(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
2017 年 6 月 22 日 (22.06.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/101729 A1

(51) 国际专利分类号:
G05B 15/02 (2006.01)

(21) 国际申请号: PCT/CN2016/108981

(22) 国际申请日: 2016 年 12 月 8 日 (08.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510958422.4 2015 年 12 月 18 日 (18.12.2015) CN

(71) 申请人: **阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED)** [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: **庄旻轩 (ZHUANG, Minxuan)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 **罗毅 (LUO, Yi)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: **北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)**; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: INTERNET OF THINGS-BASED DEVICE OPERATION METHOD AND SERVER

(54) **发明名称** : 一种基于物联网的设备操作方法及服务器

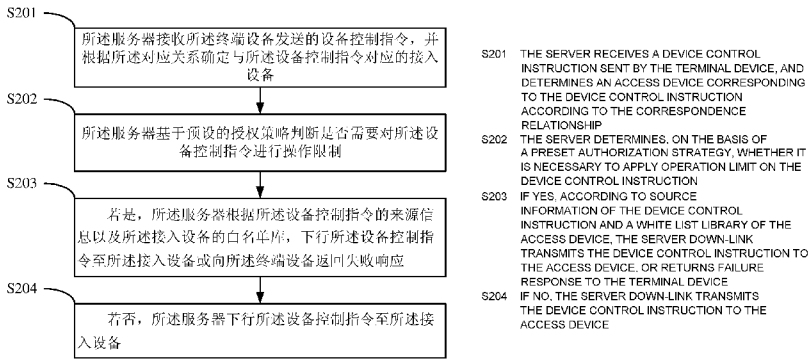

图 2

(57) **Abstract**: Disclosed in the present invention are an Internet of things-based device operation method and server: pre-storing, in the server, a correspondence relationship between a currently registered access device and a terminal device which has been authenticated, such that when the server receives a device control instruction transmitted from the terminal, the server is capable of determining an access device corresponding to the device control instruction according to the correspondence relationship; determining, on the basis of a preset authorization strategy, whether it is necessary to apply operation limit on the device control instruction; and when the determination result is yes, according to source information of the device control instruction and a white list library of the access device, down-link transmitting the device control instruction to the access device, or returning failure response to the terminal device, thus effectively preventing an unauthorized user from operating devices in the Internet of things, and effectively improving the usage security of the Internet of things.

(57) **摘要**:

[见续页]

WO 2017/101729 A1

本发明公开了一种基于物联网的设备操作方法及服务器。在服务器中预先存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，这样在当服务器接收终端设备发送的设备控制指令时，可根据对应关系确定与设备控制指令对应的接入设备，并基于预设的授权策略判断是否需要对该设备控制指令进行操作限制，以及在判断结果为是时根据设备控制指令的来源信息以及接入设备的白名单库下行设备控制指令至接入设备或向终端设备返回失败响应。从而有效地避免了非法用户擅自对物联网的设备进行操作的风险，有效地提高了物联网使用的安全性。

一种基于物联网的设备操作方法及服务器

本申请要求 2015 年 12 月 18 日递交的申请号为 201510958422.4、发明名称为“一种基于物联网的设备操作方法及服务器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，特别涉及一种基于物联网的设备操作方法。本申请同时还涉及一种服务器。

背景技术

物联网是一个基于互联网、传统电信网等讯息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。其利用局部网络或互联网等通信技术把传感器、控制器、机器、人员和物等通过新的方式联在一起，形成人与物、物与物相联，实现信息化、远程管理控制和智能化的网络。物联网是互联网的延伸，它包括互联网及互联网上所有的资源，兼容互联网所有的应用，但物联网中所有的元素（所有的设备、资源及通信等）都是个性化和私有化的。

通常意义上来讲，应用于物联网的设备都是接入物联网的物理设备，主要为空调，冰箱，等含有芯片的嵌入式设备。而物联网中的服务端（又称为云端）则一般为部署在机房的为设备提供服务的服务器或者服务器集群。服务端通过控制指令与物联网中的接入设备进行交互。该控制指令为服务端下行给设备端的，控制设备行为的指令。通常由手机端发起或者定时任务触发。

如图 1 所示，为现有技术中针对物联网中的接入设备的控制示意图。目前接入物联网的设备大部分需要用户通过终端设备（移动终端居多）来进行操作。具体流程为：用户通过手机发送请求给服务器，服务器将消息下行给设备，完成对设备的控制,在此过程中，对于部分敏感的指令，需要由服务端验证用户使用的 APP 是否有权限对该设备进行操作，从而防止恶意攻击。

然而，发明人在实现本申请的过程中发现，虽然现有的方案能够使用户通过终端设备实现物联网中对接入设备的控制，但是需要进行权限控制的部分非常有限，以至于在某些场景下会造成安全隐患。举例来说，当非法用户知道了某个接入设备的 ID 或其他身份标识信息，就可以利用手机 app 对来对该接入设备进行控制，在智能家居场景中，烤箱，热水器等设备均存在这样的风险。因此如何提高现有的物联网下设备操作的安全

性，成为了本领域技术人员亟待解决的技术问题。

发明内容

本发明提供了一种基于物联网的设备操作方法，用以防止物联网中针对接入设备的恶意操作行为，为安全使用物联网提供保障。该方法应用于包括终端设备、服务器以及接入设备的物联网中，所述服务器中存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，该方法包括：

