

(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 7 月 5 日 (05.07.2018)



(10) 国际公布号
WO 2018/121387 A1

(51) 国际专利分类号:
G06F 21/44 (2013.01)

(21) 国际申请号: PCT/CN2017/117600

(22) 国际申请日: 2017 年 12 月 21 日 (21.12.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611259993.X 2016 年 12 月 30 日 (30.12.2016) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 童耀刚(TONG, Yaogang); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 郑建宾(ZHENG, Jianbin); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 周钰(ZHOU, Yu); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 张玉凤(ZHANG, Yufeng); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: 中国专利代理(香港)有限公司 (CHINA PATENT AGENT (HK)LTD.); 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (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,

(54) Title: SECURITY VERIFICATION METHOD, PLATFORM, APPARATUS AND SYSTEM

(54) 发明名称: 安全验证方法、平台、装置和系统

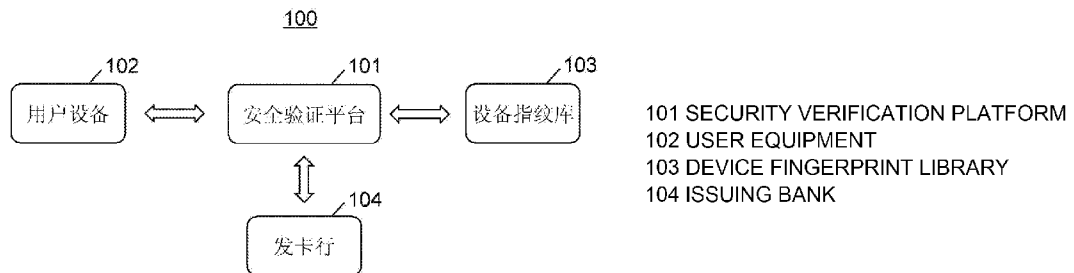


图 1

(57) Abstract: Provided are a security verification method, comprising: receiving a service request from a user, wherein the service request comprises user information and device information; creating a current device fingerprint based on the device information; acquiring a device fingerprint list, wherein the device fingerprint list comprises pre-stored device fingerprints of all the devices associated with the user; comparing the current device fingerprint with the device fingerprint list; and determining that the service request passes security verification where the current device fingerprint matches at least one item in the device fingerprint list, wherein the device information comprises a device hardware parameter and device usage condition data, and the device fingerprint is a device model built based on the device hardware parameter and the device usage condition data. Further provided are a corresponding security verification platform, a corresponding security verification method implemented on a user equipment, a corresponding security verification apparatus, and a security verification system.

(57) 摘要: 本发明提供了一种安全验证方法, 其包括: 接收来自用户的业务请求, 所述业务请求包括用户信息以及设备信息; 基于所述设备信息创建当前设备指纹; 获取设备指纹列表, 所述设备指纹列表包括与所述用户关联的所有设备的先前存储的设备指纹; 将所述当前设备指纹与所述设备指纹列表比对; 以及在所述当前设备指纹与所述设备指纹列表中的至少一项匹配的情况下判定所述业务请求通过安全验证, 其中所述设备信息包括设备硬件参数以及设备使用情况数据, 并且所述设备指纹是基于设备硬件参数以及设备使用情况数据构建的设备模型。本发明还提供了相应的安全验证平台、在用户设备上实现的相应的安全验证方法、相应的安全验证装置以及安全验证系统。

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))。

安全验证方法、平台、装置和系统

技术领域

[0001] 本发明一般地涉及银行卡安全技术领域，并且具体地，涉及与诸如无卡支付等应用相关的安全验证方法和系统。

背景技术

[0002] 随着虚拟化交易的普及，银行系统也开始越来越多地尝试无卡支付。在无卡支付的情况下，将银行卡放于手机中典型地可以有两种方式：一种是在无实体卡的情况下，用户通过特定的手机应用程序，向银行申请“空中发卡”，银行进行身份验证后，会将一张金融 IC 卡的全部信息加载到用户手机的 SIM 卡或者 SD 卡上；另一种是在已有实体卡的情况下，通过向发卡行申请实体卡的虚拟账户，发卡行基于令牌技术向用户发虚拟卡。这两种方式都存在认证难度大的问题，一般银行只会发卡给老客户。一般短信验证的方式也容易由于手机卡补办或者直接盗取验证码的原因而存在很大的安全隐患。

[0003] 目前现有的一些空中发卡方法包括采集用户的生物特征信息进行用户身份认证，通过认证审核成功进行发卡。此类方法具有如下几个缺点：**(1)** 如指纹、声纹等生物特征信息容易被盗取伪造，并且还需要硬件设备支持生物特征信息的采集功能，对硬件要求较高；**(2)** 用户的生物特征信息被盗取或者伪造不易被察觉，导致盗取或者伪造者可利用该方法进行大量卡片申请，造成用户财产的持续损失；**(3)** 没有屏蔽非法行为的机制。

[0004] 空中方法在很大程度上也依赖于用户所使用的设备，通常可能需要将与虚拟卡关联的账户信息与特定的用户设备进行绑定。目前对于诸如手机这样的多厂商不可控设备，也没有有效的终端 ID 可用于设备识别。这对于无卡支付的发卡阶段以及后续的交易阶段都造成了很大的安全隐患。

[0005] 因此，所期望的是设计一种可靠的安全验证方案，以提高无卡支付系统的安全性并且促进无卡支付技术的推广。

[0006]

发明内容

[0007] 有鉴于此，本发明提供了一种安全验证方案，可改善上述问题。

[0008] 一方面，本发明提供了一种安全验证方法，其包括：接收来自用户的业务请求，所述业务请求包括用户信息以及设备信息；基于所述设备信息创建当前设备指纹；获取设备指纹列表，所述设备指纹列表包括与所述用户关联的所有设备的先前存储的设备指纹；将所述当前设备指纹与所述设备指纹列表比对；以及在所述当前设备指纹与所述设备指纹列表中的至少一项匹配的情况下判定所述业务请求通过安全验证，其中所述设备信息包括设备硬件参数以及设备使用情况数据，并且所述设备指纹是基于所述设备信息构建的设备模型。

