

(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
2016 年 3 月 17 日 (17.03.2016)



(10) 国际公布号
WO 2016/037496 A1

- (51) 国际专利分类号:
G06F 21/62 (2013.01)
- (21) 国际申请号: PCT/CN2015/079817
- (22) 国际申请日: 2015 年 5 月 26 日 (26.05.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410459570.7 2014 年 9 月 10 日 (10.09.2014) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 翟征德 (ZHAI, Zhengde); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 申宇 (SHEN, Yu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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))。

(54) Title: DATA ACCESS CONTROL METHOD, DEVICE AND TERMINAL

(54) 发明名称: 一种数据访问控制方法、装置以及终端

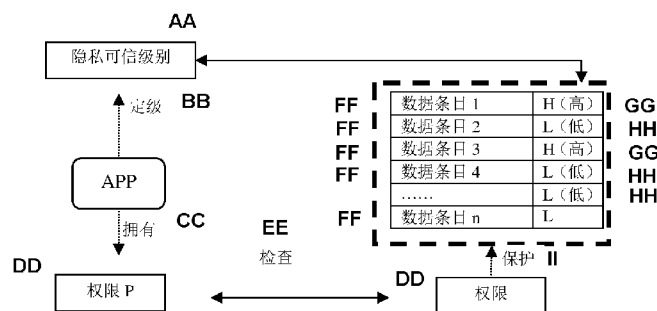


图 1 / Fig. 1

AA Privacy/trust level
BB Determine level
CC Owning
DD Permission P
EE Checking

FF Data item
GG H (high)
HH L (low)
II Protection

(57) Abstract: A data access control method, device and terminal, comprising: acquiring a data access request of a first application program APP with respect to a second application program APP, the data of the second APP comprising a plurality of data items, and each data item in the plurality of data items having respective privacy levels; determining the trust level of the first APP and the privacy level of each data item in the second APP data to be accessed by the first APP; and according to the trust level of the first APP and the privacy level of each data item, for each data item in the plurality of data items, determining a response and processing method with respect to the data request of the second APP, the response and processing method comprising one or more of the following: returning the data item requested to access by the first APP, not returning the data item requested to access by the first APP, returning a modified data item, and auditing and recording a return result.

(57) 摘要:

[见续页]

一种数据访问控制方法、装置以及终端，包括获取第一应用程式 APP 对第二应用程序 APP 的数据访问请求，所述第二 APP 的数据包括多个数据条目，所述多个数据条目中的各数据条目具有各自的隐私级别；确定所述第一 APP 的可信级别以及所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别；根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中各数据条目，确定对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

一种数据访问控制方法、装置以及终端

技术领域

本发明涉及数据访问安全管理领域，特别是涉及一种数据访问控制方法、装置以及终端。

背景技术

智能终端上存储了诸多个人数据，包括通信录、短信、通话记录、照片、视频等，这些个人数据构成了用户重要的个人信息资产。每类个人数据中(如通信录)通常都包含了很多数据条目（如多个联系人、多条短信、多张图片等），所有这些数据条目受到同一个系统权限的保护。系统权限(Permissions)是操作系统提供的一种资源限制机制，应用程序（APP）必须取得相应的权限才能访问特定受保护的数据（如通信录）或者执行某些业务功能（如访问网络）。如果 APP 拥有相应的权限，则访问到某类数据中的所有数据条目。然而，同一 APP 下的所有数据条目，例如联系人，具有不同的敏感级别，按照现有的权限控制方式就容易造成，安全级别不高的另一个 APP 读取到该 APP 下的所有数据条目，包括其中的高敏感级别的数据条目，这样容易造成终端用户高敏感数据的泄露或者被恶意窃取。

发明内容

有鉴于此，本发明实施例提供一种有效防止应用程序下的高敏感级别的数据条目泄露或被窃取的数据访问控制方法、装置以及终端。

本发明实施例第一方面提供一种数据访问控制方法、装置以及终端，包括获取第一应用程式 APP 对第二应用程序 APP 的数据访问请求，所述第二 APP 的数据包括多个数据条目，所述多个数据条目中的各数据条目具有各自的隐私级别；确定所述第一 APP 的可信级别以及所述第一 APP 要访问的

第二 APP 数据下各数据条目的隐私级别；根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中每一数据条目，确定对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

结合第一方面，在第一方面的第一种可能的实现方式中，所述第二 APP 数据的多个数据条目分为一种或多种数据类型，所述数据类型是指描述对象相同的数据。

10 结合第一方面或第一方面的第一种可能，在第一方面的第二可能的实现方式中，所述获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求包括获取第一應用程式 APP 对第二应用程序 APP 的同一类型数据的访问请求。

结合第一方面或第一方面的第一种或第二种可能，在第一方面的第三种可能的实现方式中，所述确定所述第一 APP 的可信级别包括：根据所述第一 APP 的来源以及是否具有联网权限确定所述第一 APP 的可信级别。

结合第一方面或第一方面的第一至第三种可能中的任意一种可能，在第一方面的第四种可能的实现方式中，所述 APP 来源包括预装系统软件、用户信任的应用市场（APP Market）以及其它来源，其中可信级别由预装系统软件、用户信任的应用市场（APP Market）到其它来源依次降低。

结合第一方面或第一方面的第一至第四种可能中的任意一种可能，在第一方面的第五种可能的实现方式中，所述确定所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别包括：手动设置各个数据条目的隐私级别或者根据不同 APP 数据之间的关联关系确定隐私级别，其中所述关联关系包括数据产生地点或时间相同的数据条目以及来自同一个联系人的数据条目。

结合第一方面或第一方面的第一至第五种可能中的任意一种可能,在第一方面的第六种可能的实现方式中,所述根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别,针对所述多个数据条目中各数据条目,确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式包括:

- 5 当所述第一 APP 的可信级别高于或等于其需要访问的数据条目的隐私级别时,所述回应以及处理方式为返回所述第一 APP 请求访问的数据条目;

当所述第一 APP 的可信级别低于其需要访问的数据条目的隐私级别时,所述回应以及处理方式不予返回所述第一 APP 请求访问的数据条目或者返回修改后的数据条目,其中修改后的数据条目包括虚假数据或者混淆数据。

- 10 结合第一方面或第一方面的第一至第六种可能中的任意一种可能,在第一方面的第七种可能的实现方式中,所述第二 APP 包括第一通信录以及第二通信录,所述第一通信录或第二通信录包括多个数据条目,各数据条目对应为一联系人信息,其中所述第一通信录存储的联系信息的隐私级别高于所述第二通信录存储的联系人信息的隐私级别。