所述服务器接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备；

所述服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制；

若是，所述服务器根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应

若否，所述服务器下行所述设备控制指令至所述接入设备。

优选地，所述服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制，具体为：

根据所述接入设备的敏感等级判断所述接入设备是否需要进行权限控制；

若所述接入设备需要进行权限控制，判断执行所述设备控制指令是否需要授权；

若执行所述设备控制指令需要授权，确认需要对所述设备控制指令进行操作限制；

若所述接入设备不需要进行权限控制或执行所述设备控制指令不需要授权，确认不需要对所述设备控制指令进行操作限制。

优选地，所述服务器根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应，具体为：

所述服务器判断所述接入设备是否存在对应的白名单库；

若所述接入设备不存在任何白名单库，根据所述来源信息判断所述设备控制指令的发送方是否具有所述接入设备的控制权；

若所述接入设备存在白名单库，根据所述来源信息判断所述设备控制指令的发送方是否包含于所述白名单库；

当所述设备控制指令的发送方具有所述接入设备的控制权或所述设备控制指令的发送方包含于所述白名单库时，下行所述设备控制指令至所述接入设备；

当所述设备控制指令的发送方不具有所述接入设备的控制权或所述设备控制指令

的发送方不包含于所述白名单库时，向所述终端设备返回错误响应。

优选地，在所述服务器接收所述终端设备发送的设备控制指令之前，还包括：

所述服务器接收所述终端设备发送的绑定请求，所述绑定请求中携带待绑定接入设备的标识以及验证信息；

若所述验证信息合法，所述服务器判断所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息是否一致；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息一致，所述服务器生成所述终端设备与所述待绑定设备之间的对应关系；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息不一致或若所述验证信息非法，所述服务器向所述终端设备返回错误响应。

优选地，还包括：

所述白名单库由所述接入设备在接收到用户发送的白名单库授权指令时，对所述用户鉴权通过后根据所述白名单库授权指令携带的来源信息设置的。

相应地，本申请还提出了一种服务器，所述服务器应用于包括终端设备、所述服务器以及接入设备的物联网中，所述服务器中存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，该服务器还包括：

接收模块，接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备；

判断模块，基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制；

处理模块，在所述判断模块确认需要对所述设备控制指令进行操作限制时，根据所述设备控制指令的来源信息以及所述接入设备的白名单库下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应；以及在所述判断模块确认不需要对所述设备控制指令进行操作限制时下行所述设备控制指令至所述接入设备。

优选地，所述判断模块具体用于：

根据所述接入设备的敏感等级判断所述接入设备是否需要进行权限控制；

若所述接入设备需要进行权限控制，所述判断模块判断执行所述设备控制指令是否需要授权；

若执行所述设备控制指令需要授权，所述判断模块确认需要对所述设备控制指令进行操作限制；

若所述接入设备不需要进行权限控制或执行所述设备控制指令不需要授权，所述判断模块确认不需要对所述设备控制指令进行操作限制。

优选地，所述处理模块根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应，具体为：

判断所述接入设备是否存在对应的白名单库；

若所述接入设备不存在任何白名单库，所述处理模块根据所述来源信息判断所述设备控制指令的发送方是否具有所述接入设备的控制权；

若所述接入设备存在白名单库，所述处理模块根据所述来源信息判断所述设备控制指令的发送方是否包含于所述白名单库；

当所述设备控制指令的发送方具有所述接入设备的控制权或所述设备控制指令的发送方包含于所述白名单库时，所述处理模块下行所述设备控制指令至所述接入设备；

当所述设备控制指令的发送方不具有所述接入设备的控制权或所述设备控制指令的发送方不包含于所述白名单库时，所述处理模块向所述终端设备返回错误响应。

优选地，还包括：

绑定模块，接收所述终端设备发送的绑定请求，并在若所述验证信息合法时判断所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息是否一致，所述绑定请求中携带待绑定接入设备的标识以及验证信息；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息一致，所述绑定模块生成所述终端设备与所述待绑定设备之间的对应关系；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息不一致或若所述验证信息非法，所述绑定模块向所述终端设备返回错误响应。

优选地，还包括：

所述白名单库由所述接入设备在接收到用户发送的白名单库授权指令时，对所述用户鉴权通过后根据所述白名单库授权指令携带的来源信息设置的。

由此可见，通过应用本申请的技术方案，在服务器中预先存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，这样在当服务器接收终端设备发送的设备控制指令时，可根据对应关系确定与设备控制指令对应的接入设备，并基于预设的授权策略判断是否需要对该设备控制指令进行操作限制，以及在判断结果为是时根据设备控制指令的来源信息以及接入设备的白名单库下行设备控制指令至接入设备或向终端设备