[0009] 如上所述的安全验证方法，其中，所述设备使用情况数据包括设备的网络信息、地理位置信息以及用户偏好行为信息中的一个或多个。

[0010] 如上所述的安全验证方法，其中，设备的网络信息包括设备的网络连接信息、TCP 包属性、连接的路由器属性、HTTP 协议属性、WiFi 列表中的一个或多个。

[0011] 如上所述的安全验证方法，其中，设备的地理位置信息包括基站定位地点、GPS 定位地点、与时间相关联的轨迹及常用地中的一个或多个。

[0012] 如上所述的安全验证方法，其中，设备的用户偏好行为信息包括操作系统类型、版本号、偏好设置、应用安装偏好设置、闹钟时间、开关机时间、应用使用频率及时间、屏幕操作时的接触面积、滑动方向、键盘输入的时间间隔、按压力度、陀螺仪信息、加速度计信息中的一个或多个。

[0013] 如上所述的安全验证方法，其中，将所述当前设备指纹与所述设备指纹列表比对包括：根据所述设备模型所包含的所有参数进行逐项对比；为每个参数赋予匹配权重；将各个参数的对比结果按所述匹配权重进行加权平均；并且根据所述加权平均的结果来判断所述当前设备指纹是否与所述设备指纹列表中的项匹配。

[0014] 如上所述的安全验证方法，其中，将所述当前设备指纹与所述设备指纹列表对比包括：依据所述设备历史使用情况对所述设备指纹列表中的每个设备指纹变化进行预测；并且将所述当前设备指纹与每个所述预测结果进行对比。

[0015] 如上所述的安全验证方法，其中，所述方法还包括在将所述当前设备指纹与所述设备指纹列表比对之前，将所述当前设备指纹与设备指纹黑名单库进行

对比，其中所述设备指纹黑名单库保存非法设备的设备指纹。

[0016] 如上所述的安全验证方法，其中，与设备指纹黑名单库进行对比包括按关键设备参数的优先级逐级将所述当前设备指纹与黑名单库中的设备指纹进行比对。

[0017] 如上所述的安全验证方法，其中，所述关键设备参数包括 MAC 地址、国际移动设备标识 IMEI、设备序列号以及系统标识。

[0018] 如上所述的安全验证方法，其中，所述先前存储的设备指纹基于设备硬件参数以及历史的设备使用情况数据生成。

[0019] 如上所述的安全验证方法，其还包括周期性地从与所述用户关联的所有设备接收设备使用情况数据来更新所述设备指纹列表中的设备指纹。

[0020] 如上所述的安全验证方法，其中，所述业务请求包括发卡请求以及交易请求。

[0021] 如上所述的安全验证方法，其中，所述用户信息包括与所述业务相关联的用户名和密码。

[0022] 另一方面，本发明还提供了一种安全验证平台，其包括：数据接收模块，用于接收来自用户的业务请求，所述业务请求包括用户信息以及设备信息；设备指纹创建模块，用于基于所述设备信息创建当前设备指纹；列表获取模块，用于获取设备指纹列表，所述设备指纹列表包括与所述用户关联的所有设备的先前存储的设备指纹；比对模块，用于将所述当前设备指纹与所述设备指纹列表比对；以及判定模块，用于在所述当前设备指纹与所述设备指纹列表中的至少一项匹配的情况下判定所述业务请求通过安全验证，其中所述设备信息包括设备硬件参数以及设备使用情况数据，并且所述设备指纹是基于所述设备信息构建的设备模型。

[0023] 还有另一方面，本发明提供了一种安全验证方法，其包括：在设备处从用户获取采集设备信息的授权；依据所述授权从所述设备采集设备信息，所述设备信息包括设备硬件参数和设备使用情况数据；以及在用户使用所述设备向安全验证平台发送业务请求时在所述业务请求中添加所述设备信息。

[0024] 如上所述的安全验证方法，其还包括：周期性地向所述安全验证平台传送所述设备使用情况数据。

[0025] 又一方面，本发明提供了安全验证装置，其包括：授权模块，用于在设

备处从用户获取采集设备信息的授权；信息采集模块，用于依据所述授权从所述设备采集设备信息，所述设备信息包括设备硬件参数和设备使用情况数据；以及信息添加模块，用于在用户使用所述设备向安全验证平台发送业务请求时在所述业务请求中添加所述设备信息。

[0026] 还有另一方面，本发明提供了安全验证系统，其包括用户设备、如上所述的安全验证平台以及设备指纹库，其中所述用户设备包括如上所述的安全验证装置，并且其中，所述设备指纹库被配置为存储所述设备指纹列表。

附图说明

[0027] 本发明的前述和其他目标、特征和优点根据下面对本发明的实施例的更具体的说明将是显而易见的，这些实施例在附图中被示意。

[0028] 图 1 是根据本发明一个示例的安全验证系统的示意应用场景。

[0029] 图 2 是根据本发明一个示例的安全验证方法的示意流程图。

[0030] 图 3 是根据本发明另一示例的安全验证方法的示意流程图。

[0031] 图 4 是根据本发明一个示例的安全验证平台的示意框图。

[0032] 图 5 是根据本发明另一示例的安全验证装置的示意框图。

具体实施方式

[0033] 现在参照附图描述本发明的示意性示例，相同的附图标号表示相同的元件。下文描述的各示例有助于本领域技术人员透彻理解本发明，且各示例意在示例而非限制。图中各元件、部件、模块、装置及设备本体的图示仅示意性表明存在这些元件、部件、模块、装置及设备本体同时亦表明它们之间的相对关系，但并不用以限定它们的具体形状；流程图中各步骤的关系也不以所给出的顺序为限，可根据实际应用进行调整但不脱离本申请的保护范围。

