

(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
2018 年 6 月 7 日 (07.06.2018)



(10) 国际公布号
WO 2018/099276 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/111506

(22) 国际申请日: 2017 年 11 月 17 日 (17.11.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611089354.3 2016年11月30日 (30.11.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛
大开曼资本大厦一座四层 847 号邮箱,
Grand Cayman (KY)。

(72) 发明人: 于鲲(YU, Kun); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 王炎(WANG, Yan); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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,

(54) Title: IDENTITY AUTHENTICATION METHOD AND APPARATUS, AND COMPUTING DEVICE

(54) 发明名称: 身份认证方法及装置和计算设备

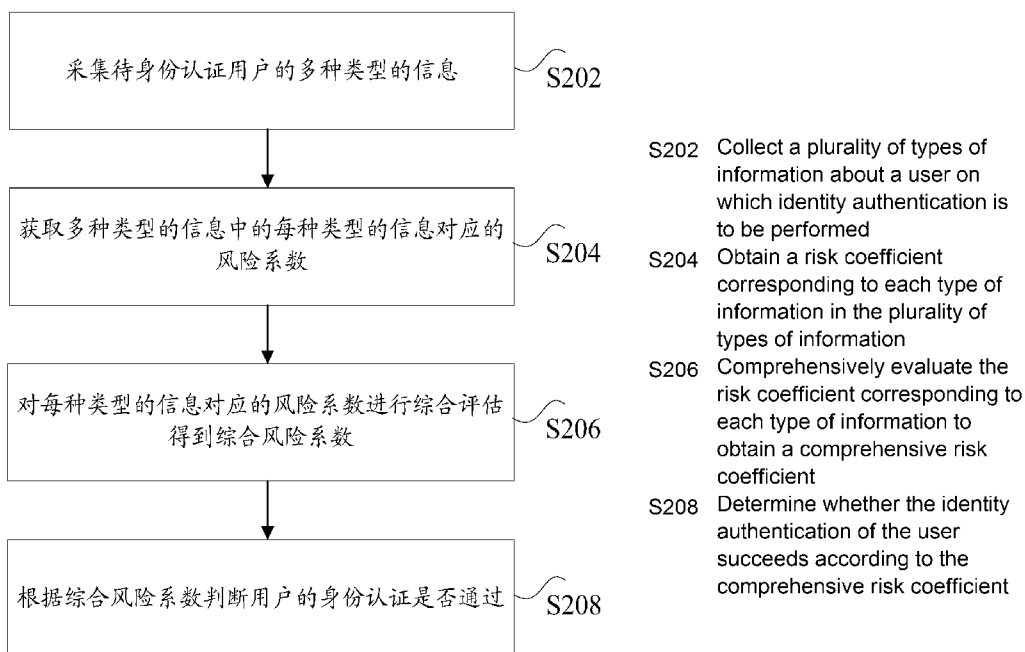


图 2

(57) Abstract: Disclosed are an identity authentication method and apparatus, and a computing device. The method comprises: collecting a plurality of types of information about a user on which identity authentication is to be performed, wherein the plurality of types of information is used for authenticating the identity of the user; obtaining a risk coefficient corresponding to each type of information in the plurality of types of information, wherein the risk coefficient is used for indicating a degree of trust of the identity of the user; comprehensively evaluating the risk coefficient corresponding to each type of information to obtain a comprehensive risk coefficient;

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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(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))。

and determining whether the identity authentication of the user succeeds according to the comprehensive risk coefficient. The present invention resolves the technical problem in the related art of impact on user experience caused by a high risk of error during identity authentication decision making due to that determinations of whether identity authentication of the user succeeds based on different identity authentication conditions are independent of each other and have no relevance.

(57) 摘要: 本发明公开了一种身份认证方法及装置和计算设备。其中, 该方法包括: 采集待身份认证用户的多种类型的信息, 其中, 多种类型的信息用于对用户的身份进行认证; 获取多种类型的信息中的每种类型的信息对应的风险系数, 其中, 风险系数用于指示用户的身份被信任的程度; 对每种类型的信息对应的风险系数进行综合评估得到综合风险系数; 根据综合风险系数判断用户的身份认证是否通过。本发明解决了由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大, 影响用户体验的技术问题。

身份认证方法及装置和计算设备

本申请要求 2016 年 11 月 30 日递交的申请号为 201611089354.3、发明名称为“身份认证方法及装置和计算设备”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。

5

技术领域

本发明涉及互联网技术领域，具体而言，涉及一种身份认证方法及装置和计算设备。

背景技术

10 身份认证也称为“身份验证”或“身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。对于互联网身份认证，通常是

15 根据身份认证条件认定用户身份，从而对通过所有身份认证条件的用户进行授权。例如，身份认证条件为身份证信息，根据输入的身份证信息即可判定用户是否通过身份认证。再例如，身份认证条件为用户的人脸信息，根据用户的人脸信息即可判定用户是否通过身份认证。也即，相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联，因此身份认证决策时出错的风险较大，影响用户体验。

20 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

本发明实施例提供了一种身份认证方法及装置和计算设备，以至少解决由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关

25 联造成的身份认证决策时出错的风险较大，影响用户体验的技术问题。

根据本发明实施例的一个方面，提供了一种身份认证方法，该方法包括：采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度；对每种类型的信息对应的风险系数进行综合评估得到综合风险系

30 数；根据综合风险系数判断用户的身份认证是否通过。

根据本发明实施例的另一方面，还提供了一种身份认证装置，该装置包括：采集单元，用于采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；第一获取单元，用于获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度；第二获取单元，用于对每
5 种类型的信息对应的风险系数进行综合评估得到综合风险系数；判断单元，用于根据综合风险系数判断用户的身份认证是否通过。

根据本发明实施例的另一方面，还提供了一种计算设备，提供第一界面，用于用户交互；其中，第一界面包括：多个第一控件，用于采集待身份认证用户的多种类型的信息，多种类型的信息用于对用户的身份进行认证；第一发送单元，用于将多种类型的信
10 息发送至服务器，通过服务器对多种类型的信息的风险系数进行评估，得到综合风险系数，其中，风险系数用于指示用户的身份被信任的程度；第二接收单元，用于接收服务器发送的与多种类型的信息对应的风险系数以及综合风险系数；与多个第一控件对应的多个第二控件，用于体现每种类型的信息对应的风险系数；第三控件，用于体现待身份认证用户的综合风险系数。

在本发明实施例中，采用多种类型的信息对用户进行身份认证的方式，通过采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度；对每种类型的信息对应的风险系数进行综合评估得到综合风险系数；根据综合风险系数判断用户的身份认证是否通过，从而将每种类型的信息对应的
20 风险系数进行关联，避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大，达到了提升对用户的身份认证准确性的目的，从而实现了提升用户体验度的技术效果，进而解决了由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大，影响用户体验的技术问题。

附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是根据本发明实施例的一种可选的身份认证方法的计算机终端的硬件结构框
30 图；

图 2 是根据本发明实施例的一种身份认证方法的流程图；

图 3 是根据本发明实施例的一种可选的身份认证方法的流程图；

图 4 是根据本发明实施例的一种可选的身份认证方法的流程图；

图 5 是根据本发明实施例的一种可选的身份认证方法的流程图；

5 图 6 是根据本发明实施例的一种可选的身份认证方法的示意图；

图 7 是根据本发明实施例的一种可选的身份认证方法的示意图；

图 8 是根据本发明实施例的一种身份认证装置的示意图；

图 9 是根据本发明实施例的一种计算设备的示意图；以及

图 10 是根据本发明实施例的一种可选的计算机终端的结构框图。

10

具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范

15 围。

需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里

20 图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

实施例 1

25 本发明实施例提供了一种身份认证方法实施例。该身份认证方法可以使用到在互联网中对用户的身份认证上，例如，在金融相关的应用中，用户注册到该应用当中之后，需要确认用户的身份，如果用户仅仅上传一张图片其实并不足以认为该张照片是这个用户拍摄的自己的照片，这是由于用户完全可以从互联网上下载照片进行冒充。如果采集用户的多种类型的信息，则可以降低这种风险。当采集到用户的多种类型的信息时，则

30 对每种类型的信息对应的风险系数进行综合评估得到综合风险系数；根据综合风险系数

判断用户的身份认证是否通过。

以下的方案可以实施到安装在移动终端的应用中，即可以通过移动终端的应用来判断用户的身份认证是否通过。

以下的方案也可以实施到服务器上，例如，应用或者软件可以仅仅作为获取照片的一个接口，用户可以通过应用或软件上传照片，然后，应用或者软件将这些照片传送到服务器，由服务器进行判断。服务器的计算能力是要强于应用本身的，因此，在服务器上进行使用可以同时来自不同应用或软件的大量的照片进行处理。服务器可以是真实的硬件服务器，也可以是一种服务。随着云计算的发展，这种服务也可以安置在云服务上进行处理。

无论是在终端上实施还是在服务器上实施，以下方案的识别结果都可以被其他的应用或者服务所使用。总之，根据对用户的身份进行认证的多种类型的信息来对用户进行身份认证可以实施到多种情况中，在此不再一一介绍。

在下文中首先对实施本申请实施例方案的移动终端、计算机、服务器等硬件结果进行说明。以下所说明的硬件结构是当前比较通用的硬件结构，随着技术的发展，这些硬件结构会发生变化，无论怎样的硬件结构只要能够实施本申请实施例中的方案就可以实现判断用户的身份认证是否通过。

本申请实施例一所提供的身份认证方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。图 1 示出了一种用于实现身份认证方法的计算机终端（或移动设备）的硬件结构框图。如图 1 所示，计算机终端 10（或移动设备 10）可以包括一个或多个（图中采用 102a、102b，……，102n 来示出）处理器 102（处理器 102 可以包括但不限于微处理器 MCU 或可编程逻辑器件 FPGA 等的处理装置）、用于存储数据的存储器 104、以及用于通信功能的传输模块。除此以外，还可以包括：显示器、输入/输出接口（I/O 接口）、通用串行总线（USB）端口（可以作为 I/O 接口的端口中的一个端口被包括）、网络接口、电源和/或相机。本领域普通技术人员可以理解，图 1 所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，计算机终端 10 还可包括比图 1 中所示更多或者更少的组件，或者具有与图 1 所示不同的配置。

