可信数据空间在电力行业的应用研究

国　丽，朱永春，丁　浩
（中国电子数据产业集团，北京　100080）

摘　要：随着电力交易市场化改革的深入推进及“双碳”目标的提出，电力交易模式日趋复杂。数据作为电力交易智能化应用构建的核心支撑，其质量与范围直接决定应用的质量与价值。围绕可信数据空间融合电力交易相关多主体数据联合应用的问题展开研究，首先阐述数据在电力交易智能化应用中的核心重要性；其次梳理现有研究中智能化应用所使用的各类数据资源；进而分析为提升智能化应用水平可引入的跨域跨主体数据类型；随后提出基于可信数据空间实现多主体数据安全可信共享与应用的方案以及数据空间在数据流通中发挥的价值和效用。该研究可为电力交易智能化应用的优化升级及多主体协同的高效开展提供参考。

关键词：电力交易；可信数据空间；数据安全；数据共享
中图分类号：TP399　　**文献标志码：**A　　**DOI：**10.19358/j.issn.2097-1788.2026.04.011

中文引用格式：国丽，朱永春，丁浩. 可信数据空间在电力行业的应用研究[J]. 网络安全与数据治理，2026，45(4)：81-86.
英文引用格式：Guo Li，Zhu Yongchun，Ding Hao. Research on the application of trusted data space in the power industry[J]. Cyber Security and Data Governance，2026，45(4)：81-86.

Research on the application of trusted data space in the power industry

Guo Li，Zhu Yongchun，Ding Hao
（Data Industry Corporation，China Electronics Corporation，Beijing 100080，China）

Abstract：With the further advancement of the market-oriented reform of power trading and the proposal of the "dual carbon" goals，the power trading modes have become increasingly complex. As the core support for the construction of intelligent applications in power trading，data quality and coverage directly determine the quality and value of such applications. This paper focuses on the issue of the integrated and joint application of multi-entity data related to power trading based on the trusted data space. First，it expounds the core importance of data in the intelligent applications of power trading. Second，it sorts out various types of data resources adopted by intelligent applications in existing research. Furthermore，it analyzes the types of cross-domain and cross-entity data that can be introduced to improve the level of intelligent applications. Subsequently，it proposes a solution for realizing secure and trusted sharing and application of multi-entity data based on the trusted data space，as well as the value and utility of the data space in data circulation. This research can provide a reference for the optimization and upgrading of intelligent applications in power trading and the efficient development of multi-entity collaboration.

Key words：power trading；trusted data space；data security；data sharing

0　引言

电力交易智能化应用的核心目标是实现交易策略优化、市场出清高效及多主体利益均衡，而数据作为智能化应用的“血液”，贯穿于应用构建与使用的全过程，其重要性主要体现在智能化应用构建的基础支撑[1]、应用优化的关键依据[2]、交易策略优化的核心驱动[3]等多个方面。

2024年12月，国家数据局等五部门发布《关于促进企业数据资源开发利用的意见》，鼓励企业采用数据空间、区块链、隐私计算、匿名化等技术模式，以促进数据的安全流动和高效开发利用[4]。

电力企业通过采用国家数据局鼓励的技术路线，不仅可以促进数据资源汇聚与高效流通，还能保障跨利益主体的数据要素化治理，实现安全、高效、标准化、大规模、多场景复用的数据流通[5]，提升电力交易智能化应用的质量。

1　现有应用使用的数据类型

现有电力交易相关智能化应用已采用多种数据支

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

撑决策，但数据类型仍集中于传统交易数据、物理运行数据及部分市场环境数据，具体可分为以下 3 类。

1.1 电力系统物理运行数据

此类数据直接反映电力系统的运行状态，是交易智能化应用的基础数据，主要包括：发电侧数据（火电机组发电成本数据、水电机组出力数据[2]、风光新能源出力预测数据[3]、储能充放电功率与荷电状态数据[6]）、输电与配电侧数据（输电阻塞数据[1]、节点电压数据、配电网运行约束数据[6]）、负荷侧数据（用户负荷预测数据[1]、可控负荷中断容量数据[6]、柔性负荷响应特性数据[3]）。

