别结果包括：由分类模型输出的第二操作行为数据对应的匹配分数B以及第二操作行为数据对应的匹配结果B。

例如，至少两个阈值包括第一阈值B和第二阈值B，第一阈值B大于第二阈值B。由分类模型输出的第二操作行为数据对应的匹配结果B包括：基于第一阈值B确定的匹配结果和基于第二阈值B确定的匹配结果。当匹配分数B大于或等于第一阈值B时，基于第一阈值B确定的匹配结果为认证用户；当匹配分数B小于第一阈值B时，基于第一阈值B确定的匹配结果为非认证用户。当匹配分数B大于或等于第二阈值B时，基于第二阈值B确定的匹配结果为认证用户；当匹配分数B小于第二阈值B时，基于第二阈值B确定的匹配结果为非认证用户。

示例性地，该至少两个阈值可以是根据所述识别结果的准确率确定的。

在本申请实施例中，认证模型输出的识别结果包括匹配分数和至少两个匹配结果，通过不同的阈值能够调节认证模型的不同性能，以使认证模型的性能达到预期，例如，通过不同的阈值调节模型的抗攻击能力和机主识别率，以使认证模型的性能达到平衡。此外，区别于现有认证模型仅能提供一种识别结果，本方案能够为决策融合模型提供更多的特征，有利于提高决策融合模型认证的准确性，从而提高身份认证的准确性。

结合第一方面，在第一方面的某些实现方式中，将第一识别结果、所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果，包括：根据第一操作行为数据对应的匹配分数得到第一分数特征；根据第二操作行为数据对应的匹配分数得到第二分数特征；以所述第一分数特征、所述第二分数特征、所述第一识别结果和所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果。

例如，根据第一操作行为数据对应的匹配分数得到分数特征，包括：对该匹配分数进行数学运算，得到分数特征。

在本申请实施例中，对匹配分数进行特征提取，进一步为决策融合模型提供更多的特征，有利于提高决策融合模型认证的准确性，从而提高了身份认证的准确性。

结合第一方面，在第一方面的某些实现方式中，第一操作行为数据和/或第二操作行为数据包括以下数据中的至少一种：触摸点X/Y轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度X/Y/Z轴数据或陀螺仪X/Y/Z轴数据。

结合第一方面，在第一方面的某些实现方式中，认证模型的模型参数是根据第三样本数据中的第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果进行训练得到的，第三操作行为样本数据对应的身份认证结果是通过将第三操作行为样本数据输入第一认证模型和第二认证模型中，得到第三操作行为样本数据的识别结果，将第三操作行为样本数据的识别结果输入决策融合模型中得到的，第三样本数据包括：第三操作行为样本数据。

在获取样本数据的过程中，可能由于用户有意识或无意识的行为等引入错误的数据，造成样本数据对应的标签出现错误。在本申请实施例中，根据决策融合模型的身份认证结果对认证模型再次训练，以其输出实现反馈，再次对认证模型进行训练，能够进一步提高认证模型的准确度，从而进一步提高身份认证模型的准确度。

第二方面，提供了一种身份认证模型的训练方法，该身份认证模型包括第一认证模型、

第二认证模型和决策融合模型，其中，所述第一、第二认证模型分别为异常检测模型和分类模型，该方法包括：获取第二样本数据，所述第二样本数据包括第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户；将所述第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到所述第二操作行为数据的识别结果，所述第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括第一操作行为样本数据和所述第一操作行为样本数据对应的标签，所述第一操作行为样本数据对应的标签用于表示所述第一操作行为样本数据对应的用户为认证用户或非认证用户，所述第二认证模型的模型参数是基于第五样本数据进行训练得到的，所述第五样本数据包括第五操作行为样本数据和所述第五操作行为样本数据对应的标签，所述第五操作行为样本数据对应的标签用于表示所述第五操作行为数据对应的用户为认证用户或非认证用户；以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型。

在本申请实施例中，认证用户的操作行为数据可以称为正样本，非认证用户的操作行为数据可以称为负样本。

样本数据可以是根据传感器采集的原始数据确定的。具体地，可以从原始数据中提取特征数据，得到样本数据。该传感器可以包括触屏传感器和/或运动传感器。

或者，样本数据也可以包括预先设置的数据。

例如，正样本可以是根据传感器采集的原始数据确定，负样本可以是预先设置的数据。

在本申请实施例中，将两个认证模型的识别结果输入决策融合模型进行决策融合，得到身份认证结果，通过对决策融合模型进行训练，能够提高身份认证的准确性。同时，通过用户的操作行为数据进行身份验证，不会改变用户的用机习惯，有利于实现无感验证。

此外，采用异常检测模型和分类模型，一方面通过异常检测模型提高了认证用户识别率，另一方面通过分类模型提高了抗攻击能力，整体上提高了身份认证模型的识别能力。

此外，异常检测模型和分类模型均可以使用小规模算法，例如，异常检测模型可以使用单分类支持向量机 SVM，分类模型可以使用二分类 SVM。这样，在身份认证过程中，算法开销小，无需额外的硬件支持，该身份认证模型可以在用户端侧进行训练，能够实现用户端侧数据安全存储，避免上传云端造成的隐私安全问题。

需要说明的是，第一样本数据和第二样本数据可以相同，也可以不同。

结合第二方面，在第二方面的某些实现方式中，所述第二操作行为样本数据的识别结果包括所述第一认证模型输出的识别结果和所述第二认证模型输出的识别结果；所述第一认证模型输出的识别结果包括：所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第一认证模型输出的第二操作行为样本对应的匹配结果；所述第二认证模型输出的识别结果包括：所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第二认证模型输出的第二操作行为样本数据对应的匹配结果；其中，所述第二操作行为样本数据对应的匹配分数用于指示所述第二操作行为样本数据对应的用户被识别为认证用户的概率，所述第二操作行为样本数据对应的匹配结果用于指示所述第二操作行为样本数据对应的用户被识别为认证用户或非认证用户，所述第二操作行为样

本数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为样本数据对应的匹配分数确定的至少两个匹配结果。

应理解，两个认证模型的至少两个阈值可以不同。

示例性地，该两个认证模型分别为异常检测模型和分类模型。第二操作行为样本数据的识别结果，包括：异常检测模型输出的第二操作行为样本数据的识别结果和分类模型输出的第二操作行为样本数据的识别结果。

异常检测模型输出的第二操作行为样本数据的识别结果包括：由异常检测模型输出的第二操作行为样本数据对应的匹配分数 A 以及第二操作行为样本数据对应的匹配结果 A。

例如，至少两个阈值包括第一阈值 A 和第二阈值 A，第一阈值 A 大于第二阈值 A。由异常检测模型输出的第二操作行为样本数据对应的匹配结果 A 包括：基于第一阈值 A 确定的匹配结果和基于第二阈值 A 确定的匹配结果。当匹配分数 A 大于或等于第一阈值 A 时，基于第一阈值 A 确定的匹配结果为认证用户；当匹配分数 A 小于第一阈值 A 时，基于第一阈值 A 确定的匹配结果为非认证用户。当匹配分数 A 大于或等于第二阈值 A 时，基于第二阈值 A 确定的匹配结果为认证用户；当匹配分数 A 小于第二阈值 A 时，基于第二阈值 A 确定的匹配结果为非认证用户。

分类模型输出的识别结果包括：由分类模型输出的第二操作行为样本数据对应的匹配分数 B 以及第二操作行为样本数据对应的匹配结果 B。

例如，至少两个阈值包括第一阈值 B 和第二阈值 B，第一阈值 B 大于第二阈值 B。由分类模型输出的第二操作行为样本数据对应的匹配结果 B 包括：基于第一阈值 B 确定的匹配结果和基于第二阈值 B 确定的匹配结果。当匹配分数 B 大于或等于第一阈值 B 时，基于第一阈值 B 确定的匹配结果为认证用户；当匹配分数 B 小于第一阈值 B 时，基于第一阈值 B 确定的匹配结果为非认证用户。当匹配分数 B 大于或等于第二阈值 B 时，基于第二阈值 B 确定的匹配结果为认证用户；当匹配分数 B 小于第二阈值 B 时，基于第二阈值 B 确定的匹配结果为非认证用户。

其中，第一阈值 A 与第一阈值 B 可以不同，也可以相同。第二阈值 A 和第二阈值 B 可以相同，也可以不同。

示例性地，该至少两个阈值可以是根据所述两个认证模型输出的第二操作行为样本数据对应的识别结果的准确率确定的。

在本申请实施例中，两个认证模型输出的识别结果包括匹配分数和至少两个匹配结果，区别于现有认证模型仅能提供一种识别结果，本方案能够为决策融合模型提供更多的特征，有利于训练出更好的决策融合模型，提高决策融合模型认证的准确性，从而提高身份认证的准确性。

结合第二方面，在第二方面的某些实现方式中，至少两个阈值包括第一阈值，方法还包括：获取第四样本数据，所述第四样本数据包括第四操作行为样本数据和所述第四操作行为样本数据对应的标签，所述第四操作行为样本数据对应的标签用于表示所述第四操作行为样本数据对应的用户为认证用户或非认证用户；将所述第四操作行为样本数据输入所述第一认证模型，得到所述第一认证模型输出的所述第四操作行为样本数据对应的匹配分数，所述第四操作行为样本数据对应的匹配分数用于指示所述第四操作行为样本数据对应的用户被识别为认证用户的概率；基于多个候选阈值确定所述第四操作行为样本数据对应

的匹配分数对应的多个候选匹配结果，所述多个候选匹配结果用于指示所述第四操作行为样本数据对应的用户被识别为认证用户或非认证用户；将所述多个候选匹配结果中准确率满足预设条件的候选匹配结果对应的候选阈值确定为所述第一阈值。

示例性地，该预设条件可以为候选匹配结果的准确率达到设定阈值。

需要说明的是，第二认证模型的第一阈值也可以通过上述方式确定，此处不再赘述。

在本申请实施例中，从候选阈值中确定满足预设条件的第一阈值，通过不同的第一阈值能够调节认证模型的不同性能，以使认证模型的性能达到预期，例如，通过不同的阈值调节模型的抗攻击能力和机主识别率，有利于训练出更好的决策融合模型，提高决策融合模型认证的准确性，从而提高身份认证的准确性。

结合第二方面，在第二方面的某些实现方式中，以所述第二操作行为数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型，包括：根据所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第一分数特征；根据所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第二分数特征；以所述第二操作行为样本数据的第一分数特征、第二操作行为样本数据的第二分数特征和所述第二操作行为样本数据的识别结果作为决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练。

在本申请实施例中，对匹配分数进行特征提取，进一步为决策融合模型提供更多的特征，有利于训练出更好的决策融合模型，提高决策融合模型认证的准确性，从而提高身份认证的准确性。

结合第二方面，在第二方面的某些实现方式中，第二操作行为样本数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

第一操作行为样本数据、第三操作行为样本数据、第四操作行为样本数据或第五操作行为样本数据也可以包括上述数据中的至少一种。

结合第二方面，在第二方面的某些实现方式中，第二样本数据是根据用户在触摸屏上的滑动时长和/或所述用户在触摸屏上的触摸点数进行筛选得到的。

具体地，在从传感器采集的原始数据中提取特征数据之前，可以根据用户在触摸屏上的滑动时长和/或所述用户在触摸屏上的触摸点数对原始数据进行预处理，筛选出有效操作行为数据。然后对有效操作行为数据提取特征数据，得到第二样本数据。

例如，例如，用户的触摸点数大于预设阈值即为有效触屏行为，从原始数据中筛选得到满足用户的触摸点数大于预设阈值的操作行为数据作为有效操作行为数据。。然后对有效操作行为数据提取特征数据，得到第二样本数据。

由于用户可能有意识或无意识的产生异常行为，这样的数据被采集后作为训练样本会影响训练样本的准确性，进而影响身份认证的结果，在本申请实施例中，通过对原始数据进行筛选，剔除用户本身的异常操作行为数据，提高了训练样本的准确性，从而提高了模型训练的准确性。

结合第二方面，在第二方面的某些实现方式中，方法还包括：获取第三样本数据，其中，所述第三样本数据包括：第三操作行为样本数据；将所述第三操作行为样本数据输入到所述第一认证模型中，得到所述第一认证模型输出的第三操作行为样本数据的识别结果；将所述第三操作行为样本数据输入到所述第二认证模型中，得到所述第二认证模型输出的第三操作行为样本数据的识别结果；将所述第一认证模型输出的第三操作行为样本数据的识别结果、所述第二认证模型输出的第三操作行为样本数据的识别结果输入到所述训练好的决策融合模型中，得到所述第三操作行为样本数据对应的身份认证结果；根据所述第三操作行为样本数据和所述第三操作行为样本数据对应的身份认证结果对所述第一认证模型和/或所述第二认证模型进行训练。

也就是说在基于第一样本数据对该至少两个认证模型训练后，可以根据第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果对两个认证模型再次进行训练。

示例性地，第一样本操作行为数据和第三操作行为样本数据可以包括相同的样本数据，根据第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果对两个认证模型进行训练，包括：根据第一操作行为样本数据对应的标签和第三操作行为样本数据对应的身份认证结果，筛选第一样本数据，基于筛选后的第一样本数据对至少两个认证模型再次进行训练。

具体地，可以从第一样本数据中剔除标签与第三样本操作行为数据对应的身份认证结果不同的样本数据。

在获取样本数据的过程中，可能由于用户有意识或无意识的行为等引入错误的数据，造成样本数据对应的标签出现错误。在本申请实施例中，根据决策融合模型的身份认证结果对认证模型再次训练，以其输出实现反馈，再次对认证模型进行训练，能够进一步提高认证模型的准确度，从而进一步提高身份认证模型的准确度。

应理解，在上述第一方面中对相关内容的扩展、限定、解释和说明也适用于第二方面中相同的内容。

第三方面，提供了一种身份认证的装置，装置包括用于执行上述第一方面以及第一方面中的任意一种实现方式中的方法的模块或单元。

第四方面，提供了一种身份认证模型的训练装置，所述装置包括用于执行上述第二方面以及第二方面中的任意一种实现方式中的方法的模块或单元。

第五方面，提供了一种身份认证的装置，包括输入输出接口、处理器和存储器。该处理器用于控制输入输出接口收发信息，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得该训练装置执行上述第一方面以及第一方面中的任意一种实现方式中的方法。

可选地，上述装置可以是终端设备/服务器，也可以是终端设备/服务器内的芯片。

可选地，上述存储器可以位于处理器内部，例如，可以是处理器中的高速缓冲存储器（cache）。上述存储器还可以位于处理器外部，从而独立于处理器，例如，装置的内部存储器（memory）。

第六方面，提供了一种身份认证模型的训练装置，包括输入输出接口、处理器和存储器。该处理器用于控制输入输出接口收发信息，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得该训练装置执行上述第一方面以及第一方

面中的任意一种实现方式中的方法。

可选地，上述训练装置可以是终端设备/服务器，也可以是终端设备/服务器内的芯片。

可选地，上述存储器可以位于处理器内部，例如，可以是处理器中的高速缓冲存储器（cache）。上述存储器还可以位于处理器外部，从而独立于处理器，例如，训练装置的内部存储器（memory）。

第七方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行上述各方面中的方法。

需要说明的是，上述计算机程序代码可以全部或者部分存储在第一存储介质上，其中，第一存储介质可以与处理器封装在一起的，也可以与处理器单独封装，本申请实施例对此不作具体限定。

第八方面，提供了一种计算机可读介质，所述计算机可读介质存储有程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行上述各方面中的方法。

第九方面，提供一种芯片，所述芯片包括处理器与数据接口，所述处理器通过所述数据接口读取存储器上存储的指令，执行上述各方面中的方法。

可选地，作为一种实现方式，所述芯片还可以包括存储器，所述存储器中存储有指令，所述处理器用于执行所述存储器上存储的指令，当所述指令被执行时，所述处理器用于执行第一方面或第二方面中的任意一种实现方式中的方法。

上述芯片具体可以是现场可编程门阵列（field-programmable gate array，FPGA）或者专用集成电路（application-specific integrated circuit，ASIC）。

附图说明

图 1 是本申请实施例提供的一种人工智能主体框架示意图；

图 2 为本申请实施例提供的一种系统架构的结构示意图；

图 3 为本申请实施例提供的另一种系统架构的结构示意图；

图 4 为本申请实施例提供的又一种系统架构的结构示意图；

图 5 为本申请实施例提供的一种身份认证模块的结构示意图；

图 6 为本申请实施例提供的一种身份认证模型的训练方法的示意性流程图；

图 7 为本申请实施例提供的另一种身份认证模型的训练方法的示意性流程图；

图 8 为本申请实施例提供的一种身份认证的方法的示意性流程图；

图 9 为本申请实施例提供的一种决策融合的示意性流程图；

图 10 为本申请实施例提供的另一种决策融合的示意性流程图；

图 11 为本申请实施例提供的一种应用方法的示意性流程图；

图 12 为本申请实施例提供的一种应用场景的示意图；

图 13 是本申请实施例提供的另一种应用场景的示意图；

图 14 是本申请实施例提供的又一种应用场景的示意图；

图 15 是本申请实施例提供的身份认证模型的训练装置的示意性框图；

图 16 是本申请实施例提供的身份认证的装置的示意性框图；

图 17 是本申请实施例提供的身份认证模型的训练装置的示意性框图；

图 18 是本申请实施例提供的身份认证的装置的示意性框图；

图 19 是本申请实施例提供的身份认证的装置和身份认证模型的训练装置的示意性框图。

具体实施方式

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描述。

图 1 示出一种人工智能主体框架示意图，该主体框架描述了人工智能系统总体工作流程，适用于通用的人工智能领域需求。

下面从“智能信息链”（水平轴）和“信息技术（information technology，IT） 价值链”（垂直轴）两个维度对上述人工智能主题框架进行详细的阐述。

“智能信息链”反映从数据的获取到处理的一列过程。举例来说，可以是智能信息感知、智能信息表示与形成、智能推理、智能决策、智能执行与输出的一般过程。在这个过程中，数据经历了“数据—信息—知识—智慧”的凝练过程。

“IT 价值链”从人智能的底层基础设施、信息（提供和处理技术实现）到系统的产业生态过程，反映人工智能为信息技术产业带来的价值。

（1）基础设施:

基础设施为人工智能系统提供计算能力支持，实现与外部世界的沟通，并通过基础平台实现支撑。

基础设施可以通过传感器与外部沟通，基础设施的计算能力可以由智能芯片提供。

这里的智能芯片可以是中央处理器（central processing unit，CPU）、神经网络处理器（neural-network processing unit，NPU）、图形处理器（graphics processing unit，GPU）、专门应用的集成电路（application specific integrated circuit，ASIC)以及现场可编程门阵列（field programmable gate array，FPGA）等硬件加速芯片。

基础设施的基础平台可以包括分布式计算框架及网络等相关的平台保障和支持，可以包括云存储和计算、互联互通网络等。

例如，对于基础设施来说，可以通过传感器和外部沟通获取数据，然后将这些数据提供给基础平台提供的分布式计算系统中的智能芯片进行计算。

（2）数据:

基础设施的上一层的数据用于表示人工智能领域的数据来源。该数据涉及到图形、图像、语音、文本，还涉及到传统设备的物联网数据，包括已有系统的业务数据以及力、位移、液位、温度、湿度等感知数据。

（3）数据处理:

