教育信息化背景下学校网络安全风险分析与应对策略

何兆佳
广东 江门 529000

DOI: 10.61369/TACS.2025090002

摘　　要： 教育信息化背景下，云计算、物联网等技术给学校网络安全带来新挑战，风险特征演变，技术与管理层面隐患多。构建融合层次分析法与模糊综合评价法的量化评估模型，明确风险分级标准，经实践验证与误差分析后更精准。提出从技术、管理、人员等方面构建三维防护体系，以保障学校网络安全，助力教育信息化发展。

关 键 词： 教育信息化；学校网络安全；风险评估

Risk Analysis and Countermeasures of School Network Security under the Background of Education Informatization

He Zhaojia
Jiangmen, Guangdong 529000

Abstract: Under the background of education informatization, cloud computing, Internet of things and other technologies have brought new challenges to school network security, risk characteristics have evolved, and there are many hidden dangers in technology and management. A quantitative evaluation model integrating analytic hierarchy process and fuzzy comprehensive evaluation method is constructed to clarify the risk classification standard, which is more accurate after practical verification and error analysis. It is proposed to build a three-dimensional protection system from the aspects of technology, management and personnel, so as to ensure the school network security and help the development of education informatization.

Keywords: education informatization; school network security; risk assessment

引言

在教育信息化快速发展的时代，学校网络安全面临诸多挑战。2021 年颁布的《教育信息化 2.0 行动计划》旨在全面推进教育信息化进程，在此背景下，云计算、物联网等技术在教育场景广泛应用，但也带来数据泄露、网络攻击面扩大等安全问题，学校网络风险特征显著演变。技术层面存在服务器漏洞、无线 AP 劫持等威胁，管理层面有应急预案缺失、设备管理混乱等隐患。因此，需构建科学评估模型，明确风险分级标准，加强网络安全管理，以应对这些挑战，确保教育信息化有序推进。

一、教育信息化与学校网络安全的内在关联

（一）教育信息化技术架构对网络安全的影响

在教育信息化进程中，云计算、物联网等新型技术设备在教育场景广泛应用。云计算为学校提供便捷的数据存储与共享服务，然而，多用户共用云资源，若云服务提供商安全防护不足，易导致数据泄露风险，攻击者可能借此获取学校敏感教学资料。物联网设备如智能教学终端、校园监控等实现校园智能化管理，但众多物联网设备接入网络，扩展了网络攻击面[1]。因其可能存在安全漏洞，黑客可通过攻击物联网设备，进一步渗透学校网络系统，干扰教学秩序，窃取学生及教师信息。这些技术虽推动教育信息化发展，却从攻击目标数量、范围等方面对网络安全产生新挑战，改变了学校网络安全的风险态势，需重视并加以应对。

（二）学校网络风险特征演变分析

随着教育信息化的推进，学校网络风险特征发生显著演变。数据高度集中化，大量教学、管理等数据汇聚于校园网络系统，一旦遭受攻击，数据泄露或丢失将造成严重后果[2]。设备泛在接入化，众多智能教学设备、移动终端等接入校园网络，增加了网络入口与攻击面，非法设备接入易引发安全威胁。用户群体特殊性方面，学校网络用户涵盖师生，学生安全意识相对薄弱，易因误操作或受网络诱惑陷入安全陷阱；教师在使用信息化教学工具时，也可能因对安全规范掌握不足而带来风险。这些新型风险属性给学校网络安全带来更大挑战，凸显了在教育信息化背景下加强网络安全管理的紧迫性与重要性。

