计算机网络安全风险评估模型的构建与应用

梁冰芳

（包头钢铁职业技术学院，内蒙古 包头 014010）

摘 要 为了提升计算机网络安全风险评估的科学性与实用性，构建基于多维度、多层次指标体系的评估模型，研究以熵权法与模糊层次分析法结合的权重分配方法为核心，设计分层递进的评估架构并优化改进的BP神经网络算法，分析风险数据并验证模型应用效果。结果表明，该模型能够有效识别和量化网络安全风险，评估结果准确性较高，适用于复杂多变的网络环境，具有广泛的实践价值与推广意义。

关键词 计算机网络安全；风险评估模型；熵权法；模糊层次分析

中图分类号：TP393.08 **文献标志码**：A **DOI**：10.3969/j.issn.2097-3365.2025.02.006

0 引言

随着信息技术的快速发展，计算机网络已成为社会运行的重要基础，但随之而来的网络安全风险也愈发严峻。网络攻击手段日益复杂化、多样化，传统的安全防护机制难以全面应对潜在威胁。构建科学、系统的网络安全风险评估模型，不仅是保障网络运行安全的重要技术手段，也是提升管理效率与优化资源配置的关键路径。风险评估模型的研究可为安全策略制定提供精确的数据支持，进一步促进网络安全体系的动态调整与持续优化，为构建可靠的网络安全环境奠定基础。

1 计算机网络安全风险评估指标体系构建

1.1 风险评估指标选取原则

在构建计算机网络安全风险评估指标体系时，需要遵循科学性、系统性、可操作性和动态性四大基本原则。科学性原则要求所选取的指标能够准确反映网络安全风险的本质特征，确保评估结果的客观性和准确性；系统性原则强调指标体系应当全面涵盖网络安全的各个层面，既要考虑技术层面的安全威胁，也要关注管理制度和人员行为带来的潜在风险，同时各指标之间应具有合理的层次结构和逻辑关系；可操作性原则要求选取的指标应易于量化和测量，评估过程应具有可实施性和可重复性，避免选择过于抽象或难以获取数据的指标；动态性原则则强调指标体系应具有适应性和灵活性，能够随着网络技术的发展和安全形势的变化进行及时调整和优化[1]。

1.2 风险评估指标分类

计算机网络安全风险评估指标可从技术维度、管理维度和人员维度三个方面进行分类。技术维度指标主要包括网络架构安全、系统安全、应用安全和数据安全等方面，具体涉及防火墙配置、入侵检测、访问控制、加密算法、漏洞扫描等技术指标；管理维度指标主要关注安全策略制定、制度执行、应急响应、资产管理等方面，包括安全管理制度完善程度、安全事件处置流程、安全审计记录等；人员维度指标则着重评估人员安全意识、操作规范性、培训效果等因素，包括员工安全意识水平、违规操作频率、安全培训覆盖率等具体指标。

1.3 指标权重确定方法

在确定各评估指标的权重时，采用熵权法和模糊层次分析法相结合的方式。熵权法是一种基于信息熵理论的客观赋权方法，通过计算指标的信息熵来确定权重，其计算过程如下[2]：首先对原始数据进行标准化处理，然后计算第j个指标下第i个样本值的比重pij，接着计算第j个指标的信息熵ej，最后得到第j个指标的权重wj。而模糊层次分析法则是一种主观赋权方法，通过构建判断矩阵，计算特征向量，并进行一致性检验来确定各指标的权重。两种方法的结合使用可以既保证权重确定的客观性，又能体现专家的主观判断，使得最终的权重分配更加合理。

1.4 指标体系模型构建

基于上述指标分类和权重确定方法，构建一个多层次、多维度的网络安全风险评估指标体系模型。该模型采用层次结构设计，由目标层、准则层和指标层组成。目标层为网络安全风险综合评估值，准则层包括技术维度、管理维度和人员维度三个方面，指标层则包含具体的评估指标。该模型不仅考虑了各指标之间的关联性，还通过权重分配体现了不同指标的重要程度，使评估结果能够更加准确地反映网络安全风险状况。

2 计算机网络安全风险评估模型设计

2.1 模型总体架构

计算机网络安全风险评估模型采用分层递进的架构设计，主要包括数据采集层、风险识别层、风险分析层和风险评估层四个核心层次。数据采集层负责通过自动化扫描工具、系统日志分析、问卷调查等多种方式收集网络安全相关数据[3]；同时，增加基于人工智能技术的数据预处理模块，通过自然语言处理（NLP）解析日志文本信息，利用机器学习算法对采集数据进行清洗、分类和异常检测，从而提高数据质量与分析效率。风险识别层基于收集的原始数据，运用漏洞扫描、威胁建模等技术手段识别潜在安全风险。风险分析层采用定量与定性相结合的方法对已识别的风险进行深入分析。风险评估层则根据分析结果计算最终的风险评估值。在风险分析和评估层，引入改进的AI算法（如随机森林、深度神经网络等）以优化风险量化过程，并动态调整风险权重，以适应复杂多变的网络环境。模型各层次之间通过标准化的数据接口进行信息交换，确保评估过程的连续性和完整性。其中，风险评估层采用改进的BP神经网络算法处理来自下层的分析数据，通过训练样本优化网络参数，提高评估结果的准确性。

