

文章编号: 1673-8411(2019)03-0106-04

## 基于 OAuth2.0 协议的气象数据共享接口的设计

孙伟忠, 吴贵义, 胡鹏, 黄华栋

(广州市突发事件预警信息发布中心, 广州 511430)

**摘要:** 针对气象数据共享服务中存在的安全问题, 提出基于 oAuth2.0 协议的数据共享方法, 给出了接口的设计和实现过程, 并分析总结了 oAuth2.0 协议在气象数据共享中的优势, 为进一步开展气象数据服务提供更加安全高效的技术支撑。

**关键词:** OAuth2.0; 气象数据共享; 开放授权; REST API

中图分类号: DH

文献标识码: A

## Design of Meteorological Data Sharing Interface Based on OAuth2.0 Protocol

Sun Weizhong, Wu Guiyi, Hu Peng, Huang Huadong

(Guangzhou Emergency Warning Information Release Center, Guangzhou Guangdong 511430)

**Abstract:** Aiming at the security problems in meteorological data sharing service, this paper proposes a data sharing method based on OAuth2.0 protocol, gives the design and implementation process of the interface, and summarizes the advantages of OAuth2.0 protocol in meteorological data sharing to provide a safer and more efficient technical support for further development of meteorological data services.

**Keywords:** OAuth2.0; meteorological data sharing; open authorization; REST API

近年来, 随着互联网+时代新媒体的不断发展, 社会企业及政府部门对气象数据的需求不断提升, 气象部门围绕“数据好用, 用好数据”的理念, 不断深化跨部门联动的工作, 为多个政府部门及企事业单位提供各种特色的气象服务。如何更安全和高效的提供气象产品, 是气象部门一直在不断探索和优化的问题<sup>[1-4]</sup>。传统基于互联网的气象数据共享服务, 常用WebService接口协议来获取相应的数据, 此时第三方平台会触及到用户的账户信息, 然而这种调取方式存在用户账户信息泄露的风险, 本文提出引用 OAuth2.0 协议来封装气象数据接口, OAuth2.0 协议能够使得用户在调用气象共享平台资源的过程当中, 第三方应用无需触及到用户的账号信息, 只要求用户通过 OAuth2.0 预先授权, 运用 REST API 方式来访问资源, 便可以申请获得用户授权的资源, 从而极大提升了气象数据资源应用的安全性和高效性。

### 1 接口协议及设计思路

#### 1.1 OAuth协议的优劣

当前传统气象数据获取方法<sup>[5-8]</sup>, 需要用户将用户名和密码告诉第三方服务平台(第三方软件开发公司或者应用程序, 以下简称第三方), 由第三方调用接口获取到数据。这种做法存在以下几个问题: (1) 第三方为了后续的服务, 可能会保存用户密码, 一旦第三方被利用, 就会导致用户密码泄露, 以及所有被密码保护的数据泄露, 从而给数据提供方和用户带来了较大安全隐患;

(2) 第三方拥有了获取用户储存在气象共享网所有资料的权限, 用户无法有效限制第三方获得授权的范围和有效期; (3) 用户只有修改密码才能收回赋予第三方的权力, 但是修改密码可能会导致其他所有获得用户授权的第三方调用失效。

OAuth (Open Authorization 的简写) 协议

收稿日期: 2019-01-10

基金项目: 广州市科创委科技计划项目“多气象灾害模型融合及网格化服务技术研究及应用”(项目编号: 201803030014)

作者简介: 孙伟忠(1986-), 男, 工程师, 硕士, 主要从事气象数据信息处理等工作。E-mail: 465183393@qq.com

能够在第三方不涉及用户密匙等信息的情况下, 就可以申请访问该用户的受保护资源<sup>[9]</sup>, 为服务提供者和用户方提供简便的传输服务, 同时由于协议兼容大部分第三方, 因此能够有效解决传统气象数据共享存在的安全问题。

## 1.2 设计思路

本文从气象数据共享服务的安全和高效性出发, 采用基于 OAuth2.0 协议的方式提供结构化气象数据的共享服务。用户、第三方服务平台、气象数据共享平台之间的工作流程主要根据 OAuth2.0 协议标准, 用户首先要在要登录气象数据共享平台注册用户账号, 按照数据共享设置好的规定, 提供如申请人姓名、有效证件等有效信息, 并通过 web 端页面将填报的信息上传, 由气象部门的后台管理员审核通过后, 用户将获得气象数据共享平台分配的用户唯一凭证 (appid) 和唯一凭证密匙 (secret) 等相关信息, 然后调用共享平台授权接口, 获取到全局唯一接口调用凭据 (token), 最后用户通过接口调用凭据 (token) 访问相应的气象共享数据资源。整体数据共享流程图如图 1 所示。