上述数据处理通常包括数据训练，机器学习，深度学习，搜索，推理，决策等处理方式。

其中，机器学习和深度学习可以对数据进行符号化和形式化的智能信息建模、抽取、预处理、训练等。

推理是指在计算机或智能系统中，模拟人类的智能推理方式，依据推理控制策略，利用形式化的信息进行机器思维和求解问题的过程，典型的功能是搜索与匹配。

决策是指智能信息经过推理后进行决策的过程，通常提供分类、排序、预测等功能。

（4）通用能力:

对数据经过上面提到的数据处理后，进一步基于数据处理的结果可以形成一些通用的能力，比如可以是算法或者一个通用系统，例如，翻译，文本的分析，计算机视觉的处理，语音识别，图像的识别等等。

（5）智能产品及行业应用:

智能产品及行业应用指人工智能系统在各领域的产品和应用，是对人工智能整体解决方案的封装，将智能信息决策产品化、实现落地应用，其应用领域主要包括：智能制造、智能交通、智能家居、智能医疗、智能安防、自动驾驶，平安城市，智能终端等。

本申请实施例可以应用在需要身份认证的场景中。例如，本申请实施例提供的方法能够应用在智能终端解锁、应用软件（application，APP）登录、安全支付等需要身份认证的场景。

下面对两种常见的应用场景进行简单的介绍。

终端设备解锁:

当终端设备（例如，手机）的屏幕处于锁屏状态，用户需要先解锁屏幕才能使用终端设备，通过身份认证解锁屏幕能够提高系统安全性，保护用户的财产、隐私安全等。

利用本申请实施例的身份认证的方法解锁屏幕，能够更准确地识别认证用户与非认证用户，提高了系统的安全性。

能够获得或者优化适用于相册分类的神经网络。接下来就可以利用该神经网络对图片进行分类，从而为不同的类别的图片打上标签，便于用户查看和查找。另外，这些图片的分类标签也可以提供给相册管理系统进行分类管理，节省用户的管理时间，提高相册管理的效率，提升用户体验。

安全支付:

在使用终端设备（例如，手机）进行支付时，用户需要通过身份认证才能执行支付操作，以保护用户的财产、隐私安全等。

通过采用本申请实施例的身份认证的方法，能够更准确地识别认证用户与非认证用户，提高系统的安全性。

为了便于理解本申请实施例，下面先对本申请实施例涉及的相关术语的相关概念进行介绍。

（1）支持向量机（support vector machine, SVM）

支持向量机是一种二分类模型，目的是寻找一个超平面对样本数据进行分割。SVM的学习策略是间隔最大化，可形式化为一个求解凸二次规划问题。

（2）神经网络

神经网络可以是由神经单元组成的，神经单元可以是指以 xs 和截距 1 为输入的运算单元，该运算单元的输出可以为:

$$h_{W,b}(x)=f\left(W^{T}x\right)=f(\sum_{s=1}^{n}W_{s}x_{s}+b) \qquad (1\text{-}1)$$

其中，s=1、2、……n，n 为大于 1 的自然数，W_s 为 x_s 的权重，b 为神经单元的偏置。f 为神经单元的激活函数（activation functions），用于将非线性特性引入神经网络中，来将神经单元中的输入信号转换为输出信号。该激活函数的输出信号可以作为下一层卷积层的输入，激活函数可以是 sigmoid 函数。神经网络是将多个上述单一的神经单元联结在一

起形成的网络，即一个神经单元的输出可以是另一个神经单元的输入。每个神经单元的输入可以与前一层的局部接受域相连，来提取局部接受域的特征，局部接受域可以是由若干个神经单元组成的区域。

（3）深度神经网络

深度神经网络（deep neural network，DNN），也称多层神经网络，可以理解为具有多层隐含层的神经网络。按照不同层的位置对 DNN 进行划分，DNN 内部的神经网络可以分为三类：输入层，隐含层，输出层。一般来说第一层是输入层，最后一层是输出层，中间的层数都是隐含层。层与层之间是全连接的，也就是说，第 i 层的任意一个神经元一定与第 i+1 层的任意一个神经元相连。

虽然 DNN 看起来很复杂，但是就每一层的工作来说，其实并不复杂，简单来说就是如下线性关系表达式：$\vec{y}=\alpha(W\vec{x}+\vec{b})$，其中，$\vec{x}$是输入向量，$\vec{y}$是输出向量，$\vec{b}$是偏移向量，$W$是权重矩阵（也称系数），$\alpha()$是激活函数。每一层仅仅是对输入向量$\vec{x}$经过如此简单的操作得到输出向量$\vec{y}$。由于 DNN 层数多，系数$W$和偏移向量$\vec{b}$的数量也比较多。这些参数在 DNN 中的定义如下所述：以系数W为例：假设在一个三层的 DNN 中，第二层的第 4 个神经元到第三层的第 2 个神经元的线性系数定义为W_{24}^{3}。上标 3 代表系数W所在的层数，而下标对应的是输出的第三层索引 2 和输入的第二层索引 4。

综上，第 L−1 层的第 k 个神经元到第 L 层的第 j 个神经元的系数定义为W_{jk}^{L}。

需要注意的是，输入层是没有W参数的。在深度神经网络中，更多的隐含层让网络更能够刻画现实世界中的复杂情形。理论上而言，参数越多的模型复杂度越高，“容量”也就越大，也就意味着它能完成更复杂的学习任务。训练深度神经网络的也就是学习权重矩阵的过程，其最终目的是得到训练好的深度神经网络的所有层的权重矩阵（由很多层的向量W形成的权重矩阵）。

（4）损失函数

在训练深度神经网络的过程中，因为希望深度神经网络的输出尽可能的接近真正想要预测的值，所以可以通过比较当前网络的预测值和真正想要的目标值，再根据两者之间的差异情况来更新每一层神经网络的权重向量（当然，在第一次更新之前通常会有化的过程，即为深度神经网络中的各层预先配置参数），比如，如果网络的预测值高了，就调整权重向量让它预测低一些，不断地调整，直到深度神经网络能够预测出真正想要的目标值或与真正想要的目标值非常接近的值。因此，就需要预先定义“如何比较预测值和目标值之间的差异”，这便是损失函数（loss function）或目标函数（objective function），它们是用于衡量预测值和目标值的差异的重要方程。其中，以损失函数举例，损失函数的输出值（loss）越高表示差异越大，那么深度神经网络的训练就变成了尽可能缩小这个 loss 的过程。

（5）反向传播算法

神经网络可以采用误差反向传播（back propagation，BP）算法在训练过程中修正的神经网络模型中参数的大小，使得神经网络模型的重建误差损失越来越小。具体地，前向传递输入信号直至输出会产生误差损失，通过反向传播误差损失信息来更新的神经网络模型中参数，从而使误差损失收敛。反向传播算法是以误差损失为主导的反向传播运动，旨在

得到最优的神经网络模型的参数，例如权重矩阵。

如图 2 所示，本申请实施例提供了一种系统架构 100。系统架构 100 包括执行设备 110、训练设备 120、数据库 130、客户设备 140、数据存储系统 150、以及数据采集系统 160。

另外，执行设备 110 包括计算模块 111、I/O 接口 112、预处理模块 113 和预处理模块 114。其中，计算模块 111 中可以包括目标模型/规则 101，预处理模块 113 和预处理模块 114 是可选的。

在图 2 中，数据采集设备 160 用于采集训练数据。针对本申请实施例的身份认证的方法来说，训练数据可以包括用户的操作行为数据以及用户的操作行为数据对应的身份认证结果。例如，用户包括认证用户和非认证用户，用户的操作行为数据对应的身份认证结果包括认证用户或非认证用户。

在采集到训练数据之后，数据采集设备 160 将这些训练数据存入数据库 130，训练设备 120 基于数据库 130 中维护的训练数据训练得到目标模型/规则 101。

下面对训练设备 120 基于训练数据得到目标模型/规则 101 进行描述，训练设备 120 对输入的用户的操作行为数据进行处理，将输出的身份认证结果与真实的用户的操作行为数据对应的身份认证结果进行对比，直到训练设备 120 输出的身份认证结果与真实的用户的操作行为数据对应的身份认证结果的差值小于一定的阈值，从而完成目标模型/规则 101 的训练。

上述目标模型/规则 101 能够用于进行身份认证。本申请实施例中的目标模型/规则 101 具体可以包括神经网络或 SVM 等。

需要说明的是，在实际的应用中，所述数据库 130 中维护的训练数据不一定都来自于数据采集设备 160 的采集，也有可能是从其他设备接收得到的。另外需要说明的是，训练设备 120 也不一定完全基于数据库 130 维护的训练数据进行目标模型/规则 101 的训练，也有可能从云端或其他地方获取训练数据进行模型训练，上述描述不应该作为对本申请实施例的限定。

根据训练设备 120 训练得到的目标模型/规则 101 可以应用于不同的系统或设备中，如应用于图 2 所示的执行设备 110，所述执行设备 110 可以是终端，如手机终端，平板电脑，笔记本电脑，增强现实（augmented reality，AR）AR/虚拟现实（virtual reality，VR），车载终端等，还可以是服务器或者云端等。在图 2 中，执行设备 110 配置输入/输出（input/output，I/O）接口 112，用于与外部设备进行数据交互，用户可以通过客户设备 140 向 I/O 接口 112 输入数据，所述输入数据在本申请实施例中可以包括：客户设备输入的用户的操作行为数据。这里的客户设备 140 具体可以是终端设备。

预处理模块 113 和预处理模块 114 用于根据 I/O 接口 112 接收到的输入数据进行预处理，例如，预处理模块 113 可以用于从待认证用户的操作行为数据中提取特征数据。在本申请实施例中，也可以没有预处理模块 113 和预处理模块 114（也可以只有其中的一个预处理模块），而直接采用计算模块 111 对输入数据进行处理。

在执行设备 110 对输入数据进行预处理，或者在执行设备 110 的计算模块 111 执行计算等相关的处理过程中，执行设备 110 可以调用数据存储系统 150 中的数据、代码等以用于相应的处理，也可以将相应处理得到的数据、指令等存入数据存储系统 150 中。

最后，I/O 接口 112 将处理结果，如上述得到的身份认证结果返回给客户设备 140，

从而提供给用户。

在本申请实施例中，上述身份认证结果可以包括身份认证成功或身份认证失败，身份认证成功指的是待认证用户为认证用户，身份认证失败指的是待认证用户为非认证用户。例如，该身份认证结果可以包括解锁成功或者解锁失败。或者，该身份认证结果可以包括登录成功或者登录失败。应理解，以上仅为示意，在不同应用场景中，具体的身份认证结果可以包括不同的形式。本申请实施例对此不做限制。

值得说明的是，训练设备 120 可以针对不同的目标或称不同的任务，基于不同的训练数据生成相应的目标模型/规则 101，该相应的目标模型/规则 101 即可以用于实现上述目标或完成上述任务，从而为用户提供所需的结果。

在图 2 中所示情况下，用户可以手动给定输入数据，该手动给定可以通过 I/O 接口 112 提供的界面进行操作。另一种情况下，客户设备 140 可以自动地向 I/O 接口 112 发送输入数据，如果要求客户设备 140 自动发送输入数据需要获得用户的授权，则用户可以在客户设备 140 中设置相应权限。用户可以在客户设备 140 查看执行设备 110 输出的结果，具体的呈现形式可以是显示、声音、动作等具体方式。客户设备 140 也可以作为数据采集端，采集如图所示输入 I/O 接口 112 的输入数据及输出 I/O 接口 112 的输出结果作为新的样本数据，并存入数据库 130。当然，也可以不经过客户设备 140 进行采集，而是由 I/O 接口 112 直接将如图所示输入 I/O 接口 112 的输入数据及输出 I/O 接口 112 的输出结果，作为新的样本数据存入数据库 130。

值得注意的是，图 2 仅是本申请实施例提供的一种系统架构的示意图，图中所示设备、器件、模块等之间的位置关系不构成任何限制，例如，在图 2 中，数据存储系统 150 相对执行设备 110 是外部存储器，在其它情况下，也可以将数据存储系统 150 置于执行设备 110 中。

如图 3 所示，本申请实施例提供了一种系统架构 300。该系统架构包括本地设备 301、本地设备 302 以及执行设备 310 和数据存储系统 350，其中，本地设备 301 和本地设备 302 通过通信网络与执行设备 310 连接。

执行设备 310 可以由一个或多个服务器实现。可选的，执行设备 310 可以与其它计算设备配合使用，例如：数据存储器、路由器、负载均衡器等设备。执行设备 310 可以布置在一个物理站点上，或者分布在多个物理站点上。执行设备 310 可以使用数据存储系统 350 中的数据，或者调用数据存储系统 350 中的程序代码来实现本申请实施例的身份认证的方法以及身份认证模型的训练方法。

示例性地，数据存储系统 350 可以部署于本地设备 301 或者本地设备 302 中，例如，数据存储系统 350 可以用于存储训练样本。

具体地，在一种实现方式中，执行设备 310 可以执行以下过程：

获取第二样本数据，所述第二样本数据包括第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户；

将所述第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到所述第二操作行为样本数据的识别结果，所述第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括第一操作行为样本数据和所述第一

操作行为样本数据对应的标签，所述第一操作行为样本数据对应的标签用于表示所述第一操作行为样本数据对应的用户为认证用户或非认证用户，所述第二认证模型的模型参数是基于第五样本数据进行训练得到的，所述第五样本数据包括第五操作行为样本数据和所述第五操作行为样本数据对应的标签，所述第五操作行为样本数据对应的标签用于表示所述第五操作行为数据对应的用户为认证用户或非认证用户；

以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型。

通过上述过程执行设备 310 能够得到身份认证模型，该身份认证模型提高身份认证的准确率。

用户可以操作各自的用户设备（例如本地设备 301 和本地设备 302）与执行设备 310 进行交互。每个本地设备可以表示任何计算设备，例如个人计算机、计算机工作站、智能手机、平板电脑、智能摄像头、智能汽车或其他类型蜂窝电话、媒体消费设备、可穿戴设备、机顶盒、游戏机等。

每个用户的本地设备可以通过任何通信机制/通信标准的通信网络与执行设备 310 进行交互，通信网络可以是广域网、局域网、点对点连接等方式，或它们的任意组合。

在一种实现方式中，本地设备 301、本地设备 302 从执行设备 310 获取到身份认证模型的相关参数，将身份认证模型部署在本地设备 301、本地设备 302 上，利用该身份认证模型进行身份认证。

在另一种实现中，执行设备 310 上可以直接部署身份认证模型，执行设备 310 通过从本地设备 301 和本地设备 302 获取待处理用户行为，并采用身份认证模型对待处理用户行为进行身份认证。

上述执行设备 310 也可以为云端设备，此时，执行设备 310 可以部署在云端；或者，上述执行设备 310 也可以为终端设备，此时，执行设备 310 可以部署在用户终端侧，本申请实施例对此并不限定。

示例性地，数据存储系统 350 可以部署于本地设备 301 或者本地设备 302 中，例如，数据存储系统 350 可以用于存储训练样本。

示例性地，数据存储系统 350 可以独立于本地设备 301 或者本地设备 302，单独部署在存储设备上，存储设备可以与本地设备进行交互，获取本地设备中用户行为日志，并存入存储设备中。

图 4 示出了本申请实施例提供的系统架构的示意图。如图 4 所示，系统 400 中可以包括 APP410、数据采集模块 420、身份认证模块 440 和存储模块 440。

应用层中包括多个 APP410，APP410 能够在特定场景下，例如应用锁解锁、支付应用时，请求身份认证服务。这样可以实现无感身份认证。应用锁解锁也可以称为应用解锁，即在身份认证后打开应用。

示例性地，该 APP410 可以是集成身份认证软件开发工具包（software development kit，SDK）的 APP。

框架（framework）层提供数据采集模块 420 和身份认证模块 430，可以供上层 APP 使用。

数据采集模块 420，用于监听传感器的数据。示例性地，传感器包括：环境光传感器，健康类传感器、声音传感器、触屏传感器和运动传感器。运动传感器指的能够实时监测设备移动状态的传感器，能够内嵌于设备中。例如，加速度、陀螺仪或磁力计等。声音传感器可以包括麦克风或扬声器等。

具体地，数据采集模块可以通过本地（native）层的传感器管理器（sensor manager）监听传感器的数据。

传感器管理器是传感器事件的总管理器，用于读取实践、分发事件等。例如，传感器管理器可以创建监听来监听某个传感器的事件。

具体地，传感器管理器（sensor manager）通过内核（kernel）中的传感器驱动与传感器实现交互。

身份认证模块 430，用于身份认证。例如，该身份认证模块 430 执行本申请实施例中的身份认证方法实现身份认证。进一步地，身份认证模块 430，还用于身份认证模型的建模训练。例如，该身份认证模块 430 执行本申请实施例中的身份认证模型的训练方法以得到训练好的身份认证模型。应理解，图 4 中由身份认证模块 430 完成身份认证模型的建模训练仅为示意。可替换地，身份认证模型的建模训练也可以由其他设备完成。该训练好的身份认证模型可以存储于存储模块 440 中。

存储模块 440，用于存储用户的操作行为数据和身份认证模型，实现安全存储。如图 4 所示，用户的操作行为数据可以存储于操作行为数据库中。

图 5 示出了本申请实施例中的一种身份认证模块 500 的示意性框图。图 5 可以作为图 4 中的身份认证模块 430 的一例。身份认证模块 500 能够实现特征提取 510、行为建模 520、行为匹配 530、增量学习 540、模型升级 550 以及防伪检测 560 等功能。

如图 5 所示，身份认证模块 500 可以用于实现特征提取 510。例如，从原始数据中提取特征数据，该特征数据可以输入身份认证模型中，以实现身份认证。原始数据指的是传感器采集的原始数据。进一步地，特征提取还包括，其他对特征数据的预处理操作，例如，从提取的特征数据中剔除无效特征数据。

可选地，身份认证模块 500 可以基于特征数据建立身份认证模型，或者说，基于特征数据实现身份认证模型的建模训练，即图 5 中的行为建模 520。示例性地，身份认证模块 500 可以执行图 6 中的方法 700 或图 7 中的方法 730 以训练身份认证模型。

身份认证模块 500 可以用于身份认证/行为匹配 530。具体地，将特征数据输入身份认证模型中，实现身份认证。示例性地，身份认证模块 500 可以执行图 8 中的方法 800，实现身份认证。应理解，该身份认证模型可以是身份认证模块 500 训练得到的，也就是说，该身份认证模块 500 可以用于建模，得到身份认证模型，然后利用该身份认证模型实现身份认证。可替换地，该身份认证模块 500 也可以利用其它设备训练得到的身份认证模型实现身份认证。

由于随着时间推移，用户的行为可能发生变化，因此用户的操作行为数据具有不稳定性。

可选地，身份认证模块 500 还可以用于增量学习 540。

增量学习是指一个学习系统能不断地从新样本中学习新的知识，并能保存大部分以前已经学习到的知识。

具体地，在得到训练好的身份认证模型后，身份认证模块 500 可以持续采集用户的操作行为数据，也即新增的用户的操作行为数据，通过增量学习可以在原有的数据库的基础上，仅对由于新增的用户的操作行为数据所引起的变化进行身份认证模型的更新。

通过增量学习能够不断优化身份认证模型，适应变化的用户行为，增强识别能力。

可选地，身份认证模块 500 还可以用于实现模型升级 550。具体地，用于身份认证模型的结构的升级、与云服务实现交互等。

示例性地，身份认证模块 500 可以获取升级后的身份认证模型的结构参数，以更新原身份认证模型的结构参数。也就是升级身份认证模型的结构。该身份认证模型的结构参数可以是人为设定的。