[0034] 图 1 是根据本发明一个示例的安全验证系统的示意框图。如图 1 所示，根据本发明的安全验证系统包括安全验证平台 101、用户设备 102 以及设备指纹库 103，其中安全验证平台 101 被配置为与发卡行通信。图 1 所示的场景可以例如是无卡支付过程中的发卡环节。发卡行可以依赖于本发明所提供的安全验证平台 101 对来自用户设备 102 的发卡请求进行安全验证。也就是说，发卡行 104 可以在用户设备 102 通过安全验证平台的验证之后将用户设备 102 确定为可信设备，从而对该设备进行虚拟卡的发卡操作。

[0035] 该安全验证平台 101 可以例如同时为多个发卡行进行服务。除图 1 所示的发卡环节应用之外，该安全验证平台 101 还可以为交易环节提供验证。例如，当用户设备需要利用与该设备绑定的虚拟卡进行支付时，支付请求同样可以首先由该安全验证平台来接收，以进行设备身份验证，并且支付确认方可以依据该验证结果来判断是否执行支付操作。在实践中，该安全验证平台可以独立地实现或者被集成在任何第三方的可信服务平台中。将在下文中结合图 2 来详细描述安全验证平台 101 的操作。

[0036] 图 1 所示的用户设备 102 可以是任何硬件条件符合各机构的无卡支付条件的设备。此外，该用户设备 102 至少应具有远程通信能力，例如通过任何有线或无线的方式。举例来说，该设备可以例如是已有的或待开发的任何智能设备，例如手机、计算机、膝上型笔记本、个人数字助理（PDA）等等。

[0037] 设备指纹库 103 可以是任何已有或待开发的数据库设备或数据服务器等。本领域技术人员能够理解该设备指纹库能够如图 1 所示的那样独立地实现，也可以与安全验证平台集成，或者与其他另外的数据处理设备集成。

[0038] 图 2 是根据本发明一个示例的安全验证方法的示意流程图。该方法可以例如在图 1 所示的安全验证平台 101 中执行。以下结合图 1 所示的场景来对各步骤进行描述。

[0039] [038] 首先，在步骤 21 中，安全验证平台 101 接收来自用户的业务请求。该业务请求可以例如是用户通过其所持有的某一智能设备，例如用户设备 102 所发出的。该业务请求可以例如是向银行端发送的虚拟卡申请请求。在其他一些示例中，该业务请求也可以是交易请求，例如支付请求。

[0040] 在本发明的一些示例中，用户通过智能设备所发出的业务请求均包含用户信息以及设备信息两部分。用户信息可以例如是用户名和密码，该用户名和密码可以是由用户针对某个机构的虚拟业务所设置的。举例来说，银行可能向用户提供诸如网上银行或手机银行之类的远程客户服务，用户可能需要为使用这些服务而在本地设备上进行用户注册，这通常以用户名和密码的形式来实现。本领域技术人员能够理解用户信息还可以包括其他任何能够唯一地标识用户身份的信息。

[0041] 进一步地，设备信息至少需要包括设备硬件参数以及设备使用情况数据。

设备硬件参数包括设备本身出厂时的设备硬件基本参数及编号等任何能够唯一识别该设备的信息。在一些示例中，设备硬件参数可以例如包括国际移动设备标识 IMEI、设备的出厂序列号等等。

[0042] 设备使用情况数据是与用户应用设备的方式相关的信息。在一些示例中，设备使用情况数据包括设备的网络信息、地理位置信息以及用户偏好行为信息中的一个或多个。举例来说，设备的网络信息可以包括设备的网络连接信息、TCP 包属性、连接的路由器属性、HTTP 协议属性、WiFi 列表中的一个或多个。设备的地理位置信息可以例如是基站定位地点、GPS 定位地点、与时间相关联的轨迹及常用地中的一个或多个。设备的用户偏好行为信息可以例如是操作系统类型、版本号、偏好设置、应用安装偏好设置、闹钟时间、开关机时间、应用使用频率及时间、屏幕操作时的接触面积、滑动方向、键盘输入的时间间隔、按压力度、陀螺仪信息、加速度计信息中的一个或多个。

[0043] 在步骤 23 中，安全验证平台 101 将基于业务请求中所包含的设备信息为该设备创建当前设备指纹。设备指纹是基于设备硬件参数以及设备使用情况数据两者所构建的设备模型。设备使用情况数据可以是对该设备进行长期数据采集和统计的结果。由于加入了设备使用情况数据，依此构建的设备模型具有实时性和动态性，能够更可靠地对各个设备进行标识，消除了例如在设备被盗、遭到恶意篡改等情况下重要信息泄露、恶性邦卡、账户盗刷等的风险。

[0044] 在步骤 25 中，安全验证平台 101 还将获取设备指纹列表，该设备指纹列表包括与用户关联的所有设备的、先前存储的设备指纹。在一些示例中，该设备指纹列表被存储在设备指纹库 103 中。

[0045] 在一些示例中，先前存储的设备指纹基于设备硬件参数以及历史的设备使用情况数据生成。安全验证平台 101 可以例如在用户发送业务请求之前就从该设备接收设备使用情况数据。这些设备使用情况数据可以例如从用户为使用机构的远程服务在本地设备上开始被收集并且与设备硬件参数和用户信息一起向安全验证平台发送。安全验证平台 101 可以利用预先设计的建模算法将这些硬件信息和动态信息汇总为能够表征设备的设备指纹，并且将所生成的设备指纹与相应的用户信息一起发送至设备指纹库 103。在设备指纹库中，可以以用户信息为索引以列表的形式存储用户的每个设备的设备指纹。在实践中，一