返回失败响应。从而有效地避免了非法用户擅自对物联网的设备进行操作的风险，有效地提高了物联网使用的安全性。

附图说明

图 1 为现有技术中针对物联网中的接入设备的控制示意图；

图 2 为本申请提出的一种基于物联网的设备操作方法的流程示意图；

图 3 为本申请具体实施例提出的一种物联网设备操作示意图；

图 4 为本申请具体实施例提出的一种物联网设备操作方法的流程示意图；

图 5 为本申请提出的一种服务器的结构示意图。

具体实施方式

有鉴于背景技术中的问题，本申请提出了一种基于物联网的设备操作方法。通过在对物联网中的接入设备进行控制之前建立一定的关联属性，并针对不同类型的接入设备以及不同的指令的来源信息采取相应的授权策略，这样不仅能够在一些比较容易引发危险的接入设备中防止误操作，同时还能避免非法用户的恶意操作。由于该方法应用在包括终端设备、服务器以及接入设备的物联网中，因此在实施本方案之前，需要在服务器中存储当前已注册的接入设备与验证通过的终端设备之间的对应关系。具体地，该对应关系可以为接入设备与终端设备之间的设备码之间的对应关系，也可以为接入设备与终端设备之间的 MAC 地址之间的对应关系，在能够清楚地确定该接入设备与终端设备为对应的前提下，具体的对应关系的形式的不同并不影响本申请的保护范围。其中，终端设备包括但不限于移动终端、个人计算机、服务器与网络设备等。

如图 2 所示，为本申请提出的一种基于物联网的设备操作方法的流程示意图，包括如下步骤：

S201，所述服务器接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备。

由于本申请旨在保障合法用户能够正常安全地使用物联网中的接入设备，因此本申请需要预先在服务器中为各个接入设备以及对应的终端设备设置对应关系。该对应关系可由技术人员根据用户使用的终端设备以及物联网中的接入设备手动设置，也可以由服务器根据用户的终端设备所发起的请求生成。在本申请的优选实施例中，用户在通过终

端设备向服务器发起绑定请求后，服务器的执行步骤如下：

步骤 a） 所述服务器接收所述终端设备发送的绑定请求，所述绑定请求中携带待绑定接入设备的标识以及验证信息；

步骤 b） 若所述验证信息合法，所述服务器判断所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息是否一致。

以下为对应上述判断步骤的处理结果：

（1） 若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息一致，所述服务器生成所述终端设备与所述待绑定设备之间的对应关系；

（2） 若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息不一致或若所述验证信息非法，所述服务器向所述终端设备返回错误响应。

通过上述终端设备与服务器的绑定交互过程，服务器中保存了终端设备与接入设备的对应关系。需要说明的是，上述过程中的验证信息的以及验证方式的具体形式可以根据实际情况灵活设置，其目的在于针对用户本身是否为合法用户进行判断。而接入设备的注册信息亦可采用例如设备标识、MAC 地址等唯一可识别该接入设备的因素，具体的注册信息的形式以及数量上的改变并不影响本申请的保护范围。

在图 3 所示的具体实施例中，在前期的流程包括以下部分：

（1） 当智能硬件设备通过物联网连接到服务器后，将上报自己的注册信息（例如 MAC 地址、设备 ID 等），部分权限要求较高的接入设备在此过程中还将同时上传允许敏感操作的账户，以便于服务器后续根据指令的来源信息中的账户信息确定是否向接入设备发送指令。

（2）用户通过手机 APP 向物联网的服务端发送请求，绑定对应的接入设备。该请求内容为接入设备的注册信息以及相应的密码，由于传输通道经过 SSL 加密，因此传输是安全的。

（3）服务端获取 APP 发送的接入设备信息和密码，与之前智能硬件上报的信息进行对比验证。若验证通过，服务端认为该手机拥有对设备的控制权，并且将该手机到设备的对应关系进行保存，若验证失败，服务端向 APP 返回错误提示。

S202，所述服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制。

由于物联网中的接入设备的类型繁多，其中有些重要的电气设备（例如烤箱、加热器）在由用户远程进行某些特定类型的操作时是需要权限的，相应地例如电灯电视等设备则不需要那么高的权限。因此本申请预设了授权策略，该授权策略首先按照设备进行了划分：有些设备对于权限的敏感度较低，不对指令进行任何限制，只要是绑定到该设备，甚至没有绑定设备的 APP 都可以进行操作，同时针对包含一些比较敏感的指令的部分接入设备，该授权策略只允许注册过的 APP 进行该类指令的控制操作，以此在保证接入设备操作安全的同时提高处理效率。

在本申请的优选实施例中，当服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制，可首先根据接入设备的敏感等级判断接入设备是否需要进行权限控制，并基于以下结果分别进行处理：

（1） 若所述接入设备需要进行权限控制，判断执行所述设备控制指令是否需要授权；

（2） 若执行所述设备控制指令需要授权，确认需要对所述设备控制指令进行操作限制；

（3） 若所述接入设备不需要进行权限控制或执行所述设备控制指令不需要授权，确认不需要对所述设备控制指令进行操作限制。

通过该优选实施例的方案，可以快速地基于接入设备以及指令的重要等级确定是否需要进行下一步的处理。

S203，若是，所述服务器根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应。

S204，若否，所述服务器下行所述设备控制指令至所述接入设备。

对于极其重要的接入设备（涉及人身安全或财产安全），本申请针对该部分设备设置包含一些权限更加严格的指令，同时设置白名单库，只允许注册过的，并且用户名在白名单中的设备进行该类指令的权限控制。因此本申请的优选实施例针对接入设备是否具有白名单库以及具有白名单库的情况提出了以下处理方式：

一、接入设备是否具有白名单库

服务器首先判断所述接入设备是否存在对应的白名单库，若接入设备不存在任何白名单库，服务器根据所述来源信息判断所述设备控制指令的发送方是否具有所述接入设备的控制权，若所述接入设备存在白名单库，根据所述来源信息判断所述设备控制指令

