(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
2019 年 10 月 10 日 (10.10.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/192129 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2018/101558

(22) 国际申请日: 2018 年 8 月 21 日 (21.08.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810294695.7 2018年4月4日 (04.04.2018) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 刘俊廷 (LIU, Junting); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市隆天联鼎知识产权代理有限公司 (SHENZHEN LUNGTIN LIANDING INTELLECTUAL PROPERTY AGENT.LTD.); 中国广东省深圳市福田区南园路上田大厦4A刘抗美, Guangdong 518000 (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,

(54) **Title:** CUSTOMER DATA SECURITY ACCESS METHOD AND DEVICE BASED ON MOBILE TERMINAL

(54) **发明名称:** 基于移动终端的客户数据安全访问方法及装置

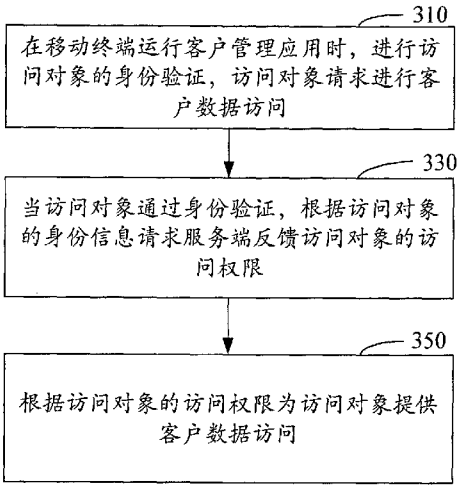

图 3

310 WHEN A MOBILE TERMINAL RUNS A CUSTOMER MANAGEMENT APPLICATION, PERFORM IDENTITY VERIFICATION ON AN ACCESS USER, THE ACCESS USER REQUESTING CUSTOMER DATA ACCESS

330 WHEN THE ACCESS USER PASSES THE IDENTITY VERIFICATION, REQUEST A SERVER TO FEED BACK ACCESS AUTHORITY OF THE ACCESS USER ACCORDING TO IDENTITY INFORMATION OF THE ACCESS USER

350 PROVIDE CUSTOMER DATA ACCESS FOR THE ACCESS USER ACCORDING TO THE ACCESS AUTHORITY OF THE ACCESS USER

(57) **Abstract:** The present application relates to a customer data security access method and device based on a mobile terminal. The customer data security access method based on a mobile terminal comprises: when a mobile terminal runs a customer management application, performing identity verification on an access user, the access user requesting customer data access; when the access user passes the identity verification, requesting a server to feed back access authority of the access user according to identity information of the access user; and providing customer data access for the access user according to the access authority of the access user. The customer data security access method based on a mobile terminal provided by the present application solves the problem in the prior art of poor security for accessing customer data by means of an external network.

WO 2019/192129 A1

[见续页]

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))。

(57) 摘要：本申请涉及了一种基于移动终端的客户数据安全访问方法及装置，所述基于移动终端的客户数据安全访问方法包括：在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据访问；当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；根据所述访问对象的访问权限为所述访问对象提供客户数据访问。采用本申请所提供的基于移动终端的客户数据安全访问方法解决了现有技术中外网访问客户数据的安全性较差的问题。

发明名称：基于移动终端的客户数据安全访问方法及装置

技术领域

[0001] 本申请要求2018年4月4日递交、发明名称为“基于移动终端的客户数据安全访问方法及装置”的中国专利申请CN201810294695.7的优先权，在此通过引用将其全部内容合并于此。

[0002] 本申请涉及计算机技术领域，尤其涉及一种基于移动终端的客户数据安全访问方法及装置。

背景技术

[0003] 目前，为了保证客户数据访问的安全性，客户数据通常部署于内网，访问对象仅能通过PC端接入内网来访问客户数据，这就导致在非工作时间段，因无法接入内网，访问对象无法进行客户数据访问，进而不能跟进客户，也不能维护客户关系。

[0004] 随着计算机技术的发展，如果访问对象需要通过外网进行客户数据访问，则需要对访问对象的身份加以验证，以此来保证外网访问客户数据的安全性。然而，发明人意识到：访问对象的身份在外网中容易受到病毒的攻击，尚无法充分地保障外网进行客户数据访问的安全性。

[0005] 由上可知，如何安全地通过外网进行客户数据访问仍亟待解决。

发明概述

技术问题

问题的解决方案

技术解决方案

[0006] 为了解决上述技术问题，本申请的一个目的在于提供一种基于移动终端的客户数据安全访问方法及装置。

[0007] 其中，本申请所采用的技术方案为：

[0008] 一方面，一种基于移动终端的客户数据安全访问方法，包括：在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据

访问；当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；根据所述访问对象的访问权限为所述访问对象提供客户数据访问。

[0009] 另一方面，一种基于移动终端的客户数据安全访问装置，包括：身份验证模块，配置为在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据访问；权限获取模块，配置为当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；数据访问模块，配置为根据所述访问对象的访问权限为所述访问对象提供客户数据访问。

[0010] 另一方面，一种基于移动终端的客户数据安全访问装置，包括处理器及存储器，所述存储器上存储有计算机可读指令，所述计算机可读指令被所述处理器执行时实现如上所述的基于移动终端的客户数据安全访问方法。

[0011] 另一方面，一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如上所述的基于移动终端的客户数据安全访问方法。

[0012] 在上述技术方案中，通过运行于移动终端的客户管理应用为访问对象提供外网访问客户数据，并基于访问对象的身份验证和访问权限充分地保障了外网访问客户数据的安全性，进而解决了现有技术中外网访问客户数据的安全性较差的问题。

[0013] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

发明的有益效果

对附图的简要说明

附图说明

[0014] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并于说明书一起用于解释本申请的原理。

[0015] 图1是根据本申请所涉及的实施环境的示意图。

[0016] 图2是根据一示例性实施例示出的一种移动终端的硬件结构框图。

[0017] 图3是根据一示例性实施例示出的一种基于移动终端的客户数据安全访问方法

的流程图。

[0018] 图4是根据一示例性实施例示出的另一种基于移动终端的客户数据安全访问方法的流程图。

[0019] 图5是图3对应实施例中步骤310在一个实施例的流程图。

[0020] 图6是根据一示例性实施例示出的另一种基于移动终端的客户数据安全访问方法的流程图。

[0021] 图7是图3对应实施例中步骤350在一个实施例的流程图。

[0022] 图8是根据一示例性实施例示出的一种基于移动终端的客户数据安全访问装置的框图。

[0023] 图9是根据一示例性实施例示出的一种基于移动终端的客户数据安全访问装置的结构框图。

[0024] 通过上述附图，已示出本申请明确的实施例，后文中将有更详细的描述，这些附图和文字描述并不是为了通过任何方式限制本申请构思的范围，而是通过参考特定实施例为本领域技术人员说明本申请的概念。