应当注意到的是上述一个或多个处理器 102 和/或其他数据处理电路在本文中通常可以被称为“数据处理电路”。该数据处理电路可以全部或部分的体现为软件、硬件、固件或其他任意组合。此外，数据处理电路可为单个独立的处理模块，或全部或部分的结合到计算机终端 10（或移动设备）中的其他元件中的任意一个内。如本申请实施例中所

涉及到的，该数据处理电路作为一种处理器控制（例如与接口连接的可变电阻终端路径的选择）。

存储器 104 可用于存储应用程序的软件程序以及模块，如本发明实施例中的身份认证方法对应的程序指令/数据存储装置，处理器 102 通过运行存储在存储器 104 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的身份认证方法。存储器 104 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 104 可进一步包括相对于处理器 102 远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端 10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

传输装置用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端 10 的通信供应商提供的无线网络。在一个实例中，传输装置 106 包括一个网络适配器（Network Interface Controller，NIC），其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置可以为射频（Radio Frequency，RF）模块，其用于通过无线方式与互联网进行通讯。

显示器可以例如触摸屏式的液晶显示器（LCD），该液晶显示器可使得用户能够与计算机终端 10（或移动设备）的用户界面进行交互。

此处需要说明的是，在一些可选实施例中，上述图 1 所示的计算机设备（或移动设备）可以包括硬件元件（包括电路）、软件元件（包括存储在计算机可读介质上的计算机代码）、或硬件元件和软件元件两者的结合。应当指出的是，图 1 仅为特定具体实例的一个实例，并且旨在示出可存在于上述计算机设备（或移动设备）中的部件的类型。

在上述运行环境下，本申请提供了如图 2 所示的身份认证方法，该方法具体包括如下步骤：

步骤 S202，采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证。

在很多场景下需要在互联网上对用户进行身份认证。为了对待身份认证用户进行身份认证，首先采集对该用户的身份进行身份认证的多种类型的信息。

例如，用户 A（待身份认证用户）为了在某网站上为自己开设一实名账户，因此需要在互联网上进行身份认证，待身份认证通过之后，某网站才会对用户 A 进行授权，为其开设实名账户。通常，用户 A 为了在互联网上进行身份认证，可能会上传一些用户 A 的相关材料。对于互联网端，为了对用户 A 的身份进行认证，在上传了一些用户 A 的相

关材料的情况下，采集用户 A 上传的相关材料中的信息，该信息中包括对用户 A 的进行身份认证的信息。同时也在互联网中采集可对用户 A 的进行身份认证的信息。如果未上传一些用户 A 的相关材料，则在互联网中采集可对用户 A 的进行身份认证的信息。

在一种可选的实施例中，用户的信息的类型包括以下至少之一：证件信息、生物特征信息、权限信息、用户在互联网上的行为信息。

再以用户 A 为例，上传的相关材料中包括以下至少之一：用户 A 的证件、用户 A 的生物特征，采集用户 A 上传的相关材料中的信息，该信息中包括上传的证件中的证件信息，上传的用户 A 的生物特征中的生物特征信息。

采集用户 A 在互联网中的权限信息，例如，判断在互联网中用户 A 是否在互联网黑名单中，如果用户 A 在黑名单中，那么用户 A 的在互联网中的权利会被限制。

用户 A 在互联网上的行为信息可以为用户 A 在互联网上的访问轨迹，例如，根据用户 A 在互联网上的访问轨迹可以确定用户 A 在互联网上的操作是否存在风险。

步骤 S204，获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度。风险系数可以是正向进行评估的系数，此时风险系数数值越大，用户的身份被信任的程度越高，用户的身份被认证通过之后风险越低；风险系数也可以是从反向进行评估的系数，此时风险系数数值越大，用户的身份被信任的程度越低，用户的身份被认证通过之后风险越高。

用户信息的类型可能有很多种，作为一个可选的实施例，用户的信息的类型可以包括以下至少之一：证件信息、生物特征信息、权限信息、用户在互联网上的行为信息。在这几种信息中，用户在互联网上的行为信息是比较优的一种信息，通过用户的行为信息也可以作为对用户进行评估的一种参考，这在下文中将举例说明。

在上述几种信息中，证件信息是比较重要的一个信息，对于证件信息的评估可以采用多个维度，例如，在一个可选的实施方式中，可以根据如下条件的至少之一确定证件信息对应的风险系数：证件清晰度、证件齐全度、证件有效性。证件清晰度可以用来判断该证件是否是从网上下载的证件，而并非为用户拍摄的证件照片；证件的齐全度可以用作综合的评估，比如只有身份证照片并足以说明用户上传的身份证照片就是他自己，如果用户上传了身份证和驾照，那么该用户作假的风险就降低很多了。证件的有效性可以用来验证该证件是否仍然有效，这对于判断该用户作假的风险也有所帮助。当然，证件信息并不限于此，上述的这几种证件信息可以单独使用也可以组合使用，只要能够评估用户的风险系数即可。

需要说明的是，风险系数可以为系数值，也可以为概率。

例如，针对证件清晰度，以用户 A 为例，根据用户 A 的上传的证件的清晰度确定风险系数。如果使用概率来表示的话，100%认为是用户证件照是清晰的，完全没有风险。照片清晰程度可以使用照片的一些参数来进行限定，例如照片的像素、照片的大小等等，
5 现有的一些照片清晰度的算法可以应用在本实施例中，在此不再赘述。如过上传的证件的清晰度为 80%，则确定上传的证件合格的可能性为 80%，根据证件合格的可能性确定风险系数为 80%。需要说明的是，证件的清晰度可以根据对证件中的信息进行成功识别的可能性得到。作为另一个可选的实施方式，使用证件不合格的概率来表示风险系数，在本例子中，风险系数也可以认为是 $100\%-80\%=20\%$ 。如论从正相关的角度还是从负相关的角度来定义风险系统，均可以取得相应的技术效果，在实施时，可以根据实际需要来进行选择。以下实施例中列举的风险系数也可以从正相关和负相关两种角度来进行定义，在下文中不再一一赘述。
10

又例如，针对证件齐全度，可以根据用户 A 的上传的证件的齐全度确定风险系数，具体地，如上传的证件的齐全度为 55%，则确定上传的证件合格的可能性为 55%，根据
15 证件合格的可能性确定风险系数 55%。需要说明的是，证件的齐全度可以通过上传证件的数量和类型与要求上传证件的数量和类型进行计算得到。

又例如，针对证件有效性，可以根据用户 A 的上传的证件的有效性确定风险系数，具体地，如上传的证件的有效性为 68%，则确定上传的证件合格的可能性为 68%，根据
20 证件合格的可能性确定风险系数为 68%。需要说明的是，证件的有效性可以根据识别上传的证件中的信息判断是否符合预设要求得到。

生物信息也是比较重要的信息，在对用户进行评估的时候也可以参考使用，例如，在信息的类型为生物特征信息的情况下，可以根据如下条件的至少之一确定生物特征信息对应的风险系数：来自用户的人像图片是否与用户相符、来自用户的声纹信息是否与
25 用户相符、来自用户的指纹信息是否与用户相符等。

再以用户 A 为例，根据来自用户 A 的人像图片是否与用户相符确定风险系数。可以根据判断来自用户 A 的人像图片是否与用户 A 相符（也即来自用户 A 的人像图片是否是用户 A 本人），确定上传的生物特征信息合格的可能性，根据生物特征信息合格的可能性确定风险系数。

又例如，针对声纹信息，可以根据来自用户 A 的声纹信息确定风险系数。具体地，
30 根据判断来自用户 A 的声纹信息是否与用户 A 相符（也即来自用户 A 的声纹信息是否

来自用户 A 本人），确定上传的生物特征信息合格的可能性，根据生物特征信息合格的可能性确定风险系数。

又例如，针对指纹信息，可以根据来自用户 A 的指纹信息是否与用户相符确定风险系数。具体地，根据判断来自用户的指纹信息是否与用户 A 相符（也即来自用户 A 的指纹信息是否来自用户 A 本人），确定上传的生物特征信息合格的可能性，根据生物特征信息合格的可能性确定风险系数。

权限信息可以包括类似于黑名单或者白名单，权限信息在某种程度上标识该用户已经被认为是安全或者安全的，因此，在评估时也可以使用。即在信息的类型为权限信息的情况下，可以根据如下条件的至少之一确定权限信息对应的风险系数：用户是否被限制预定权力、用户是否被允许预定权力；

再以用户 A 为例，可以根据用户 A 是否被限制预定权力确定风险系数。如果判断用户 A 未被限制预定权力，风险系数较大；如果判断用户 A 被限制预定权力，风险系数较小。

又例如，可以根据用户 A 是否被允许预定权力确定风险系数。如果判断用户 A 未被允许预定权力，风险系数较小；如果判断用户 A 被允许预定权力，风险系数较大。

随着大数据技术的发展，用户行为的获取成为可能，而用户的行为也可以作为对该用户进行评估的一种参考，例如，在信息的类型为用户在互联网上的行为信息的情况下，可以根据如下条件的至少之一确定行为信息对应风险系数：用户访问的网站信息、用户的网络地址信息、用户的操作行为。

再以用户 A 为例，可以根据用户 A 访问的网站信息确定风险系数。如果用户 A 未访问过非法网站或者访问过的网站存在风险，风险系数较大；如果用户 A 访问过非法网站或者未访问过的网站存在风险，风险系数较小。

又例如，还可以根据用户 A 的网络地址信息确定风险系数。如果用户 A 的网络地址信息未被标注过存在风险等等，风险系数较大；如果用户 A 的网络地址信息被标注过存在风险等等，风险系数较小。

又例如，还可以根据用户的操作行为确定风险系数。如果用户在互联网上的操作行为不存在风险，风险系数较大；如果用户在互联网上的操作行为存在风险，风险系数较小。

步骤 S206，对每种类型的信息对应的风险系数进行综合评估得到综合风险系数。

可以根据上述得到的每种类型的信息对应的风险系数进行综合评估得到综合风险系

数。

再以用户 A 为例，用户 A 在互联网中上传了身份证、户口本、护照等材料，如果身份证中的身份有效期已过期，在互联网中基于身份证对用户 A 进行身份认证时，导致身份证认证失败，不能通过身份认证。通过本发明中的技术方案，将身份证、户口本、护照等材料综合进行考虑，根据各个材料中的信息评估用户 A 的身份被信任的程度，最后进行评估得到综合风险系数。也即，如果身份证中的身份有效期已过期，在互联网中对用户 A 进行身份认证时，身份证认证不一定失败，通过对户口本、护照等材料对用户 A 进行身份认证，进行综合评估用户 A 的身份被信任的程度（将采集到的用户 A 的用于进行身份认证的信息对应的风险系数进行关联，得到综合风险系数），最后确定用户 A 的身份认证是否通过。通过本技术方案也提升了对身份认证的通过率，用户不必重复进行身份认证，从而提升用户体验。

