DOI:10.20033/j.1003-7241.(2026)08-0132-06

基于可信计算环境的气象数据可信空间研究

朱 辉[1,2,3], 徐晓琳[1,2,3], 李建明[1,4], 孟 金[1,2,3]

(1.山东省气象防灾减灾重点实验室,济南 250031;2.山东省气象数据中心,济南 250031;
3.山东省数据开放创新应用实验室,济南 250031;4.东营市气象局,山东 东营 257000)

摘 要:随着气象数据的广泛应用,数据安全风险与共享需求之间的矛盾日益凸显,构建安全、可信的气象数据服务体系成为亟需解决的重要问题。研究采用海光、天数智芯及华为昇腾等国产化算力架构,结合Kubernetes容器化编排技术,构建了多源异构的可信计算基础设施。针对地面气象观测数据的多模态特征,对比分析了差分隐私、同态加密、安全多方计算等隐私保护技术的计算效率与安全性边界,提出基于可信计算环境的动态分级保护方案。通过构建"数据可用不可见"的气象数据可信空间,实现了统计分析服务接口、个性化计算引擎、基于属性的访问控制及全链路审计追踪等核心功能。实践表明,该平台在确保"原始数据不出域"的前提下,有效提升了气象数据使用的安全性与灵活性,为气象数据在科研领域的安全共享与深度应用提供了有力支撑。

关键词:可信计算环境;气象数据;可信空间;国产化;数据服务

中图分类号:TP393.083;P409 **文献标志码**:A **文章编号**:1003-7241(2026)08-0132-06

Research on trusted space of meteorological data based on trusted computing environment

Zhu Hui[1,2,3], Xu Xiaolin[1,2,3], Li Jianming[1,4], Meng Jin[1,2,3]

(1. Key Laboratory for Meteorological Disaster Prevention and Mitigation of Shandong, Jinan 250031, China;
2. Shandong Provincial Meteorological Data Center, Jinan 250031, China;
3. Shandong Data Open Innovative Application Laboratory, Jinan 250031, China;
4. Dongying Meteorological Bureau, Dongying 257000, Shandong, China)

Abstract: With the widespread application of meteorological data, the contradiction between data security risks and sharing demands has become increasingly prominent. Constructing a secure and trustworthy meteorological data service system has emerged as a crucial issue requiring urgent resolution. This study employs domestic computing architectures such as Haiguang, Tianshu Zhixin, and Huawei Ascend, combined with Kubernetes container orchestration technology, to establish a multi-source heterogeneous trusted computing infrastructure. Aiming at the multimodal characteristics of surface meteorological observation data, this paper comparatively analyzes the computational efficiency and security boundaries of privacy-preserving technologies such as differential privacy, homomorphic encryption, and secure multi-party computation, and proposes a dynamic hierarchical protection scheme based on trusted computing environments. By constructing a trusted space for meteorological data where "data is usable but invisible," core functions such as statistical analysis service interfaces, personalized computing engines, attribute-based access control, and full-link audit tracking are realized. Practices show that the platform effectively enhances the security and flexibility of meteorological data usage under the premise of ensuring that "original data does not leave the domain," providing strong support for the secure sharing and in-depth application of meteorological data in the scientific research field.

Keywords: trusted computing environment; meteorological data; trusted space; indigenization; data service

气象数据作为国家基础性战略资源,在灾害预警、农业生产、智慧城市等领域发挥着重要支撑作用[1-3]。随着人工智能和大数据技术的深入应用,气象数据的开放共享与价值挖掘成为推动气象现代化转型的核心动力。然而,气象数据具有强时空关联、多模态异构和高敏感性等特性,其开放共享面临两大核心矛盾:一是数据市场化需求与隐私泄露风险的冲突;二是跨域协同计算效率与数据主权保护的平衡难题[4-6]。如何在确保"数据不出域"的前提下,构建安全高效的可信服务体系,成为亟待解决的关键问题。

国际上,美国NOAA、欧洲ECMWF等机构已构建了融合分级授权与隐私计算的数据服务平台[7-8],Google、IBM等企业通过差分隐私和同态加密技术在医疗、金融领

收稿日期:2025-07-07;**录用日期**:2025-08-19

基金项目:山东省气象局重点课题(2023sdqxz05)

作者简介:朱 辉(1993—),男,工程师,研究方向为气象大数据云服务、数据安全。

通信作者:徐晓琳(1978—),女,工程师,研究方向为气象数据管理、气象信息化。

引用本文:朱辉,徐晓琳,李建明,等.基于可信计算环境的气象数据可信空间研究[J].自动化技术与应用,2026,45(8):132-137.(Zhu Hui, Xu Xiaolin, Li Jianming, et al. Research on trusted space of meteorological data based on trusted computing environment[J]. Techniques of Automation and Applications, 2026, 45(8): 132-137.)

