Journal of Security and Safety Technology 安防技术, 2026, 14(3), 105-114
Published Online September 2026 in Hans. https://www.hanspub.org/journal/jsst
https://doi.org/10.12677/jsst.2026.143011

Hans汉斯

开放教育数据安全能力体系构建

——以国家开放大学为例

马伟娜[1]，宋　星[1]，吴淑苹[1]，魏顺平[2]

[1]国家开放大学数字化部，北京
[2]中央民族大学教育学院，北京

收稿日期：2026年8月7日；录用日期：2026年8月31日；发布日期：2026年9月4日

摘　要

自《数据安全法》颁布实施以来，数据安全问题日益受到关注。开放教育场景下，校务数据治理、数据共享与开放应用伴随大量师生个人隐私等敏感信息，其安全保障直接关系高校办学稳定与长远发展。当前，制度漏洞、技术短板、环境风险等多重因素交织叠加，高校数据安全面临的威胁持续加剧。大模型、云计算及智能终端的广泛应用推动数据深度集成与高频交互，大数据的存储、共享与应用暴露出数据泄露与隐私外溢等问题，给师生个人权益、高校办学安全乃至国家信息安全带来潜在风险。本文结合开放教育数据特征与学校数据安全现实困境，基于数据生命周期理论，围绕在线教育数据的采集、传输、存储、共享、销毁等全流程，从制度、技术、环境等多维度对高校数据安全风险进行溯源，构建覆盖数据全生命周期、融合制度规范与技术防护的开放教育数据安全预警监测与防护体系，为开放教育数据安全治理提供实践参考。

关键词

开放教育，数据安全，数字教育，隐私数据

Building a Data Security Capability Framework for Open Education

—A Case Study of The Open University of China

Weina Ma[1], Xing Song[1], Shuping Wu[1], Shunping Wei[2]

[1]Department of Digitalization, The Open University of China, Beijing
[2]School of Education, Minzu University of China, Beijing

Received: August 7, 2026; accepted: August 31, 2026; published: September 4, 2026

文章引用: 马伟娜, 宋星, 吴淑苹, 魏顺平. 开放教育数据安全能力体系构建[J]. 安防技术, 2026, 14(3): 105-114.
DOI: 10.12677/jsst.2026.143011

Abstract

Since the promulgation and implementation of the *Data Security Law*, data security has drawn increasing attention. In open education settings, the governance of institutional data and the sharing and open application of data involve a large volume of sensitive information, such as the personal privacy of teachers and students; safeguarding such data bears directly on the operational stability and long-term development of higher education institutions. At present, multiple factors—institutional loopholes, technological shortcomings, and environmental risks—are interwoven and superimposed, and the threats confronting data security in higher education continue to intensify. The widespread application of large models, cloud computing, and intelligent terminals has driven the deep integration and high-frequency interaction of data, while the storage, sharing, and application of big data have exposed problems such as data breaches and privacy leakage, posing potential risks to the individual rights and interests of teachers and students, the operational security of institutions, and even national information security. Drawing on the characteristics of open education data and the real-world dilemmas of data security in universities, and grounded in data lifecycle theory, this paper traces the sources of data security risks in higher education from the multiple dimensions of institution, technology, and environment across the full process of online education data—collection, transmission, storage, sharing, and destruction. It constructs an early-warning, monitoring, and protection system for open education data security that spans the full data lifecycle and integrates institutional and technical safeguards, thereby providing a practical reference for the governance of open education data security.

Keywords

Open Education, Data Security, Digital Education, Private Data

Copyright © 2026 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

数据已成为驱动教育数字化转型的核心要素，其安全问题直接关乎国家安全与社会稳定。数字经济时代，数据作为核心生产要素与国家基础性战略资源，在赋能教育数字化转型的同时，也衍生出多重安全风险，网络安全已升级为数据安全，直接关乎国家安全与社会稳定。我国相继颁布《网络安全法》[1]《数据安全法》[2]《个人信息保护法》[3]等法律法规，明确要求建立数据分类分级保护制度，强化全流程数据安全管控。教育领域先后印发《教育部关于加强新时代教育管理信息化工作的通知》[4]《关于加强教育系统数据安全工作的通知》[5]等文件，强调提升安全保障能力，全面加强数据安全保障，建立覆盖全生命周期的数据安全保障机制，重点保护广大师生和家长，特别是未成年人的个人隐私信息[1]。要求健全覆盖数据收集、传输存储、使用处理、开放共享等全生命周期的数据安全保障制度。探索建立个人生物识别信息审查制度、数据安全评估制度，开展常态化的数据安全监测预警通报。构建数据安全协同治理的新格

