



(12)发明专利

(10)授权公告号 CN 109040301 B

(45)授权公告日 2019.09.03

(21)申请号 201811034297.8

(22)申请日 2018.09.05

(65)同一申请的已公布的文献号

申请公布号 CN 109040301 A

(43)申请公布日 2018.12.18

(73)专利权人 梅州市万通电脑科技有限公司

地址 514299 广东省梅州市大埔县湖寮镇
同仁路南安苑A幢7号门店

(72)发明人 罗孝琼

(74)专利代理机构 广州越华专利代理事务所

(普通合伙) 44523

代理人 杨艳珊

(51)Int.Cl.

H04L 29/08(2006.01)

(56)对比文件

CN 105635283 A,2016.06.01,

CN 104599042 A,2015.05.06,

CN 103809542 A,2014.05.21,

US 2015/0142963 A1,2015.05.21,

审查员 徐苏宁

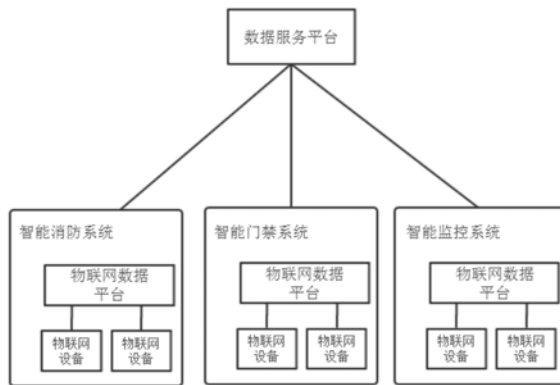
权利要求书2页 说明书6页 附图1页

(54)发明名称

基于物联网的智慧安防数据系统

(57)摘要

本发明涉及一种基于物联网的智慧安防数据系统,其包括数据服务平台和智慧安防子系统,智慧安防子系统包括智能消防系统、智能门禁系统和智能监控系统,智慧安防子系统包括物联网设备和物联网数据平台。数据服务平台中的数据中介服务器根据接收到的数据服务请求将相关的智慧安防子系统分为数据生产方和数据应用方。数据中介服务器接收由数据生产方发送的可用数据流的元数据以及由数据应用方发送的数据需求信息,然后将数据应用方与数据生产方进行配对。数据中介服务器生成生产方配置和应用方配置,并将其传输至相应的物联网数据平台;基于识别的配对,数据生产方与数据应用方建立对等连接,从而实现智慧安防子系统之间的实时数据共享。



1. 一种基于物联网的智慧安防数据系统,其特征就在于,其包括数据服务平台和智慧安防子系统,所述智慧安防子系统包括智能消防系统、智能门禁系统和智能监控系统,智能消防系统、智能门禁系统和智能监控系统分别包括物联网设备和物联网数据平台,所述物联网数据平台包括数据处理模块和数据代理模块,数据代理模块包括通信单元和数据字段映射单元,

数据服务平台中的数据中介服务器根据接收到的数据服务请求将相关的智慧安防子系统分为数据生产方和数据应用方,

数据中介服务器接收由数据生产方发送的可用数据流的元数据以及由数据应用方发送的数据需求信息,然后将数据应用方与满足其需求的数据生产方进行配对,所述数据需求信息包括对与多个数据流相关联的各个数据字段的选择,

数据中介服务器生成生产方配置和应用方配置,并将其传输至相应的物联网数据平台;所述生产方配置由数据中介服务器产生并将其发送至与单次数据服务相关联的数据生产方,所述生产方配置用于标识数据应用方并且指定由数据生产方提供的数据流的所选数据字段;

所述应用方配置由数据中介服务器产生并将其发送至与单次数据服务相关联的数据应用方,所述应用方配置用于标识将数据流传输到数据应用方的数据生产方并且指定将流传输的数据映射到单个目标数据流时的映射策略;基于识别的配对,数据生产方与数据应用方建立对等连接,从而实现智慧安防子系统之间的实时数据共享,其包括:

数据中介服务器响应于数据应用方的数据请求并根据其数据需求信息使相应的数据生产方选择性地数据字段发送给数据应用方,数据应用方将从数据生产方接收到的多个数据流的数据字段组装成用于智慧安防应用的单个目标数据流,经由通信单元接收到的数据流被传输至数据字段映射单元,数据字段映射单元根据应用方配置聚合多个数据流上的数据字段以生成单个目标数据流。