又例如，用户不仅仅上传了一系列的证件照，还发现该用户在某知名网站是实名认证的客户，该用户被实名网站认证是作为该用户在互联网上的行为信息中的一种，通过证件照以及用户在互联网上的行为信息可以得到该用户的综合风险系统，用于对该用户进行判断。

下面结合一个例子进行说明

用户 A 用于认证的信息有三种：

第一种，证件信息：上传的证件的清晰度为 80%，对应的风险系数为 80%（表明该用户被信任的概率为 80%）；上传证件的齐全度为 55%，对应的风险系数为 55%（表明该用户被信任的概率为 55%）。预先配置的上传证件的清晰度的权值为 0.9，上传证件齐全度的权值为 0.1，此时，证件信息对应的风险系数为 $0.8*0.9+0.55*0.1=0.72+0.055=0.772$ 。

第二种，生物信息：验证了用户的指纹，并且验证通过，对应的风险系数为 100%（表明该用户被信任的概率为 100%）。

第三种，用户的互联网上行为信息：获取该用户的互联网行为信息发现该用户在 A 网站为实名认证用户，A 网站信息的被接受程度为 70%，则对应的风险系数为 70%（表明该用户被信任的概率为 70%）。

可以根据预先配置的权值来综合评估证件信息、生物信息和互联网上的行为信息，证件信息的权值为 0.4，生物信息的权值为 0.4，互联网上的行为信息的权值为 0.2，此时综合风险系数为： $0.772*0.4+1*0.4+0.7*0.2=0.3088+0.4+0.14=0.8488$ 。

在这个例子中，风险系数越高表明该用户被信任的程度越高。

步骤 S208, 根据综合风险系数判断用户的身份认证是否通过。

通过综合风险系数判断用户的身份认证是否通过, 避免了相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大, 影响用户体验的问题。

5 基于上述实施例中步骤 S202 至步骤 S208 所公开的方案, 可以获知采集待身份认证用户的多种类型的信息, 其中, 多种类型的信息用于对用户的身份进行认证; 获取多种类型的信息中的每种类型的信息对应的风险系数, 其中, 风险系数用于指示用户的身份被信任的程度; 对每种类型的信息对应的风险系数进行综合评估得到综合风险系数; 根据综合风险系数判断用户的身份认证是否通过, 从而将每种类型的信息对应的风险系数
10 进行关联, 避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大, 达到了提升对用户的身份认证准确性的目的, 从而实现了提升用户体验的技术效果, 进而解决了由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大, 影响用户体验的技术问题。

15 图 3 示出了在上述步骤 S206 所公开的技术方案中, 对每种类型的信息对应的风险系数进行综合评估得到综合风险系数的流程图。如图 3 所示, 该方法具体中还包括如下步骤:

 步骤 S302, 将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数, 其中, 数据模型是根据训练集进行训练得到的, 训练集包括身份认证通过的用户
20 和/或身份认证未通过的用户对应的综合风险系数, 身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

 本发明实施例中提及的数据模型是根据训练集进行训练得到的, 训练集包括身份认证通过的用户对应的综合风险系数, 身份认证通过的用户对应的综合风险系数是根据该
25 用户的每种类型的信息对应的风险系数得到的。例如, 训练集中包括, 用户 B1、用户 B2、用户 B3……用户 Bn 为身份认证通过的用户, 此时可以根据这些用户的综合风险系数来确定哪些用户是可以被认证通过的。

 为了是训练集更加准确, 在一个可选的实施方式中, 训练集还可以包括训练集包括身份未认证通过的用户对应的综合风险系数, 身份未认证通过的用户对应的综合风险系
30 数是根据该用户的每种类型的信息对应的风险系数得到的。例如, 用户 C1、用户 C2、

用户 C3……用户 Cn 为身份认证未通过的用户，根据训练集进行训练得到数据模型。将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数。例如，根据用户 A 的证件信息对应的风险系数和/或生物特征信息对应的风险系数和/或权限信息对应的风险系数通过数据模型进行评估得到综合风险系数。

- 5 通过本方案，将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数。也即，将每种类型的信息对应的风险系数进行关联，避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大，达到了提升对用户的身份认证的通过率和准确性的目的，从而实现了提升用户体验的技术效果。

10 图 4 示出了在上述步骤 S206 所公开的技术方案中，对每种类型的信息对应的风险系数进行综合评估得到综合风险系数的流程图。如图 4 所示，该方法具体包括如下步骤：

 步骤 S402，根据每种类型的信息对应的风险系数以及权值对所有类型的信息对应的风险系数进行加权和计算，得到综合风险系数，其中，每种类型的信息对应的权值可以表示该种类型的信息对综合风险系数的影响，一个可选的实施方式中，每种类型的信息对应的权值为预先配置的。

- 15 在本发明实施例中，对用户进行身份认证的每种类型的信息预先设置对应的权值，或者根据对多个用户进行身份认证的各种类型的信息进行训练学习得到风险系数数据模型，通过该风险系数数据模型获取采集到的每种类型的信息对应的权值，然后根据获取到的每种类型的信息对应的权值对所有类型的信息对应的风险系数进行加权和计算，得到综合风险系数。

- 20 例如，用户 A 的证件信息对应的权值为 0.6，生物特征信息对应的权值为 0.25，权限信息对应的权值为 0.15，在获取综合风险系数时，根据证件信息对应的权值、生物特征信息对应的权值、权限信息对应的权值对各类型的信息对应的风险系数进行加权求和得到用户 A 通过身份认证的综合风险系数。

- 25 通过本方案，充分考虑了不同类型的信息对用户身份认证的重要程度和影响程度，通过不同类型的信息对应的权值对各类型的信息对应的风险系数进行加权求和，得到综合风险系数。进一步地平衡了用户通过身份认证的风险和提升了用户的体验。

 图 5 示出了在上述步骤 S204 所公开的技术方案中，获取多种类型的信息中的每种类型的信息对应的风险系数的流程图。如图 5 所示，该方法具体包括如下步骤：

- 30 步骤 S502，获取每种类型的子类型对应的风险系数，其中，子类型对应的风险系数包括以下至少之一：每个子类型分别对应的风险系数、至少两个子类型的组合对应的风

险系数。

例如，信息的类型为证件信息，该类型的子类型为证件上的号码、图片、有效期等等。如，证件上的号码对应的风险系数为 2，证件上的图片对应的风险系数为 3，证件上的有效期对应的风险系数为 1 等等，或者，证件上的号码与图片的组合对应的风险系数为 3.5，证件上的号码与有效期的组合对应的风险系数为 2.5 等等。

步骤 S504，根据子类型对应的风险系数获取该类型信息的风险系数。

例如，信息的类型为证件信息，该类型的子类型为证件上的号码、图片、有效期等等。如，证件上的号码对应的风险系数为 2，证件上的图片对应的风险系数为 3，证件上的有效期对应的风险系数为 1，则根据子类型对应的风险系数获取该类型信息的风险系数为 6。

通过本方案，根据不同类型的信息的子类型的风险系数，确定每种类型的信息对应的风险系数，提升了获取每种类型的信息对应的风险系数的准确性。进一步地平衡了用户通过身份认证的风险和提升了用户的体验。

图 6 是根据本发明实施例的一种可选的身份认证方法的示意图，如图 6 所示，通过用户上传的证件、本人生物特征、在互联网上用户轨迹和在互联网上用户访问行为等信息对用户进行身份认证，如果用户的身份认证通过，对用户进行授权。例如，根据上传证件的清晰度、证件的齐全度和证件完整有效性等信息，判断证件是否合格，如果证件不合格，则不符合要求，用户的身份认证失败，也即不能通过身份验证，进一步地互联网拒绝授权给用户。判断上传的本人生物特征中的人像照和/或声纹和/或其他生物特征清晰度等等是否合格，如果不合格，则不符合要求，用户的身份认证失败，也即不能通过身份验证，进一步地互联网拒绝授权给用户。判断在互联网上用户命中黑名单、注册垃圾账号是否存在风险，如果存在风险，则不符合要求，用户的身份认证失败，也即不能通过身份验证，进一步地互联网拒绝授权给用户等等，最后根据采集到的用户所有类型的信息进行判断用户身份认证是否通过，是否对其进行授权。

图 7 是根据本发明实施例的一种可选的身份认证方法的示意图，如图 7 所示，通过用户上传的证件、本人生物特征、在互联网上用户轨迹和在互联网上用户访问行为等信息对用户进行身份认证，如果用户的身份认证通过，对用户进行授权。例如，根据上传证件的清晰度、证件的齐全度和证件完整有效性、本人生物特征中的人像照/声纹/其它生物特征清晰度，在互联网上用户存在风险操作等信息进行联合，得到多维度特征融合模型，根据多维度特征融合模型判断用于对用户身份进行认证的所有类型的信息是否满

足身份认证通过条件，如果满足身份认证通过条件，授权给用户；如果不满足身份认证通过条件，拒绝授权。

通过以上本方案，扩充了对用户进行身份认证的维度，从而在覆盖更多的风险的同时改善正常用户身份认证体验。

5 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于可选实施例，所涉及的动作和模块并不一定是本发明所必须的。

10 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献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（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可
15 以是手机，计算机，服务器，或者网络设备等）执行本发明各个实施例的方法。

实施例 2

根据本发明实施例，还提供了一种用于实施上述身份认证装置，如图 8 所示，该装置包括：采集单元 100、第一获取单元 102、第二获取单元 104 和判断单元 106。

采集单元 100，用于采集待身份认证用户的多种类型的信息，其中，多种类型的信息
20 用于对用户的身份进行认证。

在很多场景下需要在互联网上对用户进行身份认证。为了对待身份认证用户进行身份认证，采集单元 100 采集对该用户的身份进行身份认证的多种类型的信息。

例如，用户 A（待身份认证用户）为了在某网站上为自己开设一实名账户，因此需要在互联网上进行身份认证，待身份认证通过之后，某网站才会对用户 A 进行授权，为其开设实名账户。通常，用户 A 为了在互联网上进行身份认证，可能会上传一些用户 A 的相关材料。对于互联网端，为了对用户 A 的身份进行认证，在上传了一些用户 A 的相关材料的情况下，采集用户 A 上传的相关材料中的信息，该信息中包括对用户 A 的进行身份认证的信息。同时也在互联网中采集可对用户 A 的进行身份认证的信息。如果未上传一些用户 A 的相关材料，则在互联网中采集可对用户 A 的进行身份认证的信息。