发明实施例

本发明的实施方式

[0025] 这里将详细地对示例性实施例执行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0026] 图1为一种基于移动终端的客户数据安全访问方法所涉及的实施环境的示意图。该实施环境包括移动终端100、服务端200和PC端300。

[0027] 其中，移动终端100可以是笔记本电脑、平板电脑、智能手机、或者其他可供客户管理应用运行的便携式电子设备，在此不进行限定。

[0028] PC端300区别于移动终端100，是指不具有便携性的台式电脑。

[0029] 移动终端100、PC端300分别与服务端200之间建立通信连接，该通信连接包括但不限于无线网络连接、有线网络连接等，进而通过所建立的通信连接进行客

户数据传输。

[0030] 具体地，对于移动终端100而言，利用运行的客户管理应用，为访问对象提供外网客户数据访问，而对于PC端300来说，为访问对象提供内网客户数据访问，由此，提高客户数据访问的通用性。

[0031] 请参阅图2，图2是根据一示例性实施例示出的一种移动终端的框图。

[0032] 需要说明的是，该移动终端100只是一个适配于本申请的示例，不能认为是提供了对本申请的使用范围的任何限制。该移动终端100也不能解释为需要依赖于或者必须具有图2中示出的示例性的移动终端100中的一个或者多个组件。

[0033] 如图2所示，移动终端100包括存储器101、存储控制器103、一个或多个（图2中仅示出一个）处理器105、外设接口107、射频模块109、定位模块111、摄像模块113、音频模块115、触控屏幕117以及按键模块119。这些组件通过一条或多条通讯总线/信号线121相互通讯。

[0034] 其中，存储器101可用于存储计算机程序以及模块，如本申请示例性实施例中的基于移动移动终端的客户数据安全访问方法及装置对应的计算机可读指令及模块，处理器105通过运行存储在存储器101内的计算机可读指令，从而执行各种功能以及数据处理，即完成基于移动移动终端的客户数据安全访问方法。

[0035] 存储器101作为资源存储的载体，可以是随机存储器、例如高速随机存储器、非易失性存储器，如一个或多个磁性存储装置、闪存、或者其它固态存储器。存储方式可以是短暂存储或者永久存储。

[0036] 外设接口107可以包括至少一有线或无线网络接口、至少一串并联转换接口、至少一输入输出接口以及至少一USB接口等，用于将外部各种输入/输出装置耦合至存储器101以及处理器105，以实现与外部各种输入/输出装置的通信。

[0037] 射频模块109用于收发电磁波，实现电磁波与电信号的相互转换，从而通过通讯网络与其他设备进行通讯。通信网络包括蜂窝式电话网、无线局域网或者城域网，上述通信网络可以使用各种通信标准、协议及技术。

[0038] 定位模块111用于获取移动终端100的当前所在的地理位置。定位模块111的实例包括但不限于全球卫星定位系统（GPS）、基于无线局域网或者移动通信网的定位技术。

[0039] 摄像模块113隶属于摄像头，用于拍摄图片或者视频。拍摄的图片或者视频可以存储至存储器101内，还可以通过射频模块109发送至上位机。

[0040] 音频模块115向用户提供音频接口，其可包括一个或多个麦克风接口、一个或多个扬声器接口以及一个或多个耳机接口。通过音频接口与其它设备进行音频数据的交互。音频数据可以存储至存储器101内，还可以通过射频模块109发送。

[0041] 触控屏幕117在移动终端100与用户之间提供一个输入输出界面。具体地，用户可通过触控屏幕117进行输入操作，例如点击、触摸、滑动等手势操作，以使移动终端100对该输入操作进行响应。移动终端100则将文字、图片或者视频任意一种形式或者组合所形成的输出内容通过触控屏幕117向用户显示输出。

[0042] 按键模块119包括至少一个按键，用以提供用户向移动终端100进行输入的接口，用户可以通过按下不同的按键使移动终端100执行不同的功能。例如，声音调节按键可供用户实现对移动终端100播放的声音音量的调节。

[0043] 可以理解，图2所示的结构仅为示意，移动终端100还可包括比图2中所示更多或更少的组件，或者具有与图2所示不同的组件。图2中所示的各组件可以采用硬件、软件或者其组合来实现。

[0044] 请参阅图3，在一示例性实施例中，一种基于移动移动终端的客户数据安全访问方法适用于图1所示实施环境的移动终端，该移动终端的结构可以如图2所示。

[0045] 该种基于移动移动终端的客户数据安全访问方法可以由移动终端执行，可以包括以下步骤：

[0046] 步骤310，在移动终端运行客户管理应用时，进行访问对象的身份验证。

[0047] 首先说明的是，客户管理应用，被预先安装部署于移动终端，用于为访问对象提供外网客户数据访问。也就是说，随着客户管理应用安装部署于移动终端，访问对象便可以通过客户管理应用接入外网而访问客户数据，进而实施客户管理，即跟进客户，维护客户关系等等。

[0048] 其次，为了保证客户数据访问的安全性，将对访问对象进行身份验证，仅在访问对象通过身份验证时，方可借助客户管理应用接入外网进行后续的客户数据

访问。

[0049] 可选地，访问对象的身份验证，是指对访问对象的身份信息进行合法性校验。合法性校验是将访问对象的身份信息与服务端所存储的海量访问对象的身份信息进行逐一比对，比对一致即视为访问对象通过身份验证。

[0050] 其中，访问对象的身份信息是对访问对象进行了唯一的标识，访问对象的身份信息包括但不限于：访问对象的账号、密码、身份证号码、联系方式等等。也就是说，访问对象的身份信息实现了对访问对象身份的准确描述，即如果访问对象不同，则身份将有所区别，进而访问对象的身份信息也各不相同。

[0051] 在一实施例的具体实现中，访问对象为保单营销坐席，客户数据与客户所购买的保单相关，包括但不限于：客户姓名、客户身份证号、客户联系方式、保单号、保单缴费年限、保单缴费金额等等。

[0052] 下面对服务端存储海量访问对象的身份信息的过程加以说明。

[0053] 具体地，访问对象为了进行客户数据访问，首先通过PC端向服务端发起客户数据访问请求，在服务端接收到该客户数据访问请求时，从客户数据访问请求携带的访问对象身份信息中提取身份证号码，并以此进行访问对象的身份认证。

[0054] 此处的身份认证是通过第三方身份认证机构完成的，例如，通过第三方身份认证机构中存储的身份证号码进行，即如果第三方认证机构中存储有相一致的身份证号码，则访问对象通过身份认证。

[0055] 当访问对象通过身份认证，则服务端将访问对象通过认证的身份信息进行存储，以供后续实现移动终端发起的访问对象身份验证，进而保证基于移动终端的客户数据安全访问得以实施。

[0056] 也就是说，访问对象只有通过PC端进行客户数据访问过程中，通过了第三方身份认证机构的身份认证之后，才能够基于移动终端实现客户数据访问，从而为外网访问客户数据的安全性提供充分的保障。

