(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 1 月 10 日 (10.01.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/006595 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2017/091491

(22) 国际申请日: 2017 年 7 月 3 日 (03.07.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深圳前海达闼云端智能科技有限公司 (CLOUDMINDS (SHENZHEN) ROBOTICS SYSTEMS CO., LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。

(72) 发明人: 周勇 (ZHOU, Yong); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。

(74) 代理人: 深圳市爱迪森知识产权代理事务所（普通合伙）(SHENZHEN AIDISEN INTELLECTUAL PROPERTY OFFICE); 中国广东省深圳市南山区南海大道 4050 号上海汽车大厦 206 室, Guangdong 518057 (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) **Title:** CONTROL METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) **发明名称**: 一种管控方法、装置及电子设备

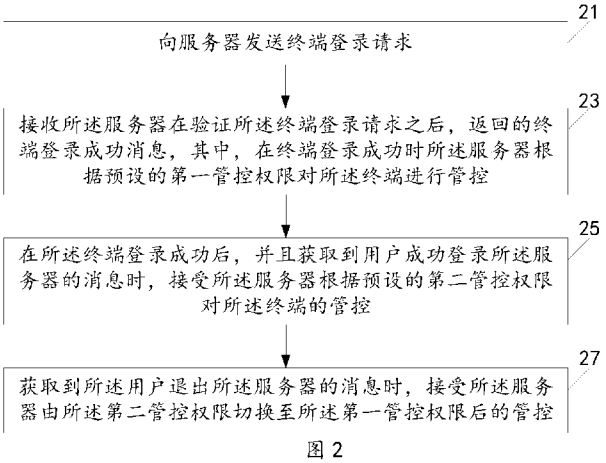


图 2

21 SEND A TERMINAL LOGIN REQUEST TO A SERVER
23 RECEIVE A TERMINAL LOGIN SUCCESS MESSAGE RETURNED AFTER THE SERVER VERIFIES THE TERMINAL LOGIN REQUEST, THE SERVER CONTROLLING THE TERMINAL ACCORDING TO A PRESET FIRST CONTROL PERMISSION WHEN THE TERMINAL SUCCESSFULLY LOGS IN
25 AFTER THE TERMINAL SUCCESSFULLY LOGS IN AND OBTAINS A MESSAGE INDICATING THAT A USER SUCCESSFULLY LOGS INTO THE SERVER, ACCEPT THE CONTROL OF THE TERMINAL PERFORMED BY THE SERVER ACCORDING TO A PRESET SECOND CONTROL PERMISSION
27 WHEN A MESSAGE INDICATING THAT THE USER QUITS THE SERVER IS OBTAINED, ACCEPT THE CONTROL AFTER THE SERVER SWITCHES FROM A SECOND CONTROL PERMISSION TO A FIRST CONTROL PERMISSION

(57) **Abstract:** A control method and apparatus, and an electronic device, which relate to the technical field of terminal control. The method comprises: sending a terminal login request to a server (21); receiving a terminal login success message returned after the server verifies the terminal login request, the server controlling the terminal according to a preset first control permission when the terminal successfully logs in (23); after the terminal successfully logs in and obtains a message indicating that a user successfully logs into the server, accepting the control of the terminal performed by the server according to a preset second control permission (25); and when a message indicating that the user quits the server is obtained, accepting the control after the server switches from a second control permission to a first control permission (27). By means of the method, management modes of a device management system are enriched, device management is facilitated, and the device utilization rate is increased.

WO 2019/006595 A1

[见续页]

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: 一种管控方法、装置及电子设备，涉及终端控制技术领域。该方法包括：向服务器发送终端登录请求(21)；接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控(23)；在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控(25)；获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控(27)。该方法丰富了设备管理系统的管理方式，方便了设备的管理，提高了设备利用率。

一种管控方法、装置及电子设备

技术领域

本申请实施方式涉及终端控制技术领域，特别是涉及一种管控方法、装置及电子设备。

背景技术

目前的设备管理系统中，如果一台设备想要接受某个服务器的管控，一般都是通过用户登录设备，设备将用户登入的身份信息发送服务器进行验证，验证通过后，用户登录服务器并且该设备接受服务器的管控，从而可以与服务器进行通信。

此外，在用户成功登录服务器后，用户的身份信息与该设备通常都是绑定的，并且用户与设备一一对应。

在实现本申请的过程中，发明人发现相关技术至少存在以下问题：必须在用户登录设备后，设备才可以接受服务器的管控；用户登录的设备只能给该用户使用，而不能满足多个用户交替的使用不同的权限使用该受管控的设备。

发明内容

本申请实施方式提供一种管控方法、装置及电子设备，解决相关技术中一台设备只能给其绑定的一位用户使用的问题。

为解决上述技术问题，第一方面，本申请实施方式采用的一个技术方案是：提供一种管控方法，应用于终端，包括：

向服务器发送终端登录请求；

接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控；

在所述终端登录成功后，并且获取到用户成功登录所述服务器的消

息时，接受所述服务器根据预设的第二管控权限对所述终端的管控；

获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

其中，在所述获取到所述用户退出所述服务器的消息时之前，还包括：

向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据。

其中，所述用户成功登录所述服务器具体包括：

根据向所述服务器发送的用户登录请求登录所述服务器；或者，

根据所述服务器分配的用户账户登录所述服务器。

其中，所述用户退出所述服务器具体包括：

根据向所述服务器发送的退出登录请求退出所述服务器；或者，

根据所述服务器推送的管控指令退出所述服务器。

第二方面，本申请实施方式采用的一个技术方案是：提供一种管控方法，应用于服务器，包括：

接收终端登录请求；

验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控；

在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控；

获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

其中，所述在获取到所述用户退出所述服务器的消息时之前，还包括：

接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据。

其中，所述用户成功登录所述服务器具体包括：

根据向所述服务器发送的用户登录请求登录所述服务器；或者，

根据所述服务器分配的用户账户登录所述服务器。

其中，所述用户退出所述服务器具体包括：

根据向所述服务器发送的退出登录请求退出所述服务器；或者，

根据所述服务器推送的管控指令退出所述服务器。

第三方面，本申请实施方式采用的一个技术方案是：提供一种管控装置，应用于终端，所述装置包括：

第一发送模块，用于向服务器发送终端登录请求；

第一接收模块，用于接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控；

第一接受模块，用于在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控；

第二接受模块，用于获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备

锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

其中，所述装置还包括：第二发送模块，用于向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据。

第四方面，本申请实施方式采用的一个技术方案是：提供一种管控装置，应用于服务器，所述装置包括：

第二接收模块，用于接收终端登录请求；

第一管控模块，用于验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控；

第二管控模块，用于在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控；

第三管控模块，用于获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

其中，所述装置还包括：

备份模块，用于接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据。

第五方面，本申请实施方式的一个技术方案是：提供一种电子设备，包括：至少一个处理器；以及，与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行如上所述的方法。