二、学校网络安全威胁的多维度解构

（一）技术层面威胁分析

在教育信息化背景下，学校网络在技术层面存在诸多威胁。服务器漏洞是一大风险点，黑客可利用未及时修复的漏洞，如常

见的 SQL 注入漏洞，非法获取学校服务器中的学生信息、教学资料等敏感数据，像某学校曾因服务器存在 SQL 注入漏洞，导致大量学生成绩数据泄露[3]。无线 AP 劫持也不容小觑，攻击者通过搭建与学校无线 AP 相似的热点，诱导师生连接，从而窃取用户在网络中的登录账号、密码等信息。随着物联网设备在学校的广泛应用，其漏洞带来的威胁日益凸显，例如智能教学设备、校园监控设备若存在漏洞，可能被攻击者控制，干扰正常教学秩序或泄露校园监控画面。

（二）管理层面隐患诊断

在教育信息化背景下，学校网络安全管理层面存在诸多隐患。应急预案缺失是重要问题，一旦遭遇网络攻击，如病毒入侵、数据泄露等突发情况，因缺乏完善的应急预案，学校往往难以快速、有效地应对，可能导致损失进一步扩大[4]。设备管理混乱同样不容忽视，学校网络设备众多，若管理不善，如设备登记不清晰、维护不及时，会增加设备故障风险，影响网络正常运行，甚至可能因设备漏洞被黑客利用。师生安全意识薄弱也较为突出，部分师生对网络安全知识了解有限，易在不经意间点击恶意链接、泄露个人信息，给学校网络安全带来潜在威胁。这些管理层面的隐患成因复杂，相互交织，严重影响学校网络安全与教育信息化的有序推进。

三、风险分析模型的构建与实践验证

（一）量化评估模型设计

1. 层次分析法与模糊综合评价法融合模型

在教育信息化背景下，构建学校网络安全风险量化评估模型时，将层次分析法与模糊综合评价法融合具有重要意义。层次分析法能够将复杂的网络安全风险问题分解为多个层次，通过对各层次指标的两两比较确定其相对重要性，构建判断矩阵并计算权重向量，得出各指标权重[5]。而模糊综合评价法可处理网络安全风险中诸多模糊概念与不确定性。把两者融合，先利用层次分析法确定各层级指标权重，再基于模糊综合评价法构建模糊评价矩阵，综合考虑各因素对学校网络安全风险状况做出全面、客观评价。通过这种融合模型，能更精准地量化评估学校网络安全风险，为后续应对策略的制定提供有力依据。

2. 风险评价矩阵构建

在教育信息化背景下学校网络安全风险评价矩阵构建过程中，需先明确风险发生概率与影响程度的分级标准。依据学校网络安全相关历史数据、行业经验以及专家意见，将风险发生概率分为极低、低、中、高、极高五个等级，分别对应不同的可能性范围；把影响程度从轻微、一般、严重、非常严重到极其严重划分成五级，涵盖对教学活动、师生数据、学校声誉等多方面的影响。基于此，建立三维风险热力图可视化表达方法，以风险发生概率、影响程度以及风险类别作为三个维度，直观展示不同风险的分布情况[6]。通过这种方式，学校管理者和网络安全人员能更清晰地识别和评估各类网络安全风险，为制定精准有效的应对策略提供有力支撑。

（二）实证研究案例剖析

1. 某市智慧校园试点项目检测分析

在某市智慧校园试点项目检测分析中，以采集到的部署 EDR 系统的 42 所学校近三年 17 类高危隐患的安全日志数据为基础构建风险分析模型。借助这些真实且丰富的数据，剖析各类隐患产生的频率、影响范围及潜在危害程度，运用科学的算法与指标体系，构建起贴合学校网络安全实际情况的风险分析模型。随后进行实践验证，将该模型应用于智慧校园网络环境中，观察其对实时安全威胁的预警能力及风险评估的准确性。经实践检验，该模型能够较为精准地识别潜在风险，为后续制定针对性的应对策略提供有力依据[7]，有效提升智慧校园网络安全防护水平。

