能源企业网络安全风险识别与智能分析平台研究

郭雅楠
福州大学，福建 福州 350108

DOI:10.61369/EPTSM.2026050021

摘　　要： 伴随着能源企业信息化发展，能源企业面临的安全威胁越来越多。利用大数据以及人工智能技术开发能源企业网络安全风险识别及智能化分析系统，可以有效提升能源企业对于各种可能存在的安全隐患进行发现以及处置的能力。该系统应用多种分析方法，运用机器学习和深度学习的方法来分析网络流量、设备的状态以及用户的操作行为等信息，做到及时监测和告警。同时它也增强了能源企业自身抵御各种复杂安全威胁的能力并且给能源企业提供更加准确的安全建议。

关 键 词： 能源企业；网络安全；风险识别；智能分析；人工智能

Research on Cybersecurity Risk Identification and Intelligent Analysis Platform for Energy Enterprises

Guo Yanan
Fuzhou University, Fuzhou, Fujian 350108

Abstract: With the advancement of digital transformation in the energy sector, energy enterprises face an increasing number of security threats. By leveraging big data and artificial intelligence technologies to develop cybersecurity risk identification and intelligent analysis systems, these enterprises can significantly enhance their capability to detect and address potential security vulnerabilities. The system employs various analytical methods, utilizing machine learning and deep learning techniques to analyze network traffic, device status, and user behavior patterns, enabling real-time monitoring and alerts. Furthermore, it strengthens energy enterprises' resilience against complex security threats while providing more precise security recommendations.

Keywords: energy enterprises; cybersecurity; risk identification; intelligent analysis; artificial intelligence

引言

伴随着能源企业的发展以及信息化水平的提高，在给能源企业带来智能化优势的同时，也使能源企业面临前所未有的网络安全问题。传统的网络安全防护方法已不能满足不断出现的新类型网络攻击以及日益严峻的安全形势需求。能源企业内部的各种自动化系统、控制系统及重要信息等安全是保证电力生产和运行的基础。而怎样借助新技术来发现并防范这些问题则成为了当务之急。采用大数据及人工智能技术建立一种智能化的网络安全风险检测与分析系统对能源企业进行有效的即时监测及准确的风险预测是提高能源企业安全性的一个重要方面。本研究旨在探索这一创新解决方案的可行性与实际应用。

一、电力企业能源企业网络安全现状与挑战

（一）电力能源企业网络安全面临的主要威胁

电力企业能源企业所面临的主要网络安全问题有外部黑客攻击、内部威胁以及设备故障等。伴随着电力企业信息化程度日益提高，越来越多的重要设施及系统与外界相连，因此能源企业易遭受网络攻击。外部攻击可能是 DDoS（分布式拒绝服务）、恶意代码、勒索病毒等。它们可以经由网络入侵能源企业边界防御设备进而干扰能源企业生产活动。同时能源企业内部也存在安全隐患，某些安全事件是由职工误操作或者恶意人员造成。能源企业自动化设备及控制系统由于存在硬件问题、软件缺陷或者设置不当也会带来安全隐患。比如像 PLC（可编程逻辑控制器）这样的控制设备是能源企业的重要控制手段，如果被黑客入侵会造成生产中断甚至造成设备损毁。

（二）能源企业网络安全管理的现有问题

能源企业网络安全管理存在诸多问题，其一是安全防护措施滞后。传统的防火墙、入侵检测等安全措施可以解决一部分安全问题，但是对于日益复杂的攻击方式却无能为力。随着信息技术的发展，能源企业网络安全越来越复杂，传统的安全防护方法难以及时发现所有的网络活动，从而造成安全隐患频出。其二是能

作者简介：郭雅楠（1982-），女，福建省福州人，国家能源集团福建能源有限责任公司专责，专业方向为能源企业数字化转型及网络安全管理。

源企业在安全管理上缺乏有效的风险管理的方法。虽然能源企业一般都有基本的安全防护能力，但是对各种各样的风险没有做到全面的风险分析并且制定相应的防范措施，特别是对于一些复杂的攻击方式缺乏提前预警以及应急预案。此外，能源企业网络安全管理的组织架构以及职责分工不明晰也是造成能源企业网络安全水平较低的原因之一[1]。