在本申请实施例中，通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用。该实施方式丰富了设备管理系统的管理方式，方便了设备的管理，提高了设备利用率。

附图说明

图 1 是本申请实施例提供的应用场景示意图；

图 2 是本申请实施例一提供的一种管控方法的流程图；

图 3 是本申请实施例二提供的一种管控方法的流程图；

图 4 是本申请实施例三提供的一种管控方法的流程图；

图 5 是本申请实施例四提供的一种管控方法的流程图；

图 6 是本申请实施例五提供的一种管控装置的结构框图；

图 7 是本申请实施例六提供的一种管控装置的结构框图；

图 8 是本申请实施例七提供的一种系统的结构框图；

图 9 是本申请实施例八提供的一种电子设备的结构示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及本申请实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体本申请实施例仅用以解释本申请，并不用于限定本申请。

图 1 是本申请实施例提供一种管控方法的可选地一应用场景的示意图。如图 1 所示，该应用场景包括智能机器人 1 和服务器 2。智能机器人 1 和服务器 2 建立连接后，智能机器人 1 接受服务器 2 的管控。之后，

智能机器人 1 即可接受服务器 2 管理平台的管控,管理平台可发送铃声、消息、定位等各种指令，也可按需求推送部分和登录账户不相关的特定策略管控机器人 1，或推送部分和登录账户不相关的特定应用给该智能机器人 1。此时的智能机器人 1 虽然受控，但还没有登录具体的登录账户，所能收到的策略和应用的管控都不和特定登录账户相关。接着智能机器人 1 根据登录账户的鉴权信息登录服务器 2，并获得与登录账户相关的服务内容。智能机器人 1 登录账户登录后，在登录账户不退出的情况下，除了接受和登录账户不相关的管控操作、管控策略、配置和所有受管控的终端都可以安装的应用程序之外，智能机器人 1 还开始接受和登录账户相关的管控操作、管控策略和安装推送。如果当前登录账户退出使用，该登录账户需要遵循的管控策略和可以安装的应用程序都会从智能机器人 1 上删除，智能机器人 1 恢复到登录账户登录前的状态，依然接受和登录账户不相关的各种管控。此时任何合法登录账户就可以根据需要登录并接着使用该受管控的智能机器人 1。

现有技术中，通常没有登录账户登录的智能机器人1，不能接受服务器2的管控。并且登录账户登录后，一个智能机器人1对应一个登录账户，只能给一个登录账户使用，智能机器人1和登录账户绑定。无法满足多个登录账户可随意交替用不同权限使用同一台受控智能机器人1。

请再参阅图1，在本申请实施例提供的可能应用场景中，智能机器人1在没有登录账户登录的情况下就可以接受服务器2的管控，多个用户中不同的用户可以交替用不同权限使用同一台受控智能机器人1。

需要说明的是，图1仅示出了一个机器人和一台服务器，本领域技术人员可以理解的是，该应用场景还可以包括人任意数量的机器人和服务器。

结合上述应用场景，下述实施例提供了具体的管控方法和管控装置。在下述实施例中，终端包括：手机、平板电脑、PC、智能机器人等电子设备。

实施例一

参阅图 2，本申请的第一实施例，提供一种管控方法，所述方法的执行主体为终端，所述方法包括：

步骤21、向服务器发送终端登录请求。

步骤23、接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控。

在本实施例中，由终端向服务器发送登录请求，此时，该终端处于非管控状态，并且不存在用户登录。

在非受管控的终端上，通过内置管控软件或安装的管控软件输入服务器的地址信息，发送登录请求到服务器。具体可根据需要，输入服务器规定的信息或自动携带某些可用于唯一标识该终端的信息。登录请求也可附加输入类似于公司或部门的信息，限制终端以后可以被多用户使用，但仅限特定团体内的用户。

通过输入的服务器地址信息，登录请求携带服务器所需的信息，服务器可根据配置决定是否允许该终端接受管理平台的管控。

如果服务器对终端验证无误，则返回正确的结果，通知终端已受管控。但该已受管控的终端并没有关联的登录账户。

此时与服务器建立连接的终端即可接受服务器管理平台的管控，并且服务器根据预设的第一管控权限管控所述终端。基于所述第一管控权限，服务器可发送铃声、消息、定位等各种信息至终端，也可按需求推送部分和登录账户不相关的管控操作或管控策略，以管控终端，或推送部分和登录账户不相关的特定应用给该终端。此时的终端虽然受控，但还没有登录具体的登录账户，所能收到的管控操作、管控策略和应用的管控，都不和特定登录账户相关。

其中，所述第一管控权限包括基础操作，该基础操作即与登录账户不相关的全部操作，服务器管控下的所有终端都可以执行所述基础操作。所述基础操作例如但并不仅限于：设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级中的一种或几种。

此外，终端也可将终端的基本信息主动向服务器上报，上报所述基本信息也即是执行所述基本操作，此时，所述基本操作例如但并不仅限于：发送电源余量、发送磁盘余量、发送内存状态、发送设备是否被破

解的消息、发送开机时长、发送设备和登录账户不相关的日志中的一种或几种。

步骤25、在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控。

其中，所述用户成功登录所述服务器可以是根据向所述服务器发送的用户登录请求登录所述服务器；具体地，终端接收用户输入的登录账户的鉴权信息，并根据登录账户的鉴权信息发送用户登录请求到服务器，服务器对登录账户的鉴权信息进行鉴权。经过对登录账户鉴权信息的鉴权并验证通过后，在服务器上的管理平台对通过该登录账户进行服务器登录的终端进行标记，并且用户成功登录所述服务器。

所述用户成功登录所述服务器还可以是根据所述服务器分配的用户账户登录所述服务器。也即是服务器主动的为终端分配用户，配置好用户至终端后，在服务器上的管理平台对该终端进行标记。

此时，服务器根据预设的第二管控权限对通过登录账户登录服务器的终端进行管控，并且服务器会推送与该终端登录账户相关的管控操作、管控策略或应用等相应的服务内容。同时，服务器会根据需要记录使用设备的日志。

其中，所述第二管控权限包括专属操作以及上述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。在有用户登录受控的终端时，终端和服务器之间的通信可以是和用户账户无关的基础操作，也可以是与该用户账户相关的专属操作。