30 可选地，在本发明实施例提供的身份认证装置中，用户的信息的类型包括以下至少

之一：证件信息、生物特征信息、权限信息、用户在互联网上的行为信息。

再以用户 A 为例，上传的相关材料中包括以下至少之一：用户 A 的证件、用户 A 的生物特征，采集用户 A 上传的相关材料中的信息，该信息中包括上传的证件中的证件信息，上传的用户 A 的生物特征中的生物特征信息。

5 采集用户 A 在互联网中的权限信息，例如，判断在互联网中用户 A 是否在互联网黑名单中，如果用户 A 在黑名单中，那么用户 A 的在互联网中的权利会被限制。

用户 A 在互联网上的行为信息可以为用户 A 在互联网上的访问轨迹，例如，根据用户 A 在互联网上的访问轨迹可以确定用户 A 在互联网上的操作是否存在风险。

10 第一获取单元 102，用于获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度。

由于用户的信息的类型包括以下至少之一：证件信息、生物特征信息、权限信息、用户在互联网上的行为信息。

可选地，在本发明实施例提供的身份认证装置中，第一获取单元 102 包括以下至少之一：第一确定模块 1021、第二确定模块 1022、第三确定模块 1023 和第四确定模块 1024。

15 第一确定模块 1021，用于在信息的类型为证件信息的情况下，根据如下条件的至少之一确定证件信息对应的风险系数：证件清晰度、证件齐全度、证件有效性。

需要说明的是，风险系数可以为系数值，也可以为概率。以用户 A 为例，第一确定模块 1021 根据用户 A 的上传的证件的清晰度确定风险系数。具体地，如上传的证件的清晰度为 80%，则确定上传的证件合格的可能性为 80%，根据证件合格的可能性确定风
20 险系数为 80%。需要说明的是，证件的清晰度可以根据对证件中的信息进行成功识别的可能性得到。

和/或，第一确定模块 1021 根据用户 A 的上传的证件的齐全度确定风险系数，具体地，如上传的证件的齐全度为 55%，则确定上传的证件合格的可能性为 55%，根据证件合格的可能性确定风险系数 55%。需要说明的是，证件的齐全度可以通过上传证件的数量和类型与要求上传证件的数量和类型进行计算得到。
25

和/或，第一确定模块 1021 根据用户 A 的上传的证件的有效性确定风险系数，具体地，如上传的证件的有效性为 68%，则确定上传的证件合格的可能性为 68%，根据证件合格的可能性确定风险系数 68%。需要说明的是，证件的有效性可以根据识别上传的证件中的信息判断是否符合预设要求得到。

30 第二确定模块 1022，用于在信息的类型为生物特征信息的情况下，根据如下条件的

至少之一确定生物特征信息对应的风险系数：来自用户的人像图片是否与用户相符、来自用户的声纹信息是否与用户相符、来自用户的指纹信息是否与用户相符。

再以用户 A 为例，第二确定模块 1022 根据来自用户 A 的人像图片是否与用户相符确定风险系数。具体地，根据判断来自用户 A 的人像图片是否与用户 A 相符（也即来自用户 A 的人像图片是否是用户 A 本人），确定上传的生物特征信息合格的可能性，根据生物特征信息合格的可能性确定风险系数。

和/或，第二确定模块 1022 根据来自用户 A 的声纹信息确定风险系数。具体地，根据判断来自用户 A 的声纹信息是否与用户 A 相符（也即来自用户 A 的声纹信息是否来自用户 A 本人），确定上传的生物特征信息合格的可能性，根据生物特征信息合格的可能性确定风险系数。

和/或，第二确定模块 1022 根据来自用户 A 的指纹信息是否与用户相符确定风险系数。具体地，根据判断来自用户的指纹信息是否与用户 A 相符（也即来自用户 A 的指纹信息是否来自用户 A 本人），确定上传的生物特征信息合格的可能性，根据生物特征信息合格的可能性确定风险系数。

第三确定模块 1023，用于在信息的类型为权限信息的情况下，根据如下条件的至少之一确定权限信息对应的风险系数：用户是否被限制预定权力、用户是否被允许预定权力。

再以用户 A 为例，第三确定模块 1023 根据用户 A 是否被限制预定权力确定风险系数。如果判断用户 A 被限制预定权力，风险系数较大；如果判断用户 A 未被限制预定权力，风险系数较小。

和/或，第三确定模块 1023 根据用户 A 是否被允许预定权力确定风险系数。如果判断用户 A 被允许预定权力，风险系数较小；如果判断用户 A 未被允许预定权力，风险系数较大。

第四确定模块 1024，用于在信息的类型为用户在互联网上的行为信息的情况下，根据如下条件的至少之一确定行为信息对应风险系数：用户访问的网站信息、用户的网络地址信息、用户的操作行为。

再以用户 A 为例，第四确定模块 1024 根据用户 A 访问的网站信息确定风险系数。如果用户 A 访问过非法网站或者访问过的网站存在风险，风险系数较大；如果用户 A 未访问过非法网站或者未访问过的网站存在风险，风险系数较小。

和/或，第四确定模块 1024 根据用户 A 的网络地址信息确定风险系数。如果用户 A

的网络地址信息被标注过存在风险等等，风险系数较大；如果用户 A 的网络地址信息未被标注过存在风险等等，风险系数较小。

和/或，第四确定模块 1024 根据用户的操作行为确定风险系数。如果用户在互联网上的操作行为存在风险，风险系数较大；如果用户在互联网上的操作行为不存在风险，

5 风险系数较小。

第二获取单元 104，用于对每种类型的信息对应的风险系数进行综合评估得到综合风险系数。

第二获取单元 104 根据上述得到的每种类型的信息对应的风险系数进行综合评估得到综合风险系数。

10 判断单元 106，用于根据综合风险系数判断用户的身份认证是否通过。

判断单元 106 通过综合风险系数判断用户的身份认证是否通过，避免了相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大，影响用户体验的问题。

再以用户 A 为例，用户 A 在互联网中上传了身份证、户口本、护照等等材料，如果
15 身份证中的身份有效期已过期，在互联网中基于身份证对用户 A 进行身份认证时，导致身份证认证失败，不能通过身份认证。通过本发明实施例中的技术方案，将身份证、户口本、护照等等材料综合进行考虑，根据各个材料中的信息评估用户 A 的身份被信任的程度，最后进行评估得到综合风险系数，根据综合风险系数判断用户 A 的身份认证是否通过。也即，如果身份证中的身份有效期已过期，在互联网中对用户 A 进行身份认证时，
20 身份证认证不一定失败，通过对户口本、护照等等材料对用户 A 进行身份认证，进行综合评估用户 A 的身份被信任的程度（将采集到的用户 A 的用于进行身份认证的信息对应的风险系数进行关联，得到综合风险系数），最后确定用户 A 的身份认证是否通过。通过本技术方案也提升了对身份认证的通过率，用户不必重复进行身份认证，从而提升用户体验。

25 基于上述实施例中采集单元 100、第一获取单元 102、第二获取单元 104 和判断单元 106 所公开的方案，可以获知采集单元 100 采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；第一获取单元 102 获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度；第二获取单元 104 对每种类型的信息对应的风险系数进行综合评估得到综合风险
30 系数；判断单元 106 根据综合风险系数判断用户的身份认证是否通过，从而将每种类型

的信息对应的风险系数进行关联，避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大，达到了提升对用户的身份认证准确性的目的，从而实现了提升用户体验的技术效果，进而解决了由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大，影响用户体验的技术问题。

此处需要说明的是，上述采集单元 100、第一获取单元 102、第二获取单元 104 和判断单元 106 对应于实施例 1 中的步骤 S202 至步骤 S208，四个单元与对应的步骤所实现的实例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端 10 中。

可选地，在本发明实施例提供的身份认证装置中，第二获取单元 104 还用于将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数，其中，数据模型是根据训练集进行训练得到的，训练集包括身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数，身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

本发明实施例中提及的数据模型是根据训练集进行训练得到的，训练集包括身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数，身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。例如，训练集中包括，用户 B1、用户 B2、用户 B3……用户 Bn 为身份认证通过的用户，用户 C1、用户 C2、用户 C3……用户 Cn 为身份认证未通过的用户，根据训练集进行训练得到数据模型。将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数。例如，根据用户 A 的证件信息对应的风险系数和/或生物特征信息对应的风险系数和/或权限信息对应的风险系数通过数据模型进行评估得到综合风险系数。

通过本方案，将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数。也即，将每种类型的信息对应的风险系数进行关联，避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大，达到了提升对用户的身份认证的通过率和准确性的目的，从而实现了提升用户体验的技术效果。

此处需要说明的是，上述代码第二获取单元 104 对应于实施例 1 中的步骤 S206，三个模块与对应的步骤所实现的实例和应用场景相同，但不限于上述实施例一所公开的内容。需要说明的是，上述模块作为装置的一部分可以运行在实施例一提供的计算机终端

10 中。

可选地，在本发明实施例提供的身份认证装置中，第二获取单元 104 还用于根据每种类型的信息对应的风险系数以及权值对所有类型的信息对应的风险系数进行加权和计算，得到综合风险系数。

5 在本发明实施例中，对用户进行身份认证的每种类型的信息预先设置对应的权值，或者第二获取单元 104 根据对多个用户进行身份认证的各种类型的信息进行训练学习得到风险系数数据模型，通过该风险系数数据模型获取采集到的每种类型的信息对应的权值，然后根据获取到的每种类型的信息对应的权值对所有类型的信息对应的风险系数进行加权和计算，得到综合风险系数。

10 例如，用户 A 的证件信息对应的权值为 0.6，生物特征信息对应的权值为 0.25，权限信息对应的权值为 0.15，在获取综合风险系数时，根据证件信息对应的权值、生物特征信息对应的权值、权限信息对应的权值对各类型的信息对应的风险系数进行加权求和得到用户 A 通过身份认证的综合风险系数。

通过本方案，充分考虑了不同类型的信息对用户身份认证的重要程度和影响程度，
15 通过不同类型的信息对应的权值对各类型的信息对应的风险系数进行加权求和，得到综合风险系数。进一步地平衡了用户通过身份认证的风险和提升了用户的体验。

