



(12) 发明专利

(10) 授权公告号 CN 110351688 B

(45) 授权公告日 2022. 04. 05

(21) 申请号 201910449677.6

(22) 申请日 2019.05.28

(65) 同一申请的已公布的文献号  
申请公布号 CN 110351688 A

(43) 申请公布日 2019.10.18

(73) 专利权人 杭州电力设备制造有限公司  
地址 311215 浙江省杭州市杭州经济技术  
开发区11号大街91号

专利权人 杭州电力设备制造有限公司萧山  
欣美成套电气制造分公司

(72) 发明人 宋惠忠 陈晓刚 叶剑 黄吾康  
胡苏剑 吕峻 王鹏程 谭海云  
黄俊 蒋耀炯 莫洪亮 王莉芳  
童林杰 吕渭 古永富

(74) 专利代理机构 杭州融方专利代理事务所  
(普通合伙) 33266

代理人 沈相权

(51) Int.Cl.  
H04W 4/70 (2018.01)  
H04W 12/122 (2021.01)  
H04W 16/20 (2009.01)

审查员 程佳丽

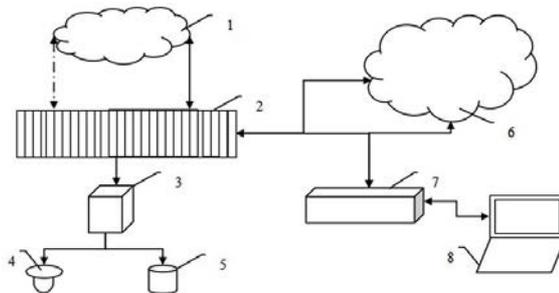
权利要求书2页 说明书5页 附图1页

(54) 发明名称

一种泛在物联网室内分布的共享系统

(57) 摘要

本发明涉及一种共享系统,尤其涉及一种泛在物联网室内分布的共享系统。包含电力专网无线和有线网络、运营商无线和有线网络、中心服务器或节点服务器、发射单元、天线或小型站、分流阻断设备、全频段扫描设备和“黑盒子”安全解析监测平台。一种泛在物联网室内分布的共享系统,极大的保障网络信息安全。



1. 一种泛在物联网室内分布的共享系统,其特征在于:包含电力专网无线和有线网络、运营商无线和有线网络、中心服务器或节点服务器、发射单元、天线或小型站、分流阻断设备、全频段扫描设备和“黑盒子”安全解析监测平台;

采用2G+4G+5G集约式机制,利用共享理念,不但实现中心节点或子节点的共享,也实现机房共享、机柜共享、链路共享、发射单元、天线和小型站共享;

通过无线、网线或光网络接入电力专网和运营商的无线网络及有线网络;中心服务器或节点服务器通过无线、网线或光网络的方式与发射单元连接;发射单元通过射频馈线与天线或小型站连接;天线或小型站通过无线的方式与用户及物联网终端连接;

中心服务器、节点服务器实现光信号与数字信号、数字信号与模拟射频信号的相互转化、光信号、数字信号和模拟射频信号的转发;发射单元实现光信号与数字信号、数字信号与模拟射频信号的相互转化、模拟射频信号的转发;

在用户、物联网终端和应用平台发起操作指令和数据传送中,分流一路信号到分流阻断设备,通过“黑盒子”安全解析监测平台在不泄露数据的情况下,监测和阻断覆盖区域的非法源;

在电力、运营商及其他政企事业单位的重点区域,中心服务器或节点服务器可以下挂全频段扫描设备,可定时或实时的扫描和定位区域内的所有发射源,并将非法源或攻击源通过“黑盒子”安全解析监测平台上报给安全管理部门,方便安全管理部门定点清除重点区域的非法源和攻击源;

分流阻断设备可以直接或通过电力专网无线和有线网络通过中心服务器或节点服务器连接;

天线室内最优布点的方法包含但不限于空间三维间隔布点法或将所有的信号集成到一面天线或小型站中布点法;