域实现“数据可用不可见”[9-11]。然而,这些技术路径多依赖国外软硬件生态,存在自主可控风险。国内方面,国家气象信息中心建设了国省两级气象大数据云平台和中国气象数据网[12-16],实现了数据资源集约化管理和开放共享,为科研、经济和社会发展提供了有力支持。2024 年 11 月,国家数据局发布《可信数据空间发展行动计划(2024—2028 年)》,但国内各行业仍处于可信数据空间的初级探索阶段[17-19],现有平台多依赖物理隔离和权限控制,缺乏动态分级保护与可信协同计算的支持,难以满足科研场景下“精准可用、安全可控”的双重需求。

针对上述问题,本研究依托国产化算力架构,提出基于可信计算环境(trusted computing environment, TCE)的气象数据可信空间构建方法,旨在实现地面气象数据在科研场景下的安全高效应用,为数据共享与隐私保护提供创新解决方案。

1 地面气象数据特征与科研需求

1.1 地面气象数据资源特征分析

山东省地面气象数据主要来源于覆盖全省的地面气象观测站网,包括国家级自动气象站、省级自动气象站、公路交通气象站等多种类型,总数超过 2 000 个;观测要素涵盖温度、湿度、气压、风速风向、降水量、日照时数、能见度等,数据采集频率从分钟级到小时级不等;自 1950 年起,山东省气象观测数据实现了连续保存,形成了丰富的历史数据资源。然而,数据格式多样、质量参差不齐等问题仍然存在,部分观测站点存在数据缺测、异常值等情况,影响数据的可用性。山东省地面气象数据资源呈现多模态特征,如表 1 所示。

表 1 山东省地面气象数据资源特征

Tab. 1 Characteristics of surface meteorological data resources in shandong province

特征维度	具体描述
数据来源	覆盖 2 000 +站点(自动气象站、交通气象站等),水平分辨率达 7.62 km。
要素类型	温度、湿度、气压、风速风向、降水量等 80 余种。
时序连续性	数据可追溯至 1950 年,分钟级至小时级观测频率,日均增量超 85 万条记录。
数据质量	存在数据缺测或异常值,需动态清洗与插值修复。

1.2 科研场景下的数据服务需求

通过对山东省气象部门用户的调研,并结合气象大数据云平台中用户数据访问行为的统计分析,科研用户的核心需求可归纳为以下 3 类。

1)高精度数据访问需求。科研人员在开展气象模型开发与验证、气候变化研究等工作时,高度关注数据的历史积累与多维特征信息。此类用户对数据的长期连续性、时空分辨率和要素多样性具有较高要求。平台需支持多维度数据检索功能(时间、空间、要素等),并提供标准化的数据访问接口,以实现高效、灵活的数据获取。

2)常见要素的统计分析需求。针对具体科研课题,科研人员通常需针对特定时段、区域或气象要素开展数据提取与分析工作。平台应预置通用数据服务接口或处理算法,如均一化处理、距平计算、极值统计等,同时支持用户自定义参数配置,提供定制化的数据服务,提升科研效率与数据分析深度。

3)灵活的高性能计算能力需求。在处理大规模气象数据集时,科研人员对计算资源和读写性能有较高要求,尤其在模型训练、AI 算法应用等方面。平台需提供 CPU 算力和 AI 加速能力,并具备资源动态分配、存储扩展及运行环境隔离等功能,以满足不同科研任务对计算性能与安全性的多样化需求。

2 可信空间技术选型

2.1 差分隐私

差分隐私通过在数据中加入噪声,保护数据信息的隐私[20-21]。然而,在气象数据处理场景中,数据的精度和连续性至关重要,添加噪声可能影响数据的可用性和分析结果的准确性。因此,差分隐私在气象数据处理中的应用受到一定限制。

2.2 同态加密

同态加密允许在加密数据上直接进行计算[22-23],保障数据在处理过程中的安全性。然而,该技术在计算效率和资源消耗方面面临显著挑战,尤其是在处理大规模气象数据时,可能导致性能瓶颈,不适合实时性要求高、计算资源稀缺的应用场景。