的发送方是否包含于所述白名单库。

二、接入设备具有白名单库

当所述设备控制指令的发送方具有所述接入设备的控制权或所述设备控制指令的发送方包含于所述白名单库时，下行所述设备控制指令至所述接入设备；当所述设备控制指令的发送方不具有所述接入设备的控制权或所述设备控制指令的发送方不包含于所述白名单库时，向所述终端设备返回错误响应。

如 S202 中所说的，服务器可为接入设备设置专属的白名单库，并且在下达指定的 APP 或是用户存在于该白名单库中方才下行指令。因此上述实施例中的来源信息可设置为通过终端设备下达指令的用户的个人信息（例如手机号码、邮箱账户等），或者是用户所下达指令的 APP 的信息，相应地，白名单库中包含可允许用户的个人信息以及 APP 信息。技术人员可在此基础上针对来源信息以及白名单库中的内容进行进一步的调整以及增加，这些都属于本申请的保护范围。

为了避免了远程控制的可能性，本申请进一步将设置白名单库的途径限制于仅直接通过接入设备上操作，因此在该优选实施例中，白名单库由所述接入设备在接收到用户发送的白名单库授权指令时，对所述用户鉴权通过后根据所述白名单库授权指令携带的来源信息设置的。

以图 3 为例，该具体实施例在用户通过手机向服务端发送设备控制指令后，由服务端会进行几个不同级别的检查，具体如图 4 所示，主要包括以下几个方面的检查：

（1） 检查请求的设备是否存在；

（2）检查该设备是否对指令进行了权限控制；

（3）检查请求的指令类型是否属于授权指令；

（4）检查该设备是否对授权指令设置了白名单；

（5）检查该 APP 的用户是否在白名单中。

在上述具体实施例中，基于权限的角度，指令被分成了三种类型：普通指令，注册授权指令以及白名单授权指令。在此需要说明的是，本申请中接入设备和终端设备的绑定可以是一对多的关系，即同一个接入设备可以接受来自于多个终端设备的指令。相应地，终端设备在绑定某个接入设备后，也可以通过发送解绑指令解除对改设备的绑定。此后，该终端设备只能对接入设备发送普通指令。

上述指令分类机制可以保证手机端能够共享一些不太敏感的服务，比如获取设备当前状态等信息，又保证了执行敏感服务时候的安全性，防止恶意破坏和攻击。基于设备提供白名单的方式，使得权限控制更加灵活，对于控制指令的分类更加细化。

为达到以上技术目的，本申请还提出了一种服务器，如图 5 所示，该服务器应用于包括终端设备、所述服务器以及接入设备的物联网中，所述服务器中存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，该服务器还包括：

接收模块 510，接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备；

判断模块 520，基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制；

处理模块 530，在所述判断模块确认需要对所述设备控制指令进行操作限制时，根据所述设备控制指令的来源信息以及所述接入设备的白名单库下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应；以及在所述判断模块确认不需要对所述设备控制指令进行操作限制时下行所述设备控制指令至所述接入设备。

在具体的应用场景中，所述判断模块具体用于：

根据所述接入设备的敏感等级判断所述接入设备是否需要进行权限控制；

若所述接入设备需要进行权限控制，所述判断模块判断执行所述设备控制指令是否需要授权；

若执行所述设备控制指令需要授权，所述判断模块确认需要对所述设备控制指令进行操作限制；

若所述接入设备不需要进行权限控制或执行所述设备控制指令不需要授权，所述判断模块确认不需要对所述设备控制指令进行操作限制。

在具体的应用场景中，所述处理模块根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应，具体为：

判断所述接入设备是否存在对应的白名单库；

若所述接入设备不存在任何白名单库，所述处理模块根据所述来源信息判断所述设备控制指令的发送方是否具有所述接入设备的控制权；

若所述接入设备存在白名单库，所述处理模块根据所述来源信息判断所述设备控制

指令的发送方是否包含于所述白名单库；

当所述设备控制指令的发送方具有所述接入设备的控制权或所述设备控制指令的发送方包含于所述白名单库时，所述处理模块下行所述设备控制指令至所述接入设备；

当所述设备控制指令的发送方不具有所述接入设备的控制权或所述设备控制指令的发送方不包含于所述白名单库时，所述处理模块向所述终端设备返回错误响应。

在具体的应用场景中，还包括：

绑定模块，接收所述终端设备发送的绑定请求，并在若所述验证信息合法时判断所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息是否一致，所述绑定请求中携带待绑定接入设备的标识以及验证信息；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息一致，所述绑定模块生成所述终端设备与所述待绑定设备之间的对应关系；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息不一致或若所述验证信息非法，所述绑定模块向所述终端设备返回错误响应。

在具体的应用场景中，还包括：

所述白名单库由所述接入设备在接收到用户发送的白名单库授权指令时，对所述用户鉴权通过后根据所述白名单库授权指令携带的来源信息设置的。

通过应用本申请的技术方案，在服务器中预先存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，这样在当服务器接收终端设备发送的设备控制指令时，可根据对应关系确定与设备控制指令对应的接入设备，并基于预设的授权策略判断是否需要对该设备控制指令进行操作限制，以及在判断结果为是时根据设备控制指令的来源信息以及接入设备的白名单库下行设备控制指令至接入设备或向终端设备返回失败响应。从而有效地避免了非法用户擅自对物联网的设备进行操作的风险，有效地提高了物联网使用的安全性。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施场景所述的

