数智时代校园网络安全防护策略研究

韦甜
商洛学院，陕西 商洛 726000
DOI: 10.61369/TACS.2026060042

摘　　要： 数智时代的到来，推动校园网络向智能化、数字化、协同化深度转型，云计算、大数据、人工智能、物联网等技术与校园教学、科研、管理、生活深度融合，构建起“全场景、全连接、全数据”的智慧校园生态。但与此同时，校园网络的攻击手段呈现智能化、隐蔽化、规模化趋势，传统“被动防御、单点防护”的安全模式已难以应对新型安全威胁，数据泄露、APT 攻击、勒索病毒、设备入侵等安全事件频发，严重威胁校园数据安全、师生隐私安全及教学科研秩序。

关 键 词： 数智时代；智慧校园；网络安全；防护体系；零信任；人工智能

Research on Campus Network Security Protection Strategies in the Era of Digital Intelligence

Wei Tian
Shangluo University, Shangluo, Shaanxi 726000

Abstract: The advent of the digital intelligence era has driven the deep transformation of campus networks toward intelligence, digitization, and collaboration. Technologies such as cloud computing, big data, artificial intelligence, and the Internet of Things are deeply integrated with campus teaching, research, management, and daily life, forming a smart campus ecosystem characterized by "full scenarios, full connectivity, and full data." However, this progress is accompanied by increasingly intelligent, covert, and large-scale cyberattack tactics in campus networks. Traditional security models based on "passive defense and single-point protection" can no longer effectively counter emerging threats. Frequent security incidents—data breaches, APT attacks, ransomware, and device intrusions—pose severe risks to campus data security, faculty and student privacy, and the integrity of teaching and research activities.

Keywords: digital intelligence era; smart campus; cybersecurity; protection system; zero trust artificial intelligence

引言

随着数字中国战略的深入推进，数智化转型已成为高校高质量发展的核心驱动力，智慧校园建设进入规模化落地阶段。校园网络不再是简单的“网络连接”，而是融合了智慧教学、智能科研、智慧管理、智慧生活的综合性数字生态，承载着师生个人信息、科研数据、教学资源、校园管理等核心敏感数据，是高校开展各项工作的核心基础设施。据《中国教育信息化发展报告（2024-2025）》显示，目前我国高校智慧校园覆盖率已达89.7%，92% 的高校部署了云计算平台，87% 的高校实现了物联网设备规模化应用，78% 的高校引入了人工智能辅助教学与管理系统。

一、数智时代校园网络的核心特征与安全痛点

（一）数智时代校园网络的核心特征

数智时代的校园网络，是在传统校园网络的基础上，融合云计算、大数据、人工智能、物联网等技术形成的新型网络生态，其核心特征主要体现在以下三个方面：

1. 网络架构协同化：打破传统校园网络“内外隔离”的静态架构，形成“人－机－物”三元协同的动态网络架构，校园内的终端设备、应用系统、数据资源、师生用户实现全面连接，教学、科研、管理、生活等场景深度融合，网络边界呈现模糊化特征。

2. 数据资源价值化：数智时代的校园网络，积累了海量的核心数据，包括师生个人信息、教学资源数据、科研数据、校园管理数据等，这些数据成为智慧校园建设的核心资产，其价值不断凸显。通过对校园数据的分析与挖掘，能够优化教学模式、提升管理效率、推动科研创新，但同时也增加了数据泄露、数据滥用

的安全风险。

3. 技术应用智能化：人工智能、大数据、云计算等技术在校园网络中广泛应用，实现了校园网络的智能化运维、智能化监测、智能化服务。例如，基于人工智能的网络运维系统，能够自动识别网络故障、优化网络配置；基于大数据的安全监测系统，能够实时分析网络流量、识别异常行为；基于云计算的校园云平台，实现了教学资源的集中管理与共享。

（二）数智时代校园网络的安全痛点

结合数智时代校园网络的核心特征，当前校园网络安全防护面临的痛点主要体现在以下三个方面，这些痛点也凸显了传统防护模式的局限性：

1. 新型攻击手段频发，防护技术滞后：数智时代，网络攻击手段向智能化、隐蔽化、规模化升级，APT 高级持续性威胁、勒索病毒、AI 生成式钓鱼攻击、物联网设备入侵等新型攻击方式层出不穷。这类攻击具有隐蔽性强、传播速度快、破坏范围广、难以检测的特点，而传统校园网络安全防护主要依赖防火墙、杀毒软件等被动防御技术，缺乏对新型攻击的精准识别与快速响应能力，防护技术明显滞后于攻击手段的发展。例如，AI 生成式钓鱼邮件能够模拟师生熟悉的语气与内容，迷惑性极强，传统邮件过滤系统难以识别，容易导致师生泄露个人账号、密码等敏感信息。