[0057] 步骤330，当访问对象通过身份验证，根据访问对象的身份信息请求服务端反馈访问对象的访问权限。

[0058] 访问对象的访问权限，反映了访问对象通过PC端进行客户数据访问过程中的访问行为。访问权限包括但不限于：新建权限、新增权限、修改权限、删除权限

等等。

[0059] 举例来说，访问对象在通过PC端进行客户数据访问过程中，对客户数据进行了修改，相应地，通过上述修改数据的访问行为，访问对象的访问权限为修改权限。

[0060] 可选地，访问对象的访问权限将由PC端上报至服务端中进行存储。

[0061] 在一实施例的具体实现中，如图4所示，步骤330之前，如上所述的方法还可以包括以下步骤:

[0062] 步骤410，在访问对象通过PC端进行客户数据访问过程中，服务端接收PC端为访问对象上报的访问权限。

[0063] 步骤430，建立访问对象的访问权限与身份信息之间的关联关系，通过关联关系的建立提供访问权限反馈服务。

[0064] 具体而言，如前所述，为了进行访问对象的身份验证，服务端中存储了海量访问对象的身份信息。此时，通过PC端所上报的访问权限，服务端中还获得了访问对象的访问权限，使得服务端能够对访问对象的访问权限进行存储，并建立访问对象的身份信息与访问权限之间的关联关系，进而实现访问对象的身份信息与访问权限的关联存储，方便于提供访问权限反馈服务。

[0065] 由此可知，当访问对象通过身份验证，根据访问对象的身份信息，便能够通过服务端获取到访问对象的访问权限。

[0066] 在上述过程中，对于移动终端而言，访问对象的访问权限是与PC端中访问对象访问客户数据的访问行为密切相关的，也可以理解为，无论访问对象是基于PC端进行的客户数据访问，还是基于移动终端进行的客户数据访问，访问对象对客户数据的访问权限始终保持一致，以为后续客户数据的安全访问提供了充分的保障。

[0067] 步骤350，根据访问对象的访问权限为访问对象提供客户数据访问。

[0068] 在获得访问对象的访问权限之后，便能够基于该访问权限控制访问对象进行客户数据访问。

[0069] 也就是说，基于移动终端的客户数据访问，将受限于访问对象的访问权限，以此进一步地保障了客户数据访问的安全性。

[0070] 通过如上所述的过程，借助运行于移动终端的客户管理应用，实现了访问对象通过外网接入所进行的客户数据访问，也就是说，利用移动终端的便携性，访问对象可以随时接入外网访问客户数据，进而实时地跟进客户，维护客户关系，充分地保证了其与客户的粘度。

[0071] 在一应用场景中，为了基于移动终端访问客户数据，首先要通过PC端请求第三方身份认证机构对访问对象进行第一次身份认证，然后再通过移动终端请求服务端对访问对象进行第二次身份验证，最后，方能够根据服务端反馈的访问权限控制访问对象进行客户数据的安全访问，以此为客户数据的安全访问提供了多重保证，进而充分地保障了客户数据访问的安全性。

[0072] 请参阅图5，在一示例性实施例中，步骤310可以包括以下步骤：

[0073] 步骤311，在移动终端运行的客户管理应用中，根据访问对象触发进行的操作获取访问对象的身份信息。

[0074] 其中，为了对访问对象进行身份验证，客户管理应用将为访问对象的身份信息获取提供入口。当访问对象希望进行客户数据访问时，将在该入口中触发相应的操作，以使客户管理应用获得访问对象的身份信息，进而根据该身份信息进行访问对象的身份验证。

[0075] 例如，客户管理应用在显示页面中显示一输入对话框，访问对象便可以在该输入对话框中输入身份信息，其中，该输入对话框即为入口，该输入操作即为访问对象为进行客户数据访问而在该入口触发进行的操作。

[0076] 步骤313，根据访问对象的身份信息请求服务端进行身份信息匹配搜索，获得匹配搜索结果。

[0077] 如前所述，服务端中存储了海量访问对象的身份信息，由此，身份信息匹配搜索，即是指将访问对象的身份信息与服务端所存储的海量访问对象的身份信息逐一进行比对。

[0078] 因此，通过身份信息匹配搜索，如果服务端中存在与访问对象的身份信息一致的身份信息，则跳转至步骤315，判定访问对象通过身份验证。

[0079] 反之，如果服务端中不存在与访问对象的身份信息一致的身份信息，则判定访问对象未通过身份验证，即访问对象为非法访问者，进而无权通过移动终端进

行客户数据访问。

[0080] 步骤315，如果匹配搜索结果指示服务端存在与访问对象身份信息一致的身份信息，则判定访问对象的身份信息通过身份验证。

[0081] 在一实施例的具体实现中，对于移动终端而言，当访问对象通过身份验证，便允许访问对象登录客户管理应用，进而，随着访问对象登录客户管理应用，便使得访问对象能够借助客户管理应用接入外网而进行客户数据访问。

[0082] 在上述实施例的作用下，仅当通过身份验证的访问对象才有资格接入外网访问客户数据，以此保证外网接入的安全性，进而有利于提高客户数据访问的安全性。

[0083] 请参阅图6，在一示例性实施例中，步骤410之前，如上所述的方法还可以包括以下步骤：

[0084] 步骤510，PC端在访问对象进行客户数据访问过程中，生成用于指示访问对象访问行为的日志记录。

[0085] 在访问对象进行客户数据访问过程中，会进行一系列的访问行为，例如，对客户数据进行修改、新增等等，为此，PC端将根据该些访问行为生成日志记录，以便于后续系统故障时能够对访问对象的访问行为进行追溯。

[0086] 由上可知，日志记录是指示了访问对象的访问行为的，也可以理解为，日志记录实现了对访问对象的访问行为的准确描述。

[0087] 举例来说，访问对象在进行客户数据访问过程中，删除了客户数据，则PC端将根据删除数据的访问行为生成相应的日志记录。其中，日志记录携带了行为id，该行为id即唯一地标识了该删除数据的访问行为。

[0088] 步骤530，根据日志记录指示的访问行为配置访问对象的访问权限，并将访问对象的访问权限上报至服务端。

[0089] 在获得指示了访问对象访问行为的日志记录之后，便能够进行访问对象的访问权限配置。例如，访问行为是删除客户数据，则为访问对象配置的访问权限为删除权限。

[0090] 对于服务端而言，在PC端完成访问权限的配置之后，即可接收到PC端为访问对象配置的访问权限。

[0091] 可选地，访问权限还可以根据访问对象在PC端中触发进行的选择操作上报。也就是说，被允许上报至服务端的访问权限是根据访问对象的实际需要进行选择的。

[0092] 较优地，被允许上报至服务端的访问权限为新建权限、新增权限，而不包含修改权限、删除权限，避免客户数据因外网接入受到非法攻击时被误操作，以此可选地保证了客户数据访问的安全性。