[1]https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm
[2]http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html
[3]http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html
[4]http://www.moe.gov.cn/srcsite/A16/s3342/202103/t20210322_521669.html
[5]https://wlzx.bbc.edu.cn/2024/0110/c2926a102214/page.htm

局，有效遏制数据安全违法违规活动。全面加强数据安全保护能力，提升数据安全合法合规管理水平，有力支撑教育事业发展[2]。教育部《关于加快推进教育数字化的意见》[6]进一步明确，要筑牢教育数字化安全屏障，全面落实教育数据全生命周期安全防护，强化核心和重要数据防篡改、防泄露、防滥用能力，强化人工智能安全保障，加强教育数字化领域意识形态和网络安全、数据安全、个人信息保护监管及信息技术发展应用[3]，为高校数据安全建设划定合规底线与实践方向。

教育数据安全事件频发凸显治理紧迫性，在线教育数据安全已成为数字教育发展的关键命题。近年来，教育行业数据泄露事件频发，个人数据被暗网售卖、中学教师因网课遭遇“网络爆破”后猝死等事件[4]，无不警示数据安全治理的紧迫性。加强学校数据安全防护，是推进国家教育数字化战略行动的重要内容。在线教育面向全网海量学生群体，数据体量庞大、敏感程度高，其安全保障成为数字教育发展的关键命题。国家开放大学作为我国开放教育的核心载体，承担着大规模远程教育办学职责，亟需构建系统化数据安全防护体系，提升数据安全合规管理水平，为在线教育高质量发展与国家开放大学数字化建设奠定安全基础。

在国内外研究方面，数据安全治理已形成较为丰富的理论与实践成果。欧盟《通用数据保护条例》[7](GDPR)以严格的个人数据处理规则与问责机制，成为国际数据保护立法的重要参照[5]。在治理模型层面，Gartner 提出的数据安全治理(Data Security Governance, DSG)理念，强调自决策层至技术层、自管理制度至工具支撑的自上而下治理路径[6]；在数据生命周期理论方面，ISO/IEC 27001 信息安全管理体系与数据全生命周期管理理论，为数据在采集、传输、存储、处理、共享与销毁各环节的安全控制提供了通用范式[7]；《信息安全技术 数据安全能力成熟度模型》[8](GB/T 37988—2019, DSMM)以数据生命周期为主线，从组织建设、制度流程、技术工具与人员能力等维度刻画数据安全能力的成熟度等级，已成为国内数据安全能力建设的重要参照[8]。在教育领域，研究者们关注在线教育平台的数据隐私保护、学习者数据安全合规等议题，但针对开放教育这一特定场景的系统性数据安全能力体系研究尚较为有限。本研究在上述理论框架基础上，以数据生命周期理论为指导，结合开放教育数据特征，构建覆盖制度规范与技术防护的综合体系，以期弥补该领域研究空白。

2. 在线教育数据特征分析

国家开放大学由教育部批准，在原中央广播电视大学基础上组建，是以现代信息技术为支撑的新型高等学校[4]，已建成覆盖城乡的四级远程教育办学体系，涵盖总部、分部、学院及地市级分校、学习中心，形成多元丰富的数据资产体系，成为开放教育数字化发展的核心资源。结合办学实践，开放教育数据呈现五大典型特征：

(1) 多样性：在线教育教学模式灵活，课程资源形式丰富，数据资产呈现异构多元特征，涵盖视频、音频、PPT/Word/PDF 文档、图片、纸质资源数字化副本等多种类型。业务类型多样，涵盖学历教育、非学历教育、终身教育、老年大学、学分银行、质量监控、师资、学习网等模块。数据来源平台多样化，同时支持 PC 端、移动端、大屏端等多终端数据源。

(2) 动态性：教学活动持续开展推动数据实时生成与更新，数据增量显著，如学习网教师学生行为数据日均 60 万条新增访问记录，统一认证与融合门户系统数据呈高速增长态势。除基本数据以外，衍生数据日益更新，如综合数据分析指标、动态监控预警指标等。