进一步地，身份认证模块 500 可以对升级后的身份认证模型进行训练。例如，从原始数据中提取特征数据，基于特征数据对升级后的身份认证模型进行训练。

进一步地，身份认证模块 500 与云服务实现交互，具体地，可以将升级后的身份认证模型的结构参数发送至云服务。

可选地，身份认证模型 500 还可以用于实现防伪检测 560。具体地，用于验证身份认证模块 500 的合法性等。例如，确保身份认证模型不会被篡改，实现安全存储。

图 6 示出了本申请实施例的身份认证模型的训练方法 700。方法 700 包括步骤 S710 至步骤 S720。该方法 700 可以由图 2 中的训练设备 120 执行。该训练设备可以是云服务设备，也可以是移动终端，例如，电脑、服务器等能够用来训练身份认证模型的设备。

下面对步骤 S710 至步骤 S720 进行详细介绍。

S710，获取第一样本数据。其中，第一样本数据包括：第一操作行为样本数据和第一操作行为样本数据对应的标签，第一操作行为样本数据对应的标签用于表示第一操作行为样本数据对应的用户为认证用户或非认证用户。

可选地，步骤 S710 还包括：获取第五样本数据。其中，第五样本数据包括：第五操作行为样本数据和第五操作行为样本数据对应的标签，第五操作行为样本数据对应的标签用于表示第五操作行为样本数据对应的用户为认证用户或非认证用户。

认证用户也可以理解为机主，非认证用户也可以理解为攻击者。认证用户的数据可以称为正样本，非认证用户的数据可以称为负样本。

示例性地，认证用户的操作行为样本数据为正样本，非认证用户的操作行为样本数据为负样本。

其中，该第一样本数据可以是根据传感器采集的原始数据确定的。例如，该传感器包括触屏传感器和/或运动传感器。或者，第一样本数据也可以包括预先设置的数据。

例如，正样本可以是根据传感器采集的原始数据确定的，负样本可以是预先设置的数据。

示例性地，通过传感器采集数据可以包括：屏幕解锁时，注册触屏传感器和/或运动传感器监听；屏幕锁屏时，注销触屏传感器和/或运动传感器监听。

其中，触屏传感器采集的原始数据包括：时间戳、触摸点 X/Y 轴坐标、触摸面积、触摸压力、动作（action）和屏幕方向等。

运动传感器采集的原始数据包括：时间戳、加速度 X/Y/Z 轴数据、陀螺仪 X/Y/Z 轴数据等。

应理解，以上仅为示意，传感器采集的数据可以包括以上中的任一项或几项，也可以包括其他数据。

action 指的是触屏事件。例如，当触屏行为为按下和抬起，则该触屏事件为用户的“点击”操作。当触屏行为为“按下、滑动和抬起”，则该触屏事件为用户的“滑动”操作。屏幕方向包括横屏或竖屏。

具体地，可以从原始数据中提取特征数据，得到第一样本数据。

可选地，第一操作行为样本数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

示例性地，第一操作行为样本数据可以包括上述任意一个或几个特征的相关值。该相关值可以包括：开始值、结束值、平均值、标准差、20%分位数、50%分位数、80%分位数。例如，第一样本数据可以包括：触摸点 X/Y 轴坐标的开始值和结束值，触摸面积的开始值、结束值、平均值、标准差、20%分位数、50%分位数和 80%分位数以及加速度 X/Y/Z 轴数据的平均值和标准差。

start 值以及 end 值的定义方式可以是预先设定的。例如，传感器采集的数据中包括 n 个触摸点。触屏速度的 start 值指的是第一个触摸点和第二个触摸点之间的速度；触屏速度的 end 值指的是第 n-1 个触摸点和第 n 个触摸点之间的速度。

可选地，在从原始数据中提取特征数据之前，可以对原始数据进行预处理，筛选出有效操作行为数据。然后对有效操作行为数据提取特征数据，得到第一操作行为样本数据。有效操作行为数据是在发生有效触屏行为的情况下采集的数据，其定义方式可以根据需要设定。例如，用户的触摸点数大于预设阈值即为有效触屏行为，从原始数据中筛选得到满足用户的触摸点数大于预设阈值的操作行为数据作为有效操作行为数据。

其中，一个触摸点代表一个触屏事件。触摸点数大于预设阈值指的是触屏事件超过预设阈值。

这样可以剔除用户本身的异常操作行为数据，提高了训练样本的准确性。

应理解，本申请实施例中对于第一样本数据的解释、说明、扩展等也适用于第五样本数据，本申请实施例中不再详细描述第五样本数据。

S720，建立身份认证模型。

可选地，在步骤 S720 之前，可以判断是否开始建立身份认证模型。

示例性地，当第一样本数据的采集的时段超过预设时长和/或第一样本数据的数据量超过预设数量，开始建立身份认证模型。如前所述，第一样本数据可以包括通过传感器采集的用户的操作行为数据，第一样本数据采集的时段可以包括传感器采集的时段。

或者，当第一样本数据中的正样本的采集的时段超过预设时长和/或正样本的数据量超过预设数量，开始建立身份认证模型。例如，预设时长为一周，预设数量为 2000。若认证用户使用该设备超过一周，即正样本的采集时段超过一周，且有效触屏行为达到 2000 次，即有效操作行为数据超过 2000，则开始建立异常检测模型。

在认证用户数据的采集满足一定时长、数据量达到一定数量的情况下，样本数据更能真实反映认证用户的习惯，通过设置模型建立的起始条件，能够得到更符合用户习惯的身份认证模型，提高了身份认证的准确率。

该身份认证模型包括至少两个认证模型，可以基于第一样本数据对第一认证模型进行训练，基于第五样本数据对第二认证模型进行训练。

可选地，该第一认证模型和第二认证模型分别为异常检测模型和分类模型。

下面以第一认证模型为异常检测模型，第二认证模型为分类模型为例，对身份认证模型的训练方法进行说明。

具体地，步骤 S720 包括步骤 S721 和步骤 S722。

S721，建立异常检测模型。

基于第一样本数据训练异常检测模型。

该异常检测（anomaly detection）模型用于检测异常数据，通过检测出非认证用户的数据来判断认证用户和非认证用户。

例如，异常检测模型可以采用单分类（one class）SVM 或孤立森林（isolation forest）等。应理解，本申请实施例对异常检测模型所采用的算法不做限制。

可选地，步骤 S721 包括设定异常检测模型的参数，例如，数据异常率。

由于认证用户可能有意识或无意识产生异常行为，设定数据异常率能够保证认证用户检测的准确率。例如，数据异常率设定为 0.1，理论上，能够保障认证用户的识别率达到 90%以上。

特征区分度会影响异常检测模型的识别能力。在训练异常检测模型的过程中，特征区分度差会导致“相似行为”增多。也就是将不同的操作行为数据识别为相同的操作行为数据，降低了整体的行为识别能力。

可选地，步骤 S721 包括选择最优特征组合。

具体地，可以通过特征工程选择最佳特征组合。

示例性地，每次选定若干特征，例如，从步骤 S710 的特征中选择若干特征，得到特征组合，将该特征组合输入异常检测模型中，得到准确率最高的异常检测模型对应的特征组合，将该特征组合作为最佳特征组合。

应理解，以上仅为示意，本申请实施例对特征选择的具体方式不做限定。

可选地，在训练异常检测模型前，可以是对第一数据样本进行预处理，例如，对第一数据样本进行标准化处理等。

S722，建立分类模型。

基于第五样本数据训练分类模型。

需要说明的是，第五样本数据中包括多个样本数据。用于训练异常检测模型的样本数据和用于训练分类模型的样本数据可以相同，也可以不同。

该分类模型可以为二分类模型，通过分类来判断认证用户和非认证用户。

例如，分类模型可以采用 SVM 或神经网络等。应理解，本申请实施例对分类模型所采用的算法不做限制。

可选地，步骤 S722 包括，确定分类模型的最优超参数。

示例性地，可以通过网格法确定分类模型的最优超参数。具体地，每次选定分类模型的超参数，并测试该分类模型的准确率，将准确率最高的分类模型对应的超参数作最优超参数。

应理解，以上仅为示意，本申请实施例对最优超参数的确定方式不做限定。

步骤 S722 包括，确定非认证用户的操作行为数据的类别 N，也就是 N 种非认证用户。例如，N=10。

理论上，若二分类模型已知的行为包括认证用户的行为和 N 种非认证用户的行为，即 N+1 种行为，非认证用户的行为被误识别为认证用户的概率为 1/(N+1)。增加非认证用户的类别能够有效降低误识率（false acceptance rate，FAR），但会提高拒识率（false rejection rate，FRR）。误识率降低能够提高抗攻击能力，拒识率提高会导致认证用户的识别率降低。当 FAR 的降幅小于 FRR 增幅时，整体的识别能力下降。

可选地，在训练分类模型前，可以是对第一样本数据进行预处理，例如，对第一样本数据进行标准化处理等。

应理解，步骤 S721 和步骤 S722 的执行顺序不分先后。例如，步骤 S721 和步骤 S722 可以同时执行。或者，步骤 S721 先执行，S722 后执行。或者，步骤 S722 先执行，步骤 S721 后执行。

由步骤 S721 和步骤 S722 可以得到训练好的异常检测模型和训练好的分类模型。

在应用该身份认证进行身份认证时，可以将异常检测模型的识别结果和分类模型的识别结果输入决策融合模型，将融合后的结果作为身份认证结果。本申请实施例中的识别结果可以包括输入的操作行为数据被识别为认证用户或非认证用户。具体地，识别结果可以包括输入的操作行为数据被识别为认证用户的概率或非认证用户的概率。

可选地，该决策融合模型用于根据该至少两个认证模型对应的权重对至少两个认证模型输出的识别结果进行加权计算，根据加权计算得到的结果确定身份认证结果。

该决策融合模型的模型参数，例如，该两个认证模型对应的权重，可以是预先设定的。或者，该权重可以是训练得到的。

可选地，方法 700 还包括建立决策融合模型。图 7 示出了本申请实施例的一种决策融合模型的训练方法 730 示意性流程图。本申请实施例中的身份认证模型包括至少两个认证模型和决策融合模型，对决策融合模型的训练也是身份认证模型的训练。该决策融合模型的训练方法也可以理解为身份认证模型的训练方法。方法 730 包括步骤 S731 至步骤 S733。

S731，获取第二样本数据。

第二样本数据包括第二操作行为样本数据及第二操作行为样本数据对应的标签，第二操作行为样本数据对应的标签用于指示第二操作行为样本数据所对应的用户为认证用户或非认证用户。

S732，将第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到第二操作行为样本数据的识别结果。

可选地，第二操作行为样本数据的识别结果包括第一认证模型输出的识别结果和第二认证模型输出的识别结果。

第一认证模型输出的识别结果包括：第一认证模型输出的第二操作行为样本数据对应的匹配分数和/或第一认证模型输出的第二操作行为样本对应的匹配结果；第二认证模型输出的识别结果包括：第二认证模型输出的第二操作行为样本数据对应的匹配分数和/或第二认证模型输出的第二操作行为样本数据对应的匹配结果；

其中，第二操作行为样本数据对应的匹配分数用于指示第二操作行为样本数据对应的用户被识别为认证用户的概率，第二操作行为样本数据对应的匹配结果用于指示第二操作

行为样本数据对应的用户被识别为认证用户或非认证用户，第二操作行为样本数据对应的匹配结果包括基于至少两个阈值和第二操作行为样本数据对应的匹配分数确定的至少两个匹配结果。

具体地，将第二操作行为样本数据输入认证模型中，可以得到匹配分数，根据该匹配分数和至少两个阈值可以确定第二操作行为样本数据对应的用户被识别为认证用户或非认证用户。

该至少两个阈值可以根据需要设置。

示例性地，该至少两个阈值可以是根据所述两个认证模型输出的第二操作行为样本数据对应的识别结果的准确率确定的。

示例性地，该至少两个阈值可以包括第一阈值和第二阈值。其中，第一阈值大于第二阈值。基于第一阈值得到的匹配结果可以称为第一阈值对应的匹配结果。基于第二阈值得到的匹配结果可以称为第二阈值对应的匹配结果。第一阈值对应的匹配结果置信度更高。

当该匹配分数大于或等于第一阈值时，则该第二操作行为样本数据对应的用户被识别为认证用户；当该匹配分数小于第一阈值时，则该第二操作行为样本数据对应的用户被识别为非认证用户。

当该匹配分数大于或等于第二阈值时，则该第二操作行为样本数据对应的用户被识别为认证用户；当该匹配分数小于第二阈值时，则该第二操作行为样本数据对应的用户被识别为非认证用户。

例如，该第二阈值可以为默认阈值。例如，匹配分数的取值范围为[0,1]，第二阈值为0.5，当该匹配分数大于或等于0.5时，该第二操作行为样本数据对应的用户被识别为认证用户；当该匹配分数小于0.5时，该第二操作行为样本数据对应的用户被识别为非认证用户。

下面以异常检测模型和分类模型为例说明第二操作行为样本数据的识别结果。

第二操作行为样本数据的识别结果，包括：异常检测模型输出的第二操作行为样本数据的识别结果和分类模型输出的第二操作行为样本数据的识别结果。

异常检测模型输出的第二操作行为样本数据的识别结果包括：由异常检测模型输出的第二操作行为样本数据对应的匹配分数A以及第二操作行为样本数据对应的匹配结果A。

例如，至少两个阈值包括第一阈值A和第二阈值A，第一阈值A大于第二阈值A。由异常检测模型输出的第二操作行为样本数据对应的匹配结果A包括：基于第一阈值A确定的匹配结果和基于第二阈值A确定的匹配结果。当匹配分数A大于或等于第一阈值A时，基于第一阈值A确定的匹配结果为认证用户；当匹配分数A小于第一阈值A时，基于第一阈值A确定的匹配结果为非认证用户。当匹配分数A大于或等于第二阈值A时，基于第二阈值A确定的匹配结果为认证用户；当匹配分数A小于第二阈值A时，基于第二阈值A确定的匹配结果为非认证用户。

分类模型输出的识别结果包括：由分类模型输出的第二操作行为样本数据对应的匹配分数B以及第二操作行为样本数据对应的匹配结果B。

例如，至少两个阈值包括第一阈值B和第二阈值B，第一阈值B大于第二阈值B。由分类模型输出的第二操作行为样本数据对应的匹配结果B包括：基于第一阈值B确定的匹配结果和基于第二阈值B确定的匹配结果。当匹配分数B大于或等于第一阈值B时，

基于第一阈值 B 确定的匹配结果为认证用户；当匹配分数 B 小于第一阈值 B 时，基于第一阈值 B 确定的匹配结果为非认证用户。当匹配分数 B 大于或等于第二阈值 B 时，基于第二阈值 B 确定的匹配结果为认证用户；当匹配分数 B 小于第二阈值 B 时，基于第二阈值 B 确定的匹配结果为非认证用户。

其中，第一阈值 A 与第一阈值 B 可以不同，也可以相同。第二阈值 A 和第二阈值 B 可以相同，也可以不同。

可选地，将测试样本集中的样本数据输入训练好的认证模型，得到该样本数据对应的匹配分数。基于多个候选阈值得到多个候选阈值对应的多个候选匹配结果。将多个候选匹配结果中满足预设条件的候选匹配结果对应的候选阈值确定为第一阈值。

具体地，可以通过如下步骤确定第一认证模型的第一阈值。

（1）获取第四样本数据，第四样本数据包括：第四操作行为样本数据和第四非操作行为样本数据对应的标签。第四操作行为样本数据对应的标签用于表示第四操作行为样本数据对应的用户为认证用户或非认证用户。

（2）将第四操作行为样本数据输入第一认证模型，得到第一认证模型输出的第四操作行为样本数据的匹配分数，第四操作行为样本数据的匹配分数用于指示第四操作行为样本数据对应的用户被识别为认证用户的概率。

（3）基于多个候选阈值确定第四操作行为样本数据的匹配分数对应的多个候选匹配结果，多个候选匹配结果包括第四操作行为样本数据对应的用户被识别为认证用户或非认证用户。

（4）将多个候选匹配结果中满足预设条件的候选匹配结果对应的候选阈值确定为第一阈值。

需要说明的是，第二认证模型的第一阈值也可以通过上述方式确定，此处不再赘述。

下面以异常检测模型和分类模型为例说明确定第一阈值的方法。为了便于描述，将异常检测模型对应的第一阈值称为第一阈值 A，用于确定第一阈值 A 的第四操作行为样本数据称为第四操作行为样本数据 A。分类模型对应的第一阈值称为第一阈值 B，用于确定第一阈值 B 的第四操作行为样本数据称为第四操作行为样本数据 B。

异常检测模型

如前所述，异常检测模型的参数包括数据异常率。由于认证用户可能有意识或无意识产生异常行为，调整异常数据率能够提高认证用户检测的准确率。

在步骤 S720 中可以设置数据异常率为 0.5，然后对异常检测模型进行训练。

将第四操作行为样本数据 A 输入训练好的异常检测模型，得到第四操作行为样本数据 A 对应的匹配分数 A。基于多个候选阈值得到多个候选阈值对应的多个候选匹配结果 A。将多个候选匹配结果 A 中准确率高于 90%的候选阈值作为第一阈值 A。

分类模型

将第四操作行为样本数据 B 输入训练好的分类模型，得到第四操作行为样本数据 B 对应的匹配分数 B。基于多个候选阈值得到多个候选阈值对应的多个候选匹配结果 B。将多个候选匹配结果 B 识中 FAR 满足预设条件的候选阈值作为第一阈值 A。

从候选阈值中确定满足预设条件的第一阈值，通过不同的第一阈值能够调节认证模型的不同性能，以使认证模型的性能达到预期，例如，通过不同的阈值能够调节模型的抗攻

击能力和机主识别率，以其达到平衡。

在本申请实施例中，两个认证模型输出的识别结果包括匹配分数和至少两个匹配结果，区别于现有认证模型仅能提供一种识别结果，本方案能够为决策融合模型提供更多的特征，有利于训练出更好的决策融合模型，提高决策融合模型认证的准确性，从而提高身份认证的准确性。

S733，以第二操作行为样本数据的识别结果作为决策融合模型的输入，以第二操作行为样本数据对应的标签作为决策融合模型的目标输出值对决策融合模型进行训练，得到训练好的决策融合模型。

例如，该决策融合模型可以为 SVM。

需要说明的是，上述对第一样本数据的说明、限定和扩展等也适用于第二样本数据。第一样本数据与第二样本数据可以相同，也可以不同。

下面以异常检测模型和分类模型为例进行说明。

将第二操作行为样本数据输入异常检测模型，输出第一识别结果；将第二操作行为样本数据输入分类模型，输出第二识别结果。将第一识别结果和第二识别结果输入决策融合模型，以第二操作行为样本数据对应的标签作为决策融合模型的目标输出值对决策融合模型进行训练，得到训练好的决策融合模型。

示例性地，异常检测模型和分类模型的识别结果可以为匹配分数，即该第二操作行为样本数据对应的用户被识别为认证用户的概率。匹配分数越高，表示第二操作行为样本数据对应的用户被识别为认证用户的概率越高。

