

工程建设项目审批系统 API 网关设计

方钟亮¹

FANG Zhongliang

摘要

随着数字政府建设深入推进,跨部门、跨层级业务信息系统间协同交互显著增强。随着系统规模不断扩大,传统单体架构模式下的接口集成方式出现局限性,包括数据泄露、维护成本高、无法统一管理。围绕工程建设项目审批系统建设,文章提出通过部署 API 网关来实现 API 接口调用的鉴权服务、加密传输、流量管理和日志管理,对日志数据分析和基于 APIfox 软件对原始接口模拟测试来评估 API 网关开销。通过 API 网关部署可以加强系统间对接的安全性和接口调用的统一管理,为数字政府建设工作提供了一定的参考经验。

关键词

工程建设项目审批; API 网关; 鉴权服务; 加密传输; 日志管理

doi: 10.3969/j.issn.1672-9528.2025.03.010

0 引言

近年来,政务服务管理部门不断建设完善各类信息系统,在审批服务领域进行了多项改革,包括工程建设审批制度改革、一件事一次办、电子证照互认共享等^[1-2]。

不同的系统所面向的业务场景、技术架构和标准各有区别。传统系统建设为单体模式^[3],系统间交互基于 API 接口的点对点通信,随着需求的增多和业务的扩展,往往伴随数据泄露等安全风险,且维护成本高,并缺少有效的接口调用管理功能。

《关于加强数字政府建设的指导意见》中,明确提出加强系统对接整合、确保数据安全、促进跨业务协同是数字政府建设的目标之一^[4]。本文面向工程建设项目审批管理系统,在服务多方业务功能对接中,将 API 网关和系统建设相结合,实现安全保障和有效管控,促进可靠审批数据应用和功能扩展。

1 建设背景

根据改革要求,江苏省昆山市积极构建工程建设项目审批管理系统(简称工改系统),有效推进审批流程优化与政务服务数字化转型。该系统面向工程建设领域,服务企业工程项目报建,涵盖从立项用地规划到项目竣工验收各阶段的全流程审批功能^[5],是数据汇聚和审批业务协同的枢纽平台。但在具体工作中第三方应用需要对接工改系统,涉及政务服务网旗舰店专区、市民服务 APP、省级条线系统、纪检监察管理、部门个性化业务、数据底座公共基础能力等。

传统的单模块点对点 API 对接,面临如下问题:

(1) 安全问题凸显。针对 API 接口攻击,包括身份认证、未授权访问、数据泄露、注入问题等^[6],严重影响政务信息系统安全。

(2) 维护成本高。以事件为驱动建设 API,各类接口开发、测试和维护呈“碎片化”现象。

(3) 缺少管理功能。无法对 API 调用、流量监控、日志审计等方面,形成统一的管理和数据分析功能。

本文以昆山市工改系统为例,探讨了 API 网关在系统设计中的应用,实现客户端系统在接口调用时的鉴权管理、加密传输、日志分析等功能,加强了审批数据共享的安全性和应用拓展规范化管理。

2 总体设计

2.1 设计思路

(1) 授权模式:目前网关授权模式主要有 OAuth2.0 和 APIKeys 两种方式^[7-8]。OAuth2.0 是一套完备的框架协议,安全性较高,但系统部署实现复杂,使用中存在用户发起认证请求操作的环节,普遍应用在互联网环境的 OpenAPI 调用,如谷歌、脸书等登录服务。APIKeys 授权应用在可信任网络环境,同受信任应用对接,部署实施相对简单,使用中无须用户进行认证操作,只需通过客户端密钥保存、定期更新和 IP 绑定等措施来确保安全,主要面向企业级 API 管理,如阿里云、腾讯云等环境。从应用场景分析,工改系统主要功能是处理审批业务,并提供各类审批服务政务类应用接入,服务器部署在电子政务网和政务云。系统间调用通过服务器之间通信实现,且需要业务管理部门协商确认,因此选择 APIKeys 授权模式开展服务鉴权。