(3) 敏感性：开放教育体系涵盖学生个人身份信息、学习行为数据、学业成绩、学籍档案、教师教学行为等核心敏感数据，涉及个人隐私与办学机密，泄露或篡改将严重损害师生权益与学校公信力。且各

[6]http://www.moe.gov.cn/srcsite/A01/s7048/202504/t20250416_1187476.html
[7]https://eur-lex.europa.eu/eli/reg/2016/679/oj
[8]https://openstd.samr.gov.cn/bzgk/std/showGb?type=online&hcno=3CFD5E5A14C24D303EA1E139E6EB75C8&request_locale=zh

系统存在用户隐私数据明文存储、传输、导出等情况，有未知的隐私泄露风险。

(4) 分散性：数据分散存储于各级办学机构服务器、云平台、机房等，跨层级、跨地域管理难度大，数据管控协同性不足。

(5) 共享性：四级办学体系与总部集中管理模式，决定了数据需在总部与分部间同步共享，学校已建成数据资源共享服务平台支撑跨机构数据交互，共享过程中的安全管控需求突出。

3. 数据安全治理

3.1. 数据治理与数据安全治理

吴信东等在《数据治理技术》[9]中指出，数据治理是将机构数据作为战略资产进行管理，通过提供从收集到处理应用的管理机制，提升数据质量，实现数据共享与价值最大化。国家开放大学校务数据服务于学校各项事业及各部门、办学体系业务需求，发挥其在管理服务提升、数据挖掘分析、辅助决策支持、信息公开等方面的作用。数据治理有助于提升数据质量，释放数据价值。

国际咨询机构 Gartner 指出：“数据安全治理不仅是一套工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿组织架构的完整链条。”从狭义层面看，数据安全治理是组织从自身视角出发，多部门协作，推动合法合规使用数据的一系列活动集合，核心包括明确团队职责、规划制度规范、构建技术体系等。依据顶层数据安全战略，从组织、人员、制度、工具等多方面，协同内外部相关方，实施一系列治理活动，以确保数据安全，推动发展与安全并重[6]。数据安全治理的核心内涵包括：从战略层面形成自上而下的治理共识；关注数据全生命周期安全；重视管理与技术措施并举；动态适应安全形势与技术演进。

开放教育体系下，数据治理的目标是数据驱动教育发展，管理学校的数据资产，提升学校数据资产价值。数据安全治理的目标是让教育数据的使用更安全，保障数据的安全使用和共享，提升学校数据资产利用效率，促进数据要素价值释放。数据治理是数据质量的提升，通过数据的清洗、稽核、标准化，获得有价值的数据，而数据安全治理是基于数据分类分级实现数据的动态防护，保障数据安全有序流动。开放教育下的数据安全治理将主要关注保护教育数据安全，保护师生隐私。通过制定数据安全管理制度、建立数据安全服务、实施数据传输监管、严控访问权限和审计，构建开放教育数据安全能力体系。

3.2. 开放教育面临的数据安全风险

随着教育数字化深入，在线教育形式多样，直播课、视频课等网络资源丰富，数据资产涵盖师生个人信息、学习行为、课程资源、管理数据等，成为开放教育数字化发展的核心资产。但其多主体共享、全流程流转的特性也带来多重数据安全风险：

(1) 数据泄露：未经授权访问与获取敏感数据。国家开放大学海量师生信息、学分银行数据、考试测评数据等属高价值敏感信息。平台用户层级多、跨域协作频繁，易出现权限管理漏洞，或遭受勒索软件攻击，导致数据被窃取，进而暴露学校教学管理机密，衍生连锁安全风险。

(2) 数据篡改：数据被恶意修改，破坏完整性。学习成绩、学籍档案、学分认定等数据对师生权益至关重要。内部违规操作或外部攻击篡改数据库，可能导致教学评价失真、学分管理混乱，影响学历认证有效性，冲击开放教育公信力。

(3) 数据滥用：数据被用于非授权目的。数据中台汇聚的学习行为、服务记录等数据，可能被违规用于商业推广、精准营销。部分协作机构或技术服务商超出授权范围挖掘数据价值，违背数据收集初衷，破坏数据使用秩序。