（三）网络安全事件对能源企业运营的影响

网络安全事件对能源企业运营的影响主要体现在设备停机、生产效率降低及经济损失等几个方面。网络攻击可通过破坏能源企业控制系统使能源企业无法正常工作而致其停机，从而影响能源企业正常发电。如2015年发生于乌克兰的电力系统遭受网络攻击导致约200万户家庭断电。这给能源企业带来的损失是巨大的直接经济损失，而且有可能对整个电网的安全稳定带来不利影响。同时，电力行业所受到的勒索病毒的攻击日益增多，一旦控制系统的被锁住，则能源企业只能付钱才能使其恢复正常运转，造成了极大的资源浪费。此外，网络安全事件发生也会给能源企业带来负面影响，使客户对能源企业失去信心并可能导致能源企业受到法律以及监管部门处罚等风险[2]。

二、能源企业网络安全风险识别的技术框架

（一）风险识别模型的构建

能源企业网络安全风险识别模型建立是保障能源企业信息系统的首要任务。该模型是对能源企业网络中的各种资产、操作、外部因素等进行全面考察的基础上找出存在的问题所在。在建立的过程中，首先要对能源企业的网络结构、硬件设施、信息传输、通讯方式等方面做出详细的描述，确定主要资产和重要数据。这需要根据电力行业的生产工艺和管理系统（例如SCADA系统、DCS系统等）来判断其安全性及易受攻击程度。其次，利用一定的风险管理手段（例如FMEA（失效模式与效应分析）、HAZOP（危害与可操作性分析）等）衡量各个部分所面临的风险大小。此外，风险识别模型需要具有动态的风险更新能力，在网络发生变化的情况下（例如新加入设备、网络结构调整等），及时对模型进行更新，保证其有效性.而且该模型要能给能源企业网络安全提供一个完整、准确的风险识别方法。

（二）基于数据挖掘的风险识别方法

数据挖掘技术在能源企业网络安全风险管理方面发挥着重要作用。能源企业内部的各种网络设备产生大量的数据，除了系统日志、流量监控信息外还包括设备状态、操作行为等。使用数据挖掘技术可以从这些海量的数据当中筛选出可能存在的安全隐患。比如采用聚类分析、关联规则挖掘等方式发现设备之间存在的一些隐式攻击方式以及异常情况；通过对不同类型网络事件用分类方法（如支持向量机、决策树等）区分它们，从而判断出潜在的网络威胁。而在现实中基于数据挖掘的风险检测手段可以做到自动化的异常检测，减轻了人们的工作负担。对于能源企业复杂的网络环境，基于时序分析以及异常检测的方法可以对实时流量进行监测和分析，发现可疑威胁。而数据挖掘技术也提升了威胁检测准确率，使能源企业更好地防御突发网络安全事件的发生[3]。

（三）风险评估与预警机制设计

风险评估及预警是能源企业网络安全管理工作的一部分。而在风险评估中需要对发现的风险进行量化和定性分析，判断其发生的可能性以及后果严重程度等。常用的有蒙特卡洛模拟、贝叶斯网络以及专家打分法等方式来进行综合打分从而得到风险等级，便于能源企业集中力量解决重点问题。预警应具有及时性和自动化功能，建立多层次的风险预警机制，在第一时间发现高危事件并且做出相应措施。如可以设定阈值和触发条件对网络流量和服务器负载进行监视，当超过一定范围时会发出警报。同时利用人工智能技术，预警系统可以进行智能化分析以及预测，更准确、快速响应。从而，风险评估及预警对能源企业防止受到网络攻击具有重要意义并且能够为安全管理提供指导性意见[4]。