1. 苏州市公共资源交易中心昆山分中心 江苏昆山 215300

(2) 数据加密: 在通过授权接入“工改”平台后, 为确保数据传输安全, 在客户端和 API 网关之间的数据传输以双向加解密和数字签名作为保障, 主要采用 SM2 椭圆曲线公钥算法。

(3) 日志管理: API 接口产生的各类访问日志需要进行存储管理, 用于后续分析监管。Elasticsearch 是在 Apache Lucene 基础上一个分布式实时文档存储库, 支持 RESTful API 的搜索引擎^[9-10]。工改平台的日志管理利用 Elasticsearch 进行部署。

2.2 总体架构

系统的设计包括后端服务、API 网关、前端系统对接三部分。其中, 后端服务部分是平台的支撑, 涉及基础设施、数据管理和工改业务, 主要面向审批人员实现工程建设项目行政审批、数据汇聚分析等功能; 中间层是 API 网关, 连接前端系统对接和后端服务, 提供包括接口审计、接口鉴权、数据加解密、限流处理、熔断处理、监控告警等功能; 前端系统对接部分主要面向报建单位、相关业务监管部门建设各类服务应用, 统一通过 API 网关来访问后端服务, 实现数据的共享应用, 系统的总体设计架构如图 1 所示。

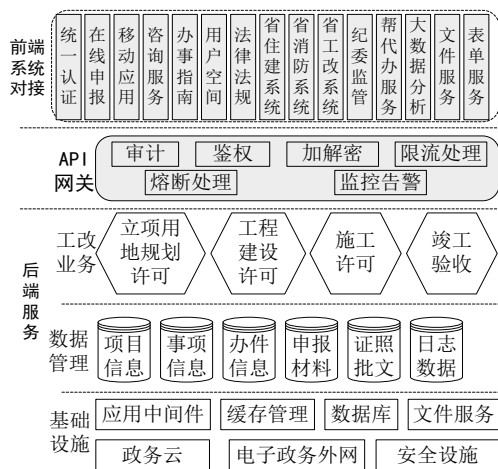


图 1 总体架构

2.3 业务流程

API 网关在应用过程中主要涉及网关应用配置和前端系统调用两部分。对于提供外接服务的后端应用, 首先需要在 API 网关进行注册, 登记服务名称、生成标识、创建网关密钥对和数据密钥对, 分别应用于前端系统调用时的鉴权和数据传输服务, 并提供更新替换功能。在注册同时需完成接口的路径配置, 用于接口地址重定向后, 可拼接生成新访问地址。其次是接口设计规范导入, 在此通过 Swagger 规范^[11], 支持 API 对接和 JSON 文件导入方式, 完成后端应用接口规范在网关同步。最后是网关接口功能配置, 包括鉴权、加密、调试、流量和日志统计等功能, 配置流程如图 2 所示。

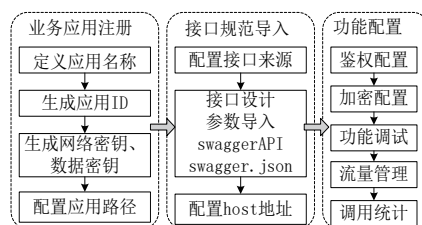


图 2 网关配置

调用 API 网关的流程, 首先, 基于网关密钥, 对 API 进行鉴权申请, 获取票据 ticket。然后, 应用数据密钥加密入参数信息, 同 ticket 一起发送给 API 网关, 网关审核后, 解密请求参数, 路由至后端服务接口, 对获取的数据加密后返回客户端, 客户端对得到的密文再进行解密展示, 网关处理日志将存储到 Elasticsearch 进行统一管理。系统的调用流程如图 3 所示。

