

(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
2015 年 6 月 18 日 (18.06.2015)



(10) 国际公布号
WO 2015/085819 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2014/087815

(22) 国际申请日: 2014 年 9 月 30 日 (30.09.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310666504.2 2013 年 12 月 10 日 (10.12.2013) CN
201310713538.2 2013 年 12 月 20 日 (20.12.2013) CN

(71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: 王力 (WANG, Li); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。王鹏程 (WANG, Pengcheng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。李旋 (LI, Xuan);

中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。苏云琳 (SU, Yunlin); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。刘伟 (LIU, Wei); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (CN)。

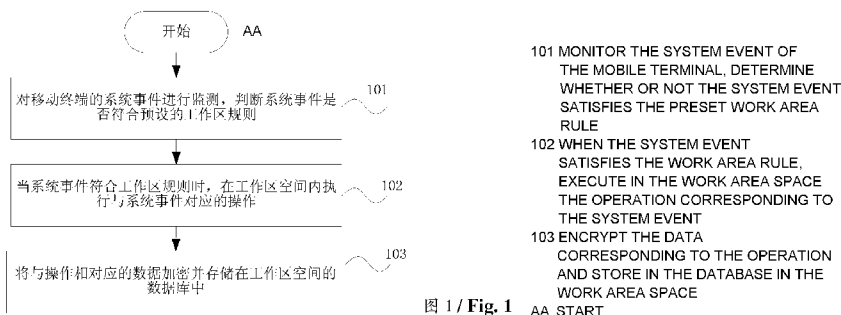
(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, 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,

[见续页]

(54) Title: METHOD AND DEVICE FOR PUBLIC/PRIVATE SEPARATION

(54) 发明名称: 一种公私隔离的方法及装置



(57) Abstract: A method and device for public/private separation. A system event of a mobile terminal is monitored; whether or not the system event satisfies a preset work area rule is determined; when the system event satisfies the work area rule, an operation corresponding to the system event is executed in a work area space; and, data corresponding to the operation is encrypted and stored in a database in the work area space. The method and device for public/private separation establish one secure and discrete work area on the mobile terminal, have all work data stored in a protected secure area, deny personal applications access to enterprise data, prevent the enterprise data from being accessed illegally by the personal applications, allow an IT department to better protect applications and data of an enterprise, and provide an employee with undifferentiated personal application experience, thus effecting dual use of one machine.

(57) 摘要: 一种公私隔离的方法和装置, 对移动终端的系统事件进行监测, 判断系统事件是否符合预设的工作区规则, 当系统事件符合工作区规则时, 在工作区空间内执行与系统事件对应的操作, 将与操作相对应的数据加密并存储在在工作区空间的数据库中。所述公私隔离的方法和装置, 在移动终端上建立一个安全、独立的工作区, 将所有的工作数据存储存储在受保护的安全区内, 使个人应用无法访问企业数据, 避免企业数据被个人应用非法存取, 能够使 IT 部门更好地保护企业的应用和数据, 也为员工提供了无差别的个人应用体验, 达到一机两用的效果。

WO 2015/085819 A1



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))。
- 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布(细则 48.2(h))。

一种公私隔离的方法及装置

技术领域

本申请涉及网络安全技术领域，尤其涉及一种公私隔离的方法及装置。

背景技术

随着智能终端的成熟与普及，以手机、平板为代表的个人智能终端设备逐渐进入企业领域。据国际权威咨询公司预测，到2014年90%的企业将会支持员工在个人移动终端上运行企业办公应用程序，员工使用个人智能终端设备办公已经成为一种无法逆转的潮流。这类被称为BYOD (Bring Your Own Device, 自带设备办公) 的现象为企业安全和管理带来了新的挑战。企业员工的移动设备可以在任何时间、地点接入移动互联网或公共/家庭Wi-Fi (Wireless-Fidelity, 无线保真) 网络，移动终端中的企业数据也会暴露在来自互联网的攻击之下，BYOD打破了原有企业网络边界，正是这种边界的模糊性使BYOD成为企业信息安全体系的薄弱环节，需要新的方法保护企业数据的安全。

同一移动终端设备上既有个人应用，又有企业应用个数据，个人应用可以随意访问、存取企业数据，从而存在企业数据被个人应用非法上传、共享和外泄的风险。如存储在手机中的办公邮件、文件、图片、通信记录以及与业务内容有关的短信等，这些敏感信息的泄露会给企业带来极大的信息安全风险。移动设备容易丢失，移动设备中所保存的企业敏感数据也因此面临泄密风险，丢失的设备也可能会成为攻击企业网络的跳板。根据国家互联网应急中心统计，2012年新发现的恶意程序超过16万，较2011年增长25倍。2013年上半年安卓手机病毒暴涨了8倍左右。同时，由于Root (超级用户权限) 权限滥用和新的黑客攻击技术，移动终端很容易成为黑客入侵渗透企业内网的跳板。

发明内容

有鉴于此，本申请要解决的一个技术问题是提供一种公私隔离的方法及装置，在移动终端上设置工作区并完成相应的操作。

一种公私隔离的方法，包括：对移动终端的系统事件进行监测，判断所述系统事件是否符合预设的工作区规则；当所述系统事件符合所述工作区规则时，在工作区空间内执行与所述系统事件对应的操作，将与所述操作相对应的数据加密并存储在所述工作区空间的数据库中。

一种公私隔离的装置，包括：事件监控模块，配置为对移动终端的系统事件进行监测，判断所述系统事件是否符合预设的工作区规则；执行模块，配置为当所述系统事件符合所述工作区规则时，在工作区空间内执行与所述系统事件对应的操作，将与所述操作相对应的数据加密并存储在所述工作区空间的数据库中。

本申请的公私隔离的方法和装置，在移动终端上建立一个安全、独立的工作区，将所

有的工作数据，即企业应用和数据存储在受保护的安全区内，使个人应用无法访问企业数据，避免企业数据被个人应用非法存取，不仅仅将企业数据和个人数据完全隔离，使 IT 部门能够更好地保护企业的应用和数据，也为员工提供了无差别的个人应用体验，达到一机两用的效果。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为根据本申请的公私隔离的方法的一个实施例的流程图；

图 2 为根据本申请的公私隔离的方法的一个实施例中对通话、短信处理的流程图；

图 3 为根据本申请的公私隔离的方法的另一个实施例中对通话、短信处理的流程图；

图 4 为根据本申请的公私隔离的装置的一个实施例的示意图；

图 5 为根据本申请的公私隔离的装置的一个实施例与企业网信息交互的示意图；

图 6 示意性地示出了用于执行根据本申请的方法的计算设备的框图；以及

图 7 示意性地示出了用于保持或者携带实现根据本申请的方法的程序代码的存储单元。

具体实施方式

下面参照附图对本申请进行更全面的描述，其中说明本申请的示例性实施例。下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

本申请的公司隔离的方法，通过在移动终端上建立一个严格的办公区域或工作区，通过加密、监测等多种手段，保证工作中的数据和应用在移动终端上的安全，与工作区对应，移动终端中还存在一个人区，用以存储于工作无关的数据。

其中，在本申请实施例中，工作区和个人区可以定义如下：在设备使用过程中，为了方便管理设备中的个人资料和工作资料，可以在设备中划出一部分磁盘存储空间，配置新的权限信息，可以用于存储和管理工作资料，可以将这部分磁盘存储空间称为工作区。而该设备中剩余的另一部分磁盘存储空间，可以用于存储、管理个人资料或者其他资料，所述剩余的另一部分磁盘存储空间可以拥有初始的权限信息，可以将这部分磁盘存储空间称为个人区。

此外，为方便操作，个人区和工作区可以具有不同的 UI (User Interface, 用户界

面), 但是可以共同使用某些系统文件。

实施例一

图1为本申请的公私隔离的方法的一个实施例的流程图, 如图1所示:

