电力系统自动化中云平台的资源调度与数据安全防护策略

许凯凯

河南灿迪电力科技有限公司，河南许昌，461111；

摘要：随着信息技术的飞速发展和电力行业的数字化转型，电力系统自动化已成为提升电网运行效率、保障供电稳定性的关键手段。云平台作为支撑电力系统自动化的重要基础设施，其资源调度与数据安全防护策略的制定与实施显得尤为重要。本文旨在探讨电力系统自动化中云平台的资源调度策略，分析数据安全防护的关键技术，并提出两者协同工作的有效策略，以期为电力行业的信息化建设提供有益参考。

关键词：电力系统；自动化中云平台；资源调度；数据安全防护策略

DOI：10.64216/3080-1508.25.08.024

引言

在当前的电力系统中，自动化技术的应用日益广泛，不仅提高了电网的运行效率，还显著增强了供电的稳定性和可靠性。云平台作为这一过程中的核心支撑，承载着大量的数据处理和存储任务，其重要性不言而喻。然而，随着云平台在电力系统中的深入应用，资源调度与数据安全防护问题也逐渐凸显出来。资源调度不当可能导致系统性能下降，而数据安全防护不足则可能引发信息泄露等严重后果。

1 资源调度与数据安全防护在电力系统自动化中的重要性

在电力系统自动化向智能化转型的过程中，云平台凭借其强大的算力、弹性的存储能力与高效的资源共享特性，已成为整合海量监测数据、支撑调度决策、实现设备协同控制的核心载体。而资源调度与数据安全防护，正是保障云平台稳定、高效、可靠运行的两大支柱，直接关系到电力系统自动化的整体效能。

资源调度的合理性决定了云平台的运行效率与服务质量。电力系统自动化云平台承载着SCADA数据采集、负荷预测、故障诊断、电网仿真等多样化任务，不同任务对计算资源、存储资源、网络资源的需求差异显著，例如电网仿真任务需大量算力支撑，而历史数据存储任务则对存储空间要求较高。科学的资源调度能根据任务优先级与资源需求，实现资源的动态分配与优化配置，避免资源闲置或过载，确保各类自动化任务高效推进，从而保障电力系统运行监测的实时性与调度决策的及时性。

数据安全防护则是云平台运行的底线保障。电力系统自动化云平台存储与处理的数据涵盖电网运行参数、设备状态信息、用户用电数据等核心敏感数据，这些数据不仅关系到电力系统的安全稳定运行，还涉及国家能源安全与用户隐私。一旦发生数据泄露、篡改或丢失，可能导致调度决策失误、设备故障失控，甚至引发大面积停电等严重事故。因此，完善的数据安全防护体系能有效抵御各类网络攻击与安全威胁，保障数据的机密性、完整性与可用性，为电力系统自动化业务的开展筑牢安全屏障。

2 资源调度策略

2.1 基于启发式算法的资源调度

基于启发式算法的资源调度是应对电力系统自动化云平台资源分配问题的有效手段，其核心是通过模拟自然规律或优化逻辑的算法，快速寻找近优的资源分配方案。常用的启发式算法包括遗传算法、粒子群优化算法、蚁群算法等，这类算法无需遍历所有可能的解，能在复杂的资源约束条件下高效收敛到较优解。在电力系统自动化云平台中，可将资源调度问题转化为“在满足任务截止时间、资源容量等约束条件下，最小化资源闲置率与任务延迟率”的优化问题，通过启发式算法进行求解。例如，采用遗传算法时，将资源分配方案编码为染色体，以资源利用率与任务完成效率为适应度函数，通过选择、交叉、变异等操作迭代优化，最终得到最优的资源分配方案。启发式算法尤其适用于处理多约束、多目标的资源调度问题，能根据电力系统任务的动态变化快速调整资源分配，平衡不同任务的资源需求，有效缓解资源分配不均的问题，提升资源利用的合理性。

2.2 基于人工智能的资源调度

基于人工智能的资源调度通过机器学习与深度学

习技术，实现资源调度的智能化与自适应，更贴合电力系统自动化任务的动态特性。该策略首先利用历史运行数据（如任务类型、资源需求、调度效果等）训练调度模型，使模型能学习不同任务与资源分配之间的映射关系。在实际调度中，模型可根据实时任务特征（如任务优先级、资源需求预测）与云平台资源状态（如 CPU 利用率、内存占用率），自动生成最优调度方案。例如，采用 LSTM 神经网络预测未来一段时间内的任务量与资源需求，为提前调度资源提供依据；利用强化学习算法，将资源调度过程视为智能体与环境的交互过程，通过试错学习不断优化调度策略，提高对突发任务（如故障诊断）的响应速度。此外，基于人工智能的资源调度还能实现跨模块资源协同共享，通过分析各业务模块的资源使用规律，将闲置资源动态调配给需求模块，打破资源壁垒，大幅提升资源利用率。同时，该策略具备自优化能力，可根据调度效果实时调整模型参数，适应电力系统运行状态的变化。