[0093] 通过上述实施例的配合，实现了访问对象的访问权限配置，使得服务端提供访问权限反馈服务得以实施，以此为保证客户数据的安全访问提供了可靠依据。

[0094] 此外，通过日志记录所进行的访问权限配置，使得访问对象的访问权限能够动态更新，即访问对象的访问权限将随着日志记录所指示的访问行为的变化而变化，由此，即使在本次所进行的外网访问客户数据过程中，访问对象的访问权限因受到病毒攻击而外泄，在后续所进行的外网访问客户数据过程中，只要访问对象的访问行为发生了变化，访问对象的访问权限将随之相应地变化，进而造成之前外泄的访问对象的访问权限失效，以此降低外网易受病毒攻击的风险，从而充分地保障了外网进行客户数据访问的安全性。

[0095] 请参阅图7，在一示例性实施例中，客户数据的网页资源存储于隔离区（demilitarized zone，DMZ）。

[0096] 可以理解，通过移动终端接入外网进行的客户数据访问，很有可能存在不安全隐患，而导致客户数据受损，例如，受到黑客的攻击。

[0097] 为此，本实施例中，客户数据的网页资源存储于隔离区，该隔离区为外网与内网之间的网络区域，以此实现外网与内网之间无法直接通信的目的，进而保障内网的安全性。

[0098] 可选地，隔离区可以是部署于独立服务器，以区别于外网服务器或者内网服务器，也可以部署于服务器中的虚拟机，例如，外网服务器中的虚拟机或者内网服务器中的虚拟机，以此增强隔离区部署的灵活性，还有利于降低隔离区部署的复杂度，本实施例对此并未加以限定。

[0099] 应当说明的是，隔离区中存储的是客户数据的网页资源，是为了客户管理应用中方便通过显示网页的方式进行客户数据的显示。

[0100] 相应地，步骤350可以包括以下步骤：

[0101] 步骤351，根据客户管理应用所存储的网页链接地址发起客户数据访问请求。

[0102] 网页链接地址，对应于客户数据的网页资源，记录了客户数据的网页资源在隔离区中的存储位置。

[0103] 由此，客户数据不同，则隔离区中存储的相应网页资源有所区别，进而使得网页链接地址也各不相同。由此，便能够通过不同的网页链接地址发起客户数据访问请求，以对隔离区中不同存储位置的客户数据进行访问。

[0104] 步骤353，通过客户数据访问请求向隔离区请求客户数据的网页资源。

[0105] 对于隔离区而言，由客户数据访问请求中提取网页链接地址，便能够得到隔离区中相应存储位置的客户数据的网页资源，进而向发起客户数据访问请求的移动终端反馈所获得的网页资源。

[0106] 也就是说，隔离区为客户管理应用存储客户数据的网页资源，只要移动终端与隔离区交互，便能够通过客户管理应用所存储的网页链接地址向隔离区发起客户数据访问请求，进而由隔离区获得客户数据的网页资源。

[0107] 步骤355，根据客户数据的网页资源在客户管理应用中进行客户数据显示。

[0108] 步骤357，控制访问对象按照访问权限对显示的客户数据进行访问。

[0109] 在上述过程中，基于移动终端中预先安装部署的客户管理应用，实现了访问对象通过外网对隔离区中客户数据的访问，避免了仅能够由PC端接入内网所进行的客户数据访问，不仅保证了客户数据访问的安全性，而且增强了客户数据访问的通用性。

[0110] 下述为本申请装置实施例，可以用于执行本申请所涉及的基于移动移动终端的客户数据安全访问方法。对于本申请装置实施例中未披露的细节，请参照本申请所涉及的基于移动移动终端的客户数据安全访问方法的方法实施例。

[0111] 请参阅图8，在一示例性实施例中，一种基于移动移动终端的客户数据安全访问装置900包括但不限于：身份验证模块910、权限获取模块930和数据访问模块950。

[0112] 其中，身份验证模块910用于在移动终端运行客户管理应用时，进行访问对象的身份验证，访问对象请求进行客户数据访问。

[0113] 权限获取模块930用于当访问对象通过身份验证，根据访问对象的身份信息请求服务端反馈访问对象的访问权限。

[0114] 数据访问模块950用于根据访问对象的访问权限为访问对象提供客户数据访问。

[0115] 需要说明的是，上述实施例所提供的基于移动移动终端的客户数据安全访问装置在进行基于移动移动终端的客户数据安全访问处理时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即基于移动移动终端的客户数据安全访问装置的内部结构将划分为不同的功能模块，以完成以上描述的全部或者部分功能。

[0116] 另外，上述实施例所提供的基于移动移动终端的客户数据安全访问装置与基于移动移动终端的客户数据安全访问方法的实施例属于同一构思，其中各个模块执行操作的具体方式已经在方法实施例中进行了详细描述，此处不再赘述。

[0117] 请参阅图9，在一示例性实施例中，一种基于移动移动终端的客户数据安全访问装置，包括处理器1001及存储器1004。所述装置1000还包括通信接口1002和通信总线1003。所述处理器1001通过通信总线1003读取所述存储器1004中存储的计算机可读指令。

[0118] 其中，存储器1004上存储有计算机可读指令，该计算机可读指令被处理器1001执行时实现上述各实施例中的基于移动移动终端的客户数据安全访问方法。

[0119] 在一示例性实施例中，一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述各实施例中的基于移动移动终端的客户数据安全访问方法。

[0120] 上述内容，仅为本申请的较佳示例性实施例，并非用于限制本申请的实施方案，本领域普通技术人员根据本申请的主要构思和精神，可以十分方便地进行相应的变通或修改，故本申请的保护范围应以权利要求书所要求的保护范围为准。

权利要求书

[权利要求 1] 一种基于移动终端的客户数据安全访问方法，其中，所述方法包括：

在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据访问；

当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；

根据所述访问对象的访问权限为所述访问对象提供客户数据访问。

[权利要求 2] 如权利要求1所述的方法，其中，所述在移动终端运行客户管理应用时，进行访问对象的身份验证，包括：

在所述移动终端运行的客户管理应用中，根据所述访问对象触发进行的操作获取所述访问对象的身份信息；

根据所述访问对象的身份信息请求服务端进行身份信息匹配搜索，获得匹配搜索结果；

如果所述匹配搜索结果指示所述服务端存在与所述访问对象身份信息一致的身份信息，则判定所述访问对象的身份信息通过身份验证。

[权利要求 3] 如权利要求1或2所述的方法，其中，所述根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限之前，所述方法还包括：

在所述访问对象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限；

建立所述访问对象的访问权限与身份信息之间的关联关系，通过所述关联关系的建立提供访问权限反馈服务。

[权利要求 4] 如权利要求3所述的方法，其中，所述在所述访问对象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限之前，所述方法还包括：

