

(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 5 月 24 日 (24.05.2018)



(10) 国际公布号
WO 2018/090839 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2017/109215
- (22) 国际申请日: 2017 年 11 月 3 日 (03.11.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201611010182.6 2016 年 11 月 16 日 (16.11.2016) 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: 王珊珊(WANG, Shanshan); 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)。陆琴(LU, Qin); 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)。

叶鹏(YE, Peng); 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)。林晶晶(LIN, Jingjing); 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)。余莲斌(YU, Lianbin); 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)。王盛(WANG, Sheng); 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)。朱凯(ZHU, Kai); 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)。薛晖(XUE, Hui); 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)。李东(LI, Dong); 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)。

(54) Title: IDENTITY VERIFICATION SYSTEM, METHOD, DEVICE, AND ACCOUNT VERIFICATION METHOD

(54) 发明名称: 身份认证系统、方法、装置及账号认证方法

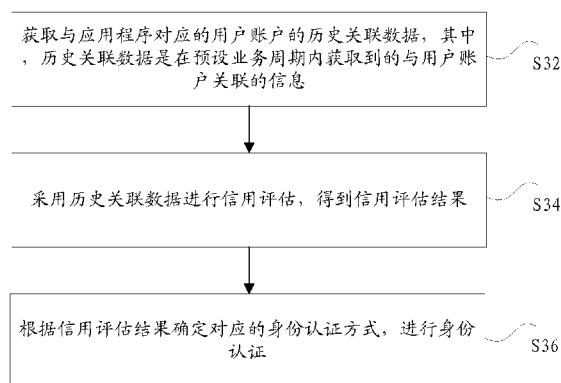


图 3

- S32 OBTAIN HISTORICAL ASSOCIATION DATA OF A USER ACCOUNT CORRESPONDING TO AN APPLICATION, WHEREIN THE HISTORICAL ASSOCIATION DATA COMPRISES INFORMATION ASSOCIATED WITH THE USER ACCOUNT AND OBTAINED IN A PRECONFIGURED SERVICE PERIOD
- S34 ADOPT THE HISTORICAL ASSOCIATION DATA TO PERFORM AN EVALUATION TO OBTAIN AN EVALUATION RESULT
- S36 DETERMINE, ACCORDING TO THE EVALUATION RESULT, AN IDENTITY VERIFICATION METHOD TO PERFORM IDENTITY VERIFICATION

(57) Abstract: The invention discloses an identity verification system, a method, a device, and an account verification method. The method comprises: obtaining historical association data of a user account corresponding to an application, wherein the historical association data comprises information associated with the user account and obtained in a preconfigured service period; adopting the historical association data to perform an evaluation to obtain an evaluation result; and determining, according to the evaluation result, an identity verification method to perform identity verification. The invention resolves a technical issue of having difficulty to prevent identity theft or forgery in the prior art, owing to employing a single identity verification method in the related art.

(57) 摘要: 本发明公开了一种身份认证系统、方法、装置及账号认证方法。其中，该方法包括：获取与应用程序对应的用户账户的历史关联数据，其中，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息；采用历史关联数据进行评估，得到评估结果；根据评估结果确定对应的身份认证方式，进行身份认证。本发明解决了相关技术中所采用的身份认证方式较为单一，难以防止伪造、变造虚假身份信息的技术问题。

(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, 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))。

身份认证系统、方法、装置及账号认证方法

本申请要求 2016 年 11 月 16 日递交的申请号为 201611010182.6、发明名称为“身份认证系统、方法、装置及账号认证方法”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

本发明涉及互联网领域，具体而言，涉及一种身份认证系统、方法、装置及账号认证方法。

10 背景技术

目前，随着科学技术不断创新，开展个人网上业务（例如：在购物平台网站上开设个人网店）的身份认证过程也发生了日新月异的变化。从最初的身份认证，为确保“人证合一”，提出了个人用户手持证件照的认证方式；后来，逐步升级为要求个人用户上传/提交指定的动态手势图像；现如今，在实人认证方式加入到大数据风险管理模式后，

15 为身份认证的技术手段的丰富多样化提供了拓展可能性。

然而，相关技术中所采用的主流身份认证方式通常仅能够实现在认证阶段开展基于用户姓名，用户个人身份证件以及用户面部图像等多项信息对用户身份进行核实。然而，却无法长期对用户身份的真实性进行实时监控，由此造成安全可靠较低。

针对上述的问题，目前尚未提出有效的解决方案。

20

发明内容

本发明实施例提供了一种身份认证系统、方法、装置及账号认证方法，以至少解决相关技术中所采用的身份认证方式较为单一，难以防止伪造、变造虚假身份信息的技术问题。

25

根据本发明实施例的一个方面，提供了一种身份认证系统，包括：用户设备和认证服务器；用户设备，用于运行应用程序，并请求认证服务器对应用程序对应的用户账户进行认证状态检测；认证服务器，用于在确定用户账户为待认证账户后，采用获取到的用户账户的历史关联数据进行评估，得到评估结果，并根据评估结果确定对应的身份认证方式，进行身份认证，其中，历史关联数据是在预设业务周期内获取到的与用户账户

30 关联的信息。

可选地，上述历史关联数据包括以下至少之一：用户设备信息、用户身份信息、用户网络行为信息、用户业务信息。

可选地，认证服务器，还用于向用户设备下发授权认证信息。

可选地，认证服务器，还用于对历史关联数据进行分析，构建评估模型，并统计评估模型中每个特征指标对应的等级或评分，得到评估结果。

可选地，用户设备信息至少包括：用户设备使用的互联网协议 IP 地址信息，用户设备所使用的操作系统类型，用户设备的使用记录，认证服务器，还用于根据用户设备信息构建评估模型，并统计评估模型中每个特征指标对应的等级或评分，得到评估结果，其中，评估模型中的特征指标包括：根据 IP 地址信息确定用户设备是否执行过违法操作、根据用户设备所使用的操作系统类型确定用户设备所使用的操作系统是否存在安全漏洞、根据用户设备的使用记录确定用户设备是否安装过高危应用。

可选地，预设业务周期包括：第一评估周期和第二评估周期，认证服务器，还用于对历史关联数据在第一评估周期与第二评估周期的变化趋势进行分析，得到评估结果。

可选地，认证服务器，还用于根据评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息，并按照待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行身份认证。

根据本发明实施例的另一方面，还提供了一种身份认证方法，用于选择身份认证方式，包括：

获取与应用程序对应的用户账户的历史关联数据，其中，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息；采用历史关联数据进行评估，得到评估结果；根据评估结果确定对应的身份认证方式，进行身份认证。

可选地，历史关联数据包括以下至少之一：用户设备信息、用户身份信息、用户网络行为信息、用户业务信息。

可选地，在获取历史关联数据之前，还包括：接收来自于用户设备的第一请求消息，其中，用户设备用于运行应用程序；根据第一请求消息用户账户进行认证状态检测，并向用户设备返回第一响应消息，其中，第一响应消息用于确认用户账户为待认证账户。

可选地，在向用户设备返回第一响应消息之后，还包括：接收来自于用户设备的第二请求消息；根据第二请求消息确定待下发的授权认证信息；向用户设备返回第二响应消息，其中，第二响应消息中携带有授权认证信息。

可选地，采用历史关联数据进行评估，得到评估结果包括：对历史关联数据进行分析

析，构建评估模型，其中，评估模型包括：与历史关联数据中每个特征指标对应的等级或评分；统计评估模型中每个特征指标对应的等级或评分，得到评估结果。

5 可选地，用户设备信息至少包括以下特征指标：用户设备使用的互联网协议 IP 地址信息，用户设备所使用的操作系统类型，用户设备的使用记录；对历史关联数据进行分析，构建评估模型包括：获取用户设备信息中所包含的 IP 地址信息，操作系统类型，使用记录，并构建评估模型；统计评估模型中每个特征指标对应的等级或评分，得到评估结果包括：根据 IP 地址信息确定用户设备是否执行过违法操作并统计对应的等级或评分，根据用户设备所使用的操作系统类型确定用户设备所使用的操作系统是否存在安全漏洞并统计对应的等级或评分，以及根据用户设备的使用记录确定用户设备是否安装过高危应用并统计对应的等级或评分；通过统计每个特征指标对应的等级或评分，得到评估结果。

