

电力行业数据隐私保护技术研究与应用

毛舒扬

阳城国际发电有限责任公司

DOI:10.12238/etd.v6i3.14368

[摘要] 伴随着电力行业信息化水平的持续提升,该行业面临的重要难题是数据隐私保护,由于电力行业数据既敏感又复杂,所以要采取有效技术手段保障数据安全。基于此,本文说明了电力行业数据隐私保护的必需性,详细说明了数据加密、数据匿名化、数据访问控制和数据安全审计等核心技术,研讨了这些技术在电力系统、电力营销、电力设备维护等具体应用范畴的实践情况,通过深入剖析,本文旨在为电力行业的数据隐私保护工作提供参考与指引,以促进该行业的健康成长。

[关键词] 电力行业; 数据隐私保护; 数据加密; 数据匿名化; 数据安全审计

中图分类号: TM727 **文献标识码:** A

Research and application of data privacy protection technology in electric power industry

Shuyang Mao

Yangcheng International Power Generation Co., LTD.

[Abstract] As the informatization level of the power industry continues to rise, a key challenge is data privacy protection. Given the sensitivity and complexity of power industry data, it is essential to employ effective technical measures to ensure data security. This article highlights the necessity of data privacy protection in the power industry, detailing core technologies such as data encryption, data anonymization, data access control, and data security auditing. It also examines the practical applications of these technologies in specific areas like power systems, power marketing, and power equipment maintenance. Through an in-depth analysis, this article aims to provide guidance and references for data privacy protection efforts in the power industry, promoting its healthy development.

[Key words] electric power industry; data privacy protection; data encryption; data anonymization; data security audit

引言

在数字化转型的浪潮中,电力行业作为国家关键基础设施的重要组成部分,其数据安全和隐私保护问题日益凸显。电力行业不仅涉及庞大的用户信息,还包含关键的运营数据,一旦泄露,后果不堪设想。

1 电力行业数据隐私保护的必要性

面对数字化转型的滚滚浪潮,在电力行业里,要保障企业安全运营与社会稳定供电,数据隐私保护是关键一环。在类似大唐集团这样的发电企业,抑或是国家电网的生产运营进程中,从电力设备运转的相关数据、核心技术的参数等,均牵扯到大量敏感数据。若这些数据出现泄露,也许会造成企业核心技术外溢、商业机密暴露,危及企业市场竞争地位及长期发展策略,也可能因用户用电数据的外漏,引发个人隐私的安全危机,危及企业信誉和公众信任根基,电力系统为国家关键基础设施范畴,其数据安全与国家安全、民生稳定息息相关,如果数据被蓄意篡改或窃取,

说不定会引发电力供应中断,造成极大经济损失且破坏社会秩序,伴随《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》等法律法规不断完善,对于电力行业而言,切实落实数据隐私保护是履行社会责任、规避法律风险、实现合规运营的必然需要。

2 电力行业数据隐私保护技术研究

2.1 数据加密技术

电力行业数据涵盖发电设备运行、电力交易及电费结算等核心信息,一旦泄露将引发严重安全风险。在数据传输环节,SSL/TLS加密协议为电力数据打造“隐形防护罩”,通过双向身份认证与端到端加密,保障发电设备运行数据、电力交易指令及电费结算信息在电网与用户端、电厂与调度中心之间传输时,即便被截取也无法被破解,杜绝数据泄露与篡改风险。面对静态存储的海量数据,AES高级加密标准构建起坚固“数字保险箱”,无论是电网侧用户用电行为数据,还是发电企业的设备维护记

录,经加密存储后,能有效抵御非法入侵与恶意篡改,确保电力行业全链条数据从动态传输到静态存储的全生命周期隐私安全。

2.2数据匿名化技术

在电力行业中,用户用电数据等包含大量个人信息,保护其隐私至关重要。数据匿名化技术通过去除或变换可识别个人身份信息,在保障数据可用性的同时守护隐私。数据脱敏是常用的匿名化手段。对于数据集中姓名、身份证号、手机号等敏感信息,可采用随机化、替换、扰动等技术处理。随机化以预定义规则生成的随机或虚值替换原始数据,切断与可识别信息的联系;替换使用掩码值隐藏原始数据,保留数据格式特征;扰动则通过添加随机噪声,增强对敏感信息的保护。

2.3数据访问控制技术

在电力企业中,数据访问控制技术是保障数据隐私安全的核心防线。通过精细化权限管理,严格限制数据访问与操作权限,确保仅授权用户能够接触相关数据。基于员工岗位职责与业务需求,企业构建差异化权限体系:设备运维人员仅能获取设备状态监测、维护相关数据;财务人员仅可访问财务数据,从根源上杜绝跨部门数据违规访问行为。面对远程监控场景,多重身份认证机制成为数据安全的“守门人”。通过生物特征识别、动态密码验证等技术,精准核验访问者身份,仅授权的外部运维或管理人员可通过加密安全通道接入电力系统,有效抵御外部非法入侵。