例如，将第一识别结果和第二识别结果输入决策融合模型，得到身份认证结果，包括：根据第一识别结果和第二识别结果分别对应的权重进行加权计算，得到加权结果，根据该加权结果得到身份认证结果。例如，当该加权结果大于或等于设定阈值 A 时，认证成功，即该第二操作行为样本数据对应的用户被识别为认证用户；当该加权结果小于设定阈值 A 时，认证失败，即该第二操作行为样本数据对应的用户被识别为非认证用户。或者，当该加权结果大于设定阈值 A 时，认证成功，即该第二操作行为样本数据对应的用户被识别为认证用户；当该加权结果小于或等于设定阈值 A 时，认证失败，即该第二操作行为样本数据对应的用户被识别为非认证用户。或者，当该加权结果大于设定阈值 A 时，认证成功，即该第二操作行为样本数据对应的用户被识别为认证用户；当该加权结果小于设定阈值 B 时，认证失败，即第二操作行为样本数据对应的用户被识别为非认证用户；当该加权结果大于设定阈值 B 且小于设定阈值 A 时，无法识别。在上述方案中，对决策融合模型进行训练，对决策融合模型进行训练包括对至少两个认证模型对应的权重的训练。即对异常检测模型和分类模型的识别结果对应的权重进行训练，以得到最佳的权重比例。

可选地，步骤 S733 还包括：对第二操作行为样本数据对应的匹配分数进行特征提取，得到分数特征；以分数特征和第二操作行为样本数据的识别结果作为决策融合模型的输入，以第二操作行为样本数据对应的标签作为决策融合模型的目标输出值进行训练。

示例性地，对第二样本数据的匹配分数进行特征提取，包括：对该分数进行数学运算，例如加减乘除运算，将运算结果作为分数特征。

下面以异常检测模型和分类模型为例说明步骤 S733。

（1）将第二操作行为样本数据分别输入异常检测模型和分类模型，分别得到异常检

测模型和分类模型输出的识别结果。

异常检测模型输出的识别结果包括由异常检测模型输出的第二操作行为样本数据对应的匹配分数 A 以及第二操作行为样本数据对应的匹配结果 A。该匹配结果 A 包括第一阈值 A 对应的匹配结果和第二阈值 A 对应的匹配结果。

分类模型输出的识别结果包括由分类模型输出的第二操作行为样本数据对应的匹配分数 B 以及第二操作行为样本数据对应的匹配结果 B。该匹配结果 B 包括第一阈值 B 对应的匹配结果和第二阈值 B 对应的匹配结果。

（2）对异常检测模型对应的匹配分数和分类模型对应的匹配分数分别进行加减乘除运算，得到四个运算结果，作为四个分数特征。

将异常检测模型对应的匹配分数和分类模型对应的匹配分数作为两个分数特征。

示例性地，可以将异常检测模型和分类模型输出的识别结果以及四个分数特征中的部分或全部作为决策融合模型的输入，以第二操作行为样本数据对应的标签作为决策融合模型的目标输出值进行训练。在本申请实施例中，对匹配分数进行特征提取，进一步为决策融合模型提供更多的特征，有利于训练出更好的决策融合模型，提高决策融合模型认证的准确性，从而提高身份认证的准确性。

可选地，步骤 S720 还包括:

（1）获取第三样本数据。所述第三样本数据包括第三操作行为样本数据

（2）将第三操作行为样本数据输入到第一认证模型中，得到第一认证模型输出的第三操作行为样本数据的识别结果;

将第三操作行为样本数据输入到第二认证模型中，得到第二认证模型输出的第三操作行为样本数据的识别结果。

（3）将第一认证模型输出的第三操作行为样本数据的识别结果、第二认证模型输出的第三操作行为样本数据的识别结果输入到训练好的决策融合模型中，得到第三操作行为样本数据对应的身份认证结果。

（4）根据第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果对第一认证模型和/或第二认证模型进行训练。

需要说明的是，上述对第一样本数据的说明、限定和扩展等也适用于第三样本数据。第三样本数据与第一样本数据可以相同，也可以不同。第三样本数据与第二样本数据可以相同，也可以不同。

在获取样本数据的过程中，可能由于用户有意识或无意识的行为等引入错误的数据，造成样本数据对应的标签出现错误。例如，通过传感器采集用户的操作行为数据时，若是认证用户出现异常行为，则该异常操作行为数据被采集之后，对应的样本标签为认证用户，基于该样本数据以及对应的标签训练得到的认证模型存在准确率不高的问题。而通过训练好的决策融合模型得到的身份认证结果的准确度较高，以其输出实现反馈，再次对认证模型进行训练，能够进一步提高认证模型的准确度，从而进一步提高身份认证模型的准确度。

下面以身份认证模型包括异常检测模型和分类模型为例进行说明。

将第三操作行为样本数据输入异常检测模型，输出第一识别结果；将第三操作行为样本数据输入分类模型，输出第二识别结果。将第一识别结果和第二识别结果输入训练好的决策融合模型，得到第三操作行为样本数据对应的身份认证结果。

根据第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果对至少异常检测模型和分类模型进行训练。

示例性地，第一操作行为样本数据和第三操作行为样本数据可以包括相同的样本数据，根据第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果对异常检测模型和分类模型进行训练，包括:

根据第一操作行为样本数据对应的标签和第三操作行为操作行为样本数据对应的身份认证结果，筛选第一样本数据，基于筛选后的第一样本数据对异常检测模型和分类模型进行训练。

具体地，可以从第一样本数据中剔除标签与第三操作行为样本数据对应的身份认证结果不同的样本数据。

例如，样本数据 A 为第一操作行为样本数据和第三操作行为样本数据中的一条样本数据。在第一操作行为样本数据中，样本数据 A 对应的标签为非认证用户。将该样本数据 A 输入身份认证模型中，得到的身份认证结果为认证用户。在该情况下，可以从第一样本数据中剔除样本数据 A，基于筛选后的第一样本数据对异常检测模型和分类模型进行训练。

这样可以剔除掉错误的样本数据，提高了样本数据的准确率，并实现对以往数据的持续学习，提高了认证模型的准确率，从而提高身份认证模型的整体的准确率。

示例性地，根据第三操作行为样本数据和第三操作行为样本数据对应的身份认证结果对异常检测模型和分类模型进行训练，包括:

根据第三操作行为样本数据对异常检测模型进行训练;

以第三操作行为样本数据作为分类模型的输入，以第三操作行为数据样本对应的身份认证结果作为分类模型的目标输出值对分类模型进行训练。

这样，可以扩充训练样本的数据量，例如，在第三操作行为数据样本没有对应标签的情况下，也可以以第三操作行为数据样本对应的身份认证结果作为三操作行为样本数据对应的标签对认证模型进行训练，提高了认证模型的准确率，从而提高身份认证模型的整体准确率。

可选地，方法 700 还包括，通过增量学习更新身份认证模型。

增量学习是指一个学习系统能不断地从新样本中学习新的知识，并能保存大部分以前已经学习到的知识。

具体地，在由方法 730 得到训练好的身份认证模型后，可以持续采集用户的操作行为数据，也即新增的用户的操作行为数据，通过增量学习可以在原有的数据库的基础上，仅对由于新增的用户的操作行为数据所引起的变化进行身份认证模型的更新。

通过增量学习能够不断优化身份认证模型，适应变化的用户行为，增强识别能力。

在本申请实施例中，将至少两个认证模型的识别结果输入决策融合模型进行决策融合，得到身份认证结果，通过对决策融合模型进行训练，能够提高身份认证的准确性。同时，通过用户的操作行为数据进行身份验证，不会改变用户的用机习惯，有利于实现无感验证。

此外，异常检测模型和分类模型相结合得到身份认证模型，一方面通过异常检测模型提高了认证用户识别率，另一方面通过分类模型提高了抗攻击能力，整体上提高了身份认证模型的识别能力。

此外，异常检测模型和分类模型均可以使用小规模算法，例如，异常检测模型可以使用单分类 SVM，分类模型可以使用二分类 SVM，只需要引入 libsvm 库即可实现。这样，在身份认证过程中，算法开销小，无需额外的硬件支持，该身份认证模型可以在用户端侧进行训练，能够实现用户端侧数据安全存储，避免上传云端造成的隐私安全问题。

图 8 示出了本申请实施例的身份认证的方法 800。方法 800 包括步骤 S810 至步骤 S830。该方法 800 可以能够进行身份认证的装置或设备执行。该方法可以由终端设备、电脑、服务器等执行。例如，图 2 中的执行设备 110。下面对步骤 S810 至步骤 S830 进行介绍。

图 8 中的身份认证的方法 800 中使用的身份认证模型可以是通过上述图 6 或图 7 中的方法构建的。为了避免不必要的重复，下面在介绍方法 800 时适当省略重复的描述。

S810，获取待认证用户的第一操作行为数据；获取待认证用户的第二操作行为数据。

其中，该待认证用户的操作行为数据可以包括通过传感器采集的数据。

传感器包括运动传感器和/或触屏传感器。

待认证用户的操作行为数据可以为对传感器采集的原始数据进行处理后得到的数据。

例如，触屏传感器采集的原始数据包括：时间戳、触摸点 X/Y 轴坐标、触摸面积、触摸压力、动作（action）和屏幕方向等。运动传感器采集的数据包括：时间戳、加速度 X/Y/Z 轴数据、陀螺仪 X/Y/Z 轴数据等。应理解，以上仅为示意，传感器采集的数据可以包括以上中的任一项或几项，也可以包括其他数据。

可选地，待认证用户的操作行为数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

S820，以第一操作行为数据输入通过第一认证模型，获得第一认证模型输出的第一识别结果；以第二操作行为数据输入通过第二认证模型，获得第二认证模型输出的第二识别结果。

其中，第一、第二认证模型分别为异常检测模型和分类模型

其中，两个认证模型的模型参数分别是基于第一样本数据和第五样本数据进行训练得到的。具体的训练过程可以参见前述方法 700。

可选地，两个认证模型的模型参数是基于第一样本数据、第五样本数据以及第三样本数据进行训练得到的，第三样本数据包括：第三操作行为数据。具体的训练过程可以参见前述方法 700。

异常检测模型和分类模型的训练过程可以参见前述方法 700。

该异常检测模型用于检测异常数据，通过检测出非认证用户的数据来判断认证用户和非认证用户。该分类模型可以为二分类模型，通过分类来判断认证用户和非认证用户

S830，将第一识别结果、第二识别结果输入到决策融合模型中，得到输出的身份认证结果，其中，决策融合模型用于根据第一识别结果和第二识别结果的权重参数确定身份认证结果。

示例性地，如图 9 所示，将第一操作行为数据输入异常检测模型 910，输出第一识别结果；将第二操作行为数据输入分类模型 920，输出第二识别结果。将第一识别结果和第二识别结果输入决策融合模型 930，得到身份认证结果。其中识别结果包括待认证用户为认证用户或待认证用户为非认证用户。

例如，若异常检测模型和分类模型的识别结果均为认证用户，则该身份认证结果为认证用户。若异常检测模型和分类模型的识别结果均为非认证用户，则该身份认证结果为非认证用户。若异常检测模型和分类模型的识别结果中一个为认证用户，另一个为非认证用户，则该身份认证结果为无法识别。

再如，若异常检测模型和分类模型的识别结果中存在一个识别结果为认证用户，则该身份认证结果为认证用户。若异常检测模型和分类模型的识别结果均为非认证用户，则该身份认证结果为非认证用户。

再如，若异常检测模型和分类模型的识别结果中存在一个识别结果为非认证用户，则该身份认证结果为非认证用户。若异常检测模型和分类模型的识别结果均为认证用户，则该身份认证结果为认证用户。

可选地，决策融合模型用于根据至少两个认证模型对应的权重对至少两个认证模型输出的识别结果进行加权计算，根据加权计算得到的结果确定身份认证结果。

通过为认证模型设置对应的权重，将识别结果进行加权计算，能够根据需要调整权重值，进一步提高了身份认证的准确性。

可选地，决策融合模型的权重参数是通过将第二样本数据中的第二操作行为样本数据输入到所述第一认证模型和所述第二认证模型中，得到所述第一认证模型和所述第二认证模型输出的第二操作行为样本数据的识别结果，以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练得到的，所述第二样本数据包括所述第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户。具体的训练过程可以参见方法 730。

示例性地，如图 10 所示，将待认证用户的操作行为数据输入异常检测模型 1010，输出第一匹配分数；将待认证用户的操作行为数据输入分类模型 1020，输出第二匹配分数。将第一匹配分数和第二匹配分数输入决策融合模型 1030，根据至少两个认证模型对应的权重对进行加权计算，根据加权计算得到的结果确定身份认证结果。其中图 10 中的匹配分数即为认证模型输出的识别结果，即待认证用户为认证用户的概率。

例如，若该加权计算的结果大于或等于设定阈值 A 时，认证成功，即该待认证用户被识别为认证用户；当该加权计算的结果小于设定阈值 A 时，认证失败，即该待认证用户被识别为非认证用户。或者，当该加权计算的结果大于设定阈值 A 时，认证成功，即该待认证用户被识别为认证用户；当该加权计算的结果小于或等于设定阈值 A 时，认证失败，即该待认证用户被识别为非认证用户。或者，当该加权计算的结果大于设定阈值 A 时，认证成功，即该待认证用户被识别为认证用户；当该加权计算的结果小于设定阈值 B 时，认证失败，即该待认证用户被识别为非认证用户；当该加权计算的结果大于设定阈值 B 且小于设定阈值 A 时，无法识别。

可选地，第一识别结果包括：第一操作行为数据对应的匹配分数和/或第一操作行为数据对应的匹配结果；第二识别结果包括第二操作行为数据对应的匹配分数和/或第二操作行为数据对应的匹配结果。

其中，第一操作行为数据对应的匹配分数用于指示待认证用户被识别为认证用户的概

率，第一操作行为数据对应的匹配结果用于指示待认证用户被识别为认证用户或非认证用户，第一操作行为数据对应的匹配结果包括基于至少两个阈值和第一操作行为数据对应的匹配分数确定的至少两个匹配结果。第二操作行为数据对应的匹配分数用于指示待认证用户被识别为认证用户的概率，第二操作行为数据对应的匹配结果用于指示待认证用户被识别为认证用户或非认证用户，第二操作行为数据对应的匹配结果包括基于至少两个阈值和第二操作行为数据对应的匹配分数确定的至少两个匹配结果。

下面以异常检测模型输出的识别结果和分类模型输出的识别结果为例进行说明。

异常检测模型输出的识别结果包括：由异常检测模型输出的待认证用户的操作行为数据对应的匹配分数 A 以及第一操作行为数据对应的匹配结果 A。

例如，至少两个阈值包括第一阈值 A 和第二阈值 A，第一阈值 A 大于第二阈值 A。由异常检测模型输出的第一操作行为数据对应的匹配结果 A 包括：基于第一阈值 A 确定的匹配结果和基于第二阈值 A 确定的匹配结果。当匹配分数 A 大于或等于第一阈值 A 时，基于第一阈值 A 确定的匹配结果为认证用户；当匹配分数 A 小于第一阈值 A 时，基于第一阈值 A 确定的匹配结果为非认证用户。当匹配分数 A 大于或等于第二阈值 A 时，基于第二阈值 A 确定的匹配结果为认证用户；当匹配分数 A 小于第二阈值 A 时，基于第二阈值 A 确定的匹配结果为非认证用户。

分类模型输出的识别结果包括：由分类模型输出的第二操作行为数据对应的匹配分数 B 以及第二操作行为数据对应的匹配结果 B。

例如，至少两个阈值包括第一阈值 B 和第二阈值 B，第一阈值 B 大于第二阈值 B。由分类模型输出的第二操作行为数据对应的匹配结果 B 包括：基于第一阈值 B 确定的匹配结果和基于第二阈值 B 确定的匹配结果。当匹配分数 B 大于或等于第一阈值 B 时，基于第一阈值 B 确定的匹配结果为认证用户；当匹配分数 B 小于第一阈值 B 时，基于第一阈值 B 确定的匹配结果为非认证用户。当匹配分数 B 大于或等于第二阈值 B 时，基于第二阈值 B 确定的匹配结果为认证用户；当匹配分数 B 小于第二阈值 B 时，基于第二阈值 B 确定的匹配结果为非认证用户。

在本申请实施例中，两个认证模型输出的识别结果包括匹配分数和至少两个匹配结果，通过不同的阈值能够调节认证模型的不同性能，以使认证模型的性能达到预期，例如，通过不同的阈值调节模型的抗攻击能力和机主识别率，以使认证模型的性能达到平衡。此外，区别于现有认证模型仅能提供一种识别结果，本方案能够为决策融合模型提供更多的特征，有利于提高决策融合模型认证的准确性，从而提高身份认证的准确性。

可选地，将第一识别结果、第二识别结果输入到决策融合模型中，得到输出的身份认证结果，包括：根据第一操作行为数据对应的匹配分数得到第一分数特征；根据第二操作行为数据对应的匹配分数得到第二分数特征；以第一分数特征、第二分数特征、第一识别结果和第二识别结果输入到决策融合模型中，得到输出的身份认证结果。

示例性地，对待认证用户的操作行为数据对应的匹配分数进行特征提取，包括：对该分数进行数学运算，例如加减乘除运算，将运算结果作为分数特征。

下面以异常检测模型和分类模型为例说明步骤 S830。

（1）将待认证用户的操作行为数据分别输入异常检测模型和分类模型，分别得到异常检测模型和分类模型输出的识别结果。

异常检测模型输出的识别结果包括由异常检测模型输出的第一操作行为数据对应的匹配分数 A 以及第一操作行为数据对应的匹配结果 A。该匹配结果 A 包括第一阈值 A 对应的匹配结果和第二阈值 A 对应的匹配结果。

分类模型输出的识别结果包括由分类模型输出的第二操作行为数据对应的匹配分数 B 以及第二操作行为数据对应的匹配结果 B。该匹配结果 B 包括第一阈值 B 对应的匹配结果和第二阈值 B 对应的匹配结果。

（2）对异常检测模型对应的匹配分数和分类模型对应的匹配分数分别进行加减乘除运算，得到四个运算结果，作为四个分数特征。

将异常检测模型对应的匹配分数和分类模型对应的匹配分数作为两个分数特征。

示例性地，可以将异常检测模型和分类模型输出的识别结果以及四个分数特征中的部分或全部输入决策融合模型，得到身份认证结果。

在本申请实施例中，对匹配分数进行特征提取，进一步为决策融合模型提供更多的特征，有利于提高决策融合模型认证的准确性，从而提高了身份认证的准确性。

在本申请实施例中，通过对决策融合模型进行训练，得到更优的模型参数，例如，得到更优的认证模型的权重比例，进一步提高了身份认证的准确性。

可选地，方法 800 还包括：将 s 条待认证的用户操作行为数据输入身份认证模型中，得到 s 个身份认证结果；根据该 s 个身份认证结果得到最终的身份认证结果。

例如，s 个身份认证结果中，认证成功的次数超过认证失败的次数，则认证成功，即该待认证用户被识别为认证用户；认证成功的次数少于认证失败的次数，则认证失败，即该待认证用户被识别为非认证用户；认证成功的次数等于认证失败的次数，则无法识别。或者，该 s 个身份认证结果可以为 s 个加权结果，对该 s 个加权结果计算平均值，根据该平均值确定最终的身份认证结果。这样，进一步提高了认证结果的准确率。

表 1 示出了采用不同的算法进行身份认证的仿真结果。由表 1 可以看出，本申请实施例提供的身份认证方法能够提高身份认证的准确率。

表 1

算法	抗攻击率	机主识别率
单分类 SVM 算法	73.38%	84.87%
二分类 SVM 算法	92.13%	86.13%
本申请的身份认证方法	90.19%	91.77%

在本申请实施例中，将至少两个认证模型的识别结果输入决策融合模型进行决策融合，得到身份认证结果，能够提高身份认证的准确性。同时，通过用户的操作行为数据进行身份验证，不会改变用户的用机习惯，有利于实现无感验证。