步骤101, 对移动终端的系统事件进行监测, 判断系统事件是否符合预设的工作区规

则。

步骤102, 当系统事件符合工作区规则时, 在工作区空间内执行与系统事件对应的操作,

步骤103, 将与操作相对应的数据加密并存储在工作区空间的数据库中。

本实施例中, 所谓公私隔离指的是将用户的办公相关的数据和私人数据相隔离, 其中, 移动终端可采用如游戏控制台, 膝上型计算机, 便携式媒体播放器, 板式计算机, 平板计算机, PDA, 移动计算机, 以及移动电话等等。

其中, 移动终端可以采用滑动输入, 手势输入, 触摸输入, 以及语音输入等输入形式进行输入。

本实施例中, 工作区空间的数据库是相对于移动终端中原有的数据库、或相对于移动终端中各种应用的数据库独立设置的数据库, 为工作区存储数据使用。区空间是移动终端的资源(内存和存储卡等)和用户划分的逻辑运行空间。工作区规则可以是依据联系人、短信中的关键字等进行配置。

可以在工作区空间的数据库中, 或者在移动终端的存储装置中放置工作区空间加密的数据, 加密的数据可以是涉及系统文件内的数据, 或者是用户选定的财务文件、生产文件、销售文件、市场文件、人力资源文件等内的数据; 加密的数据还可以是用户个人文件的数据, 例如: 照片、视频、日志等等。

根据本申请的一个实施例, 用户进入工作区进行有关工作(企业)操作, 例如编辑日程安排、发短信、写邮件、下载报表或拍照等等, 可以将与工作操作相同的数据人, 如日程安排、图片、邮件、报表、短信等数据进行加密, 并存储在工作区空间的数据库中, 而与工作无关的操作数据存储在给工作区空间内, 如移动终端的公共空间等, 使得公、私的数据得以隔离, 通过对数据加密使得移动终端内的其它应用即使获取数据也无法使用。

当用户查看存储在工作区空间的数据库中的数据时, 需要输入密码, 当移动终端丢失时, 由于用户设置了查看工作区数据的用户密码(此功能可以由用户根据自身的习惯、意愿进行设置), 如不知道用户密码则无法查看工作区数据, 或者, 可以通过企业管理服务器远程操作, 调用移动终端中的工作区应用, 删除移动终端中存储的工作区数据, 能够保护企业数据的安全。

实施例二

本申请实施例中, 系统事件可以包括通话事件和短信事件, 其中, 通话事件包括: 来电事件、去电事件, 其中来电事件包括已接来电事件和未接来电事件; 短信事件包括接收短信事件和发送短信事件。因此, 对于通话事件的工作区规则可以配置为通话事件的联系人存储于工作区空间的数据库中, 对于短信事件的工作区规则可以配置为短信的联系人存储于工作区空间的数据库中, 其中, 联系人的信息包括通话事件中主叫方或被叫方的电话号码MSISDN (Mobile Subscriber International ISDN/PSTN Number, 即移动台识别号

码)，以及短信事件中短信的收件人或发件人的MSISDN。

在检测到上述几种事件后可以依据具体的系统事件执行相应的操作，下面举例论述具体的公私隔离方法。

图2为根据本申请的公私隔离的方法的一个实施例中对通话、短信处理的流程图，如图2所示：

步骤201，判断系统事件是否为通话事件和短信事件。

步骤202，判断联系人是否存储在工作区空间的数据库中。

步骤203，当通话的主叫方或被叫方电话号码、或短信的发件人或收件人的电话号码存储在工作区空间的数据库中，对通话记录或短信加密，将此通话记录或短信存储在工作区空间的数据库中。

步骤204，在移动终端的通话记录或短消息记录中将此通话记录或短消息删除。

因此当系统事件为通话事件时，可以依据检测该通话事件的主叫方或被叫方的电话号码是否存储于工作区空间的数据库中确定是否符合工作区规则，如是，即存储于工作区空间的数据库中则符合工作区规则，否则不符合工作区规则。从而可以在工作区空间进行该通话，例如在工作区空间的数据库中查找联系人拨打电话，又如在工作区空间内查看未接来电的通话记录等，然后将该通话事件对应的数据如来电或去电或未接来电的记录等进行加密，并将其存储到工作区空间的数据库中。并且，可以将移动终端的通话记录中该通话事件的记录删除。本申请实施例中，移动终端的通话记录和短消息记录指的是非工作区（即个人区）的通话记录和短消息记录。

对于短信事件，与通话事件类似，当短信事件的发件人或收件人的电话号码存储于工作区空间的数据库中则符合工作区规则，否则不符合工作区规则。则在工作区空间内执行与该短信事件相关的操作，如在工作区空间内编辑、查看短信等。然后将该短信进行加密并存储在工作区空间的数据库中，并且该短信的相关记录信息如发送记录、接收记录等均可加密后存储在工作区空间的数据库中，并且，还可以将移动终端的短消息记录中将该短信删除。

本申请实施例中，还可以提供通话选项界面，由用户选择当通话事件的主叫方MSISDN或被叫方MSISDN存储在工作区空间的数据库中时，是否删除移动终端的通话记录，这样，用户能够根据自己的习惯进行设置，提高用户使用的满意度。

通过上述的步骤，能够使工作的通话、邮件与私人的通话和邮件进行隔离，从而保证工作信息的安全。

本申请实施例中，系统事件包括通话事件和短信事件，其中通话事件包括已接来电事件、去电事件和未接来电事件；短信时间包括接收短信事件和发送短信事件，基于上述系统事件详细论述公私隔离的一种可选方法。

图3为根据本申请的公私隔离的方法的另一个实施例中对通话、短信处理的流程图，该方法包括步骤S301至S312。

步骤S301, 在移动终端中建立一个用于存储企业数据的工作区。

其中, 建立该工作区的目的在于存储工作中所产生的数据, 实现将工作区中的数据与个人区的数据进行隔离存储(即公私隔离), 以便对工作区中的数据进行管理。为了保证工作区数据的安全, 工作区的数据可以采用加密的方式进行保存, 用户可以为工作区的数据设置解锁密码, 当用户输入的解锁码正确时, 才允许用户访问工作区中的数据。

以在安卓系统中为例, 在对工作区的数据设置解锁密码并隔离保存时, 可以采取如下方式: 分别创建并记录用户的个人区和工作区的Launcher, 在显示桌面前, 提示用户输入密码进行登录。若用户密码输入正确可以合法登入工作区, 则启动工作区Launcher, 给用户提供工作区的桌面, 用户可以通过该桌面进入工作区中的应用; 若用户未进行登录, 则从选择默认的个人区Launcher 启动, 用户通过该默认的Launcher进入个人区的应用, 以达到工作区和个人区的隔离。其中, Launcher为卓系统中的启动器或者桌面, 可以从桌面上的图标进入其他应用。

步骤S302, 对系统事件进行监听, 并判断该系统事件是否符合工作区规则。

其中, 若符合, 在工作区内执行与该事件对应的操作。若不符合, 则在个人区执行与系统事件对应的操作。

本实施例中, 为了能够更好地对工作区的数据进行管理, 移动终端中设置有通讯录来存储联系人的信息, 其中通讯录可以配置一个或多个, 以配置两个为例, 其中, 一个为配置为工作的企业通讯录, 另一个为用户的私人通讯录, 通讯录中可以保存有联系人的电话号码, 邮箱账号, 即时通讯账号等联系方式。