所述PC端在所述访问对象进行客户数据访问过程中，生成用于指示所述访问对象访问行为的日志记录；

根据所述日志记录指示的访问行为配置所述访问对象的访问权限，并将所述访问对象的访问权限上报至所述服务端。

[权利要求 5] 如权利要求1至4任一项所述的方法，其中，所述客户数据的网页资源存储于隔离区，所述根据所述访问对象的访问权限为所述访问对象提供客户数据访问，包括：

根据所述客户管理应用所存储的网页链接地址发起客户数据访问请求；

通过所述客户数据访问请求向所述隔离区请求所述客户数据的网页资源；

根据所述客户数据的网页资源在所述客户管理应用中进行客户数据显示；

控制所述访问对象按照访问权限对显示的客户数据进行访问。

[权利要求 6] 一种基于移动终端的客户数据安全访问装置，其中，所述装置包括：

身份验证模块，配置为在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据访问；

权限获取模块，配置为当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；

数据访问模块，配置为根据所述访问对象的访问权限为所述访问对象提供客户数据访问。

[权利要求 7] 如权利要求6所述的装置，其中，所述身份验证模块包括：

信息获取单元，配置为在所述移动终端运行的客户管理应用中，根据所述访问对象触发进行的操作获取所述访问对象的身份信息；

结果获取单元，配置为根据所述访问对象的身份信息请求服务端进行身份信息匹配搜索，获得匹配搜索结果；

验证通过单元，配置为如果所述匹配搜索结果指示所述服务端存在与所述访问对象身份信息一致的身份信息，则判定所述访问对象的身份信息通过身份验证。

[权利要求 8] 如权利要求6或7所述的装置，其中，所述装置还包括：

权限接收模块，配置为在所述访问对象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限

；

关系建立模块，配置为建立所述访问对象的访问权限与身份信息之间的关联关系，通过所述关联关系的建立提供访问权限反馈服务。

[权利要求 9] 如权利要求8所述的装置，其中，所述装置还包括：

日志记录生成模块，配置为所述PC端在所述访问对象进行客户数据访问过程中，生成用于指示所述访问对象访问行为的日志记录；

权限配置模块，配置为根据所述日志记录指示的访问行为配置所述访问对象的访问权限，并将所述访问对象的访问权限上报至所述服务端。

[权利要求 10] 如权利要求6至9任一项所述的装置，其中，所述客户数据的网页资源存储于隔离区，所述数据访问模块包括：

请求发起单元，配置为根据所述客户管理应用所存储的网页链接地址发起客户数据访问请求；

资源请求单元，配置为通过所述客户数据访问请求向所述隔离区请求所述客户数据的网页资源；

数据显示单元，配置为根据所述客户数据的网页资源在所述客户管理应用中进行客户数据显示；

控制访问单元，配置为控制所述访问对象按照访问权限对显示的客户数据进行访问。

[权利要求 11] 一种基于移动终端的客户数据安全访问装置，其中，所述装置包括：

处理器；及

存储器，所述存储器上存储有计算机可读指令，所述计算机可读指令被所述处理器执行以下步骤：

在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据访问；

当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；

根据所述访问对象的访问权限为所述访问对象提供客户数据访问。

[权利要求 12] 如权利要求11所述的装置，其中，所述在移动终端运行客户管理应用时，进行访问对象的身份验证步骤中，所述处理器执行以下步骤：

在所述移动终端运行的客户管理应用中，根据所述访问对象触发进行的操作获取所述访问对象的身份信息；

根据所述访问对象的身份信息请求服务端进行身份信息匹配搜索，获得匹配搜索结果；

如果所述匹配搜索结果指示所述服务端存在与所述访问对象身份信息一致的身份信息，则判定所述访问对象的身份信息通过身份验证。

[权利要求 13] 如权利要求11或12所述的装置，其中，所述根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限步骤之前，所述处理器还执行以下步骤：

在所述访问对象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限；

建立所述访问对象的访问权限与身份信息之间的关联关系，通过所述关联关系的建立提供访问权限反馈服务。

[权利要求 14] 如权利要求13所述的装置，其中，所述在所述访问对象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限步骤之前，所述处理器还执行以下步骤：

所述PC端在所述访问对象进行客户数据访问过程中，生成用于指示所述访问对象访问行为的日志记录；

根据所述日志记录指示的访问行为配置所述访问对象的访问权限，并将所述访问对象的访问权限上报至所述服务端。

[权利要求 15] 如权利要求11至14任一项所述的装置，其中，所述客户数据的网页资源存储于隔离区，所述根据所述访问对象的访问权限为所述访问对象提供客户数据访问步骤中，所述处理器执行以下步骤：

根据所述客户管理应用所存储的网页链接地址发起客户数据访问请求；

通过所述客户数据访问请求向所述隔离区请求所述客户数据的网页资

源；

根据所述客户数据的网页资源在所述客户管理应用中进行客户数据显示；

控制所述访问对象按照访问权限对显示的客户数据进行访问。

[权利要求 16] 一种计算机可读存储介质，其上存储有计算机程序，其中，所述计算机程序被处理器执行以下步骤：

在移动终端运行客户管理应用时，进行访问对象的身份验证，所述访问对象请求进行客户数据访问；

当所述访问对象通过身份验证，根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限；

根据所述访问对象的访问权限为所述访问对象提供客户数据访问。

[权利要求 17] 如权利要求16所述的计算机可读存储介质，其中，所述在移动终端运行客户管理应用时，进行访问对象的身份验证步骤中，所述处理器执行以下步骤：

在所述移动终端运行的客户管理应用中，根据所述访问对象触发进行的操作获取所述访问对象的身份信息；

根据所述访问对象的身份信息请求服务端进行身份信息匹配搜索，获得匹配搜索结果；

如果所述匹配搜索结果指示所述服务端存在与所述访问对象身份信息一致的身份信息，则判定所述访问对象的身份信息通过身份验证。

[权利要求 18] 如权利要求16或17所述的计算机可读存储介质，其中，所述根据所述访问对象的身份信息请求服务端反馈所述访问对象的访问权限步骤之前，所述处理器还执行以下步骤：

在所述访问对象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限；

建立所述访问对象的访问权限与身份信息之间的关联关系，通过所述关联关系的建立提供访问权限反馈服务。

[权利要求 19] 如权利要求18所述的计算机可读存储介质，其中，所述在所述访问对

象通过PC端进行客户数据访问过程中，所述服务端接收所述PC端为所述访问对象上报的访问权限步骤之前，所述处理器还执行以下步骤：

所述PC端在所述访问对象进行客户数据访问过程中，生成用于指示所述访问对象访问行为的日志记录；

根据所述日志记录指示的访问行为配置所述访问对象的访问权限，并将所述访问对象的访问权限上报至所述服务端。

[权利要求 20] 如权利要求16至19任一项所述的计算机可读存储介质，其中，所述客户数据的网页资源存储于隔离区，所述根据所述访问对象的访问权限为所述访问对象提供客户数据访问步骤中，所述处理器执行以下步骤：