2. 根据权利要求1所述的智慧安防数据系统,其特征就在于,所述智能消防系统的应用包括消防预警和消防信息发布,所述智能门禁系统的应用包括车辆识别、人员识别和门禁预警,所述智能监控系统的应用包括智能跟踪和行为预警。

3. 根据权利要求2所述的智慧安防数据系统,其特征就在于,所述可用数据流的元数据包括:数据类型,数据速率,收集数据的物联网设备的信息,所述物联网设备的信息包括地理位置、制造商、型号、序列号和测量精度;

所述数据需求信息还包括:数据类型、数据速率以及收集数据时的地理位置信息和时间信息。

4. 根据权利要求3所述的智慧安防数据系统,其特征就在于,所述数据中介服务器生成安全令牌并将其连同数据应用方的网络地址一并发送给数据生产方,数据生产方中的数据代理模块根据安全令牌和网络地址与数据应用方建立对等连接。

5. 根据权利要求4所述的智慧安防数据系统,其特征就在于,在建立对等连接后,数据生产方根据生产方配置过滤原始数据流并将数据需求信息中选择的数据字段发送给数据应用方;

数据应用方接收来自数据生产方的数据流,然后通过数据代理模块将各个接收到的数据流组合成单个目标数据流。

6. 根据权利要求5所述的智慧安防数据系统,其特征在于,所述数据中介服务器包括通信模块、用户界面模块、配置创建器、供需信息库和标识信息库,其中,

所述供需信息库用于存储可用数据流的元数据和各个智慧安防子系统所需的数据流的元数据,

所述标识信息库用于存储各个智慧安防子系统的标识信息,

所述配置创建器用于生成生产方配置和应用方配置。

基于物联网的智慧安防数据系统

技术领域

[0001] 本发明涉及安防数据共享和物联网领域,尤其涉及一种基于物联网的智慧安防数据系统。

背景技术

[0002] 智慧安防,即安防物联网技术是实现智能安全小区、楼群和城区的安防网络系统设施,通过建立功能齐全的综合系统,运用有线和无线的传输手段、人员监管和机器智能分析处理方法,达到区域安防物联网的目的。智慧安防采用物联网和大数据等技术,整合了智能化信息采集、大数据处理和智慧安防应用,能够提升社区、小区的整体感知、分析和应急事件处理能力。

[0003] 现有的智慧安防技术方案中,往往以社区或小区为单位,将所有物联网设备采集的数据传输至安防控制中心,由安防控制中心的人员基于采集的数据和安防软件预设的策略来进行安防管理。现有技术存在以下缺陷:1、安防控制中心往往以社区或小区为单位进行建立并工作,在通常情况下,物联网设备采集的数据就局限在各个安防控制中心覆盖的范围内,数据没有得到充分的应用,不利于实现更科学的区域安防联防联控的目的。2、安防系统中各个安防子系统(例如,门禁系统、消防系统、监控系统、停车系统)中物联网设备采集的数据都需要全部传输至安防控制中心,然后各个安防子系统再从安防控制中心的数据库请求其它子系统采集的数据以支持其具体的安防应用。这样,安防子系统需要将数据流重新组合再筛选,然而实际只使用了数据流中的部分数据。因此造成了带宽资源的浪费,并且降低了安防应用的响应速度。

发明内容

[0004] 针对现有技术之不足,本发明提供了一种基于物联网的智慧安防数据系统,其包括数据服务平台和智慧安防子系统,所述智慧安防子系统包括智能消防系统、智能门禁系统和智能监控系统,所述智慧安防子系统包括物联网设备和物联网数据平台,所述物联网数据平台包括数据处理模块和数据代理模块;

[0005] 数据服务平台中的数据中介服务器根据接收到的数据服务请求并结合智慧安防子系统的标识信息将相关的智慧安防子系统分为数据生产方和数据应用方;

[0006] 数据中介服务器接收由数据生产方发送的可用数据流的元数据以及由数据应用方发送的数据需求信息,然后将数据应用方与满足其需求的数据生产方进行配对,所述数据需求信息包括对与多个数据流相关联的各个数据字段的选择;

[0007] 数据中介服务器生成生产方配置和应用方配置,并将其传输至相应的物联网数据平台;基于识别的配对,数据生产方与数据应用方建立对等连接,从而实现智慧安防子系统之间的实时数据共享,其包括:

[0008] 数据中介服务器响应于数据应用方的数据请求并根据其数据需求信息使相应的数据生产方选择性地将数据字段发送给数据应用方,数据应用方将从数据生产方接收到的

多个数据流的数据字段组装成用于智慧安防应用的单个目标数据流。

[0009] 根据一个优选实施方式,所述智能消防系统的应用包括消防预警和消防信息发布,所述智能门禁系统的应用包括车辆识别、人员识别和门禁预警,所述智能监控系统的应用包括智能跟踪和行为预警。

[0010] 根据一个优选实施方式,所述可用数据流的元数据包括:数据类型,数据速率,收集数据的物联网设备的信息,所述物联网设备的信息包括地理位置、制造商、型号、序列号和测量精度;

[0011] 所述数据需求信息还包括:数据类型、数据速率以及收集数据时的地理位置信息和时间信息。

[0012] 根据一个优选实施方式,所述生产方配置由数据中介服务器产生并将其发送至与单次数据服务相关联的数据生产方,所述生产方配置用于标识数据应用方并且指定由数据生产方提供的数据流的所选数据字段;

[0013] 所述应用方配置由数据中介服务器产生并将其发送至与单次数据服务相关联的数据应用方,所述应用方配置用于标识将数据流传输到数据应用方的数据生产方并且指定将流传输的数据映射到单个目标数据流时的映射策略。

[0014] 根据一个优选实施方式,所述数据中介服务器生成安全令牌并将其连同数据应用方的网络地址一并发送给数据生产方,数据生产方中的数据代理模块根据安全令牌和网络地址与数据应用方建立对等连接。

[0015] 根据一个优选实施方式,在建立对等连接后,数据生产方根据生产方配置过滤原始数据流并将数据需求信息中选择的数据字段发送给数据应用方;

[0016] 数据应用方接收来自数据生产方的数据流,然后通过数据代理模块将各个接收到的数据流组合成单个目标数据流。

[0017] 根据一个优选实施方式,所述数据中介服务器包括通信模块、用户界面模块、配置创建器、供需信息库和标识信息库,其中,

[0018] 所述供需信息库用于存储可用数据流的元数据和各个智慧安防子系统所需的数据流的元数据,

[0019] 所述标识信息库用于存储各个智慧安防子系统的标识信息,

[0020] 所述配置创建器用于生成生产方配置和应用方配置。

[0021] 本发明具有以下有益效果:

[0022] 数据服务平台中的数据中介服务器根据接收到的数据服务请求将相关的智慧安防子系统分为数据生产方和数据应用方。数据中介服务器根据接收到的由数据生产方发送的可用数据流的元数据以及由数据应用方发送的数据需求信息生成生产方配置和应用方配置,并将其传输至相应的物联网数据平台;基于识别的配对,数据生产方与数据应用方建立对等连接,从而实现智慧安防子系统之间的实时数据共享。因此,本发明能够将属于不同小区的智慧安防子系统中产生的物联网数据根据智慧安防应用的需求进行实时数据共享。由于这种数据实时共享是通过不同智慧安防子系统之间直接建立对等连接以选择性地传输数据流,相比于传统的智慧安防系统的数据传输方案,能够大大拓展安防数据的应用边界,同时还能够有效地节约带宽并具有更快地响应速度。

[0023] 此外,数据应用方能够将将从多个数据生产方接收到的多个数据流的数据字段组装

成用于指定智慧安防应用的单个目标数据流,不需要大量的人力来进行跨数据流过滤和聚合数据,从而显著降低了人工成本,更利于推广应用。

附图说明

[0024] 图1示出了本发明的智慧安防数据系统的系统框图;

[0025] 图2示出了本发明中一个实施例的系统连接示意图。

具体实施方式

[0026] 为使本发明的目的、技术方案和优点更加清楚了,下面结合具体实施方式并参照附图,对本发明进一步详细说明。应该理解,这些描述只是示例性的,而并非要限制本发明的范围。此外,在以下说明中,省略了对公知结构和技术的描述,以避免不必要地混淆本发明的概念。需要说明的是,本发明中的“数据生产方”和“数据应用方”分别用于代指生成数据和应用数据的物联网数据平台,其在不同的实际应用情况时可以相互转换,简言之,在单次数据服务过程中,发送数据流的物联网数据平台为数据生产方,接收数据流的物联网数据平台为数据应用方。

