



(12) 发明专利

(10) 授权公告号 CN 113596124 B

(45) 授权公告日 2023.04.28

(21) 申请号 202110817045.8

H04L 67/10 (2022.01)

(22) 申请日 2021.07.20

(56) 对比文件

(65) 同一申请的已公布的文献号

申请公布号 CN 113596124 A

JP 2003099507 A, 2003.04.04

JP 2016218770 A, 2016.12.22

US 10180962 B1, 2019.01.15

US 10404759 B1, 2019.09.03

(43) 申请公布日 2021.11.02

US 2014372583 A1, 2014.12.18

WO 2017175933 A1, 2017.10.12

WO 2020133495 A1, 2020.07.02

(73) 专利权人 四川虹美智能科技有限公司

地址 621050 四川省绵阳市涪城区九州大道303号

陈帅. 基于Web技术的金川公司三矿区通风管理系统研究. 中国优秀硕士学位论文全文数据库. 2021, 全文.

(72) 发明人 朱堂华 邓宏 陈良

审查员 刘磊

(74) 专利代理机构 济南信达专利事务所有限公司

37100

专利代理师 李世喆

(51) Int. Cl.

H04L 67/125 (2022.01)

H04L 9/40 (2022.01)

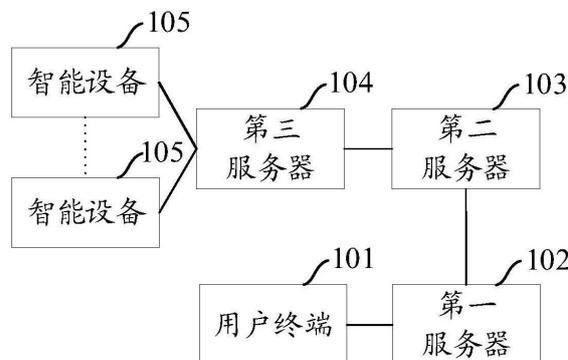
权利要求书3页 说明书10页 附图2页

(54) 发明名称

智能设备的控制系统和方法

(57) 摘要

本发明实施例提供了智能设备的控制系统和方法, 该系统包括: 用户终端、第一服务器、第二服务器、第三服务器和至少一个智能设备; 用户终端与第一服务器配置连接; 第二服务器和第三服务器配置连接, 且第三服务器和至少一个智能设备配置连接; 用户终端, 用于根据用户触发产生对至少一个智能设备中的目标智能设备进行控制的控制指令, 并将该控制指令发送给第一服务器; 第一服务器, 用于根据该控制指令向第二服务器发送与该控制指令对应的控制接口调用请求; 第二服务器, 用于将该控制接口调用请求发送给第三服务器; 第三服务器, 用于根据该控制接口调用请求访问对应的控制接口, 以对目标智能设备进行控制。本方案能够实现对智能设备的控制。



1. 智能设备的控制系统,其特征在于,包括:用户终端、第一服务器、第二服务器、第三服务器和至少一个智能设备;其中,所述第一服务器与所述第二服务器分别对应同一公司的不同部门;所述用户终端为所述第一服务器对应的部门的应用程序;所述第三服务器对应所述智能设备的厂商;所述智能设备的厂商对应的所述第三服务器与所述公司的所述第二服务器对接;所述同一公司的不同部门之间建立有授权机制;

所述用户终端与所述第一服务器配置连接;

所述第二服务器和所述第三服务器配置连接,且所述第三服务器和所述至少一个智能设备配置连接;

所述用户终端,用于根据用户触发产生对所述至少一个智能设备中的目标智能设备进行控制的控制指令,并将该控制指令发送给所述第一服务器;

所述第一服务器,用于接收所述控制指令,并根据该控制指令向所述第二服务器发送与该控制指令对应的控制接口调用请求;

所述第二服务器,用于接收所述控制接口调用请求,并将该控制接口调用请求发送给所述第三服务器;

所述第三服务器,用于接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,以对所述目标智能设备进行控制。

2. 根据权利要求1所述的系统,其特征在于,

所述用户终端,用于向所述第三服务器发送授权请求;

所述第三服务器,用于根据所述授权请求进行授权,并将授权成功的信息发送给所述第二服务器;

所述第二服务器,用于接收所述授权成功的信息,并发送给所述第一服务器;

所述第一服务器,用于接收所述授权成功的信息,并将所述授权成功的消息发送给所述用户终端;

所述用户终端,进一步用于在接收到所述授权成功的消息后,更新设备控制列表以展示给用户。

3. 根据权利要求2所述的系统,其特征在于,

所述第二服务器,用于根据预先设定的授权码生成规则生成第一授权码,并将携带有第一授权码的授权请求发送给所述第三服务器;

所述第三服务器,用于接收所述携带有第一授权码的授权请求,并根据所述授权码生成规则生成第二授权码;判断所述第一授权码和所述第二授权码是否一致,并在所述第一授权码和所述第二授权码一致时对所述第二服务器进行授权。

4. 根据权利要求3所述的系统,其特征在于,

所述第三服务器,用于在所述第一授权码和所述第二授权码一致时,将第一令牌发送给所述第二服务器;