1.2 电力市场交易数据

此类数据记录电力市场的交易过程与结果，为智能化应用分析市场规律提供依据，主要包括：电价数据（日前市场电价、实时市场电价[1]、节点边际电价[1]、中长期合约电价[2]）、交易量数据（发电商中标电量[2]、用户购电量[3]、虚拟电厂交易电量[6]）、市场规则数据（合约偏差考核标准[2]、辅助服务定价规则[3]、碳交易机制参数[2]）。

1.3 外部环境影响数据

此类数据反映电力市场运行的外部约束条件，为智能化应用引入不确定性因素提供支撑，主要包括：能源价格数据（煤炭价格、天然气价格[1]、绿证价格[2]）、气候环境数据（风速数据、光照强度数据[3]、气温数据[1]）、政策法规数据（碳配额分配数据[2]、新能源补贴政策数据[3]、电力市场改革政策数据）。

2 实现智能化应用优化可引入的多主体数据

为进一步提升复杂电力市场环境下数据对智能化应用优化的支撑，可考虑引入以下 3 类多主体数据，进一步挖掘市场规律与多主体协同潜力。

2.1 多主体互动行为数据

电力交易的多主体特性（发电商、用户、虚拟电厂、配电网运营商等）要求智能化应用充分考虑主体间的互动关系，而现有数据多聚焦于单一主体行为，缺乏互动行为数据支撑。可考虑引入的多主体数据有：主体间合约签订数据[2]、协同调度响应数据[3]、利益分配数据[2]等。此类数据可帮助应用准确刻画多主体间的合作与竞争关系，优化协同交易策略，提升智能化应用的质量。

2.2 不确定性量化数据

电力市场的不确定性（风光出力波动、负荷突变、电价随机波动等）是影响智能化应用决策效果的关键因素，现有数据多为确定性预测数据，缺乏不确定性量化信息。可考虑引入的多主体数据有：概率性预测数据（风光出力概率分布数据[3]、负荷突变概率数据）、不确定性影响程度数据（电价波动方差数据[1]、出力预测误差分布数据[2]）、风险评估数据（合约偏差风险数据[2]、市场力滥用风险数据[1]）。通过此类数据，可进一步量化不确定性对交易结果的影响，引入风险控制机制[3]，提升决策的稳健性。

2.3 跨领域关联数据

电力市场与能源市场、碳市场的关联性日益增强，现有智能化应用对跨领域数据的应用不足，限制了多目标优化效果。可考虑引入的多主体数据有：能源市场关联数据（石油价格数据、天然气期货价格数据[1]）、碳市场数据（碳配额成交量数据、碳排放强度监测数据[2]）等。通过跨领域数据的融合分析，应用可实现电力交易与其他市场的协同优化，提升多目标决策效果。

3 可信数据空间在多主体数据流通共享中的价值

3.1 可信数据空间的产生背景与定位

随着大数据以及人工智能等新兴信息技术的快速发展，数据已成为现代经济体系中的核心战略资源，是推动技术革新、市场需求挖掘和效率提升的重要动力。在电力行业数字化转型背景下，数据的广泛应用贯穿发电、输配电、用电及储能等各环节，覆盖运行、管理、服务等多个维度。

然而，数据在实现其价值的过程中仍面临着诸多挑战。数据的非竞争性决定了同一组数据可以同时被多个企业使用，新增的数据使用者不会减少现存使用者的效用。数据的非排他性意味着数据一经公开，则最初持有者无法排除他人对该数据的使用。数据的非消耗性表明了数据不会因为使用而发生损耗[7]。对于数据这样一种无形的、有价值的生产要素，需要一种有效的方法和工具保证其自身的安全和使用的合规，避免数据泄露、违规滥用等事件的发生，打破不同主体之间的数据孤岛现象，化解数据难以共享和协同的难题，助力数据价值的最大化。

3.1.1 可信数据空间与数据中台的定位

传统的数据中台虽然在数据治理和数据归集方面做了大量的工作，但是并不能承担多主体数据在安全可信环境下的融合共享任务。在此背景下，国家数据局提出可信数据空间技术路线。可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施[8]。可信数据空间通过可信管控能力、资源交互能力和价值共创能力实现多主