方法。

本领域技术人员可以理解附图只是一个优选实施场景的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

本领域技术人员可以理解实施场景中的装置中的模块可以按照实施场景描述进行分布于实施场景的装置中，也可以进行相应变化位于不同于本实施场景的一个或多个装置中。上述实施场景的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

上述本发明序号仅仅为了描述，不代表实施场景的优劣。

以上公开的仅为本发明的几个具体实施场景，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

权 利 要 求 书

1、一种基于物联网的设备操作方法，其特征在于，所述方法应用于包括终端设备、服务器以及接入设备的物联网中，所述服务器中存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，该方法包括：

所述服务器接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备；

所述服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制；

若是，所述服务器根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应；

若否，所述服务器下行所述设备控制指令至所述接入设备。

2、如权利要求 1 所述的方法，其特征在于，所述服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制，具体为：

根据所述接入设备的敏感等级判断所述接入设备是否需要进行权限控制；

若所述接入设备需要进行权限控制，判断执行所述设备控制指令是否需要授权；

若执行所述设备控制指令需要授权，确认需要对所述设备控制指令进行操作限制；

若所述接入设备不需要进行权限控制或执行所述设备控制指令不需要授权，确认不需要对所述设备控制指令进行操作限制。

3、如权利要求 1 所述的方法，其特征在于，所述服务器根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应，具体为：

所述服务器判断所述接入设备是否存在对应的白名单库；

若所述接入设备不存在任何白名单库，根据所述来源信息判断所述设备控制指令的发送方是否具有所述接入设备的控制权；

若所述接入设备存在白名单库，根据所述来源信息判断所述设备控制指令的发送方是否包含于所述白名单库；

当所述设备控制指令的发送方具有所述接入设备的控制权或所述设备控制指令的发送方包含于所述白名单库时，下行所述设备控制指令至所述接入设备；

当所述设备控制指令的发送方不具有所述接入设备的控制权或所述设备控制指令的发送方不包含于所述白名单库时，向所述终端设备返回错误响应。

4、如权利要求 1 所述的方法，其特征在于，在所述服务器接收所述终端设备发送

的设备控制指令之前，还包括：

所述服务器接收所述终端设备发送的绑定请求，所述绑定请求中携带待绑定接入设备的标识以及验证信息；

若所述验证信息合法，所述服务器判断所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息是否一致；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息一致，所述服务器生成所述终端设备与所述待绑定设备之间的对应关系；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息不一致或若所述验证信息非法，所述服务器向所述终端设备返回错误响应。

5、如权利要求 1-4 任一项所述的方法，其特征在于，还包括：

所述白名单库由所述接入设备在接收到用户发送的白名单库授权指令时，对所述用户鉴权通过后根据所述白名单库授权指令携带的来源信息设置的。

6、一种服务器，其特征在于，所述服务器应用于包括终端设备、所述服务器以及接入设备的物联网中，所述服务器中存储当前已注册的接入设备与验证通过的终端设备之间的对应关系，该服务器还包括：

接收模块，接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备；

判断模块，基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制；

处理模块，在所述判断模块确认需要对所述设备控制指令进行操作限制时，根据所述设备控制指令的来源信息以及所述接入设备的白名单库下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应；以及在所述判断模块确认不需要对所述设备控制指令进行操作限制时下行所述设备控制指令至所述接入设备。

7、如权利要求 6 所述的服务器，其特征在于，所述判断模块具体用于：

根据所述接入设备的敏感等级判断所述接入设备是否需要进行权限控制；

若所述接入设备需要进行权限控制，所述判断模块判断执行所述设备控制指令是否需要授权；

若执行所述设备控制指令需要授权，所述判断模块确认需要对所述设备控制指令进行操作限制；

若所述接入设备不需要进行权限控制或执行所述设备控制指令不需要授权，所述判

断模块确认不需要对所述设备控制指令进行操作限制。

8、如权利要求 6 所述的服务器，其特征在于，所述处理模块根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应，具体为：

判断所述接入设备是否存在对应的白名单库；

若所述接入设备不存在任何白名单库，所述处理模块根据所述来源信息判断所述设备控制指令的发送方是否具有所述接入设备的控制权；

若所述接入设备存在白名单库，所述处理模块根据所述来源信息判断所述设备控制指令的发送方是否包含于所述白名单库；

当所述设备控制指令的发送方具有所述接入设备的控制权或所述设备控制指令的发送方包含于所述白名单库时，所述处理模块下行所述设备控制指令至所述接入设备；

当所述设备控制指令的发送方不具有所述接入设备的控制权或所述设备控制指令的发送方不包含于所述白名单库时，所述处理模块向所述终端设备返回错误响应。

9、如权利要求 6 所述的服务器，其特征在于，还包括：

绑定模块，接收所述终端设备发送的绑定请求，并在若所述验证信息合法时判断所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息是否一致，所述绑定请求中携带待绑定接入设备的标识以及验证信息；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息一致，所述绑定模块生成所述终端设备与所述待绑定设备之间的对应关系；