可选地，将 IP 地址信息，操作系统类型，使用记录作为输入信息，通过采用随机森林算法构建评估模型。

15 可选地，预设业务周期包括：第一评估周期和第二评估周期，采用历史关联数据进行评估，得到评估结果包括：获取历史关联数据在第一评估周期与第二评估周期的变化趋势；对变化趋势进行分析，得到评估结果。

可选地，根据评估结果确定身份认证方式，进行身份认证包括：根据评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息；按照待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行身份认证。

20 根据本发明实施例的又一方面，还提供了另一种身份认证方法，用于选择身份认证方式，包括：

运行应用程序；触发认证服务器对应用程序对应的用户账户进行认证状态检测，其中，认证状态检测用于采用获取到的用户账户的历史关联数据进行评估以得到评估结果，并根据评估结果确定对应的身份认证方式，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息。

根据本发明实施例的再一方面，还提供了一种账号认证方法，用于判断账号操作者是否改变，包括：

30 获取待认证账户的第一期间关联数据和第二期间关联数据，其中，第一期间关联数据是在第一时间周期内与待认证账户关联的数据，第二期间关联数据是在第二时间周期内与待认证账户关联的数据，并且第一时间周期与第二时间周期不完全相同；对第一期

间关联数据和第二期间关联数据进行相似度计算，得到相似度结果；根据相似度结果判断待认证账户的操作者是否改变。

可选地，在第一时间周期内与待认证账户关联的数据，为第一操作信息集合；在第二时间周期内与待认证账户关联的数据，为第二操作信息集合；对第一期间关联数据和第二期间关联数据进行相似度计算包括：计算第一操作信息集合和第二操作信息集合的差集；根据相似度结果判断待认证账户的操作者是否改变包括：如果差集超过预定阈值，则确定待认证账户的操作者发生改变。

可选地，在第一时间周期内与待认证账户关联的数据，为第一设备信息集合；在第二时间周期内与待认证账户关联的数据，为第二设备信息集合；对第一期间关联数据和第二期间关联数据进行相似度计算包括：计算第一设备信息集合和第二设备信息集合的差集；根据相似度结果判断待认证账户的操作者是否改变包括：如果差集超过预定阈值，则确定待认证账户的操作者发生改变。

根据本发明实施例的再一方面，还提供了一种身份认证装置，用于选择身份认证方式，包括：

获取模块，用于获取与应用程序对应的用户账户的历史关联数据，其中，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息；评估模块，用于采用历史关联数据进行评估，得到评估结果；认证模块，用于根据评估结果确定对应的身份认证方式，进行身份认证。

根据本发明实施例的再一方面，还提供了另一种身份认证装置，用于选择身份认证方式，包括：

运行模块，用于运行应用程序；触发模块，用于触发认证服务器对应用程序对应的用户账户进行认证状态检测，其中，认证状态检测用于采用获取到的用户账户的历史关联数据进行评估以得到评估结果，并根据评估结果确定对应的身份认证方式，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息。

在本发明实施例中，采用获取与应用程序对应的用户账户的历史关联数据（即，在预设业务周期内获取到的与用户账户关联的信息）；采用历史关联数据进行评估，得到评估结果的方式，通过评估结果确定对应的身份认证方式，进而执行身份认证流程，达到了通过对用户账户积累的历史关联数据进行分别识别用户账户是否存在风险的目的，从而实现了长期实时监控用户身份的真实性与可靠性，提升身份认证安全等级的技术效果，进而解决了相关技术中所采用的身份认证方式较为单一，难以防止伪造、变造虚假

身份信息的技术问题。另外，对于账号交易导致的账号操作者改变，通过不同周期内的账户关联信息和/或相关操作记录之间相似度的匹配，也能提供客观的操作依据。

附图说明

5 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身份认证系统的硬件结构框图；

图 2 是根据本发明优选实施例的触发认证流程的应用界面操作示意图；

图 3 是根据本发明实施例的身份认证方法的流程图；

10 图 4 是根据本发明实施例的另一种身份认证方法的流程图；

图 5 是根据本发明实施例的账号认证方法的流程图；

图 6 是根据本发明实施例的身份认证装置的结构框图；

图 7 是根据本发明优选实施例的身份认证装置的结构框图；

图 8 是根据本发明实施例的另一种身份认证装置的结构框图。

15

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

20 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

25 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。

首先，在对本申请实施例进行描述的过程中出现的部分名词或术语适用于如下解释：

30 (1) 智能终端应用（APP）：安装于智能终端，对智能终端本身功能进行扩展，用

于实现用户个性化业务需求的客户端，例如：网上购物类 APP、网上支付类 APP、二手货买卖 APP。

(2) 用户账户：为了使用应用程序提供的完整性功能服务，通过在注册页面填写用户个人信息，生成的独立信息存储区域。

5 (3) 历史关联数据：在预设业务周期内所能够获取到的与该用户账户关联的信息，其中，预设业务周期既可以从用户账户注册成功开始至触发认证流程时刻截止，也可以是用户账户注册成功后的特定时间段；与该用户账户关联的信息可以包括但不限于以下至少之一：用户身份信息、用户网络行为信息、用户所使用的用户设备信息、用户业务信息，其中，用户身份信息可以包括但不限于以下至少之一：用户为使用特定应用程序
10 提供的功能而注册的用户账号、用户在注册时所提供的身份证件中呈现的信息、用户的联系方式、用户的家庭住址和/或工作单位住址；用户设备信息可以包括但不限于以下至少之一：用户设备所使用的操作系统、用户设备的机型、用户设备的国际移动用户识别码（IMSI）/国际移动设备识别码（IMEI）、用户设备所使用的互联网协议（IP）地址和/或媒体接入控制（MAC）地址；用户网络行为信息可以包括但不限于以下至少之一：当
15 前认证操作行为、在执行身份认证之前与用户账户关联的过往行为（例如：购物记录体现的购物行为）；用户业务信息可以包括但不限于以下至少之一：购物记录、用户操作轨迹。

实施例 1

20 图 1 是根据本发明实施例的身份认证系统的硬件结构框图，如图 1 所示，用户设备 10 可以经由数据网络连接或电子连接到一个或多个认证服务器 20。一种可选实施例中，上述用户设备 10 可以是个人计算机（PC）、智能手机、平板电脑。数据网络连接可以是局域网连接、广域网连接、因特网连接，或其他类型的数据网络连接。用户设备 10 可以执行以连接到由一个服务器或一组服务器执行的网络服务。网络服务器是基于网络的
25 用户服务，诸如社交网络、云资源、电子邮件、在线支付或其他在线应用。

 在本实施例中，用户设备 10，用于运行应用程序，并请求认证服务器对应用程序对应的用户账户进行认证状态检测；认证服务器 20，用于在确定用户账户为待认证账户后，采用获取到的用户账户的历史关联数据进行评估，得到评估结果，并根据评估结果确定对应的身份认证方式，进行身份认证，其中，历史关联数据是在预设业务周期内获取到
30 的与用户账户关联的信息。

图 2 是根据本发明优选实施例的触发认证流程的应用界面操作示意图。如图 2 所示，用户如果需要在网上执行二手货交易，则用户设备上安装的应用程序（例如：用户二手货买卖）在运行后，用户可以登入预先注册的用户账号。用户设备需要检测该用户账号是否开通过网上店铺账号，如果尚未开通，则需要触发用户设备对用户认证状态进行检查。而用户设备则会调用实人认证服务器（即上述认证服务器 20）来判断当前的用户认证状态，进而确定是否需要对该用户执行认证流程，其中，实人认证服务器的判断依据可以包括但不限于以下至少之一：用户身份信息（例如：用户姓名、用户的身份证号）、用户设备所使用的操作系统（例如：android 系统、iOS 系统）、用户设备自身的性能（例如：硬件配置、是否执行过越狱操作）。

可选地，认证服务器 20，还用于向用户设备下发授权认证信息。

如果实人认证服务器确定需要对该用户执行认证流程，则用户设备需要向实人认证服务器请求下发授权认证信息，例如：令牌（Token），并获取实人认证服务器返回的授权认证信息，其中，上述授权认证信息用于认证权限校验，生成认证任务以及在不同认证执行主体之间传递。

