科睿特物联网云平台方案

版本管理

序号	版本号	更改内容
1	V0.1	初始版本
2	V0.2	细化对接协议部分，增加数据加密章节，增加版本管理
3		
4		
5		
6		
7		

目录

1.简介

物联网是当前最具发展潜力的技术潮流，到 2020 年全球将有 200 亿—2000 亿物联网设备(Gartner 预测 260 亿，ABI 预测 300 亿，Oracle 预测 500 亿，Intel 预测 2000 亿)。管理众多的联网设备产生的（动态）数据，相比管理传统档案（静态）数据要复杂很多 —— 最重要的难点是“数据量”大幅提升和“处理实时性”要求显著加强。

- **数据量**：数据量提升包含数据总量和数据产生速度两个方面。物联网应用系统演化过程中，传感器数量不断增多；数据采样频率不断提升；数据积累时间也越来越久，因此产生的数据量非常大（动即十亿、百亿、千亿存储规模），而且数据产生速度也非常快（动即每秒十万、百万纪录）。
- **实时性**：传感器时序数据很多时候用于异常预警、趋势预测等目的，要求能根据数据立刻做出反应。因此数据必须能实时查询、实时分析。

数据量变和实时性要求提升的大前提下，面向于 IOT 的数据库朴素需求细化：

读写特性

- 写操作多于读操作，但读写都要求高速
- 追加为主，但应允许少量更新操作
- 顺序追加为主，但应允许乱序入库
- 可按时间段删除记录，但应允许删除给定纪录
- 支持（优化）给定时间段查询，允许给定字段的精确、模糊、前缀等查询
- 读写并发要求较高，尤其读并发
- 海量存储支持（T - P 级别）

实时性

数据入库即可用（ingest realtime），即任意数据入（input）库后就可立即被第三方应用使用数据 Adhoc 查询 / 分析。

检索和分析特性

- 支持过滤投影
- 支持聚合分析
- 支持关联分析（Join 分析）
- 支持数据挖掘

高可扩展性

- 可按需在线水平扩展

高可用性

- 7*24 小时在线

2.物联网云平台系统架构

物联网云平台系统架构主要包含四大组件：

- 设备接入
- 设备管理
- 设备数据存储与解析
- 规则引擎

2.1 设备接入

物接入（IoT Hub）是一个全托管的云服务，帮助建立设备与云端之间安全可靠的双向连接，以支撑海量设备的数据收集、监控、故障预测等各种物联网场景。

设备接入功能：

- 安全可靠的双向连接
- 认证与授权
- 支持主流物联网协议
- 设备影子

2.1.1 安全可靠的双向连接

物接入服务是全托管的服务，用户可以快速创建物联网服务的实例并安全可靠地连接设备与云端并而不用为运维操心。

提供不同网络的设备接入方案，例如 2/3/4G、NB-IoT、LoRa 等，解决企业异构网络设备接入管理的痛点

2.1.2 认证与授权

提供设备级别的认证，以及基于策略的授权，允许控制设备对特定主题的读写等权限，保障物联网应用的安全。

提供一机一密的设备认证机制，降低设备被攻破的安全风险。

提供设备权限管理机制，保障设备与云端安全通信。

2.1.3 支持主流物联网协议

需要支持 MQTT,COAP,HTTP 等物联网协议，以支持不同的物联网设备。

MQTT 是标准物联网协议，用户可以使用丰富的 MQTT 客户端，使用熟悉的编程语言以及设备平台开发物联网项目。

Coap（Constrained Application Protocol）是一种在物联网世界的类 web 协议，它的详细规范定义在 RFC 7252。COAP 名字翻译来就是“受限应用协议”，顾名思义，使用在资源受限的物联网设备上。物联网设备的 RAM，ROM 都通常非常小，运行 TCP 和 HTTP 是不可以接受的。

2.1.4 设备影子

设备在云端的影子，实时反应设备的当前状态，实现监控、告警、可视化及设备反控等场景。

提供设备影子缓存机制，将设备与应用解耦，解决在无线网络不稳定情况下的通信不可靠痛点。

平台应提供虚拟设备，使用虚拟设备可以模拟实际设备发送数据到云端，亦可以虚拟设备命令发送到物联网设备，方便开发人员的调试与测试。

2.2 设备管理

物联网设备管理提供方便快捷的设备管理能力，在海量设备中快速检索到指定设备，您可以定义设备的属性、事件、服务，基于定义的物模型对设备进行远程调试、远程监控、远程维护等操作。

提供设备和网关的注册、在线离线状态、数据上报、控制设备、禁用删除等基础设备管理功能。

其功能应包含以下模块：

- 设备注册

  可以自定义设备唯一标识 ID 进行单个或者批量注册需要连接的设备

- 设备产品分组

  可以为某些设备创建分组，基于不同产品进行分组管理搜索

- 设备标签

  可以为设备创建标签，定义设备编号并且可以基于标签搜索管理您的设备

  可以为设备创建设备拥有人，设备地址信息，设备铺设日期，设备详情等基础信息选项，丰富设备信息。

- 设备状态

  可以实时从平台获取设备设备的状态变更信息，例如设备的上下线

- 设备数据采集

  可以基于物模型上报设备数据到云端，并且会帮您将设备物模型数据结构化存储下来，您可以随时查询设备历史数据

- 设备禁用删除

  可以对可疑设备进行远程禁用或者删除，避免可疑设备造成不必要的损失

2.3 设备数据存储与解析

云平台应具备设备数据的分类存储与解析功能，对设备端上传的数据进行在线监控与存储，支持 SQL 等大数据分析平台，必要时能够进行数据可视化图表管理应用。其数据存储应存储副本，采取分布式部署保证数据的存储可靠性。提供设备全链路日志监控，实时知晓设备当前状态，监控设备并排除问题。