所述第三服务器,进一步用于在接收到所述第二服务器发送的所述控制接口调用请求时,判断所述控制接口调用请求中是否包含所述第一令牌;若包含,则根据所述控制接口请求访问对应的控制接口;否则,向所述用户终端返回第一令牌不存在的提示。

5. 根据权利要求3所述的系统,其特征在于,

所述第三服务器,用于在所述第一授权码和所述第二授权码一致时,将第二令牌发送

给所述第二服务器；

所述第三服务器,进一步用于接收到所述第二服务器发送的所述控制接口调用请求时,判断所述第二令牌是否超过有效期;若是,则向所述用户终端返回令牌无效的提示;否则,根据所述控制接口调用请求访问对应的控制接口。

6. 利用权利要求1至5中任一所述的智能设备的控制系统实现智能设备的控制方法,其特征在于,包括:

利用用户终端根据用户触发产生对至少一个智能设备中的目标智能设备进行控制的控制指令,并将该控制指令发送给第一服务器;

利用所述第一服务器接收所述控制指令,并根据该控制指令向第二服务器发送与该控制指令对应的控制接口调用请求;

利用所述第二服务器接收所述控制接口调用请求,并将该控制接口调用请求发送给第三服务器;

利用第三服务器接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,以对所述目标智能设备进行控制。

7. 根据权利要求6所述的方法,其特征在于,在利用用户终端根据用户触发产生对至少一个智能设备中的目标智能设备进行控制的控制指令之前,进一步包括:

利用所述用户终端向所述第三服务器发送授权请求;

利用所述第三服务器根据所述授权请求进行授权,并将授权成功的信息发送给所述第二服务器;

利用所述第二服务器接收所述授权成功的信息,并发送给所述第一服务器;

利用所述第一服务器接收所述授权成功的信息,并将该授权成功的信息发送给所述用户终端;

利用所述用户终端在接收到所述授权成功的消息后,更新设备控制列表以展示给用户。

8. 根据权利要求7所述的方法,其特征在于,所述利用所述第三服务器根据所述授权请求完成授权,包括:

利用所述第二服务器根据预先设定的授权码生成规则生成第一授权码,并将携带有第一授权码的授权请求发送给所述第三服务器;

利用所述第三服务器接收所述携带有第一授权码的授权请求;

利用所述第三服务器根据所述授权码生成规则生成第二授权码;

判断所述第一授权码和所述第二授权码是否一致;

若所述第一授权码和所述第二授权码一致,则对所述第二服务器进行授权。

9. 根据权利要求8所述的方法,其特征在于,在所述第一授权码和所述第二授权码一致时,进一步包括:

利用第三服务器将第一令牌发送给所述第二服务器;

所述利用第三服务器接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,包括:

利用所述第三服务器接收所述第二服务器发送的所述控制接口调用请求;

利用所述第三服务器判断所述控制接口调用请求中是否包含所述第一令牌;

若包含,则根据所述控制接口调用请求访问对应的控制接口;

否则,向所述用户终端返回第一令牌不存在的提示。

10.根据权利要求8所述的方法,其特征在于,在所述第一授权码和所述第二授权码一致时,进一步包括:

利用第三服务器将第二令牌发送给所述第二服务器;

所述利用第三服务器接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,包括:

利用所述第三服务器接收所述第二服务器发送的所述控制接口调用请求;

利用所述第三服务器判断所述第二令牌是否超过有效期;

若是,则向所述用户终端返回令牌无效的提示;

否则,根据所述控制接口调用请求访问对应的控制接口。

智能设备的控制系统和方法

技术领域

[0001] 本发明涉及物联网技术领域,特别涉及智能设备的控制系统和方法。

背景技术

[0002] 随着物联网技术的发展,厂商之间的对接也越来越频繁。然而,频繁的和厂商对接会造成资源的浪费和管理不统一等问题。比如,一家公司内部可能有多个部门同时在和外部的某个厂商进行对接,那么如果每一个部门都去和该厂商对接一次的话,势必会造成资源的浪费和不易同一管理的问题。

[0003] 申请号为CN201910793937.1的专利申请公开了一种基于oauth2协议的用户认证系统,该专利通过中心模块、Redis存储模块、用户中心模块和服务网关等几个模块实现众多微服务客户端节点用户的认证,能够提升各节点的安全性、效率和稳定性。然而,该方案并未具体提出如何通过一方去解决多方业务的需求。因此,在本专利中,由于不同用户对该设备进行控制时均需要与该智能设备的厂商进行对接,从而会造成资源浪费的问题。

发明内容

[0004] 本发明实施例提供了智能设备的控制系统和方法,能够实现对智能设备的控制。

[0005] 第一方面,本发明实施例提供了一种智能设备的控制系统,包括:用户终端、第一服务器、第二服务器、第三服务器和至少一个智能设备;

[0006] 所述用户终端与所述第一服务器配置连接;

[0007] 所述第二服务器和所述第三服务器配置连接,且所述第三服务器和所述至少一个智能设备配置连接;

[0008] 所述用户终端,用于根据用户触发产生对所述至少一个智能设备中的目标智能设备进行控制的控制指令,并将该控制指令发送给所述第一服务器;

[0009] 所述第一服务器,用于接收所述控制指令,并根据该控制指令向所述第二服务器发送与所述控制指令对应的控制接口调用请求;

