教育信息化网络数据安全与隐私保护技术研究

张　磊

（铁岭师范高等专科学校信息中心，辽宁 铁岭 112008）

摘　要：针对教育信息系统存在的身份认证机制简单、数据加密保护不足、访问权限划分不精细、异常行为监测能力较弱及隐私保护机制不完善等问题，提出一种融合数据加密、零信任访问控制、人工智能异常检测及隐私计算的数据安全防护体系。基于该体系构建安全防护系统，并采用分层安全架构，覆盖数据采集、传输及认证访问等环节，实现教育数据全生命周期安全管理，同时结合智能分析技术实现异常访问实时预警。实践结果表明，该系统可有效提升教育信息系统的安全防护能力与异常行为识别准确率，降低数据泄露风险，提高系统运行稳定性，为教育数字化转型提供安全保障。

关键词：教育信息化；网络安全；数据安全；隐私保护；人工智能；零信任

中图分类号：TP393　　**文献标识码：**A

Research on network data security and privacy protection technology in education informatization

ZHANG Lei

（Information Center, Tieling Normal College, Tieling, Liaoning 112008, China）

Abstract: Aiming at the problems existing in traditional education information systems, such as insufficient data encryption, coarse access control granularity, weak abnormal behavior identification capability, and imperfect privacy protection mechanisms, a data security protection system integrating data encryption, zero-trust access control, artificial intelligence anomaly detection, and privacy computing is proposed. The system adopts a layered security architecture to achieve full lifecycle security management of educational data, and combines intelligent analysis technology to achieve real-time warning of abnormal access. Practical results show that this scheme can effectively improve the security protection capability of education information systems, reduce data leakage risks, and enhance system operational stability, providing security guarantees for education digital transformation.

Key words: education informatization, network security, data security, privacy protection, artificial intelligence, zero trust

1　引言

教育信息系统普遍存在身份认证机制简单、数据共享安全不足、终端接入管理薄弱及敏感信息保护不到位等问题。随着智慧校园、在线教学平台、学习管理系统及教育大数据平台广泛应用，学生基本信息、学籍档案、成绩数据、教学资源、在线考试数据、科研成果及校园管理数据等信息持续汇聚，教育数据呈现来源多元、规模庞大、更新频繁的特点。同时，移动办公、在线课堂、云计算及移动终端的普及，使教育数据跨平台、跨终端共享更加频繁，数据流转链路不断延长，网络攻击面进一步扩大[1]。

由于教育平台具有开放性强、用户数量大、访问终端复杂等特点，大量师生通过互联网开展教学、学习与管理活动，易受到恶意攻击、账号盗用、勒索软件、非法越权访问及数据泄露等安全威胁。此外，部分教育信息系统仍存在敏感数据加密保护不足、访问权限划分不够精细、异常访问行为监测和预警能力较弱、跨部门数据共享缺乏有效隐私保护机制以及日志审计与安全溯源能力不足等问题。一旦发生安全事件，不仅可能导致学生个人隐私和学校核心数据泄露，还会影响教学秩序与教育管理工作的正常开展。因此，有必要研究教育信息化网络数据安全与隐私保护关键技术，构建覆盖数据全生命周期的安全防护体系，为教育数字化高质量发展提供保障[2]。

2　教育信息化网络数据安全架构设计

针对教育信息化网络环境数据类型多、访问主体复杂、业务系统众多及跨平台共享频繁等特点，本文构建了教育信息化网络数据安全总体架构。该架构采用分

层安全设计思想，自下而上包括数据采集层、数据传输安全层、身份认证与访问控制层、数据隐私保护层及智能安全分析层。各层既相互独立又协同工作，共同实现教育数据采集、传输等过程的安全防护。

2.1 数据采集层

数据采集层是整个安全体系的数据入口，负责学校各类业务系统的统一接入和规范管理，包括教务管理系统、在线学习平台、在线考试系统、校园一卡通系统、图书管理系统、教学资源平台及科研管理系统等。该层对上传数据进行格式转换、完整性校验和统一编码，并建立数据标签体系，为后续分类分级管理提供基础[3]。为衡量数据采集规模，设教育系统共有 n 个业务系统，每个系统采集数据量为 d_i，则平台采集数据总量可表示为：

$$D=\sum_{i=1}^{n} d_i \tag{1}$$

其中，D 表示平台统一采集的数据规模。

2.2 数据传输安全层

数据传输安全层负责保障教育数据在网络传输过程中的机密性、完整性和可用性。该层对客户端与服务器之间的通信进行加密传输，防止中间人攻击和数据窃听；对敏感数据实施更强加密保护，并结合安全网关和流量监测机制识别异常通信行为[4]。为衡量网络传输可靠性，设数据传输成功的数据包数量为 N_s，发送数据包总数为 N_t，则数据传输成功率可表示为：