其中, 企业通讯录设置在上述工作区内, 企业通讯录中存储有与该用户工作相关的联系人, 例如, 企业通讯录中包括的联系人可以是该用户所处部门的全部同事, 并且该企业通讯录中也可以包括该用户的客户等。另外, 为了方便对企业通讯录进行管理和更新, 该企业通讯录还可以与服务器端同步, 即用户的企业通讯录则会定时根据服务器来进行同步更新, 例如, 将企业通讯录管理人员新加入的联系人更新至用户的企业通讯录中。需要说明的是, 处于相同部门的用户, 其所面对的工作联系人往往是不同的, 例如, 用户A所属行政部, 其与人事部的工作来往较为密切, 用户B也所属行政部, 而其与国际部的工作来往较为密切, 而往往从服务器同步的联系人通常仅是该部门所共同的工作联系人, 而不能完全涵盖每个同事所面对的工作联系人。本实施例为了满足不同用户的需求, 在工作区中, 还可以在上述企业通讯录中存储用户个人导入的联系人, 这些联系人可以为与该用户工作关系密切而又非本部门的联系人, 如上例所提到的客户等。个人导入联系人的设置能够使得不同的用户根据其自身的需求来设定工作区的联系人, 方便用户操作, 同时也保证了企业数据的安全。

与上述描述的工作区通讯录不同的是, 私人通讯录设置在非工作区, 可以包括与用户个人相关的联系人, 例如, 亲人、朋友等。但是, 工作区的联系人可以与用户私人通讯录中的联系人可以重合, 例如, 联系人A即为该用户的同事, 也是该用户的朋友, 则联系

人A可以同时被保存在企业通讯录和私人通讯录中，以保证企业数据的安全。

由于本实施例中存在多种不同的系统事件，因此上述步骤S302中对系统事件进行监听，依据不同的系统事件可以执行步骤的操作，具体包括如下步骤：

对系统事件进行监测，判断与系统事件对应的联系人是否为工作联系人。当为工作联系人时，确认符合工作区规则，此时，根据系统事件的类别在工作区执行相应的操作，例如编辑短信、查看短信、查看未接来电等。当不为工作联系人时，确认不符合预设规则符合，此时，根据系统事件的类别在非工作区内执行相应的操作。

其中，工作联系人为处于上述企业设定的企业通讯录中或处于上述用户个人导入到工作区的通讯录中的联系人，即该联系人的信息存储于工作区空间的数据库中。

下面分别介绍上述五种系统事件发生时，本方法的具体执行过程。

第一种情况，系统事件为接收短信事件。

当系统事件为接收短信事件时，步骤S302判断与接收短信事件对应的联系人是工作联系人时，执行步骤S303，否则执行步骤S304。

步骤S303，拦截该短信进入移动终端的短消息记录，在工作区空间查看该短信，并将该短信加密后存储到工作区的数据库中。

步骤S304，将该短信存入移动终端的短消息记录。

步骤S303拦截该短信进入移动终端的短消息记录的收件箱中（即非工作区中存储短信的位置），并将该短信加密后存储到工作区中的操作，实现了公私数据的分离，避免了与工作相关的来信处于用户的系统收件箱中而被恶意查看，从而保证了企业数据的安全。

第二种情况，系统事件为发送短信事件中。

当系统事件为发送短信事件时，步骤S302判断与发送短信事件对应的联系人是否为工作联系人。当是工作联系人时，执行步骤S305，当不是工作联系人时，则执行步骤S306。

步骤S305，拦截该短信及其发送记录进入的移动终端的短消息记录，在工作区空间编辑该短信，并将该短信以及其发送记录加密后存储到工作区空间的数据库中。

步骤S306，将该短信及其发送记录存储到移动终端的短消息记录中。

步骤S305拦截该短信及其发送记录进入的移动终端的短消息记录箱，并将该短信及其发送记录加密后存储到工作区中的操作，实现了公私数据的分离，避免了与工作相关的发信处于用户的系统发件箱中而被恶意查看，从而保证了企业数据的安全。

第三种情况，系统事件为去电事件。

当系统事件为去电事件时，步骤S302判断与去电事件对应的联系人是否为工作联系人。当是工作联系人时，执行步骤S307，当不是工作联系人，则执行步骤S308。

步骤S307，将去电记录加密后存储在工作区空间的数据库中。

步骤S308，在移动终端的通话记录中存储该去电记录。

需要说明的是，为了使得用户方便查看拨打记录，在步骤S307存储去电记录之前，

还可以包括如下操作：判断用户是否已设置在操作系统的通话记录中显示工作联系人的通话记录。当未设置在操作系统的通话记录中显示工作联系人的通话记录时，步骤S207存储去电记录之前可以将移动终端的通话记录中该去电记录删除或者拦截该去电记录进入移动终端的通话记录中。当设置在操作系统的通话记录中显示工作联系人的通话记录时，则将该拨打记录显示在移动终端的通话记录中，并同时在工作区空间的数据库中存储。并且，本实施例中，根据不同的需求，用户可以分别设置工作区中每个联系人的通话记录是否显示在系统通话记录中，也可以进行统一设置，即设置成全部通话记录显示在系统通话记录中或者全部通话记录不显示在系统通话记录中。

第四种情况，系统事件为已接来电事件。

当系统事件为已接来电事件时，步骤S302判断与接听电话事件对应的联系人是否为工作联系人。当是工作联系人时，执行步骤S309，当不是工作联系人，则执行步骤S310。

步骤S309，将该已接来电事件的记录存储在所述工作区空间的数据库中。

其中，对于系统事件的监听以及通讯记录或短消息记录中记录的删除，移动终端中不同的操作系统具有不同的方式，可以依据不同的操作系统类型确定操作方式。

例如，操作系统为安卓，首先，注册去电广播监听、由OutCallReceiver获取拨出号码，判断是否为存储在工作区空间的数据库中的联系人，如果是，则在移动终端的来电记录中删除此通话记录。监听系统来电或去电的方法主要包括：TelephonyManager.listen()（监听来电状态）。

又如，在安卓系统中对于当系统事件为去电事件或来电事件时，对操作系统的通话记录的维护（拷贝和转移），可采用如下方式：通过PhoneStateReceiver广播接收器接收去电事件和来电事件，当去电事件或来电事件时，启动CallLogObserverService服务对通话记录进行维护，包括通话记录的拷贝和转移操作。其中，PhoneStateReceiver广播接收器，保证在出现通话事件时启动CallLogObserverService服务时，并可通过操作系统提供的startService服务实现。PhoneStateReceiver广播接收器接收对于拨打电话和接听电话的事件可通过如下代码实现：

```
<intent-filter>
    <action android:name="android.intent.action.PHONE_STATE" />
    <action android:name="android.intent.action.NEW_OUTGOING_CALL" />
</intent-filter>
```

具体地，在启动CallLogObserverService服务之前，还需要获取对于操作系统通讯录的读写权限，可采用如下方式：在androidmanifest.xml中声明用到的权限：

```
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
```

其中，在进行通话记录的拷贝时可通过 CallLogObserverService服务实现：在CallLogObserverService服务启动的过程中注册了一个监听服务ContentObserver，以及处理变化的Handler；监听服务ContentObserver用语监听系统的通话记录数据库的变化

(其URI为android.provider.CallLog.Calls.CONTENT_URI)，当有通话记录的变动时，调用该Handler的onChange方法，更新工作区的通话记录数据库。

步骤S310，将该已接来电事件产生的通话记录存储在移动终端的通话记录中。

其中，当来电事件的工作联系人同时也是私人通讯路中的联系人时，在步骤S309存储该来电事件的记录之前，还可以包括如下操作：提示用户是否在移动终端的通话记录中存储该已接来电事件的记录。当用户选择否时，通过步骤S209将该次已接来电事件产生的通话记录在移动终端的通话记录中删除或预先拦截其进入移动终端的通话记录中。当用户选择是时，则将该次已接来电事件的记录存储在移动终端的通话记录中，然后对该已接来电事件的记录加密后存储在工作区空间的数据库中。上述提示用户操作能够根据用户的不同需求来实现保存或者删除通话记录，保证了工作区数据安全性的同时也便于用户操作。