(4) 隐私侵犯：个人隐私信息被不当收集与使用。在线教育场景中易出现过度采集师生隐私数据现象，如收集家庭背景、消费习惯等非必要信息。数据流转过程中隐私边界模糊，易导致生物识别信息、学习隐私等泄露或滥用，侵犯师生数据人格权。

尤其是 AI 时代，人工智能技术的迅猛发展为开放教育带来了个性化学习、智能评测、自适应推荐等创新应用，显著提升了教学效率与用户体验。数据不仅是教育运行的基础支撑，更是驱动模型训练与决策的核心要素，数据安全的内涵与外延因此发生深刻变化。国家开放大学作为大规模在线教育实体，其海量、多元、动态的数据资产在赋能 AI 应用的同时，也暴露于风险之中。

4. 构建在线教育数据安全防护体系

随着在线教育平台用户规模与数据资产的快速增长，数据安全已成为平台稳定运营与用户信任的关键要素。针对前文所剖析的安全风险与薄弱环节，本章从制度规范与技术防护两个维度出发，提出一套覆盖事前、事中、事后全生命周期的在线教育数据安全防护体系。该体系以数据安全制度为顶层指引，规范数据全流程的管理职责与操作规范；以隐私数据服务抽离为应用层基础，通过敏感数据集中托管降低暴露面；以数据传输防护监测为通信层屏障，借助加密传输与流量分析保障链路安全；以资源访问权限控制为访问层关卡，依托细粒度授权防止越权访问；以数据库操作审计为追溯层支撑，实现关键操作可记录、可回溯、可追责。如图 1 可见五大模块分工协作，构建覆盖管理、应用、网络、访问与数据库的多层次纵深防御架构，为在线教育平台数据安全提供系统性防护。

Figure 1. Online education data security protection system
图 1. 在线教育数据安全防护体系

4.1. 建立数据安全制度

国家开放大学积极推动数据安全工作，为加强数据安全管理，保护个人与学校合法权益，贯彻落实《网络安全法》《数据安全法》等法律法规，结合《教育部机关及直属事业单位教育数据管理办法》[9]《国家开放大学校务数据管理办法(试行)》等文件，制定并发布《国家开放大学数据安全管理细则(试行)》。

[9]http://www.moe.gov.cn/srcsite/A03/s7050/201802/t20180211_327248.html

细则要求建立数据全生命周期安全保障与监督检查机制，实施数据分类分级管理，指导各部门及办学体系开展数据安全治理，从制度层面保障在线教育数据安全。

同时，我校强化开放体系数据共享安全，制定发布《国家开放大学校务数据共享应用管理细则(试行)》。要求各分部严格按照“申请－审批－使用”流程进行数据共享。校务数据共享应用应当遵循统筹规划、按需共享、依法应用、安全可控的原则。数据共享遵循“谁产生，谁负责”原则，各信息系统主管单位负责明确共享范围与安全防护要求。

面向学校各部门及办学体系的数据共享服务，原则上不提供敏感数据共享，如确需申请敏感数据，敏感数据不允许使用库表对接方式，数据传输必须进行加密或脱敏处理，在提交申请单的同时需提交《国家开放大学数据安全保密承诺书》，履行数据保密义务，并向数字化部提供第三方数据运维人员备案信息。

4.2. 抽离隐私数据服务

在线教育场景中，除常规教学与管理类数据外，还涉及教师与学生的手机号、身份证号等大量高敏感度个人信息。为保障此类隐私数据在存储、访问与交互过程中的安全性，我校从隐私数据存储保障机制与隐私数据访问交互体系两大方面进行系统设计。构建覆盖隐私数据存储与调用的安全服务体系，保障隐私数据安全。

建立多维度的隐私数据存储保障机制。我校制定专门的隐私数据存储方案，确保用户数据在存储过程中得到有效保护。具体包括以下措施：(1) 数据加密：在数据存储前采用 SM4 算法对数据进行加密，即使数据遭遇窃取，攻击者也无法直接读取明文内容，从源头规避数据泄露风险，契合国家数据安全相关规范要求。(2) 访问控制：实施严格的访问控制策略，遵循最小权限原则，明确授权边界，确保仅有授权用户或系统可访问敏感数据；(3) 数据隔离：根据不同机构或部门对数据进行物理或逻辑隔离存储，降低数据泄露与跨域滥用的风险；(4) 数据备份与恢复：定期对数据进行备份，防范意外丢失，并支持快速恢复；备份数据同样采用加密与访问控制手段，确保其存储与使用过程中的安全性。