$$P=\frac{N_s}{N_t}\times 100\% \tag{2}$$

其中，P 表示网络传输可靠性指标。

2.3 身份认证与访问控制层

身份认证与访问控制层负责确认访问主体身份并控制其访问范围。该层遵循零信任安全理念，对任何访问请求均重新验证，不再默认内部网络可信；综合采用多种认证方式确认教师、学生及管理人员身份，并根据用户身份、岗位职责、访问时间、终端设备和访问位置等因素动态调整访问权限，实现最小权限授权。为衡量权限配置的精细程度，设用户拥有权限数量为 A_u，系统总权限数量为 A_t，则权限授权比例可表示为：

$$R=\frac{A_u}{A_t} \tag{3}$$

其中，R 表示用户权限配置比例。

2.4 数据隐私保护层

数据隐私保护层主要面向教育数据共享与开放应用场景，重点保护学生、教师及科研数据等敏感信息。该层建立数据分类分级机制，对不同敏感等级的数据采用差异化保护策略；对于共享数据，综合采用数据脱敏、匿名化处理、差分隐私、动态水印及敏感字段自动识别等技术，在保证数据可用性的同时降低隐私泄露风险。为衡量隐私保护覆盖程度，设原始敏感字段数量为 M，完成脱敏字段数量为 M_d，则数据脱敏覆盖率为：

$$C=\frac{M_d}{M}\times 100\% \tag{4}$$

其中，C 表示隐私保护覆盖程度。

2.5 智能安全分析层

智能安全分析层负责对教育信息系统运行状态进行实时监测和风险分析。该层采集用户登录时间、登录地点、访问频率、访问内容、设备类型及网络行为等特征，建立正常行为模型；当检测到异常登录、暴力破解、异常下载、大规模数据导出或越权访问等行为时，自动进行风险评分并联动安全策略实施响应。为衡量异常行为识别效果，设该层检测出的异常事件数量为 N_d，实际异常事件数量为 N_a，则异常行为检测准确率表示为：

$$A=\frac{N_d}{N_a}\times 100\% \tag{5}$$

其中，A 表示异常行为识别准确率。

3 关键技术研究

教育数据安全涉及采集、传输、认证访问、隐私保护和智能分析等环节，任一环节存在漏洞都可能造成数据泄露或隐私侵犯。为此，结合教育信息系统特点，围绕上述层级研究相应关键技术，为构建覆盖数据全生命周期的安全防护体系提供技术支撑。

3.1 数据采集与质量检测技术

在数据采集环节，采用统一数据接口标准，对教务、在线学习、在线考试、校园一卡通、图书、科研等业务系统数据进行格式转换、完整性校验和统一编码，并建立数据标签体系。通过数据质量检测模块自动识别缺失值、重复数据和异常数据，为后续分类分级管理提供基础。

3.2 数据传输加密技术

数据传输过程中，采用TLS协议建立安全通信信道，对客户端和服务器之间的数据进行加密传输。对于学生个人信息、考试成绩、科研数据等敏感内容，进一步采用AES对称加密算法保护数据正文，利用RSA非对称算法完成密钥交换，并结合数字签名验证数据完整性。此外，通过安全网关与流量监测模块识别异常通信行为，提高网络传输安全性。

3.3 零信任身份认证与访问控制技术

在身份认证与访问控制方面，遵循零信任安全理念，对任何访问请求均重新验证。综合采用用户名密码、多因素认证、短信验证码及生物特征识别等方式确认身份，并结合RBAC角色访问控制和ABAC属性访问控制，根据用户身份、岗位职责、访问时间、终端设备及访问位置动态调整权限。发现异常登录或权限越界时，触发二次认证或限制访问。

3.4 数据隐私保护技术

为保护教育数据共享过程中的隐私安全，本文建立

数据分类分级机制，将教育数据划分为公开数据、内部教学数据、学生个人信息以及考试试题、科研成果等核心数据4个等级，并针对不同等级采用差异化保护策略。对于共享数据，综合采用数据脱敏、匿名化处理、差分隐私、动态水印及敏感字段自动识别等技术，并引入联邦学习等隐私计算技术，使各业务部门仅共享模型参数而无需传输原始数据，在保证数据可用性的同时降低隐私泄露风险。