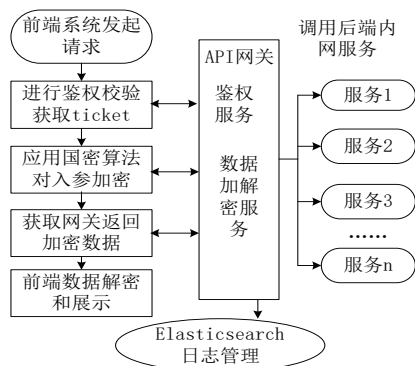


图 3 网关调用流程

3 主要功能设计

3.1 接口鉴权

API 网关需对接口调用进行认证管理, 按客户端分配认证权限, 鉴权过程基于国密算法开展签名和验证, 流程如图 4 所示。

(1) 网关应用注册时, 创建对应客户端标识 ID 和网关密钥对, 并分配至对应客户端系统进行保存, 密钥对保持定期更新。

(2) 客户端系统在发起网关接口调用请求前, 需将自己的请求参数 param 用 SM2 进行签名, 会同客户端标识和参数一起发送给 API 网关。

(3) API 网关进行对客户端标识 ID 和签名进行验证, 通过用 SM3 对参数进行 hash 处理, 再通过字符串方式拼接客户端 ID 和请求参数, 用 SM2 方式进行加密形成票据 ticket, 返回客户端系统, 同时在缓存数据库中记录票据生成时间戳 timestamp。

ticket=SM2(STR(clientId+', '+SM3(param)+'+', '+QueryType), PublicKey)

(4) 客户端系统获取票据后，再次发送请求参数，并将票据一起发送给 API 网关。后者对票据进行验证，先是判断时间戳有效期，系统设置为 2 min，超期则访问无效，未超期则解码票据，对本次提交参数进行 SM3 验证比对，验证成功则放行调用，否则调用失败。

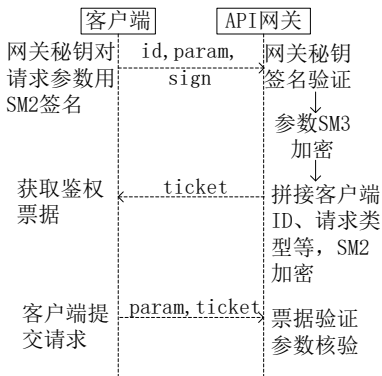


图 4 鉴权流程

3.2 安全传输

为保障数据安全，在客户端系统和 API 网关之前建设了加密传输功能。在应用接口注册配置过程中，API 网关为每个接口基于 SM2 算法创建两套密钥，定义为客户端密钥 (pubKey_cli, priKey_cli) 和服务端密钥 (pubKey_srv, priKey_srv)，并对前端系统进行提前分配告知。在数据传输中，客户端系统保存客户端私钥和服务端公钥，API 网关则保存客户端公钥和服务端私钥，通过使用不同密钥对进行加密和签名来提升数据传输的安全性。传输过程分为客户端系统请求发送和 API 网关响应值返回两个阶段，如图 5 所示。

(1) 客户端请求传输：客户端系统在需向 API 网关发送请求过程中，首先利用客户端密钥的私钥 priKey_cli 对请求参数 param 进行签名，形成签名值 c_sign，再用服务端密钥的公钥 pubKey_srv 对请求参数和签名值一起进行加密，形成加密字符串 request 发送 API 网关；API 网关在接收到客户端发送过来的请求信息，先利用服务端密钥私钥 priKey_srv 进行解密，获取请求参数 param 和签名值 c_sign，再用客户端公钥 pubKey_cli 对参数和签名进行验证。通过验证后，再将请求参数路由至后端接口处理。

(2) API 网关响应传输：后端系统在完成前端请求处理后形成返回值，由 API 网关加密处理后发送客户端系统，首先利用服务端私钥 priKey_srv 对返回值 value 进行签名，形成签名值 s_sign，再用客户端公钥 pubKey_cli 对签名值和返回值一起进行加密，形成返回字符串 return 发送客户端系统；客户端系统对获取的返回值先利用客户端私钥 priKey_cli 对返回字符串解密，获取返回值 value 和服务端签名 s_sign，再用服务端公钥 pubKey_srv 对两者进行签名验证，验证通过后