[0027] 如图1所示,本发明提供了一种基于物联网的智慧安防数据系统,其包括数据服务平台和智慧安防子系统。智慧安防子系统包括智能消防系统、智能门禁系统和智能监控系统。智慧安防子系统包括物联网设备和物联网数据平台,物联网数据平台包括数据处理模块和数据代理模块。

[0028] 数据服务平台中的数据中介服务器根据接收到的数据服务请求并结合智慧安防子系统的标识信息将相关的智慧安防子系统分为数据生产方和数据应用方。

[0029] 数据中介服务器接收由数据生产方发送的可用数据流的元数据以及由数据应用方发送的数据需求信息,然后将数据应用方与满足其需求的数据生产方进行配对。数据需求信息包括对与多个数据流相关联的各个数据字段的选择。

[0030] 数据中介服务器生成生产方配置和应用方配置,并将其传输至相应的物联网数据平台;基于识别的配对,数据生产方与数据应用方建立对等连接,从而实现智慧安防子系统之间的实时数据共享,其具体包括:数据中介服务器响应于数据应用方的数据请求并根据其数据需求信息使相应的数据生产方选择性地数据字段发送给数据应用方,数据应用方将从数据生产方接收到的多个数据流的数据字段组装成用于智慧安防应用的单个目标数据流。

[0031] 示例性地,智能消防系统的应用包括消防预警和消防信息发布,智能门禁系统的应用包括车辆识别、人员识别和门禁预警,智能监控系统的应用包括智能跟踪和行为预警。

[0032] 本发明避免了现有的智能安防技术方案中存在的各个社区的安防系统的物联网数据应用范围受限,以及集中式存储造成的大带宽需求和资源浪费的问题,能够实现物联网数据跨社区以及跨安防系统的数据共享,具有很好的可扩展性。此外,本发明不需要大量的人力来进行跨数据流过滤和聚合数据,有利于节省人力开支和推广应用。

[0033] 实施例1

[0034] 图2为本实施例的智慧安防数据系统的连接示意图,需要说明的是,为了简明清晰地表达出该实施例的技术方案特点,图中略去了数据服务平台、智慧安防子系统,而分别采

用其具体构成结构来说明本发明的技术方案。此外图中略去了与物联网数据平台相连接的多个物联网设备。

[0035] 在本实施例中,位于左侧及右侧的物联网数据平台为数据生产方,位于中间的接收数据流的物联网数据平台为数据应用方。为了便于理解,该实施例可以看做为了执行智能消防系统的消防信息发布应用时的示意图,中间的物联网数据平台属于智能消防系统,左侧和右侧的物联网数据平台分别属于智能门禁系统和智能监控系统。数据流10为特定时段的门禁信息,数据流20为特定时段和特定区域的监控信息。这样,智能消防系统在进行消防信息发布时,就能够接收数据流10和数据流20中指定的数据字段并将其重新组合以用于确定消防事故责任人并进行发布。

[0036] 应该理解的是,智慧安防数据系统通常可以包括任意数量的物联网数据平台,并且每个单独的物联网数据平台通常可以充当数据生产方或数据应用方。此外,图中物联网设备的数量通常来说为多个,为了表达方便仅示例性地示出了部分物联网设备,因此不应将此看作对本发明的限制。

[0037] 在智慧安防数据系统中,连接到物联网数据平台的多个物联网设备包括但不限于音视频设备、环境传感器和监测装置(例如,温度传感器,压力传感器,红外传感器,ID卡设备和相关的警报系统)以及固定或移动计算设备。每个物联网数据平台中的数据处理模块可以处理或分析从相应的物联网设备接收的原始数据。此外,每个物联网数据平台中的数据代理模块用于与数据中介服务器进行通信以及与其它物联网数据平台进行数据交换。

[0038] 对于充当数据生产方的物联网数据平台,其数据代理模块将关于可用数据流的元数据发送到数据中介服务器。该元数据可以包括数据类型、数据速率、关于收集数据的物联网设备的信息,物联网设备的信息包括它们的位置,制造商,型号/序列号以及测量精度。类似地,对于充当数据应用方的物联网数据平台,数据代理模块将数据需求信息传输到数据中介服务器,前述数据需求信息包括对与多个数据流相关联的各个数据字段的选择,此外数据需求信息还包括数据类型、数据速率以及收集数据时的地理位置信息和时间信息。