可选地，在本发明实施例提供的身份认证装置中，第一获取单元 102 还包括：第一获取模块，用于获取每种类型的子类型对应的风险系数，其中，子类型对应的风险系数包括以下至少之一：每个子类型分别对应的风险系数、至少两个子类型的组合对应的风
20 险系数；第二获取模块，用于根据子类型对应的风险系数获取该类型信息的风险系数。

通过本方案，根据不同类型的信息的子类型的风险系数，确定每种类型的信息对应的风险系数，提升了获取每种类型的信息对应的风险系数的准确性。进一步地平衡了用户通过身份认证的风险和提升了用户的体验。

需要说明的是，上述单元作为装置的一部分可以运行在实施例一提供的计算机终端
25 10 中。

实施例 3

根据本发明实施例，还提供了一种计算设备，图 9 是根据本发明实施例的一种计算设备的示意图，如图 9 所示，该计算设备 100，提供第一界面 110。

该第一界面 110 包括：多个第一控件 111，用于采集待身份认证用户的多种类型的
30 信息，多种类型的信息用于对用户的身份进行认证；第一发送单元，用于将多种类型的

信息发送至服务器，通过服务器对多种类型的信息的风险系数进行评估，得到综合风险系数，其中，风险系数用于指示用户的身份被信任的程度；第二接收单元，用于接收服务器发送的与多种类型的信息对应的风险系数以及综合风险系数；与多个第一控件对应的多个第二控件 121，用于体现每种类型的信息对应的风险系数；第三控件 122，用于体现待身份认证用户的综合风险系数。

在本方案公开的内容中，如图 9 所示，通过多个第二控件 121 将证件风险系数、指纹风险系数等等多种类型的信息对应的风险系数进行体现，通过多个第三控件 122 将综合风险系数进行体现，用户可以查看到以上信息，进一步地提升用户体验度的技术效果。

在本发明实施例中，采用多种类型的信息对用户进行身份认证的方式，通过多个第一控件 111 采集待身份认证用户的多种类型的信息，多种类型的信息用于对用户的身份进行认证；第一发送单元将多种类型的信息发送至服务器，通过服务器对多种类型的信息的风险系数进行评估，得到综合风险系数，其中，风险系数用于指示用户的身份被信任的程度；第二接收单元，用于接收服务器发送的与多种类型的信息对应的风险系数以及综合风险系数；与多个第一控件对应的多个第二控件 121 体现每种类型的信息对应的风险系数；第三控件 122 体现待身份认证用户的综合风险系数，将每种类型的信息对应的风险系数进行关联，避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大，达到了提升对用户的身份认证准确性的目的，还通过第二控件体现每种类型的信息对应的风险系数，第三控件体现待身份认证用户的综合风险系数，从而用户可以查看到相关信息，进一步提升了用户体验度的技术效果，进而解决了由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大，影响用户体验的技术问题。

实施例 4

本发明的实施例可以提供一种计算机终端，该计算机终端可以是计算机终端群中的任意一个计算机终端设备。可选地，在本实施例中，上述计算机终端也可以替换为移动终端等终端设备。

可选地，在本实施例中，上述计算机终端可以位于计算机网络的多个网络设备中的至少一个网络设备。

在本实施例中，上述计算机终端可以执行应用程序的身份认证方法中以下步骤的程序代码：采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险

系数用于指示用户的身份被信任的程度；对每种类型的信息对应的风险系数进行综合评估得到综合风险系数；根据综合风险系数判断用户的身份认证是否通过。

可选地，图 10 是根据本发明实施例的一种计算机终端的结构框图。如图 10 所示，该计算机终端 10 可以包括：一个或多个（图中仅示出一个）处理器和存储器。

5 其中，存储器可用于存储软件程序以及模块，如本发明实施例中的安全漏洞检测方法和装置对应的程序指令/模块，处理器通过运行存储在存储器内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的系统漏洞攻击的检测方法。存储器可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器可进一步包括相对于处理
10 器远程设置的存储器，这些远程存储器可以通过网络连接至终端 10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

处理器可以通过传输装置调用存储器存储的信息及应用程序，以执行下述步骤：采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指
15 示用户的身份被信任的程度；对每种类型的信息对应的风险系数进行综合评估得到综合风险系数；根据综合风险系数判断用户的身份认证是否通过。

可选的，上述处理器还可以执行如下步骤的程序代码：将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数，其中，数据模型是根据训练集进行训练得到的，训练集包括身份认证通过的用户和/或身份认证未通过的用户对应的综合风险
20 系数，身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

可选的，上述处理器还可以执行如下步骤的程序代码：根据每种类型的信息对应的风险系数以及权值对所有类型的信息对应的风险系数进行加权和计算，得到综合风险系数。

25 可选的，上述处理器还可以执行如下步骤的程序代码：用户的信息的类型包括以下至少之一：证件信息、生物特征信息、权限信息、用户在互联网上的行为信息。

可选的，上述处理器还可以执行如下步骤的程序代码：在信息的类型为证件信息的情况下，根据如下条件的至少之一确定证件信息对应的风险系数：证件清晰度、证件齐全度、证件有效性；在信息的类型为生物特征信息的情况下，根据如下条件的至少之一
30 确定生物特征信息对应的风险系数：来自用户的人像图片是否与用户相符、来自用户的

声纹信息是否与用户相符、来自用户的指纹信息是否与用户相符；在信息的类型为权限信息的情况下，根据如下条件的至少之一确定权限信息对应的风险系数：用户是否被限制预定权力、用户是否被允许预定权力；在信息的类型为用户在互联网上的行为信息的情况下，根据如下条件的至少之一确定行为信息对应风险系数：用户访问的网站信息、

5 用户的网络地址信息、用户的操作行为。

可选的，上述处理器还可以执行如下步骤的程序代码：获取多种类型的信息中的每种类型的信息对应的风险系数包括：获取每种类型的子类型对应的风险系数，其中，子类型对应的风险系数包括以下至少之一：每个子类型分别对应的风险系数、至少两个子类型的组合对应的风险系数；根据子类型对应的风险系数获取该类型信息的风险系数。

10 采用本发明实施例，提供了一种身份认证的方案。通过采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度；对每种类型的信息对应的风险系数进行综合评估得到综合风险系数；根据综合风险系数判断用户的身份认证是否通过，从而将每种类型的信息对应的风险系数进行关联，

15 避免了身份认证之间独立、无任何关联造成的身份认证决策时出错的风险较大，达到了提升对用户的身份认证准确性的目的，从而实现了提升用户体验度的技术效果，进而解决了由于相关技术中根据各个身份认证条件认定用户身份是否通过身份认证之间是相互独立、无任何关联造成的身份认证决策时出错的风险较大，影响用户体验的技术问题。

本领域普通技术人员可以理解，图 10 所示的结构仅为示意，计算机终端也可以是智能手机（如 Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices，MID）、PAD 等终端设备。图 10 其并不对上述电子装置的结构造成限定。例如，计算机终端 10 还可包括比图 10 中所示更多或者更少的组件（如网络接口、显示装置等），或者具有与图 10 所示不同的配置。

20

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通

25 过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（Read-Only Memory，ROM）、随机存取器（Random Access Memory，RAM）、磁盘或光盘等。

实施例 5

本发明的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以

30 用于保存上述实施例一所提供的身份认证方法所执行的程序代码。

可选地，在本实施例中，上述存储介质可以位于计算机网络中计算机终端群中的任意一个计算机终端中，或者位于移动终端群中的任意一个移动终端中。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：采集待身份认证用户的多种类型的信息，其中，多种类型的信息用于对用户的身份进行认证；获取多种类型的信息中的每种类型的信息对应的风险系数，其中，风险系数用于指示用户的身份被信任的程度；对每种类型的信息对应的风险系数进行综合评估得到综合风险系数；根据综合风险系数判断用户的身份认证是否通过。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：将每种类型的信息对应的风险系数通过数据模型进行评估得到综合风险系数，其中，数据模型是根据训练集进行训练得到的，训练集包括身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数，身份认证通过的用户和/或身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：根据每种类型的信息对应的风险系数以及权值对所有类型的信息对应的风险系数进行加权

和计算，得到综合风险系数。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：用户的信息的类型包括以下至少之一：证件信息、生物特征信息、权限信息、用户在互联网上的行为信息。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：在信息的类型为证件信息的情况下，根据如下条件的至少之一确定证件信息对应的风险系数：证件清晰度、证件齐全度、证件有效性；在信息的类型为生物特征信息的情况下，根据如下条件的至少之一确定生物特征信息对应的风险系数：来自用户的人像图片是否与用户相符、来自用户的声纹信息是否与用户相符、来自用户的指纹信息是否与用户相符；在信息的类型为权限信息的情况下，根据如下条件的至少之一确定权限信息对应的风险系数：用户是否被限制预定权力、用户是否被允许预定权力；在信息的类型为用户在互联网上的行为信息的情况下，根据如下条件的至少之一确定行为信息对应风险系数：用户访问的网站信息、用户的网络地址信息、用户的操作行为。

可选地，在本实施例中，存储介质被设置为存储用于执行以下步骤的程序代码：获取多种类型的信息中的每种类型的信息对应的风险系数包括：获取每种类型的子类型对应的风险系数，其中，子类型对应的风险系数包括以下至少之一：每个子类型分别对应

的风险系数、至少两个子类型的组合对应的风险系数；根据子类型对应的风险系数获取该类型信息的风险系数。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没
5 述的部分，可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中，应该理解到，所揭露的技术内容，可通过其它的方式实现。其中，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
10 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，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

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。
15

另外，在本发明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。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元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
20 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，本发明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全部或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（可为个人计算机、服务器或者网络设备等）执行本发明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、只读存储器（ROM，Read-Only Memory）、
25 随机存取存储器（RAM，Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述仅是本发明的可选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权利要求书

1. 一种身份认证方法，其特征在于，包括：

采集待身份认证用户的多种类型的信息，其中，所述多种类型的信息用于对所述用户的身份进行认证；

5 获取所述多种类型的信息中的每种类型的信息对应的风险系数，其中，所述风险系数用于指示所述用户的身份被信任的程度；

对所述每种类型的信息对应的风险系数进行综合评估得到综合风险系数；

根据所述综合风险系数判断所述用户的身份认证是否通过。

2. 根据权利要求 1 所述的方法，其特征在于，对所述每种类型的信息对应的风险系
10 数进行综合评估得到所述综合风险系数包括：

将所述每种类型的信息对应的风险系数通过数据模型进行评估得到所述综合风险系数，其中，所述数据模型是根据训练集进行训练得到的，所述训练集至少包括身份认证通过的用户对应的综合风险系数，所述身份认证通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