个用户可以有一台或者多台智能设备，因此同一用户信息可以对应一个设备指纹，也可以对应多个设备指纹。

[0046] 在一些示例中，安全验证平台还可以周期性地从与用户关联的设备接收设备使用情况数据来更新所述设备指纹列表中的设备指纹。由于用户的实际情况可能发生变化，设备使用情况也可能相应地发生变化。例如用户由于居住地变化而导致设备的地理位置信息改变。通过不断接收最近的设备使用情况可以保证设备指纹的时效性，从而提供更好的用户体验。

[0047] 此外，设备指纹库还可以通过由用户直接去发卡行对设备进行现场备案来生成。设备指纹库的这种建立方式尤其适合用户在首次通过该设备针对发卡机构创建账户时要求虚拟卡绑定的情况。在另外一些示例中，安全验证平台还可以从第三方接收类似的设备信息来进行设备指纹的构建。无论在哪种情况下，在设备使用情况数据的传输过程中优选地采用单向加密传输的方式，以确保用户信息及设备信息的安全性。

[0048] 在步骤 27 中，安全验证平台 101 将所生成的当前设备指纹与设备指纹列表中的所有设备指纹进行比对，以确定发送业务请求的设备的正当性。

[0049] 在一些示例中，可以根据设备指纹所代表的设备模型中包含的所有参数进行逐项对比。这种逐项对比可以被认为是一种静态匹配。其中，参数可以包括设备硬件参数以及诸如网络信息、地理位置信息以及用户偏好行为信息的设备使用情况参数。在按各个参数进行精确匹配的过程中，可以为每个参数赋予匹配权重。如在上文中所提及的，设备指纹是一种具有动态性的设备标识，其中与设备使用情况相关的参数会随着用户状态的改变而发生变化。设备指纹库中所存储的设备指纹与当前生成的设备指纹之间在时效性上存在一定的差异，因此不一定需要每个参数都完全一致，而是可以通过权重来加以区别。进一步地，可以将当前设备指纹与列表中的每一项的各个参数的对比结果按预先分配的匹配权重进行加权平均，计算多值匹配度。最后，根据加权平均的结果，即多值匹配度来判断当前设备指纹是否与设备指纹列表中的项匹配。在一些示例中，例如可以将加权平均的结果与预先确定的阈值进行比较：如高于阈值则认为是匹配，否则认为是不匹配。

[0050] 在另外一些示例中，还可以采用动态匹配的方式。如在上文中所提及的，

设备指纹是一种具有动态性的设备标识,尤其是其中与设备使用情况相关的参数可能不断发生变化。因此,在设备指纹匹配时,除了当前值与存储值的精确匹配之外,还可以将当前值与基于以往数据的预测进行比较。在一些示例中,利用与设备指纹库集成的或独立于该设备指纹库的外部处理设备通过机器学习的方法,分析前期采集的硬件信息和设备使用情况数据,由此预测持续的设备指纹变化,并将该预测结果作为更新的设备指纹存储在设备指纹库中,用于后续的设备指纹比对。通过动态方法进行比对,可以在保证安全性的同时,大大改善用户体验,为整个业务处理过程增加便利性。此外,还可以同时地或交替地采用动态或静态的对比方式。

[0051] 在将当前设备指纹与设备指纹列表中的各项进行比对,并且确定至少有一项匹配的情况下,安全验证平台在步骤 29 中判定所收到的业务请求通过安全验证。进一步地,在图 1 所示的场景中,安全验证平台 101 会通知发卡行可以开始正常的虚拟卡发卡或绑卡操作。

[0052] 在本发明中,通过结合设备的使用情况数据来构建设备指纹,有效地解决了现有无卡支付发卡和交易环节仅基于卡号信息及手机码验证等方式的不足,大大降低了恶意绑卡及盗刷的风险。相比于生物特征信息,用户的智能设备在被盗取后可以及时由安全验证平台发觉,从而及时联系验证平台或者发卡行进行设备指纹的报失冻结或者信息的更新,并且由于采取了单向加密的保护措施,即使智能设备被盗取也不会丢失个人信息。此外,本发明所提供的方案通过加强服务器端的验证处理,使得在用户端的验证条件要求被降低。

[0053] 在一些优选示例中,除图 2 所示的步骤之外,安全验证平台 101 还可以被配置为在将当前设备指纹与设备指纹列表比对之前,将该当前设备指纹与设备指纹黑名单库进行对比。一般地,设备指纹黑名单库保存非法设备的设备指纹,这些非法设备的信息可以从外部收集也可以通过在之前的比对过程中不断积累。

[0054] 与设备指纹黑名单库的比对同样可以采用上文中就设备指纹列表比对所描述的静态和动态方法。在另外一些示例中,与设备指纹黑名单库进行对比可以是按关键设备参数的优先级逐级将所述当前设备指纹与黑名单库中的设备指纹进行比对。举例来说,关键设备参数可以是 MAC 地址、国际移动设备标识 IMEI、设备序列号以及系统标识,优先级按各项所列出的顺序为从高到低。也就是说,

在黑名单比对中，首先将当前设备指纹包含的 MAC 地址信息与黑名单库中的每个设备指纹项中的 MAC 地址信息比对。如果找到匹配，则可以将当前请求中的设备指纹判定为审核失败。如果没有找到 MAC 地址信息匹配的项，则接着比对设备序列号，以此类推。

[0055] 相比于传统的单因子体系和设备信息字符串体系的不足，采用多因子分离式认证方式，基于诸如 MAC 地址、IMEI、序列号和安卓 ID 等关键设备参数作为黑名单设备指纹因子，并根据几个设备指纹因子的唯一性和可靠性的强度优先级，构建设备指纹黑名单因子层级库。在黑名单入库阶段，会对相关指纹因子的唯一性和可靠性进行检测，并依据检测结果选择可靠的因子入黑名单因子层级库，从而提高了黑名单库的有效性。依据预先设定的可靠度优先级逐级比较，可以实现对黑名单设备的精确匹配追踪。