体数据的协同，其与数据中台各有侧重，互为补充。数据中台作为资源层，其数据归属于单一主体，是一个集中的资源池与核心节点。可信数据空间的数据归属于多主体，各类数据中心与各方数据在其中融合，实现安全流通。基于此，可信数据空间的架构定位是内部跨主体数据合规共享的基础设施，是与外部生态数据资源交互的核心枢纽。

3.1.2 可信数据空间与数据元件的协同

数据元件作为国家数据流通利用基础设施的技术路线之一，可以通过将数据资源加工成标准化、高价值、可复用、形态稳定的数据初级产品，实现“数据可用不可见”，具有安全属性、价值属性、品质属性，可破解确权、估值、定价和安全风险难题，并作为标准化的流通标的物保障数据安全、高效、大规模流通[5]。

电力数据的跨主体协同与流通，通常需先对原始数据进行脱敏和标准化加工，然后再将加工后的数据登记至可信数据空间，实现流通共享。数据元件技术路线可以很好地实现电力原始数据加工和脱敏，为可信数据空间提供优质的标准化数源。

3.2 可信数据空间在多主体协同中的技术先进性

可信数据空间通过多种技术手段的组合保障数据在多主体协同中的安全、可信、融合与共享，包括全链路安全防护体系、智能合规监管引擎、分布式可信身份认证及多维度使用控制技术。

3.2.1 全链路安全防护体系

可信数据空间从数据接入、数据开发、数据交付的全链路进行安全防护。可信数据空间在数据接入环节具备多源异构兼容与安全准入特性，支持结构化、非结构化、流式等全类型数据跨系统接入，通过脱敏预处理与身份核验确保数据安全进入；数据开发环节以数据元件安全加工与审核、隐私计算等技术为手段，结合动态规则管控确保开发过程合规可控，同时提供标准化工具提升开发效率；数据交付环节则通过使用规则控制、加密传输与全链路存证，确保数据结果按需交付、全程可追溯，且交付后仍能对数据使用范围进行动态管控，形成“接入安全、开发合规、交付可控”的全流程闭环特性。

3.2.2 智能合规监管引擎

通过集成自然语言处理与知识图谱技术的人工智能大模型，可自动解析法律法规（如《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》）及行业规范，动态生成合规算子并构建空间策略库。引擎能深度理解法律条文的语义和逻辑，将抽象的法律条款转化为具体、可执行的合规算子，涵盖数据收集、存储、使用、传输等各个环节。空间策略库会随着法律法规的更新实时更新，确保合规监管的时效性与准确性。通过字段级细粒度管控，对数据流通全流程进行实时监测，一旦发现违规行为，立即发出预警并进行实时拦截。可适配不同行业的差异化合规场景进行进一步的合规保障。人工智能驱动的合规监管引擎可大幅减少人工介入合规检查的工作量，降低人工合规成本，同时提高合规监管的效率和准确性，让数据在流通中始终保持合规状态。

3.2.3 分布式可信身份认证

基于分布式身份认证（DID）机制，为可信数据空间内所有参与主体（数据提供方、使用方、服务方等）构建自主安全、跨域互认的数字身份体系。其身份信息（如资质、权限、交互记录）上链存证，不可篡改。该机制支持跨可信数据空间、跨主体的身份互通，通过标准化协议实现一次身份多场景复用，所有操作行为均可通过 DID 溯源至责任主体。这种“自主管理、跨域互认、全程可溯”的特性，从根源上解决了传统身份体系中信任依赖单一机构、跨域协同效率低、责任认定难等问题，为可信数据空间多主体可信交互筑牢身份信任基石。