三、基于人工智能的能源企业网络安全智能分析

（一）机器学习在安全风险分析中的应用

机器学习在能源企业网络安全风险分析中，也是提高风险识别及预测水平的有效方法。通过对以往的数据进行训练，机器学习可以识别出其中的规律以达到对风险进行预警的目的。常用的有决策树、支持向量机（SVM）、随机森林等，这些都可以从网络流量、系统日志以及用户的操作行为中提取出有用的信息并利用分类或回归来判断是否有异常情况发生。比如决策树根据流量的特点来进行分类从而检测出威胁；而支持向量机会比较好地解决高维问题并且能够识别出攻击的行为。机器学习不仅可以发现已知的风险还可以通过无监督学习发现新的隐患进而增强能源企业对于未知风险的防御能力。通过不断改进与训练，使机器学习不断提高能源企业网络信息安全防护能力[5]。

（二）深度学习在能源企业安全态势感知中的优势

深度学习在能源企业安全态势感知方面有明显的优势。相比于传统的机器学习算法，深度学习利用多层次神经网络有效应对复杂的数据并能发现细粒度的安全信息，在能源企业的安全感知上可以对能源企业的各种网络流量、设备状态以及用户的操作等进行综合考虑，建立较为复杂的安全模型，自主学习攻击的变化趋势。卷积神经网络（CNN）适合处理图像类的信息，可用于对设备监控视频进行分析，发现其中的问题；而循环神经网络（RNN）适合处理时序类型的数据，例如能源企业设备过去的工作情况，可用于监测设备出现问题或者有威胁的行为。深度学习自动特征提取可以使得能源企业及时了解自身网络安全情况，提高对于各种复杂攻击发现以及应对的能力[6]。

（三）智能分析系统的实时响应能力与优化策略

智能分析系统在能源企业网络安全中及时响应十分重要，尤其是能源企业自动化程度提高之后，对设备以及网络流量进行实时监控就显得尤为重要。系统基于分布式设计思想，把数据采集、处理以及分析等工作分派到各个节点上，以保证其高效性和可扩展性。为了更快捷地做出反应并且更准确地发现威胁，在该系统中使用基于规则检测方法、机器学习以及深度学习等技术来实现。同时优化也是提高整个系统的性能的一个重要方面，包括算法优化、数据流量智能过滤以及异常事件自动分类等。比如可以设置一个动态阈值，在有新的警报产生时就及时更新这个阈值从而降低误报率和漏报率。系统还可以基于当前情况不断学习，改进预测模型来应对新的环境以及新的攻击方式等。这使得能源企业可以及时发现网络安全隐患并加以防范。

四、能源企业网络安全风险识别与智能分析平台的实现

（一）平台的整体架构设计

能源企业网络安全风险识别与智能分析平台是分层式结构，包含数据采集层、数据存储层、智能分析引擎层以及可视化展示层。数据采集层利用流量采集器、日志采集器以及终端探针等方式获取网络流量、主机日志、设备状态等相关信息，实现对能源企业网络情况全方位了解。数据存储层使用分布式存储技术（例如 Hadoop HDFS或 Elasticsearch）来存储以及查询大量安全相关数据。智能分析引擎层结合机器学习、深度学习算法以及规则引擎来进行深层次挖掘以及异常发现。可视化呈现层利用图形化仪表板展示安全态势、风险指标以及告警信息，支持根据时间、资产、风险级别进行检索等操作。平台架构保证高可用性、可扩展性和及时性，为能源企业网络安全管理工作提供技术支持。存储层及引擎层之间使用消息队列（例如：Kafka）进行通信以提高整个分析过程平滑度，在一定程度上解决了由于大量数据而造成的问题[7]，如图1所示。