以 Token 为例，其格式可以包括以下三个部分：

- （1）header，用于表示该 Token 的类型；
- （2）claims set，用于表示存储的数据，其可以包括：用户授权信息；
- （3）signature，用于验证 Token 的真伪。

可选地，认证服务器 20，还用于对历史关联数据进行分析，构建评估模型，并统计评估模型中每个特征指标对应的等级或评分，得到评估结果。

用户设备在获取到实人认证服务器颁发的 Token 之后，向实人认证服务器请求开始身份认证流程。实人认证服务器根据用户使用的应用程序的业务类型为该用户选取对应的认证通道。在利用选取的认证通道进行身份认证过程中，实人认证服务器可以获取用户通过用户设备上传过的用户身份信息、用户执行过的网络行为信息、用户所使用的用户设备信息、曾经采集过的用户生物特征信息等历史关联数据建立评估模型进行综合判断，以确定用户的风险程度，并为不同风险程度的用户提供差异化认证方式，其中，用户身份信息可以包括但不限于以下至少之一：用户为使用特定应用程序提供的功能而注册的用户账号、用户在注册时所提供的身份证件中呈现的信息、用户的联系方式、用户的家庭住址和/或工作单位住址；用户设备信息可以包括但不限于以下至少之一：用户设备所使用的操作系统、用户设备的机型、用户设备的国际移动用户识别码（IMSI）/国际

移动设备识别码（IMEI）、用户设备所使用的互联网协议（IP）地址和/或媒体接入控制（MAC）地址；用户网络行为信息可以包括但不限于以下至少之一：当前认证操作行为、在执行身份认证之前与用户账户关联的过往行为（例如：购物记录）；生物特征信息可以包括但不限于以下至少之一：声纹、指纹、眼纹、虹膜、静态用户图像、动态活体检测用户图像。

活体检测通过要求用户在特定场景下指示用户完成一个或多个指定动作，例如：指示用户摇头、指示用户点头、指示用户说一句话，其目的在于：判定当前接受身份认证的用户为真实的活人而并非是一张照片。

可选地，用户设备信息至少包括：用户设备使用的互联网协议 IP 地址信息，用户设备所使用的操作系统类型，用户设备的使用记录，认证服务器，还用于根据用户设备信息构建评估模型，并统计评估模型中每个特征指标对应的等级或评分，得到评估结果，其中，评估模型中的特征指标包括：根据 IP 地址信息确定用户设备是否执行过违法操作、根据用户设备所使用的操作系统类型确定用户设备所使用的操作系统是否存在安全漏洞、根据用户设备的使用记录确定用户设备是否安装过高危应用。

作为本发明的一个优选实施例，可以采用诸如随机森林算法来构建上述评估模型，并采用该评估模型作为风险防控的主要判断因子。该评估模型的输入信息可以包括但不限于上述用户设备信息、用户身份信息、用户网络行为信息、用户业务信息，通过随机森林算法进行计算后得到的输出信息即为模型分值，然后最终依照模型分值来确定对应的身份认证方式。具体地，首先需要获取可用数据（例如：用户设备信息、用户身份信息、用户网络行为信息、用户业务信息）；其次，需要进行特征构建，即判定获取到的可用数据的真实度；再次，需要进行特征分析，即，对构建的特征进行特征质量分析、特征单调情况分析、特征重要性分析以及特征合成；然后，再选用随机森林算法来进行模型选连，并最终得到评估结果。

在优选实施过程中，以历史关联数据为用户设备为例加以说明，通过构建评估模型综合判断用户的风险程度可以包括：如果 IP 地址归属地先前发生过电信诈骗案件，那么可以降低使用该 IP 地址的用户设备的安全等级（例如：安全等级降低 1 级）或安全评分（例如：安全评分扣去 1 分），进而降低意图运行应用程序执行购物操作或转账操作前的信用度，进而提升身份认证门槛；如果用户设备使用的是 android 系统或者执行过越狱操作的 iOS 系统，由于存在安全漏洞，因此可以降低使用该 IP 地址的用户设备的安全等级（例如：安全等级降低 1 级）或安全评分（例如：安全评分扣去 1 分），进而降低意

图运行应用程序执行购物操作或转账操作前的信用度，进而提升身份认证门槛；如果用户设备安装过作弊软件或浏览过非法（例如：色情、赌博）网站，那么可以降低使用该 IP 地址的用户设备的安全等级（例如：安全等级降低 1 级）或安全评分（例如：安全评分扣去 1 分），进而降低意图运行应用程序执行购物操作或转账操作前的信用度，进而提升身份认证门槛。

此外，针对历史关联数据包含的其他信息同样也可以依次构建评估模型，进行安全评估。例如：如果在特定用户设备的用户账户下存在多次恶意网络行为（例如：刷单）那么可以降低使用该用户设备意图运行应用程序执行购物操作前的信用度，进而提升身份认证门槛；如果用户在登录用户账户后上传的个人信息与实人认证服务器先前存储过的相关信息不符，那么可以降低使用该用户账户意图运行应用程序执行购物操作或转账操作前的信用度，进而提升身份认证门槛。如果用户登记过的用户的联系方式、用户的家庭住址和/或工作单位住址存在虚假信息，那么可以降低使用该用户账户意图运行应用程序执行购物操作或转账操作前的信用度，进而提升身份认证门槛。如果用户在购物车内放入大量商品的订单却并未按时付款，那么可以降低使用该用户账户意图运行应用程序执行购物操作或转账操作前的信用度，进而提升身份认证门槛。

需要说明的是，评估可以根据应用程序的业务类型仅针对其中一种判定因素进行评分，还可以同时综合多种判定因素进行评分，最终确定是否需要提升身份认证门槛。上述关于历史关联数据的示例仅为举例说明，而并非对历史关联数据所包含的内容构成不当限制。

可选地，上述预设业务周期至少包括：第一评估周期和第二评估周期，认证服务器还用于对历史关联数据在第一评估周期与第二评估周期的变化趋势进行分析，得到评估结果。

上述第一评估周期与上述第二评估周期可以是预先选取的两个相邻时间段，假设第一评估周期为距离当前时间最近的十天，而第二评估周期为与最近十天相邻的过去十天，那么通过比对历史关联数据在第一评估周期与第二评估周期的变化趋势，即比对历史关联数据在第一评估周期内与在第二评估周期内的相似度来确定评估结果。

以用户网络行为信息为例，假设账户 A 在第一评估周期内的销售行为或者购物行为始终保持正常状态（即正常按照订单进行发货且物品质量良好，或者，在下订单后及时付款），然而账户 A 在第二评估周期内由于账户被盗等缘故出现异常销售行为（例如：由于原先销售物美价钱的商品转变为销售高价的劣质商品或者基于买家的长期信任进行

付款后，该账户 A 长时间没有发货）或者异常购物行为（例如：频繁下单但不支付或频繁向卖家投诉完好商品存在质量问题并要求卖家退/换货），那么可以据此判定账户 A 可能存在被盗号等异常，需要重新对使用账户 A 的用户进行实人认证。

以用户设备信息和用户网络行为信息为例，假设账户 A 在第一评估周期内使用的是
5 ioS 系统的苹果手机，使用的 IP 地址显示在 C 地，在此期间的销售行为始终处于正常状态，然而账户 A 在第二评估周期内由于账户转让等缘故，由使用 ioS 系统的苹果手机转变为使用 Android 系统的华为手机，使用的 IP 地址显示由 C 地转变为 D 地，并且在此期间出现异常销售行为（例如：由于原先销售物美价钱的商品转变为销售高价的劣质商品或者基于买家的长期信任进行付款后，该账户 A 长时间没有发货），那么可以据此判定
10 账户 A 可能存在账户使用用途发生异常，需要重新对使用账户 A 的用户进行实人认证。

可选地，认证服务器 20，还用于根据评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息，并按照待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行身份认证。

在身份认证过程中，集成在应用程序内部的用于执行身份认证功能的软件开发工具
15 包（SDK）按照认证流程所需要执行的步骤序列以及每个步骤中需要采集的身份认证相关信息进行采集，并实时与实人认证服务器进行交互。通过上述评估模型得到的评估结果可以将用户账户为正常账户与风险账户，对于正常账户则可以按照常规设置的自动化认证流程，包括：采集静态身份证件图像、动态活体检测用户图像等信息；对于危险账户则需要在常规设置的自动化认证流程基础上增加补充资料采集过程，例如：增加动态
20 手势验证环节，以采集更多用户信息，便于进一步查验。