- 15 结合第一方面或第一方面的第一至第七种可能中的任意一种可能,在第一方面的第八种可能的实现方式中,所述根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别,确定对所述第二 APP 的数据请求的回应以及处理方式包括:

- 20 确定所述第一 APP 的可信级别,如果所述第一 APP 属于高可信级别,则所述回应以及处理方式为返回第一通信录的联系人信息或者返回所述第一、第二通信录的所有联系人信息;

如果所述第一 APP 属于中或低可信级别,则所述回应以及处理方式仅为返回第二通信录的联系人信息或者不返回联系人信息。

- 25 本发明实施例第二方面提供一种智能终端,包括一访问控制模块以及隐私控制模块,其中:所述访问控制模块用于获取第一应用程序 APP 对第二应用程序 APP 的数据访问请求,所述第二 APP 的数据包括多个数据条目,

所述多个数据条目中的各数据条目具有各自的隐私级别；所述隐私控制模块用于确定所述第一 APP 的可信级别以及所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别；所述访问控制模块还用于根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中每一数据条目，确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

本发明实施例第三方面提供一种智能终端，包括处理器以及存储器，其特征在于，所述存储器存储有第二 APP 的数据下的多个数据条目、所述多个数据条目中各数据条目的隐私级别以及所述第一 APP 的可信级别；所述处理器获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求，并据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中每一数据条目，确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

本方案提供了一种对智能终端上 APP 中受到相同权限保护的个人信息数据中的不同数据条目按照其各自对用户而言的敏感性进行隐私分级并进行保护，解决现有权限机制粒度过粗而不能有效保护个人信息数据中某些敏感条目的问题，有效防止第三方 APP 收集和泄露这些敏感数据，同时又不影响 APP 的正常业务功能。

本发明实施例的优点将会在下方的说明书中部分阐明，一部分根据说明书是显而易见的，或者可以通过本发明实施例的实施而获知。

附图说明

图1为本发明实施例一中應用程式APP可信级别以及数据条目隐私级别管理的示意图。

图2为本发明实施例一中数据访问控制方法流程示意图。

图3为本发明实施例一中数据条目之间关联关系的示意图之一。

5 图4为本发明实施例一中数据条目之间关联关系的示意图之二。

图5为本发明实施例一中数据条目之间关联关系的示意图之三。

图6为本发明实施例二中智能终端的模块示意图。

图7为本发明实施例三中智能终端的硬件结构示意图。

10 具体实施方式

以下所述是本发明实施例的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本发明实施例的保护范围。

在当前的终端应用中，有些文件类型，如图片文件，在一些系统上没有明确的系统权限保护，但它们明显是同一类文件，此时可以认为他们受到同一个特殊的”读图片”(permissions.picture.read)权限保护，而所有应用程序(APP)都缺省具有此权限。通常情况下，某类个人数据中的大部分条目(例如大部分的联系人、大部分的照片)都不是特别敏感的(例如一般性联系人，一般性风景照片等)，而有些数据条目可能是很敏感的，例如
15 通信录中一些特殊的联系人记录如工作上司、生意伙伴、政界人士、其它公众人士朋友等，短信记录及通话记录中与上述特殊敏感联系人的短信和电话来往记录，照片中的家人照片等。

终端上运行的APP在很多情况下都需要读取终端中某一类或者某几类个人数据中的部分信息条目(如部分联系人、部分短信、部分照片)以便执行
25 正常的业务功能，例如微信需要读取用户的手机通信录以便为用户搜索好友，很多社交应用都需要读取用户终端中的部分图片以便进行分享。目前

终端上的 APP 在安装时都会申请各种访问权限(例如读取通信录的权限), 用户如果希望使用该 APP, 则必须同意授予 APP 所申请的访问权限, APP 一旦获得对应的权限则可以不受限制的读取某一类或者几类个人数据中的所有条目。例如, APP 一旦被授予了 `Android.permission.READ_CONTACTS` 权限, 则它可以随意读取所有的通信录联系人以及所有的通话记录, 或者 APP 一旦被授予了 `android.permission.READ_SMS` 权限, 则可以随意读取所有的短信记录, 或者 APP 如果取得了 `com.android.browser.permission.READ_HISTORY_BOOKMARKS` 权限则可以访问则可以读取浏览器历史记录。然而 APP 在一般情况下, 并不需要读取所有的个人数据条目, 例如大部分终端用户一般不会把自己通信录中的工作上司或者生意伙伴加为微信好友; 很多基于地理位置的应用都支持基于通信录的地理位置分享功能, 但用户一般不会跟通信录中的父母、工作上司等进行位置分享; 淘宝需要读取来自指定平台的短信以获取验证码, 而不需要读取其它的短信记录。

APP 以编译代码的形式在用户终端上运行, 用户通常难以得知其内部的程序逻辑, 例如 APP 如何对用户个人数据进行处理, 是否会把部分个人数据发送到网络上等。根据目前的研究分析, APP 普遍存在过度收集用户个人数据的情况。例如 2014 年 2 月, MetaIntell 公司对 500 个最流行的 Android APP 进行测试, 发现 92% 的程序存在用户个人数据泄露行为; 2013 年 12 月 HP 公司发布测试报告, 一个用户平均使用 26 个 APP, 其中平均 97% 程序存在隐私问题。这些 APP 可能过度收集用户智能终端中的联系人、短信、通话记录、照片等, 特别是部分敏感的数据条目, 这对用户的个人隐私构成了严重的威胁。

针对智能终端上系统权限过于粗略而难以针对个人信息中某些特别敏感的数据条目进行保护的现状, 对智能终端上每个权限覆盖保护的同一类数据中的不同数据条目按照其各自对用户而言的敏感性进行隐私分级, 使

每个数据条目都有相应的隐私敏感级别以标识其敏感性，通过隐私限制确保只有可信级别或程度高的 APP 才能读取到终端上的敏感个人数据条目，使得用户可以精确管理和控制第三方 APP 对部分用户敏感数据的访问和收集。