[0010] 所述第二服务器,用于接收所述控制接口调用请求,并将该控制接口调用请求发送给所述第三服务器;

[0011] 所述第三服务器,用于接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,以对所述目标智能设备进行控制。

[0012] 在一种可能的实现方式中,

[0013] 所述用户终端,用于向所述第三服务器发送授权请求;

[0014] 所述第三服务器,用于根据所述授权请求进行授权,并将授权成功的信息发送给所述第二服务器;

[0015] 所述第二服务器,用于接收所述授权成功的信息,并发送给所述第一服务器;

[0016] 所述第一服务器,用于接收所述授权成功的信息,并将所述授权成功的消息发送给所述用户终端;

[0017] 所述用户终端,进一步用于在接收到所述授权成功的消息后,更新设备控制列表以展示给用户。

[0018] 在一种可能的实现方式中,

[0019] 所述第二服务器,用于根据预先设定的授权码生成规则生成第一授权码,并将携带有第一授权码的授权请求发送给所述第三服务器;

[0020] 所述第三服务器,用于接收所述携带有第一授权码的授权请求,并根据所述授权码生成规则生成第二授权码;判断所述第一授权码和所述第二授权码是否一致,并在所述第一授权码和所述第二授权码一致时对所述第二服务器进行授权。

[0021] 在一种可能的实现方式中,

[0022] 所述第三服务器,用于在所述第一授权码和所述第二授权码一致时,将第一令牌发送给所述第二服务器;

[0023] 所述第三服务器,进一步用于在接收到所述第二服务器发送的所述控制接口调用请求时,判断所述控制接口调用请求中是否包含所述第一令牌;若包含,则根据所述控制接口请求访问对应的控制接口;否则,向所述用户终端返回第一令牌不存在的提示。

[0024] 在一种可能的实现方式中,

[0025] 所述第三服务器,用于在所述第一授权码和所述第二授权码一致时,将第二令牌发送给所述第二服务器;

[0026] 所述第三服务器,进一步用于接收到所述第二服务器发送的所述控制接口调用请求时,判断所述第二令牌是否超过有效期;若是,则向所述用户终端返回令牌无效的提示;否则,根据所述控制接口调用请求访问对应的控制接口。

[0027] 第二方面,本发明实施例提供了一种智能设备的控制方法,包括:利用用户终端根据用户触发产生对至少一个智能设备中的目标智能设备进行控制的控制指令,并将该控制指令发送给第一服务器;

[0028] 利用所述第一服务器接收所述控制指令,并根据该控制指令向第二服务器发送与该控制指令对应的控制接口调用请求;

[0029] 利用所述第二服务器接收所述控制接口调用请求,并将该控制接口调用请求发送给第三服务器;

[0030] 利用第三服务器接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,以对所述目标智能设备进行控制。

[0031] 在一种可能的实现方式中,在利用用户终端根据用户触发产生对至少一个智能设备中的目标智能设备进行控制的控制指令之前,进一步包括:

[0032] 利用所述用户终端向所述第三服务器发送授权请求;

[0033] 利用所述第三服务器根据所述授权请求进行授权,并将授权成功的信息发送给所述第二服务器;

[0034] 利用所述第二服务器接收所述授权成功的信息,并发送给所述第一服务器;

[0035] 利用所述第一服务器接收所述授权成功的信息,并将该授权成功的信息发送给所述用户终端;

[0036] 利用所述用户终端在接收到所述授权成功的消息后,更新设备控制列表以展示给用户。

[0037] 在一种可能的实现方式中,所述利用所述第三服务器根据所述授权请求完成授权,包括:

[0038] 利用所述第二服务器根据预先设定的授权码生成规则生成第一授权码,并将携带有第一授权码的授权请求发送给所述第三服务器;

[0039] 利用所述第三服务器接收所述携带有第一授权码的授权请求;

[0040] 利用所述第三服务器根据所述授权码生成规则生成第二授权码;

[0041] 判断所述第一授权码和所述第二授权码是否一致;

[0042] 若所述第一授权码和所述第二授权码一致,则对所述第二服务器进行授权。

[0043] 在一种可能的实现方式中,在所述第一授权码和所述第二授权码一致时,进一步包括:

[0044] 利用第三服务器将第一令牌发送给所述第二服务器;

[0045] 所述利用第三服务器接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,包括:

[0046] 利用所述第三服务器接收所述第二服务器发送的所述控制接口调用请求;

[0047] 利用所述第三服务器判断所述控制接口调用请求中是否包含所述第一令牌;

[0048] 若包含,则根据所述控制接口调用请求访问对应的控制接口;

[0049] 否则,向所述用户终端返回第一令牌不存在的提示。

[0050] 在一种可能的实现方式中,在所述第一授权码和所述第二授权码一致时,进一步包括:

[0051] 利用第三服务器将第二令牌发送给所述第二服务器;

[0052] 所述利用第三服务器接收所述控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,包括:

[0053] 利用所述第三服务器接收所述第二服务器发送的所述控制接口调用请求;

[0054] 利用所述第三服务器判断所述第二令牌是否超过有效期;

[0055] 若是,则向所述用户终端返回令牌无效的提示;

