数据安全在智慧校园建设方案中的关键作用及应用研究

肖勇
身份证号：420111198002124058
DOI: 10.61369/TACS.2025050010

摘　　要： 智慧校园建设中数据安全至关重要。它是基础设施建设基石，涉及教务管理、教学创新等多方面。阐述了其防护机制、技术框架、管理制度等内容，还提及多种技术应用及相关案例，强调从多方面构建安全生态体系。
关 键 词： 智慧校园；数据安全；安全生态

The Critical Role and Application Research of Data Security in Smart Campus Construction

Xiao Yong
ID: 420111198002124058

Abstract: Data security is paramount in smart campus development, serving as the cornerstone of infrastructure that underpins academic administration, teaching innovation, and other domains. This paper elaborates on protection mechanisms, technical frameworks, and management systems, introduces multiple technological applications with case studies, and emphasizes building a comprehensive security ecosystem through multidimensional approaches.
Keywords: smart campus; data security; security ecosystem

引言

随着教育数字化转型的加速推进，智慧校园建设成为教育领域的重要发展方向。国家教育信息化2.0行动计划（2018年）强调了教育信息化的重要性，为智慧校园建设提供了政策指引。智慧校园建设涵盖多个方面，其中数据安全处于关键地位。它不仅是新型教育基础设施建设的基石，还在教务管理、教学创新、信息资产防护等诸多领域发挥着至关重要的作用。从保障数据的准确性和完整性，到保护师生隐私和科研成果，再到构建全生命周期技术防护框架、设计安全管理制度以及探索各种先进技术在数据安全中的应用，都体现了数据安全在智慧校园建设中的核心价值，对推动教育数字化转型深入发展意义重大。

一、智慧校园建设中数据安全的关键作用

（一）教育数字化转型中的战略定位

智慧校园建设是教育数字化转型的重要内容，而数据安全在其中具有关键的战略定位。智慧校园数据安全是新型教育基础设施建设的基石，这是必然的。随着教育数字化的推进，教育大数据在教务管理和教学创新中占据核心地位[1]。在教务管理方面，数据安全保障了学生信息、课程安排、教学资源分配等数据的准确性和完整性，确保教务工作的高效有序进行。在教学创新中，安全的教育大数据为个性化教学、智能学习分析等提供了可靠支撑，促进教学方法和模式的不断创新，从而提升教育质量和效果，推动教育数字化转型的深入发展。

（二）信息资产防护的保障机制

数据安全在智慧校园建设中对信息资产防护具有关键保障机制。它能保护师生隐私，避免个人信息泄露，如姓名、学号、家庭住址等敏感信息的不当获取与传播[2]。对于科研成果而言，确保相关数据的安全性，防止科研过程中的数据被窃取或篡改，保障科研工作的顺利进行和成果的真实性与独特性。在校务数据方面，涵盖教学管理、行政事务等多方面的数据，数据安全可保证这些数据的完整性和可用性，维持学校正常运转秩序。这符合国家教育信息化2.0行动计划要求，通过保障数据安全，为智慧校园建设提供坚实基础，推动教育信息化的健康发展。

二、智慧校园数据安全体系构建

（一）全生命周期技术防护框架

在智慧校园数据安全体系构建的全生命周期技术防护框架中，需建立涵盖多维度的技术体系架构。对于数据采集，应进行分级分类，依据数据的重要性和敏感性加以区分，确保不同级别数据得到相应的保护措施[3]。在传输和存储阶段，采用加密技术，防止数据在传输过程中被窃取或篡改，以及在存储时的泄露风险。同时，智能脱敏处理需依据数据分级结果与使用场景，选择静态脱敏（如 ETL 过程对导出测试数据实施泛化、抑制）或动态脱敏（如数据库代理对实时查询结果进行遮蔽、扰乱）。关键技术包括基于规则引擎的字段级脱敏策略（如身份证号遮蔽中间段、成绩区间泛化）与差分隐私扰动（保障群体统计分析可用性下的个体隐私）。部署需平衡数据效用与隐私保护强度，并建立脱敏策略的自动化更新机制。

（二）管理运营规范化建设

设计符合 ISO/IEC 27001标准的校园数据安全管理制度至关重要。在权限审批流程方面，需明确不同级别用户对数据的访问权限，确保只有经过授权的人员能够获取相应数据，防止数据泄露和滥用[4]。对于第三方服务监管，要建立严格的准入机制和监督体系。在选择第三方服务提供商时，需对其数据安全保障能力进行全面评估，签订详细的数据安全协议，明确双方的权利和义务。在服务过程中，持续监督其数据处理活动，确保符合校园数据安全要求，保障智慧校园数据的安全性和完整性。