[0039] 在数据中介服务器接收到数据应用方发送的数据服务请求以及数据需求信息后,将数据应用方与满足其需求的数据生产方进行配对。进一步地,数据中介服务器生成生产方配置和应用方配置,并将其传输至相应的物联网数据平台。

[0040] 生产方配置由数据中介服务器产生并将其发送至与单次数据服务相关联的数据生产方,生产方配置用于标识数据应用方并且指定由数据生产方提供的数据流的所选数据字段。

[0041] 应用方配置由数据中介服务器产生并将其发送至与单次数据服务相关联的数据应用方,应用方配置用于标识将数据流传输到数据应用方的数据生产方并且指定将流传输的数据映射到单个目标数据流时的映射策略。

[0042] 为了使指定的数据生产方和数据应用方连接并进行数据传输,数据中介服务器生成安全令牌并将其连同数据应用方的网络地址一并发送给数据生产方,数据生产方中的数据代理模块根据安全令牌和网络地址与数据应用方建立对等连接。优选地,安全令牌被设置为在特定时间段之后到期,并且更新的安全令牌被周期性地发送给数据应用方和数据生产方以重新建立连接。

[0043] 在建立对等连接后,数据生产方根据生产方配置过滤原始数据流并将数据需求信

息中选择的数据字段发送给数据应用方。数据应用方接收来自多个数据生产方的数据流。基于应用方配置,数据应用方的数据代理模块将各个接收到的数据流组合成单个目标数据流,以供物联网数据平台进一步使用。

[0044] 数据中介服务器包括通信模块、用户界面模块、配置创建器、供需信息库和标识信息库。

[0045] 供需信息库用于存储可用数据流的元数据和各个智慧安防子系统所需的数据流的元数据。

[0046] 标识信息库用于存储各个智慧安防子系统的标识信息,例如,所属社区/小区、地理区域、社区规模、其内部运行的物联网设备类型和/或获取的数据类型的信息。应当说明的是,尽管供需信息库和标识信息库被分开描述,但是它们也可以被集成到单个数据库中,在这种情况下,其属于数据库中的不同类目。

[0047] 配置创建器用于生成生产方配置和应用方配置。通信模块用于从物联网数据平台接收数据服务请求、数据需求信息以及可用数据流的元数据。此外,通信模块还可以被配置为将安全令牌、生产方配置、应用方配置发送到物联网数据平台,并且为物联网数据平台提供用户接口。用户界面模块生成用于向平台用户呈现信息或请求信息的用户界面。

[0048] 物联网数据平台包括数据处理模块和数据代理模块,其中,数据代理模块包括数据过滤单元、数据字段映射单元、数据格式化单元和通信单元。

[0049] 数据处理模块可对传入的原始数据流进行调节,过滤,聚合,平均和/或重新采样。此外,数据处理模块可以分析和处理数据,在充当数据生产方时,原始数据和/或经处理的数据可以被传递到数据代理模块以用于传输到其他物联网数据平台。相对应地,在充当数据应用方时,数据代理模块从其他物联网数据平台接收到的数据流可以被转发到数据处理模块进行分析和处理,或者存储在物联网数据平台的永久存储器中以备将来使用。

[0050] 数据代理模块中的通信单元用于与数据中介服务器通信并且与其他物联网数据平台建立对等连接。

[0051] 在作为数据生产方时,数据过滤单元可以基于生产方配置过滤原始数据流,从而得到仅包括数据需求信息中所选择的数据字段。

[0052] 在作为数据应用方时,经由通信单元接收到的数据流被传输至数据字段映射单元,数据字段映射单元可以根据应用方配置聚合多个数据流上的数据字段以生成单个目标数据流。数据格式化单元用于执行单位转换、数据类型转换从而将接收到的数据格式转换为目标数据流所需的格式。此外数据格式化单元还用于对时间进行校正,其用于确保每个数据样本所属的时间点一致。

[0053] 实施例2

[0054] 作为实施例1的改进和补充,物联网数据平台的网关以及其连接的物联网设备具有带外通信系统。物联网数据平台的网关通过网络广播网关与对应的物联网设备通信的带外无线信标,该带外无线信标包括令牌。在工作时,网关接收到加密分组,网关使用公开密钥将前述加密分组解密为中间有效载荷,然后由网关使用前述令牌将中间有效负载解密为解密的分组。