3.2.4 多维度使用控制技术

可信数据空间在数据使用控制上构建了多维度精细化管控体系，围绕行为、主体、地点、时间、用量等形成全场景约束：针对下载、查看、计算、传输等不同操作行为，预设差异化管控规则（如禁止核心数据下载等）；结合使用地点（如限定仅在办公区域或可信网络环境内访问）、时间范围（如工作日 8：00 ~ 18：00 开放权限）及用量阈值（如单次查询不超过 100 条、单日计算上限 50 次）动态调整管控强度，一旦触发异常，系统自动阻断操作并生成审计日志。这种“行为有边界、主体有分级、时空有约束、用量有上限”的多维度协同控制，确保数据使用全程可控、合规可溯，在释放数据价值的同时筑牢安全防线。

4 基于可信数据空间的电力交易试点场景建设实践

本文以某大型发电集团基于可信数据空间开展电厂辅助电力交易试点的实践为例，进行详细说明。

4.1 可信数据空间各参与主体的角色分工

数据提供方 1：电力交易中心。目前各电力交易中心主要通过公开网站开放数据，部分交易中心通过接口方式开放数据。但从电厂的视角看，开放数据的

质量和范围都不能达到预期。为了更好地服务参与电力交易的电厂，电力交易中心将电厂所需的因安全和隐私原因未公开开放的数据整理后以数据目录的形式登记在数据空间。

数据提供方 2：气象数据服务商。将可付费提供的气象数据以数据目录的形式登记在数据空间中。

数据提供方 3：参与电力交易的电厂。电厂自有发电数据通过空间连接器与数据空间实现安全传输，与其他数据源在数据空间通过数据隔离、隐私计算实现可用不可见的联合建模。

数据运营方：发电集团下属的数字化科技公司。依照数据空间的管理办法，承担空间各参与主体的身份认证、数据目录登记、数据产品上架、数据服务调用的审批与核实工作。

数据开发方：可信数据空间产品与服务公司。通过将电力行业的领域知识与多主体数据合规使用的领域知识相结合，将应用开发的成果体现在数据价值的增值中。在数据空间上架的数据产品收入中获得应得的一部分收益[7]。

数据使用方：参与电力交易的电厂。对数据空间内联合建模的结果进行使用，辅助电力交易提质增效。

4.2 数据安全与隐私保护机制

可信数据空间通过全流程的数据安全保障与可信管控，实现多主体数据“可用不可见”的融合开发。图 1 描述了数据在可信数据空间内全生命周期的安全与隐私保护过程。数据提供方在可信数据空间中登记注册的数据目录仅存储元数据，以及用于开发测试目的的脱敏样本数据（节点 1）。数据提供方和数据运营方根据数据使用方的使用场景进行数据使用授权（节点 2）。

在可信数据空间中，开发环境与生产环境相互隔离，数据开发方基于样本数据进行数据产品开发（节点 3）。数据产品发布前，内置的安全算子会进行数据授权检查和代码检查并给出风险告警（节点 4）。数据运营方与数据提供方确认安全合规后数据产品才会在可信数据空间发布。

在数据使用方使用数据产品或服务时才会将依场景授权的真实数据通过五层加密通道加载到内存计算专区（节点 5），安全计算后销毁供方真实数据，需方仅获得结果数据（节点 6）。在更高的安全要求下，可以使用隐私计算环境或基于国产硬件支持的可信执行环境来进一步提升安全水位线（节点 7）。

可信数据空间使用安全网关实时依照安全策略中心的设定进行访问控制，并使用区块链智能合约进行全过程存证，包括申请存证、授权存证、使用存证等（节点 8）。安全策略中心内置了依据安全合规相关法律条例及规章制度实现的安全算子，通过安全网关进行实时告警与拦截（节点 9）。

4.3 部署实践与效果体现

发电企业、电网企业、供电企业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区。在生产控制大区与管理信息大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置[9]。现有数据按照电力行业的要求分布在被横向隔离、纵向认证的不同网络安全区内，如图 2 所示。