在完成上述身份认证流程之后，实人认证服务器会向用户设备反馈最终的身份认证结果。

在上述运行环境下，本申请提供了如图 3 所示的身份认证方法，需要说明的是，在
25 附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所
示出或描述的步骤。

图 3 是根据本发明实施例的身份认证方法的流程图。如图 3 所示，该方法可以包括以下处理步骤：

30 步骤 S32，获取与应用程序对应的用户账户的历史关联数据，其中，历史关联数据

是在预设业务周期内获取到的与用户账户关联的信息；

步骤 S34，采用历史关联数据进行评估，得到评估结果；

步骤 S36，根据评估结果确定对应的身份认证方式，进行身份认证。

在优选实施过程中，上述历史关联数据可以包括但不限于以下至少之一：用户设备

5 信息、用户身份信息、用户网络行为信息、用户业务信息。

可选地，在步骤 S32，获取历史关联数据之前，还可以包括以下执行步骤：

步骤 S30，接收来自于用户设备的第一请求消息，其中，用户设备用于运行应用程序；

10 步骤 S31，根据第一请求消息用户账户进行认证状态检测，并向用户设备返回第一响应消息，其中，第一响应消息用于确认用户账户为待认证账户。

可选地，在步骤 S31，向用户设备返回第一响应消息之后，还可以包括以下执行步骤：

步骤 S37，接收来自于用户设备的第二请求消息；

步骤 S38，根据第二请求消息确定待下发的授权认证信息；

15 步骤 S39，向用户设备返回第二响应消息，其中，第二响应消息中携带有授权认证信息。

可选地，在步骤 S34 中，采用历史关联数据进行评估，得到评估结果可以包括以下执行步骤：

20 步骤 S340，对历史关联数据进行分析，构建评估模型，其中，评估模型包括：与历史关联数据中每个特征指标对应的等级或评分；

步骤 S342，统计评估模型中每个特征指标对应的等级或评分，得到评估结果。

可选地，上述用户设备信息至少包括以下特征指标：用户设备使用的互联网协议 IP 地址信息，用户设备所使用的操作系统类型，用户设备的使用记录；

在步骤 S340 中，对历史关联数据进行分析，构建评估模型可以包括以下执行步骤：

25 步骤 S3400，获取用户设备信息中所包含的 IP 地址信息，操作系统类型，使用记录，并构建评估模型；

在步骤 S342 中，统计评估模型中每个特征指标对应的等级或评分，得到评估结果可以包括以下执行步骤：

30 步骤 S3420，根据 IP 地址信息确定用户设备是否执行过违法操作并统计对应的等级或评分，根据用户设备所使用的操作系统类型确定用户设备所使用的操作系统是否存在

安全漏洞并统计对应的等级或评分，以及根据用户设备的使用记录确定用户设备是否安装过高危应用并统计对应的等级或评分；通过统计每个特征指标对应的等级或评分，得到评估结果。

可选地，预设业务周期包括：第一评估周期和第二评估周期，在步骤 S34 中，采用

5 历史关联数据进行评估，得到评估结果可以包括以下执行步骤：

步骤 S344，获取历史关联数据在第一评估周期与第二评估周期的变化趋势；

步骤 S346，对变化趋势进行分析，得到评估结果。

可选地，在步骤 S36 中，根据评估结果确定身份认证方式，进行身份认证可以包括以下执行步骤：

10 步骤 S360，根据评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息；

步骤 S362，按照待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行身份认证。

15 在上述运行环境下，本申请提供了如图 4 所示的另一种身份认证方法，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

图 4 是根据本发明实施例的另一种身份认证方法的流程图。如图 4 所示，该方法可以包括以下处理步骤：

步骤 S42，运行应用程序；

20 步骤 S44，触发认证服务器对应用程序对应的用户账户进行认证状态检测，其中，认证状态检测用于采用获取到的用户账户的历史关联数据进行评估以得到评估结果，并根据评估结果确定对应的身份认证方式，历史关联数据是在预设业务周期内获取到的与
25 用户账户关联的信息。

在上述运行环境下，本申请提供了如图 5 所示的账号认证方法，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所
30 示出或描述的步骤。

图 5 是根据本发明实施例的账号认证方法的流程图。如图 5 所示，该方法可以包括以下处理步骤：

步骤 S52，获取待认证账户的第一期间关联数据和第二期间关联数据，其中，第一期间关联数据是在第一时间周期内与待认证账户关联的数据，第二期间关联数据是在第二时间周期内与待认证账户关联的数据，并且第一时间周期与第二时间周期不完全相同；

步骤 S54，对第一期间关联数据和第二期间关联数据进行相似度计算，得到相似度结果；

步骤 S56，根据相似度结果判断待认证账户的操作者是否改变。

上述第一时间周期与上述第二时间周期可以是预先选取的两个相邻时间段，即第一时间周期与第二时间周期在时间范围上并不发生重叠，假设第一时间周期为距离当前时间最近的十天，而第二时间周期为与最近十天相邻的过去十天；上述第一时间周期与上述第二时间周期可以是预先选取的两个部分重叠的时间段，假设第一时间周期为当月的 1 号至 10 号，而第二时间周期为当月的 5 号至 15 号。通过对第一期间关联数据和第二期间关联数据进行相似度比较，来判断待认证账户的操作者是否改变。

在优选实施过程中，在第一时间周期内与待认证账户关联的数据可以为第一操作信息集合；在第二时间周期内与待认证账户关联的数据可以为第二操作信息集合；

在步骤 S54 中，对第一期间关联数据和第二期间关联数据进行相似度计算可以包括以下执行步骤：

步骤 S540，计算第一操作信息集合和第二操作信息集合的差集；

在步骤 S56 中，根据相似度结果判断待认证账户的操作者是否改变可以包括以下执行步骤：

步骤 S560，如果差集超过预定阈值，则确定待认证账户的操作者发生改变。

假设账户 A 在第一时间周期内的销售行为或者购物行为始终保持正常状态（即正常按照订单进行发货且物品质量良好，或者，在下订单后及时付款），然而账户 A 在第二时间周期内由于账户被盗等缘故出现异常销售行为（例如：由于原先销售物美价廉的商品转变为销售高价的劣质商品或者基于买家的长期信任进行付款后，该账户 A 长时间没有发货）或者异常购物行为（例如：频繁下单但不支付或频繁向卖家投诉完好商品存在质量问题并要求卖家退/换货），那么通过比对第一期间关联数据（即账户 A 在第一时间周期内的销售行为或者购物行为的日志记录）与第二期间关联数据（即账户 A 在第二时间周期内的销售行为或者购物行为的日志记录）之间的相似度，可以据此判定账户 A 的

操作人员很有可能发生变化，需要重新对使用账户 A 的操作人员进行实人认证。

在优选实施过程中，在第一时间周期内与待认证账户关联的数据，为第一设备信息集合；在第二时间周期内与待认证账户关联的数据，为第二设备信息集合；

在步骤 S54 中，对第一期间关联数据和第二期间关联数据进行相似度计算可以包括

5 以下执行步骤：

步骤 S542，计算第一设备信息集合和第二设备信息集合的差集；

在步骤 S56 中，根据相似度结果判断待认证账户的操作者是否改变可以包括以下执行步骤：

步骤 S562，如果差集超过预定阈值，则确定待认证账户的操作者发生改变。

10 假设账户 A 在第一时间周期内使用的是 iOS 系统的苹果手机，使用的 IP 地址显示在 C 地，使用的 IMSI 中 MNC 显示的运营商为中国移动，然而账户 A 在第二时间周期内由使用 iOS 系统的苹果手机转变为使用 Android 系统的华为手机，使用的 IP 地址显示由 C 地转变为 D 地，并且在此期间还发现其使用的 IMSI 中 MNC 显示的运营商由中国移动转变为中国联通，那么通过比对第一期间关联数据（即账户 A 在第一时间周期内使用的用户设备信息相关的日志记录）与第二期间关联数据（即账户 A 在第二时间周期内使用的用户设备信息相关的日志记录）之间的相似度，可以据此判定账户 A 的操作人员很有可能发生变化，需要重新对使用账户 A 的操作人员进行实人认证。