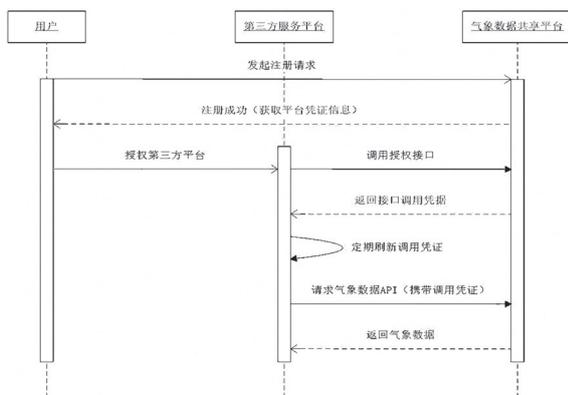


图 1 数据共享流程图

用户授权给第三方后, 第三方通过共享平台分配给用户的凭证 (appid) 和凭证密匙 (secret), 获取接口调用凭据 (token)。由于担心接口调用凭据可能泄露的风险, token 可以设置有效期, 第三方需定时刷新, 如果重复获取将会导致上次获取的接口调用凭据 (token) 失效。第三方获取到接口调用凭据后, 就可以携带接口调用凭据 token 访问该用户权限范围内的气象共享数据。

## 2 接口设计

### 2.1 用户信息注册

用户通过 OAuth2.0 协议访问共享平台, 首先需要获取共享平台信任, 即注册平台账号。注册

账号时需要提供用户邮箱、单位信息、联系人、联系电话、营业执照、身份证信息等相关信息。注册信息提交后, 平台管理员会在一个工作日内对注册信息进行审核, 并通过邮件的方式通知用户审核结果。审核通过后, 用户登录气象共享平台进入个人中心界面获得用户唯一凭证 (appid) 和用户唯一凭证密匙 (secret) 等信息。

用户唯一凭证 (appid) 是通过 UUID 生成的, UUID 含义是通用唯一识别码 (Universally Unique Identifier), 是指在一台机器上生成的数字, 它保证对在同一时空中的所有机器都是唯一的。

用户唯一凭证密匙 (secret) 则是通过全局密匙和 appid, 经过 MD5 加密生成的<sup>[10-11]</sup>, 其算法公式如下:

$$\text{secret} = \text{MD5}(\text{MD5}(\text{key} + \text{appid}). \text{toLowerCase}(:))$$

其中 secret 为用户唯一凭证密匙; MD5 为 MD5 加密函数; key 为共享平台全局密匙; appid 为用户唯一凭证; toLowerCase 为字符串转小写函数。

### 2.2 接口调用凭据

基于 OAuth2.0 协议, 用户在调用气象数据 API 之前, 需通过 OAuth2.0 授权的方式<sup>[12]</sup> 获取接口调用凭据 (token), 接口调用凭据是用户的全局唯一票据, 为了保密用户唯一凭证密匙 (secret), 用户需要一个 token 获取和刷新的中控服务器, 而其他业务逻辑服务器所使用的 token 均来自于该中控服务器, 不应该各自去刷新, 否则会造成 token 覆盖而影响业务, Token 与 RefreshToken 数据传输原理如图 2 所示。

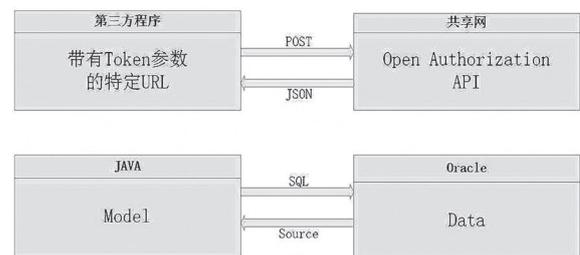


图 2 Token 与 RefreshToken 数据传输原理图

接口调用凭据 (token) 是由用户唯一凭证 (appid) 和用户唯一凭证密匙 (secret) 加密生成的。其中加密的规则比较多, 每个开放平台都可以根据自己的规则, 定义一套加密算法, 本文采用的算法公式如下:

$$\text{token} = \text{MD5}(\text{MD5}(\text{key} + \text{appid} + \text{secret}). \text{toLowerCase}(:))$$