根据所述客户管理应用所存储的网页链接地址发起客户数据访问请求；

通过所述客户数据访问请求向所述隔离区请求所述客户数据的网页资源；

根据所述客户数据的网页资源在所述客户管理应用中进行客户数据显示；

控制所述访问对象按照访问权限对显示的客户数据进行访问。

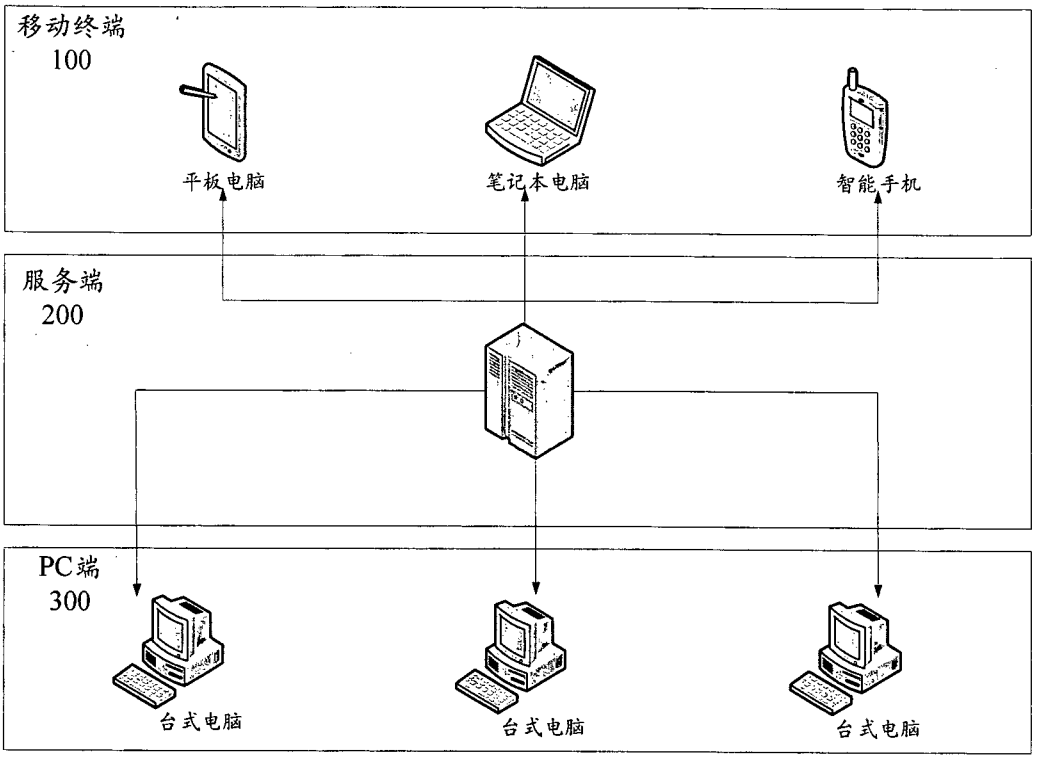
移动终端
100
平板电脑
笔记本电脑
智能手机
服务端
200
PC端
300
台式电脑
台式电脑
台式电脑

图 1

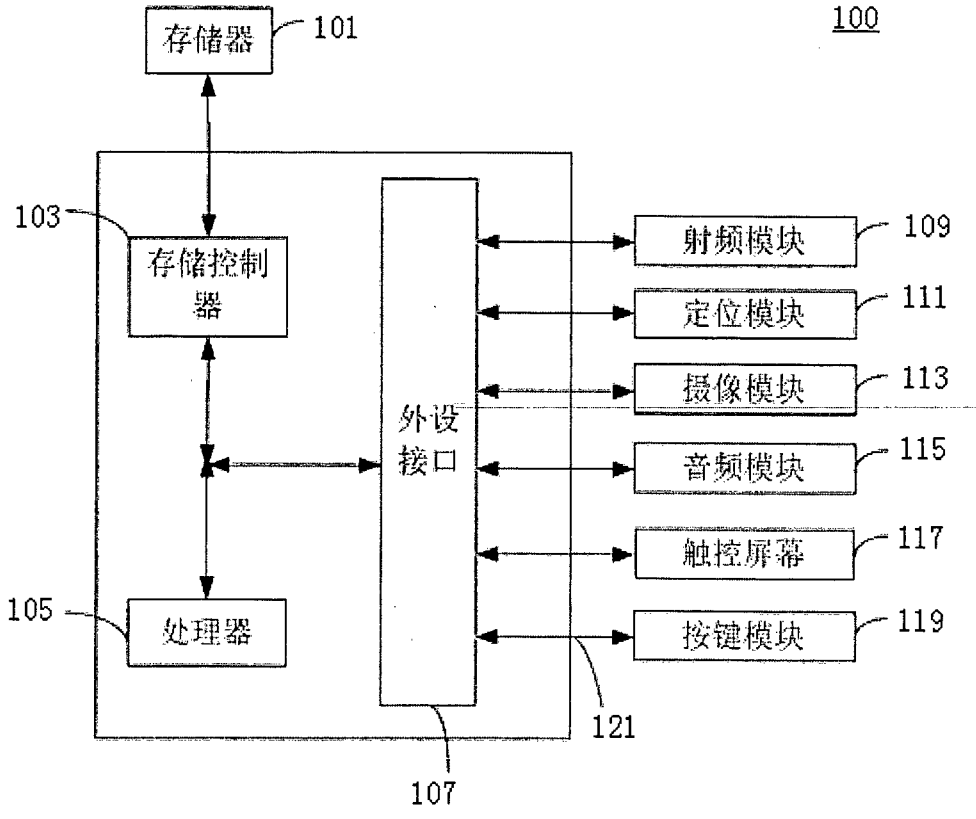
100
存储器
101
103
存储控制器
处理器
105
外设接口
107
射频模块
109
定位模块
111
摄像模块
113
音频模块
115
触控屏幕
117
按键模块
119
121