5 如图 1 所示，在智能终端上，每类用户个人数据都为对应的权限所保护，本方案对智能终端 APP 中受到相同权限保护的同一类数据中的不同数据条目按照其各自对用户而言的敏感性进行隐私分级，使得数据条目都有相应的隐私敏感级别以反映其对用户而言的敏感性。这里每个数据条目都需要有相应的隐私级别信息，但这些信息未必直接与对应的数据条目存储在一起，隐私级别可能从其它信息中推导出来，如不同的存储位置。为了降低用户的管理代价，数据条目的隐私敏感级别可以按照系统提供的推导规则进行自动推导确定并由用户进行自主调整。对系统中的 APP 按照其隐私可信性进行分级，基于其所拥有的权限及其来源对其评估并确定其隐私可信级别。当拥有对应访问权限的 APP 并试图读取某类个人数据时，在系统缺省的权限检查通过之后，对该类个人数据中的每个数据条目检查其隐私敏感级别与 APP 的隐私可信级别的关系，根据两个级别的差异关系决定当前数据条目在应用程序访问结果集中的可见性和呈现形式。这里可以采用的策略可以是：不予返回、返回虚假数据、返回混淆数据、访问审计、不加限制等。这称为隐私限制策略。

20 **实施例一**

如图 2 所示，本发明实施例提供一种数据访问控制方法，所述方法包括以下步骤：

步骤 101、获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求，所述第二 APP 的数据包括多个数据条目，所述多个数据条目中的各数据条目具有各自的隐私级别；

步骤 102、确定所述第一 APP 的可信级别以及所述第一 APP 要访问的

第二 APP 数据下各数据条目的隐私级别;

步骤 103、根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别, 针对所述多个数据条目中各数据条目, 确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式, 所述回应以及处理方式包括返回
5 所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目、不加限制而直接返回隐私级别低于所述第一 APP 可信级别的数据条目以及审计并记录返回结果中的一种或多种方式。

步骤 101 中, 所述第一 APP 包括各种来源的安装软件, 如来自系统软件、应用市场 (APP Market) 以及其它来源等软件。所述第二 APP 可以是
10 短信信息、通信录、相册等等具有多个数据条目的应用程序。所述第一 APP 通常在安装或者启动的时候需要调用其它 APP 的数据的时候发起的访问请求。

在一些实施例中, 所述第二 APP 数据的多个数据条目分为一种或多种
15 数据类型, 所述数据类型是指描述对象相同的数据, 例如联系人、短信、通话记录、照片为不同类型的数据。所述获取第一应用程序 APP 对第二应用程序 APP 的数据访问请求包括获取第一应用程序 APP 对第二应用程序 APP 的同一类型数据的访问请求。

步骤 102 中, 确定所述第一 APP 的可信级别包括: 根据所述第一 APP
20 的来源以及是否具有联网权限确定所述第一 APP 的可信级别, 其中所述 APP 来源包括预装系统软件、用户信任的应用市场 (APP Market) 以及其它来源, 其中可信级别由预装系统软件、用户信任的应用市场 (APP Market) 到其它来源依次降低。例如, APP 可信级别反应了用户对于该 APP 不会泄露用户个人数据的确信程度, 它可以通过客观的标准进行度量, 也可以由
25 用户主观指定。本发明实施方式中使用一种客观的可信级别评估方法, 该方法主要基于 APP 的来源和 APP 是否具有联网权限进行分类并指定可信级

别。这种 APP 的隐私可信级别评定，可以在云端执行并下发到终端上。

其中，是否具有联网权限是影响 APP 隐私可信级别的重要因素，一款没有联网权限的 APP 自己是不可能泄露用户隐私的，APP 如果具有了联网权限，就具有泄露用户隐私的基本能力。这里定义所有 APP 的集合为 ALL，
5 所有不具有联网权限的 APP 的集合为 PLAIN，具有联网权限的 APP 的集合为 NET，显然 $ALL=PLAIN+NET$ 。

APP 的来源反应了该 APP 是从何处获得的，也即 APP 的提供者。可信提供者提供的 APP 通常相对较为可信。APP 按照其来源可以分为以下几类：

1) 预装的系统软件（定义为 SYS），这些 APP 是设备制造商在出厂时
10 预装的不可卸载的系统软件，这些软件构成了终端系统的一部分，有明确的软件责任归属，具有最好的来源可信性。

2) 来自用户信任的 APP Market(如 Google Play)或者网站(如 Baidu.com) 的 APP，这里定义其集合为 MARKETS。

3) 其它来源的 APP，定义为 OTHERS。

15 对于一款 APP（设为 a），其隐私可信级别 $L(a)$ 定义如下：

a) $L(a)=H$ （高）当且仅当 $a \in PLAIN \cup SYS$ ，即系统软件或者无联网权限软件的隐私信任级别可以为 H。

b) $L(a)=M$ （普通）当且仅当 $a \in MARKETS$ ，即用户从可信提供者处获得 APP 其隐私可信级别可以为 M。

20 c) $L(a)=L$ （低）当且仅当 $a \in OTHERS \cap NET$ ，上述两种情况之外的 APP，其隐私可信级别都为 L。

步骤 102 中，确定所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别包括：手动设置各个数据条目的隐私级别或者根据根据不同 APP 数据之间的关联关系确定隐私级别，其中所述关联关系包括数据产生
25 地点或时间相同的数据条目以及来自同一个联系人的数据条目。

例如，智能终端中，不同类别的个人数据条目之间往往具有内在的关联

关系，例如图 3 所示，如果一条通话记录或者短信记录的通讯主体正好是通信录中的某个联系人，则该条通话记录或者短信记录与该联系人存在关联关系；如果一张照片是在某个地理位置上拍摄的，则这张照片与该地理位置存在关联关系。

- 5 本专利中使用这种关联关系来自动推导某些数据条目的隐私敏感级别，避免用户逐条设置所有个人数据条目的隐私敏感性，降低用户管理代价。假设用户已经指定联系人 A 的隐私敏感级别是 H，系统可以自然地计算出与 A 的某条短信记录或者某条通话记录的隐私敏感级别可以自动设定为 H，该联系人 A 的邮件也可以自动标记为 H。当然用户对系统自动推导的个人
- 10 数据条目的隐私敏感级别具有最终控制权，可以基于自动推导的结果进行手动调整。

- 例如图 4 所示，智能终端上的照片、录音、录制的视频等产生于某个地理位置上，地理位置界定了这些数字内容产生的外部环境和可能的内容范围。如果某个地理位置区域是敏感的，则该该地理位置上产生的照片、录
- 15 音和录制的视频等都潜在是敏感的。由此可以从地理位置区域的敏感级别出发自动推导在该位置区域上产生的照片、录音、录制的视频等的敏感级别。