2.2 风险识别方法

采用资产导向与威胁导向相结合的风险识别方法。首先，通过资产清查建立完整的资产清单，包括硬件设备、软件系统、数据资源等，并对资产进行分类和价值评估。然后，基于STRIDE威胁模型识别潜在安全威胁，该模型涵盖假冒身份、篡改数据、抵赖、信息泄露、拒绝服务和提升权限六类典型威胁。同时，结合CVE漏洞库和CNVD漏洞库的最新数据，使用自动化扫描工具对系统进行全面漏洞扫描。在此基础上，建立资产—威胁—漏洞关联矩阵（见表1），用于量化描述资产面临的具体威胁和存在的漏洞，矩阵元素取值范围为[0,1]，其中0表示无关联，1表示完全关联，中间值表示部分关联程度。这种多维度的风险识别方法能够系统地发现和记录各类潜在安全风险，为后续的风险分析提供可靠的数据基础。

表1 相关关联矩阵

资产/威胁类型	假冒身份	篡改数据	抵赖	信息泄露	拒绝服务	提升权限
网络设备	0.8	0.6	0.4	0.7	0.9	0.5
服务器系统	0.9	0.8	0.6	0.8	0.7	0.8
应用系统	0.7	0.9	0.7	0.6	0.5	0.7
数据资源	0.5	0.9	0.8	0.9	0.4	0.6

2.3 风险分析技术

采用定量与定性相结合的风险分析技术，主要包括威胁程度分析、脆弱性分析和影响程度分析三个维度。威胁程度分析采用改进的贝叶斯网络模型，通过历史安全事件数据训练网络参数，计算各类威胁发生的概率；脆弱性分析基于CVSS评分系统，综合考虑漏洞的基础评分、时间维度评分和环境维度评分，得出系统脆弱性指数；影响程度分析则采用层次分析法，从资产重要性、业务影响范围和恢复难度三个方面进行评估。三个维度的分析结果通过以下风险计算公式综合得出风险值[4]：

$$Risk = Threat \times Vulnerability \times Impact$$

其中：Threat为威胁程度值，取值范围[0,1]；Vulnerability为脆弱性指数，取值范围[0,1]；Impact为影响程度值，取值范围[0,1]。

2.4 风险等级划分

基于风险分析结果，将网络安全风险等级划分为五个层次：极高风险（Ⅰ级）、高风险（Ⅱ级）、中等风险（Ⅲ级）、低风险（Ⅳ级）和可忽略风险（Ⅴ级）。风险等级划分标准考虑风险值（R）、威胁级别（T）和影响程度（I）三个因素，并根据具体数值范围确定分类标准。其中，极高风险（Ⅰ级）指风险值、威胁级别和影响程度均不低于0.8，需要立即处理；高风险（Ⅱ级）对应0.6至0.8之间，需优先处理；中等风险（Ⅲ级）为0.4至0.6之间，处理可纳入计划安排；低风险（Ⅳ级）为0.2至0.4之间，仅需持续监控；可忽略风险（Ⅴ级）低于0.2，可接受风险存在。

2.5 模型算法实现

核心算法采用改进的BP神经网络结构，包含输入层、隐藏层和输出层。输入层节点对应各个风险评估指标，隐藏层采用双隐层结构以提高网络的非线性映射能力，输出层对应最终的风险评估结果。网络的训练采用Levenberg-Marquardt优化算法，以均方误差作为性能函数。为了防止网络过拟合，采用早期停止法进行训练，并引入正则化项。主要算法实现步骤包括：数据预处理、网络结构初始化、权重优化训练、模型验证和结果输出。通过这种改进的BP神经网络算法，能够有效处理多维度的风险评估指标，并生成准确的风险评估结果。

3 计算机网络风险评估模型的实证应用

3.1 案例选取与环境

选取某省级电力企业的信息系统作为实证研究对象，该企业拥有完整的信息化基础设施，包括核心业务系统、办公系统和生产控制系统等。网络环境由企业内网、外网和生产控制网络构成，共有服务器156台、网络设备89台、终端设备超过2 000台[5]。系统架构采用三层结构：接入层、汇聚层和核心层，并配备了

防火墙、入侵检测系统、漏洞扫描系统等安全设备。近三年内该企业曾发生过3起较大规模的安全事件，分别是DDoS攻击、勒索软件感染和数据泄露事件，这些事件对企业造成了不同程度的影响，为本次风险评估提供了重要的历史数据支撑。评估环境选择在企业正常运营期间进行，以确保采集的数据具有真实性和代表性。