由系统展示。

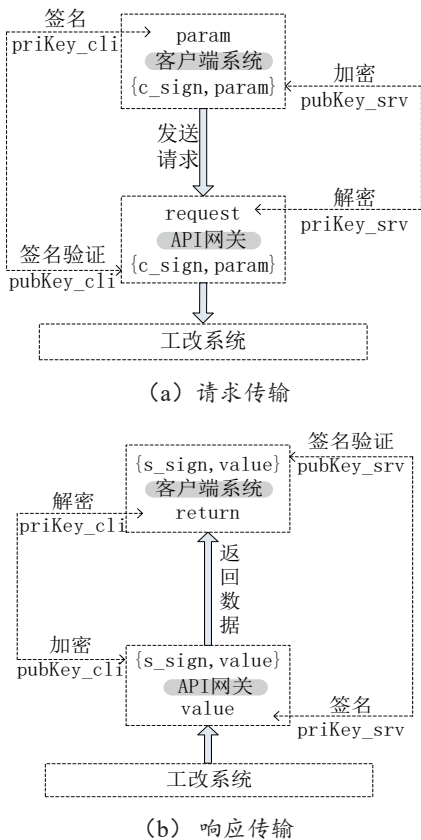


图 5 安全传输流程

3.3 流量管理

API 网关对于接口调用流量管理，包括了限流处理、熔断处理和监控告警：

(1) 限流处理，为避免工改系统 API 接口服务的过高负载，防止接口被过度调用，系统提供限流设置，可限定对一个客户端系统在规定时间内，调用某个特定 API 服务的次数，实际工作中根据 API 接口使用特性进行分别设置，超过调用次数则提示告警信息并限制访问；

(2) 熔断处理，在 API 接口服务处于繁忙状态，对接口调用连续出现超时，为防止后续的请求调用给系统增加负载，此时网关系统会启动熔断机制，比如请求超时 5 次以后，熔断 3 min，在 3 min 内请求该接口都会提示：“接口暂时无法访问，请稍后再试”；

(3) 监控告警，为使接口服务在发生异常时，能够及时告知技术人员，API 网关系统开展钉钉 APP 对接，将异常信息实时推送给技术人员，后者可以及时进行故障排查。

3.4 日志管理

3.4.1 网关日志索引

《互联网政务应用安全管理规定》要求网络系统日志保

留不少于 1 年^[12]。API 网关负责将请求信息和响应信息中的关键数据以日志文件的形进行保存,日志以 JSON 文件格式编制,具备一定的扩展性和通用性。一次请求和对应的反馈响应数据组成一个独立的日志文件,存储在 Elasticsearch 搜索引擎中^[13],日志索引主要数据格式设计如下:

```
{
  "clientAddress": "客户端地址",
  "clientId": "客户端编号",
  "clientName": "客户端名称",
  "requestPath": "请求路径",
  "requestTime": "请求时间",
  "routeAddress": "路由目标地址",
  "routeName": "调用资源名称",
  "method": "请求方式",
  "projectCode": "工程项目代码",
  "requestBody": "请求 body 内容",
  "requestParam": "请求参数",
  "encryptRequestBody": "请求 body 密文",
  "encryptRequestParam": "请求参数密文",
  "requestHeader": "请求头"
  {
    "host": "服务端主机地址",
    "ticket": "票据",
    "sign": "签名",
  }
  "encryptResponseBody": "响应密文",
  "responseBody": "响应明文",
  "handlerSituation": "服务器状态",
  "responseContentType": "响应类型",
  "responseStatus": "响应状态",
  "responseTime": "响应时间"
}
```

3.4.2 网关日志审计

日志审计功能主要对接口调用产生的日志,通过 API 网关读取 Elasticsearch 引擎数据,开展综合查询,并提供日志全部索引字段详情信息的展示。为应对多种查询场景需求,日志审计功能提供多方面的组合查询:

(1) 基础查询,包括按时间段、接口资源路径、客户端系统名称查询。

(2) 状态选择,包括服务响应状态:请求成功、重定向、客户端错误、服务端错误;请求方式:GET、POST、OPTION、PUT、DELETE;网关请求失败类型:路由失败、身份认证失败、请求缓存失败、请求限流、服务调用失败。