若所述标识与所述待绑定接入设备在连接至服务器时所上报的注册信息不一致或若所述验证信息非法，所述绑定模块向所述终端设备返回错误响应。

10、如权利要求 6-9 任一项所述的服务器，其特征在于，还包括：

所述白名单库由所述接入设备在接收到用户发送的白名单库授权指令时，对所述用户鉴权通过后根据所述白名单库授权指令携带的来源信息设置的。

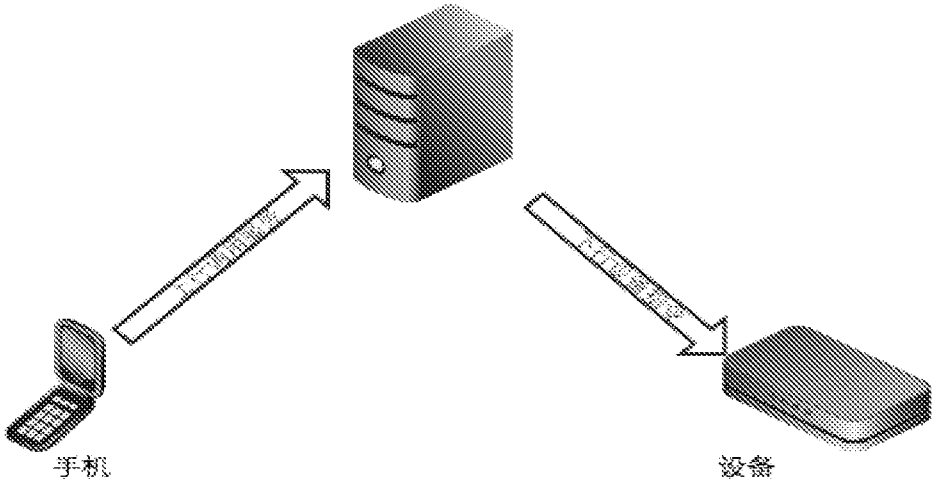
手机
设备

图 1

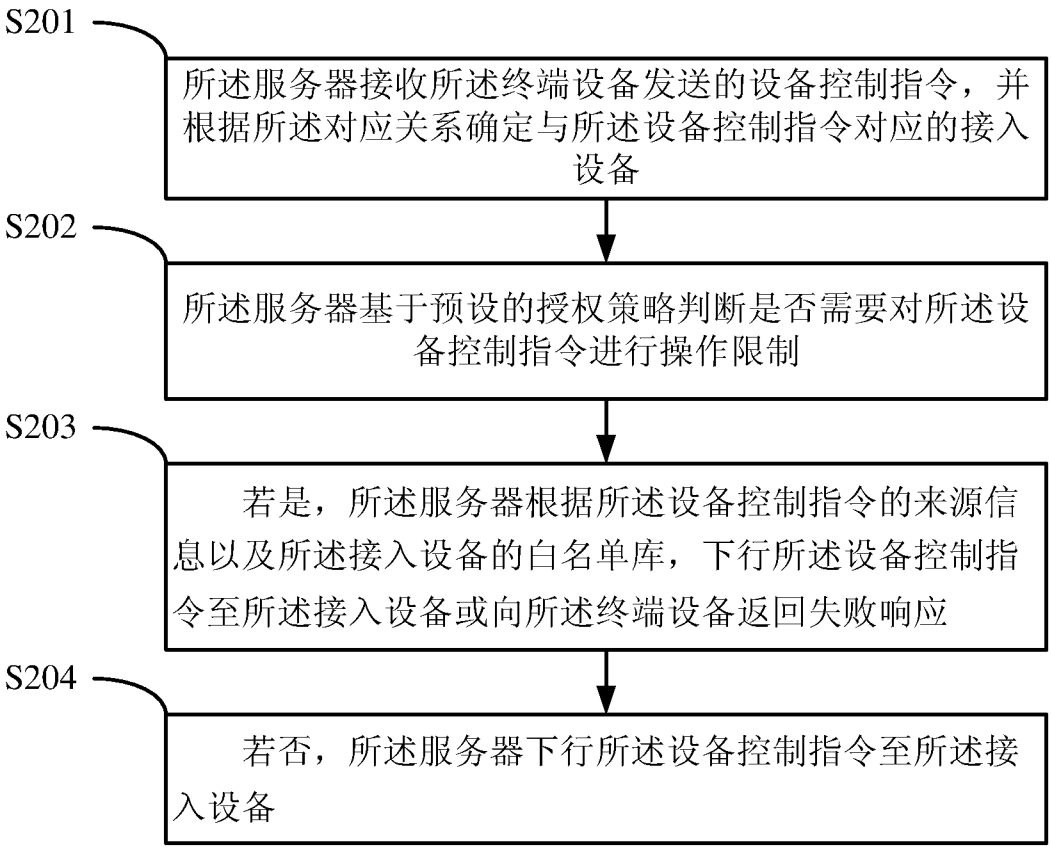
S201
所述服务器接收所述终端设备发送的设备控制指令，并根据所述对应关系确定与所述设备控制指令对应的接入设备
S202
所述服务器基于预设的授权策略判断是否需要对所述设备控制指令进行操作限制
S203
若是，所述服务器根据所述设备控制指令的来源信息以及所述接入设备的白名单库，下行所述设备控制指令至所述接入设备或向所述终端设备返回失败响应
S204
若否，所述服务器下行所述设备控制指令至所述接入设备