构建基于微服务架构的隐私数据访问与交互体系。在平台建设层面，通过开放平台改造与功能优化，结合物理层面与技术层面的双重防护，实现隐私数据的集中抽离、规范调用与安全流转，隐私数据微服务架构见图 2。具体包括：

(1) 抽离用户隐私微服务：从物理层面采取单点存储与微服务架构，单独构建用户隐私微服务模块，专门用于存储师生所有个体隐私数据，承担为平台其他业务系统提供隐私数据调用服务的核心功能；改造后，下游业务系统不再保存完整的用户隐私数据，从根本上减少隐私数据的存储节点，避免多系统重复存储风险，降低泄露隐患。

(2) 规范隐私数据调用机制：其他系统按需获取用户隐私字段的脱敏或摘要信息，严禁保存隐私数据原文；若确需查看原文，仅可通过 API 接口方式从隐私微服务中获取单条原文数据，且调用行为全程留痕；如因特殊业务要求必须存储原文，则禁止对原文进行修改，并严格遵循前述存储方案中的加密要求进行保存，且定期更新密钥。

(3) 构建独立密钥体系：技术层面采用对称加密与非对称加密相结合的混合加密策略，要求各业务系统分别配置至少一套国密 SM2 非对称加密密钥，各系统密钥相互独立、互不干扰；同时要求加密参数动态生成并定期更新，密钥实行有限期管理，有效防范长期使用同一密钥带来的泄露风险，为数据加密传输提供双重安全支撑。

(4) 优化数据加密传输流程：当 A 系统通过 API 接口调用用户隐私微服务获取隐私数据时，需先向微服务提供自身公钥；用户隐私微服务接收请求后，采用该公钥对隐私数据进行加密处理，再将加密后的密文数据返回给 A 系统；A 系统接收后，使用自身私钥进行解密，确保数据在传输过程中不被窃取、

篡改；同时严格控制 API 调用频次与数据请求量，从源头降低隐私数据被滥用的可能，实现隐私数据调用全流程加密防护与规范管控。

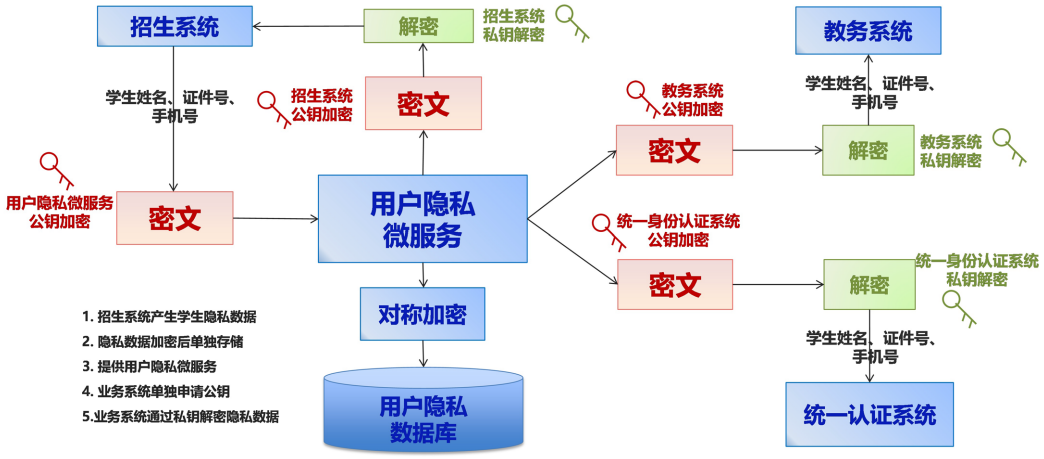

Figure 2. Privacy data microservice architecture
图 2. 隐私数据微服务架构

4.3. 防护监测数据传输

当前，国家开放大学一网一平台各系统间的数据传输均通过 API 接口实现请求与交互，数据传输环节的安全直接关系学校整体数据安全成效。为此，我校上线 API 安全监测防护系统，实现对全平台 API 接口的统一监管与安全防护。

API 安全监测防护系统对我校网络数据流量进行数据解密，分析流量数据，识别网络中的 API 资产信息，并提供基于 API 级别的资产发现能力、敏感数据分析识别能力以及威胁攻击的检测能力。平台架构如图 3 所示：