2.3 安全多方计算

安全多方计算允许多个参与方在不泄露各自数据的前提下共同计算结果[24-25]。该技术适用于跨组织的数据协同计算,但在气象数据科研应用场景中,涉及的数据参与方较少,且数据主要集中在气象部门内部,应用场景有限。

2.4 可信计算环境

可信计算环境通过硬件隔离、数据权限控制和安全审计等方式,提供一个安全的计算环境,保护数据在使用过程中的机密性和完整性[26-28]。海光 CPU 内置的安全处理器和密码协处理器,支持 TPM2.0 和 TCM2.0 标准,可与现有的气象基础设施资源等软硬件平台无缝集成,实现从系统启动到运行的全方位安全保障。

2.5 选型总结

针对气象数据强时空关联、高精度需求的特点,从安全性、计算效率、适用性三个维度对主流隐私计算技术进行总结比较,如表 2 所示。

表2 常见隐私计算技术在气象数据处理中的性能与适用性对比

Tab. 2 Performance and applicability comparison of common privacy computing techniques in meteorological data processing

技术	安全性	计算效率	适用场景	气象数据适配性
差分隐私	中	高	统计发布	噪声干扰时空连续性、分析准确性
同态加密	高	低	小规模加密计算	日均超85万条数据,加密计算资源与时间消耗大
安全多方计算	高	中	跨机构协同计算	气象数据单方持有,协同需求弱
可信计算环境	极高	高	高安全单方计算	支持硬件级隔离,数据精度无损

综合考虑各技术特点及气象数据适配性,可信计算环境在气象数据的安全处理和共享中具有明显优势。其硬件级的安全保障和高效的计算能力,结合身份认证和数据访问控制策略,满足了气象数据处理对安全性和实时性的双重需求。因此,选定可信计算环境作为气象数据可信空间的实现基础。

3 平台系统架构与国产化集成

为实现地面气象观测数据在科研场景下的安全可控共享与高效计算处理,本研究设计并实现了基于国产化技术栈与可信计算环境的气象数据可信空间平台。平台整体架构遵循“软硬件协同、分层解耦、服务可信”的原则,融合异构算力、容器化调度、安全机制和访问审计机制,支撑气象科研用户对大规模敏感数据的高性能分析需求。

3.1 国产算力与可信执行基础

平台采用国产主流处理器与加速卡构建多源异构算力池,包括海光Hygon C86处理器、天数智芯天垓加速卡、华为昇腾AI加速卡等。其中,海光处理器内嵌安全模块与密码协处理器,支持国密算法与可信启动;天垓与昇腾卡具备强大并行计算与深度学习支持能力,其中天垓兼容CUDA与主流AI框架,满足气象数据的建模与智能分析需求。

为增强资源调度的灵活性,平台引入Kubernetes容器编排技术,构建支持CPU/GPU混合调度的异构集群环境。通过Docker容器技术结合沙箱机制,实现任务级的资源隔离、快速部署与可信运行。