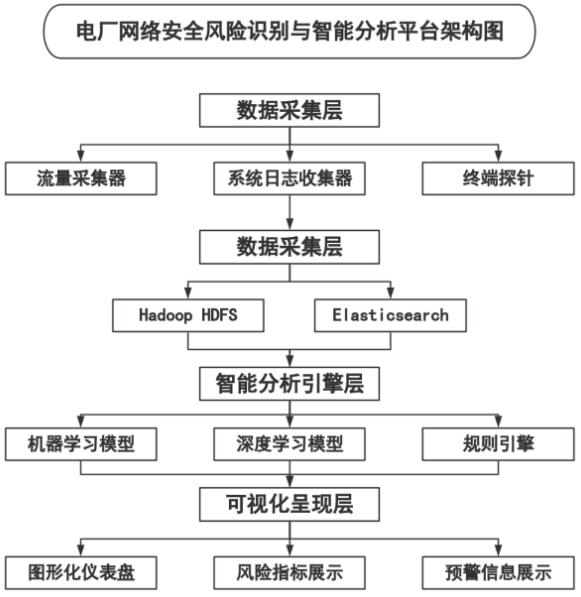

图1 平台架构图

（二）核心技术与实现细节

平台核心关键技术包括大数据处理、机器学习、深度学习及规则引擎。大数据处理使用 ETL流程对数据进行清洗、规范化以及特征提取，建立安全事件和行为特征库；机器学习算法（例如随机森林和支持向量机）用于区分正常流量以及恶意流量，而深度学习方法（例如自编码器和 LSTM）用于发现复杂的攻击方式；平台加入电力行业的相关规则集，根据《电力监控系统安全防护规定》等相关文件来进行规则比对，及时发现潜在的安全风险；多种模型集成（如投票法或者加权融合的方法）可以提高检测精度；智能化分析利用知识图谱技术，将电力设备与其所发生的事情联系起来，从而更好地理解跨域事件之间的关系。平台也有行业大模型，可进行情报分析、漏洞发现等工作，提高工作效率，可针对不同的电力场景提供个性化服务。

（三）平台实施的实际效果与案例分析

以国网浙江省电力有限公司杭州供电公司场景化网络安全运营情况为例，该公司从2021年开始建设全网覆盖的网络安全运营平台，引入多种模型以及数据智能技术的应用，实现由“静态防护”到“动态监控、纵深防御”。平台中的账号越权审计模型、设备仿冒检测模型以及自研的小系统分析模型，对于内部越权访问、异常设备以及敏感数据的异常访问等行为的识别率较高。根据2024年内部安全监控数据显示，在平台上对于越权访问事件检测准确率达到96.2%，对于仿冒设备行为漏报率低于等于2.5%，并且响应时间由原来的均值18小时减少到小于等于2小时，大幅提高工作效率以及安全性[8]，如表1所示。

表1 安全指标实施前后变化表

安全指标	实施前	实施后
越权访问事件识别准确率	72.5%	96.2%
仿冒设备误报率	15.8%	≤2.5%
平均响应时间	18 h	≤2 h
异常行为检测率	68.4%	94.7%

五、结语

能源企业网络安全风险识别与智能分析平台利用大数据、人工智能等先进技术手段对能源企业进行有效保护，在线监测、风险发现以及处理上表现良好，极大提升了能源企业安全水平。基于良好结构及智能化分析功能，该平台可以迅速发现安全隐患并发出警告，有利于保证电网安全可靠运行。同时，随着进一步智能化发展和完善，平台将使能源企业管理更加智能、准确。

参考文献

[1]李威星，章修齐.智能技术在电力安全风险控制中的应用[J].电子技术，2025,54(12):306-307.
[2]黄海波.人工智能技术在电力网络安全防护中的研究与应用[J].中国新通信，2025,27(23):16-18.
[3]叶子源.数字化转型背景下电力企业作业人员安全行为智能干预机制研究[J].中国高新科技，2025,(22):93-95.
[4]王立军，白练.基于人工智能的电力行业移动介质安全风险评估模型研究[J].中国高新科技，2025,(22):115-117.
[5]李献.人工智能驱动的电力物资信息安全实时监测系统研究[J].中国科技纵横，2025,(19):63-65.
[6]彭素华，钟志富，郑吓耕，等.电力生产企业工业互联网安全能力建设探讨[J].中国信息界，2025,(08):66-68.
[7]叶硕.S公司电力工程作业现场安全风险管理研究[D].重庆交通大学，2025.
[8]司锦涛.人工智能时代下网络安全企业发展战略研究[D].北京邮电大学，2025.