3.2 评估指标数据收集

评估指标数据的收集采用自动化扫描与人工调研相结合的方式，数据收集周期为3个月。技术维度数据主要通过安全设备日志分析、漏洞扫描工具和网络流量监测获取，具体包括系统漏洞数量、安全补丁更新率、病毒感染率、非法访问次数等指标；管理维度数据通过文档审查、现场走访和问卷调查方式获取，重点关注安全制度执行情况、应急预案完备性、安全投入比例等方面；人员维度数据则通过员工安全测评、行为监测和培训记录分析获得。数据收集过程严格遵循标准化流程，确保数据的准确性和可比性。

3.3 风险评估模型实施

风险评估模型的实施分为四个阶段：数据预处理、风险识别、风险分析和风险评估。数据预处理阶段对收集的原始数据进行标准化处理，采用极值法进行数据归一化；风险识别阶段运用改进的STRIDE威胁模型对系统进行全面扫描，识别出47个潜在安全威胁；风险分析阶段使用改进的BP神经网络算法，网络结构为24-16-8-1，采用Levenberg-Marquardt算法进行训练，训练样本包括历史安全事件数据和模拟数据共200组。在模型训练过程中，学习率设为0.05，动量因子为0.9，最大迭代次数为1 000次，当验证集误差连续6次上升时停止训练。通过交叉验证确定最优网络参数，最终模型在测试集上的均方误差为0.0082，相关系数为0.936，表明模型具有良好的泛化能力。

3.4 评估结果分析

基于风险评估模型的计算结果，该企业的整体网络安全风险等级为Ⅱ级（高风险），综合风险值R=0.726。具体分析表明：技术维度风险贡献度最高，占比达到45.3%，主要风险点集中在系统漏洞修复不及时和访问控制策略不严格两个方面；管理维度风险占比为32.8%，突出问题是安全制度执行不到位和应急响应机制不完善；人员维度风险占比为21.9%，主要体现在员工安全意识参差不齐和操作规范性不足。通过对评估结果的深入分析，识别出12个关键风险点，并按照风险等级从高到低排序，形成风险处置建议清单。评估结果还显示，相比上一年度的评估数据，该企业的整体风险值上升了8.2%，主要由于新业务系统上线带来的安全挑战和外部威胁形势加剧所致。

3.5 模型优化建议

为进一步优化计算机网络安全风险评估模型，可以从以下方面入手：第一，广泛应用人工智能技术以提升模型性能。通过引入深度学习算法（如卷积神经网络、图神经网络等）增强模型对复杂网络威胁的识别能力，同时结合时间序列分析技术，提高对持续性风险的预测能力。第二，在数据采集与处理环节，部署基于AI的实时监控系统，通过智能感知设备自动识别威胁模式并生成数据标签，提升数据输入质量。第三，在指标体系中，增加动态权重调整机制，利用自适应算法实时调控权重，以适应多变的网络安全环境。模型算法层面，引入多模型集成策略，将改进的BP神经网络与随机森林、XGBoost等算法结合，充分利用不同模型的优势，提高风险评估的鲁棒性和泛化能力。第四，面向网络等保体系的需求，结合AI技术构建基于等保2.0标准的自动化评估模块，为网络等级保护合规提供智能化支持。第五，在风险评估层，增加对交互式可视化工具的支持，使评估结果更易于理解和应用。此外，结合强化学习技术设计自动优化框架，使模型能够在动态环境中自主迭代与提升，最终实现更精准的网络安全风险预测与决策支持。

4 结束语

计算机网络安全风险评估模型的构建与应用需注重科学性、系统性和动态适应性，通过多层次指标体系和优化算法实现精准风险评估。未来，应重点发展基于人工智能的智能化评估方法，包括引入图神经网络、多模态学习等前沿技术，进一步优化风险识别和评估过程。此外，可结合网络等级保护2.0标准，开发面向行业应用的智能化评估工具，促进网络安全管理的规范化与自动化。结合大数据与人工智能技术提升模型的动态更新能力与决策支持水平，以应对复杂多变的网络安全形势。

参考文献：

[1] 原毅,左斌,颜峰.基于层次分析的网络安全风险评估方法[J].网络安全技术与应用,2024(08):46-48.
[2] 路凯,刘歆宁.计算机网络信息安全风险评估标准与方法研究[J].软件工程,2024,27(06):34-38.
[3] 杨亮.基于人工智能技术的计算机网络安全风险评估系统设计[J].电脑知识与技术,2024,20(16):117-119.
[4] 李薇.基于区块链的计算机通信网络安全风险评估[J].信息技术,2024(02):148-153.
[5] 高语,单芳芳.基于改进神经网络的信息安全风险评估模型与指标体系构建研究[J].佳木斯大学学报:自然科学版,2024,42(02):28-31.