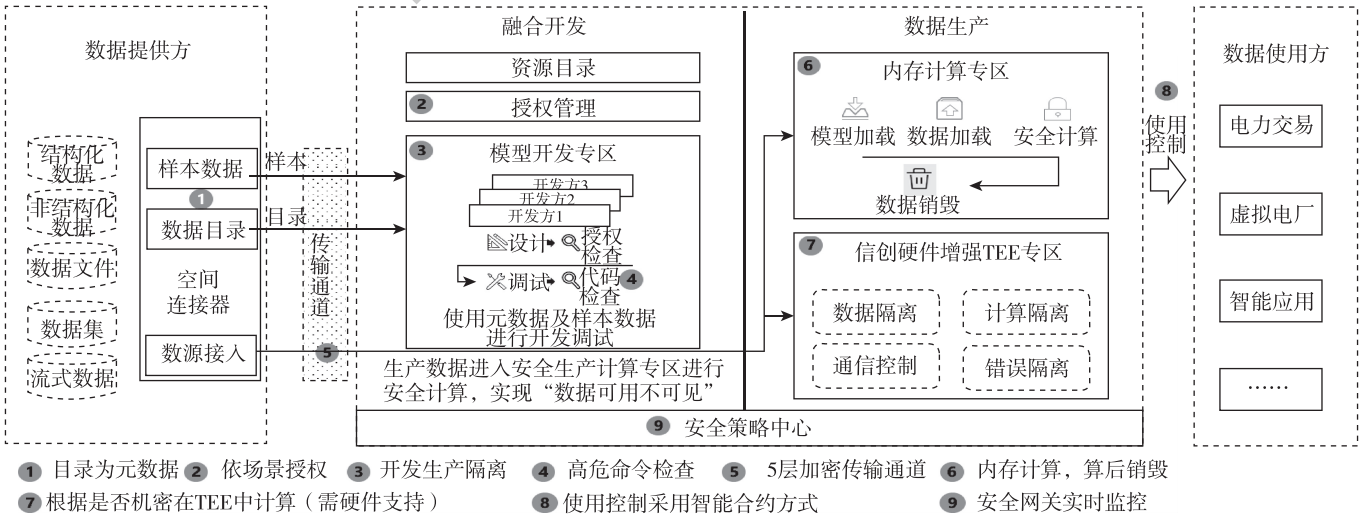

图 1　数据空间的数据安全与隐私保护机制

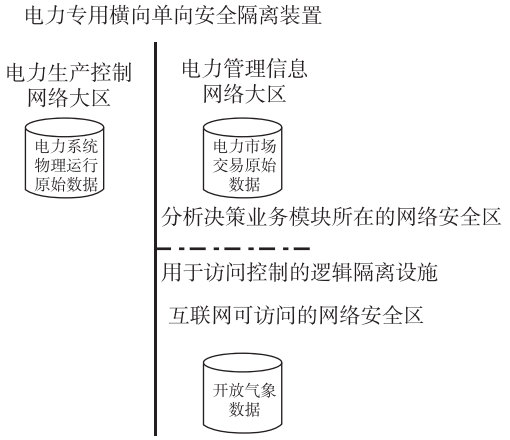

图 2　电力网络隔离装置

综合考虑现有数据和智能应用优化可引入的多主体数据的分布情况，一种相对较优的部署原则如图 3 所示。

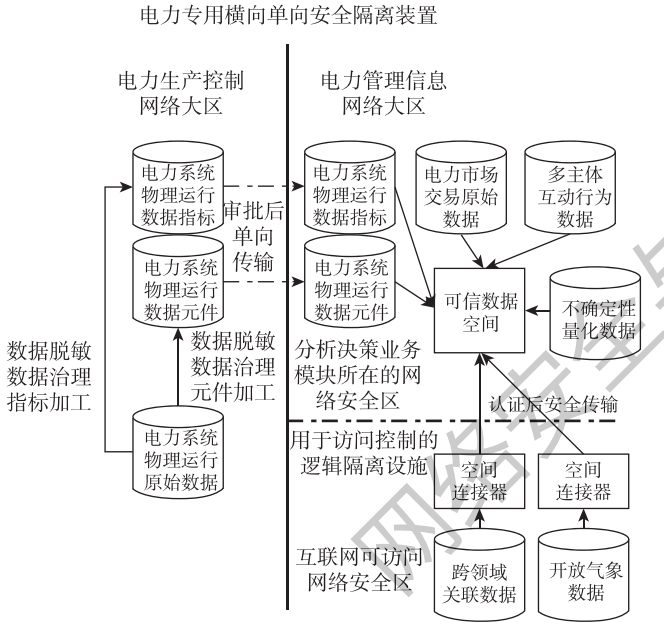

图 3　可信数据空间与多主体数据部署图

在实践中需要基于部署原则，结合业务现状与业务需求进行细化和微调。目前该发电集团已经接入电力生产、技术管理、设备资产、售电管理、运营管理、客户营销、电力营销、电力交易、碳排放、绿证交易等多类数据资源开展电力数据产品融合共享，具备智能化应用优化所需的多主体数据源，更多数据资源的引入与应用优化的开展同步进行。

通过构建“数据元件 + 数据空间”的联合技术路径，实现了多主体数据在隔离状态下的安全合规融合与共享，该方案既落实了国家发展改革委关于电力安防的相关规定，也契合了国家数据局推动数据资源开发利用的指导意见，为电力行业智能化应用的优化提供了数字化基础设施。

5　结论

基于可信数据空间的多主体数据应用试点为电力交易智能化应用优化提供了一种可能的新路径，本文的主要创新体现在：

（1）首次将可信数据空间系统性引入电力交易多主体协同场景，使得在数据赋能下的电力交易变得更加智能化和自动化。

（2）提出“数据元件 + 数据空间”的联合技术路径，两条技术路线优势互补，使得电力数据从源端到应用端实现了端到端的安全与共享保障。

（3）提出适用于电力行业的空间连接器研究方向、多主体安全共享和授权机制。

以下两个方向值得进一步开展研究：

（1）符合电力行业特点的接入连接器

为了确保电力系统的稳定运行，电力行业的网络依据不同的安全要求进行分区隔离管控。如生产控制大区和管理信息大区之间通过安全隔离装置进行隔离。管理信息大区根据各企业不同的安全要求划分安全区。互联网业务系统所在的安全区通过逻辑隔离设施与互联网进行有限的安全网络连接[9]。

可信数据空间作为国家数据基础设施中的一种业务节点，接入连接器应按照技术规范的要求向行业功能节点报送运行和业务信息[10]。未来可专项研究基于现有电力行业网络条件，业务节点向电力行业功能节点进行运行情况报送的安全实现方法。

（2）跨域跨主体的可信数据空间互联互通