此外，采用异常检测模型和分类模型，一方面通过异常检测模型提高了认证用户识别率，另一方面通过分类模型提高了抗攻击能力，整体上提高了身份认证模型的识别能力。

此外，异常检测模型和分类模型均可以使用小规模算法，例如，异常检测模型可以使用单分类 SVM，分类模型可以使用二分类 SVM，只需要引入 libsvm 库即可实现。这样，

在身份认证过程中，算法开销小，无需额外的硬件支持，该身份认证模型可以在用户端侧进行训练，能够实现用户端侧数据安全存储，避免上传云端造成的隐私安全问题。

图 11 示出了本申请实施例提供的身份认证的方法和身份认证模型的训练方法的应用流程示意图。下面以图 11 所示的场景为例对本申请实施例的身份认证方法和身份认证模型的训练方法的应用流程进行说明。

如图 11 所示，身份认证的过程可以包括两个阶段：训练阶段和认证阶段。

其中，训练阶段是指基于用户的操作行为数据生成身份认证模型的过程；认证阶段是指验证待认证用户的操作行为数据与身份认证模型的匹配的过程，最终给出身份认证的结果。下面分别对这两个阶段的步骤进行说明。

训练阶段

S1110，数据采集模块获取用户的操作行为数据。操作行为数据也可以称为操作习惯行为数据。

具体地，数据采集模块注册传感器的监听器，通过传感器采集用户的操作行为数据。该数据采集模块可以为图 4 中的数据采集模块 420。

示例性地，该传感器包括触屏传感器和/或运动传感器。

例如，触屏传感器采集的数据包括：时间戳、触摸点 X/Y 轴坐标、触摸面积、触摸压力、动作（action）和屏幕方向等。

运动传感器采集的数据包括：时间戳、加速度 X/Y/Z 轴数据、陀螺仪 X/Y/Z 轴数据等。

应理解，以上仅为示意，传感器采集的数据可以包括以上中的任一项或几项，也可以包括其他数据。

示例性地，可以屏幕解锁时，注册传感器的监听器；在屏幕锁屏时，注销传感器的监听器。

S1120，对传感器采集的操作行为数据进行数据预处理，得到第一训练样本。

例如，预处理包括：剔除异常数据、筛选有效操作行为数据或提取特征数据等，得到第一训练样本。该第一训练样本可以存储于图 4 所示的存储模块 440 中。

示例性地，可以将预处理后得到的数据作为第一训练样本中的正样本，将预置的非认证用户的操作行为数据作为第一训练样本中的负样本。

应理解，图 11 中步骤（A2）由数据采集模块执行仅为示例。可选地，步骤（A2）可以由身份认证模块执行。

S1130，身份认证模块训练身份认证模型。该身份认证模块可以为图 4 中的身份认证模块 430。该步骤与方法 700 中的 S720 对应。

可选地，在开始训练身份认证模型之前，身份认证模型还可以判断是否开始训练身份认证模型。

示例性地，当第一样本数据的采集的时段超过预设时长和/或第一样本数据的数据量超过预设数量，开始建立身份认证模型。

可替换地，若步骤（A2）由数据采集模块执行，则可以由数据采集模块判断是否开始训练身份认证模型。例如，如图 11 的步骤 S1121 所示，当第一样本数据的采集的时段超过预设时长和/或第一样本数据的数据量超过预设数量，向身份认证模块发送建模指令，通知身份认证模块开始训练身份认证模型。

具体地，身份认证模型的训练方法可以采用本申请实施例中的身份认证模型的训练方法。

用户在不同的应用场景下的行为可能不同，因此，可以针对不同的应用场景分别建立身份认证模型。

S1130 还包括验证身份认证模型的有效性。

若身份认证模型的指标满足预设指标，则该身份认证模型有效，建模阶段结束，得到训练好的身份认证模型。例如，可以标记建模完成状态。

该身份认证模型的有效性验证方式可以根据应用场景设定。即在不同的应用场景中，对身份认证模型的有效性的验证方式可以不同。

例如，该身份认证模型应用于屏幕解锁时，该身份认证模型的指标满足预设指标可以为该身份认证模型的抗攻击能力满足要求。

训练好的身份认证模型可以存储于图 4 所述的存储模块 440 中。存储模块 440 中存储的身份认证模型可以为一个或多个。

认证阶段

S1140，启动身份认证功能。

示例性地，该身份认证模型可以应用于应用程序中的身份认证。例如，如图 11 所示，该 APP 可以是集成身份认证 SDK 的 APP。该 APP 可以为图 4 中的 APP410。

例如，在身份认证模型应用于应用锁解锁的情况下，待认证的用户需要使用 APP 时，可以通知身份认证模型启动身份认证。该 APP 可以称为待认证 APP。

进一步地，该 APP 可以提示用户需要获取用户的操作行为数据。若用户同意，则启动身份认证。

进一步地，身份认证模块可以通知数据采集模块监听传感器的数据。具体地，如图 11 的步骤 S1141 所示，身份认证模块可以将上下文环境信息反馈至数据采集模块。上下文环境信息用于指示应用环境，例如，如图 11 所示，上下文环境信息包括待认证 APP 的类型，比如支付类，新闻类等。或者上下文信息还可以包括时间或地点等信息。

S1150，数据采集模块监听传感器采集的待认证用户的操作行为数据。

如前所述，不同的身份认证模型可以由不同的操作行为数据训练得到。在该情况下，数据采集模块监听传感器的数据指的是该应用场景对应的用户的操作行为数据，如图 11 所示，数据采集模块监听待认证 APP 对应的用户的操作行为数据。

数据采集模块可以根据上下文环境信息确定需要采集的用户的操作行为数据。

示例性地，对于不同的待认证 APP，身份认证模型可以通过不同的用户操作行为数据进行身份认证。

或者，对于同一个待认证 APP，身份认证模型应用于应用锁解锁和应用于支付时可以通过不同的用户操作行为数据进行身份认证。

例如，对于同一待认证 APP，身份认证模型应用于应用锁解锁时，数据采集模块监听用户操作行为数据 1，将用户操作行为数据 1 输入身份认证模型；身份认证模型应用于支付时，数据采集模块监听用户操作行为数据 2，将用户操作行为数据 2 输入身份认证模型。用户操作行为数据 1 的参数可以少于用户操作行为数据 2 的参数。例如，用户操作行为数据 1 可以包括触屏传感器采集的数据。用户操作行为数据 2 可以包括触屏传感器和运动传

感器采集的数据。这样，针对不同的应用场景，监听不同的数据，能够有针对性的实现身份认证，进一步保证了系统的安全性。

S1160，发起身份认证请求。

示例性地，该身份认证模型可以应用于应用程序中的身份认证。待认证 APP 可以发起身份认证请求，例如，向图 4 中的身份认证模块 430 发起身份认证请求。

S1170，匹配待认证用户的操作行为数据。

该待认证用户的操作行为数据是根据步骤（B2）中数据采集模块监听的传感器的数据确定的。

具体地，将该待认证用户的操作行为数据输入身份认证模型中，识别是否为认证用户。进一步地，如图 11 的步骤 S1171 所示，将识别结果反馈至待认证应用程序。

可以采用本申请实施例中的身份认证方法匹配待认证用户的操作行为数据。例如，该身份认证方法可以为图 8 中的方法 800。

在本申请实施例中，将至少两个认证模型的识别结果输入决策融合模型进行决策融合，得到身份认证结果，能够提高身份认证的准确性。同时，通过用户的操作行为数据进行身份验证，不会改变用户的用机习惯，有利于实现无感验证。

本申请实施例提供的身份认证的方法可以应用于持续的身份认证。在用户唤醒智能终端时可以对指示唤醒智能终端的待认证用户进行身份认证，在智能终端处于唤醒状态即非锁定状态时，可以在待认证用户下发指令或者预设时间间隔之外，对待认证用户再次进行身份认证，从而能够有效的避免用户在唤醒智能终端后离开，任何再接触智能终端的用户均可以使用智能终端，从而导致智能终端中用户隐私数据泄露等安全性问题。或者，在用户登录 APP 时，可以对登录 APP 的待认证用户进行身份认证，在处于登录状态时，可以在待认证用户下发指令或者预设时间间隔之外，对待认证用户再次进行身份认证，从而能够有效的避免用户在登录 APP 后离开，任何再接触智能终端的用户均可以使用该 APP，从而导致智能终端中用户隐私数据泄露等安全性问题。

本申请实施例提供的身份认证方法可以和其他身份认证方法结合。

示例性地，将本申请实施例提供的身份认证方法作为辅助认证方法，与其他认证方法结合进行身份认证，提高了系统的安全性和可靠性。例如，如图 12 所示，通过人脸识别或指纹识别进行第一次身份认证，若认证成功，则采用本申请实施例提供的身份认证方法进行第二次身份认证，若认证成功，则认证通过。若出现一次认证失败，则提示用户进行密码认证。

示例性地，将本申请实施例提供的身份认证方法作为持续保护方法，与其他认证方法结合进行身份认证，提高了系统的安全性和可靠性。例如，如图 13 所示，在用户登录 APP 时，对登录 APP 的待认证用户进行身份认证。在处于登录状态时，可以在待认证用户下发指令或者预设时间间隔之外，可以采用本申请提供的身份认证方法对待认证用户再次进行身份认证，若认证失败，则弹出应用锁或者其他认证界面。这样能够有效的避免用户在登录 APP 后离开，任何再接触智能终端的用户均可以使用该 APP，从而导致智能终端中用户隐私数据泄露等安全性问题。本申请实施例提供的身份认证方法采用行为认证方法，能够实现无感认证。

示例性地，将本申请实施例提供的身份认证方法用于支付风险控制，与其他认证方法

结合进行身份认证，提高了系统的安全性和可靠性。例如，如图 14 所示，在用户进行支付时，通过本申请实施例提供的身份认证方法进行身份认证，将身份认证的结果作为行为风险控制信息输入业务风险控制系统，进行风险控制。若风险控制合格，则进行支付操作；若风险控制不合格，则可以提示用户采用其他方式进行身份认证。

下面结合附图对本申请实施例的训练装置和身份认证的装置进行详细的描述，应理解，下面描述的身份认证模型的训练装置能够执行前述本申请实施例的身份认证模型的训练方法，身份认证的装置可以执行前述本申请实施例的身份认证的方法，为了避免不必要的重复，下面在介绍本申请实施例的身份认证的装置和身份认证模型的训练装置时适当省略重复的描述。

图 15 是本申请实施例的的示意性框图。图 15 所示的身份认证模型的训练装置 1500 包括获取单元 1510 和处理单元 1520。身份认证模型包括第一认证模型、第二认证模型和决策融合模型，其中，所述第一、第二认证模型分别为异常检测模型和分类模型。

获取单元 1510 和处理单元 1520 可以用于执行本申请实施例的身份认证模型的训练方法，具体地，获取单元 1510 可以执行上述步骤 S731，处理单元 1520 可以执行上述步骤 S732 和 S733。

获取单元 1510 用于获取第二样本数据，所述第二样本数据包括第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户。处理单元 1520 用于将所述第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到所述第二操作行为数据的识别结果，所述第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括第一操作行为样本数据和所述第一操作行为样本数据对应的标签，所述第一操作行为样本数据对应的标签用于表示所述第一操作行为样本数据对应的用户为认证用户或非认证用户，所述第二认证模型的模型参数是基于第五样本数据进行训练得到的，所述第五样本数据包括第五操作行为样本数据和所述第五操作行为样本数据对应的标签，所述第五操作行为样本数据对应的标签用于表示所述第五操作行为数据对应的用户为认证用户或非认证用户；以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型。

可选地，作为一个实施例，所述第二操作行为样本数据的识别结果包括所述第一认证模型输出的识别结果和所述第二认证模型输出的识别结果；所述第一认证模型输出的识别结果包括：所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第一认证模型输出的第二操作行为样本对应的匹配结果；所述第二认证模型输出的识别结果包括：所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第二认证模型输出的第二操作行为样本数据对应的匹配结果；其中，所述第二操作行为样本数据对应的匹配分数用于指示所述第二操作行为样本数据对应的用户被识别为认证用户的概率，所述第二操作行为样本数据对应的匹配结果用于指示所述第二操作行为样本数据对应的用户被识别为认证用户或非认证用户，所述第二操作行为样本数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为样本数据对应的匹配分数确定的至少两个匹配结果。

可选地，作为一个实施例，至少两个阈值包括第一阈值，以及，获取单元 1510 还用于获取第四样本数据，所述第四样本数据包括第四操作行为样本数据和所述第四操作行为样本数据对应的标签，所述第四操作行为样本数据对应的标签用于表示所述第四操作行为样本数据对应的用户为认证用户或非认证用户。处理单元 1520 还用于：将所述第四操作行为样本数据输入所述第一认证模型，得到所述第一认证模型输出的所述第四操作行为样本数据对应的匹配分数，所述第四操作行为样本数据对应的匹配分数用于指示所述第四操作行为样本数据对应的用户被识别为认证用户的概率；基于多个候选阈值确定所述第四操作行为样本数据对应的匹配分数对应的多个候选匹配结果，所述多个候选匹配结果用于指示所述第四操作行为样本数据对应的用户被识别为认证用户或非认证用户；将所述多个候选匹配结果中准确率满足预设条件的候选匹配结果对应的候选阈值确定为所述第一阈值。

可选地，作为一个实施例，处理单元 1520 具体用于：根据所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第一分数特征；根据所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第二分数特征；以所述第二操作行为样本数据的第一分数特征、第二操作行为样本数据的第二分数特征和所述第二操作行为样本数据的识别结果作为决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练。

可选地，作为一个实施例，第二操作行为样本数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据

可选地，作为一个实施例，第二样本数据是根据用户在触摸屏上的滑动时长和/或所述用户在触摸屏上的进行筛选得到的。

可选地，作为一个实施例，获取单元 1510 还用于：获取第三样本数据，其中，所述第三样本数据包括：第三操作行为样本数据。处理单元 1520 还用于：将所述第三操作行为样本数据输入到所述第一认证模型中，得到所述第一认证模型输出的第三操作行为样本数据的识别结果；将所述第三操作行为样本数据输入到所述第二认证模型中，得到所述第二认证模型输出的第三操作行为样本数据的识别结果；将所述第一认证模型输出的第三操作行为样本数据的识别结果、所述第二认证模型输出的第三操作行为样本数据的识别结果输入到所述训练好的决策融合模型中，得到所述第三操作行为样本数据对应的身份认证结果；根据所述第三操作行为样本数据和所述第三操作行为样本数据对应的身份认证结果对所述第一认证模型和/或所述第二认证模型进行训练。

图 16 是本申请实施例提供的身份认证的装置 1600 的示意性框图。图 16 所示的身份认证的装置 1600 包括获取单元 1610 和处理单元 1620。

获取单元 1610 和处理单元 1620 可以用于执行本申请实施例的身份认证的方法，具体地，获取单元 1610 可以执行上述步骤 S810，处理单元 1620 可以执行上述步骤 S820 和 S830。

获取单元 1610 用于待认证用户的第一操作行为数据；获取待认证用户的第二操作行为数据。处理单元 1620 用于以所述第一操作行为数据输入通过第一认证模型，获得所述第一认证模型输出的第一识别结果；以所述第二操作行为数据输入通过第二认证模型，获得所述第二认证模型输出的第二识别结果；其中，所述第一、第二认证模型分别为异常检

测模型和分类模型； 将所述第一识别结果、所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果，其中，所述决策融合模型用于根据所述第一识别结果和所述第二识别结果的权重参数确定所述身份认证结果。

可选地，作为一个实施例，第一操作行为数据和/或第二操作行为数据是通过传感器采集的数据。

可选地，作为一个实施例，决策融合模型的权重参数是通过将第二样本数据中的操作行为样本数据输入到所述第一认证模型和所述第二认证模型中，得到所述第一认证模型和所述第二认证模型输出的所述第二操作行为样本数据的识别结果，以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练得到的，所述第二样本数据包括所述第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户。

可选地，作为一个实施例，所述第一识别结果包括：所述第一操作行为数据对应的匹配分数和/或所述第一操作行为数据对应的匹配结果；第二识别结果包括所述第二操作行为数据对应的匹配分数和/或所述第二操作行为数据对应的匹配结果；其中，所述第一操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，所述第一操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，所述第一操作行为数据对应的匹配结果包括基于至少两个阈值和所述第一操作行为数据对应的匹配分数确定的至少两个匹配结果；所述第二操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，所述第二操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，所述第二操作行为数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为数据对应的匹配分数确定的至少两个匹配结果。

可选地，作为一个实施例，处理单元 1620 具体用于：根据所述第一操作行为数据对应的匹配分数得到第一分数特征；根据所述第二操作行为数据对应的匹配分数得到第二分数特征；以所述第一分数特征、所述第二分数特征、所述第一识别结果和所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果。

可选地，作为一个实施例，第一操作行为数据和/或第二操作行为数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

需要说明的是，上述训练装置 1500 以及身份认证的装置 1600 以功能单元的形式体现。这里的术语“单元”可以通过软件和/或硬件形式实现，对此不作具体限定。

例如，“单元”可以是实现上述功能的软件程序、硬件电路或二者结合。所述硬件电路可能包括应用特有集成电路（application specific integrated circuit，ASIC）、电子电路、用于执行一个或多个软件或固件程序的处理器（例如共享处理器、专有处理器或组处理器等）和存储器、合并逻辑电路和/或其它支持所描述的功能的合适组件。

因此，在本申请的实施例中描述的各示例的单元，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的

特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

图 17 是本申请实施例提供的一种身份认证模型的训练装置的硬件结构示意图。图 17 所示的训练装置 900（该装置 900 具体可以是一种计算机设备）包括存储器 901、处理器 902、通信接口 903 以及总线 904。其中，存储器 901、处理器 902、通信接口 903 通过总线 904 实现彼此之间的通信连接。

存储器 901 可以是只读存储器（read only memory，ROM），静态存储设备，动态存储设备或者随机存取存储器（random access memory，RAM）。存储器 901 可以存储程序，当存储器 901 中存储的程序被处理器 902 执行时，处理器 902 用于执行本申请实施例的身份认证模型的训练方法的各个步骤，例如，执行图 6 或图 7 所示的各个步骤。

应理解，本申请实施例所示的训练装置可以是服务器，例如，可以是云端的服务器，或者，也可以是配置于云端的服务器中的芯片。

或者，本申请实施例所示的装置可以是智能终端，或者，也可以是配置于智能终端中的芯片。

处理器 902 可以采用通用的中央处理器（central processing unit，CPU），微处理器，应用专用集成电路（application specific integrated circuit，ASIC），图形处理器（graphics processing unit，GPU）或者一个或多个集成电路，用于执行相关程序，以实现本申请方法实施例的身份认证模型的训练方法。

处理器 902 还可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，本申请的身份认证模型的训练方法的各个步骤可以通过处理器 902 中的硬件的集成逻辑电路或者软件形式的指令完成。

上述处理器 902 还可以是通用处理器、数字信号处理器（digital signal processing，DSP）、专用集成电路（ASIC）、现成可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 901，处理器 902 读取存储器 901 中的信息，结合其硬件完成本申请实施中图 17 所示的训练装置中包括的单元所需执行的功能，或者，执行本申请方法实施例的图 6 或图 7 所示的身份认证模型的训练方法。