[0056] 在一些示例中，黑名单的建立可以按照以下原则：一次审核失败的设备指纹信息进入灰名单列表，多次审核失败的进入黑名单。此外，机构的其他业务系统也可以按照业务规则将违规的设备列入设备指纹黑名单。

[0057] 此外，黑名单列表中的设备指纹也可以进行恢复。例如，用户可以向安全验证平台提交用户资料，经过审核成功则可删除黑名单列表中用户的对应设备。

[0058] 在设备指纹列表比对之前，通过黑名单比对直接对于非法设备拒绝审核，这提高了无卡支付发卡的安全性以及高危情况下非法设备审核的效率。

[0059] 图 3 是根据本发明另一示例的安全验证方法的示意流程图。图 3 所示的安全验证方法通常可以在图 1 所示的用户设备 102 中实现，与图 2 所示的方法共同来完成本发明所提供的安全验证方案。

[0060] 如图 3 所示，首先在步骤 31 在设备处从用户获取采集设备信息的授权。接着，在步骤 33 中，依据该授权从用户的设备采集设备信息。在本发明中，所采集的设备信息至少包括设备硬件参数和设备使用情况数据两者，其中设备使用情况数据例如可以是设备的网络信息、地理位置信息以及用户偏好行为信息等等。进一步地，在步骤 35 中，当用户使用该设备向安全验证平台发送业务请求时在该业务请求中添加所采集的设备信息。

[0061] 图 3 所示的方法可以例如在用户设备上安装的应用程序(APP)中实现，或者被实现为软件开发工具包 SDK 以嵌入机构向用户设备所提供的应用程序中。举

例来说,用户为使用机构所提供的手机银行服务可能需要在手机设备上安装相应的 APP。该 APP 可以在用户创建帐户(通常包括用户名和密码)并用该帐户登录之后向用户请求授权,并在获得授权之后对设备信息进行采集。所采集的信息可以被发送至安全验证平台以为该设备创建设备指纹,无论用户是否进行任何业务请求。安全验证平台可以将所有来自同一用户账户的设备指纹信息存储为设备指纹列表,如在上文中所描述的那样。在一些示例中,用户设备上的应用程序还可以周期性地向安全验证平台传送设备使用情况数据,以供安全验证平台不断地对设备指纹库进行更新,从而有助于与之后收到的业务请求中的设备信息进行比对。

[0062] 本领域技术人员能够理解图 3 所示的方法不必须实现在用户的设备上,而可以例如由独立的第三方来实现。此外,该方法也可以任何软件或硬件的形式来实现。

[0063] [062] 总的来说,采用本发明所提供的安全验证方案对于用户使用的智能设备没有附加的功能要求,通常只需要用户授权验证方或机构方获取设备的权利,这大大提高了用户体验并且降低了各方用于设备审核的成本。

[0064] 图 4 是根据本发明一个示例的安全验证平台的示意框图。如图 4 所示,安全验证平台 400 包括数据接收模块 41, 设备指纹创建模块 43、列表获取模块 45、比对模块 47 以及判定模块。具体地,数据接收模块 41 用于接收来自用户的业务请求。在本发明中,这些业务请求就包括用户信息和设备信息两者,其中设备信息将包括设备硬件参数以及设备使用情况数据。设备指纹创建模块 43 用于基于设备信息创建当前设备指纹。在本发明中,设备指纹是基于设备硬件参数以及设备使用情况数据构建的设备模型。列表获取模块 45 用于获取设备指纹列表,该设备指纹列表包括与该用户关联的所有设备的先前存储的设备指纹。比对模块 47 用于将当前设备指纹与设备指纹列表中的各个设备指纹进行比对。判定模块 49 用于在当前设备指纹与设备指纹列表中的至少一项匹配的情况下判定所接收的业务请求通过安全验证。

[0065] 图 4 所示的安全验证平台 400 能够被配置为实现上文所描述的任何与本发明所提供的、在安全验证平台处实现的安全验证过程相关的操作。本领域技术人员能够理解,图 4 所示的模块划分仅是示意性的,这些模块能够按照具体实现来集成或进一步划分,并且以任何软件或硬件的形式来实现。

[0066] 图 5 是根据本发明另一示例的安全验证装置的示意框图。如图 5 所示，安全验证装置 500 包括授权模块 51、信息采集模块 53 以及信息添加模块 55。在实践中，该安全验证装置 500 可以被集成或安装在用户可能用来向机构发送业务请求的设备中。具体地，授权模块 51 用于在设备处从用户获取采集设备信息的授权。信息采集模块 53 用于依据所获得的授权从用户的设备采集设备信息。在本发明中，所采集的设备信息将包括设备硬件参数和设备使用情况数据两者。信息添加模块 55 用于在用户使用其设备向安全验证平台发送业务请求时在该业务请求中添加所采集的设备信息。

[0067] 图 5 所示的安全验证装置 500 能够被配置为实现上文所描述的任何与本发明所提供的安全验证过程相关的、在用户设备处实现的操作。本领域技术人员能够理解，图 5 所示的模块划分仅是示意性的，这些模块能够按照具体实现来集成或进一步划分，并且以任何软件或硬件的形式来实现。

[0068] 应当说明的是，以上具体实施方式仅用以说明本发明的技术方案而非对其进行限制。尽管参照上述具体实施方式对本发明进行了详细的说明，本领域的普通技术人员应当理解，依然可以对本发明的具体实施方式进行修改或对部分技术特征进行等同替换而不脱离本发明的实质，其均涵盖在本发明请求保护的范围内。