[0056] 否则,根据所述控制接口调用请求访问对应的控制接口。

[0057] 由上述技术方案可知,在对智能设备进行控制时,考虑用户终端与第一服务器配置连接,第二服务器和第三服务器配置连接,且第三服务器和智能设备配置连接。如此当用户终端生成对目标智能设备进行控制的控制指令后,用户终端会将该控制指令发送给与其配置连接的第一服务器,第一服务器根据该控制指令向第二服务器发送用于访问目标智能设备的控制接口访问请求。进一步,第二服务器将该控制接口访问请求发送给与其连接的第三服务器,如此第三服务器即可根据该控制接口调用请求访问对应的控制接口,从而实现目标智能设备的控制。由此可见,本方案中的第一服务器和第二服务器在需要对智能设备进行控制时,不需要第一服务器和第二服务器分别去和第三服务器进行对接即可实现对智能设备的控制,从而减少由于频繁对接所造成的资源浪费。

附图说明

[0058] 为了更清楚地说明本发明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简单地介绍,显而易见地,下面描述中的附图是本发明

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的前提下,还可以根据这些附图获得其他的附图。

[0059] 图1是本发明一个实施例提供的一种智能设备的控制系统的示意图;

[0060] 图2是本发明一个实施例提供的另一种智能设备的控制系统的示意图;

[0061] 图3是本发明一个实施例提供的一种智能设备的控制方法的流程图。

具体实施方式

[0062] 如前所述,随着智能家居的发展,各个厂商之间的对接越来越多。一个设备可以被多家厂商所控制,一家厂商也可以控制多家其他厂商的设备,从而在对接过程中产生了多种对接方式。然而在有些情况下,频繁的与厂商对接会造成资源的浪费和管理不统一等问题。比如,一家公司内部可能有多个部门同时在和外部厂商进行对接,那么如果每一个部门都去和该厂商对接一次的话,势必会造成资源的浪费和不易同一管理等问题。

[0063] 目前,在处理多厂商之间的设备控制问题时,通常采用的方式是控制方分别去和设备对应的厂商进行对接,从而实现对智能设备的控制。比如A厂商是设备方,能够直接控制智能设备M,若B厂商和C厂商要控制智能设备M时,需要厂商B和厂商C分别去和厂商A进行对接,从而在得到认证许可后对设备M进行控制。显然,如此频繁的和设备的厂商A进行对接,会造成资源的浪费,尤其是当厂商B和厂商C是一个公司的不同部门时更为显著。

[0064] 基于此,本方案考虑通过一方和设备的厂商进行对接,其他厂商或部门之间形成一种协同授权的机制,从而其他厂商或部门不需要都去和设备的厂商进行对接,从而解决多部门与多个外部厂商对接中的资源浪费问题。

[0065] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例,基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0066] 如图1所示,本发明实施例提供了一种智能设备的控制系统,该系统可以包括:用户终端101、第一服务器102、第二服务器103、第三服务器104和至少一个智能设备105;

[0067] 用户终端101与第一服务器102配置连接;

[0068] 第二服务器103和第三服务器104配置连接,且第三服务器104和至少一个智能设备105配置连接;

[0069] 用户终端101,用于根据用户触发产生对至少一个智能设备105中的目标智能设备进行控制的控制指令,并将该控制指令发送给第一服务器102;

[0070] 第一服务器102,用于接收控制指令,并根据该控制指令向第二服务器103发送与该控制指令对应的控制接口调用请求;

[0071] 第二服务器103,用于接收控制接口调用请求,并将该控制接口调用请求发送给第三服务器104;

[0072] 第三服务器104,用于接收控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,以对目标智能设备进行控制。

[0073] 本发明实施例中,在对智能设备进行控制时,考虑用户终端101与第一服务器102配置连接,第二服务器103和第三服务器104配置连接,且第三服务器104和智能设备配置连

接。如此当用户终端101生成对目标智能设备进行控制的控制指令后,用户终端101会将该控制指令发送给与其配置连接的第一服务器102,第一服务器102根据该控制指令向第二服务器103发送用于访问目标智能设备的控制接口访问请求。进一步,第二服务器103将该控制接口访问请求发送给与其连接的第三服务器104,如此第三服务器104即可根据该控制接口调用请求访问对应的控制接口,从而实现目标智能设备的控制。由此可见,本方案中的第一服务器102和第二服务器103在需要对智能设备进行控制时,不需要第一服务器102和第二服务器103分别去和第三服务器104进行对接即可实现对智能设备的控制,从而减少由于频繁对接所造成的资源浪费。

[0074] 比如,在本发明实施例中,第一服务器102可以是A部门,而对应的用户终端101则是A部门的应用程序APP,第二服务器103可以是与A部门所属同一公司的B部门,第三服务器104是智能设备对应的C厂商,考虑让B部门和C厂商进行对接,如此B部门可以实现对C厂商的智能设备的控制。而当A部门要对C厂商的智能设备进行控制时,可以通过A部门的用户终端101,向同公司的B部门发送控制接口调用请求,从而由B部门去和C厂商进行对接,以获得对应的控制接口,实现对智能设备的控制。如此避免了频繁的和C厂商进行对接验证,浪费大量的资源,同时也能够解决公司内部多个部门与外部厂商进行对接时很难同一管理的问题。