通信接口 903 使用例如但不限于收发器一类的收发装置，来实现训练装置 900 与其他设备或通信网络之间的通信。

总线 904 可包括在训练装置 900 各个部件（例如，存储器 901、处理器 902、通信接口 903）之间传送信息的通路。

图 18 是本申请实施例提供的身份认证的装置的硬件结构示意图。图 18 所示的身份认证的装置 1000（该装置 1000 具体可以是一种计算机设备）包括存储器 1001、处理器 1002、通信接口 1003 以及总线 1004。其中，存储器 1001、处理器 1002、通信接口 1003 通过总

线 1004 实现彼此之间的通信连接。

存储器 1001 可以是只读存储器（read only memory，ROM），静态存储设备，动态存储设备或者随机存取存储器（random access memory，RAM）。存储器 1001 可以存储程序，当存储器 1001 中存储的程序被处理器 1002 执行时，处理器 1002 用于执行本申请实施例的身份认证的方法的各个步骤，例如，执行图 8 所示的各个步骤。

应理解，本申请实施例所示的装置可以是智能终端，或者，也可以是配置于智能终端中的芯片。

处理器 1002 可以采用通用的中央处理器（central processing unit，CPU），微处理器，应用专用集成电路（application specific integrated circuit，ASIC），图形处理器（graphics processing unit，GPU）或者一个或多个集成电路，用于执行相关程序，以实现本申请方法实施例的身份认证的方法。

处理器 1002 还可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，本申请的身份认证的方法的各个步骤可以通过处理器 1002 中的硬件的集成逻辑电路或者软件形式的指令完成。

上述处理器 1002 还可以是通用处理器、数字信号处理器（digital signal processing，DSP）、专用集成电路（ASIC）、现成可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1001，处理器 1002 读取存储器 1001 中的信息，结合其硬件完成本申请实施中图 16 所示的装置中包括的单元所需执行的功能，或者，执行本申请方法实施例的图 8 所示的身份认证的方法。

通信接口 1003 使用例如但不限于收发器一类的收发装置，来实现装置 1000 与其他设备或通信网络之间的通信。

总线 1004 可包括在装置 1000 各个部件（例如，存储器 1001、处理器 1002、通信接口 1003）之间传送信息的通路。

应注意，尽管上述训练装置 900 和装置 1000 仅仅示出了存储器、处理器、通信接口，但是在具体实现过程中，本领域的技术人员应当理解，训练装置 900 和装置 1000 还可以包括实现正常运行所必须的其他器件。同时，根据具体需要本领域的技术人员应当理解，上述训练装置 900 和装置 1000 还可包括实现其他附加功能的硬件器件。此外，本领域的技术人员应当理解，上述训练装置 900 和装置 1000 也可仅仅包括实现本申请实施例所必需的器件，而不必包括图 17 或图 18 中所示的全部器件。

图 19 是本申请实施例提供的身份认证的装置和身份认证模型的训练装置的硬件结构示意图。图 19 所示的装置 1100（该装置 1100 具体可以是一种计算机设备）包括存储器 1101、处理器 1102、输出接口 1103。

存储器 1101 可以是只读存储器（read only memory，ROM），静态存储设备，动态存储设备或者随机存取存储器（random access memory，RAM）。存储器 1101 可以存储程序

指令和数据，当存储器 1101 中存储的程序指令被处理器 1102 执行时，处理器 1102 用于执行本申请实施例的身份认证的方法或身份认证模型的训练方法的各个步骤。

例如，处理器 1102 接收触屏传感器和运动传感器的数据，能够实现上述实施例中的身份认证过程中的相应功能，包括如图 19 中的特征提取和行为匹配等。再如，处理器 1102 接收触屏传感器和运动传感器的数据，能够实现上述实施例中的身份认证模型的训练过程中的相应功能，包括如图 19 中的特征提取和行为建模等。进一步地，处理器 1102 还可以用于实现图 5 中的其他功能。

应理解，本申请实施例所示的装置可以是智能终端，或者，也可以是配置于智能终端中的芯片。

处理器 1102 可以采用通用的中央处理器（central processing unit，CPU），微处理器，应用专用集成电路（application specific integrated circuit，ASIC），图形处理器（graphics processing unit，GPU）或者一个或多个集成电路，用于执行相关程序，以实现本申请方法实施例的身份认证的方法或身份认证模型的训练方法。

处理器 1102 还可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，本申请的身份认证的方法或身份认证模型的训练方法的各个步骤可以通过处理器 1102 中的硬件的集成逻辑电路或者软件形式的指令完成。

上述处理器 1102 还可以是通用处理器、数字信号处理器（digital signal processing，DSP）、专用集成电路（ASIC）、现成可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 1101，处理器 1102 读取存储器 1101 中的信息，结合其硬件完成本申请实施中图 15 或图 16 所示的装置中包括的单元所需执行的功能，或者，执行本申请方法实施例的图 6 或图 7 或图 8 所示的方法。

输出接口 1103 使用例如但不限于收发器一类的收发装置，来实现装置 1100 与其他设备或通信网络之间的通信。

应注意，尽管上述装置 1100 仅仅示出了存储器、处理器、输出接口，但是在具体实现过程中，本领域的技术人员应当理解，装置 1100 还可以包括实现正常运行所必须的其他器件。同时，根据具体需要本领域的技术人员应当理解，上述装置 1100 还可包括实现其他附加功能的硬件器件。此外，本领域的技术人员应当理解，上述装置 1100 也可仅仅包括实现本申请实施例所必需的器件，而不必包括图 19 中所示的全部器件。

应理解，本申请实施例中的处理器可以为中央处理单元（central processing unit，CPU），该处理器还可以是其他通用处理器、数字信号处理器（digital signal processor，DSP）、专用集成电路（application specific integrated circuit，ASIC）、现成可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

还应理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory，ROM）、可编程只读存储器（programmable ROM，PROM）、可擦除可编程只读存储器（erasable PROM，EPROM）、电可擦除可编程只读存储器（electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的随机存取存储器（random access memory，RAM）可用，例如静态随机存取存储器（static RAM，SRAM）、动态随机存取存储器（DRAM）、同步动态随机存取存储器（synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM，DR RAM）。

上述实施例，可以全部或部分地通过软件、硬件、固件或其他任意组合来实现。当使用软件实现时，上述实施例可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令或计算机程序。在计算机上加载或执行所述计算机指令或计算机程序时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以为通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集合的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质。半导体介质可以是固态硬盘。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A,B 可以是单数或者复数。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系，但也可能表示的是一种“和/或”的关系，具体可参考前后文进行理解。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项（个）”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a,b,或 c 中的至少一项（个），可以表示：a, b, c, a-b, a-c, b-c, 或 a-b-c，其中 a,b,c 可以是单个，也可以是多个。

应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本

申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案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中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1.一种身份认证的方法，其特征在于，包括:

获取待认证用户的第一操作行为数据;

获取所述待认证用户的第二操作行为数据;

以所述第一操作行为数据输入通过第一认证模型，获得所述第一认证模型输出的第一识别结果;

以所述第二操作行为数据输入通过第二认证模型，获得所述第二认证模型输出的第二识别结果;

其中，所述第一认证模型、第二认证模型分别为异常检测模型和分类模型;

将所述第一识别结果、所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果，其中，所述决策融合模型用于根据所述第一识别结果和所述第二识别结果的权重参数确定所述身份认证结果。

2.根据权利要求 1 所述的方法，其特征在于，所述第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括: 第一操作行为样本数据及所述第一操作行为样本数据对应的标签，所述第一操作行为样本数据对应的标签用于指示所述第一操作行为样本数据所对应的用户为认证用户或非认证用户。

3.根据权利要求 1 或 2 所述的方法，其特征在于，所述第一操作行为数据和/或所述第二操作行为数据是通过传感器采集的数据。

4.根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述异常检测模型包括: 单分类支持向量机 SVM 模型或孤立森林，所述分类模型包括: SVM 模型或神经网络。

5.根据权利要求 1 至 4 中任一项所述的方法，其特征在于，所述决策融合模型的权重参数是通过将第二样本数据中的第二操作行为样本数据输入到所述第一认证模型和所述第二认证模型中，得到所述第一认证模型和所述第二认证模型输出的所述第二操作行为样本数据的识别结果，以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练得到的，所述第二样本数据包括所述第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户。

6.根据权利要求 1 至 5 中任一项所述的方法，其特征在于，

所述第一识别结果包括: 所述第一操作行为数据对应的匹配分数和/或所述第一操作行为数据对应的匹配结果;

第二识别结果包括所述第二操作行为数据对应的匹配分数和/或所述第二操作行为数据对应的匹配结果;

其中，所述第一操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，所述第一操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，所述第一操作行为数据对应的匹配结果包括基于至少两个阈值和所述第一操作行为数据对应的匹配分数确定的至少两个匹配结果;

所述第二操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，所述第二操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，所述第二操作行为数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为数据对应的匹配分数确定的至少两个匹配结果。

7.根据权利要求 6 所述的方法，其特征在于，所述将第一识别结果、所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果，包括:

根据所述第一操作行为数据对应的匹配分数得到第一分数特征;

根据所述第二操作行为数据对应的匹配分数得到第二分数特征;

以所述第一分数特征、所述第二分数特征、所述第一识别结果和所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果。

8.根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述第一操作行为数据或所述第二操作行为数据包括以下数据中的至少一种: 触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

9.一种身份认证模型的训练方法，其特征在于，所述身份认证模型包括第一认证模型、第二认证模型和决策融合模型，其中，所述第一认证模型、第二认证模型分别为异常检测模型和分类模型，所述方法包括:

获取第二样本数据，所述第二样本数据包括第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户;

将所述第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到所述第二操作行为样本数据的识别结果，所述第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括第一操作行为样本数据和所述第一操作行为样本数据对应的标签，所述第一操作行为样本数据对应的标签用于表示所述第一操作行为样本数据对应的用户为认证用户或非认证用户，所述第二认证模型的模型参数是基于第五样本数据进行训练得到的，所述第五样本数据包括第五操作行为样本数据和所述第五操作行为样本数据对应的标签，所述第五操作行为样本数据对应的标签用于表示所述第五操作行为数据对应的用户为认证用户或非认证用户;

以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型。

10.根据权利要求 9 所述的方法，其特征在于，所述第二操作行为样本数据的识别结果包括所述第一认证模型输出的识别结果和所述第二认证模型输出的识别结果; 所述第一认证模型输出的识别结果包括: 所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第一认证模型输出的第二操作行为样本对应的匹配结果; 所述第二认证模型输出的识别结果包括: 所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第二认证模型输出的第二操作行为样本数据对应的匹配结果;

其中，所述第二操作行为样本数据对应的匹配分数用于指示所述第二操作行为样本数据对应的用户被识别为认证用户的概率，所述第二操作行为样本数据对应的匹配结果用于

指示所述第二操作行为样本数据对应的用户被识别为认证用户或非认证用户，所述第二操作行为样本数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为样本数据对应的匹配分数确定的至少两个匹配结果。

11.根据权利要求 10 所述的方法，其特征在于，所述至少两个阈值包括第一阈值，所述方法还包括：

获取第四样本数据，所述第四样本数据包括第四操作行为样本数据和所述第四操作行为样本数据对应的标签，所述第四操作行为样本数据对应的标签用于表示所述第四操作行为样本数据对应的用户为认证用户或非认证用户；

将所述第四操作行为样本数据输入所述第一认证模型，得到所述第一认证模型输出的所述第四操作行为样本数据对应的匹配分数，所述第四操作行为样本数据对应的匹配分数用于指示所述第四操作行为样本数据对应的用户被识别为认证用户的概率；

基于多个候选阈值确定所述第四操作行为样本数据对应的匹配分数对应的多个候选匹配结果，所述多个候选匹配结果用于指示所述第四操作行为样本数据对应的用户被识别为认证用户或非认证用户；

将所述多个候选匹配结果中准确率满足预设条件的候选匹配结果对应的候选阈值确定为所述第一阈值。

12.根据权利要求 10 或 11 所述的方法，其特征在于，所述以所述第二操作行为数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型，包括：

根据所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第一分数特征；

根据所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第二分数特征；

以所述第二操作行为样本数据的第一分数特征、第二操作行为样本数据的第二分数特征和所述第二操作行为样本数据的识别结果作为决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练。

13.根据权利要求 9 至 12 中任一项所述的方法，其特征在于，所述第二操作行为样本数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

14.根据权利要求 9 至 13 中任一项所述的方法，其特征在于，所述第二样本数据是根据用户在触摸屏上的滑动时长和/或所述用户在触摸屏上的触摸点数进行筛选得到的。

15.根据权利要求 9 至 14 中任一项所述的方法，其特征在于，所述方法还包括：

获取第三样本数据，其中，所述第三样本数据包括：第三操作行为样本数据；

将所述第三操作行为样本数据输入到所述第一认证模型中，得到所述第一认证模型输出的第三操作行为样本数据的识别结果；

将所述第三操作行为样本数据输入到所述第二认证模型中，得到所述第二认证模型输出的第三操作行为样本数据的识别结果；

将所述第一认证模型输出的第三操作行为样本数据的识别结果、所述第二认证模型输

出的第三操作行为样本数据的识别结果输入到所述训练好的决策融合模型中，得到所述第三操作行为样本数据对应的身份认证结果；

根据所述第三操作行为样本数据和所述第三操作行为样本数据对应的身份认证结果对所述第一认证模型和/或所述第二认证模型进行训练。

16.一种身份认证的装置，其特征在于，包括：

获取单元，用于：

获取待认证用户的第一操作行为数据；

获取所述待认证用户的第二操作行为数据；

处理单元，用于：

以所述第一操作行为数据输入通过第一认证模型，获得所述第一认证模型输出的第一识别结果；

以所述第二操作行为数据输入通过第二认证模型，获得所述第二认证模型输出的第二识别结果；

其中，所述第一认证模型、第二认证模型分别为异常检测模型和分类模型；

将所述第一识别结果、所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果，其中，所述决策融合模型用于根据所述第一识别结果和所述第二识别结果的权重参数确定所述身份认证结果。

17.根据权利要求 16 所述的装置，其特征在于，所述决策融合模型的权重参数是通过将第二样本数据中的第二操作行为样本数据输入到所述第一认证模型和所述第二认证模型中，得到所述第一认证模型和所述第二认证模型输出的所述第二操作行为样本数据的识别结果，以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练得到的，所述第二样本数据包括所述第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户。

18.根据权利要求 16 或 17 所述的装置，其特征在于，

所述第一识别结果包括：所述第一操作行为数据对应的匹配分数和/或所述第一操作行为数据对应的匹配结果；

第二识别结果包括所述第二操作行为数据对应的匹配分数和/或所述第二操作行为数据对应的匹配结果；

其中，所述第一操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，所述第一操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，所述第一操作行为数据对应的匹配结果包括基于至少两个阈值和所述第一操作行为数据对应的匹配分数确定的至少两个匹配结果；

所述第二操作行为数据对应的匹配分数用于指示所述待认证用户被识别为认证用户的概率，所述第二操作行为数据对应的匹配结果用于指示所述待认证用户被识别为认证用户或非认证用户，所述第二操作行为数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为数据对应的匹配分数确定的至少两个匹配结果。

19.根据权利要求 18 所述的装置，其特征在于，所述处理单元具体用于：

根据所述第一操作行为数据对应的匹配分数得到第一分数特征;

根据所述第二操作行为数据对应的匹配分数得到第二分数特征;

以所述第一分数特征、所述第二分数特征、所述第一识别结果和所述第二识别结果输入到决策融合模型中，得到输出的身份认证结果。

20.根据权利要求 16 至 19 中任一项所述的装置，其特征在于，所述第一操作行为数据和/或所述第二操作行为数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

21.一种身份认证模型的训练装置，其特征在于，所述身份认证模型包括第一认证模型、第二认证模型和决策融合模型，其中，所述第一认证模型、第二认证模型分别为异常检测模型和分类模型，所述装置包括:

获取单元，用于获取第二样本数据，所述第二样本数据包括第二操作行为样本数据及所述第二操作行为样本数据对应的标签，所述第二操作行为样本数据对应的标签用于指示所述第二操作行为样本数据所对应的用户为认证用户或非认证用户;

处理单元，用于:

将所述第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到所述第二操作行为数据的识别结果，所述第一认证模型的模型参数是基于第一样本数据进行训练得到的，所述第一样本数据包括第一操作行为样本数据和所述第一操作行为样本数据对应的标签，所述第一操作行为样本数据对应的标签用于表示所述第一操作行为样本数据对应的用户为认证用户或非认证用户，所述第二认证模型的模型参数是基于第五样本数据进行训练得到的，所述第五样本数据包括第五操作行为样本数据和所述第五操作行为样本数据对应的标签，所述第五操作行为样本数据对应的标签用于表示所述第五操作行为数据对应的用户为认证用户或非认证用户;

以所述第二操作行为样本数据的识别结果作为所述决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练，得到训练好的决策融合模型。

22.根据权利要求 21 所述的装置，其特征在于，所述第二操作行为样本数据的识别结果包括所述第一认证模型输出的识别结果和所述第二认证模型输出的识别结果;所述第一认证模型输出的识别结果包括:所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第一认证模型输出的第二操作行为样本对应的匹配结果;所述第二认证模型输出的识别结果包括:所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数和/或所述第二认证模型输出的第二操作行为样本数据对应的匹配结果;

其中，所述第二操作行为样本数据对应的匹配分数用于指示所述第二操作行为样本数据对应的用户被识别为认证用户的概率，所述第二操作行为样本数据对应的匹配结果用于指示所述第二操作行为样本数据对应的用户被识别为认证用户或非认证用户，所述第二操作行为样本数据对应的匹配结果包括基于至少两个阈值和所述第二操作行为样本数据对应的匹配分数确定的至少两个匹配结果。

23.根据权利要求 22 所述的装置，其特征在于，所述至少两个阈值包括第一阈值，以及

所述获取单元还用于：获取第四样本数据，所述第四样本数据包括第四操作行为样本数据和所述第四操作行为样本数据对应的标签，所述第四操作行为样本数据对应的标签用于表示所述第四操作行为样本数据对应的用户为认证用户或非认证用户；

所述处理单元还用于：

将所述第四操作行为样本数据输入所述第一认证模型，得到所述第一认证模型输出的所述第四操作行为样本数据对应的匹配分数，所述第四操作行为样本数据对应的匹配分数用于指示所述第四操作行为样本数据对应的用户被识别为认证用户的概率；

基于多个候选阈值确定所述第四操作行为样本数据对应的匹配分数对应的多个候选匹配结果，所述多个候选匹配结果用于指示所述第四操作行为样本数据对应的用户被识别为认证用户或非认证用户；

将所述多个候选匹配结果中准确率满足预设条件的候选匹配结果对应的候选阈值确定为所述第一阈值。

24.根据权利要求 22 或 23 所述的装置，其特征在于，所述处理单元具体用于：

根据所述第一认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第一分数特征；

根据所述第二认证模型输出的所述第二操作行为样本数据对应的匹配分数得到第二操作行为样本数据的第二分数特征；

以所述第二操作行为样本数据的第一分数特征、第二操作行为样本数据的第二分数特征和所述第二操作行为样本数据的识别结果作为决策融合模型的输入，以所述第二操作行为样本数据对应的标签作为所述决策融合模型的目标输出值进行训练。

25.根据权利要求 21 至 24 中任一项所述的装置，其特征在于，所述第二操作行为样本样本数据包括以下数据中的至少一种：触摸点 X/Y 轴坐标、触摸面积、触摸压力、触屏速度、触屏加速度、触屏轨迹的斜率、触屏长度、触屏位移、触屏角度、触屏方向、加速度 X/Y/Z 轴数据或陀螺仪 X/Y/Z 轴数据。