权 利 要 求 书

1. 一种安全验证方法，其包括：

接收来自用户的业务请求，所述业务请求包括用户信息以及设备信息；

基于所述设备信息创建当前设备指纹；

获取设备指纹列表，所述设备指纹列表包括与所述用户关联的所有设备的先前存储的设备指纹；

将所述当前设备指纹与所述设备指纹列表比对；以及

在所述当前设备指纹与所述设备指纹列表中的至少一项匹配的情况下判定所述业务请求通过安全验证，

其中所述设备信息包括设备硬件参数以及设备使用情况数据，并且所述设备指纹是基于设备硬件参数以及设备使用情况数据构建的设备模型。

2. 如权利要求 1 所述的安全验证方法，其中，所述设备使用情况数据包括设备的网络信息、地理位置信息以及用户偏好行为信息中的一个或多个。

3. 如权利要求 2 所述的安全验证方法，其中，设备的网络信息包括设备的网络连接信息、TCP 包属性、连接的路由器属性、HTTP 协议属性、WiFi 列表中的一个或多个。

4. 如权利要求 2 所述的安全验证方法，其中，设备的地理位置信息包括基站定位地点、GPS 定位地点、与时间相关联的轨迹及常用地中的一个或多个。

5. 如权利要求 2 所述的安全验证方法，其中，设备的用户偏好行为信息包括操作系统类型、版本号、偏好设置、应用安装偏好设置、闹钟时间、开关机时间、应用使用频率及时间、屏幕操作时的接触面积、滑动方向、键盘输入的时间间隔、按压力度、陀螺仪信息、加速度计信息中的一个或多个。

6. 如权利要求 1 所述的安全验证方法，其中，将所述当前设备指纹与所述设备指纹列表比对包括：

根据所述设备模型所包含的所有参数进行逐项对比；

为每个参数赋予匹配权重；

将各个参数的对比结果按所述匹配权重进行加权平均；并且

根据所述加权平均的结果来判断所述当前设备指纹是否与所述设备指纹列表中

的项匹配。

7. 如权利要求 1 所述的安全验证方法，其中，将所述当前设备指纹与所述设备指纹列表对比包括：

依据所述设备历史使用情况对所述设备指纹列表中的每个设备指纹变化进行预测；并且

将所述当前设备指纹与每个所述预测结果进行对比。

8. 如权利要求 1 所述的安全验证方法，其中，所述方法还包括在将所述当前设备指纹与所述设备指纹列表比对之前，将所述当前设备指纹与设备指纹黑名单库进行对比，其中所述设备指纹黑名单库保存非法设备的设备指纹。

9. 如权利要求 8 所述的安全验证方法，其中，与设备指纹黑名单库进行对比包括按关键设备参数的优先级逐级将所述当前设备指纹与黑名单库中的设备指纹进行比对。

10. 如权利要求 9 所述的安全验证方法，其中，所述关键设备参数包括 MAC 地址、国际移动设备标识 IMEI、设备序列号以及系统标识。

11. 如权利要求 1 所述的安全验证方法，其中，所述先前存储的设备指纹基于设备硬件参数以及历史的设备使用情况数据生成。

12. 如权利要求 1 所述的安全验证方法，其还包括周期性地从与所述用户关联的所有设备接收设备使用情况数据来更新所述设备指纹列表中的设备指纹。

13. 如权利要求 1 所述的安全验证方法，其中，所述业务请求包括发卡请求以及交易请求。

14. 如权利要求 1 所述的安全验证方法，其中，所述用户信息包括与所述业务相关联的用户名和密码。

15. 一种安全验证平台，其包括：

数据接收模块，用于接收来自用户的业务请求，所述业务请求包括用户信息以及设备信息；

设备指纹创建模块，用于基于所述设备信息创建当前设备指纹；

列表获取模块，用于获取设备指纹列表，所述设备指纹列表包括与所述用户关联的所有设备的先前存储的设备指纹；

比对模块，用于将所述当前设备指纹与所述设备指纹列表比对；以及

判定模块,用于在所述当前设备指纹与所述设备指纹列表中的至少一项匹配的情况下判定所述业务请求通过安全验证,

其中所述设备信息包括设备硬件参数以及设备使用情况数据,并且所述设备指纹是基于设备硬件参数以及设备使用情况数据构建的设备模型。

16. 一种安全验证方法,其包括:

在设备处从用户获取采集设备信息的授权;

依据所述授权从所述设备采集设备信息,所述设备信息包括设备硬件参数和设备使用情况数据;以及

在用户使用所述设备向安全验证平台发送业务请求时在所述业务请求中添加所述设备信息。

17. 如权利要求 16 所述的安全验证方法,其还包括:周期性地向所述安全验证平台传送所述设备使用情况数据。

18. 一种安全验证装置,其包括:

授权模块,用于在设备处从用户获取采集设备信息的授权;

信息采集模块,用于依据所述授权从所述设备采集设备信息,所述设备信息包括设备硬件参数和设备使用情况数据;以及

信息添加模块,用于在用户使用所述设备向安全验证平台发送业务请求时在所述业务请求中添加所述设备信息。

19. 一种安全验证系统,其包括用户设备、如权利要求 15 所述的安全验证平台以及设备指纹库,其中所述用户设备包括如权利要求 18 所述的安全验证装置,并且其中,所述设备指纹库被配置为存储所述设备指纹列表。