图 2

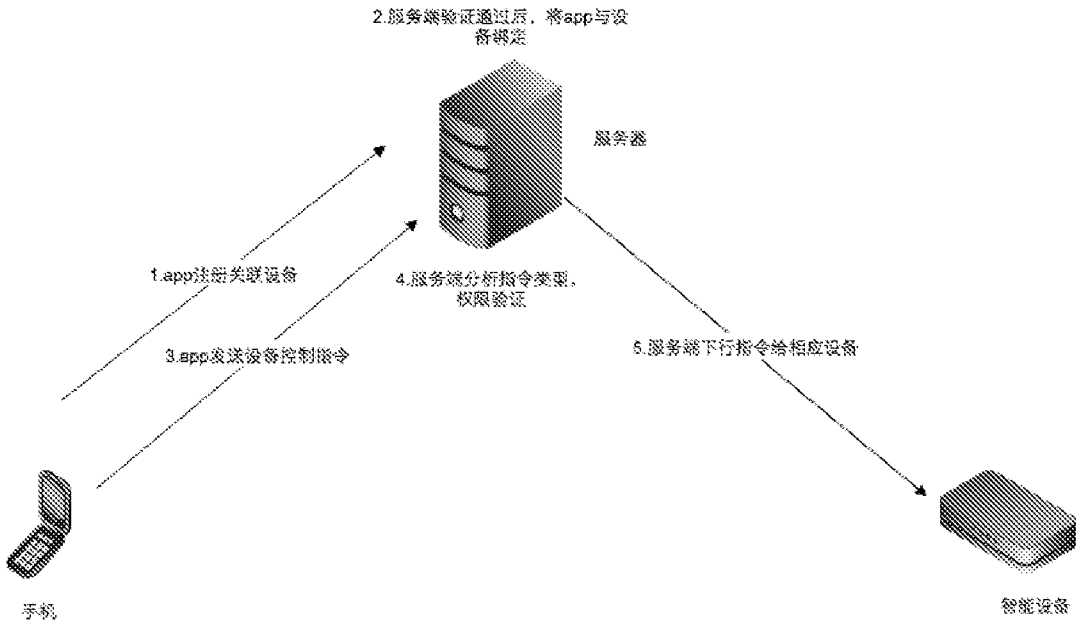
2.服务端验证通过后，将app与设备绑定
服务器
1.app注册关联设备
4.服务端分析指令类型，权限验证
3.app发送设备控制指令
5.服务端下行指令给相应设备
手机
智能设备

图 3

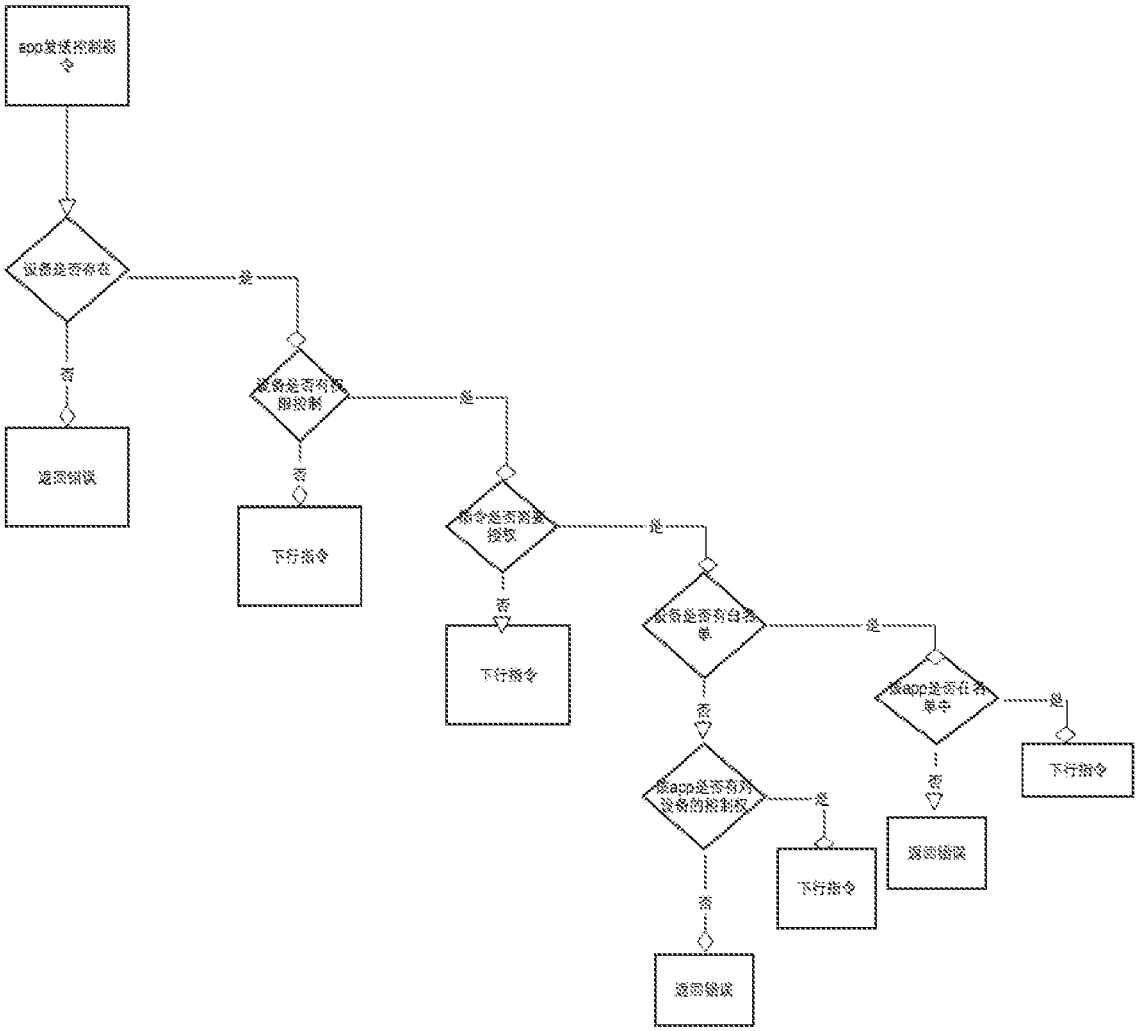
app发送控制指令
设备是否存在
是
否
返回错误
设备是否有控制权限
是
否
下行指令
指令是否需要权限
是
否
下行指令
设备是否有白名单
是
否
该app是否在白名单中
是
否
下行指令
返回错误
该app是否有对设备的控制权
是
否
下行指令
返回错误