2. 评估结果验证与误差分析

在教育信息化背景下，对学校网络安全风险分析模型的评估结果验证与误差分析至关重要。通过实证研究案例剖析可知，运用渗透测试的方法对风险分析模型的评估结论进行验证。在实际操作中，经过多次测试与数据收集，发现模型预测准确率达到 89.7%，这一数据有效验证了模型在评估学校网络安全风险方面具备较高的有效性[8]。然而，模型仍存在一定误差。误差来源可能包括网络环境的动态变化、测试样本的局限性等。对这些误差深入分析，有助于进一步优化模型，使模型能够更精准地识别和分析学校网络安全风险，为后续制定科学有效的应对策略提供更可靠的依据。

四、立体化网络安全防护体系构建

（一）技术防御系统升级方案

1. 新型威胁感知系统架构

新型威胁感知系统架构应整合流量探针、EDR 客户端与威胁情报平台等构建五位一体检测体系。流量探针负责对网络流量进行实时监测与深度分析，捕捉异常流量模式，从中挖掘潜在的威胁迹象。EDR 客户端部署在终端设备上，持续监控终端行为，通过分析进程、文件操作等行为，及时发现恶意软件的入侵与异常活动。威胁情报平台汇聚多方信息，整合外部共享的威胁情报数据，结合学校网络环境特点，为系统提供最新、精准的威胁信息。这三者相互协作，流量探针与 EDR 客户端将检测到的可疑行为数据反馈给威胁情报平台进行综合研判，威胁情报平台依据分析结果为流量探针和 EDR 客户端提供针对性的检测策略更新，从而形成一个高效、智能的新型威胁感知系统，及时发现并预警各类新型网络威胁，保障学校网络安全[9]。

2. 数据全生命周期加密策略

在教育信息化背景下，数据全生命周期加密策略对于学校网络安全至关重要。需制定从采集传输到存储销毁各环节的国密算法应用方案与密钥管理规范。数据采集阶段，运用国密算法对原始数据进行初次加密，确保数据在源头的安全性。传输过程中，采用高强度的国密加密协议，保障数据在网络传输时不被窃取或篡改。存储环节，依据数据重要性分级，使用不同强度的国密算法加密，并严格管理存储密钥[10]。当数据需销毁时，要按照规范

流程，对相关密钥和加密数据进行彻底清除，防止数据恢复。同时，建立完善的密钥管理规范，涵盖密钥的生成、分发、更新与撤销等操作，确保密钥的安全性与可用性，以此实现数据全生命周期的有效加密保护，降低学校网络安全风险。

（二）安全管理机制优化路径

1.PDCA 循环管理模型应用

在教育信息化背景下，学校可将 PDCA 循环管理模型应用于网络安全管理机制优化。计划阶段，全面评估学校网络现状，识别潜在风险，据此制定详尽的网络安全规划与目标，包括明确防护措施、资源分配等。执行阶段，严格按照规划有序推进各项网络安全措施的落实，如部署防火墙、加强人员培训等。检查阶段，定期对网络安全状况进行监测与评估，通过漏洞扫描、安全审计等技术手段，查看安全策略执行效果，及时发现新问题。处理阶段，针对检查中发现的问题，分析原因并制定改进方案，将成功经验纳入标准，未解决的问题转入下一个 PDCA 循环，实现学校网络安全防护的持续改进。

2. 人员能力提升实施方案

在人员能力提升实施方案方面，制定包含6大模块32课时的网络安全素养专项培训体系是关键。其中，技术知识模块应涵盖网络架构、操作系统安全等基础内容，让学校教职工与学生了解网络运行原理及潜在风险点。安全意识模块通过案例分析、模拟演练等形式，强化人员对钓鱼邮件、恶意链接等常见威胁的识别能力。应急响应模块传授应对网络安全事件的流程与方法，提升快速处理危机的水平。针对不同岗位与学习阶段，课程难度和侧重点应有所区分，确保培训的针对性与实用性，全方位提升学校人员的网络安全素养与应对能力，为学校网络安全防护奠定坚实的人力基础。