15 3. 根据权利要求 2 所述的方法，其特征在于，所述训练集还包括：身份认证未通过的用户对应的综合风险系数，所述身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

4. 根据权利要求 1 所述的方法，其特征在于，对所述每种类型的信息对应的风险系数进行综合评估得到所述综合风险系数包括：

20 根据所述每种类型的信息对应的风险系数以及权值对所有类型的信息对应的风险系数进行加权和计算，得到所述综合风险系数，其中，所述每种类型的信息对应的权值用于表示该种类型的信息对综合风险系数的影响，所述每种类型的信息对应的权值为预先配置的。

5. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，所述用户的信息的类型
25 包括以下至少之一：证件信息、生物特征信息、权限信息、所述用户在互联网上的行为信息。

6. 根据权利要求 5 所述的方法，其特征在于，获取所述多种类型的信息中的每种类型的信息对应的风险系数包括以下至少之一：

在所述信息的类型为证件信息的情况下，根据如下条件的至少之一确定所述证件信息
30 对应的风险系数：证件清晰度、证件齐全度、证件有效性；

在所述信息的类型为生物特征信息的情况下，根据如下条件的至少之一确定所述生物特征信息对应的风险系数：来自所述用户的人像图片是否与所述用户相符、来自所述用户的声纹信息是否与所述用户相符、来自所述用户的指纹信息是否与所述用户相符；

在所述信息的类型为权限信息的情况下，根据如下条件的至少之一确定所述权限信息对应的风险系数：所述用户是否被限制预定权力、所述用户是否被允许预定权力；

在所述信息的类型为所述用户在互联网上的行为信息的情况下，根据如下条件的至少之一确定所述行为信息对应风险系数：所述用户访问的网站信息、所述用户的网络地址信息、所述用户的操作行为。

7. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，获取所述多种类型的信息中的每种类型的信息对应的风险系数包括：

获取所述每种类型的子类型对应的风险系数，其中，所述子类型对应的风险系数包括以下至少之一：每个子类型分别对应的风险系数、至少两个子类型的组合对应的风险系数；

根据所述子类型对应的风险系数获取该类型信息的风险系数。

8. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，

所述风险系数数值越大，所述用户的身份被信任的程度越高，所述用户的身份被认证通过之后风险越低；或者，

所述风险系数数值越大，所述用户的身份被信任的程度越低，所述用户的身份被认证通过之后风险越高。

9. 一种身份认证装置，其特征在于，包括：

采集单元，用于采集待身份认证用户的多种类型的信息，其中，所述多种类型的信息用于对所述用户的身份进行认证；

第一获取单元，用于获取所述多种类型的信息中的每种类型的信息对应的风险系数，其中，所述风险系数用于指示所述用户的身份被信任的程度；

第二获取单元，用于对所述每种类型的信息对应的风险系数进行综合评估得到综合风险系数；

判断单元，用于根据所述综合风险系数判断所述用户的身份认证是否通过。

10. 根据权利要求 9 所述的装置，其特征在于，所述第二获取单元还用于将所述每种类型的信息对应的风险系数通过数据模型进行评估得到所述综合风险系数，其中，所述数据模型是根据训练集进行训练得到的，所述训练集包括身份认证通过的用户对应的

综合风险系数，所述身份认证通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

11. 根据权利要求 10 所述的装置，其特征在于，所述训练集还包括：身份认证未通过的用户对应的综合风险系数，所述身份认证未通过的用户对应的综合风险系数是根据该用户的每种类型的信息对应的风险系数得到的。

12. 根据权利要求 9 所述的装置，其特征在于，所述第二获取单元还用于根据所述每种类型的信息对应的风险系数以及权值对所有类型的信息对应的风险系数进行加权和计算，得到所述综合风险系数，其中，所述每种类型的信息对应的权值用于表示该种类型的信息对综合风险系数的影响，所述每种类型的信息对应的权值为预先配置的。

13. 根据权利要求 9 至 12 中任一项所述的装置，其特征在于，所述用户的信息的类型包括以下至少之一：证件信息、生物特征信息、权限信息、所述用户在互联网上的行为信息。

14. 根据权利要求 13 所述的装置，其特征在于，所述第一获取单元包括以下至少之一：

第一确定模块，用于在所述信息的类型为证件信息的情况下，根据如下条件的至少之一确定所述证件信息对应的风险系数：证件清晰度、证件齐全度、证件有效性；

第二确定模块，用于在所述信息的类型为生物特征信息的情况下，根据如下条件的至少之一确定所述生物特征信息对应的风险系数：来自所述用户的人像图片是否与所述用户相符、来自所述用户的声纹信息是否与所述用户相符、来自所述用户的指纹信息是否与所述用户相符；

第三确定模块，用于在所述信息的类型为权限信息的情况下，根据如下条件的至少之一确定所述权限信息对应的风险系数：所述用户是否被限制预定权力、所述用户是否被允许预定权力；

第四确定模块，用于在所述信息的类型为所述用户在互联网上的行为信息的情况下，根据如下条件的至少之一确定所述行为信息对应风险系数：所述用户访问的网站信息、所述用户的网络地址信息、所述用户的操作行为。

15. 根据权利要求 9 至 12 中任一项所述的装置，其特征在于，所述第一获取单元包括：

第一获取模块，用于获取所述每种类型的子类型对应的风险系数，其中，所述子类型对应的风险系数包括以下至少之一：每个子类型分别对应的风险系数、至少两个子类型

型的组合对应的风险系数；

第二获取模块，用于根据所述子类型对应的风险系数获取该类型信息的风险系数。

16. 一种计算设备，其特征在于，提供第一界面，用于用户交互；

其中，所述第一界面包括：

- 5 多个第一控件，用于采集待身份认证用户的多种类型的信息，所述多种类型的信息用于对所述用户的身份进行认证；

第一发送单元，用于将所述多种类型的信息发送至服务器，通过所述服务器对所述多种类型的信息的风险系数进行评估，得到综合风险系数，其中，所述风险系数用于指示所述用户的身份被信任的程度；