3.2 三层系统架构设计

平台采用“分层解耦、模块协同”的体系架构,整体划分为三大功能层。

数据安全交互层。面向用户提供统一的数据访问能力,支持多协议、多语言、多方式的数据调用,屏蔽底层存储异构性。

可信计算执行层。基于海光CPU的TCE机制构建沙箱环境,支撑数据在“可用不可见”的前提下进行安全计算,结合容器调度实现任务隔离与资源复用。

安全审计与追溯层。实现用户行为的全过程记录与异常行为检测,构建日志链与结果可溯源机制,保障平台服务的合规性与可监管性。

该架构在保障数据资源安全性的同时,实现科研用户对数据的灵活获取与个性化处理,支撑复杂多样的科研任务运行场景。

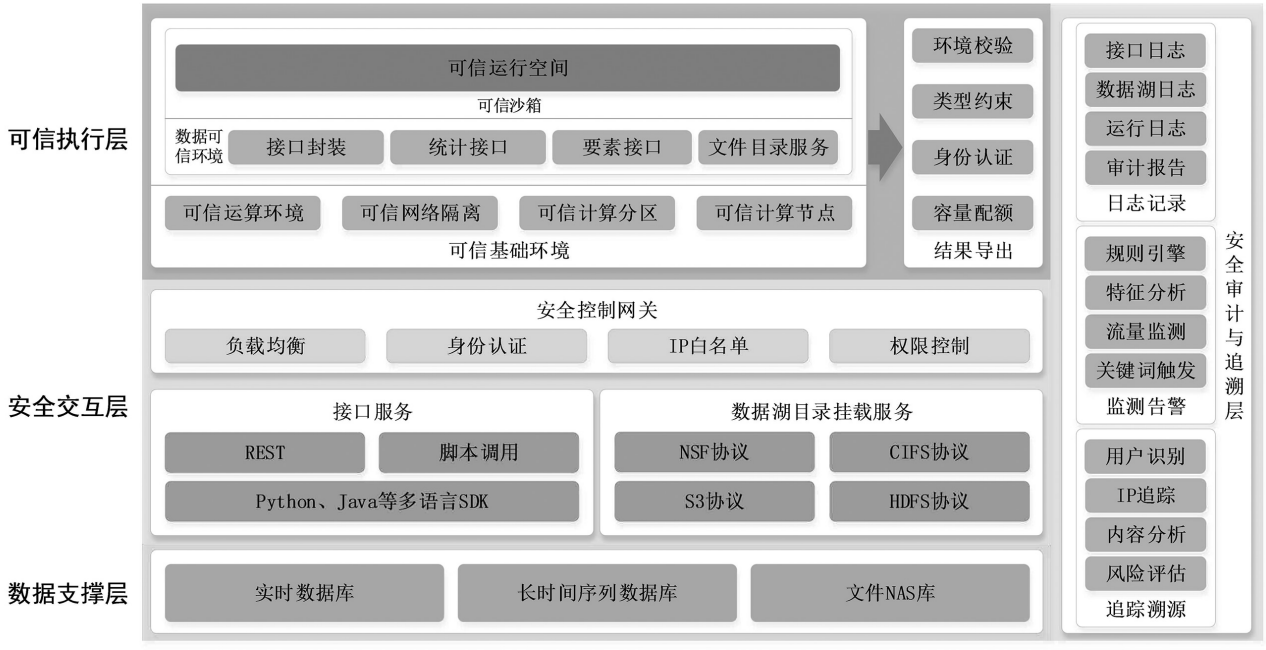


图1 气象数据可信空间平台系统整体架构

Fig. 1 Overall architecture of the trusted spatial platform system for meteorological data

4 关键功能实现与应用场景验证

4.1 统一接口服务与访问控制

平台数据服务接口采用模块化设计理念,为科研用户提供多样化、高适配度的数据调用方式。接口体系设计覆盖不同使用层级和编程习惯的科研人员,支持以下 4 类服务方式。

1) Restful API 服务。面向轻量级的数据调用,通过 HTTP 协议提供标准化 GET 数据检索查询。

2) SDK 客户端服务。提供 Java、C#、C/C++、Python、PHP、Fortran 等多语言 SDK 开发包,支持 Linux、Windows 等主流平台,便于科研人员嵌入算法模型直接调用。

3) 脚本式调用服务。面向弱编程开发场景,支持科研用户在 Notebook 或 IDE 环境中以 Python 等脚本语言访问可信接口。

4) 数据湖目录服务。针对科研用户对文件类数据的批量访问需求,将不同存储类型(如 NFS、CIFS、FTP、S3)挂载至统一的虚拟目录树中,依据业务规则重组目录结构,通过统一命名空间提供挂载式文件访问,支撑科研用户进行大规模原始文件的顺序处理、重组调用与数据导出;管理员可配置目录访问权限策略,控制用户访问路径范围,并通过调用日志进行统计分析。

接口服务体系内嵌权限管控机制,基于 RBAC 与 ABAC 模型混合,实现动态的细粒度访问控制。用户权限不仅与其角色身份绑定,还与调用数据的属性(数据级别、时间区间、数据要素等)关联,实现“最小可用性”授权原则,确保数据访问行为可控、合规。

4.2 可信计算沙箱调度机制

平台基于 TCE 机制构建可信执行节点,并将可信计算节点自动注入数据服务接口 IP 白名单,实现计算节点数据访问的自动授权。科研用户提交的任务仅在 TCE 沙箱中进行数据加载、运行、输出,原始数据只在沙箱内参与计算,用户仅能导出结果或直接可视化。具体实现机制包括以下 4 点。