第五种情况，系统事件为未接来电事件。

当系统事件为未接来电事件时，步骤S302判断与未接来电事件对应的联系人是否为工作联系人。当是工作联系人时，执行步骤S311，当不是工作联系人，则执行步骤S312。

步骤S311，将该未接来电事件的记录存储到所述工作区空间的数据库中。

步骤S312，将该未接来电事件的记录存储在移动终端的通话记录中。

需要说明的是，当未接来电事件的MSISDN（即工作联系人的MSISDN）与私人通讯录中的联系人的MSISDN重合时，在步骤S311存储该未接来电事件的记录之前，还可以包括如下：提示用户是否在移动终端的通话记录中存储该未接来电事件的记录。当用户选择否时，通过步骤S311将该条未接来电事件的记录在移动终端的通话记录中删除，或拦截该来电事件的记录进入移动终端的通话记录中。当用户选择是时，则将该次未接来电事件的记录存储在移动终端的通话记录中。

需要说明的是，本实施上述所描述的五种系统事件只是示例性的，并不限制本申请实施例所保护的范 围，其他移动终端能够支持的系统事件也在本申请实施例所保护的范 围之内。

本申请实施例通过在移动终端中建立存储企业数据的工作区，并以加密方式保存，同时对系统事件进行监测，当符合工作区规则时，在工作区内执行与该事件对应的操作。可见，本申请实施例所提供的方法可以避免由于恶意程序的攻击造成的企业数据的泄漏，即使移动终端丢失，由于工作区已加密，其他人也不能读取得到企业数据，保证了企业数据的安全性，并且能不被恶意程序所获取。

实施例三

本申请实施例中，系统事件还可以包括：邮件事件，则该邮件事件的工作区规则可以配置为邮件的发件人或收件人的邮箱账号存储于工作区空间的数据库中。因此，根据本申请的一个实施例，可以提供邮件规则选项界面，由用户设置只能在工作区或使用工作区应用接收的邮箱账号，并将邮箱账号存储在工作区空间的数据库中，使得工作邮件和私人

邮件的数据进行隔离。

当判断系统事件为接收邮件、并且发件人的邮箱账号存储在工作区空间的数据库中时，该系统事件符合工作区规则，因此可以在工作区空间内执行编辑邮件、查看邮件、下载附件、上传附件等与邮件事件相关的操作，并且可以将邮件内容以及下载的邮件附件加密，并将加密后的邮件内容以及下载的邮件的附件存储在工作区空间的数据库中。

本申请实施例中，用户在工作区空间的数据库中设置的企业通信录中可以存储工作联系人的各种信息包括：手机号码MSISDN、座机号码、邮箱账号等。当通话事件的主叫方MSISDN或被叫方MSISDN、或短信事件的发件人MSISDN或收件人MSISDN、或邮件事件的发件人邮箱账号或收件人邮箱账号是否存储于企业通讯录中，如果是则对该系统事件对应的通话记录、短信、邮件等数据加密并存储在工作区空间的数据库中。

由于工作区数据保密性要求较高，因此可以设置密码锁定工作区，当对用户输入的密码验证成功后，工作区解锁用户可进入工作区查看通话记录、短信、邮件或邮件附件等，对存储在工作区空间的数据库中的通话记录、短信、邮件或邮件附件进行解密从而供用户查看。

由于有些邮件的附件需要过第三方软件打开，因此当判断用户结束查看时，删除第三方软件打开的通过解密产生的通话记录、短信、邮件或邮件附件的临时文件。当用户退出浏览器时，将浏览器的缓存清除。

本申请实施例中对工作区数据进行加密时，可以采用多种加密算法，例如，通话记录、短信、邮件或邮件附件进行加密的加密算法为AES256加密算法。

根据本申请的一个实施例，在移动终端上运行工作区应用并进入工作区，对用户提供联系人选项界面，用户从移动终端通讯录的联系人中选取工作联系人，并将用户选取的工作联系人存储在工作区空间的数据库中，可以方便用户设置工作联系人。

接收服务器侧（如企业的企业管理平台）发送的工作区策略和规则，并将工作区策略和规则存储在工作区的数据库中，依据该工作区策略和规则可以方便地进行移动终端中的工作区应用的更新或策略、规程的更新。

根据本申请的一个实施例，移动终端可以将财务文件、生产文件、销售文件、市场文件、人力资源文件等发送到企业管理平台，并接收企业管理平台的处理结果，并加密存储。

根据本申请的一个实施例，对移动终端的系统事件进行监测、将移动终端中的记录删除可以根据不同的操作系统进行设置，例如，移动终端中的操作系统为安卓系统。

先登录工作区应用后会记录系统原来的个人区的默认Launcher（安卓系统中的桌面启动器，安卓系统的桌面UI统称为Launcher），如果没有设置过或者已经是本工作区应用，则从已有的launcher 随机选择一个作为个人区的Launcher。

根据本申请的一个实施例，对在移动终端中安装的工作区应用进行加固处理，例如，移动终端中的操作系统为安卓，因为安卓上的应用多为 JAVA 语言开发，由于用 JAVA 开发

的应用编译的最终结果不是二进制文件，比较容易通过反编译文件获取一些信息，例如，密码，部分代码等等。

改变工作区应用的 class.dex 文件的内容，例如改变一些属性名称，并对其内容通过一些算法进行加密。在工作区应用的 apk 运行时再动态的去解密，还原内容，在修改 class.dex 的时候要保证符合 dex 文件的固有格式。在对工作区应用重新打包的过程中，修改 Android 程序的全局配置文件 AndroidManifest.xml 里面的一些配置信息，例如 package; application、service、provider 的 name 属性；provider 的 authorities 属性，并且修改 .smali 文件里面和上面这些属性对应的一些引用。

通过上述的对移动终端中安装的工作区应用进行加固处理，可以防止程序被人轻易逆向，获取密钥体系等关键信息，加固同时给程序增加了数据加密的功能，增加安全系数。

根据本申请的一个实施例，第三方软件在运行时有时需要调用工作区应用，例如写字板、邮件客户端或其他的一些应用等等，由于工作区空间的数据库中存储的数据文件是经过加密处理后保存的，因此工作区应用提供了一个编译好的 so 文件，从而通过 o 文件实现对 class.dex 文件的内容加密、解密等处理。

并且，可以通过在第三方应用中注入代码，使得第三方应用 apk 初始化时去调用这个 so 文件，保证 so 库运行的时机比第三方应用的读写文件的时间早，避免出现 class.dex 文件变成“一半加密的状态”，导致文件损坏，无法实现公私隔离的功能。在第三方应用运行的过程中，工作区应用提供的 so 库里面会拦截这个第三方应用的所有文件操作，实现加密，可以实现公私隔离的功能。

图 4 为根据本申请的公私隔离的装置的一个实施例的示意图，如图 4 所示，公私隔离的装置 42 包括：事件监控模块 422 和执行模块 424。

事件监控模块 422，配置为对移动终端的系统事件进行监测，判断系统事件是否符合预设的工作区规则。执行模块 424，配置为当系统事件符合工作区规则时，例如，工作区规则为通话、短信的联系人、邮箱、短信中的关键字等是否存储在工作区数据库中等等。在工作区空间内执行与系统事件对应的操作，将与操作相对应的数据加密并存储在工作区空间的数据库中。

根据本申请的一个实施例，所述系统事件包括：通话事件和短信事件。

执行模块 424 包括通话和短信执行模块 4242、用户选项模块 4244 和邮件执行模块 4246。

通话和短信执行模块 4242，配置为当判断通话事件的主叫方的电话号码或被叫方的电话号码、或短信事件的发件人的电话号码或收件人的电话号码存储在工作区空间的数据库中时，所述系统事件符合所述工作区规则；以及对所述通话事件的记录或所述短信时间的短信加密，将所述通话事件的记录或所述短信事件的短信存储在所述工作区空间的数据库中。