[0075] 在一种可能的实现方式中,用户终端101,用于向第三服务器104发送授权请求;

[0076] 第三服务器104,用于根据授权请求进行授权,并将授权成功的信息发送给第二服务器103;

[0077] 第二服务器103,用于接收授权成功的信息,并发送给第一服务器102;

[0078] 第一服务器102,用于接收授权成功的信息,并将授权成功的消息发送给用户终端101;

[0079] 用户终端101,进一步用于在接收到授权成功的消息后,更新设备控制列表以展示给用户。

[0080] 在本发明实施例中,在用户通过与第一服务器102连接的用户终端101对第三服务器104的智能设备进行控制时,可以考虑首先完成第三服务器104和第二服务器103之间的授权。比如首先通过用户终端101向第三服务器104发送授权请求,第三服务器104在接收到授权请求时,在满足授权条件的情况下完成授权,并将授权成功的消息发送给第二服务器103,第二服务器103作为中转发给第一服务器102,第一服务器102与用户终端101配置连接,从而可以根据授权成功的消息,将用户终端101上第三服务器104的智能设备的控制列表进行更新,从而用户可以从更新后的控制列表中选择相应的智能设备进行控制。

[0081] 需要指出的是,本发明实施例中,进行授权的授权协议可以包括OAuth2.0等。

[0082] 在一种可能的实现方式中,在第三服务器104进行授权时,第二服务器103,用于根据预先设定的授权码生成规则生成第一授权码,并将携带有第一授权码的授权请求发送给第三服务器104;

[0083] 第三服务器104,用于接收携带有第一授权码的授权请求,并根据授权码生成规则生成第二授权码;判断第一授权码和第二授权码是否一致,并在第一授权码和第二授权码一致时对第二服务器103进行授权。

[0084] 在本发明实施例中,在第三服务器104进行授权时,首先由第二服务器103根据预

先设定的授权码生成规则生成第一授权码,然后将携带有该第一授权码的授权请求发送给第三服务器104。第三服务器104同样根据预先设定的授权规则生成第二授权码,然后判断第一授权码和第二授权码是否一致,如此在第一授权码和第二授权码一致时实现对第三服务器104的授权,从而保证两个服务器之间访问的安全性和可行性。

[0085] 在生成第一授权码和第二授权码时,可以考虑根据预先设定的授权码生成规则生成相应的授权码。比如授权码由APP的IP、APP的标识码code和时间戳等通过一定的算法生成。即第一授权码由第二服务器103对应的APP的IP、第二服务器103对应的APP的标识码code以及时间戳通过一定算法生成。第二授权码由第三服务器104对应的APP的IP、第三服务器104对应的APP的标识码code以及时间戳通过与第一授权码相同的算法生成。如此通过比对第一授权码和第二授权码即可实现对第二服务器103的验证授权。

[0086] 在一种可能的实现方式中,第三服务器104还可以通过给第二服务器103发送令牌的方式以使第二服务器103进行访问,具体地:

[0087] 第三服务器104,用于在第一授权码和第二授权码一致时,将第一令牌发送给第二服务器103;

[0088] 第三服务器104,进一步用于在接收到第二服务器103发送的控制接口调用请求时,判断控制接口调用请求中是否包含第一令牌;若包含,则根据控制接口请求访问对应的控制接口;否则,向用户终端101返回第一令牌不存在的提示。

[0089] 在本发明实施例中,当第一授权码和第二授权码一致时,第三服务器104可以将第一令牌发送给第二服务器103,即通过该令牌可以表示第二服务器103通过了第三服务器104的验证。如此当第二服务器103向第三服务器104发送控制接口调用请求时,第三服务器104可以判断该控制接口调用请求中是否包含第一令牌,若包含则说明该控制接口调用请求合法,即可根据控制接口调用请求访问对应的接口。而当控制接口调用请求中不包含第一令牌时,则该访问不合法,则可以返回第一令牌不存在的提示,进而可以将该提示通过第二服务器103和第一服务器102返回给用户终端101,以展示给用户。

[0090] 在一种可能的实现方式中,第三服务器104还可以对令牌的有效期进行验证,具体如下:

[0091] 第三服务器104,用于在第一授权码和第二授权码一致时,将第二令牌发送给第二服务器103;

[0092] 第三服务器104,进一步用于接收到第二服务器103发送的控制接口调用请求时,判断第二令牌是否超过有效期;若是,则向用户终端101返回令牌无效的提示;否则,根据控制接口调用请求访问对应的控制接口。

[0093] 在本发明实施例中,当第一授权码和第二授权码一致时,第三服务器104可以将第二令牌发送给第二服务器103,如此当第二服务器103将该第二令牌携带在控制接口调用请求中发送给第三服务器104时,第三服务器104会对该第二令牌的有效期进行验证,判断该第二令牌是否超过了有效期限,若超过了有效期,则返回令牌无效的提示,进一步通过第二服务器103和第一服务器102返回给用户终端101,以通知用户。若没有超过有效期,则可以根据该控制接口调用请求访问对应的控制接口,以实现目标智能设备的控制。如此通过对令牌的合法性和有效期进行验证的方式,保证了接口访问的准确性和安全性。