1) 任务容器沙箱化部署。用户提交算法脚本或云端可视化编程,由平台统一调度至可信节点执行,与外界网络隔离。

2) 数据隔离加载。对于库表类数据,每次任务运行用户访问的仅为封装的数据接口,避免对原始数据库的直接操作;对于文件类数据,用户通过数据湖的只读权限获取。

3) 执行日志记录与结果输出。运行过程中系统自动记录日志,用户可将数据结果保存并导出至数据湖的个人空间中。

4) 远程度量与运行环境校验。每次任务调度前,对可信节点进行完整性验证,防止恶意代码植入或 TCE 失效。

此机制保障了数据在计算过程中始终处于可信边界内流转与使用,为科研用户提供可信赖的执行保障。

4.3 安全审计与行为追溯

平台构建了全过程的安全审计机制,对科研用户的数据调用、任务提交、接口访问等关键操作进行全链条记录,主要包括以下 4 点。

1) 日志记录机制。自动采集操作时间、用户 ID、数据 ID、接口路径、运行状态等关键字段。

2) 日志链构建。采用哈希链技术形成不可篡改的调用记录链,支持回溯与合规性验证。

3) 异常检测机制。基于行为规则(如调用频率、资源消耗、异常参数组合)进行实时风险分析。

4) 审计报告与安全告警。系统定期生成使用报告,并在发现风险行为时触发告警,支持人工干预与事后追责。

该机制提升了平台的可监管性与运行透明度,为可信空间提供了制度层面的安全闭环支撑。

4.4 典型应用场景验证

基于上述架构与机制,平台实现了多种面向科研用户的典型应用场景。

1) 标准统计分析服务。基于平台预置代码片段,通过参数化微调和接口方式调用,用户可快速获取特定站点/区域/时间段的温度、降水、风速等要素的统计结果(如均值、极值、累计值),用于趋势分析与模型验证。

案例 1 山东省近十年月均降水趋势分析。

基于中国地面日值数据,在平台内利用 Notebook 在线参数化微调数据读取代码片段,通过平均值统计分析接口获取 2015-2024 年全省国家站月均水量数据,按月份分组输出月均降水量数据,结合 Mann-Kendall 检验与 Sen′s 斜率估算代码片段,按月份输出每月降水趋势分析结果,如图 2 所示。对近十年的逐小时数据按月统计分析,共耗时 76 s,分析效率满足科研需求,原始数据全程不可见,保障数据安全。

2) 个性化算法运行服务。用户上传自定义算法脚本或云端可视化编程,平台在可信环境中调度运行,并提供日志监控与结果可视化支持。

案例 2 济南国家气象站每日逐时降水总量分析。

基于中国地面逐小时数据,在平台内利用 IDE 在线编程环境,通过数据服务接口调用当日逐小时数据,计算 1 小时降水量、2 小时降水量等逐时降水总量结果并打印输出,生成 json 文件用于数据导出,如图 3 所示。原始数据可信计算,导出数据安全可信。

4.5 总结分析

通过构建多层次系统架构与细粒度权限控制机制,平台实现了从数据访问到计算过程的全链路可信保护。在功能层面,平台支持多类接口调用、个性化算法运行与全过程审计,为科研用户提供安全、高效、可控的数据服务能力。典型案例验证表明,该平台在保障数据不出域的同时,能满足大规模气象数据分析的性能需求,具备较强的实用性和推广价值,为气象数据安全共享与智能化应用提供了创新路径。