以智能化应用为导向，发电行业数据空间和电网企业数据空间以及其他跨行业数据空间实现互联互通，通过空间连接器接入众多微电网主体和高耗能企业，实现数据安全可信共享、数据空间资源交互、数据价值融合共创。跨域跨主体的数据融合产生跨域的大规模应用，基于数据空间的共识规则和可信管控能力，实现多方主体数据共享的大规模智能化应用落地。

参考文献

[1] 张金良. 电力市场环境下的短期电价混合预测模型研究[D]. 北京：华北电力大学，2011.

[2] 李咸善，胡家旗，张远航，等. 风光水储联合体多时间尺度市场化运营调度策略[J]. 中国电机工程学报，2025，45（2）：8879－8893.

[3] 彭道刚，税纪钧，王丹豪，等. “双碳”背景下虚拟电厂研究综述[J]. 发电技术，2023，44（5）：602－615.

[4] 国家数据局，中央网络安全和信息化委员会办公室，工业和信息化部，等. 关于促进企业数据资源开发利用的意见[EB/

OL]. (2024 - 12 - 20). https://www. gov. cn/zhengce/zhengceku/ 202412/content_6994570. htm.
[5] 陆志鹏. 国家数据基础设施技术路线的探索、研究与展望[J]. 中国计算机学会通讯, 2025, 21 (4): 15 - 21.
[6] 董雷, 涂淑琴, 李烨, 等. 基于元模型优化算法的主从博弈多虚拟电厂动态定价和能量管理[J]. 电网技术, 2020, 44 (3): 973 - 983.
[7] 申卫星, 陆志鹏. 数据产权论[M]. 北京: 商务印书馆, 2024.
[8] 国家数据局. 可信数据空间发展行动计划 (2024—2028年) [EB/OL]. (2024 - 11 - 21). https://www. gov. cn/zhengce/zhengceku/202411/content_6996363. htm.
[9] 国家发展和改革委员会. 电力监控系统安全防护规定[EB/OL]. (2024 - 11 - 25) [2025 - 12 - 09]. https://zfxxgk. ndrc. gov. cn/web/iteminfo. jsp? id = 20457.
[10] 全国数据标准化技术委员会. TC609 - 6 - 2025 - 12 数据基础设施 接入管理[S]. 北京: 全国数据标准化技术委员会, 2025.