运营商无线和有线网络:通过中心服务器或节点服务器接收公网用户或物联网终端上行指令和数据给公网应用平台;通过中心服务器或节点服务器下发公网应用平台的下行指令和数据给公网用户或物联网终端;

中心服务器或节点服务器:接收运营商无线和有线网络公网应用平台的下发指令和下行数据,并转发给发射单元;接收电力专网无线和有线网络专网应用平台的下发指令和下行数据,并转发给发射单元;接收发射单元转发的用户或公网物联网终端上行指令和数据,并转发给运营商无线和有线网络的公网应用平台;接收发射单元转发的专网物联网终端上行指令和数据,并转发给电力专网无线和有线网络的专网应用平台;用户或物联网终端向应用平台发起操作指令时,分流一路信号通过电力专网无线和有线网络或直接分流阻断设备;在应用平台数据下发中,定时或随机抽取数据信号通过电力专网无线和有线网络或直接分流阻断设备;应用平台向用户或物联网终端发起操作指令时,分流一路信号通过电力专网无线和有线网络或直接分流阻断设备;在用户或物联网终端数据上传中,定时或随机抽取数据信号通过电力专网无线和有线网络或直接分流阻断设备;接收分流阻断设备屏蔽或注销指令,阻断或注销非法用户或物联网终端;接收分流阻断设备扫频指令;搜集频段扫描设备采集到的非法源和攻击源的设备名、位置等信息,并转发给分流阻断设备;可实现光信号与数字信号、数字信号与模拟射频信号的相互转化;

发射单元:接收并转发中心服务器或节点服务器下行指令或数据给天线;接收并转发

天线的上行指令或数据给中心服务器或节点服务器;可实现光信号与数字信号、数字信号与模拟射频信号的相互转化;

天线:接收并转发发射单元下行指令或数据给用户或物联网终端;接收并转发用户或物联网终端的上行指令或数据给发射单元;

小型站:接收并转发发射单元下行指令或数据给用户或物联网终端;接收并转发用户或物联网终端的上行指令或数据给发射单元;可实现光信号与数字信号、数字信号与模拟射频信号的相互转化;

电力专网无线和有线网络:通过中心服务器或节点服务器接收专网用户或物联网终端上行指令和数据给专网应用平台;通过中心服务器或节点服务器下发专网应用平台的下行指令和数据给专网用户或物联网终端;接收并转发中心服务器或节点服务器分流的应用平台、用户或物联网终端指令和数据、扫描设备采集到的非法源和攻击源的设备名、位置等信息给分流阻断设备;接收并转发分流阻断设备的扫频、屏蔽或注销指令给中心服务器或节点服务器;

分流阻断设备:接收并解析中心服务器或节点服务器、电力专网无线和有线网络分流的 用户或物联网终端上行指令和数据、应用平台的下行指令和数据,并将解析结果传送给“黑盒子”安全解析监测平台;接收并解析中心服务器或节点服务器、电力专网无线和有线网络上报的非法源和攻击源的设备名、位置等信息,并将解析结果传送给“黑盒子”安全解析监测平台;接收并转发“黑盒子”安全解析监测平台的扫频、屏蔽或注销指令给中心服务器或节点服务器;

“黑盒子”安全解析监测平台:通过关键字和图片匹配或人工智能关键字和图片学习算法判断分流阻断设备解析后的用户或物联网终端上行指令和数据、应用平台的下行指令和数据是否非法;若非法,通过分流阻断设备下发屏蔽或注销指令给中心服务器或节点服务器,将禁止指令和数据传输,严重者可将用户和物联网终端在覆盖网络中屏蔽或注销,防止二次网络侵害;呈现分流阻断设备解析后的非法源和攻击源的设备名、位置等信息,方便安全管理部门定点清除;