图 2

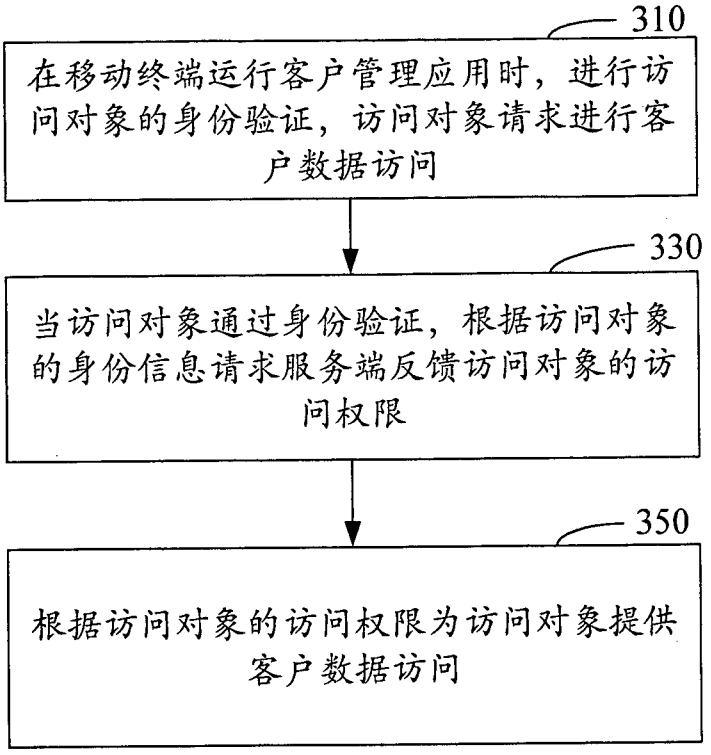
310
在移动终端运行客户管理应用时，进行访问对象的身份验证，访问对象请求进行客户数据访问
330
当访问对象通过身份验证，根据访问对象的身份信息请求服务端反馈访问对象的访问权限
350
根据访问对象的访问权限为访问对象提供客户数据访问

图 3

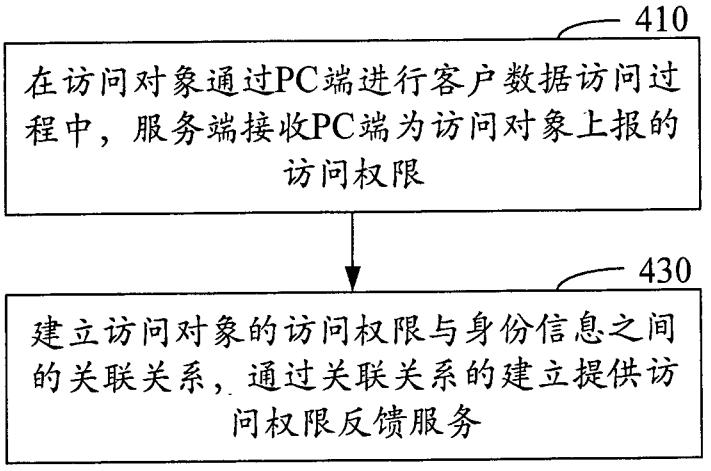
410
在访问对象通过PC端进行客户数据访问过程中，服务端接收PC端为访问对象上报的访问权限
430
建立访问对象的访问权限与身份信息之间的关联关系，通过关联关系的建立提供访问权限反馈服务

图 4

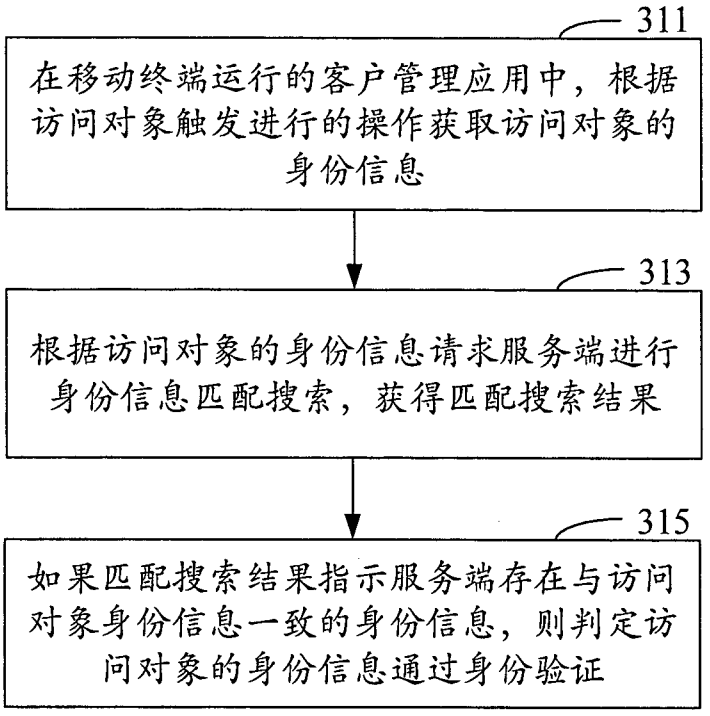
311
在移动终端运行的客户管理应用中，根据访问对象触发进行的操作获取访问对象的身份信息
313
根据访问对象的身份信息请求服务端进行身份信息匹配搜索，获得匹配搜索结果
315
如果匹配搜索结果指示服务端存在与访问对象身份信息一致的身份信息，则判定访问对象的身份信息通过身份验证

图 5

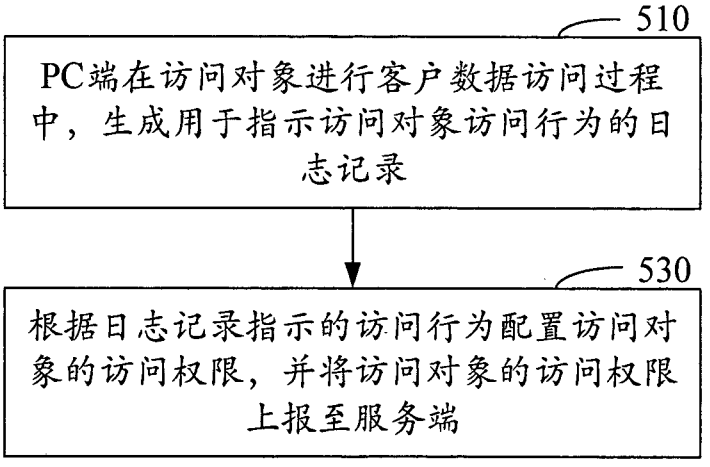
510
PC端在访问对象进行客户数据访问过程中，生成用于指示访问对象访问行为的日志记录
530
根据日志记录指示的访问行为配置访问对象的访问权限，并将访问对象的访问权限上报至服务端