[0094] 本发明解决了多部门与多个外部厂商对接中造成的资源浪费问题。比如,公司内

部分为白电和黑电两个部门,若黑电已经对接过的第三方,白电再去对接一次,将导致人力,物资、时间等资源的浪费。那么可以将黑电部门和白电部门之间做一个桥梁,让两者能够共享外部厂商的资源,将大大减少2个部门的工作量。在一种可能的实现方式中,如图2所示,用户使用和后台服务之间的关系示意如下:

[0095] 用户使用白电的app对智能设备进行控制时,首先向第三方厂商申请授权,app调用第三方厂商的授权地址,并将授权过程中产生的一个授权码authcode转发给黑电,由黑电继续用authcode去换取在用户授权许可后,授权服务器下发给客户端的授权凭证access token和用于更新访问令牌的refresh token。黑电成功获取了access token和refresh token之后,对于第三方设备的授权部分已完成,此时黑电将授权结果通知给白电,白电获取了通知之后,刷新app上厂商授权的状态。白电刷新授权状态后,授权流程就算正式完成,app即可向黑电调用设备列表接口,黑电则向第三方厂商调用相应接口后再将结果返回给白电。用户刷新了设备列表就可以看到自己拥有的第三方厂商的设备,即可点击设备的各种功能进行控制。

[0096] 当前厂商的对接方式通常是一对一的,不能解决这种公司内部多部门对接的情况。而此方案仍然是在原有的OAuth2.0授权方案的基础上通过在不同部门之间建立授权机制实现智能设备的控制,如此能够具有更好的兼容性,且适应更复杂的对接情况。

[0097] 如图3所示,本发明实施例还提供了一种智能设备的控制方法,该方法可以包括如下步骤:

[0098] 步骤301:利用用户终端101根据用户触发产生对至少一个智能设备105中的目标智能设备进行控制的控制指令,并将该控制指令发送给第一服务器102;

[0099] 步骤302:利用第一服务器102接收控制指令,并根据该控制指令向第二服务器103发送与该控制指令对应的控制接口调用请求;

[0100] 步骤303:利用第二服务器103接收控制接口调用请求,并将该控制接口调用请求发送给第三服务器104;

[0101] 步骤304:利用第三服务器104接收控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,以对目标智能设备进行控制。

[0102] 本发明实施例中,在对第三方厂商的智能设备进行控制时,可以首先利用用户终端101根据用户的触发产生对智能设备进行控制的控制指令,并将该控制指令发送给第一服务器102,然后利用第一服务器102根据该控制指令向第二服务器103发送控制接口调用请求,进一步利用第二服务器103将该控制接口调用请求发送给第三服务器104,如此第三服务器104可以根据该控制接口调用请求访问对应的控制接口,从而实现对目标智能设备的控制。由此可见,本方案在不同部门对第三方智能设备进行控制时,不需要都直接和外部厂商进行对接,在各部门之间建立授权协议,通过一个部门与外部厂商对接即可实现各个厂商之间的信息和资源贡献,从而能够减少资源的浪费,也便于公司对各个部门之间的统一管理。

[0103] 在一种可能的实现方式中,在利用用户终端101根据用户触发产生对至少一个智能设备105中的目标智能设备进行控制的控制指令之前,进一步包括:

[0104] 利用用户终端101向第三服务器104发送授权请求;

[0105] 利用第三服务器104根据授权请求进行授权,并将授权成功的信息发送给第二服

务器103;

[0106] 利用第二服务器103接收授权成功的信息,并发送给第一服务器102;

[0107] 利用第一服务器102接收授权成功的信息,并将该授权成功的信息发送给用户终端101;

[0108] 利用用户终端101在接收到授权成功的消息后,更新设备控制列表以展示给用户。

[0109] 在本发明实施例中,在对第三方的智能设备进行控制之前,还可以考虑获得智能设备所对应的第三服务器104的授权。具体可以由用户终端101向第三服务器104发送授权请求,第三服务器104在完成授权后将授权成功的消息发送给第二服务器103,第二服务器103和第一服务器102依次将授权成功的消息通知给用户终端101,从而用户终端101更新第三方的设备控制列表,从而用户可以根据更新后的设备控制列表进行相应的控制功能。

[0110] 在一种可能的实现方式中,利用第三服务器104根据授权请求完成授权,包括:

[0111] 利用第二服务器103根据预先设定的授权码生成规则生成第一授权码,并将携带有第一授权码的授权请求发送给第三服务器104;

[0112] 利用第三服务器104接收携带有第一授权码的授权请求;

[0113] 利用第三服务器104根据授权码生成规则生成第二授权码;

[0114] 判断第一授权码和第二授权码是否一致;

[0115] 若第一授权码和第二授权码一致,则对第二服务器103进行授权。

[0116] 在本发明实施例中,在第三服务器104进行授权时,可以首先考虑利用第二服务器103根据预先设定的授权码生成规则生成第一授权码,并将该第一授权码发送给第三服务器104。同样的,利用第三服务器104采用相同的授权码生成规则生成第二授权码,通过比较第一授权码和第二授权码,在第一授权码和第二授权码一致时,对第二服务器103完成授权。如此通过生成授权码,并进行授权验证的方式,保证各服务器之间访问的安全性。