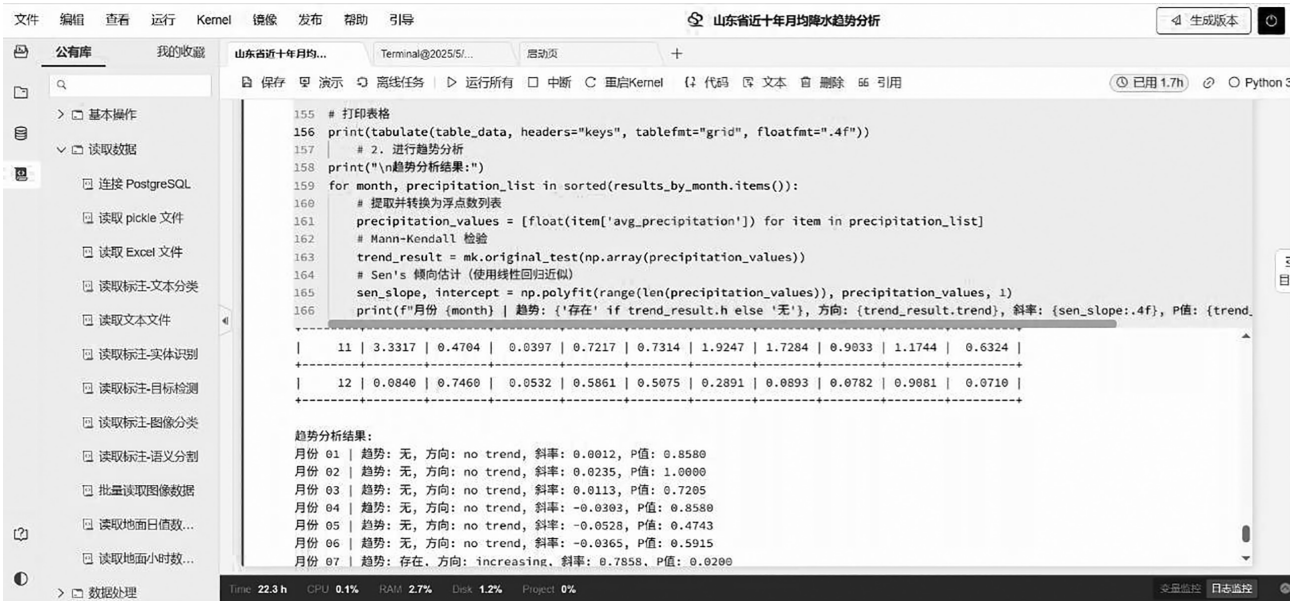


图2 山东省近十年月均降水趋势分析结果

Fig. 2 Trend analysis results of monthly average precipitation in shandong province over the past decade

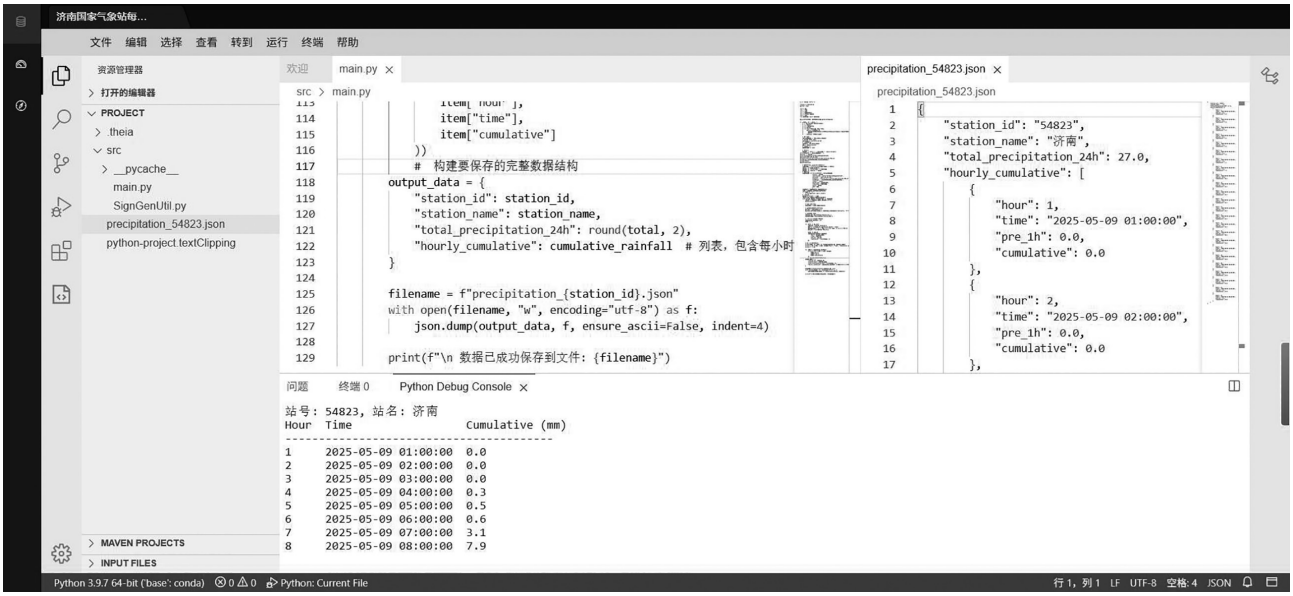


图3 在线 IDE 编程分析济南国家气象站每日逐时降水总量

Fig. 3 Programming analysis of hourly precipitation totals at jinan national meteorological station using an cloud IDE