所述通话和短信执行模块 4242，还配置为在所述移动终端的通话记录中将所述通话事

件的记录删除，或在所述移动终端的短消息记录中将所述短信事件的短信删除。

所述通话和短信执行模块4242，还配置为拦截所述通话事件的记录进入移动终端的通话记录中，或拦截所述短信事件的短信进入所述移动终端的短消息记录中。

用户选项模块4244，配置为提供通话选项界面，用户选择当来电的主叫方或被叫方电话号码存储在工作区空间的数据库中时，是否删除所述移动终端的通话记录。

用户选项模块4244，还配置为提供邮件规则选项界面，由用户设置只能在工作区或使用工作区应用接收的邮箱账号，并将邮箱账号存储在工作区空间的数据库中。

邮件执行模块4246，配置为当判断系统事件为接收邮件，并且发件人的邮箱账号存储在工作区空间的数据库中时，所述系统事件符合所述工作区规则；以及，将邮件内容以及下载的邮件附件加密，并将邮件内容以及下载的邮件的附件存在工作区空间的数据库中。

所述执行模块424，还配置为对用户输入的密码验证成功后，且用户进入工作区查看通话记录、短信、邮件或邮件附件时，对存储在所述工作区空间的数据库中的通话事件的记录、短信事件的短信、邮件事件的邮件或邮件事件的邮件附件进行解密；当判断用户结束查看时，通过解密产生的通话记录、短信、邮件或邮件附件的临时文件。

所述执行模块 424，还配置为当用户采用浏览器查看工作区数据库中存储的数据，且用户退出浏览器时，将浏览器的缓存清除。

所述用户选项模块 4244，还配置为在移动终端上运行工作区应用并进入工作区，对用户联系人选项界面，接收用户从移动终端通讯录的联系人中选取的工作联系人，并将用户选取的工作联系人存储在工作区空间的数据库中。

策略和规则接收模块 426，配置为接收企业管理平台发送的工作区策略和规则，并将工作区策略和规则存储在工作区的数据库中。例如，工作区规则包括：通话、短信的联系人、邮箱、短信中的关键字是否存储在工作区数据库中等等。工作区策略包括：当通话或短信的联系人为设定的工作区联系人时，将通话记录、短信加密存储、并在移动终端中删除记录；当用户查看工作区中的信息时需要进行密码鉴权；定期下载、更新工作区应用；定期杀毒；设置工作区应用的优先级等等。

图 5 为根据本申请的公私隔离的装置的一个实施例与企业网信息交互的示意图。如图 5 所示，在移动终端 4 中设置公私隔离的装置 42，公私隔离的装置 42 可以有多种实现方式，例如，集成电路、插件、应用等等。

公私隔离的装置 42 接收企业管理平台（服务器）52 发送的工作区策略和规则，并将工作区策略和规则存储在工作区的数据库中。通过部署于企业网内部的企业管理平台（服

务器) 52, 管理员可以轻松实现移动终端管理、策略管理下发、企业应用管理等, 可以降低管理的复杂度, 节约 IT 人力投入。

通过部署在企业网内部中的邮件、业务、OA 服务器 52 可以实现移动终端 4 的报表、公文下发等。公私隔离的装置 42 与邮件、业务、OA 服务器 54 进行通信, 进行业务操作, 例如收发短信、写邮件或下载公文等等, 将文件、图片、邮件、短信等数据进行加密, 并存储在工作区空间的数据库中。

本申请的公私隔离的方法和装置, 不仅仅可以配置为移动终端中, 也可以应用在个人 PC、平板电脑等个人终端中。

本申请的公私隔离的方法和装置, 在不影响员工对个人应用使用的感受的基础上, 在移动终端上建立一个安全、独立的工作区, 将所有的工作数据, 即企业应用和数据存储在受保护的安全区内。个人应用无法访问企业数据, 避免企业数据被个人应用非法存取, 不仅仅将企业数据和个人数据完全隔离, 使 IT 部门能够更好地保护企业的应用和数据, 也为员工提供了无差别的个人应用体验, 达到一机两用的效果。

可能以许多方式来实现本发明本申请的方法和系统。例如, 可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本发明本申请的方法和系统。用于配置为方法的步骤的上述顺序仅是为了进行说明, 本发明本申请的方法的步骤不限于以上具体描述的顺序, 除非以其它方式特别说明。此外, 在一些实施例中, 还可将本发明本申请实施为记录在记录介质中的程序, 这些程序包括用于配置为实现根据本发明本申请的方法的机器可读指令。因而, 本发明本申请还覆盖存储用于配置为执行根据本发明本申请的方法的程序的记录介质。

本申请的描述是为了示例和描述起见而给出的, 而并不是无遗漏的或者将本申请限于所公开的形式。很多修改和变化对于本领域的普通技术人员而言是显然的。选择和描述实施例是为了更好说明本申请的原理和实际应用, 并且使本领域的普通技术人员能够理解本申请从而设计适于特定用途的带有各种修改的各种实施例。

本发明的各个部件实施例可以以硬件实现, 或者以在一个或者多个处理器上运行的软件模块实现, 或者以它们的组合实现。本领域的技术人员应当理解, 可以在实践中使用微处理器或者数字信号处理器 (DSP) 来实现根据本发明实施例的公私隔离设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序 (例如, 计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上, 或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到, 或者在载体信号上提供, 或者以任何其他形式提供。

例如, 图 6 示出了可以实现根据本发明的公私隔离的方法的计算设备。该设备传统上包括处理器 610 和以存储器 620 形式的计算机程序产品或者计算机可读介质。存储器 620 可以是诸如闪存、EEPROM (电可擦除可编程只读存储器)、EPROM、硬盘或

者 ROM 之类的电子存储器。存储器 620 具有用于执行上述方法中的任何方法步骤的程序代码 631 的存储空间 630。例如，用于程序代码的存储空间 630 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 631。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 7 所述的便携式或者固定存储单元。该存储单元可以具有与图 6 的设备中的存储器 620 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 631'，即可以由例如诸如 610 之类的处理器读取的代码，这些代码当由服务器运行时，导致该服务器执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权利要求书

1、一种公私隔离的方法，其特征在于，包括：

对移动终端的系统事件进行监测，判断所述系统事件是否符合预设的工作区规则；

5 当所述系统事件符合所述工作区规则时，在工作区空间内执行与所述系统事件对应的操作，将与所述操作相对应的数据加密并存储在所述工作区空间的数据库中。

2、如权利要求1所述的方法，其特征在于：

所述系统事件包括：通话事件和短信事件；

10 当判断所述通话事件的主叫方的电话号码或被叫方的电话号码、或短信事件的发件人的电话号码或收件人的电话号码存储在所述工作区空间的数据库中时，所述系统事件符合所述工作区规则；

将与所述操作相对应的数据加密并存储在所述工作区空间的数据库中，包括：对所述通话事件的记录或所述短信事件的短信加密，将所述通话事件的记录或所述短信事件的短信存储在所述工作区空间的数据库中。

15 3、根据权利要求2所述的方法，其特征在于，将所述通话事件的记录或所述短信事件的短信存储在所述工作区空间的数据库中之后，还包括：

在所述移动终端的通话记录中将所述通话事件的记录删除，或在所述移动终端的短消息记录中将所述短信事件的短信删除。

4、根据权利要求2所述的方法，其特征在于，所述将所述通话事件的记录或所述短信事件的短信存储在所述工作区空间的数据库中之前，还包括：

20 拦截所述通话事件的记录进入移动终端的通话记录中，或拦截所述短信事件的短信进入所述移动终端的短消息记录中。

5、如权利要求2所述的方法，其特征在于，所述在所述移动终端的通话记录中将所述通话事件的记录删除之前，还包括：

25 提供通话选项界面，由用户选择当来电的主叫方或被叫方电话号码存储在所述工作区空间的数据库中时，是否删除所述移动终端的通话记录，并在用户选择删除后执行所述将通话时间的记录删除的步骤。