三、云安全技术的创新应用

（一）云端数据保护机制

1. 分布式存储加密方案

针对智慧校园海量异构数据的存储安全需求，提出基于国产密码算法（SM4）的分布式存储加密方案[5]。该方案采用分层加密架构：在存储层（如 HDFS 或 Kubernetes CSI 卷），利用 SM4 算法对静态数据进行块级加密；在传输层，结合 TLS 保障数据迁移安全。核心在于密钥管理机制（Key Management System，KMS），采用硬件安全模块（HSM）保护根密钥，通过 KMS 实现数据密钥的生命周期管理（生成、分发、轮换、销毁）。数据访问时，系统依据细粒度访问控制策略，向授权应用动态提供解密密钥，确保非授权实体无法访问明文数据。此架构在保障数据机密性与完整性的同时，满足分布式环境下高性能访问与合规性要求（遵循 GM/T 0054等标准）

2. 跨域访问安全控制

为应对智慧校园多校区、异构系统环境下的安全挑战，需构建基于零信任原则的跨域访问模型。该模型核心在于持续验证与最小权限：1) 身份强认证：所有访问请求（无论内外网）强制实施多因素认证 (MFA)，结合设备指纹与用户行为基线进行动态风险评估。2) 动态策略执行：部署策略执行点 (PEP) 于网络边界及关键应用前端，依据中央策略引擎 (PDP) 的实时授权（基于属性 ABAC，如用户角色、设备状态、资源敏感度、访问时间）实施细粒度访问控制。3) 微隔离与加密：利用软件定义边界 (SDP) 或安全隧道技术（如 mTLS VPN）建立加密通信通道，实现网络层与应用层的逻辑隔离。部署难点在于老旧系统适配与策略精细化制定，需结合校园实际业务流程逐步推进[6]。

（二）虚拟化环境安全防护

1. 容器隔离技术应用

在智慧校园虚拟化平台（如在线教育系统、微服务应用）中，容器隔离技术通过内核命名空间（Network，PID，IPC 等）实现进程、网络栈及文件系统的强隔离，利用控制组（cgroups）实施 CPU、内存等资源配额限制，防止资源滥用导致的拒绝服务攻击。其轻量化特性支持高密度部署，但面临镜像安全风险（需严格扫描基础镜像漏洞）与配置复杂性挑战（如 Seccomp/BPF 安全策略的精细调优）[7]。选型需考量容器运行时（如 containerd）的安全加固特性与编排平台（如 Kubernetes Pod Security Policies/Admission Controllers）的集成深度，确保教学应用实例间互不影响，即使单容器被攻陷亦不波及宿主机或其他业务单元。

2. 云边协同防御体系

设计融合终端感知与云端 AI 分析的协同防御系统架构。在该架构中，终端设备负责实时感知环境中的各种安全相关信息，如异常的网络连接、设备行为等，并将这些信息及时上传至云端。云端则利用先进的 AI 分析技术对上传的数据进行深度分析，能够快速准确地识别出潜在的安全威胁。通过这种云边协同的方式，不仅可以充分利用终端的实时感知能力和云端的强大计算资源，还能实现安全防护的全方位覆盖。同时，这种架构还可以根据不同的应用场景和安全需求进行灵活配置和调整，提高安全防护的针对性和有效性，为智慧校园的数据安全提供有力保障[8]。

四、应用实践与发展路径

（一）典型建设案例分析

1. 高校智慧校园示范工程

某双一流高校在智慧校园建设中高度重视数据安全中台建设。其构建了全面的数据安全防护体系，涵盖数据加密、访问控制、数据脱敏等多种技术手段[9]。通过整合校园内各业务系统的数据，实现了数据的集中管理与安全防护。在数据加密方面，采用先进的加密算法确保数据传输与存储的安全性。访问控制机制严格限制了不同用户对数据的访问权限，依据用户角色和业务需求进行精准授权。数据脱敏技术则在保障数据可用性的前提下，对敏感数据进行处理，防止数据泄露。该高校的数据安全中台建设有效提升了校园数据的安全性，为智慧校园的稳定运行提供了坚实保障。

2. 安全漏洞事件复盘

以某校园数据泄露事件为例，黑客通过 SQL 注入攻击获取了学校数据库的访问权限，导致大量学生和教职工的个人信息泄露[10]。此次事件暴露出防护体系存在多方面薄弱环节。在技术层

面，数据库的安全配置存在缺陷，未能有效阻止恶意 SQL 语句的执行。同时，系统缺乏实时监测和预警机制，无法及时察觉异常的访问行为。在管理层面，安全管理制度执行不严格，对数据库的访问权限管理混乱，存在部分人员权限过大的情况。人员安全意识淡薄也是重要原因，相关人员未能识别常见的网络攻击手段，为黑客提供了可乘之机。这些问题警示我们，在智慧校园建设中，需全面加强数据安全防护体系的建设。