- 对于通信录联系人和地理位置，用户需要去指定对应的隐私敏感级别。一般情况下，终端系统中大部分的通信录联系人和地理位置都是不敏感的，其可以被自动分配一个缺省级别，该缺省级别在系统的隐私限制策略数据库中进行定义。个别敏感的联系或者地理位置可以由用户通过管理模块
- 20 进行管理指定。在用户指定了通信录联系人的敏感级别和各个地理位置的敏感级别（可以通过地图指定）后，智能终端中的大部分个人数据条目都可以自动推导出来。

- 25 例如图 5 所示，另外一种可能的关联关系是基于时间关联的，如用户把某一段时间定义成敏感的(例如参加机密会议)，则在此时间段内终端上产生

的所有电子文档、邮件和浏览器访问记录等都会被自动标记成隐私敏感的。

步骤 103 中，根据所述第一 APP 的可信级别以及所述多条数据条目的隐私级别，针对所述多个数据条目中各数据条目，确定对所述第二 APP 的数据请求的回应以及处理方式，针对每一条数据条目的隐私级别去判断对该条数据条目的访问回应方式，可见隐私控制的粒度是在每一条数据条目，逐一对每一个数据条目进行隐私级别确定，而不是整个 APP 的数据，从而提高数据访问隐私控制的精细度。例如，隐私限制策略数据库记录访问个人数据的 APP 的隐私可信级别与数据条目的隐私敏感性的各种不同差异关系下，数据条目在 APP 访问数据结果返回集中的表现形式。其可能的结果有：

- a) 不予返回，在访问结果集中不包含该数据条目；
- b) 虚假数据，访问结果集中包含一条虚假的数据条目来代替该条目；
- c) 混淆数据，访问结果集中包含该数据条目，但该数据条目的部分字段或者内容经过混淆处理；
- d) 访问审计：系统对此次访问进行审计记录；
- e) 不加限制：在访问结果集中包含该数据条目。

与传统的各种访问控制方法不同，本方案中根据当前 APP 隐私可信级别与待访问数据条目的隐私敏感级别的不同差异（这种差异可能有多种情况）采取不同的限制手段。这种不同差异反应了当前这种访问行为自身的敏感性，需要不同的控制手段，这可以进一步避免过度限制和降低了冗余信息（审计日志等）的生成。例如对于一条敏感级别为 H(高度敏感)的联系人记录(一大公司高管)，一个隐私可信级别为 L(不可信)的 APP 来读取时，系统可能返回虚假数据条目并且进行审计，而一个可信级别为 M(较为可信)的 APP 来读取同一条目时，可能只需要返回虚假条目而无需审计（甚至可能是返回混淆数据）。本专利中，根据当前 APP 隐私可信级别与待访问数据条目的隐私敏感级别的不同差异采用不同的限制手段，以帮助用户进一步

避免过度限制和降低了冗余信息（审计日志等）的产生。

按照本方法，如果一个联系人是高度隐私敏感的，则一般的 APP（如微信）都无法读取到这样的联系人。这在绝大部多数情况下都是用户所预期的，因为用户一般不会与这样的联系人进行各种社交联系和分享。如果在极特殊的情况下，用户确实希望把这个联系人加为微信好友，则他需要手动输入联系人的号码进行添加。这种情况下，由于 APP 只得到一个号码而不能获得该联系人的任何其他信息（如姓名），本方法最大程度的保护了用户的隐私。

可见，根据第一 APP 的可信级别以及其需要访问的第二 APP 数据条目的隐私级别，确定所述访问的回应方式以及结果。例如，当所述第一 APP 的可信级别高于或等于其需要访问的数据条目的隐私级别时，如当所述第一 APP 的可信级别为 H，则第一 APP 要访问的第二 APP 的数据条目的隐私级别无论是 H、M 或者 L，回应以及处理方式都是返回所述第一 APP 请求访问的数据条目；当所述第一 APP 的可信级别低于其需要访问的数据条目的隐私级别时，如当所述第一 APP 的可信级别为 M，第一 APP 要访问的第二 APP 的数据条目的隐私级别为 H，则所述回应以及处理方式不予返回所述第一 APP 请求访问的数据条目或者返回修改后的数据条目，其中修改后的数据条目包括虚假数据或者混淆数据；其中返回以及处理方式可以包括审计以及记录返回结果，如可以设定当隐私级别为 H 的数据条目被访问时，审计并记录访问以及返回结果。

在本发明某些实施例中，所述第二 APP 包括第一通信录以及第二通信录，所述第一通信录或第二通信录包括多个数据条目，各数据条目对应为一联系人信息，其中所述第一通信录存储的联系信息的隐私级别高于所述第二通信录存储的联系信息的隐私级别，例如，一些比较重要的联系人信息放在第一通信录，一些普通或者不重要的联系人信息放在第二通信录。其中所述根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，

确定对所述第二 APP 的数据请求的回应以及处理方式包括:

确定所述第一 APP 的可信级别, 如果所述第一 APP 属于高可信级别, 则所述回应以及处理方式为返回第一通信录的联系人信息或者返回两个通信录的所有联系人信息;

- 5 如果所述第一 APP 属于中或低可信级别, 则所述回应以及处理方式为仅返回第二通信录的联系人信息或者不返回联系人信息。

本方案提供了一种对智能终端上每个保护用户个人数据的权限所覆盖的同一类或者同一 APP 个人数据中的不同数据条目按照其各自对用户而言的敏感性进行隐私分级并进行保护, 解决现有权限机制粒度过粗而不能有效保护个人数据中某些敏感条目的问题, 有效防止第三方 APP 收集和泄露这些敏感数据, 同时又不影响 APP 的正常业务功能; 另外还给予用户一种
10 相对于终端系统自身的权限管理措施更为精细化的个人数据的管理、控制和保护方式, 同时不改变原有的数据保存和展现模式, 保持用户原有的终端使用体验。

15 实施例二

如图 6 所示, 本发明另一实施例涉及一种智能终端, 所述智能终端包括一访问获取模块、隐私控制模块以及访问控制模块, 其中:

所述访问获取模块用于获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求, 所述第二 APP 的数据包括多个数据条目, 所述多个数据条
20 目中的各数据条目具有各自的隐私级别;

所述隐私控制模块用于确定所述第一 APP 的可信级别以及所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别;

所述访问控制模块还用于根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别, 针对所述多个数据条目中各数据条目, 确定所述第一
25 APP 对所述第二 APP 的数据请求的回应以及处理方式, 所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP

请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

所述隐私控制模块用于根据所述第一 APP 的来源以及是否具有联网权限确定所述第一 APP 的可信级别。其中所述 APP 来源包括预装系统软件、
5 用户信任的应用市场 (APP Market) 以及其它来源, 其中可信级别由预装系统软件、用户信任的应用市场 (APP Market) 到其它来源依次降低。

所述隐私控制模块用于手动设置各个数据条目的隐私级别或者根据根据不同 APP 数据之间的关联关系确定隐私级别, 其中所述关联关系包括数据产生地点或时间相同的数据条目以及来自同一个联系人的数据条目。

10 所述访问控制模块还用于: 当所述第一 APP 的可信级别高于或等于其需要访问的数据条目的隐私级别时, 所述回应以及处理方式为返回所述第一 APP 请求访问的数据条目;

当所述第一 APP 的可信级别低于其需要访问的数据条目的隐私级别时, 所述回应以及处理方式不予返回所述第一 APP 请求访问的数据条目或者返
15 回修改后的数据条目, 其中修改后的数据条目包括虚假数据或者混淆数据。

本发明实施例中的智能终端还包括隐私限制策略数据库、应用信息级别数据表(库)以及带有敏感级别标记的个人数据 (通信录、照片)。其中访问控制模块是智能终端操作系统缺省的权限检查模块, 用来检查一款应用是否具有访问某类个人数据所具有的权限。对于个人数据条目, 这里使用 H
20 代表高隐私敏感级别, M 代表中等敏感级别, L 代表不敏感。对于 APP, 这里 H 代表高隐私可信度, M 代表中等隐私可信度, L 代表一般可信度。

应用信任级别表(库)记录系统中的每个 APP 的隐私可信级别, 关于如何计算每个 APP 的隐私可信级别章节 2.2.2 中详述。隐私限制策略数据库记录访问个人数据的 APP 的隐私可信级别与数据条目的隐私敏感性的各种不同
25 差异关系下数据条目可见性以及其隐私限制。所述数据条目 (通信录条目和照片上等) 的隐私敏感级别可以通过实施例一所述的关联方式进行关联

系统规则自动推导并由用户负责调整。

所述数据条目隐私敏感级别可以记录在文件属性中或者数据表的冗余字段中，也可以在系统中使用新的数据库来存储这些信息，图中只是一种实现范例。应用的隐私可信级别可以通过专门的数据库记录或者每次运行时动态评估。隐私控制模块根据当前 APP 的隐私信任级别、待访问数据条目的隐私敏感级别、系统访问策略进行隐私保护控制。用户通过管理模块管理个人数据条目的隐私敏感级别和 APP 的隐私可信级别，并指定系统的隐私限制策略。

系统的执行流程如下：

10 1)用户首先通过管理模块对个人数据条目的隐私敏感级别、APP 的隐私可信级别以及系统的隐私限制策略进行管理；

2)隐私控制模块进行初始化，读取所有应用的隐私信任级别，并加载系统的隐私限制策略；

15 3)APP 通过用户程序接口（API）发起对某种个人数据的访问，系统缺省的访问控制模块拦截该访问请求，检查是否拥有访问该类个人数据的权限（权限 P），如果没有则系统拒绝访问；如果有，流程继续执行；

4)访问控制模块修改 API 的执行过程或拦截 API 返回的数据结果集，逐条比对数据条目的敏感级别与当前 APP 的隐私可信级别，根据隐私限制策略对结果集中的数据条目进行处理；

20 5)API 调用返回，应用取得经过隐私限制模块处理过的个人数据。

实施例三

如图 7 所示，本发明又一实施例中的智能终端包括处理器以及存储器，所述存储器存储有第二 APP 的数据下的多个数据条目、所述多个数据条目中各数据条目的隐私级别以及所述第一 APP 的可信级别；

25 所述处理器获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求，并据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对

所述多个数据条目中各数据条目，确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

- 5 本实施例中的智能终端的存储器中存储有执行实施例一的方法步骤中的数据以及相关策略，可以执行实施例一中的所有方法步骤。

本发明是参照根据本发明实施例的方法、装置（设备）和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、
10 嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

- 15 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

20 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

- 25 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和

修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

5

权利要求

1、一种数据访问控制方法，其特征在于，包括

获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求，所述第二 APP 的数据包括多个数据条目，所述多个数据条目中的各数据条目具有各自的隐私级别；

确定所述第一 APP 的可信级别以及所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别；

根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中各数据条目，确定对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

2、如权利要求 1 所述的数据访问控制方法，其特征在于，所述第二 APP 数据的多个数据条目分为一种或多种数据类型，所述数据类型是指描述对象相同的数据。

3、如权利要求 2 所述的数据访问控制方法，其特征在于，所述获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求包括获取第一應用程式 APP 对第二应用程序 APP 的同一类型数据的访问请求。

4、如权利要求 1 至 3 任一项所述的数据访问控制方法，其特征在于，所述确定所述第一 APP 的可信级别包括：根据所述第一 APP 的来源以及是否具有联网权限确定所述第一 APP 的可信级别。

5、如权利要求 4 所述的数据访问控制方法，其特征在于，所述 APP 来源包括预装系统软件、用户信任的应用市场（APP Market）以及其它来源，其中可信级别由预装系统软件、用户信任的应用市场（APP Market）到其它来源依次降低。

6、如权利要求 1 至 3 任一项所述的数据访问控制方法，其特征在于，

所述确定所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别包括：手动设置各个数据条目的隐私级别或者根据不同 APP 数据之间的关联关系确定隐私级别，其中所述关联关系包括数据产生地点或时间相同的数据条目以及来自同一个联系人的数据条目。

- 5 7、如权利要求 1 至 3 任一项所述的数据访问控制方法，其特征在于，所述根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中各数据条目，确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式包括：

当所述第一 APP 的可信级别高于或等于其需要访问的数据条目的隐私
10 级别时，所述回应以及处理方式为返回所述第一 APP 请求访问的数据条目；

当所述第一 APP 的可信级别低于其需要访问的数据条目的隐私级别时，所述回应以及处理方式不予返回所述第一 APP 请求访问的数据条目或者返回修改后的数据条目，其中修改后的数据条目包括虚假数据或者混淆数据。