(3) 数据更新,对日志审计查询结果可设定一个更新时间,默认 5 min 进行自动更新。

3.4.3 动态数据监控

通过实时检索 Elasticsearch 引擎日志数据,API 网关系统提供了多个维度的动态数据监控功能,通过图表方式予以展示,包括折线图、柱状图、条形图,可提供直观性能指标。监控功能包含实时流量、日访问量、接口资源访问量、项目访问量、接口异常率和 IP 访问量,功能示意如图 6 所示。实时流量监控是以分钟为间隔,动态统计每分钟网关被访问次数,页面每分钟自动更新一次,统计近 10 min 数据,并以颜色区分不同数值范围,图表实例如图 7 所示;日访问量则是统计每日网关访问总次数,统计近一周数据;IP 访问量统计指定时间段内客户端系统 IP 地址的访问次数,默认为一天;接口访问量,则是统计资源接口被访问的次数;项目访问量,是针对 API 网关除提供工改系统接口外,同时提供其他项目的接口服务,此时以项目为单位,统计被调用次数;接口异常率,是对接口调用时发生故障调用失败的比率统计。

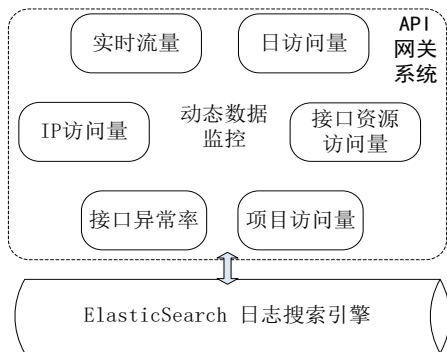


图 6 动态数据监控功能

实时流量 (分钟间隔)

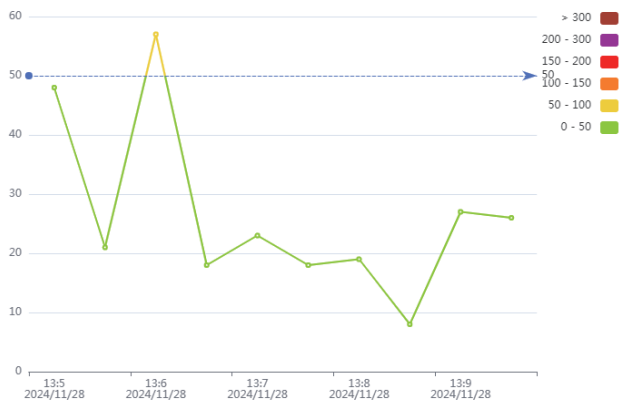


图 7 实施流量监控图表

4 性能测试

4.1 测试环境

本文利用电脑 PC 端作为测试客户端, CPU 为 Intel i5-

4570 320 GHz，内存 16 GB，安装操作系统 Windows7 x64、数据库 MySQL 5.7.44-log 和管理工具 Navicat Premium 15、编程语言 Python3.8，API 接口测试工具为 Apifox2.6.31。

4.2 数据集和测试方法

本文对 Elasticsearch 搜索引擎所记录的一个月的日志作为数据集进行统计，分析接口资源调取量前 7 个接口。分析过程中，需要对日志中的属性字段进行计算，为便于实时利用 MySQL 作为辅助数据库。通过 Elasticsearch 的字段检索和共享导出功能，将请求时间 reqesTime、响应时间 responseTime、接口资源名称 routeName 和请求路线 requestPath 等字段信息导出成 csv 文件。利用 Python 读取 csv 文件中的数据，通过参数类型转换将日志读取的文本类型时间转换成 datetime 日期型，再用日期运算来获得每次接口调用的时间开销，并将所有的参数存储至 MySQL 数据库，通过 SQL 的去重聚类和平均值计算，获取各接口的调用次数和平均总时间耗，如表 1 所示。

表 1 2024-11 月接口调用前 7 名

序号	接口资源	调用 / 次	总时耗 /ms
1	获取上传材料	288 183	209
2	获取字典列表	192 360	48
3	获取验证码	21 848	139
4	获取企业项目	20 991	149
5	我的空间首页	18 256	55
6	办事指南清单	15 613	126
7	获取事项列表	13 707	396

通过表 1 可知，计算接口总时耗是包括 API 网关和工改系统原始接口处理开销，需要分析 API 网关开销对接口调用的整体开销的影响。本文利用 Apifox 软件模拟客户端对系统原始接口调用，计算在相同参数环境下原始接口的响应开销。主要环节：