全频段扫描设备:在电力、运营商及其他政企事业单位的重点区域,定时或实时的扫描和定位区域内的所有发射源,定位非法源或攻击源。

## 一种泛在物联网室内分布的共享系统

### 技术领域

[0001] 本发明涉及一种共享系统,尤其涉及一种泛在物联网室内分布的共享系统。

### 背景技术

[0002] 在通信和物联网领域,运营商都是各自建立网络,建站和维护成本居高不下,且各自施工单位为了自身利益,相互拆台导致故障频发;2018年国家电网公司提出了“泛在物联网”的概念,但都是通信专网的户外场景应用,未涉及专网的室内应用;经过运营商多年的经验,室内与室外用户数和接入数大体相当,但室内与室外的流量比(贡献率)为27:73,因此建设室内的“泛在物联网”尤为重要。

[0003] 但室内“泛在物联网”建设却存在以下难题:一是单独建立专网,建设成本巨大;二是室内场景环境复杂,各种反射,各种干扰问题严重;三是物联网频段比较窄,三大运营商网络、WIFI等它网络频段,容易对专网形成频段挤压干扰;四是无安全的人机交互机制设计,只花钱不赚钱,很难持续投入;五是和三大运营商的大网并存,几套维护机制和人员,维护容易出故障。一种泛在物联网室内分布共享系统、装置及方法,采用2G+4G+5G集约式机制,极大的降低了建站和维护的成本;利用共享理念,可方便实现天线室内最优布点,降低室内信源干扰,提高网络覆盖效果,同时能降低覆盖区域的电磁辐射;采用全频段扫描设备和“黑盒子”安全解析监测平台,能在保证用户隐私的情况下,定位和阻断非法源和攻击源,极大的保障网络信息安全。

### 发明内容

[0004] 本发明主要是解决现有技术中存在的不足,提供一种极大的降低了建站和维护的成本;利用共享理念,可方便实现天线室内最优布点,降低室内信源干扰,提高网络覆盖效果,同时能降低覆盖区域的电磁辐射;采用全频段扫描设备和“黑盒子”安全解析监测平台,能在保证用户隐私的情况下,定位和阻断非法源和攻击源,极大的保障网络信息安全。

[0005] 本发明的上述技术问题主要是通过下述技术方案得以解决的:

[0006] 一种泛在物联网室内分布的共享系统,包含电力专网无线和有线网络、运营商无线和有线网络、中心服务器或节点服务器、发射单元、天线或小型站、分流阻断设备、全频段扫描设备和“黑盒子”安全解析监测平台。

[0007] 作为优选,采用2G+4G+5G集约式机制,利用共享理念,不但实现中心节点或子节点的共享,也实现机房共享、机柜共享、链路共享、发射单元、天线和小型站共享。

[0008] 作为优选,通过无线、网线或光网络接入电力专网和运营商的无线网络及有线网络;中心服务器或节点服务器通过无线、网线或光网络的方式与发射单元连接;发射单元通过射频馈线与天线或小型站连接;天线或小型站通过无线的方式与用户及物联网终端连接。

[0009] 作为优选,中心服务器、节点服务器实现光信号与数字信号、数字信号与模拟射频信号的相互转化、光信号、数字信号和模拟射频信号的转发;发射单元实现光信号与数字信

号、数字信号与模拟射频信号的相互转化、模拟射频信号的转发。

[0010] 作为优选,在用户、物联网终端和应用平台发起操作指令和数据传送中,分流一路信号到分流阻断设备,通过“黑盒子”安全解析监测平台在不泄露数据的情况下,监测和阻断覆盖区域的非法源。

[0011] 作为优选,在电力、运营商及其他政企事业单位的重点区域,中心服务器或节点服务器可以下挂全频段扫描设备,可定时或实时的扫描和定位区域内的所有发射源,并将非法源或攻击源通过“黑盒子”安全解析监测平台上报给安全管理部门,方便安全管理部门定点清除重点区域的非法源和攻击源。