（二）安全效能评估体系

1. 量化评估指标体系构建

构建智慧校园数据安全效能多维度量化评估模型。技术防护力维度设定具体指标：静态 / 动态数据加密覆盖率、访问控制策略违规次数（次 / 月）、漏洞平均修复时间 (MTTR)（小时）。管理成熟度维度量化：年度安全策略审计覆盖率（%）、第三方服务安全合规率、员工安全培训完成率。应急响应维度包含：安全事件平均检出时间 (MTTD)（分钟）、事件平均响应时间 (MTTR)（分钟）、重大事件复现演练达标率。指标数据通过日志审计、配置扫描、演练记录等获取，采用层次分析法（AHP）设定各维度及指标权重，计算综合安全效能指数，实现安全状况的客观度量与持续改进闭环。

2. 动态风险评估方法

开发基于大数据分析的校园网络安全态势感知平台，需建立动态风险评估方法。通过收集校园网络中的各类数据，包括用户行为数据、设备运行数据等，利用数据分析算法对潜在风险进行实时监测和评估。根据风险发生的可能性和可能造成的影响程度，确定风险等级。对于高风险事件，及时发出预警并采取相应的措施进行防范和处理。同时，持续优化评估模型和算法，以适应不断变化的网络环境和安全需求。在实践中不断验证和改进动态风险评估方法，提高其准确性和有效性，从而为校园网络安全提供有力保障。

（三）持续优化创新策略

1. 新技术融合应用路径

区块链技术应用于教育数据存证（如成绩单、学历证书）时，核心在于哈希值上链与智能合约验证：原始数据经加密哈希生成唯一指纹存入区块链，确保证书内容不可篡改；验证时通过智能合约比对链上指纹与待验证数据哈希值。落地挑战在于链下数据真实性保障及跨链互操作性。

联邦学习实现跨部门隐私数据协同（如学生画像分析），其原理是本地模型训练 + 参数聚合：各参与方（如院系、图书馆）在本地数据集训练模型，仅上传模型参数至协调服务器进行安全聚合更新全局模型。部署需解决通信开销优化与异构数据对齐问题，选型应侧重支持差分隐私的框架（如 FATE），并设计合理的激励机制促进参与。

2. 生态体系建设规划

在智慧校园建设的数据安全生态体系建设中，需从多方面着手。技术标准研制是关键，应结合校园实际需求与行业发展趋势，制定科学合理的数据安全技术标准，确保数据在各个环节的安全性与规范性。人才梯队培养不可或缺，通过高校课程设置优化、专业培训开展以及实践项目参与等方式，培养具备数据安全专业知识和实践能力的人才，为智慧校园建设提供人力支持。产教融合创新则是推动生态体系发展的重要动力，加强学校与企业的合作，促进科研成果转化，实现资源共享与优势互补，共同探索数据安全在智慧校园中的创新应用模式，提升智慧校园的数据安全水平。

五、总结

智慧校园建设中数据安全至关重要。需提炼其建设的共性规律与发展范式，这是构建稳固安全体系的基础。强调安全能力与教育业务深度融合，只有这样才能确保教育活动在安全的环境下顺利开展，使数据安全真正服务于教育教学。建立动态演进的智能安全防护体系是关键，它能适应智慧校园不断发展变化的需求，为教育新基建提供重要支撑。通过这些方面的努力，保障智慧校园数据的安全性、完整性和可用性，促进智慧校园建设的健康、可持续发展，提升教育质量和管理水平，为师生创造一个安全、高效的教育环境。

参考文献

[1] 陆慧玲 . 智慧校园建设中的高校数据治理研究 [D]. 江苏大学 , 2022.

[2] 蒋立 . 上海智慧公安建设中数据安全风险防范问题研究 [D]. 上海师范大学 , 2023.

[3] 张宇 . 大连市中小学智慧校园建设问题及对策研究 [D]. 辽宁师范大学 , 2022.

[4] 李晓燕 . 高中智慧校园建设的个案研究 [D]. 山东师范大学 ,2021.

[5] 吕嘉丽 . 基于 FAHP 的中职类学校智慧校园建设水平评价研究 [D]. 内蒙古科技大学 ,2023.

[6] 王亚楠 , 李娜 . 高校智慧校园建设中数据安全治理体系的构建研究 [J]. 齐鲁工业大学学报 ,2022,36(3):53-58.

[7] 刘蓁蓁 . 智慧校园建设背景下高校数据安全管理的研究 [J]. 网络安全技术与应用 ,2021,000(1):102-103.

[8] 沈华根 . 智慧校园高质量建设中的平台数据安全保障研究 [J]. 互联网周刊 , 2022(22):39-41.

[9] 张彬 , 范佳伟 , 李志国 , 孙威 . 智慧校园下的网络安全防护 [J]. 网络安全技术与应用 ,2022,(4):93-95

[10] 张晶 , 李洪洋 , 张文婷 , 等 . 大数据背景下智慧校园网络数据安全研究 [J]. 网络安全技术与应用 , 2023(1):76-77.