2. 网络边界模糊，防护范围难以覆盖：数智时代校园网络“人－机－物”三元协同的架构，打破了传统校园网络的内外边界，终端接入方式更加灵活，师生可以通过校外网络、移动终端随时随地接入校园网络，物联网设备的广泛应用也进一步扩大了网络接入范围。传统“边界防护”模式主要针对校园网络的出入口进行防护，无法覆盖所有接入终端与应用场景，存在大量安全盲区，容易被攻击者利用，实现对校园网络的入侵。

3. 数据安全风险突出，管控能力不足：校园网络积累的海量核心数据，包括师生个人信息、科研机密、教学资源等，价值极高，成为攻击者的主要目标。当前，部分高校缺乏完善的数据安全管控体系，数据分类分级不明确，数据加密、访问控制、备份恢复等防护措施落实不到位，存在数据泄露、数据滥用、数据丢失等安全风险。

二、数智时代校园网络安全防护体系的构建框架

针对数智时代校园网络的核心特征与安全痛点，结合当前网络安全领域的前沿技术与实践经验，本文构建“一个核心、四大维度、闭环运行”的校园网络安全防护体系。其中，“一个核心”是以“数据安全与终端安全”为核心，聚焦校园核心资产的安全保护；“四大维度”是技术防护、管理体系、人才培养、协同联动，四个维度相互支撑、协同发力；“闭环运行”是实现“监测－预警－响应－处置－优化”的全流程闭环，确保防护体系的动态迭代与持续优化。

（一）体系构建的核心原则

1. 智能化原则：充分发挥人工智能、大数据等前沿技术的优势，实现校园网络安全的智能化监测、智能化预警、智能化响应，提升防护效率与精准度，应对新型智能化攻击手段。

2. 体系化原则：打破单一防护的局限，构建技术、管理、人才、协同四位一体的防护体系，实现网络安全防护的全方位、全流程、全覆盖，形成“技术防御＋管理保障＋人才支撑＋协同联动”的合力。

3. 动态化原则：结合数智时代校园网络的发展变化与攻击手段的升级，定期更新防护技术与管理制度，优化防护体系，实现防护体系的动态迭代，确保防护能力始终适配校园网络安全需求。

4. 合规性原则：严格遵循《网络安全法》《数据安全法》《个人信息保护法》等法律法规及教育部相关政策要求，确保校园网络安全防护工作合法合规，保障师生个人信息与校园核心数据的安全。

（二）体系整体框架

数智时代校园网络安全防护体系的整体框架分为四个层面，各层面相互关联、协同发力，共同构成全方位、智能化的校园网络安全防护体系：

1. 技术防护层面：作为防护体系的核心支撑，聚焦“智能防御、精准管控”，融合人工智能、零信任、大数据、加密技术等前沿技术，构建从终端到云端、从边界到核心的数据全生命周期防护体系，实现对新型攻击的精准识别与快速响应。

2. 管理体系层面：作为防护体系的保障基础，构建“统一领导、分级负责、协同配合”的管理机制，完善管理制度，明确权责划分，加强安全考核，确保防护措施落地执行，实现校园网络安全的规范化管理。

3. 人才培养层面：作为防护体系的核心动力，构建“培养＋引进＋培训”三位一体的人才培养体系，培养适配数智时代需求的复合型校园网络安全人才，提升安全管理人员的专业能力与师生的安全意识。

4. 协同联动层面：作为防护体系的延伸拓展，加强高校与政府、企业、科研机构、其他高校的协同联动，实现威胁情报共享、应急响应协同、技术研发合作，形成校园网络安全防护的合力。

三、数智时代校园网络安全防护的具体策略

（一）技术防护策略：构建智能化、全流程的技术防御体系

技术防护是数智时代校园网络安全防护的核心，需结合前沿技术，打破传统被动防御模式，构建“智能监测－精准预警－快速响应－数据防护”的全流程技术防御体系，提升校园网络的安全防护能力。

引入零信任架构，打破边界防护局限：针对数智时代校园网络边界模糊的问题，引入零信任架构，秉持“永不信任、始终验证”的核心理念，打破传统“内外隔离”的防护模式，实现对校园网络终端、数据、应用的全流程管控。具体措施包括：一是构建基于身份的访问控制体系，将师生身份、终端状态、网络环境等作为访问认证的核心要素，实现“最小权限访问”，确保只有授权用户才能访问相应的资源；二是部署零信任网关，对所有接