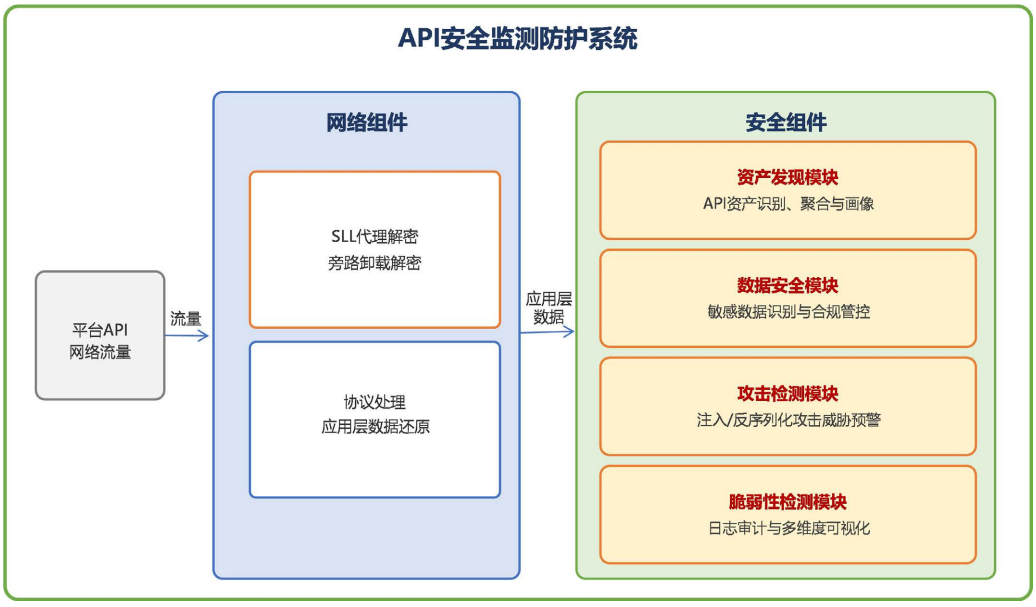

Figure 3. API security monitoring and protection system
图 3. API 安全监测防护系统

API 安全监测防护系统共包含两个组件，通信组件和安全组件。

(1) 网络组件

网络组件为平台提供基础网络通路，负责数据收发与协议处理。基于 TCP/IP 网络协议栈与旁路协议栈，实现 SSL 代理解密与旁路卸载解密能力，为后续安全分析提供完整的应用层数据内容。

(2) 安全组件

安全组件作为平台核心能力层，接收网络组件传输的应用层数据，完成 API 数据分析、提取与格式化日志生成，核心包含四大功能模块：(a) 资产发现模块：盘点 API 资产，动态更新资产画像，对流量中 API 类型和流量特征进行识别，区分 API 资产和非 API 资产，进行 API 资产的识别、聚合、功能标签的标记等；(b) 数据安全模块：精准识别敏感数据，管控数据流转合规性，针对网络流量中通过 HTTP 协议传输的数据(包括文件)，根据预定义和自定义的规则，检查是否存在相关的敏感数据。(c) 攻击检测模块：实时监测异常访问与恶意攻击行为，实现威胁预警，数据处理阶段可能会存在各种注入攻击、反序列化攻击，数据在入库阶段可能会存在 SQL 注入攻击；(d) 脆弱性检测模块：涵盖日志审计、资产可视化、行为可视化及数据泄露可视化等功能，通过多维度可视化呈现与全链路审计，为开放教育数据传输安全提供动态可视的监测与防护能力。

此架构通过网络层与安全层协同联动，实现 API 安全的全流程管控，为国家开放大学教育数据传输提供有效安全防护。

4.4. 控制资源访问权限

资源访问权限控制方面，我校部署云堡垒机，集中管理资源及资源账户，实现对资源账户的全生命周期管理。用户可通过单点登录方式访问资源，实现管理操作与运维任务的无缝衔接。通过云堡垒机可实现主机资源、应用资源、云服务(含容器资源)及数据库资源的纳管。基于云堡垒机的安全保障体系，实现了以下安全管理，具体监测指标如表 1 所示：

