基于智能化监测平台的医疗数据交互风险治理研究

王利平 熊尚华 黄玉清 周宸棋 金 珊

（金华市中心医院 金华 321000）

〔摘要〕 **目的/意义** 聚焦医疗机构应用程序编程接口（application programming interface，API）数据交互场景，通过智能化风险监测平台建设，识别高风险漏洞，防止数据泄漏，强化数据交互安全。**方法/过程** 采用数据平面开发套件技术实现旁路流量分析，实时监控医院业务系统访问行为。基于 OWASP 发布的 10 类 API 安全漏洞，建立评估机制，通过多维度风险策略模型识别异常风险，结合日常数据安全运营，构建“分析－评估－监测－溯源”数据交互安全保障体系。**结果/结论** 医院针对平台监测出的 API 安全漏洞、数据泄漏、Web 攻击、账号安全等风险进行专项整改，避免了数据泄漏，提升了医院数据交互监测水平和安全保障能力。

〔关键词〕 应用程序编程接口；风险监测；风险评估模型；旁路流量分析

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2025.07.013

Study on Risk Governance of Medical Data Interaction Based on the Intelligent Monitoring Platform

WANG Liping, XIONG Shanghua, HUANG Yuqing, ZHOU Chenqi, JIN Shan

Jinhua Central Hospital, Jinhua 321000, China

〔**Abstract**〕 **Purpose/Significance** Focusing on the data interaction scenarios of application programming interface (API) in medical institutions, through the construction of an intelligent risk monitoring platform, in order to identify high－risk vulnerabilities, prevent data leakage, and strengthen data interaction security. **Method/Process** Bypass flow analysis is implemented by adopting the data plane development kit technology to monitor the access behavior of hospital business systems in real time. Based on the 10 types of API security vulnerabilities released by OWASP, an assessment mechanism is established. Abnormal risks are identified through a multi－dimensional risk strategy model. Combined with daily data security operations, a data interaction security guarantee system of “analysis－assessment－monitoring－traceability” is constructed. **Result/Conclusion** The hospital has carried out special rectification for API security vulnerabilities, data leakage, web attack, account security and other risks detected by the platform, avoiding the occurrence of data leaks, improving the hospital’s data interaction monitoring level and security protection capabilities.

〔**Keywords**〕 application programming interface (API); risk monitoring; risk assessment model; bypass flow analysis

1 引言

数字中国战略驱动下，数据要素安全治理范式正经历结构性变革。医疗数据作为新型生产要素核

〔修回日期〕 2025－06－04

〔作者简介〕 王利平，高级工程师，发表论文 2 篇。

〔基金项目〕 浙江省医药卫生科技计划项目（项目编号：2023KY1281）。

心载体，在催生新质生产力的同时，其安全治理问题已成为掣肘健康中国战略实施的瓶颈[1]。在此背景下，2021 年《中华人民共和国数据安全法》与《中华人民共和国个人信息保护法》协同实施，构建了涵盖数据全生命周期的治理框架：前者通过分类分级管理与风险监测预警筑牢安全基线，后者以最小必要原则和知情同意规则强化个人敏感信息保护。在医疗健康领域，《医疗卫生机构网络安全管理办法》针对行业特性细化规定，强调“加强传输接口安全控制，确保传输安全，防止数据窃取”。

应用程序编程接口（application programming interface，API）具备可重用、可定制、可扩展特性，已成为医院信息系统间主要数据交互方式[2]。互联互通建设中，海量医疗数据通过 API 交互，推动临床诊疗、医院运营及医学研究等多维数据价值的指数级释放[3-4]。医院数字化应用上线提升了医疗服务质量和效率[5]，但也带来严峻的数据安全挑战，API 成为灰黑产首要攻击目标[6]。尽管各大医疗卫生机构已具备较完善的网络安全防护体系，但在医疗业务数据交互安全保障方面仍存在不足[7-9]，如 API 交互链路可视化存在监测盲区，难以深度审计数据类型、敏感级别及传输规模。2023 年开放式 Web 应用程序安全项目（open web application security project，OWASP）发布的 API 安全风险报告显示，攻击者可通过未授权访问、参数注入等手段窃取敏感数据或发起服务阻断攻击[10]。医院应针对 API 风险进行全生命周期跟踪处理，防范 Web 攻击、数据泄漏、账号权限滥用等风险，保障数据安全[11]。本研究基于“智能化数据交互风险监测平台”（以下简称“平台”），构建覆盖“画像建模分析－安全漏洞评估－多维度风险识别与智能监测－数据溯源”的多层次 API 安全防护框架。通过引入动态风险评估模型与交互式搜索技术，实现医疗数据交互路径可视化映射及威胁实时响应，为医疗行业 API 安全防护体系技术优化提供实证参考。