2.4数据安全审计技术

在电力行业数据隐私保护体系中,数据安全审计技术通过对数据全生命周期的动态监控与回溯分析,构建起主动防御与事后追责的双重防线。技术通过深度解析电力系统网络数据流,运用行为分析模型精准识别异常访问模式,如非授权IP地址的高频次试探、短时间内大规模数据批量下载等可疑行为,一旦触发预设风险阈值,系统将立即启动阻断机制并生成预警,实现对潜在数据泄露风险的毫秒级响应。合规性审查层面,审计技术持续比对数据处理操作与国家《中华人民共和国数据安全法》、行业标准及企业内部规范,确保电力生产、调度、运维等核心数据在采集、存储、共享等环节的合法合规。审计日志不仅完整记录数据操作的时间、主体、对象及操作类型,还通过哈希校验等技术保障日志不可篡改,为司法取证和责任追溯提供可靠依据。在数据安全事件应急处置中,审计记录作为关键证据链,可帮助安全团队快速定位数据泄露源头,量化影响范围,进而制定包含系统隔离、数据恢复、漏洞修复的闭环处置方案。面对勒索软件攻击、APT渗透等新型威胁,融合人工智能与机器学习的审计系统正逐步实现威胁的自动化识别与自适应防护,通过持续学习历史攻击模式,提升对未知风险的预判能力,为电力行业数据隐私筑牢智能防护屏障。

3 电力行业数据隐私保护技术应用

3.1数据隐私保护技术在电力系统中的应用

3.1.1电力调度自动化系统

在电力行业,数据隐私保护技术深度融入电网运行与管理的各个环节。电费结算作为关键场景,采用安全多方计算技术,使供电企业、用户、金融机构等多方在无需暴露原始数据的情况下协同完成电费清算,确保资金流向与用户用电金额等敏感信息不被第三方获取。区块链技术则为电费结算数据构建分布式账本,每一笔交易都经加密与共识机制验证,既保障数据不可篡改,又实现各参与方间的隐私隔离。在电力调度与运行层面,数据加密贯穿始终。传输阶段,调度指令、电网实时状态等数据借助SSL/TLS加密协议,以密文形式穿梭于网络,有效抵御传输过程中的窃听与篡改;存储环节,AES等高强度加密算法将电网拓扑结构、设备参数等核心数据层层保护,阻断非法访问途径。数据匿名化技术对用户用电数据进行脱敏处理,在满足电力调度分析需求的同时,保护用户个人隐私。

3.1.2电力市场交易系统

电力市场交易系统承载着海量敏感数据,数据隐私保护技术成为保障交易安全与市场秩序的核心防线。在数据传输环节,采用SSL/TLS加密协议,为实时交易订单、动态报价等信息在网络传输中构建安全通道;存储时启用AES加密算法,对交易历史数据、用户账户信息进行高强度加密,防止数据泄露风险。针对交易参与方的个人信息,运用数据匿名化技术进行脱敏处理,通过随机替换姓名、身份证号等关键信息,既保留数据可用性,又确保隐私安全。在权限管理方面,严格的数据访问控制机制限定不同岗位人员的操作范围,交易员仅能访问业务相关数据,财务人员仅可处理资金结算信息,有效防止跨部门数据泄露。此外,数据安全审计技术全程记录系统操作行为,定期审查数据使用合规性,一旦出现异常访问,可快速通过审计记录追溯问题源头,及时采取应对措施,全方位守护电力市场交易的数据安全与隐私边界。

3.2数据隐私保护技术在电力营销中的应用

3.2.1用电信息管理

在电力营销环节,数据隐私保护技术深度嵌入售电营销、用电信息管理与电费结算全流程。针对用户用电信息,数据匿名化技术通过动态掩码、泛化处理等手段,将敏感字段转化为不可识别的随机字符,既保留数据统计价值又规避身份泄露风险;数据加密技术则在数据传输时启用国密SM2/SM4算法与TLS1.3协议,保障采集终端与营销系统间数据传输的机密性,同时对存储在分布式数据库中的历史用电数据采用AES-256加密算法,配合动态加密技术实现密文状态下的合规分析。数据安全审计系统持续监控数据操作行为,利用AI异常检测模型识别异常访问与越权操作,自动触发预警并生成合规报告,从而全面筑牢电力营销领域的数据隐私保护防线。