[0012] 作为优选,分流阻断设备可以直接或通过电力专网无线和有线网络通过中心服务器或节点服务器连接。

[0013] 作为优选,天线室内最优布点的方法包含但不限于空间三维间隔布点法或将所有的信号集成到一面天线或小型站中布点法。

[0014] 作为优选,运营商无线和有线网络:通过中心服务器或节点服务器接收公网用户或物联网终端上行指令和数据给公网应用平台;通过中心服务器或节点服务器下发公网应用平台的下行指令和数据给公网用户或物联网终端;

[0015] 中心服务器或节点服务器:接收运营商无线和有线网络公网应用平台的下发指令和下行数据,并转发给发射单元;接收电力专网无线和有线网络专网应用平台的下发指令和下行数据,并转发给发射单元;接收发射单元转发的用户或公网物联网终端上行指令和数据,并转发给运营商无线和有线网络的公网应用平台;接收发射单元转发的专网物联网终端上行指令和数据,并转发给电力专网无线和有线网络的专网应用平台;用户或物联网终端向应用平台发起操作指令时,分流一路信号通过电力专网无线和有线网络或直接分流阻断设备;在应用平台数据下发中,定时或随机抽取数据信号通过电力专网无线和有线网络或直接分流阻断设备;应用平台向用户或物联网终端发起操作指令时,分流一路信号通过电力专网无线和有线网络或直接分流阻断设备;在用户或物联网终端数据上传中,定时或随机抽取数据信号通过电力专网无线和有线网络或直接分流阻断设备;接收分流阻断设备屏蔽或注销指令,阻断或注销非法用户或物联网终端;接收分流阻断设备扫频指令;搜集频段扫描设备采集到的非法源和攻击源的设备名、位置等信息,并转发给分流阻断设备;可实现光信号与数字信号、数字信号与模拟射频信号的相互转化;

[0016] 发射单元:接收并转发中心服务器或节点服务器下行指令或数据给天线;接收并转发天线的上行指令或数据给中心服务器或节点服务器;可实现光信号与数字信号、数字信号与模拟射频信号的相互转化;

[0017] 天线:接收并转发发射单元下行指令或数据给用户或物联网终端;接收并转发用户或物联网终端的上行指令或数据给发射单元;

[0018] 小型站:接收并转发发射单元下行指令或数据给用户或物联网终端;接收并转发用户或物联网终端的上行指令或数据给发射单元;可实现光信号与数字信号、数字信号与模拟射频信号的相互转化;

[0019] 电力专网无线和有线网络:通过中心服务器或节点服务器接收专网用户或物联网终端上行指令和数据给专网应用平台;通过中心服务器或节点服务器下发专网应用平台的下行指令和数据给专网用户或物联网终端;接收并转发中心服务器或节点服务器分流的应

用平台、用户或物联网终端指令和数据、扫描设备采集到的非法源和攻击源的设备名、位置等信息给分流阻断设备；接收并转发分流阻断设备的扫频、屏蔽或注销指令给中心服务器或节点服务器；

[0020] 分流阻断设备：接收并解析中心服务器或节点服务器、电力专网无线和有线网络分流的终端上行指令和数据、应用平台的下行指令和数据，并将解析结果传送给“黑盒子”安全解析监测平台；接收并解析中心服务器或节点服务器、电力专网无线和有线网络上报的非法源和攻击源的设备名、位置等信息，并将解析结果传送给“黑盒子”安全解析监测平台；接收并转发“黑盒子”安全解析监测平台的扫频、屏蔽或注销指令给中心服务器或节点服务器；

[0021] “黑盒子”安全解析监测平台：通过关键字和图片匹配或人工智能关键字和图片学习算法判断分流阻断设备解析后的终端上行指令和数据、应用平台的下行指令和数据是否非法；若非法，通过分流阻断设备下发屏蔽或注销指令给中心服务器或节点服务器，将禁止指令和数据传输，严重者可将用户和物联网终端在覆盖网络中屏蔽或注销，防止二次网络侵害；呈现分流阻断设备解析后的非法源和攻击源的设备名、位置等信息，方便安全管理部门定点清除；