1/3

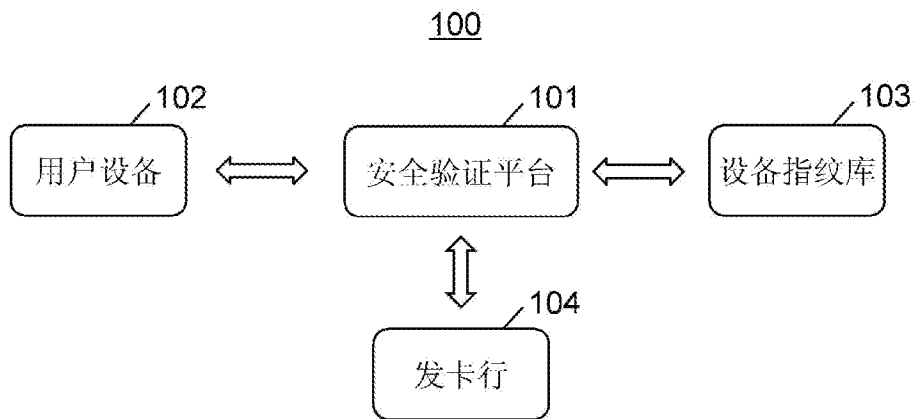


图 1

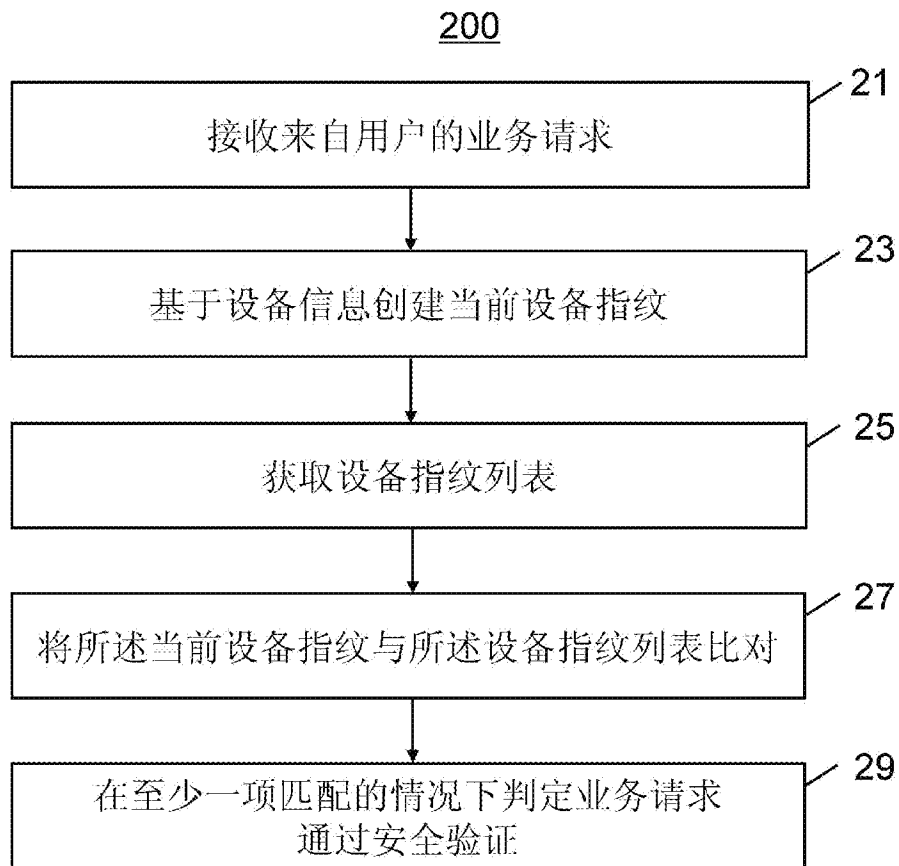


图 2

2/3

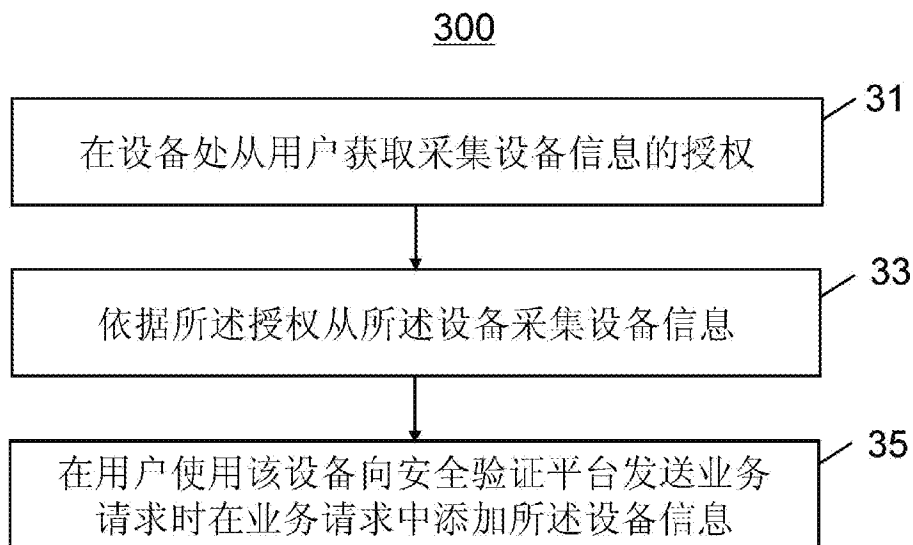


图 3

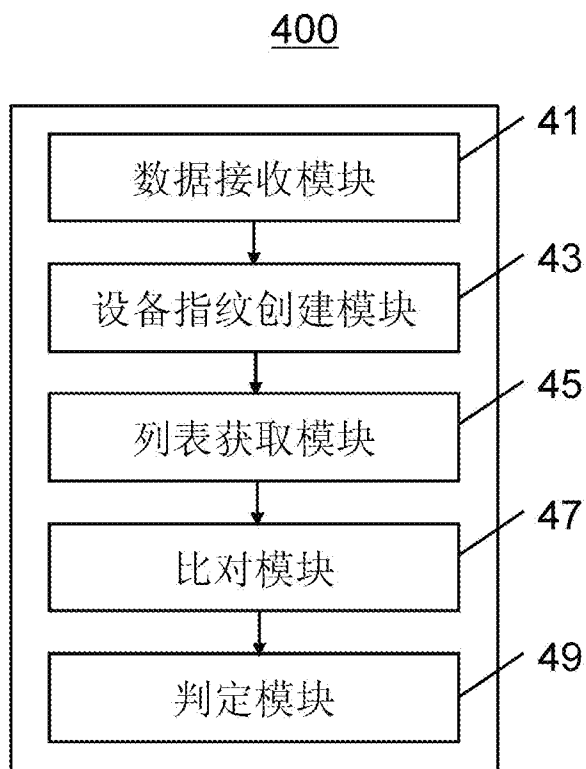


图 4

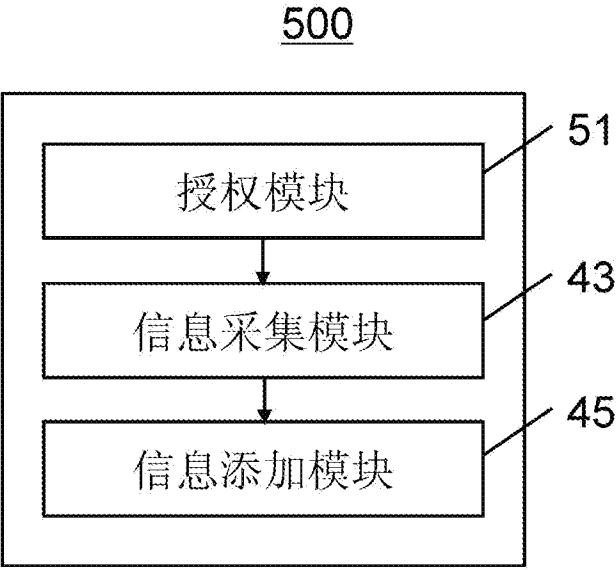


图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/117600

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44 (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; G06Q

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, CNKI, VEN: 安全, 验证, 校验, 认证, 用户, 请求, 支付, 交易, 设备, 指纹, 硬件, 比对, 对比, 比较, 匹配, safe+, security, verif+, user, request, device, fingerprint, compar+, match+, hardware

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104867011 A (CHINA TELECOM CORPORATION LIMITED), 26 August 2015 (26.08.2015), description, paragraphs [0043]-[0078]	1-19
X	CN 105144216 A (VISA INTERNATIONAL SERVICE ASSOCIATION), 09 December 2015 (09.12.2015), description, paragraphs [0056]-[0071]	1-19
PX	CN 106991317 A (CHINA UNIONPAY CO., LTD.), 28 July 2017 (28.07.2017), claims 1-19	1-19
A	CN 105989079 A (ALIBABA GROUP HOLDING LIMITED), 05 October 2016 (05.10.2016), entire document	1-19
A	CN 103186851 A (SHANGHAI PATEO ELECTRONIC EQUIPMENT MANUFACTURING CO., LTD.), 03 July 2013 (03.07.2013), entire document	1-19

☐ 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 17 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 WANG, Yue Telephone No. (86-10) 62089109

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/117600

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104867011 A	26 August 2015	None	
CN 105144216 A	09 December 2015	WO 2014145708 A1	18 September 2014
		HK 1213076 A1	24 June 2016
		JP 2016524198	12 August 2016
		AU 2014232707 A1	05 November 2015
		EP 2973276 A1	20 January 2016
		EP 2973276 A4	14 September 2016
		IN 201508894 P1	29 July 2016
		US 2014197234 A1	17 July 2014
CN 106991317 A	28 July 2017	None	
CN 105989079 A	05 October 2016	SG 11201706550 T	28 September 2017