- (1) 在已有的网关日志中根据接口资源分类，随机选择访问日志，提取请求 IP、请求路径、提交参数等数据。
- (2) 在 Apifox 中配置每个测试接口的原子操作，根据日志中提取数据，拼接原始接口调用地址和请求参数。
- (3) 利用 Apifox 平台构建自动化测试场景，设置循环数、选定测试接口、休眠时间、用户数和并发数，本文的循环数设置是参照日访问量，由表 1 中的接口月访问量计算而得，循环休眠时间设定为 3 s，模拟单用户访问，未设置并发数。
- (4) 运行测试程序，获取测试结果报告，测试流程如

图 8 所示。

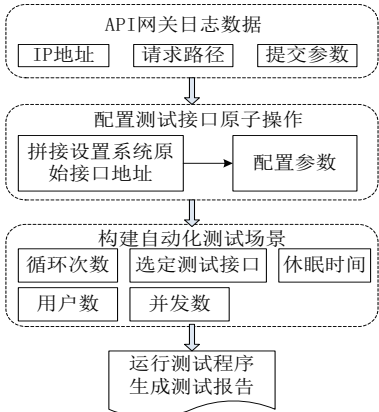


图 8 测试流程

4.3 测试结果

根据测试报告，获得每个接口资源在不经 API 网关处理时，直接被调用的平均响应时耗，用表 1 中的平均总时耗与之求差值，来估算 API 网关在处理接口调用中自身的时间开销，结果如图 9 所示。从结果分析，网关对各接口调用的处理开销最大在 123 ms，7 类接口资源的网关处理平均开销约 57 ms。从实验结果可以看出，在部署 API 网关后接口调用会产生一定时间开销，但这部分时间开销值较小，在实际运行中并不会影响业务系统操作体验，属于可接受范围。

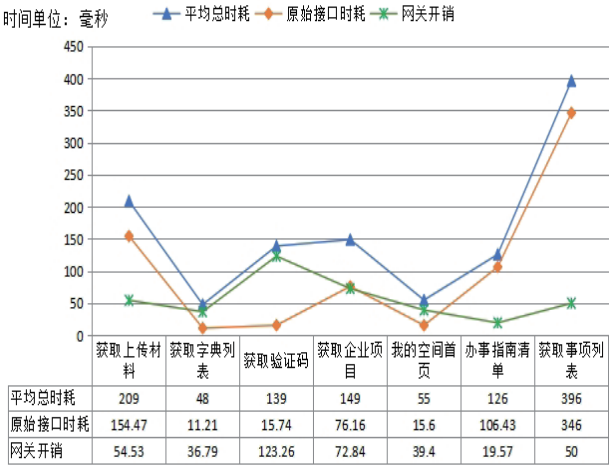


图 9 测试结果

5 结语

本文介绍了在工程建设项目审批系统建设过程中，通过部署 API 网关开展系统对接。系统应用了 APIKeys 授权模式，通过国密算法实现了加密传输，开发了流量管理功能，并基于 Elasticsearch 引擎开展了日志管理，实现了日志审计和监控。通过模拟客户端系统对原始接口的调用实验，评估了部署 API 网关后的开销对系统使用的影响在可接受范围。API 网关的应用为审批系统同第三方应用对接提供了安全保障和

统一规范的监控管理机制。下一步,API 网关将有序拓展应用场景,如一件事系统、电子证照共享平台、不动产登记等各类政务服务系统,将统一基于 API 网关提供接口调用服务,促进跨系统间安全有效的接口调用。

参考文献:

[1] 国务院关于进一步优化政务服务提升行政效能推动“高效办成一件事”的指导意见[J]. 中华人民共和国国务院公报, 2024(3): 15-22.

[2] 国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见[J]. 中华人民共和国国务院公报, 2022(7): 31-35.

[3] 卜意磊. 微服务架构应用于市场监管应用支撑中心的研究[J]. 信息系统工程, 2020(12):72-73.