其中 token 为接口调用凭据, key 为共享平台全局密匙; appid 为用户唯一凭证; secret 为用户唯

一凭证密钥；MD5为MD5加密函数；toLowerCase为字符串转小写函数。

### 2.3 数据接口设计

传统的 Web 服务通常使用的是基于 SOAP (简单对象访问协议) 的 WebService, 但伴随着 Web2.0 流行, REST API 逐渐成为了主流 [13]。SOAP 是一种轻量的、简单的、基于 XML 的协议, 它被设计成在 WEB 上交换结构化的和固化的信息。REST (Representational State Transfer 表述性状态转移) 是一种针对网络应用的设计和开发方式, 可以降低开发的复杂性, 提高系统的可伸缩性。由于 REST 面向资源接口设计以及操作抽象简化了开发者的不良设计, 同时也最大限度的利用了 Http 最初的应用协议设计理念, 所以相比较 WebService 而言, REST API 更加的高效且简洁易用。

在数据格式选择上, 由于 XML 解析规则繁多, 经常出现非法字符等问题, 这对追求高开发速度和低开发门槛是个致命伤, 相比较而言, JSON 的可读性比 XML 强, 解析规则简单易用, 并且性能上明显优于 XML [14], 因此气象共享平台在接口设计上采用 REST API 标准 [15], 使用 JSON 数据格式作为数据反馈更方便用户的解析和应用。接口调用请求及数据结果返回如图 3 所示。

http 请求方式: GET  
 http://121.8.227.152/services/SpringWsService/getData?token=TOKEN&interfaceid=GetH  
 aiZhuAwst

参数	是否必须	说明
token	是	调用接口凭证
interfaceid	是	接口 ID

返回说明  
 正确时返回 JSON 数据包:

```
[{"WD3DAYMAXTIME":1139,"WF1ODAYMAX":18,"DDATETIME":"2018-09-20 11:50:00","DAYMINT":270,"OBTID":"G1093","MINT":329,"HOURRF":0,"DAYMAXTIME":1131,"MINRHTIME":31,"DP":227,"DAYMAXI":344,"P":10082,"WD10MAXTIME":47,"T":330,"DAYMINTIME":641,"WD10DAYMAX":209,"PO":null,"MAXRH":57,"MINPTIME":48,"WD10DF":15,"WD10DAYMAXTIME":408,"WD10DD":345,"WD2DD":332,"WD3SMAXTIME":39,"MINTIME":12,"DAYRF":0,"WD2DF":10,"MAXP":10088,"MAXPTIME":1,"MAXT":344,"WD1DF":11,"WD3SMAXDF":32,"WF3DAYMAX":32,"WD1DD":326,"RH":55,"MAXRHTIME":11,"MINRH":49,"WD3DAYMAX":343,"WD3SMAXDD":343,"MINP":10082,"MAXTIME":31,"WD10MAXDF":17,"WD10MAXDD":344}]
```

图 3 接口调用请求及结果反馈图

### 2.4 数据接口配置

由 2.3 章节可知, 气象数据接口是按照 REST API 标准来实现的, 由于气象数据共享平台主要是用户通过气象 API 接口查看共享数据, 所以针对 HTTP API 的标准方法中的四种常用行为 (查看 (select), 创建 (create), 编辑 (edit) 和删除 (delete)), 只需要用到查看 (select) 方法, 即将用户请求直接映射到 HTTP 中 GET (select) 方法。用户通过 API 接口调用气

象共享数据时, 直接在请求地址后加上接口信息、接口参数、接口调用凭证等信息即可。

根据 REST API 接口标准规范, 气象共享平台将每种气象数据资源通过自定义 sql 的方法来实现接口的自动化配置, 平台管理员通过后台操作完成接口标识、接口名称、接口类型、执行 sql、备注等接口信息的配置, 其中执行 sql 以 \$ 通配符的方式, 通过对接口请求参数的解析和匹配, 完成执行 sql 中参数的自动注入, 生产可执行的静态 sql 语句。接口配置效果见图 4 所示。



图 4 接口配置图

## 3 结语

广州市气象局现已在广州市电子政务网部署了基于 OAuth2.0 协议的气象数据服务网, 为各政府部门提供数据接口服务, 目前已经有包括交通、公安、环保、文广局等 14 个政府部门通过了认证注册和数据申请流程, 外部门用户借助第三方开发正常获取了包括气象实况、预报预警等多种气象服务产品, 在有效满足各单位部门对广州气象数据需求的同时, 也避免了将数据共享网的用户账号和密码暴露给第三方开发公司的安全隐患, 提高了数据共享的安全性, 并在接口设计中继承了 REST API 标准的高效性。