5 结论

本研究基于可信计算环境技术构建了融合国产化软硬件与容器化技术的气象数据可信空间平台。平台实现了多源异构算力的统一调度与弹性管理,保障了资源的自主可控与高效利用。通过引入动态分级数据保护机制,确保了敏感气象数据的安全使用。此外,平台还构建了“数据可用不可见”的科研沙箱,满足了多样化的科研需求,提升了数据共享的安全性与灵活性。

未来,平台将朝着智能化、协同化和标准化方向发展。一方面,结合人工智能技术,提升数据敏感度识别与访问控制的智能化水平;另一方面,探索多方安全计算与可信协同计算的融合,实现跨行业、跨区域的数据联合分析与模型训练。同时,拓展平台对卫星遥感、雷达监测等多源异构数据的支持,丰富数据服务接口,优化资源调度与实时计算能力,推动平台在更广泛的气象业务场景中应用。

参考文献

[1]罗孳孳,唐云辉,武强,等. 气象大数据应用场景与气象服务技术预见研究——面向重庆农业领域[J]. 农业现代化研究,2024,45(1):150-164.

[2]王梓茜,武凤文,程宸,等. 城市规划领域气象大数据分析技术研究[J]. 城市发展研究,2020,27(11):16-21.

[3]魏晓川,王新刚. 基于气象大数据的城市电力负荷预测[J]. 电测与仪表,2021,58(2):90-95.

[4]蒲晓虎,何奇,钟美. 气象数据安全防护体系建设探索与实践[J]. 网络安全与数据治理,2025,44(3):59-62.

[5]赵忠凯,王祝先,韩书新,等. 随机森林在气象网络入侵检测中的应用[J]. 自动化技术与应用,2024,43(7):129-133.

[6]杨代才. 气象大数据云平台的网络安全防护体系设计[J]. 信息安全

研究,2023,9(7):701-706.
[7]赵强,于凯本. 美国海洋科学数据管理政策现状与启示[J]. 海洋信息,2019,34(4):1-7.
[8]Schneider R,Bonavita M,Geer A,et al. ESA-ECMWF report on recent progress and research directions in machine learning for Earth system observation and prediction[J]. npj Climate and Atmospheric Science,2022,5(51):1-8.
[9]Beaulieu-jones B K,Wu Z S,Williams C,et al. Privacy-preserving generative deep neural networks support clinical data sharing[J]. Circulation:Cardiovascular Quality and Outcomes,2019,12(7):e005122.
[10]Truex S,Liu L,Gursoy M E,et al. A hybrid approach to privacy-preserving federated learning[C]//Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security. New York:ACM,2019:1-11.
[11]Kaissis G A,Makowski M R,RÜCKERT D,et al. Secure,privacy-preserving and federated machine learning in medical imaging[J]. Nature Machine Intelligence,2020,2(6):305-311.
[12]冯勇,李微,朱辉,等. 云计算环境下山东省气象大数据云平台的设计与实现[J]. 信息技术与信息化,2021(5):147-150.
[13]韩同欣,何文春,吴鹏,等. 气象基础设施云平台关键设计与实现[J]. 气象科技,2022,50(2):290-296.
[14]霍庆,何文春,何林,等. 气象大数据云平台算法集约化环境设计与应用[J]. 应用气象学报,2024,35(1):80-89.
[15]杨英奎,王祝先,李伟金. 数据湖在气象系统中的研究与应用[J]. 自动化技术与应用,2023,42(7):91-94.
[16]陈京华,何小明,张志强. 基于云平台的气象数据共享服务平台架构建设[J]. 气象科技进展,2018,8(1):208-212.
[17]蒋雪炳,史淳樵,卢欣然. 基于区块链技术的医疗隐私信息安全共享方法[J]. 自动化技术与应用,2025,44(7):120-123,152.
[18]包晓丽. 可信数据空间:技术与制度二元共治[J]. 浙江学刊,2024(1):89-100,239-240.
[19]李星毅. 可信数据空间下的大数据治理探讨[J]. 中国安防,2025(增刊1):105-109.
[20]徐雅鑫,徐彦彦,欧阳雪,等. 基于差分隐私的矢量地理数据脱密方法[J]. 测绘学报,2025,54(2):356-370.
[21]赵婵婵,马坤明,石宝,等. 基于差分隐私的自适应联邦学习隐私保护方案[J]. 科学技术与工程,2025,25(7):2849-2855.
[22]李晓东,周苏雅,赵炽野,等. 一种基于同态加密的密文符号函数计算优化方法[J]. 信息安全研究,2025,11(2):100-106.
[23] 付爱英,熊宇峰,曾勃炜. 同态加密下用户隐私数据传输的安全保护方法[J]. 吉林大学学报(理学版),2025,63(2):573-579.
[24]韩伟力,宋鲁杉,阮雯强,等. 安全多方学习:从安全计算到安全学习[J]. 计算机学报,2023,46(7):1494-1512.
[25]马旭阳,周小凯,郑浩宇,等. 基于无服务器计算的多方数据库安全计算系统[J]. 软件学报,2025,36(3):1084-1106.
[26]尚文利,张修乐,刘贤达,等. 工控网络局域可信计算环境构建方法与验证[J]. 信息网络安全,2019(4):1-10.
[27]王晓,张建标,曾志强. 基于可信平台控制模块的可信虚拟执行环境构建方法[J]. 北京工业大学学报,2019,45(6):554-565.
[28]许书宁. 基于可信执行环境的可搜索加密数据库研究[D]. 武汉:华中科技大学,2024.