图 4

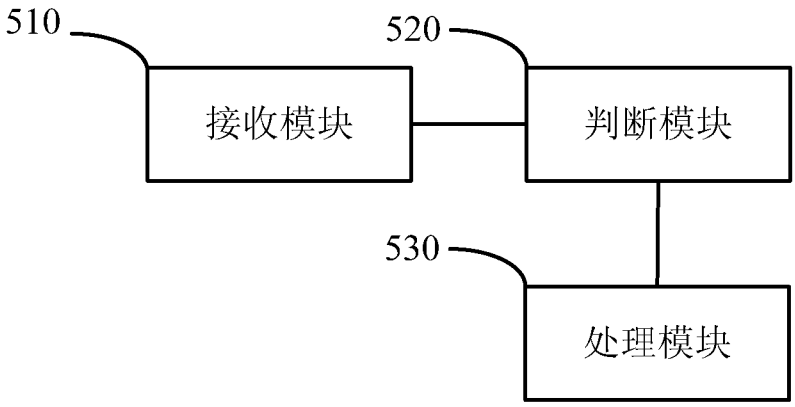

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/108981

A. CLASSIFICATION OF SUBJECT MATTER

G05B 15/02 (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)

G05B H04L 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: appliance table control intelligent smart household home command instruction operation terminal safe authority list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104615004 A (BEIJING HAIER GUANGKE DIGITAL TECHNOLOGY CO., LTD. et al.), 13 May 2015 (13.05.2015), description, paragraphs [0027]-[0073]	1-10
X	CN 103441909 A (SICHUAN CHANGHONG ELECTRIC CO., LTD.), 11 December 2013 (11.12.2013), description, paragraphs [0031]-[0046]	1-10
A	CN 105005217 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.), 28 October 2015 (28.10.2015), the whole document	1-10
A	CN 104243576 A (SHENZHEN MOMODA XINSHENG SCIENCE & TECHNOLOGY CO., LTD.), 24 December 2014 (24.12.2014), the whole document	1-10
A	US 2011137439 A1 (LU, M.W.), 09 June 2011 (09.06.2011), the whole document	1-10

☐ 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
10 February 2017 (10.02.2017)	**03 March 2017 (03.03.2017)**
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 **ZHANG, Wei** Telephone No.: (86-10) **62413356**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/108981

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104615004 A	13 May 2015	None	
CN 103441909 A	11 December 2013	None	
CN 105005217 A	28 October 2015	None	
CN 104243576 A	24 December 2014	WO 2016037411 A1	17 March 2016
US 2011137439 A1	09 June 2011	None	

国际检索报告

国际申请号
PCT/CN2016/108981

A. 主题的分类

G05B 15/02(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)

G05B H04L 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,EPODOC,CNPAT,CNKI:控制 智能 家居 家电 命令 指令 操作 终端 安全 权限 表 名单 control intelligent smart household home command instruction operation terminal safe authority list

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 104615004 A (北京海尔广科数字技术有限公司 等) 2015年 5月 13日 (2015-05-13) 说明书第[0027]-[0073]段	1-10
X	CN 103441909 A (四川长虹电器股份有限公司) 2013年 12月 11日 (2013-12-11) 说明书第[0031]-[0046]段	1-10
A	CN 105005217 A (广东欧珀移动通信有限公司) 2015年 10月 28日 (2015-10-28) 全文	1-10
A	CN 104243576 A (深圳万物新生科技有限公司) 2014年 12月 24日 (2014-12-24) 全文	1-10
A	US 2011137439 A1 (LU, MING-WEI) 2011年 6月 9日 (2011-06-09) 全文	1-10

☐ 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
2017年 2月 10日	2017年 3月 3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 张巍 电话号码 (86-10)62413356

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/108981

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 104615004 A	2015年 5月 13日	无	
CN 103441909 A	2013年 12月 11日	无	
CN 105005217 A	2015年 10月 28日	无	
CN 104243576 A	2014年 12月 24日	WO 2016037411 A1	2016年 3月 17日
US 2011137439 A1	2011年 6月 9日	无	