步骤27、获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

在本实施例中，可以通过以下两种方式退出所述服务器。

方式一：根据向所述服务器发送的退出登录请求，退出所述服务器。在这里，所述终端可以主动向服务器请求退出所述登录账户，具体的，终端发送退出登录请求指令到服务器，服务器根据接收到的退出登录请求指令，返回确认退出登录的指令，从而所述登录账户从所述终端上退

出。

方式二：接收服务器推送的管控指令，并根据所述管控指令退出所述服务器。在这里，服务器可以主动的要求所述登录账户从所述终端上退出。

当登录账户退出登录后，服务器的管控权限由第二管控权限切换至第一管控权限，并且所述终端接受第一管控权限的管控。此时，该终端上所有与用户登录账户相关的信息（比如收到的策略和下载的应用等）都可以被清除。在服务器侧，该用户登录账户的信息也被清除，此时，服务器管控的终端不存在用户登录，但该终端仍受控于所述服务器。

此外，其他用户可以根据该用户的鉴权信息登录服务器，从而接受服务器第二管控权限的管控，服务器会推送与该登录的用户相关的管控操作、管控策略或应用等相应的服务内容。同时，服务器会根据需要记录使用设备的日志。在该用户退出登录后，终端接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控，其他用户可以根据其相应的权限登录服务器，重复上述过程。在这里，一台受控于服务器的终端可以被多个用户交替的使用不同的权限访问，从而解决了一台终端只能被一个用户使用的问题。

本申请实施例提供了一种管控方法，通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用。该实施方式丰富了设备管理系统的管理方式，方便了设备的管理，提高了设备利用率。

实施例二

参阅图 3，本申请的第二实施例提供了一种管控方法，图 3 与图 2 的主要区别在于，在所述获取到所述用户退出所述服务器的消息时之前，所述方法还包括：

步骤 26、向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据。

在本实施例中，在所述用户登录所述终端期间，其产生的所有数据

可以根据需要进行备份，以便在该用户再次登录终端时，可以获取其备份的历史数据。需要说明的是，所述用户再次登录的终端并不一定就是其备份数据时所登录的终端，该终端可以是全部受管控的设备中的任一设备。

本申请实施例提供了一种管控方法，该方法通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用，此外，在用户登录了终端时，还可以备份与该用户相关的数据。该实施方式方便了设备的管理，保证了用户数据的完整性，提高了设备利用率。

实施例三

参阅图 4，本申请的第三实施例提供一种管控方法，所述方法的执行主体为服务器，所述方法包括：

步骤 31、接收终端登录请求。

步骤 33、验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控。

在本实施例中，服务器接收终端发送的登录请求，此时，该终端处于非管控状态。

在非受管控的终端上，通过内置管控软件或安装的管控软件输入服务器的地址信息，服务器接收终端发送的登录请求。具体可根据需要，输入服务器规定的信息或自动携带某些可用于唯一标识该终端信息。登录请求也可附加输入类似于公司或部门的信息，限制终端以后可以被多用户使用，但仅限特定团体内的用户。

终端通过输入的服务器地址信息，登录请求携带服务器所需的信息，服务器可根据配置决定是否允许该终端受服务器管理平台的管控。

如果服务器对终端验证无误，则返回正确的结果通知终端已受管控。但该已受管控的终端并没有关联的登录账户。

此时服务器管理平台可对登录成功的终端进行管控，并且服务器根

据预设的第一管控权限管控所述终端。基于所述第一管控权限，服务器可发送铃声、消息、定位等各种信息至终端，也可按需求推送部分和登录账户不相关的管控操作或管控策略，以管控终端，或推送部分和登录账户不相关的特定应用给该终端。此时的终端虽然受控，但还没有登录具体的登录账户，所能收到的管控操作、管控策略和应用的管控，都不和特定登录账户相关。

其中，所述第一管控权限包括基础操作，该基础操作即与登录账户不相关的全部操作，服务器管控下的所有终端都可以执行所述基础操作。所述基础操作例如但并不仅限于：设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级中的一种或几种。

此外，终端也可将终端的基本信息主动向服务器上报，上报所述基本信息也即是执行所述基本操作，此时，所述基本操作例如但并不仅限于：发送电源余量、发送磁盘余量、发送内存状态、发送设备是否被破解的消息、发送开机时长、发送设备和登录账户不相关的日志中的一种或几种。

步骤35、在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控。

其中，所述用户成功登录所述服务器可以是根据向所述服务器发送的用户登录请求登录所述服务器；具体地，终端接收用户输入的登录账户的鉴权信息，并根据登录账户的鉴权信息发送用户登录请求到服务器，服务器对登录账户的鉴权信息进行鉴权。经过对登录账户鉴权信息的鉴权并验证通过后，在服务器上的管理平台对通过该登录账户进行服务器登录的终端进行标记，并且用户成功登录所述服务器。

所述用户成功登录所述服务器还可以是根据所述服务器分配的用户账户登录所述服务器。也即是服务器主动的为终端分配用户，配置好用户至终端后，在服务器上的管理平台对该终端进行标记。

此时，服务器根据预设的第二管控权限对通过登录账户登录服务器的终端进行管控，并且服务器会推送与该终端登录账户相关的管控操作、管控策略或应用等相应的服务内容。同时，服务器会根据需要记录

使用设备的日志。

其中，所述第二管控权限包括专属操作以及上述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。在有用户登录受控的终端时，终端和服务器之间的通信可以是和用户账户无关的基础操作，也可以是与该用户账户相关的专属操作。

步骤37、获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

在本实施例中，可以通过以下两种方式退出所述服务器。

方式一：根据向所述服务器发送的退出登录请求退出所述服务器。在这里，所述终端可以主动向服务器请求退出所述登录账户，具体的，终端发送退出登录请求指令到服务器，服务器根据接收到的退出登录请求指令，返回确认退出登录的指令，从而所述登录账户从所述终端上退出。

方式二：根据所述服务器推送的管控指令退出所述服务器。在这里，服务器可以主动的要求所述登录账户从所述终端上退出。

当登录账户退出登录后，服务器的管控权限由第二管控权限切换至第一管控权限，并且所述终端接受第一管控权限的管控。此时，该终端上所有与用户登录账户相关的信息（比如收到的策略和下载的应用等）都可以被清除。在服务器侧，该用户登录账户的信息也被清除，此时，服务器管控的终端不存在用户登录，但该终端仍受控于所述服务器。