入校园网络的终端与应用进行统一认证与管控，拦截未授权访问，收缩校园网络的暴露面，减少安全盲区；三是实现终端安全基线管理，对校园内所有终端设备进行安全配置，定期检测终端漏洞与恶意软件，确保终端设备的安全。

2. 应用人工智能技术，提升智能防护能力：利用人工智能技术，构建智能化的网络安全监测与预警系统，实现对新型攻击的精准识别与快速响应。具体措施包括：一是搭建基于人工智能的入侵检测系统，融合 CNN、LSTM 等深度学习算法，对校园网络流量进行实时分析，识别 APT 攻击、勒索病毒、钓鱼攻击等新型攻击行为，精准区分正常流量与恶意流量，提高入侵检测的准确率与效率；二是部署 AI 生成式钓鱼邮件检测系统，通过自然语言处理技术，分析邮件内容、发件人信息等，识别 AI 生成的钓鱼邮件，及时拦截并提醒师生；三是利用人工智能技术实现网络故障与安全事件的自动处置，例如，当检测到终端感染恶意软件时，自动隔离终端、清除恶意软件，减少安全事件的影响范围。

（二）管理体系策略：构建规范化、常态化的安全管理机制

管理体系是数智时代校园网络安全防护的保障，需构建“统一领导、分级负责、协同配合”的管理机制，完善管理制度，强化责任落实，实现校园网络安全的规范化、常态化管理。

1. 建立统一的网络安全管理机构：成立校园网络安全工作领导小组，由学校主要领导担任组长，统筹协调校园网络安全工作，明确网络管理部门、教学部门、科研部门、行政部门等各部门的权责划分，形成“统一领导、分级负责、协同配合”的工作格局。网络管理部门负责校园网络安全的技术防护、日常监测、应急处置等工作；各二级部门负责本部门的网络安全管理，落实安全防护措施，加强本部门师生的安全教育；师生负责自身终端的安全管理，规范网络行为。

2. 完善校园网络安全管理制度：结合数智时代校园网络的发展需求与安全痛点，修订完善校园网络安全管理制度，形成“覆盖全面、权责清晰、可操作性强”的制度体系。具体包括：校园网络安全管理办法、数据安全管理办法、终端安全管理办法、物联网设备安全管理办法、网络安全应急处置预案、网络安全考核办法等。同时，定期更新管理制度，适应新型安全威胁与技术发展的需求，确保管理制度的时效性与针对性。例如，针对 AI 生成式钓鱼攻击，制定专门的防范管理制度，明确邮件使用规范与应急处置流程。

四、总结

本文围绕数智时代校园网络安全防护展开研究，立足智慧校园规模化落地背景，结合高校网络发展现状，梳理其核心特征、安全痛点并构建防护体系与策略。数智时代校园网络呈现架构协同化、数据价值化、技术智能化特征，同时面临新型攻击频发、网络边界模糊、数据安全管控不足的痛点，传统防护模式已难以适配。为此，本文构建“一个核心、四大维度、闭环运行”的防护体系，遵循四大核心原则，涵盖技术、管理、人才、协同四大层面。重点提出技术与管理层面策略，引入零信任架构、应用人工智能技术强化防护，建立统一管理机构、完善管理制度规范管理。

参考文献

[1] 汪勇 . 数智化背景下高校计算机网络安全防护策略 [J]. 移动信息 , 2022(10):0121-0123.

[2] 李智 . 基于 Internet 的学生选课信息管理系统的设计与实现 [D]. 电子科技大学 ,2007.DOI:CNKI:CDMD:2.2007.100311.

[3] 李卓君 . 大数据背景下校园网安全防范策略探究 [J]. 数码设计. CG WORLD, 2021(009):010.

[4] 秦芬 . 依托 " 金陵微校 " 平台 , 数智赋能网络安全教育 [J]. 新课程 , 2024(25).

[5] 张萌 . 高校智慧校园建设问题与对策研究 [D]. 河北师范大学 ,2020.

[6] 赵徜 . 数字化转型下高职院校智慧校园建设的研究 [J]. 微型计算机 , 2024(2):118-120.

[7] 布英塔 . 互联网背景下的高校智慧校园建设策略分析 [J]. 互联网周刊 , 2023(3):69-71.

[8] 宋佳 . 试析大数据背景下高职院校智慧校园建设 [J]. 电脑编程技巧与维护 , 2019(11):3.DOI:CNKI:SUN:DNBC.0.2019-11-031.

[9] 王晓燕 , 孙晓林 , 任锦 , 等 . 高校师生共建网络安全保障体系研究 [J]. 电脑知识与技术 , 2022(001):018.

[10] 杨扬 . 智慧校园环境下高校大数据的治理及应用策略 [J]. 网络安全和信息化 , 2023(6):31-34.