通过获取个人用户通过用户设备曾经上传过的用户身份信息、用户曾经执行过的网络行为信息、用户曾经所使用的用户设备信息、用户设备曾经采集过的用户生物特征信息等历史关联数据建立评估模型进行综合分析，对用户账户的风险程度/程序进行实时监控，同时还将认证手段进一步升级为活体检测。不仅如此，实人认证业务还可以被拓展到其他需要通过个人身份认证才能够开展的网上业务。

20 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，25 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优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

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身份认证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，30 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所述的方法。

5

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方法的装置实施例。图 6 是根据本发明实施例的身份认证装置的结构框图。如图 6 所示，该装置包括：获取模块 10，用于获取与应用程序对应的用户账户的历史关联数据，其中，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息；评估模块 20，用于采用历史关联数据进行评估，得到评估结果；认证模块 30，用于根据评估结果确定对应的身份认证方式，进行身份认证。

可选地，图 7 是根据本发明优选实施例的身份认证装置的结构框图。如图 7 所示，上述装置还可以包括：第一接收模块 40，用于接收来自于用户设备的第一请求消息，其中，用户设备用于运行应用程序；第一响应模块 50，用于根据第一请求消息用户账户进行认证状态检测，并向用户设备返回第一响应消息，其中，第一响应消息用于确认用户账户为待认证账户。

在优选实施过程中，上述历史关联数据可以包括但不限于以下至少之一：用户设备信息、用户身份信息、用户网络行为信息、用户业务信息。

20 可选地，如图 7 所示，上述装置还可以包括：第二接收模块 60，用于接收来自于用户设备的第二请求消息；第二响应模块 70，用于根据第二请求消息确定待下发的授权认证信息，并向用户设备返回第二响应消息，其中，第二响应消息中携带有授权认证信息。

可选地，评估模块 20 可以包括：分析单元（图中未示出），用于对历史关联数据进行分析，构建评估模型，其中，评估模型包括：与历史关联数据中每个特征指标对应的等级或评分；第一统计单元（图中未示出），用于统计评估模型中每个特征指标对应的等级或评分，得到评估结果。

30 可选地，上述用户设备信息至少包括以下特征指标：用户设备使用的互联网协议 IP 地址信息，用户设备所使用的操作系统类型，用户设备的使用记录；分析单元（图中未示出），用于获取用户设备信息中所包含的 IP 地址信息，操作系统类型，使用记录，并构建评估模型；统计单元（图中未示出），用于根据 IP 地址信息确定用户设备是否执行

过违法操作并统计对应的等级或评分，根据用户设备所使用的操作系统类型确定用户设备所使用的操作系统是否存在安全漏洞并统计对应的等级或评分，以及根据用户设备的使用记录确定用户设备是否安装过高危应用并统计对应的等级或评分；通过统计每个特征指标对应的等级或评分，得到评估结果。

5 可选地，上述预设业务周期至少包括：第一评估周期和第二评估周期，评估模块 20 可以包括：获取单元（图中未示出），用于获取历史关联数据在第一评估周期与第二评估周期的变化趋势；第二统计单元（图中未示出），用于对变化趋势进行分析，得到评估结果。

10 可选地，认证模块 30 可以包括：确定单元（图中未示出），用于根据评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息；认证单元（图中未示出），用于按照待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行身份认证。

15 根据本发明实施例，还提供了另一种用于实施上述身份认证方法的装置实施例。图 8 是根据本发明实施例的另一种身份认证装置的结构框图。如图 8 所示，该装置包括：运行模块 80，用于运行应用程序；触发模块 90，用于触发认证服务器对应用程序对应的用户账户进行认证状态检测，其中，认证状态检测用于采用获取到的用户账户的历史关联数据进行评估以得到评估结果，并根据评估结果确定对应的身份认证方式，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息。

20

实施例 3

25 本发明的实施例还提供了一种存储介质。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程序来指令终端设备/服务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。

 可选地，在本实施例中，上述存储介质可以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。

30 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服务端群中的任意一

个服务器中，或者位于服务端群中的任意一个服务器中。

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：

S1，获取与应用程序对应的用户账户的历史关联数据，其中，历史关联数据是在预设业务周期内获取到的与用户账户关联的信息；

5 S2，采用历史关联数据进行评估，得到评估结果；

S3，根据评估结果确定对应的身份认证方式，进行身份认证。

可选地，在本实施例中，存储介质还被设置为存储用于执行以下步骤的程序代码：

接收来自于用户设备的第一请求消息，其中，用户设备用于运行应用程序；根据第一请求消息用户账户进行认证状态检测，并向用户设备返回第一响应消息，其中，第一响应
10 消息用于确认用户账户为待认证账户。

可选地，在本实施例中，存储介质还被设置为存储用于执行以下步骤的程序代码：

接收来自于用户设备的第二请求消息；根据第二请求消息确定待下发的授权认证信息；
向用户设备返回第二响应消息，其中，第二响应消息中携带有授权认证信息。

可选地，在本实施例中，存储介质还被设置为存储用于执行以下步骤的程序代码：

15 对历史关联数据进行分析，构建评估模型，其中，评估模型包括：与历史关联数据中每个特征指标对应的等级或评分；统计评估模型中每个特征指标对应的等级或评分，得到评估结果。

可选地，用户设备信息至少包括以下特征指标：用户设备使用的互联网协议 IP 地址

20 信息，用户设备所使用的操作系统类型，用户设备的使用记录；在本实施例中，存储介质还被设置为存储用于执行以下步骤的程序代码：获取用户设备信息中所包含的 IP 地址信息，操作系统类型，使用记录，并构建评估模型；根据 IP 地址信息确定用户设备是否执行过违法操作并统计对应的等级或评分，根据用户设备所使用的操作系统类型确定用户设备所使用的操作系统是否存在安全漏洞并统计对应的等级或评分，以及根据用户设备的使用记录确定用户设备是否安装过高危应用并统计对应的等级或评分；通过统计每
25 个特征指标对应的等级或评分，得到评估结果。

可选地，预设业务周期包括：第一评估周期和第二评估周期，在本实施例中，存储介质还被设置为存储用于执行以下步骤的程序代码：获取历史关联数据在第一评估周期与第二评估周期的变化趋势；对变化趋势进行分析，得到评估结果。

可选地，在本实施例中，存储介质还被设置为存储用于执行以下步骤的程序代码：

30 根据评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息；

按照待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行身份认证。

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
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
15 目的。

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时，
20 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优选实施方式，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. 一种身份认证系统，其特征在于，包括：用户设备和认证服务器；

所述用户设备，用于运行应用程序，并请求认证服务器对所述应用程序对应的用户账户进行认证状态检测；

5 所述认证服务器，用于在确定所述用户账户为待认证账户后，采用获取到的所述用户账户的历史关联数据进行评估，得到评估结果，并根据所述评估结果确定对应的身份认证方式，进行身份认证，其中，所述历史关联数据是在预设业务周期内获取到的与所述用户账户关联的信息。

2. 根据权利要求 1 所述的系统，其特征在于，所述历史关联数据包括以下至少之一：
10 一：

 用户设备信息、用户身份信息、用户网络行为信息、用户业务信息。

3. 根据权利要求 1 所述的系统，其特征在于，所述认证服务器，还用于向所述用户设备下发授权认证信息。

4. 根据权利要求 2 所述的系统，其特征在于，所述认证服务器，还用于对所述历史关联数据进行分析，构建评估模型，并统计所述评估模型中每个特征指标对应的等级或评分，得到所述评估结果。
15 或评分，得到所述评估结果。