2 系统设计

2.1 架构设计

采用分层架构设计，主要包括数据采集处理层、数据存储层、数据分析层、场景应用层、数据展示层，见图 1。数据采集处理层对原始流量数据进行识别、提取和规范化处理，采用对业务系统零打扰的旁路流量分析模式，通过自研中间件分发处理数据；数据存储层将系统模型配置与 API 数据分别存储在不同的数据库中，以加快数据处理查询速度；数据分析层服务于上层场景应用，通过数据识别、API 上下文关联、多维风险监测等智能模型分析数据；场景应用层是平台识别 API 数据、弱点、风险及提供溯源能力的核心功能层，支持 50 多类数据标签、50 多个弱点场景和 30 多个异常行为场景识别；数据展示层涵盖 API 态势、数据交互态势、脆弱性态势、风险态势、威胁 IP 态势等，实现对 API 安全态势的全面感知。

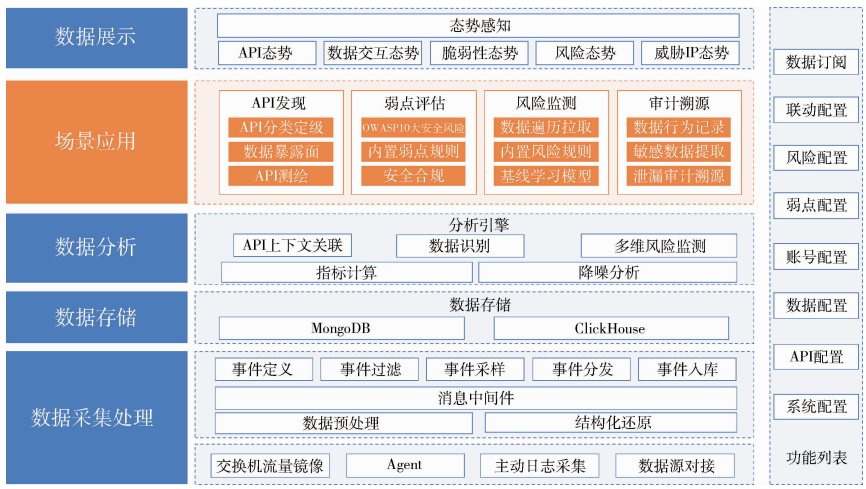

图 1 智能化数据交互风险监测平台架构

2.2 功能设计

2.2.1 API 内外网全面监测体系 采用镜像流量采集技术，在不中断业务系统运行前提下实现网络数据全量捕获。覆盖医院内网、隔离区（demilitarized zone，DMZ）、专网。基于数据平面开发套件技术构建高性能流量分析引擎。API 内外网双向监测体系核心功能包括：利用深度包检测技术动态梳理 API 数据暴露面，构建含接口地址、传输协议、数据字段的资产清单；基于漏洞特征库匹配，精准识别开放 API 的身份鉴权缺陷、内外网敏感数据暴露等安全隐患；依托威胁情报驱动的行为分析模型，实时预警非法 API 调用、数据爬取等网络攻击行为。最终形成“资产可视 - 漏洞闭环 - 攻击溯源”纵深防御链条，有效提升医疗数据交互场景主动防御能力。

2.2.2 API 数据交互安全全生命周期保障体系 依托平台监测能力，形成“风险监测 - 分析定级 - 协同处置 - 效果核验”完整处置链条，见图 2。通过“平台智能监测 + 人工专业研判”协同防御模式，建立 3 级联动闭环处置机制，主要环节如下：一是平台实时分析系统业务流量，精准捕获数据交互风险；二是运营团队基于威胁评估矩阵对平台告警进行风险评级，确认存在安全漏洞的 API 并生成处置工单；三是开发运维团队依据安全基线标准修复漏洞，并将整改结果反馈给运营端复测验证。