- 8、如权利要求 1 至 3 任一项所述的数据访问控制方法，其特征在于，
15 所述第二 APP 包括第一通信录以及第二通信录，所述第一通信录或第二通信录包括多个数据条目，各数据条目对应为一联系人信息，其中所述第一通信录存储的联系信息的隐私级别高于所述第二通信录存储的联系人信息的隐私级别。

- 9、如权利要求 8 所述的数据访问控制方法，其特征在于，所述根据所
20 述所述第一 APP 的可信级别以及所述各数据条目的隐私级别，确定对所述第二 APP 的数据请求的回应以及处理方式包括：

确定所述第一 APP 的可信级别，如果所述第一 APP 属于高可信级别，则所述回应以及处理方式为返回第一通信录的联系人信息或者返回所述第一、第二通信录的所有联系人信息；

- 25 如果所述第一 APP 属于中或低可信级别，则所述回应以及处理方式为仅返回第二通信录的联系人信息或者不返回联系人信息。

10、一种智能终端，其特征在于，包括访问获取模块、隐私控制模块以及访问控制模块，其中：

所述访问获取模块用于获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求，所述第二 APP 的数据包括多个数据条目，所述多个数据条目中的各数据条目具有各自的隐私级别；

所述隐私控制模块用于确定所述第一 APP 的可信级别以及所述第一 APP 要访问的第二 APP 数据下各数据条目的隐私级别；

所述访问控制模块用于根据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中各数据条目，确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

11、如权利要求 10 所述的智能终端，其特征在于，所述第二 APP 数据的多个数据条目分为一种或多种数据类型，所述数据类型是指描述对象相同的数据。

12、如权利要求 11 所述的智能终端，其特征在于，所述访问获取模块具体用于获取第一應用程式 APP 对第二应用程序 APP 的同一类型数据的访问请求。

13、如权利要求 10 至 12 任一项所述的智能终端，其特征在于，所述隐私控制模块用于根据所述第一 APP 的来源以及是否具有联网权限确定所述第一 APP 的可信级别。

14、如权利要求 13 所述的智能终端，其特征在于，所述 APP 来源包括预装系统软件、用户信任的应用市场（APP Market）以及其它来源，其中可信级别由预装系统软件、用户信任的应用市场（APP Market）到其它来源依次降低。

15、如权利要求 10 至 12 任一项所述的智能终端，其特征在于，所述隐私控制模块用于手动设置各个数据条目的隐私级别或者根据根据 APP 数据之间的关联关系确定隐私级别，其中所述关联关系包括数据产生地点或时间相同的数据条目以及来自同一个联系人的数据条目。

5 16、如权利要求 10 至 12 任一项所述的智能终端，其特征在于，所述访问控制模块具体用于：

当所述第一 APP 的可信级别高于或等于其需要访问的数据条目的隐私级别时，所述回应以及处理方式为返回所述第一 APP 请求访问的数据条目；

10 当所述第一 APP 的可信级别低于其需要访问的数据条目的隐私级别时，所述回应以及处理方式不予返回所述第一 APP 请求访问的数据条目或者返回修改后的数据条目，其中修改后的数据条目包括虚假数据或者混淆数据。

17、如权利要求 10 至 12 任一项所述的数据访问控制方法，其特征在于，所述第二 APP 包括第一通信录以及第二通信录，所述第一通信录或第二通信录包括多个数据条目，各数据条目对应为一联系人信息，其中所述第一通信录存储的联系信息的隐私级别高于所述第二通信录存储的联系人信息的隐私级别。

18、如权利要求 17 所述的数据访问控制方法，其特征在于，所述访问控制模块还用于：确定所述第一 APP 的可信级别，如果所述第一 APP 属于高可信级别，则所述回应以及处理方式为返回第一通信录的联系人信息或者返回两个通信录的所有联系人信息；

如果所述第一 APP 属于中或低可信级别，则所述回应以及处理方式为仅返回第二通信录的联系人信息或者不返回联系人信息。

19、一种智能终端，包括存储器以及处理器，其特征在于，所述存储器存储有第二 APP 的数据下的多个数据条目、所述多个数据条目中各数据条目的隐私级别以及所述第一 APP 的可信级；

所述处理器用于获取第一应用程序 APP 对第二应用程序 APP 的数据访

问请求，并据所述第一 APP 的可信级别以及所述各数据条目的隐私级别，针对所述多个数据条目中各数据条目，确定所述第一 APP 对所述第二 APP 的数据请求的回应以及处理方式，所述回应以及处理方式包括返回所述第一 APP 请求访问的数据条目、不予返回所述第一 APP 请求访问的数据条目、
5 返回修改后的数据条目以及审计并记录返回结果中的一种或多种方式。

20、如权利要求 19 所述的智能终端，其特征在于，所存储器存储的第一 APP 的可信级别可以根据所述第一 APP 的来源以及是否具有联网权限确定。

21、如权利要求 20 所述的智能终端，其特征在于，所述 APP 来源包括
10 预装系统软件、用户信任的应用市场（APP Market）以及其它来源，其中可信级别由预装系统软件、用户信任的应用市场（APP Market）到其它来源依次降低。

22、如权利要求 19 所述的智能终端，其特征在于，所述存储器存储的第二 APP 数据下各数据条目的隐私级别通过手动设置或者根据不同 APP 数据之间的关联关系确定，其中所述关联关系包括数据产生地点或时间相同
15 的数据条目以及来自同一个联系人的数据条目。

23、如权利要求 19 至 22 任一项所述的智能终端，其特征在于，所述处理器用于获取第一應用程式 APP 对第二应用程序 APP 的数据访问请求，当所述第一 APP 的可信级别高于或等于其需要访问的数据条目的隐私级别时，
20 所述第一應用程式 APP 对第二应用程序 APP 的数据访问请求的回应以及处理方式为返回所述第一 APP 请求访问的数据条目；

当所述第一 APP 的可信级别低于其需要访问的数据条目的隐私级别时，所述第一應用程式 APP 对第二应用程序 APP 的数据访问请求的回应以及处理方式不予返回所述第一 APP 请求访问的数据条目或者返回修改后的数据
25 条目，其中修改后的数据条目包括虚假数据或者混淆数据。