（三）多主体协同治理模式

1. 政 – 校 – 企三方联动机制

在教育信息化背景下，政 – 校 – 企三方联动机制对构建立体化网络安全防护体系至关重要。政府应发挥引领作用，制定完善网络安全相关政策法规，为学校和企业提供明确的行动指南，并提供专项资金支持。同时，搭建交流平台，促进信息共享。学校作为网络安全的直接需求方，需及时向政府反馈实际面临的安全风险，与企业合作共同开展网络安全相关课题研究，为学生开设网络安全教育课程，提升师生安全意识。企业凭借专业技术优势，为学校提供先进的网络安全技术和产品，协助学校进行安全检测与应急处理，还可参与政府组织的网络安全标准制定工作。通过政 – 校 – 企三方紧密协作，实现资源共享、优势互补，有效应对学校网络安全风险。

2. 长效运行保障制度设计

为保障教育信息化背景下学校网络安全防护体系长效运行，需建立一系列配套制度。设立专项预算保障制度，明确网络安全建设、维护及应急处理等方面的资金来源与投入比例，确保资金充足且专款专用，为网络安全工作开展提供坚实经济基础。制定设备更新计划制度，依据技术发展和实际需求，定期对网络安全设备如防火墙、入侵检测系统等进行更新换代，确保其性能满足不断变化的安全需求。构建安全审计评估制度，定期对学校网络安全状况进行全面审计，评估安全策略的有效性、技术措施的落实情况等，及时发现潜在风险并加以改进，通过这一系列制度设计，保障学校网络安全防护体系长效稳定运行。

五、总结

在教育信息化蓬勃发展的当下，学校网络安全的重要性愈发凸显。本研究对学校网络安全风险进行深入分析，揭示其在新环境下呈现的新型特征，如威胁来源多元化、攻击手段智能化等。通过构建评估模型，成功识别出诸如数据泄露风险、系统漏洞隐患等关键风险要素。提出的三维防护体系，涵盖技术、管理与机制三个维度，技术加固提升系统安全性，管理优化规范操作流程，机制创新确保应急响应高效，三者形成闭环防御，全方位保障学校网络安全。后续研究将着重深化 AI 技术在态势感知中的应用，实现更精准的风险预测；同时拓展模型在区域级网络安全监测中的普适性验证，进一步提升整体网络安全防护水平，助力教育信息化稳健发展。

参考文献

[1] 高倩 ." 教育信息化 2.0" 背景下重庆市教育硕士生信息素养提升策略研究 –– 基于对三所高校的调研 [D]. 四川外国语大学 ,2023.

[2] 杨佳烨 . 教育信息化 2.0 背景下综合性大学师范生教育技术能力测评研究 [D]. 江苏大学 ,2021.

[3] 余培 . 教育信息化背景下重庆市中小学教师信息素养发展研究 [D]. 重庆师范大学 ,2021.

[4] 蒋佳琦 . 教育信息化背景下初中生物教师专业素养研究 [D]. 河南科技学院 ,2022.

[5] 李云春 . 教育信息化 2.0 背景下信息技术教师知识评价量表的构建研究 [D]. 贵州师范大学 ,2022.

[6] 殷秀玲 , 潘晓立 , 朱晔 . 教育信息化背景下中职学校师生信息素养现状及提升策略 [J]. 现代农村科技 ,2023(11):100–102.

[7] 张宏菊 . 教育信息化背景下小学语文阅读与写作融合策略 [J]. 科普童话 ,2023(42):139–141.

[8] 徐湘皖 . 教育信息化背景下的教师专业素养 : 挑战与应对 [J]. 山西青年 ,2021(8):7–9.

[9] 孔德文 . 教育信息化背景下高校钢琴教学的实践策略分析 [J]. 戏剧之家 ,2022(1):180–181.

[10] 刘博 , 王增增 . 信息化背景下提高高职学校学生管理的有效策略 [J]. 数码世界 ,2021(4):233–234.