		US 2016234211 A1	11 August 2016
		EP 3256978 A1	20 December 2017
		KR 20170116099 A	18 October 2017
		TW 201629833 A	16 August 2016
		WO 2016130374 A1	18 August 2016
		IN 201737030418 A	13 October 2017
CN 103186851 A	03 July 2013	None	

国际检索报告

国际申请号

PCT/CN2017/117600

A. 主题的分类

G06F 21/44(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; G06Q

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, CNKI, VEN: 安全, 验证, 校验, 认证, 用户, 请求, 支付, 交易, 设备, 指纹, 硬件, 比对, 对比, 比较, 匹配, safe+, security, verif+, user, request, device, fingerprint, compar+, match+, hardware

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 104867011 A (中国电信股份有限公司) 2015年 8月 26日 (2015 - 08 - 26) 说明书第[0043]-[0078]段	1-19
X	CN 105144216 A (维萨国际服务协会) 2015年 12月 9日 (2015 - 12 - 09) 说明书第[0056]-[0071]段	1-19
PX	CN 106991317 A (中国银联股份有限公司) 2017年 7月 28日 (2017 - 07 - 28) 权利要求1-19	1-19
A	CN 105989079 A (阿里巴巴集团控股有限公司) 2016年 10月 5日 (2016 - 10 - 05) 全文	1-19
A	CN 103186851 A (上海博泰悦臻电子设备制造有限公司) 2013年 7月 3日 (2013 - 07 - 03) 全文	1-19

☐ 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 17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

受权官员

王越

传真号 (86-10)62019451

电话号码 (86-10)62089109

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/117600

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	104867011	A	2015年 8月 26日	无			
CN	105144216	A	2015年 12月 9日	WO	2014145708	A1	2014年 9月 18日
				HK	1213076	A1	2016年 6月 24日
				JP	2016524198	A	2016年 8月 12日
				AU	2014232707	A1	2015年 11月 5日
				EP	2973276	A1	2016年 1月 20日
				EP	2973276	A4	2016年 9月 14日
				IN	201508894	P1	2016年 7月 29日
				US	2014197234	A1	2014年 7月 17日
CN	106991317	A	2017年 7月 28日	无			
CN	105989079	A	2016年 10月 5日	SG	11201706550T	A	2017年 9月 28日
				US	2016234211	A1	2016年 8月 11日
				EP	3256978	A1	2017年 12月 20日
				KR	20170116099	A	2017年 10月 18日
				TW	201629833	A	2016年 8月 16日
				WO	2016130374	A1	2016年 8月 18日
				IN	201737030418	A	2017年 10月 13日
CN	103186851	A	2013年 7月 3日	无			