[0055] 具体地,带外通信系统可以为RF发射器,前述公开密钥对应于多个物联网设备中的证书。通过采用该技术方案,物联网设备与物联网数据平台的网关进行正常通信需要同

时满足以下条件:1、物联网设备具有带外通信系统2、物联网设备位于网关的有效广播通信距离范围内;3、物联网设备具有相应的证书。

[0056] 这样,只有在同时满足前述3个条件时,物联网设备才能与物联网数据平台进行有效地通信,从而有效地避免了其它网络设备攻击物联网数据平台或者与物联网数据平台进行数据交互。由于现有的物联网设备往往安全验证措施不足,因此该技术方案大大提高了物联网数据平台的网络通信安全,从而提高了整个智慧安防数据系统的数据安全性和有效性。

[0057] 实施例3

[0058] 作为实施例1、2的改进和补充,物联网数据平台的网关为智能物联网网关,智能物联网网关具有计算单元和存储器,智能物联网网关采用决策逻辑来根据数据类型和数据内容对数据流进行优先级排序,然后将高于预设优先级的数据传输至对应的物联网数据平台。智能物联网网关能够自动发现附近的物联网设备,通过有线或无线通信通道连接到它们。智能物联网网关支持的通信连接方式包括蜂窝网络、Zigbee、蓝牙、WiFi和NFC。

[0059] 智能物联网网关具有足够的计算能力,存储器和存储容量以及人工智能以分析本地数据以实现本地级别的决策。智能物联网网关具有计算单元和存储器,智能物联网网关采用的决策逻辑包括人工智能、视频分析、规则引擎和决策树。

[0060] 在工作时,智能物联网网关不是保留所有数据并将其发送到物联网数据平台,而是采用决策逻辑来根据数据类型和数据内容对数据流进行优先级排序,并创建减少的数据流,从而将选定的或高于预设优先级的数据传输到物联网数据平台。

[0061] 例如,智能物联网网关可以分析来自物联网设备中的摄像机采集的视频数据,以确定图像内容是否已经从时间T1改变到时间T2。智能物联网网关采用包含规则的规则引擎,如果“视频摄像机1在时间T2的图像内容等同于视频摄像机1在时间T1处的图像内容”,则对时间T1处的视频数据赋予低重要性。根据可用带宽,可以从传输中省略已被识别为低重要性的数据或降低分辨率后再传输。类似地,可以对传感器数据进行类似的分析。例如,低重要性数据可以替代地存储在本地。因此,要传输到物联网数据平台的总数据减少的数据量可取决于上载数据的带宽的可用性。通过这种方式,本地智能物联网网关被用于选择性地优化数据,从而在不丢失重要信息的情况下减少传输数据所需的带宽。