此外，其他用户可以根据该用户的鉴权信息登录服务器，从而接受服务器第二管控权限的管控，服务器会推送与该登录的用户相关的管控操作、管控策略或应用等相应的服务内容。同时，服务器会根据需要记录使用设备的日志。在该用户退出登录后，终端接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控，其他用户可以根据其相应的权限登录服务器，重复上述过程。在这里，一台受控于服务器的终端可以被多个用户交替的使用不同的权限访问，从而解决了一台终端只能被一个用户使用的问题。

本申请实施例提供了一种管控方法，通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用。该实施方式丰富了设备管理系统的管理方式，方便了设备的管理，提高了设备利用率。

实施例四

参阅图 5，本申请的第四实施例提供了一种管控方法，图 5 与图 4 的主要区别在于，所述在获取到所述用户退出所述服务器的消息时之前，所述方法还包括：

步骤 36、接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据。

在本实施例中，服务器可以对用户在登录所述终端期间所产生的数据进行备份，以便在该用户再次登录终端时，可以获取其备份的历史数据。需要说明的是，所述用户再次登录的终端并不一定就是其备份数据时所登录的终端，该终端可以是全部受管控的设备中的任一设备。

本申请实施例提供了一种管控方法，该方法通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用，此外，在用户登录了终端时，还可以备份与该用户相关的数据。该实施方式方便了设备的管理，保证了用户数据的完整性，提高了设备利用率。

实施例五

参阅图 6，本申请的第五实施例提供一种管控装置，该装置适用于手机、平板电脑、PC、智能机器人等终端，所述装置 40 包括：第一发送模块 41、第一接收模块 42、第一接受模块 43 以及第二接受模块 44。

其中，第一发送模块 41，用于向服务器发送终端登录请求；第一接收模块 42，用于接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第

一管控权限对所述终端进行管控；第一接受模块 43，用于在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控；第二接受模块 44，用于获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

可选地，所述装置 40 还包括：第二发送模块 45。第二发送模块 45，用于向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据。

值得说明的是，上述装置内的模块之间的信息交互、执行过程等内容，由于与本申请的方法实施例一和实施例二基于同一构思，具体内容可参见本申请方法实施例中的叙述，此处不再赘述。

本申请实施例提供了一种管控装置，该装置通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用，此外，在用户登录了终端时，还可以备份与该用户相关的数据。该实施方式方便了设备的管理，保证了用户数据的完整性，提高了设备利用率。

实施例六

参阅图 7，本申请的第六实施例提供一种管控装置，该装置适用于服务器，所述装置 50 包括：第二接收模块 51、第一管控模块 52、第二管控模块 53 以及第三管控模块 54。

其中，第二接收模块 51，用于接收终端登录请求；第一管控模块

52，用于验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控；第二管控模块 53，用于在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控；第三管控模块 54，用于获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

可选地，所述装置还包括：备份模块 55。备份模块 55，用于接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据。

值得说明的是，上述装置内的模块之间的信息交互、执行过程等内容，由于与本申请的方法实施例三和实施例四基于同一构思，具体内容可参见本申请方法实施例中的叙述，此处不再赘述。

本申请实施例提供了一种管控装置，该装置通过预设的两种管控权限分别对终端进行管控，在第一管控权限下，终端不需要用户登录就可以接受服务器的管控，在第二管控权限下，用户登录终端后，该终端接受服务器的管控，并且在该用户退出登录后，其他用户可以登录该受控的终端，从而使得一台受控终端能够被多个不同的用户交替使用，此外，在用户登录了终端时，还可以备份与该用户相关的数据。该实施方式方便了设备的管理，保证了用户数据的完整性，提高了设备利用率。

实施例七

参阅图 8，本申请的第七实施例提供一种系统，所述系统 60 包括：终端 61 和服务器 62。

所述终端 61 用于执行如下步骤：

向服务器发送终端登录请求；接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控；在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控；获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

所述服务器 62 用于执行如下步骤：

接收终端登录请求；验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控；在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控；获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

其中，所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

其中，所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

本申请实施例提供了一种系统，该系统包括终端和服务器，该系统

能够实现在所述终端没有用户登录的情况下，也能接受所述服务器的管控，并且在终端受服务器管控时，所述终端能够满足多个用户交替的使用不同的权限对其进行访问。该系统方便了设备的管理，提高了设备利用率。

实施例八

图 9 是本申请实施例提供的一种电子设备的硬件结构示意图，所述电子设备用于执行上述方法实施例。如图 9 所示，该电子设备 700 包括：

一个或多个处理器 701、存储器 702，图 7 中以一个处理器 701 为例。

处理器 701 和存储器 702 可以通过总线或者其他方式连接，图 9 中以通过总线连接为例。

存储器 702 作为一种非易失性计算机可读存储介质，可用于存储非易失性软件程序、非易失性计算机可执行程序以及模块。处理器 701 通过运行存储在存储器 702 中的非易失性软件程序、指令以及模块，从而执行各种功能应用以及数据处理，即实现上述方法实施例中的管控方法。

存储器 702 可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储根据管控装置的使用所创建的数据等。此外，存储器 702 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。

所述一个或者多个模块存储在所述存储器 702 中，当被所述一个或者多个处理器 701 执行时，执行上述任意方法实施例中的管控方法，例如，执行以上描述的图 2 中的方法步骤 21、步骤 23、步骤 25、步骤 27，图 3 中的方法步骤 21、步骤 23、步骤 25、步骤 26、步骤 27，图 4 中的方法步骤 31、步骤 33、步骤 35、步骤 37，图 5 中的方法步骤 31、步骤 33、步骤 35、步骤 36、步骤 37，实现图 6 中的模块 41-45，图 7 中的模块 51-55 的功能。

上述产品可执行本申请实施例所提供的方法，具备执行方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节，可参见本

申请实施例所提供的方法。

本申请实施例的电子设备以多种形式存在，包括但不限于：

(1)移动通信设备：这类设备的特点是具备移动通信功能，并且以提供话音、数据通信为主要目标。这类终端包括：智能手机(例如 iPhone)、多媒体手机、功能性手机，以及低端手机等。

(2)超移动个人计算机设备：这类设备属于个人计算机的范畴，有计算和处理功能，一般也具备移动上网特性。这类终端包括：PDA、MID 和 UMPC 设备等，例如 iPad。

(3)便携式娱乐设备：这类设备可以显示和播放多媒体内容。该类设备包括：音频、视频播放器(例如 iPod)，掌上游戏机，电子书，以及智能玩具和便携式车载导航设备。

(4)智能机器人：这类设备具备多种内部信息传感器和外部信息传感器，如视觉、听觉、触觉、嗅觉，除具有感受器外，它还有效应器，作为作用于周围环境的手段。并且，这类设备能够理解人类语言，用人类语言同操作者对话。