5. 根据权利要求 4 所述的系统，其特征在于，用户设备信息至少包括：所述用户设备使用的互联网协议 IP 地址信息，所述用户设备所使用的操作系统类型，所述用户设备的使用记录，所述认证服务器，还用于根据所述用户设备信息构建评估模型，并统计所述评估模型中每个特征指标对应的等级或评分，得到所述评估结果，其中，所述评估模型中的特征指标包括：根据所述 IP 地址信息确定所述用户设备是否执行过违法操作、根据所述用户设备所使用的操作系统类型确定所述用户设备所使用的操作系统是否存在安全漏洞、根据所述用户设备的使用记录确定所述用户设备是否安装过高危应用。
20 计所述评估模型中每个特征指标对应的等级或评分，得到所述评估结果，其中，所述评估模型中的特征指标包括：根据所述 IP 地址信息确定所述用户设备是否执行过违法操作、根据所述用户设备所使用的操作系统类型确定所述用户设备所使用的操作系统是否存在安全漏洞、根据所述用户设备的使用记录确定所述用户设备是否安装过高危应用。

6. 根据权利要求 2 所述的系统，其特征在于，所述预设业务周期包括：第一评估周期和第二评估周期，所述认证服务器，还用于对所述历史关联数据在所述第一评估周期与所述第二评估周期的变化趋势进行分析，得到所述评估结果。
25 周期和第二评估周期，所述认证服务器，还用于对所述历史关联数据在所述第一评估周期与所述第二评估周期的变化趋势进行分析，得到所述评估结果。

7. 根据权利要求 5 或 6 所述的系统，其特征在于，所述认证服务器，还用于根据所述评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息，并按照所述待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行所述身份认证。
30 述身份认证。

8. 一种身份认证方法，用于选择身份认证方式，其特征在于，包括：

获取与应用程序对应的用户账户的历史关联数据，其中，所述历史关联数据是在预设业务周期内获取到的与所述用户账户关联的信息；

采用所述历史关联数据进行评估，得到评估结果；

5 根据所述评估结果确定对应的身份认证方式，进行身份认证。

9. 根据权利要求 8 所述的方法，其特征在于，所述历史关联数据包括以下至少之一：

用户设备信息、用户身份信息、用户网络行为信息、用户业务信息。

10 10. 根据权利要求 8 所述的方法，其特征在于，在获取所述历史关联数据之前，还包括：

接收来自于用户设备的第一请求消息，其中，所述用户设备用于运行所述应用程序；
根据所述第一请求消息所述用户账户进行认证状态检测，并向所述用户设备返回第一响应消息，其中，所述第一响应消息用于确认所述用户账户为待认证账户。

15 11. 根据权利要求 10 所述的方法，其特征在于，在向所述用户设备返回所述第一响应消息之后，还包括：

接收来自于所述用户设备的第二请求消息；

根据所述第二请求消息确定待下发的授权认证信息；

向所述用户设备返回第二响应消息，其中，所述第二响应消息中携带有所述授权认证信息。

20 12. 根据权利要求 9 所述的方法，其特征在于，采用所述历史关联数据进行所述评估，得到所述评估结果包括：

对所述历史关联数据进行分析，构建评估模型，其中，所述评估模型包括：与所述历史关联数据中每个特征指标对应的等级或评分；

统计所述评估模型中每个特征指标对应的等级或评分，得到所述评估结果。

25 13. 根据权利要求 12 所述的方法，其特征在于，用户设备信息至少包括以下特征指标：所述用户设备使用的互联网协议 IP 地址信息，所述用户设备所使用的操作系统类型，所述用户设备的使用记录；

对所述历史关联数据进行分析，构建评估模型包括：

30 获取所述用户设备信息中所包含的所述 IP 地址信息，所述操作系统类型，所述使用记录，并构建评估模型；

统计所述评估模型中每个特征指标对应的等级或评分，得到所述评估结果包括：

根据所述 IP 地址信息确定所述用户设备是否执行过违法操作并统计对应的等级或评分，根据所述用户设备所使用的操作系统类型确定所述用户设备所使用的操作系统是否存在安全漏洞并统计对应的等级或评分，以及根据所述用户设备的使用记录确定所述
5 用户设备是否安装过高危应用并统计对应的等级或评分；通过统计每个特征指标对应的等级或评分，得到所述评估结果。

14. 根据权利要求 13 所述的方法，其特征在于，将所述 IP 地址信息，所述操作系统类型，所述使用记录作为输入信息，通过采用随机森林算法构建评估模型。

15. 根据权利要求 9 所述的方法，其特征在于，所述预设业务周期包括：第一评估
10 周期和第二评估周期，采用所述历史关联数据进行评估，得到所述评估结果包括：
获取所述历史关联数据在所述第一评估周期与所述第二评估周期的变化趋势；
对所述变化趋势进行分析，得到所述评估结果。

16. 根据权利要求 13 或 15 所述的方法，其特征在于，根据所述评估结果确定所述身份认证方式，进行所述身份认证包括：

15 根据所述评估结果确定待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息；

按照所述待执行的验证步骤以及每个验证步骤中待采集的身份认证关联信息进行所述身份认证。

17. 一种身份认证方法，用于选择身份认证方式，其特征在于，包括：
20 运行应用程序；

触发认证服务器对所述应用程序对应的用户账户进行认证状态检测，其中，所述认证状态检测用于采用获取到的所述用户账户的历史关联数据进行评估以得到评估结果，并根据所述评估结果确定对应的身份认证方式，所述历史关联数据是在预设业务周期内获取到的与所述用户账户关联的信息。

25 18. 一种账号认证方法，用于判断账号操作者是否改变，其特征在于，包括：

获取待认证账户的第一期间关联数据和第二期间关联数据，其中，所述第一期间关联数据是在第一时间周期内与所述待认证账户关联的数据，所述第二期间关联数据是在第二时间周期内与所述待认证账户关联的数据，并且第一时间周期与第二时间周期不完全相同；

30 对第一期间关联数据和第二期间关联数据进行相似度计算，得到相似度结果；

根据所述相似度结果判断所述待认证账户的操作者是否改变。

19. 根据权利要求 18 所述的方法, 其特征在于, 所述在第一时间周期内与所述待认证账户关联的数据, 为第一操作信息集合; 所述在第二时间周期内与所述待认证账户关联的数据, 为第二操作信息集合;

5 对第一期间关联数据和第二期间关联数据进行相似度计算包括:
 计算所述第一操作信息集合和第二操作信息集合的差集;
 根据所述相似度结果判断所述待认证账户的操作者是否改变包括:
 如果所述差集超过预定阈值, 则确定所述待认证账户的操作者发生改变。

20. 根据权利要求 18 所述的方法, 其特征在于, 所述在第一时间周期内与所述待认证账户关联的数据, 为第一设备信息集合; 所述在第二时间周期内与所述待认证账户关联的数据, 为第二设备信息集合;

 对第一期间关联数据和第二期间关联数据进行相似度计算包括:
 计算所述第一设备信息集合和第二设备信息集合的差集;
 根据所述相似度结果判断所述待认证账户的操作者是否改变包括:
15 如果所述差集超过预定阈值, 则确定所述待认证账户的操作者发生改变。

21. 一种身份认证装置, 用于选择身份认证方式, 其特征在于, 包括:

 获取模块, 用于获取与应用程序对应的用户账户的历史关联数据, 其中, 所述历史关联数据是在预设业务周期内获取到的与所述用户账户关联的信息;

 评估模块, 用于采用所述历史关联数据进行评估, 得到评估结果;

20 认证模块, 用于根据所述评估结果确定对应的身份认证方式, 进行身份认证。

22. 一种身份认证装置, 用于选择身份认证方式, 其特征在于, 包括:

 运行模块, 用于运行应用程序;