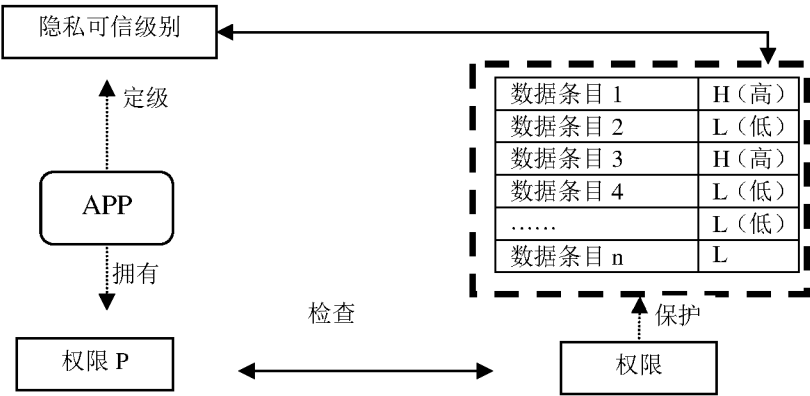


图 1

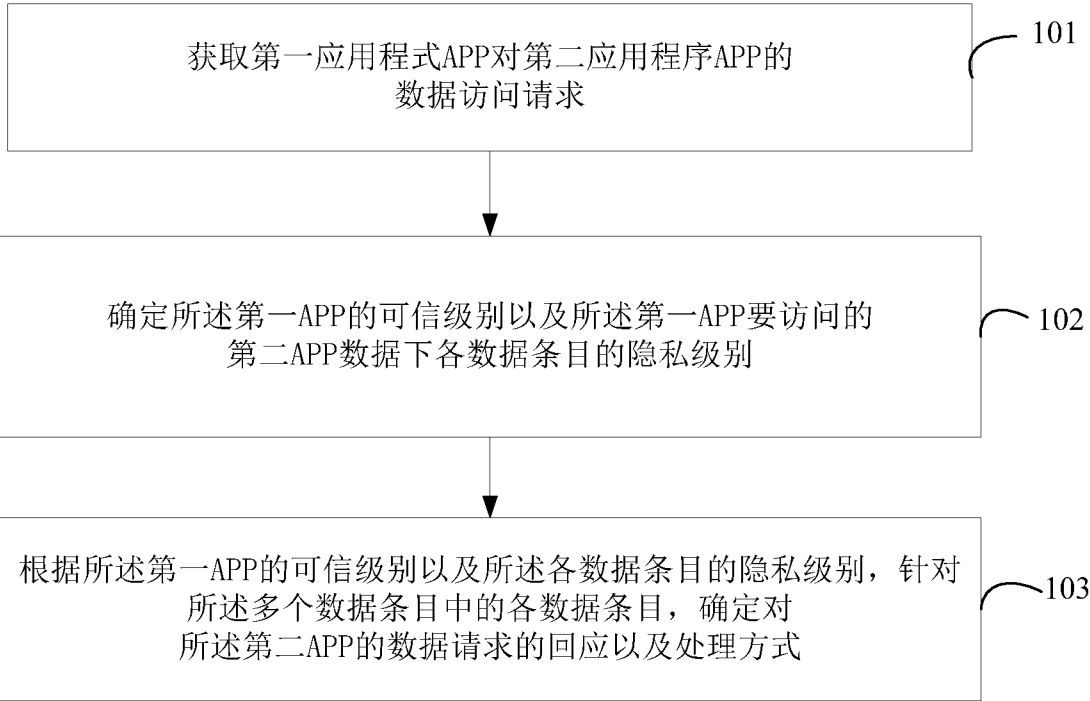


图 2

2/3

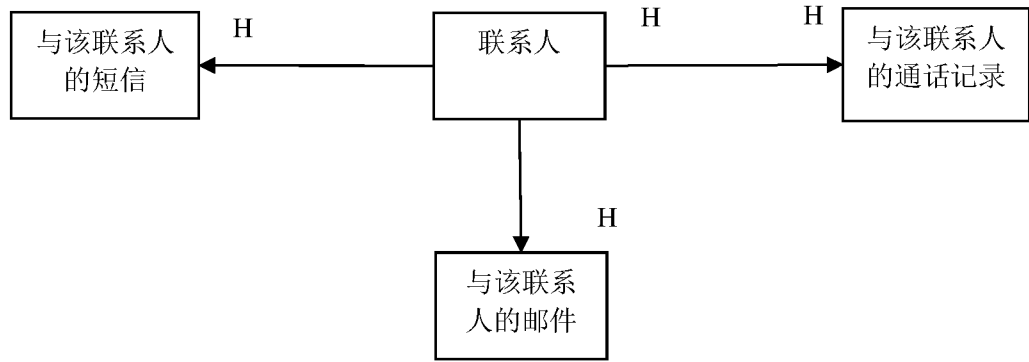


图 3

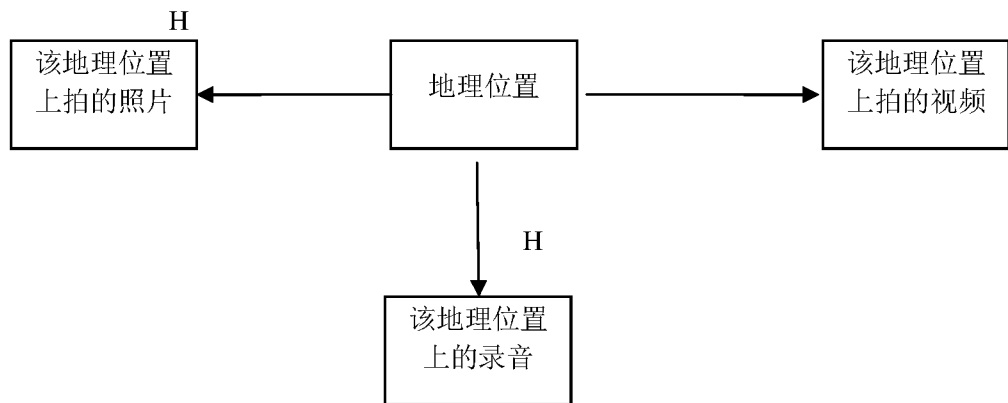


图 4

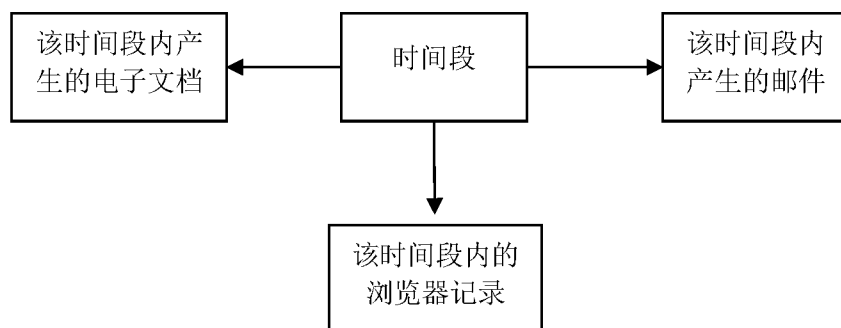


图 5

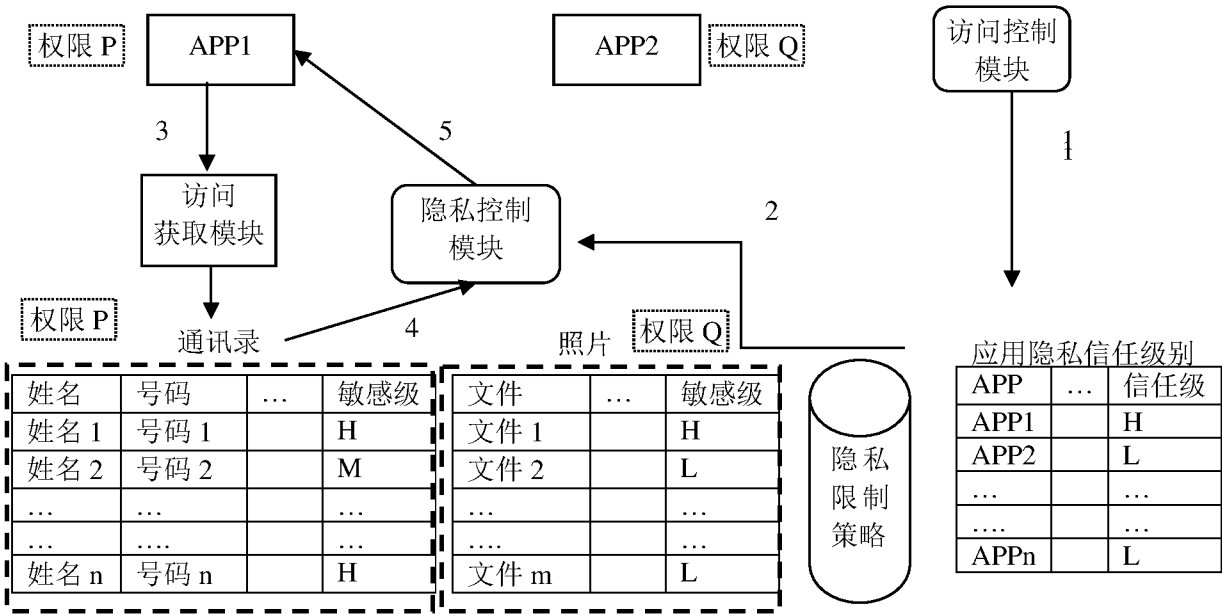


图 6

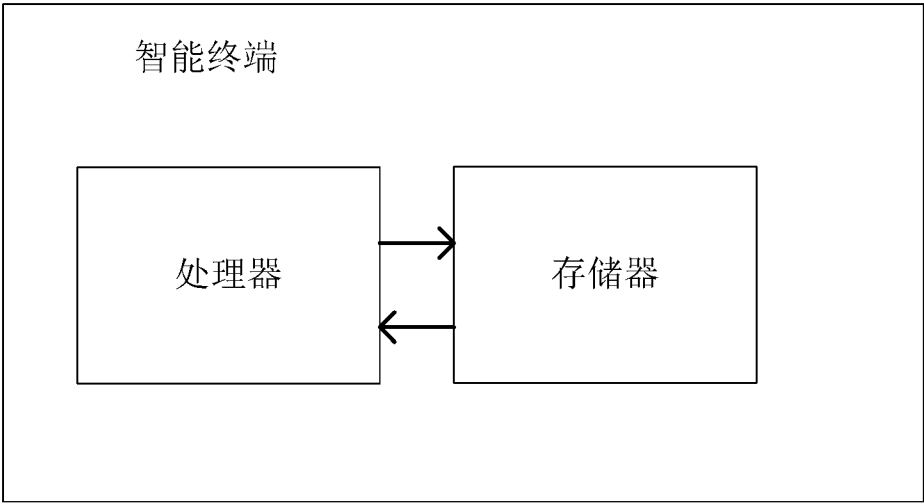


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/079817

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 (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

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)

WPI; EPODOC; CNPAT; CNKI: application, program, authority, grade, contact person, mobile phone, mobile terminal, App, program, privacy, right, access w control, level, contact, photo, android, mobile

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101917513 A (ZTE CORP.), 15 December 2010 (15.12.2010), description, paragraphs [0033]-[0054]	1-23
A	CN 102905016 A (DONGGUAN YULONG COMMUNICATION TECHNOLOGY CO., LTD. et al.), 30 January 2013 (30.01.2013), the whole document	1-23
A	US 2014245461 A1 (O'NEILL, E.K. et al.), 28 August 2014 (28.08.2014), the whole document	1-23

☐ 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 01 August 2015 (01.08.2015)	Date of mailing of the international search report 26 August 2015 (26.08.2015)