(5)服务器：提供计算服务的设备，服务器的构成包括处理器、硬盘、内存、系统总线等，服务器和通用的计算机架构类似，但是由于需要提供高可靠的服务，因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

(6)其他具有数据交互功能的电子装置。

实施例九

本申请实施例提供了一种非易失性计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，该计算机可执行指令被电子设备执行上述任意方法实施例中的管控方法，例如，执行以上描述的图 2 中的方法步骤 21、步骤 23、步骤 25、步骤 27，图 3 中的方法步骤 21、步骤 23、步骤 25、步骤 26、步骤 27，图 4 中的方法步骤 31、步骤 33、步骤 35、步骤 37，图 5 中的方法步骤 31、步骤 33、步骤 35、步骤 36、步骤 37，实现图 6 中的模块 41-45，图 7 中的模块 51-55 的功能。

实施例十

本申请实施例提供了一种计算机程序产品，包括存储在非易失性计

算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时时，使所述计算机执行上述任意方法实施例中的管控方法，例如，执行以上描述的图 2 中的方法步骤 21、步骤 23、步骤 25、步骤 27，图 3 中的方法步骤 21、步骤 23、步骤 25、步骤 26、步骤 27，图 4 中的方法步骤 31、步骤 33、步骤 35、步骤 37，图 5 中的方法步骤 31、步骤 33、步骤 35、步骤 36、步骤 37，实现图 6 中的模块 41-45，图 7 中的模块 51-55 的功能。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

通过以上的实施方式的描述，本领域普通技术人员可以清楚地了解到各实施方式可借助软件加通用硬件平台的方式来实现，当然也可以通过硬件。本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

以上所述仅为本申请的实施方式，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权 利 要 求 书

1、一种管控方法，应用于终端，其特征在于，包括：

向服务器发送终端登录请求；

接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控；

在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控；

获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

2、根据权利要求 1 所述的方法，其特征在于，

所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

3、根据权利要求 2 所述的方法，其特征在于，

所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

4、根据权利要求 1 至 3 任一项所述的方法，其特征在于，在所述获取到所述用户退出所述服务器的消息时之前，还包括：

向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据。

5、根据权利要求 4 所述的方法，其特征在于，所述用户成功登录所述服务器具体包括：

根据向所述服务器发送的用户登录请求登录所述服务器；或者，

根据所述服务器分配的用户账户登录所述服务器。

6、根据权利要求 4 所述的方法，其特征在于，所述用户退出所述服务器具体包括：

根据向所述服务器发送的退出登录请求退出所述服务器；或者，

根据所述服务器推送的管控指令退出所述服务器。

7、一种管控方法，应用于服务器，其特征在于，包括：

接收终端登录请求；

验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控；

在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控；

获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

8、根据权利要求 7 所述的方法，其特征在于，

所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

9、根据权利要求 8 所述的方法，其特征在于，

所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

10、根据权利要求 7 至 9 任一项所述的方法，其特征在于，所述在获取到所述用户退出所述服务器的消息时之前，还包括：

接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据。

11、根据权利要求 10 所述的方法，其特征在于，所述用户成功登录所述服务器具体包括：

根据向所述服务器发送的用户登录请求登录所述服务器；或者，

根据所述服务器分配的用户账户登录所述服务器。

12、根据权利要求 10 所述的方法，其特征在于，所述用户退出所

述服务器具体包括：

根据向所述服务器发送的退出登录请求退出所述服务器；或者，

根据所述服务器推送的管控指令退出所述服务器。

13、一种管控装置，应用于终端，其特征在于，包括：

第一发送模块，用于向服务器发送终端登录请求；

第一接收模块，用于接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控；

第一接受模块，用于在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控；

第二接受模块，用于获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控。

14、根据权利要求 12 所述的装置，其特征在于，

所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

15、根据权利要求 14 所述的装置，其特征在于，

所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

16、根据权利要求 13 至 15 任一项所述的装置，其特征在于，所述装置还包括：

第二发送模块，用于向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据。

17、一种管控装置，应用于服务器，其特征在于，包括：

第二接收模块，用于接收终端登录请求；

第一管控模块，用于验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控；

第二管控模块，用于在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控；

第三管控模块，用于获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控。

18、根据权利要求 17 所述的装置，其特征在于，

所述第一管控权限包括基础操作，其中，所述基础操作为设备定位、消息通知、设备振铃、标记丢失、标记找回、设置密码、设备锁屏、清除密码、恢复出厂设置、擦除企业数据、软件升级、发送电源余量、发送磁盘余量、发送内存状态、发送日志中的一种或几种。