[0117] 在一种可能的实现方式中,在第一授权码和第二授权码一致时,进一步包括:

[0118] 利用第三服务器104将第一令牌发送给第二服务器103;

[0119] 利用第三服务器104接收控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,包括:

[0120] 利用第三服务器104接收第二服务器103发送的控制接口调用请求;

[0121] 利用第三服务器104判断控制接口调用请求中是否包含第一令牌;

[0122] 若包含,则根据控制接口调用请求访问对应的控制接口;

[0123] 否则,向用户终端101返回第一令牌不存在的提示。

[0124] 在另一种可能的实现方式中,在第一授权码和第二授权码一致时,还可以包括:

[0125] 利用第三服务器104将第二令牌发送给第二服务器103;

[0126] 利用第三服务器104接收控制接口调用请求,并根据该控制接口调用请求访问对应的控制接口,包括:

[0127] 利用第三服务器104接收第二服务器103发送的控制接口调用请求;

[0128] 利用第三服务器104判断第二令牌是否超过有效期;

[0129] 若是,则向用户终端101返回令牌无效的提示;

[0130] 否则,根据控制接口调用请求访问对应的控制接口。

[0131] 在第一授权码和第二授权码一致时,本发明通过对控制接口调用请求中是和否包

含令牌,以及对令牌是否超过了有效期进行验证,能够提高各服务器之间进行访问的安全性。

[0132] 本发明的内容是针对第三方厂商的云云对接,在本公司内部的不同部门之间进行内部对接,避免和第三方厂商的多次对接。比如结合图2所示,用户有第三方厂商的设备,并已在第三方厂商注册,可以通过第三方厂商正常控制设备,此时用户也有本公司的账号,并想在本公司的app中实现对第三方设备的控制,具体实施方式如下:

[0133] 1、用户打开本公司白电的app,选择第三方厂商申请授权,此时app会调用第三方厂商的授权地址并打开相应的授权页面,用户需要登录自己的第三方厂商的账号密码来获取第三方厂商的授权。用户操作完成后第三方厂商会将OAuth2.0授权中第一步的authcode通过已经和黑电对接时配置好的回调地址转发给黑电。黑电获取authcode之后,会再调用第三方厂商的授权接口去换取access token和refresh token。

[0134] 2、黑电成功获取了access token和refresh token之后,对于第三方设备的授权部分已完成,此时黑电会将授权成功的结果通知给白电,白电获取了通知之后,去刷新app上厂商授权的状态。

[0135] 3、白电刷新授权状态后,即可向黑电调用设备列表接口,黑电则向第三方厂商调用相应接口后再将结果返回给白电。

[0136] 4、设备列表刷新成功,用户可以在本公司app上看到第三方厂商的设备,点击详情即可看到设备的详细信息和各种可控制的功能。用户在app上下发设备控制的指令,白电服务器收到控制指令后会通过调用黑电的设备控制接口,黑电继而调用第三方厂商的接口,实现设备的成功控制。第三方厂商会在设备控制成功后,将设备的最新状态返回给黑电,黑电则会将状态转发给白电。

[0137] 在这个控制过程中,黑电作为已经和第三方对接过的部门,已经具备在黑电系统中(如电视中)控制第三方设备的能力。并且黑电系统本身也将作为一个中转站,将对于第三方设备的各种控制和通知进行一次封装,用于公司内部其他部门的调用,实现了和第三方厂商的一次对接,多处使用的效果,提高了对接效率,减少出错机会。

[0138] 可以理解的是,本发明实施例示意的结构并不构成对智能设备的控制系统的各个设备的具体限定。在本发明的另一些实施例中,智能设备的控制系统中所提到的设备可以包括比图示更多或者更少的部件,或者组合某些部件,或者拆分某些部件,或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[0139] 上述各实施例提供的智能设备的控制系统中各装置内之间的信息交互、执行过程等内容与本发明各实施例提供的智能设备的控制方法基于同一发明构思。

[0140] 需要说明的是,在本文中,诸如第一和第二之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个·····”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同因素。

[0141] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过

程序指令相关的硬件来完成,前述的程序可以存储在计算机可读取的存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质中。

[0142] 最后需要说明的是:以上所述仅为本发明的较佳实施例,仅用于说明本发明的技术方案,并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所做的任何修改、等同替换、改进等,均包含在本发明的保护范围内。