2.3 评价指标体系构建

构建科学的评价指标体系是客观衡量资源调度效果的基础，需围绕“效率、公平、可靠”三个核心维度设计指标。效率维度指标用于评估资源利用与任务处理的效率，包括资源利用率（CPU 利用率、内存利用率、存储利用率的平均值）、任务完成率（按时完成的任务数量占总任务数量的比例）、任务延迟率（超出截止时间的任务数量占总任务数量的比例）以及资源周转率（单位时间内资源的分配与释放次数）。公平维度指标用于衡量资源分配的均衡性，包括资源分配方差（各模块资源占用量与平均占用量的偏差平方和）、优先级匹配度（关键任务获得优质资源的比例）。可靠维度指标用于评估调度策略的稳定性，包括调度成功率（成功执行的调度指令占总指令的比例）、故障恢复时间（资源调度系统出现故障后恢复正常运行的时间）。这些指标相互关联、相互补充，全面覆盖资源调度的核心环节，为效果评估提供量化依据。

3 数据安全防护策略

3.1 访问控制策略

访问控制策略是防范数据泄露与篡改的第一道防线，核心是实现“最小权限”与“按需授权”。首先，建立基于角色的访问控制（RBAC）体系，根据用户的岗位与职责划分不同角色（如运维人员、调度人员、审计人员），为每个角色分配明确的访问权限，确保用户仅能访问与其工作相关的数据，例如调度人员可访问负荷预测数据，但无法修改设备状态数据。其次，引入多因素认证机制，除了账号密码，还需通过短信验证码、指纹识别、USB 密钥等额外认证方式验证用户身份，防止账号被盗用后非法访问数据。此外，实施动态权限调整，根据用户的实时工作需求临时授予权限，任务完成后立即收回，减少权限滥用风险。同时，对特殊敏感数据（如电网拓扑结构、调度指令）设置多级审批流程，用户需经过上级审批同意后方可访问，进一步强化权限管控。通过严格的访问控制，从源头限制非法数据访问，降低数据泄露与篡改的风险。

3.2 加密技术与安全审计

加密技术与安全审计是保障数据安全的核心技术手段，分别从“防护”与“追溯”两个层面构建安全屏障。在加密技术应用方面，采用“全生命周期加密”策略：数据存储时，对数据库中的敏感数据采用对称加密或非对称加密技术进行加密存储，防止数据被非法读取；数据传输时，通过 SSL/TLS 协议对传输链路进行加密，避免数据在传输过程中被拦截篡改；数据共享时，采用数据脱敏技术，隐藏敏感字段（如用户身份证号、用电地址），或通过数字签名技术验证数据发送方身份与数据完整性，防止数据被篡改。在安全审计方面，建立全面的审计日志系统，记录所有用户的操作行为（如登录时间、访问数据、修改操作）、系统运行状态以及安全事件，审计日志需长期保存且不可篡改。同时，采用智能审计分析技术，对审计日志进行实时监测与异常分析，当发现频繁访问敏感数据、异常修改操作等可疑行为时，自动触发告警机制，通知安全管理人员及时处置。通过加密技术实现数据“不可泄、不可改”，通过安全审计实现“可追溯、可追责”，全方位保障数据安全。

3.3 安全性评价指标体系

安全性评价指标体系需围绕数据的“机密性、完整性、可用性”三大安全属性构建，全面反映防护策略的实施效果。机密性指标用于评估数据防泄露能力，包括未授权访问拦截率（被成功拦截的未授权访问尝试次数占总尝试次数的比例）、敏感数据加密率（已加密的敏感数据量占总敏感数据量的比例）、数据泄露事件发生率（发生数据泄露事件的次数与时长）。完整性指标用于评估数据防篡改能力，包括数据篡改检测率（被成功