19、根据权利要求 18 所述的装置，其特征在于，

所述第二管控权限包括专属操作以及所述基础操作，其中，所述专属操作为锁定企业域、解锁企业域、切换用户、接收与用户关联的推送信息中的一种或几种。

20、根据权利要求 17 至 19 任一项所述的装置，其特征在于，所述装置还包括：

备份模块，用于接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据。

21、一种电子设备，其特征在于，包括：

至少一个处理器；

以及，与所述至少一个处理器通信连接的存储器；

其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求 1-12 任一项所述的方法。

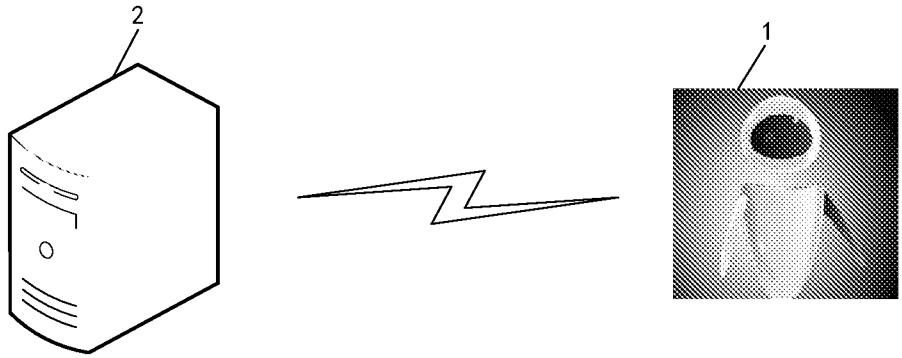

2
1

图 1

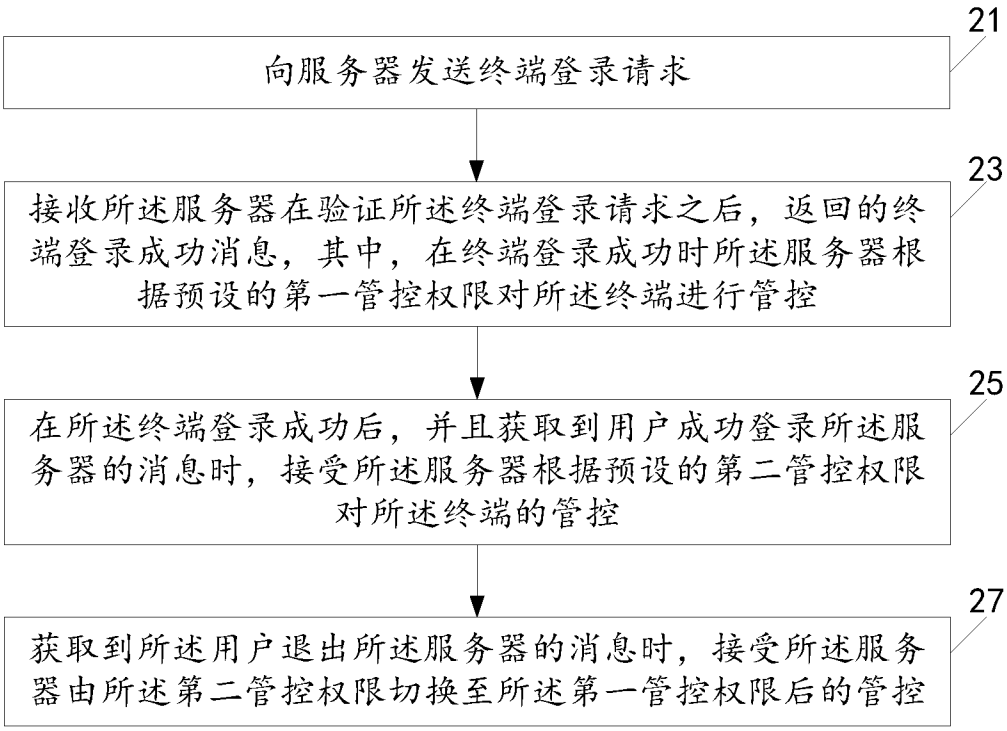

21
向服务器发送终端登录请求
23
接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控
25
在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控
27
获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控

图 2

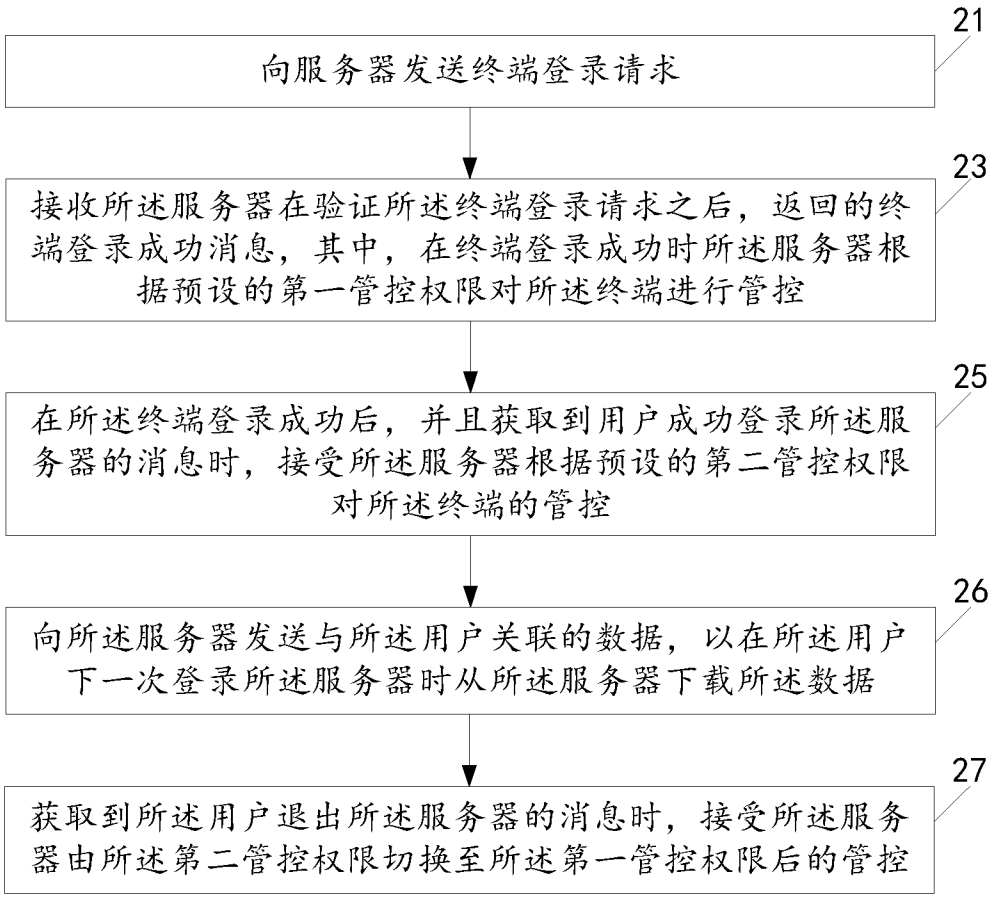

21
向服务器发送终端登录请求
23
接收所述服务器在验证所述终端登录请求之后，返回的终端登录成功消息，其中，在终端登录成功时所述服务器根据预设的第一管控权限对所述终端进行管控
25
在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，接受所述服务器根据预设的第二管控权限对所述终端的管控
26
向所述服务器发送与所述用户关联的数据，以在所述用户下一次登录所述服务器时从所述服务器下载所述数据
27
获取到所述用户退出所述服务器的消息时，接受所述服务器由所述第二管控权限切换至所述第一管控权限后的管控