26.根据权利要求 21 至 25 中任一项所述的装置，其特征在于，

所述获取单元还用于：获取第三样本数据，其中，所述第三样本数据包括：第三操作行为样本数据；

所述处理单元还用于：

将所述第三操作行为样本数据输入到所述第一认证模型中，得到所述第一认证模型输出的第三操作行为样本数据的识别结果；

将所述第三操作行为样本数据输入到所述第二认证模型中，得到所述第二认证模型输出的第三操作行为样本数据的识别结果；

将所述第一认证模型输出的第三操作行为样本数据的识别结果、所述第二认证模型输出的第三操作行为样本数据的识别结果输入到所述训练好的决策融合模型中，得到所述第三操作行为样本数据对应的身份认证结果；

根据所述第三操作行为样本数据和所述第三操作行为样本数据对应的身份认证结果对所述第一认证模型和/或所述第二认证模型进行训练。

27.一种身份认证的装置，其特征在于，包括处理器和存储器，所述处理器与所述存储器耦合，所述处理器用于读取并执行所述存储器中的指令，以执行如权利要求 1 至 8 中

任一项所述的方法。

28.一种身份认证模型的训练装置，其特征在于，包括处理器和存储器，所述处理器与所述存储器耦合，所述处理器用于读取并执行所述存储器中的指令，以执行如权利要求9至15中任一项所述的训练方法。

29.一种计算机可读介质，其特征在于，所述计算机可读介质存储有程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行如权利要求1至8中任一项所述的方法。

30.一种计算机可读介质，其特征在于，所述计算机可读介质存储有程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行如权利要求9至15中任一项所述的训练方法。

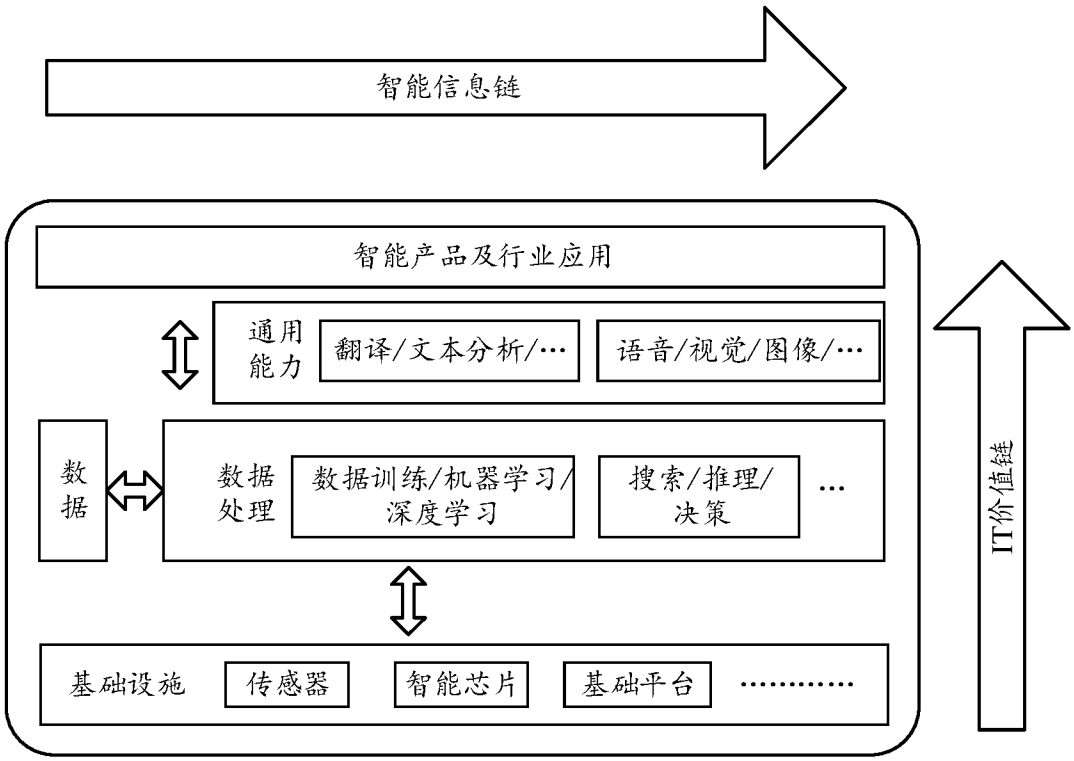

智能信息链
智能产品及行业应用
通用能力
翻译/文本分析/…
语音/视觉/图像/…
数据
数据处理
数据训练/机器学习/深度学习
搜索/推理/决策
…
基础设施
传感器
智能芯片
基础平台
……
IT价值链

图 1

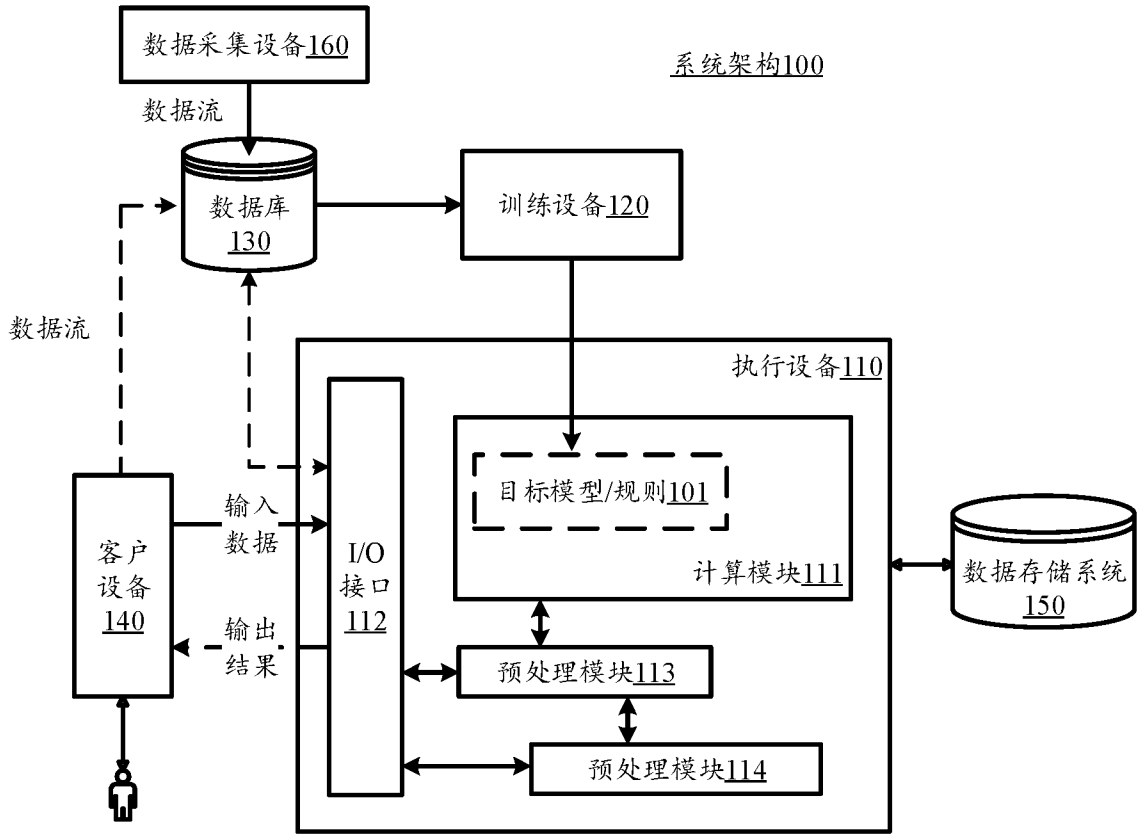

数据采集设备160
系统架构100
数据流
数据库
130
训练设备120
数据流
执行设备110
目标模型/规则101
计算模块111
数据存储系统
150
客户
设备
140
输入
数据
输出
结果
I/O
接口
112
预处理模块113
预处理模块114

图 2

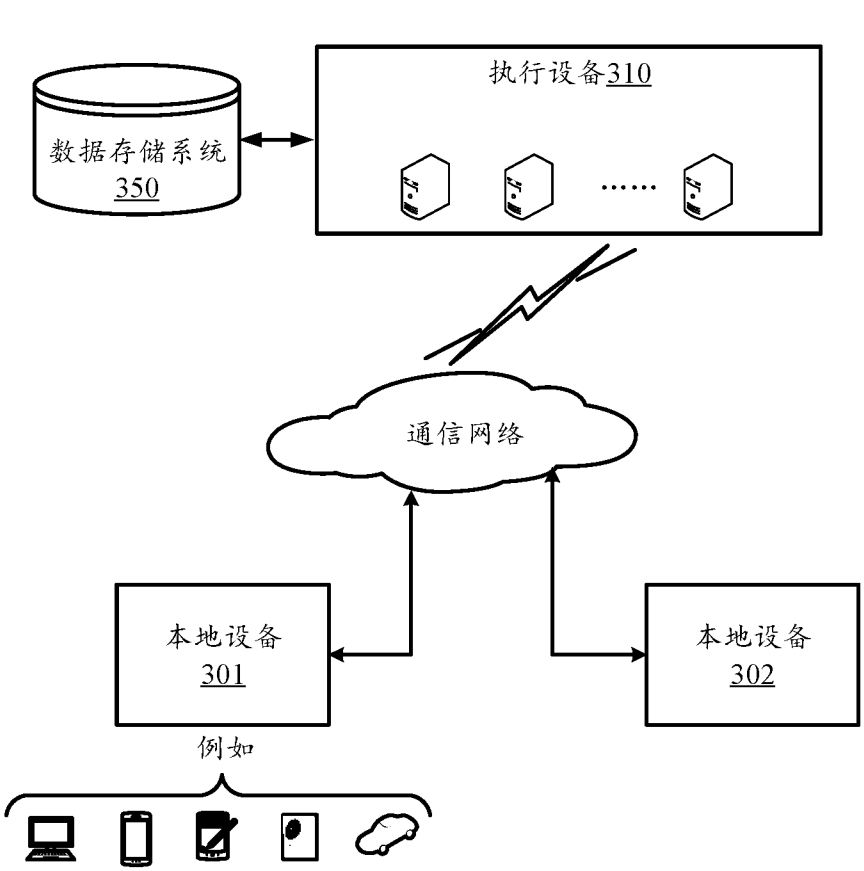


图 3

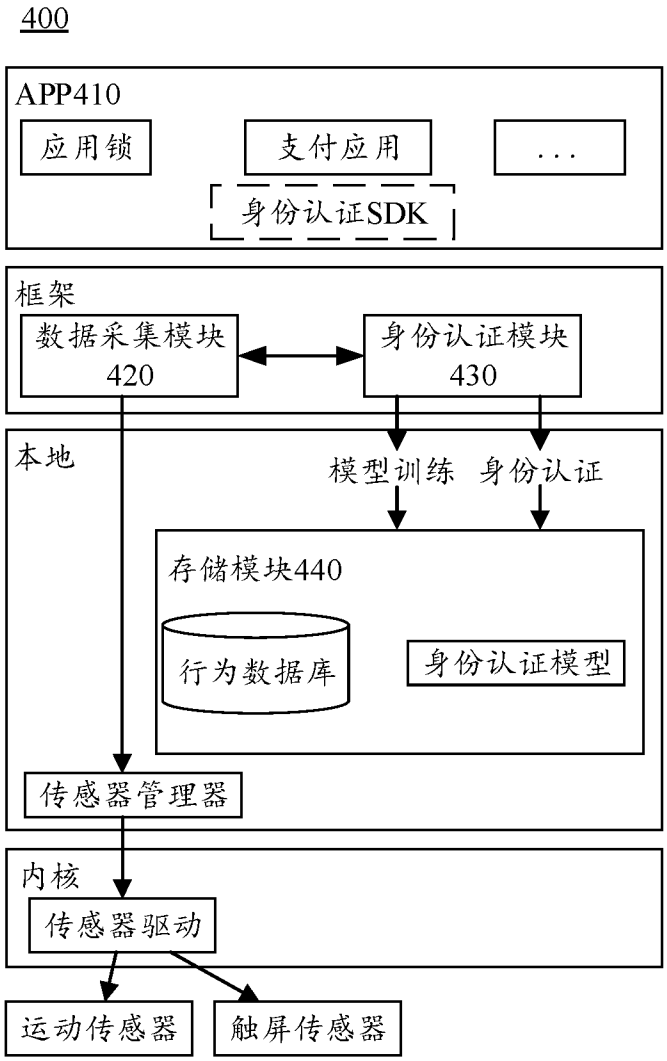

400
APP410
应用锁
支付应用
...
身份认证SDK
框架
数据采集模块
420
身份认证模块
430
本地
模型训练
身份认证
存储模块440
行为数据库
身份认证模型
传感器管理器
内核
传感器驱动
运动传感器
触屏传感器

图 4

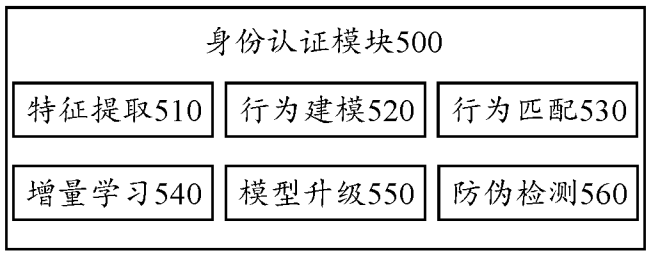

身份认证模块500
特征提取510
行为建模520
行为匹配530
增量学习540
模型升级550
防伪检测560

图 5

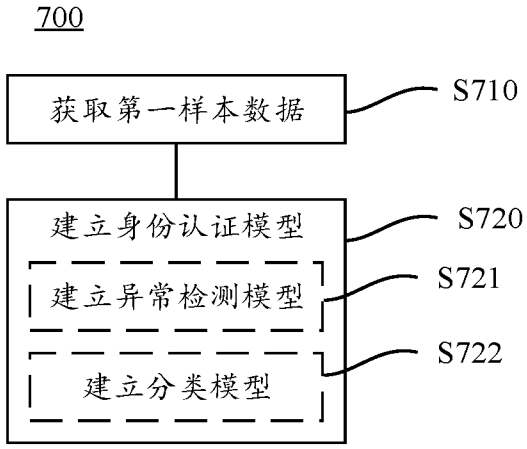

700
获取第一样本数据
S710
建立身份认证模型
S720
建立异常检测模型
S721
建立分类模型
S722

图 6

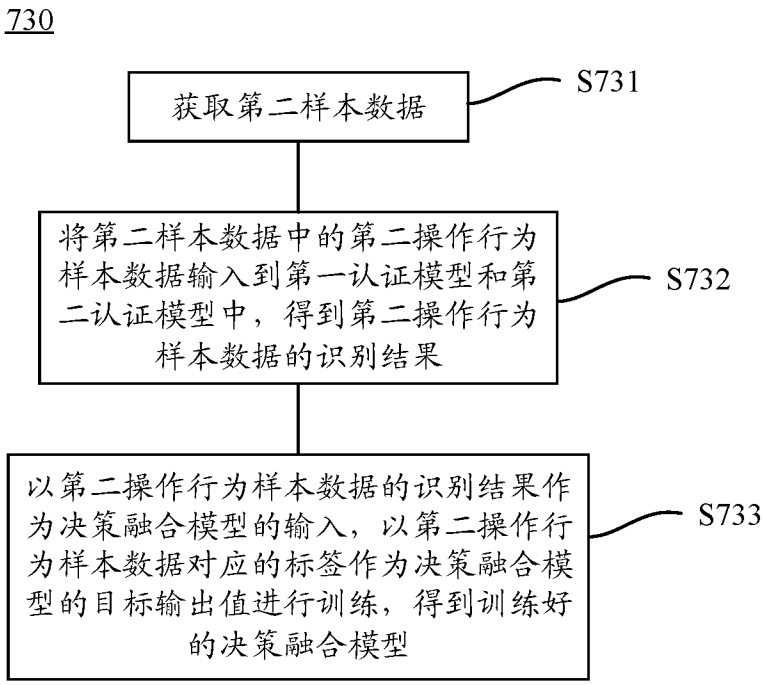

730
获取第二样本数据
S731
将第二样本数据中的第二操作行为样本数据输入到第一认证模型和第二认证模型中，得到第二操作行为样本数据的识别结果
S732
以第二操作行为样本数据的识别结果作为决策融合模型的输入，以第二操作行为样本数据对应的标签作为决策融合模型的目标输出值进行训练，得到训练好的决策融合模型
S733

图 7

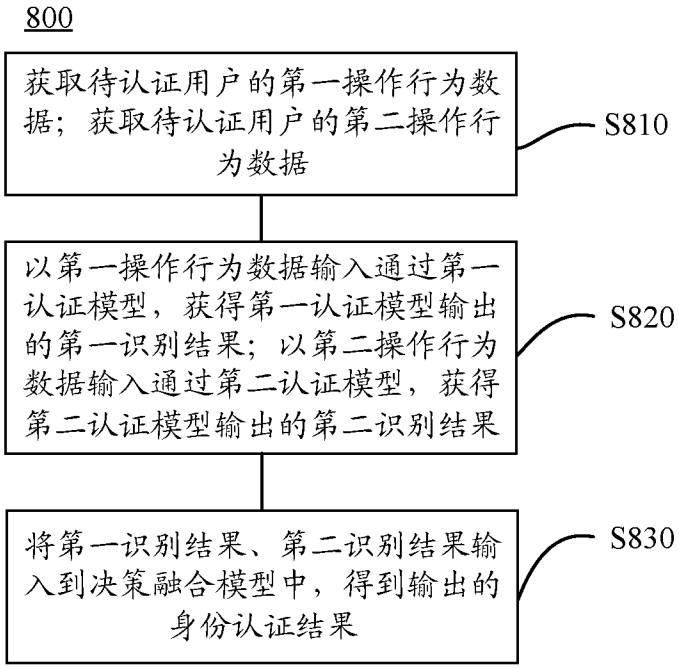

800
获取待认证用户的第一操作行为数据；获取待认证用户的第二操作行为数据
S810
以第一操作行为数据输入通过第一认证模型，获得第一认证模型输出的第一识别结果；以第二操作行为数据输入通过第二认证模型，获得第二认证模型输出的第二识别结果
S820
将第一识别结果、第二识别结果输入到决策融合模型中，得到输出的身份认证结果
S830