(上接第 12 页)

[11]刘光军,吴思齐. 基于分段聚合和卡尔曼滤波的锂电池组 SOC 估算[J]. 江苏大学学报(自然科学版),2024,45(3):281-285.
[12]Fogelquist J,Lin X. Combining electrochemistry and data-sparse Gaussian process regression for lithium-ion battery hybrid modeling[J]. Applied Energy,2025,399:126458.
[13]Zhang Y,Jiang J,Tian A. A state of health estimation method of lithiumion batteries based on improved gray wolf and SVM algorithm[J]. Energies,2026,19(8):1875.
[14]Fan X,Li B,Hao Y,et al. A novel SOC estimation method for lithiumion batteries using the fusion of deep neural network and physical information model[J]. Journal of Energy Storage,2025,122:116690.
[15]Varalakshmi S,Sesha LPN,Kotikalapudi S. Deep learning-based SoC estimation of lithium-ion batteries in EVs using 2D CNN[C]//2025 11th International Conference on Electrical Energy Systems (ICEES). Chennai:IEEE,2025:530-534.
[16]于天剑,曾笑颜,冯恩来,等. 基于 LSTM-Transformer 多通道特征融合的锂电池 SOC-SOH 联合估计[J]. 铁道科学与工程学报,2026,23(1):301-313.
[17]方斯顿,刘龙真,孔赖强,等. 基于双向长短期记忆网络含间接健康指标的锂电池 SOH 估计[J]. 电力系统自动化,2024,48(4):160-168.
[18]Barik U,Saravanan B. Hybrid long short-term memory network and Bayesian adaptive extended Kalman filter approach for reliable lithium-ion battery state-of-charge estimation in electric vehicles[J]. Journal of Energy Storage,2026,154(B):121154.
[19]阙小平. 基于深度学习的锂电池 SOH 和 RUL 联合预测方法[D]. 广州:广东工业大学,2025.
[20]杨传凯,刘皓璐,杨毅琛,等. 基于脉冲电压和 CNN-GRU 的梯次利用锂电池健康状态估计[J/OL]. 电源学报. (2026-03-24)[2026-04-15]. https://link.cnki.net/urlid/12.1420.TM.20260324.1551.002.
[21]张朝龙,张俣峰,陈阳,等. 基于 CNN-CBAM-BiLSTM 融合模型的锂离子电池健康状态估计方法[J/OL]. 电源学报. (2025-04-10)[2026-04-15]. https://link.cnki.net/urlid/12.1420.TM.20250410.1125.012.
[22]肖扬帆,李彦明,刘子翔,等. 四轮电驱动水田除草机器人运动建模与路径跟踪控制[J]. 农机化研究,2026,48(2):165-172,182.
[23]黄青青,张金波. 起重机大功率锂电池组管理系统研究[J]. 自动化技术与应用,2025,44(2):4-8,99.
[24]胡晓工,苏志坚,贾晓亮,等. 基于分布式容积信息卡尔曼滤波的锂电池 SOC 估计[J]. 自动化技术与应用,2024,43(12):1-7.