图 6

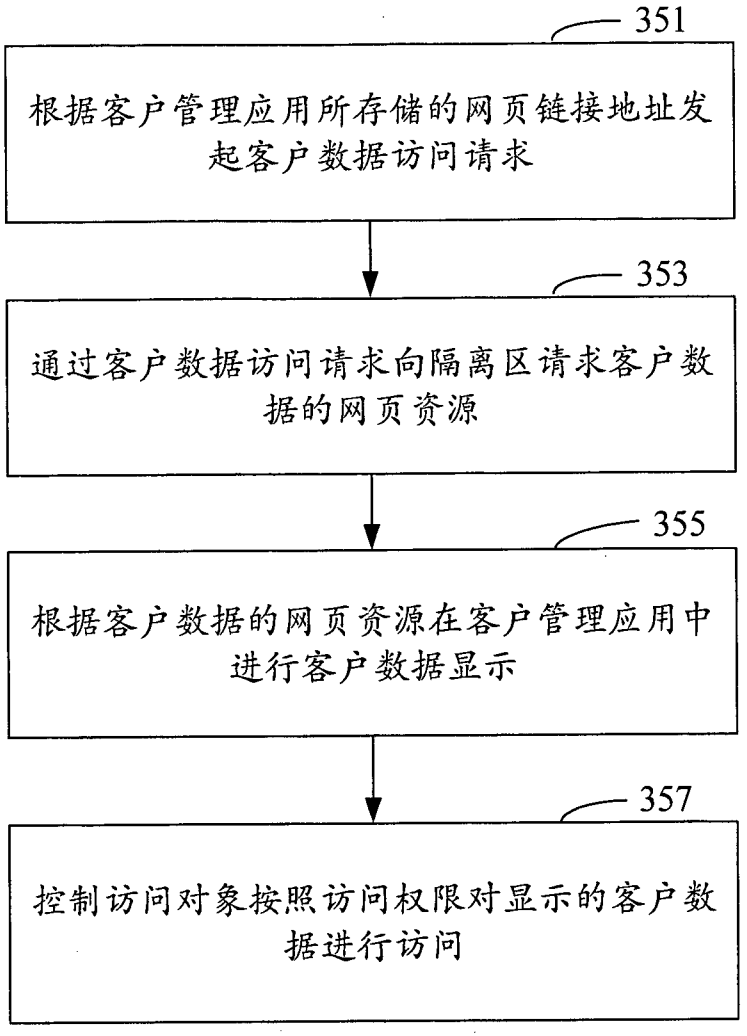
351
根据客户管理应用所存储的网页链接地址发起客户数据访问请求
353
通过客户数据访问请求向隔离区请求客户数据的网页资源
355
根据客户数据的网页资源在客户管理应用中进行客户数据显示
357
控制访问对象按照访问权限对显示的客户数据进行访问

图 7

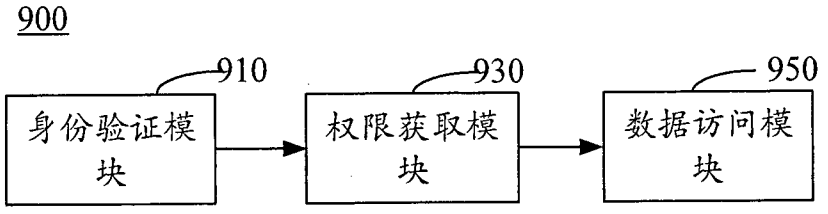
900
910
身份验证模块
930
权限获取模块
950
数据访问模块

图 8

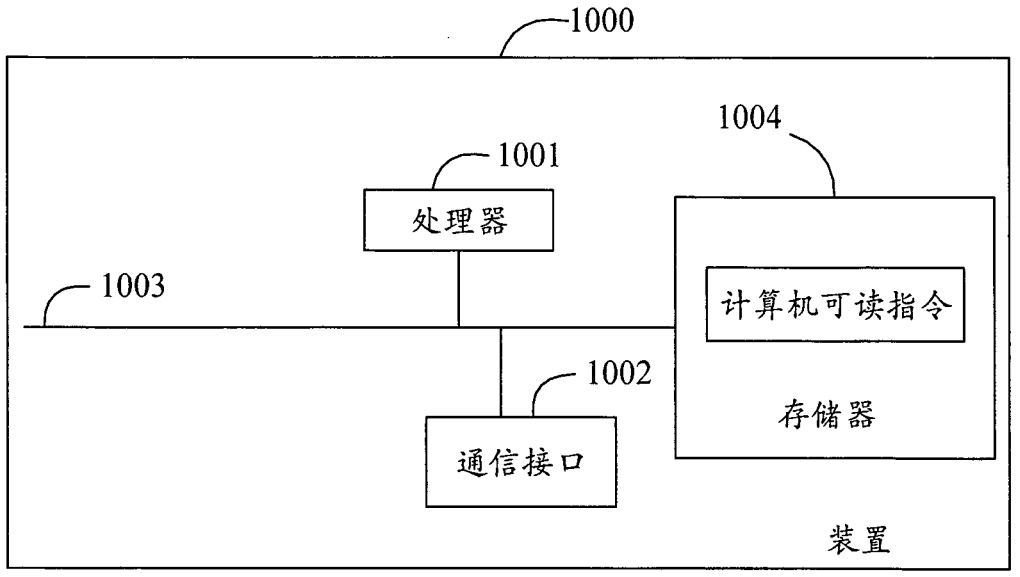

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/101558

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)

CNPAT, CNKI, EPODOC, WPI: 访问, 接入, 身份, 验证, 认证, 权限, visit, access, identity, authentication, right, authority

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103581184 A (NO. 15 RESEARCH INSTITUTE OF CHINA ELECTRONICS TECHNOLOGY GROUP CORPORATION) 12 February 2014 (2014-02-12) description, paragraphs 55-81	1-20
A	CN 103841130 A (SHENZHEN TENCENT COMPUTER SYSTEM CO., LTD.) 04 June 2014 (2014-06-04) entire document	1-20
A	WO 2017194581 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 16 November 2017 (2017-11-16) entire document	1-20
A	EP 3261375 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 27 December 2017 (2017-12-27) entire document	1-20

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 November 2018	**07 January 2019**
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 Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/101558

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 103581184 A	12 February 2014	None	
CN 103841130 A	04 June 2014	None	
WO 2017194581 A1	16 November 2017	EP 3244588 A1	15 November 2017
EP 3261375 A1	27 December 2017	WO 2017220432 A1	28 December 2017
		WO 2017220275 A1	28 December 2017

国际检索报告

国际申请号
PCT/CN2018/101558

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））

CNPAT, CNKI, EPODOC, WPI：访问，接入，身份，验证，认证，权限，visit, access, identity, authentication, right, authority

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 103581184 A (中国电子科技集团公司第十五研究所) 2014年 2月 12日 (2014-02-12) 说明书第55-81段	1-20
A	CN 103841130 A (深圳市腾讯计算机系统有限公司) 2014年 6月 4日 (2014-06-04) 全文	1-20
A	WO 2017194581 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 2017年 11月 16日 (2017-11-16) 全文	1-20
A	EP 3261375 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 2017年 12月 27日 (2017-12-27) 全文	1-20

☐ 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 11月 15日	2019年 1月 7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 田涛 电话号码 86-(10)-53961637

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/101558

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 103581184 A	2014年 2月 12日	无	
CN 103841130 A	2014年 6月 4日	无	
WO 2017194581 A1	2017年 11月 16日	EP 3244588 A1	2017年 11月 15日
EP 3261375 A1	2017年 12月 27日	WO 2017220432 A1	2017年 12月 28日
		WO 2017220275 A1	2017年 12月 28日