6、如权利要求1所述的方法，其特征在于，还包括：

提供邮件规则选项界面，由用户设置只能在工作区或使用工作区应用接收的邮箱账号，并将所述邮箱账号存储在所述工作区空间的数据库中；

30 则当判断所述系统事件为接收邮件，并且发件人的邮箱账号存储在所述工作区空间的数据库中时，所述系统事件符合所述工作区规则；

所述将与所述操作相对应的数据加密并存储在所述工作区空间的数据库中，包括：将邮件内容以及下载的邮件附件加密，并将邮件内容以及下载的邮件的附件存储在所述工作区空间的数据库中。

7、如权利要求 2 或 6 所述的方法，其特征在于，当对用户输入的密码验证成功后，且用户进入工作区查看通话记录、短信、邮件或邮件附件时，所述的方法还包括：

对存储在所述工作区空间的数据库中的通话事件的记录、短信事件的短信、邮件事件的邮件或邮件事件的邮件附件进行解密；

5 当判断用户结束查看时，删除通过解密产生的通话记录、短信、邮件或邮件附件的临时文件。

8、如权利要求 7 所述的方法，其特征在于，还包括：

若用户采用浏览器查看工作区数据库中存储的数据，当用户退出浏览器时，将浏览器的缓存清除。

10 9、如权利要求 7 所述的方法，其特征在于，还包括：

在移动终端上运行工作区应用并进入工作区，对用户提供联系人选项界面，接收用户从移动终端通讯录的联系人中选取的工作联系人，并将用户选取的工作联系人存储在所述工作区空间的数据库中；

15 接收企业管理平台发送的工作区策略和规则，并将所述工作区策略和规则存储在所述工作区空间的数据库中。

10、一种公私隔离的装置，包括：

事件监控模块，配置为对移动终端的系统事件进行监测，判断所述系统事件是否符合预设的工作区规则；

20 执行模块，配置为当所述系统事件符合所述工作区规则时，在工作区空间内执行与所述系统事件对应的操作，将与所述操作相对应的数据加密并存储在所述工作区空间的数据库中。

11、如权利要求 10 所述的装置，其特征在于，所述执行模块包括：通话和短信执行模块；

25 所述系统事件包括：通话事件和短信事件；所述通话和短信执行模块，配置为当判断所述通话事件的主叫方的电话号码或被叫方的电话号码、或短信事件的发件人的电话号码或收件人的电话号码存储在工作区空间的数据库中时，所述系统事件符合所述工作区规则；以及对所述通话事件的记录或所述短信时间的短信加密，将所述通话事件的记录或所述短信事件的短信存储在所述工作区空间的数据库中。

12、如权利要求 11 所述的装置，其特征在于：

30 所述通话和短信执行模块，还配置为在所述移动终端的通话记录中将所述通话事件的记录删除，或在所述移动终端的短消息记录中将所述短信事件的短信删除。

13、如权利要求 11 所述的装置，其特征在于：

所述通话和短信执行模块，还配置为拦截所述通话事件的记录进入移动终端的通话记录中，或拦截所述短信事件的短信进入所述移动终端的短消息记录中。

35 14、如权利要求 11 所述的装置，其特征在于，所述执行模块还包括：

用户选项模块,配置为提供通话选项界面,用户选择当来电的主叫方或被叫方电话号码存储在工作区空间的数据库中时,是否删除所述移动终端的通话记录。

15、如权利要求6所述的装置,其特征在于,所述执行模块还包括:邮件执行模块;

所述用户选项模块,还配置为提供邮件规则选项界面,由用户设置只能在工作区或使用工作区应用接收的邮箱账号,并将所述邮箱账号存储在所述工作区空间的数据库中;

所述邮件执行模块,配置为当判断所述系统事件为接收邮件,并且发件人的邮箱账号存储在工作区空间的数据库中时,所述系统事件符合所述工作区规则;以及将邮件内容以及下载的邮件附件加密,并将邮件内容以及下载的邮件的附件存储在所述工作区空间的数据库中。

10 16、如权利要求11或13所述的装置,其特征在于:

所述执行模块,还配置为对用户输入的密码验证成功后,且用户进入工作区查看通话记录、短信、邮件或邮件附件时,对存储在所述工作区空间的数据库中的通话事件的记录、短信事件的短信、邮件事件的邮件或邮件事件的邮件附件进行解密;当判断用户结束查看时,通过解密产生的通话记录、短信、邮件或邮件附件的临时文件。

15 17、如权利要求11所述的方法,其特征在于:

所述执行模块,还配置为当用户采用浏览器查看工作区数据库中存储的数据,且用户退出浏览器时,将浏览器的缓存清除。

18、如权利要求16所述的装置,其特征在于,还包括:策略和规则接收模块;

20 所述用户选项模块,还配置为在移动终端上运行工作区应用并进入工作区,对用户提供联系人选项界面,接收用户从移动终端通讯录的联系人中选取的工作联系人,并将用户选取的工作联系人存储在所述工作区空间的数据库中;