- 10 第二接收单元，用于接收服务器发送的与多种类型的信息对应的风险系数以及综合风险系数；

与所述多个第一控件对应的多个第二控件，用于体现每种类型的信息对应的风险系数；

第三控件，用于体现待身份认证用户的综合风险系数。

15

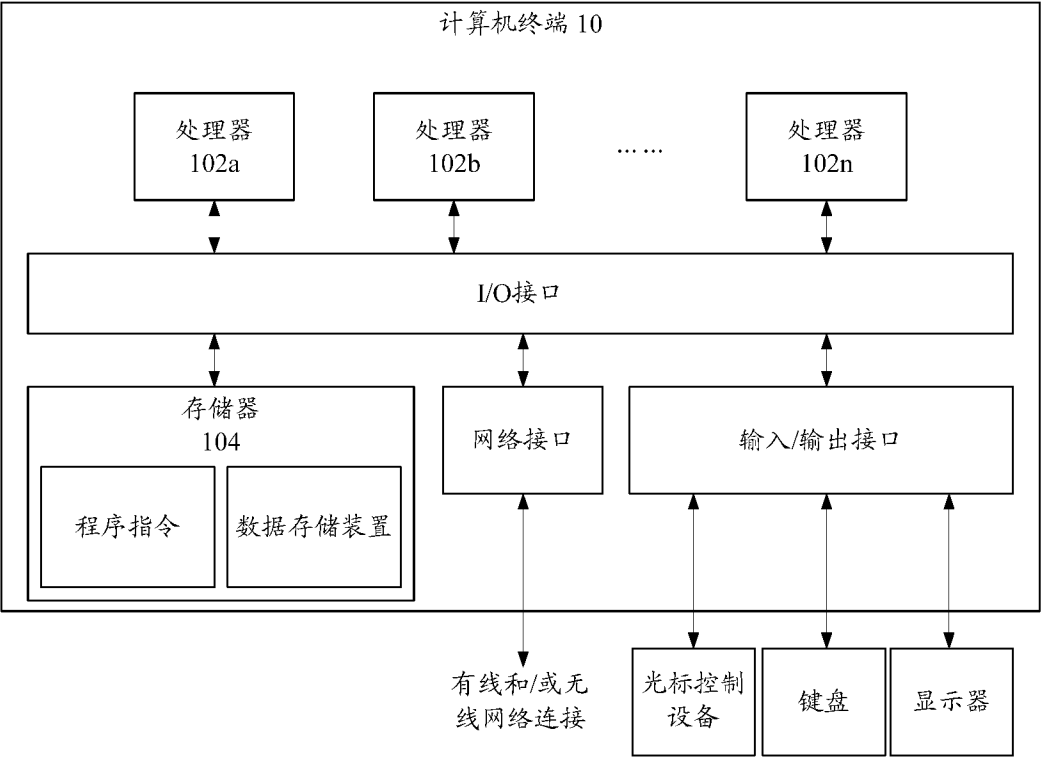


图 1

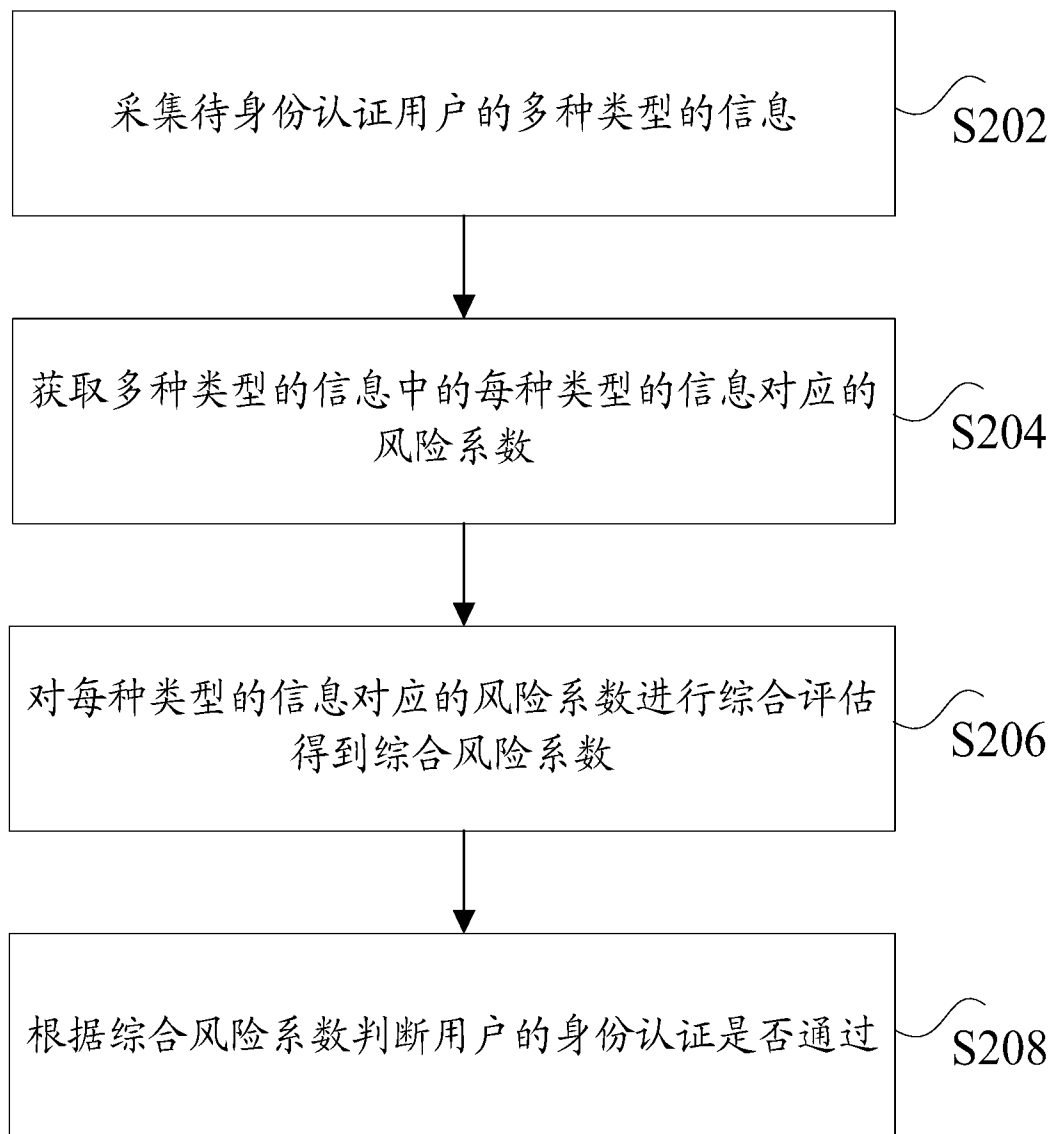


图 2

将每种类型的信息对应的风险系数通过数据模型
进行评估得到综合风险系数

S302

图 3

根据每种类型的信息对应的风险系数以及权值对所
有类型的信息对应的风险系数进行加权和计算，得
到综合风险系数

S402

图 4

获取每种类型的子类型对应的风险系数

S502



根据子类型对应的风险系数获取该类型信息的风
险系数

S504

图 5

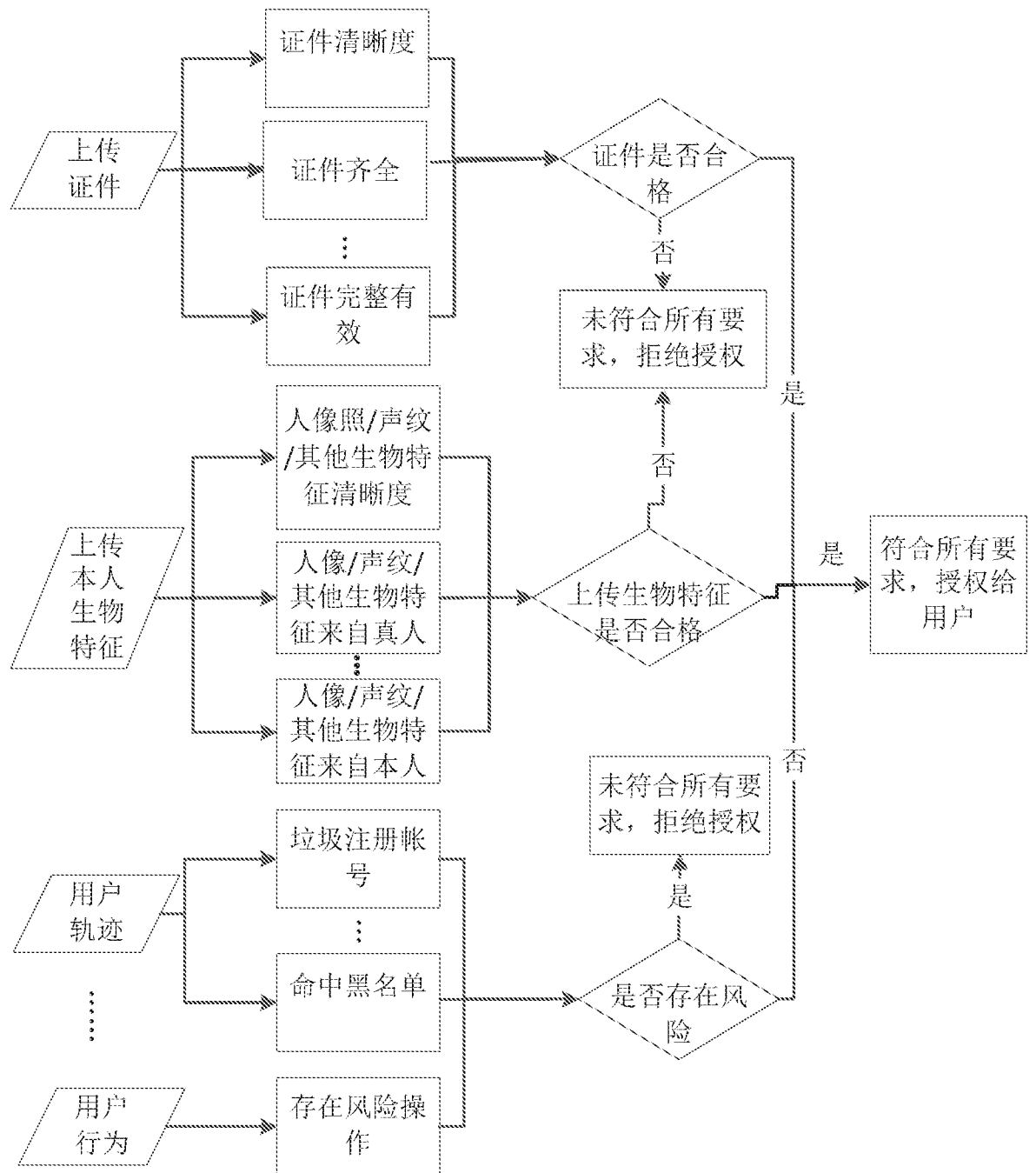


图 6

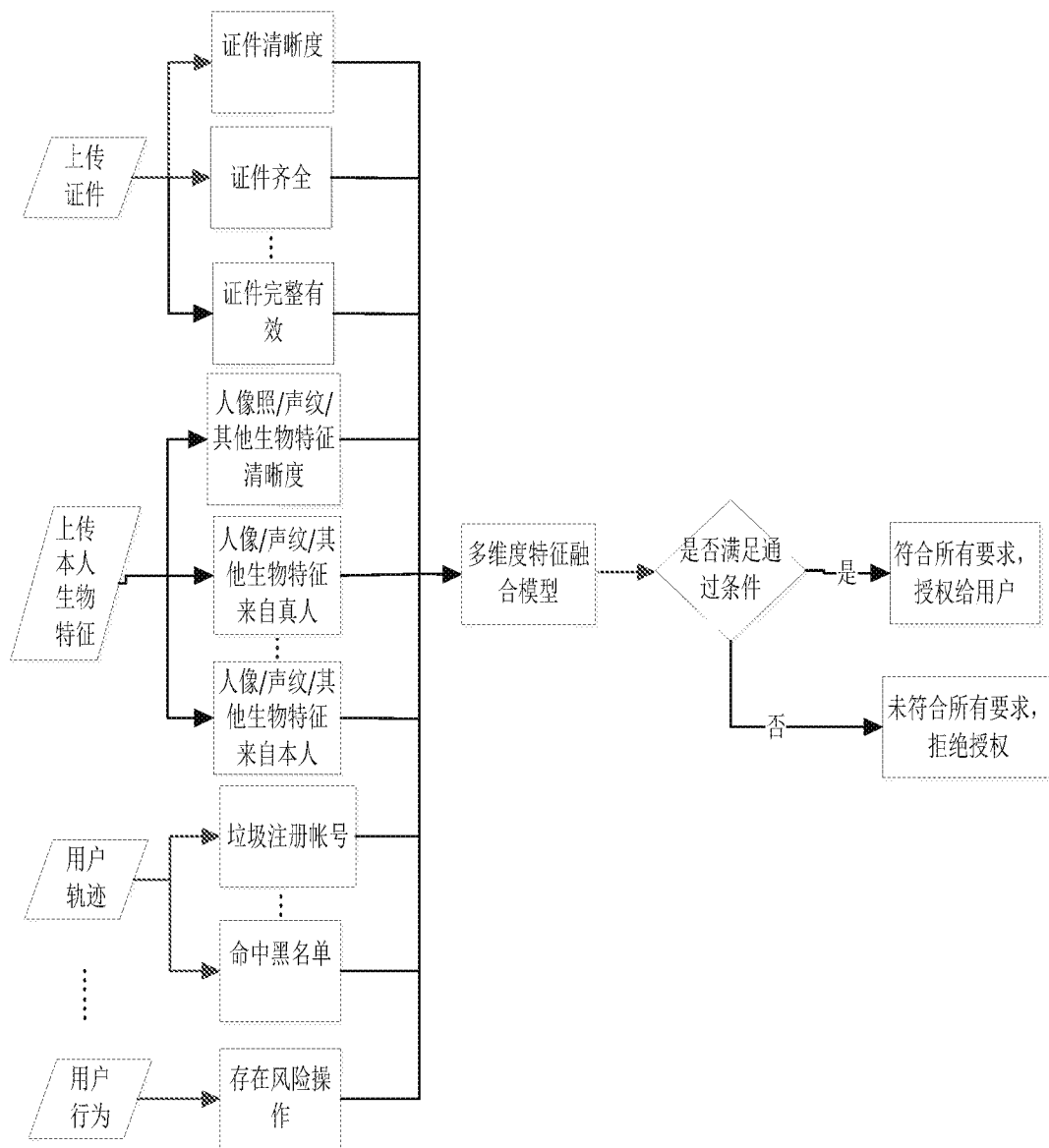


图 7



图 8

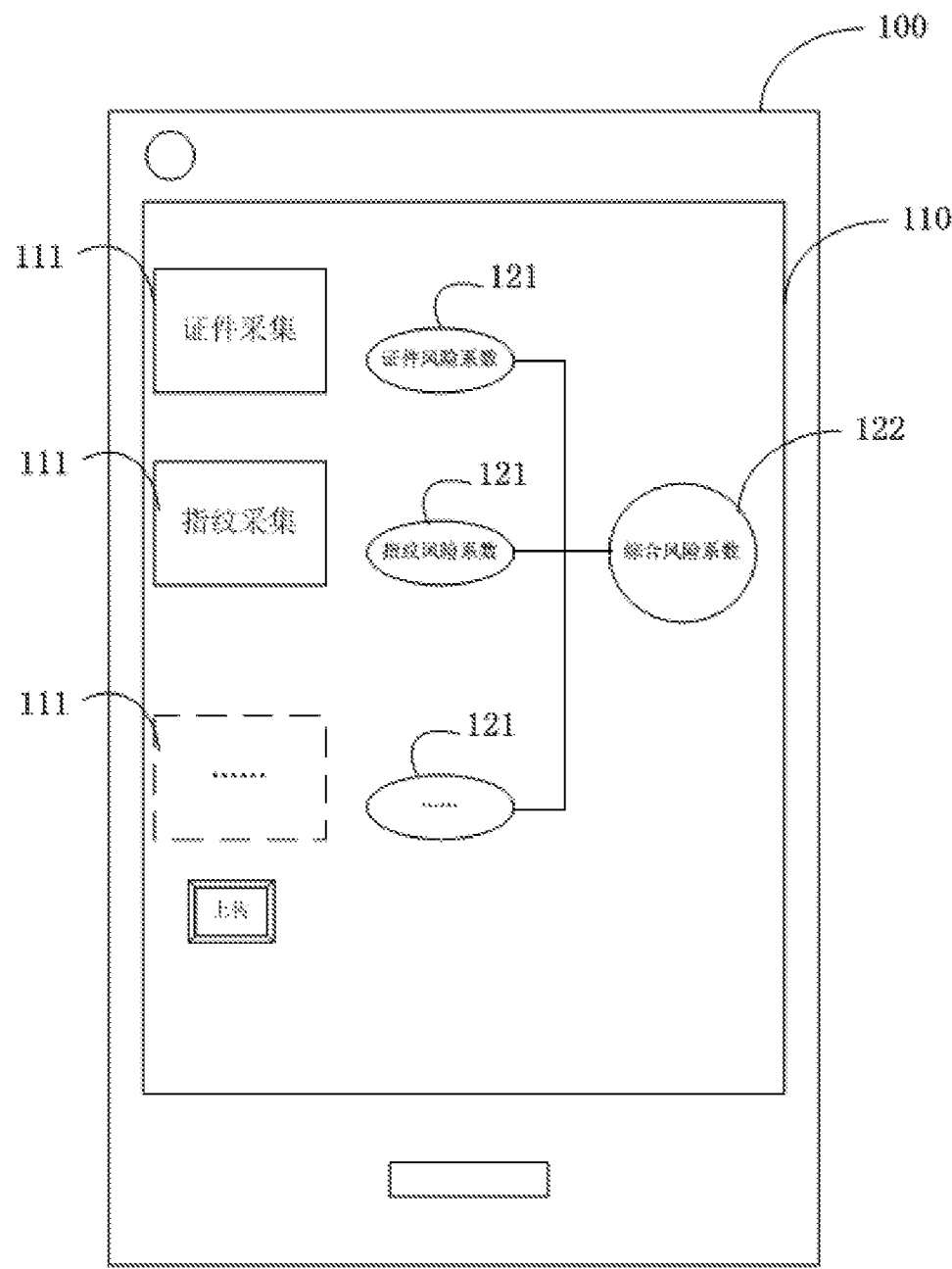


图 9

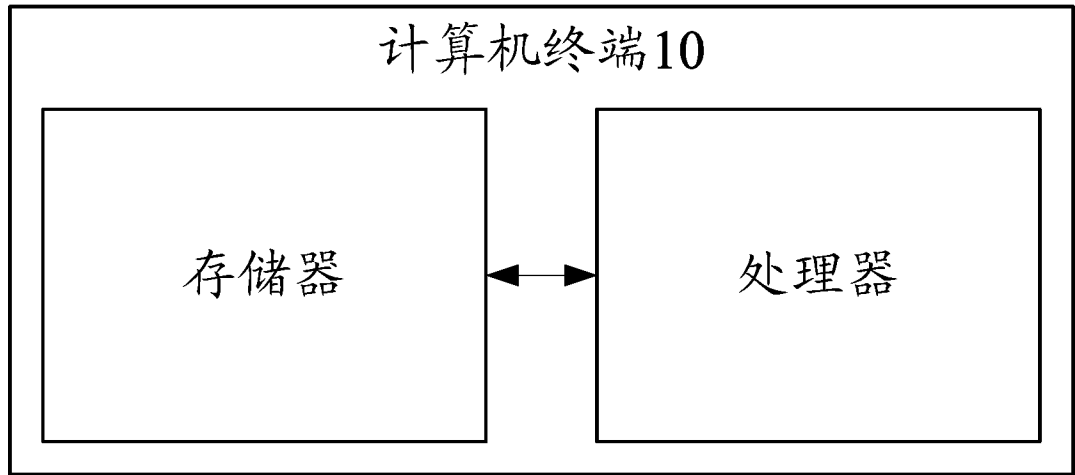


图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/111506

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L; H04W

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)

CPRSABS, CNTXT, CNKI: 身份, 认证, 验证, 鉴别, 确认, 访问, 接入, 使用, 权限, 鉴权, 授权, 防止, 恶意, 攻击, 假冒, 非法, 保证, 安全, 人脸, 面部, 相互, 彼此, 独立, 单独, 关联, 联动, 捆绑, 联合, 复合, 多重, 采集, 收集, 风险系数, 权值, 加权
VEN, EPTXT, GOOGLE: Identity Authentication, Authentication, Access, Rights, Authorize, Prevent, Malicious Attack, Counterfeit, Unlawful, Guarantee, Security, Face, Mutual, Independence, Individual, Association, Linkage, Bundle, Union, Compound, Multiple, Collect, Risk Coefficient, Weight

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102904885 A (BEIJING UNIVERSITY OF TECHNOLOGY) 30 January 2013 (30.01.2013), description, paragraphs [0009], [0010] and [0014]-[0042], and figure 2	1-16
A	CN 103440686 A (SHANGHAI JIAOTONG UNIVERSITY et al.) 11 December 2013 (11.12.2013), entire document	1-16
A	CN 105989263 A (ALIBABA GROUP HOLDING LTD.) 05 October 2016 (05.10.2016), entire document	1-16

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 26 January 2018	Date of mailing of the international search report 09 February 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer TANG, Wensen Telephone No. (86-10) 62411230

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/111506

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105426723 A (BEIJING D-EAR TECHNOLOGIES CO., LTD. et al.) 23 March 2016 (23.03.2016), entire document	1-16
A	CN 105556552 A (GUARDIAN ANALYTICS, INC.) 04 May 2016 (04.05.2016), entire document	1-16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/111506