图 3

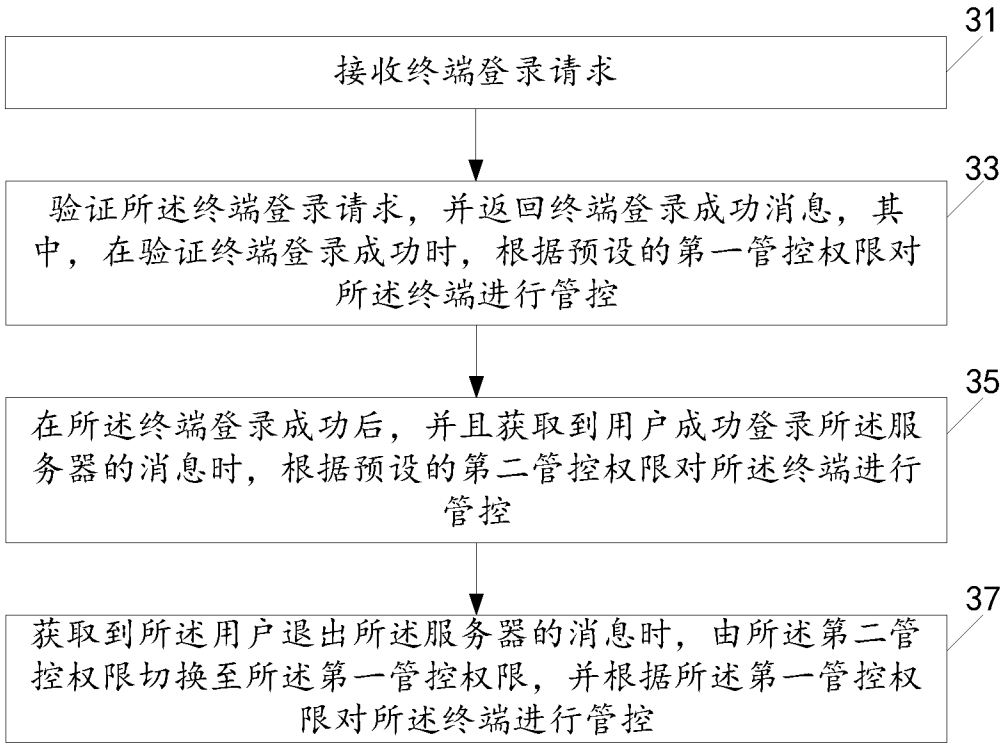

31
接收终端登录请求
33
验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控
35
在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控
37
获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控

图 4

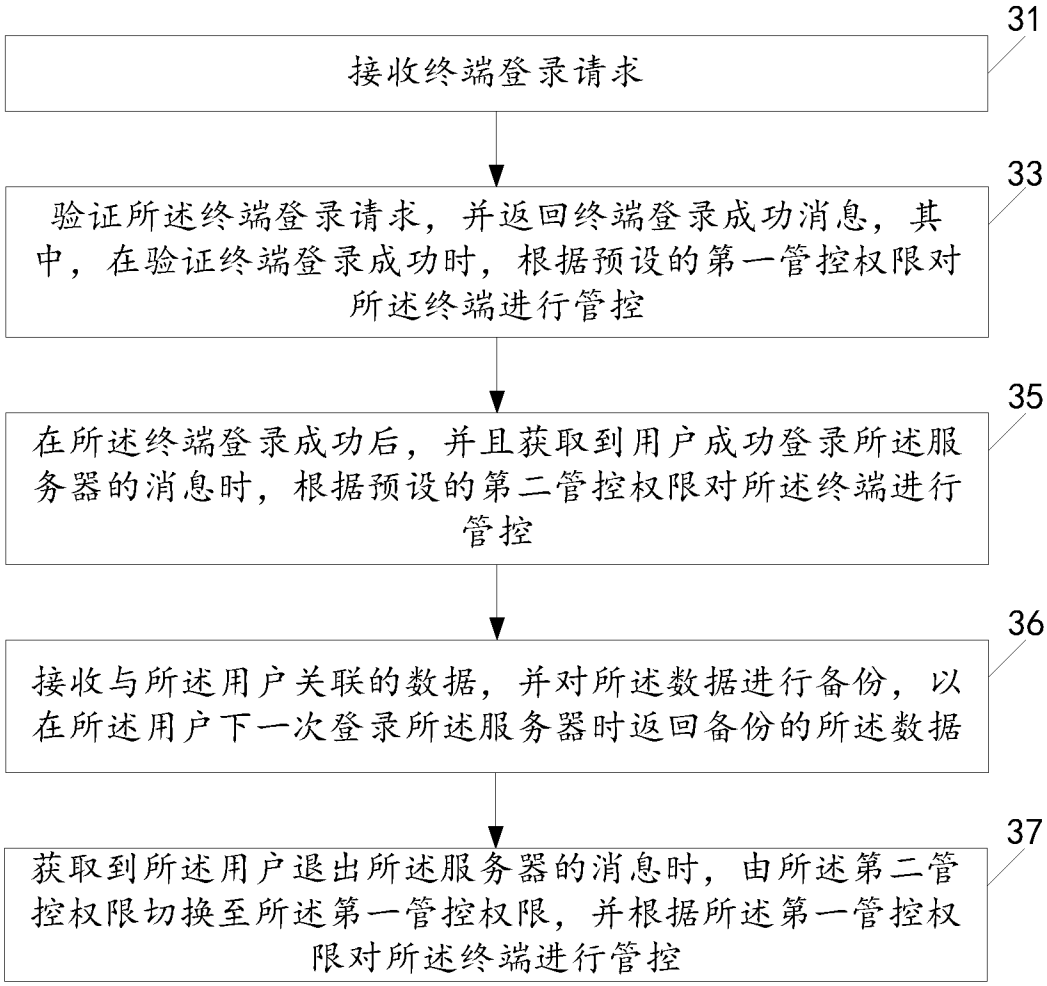

31
接收终端登录请求
33
验证所述终端登录请求，并返回终端登录成功消息，其中，在验证终端登录成功时，根据预设的第一管控权限对所述终端进行管控
35
在所述终端登录成功后，并且获取到用户成功登录所述服务器的消息时，根据预设的第二管控权限对所述终端进行管控
36
接收与所述用户关联的数据，并对所述数据进行备份，以在所述用户下一次登录所述服务器时返回备份的所述数据
37
获取到所述用户退出所述服务器的消息时，由所述第二管控权限切换至所述第一管控权限，并根据所述第一管控权限对所述终端进行管控