所述策略和规则接收模块,配置为接收企业管理平台发送的工作区策略和规则,并将所述工作区策略和规则存储在所述工作区空间的数据库中。

25 19、一种程序,包括可读代码,当所述可读代码在计算设备上运行时,导致所述计算设备执行根据权利要求1-9中的任一个所述公私隔离的方法。

20、一种可读介质,其中存储了如权利要求19所述的程序。

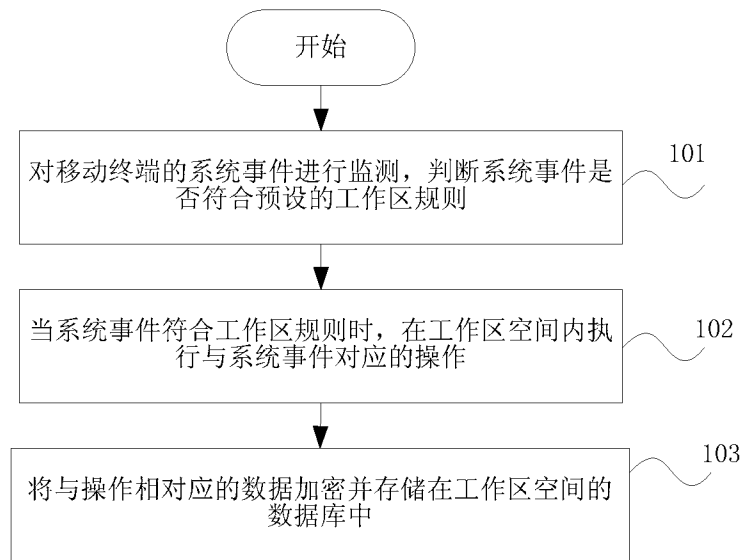


图 1

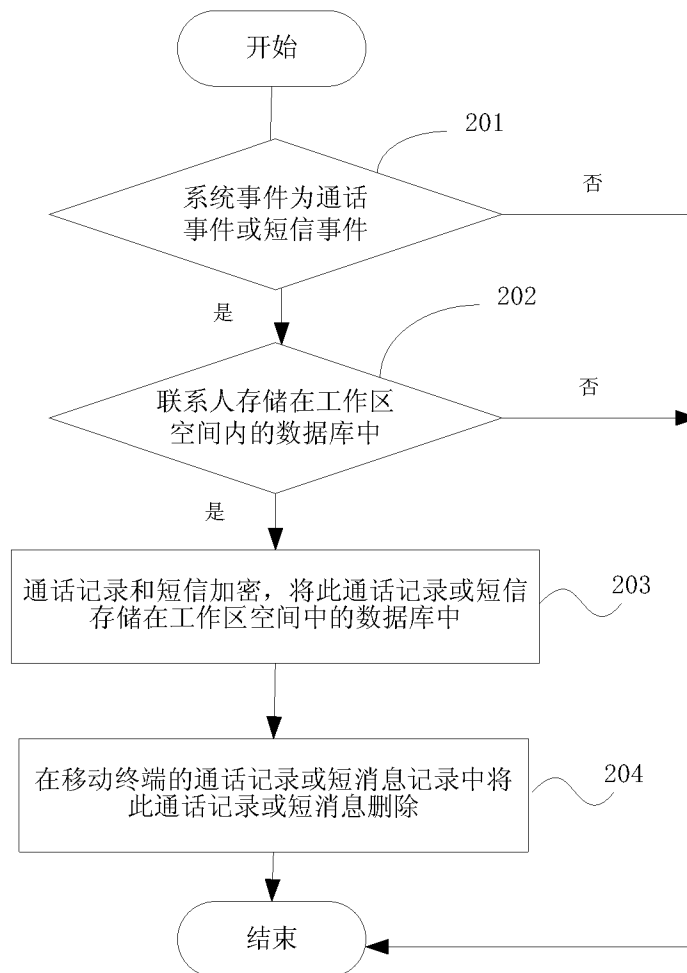


图 2

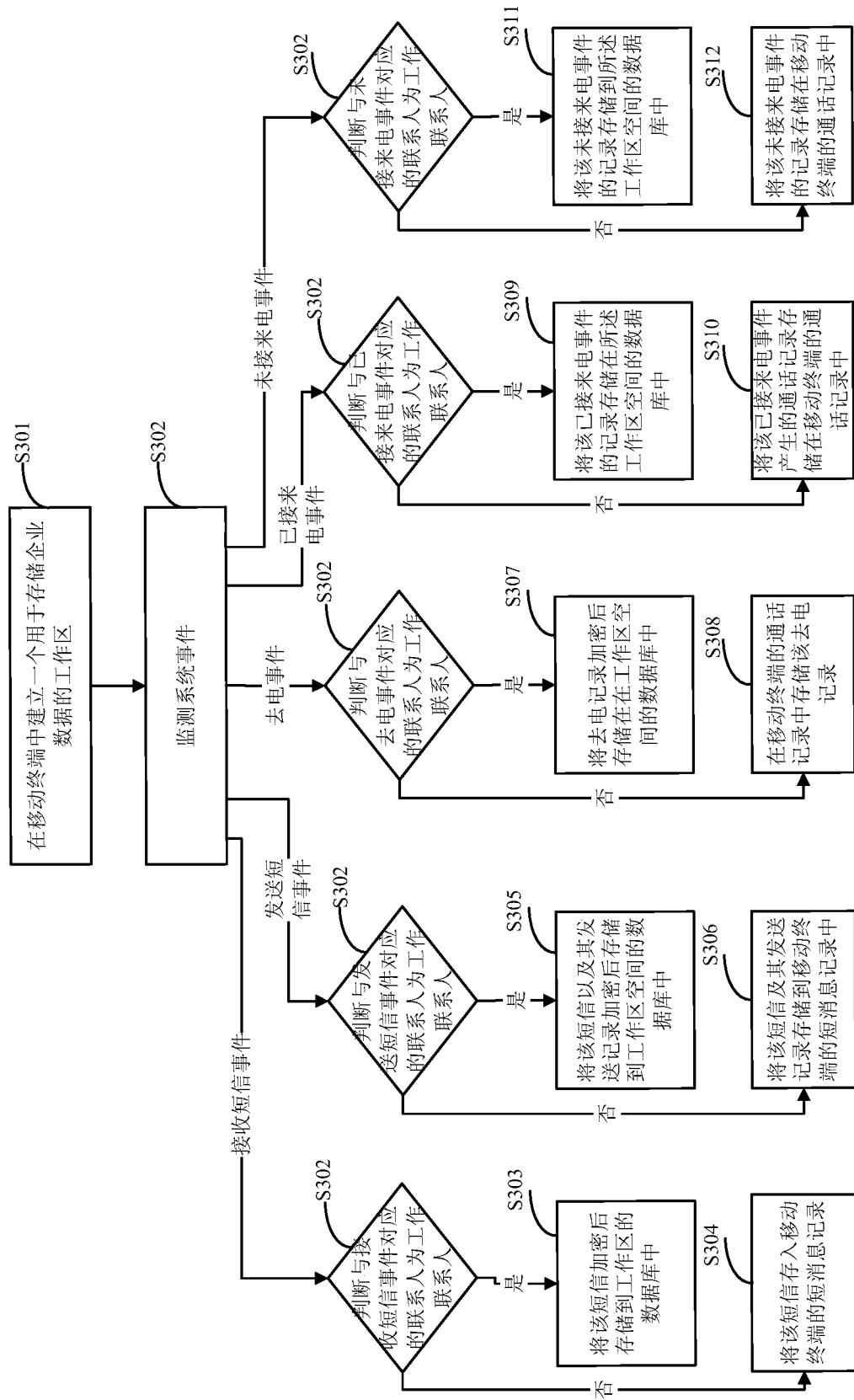


图 3



图 4

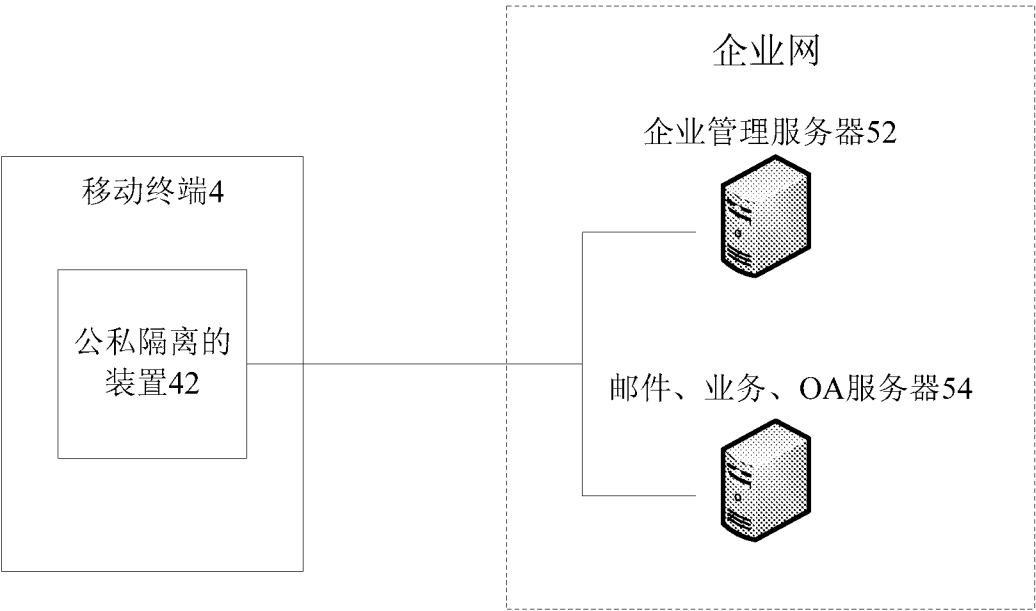


图 5

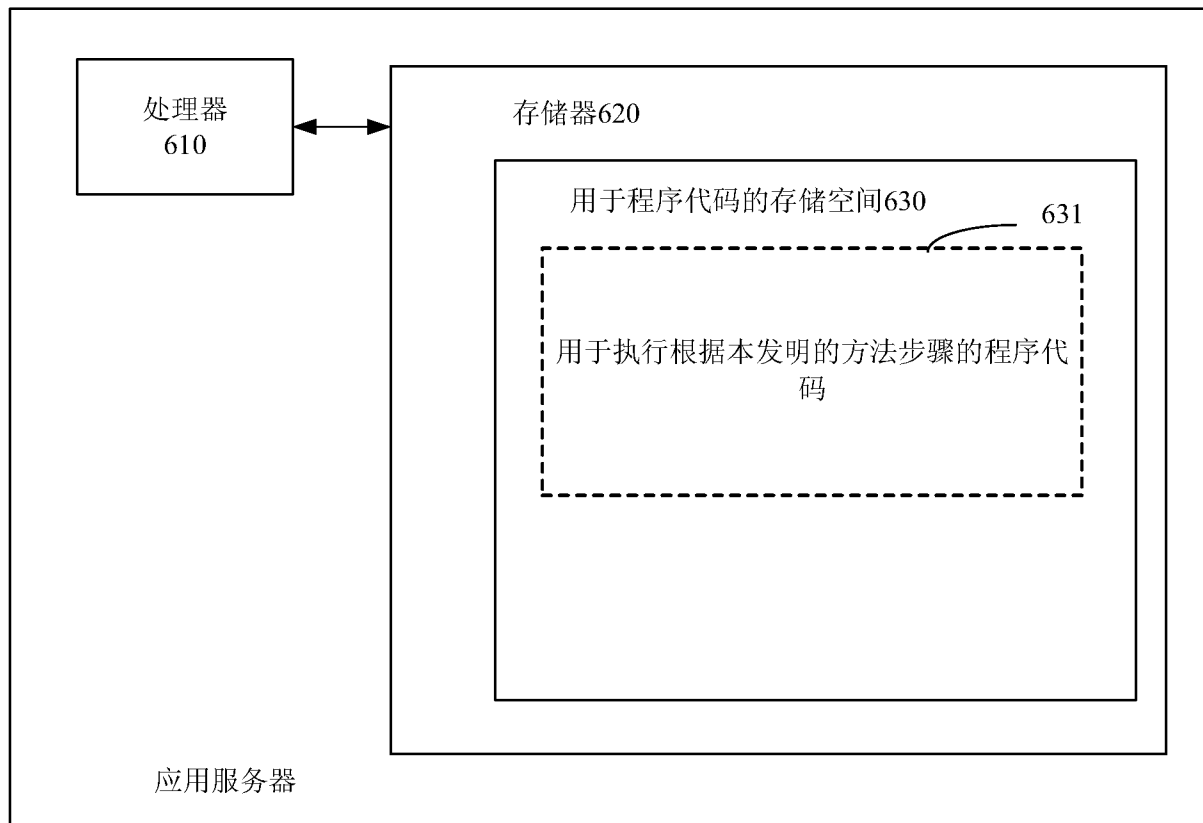


图 6

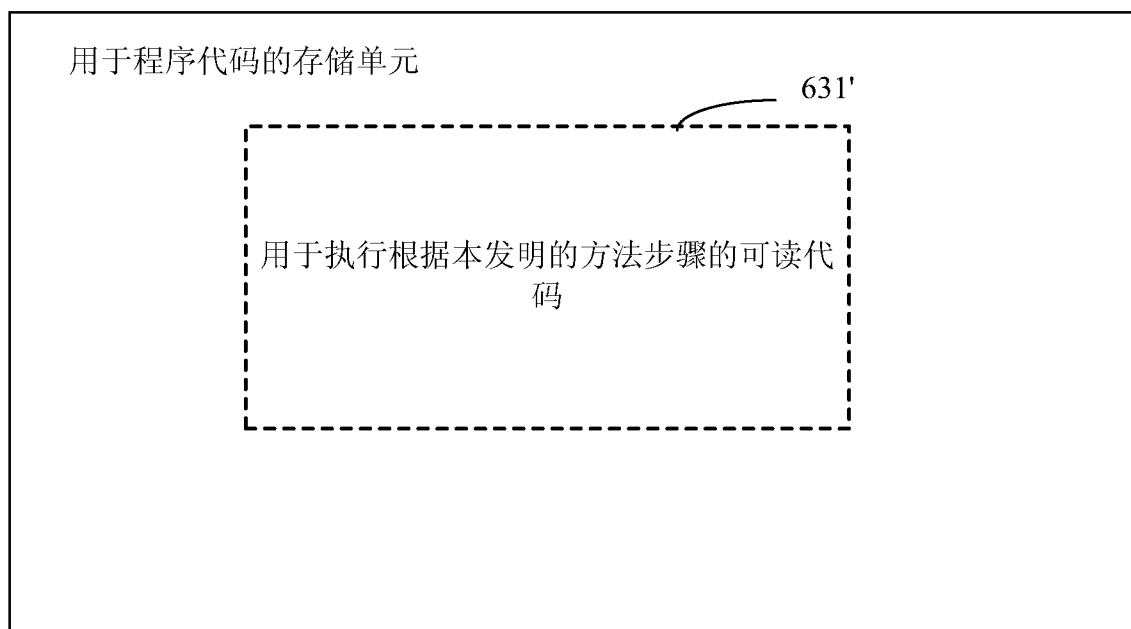


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/087815

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; H04Q; H04W; 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)

CNPAT, CNKI, WPI, EPODOC: public, private, separate, area, personal, protect, work, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1845032 A (HANGZHOU BIRDSOFT CO., LTD.) 11 October 2006 (11.10.2006) claims 1-9, and description, page 5, the sixth paragraphs, to page 7, the third paragraph	1-18
PX	CN 103647784 A (BEIJING QIHOO TECHNOLOGY CO. et al.) 19 March 2014 (19.03.2014) claims 1-5, and description, paragraphs [0024]-[0081]	1-3, 5-12, 14-18
PX	CN 103685266 A (BEIJING QIHOO TECHNOLOGY CO. et al.) 26 March 2014 (26.03.2014) claims 1-10, and description, paragraphs [0099]-[0168]	1, 10
A	US 2003051152 A1 (WUIDART, LUC et al.) 13 March 2003 (13.03.2003) the whole document	1-18

☐ 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	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“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
“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	“&” document member of the same patent family

Date of the actual completion of the international search 28 November 2014	Date of mailing of the international search report 30 December 2014