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102904885 A	30 January 2013	CN 102904885 B	29 April 2015
CN 103440686 A	11 December 2013	None	
CN 105989263 A	05 October 2016	None	
CN 105426723 A	23 March 2016	None	
CN 105556552 A	04 May 2016	EP 2973282 A4	16 November 2016
		CA 2905996 A1	02 October 2014
		WO 2014160296 A1	02 October 2014
		EP 2973282 A1	20 January 2016
		US 2015026027 A1	22 January 2015
		IN 201509462 P1	19 February 2016

国际检索报告

国际申请号

PCT/CN2017/111506

A. 主题的分类 H04L 29/06 (2006.01) 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) H04L; H04W 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)) CPRSABS, CNTXT, CNKI: 身份、认证、验证、鉴别、确认、访问、接入、使用、权限、鉴权、授权、防止、恶意、攻击、假冒、非法、保证、安全、人脸、面部、相互、彼此、独立、单独、关联、联动、捆绑、联合、复合、多重、采集、收集、风险系数、权值、加权 VEN, EPTXT, GOOGLE: Identity Authentication, Authentication, Access, Rights, Authorize, Prevent, Malicious Attack, Counterfeit, Unlawful, Guarantee, Security, Face, Mutual, Independence, Individual, Association, Linkage, Bundle, Union, Compound, Multiple, Collect, Risk Coefficient, Weight		
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 102904885 A (北京工业大学) 2013年 1月 30日 (2013 - 01 - 30) 说明书第[0009]段至第[0010]段、第[0014]段至第[0042]段, 图2	1-16
A	CN 103440686 A (上海交通大学等) 2013年 12月 11日 (2013 - 12 - 11) 全文	1-16
A	CN 105989263 A (阿里巴巴集团控股有限公司) 2016年 10月 5日 (2016 - 10 - 05) 全文	1-16
A	CN 105426723 A (北京得意音通技术有限责任公司等) 2016年 3月 23日 (2016 - 03 - 23) 全文	1-16
A	CN 105556552 A (加迪安分析有限公司) 2016年 5月 4日 (2016 - 05 - 04) 全文 全文	1-16
☐ 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
2018年 1月 26日		2018年 2月 9日
ISA/CN的名称和邮寄地址		受权官员
中华人民共和国国家知识产权局 (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		唐文森 电话号码 (86-10) 62411230

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/111506

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	102904885	A	2013年 1月 30日	CN	102904885	B	2015年 4月 29日
CN	103440686	A	2013年 12月 11日	无			
CN	105989263	A	2016年 10月 5日	无			
CN	105426723	A	2016年 3月 23日	无			
CN	105556552	A	2016年 5月 4日	EP	2973282	A4	2016年 11月 16日
				CA	2905996	A1	2014年 10月 2日
				WO	2014160296	A1	2014年 10月 2日
				EP	2973282	A1	2016年 1月 20日
				US	2015026027	A1	2015年 1月 22日
					IN201509462	P1	2016年 2月 19日