[0062] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以权利要求的保护范围为准。

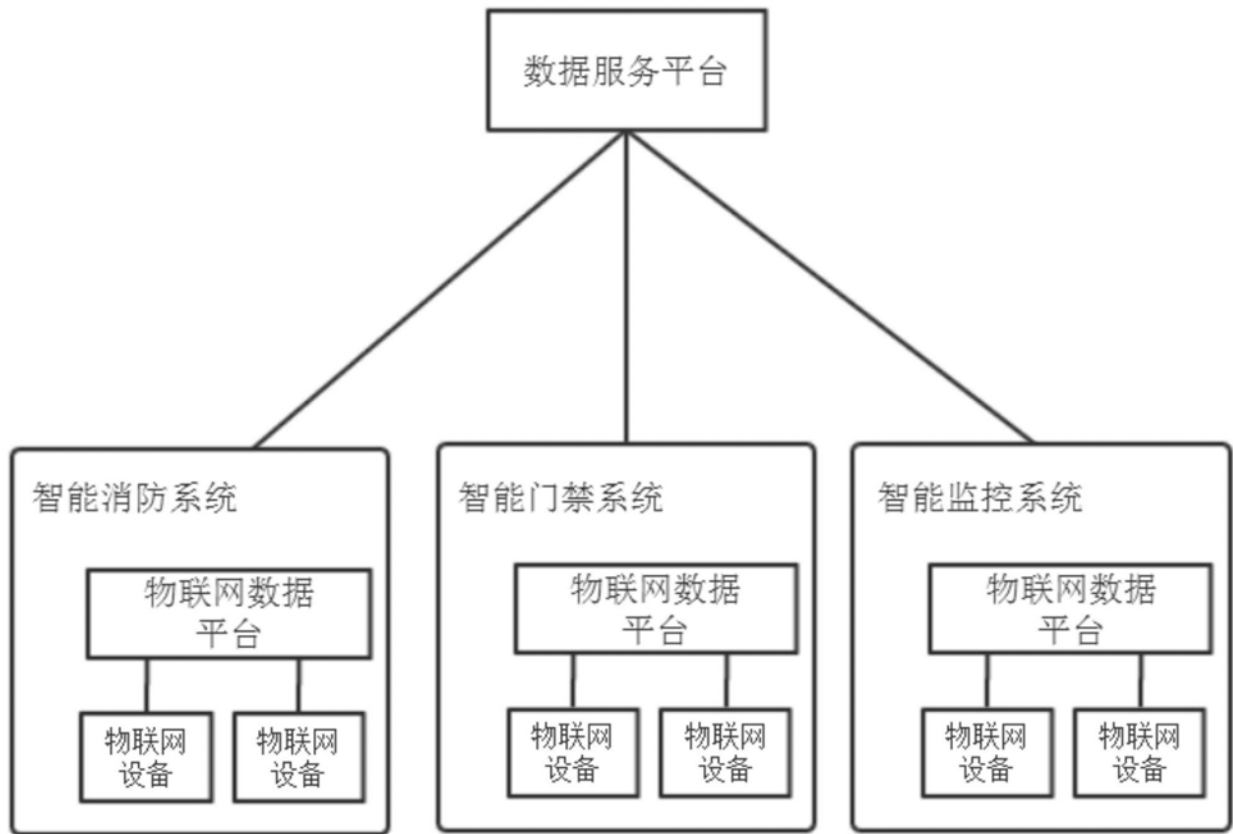


图1

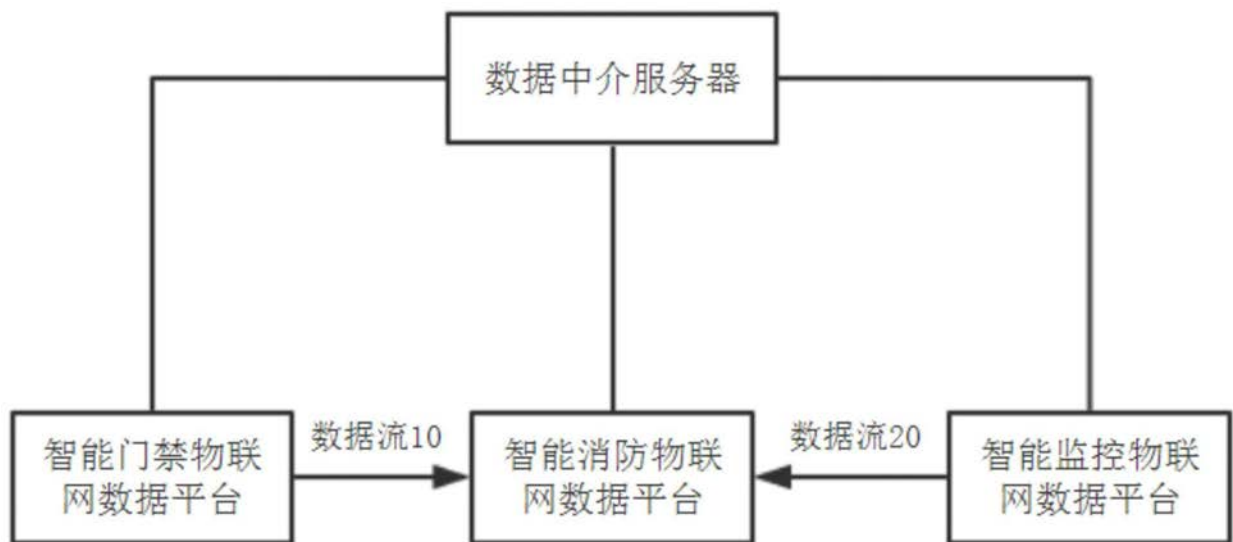


图2