 触发模块, 用于触发认证服务器对所述应用程序对应的用户账户进行认证状态检测, 其中, 所述认证状态检测用于采用获取到的所述用户账户的历史关联数据进行评估

25 以得到评估结果, 并根据所述评估结果确定对应的身份认证方式, 所述历史关联数据是在预设业务周期内获取到的与所述用户账户关联的信息。

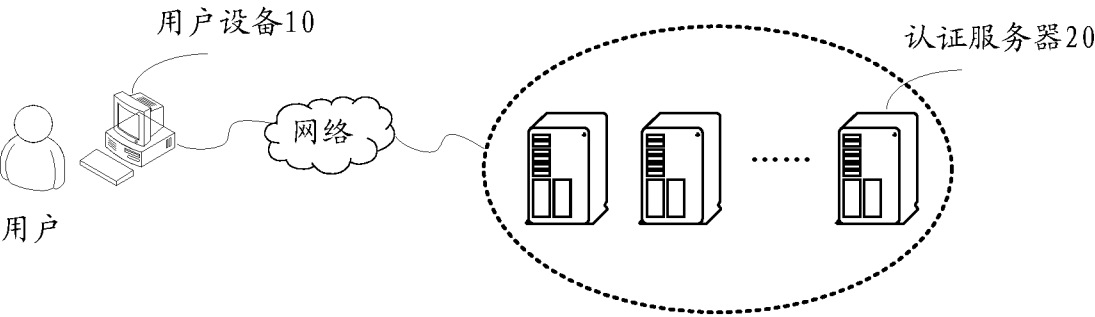


图 1

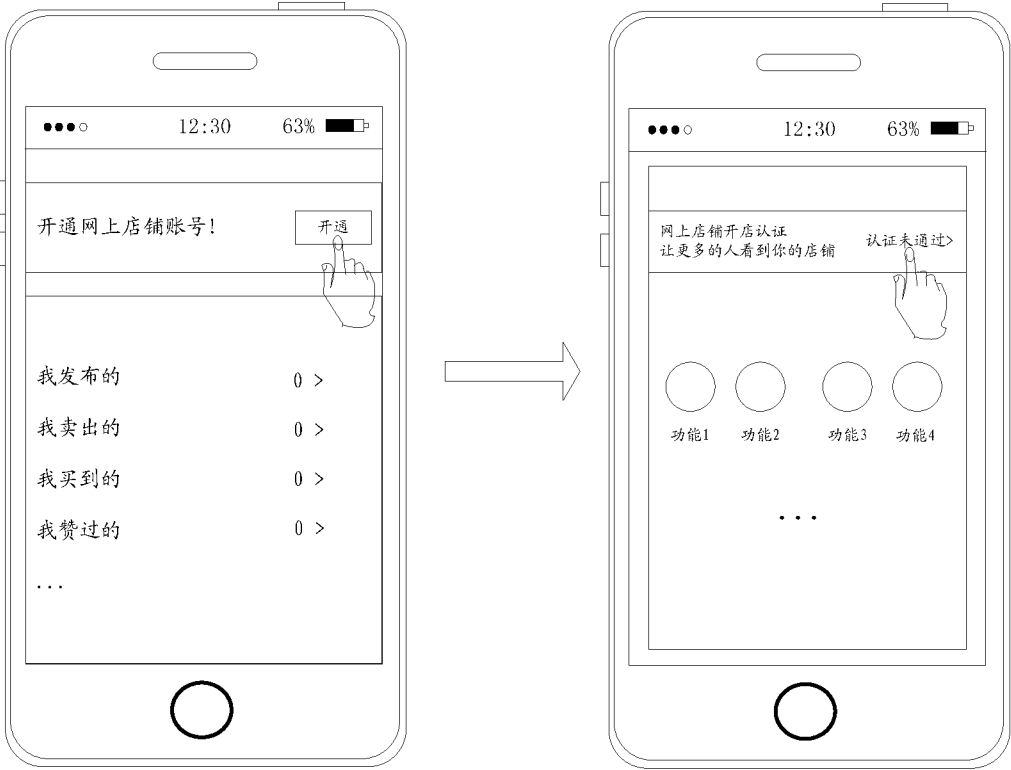


图 2

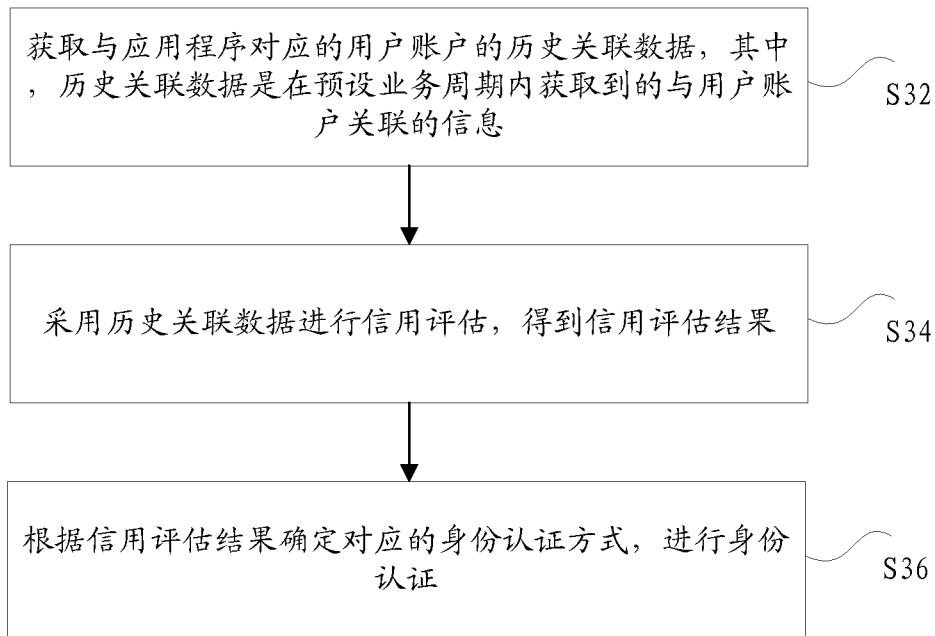


图 3

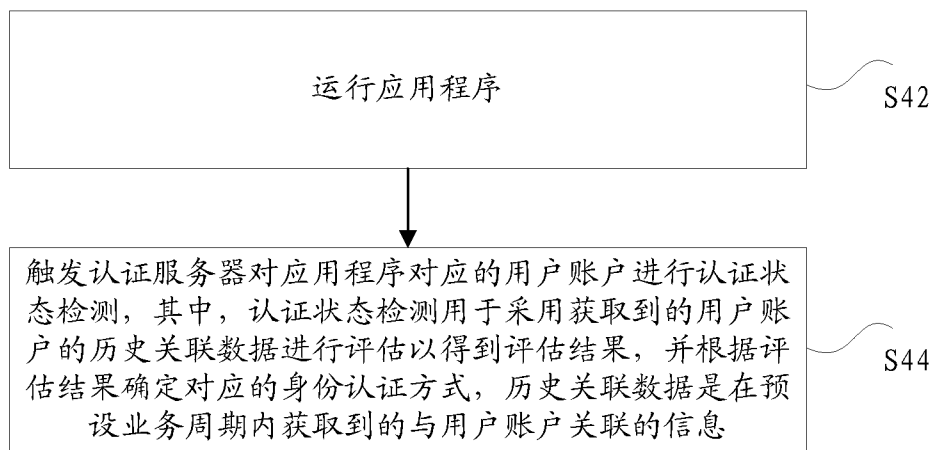


图 4

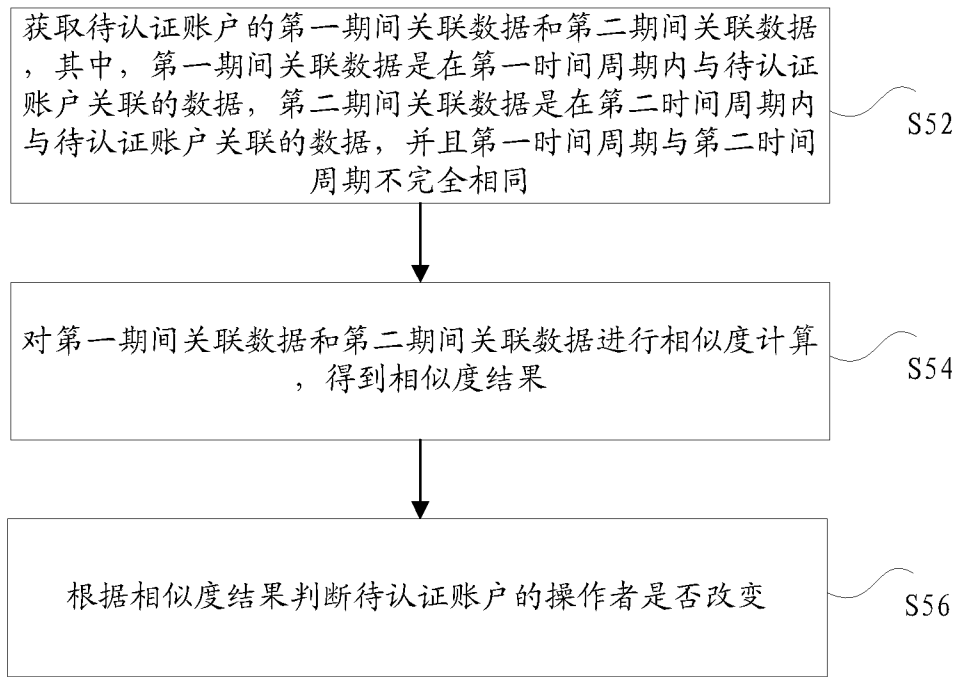


图 5

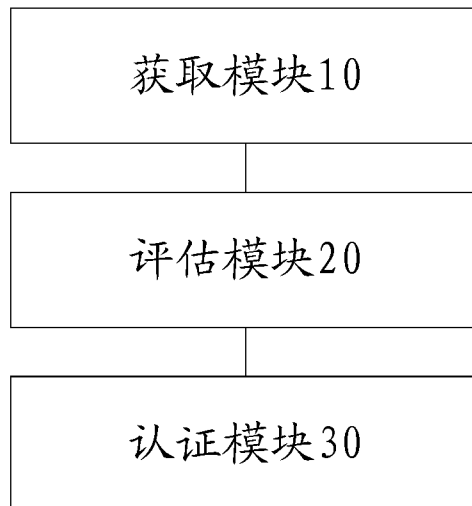


图 6

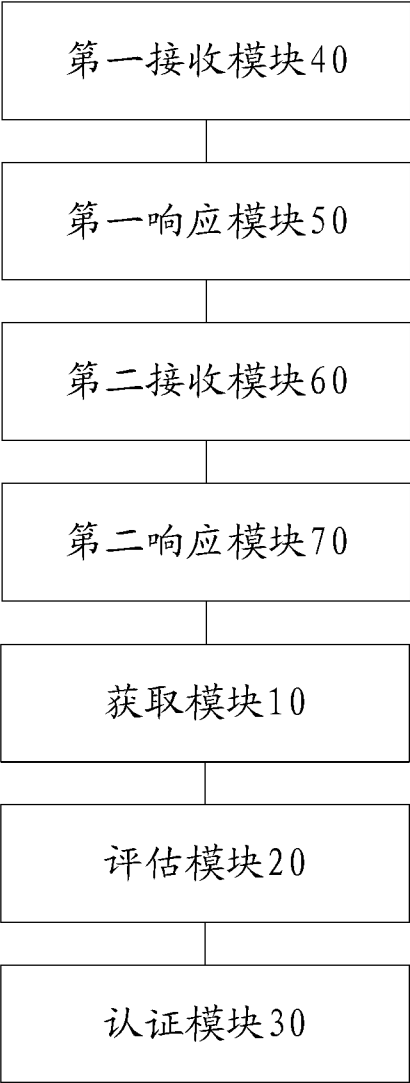


图 7



图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/109215

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 H04N

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)

CNPAT, CNKI, EPODOC, WPI, IEEE: 阿里巴巴, 认证, 鉴权, 账号, 历史, 行为, 评估, 分析, 模型, authentication, account, history, behavior, evaluat+, analy+, model

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107172049 A (BEIJING INFOSEC TECHNOLOGY CO., LTD.) 15 September 2017 (15.09.2017), description, paragraphs [0044]-[0091]	1-3, 8-11, 17, 21, 22
X	CN 104426847 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 18 March 2015 (18.03.2015), description, paragraphs [0049]-[0200]	1-3, 8-11, 17, 21, 22
Y	CN 104426847 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 18 March 2015 (18.03.2015), description, paragraphs [0049]-[0200]	4-7, 12-16
X	CN 103646197 A (CHINA UNIVERSITY OF PETROLEUM (EAST CHINA)) 19 March 2014 (19.03.2014), description, paragraphs [0047]-[0114]	18-20
Y	CN 103646197 A (CHINA UNIVERSITY OF PETROLEUM (EAST CHINA)) 19 March 2014 (19.03.2014), description, paragraphs [0047]-[0114]	6, 7, 15, 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 05 January 2018	Date of mailing of the international search report 30 January 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 ZHANG, Suqing Telephone No. (86-10) 62413957

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/CN2017/109215

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104426884 A (SHENZHEN TENCENT COMPUTER SYSTEMS COMPANY LIMITED) 18 March 2015 (18.03.2015), description, paragraphs [0029]-[0089]	4, 5, 7, 12-14, 16
A	CN 102510337 A (FUDAN UNIVERSITY) 20 June 2012 (20.06.2012), entire document	1-22
A	WO 2012116944 A1 (GEMALTO SA) 07 September 2012 (07.09.2012), entire document	1-22
A	WO 2012120355 A1 (TRUSTED LOGIC MOBILITY SAS) 13 September 2012 (13.09.2012) entire document	1-22

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/109215