3.2.2电费结算系统

在电费结算环节,数据隐私保护技术构建起全链条安全防护体系。针对企业或个人电费账单数据、缴费信息等高敏感内容,国密SM4对称加密算法与SM2非对称加密算法协同运作,在数据生成阶段即完成高强度加密,传输过程采用TLS1.3协议确保

数据不被窃取或篡改,存储时配合区块链分布式存储技术,通过哈希值锁定数据完整性,杜绝恶意篡改。数据匿名化技术对银行账号、纳税识别号等关键信息实施动态脱敏,采用泛化、掩码等策略替换原始数据,在保留结算必要字段的同时阻断身份溯源路径。基于ABAC(属性基访问控制)模型,系统根据财务人员、系统运维等不同角色的业务属性及操作场景,动态分配数据访问权限,例如仅授权特定岗位人员查看加密后的汇总数据,敏感字段需二次生物认证方可解密。

3.3 数据隐私保护技术在电力设备维护中的应用

3.3.1 设备状态监测

在电力设备维护场景中,数据隐私保护技术通过多重手段筑牢安全防线。数据加密技术贯穿设备数据全生命周期,在设备运行参数与监测数据的传输环节,SSL/TLS加密协议构建起安全通道,确保数据在远程传输时不被窃取或篡改;存储时,AES加密算法为设备历史运行数据提供高强度保护,防止数据泄露。数据访问控制技术依据运维人员的职责差异精准划分权限。基层运维人员仅能查看设备基础运行状态数据,而设备故障诊断等核心数据仅对具备资质的高级工程师开放,从源头杜绝敏感数据的不当外流。同时,数据安全审计技术24小时实时监控设备状态监测系统的访问行为,一旦发现非授权IP地址访问、高频异常查询等可疑操作,立即触发警报并阻断访问,实现主动防御。这些技术协同作用,为电力设备维护打造安全的数据环境,既保障设备状态监测与分析的高效开展,又维护各方数据隐私安全。

3.3.2 预测性维护

在电力设备预测性维护场景中,数据隐私保护技术是平衡数据价值挖掘与安全防护的关键。某发电企业在构建设备预测性维护体系时,综合运用多种技术手段筑牢数据安全防线:数据传输全程采用SSL/TLS加密协议,防止设备运行参数、预测模型数据在网络交互中被窃取;存储环节使用AES高级加密算法,对设备故障预测分析结果等核心数据进行加密处理,避免因存储介质泄露导致企业技术机密外流。在权限管理层面,基于最小权

限原则实施数据访问控制,仅赋予数据分析人员模型构建与分析所需的数据权限,运维管理人员需通过多级审批流程获取设备预测维护建议查看权限,有效隔绝非相关人员接触敏感数据。同时,部署数据安全审计系统,实时监控数据访问、修改等操作行为,自动识别异常登录、高频下载等可疑活动,并按周期生成合规审查报告。针对设备运行数据中的用户身份、地理位置等敏感信息,采用数据匿名化技术进行脱敏处理,在确保预测模型准确性的前提下,全方位保护设备数据隐私与企业商业秘密。

4 结束语

总之,处于信息化迅猛发展的如今,电力行业的数据隐私保护,已是不可忽视的重要课题,采用数据加密、数据匿名化、数据访问约束和数据安全审查等技术,可有效增进电力行业数据的安全性与隐私性。伴随技术的持续进步与应用的逐步深化,电力行业数据隐私保护技术将迈向更成熟阶段,为保障电力系统安全稳定运行、维护用户隐私权益发挥更重要意义。因此电力企业需一直关注、钻研新的数据保护技术,以应对逐步复杂的网络安全局势,助力电力行业实现可持续成长。

[参考文献]

- [1]程海涛,王泽昭,孙鸿博.电力行业无人机巡检数据安全风险与防范机制研究[J].河南电力,2025,(03):54-61.
- [2]杨劲怀,杨小娟,陈静.数据驱动的能源互联网下电力行业大数据管理与分析方法[J].电力设备管理,2025,(04):273-275.
- [3]王晓茹,郭耀宇,王泽璞.电力行业数据中心资源整合及桌面应用方案设计[J].工业控制计算机,2024,37(01):141-144.
- [4]姚明,李博,李绍宾,郑华祥.浅析隐私计算技术在电力行业的应用[J].电气技术与经济,2023,(05):64-66.
- [5]王蓓蓓,朱竞.电表数据隐私保护下的联邦学习行业电力负荷预测框架[J].电力系统自动化,2023,47(13):86-93.

作者简介:

毛舒扬(1990--),男,汉族,山西晋中人,本科,工程师,从事信息通信技术、网络安全。