检测到的篡改行为占总篡改行为的比例）、数据恢复成功率（被篡改数据成功恢复的比例）、数字签名验证通过率（通过数字签名验证的数据占总数据的比例）。可用性指标用于评估数据的可正常使用能力，包括数据服务中断时间（数据服务无法正常提供的累计时长）、安全事件响应时间（从发现安全事件到处置完成的时间）。这些指标从不同维度量化数据安全状态，为防护效果评估提供清晰的衡量标准。

4 电力系统自动化中云平台资源调度与数据安全防护的协同策略

4.1 资源调度与数据安全防护的相互关系

资源调度与数据安全防护并非独立存在，而是相互影响、相互制约的协同关系，共同决定云平台的整体运行效能。一方面，资源调度为数据安全防护提供支撑，完善的安全防护体系（如加密算法运行、安全审计分析）需要消耗大量的计算、存储资源，若资源调度不合理，安全防护模块因资源不足导致运行卡顿，会降低安全防护的响应速度与有效性；反之，科学的资源调度为安全防护模块优先分配资源，能确保加密、审计等安全机制高效运行，提升数据安全保障能力。另一方面，数据安全防护对资源调度具有约束作用，资源调度需在安全规则的框架内进行，例如调度资源时需考虑数据的敏感级别，为存储敏感数据的服务器分配更优质的安全资源（如专用加密芯片），避免因资源调度忽视安全需求而引发数据风险。此外，两者的协同能实现“效率与安全”的平衡，若仅追求资源调度效率而忽视安全，可能导致数据泄露；若过度强调安全而占用过多资源，会降低资源利用率。因此，必须建立两者的协同机制，实现资源利用效率与数据安全水平的同步提升。

4.2 协同策略设计

协同策略设计的核心是构建“安全感知-资源适配-动态调整”的闭环协同机制，实现资源调度与数据安全防护的深度融合。首先，建立安全与资源一体化感知模块，实时采集云平台的资源状态（CPU、内存利用率）与安全状态（安全事件类型、风险等级），通过数据融合技术分析两者的关联关系，例如识别出“某安全事件（如黑客攻击）导致某业务模块资源需求激增”的关联模式。其次，制定基于安全等级的资源适配规则，根据数据敏感级别与安全风险等级调整资源调度策略，例如为处理高敏感数据（如调度指令）的任务分配独立的加密计算资源，当发生高等级安全事件时，自动为安全防护模块（如入侵防御系统）优先调度资源，确保其快速响应。再次，实现动态协同调整，通过人工智能算法实时监测资源与安全状态的变化，当安全风险降低时，将闲置的安全资源调配给业务模块；当业务任务激增时，在保障基本安全需求的前提下，适当调整安全资源分配，提升业务运行效率。此外，建立协同决策平台，整合资源调度与安全防护的决策逻辑，当两者出现资源竞争时，通过平台综合评估任务优先级与安全风险，制定最优的协同方案，避免“效率与安全”顾此失彼。

4.3 协同策略的落地保障

为确保协同策略有效落地，需从技术、制度、人员三个层面构建保障体系。在技术层面，开发资源与安全协同管理接口，实现资源调度系统与安全防护系统的数据互通与指令交互，例如安全防护系统将安全事件信息实时推送至资源调度系统，资源调度系统根据信息调整资源分配；同时，部署协同监控可视化平台，直观展示资源状态、安全状态及协同调度效果，方便管理人员实时管控。在制度层面，制定协同管理规范，明确资源调度与安全防护部门的协同职责，规定协同

5 结语

总之，电力系统自动化中云平台的资源调度与数据安全防护是相互依存、相互促进的关键要素。科学的资源调度策略能确保资源的高效利用与任务的顺利执行，为数据安全提供坚实的物质基础；而完善的数据安全防护体系则能有效抵御外部威胁，保护数据资产不受侵害，为资源调度创造安全稳定的运行环境。

参考文献

[1]刘俊碧.电力系统运行中电气自动化技术的应用策略[J].通信电源技术，2020，37（2）：112-113.

[2]王辉.电力企业电气自动化技术的应用及创新[J].科技创新导报，2024，21（27）：120-122.

[3]孙宏斌，郭庆来，潘昭光，等.智能电网的控制中心技术：现状与展望[J].电力系统自动化，2023，47（2）：1-13.

[4]李海,王慧,李瑛,等.电气工程及其自动化技术下的电力系统自动化发展探讨[J].数字通信世界,2021(7):156-157.

[5]朱培燕.生产运行电力系统中电气自动化技术的应用研究[J].电子元器件与信息技术,2021,5(7):83-84.