[0022] 全频段扫描设备：在电力、运营商及其他政企事业单位的重点区域，定时或实时的扫描和定位区域内的所有发射源，定位非法源或攻击源。

[0023] 采用2G+4G+5G集约式机制，利用共享理念，将泛在物联网室内分布共享系统的中心服务器或节点服务器放置于楼宇地下配电柜或室外配电房中，通过无线、网线或光网络接入电力专网和运营商的无线网络及有线网络；中心服务器或节点服务器通过无线、网线或光网络的方式通过发射单元、天线或小型站与用户及物联网终端连接；在用户、物联网终端和应用平台发起操作指令和数据传送中，分流信号到“黑盒子”安全解析监测平台，监测和阻断覆盖区域的非法源；在电力、运营商及其他政企事业单位的重点区域，中心服务器或节点服务器可定时或实时扫描和定位非法源或攻击源，方便安全管理部门定点清除。该系统、装置和方法采用2G+4G+5G集约式机制，极大的降低了建站和维护的成本；利用共享理念，可方便实现天线室内最优布点，降低室内信源干扰，提高网络覆盖效果，同时能降低覆盖区域的电磁辐射；采用全频段扫描设备和“黑盒子”安全解析监测平台，能在保证用户隐私的情况下，定位和阻断非法源和攻击源，极大的保障网络信息安全。

[0024] 因此，本发明一种泛在物联网室内分布的共享系统，极大的保障网络信息安全。

## 附图说明

[0025] 图1是本发明共享系统示意图；

[0026] 图2是本发明中共享系统安全监测示意图。

[0027] 图中附图标记所示：

[0028] 1、运营商无线和有线网络；2、中心服务器或节点服务器；3、发射单元；4、天线；5、小型站；6、电力专网无线和有线网络；7、分流阻断设备；8、“黑盒子”安全解析监测平台；9、全频段扫描设备。

## 具体实施方式

[0029] 下面通过实施例,并结合附图,对本发明的技术方案作进一步具体的说明。

[0030] 实施例1:如图所示,一种泛在物联网室内分布的共享系统,包含电力专网无线和有线网络、运营商无线和有线网络、中心服务器或节点服务器、发射单元、天线或小型站、分流阻断设备、全频段扫描设备和“黑盒子”安全解析监测平台。

[0031] 采用2G+4G+5G集约式机制,利用共享理念,不但实现中心节点或子节点的共享,也实现机房共享、机柜共享、链路共享、发射单元、天线和小型站共享。

[0032] 通过无线、网线或光网络接入电力专网和运营商的无线网络及有线网络;中心服务器或节点服务器通过无线、网线或光网络的方式与发射单元连接;发射单元通过射频馈线与天线或小型站连接;天线或小型站通过无线的方式与用户及物联网终端连接。

[0033] 中心服务器、节点服务器实现光信号与数字信号、数字信号与模拟射频信号的相互转化、光信号、数字信号和模拟射频信号的转发;发射单元实现光信号与数字信号、数字信号与模拟射频信号的相互转化、模拟射频信号的转发。

[0034] 在用户、物联网终端和应用平台发起操作指令和数据传送中,分流一路信号到分流阻断设备,通过“黑盒子”安全解析监测平台在不泄露数据的情况下,监测和阻断覆盖区域的非法源。

[0035] 在电力、运营商及其他政企事业单位的重点区域,中心服务器或节点服务器可以下挂全频段扫描设备,可定时或实时的扫描和定位区域内的所有发射源,并将非法源或攻击源通过“黑盒子”安全解析监测平台上报给安全管理部门,方便安全管理部门定点清除重点区域的非法源和攻击源。