3.5　AI异常行为检测技术

在智能分析环节，利用机器学习算法构建用户行为画像，对登录时间、登录地点、访问频率、访问内容及终端设备等特征进行实时分析，快速识别异常登录、暴力破解、越权访问及批量数据导出等风险行为，并自动触发安全告警、访问限制及二次身份认证。通过持续学习优化模型，不断提高检测准确率、降低误报率。

4　系统实现与实践应用

4.1　系统架构与实现环境

基于上述安全架构与关键技术，本文实现教育信息化网络数据安全防护系统。该系统采用B/S架构设计和部署，整体基于分层解耦思想，将前端访问层、业务逻辑层与数据服务层分离，以提升可扩展性和可维护性。安全分层架构贯穿于各层之中，通过相应安全技术实现数据全生命周期防护。

该系统服务器统一部署在学校数据中心，依托虚拟化服务器集群与万兆核心交换网络，支撑高并发访问和稳定运行。软件环境方面，操作系统选用Linux，Web服务器采用Nginx实现请求转发与负载均衡，数据库选用MySQL 8.0存储结构化数据，业务开发框架基于Spring Boot构建微服务体系，并引入Redis作为缓存中间件、RabbitMQ实现异步消息处理。

在安全技术实现方面，该系统集成OAuth2和JWT实现统一身份认证与授权管理，采用TLS保障数据传输安全，数据库层对敏感字段实施AES-256加密，并利用TensorFlow构建AI异常行为检测模块，与数据采集、传输加密、零信任访问控制、隐私保护及异常检测等关键技术相对应。系统支持PC端和移动端多终端访问，满足教育信息化场景下的多样化业务需求。

4.2　实践环境与运行部署

为验证该系统在真实教育场景中的应用效果，选取某省属本科院校智慧校园平台作为实践对象进行部署测试。该校在校师生约2.8万人，已建成教务管理系统、学习管理平台（LMS）、在线考试系统、校园一卡通系统、数字图书馆、科研管理平台及统一身份认证平台等业务系统，累计用户规模约3.5万人，日均访问量超过18万人次，数据交互频繁且业务类型复杂。学校数据中心具备较为完善的基础设施条件，部署有虚拟化服务器集群、万兆核心网络及集中存储系统，可满足大规模数据处理和高并发访问需求。

该系统在此环境中完成整体部署，并按照关键技术实现安全防护，覆盖数据采集、传输、认证访问、隐私保护及智能分析等环节。系统持续稳定运行90天，对运行性能与安全效果进行综合评估。

4.3　实验结果与效果分析

实验以传统安全防护方案为对照组，对系统运行效果进行对比分析。结果表明，该系统在安全防护、智能分析、响应效率和运行稳定性等方面均优于对照组。

在安全防护方面，非法访问拦截率明显提升，数据泄露事件数量减少，说明该系统具备较强的攻击识别和防护能力。在智能分析方面，异常行为识别准确率较对照组大幅提高，误报与漏报有效降低。在响应效率方面，平均告警响应时间明显缩短，风险识别和处置更加及时。此外，身份认证成功率与系统可用率保持较高水平，表明该系统在强化安全性的同时未影响正常业务运行。

5　结束语

教育信息化的发展使教育数据安全和隐私保护成为数字校园建设的重要基础。针对教育信息系统存在的身份认证机制简单、数据加密保护不足、访问权限划分不精细、异常行为监测能力较弱及隐私保护机制不完善等问题，本文构建了教育信息化网络数据安全防护体系，实现了教育数据全生命周期安全管理。实践结果表明，该体系能够有效提高非法访问拦截率、异常行为识别准确率及系统整体稳定性，显著降低教育数据泄露风险，为智慧校园安全运行提供了可靠保障。

未来，可进一步深化联邦学习应用，并结合区块链、可信执行环境及国产密码技术，持续提升教育数据共享安全性和隐私保护水平，推动教育信息化向更加智能、安全、可信的方向发展。

参考文献：

[1] 刘梦君，姜雨薇，曹树真，等.信息安全技术在教育数据安全与隐私中的应用分析[J].中国电化教育，2019(6)：123-130.

[2] 刘成榆.教育服务中心计算机网络系统运维与信息化保障机制研究[J].科技与创新，2026(5)：186-188.

[3] 范夫伟.区域教育系统网络安全一体化防护体系的建设与实践[J].网络安全技术与应用，2026(1)：85-87.

[4] 田永健.新形势下教育机关网络安全问题及对策研究[J].中国教育信息化，2022，28(2)：37-42.

作者简介：

张磊（1980—），本科，副教授，研究方向：计算机网络、网络安全及教育信息化。