Name and mailing address of the ISA/CN: 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 ZHUANG, Yong Telephone No.: (86-10) 62414020

International application No.
PCT/CN2015/079817

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 G06F 21/62 (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 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)) WPI; EPDOC; CNPAT; CNKI: 应用, 程式, 程序, 隐私, 权限, 访问控制, 级别, 分级, 等级, 联系人, 照片, 安卓, 手机, 移动终端, App, program, privacy, right, access w control, level, contact, photo, android, mobile		
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 101917513 A (中兴通讯股份有限公司) 2010年 12月 15日 (2010 - 12 - 15) 说明书第[0033]-[0054]段	1-23
A	CN 102905016 A (东莞宇龙通信科技有限公司 等) 2013年 1月 30日 (2013 - 01 - 30) 全文	1-23
A	US 2014245461 A1 (O'NEILL, EDWARD KENNETH 等) 2014年 8月 28日 (2014 - 08 - 28) 全文	1-23
☐ 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 2015年 8月 1日		国际检索报告邮寄日期 2015年 8月 26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) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451		授权官员 庄湧 电话号码 (86-10)62414020

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/079817

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	101917513	A	2010年 12月 15日	无	
CN	102905016	A	2013年 1月 30日	无	
US	2014245461	A1	2014年 8月 28日	US 2015193635 A1	2015年 7月 9日