图 5

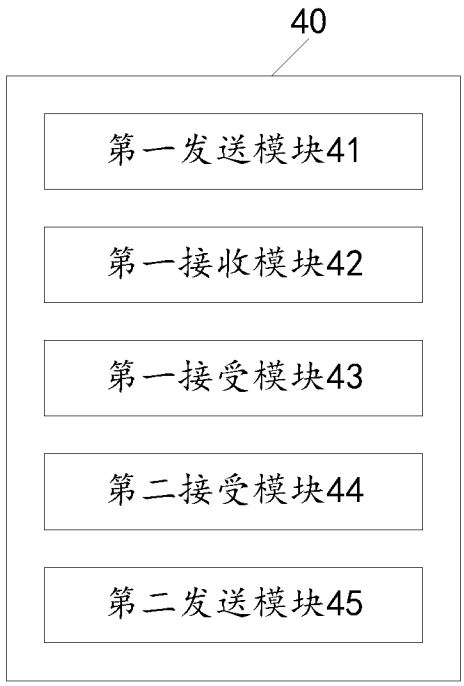

40
第一发送模块41
第一接收模块42
第一接受模块43
第二接受模块44
第二发送模块45

图 6

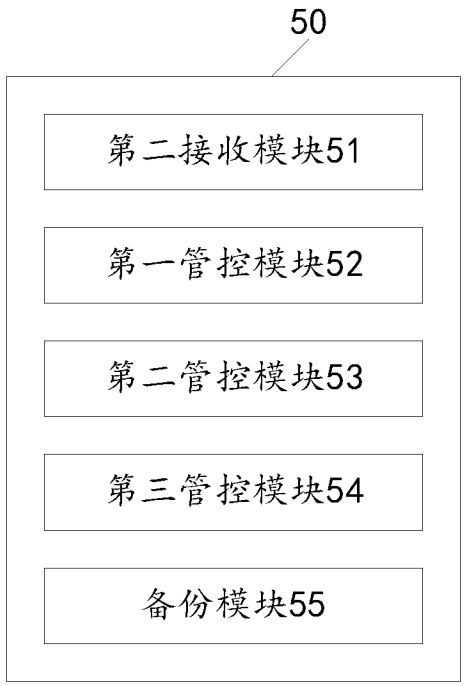

50
第二接收模块51
第一管控模块52
第二管控模块53
第三管控模块54
备份模块55

图 7

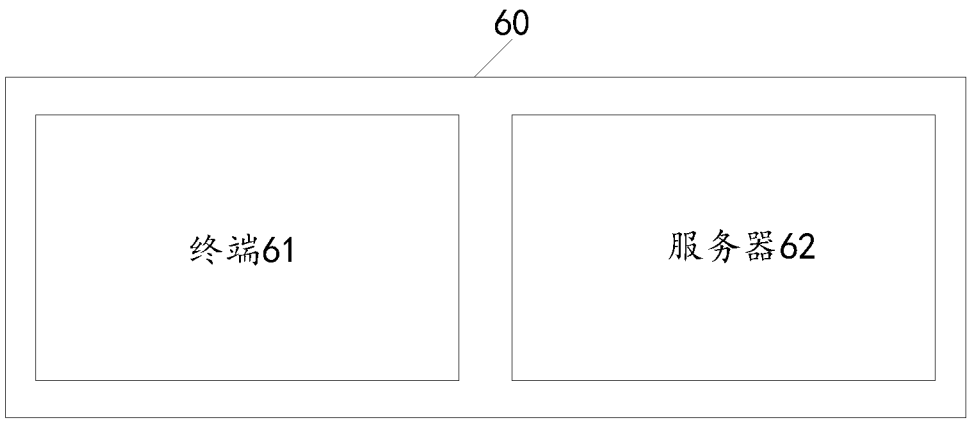

60
终端61
服务器62

图 8

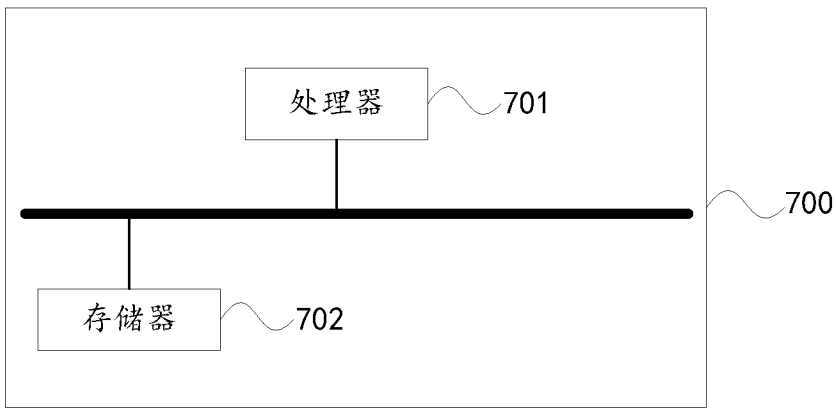

处理器
701
700
存储器
702

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/091491

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (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

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: 终端, 登录, 权限, 用户, 服务器, 管理, 控制, 切换, 配置, 客户端, terminal, login, enter, logon, authority, purview, user, server, management, control, switch, configuration, client

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103312676 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 18 September 2013 (18.09.2013), description, paragraphs 0044-0045	1-21
Y	CN 106713321 A (CHINA UNIONPAY CO., LTD.), 24 May 2017 (24.05.2017), description, paragraphs 0002, and 0050-0080	1-21
A	CN 106156549 A (ALIBABA GROUP HOLDING LIMITED), 23 November 2016 (23.11.2016), entire document	1-21
A	CN 105743841 A (FANTEM TECHNOLOGIES SHENZHEN CO., LTD.), 06 July 2016 (06.07.2016), entire document	1-21

☐ 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
28 March 2018	08 April 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 YANG, Chunyu Telephone No. (86-10) 010-53961437

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/091491

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103312676 A	18 September 2013	None	
CN 106713321 A	24 May 2017	None	
CN 106156549 A	23 November 2016	None	
CN 105743841 A	06 July 2016	None	

国际检索报告

国际申请号
PCT/CN2017/091491

A. 主题的分类

H04L 29/08(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

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, EPODOC: 终端, 登录, 权限, 用户, 服务器, 管理, 控制, 切换, 配置, 客户端, terminal, login, enter, logon, authority, purview, user, server, management, control, switch, configuration, client

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
Y	CN 103312676 A (宇龙计算机通信科技深圳有限公司) 2013年 9月 18日 (2013-09-18) 说明书第0044-0045段	1-21
Y	CN 106713321 A (中国银联股份有限公司) 2017年 5月 24日 (2017-05-24) 说明书第0002, 0050-0080段	1-21
A	CN 106156549 A (阿里巴巴集团控股有限公司) 2016年 11月 23日 (2016-11-23) 全文	1-21
A	CN 105743841 A (丰唐物联技术深圳有限公司) 2016年 7月 6日 (2016-07-06) 全文	1-21

☐ 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 3月 28日	2018年 4月 8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 杨春雨 电话号码 (86-10)010-53961437

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/091491

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	103312676	A	2013年 9月 18日	无	
CN	106713321	A	2017年 5月 24日	无	
CN	106156549	A	2016年 11月 23日	无	
CN	105743841	A	2016年 7月 6日	无	