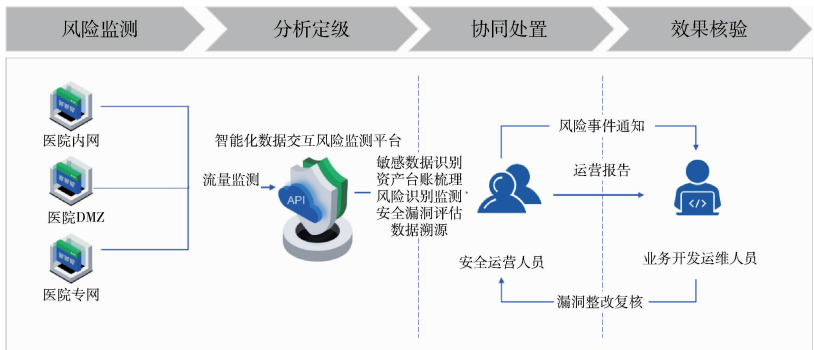

图 2 数据交互安全保障体系

3 系统实现

3.1 覆盖全局的 API 画像建模分析

采用旁路采集技术非侵入式获取医院 API 通信流量，在确保业务连续性前提下建立实时监控体系，其核心逻辑是构建多维 API 行为画像。首先解析 API 所属系统、格式、标签、请求方法等基础属性，分析终端类型、访问域、部署域等特征，量化数据交互风险，通过累计访问次数、单次最大返回数据量等动态指标评估数据暴露面，结合敏感等级、风险等级、弱点数量等安全维度建立威胁模型。其次跟踪 API 生命周期，形成覆盖协议层、应用层、数据层的三维观测矩阵。最后对海量患者诊疗数据与个人信息进行结构化解析，将离散 API 交互行为映射为医院资产台账，实现“流量捕获 - 特征解构 - 风险评估 - 资产沉淀”闭环治理路径。

3.2 API 安全漏洞评估

引入 OWASP 2023 版 10 大漏洞分类，通过内置规则对 API 进行安全评估，提供详细 API 路径、样例、数据流向域、漏洞描述、整改建议，并评估潜在影响，在漏洞被利用前及时修复，防范数据泄漏。覆盖的常见 API 漏洞包括参数可遍历、明文密码透出、登录密码弱、返回数据量可修改等。

3.3 多维度风险识别与智能监测

基于异常度、偏离度及贡献度等多维指标监测 API 异常行为，融合随机森林、极限梯度提升等算法量化风险等级，自动学习数据风险特征，结合动态阈值识别风险事件，构建动态 API 风险评估模型。首先构建正常业务基线，识别异常操作链（如

调用频次超均值行为)。其次基于医生、患者、第三方机构等用户角色建立细粒度行为画像。最后基于 API 上下文参数特征优化模型，动态调整监测策略。覆盖的医疗数据交互风险包括 3 类：数据泄漏类（异常请求参数、敏感数据查询、IP 访问频率异常等），Web 攻击类（渗透尝试、路径试探等），账号安全类（同一 IP 关联多账号、账号批量下载患者信息等）。

3.4 数据溯源

运用交互式搜索技术关联分析 API 访问信息，快速还原数据链路并定位溯源。通过数据留痕记录 API 交互详情，发现风险时以患者诊疗数据为线索，结合访问特征（如账号、接口等）进行统计分析，建立快速响应、攻击链重构、电子证据固定的完整溯源能力。

4 应用及效果

平台建设前医院业务系统存在 API 资产不清、漏洞无法评估、风险无法监测、数据暴露无法追溯等问题，监测效率、覆盖面、准确率均有不足。平台建设后，实现了 API 可视、可管、可控，标志着医疗数据交互风险监测实现从无到有的突破。截至 2025 年 3 月，平台已运营 4 个月，监测流量平均为 283 Mbps、峰值达 885 Mbps，整改高中危 API 漏洞 236 个，API 漏洞误报率 14.5%，人工运营 API 风险事件 328 起，经确认未发生真实数据泄漏。

4.1 可视：API 资产台账

平台监测应用 35 个、API 2 155 个，日均 API 请求超 200 万次。通过持续监测分析 API 数据交互，发现业务场景中的数据暴露情况和潜在安全风险。例如，171 个涉及身份证的 API 中，有 4 个单次可获取超 3 000 条数据。

4.2 可管：API 漏洞评估整改

依据 OWASP 2023 版 10 大漏洞分类，识别漏洞项 456 个，见表 1。

表 1 API 漏洞监测结果

ID	分类	级别数量（高/中/低）（个）	类别总数（个）	类别占比（%）
API1：2023	损坏的对象级别鉴权（broken object level authorization）	33/121/84	238	52.19
API2：2023	身份认证缺陷（broken authentication）	38/53/45	136	29.82
API3：2023	损坏的对象属性级别鉴权（broken object property level authorization）	0/8/38	46	10.08
API4：2023	未受限的资源消耗（unrestricted resource consumption）	1/0/0	1	0.22
API5：2023	损坏的功能级别鉴权（broken function level authorization）	0/1/0	1	0.22
API6：2023	未受限的敏感业务流访问（unrestricted access to sensitive business flows）	0/0/0	0	0
API7：2023	服务端请求伪造（server side request forgery）	0/0/0	0	0
API8：2023	安全配置错误（security misconfiguration）	0/1/13	14	3.07
API9：2023	资源管理失当（improper inventory management）	0/0/0	0	0
API10：2023	不安全的 API 使用（unsafe sonsumption of APIs）	0/20/0	20	4.40