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 107172049 A	15 September 2017	None	
CN 104426847 A	18 March 2015	US 9491182 B2	08 November 2016
		US 2015135282 A1	14 May 2015
		WO 2015024447 A1	26 February 2015
CN 103646197 A	19 March 2014	CN 103646197 B	15 June 2016
CN 104426884 A	18 March 2015	None	
CN 102510337 A	20 June 2012	CN 102510337 B	09 July 2014
WO 2012116944 A1	07 September 2012	EP 2492834 A1	29 August 2012
WO 2012120355 A1	13 September 2012	EP 2498529 A1	12 September 2012

国际检索报告

国际申请号

PCT/CN2017/109215

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 H04N

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))

CNPAT, CNKI, EPODOC, WPI, IEEE: 阿里巴巴, 认证, 鉴权, 账号, 历史, 行为, 评估, 分析, 模型, authentication, account, history, behavior, evaluat+, analy+, model

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
PX	CN 107172049 A (北京信安世纪科技有限公司) 2017年 9月 15日 (2017 - 09 - 15) 说明书第[0044]-[0091]段	1-3, 8-11, 17, 21, 22
X	CN 104426847 A (腾讯科技深圳有限公司) 2015年 3月 18日 (2015 - 03 - 18) 说明书第[0049]-[0200]段	1-3, 8-11, 17, 21, 22
Y	CN 104426847 A (腾讯科技深圳有限公司) 2015年 3月 18日 (2015 - 03 - 18) 说明书第[0049]-[0200]段	4-7, 12-16
X	CN 103646197 A (中国石油大学华东) 2014年 3月 19日 (2014 - 03 - 19) 说明书第[0047]-[0114]段	18-20
Y	CN 103646197 A (中国石油大学华东) 2014年 3月 19日 (2014 - 03 - 19) 说明书第[0047]-[0114]段	6-7, 15-16
Y	CN 104426884 A (深圳市腾讯计算机系统有限公司) 2015年 3月 18日 (2015 - 03 - 18) 说明书第[0029]-[0089]段	4-5, 7, 12-14, 16
A	CN 102510337 A (复旦大学) 2012年 6月 20日 (2012 - 06 - 20) 全文	1-22
A	WO 2012116944 A1 (GEMALTO SA) 2012年 9月 7日 (2012 - 09 - 07) 全文	1-22

☒ 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

2018年 1月 5日

国际检索报告邮寄日期

2018年 1月 30日

ISA/CN的名称和邮寄地址

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

受权官员

张素卿

电话号码 (86-10) 62413957

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
A	WO 2012120355 A1 (TRUSTED LOGIC MOBILITY SAS) 2012年 9月 13日 (2012 - 09 - 13) 全文	1-22

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/109215

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	107172049	A	2017年 9月 15日	无			
CN	104426847	A	2015年 3月 18日	US	9491182	B2	2016年 11月 8日
				US	2015135282	A1	2015年 5月 14日
				WO	2015024447	A1	2015年 2月 26日
CN	103646197	A	2014年 3月 19日	CN	103646197	B	2016年 6月 15日
CN	104426884	A	2015年 3月 18日	无			
CN	102510337	A	2012年 6月 20日	CN	102510337	B	2014年 7月 9日
WO	2012116944	A1	2012年 9月 7日	EP	2492834	A1	2012年 8月 29日
WO	2012120355	A1	2012年 9月 13日	EP	2498529	A1	2012年 9月 12日

表 PCT/ISA/210 (同族专利附件) (2009年7月)