[4] 国务院关于加强数字政府建设的指导意见[J]. 中华人民共和国国务院公报, 2022(19):12-20.

[5] 方钟亮. 工程建设项目审批监管系统设计[J]. 现代信息技术, 2024, 8(22):151-155.

[6] 何平, 刘晓毅, 王进, 等. 容器云的 API 安全技术研究[J]. 保密科学技术, 2022(7):41-46.

(上接第 44 页)

5 结语

本文设计并实现了一种基于 PYNQ 环境的轻量化实时目标检测技术,开展了 YOLOv5n 目标检测算法研究及适应 FPGA 部署的模型优化,完成 PYNQ 环境下的软硬件协同设计,并在 ZCU104 开发板上完成了系统验证。结果表明,本方案能够实现轻量化深度学习目标检测算法的快速部署与验证,具有良好的检测精度与实时性,满足边缘端设备的低功耗需求,在低成本实时目标检测领域具有较高的应用价值。

参考文献:

[1] 卢宏涛,张秦川. 深度卷积神经网络在计算机视觉中的应用研究综述[J]. 数据采集与处理, 2016,31(1):1-17.

[2] 李柯泉,陈燕,刘佳晨,等. 基于深度学习的目标检测算法综述[J]. 计算机工程, 2022,48(7):1-12.

[3] 陈超,齐峰. 卷积神经网络的发展及其在计算机视觉领域中的应用综述[J]. 计算机科学, 2019,46(3):63-73.

[4] 陈科圻,朱志亮,邓小明,等. 多尺度目标检测的深度学习研究综述[J]. 软件学报, 2021,32(4):1201-1227.

[7] 普拉巴斯. 西里瓦德纳. API 安全进阶基于 OAuth2.0 框架: 原书第 2 版[M]. 李伟,译. 北京:机械工业出版社, 2022.

[8] 冯骐,沈富可. 高校能力开放平台中的 API 网关设计与实现[J]. 中国教育信息化, 2021(3):61-66.

[9] 崔庆才. Python3 网络爬虫开发实战: 第 2 版[M]. 北京:人民邮电出版社, 2021.

[10] 钱红兵,李艳丽,张蕊. WebCollector 和 ElasticSearch 在高校网站群敏感词检测中的应用研究[J]. 电子设计工程, 2019, 27(24): 11-14.

[11] 王志军,姚文达. Web API 后端接口管理与应用[J]. 智能计算机与应用, 2024,14(5):247-251.

[12] 互联网政务应用安全管理规定[J]. 中华人民共和国公安部公报, 2024(3):7-11.

[13] 张虎,张秋萍. 基于 KONG 的 API 集成系统的设计与实现[J]. 计算机技术与发展, 2019,29(8):102-106.

【作者简介】

方钟亮(1980—),男,江苏昆山人,硕士,高级工程师,研究方向:政务信息化建设。

(收稿日期:2024-12-18)

[5] 刘俊明,孟卫华. 基于深度学习的单阶段目标检测算法研究综述[J]. 航空兵器, 2020, 27(3): 44-53.

[6] 徐渊,许晓亮,李才年,等. 结合 SVM 分类器与 HOG 特征提取的行人检测[J]. 计算机工程, 2016, 42(1): 56-60.

[7] REN S Q, HE K M, GIRSHICK R, et al. Faster R-CNN: towards real-time object detection with region proposal networks[J]. IEEE transactions on pattern analysis and machine intelligence. 2017,39(6):1137-1149.

[8] 郑婷婷,杨雪,戴阳. 基于关键点的 Anchor Free 目标检测模型综述[J]. 计算机系统应用, 2020, 29(8): 1-8.

[9] 邵延华,张铎,楚红雨,等. 基于深度学习的 YOLO 目标检测综述[J]. 电子与信息学报, 2022, 44(10): 3697-3708.

[10] 杨晓玲,江伟欣,袁浩然. 基于 YOLOv5 的交通标志识别检测[J]. 信息技术与信息化, 2021(4): 28-30.

【作者简介】

郭向楠(1988—),男,河南洛阳人,硕士,工程师,研究方向:嵌入式软件设计与测试。

(收稿日期:2025-02-20)