远程控制能力，对单个设备或者海量设备下发指令控制。

提供固件升级能力，对大规模设备进行远程升级。

2.4 规则引擎

规则引擎帮助用户灵活地转发和处理设备消息，用户可通过 SQL 的形式设定规则，对消息数据筛选、变型、转发，根据不同场景将数据无缝转发至不同的数据目的地，如时序数据库、物接入主题、机器学习、流式处理、对象存储和关系型存储等。

支持 MQTT,COAP,MODBUS 等终端设备协议解析能力，能对设备原始数据进行数据解析与可视化应用。

提供开放标准的 API，可通过调用 API 实现控制台操作，方便第三方应用快速集成云端服务。

3.设备接入协议

3.1 自定义接入协议

此协议用于设备与服务器通讯，通讯基于 TCP 链接实现，采用 JSON 数据格式进行数据交互,其设备认证采用密钥进行认证。

云平台应提供服务器 IP 地址及域名 ,端口号用于设备连接。例如 :yuapi.xinyuegogo.com ,40000。

其设备接入流程如下：

设备登录→设备鉴权→设备数据接收→设备心跳维持→设备上下线管理。

3.1.1 设备登录指令

设备发送：

```
{
"CMD":01,
"ID":"865933034485942",
"SIM":"898607B9191791469403",
"KEY":"123456abcdefg"
"HW":"V0001",
"FW":"V0001",
}
```

云台回复：

```
{
"CMD":01,
"UTC":"1554102064",
"REPLY":1,
}
```

"CMD":用于识别设备命令，其命令标识从 01~99 代表不同的设备命令。其标识格式见下表 3.1。

命令区域	命 令 符	命令含义	备注
01-10	01	设备登录指令，用于设备登录鉴权	02~10 备用，为设备登录类命令
	02	待定	
11-80	11	设备心跳，用于设备心跳发送数据	12~80 备用，为设备心跳传输数据类命令
	12	待定	
81-90	81	设备升级指令，指示设备升级开始	83~90 备用，为设备升级类命令
	82	设备升级数据包，用于发送设备升级数据包	
91-99	91	设备复位指令，将设备复位	92~99 备用，为设备控制类命令
	92	待定	

表 3.1　设备命令符含义表

"ID":设备唯一标识码，为全球唯一标识码，其一般由设备端的 NB-IOT、2G、4G 模组 IMEI 构成，用于标识唯一设备。

其由数字或字母组合而成，可以为纯数字编码或纯字母编码，亦可以由两者组合而成。

其数据长度一般为 15 位，但不限于 15 位，可低于或者高于 15 位，但长度不超过 50 位。

"SIM":设备使用无线通讯时使用到的 SIM 卡号，其由 20 位数字或者字母组成，为全球唯一标识码。

"KEY":设备认证秘钥,由云平台采用 MD5 或者 Password Hashing 加密算法生成（具体加密方式由云平台开发人员决定，但生成的密钥长度应尽量不超过 50 字节，以节省物端的数据流量费用），此密钥应与设备唯一标识码 ID 相关联，平台收到设备登录命令应对设备密钥鉴权，确认其合法性。防止非法设备入侵。

"HW":设备硬件版本号，方便云平台管理，为设备提供升级服务。

"FW":设备软件版本号，方便云平台管理，为设备提供升级服务。

"UTC":北京时间当前 UNIX 时间戳

"REPLY"：回复 1 表示登录 OK,回复 0 表示登录失败，回复 2 表示设备密钥错误。

3.1.2 其它指令

设备端心跳指令：

```
{
"CMD":11,
"ID":"865933034485942",
"LIGHT":1,
"LOCK":1,
"ORDER_SN":"13212341451642142542424333",
"DATA":"13212341451642142542424333",
}
```

云端回复：

心跳类数据，云端无需回复。设备连线后服务器定时检查心跳包，如 5 分钟无对应心跳包则主动把设备连接踢掉。

云端收到其它指令时，只需要对设备"ID"部分进行解析，将对应的数据存储到对应设备影子。

3.2 MQTT 接入协议

暂无

3.3 COAP 接入协议

暂无

3.4 数据加密

3.4.1 TCP 通道

目前采用此种方式，采用 TCP 链接方式，数据本身不加密，安全级别低。

3.4.2 TCP 通道+对称加密

采用 TCP 链接方式，数据本身采用设备密钥做对称加密。

协议待定

3.4.3 TCP 通道+TLS 协议

采用 TCP 链接方式，数据采用 TLS 协议加密。

协议待定