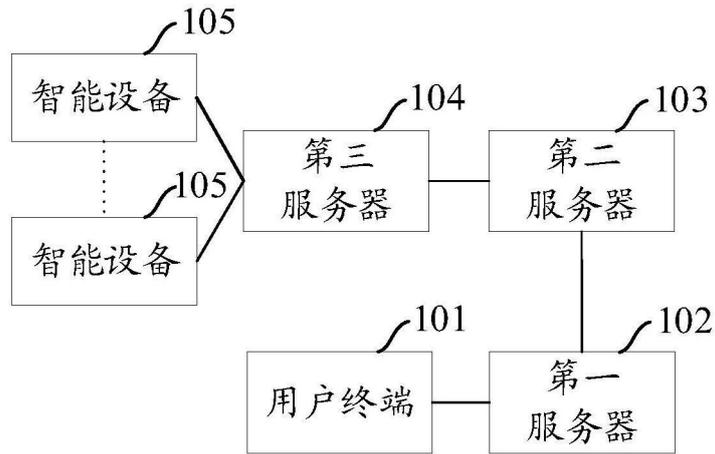


图1

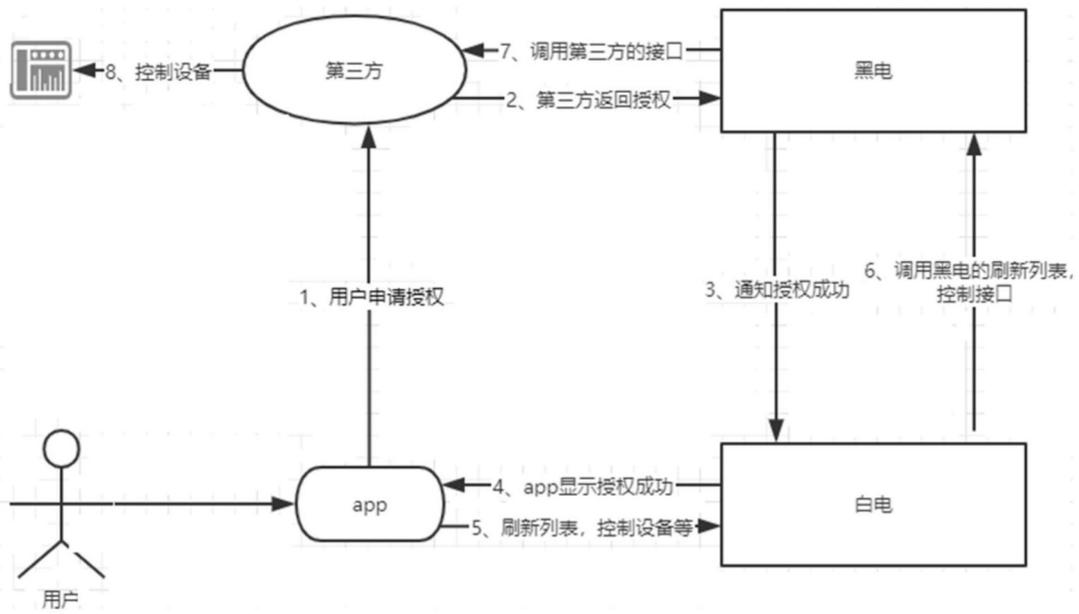


图2

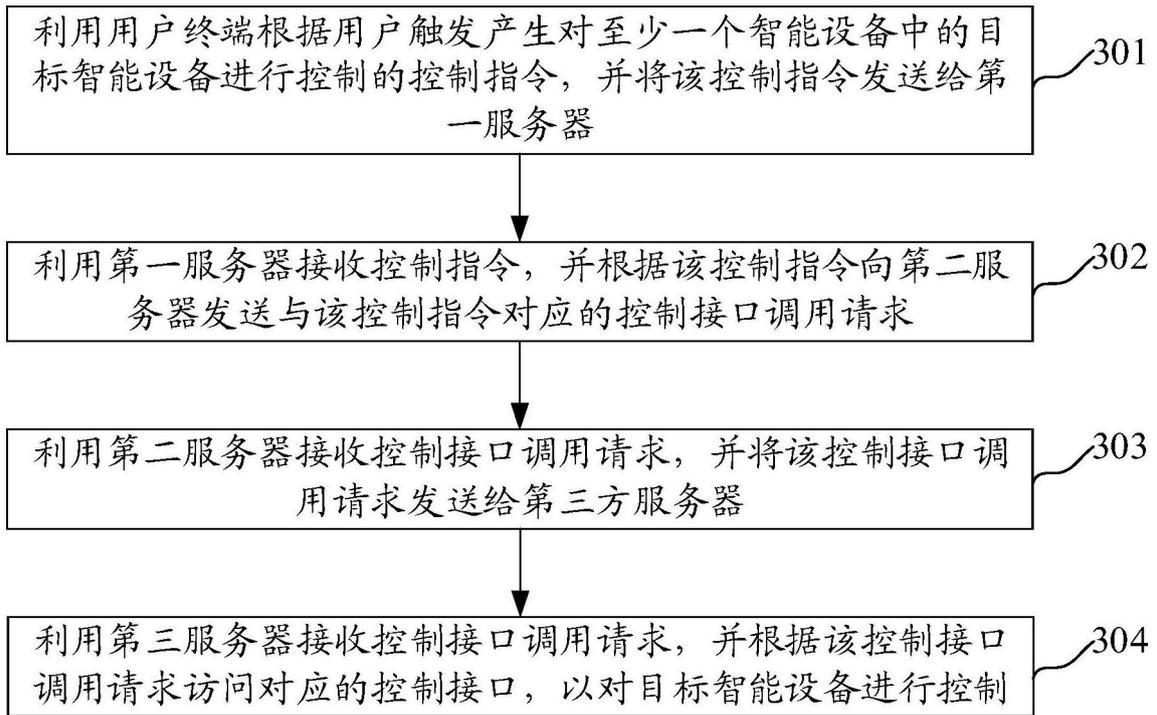


图3