[0036] 分流阻断设备可以直接或通过电力专网无线和有线网络通过中心服务器或节点服务器连接。

[0037] 天线室内最优布点的方法包含但不限于空间三维间隔布点法或将所有的信号集成到一面天线或小型站中布点法。

[0038] 运营商无线和有线网络:通过中心服务器或节点服务器接收公网用户或物联网终端上行指令和数据给公网应用平台;通过中心服务器或节点服务器下发公网应用平台的下行指令和数据给公网用户或物联网终端;

[0039] 中心服务器或节点服务器:接收运营商无线和有线网络公网应用平台的下发指令和下行数据,并转发给发射单元;接收电力专网无线和有线网络专网应用平台的下发指令和下行数据,并转发给发射单元;接收发射单元转发的用户或公网物联网终端上行指令和数据,并转发给运营商无线和有线网络的公网应用平台;接收发射单元转发的专网物联网终端上行指令和数据,并转发给电力专网无线和有线网络的专网应用平台;用户或物联网终端向应用平台发起操作指令时,分流一路信号通过电力专网无线和有线网络或直接分流阻断设备;在应用平台数据下发中,定时或随机抽取数据信号通过电力专网无线和有线网络或直接分流阻断设备;应用平台向用户或物联网终端发起操作指令时,分流一路信号通过电力专网无线和有线网络或直接分流阻断设备;在用户或物联网终端数据上传中,定时或随机抽取数据信号通过电力专网无线和有线网络或直接分流阻断设备;接收分流阻断设备屏蔽或注销指令,阻断或注销非法用户或物联网终端;接收分流阻断设备扫描指令;搜集频段扫描设备采集到的非法源和攻击源的设备名、位置等信息,并转发给分流阻断设备;可

实现光信号与数字信号、数字信号与模拟射频信号的相互转化；

[0040] 发射单元：接收并转发中心服务器或节点服务器下行指令或数据给天线；接收并转发天线的上行指令或数据给中心服务器或节点服务器；可实现光信号与数字信号、数字信号与模拟射频信号的相互转化；

[0041] 天线：接收并转发发射单元下行指令或数据给用户或物联网终端；接收并转发用户或物联网终端的上行指令或数据给发射单元；

[0042] 小型站：接收并转发发射单元下行指令或数据给用户或物联网终端；接收并转发用户或物联网终端的上行指令或数据给发射单元；可实现光信号与数字信号、数字信号与模拟射频信号的相互转化；

[0043] 电力专网无线和有线网络：通过中心服务器或节点服务器接收专网用户或物联网终端上行指令和数据给专网应用平台；通过中心服务器或节点服务器下发专网应用平台的下行指令和数据给专网用户或物联网终端；接收并转发中心服务器或节点服务器分流的应用平台、用户或物联网终端指令和数据、扫描设备采集到的非法源和攻击源的设备名、位置等信息给分流阻断设备；接收并转发分流阻断设备的扫频、屏蔽或注销指令给中心服务器或节点服务器；

[0044] 分流阻断设备：接收并解析中心服务器或节点服务器、电力专网无线和有线网络分流的用户或物联网终端上行指令和数据、应用平台的下行指令和数据，并将解析结果传送给“黑盒子”安全解析监测平台；接收并解析中心服务器或节点服务器、电力专网无线和有线网络上报的非法源和攻击源的设备名、位置等信息，并将解析结果传送给“黑盒子”安全解析监测平台；接收并转发“黑盒子”安全解析监测平台的扫频、屏蔽或注销指令给中心服务器或节点服务器；

[0045] “黑盒子”安全解析监测平台：通过关键字和图片匹配或人工智能关键字和图片学习算法判断分流阻断设备解析后的用户或物联网终端上行指令和数据、应用平台的下行指令和数据是否非法；若非法，通过分流阻断设备下发屏蔽或注销指令给中心服务器或节点服务器，将禁止指令和数据传输，严重者可将用户和物联网终端在覆盖网络中屏蔽或注销，防止二次网络侵害；呈现分流阻断设备解析后的非法源和攻击源的设备名、位置等信息，方便安全管理部门定点清除；