(收稿日期: 2025 - 12 - 09)

作者简介:

国丽 (1975 -), 女, 正高级工程师, 主要研究方向: 数据治理、数据安全、数据元件、可信数据空间。

朱永春 (1981 -), 通信作者, 男, 硕士, 主要研究方向: 可信数据空间、隐私计算、区块链。E-mail: zhuyongchun@cecdt. com. cn。

丁浩 (1988 -), 男, 硕士, 工程师, 主要研究方向: 数据治理、数字化转型、人工智能。

“工业互联网安全技术研究”主题专栏征稿启事

工业互联网作为新一代信息技术与制造业深度融合的产物, 是推动产业数字化转型、实现经济高质量发展的关键基础设施。然而, 随着其广泛部署与深度应用, 网络攻击手段不断演进, 安全风险日益凸显。工业互联网安全不仅关乎生产系统的稳定运行, 更影响着关键基础设施的安全底线与数字经济的健康发展。为集中展示我国在工业互联网安全领域的最新理论研究成果、核心技术突破与创新应用实践, 推动构建自主、安全、可靠的工业互联网安全保障体系, 本刊拟在2026年第6期推出“工业互联网安全技术研究”主题专栏, 现面向国内外广大专家学者、科研人员及行业工程师公开征稿。

一、征文主题: 工业互联网安全技术研究

包括但不限于以下学术方向:

1. 工业互联网安全参考架构与标准体系;
2. 工控协议深度分析与安全加固;
3. 工业入侵检测与威胁感知;
4. 数据安全与隐私保护;
5. 工业智能体安全;
6. 5G + MEC 环境下的工业安全;
7. 供应链安全 (第三方组件、软件库、开源工具的安全管控);
8. 人工智能/机器学习用于攻击检测与防御;
9. 区块链技术在工业数据完整性、溯源方面的应用。

二、投稿要求

1. 稿件请用 word 格式录入, 并套用本刊投稿模板。模板下载网址: http://files. chinaaet. com/files/Periodical/pcachina_Templates. doc

2. 投稿文章须未在其他期刊或者出版正式论文集的会议上刊登过, 且不在其他刊物或会议的审稿过程中, 不存在一稿多投现象。

3. 保证文章的合法性 (无抄袭、剽窃、侵权、虚假引用等不良学术行为), 且不违反相关法律法规, 不涉及国家、企业秘密, 稿件文责自负。

4. 论文要求观点鲜明、逻辑严谨、论据充分、方法合理, 字数在5000 ~ 8000字。

5. 请在官方投稿网站 (http://www. pcachina. com) 注册、投稿。注册后请投稿在“主题专栏”栏目, “稿件标题”请填“工业互联网 + 文章题目”。稿件经评审合格录用后, 在《网络安全与数据治理》2026年第6期 (正刊) 以主题专栏形式发表。

三、专栏主编

洪晟, 北京航空航天大学副教授, 博士生导师, 北京市安全学科带头人, 北京市科委技术专家, 北京航空航天大学“青年拔尖人才”。主持和参与973/863课题、国家重点研发课题、技术基础课题、国家自然科学基金等课题30余项; 担任国内外多个期刊和会议的编委, 发表论文70余篇, 其中SCI检索30余篇, 全球前1% ESI高被引论文1篇; 授权国家发明专利20项, 获国防科技进步一等奖1项, 北京市科学技术进步二等奖1项。

四、时间安排

截稿日期: 2026年4月30日
审稿反馈日期: 2026年5月15日
出版日期: 2026年6月15日

《网络安全与数据治理》编辑部
2026年3月