图 8

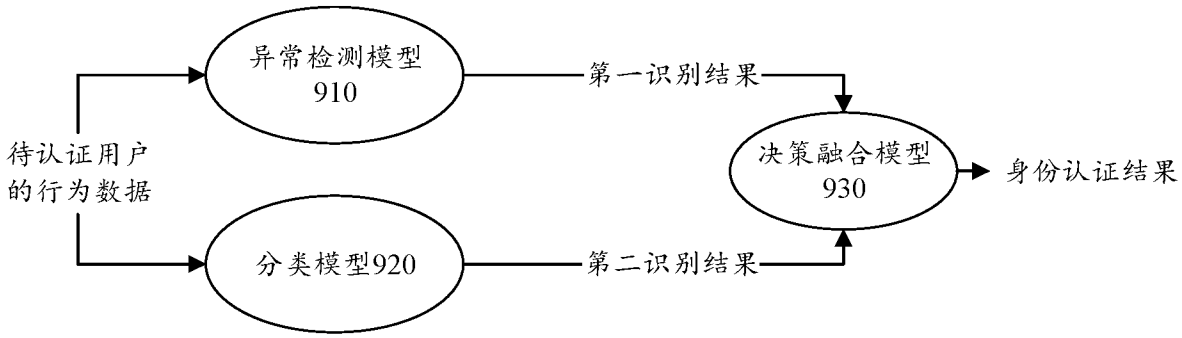

异常检测模型
910
第一识别结果
待认证用户
的行为数据
决策融合模型
930
身份认证结果
分类模型920
第二识别结果

图 9

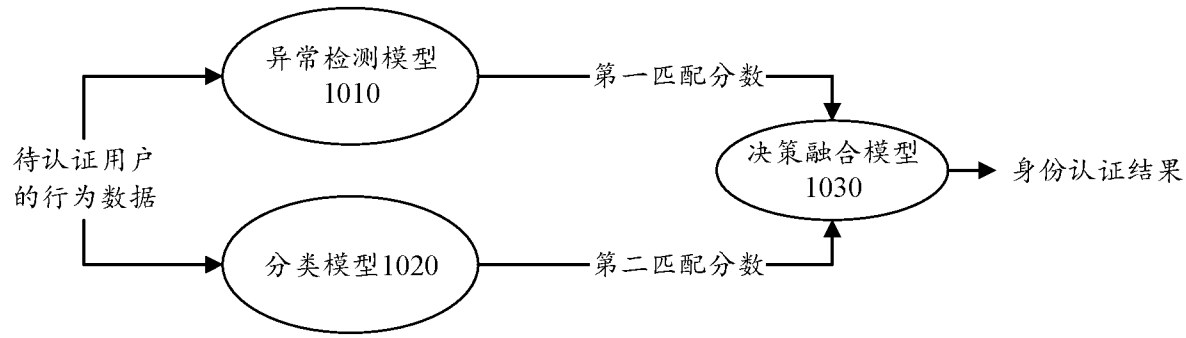

异常检测模型
1010
第一匹配分数
待认证用户
的行为数据
决策融合模型
1030
身份认证结果
分类模型1020
第二匹配分数

图 10

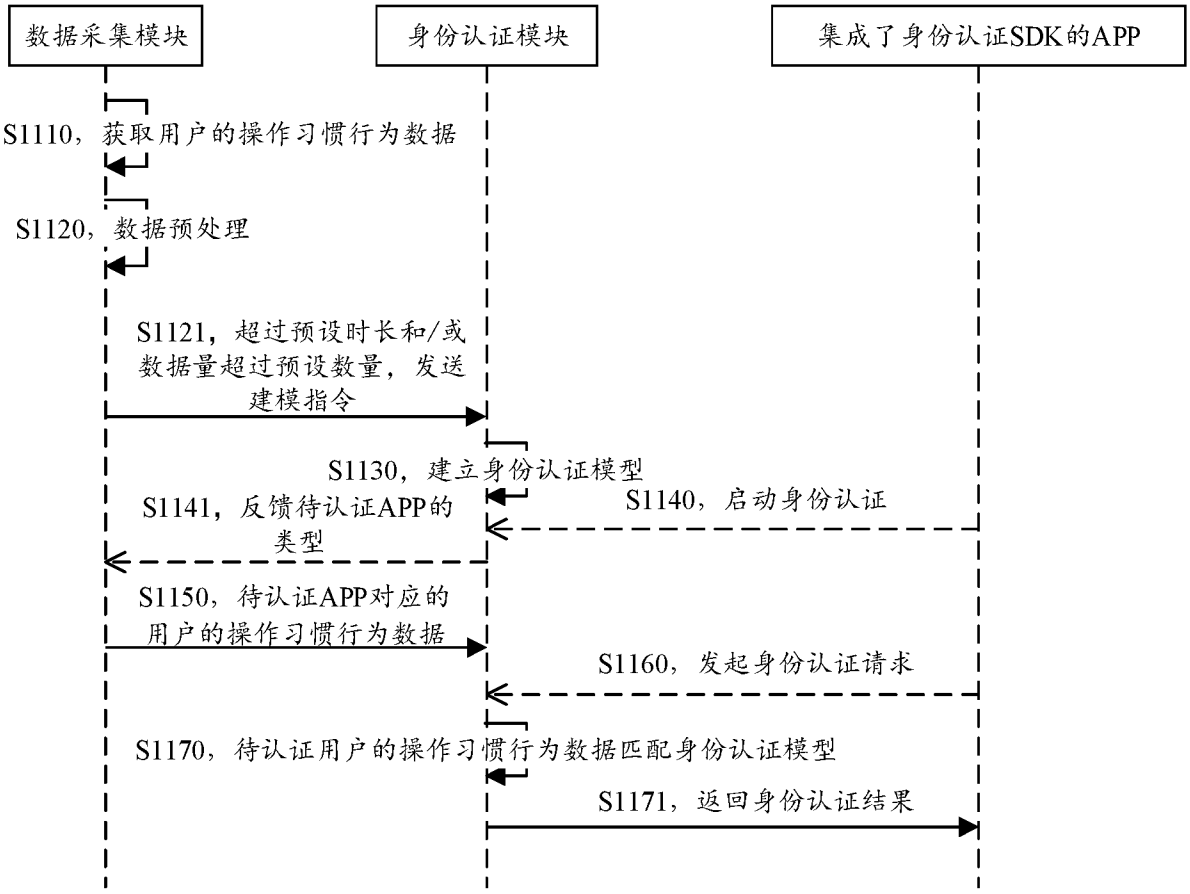

数据采集模块
身份认证模块
集成了身份认证SDK的APP
S1110，获取用户的操作习惯行为数据
S1120，数据预处理
S1121，超过预设时长和/或数据量超过预设数量，发送建模指令
S1130，建立身份认证模型
S1140，启动身份认证
S1141，反馈待认证APP的类型
S1150，待认证APP对应的用户的操作习惯行为数据
S1160，发起身份认证请求
S1170，待认证用户的操作习惯行为数据匹配身份认证模型
S1171，返回身份认证结果

图 11

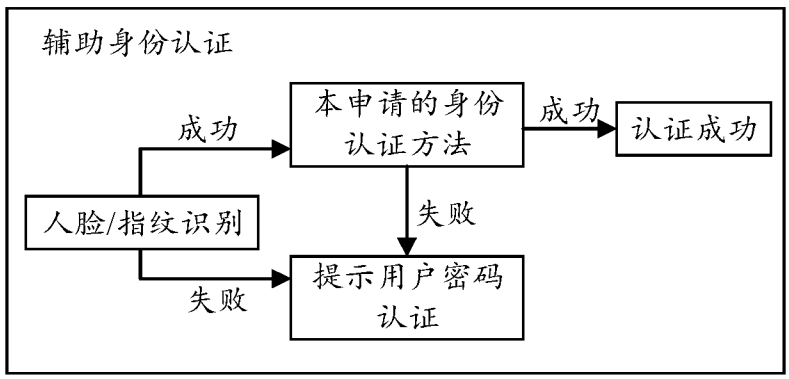

辅助身份认证
本申请的身份认证方法
成功
成功
认证成功
人脸/指纹识别
失败
失败
提示用户密码认证

图 12

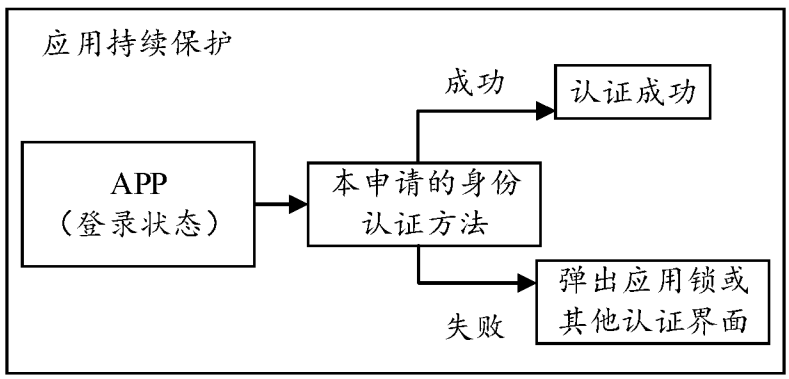

应用持续保护
成功
认证成功
APP
（登录状态）
本申请的身份认证方法
弹出应用锁或其他认证界面
失败

图 13

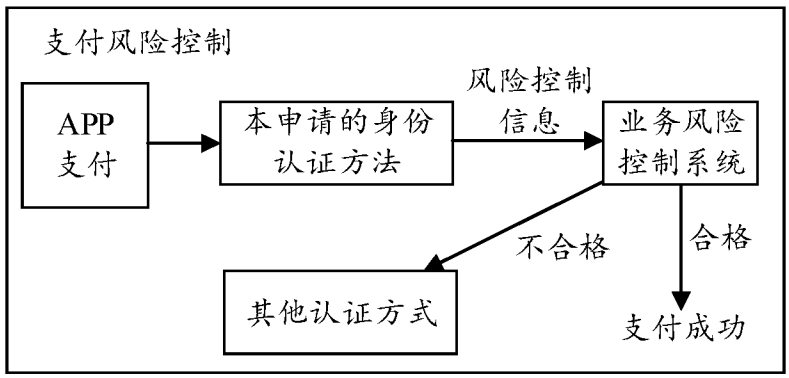

支付风险控制
APP
支付
本申请的身份
认证方法
风险控制
信息
业务风险
控制系统
不合格
合格
其他认证方式
支付成功

图 14

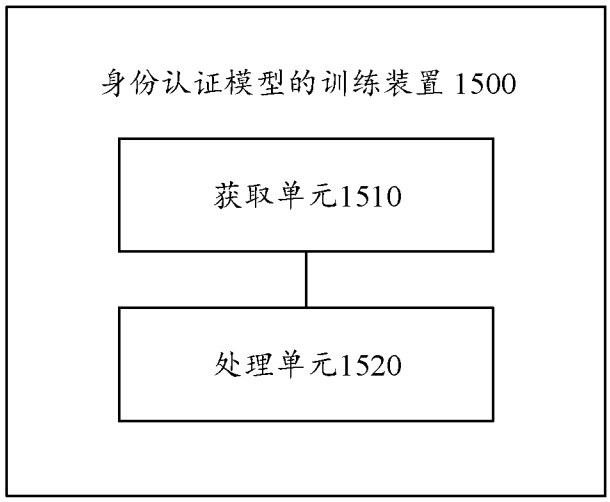

身份认证模型的训练装置 1500
获取单元1510
处理单元1520

图 15

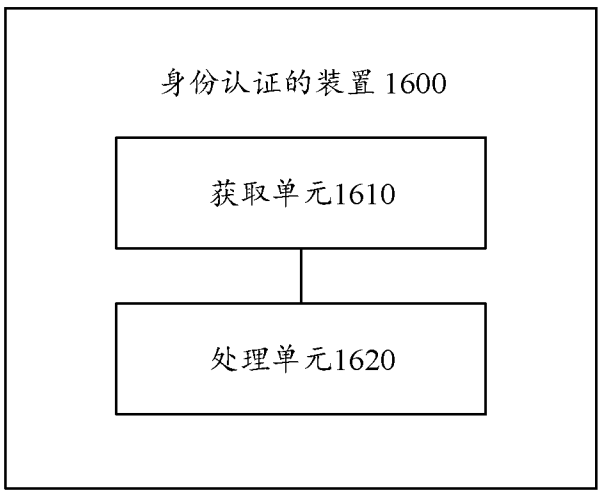

身份认证的装置 1600
获取单元1610
处理单元1620

图 16

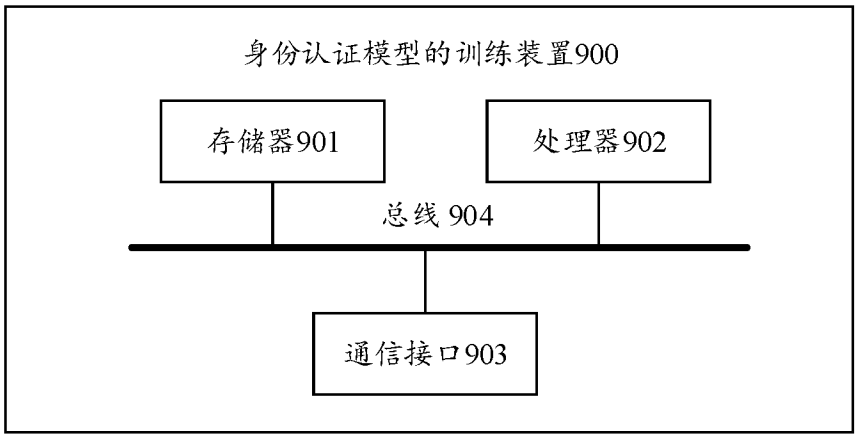

身份认证模型的训练装置900
存储器901
处理器902
总线 904
通信接口903

图 17

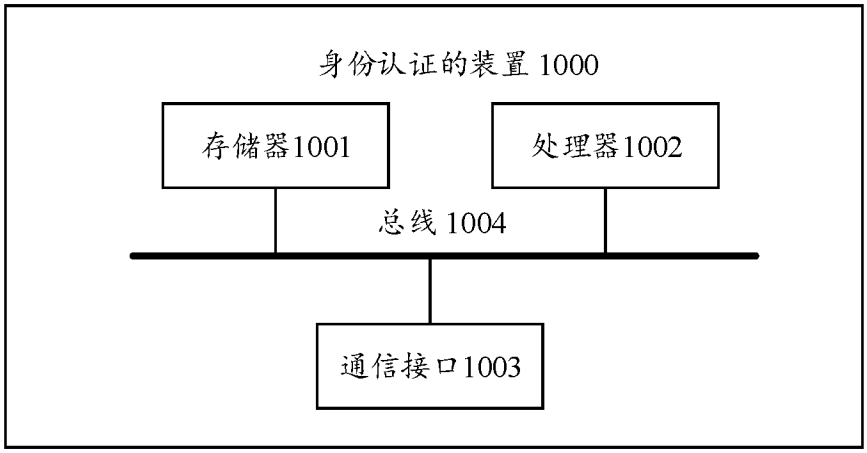

身份认证的装置 1000
存储器1001
处理器1002
总线 1004
通信接口1003

图 18

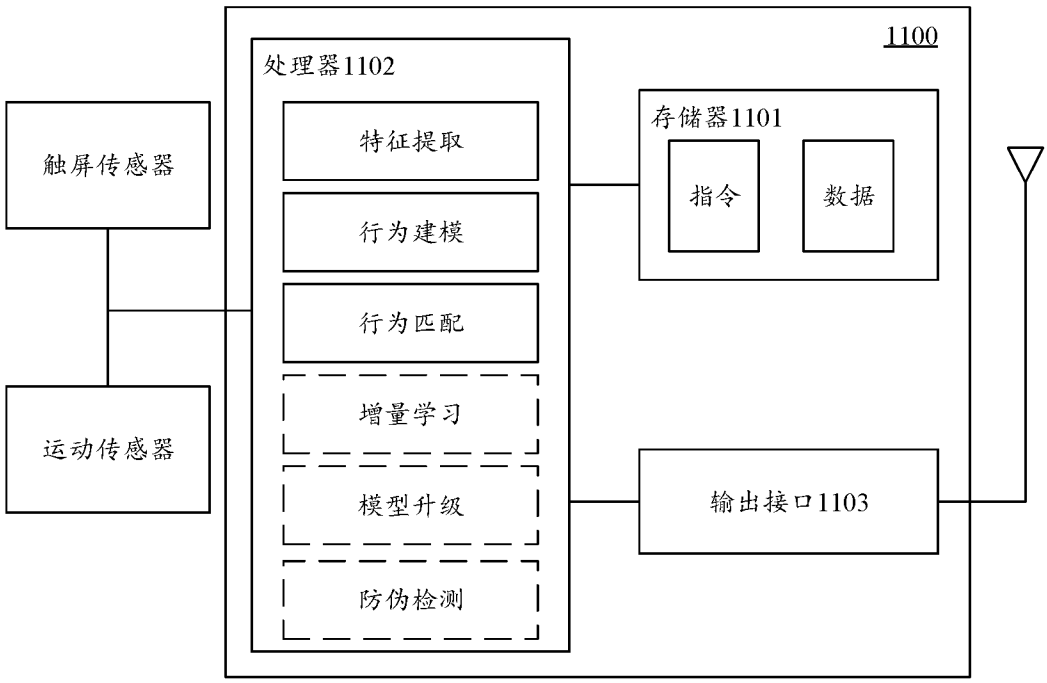

1100
处理器1102
特征提取
行为建模
行为匹配
增量学习
模型升级
防伪检测
存储器1101
指令
数据
触屏传感器
运动传感器
输出接口1103

图 19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/085319

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i; G06N 3/08(2006.01)i; G06F 21/31(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; SIPOABS; DWPI; USTXT; WOTXT; EPTXT: 身份, 认证, 验证, 模型, 第一, 第二, 分类, 融合, 权重, 训练, 异常, 用户, 分数, 概率, 触摸, 加速度, identity, authentication, model, first, second, classification, fusion, weight, train, abnormal, score, probability, touch, acceleration

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106039711 A (NETEASE (HANGZHOU) NETWORK CO., LTD.) 26 October 2016 (2016-10-26) description paragraphs [0042]-[0105], [0197]-[0204]	1-30
A	CN 110674483 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 10 January 2020 (2020-01-10) entire document	1-30
A	CN 104239761 A (XI'AN JIAOTONG UNIVERSITY) 24 December 2014 (2014-12-24) entire document	1-30
A	CN 104408341 A (XI'AN JIAOTONG UNIVERSITY) 11 March 2015 (2015-03-11) entire document	1-30

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2021	**23 June 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/085319

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106039711 A	26 October 2016	CN 106039711 B	14 May 2019
CN 110674483 A	10 January 2020	None	
CN 104239761 A	24 December 2014	CN 104239761 B	27 June 2017
CN 104408341 A	11 March 2015	CN 104408341 B	27 June 2017

国际检索报告

国际申请号
PCT/CN2021/085319

A. 主题的分类

G06F 21/32(2013.01)i; G06N 3/08(2006.01)i; G06F 21/31(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F G06N

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;SIPOABS;DWPI;USTXT;WOTXT;EPTXT：身份，认证，验证，模型，第一，第二，分类，融合，权重，训练，异常，用户，分数，概率，触摸，加速度，identity，authentication，model，first，second，classification，fusion，weight，train，abnormal，score，probability，touch，acceleration

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 106039711 A (网易杭州网络有限公司) 2016年 10月 26日 (2016 - 10 - 26) 说明书第[0042]-[0105]、[0197]-[0204]段	1-30
A	CN 110674483 A (广东工业大学) 2020年 1月 10日 (2020 - 01 - 10) 全文	1-30
A	CN 104239761 A (西安交通大学) 2014年 12月 24日 (2014 - 12 - 24) 全文	1-30
A	CN 104408341 A (西安交通大学) 2015年 3月 11日 (2015 - 03 - 11) 全文	1-30

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
“A” 认为不特别相关的表示了现有技术一般状态的文件
“E” 在国际申请日的当天或之后公布的在先申请或专利
“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
“O” 涉及口头公开、使用、展览或其他方式公开的文件
“P” 公布日先于国际申请日但迟于所要求的优先权日的文件
“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 5月 31日	2021年 6月 23日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 石蒙蒙 电话号码 (86-512) 88995856

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/085319

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106039711	A	2016年 10月 26日	CN	106039711	B	2019年 5月 14日
CN	110674483	A	2020年 1月 10日		无		
CN	104239761	A	2014年 12月 24日	CN	104239761	B	2017年 6月 27日
CN	104408341	A	2015年 3月 11日	CN	104408341	B	2017年 6月 27日