其中细分小类含 11 个未鉴权 API、32 个参数可遍历 API、14 个泄漏明文密码 API、37 个可修改返回数据 API。例如，某未鉴权接口在互联网上被访问后，可修改手术时间并获取医院所有孕产妇的姓名、身份证号、手术名称等信息。通过对接口添加鉴权认证、对隐私数据脱敏处理，有效防范了数据泄漏风险。

4.3 可控：API 风险监测

平台常态化监测全面覆盖接口、IP、账号的

异常风险。监测发现高危风险行为：某账号在凌晨 1 点至 6 点每 10 分钟访问一次电子病历系统，每次获取约 4 700 条患者信息。经安全运营人员溯源查证，该职工无主观恶意，实为系统页面定时刷新 API 所致。确认风险后，运营人员协同系统开发人员修改 API，调整接口鉴权过期时间并限制单次返回数据量，规避了大量敏感数据泄漏的风险。

5 结语

医疗机构可通过 API 构建标准化通道，实现院内私有网络与开放网络间数据的可控、合规交互。本研究根据医疗业务场景需求，建立 59 类敏感数据自动化标识体系，监测覆盖 OWASP 公布的 10 类安全漏洞风险。通过专项整改，采取鉴权加固、优化数据脱敏策略等措施，极大提升医院医疗数据交互监测水平和安全保障能力。未来将进一步从 API 治理、数据分类分级、数据脱敏等方面开展研究实践，在保障数据安全的前提下，构建“以数据为中心、以接口为最小治理单元”的精细化治理模式。

作者贡献：王利平负责研究设计、论文撰写；熊尚华、黄玉清负责论文修订；周宸棋负责现状调研；金珊负责相关政策梳理。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 “十四五”数字经济发展规划［EB/OL］.［2024－12－12］. https://www.gov.cn/gongbao/content/2022/content_5671108.htm.

2 汤其宇，陈昌杰，王士勇. 医院网络环境中 API 接口的安全性问题与对策探讨［J］. 中国数字医学，2024，19（6）：115－120.

3 金山. 面向医疗大数据的网络数据安全存储检索系统的设计及实验分析［J］. 科学技术创新，2023（8）：96－99.

4 高竞，李碧辉. 互联互通背景下对医疗数据安全保护的思考［J］. 中国信息安全，2022（7）：52－54.

5 胡晓兰，贾丹，吴玮，等. 医院自助医疗系统在提高门诊服务质量与就诊体验中的效果评价［J］. 中国医学装备，2020，17（10）：139－142.

6 网宿安全 2022 年 Web 安全观察报告：API 成头号攻击目标，DDoS、Bot 攻击倍增［J］. 中国信息安全，2023（7）：108.

7 孟晓阳，杨巍，张楠，等. 医院近源网络攻击风险分析及对策建议［J］. 医学信息学杂志，2024，45（9）：87－90.

8 郑攀，刘华，琚文胜，等. 我国医院数据安全现状调查分析［J］. 医学信息学杂志，2024，45（5）：71－75.

9 郑攀，陈臣，马扬，等. 医疗卫生机构数据安全管理建设［J］. 中国数字医学，2023，18（1）：7－11.

10 OWASP. OWASP top 10 API security risks－2023［EB/OL］.［2024－10－18］. https://owasp.org/API－Security/editions/2023/en/0x11－t10.

11 孙保峰，葛晓伟，杨扬，等. 某三级甲等公立医院 API 接口安全监测实践与思考［J］. 中国数字医学，2024，19（7）：115－120.

关于《医学信息学杂志》启用“科技期刊学术不端文献检测系统”的启事

为了提高编辑部对于学术不端文献的辨别能力，端正学风，维护作者权益，《医学信息学杂志》已正式启用“科技期刊学术不端文献检测系统”，对来稿进行逐篇检查。该系统以《中国学术文献网络出版总库》为全文比对数据库，可检测抄袭与剽窃、伪造、篡改、不当署名、一稿多投等学术不端文献。如查出作者所投稿件存在上述学术不端行为，本刊将立即做退稿处理并予以警告。希望广大作者在论文撰写中保持严谨、谨慎、端正的态度，自觉抵制任何有损学术声誉的行为。

《医学信息学杂志》编辑部