气象数据使用安全性是无止境的问题, 随着用户的不断增多, 对共享气象数据接口调取的频次及数据量日益增大, 届时气象共享平台的访问压力将会急剧加大, 加上管理部门或个体开发能力的不足, 可能会导致调用凭证等重要信息的泄露, 所以下一步共享平台还将进一步研究数据接口安全技术和性能提升技术, 如在接口凭证调用时, 加入 IP 白名单过滤等方式的处理。

### 参考文献:

[1] 丁钱美, 俞宙. 现代传媒高效气象服务的新模式 [J]. 气象研究与应用, 2014, 35(3): 122-124

(下转第112页)

为了让仪器使用人员方便区分目前正在测量的是哪个通道,该程序利用了LCD240128液晶显示屏的反白功能。如图6所示,该仪器已经完成⑥号通道数据的采集并将其显示出来。



图6 LCD240128 驱动原理构架图

### 3 结语

18路Pt100温度传感器法取代能够使用220V交流电进行工作,实现自动依次读取8支Pt100温度传感器的温度值并通过LCD240128液晶屏显示的功能。仪器功能齐全,性能优良,界面友好,极大地提高地市级气象部门区域自动气象站校准工作效率及质量,实现校准工作的高效化、模块化、智能化。

下一步计划在仪器上增加一个能与计算机进行通信的接口。同时开发一款能够获取该仪器数据并自动生成校准报告的计算机软件<sup>[7]</sup>。从而进一步减轻地市级气象部门仪器校准人员的工作量,提高他们的校准效率。

#### 参考文献:

- [1] 蒋冬雁,李伟雄,陈平.从计量角度探讨自动气象站观测数据的质量[J].气象研究与应用,2018,39(4):71-73.
- [2] 毛寿兴.自动气象站风速传感器的检定及提高检定精度的方法[J].气象研究与应用,2018,39(3):96-98,123.
- [3] 晏敏,柳鸣.区域自动气象站校准工作的思考和实现[J].气象研究与应用,2018,39(2):86-89.
- [4] 晏敏,柳鸣,刘希林,等.铂电阻温度传感器检定结果的不确定度评定[J].气象研究与应用,2017,38(1):140-143,155.
- [5] 韦庆玲,韩宇龙,卓健,等.Pt100温度传感器检定仪的研发[J].气象研究与应用,2017,38(S1):69-70.
- [6] 侯江生,段利军,韦继忠.区域自动气象站校准实验室校准方法技巧[J].气象研究与应用,2016,37(2):81-82.
- [7] 梁宏光.市级仪器校准检定工作现状分析与未来设想[J].气象研究与应用,2016,37(2):91-93.

(上接第108页)

- [2] 吴风波,肖海平,成永勤.新形势下发展基础公共气象服务的几点思考[J].气象研究与应用,2012,33(1):101-104
- [3] 赵卓宁,敬枫蓉,肖天贵.国内气象服务研究中的公共气象服务主题分析[J].成都信息工程学院学报,2012,27(1):112-119
- [4] 陈静,梁宏升.自媒体时代的气象服务[J].广东气象,2013,35(6):52-55
- [5] 吴国锐,李友,莫伟元.肇庆远程气象服务通道的设计与制作[J].广东气象,2009,31(4):49-50
- [6] 李涛,王丽玫,张薇.广州气象科学数据共享平台建设[J].气象研究与应用,2010,31(1):63-67
- [7] 王刚,孙周军,吴映,等.基于IDEA数据平台的海珠城市生态气象综合系统建设[J].广东气象,2016,38(2):77-78
- [8] 梅清银.SSH框架在气象数据共享中的应用[J].科技情报开发与经济,2009,19(29):79-81
- [9] 时子庆.基于OAuth2.0的认证授权技术[J].计算机系统应用,2012,21(3):260-264
- [10] 周小红,周建秋.MD5加密算法在注册及登录验证模块中的应用[J].工业控制计算机,2015,28(11):18-119
- [11] 黄志,高钰杰,唐兵兵.气象数字档案检索平台MD5加密技术应用[J].气象科技,2015,43(2):232-235
- [12] 刘大红,刘明.第三方应用与开放平台OAuth认证互连技术研究[J].电脑知识与技术,2012,8(22):5367-5369
- [13] 胡君,程京,王敏.基于XML的REST API设计与实现[J].软件时空,2010,26(3):77-80
- [14] 高静,段会川.JOSN数据传输效率研究[J].计算机工程与设计,2011,32(7):2267-2270
- [15] 王效武,刘英.互联网信息发布系统设计[J].通信技术,2013,46(8):166-168