[0046] 全频段扫描设备：在电力、运营商及其他政企事业单位的重点区域，定时或实时的扫描和定位区域内的所有发射源，定位非法源或攻击源。

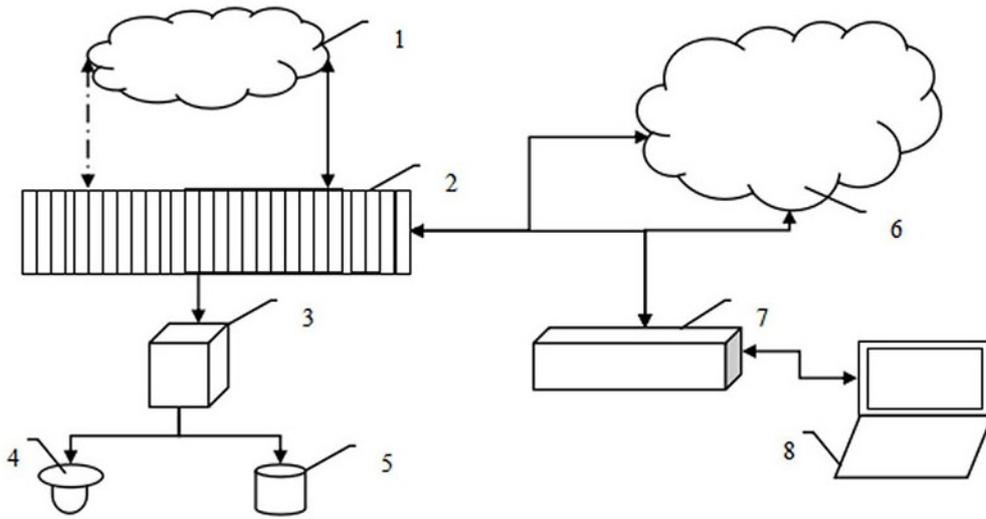


图1

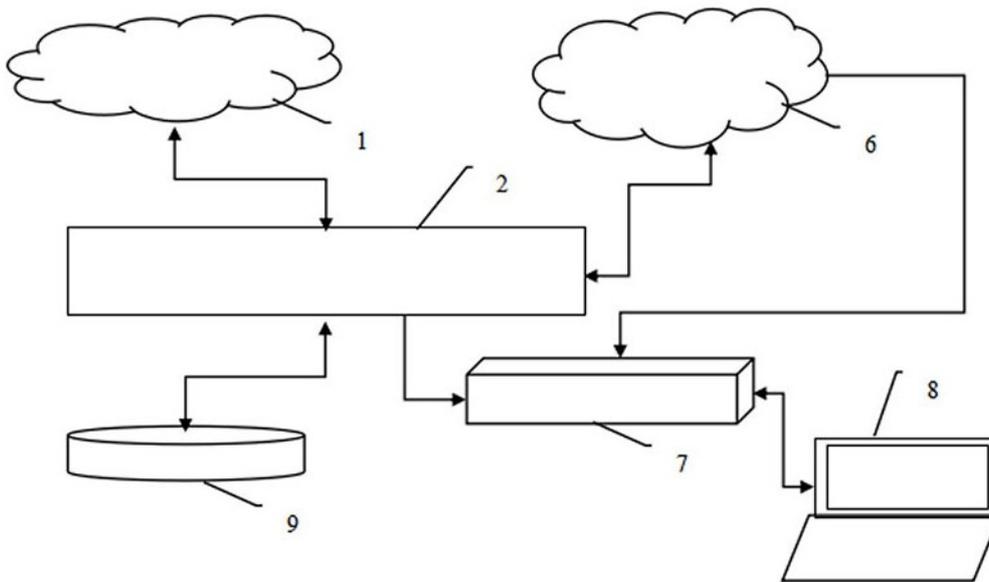


图2