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 WU, Wenchen Telephone No. (86-10) 62414445

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/087815

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1845032 A	11 October 2006	None	
CN 103647784 A	19 March 2014	None	
CN 103685266 A	26 March 2014	None	
US 2003051152 A1	13 March 2003	JP 2003177971 A	27 June 2003
		FR 2829603 A1	14 March 2003
		EP 1291868 A1	12 March 2003

国际检索报告

国际申请号

PCT/CN2014/087815

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, H04Q, H04W, 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))

CNPAT, CNKI, WPI, EPDOC: 公, 私, 隔离, 分开, 分区, 区域, 个人, 保护, 工作, 加密, 私密, public, private, separate, area, personal, protect, work, encrypt

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 1845032 A (杭州波导软件有限公司) 2006年 10月 11日 (2006 - 10 - 11) 权利要求1-9, 说明书第5页第6段至第7页第3段	1-18
PX	CN 103647784 A (北京奇虎科技有限公司等) 2014年 3月 19日 (2014 - 03 - 19) 权利要求1-5, 说明书第[0024]-[0081]段	1-3, 5-12, 14-18
PX	CN 103685266 A (北京奇虎科技有限公司等) 2014年 3月 26日 (2014 - 03 - 26) 权利要求1-10, 说明书第[0099]-[0168]段	1, 10
A	US 2003051152 A1 (WUIDART, LUC等) 2003年 3月 13日 (2003 - 03 - 13) 全文	1-18

☐ 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

2014年 11月 28日

国际检索报告邮寄日期

2014年 12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)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10)62019451

受权官员

武文琛

电话号码 (86-10)62414445

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/087815

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	1845032	A	2006年 10月 11日	无			
CN	103647784	A	2014年 3月 19日	无			
CN	103685266	A	2014年 3月 26日	无			
US	2003051152	A1	2003年 3月 13日	JP	2003177971	A	2003年 6月 27日
				FR	2829603	A1	2003年 3月 14日
				EP	1291868	A1	2003年 3月 12日

表 PCT/ISA/210 (同族专利附件) (2009年7月)