(1) 账号管理：集中管理系统用户与资源账户信息，构建覆盖账号全生命周期的可视、可控、可管的运维管理体系。

(2) 权限管控：集中管控用户对系统及资源的访问权限，实现细粒度的权限设置，保障系统管理安全与资源运维安全。

(3) 操作审计：基于用户身份的唯一标识，从用户登录系统开始，全程记录用户在系统中的操作行为，监控并审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。

Table 1. Dynamic monitoring indicators for resource access
表 1. 资源访问动态监测指标

监测维度	监测指标	审计与预警说明
会话概览	在线会话数、活跃资源数、当日新增会话	实时汇总资源访问会话状态，掌握访问规模与活跃度
访问账号	登录用户数、访问来源分布	基于唯一身份标识全程记录用户对资源的访问行为
操作审计	高风险操作数、操作类型分布	记录并审计用户对目标资源的关键操作，支持事后追溯
访问趋势	会话数时序变化、访问频次趋势	通过趋势曲线识别访问异常波动，辅助容量与安全研判
风险预警	异常访问事件、越权访问告警	对越权、异常访问等安全事件实时发现与预警

4.5. 审计数据库操作记录

国家开放大学数据库系统承载着学校的招生数据、考试数据、教务数据、师生敏感数据等重要信息。

容易受到外部攻击者利用 Web 应用程序实施的攻击以及内部员工利用更直接的权限实施的攻击，存在着诸多安全性风险。各信息系统在日常运行过程中无审计机制，学校无法对维护内部控制系统及相应控制程序做出充分有效的评价；同时也会导致安全事件难于追溯、安全事件难于定位、无法追溯事故责任人等问题。基于此，国家开放大学上线数据库安全审计系统，对国家开放大学考务、教务、招生、科研、师资、认证及学习网等业务系统的数据库进行数据操作审计、数据访问异常检测和预警、数据安全风险评估。

国家开放大学数据库安全审计系统，对内部用户在数据库中的所有操作进行审计，包括查询、修改、删除等，并将这些操作记录保存到审计日志中，比如用户隐私微服务，记录哪个用户(Who)通过哪个应用(App)在哪个时间点(When)在哪里(Where)查看了哪个用户(Who)的什么隐私数据(What)。实时检测数据库中的异常操作，例如异常查询、异常修改、异常删除等，以防止恶意操作或误操作导致的数据损失。发现异常操作后及时发出警报，以便学校及时采取措施阻止这些操作，保护数据的安全性和完整性。定期对数据库的安全风险进行评估，以确定存在的安全漏洞和威胁，并采取相应的措施进行防范。提供安全风险评估报告，列出存在的安全风险和威胁，帮助学校制定更加完善的数据安全策略。

5. 结语

教育数据是驱动教育数字化转型的核心要素，本文以国家开放大学为研究对象，围绕开放教育数据安全能力体系的构建展开探讨，提出了集制度规范与技术防护于一体、覆盖应用、传输、访问与数据层的多层次纵深防御体系，为开放教育机构数据安全治理提供了可行路径。展望未来，随着大模型、智能体与多模态学习应用在开放教育中的深度落地，数据安全将面临训练语料泄露、模型反演、Prompt 注入等新型威胁。后续研究将持续深化，融合人工智能实现风险的智能感知与主动处置，在保障数据“可用不可见”的前提下释放开放教育数据要素价值，构建适应智能时代的数据安全能力体系，推动开放教育数据安全能力向智能化、动态化与生态化方向发展。

基金项目

本文系中国教育技术协会网络安全专业委员会 2025 年度教育网络安全专项研究课题“基于联邦学习的跨机构教育数据共享及模型效果优化研究”(课题编号：CAETCS25011)、数字化学习技术集成与应用教育部工程研究中心 2024 年创新基金项目“面向人工智能的终身教育领域高质量数据资源治理与应用研究”(项目编号：1441001)的阶段性研究成果。

参考文献

[1] 教育部关于加强新时代教育管理信息化工作的通知[EB/OL]. http://www.moe.gov.cn/srcsite/A16/s3342/202103/t20210322_521669.html, 2021-03-10.

[2] 教育部等七部门关于加强教育系统数据安全工作的通知[EB/OL]. https://xxzx.hebcm.edu.cn/col/1559021415599/2023/05/16/1684228560091.html, 2023-05-16.

[3] 教育部等九部门关于加快推进教育数字化的意见[EB/OL]. https://www.gov.cn/zhengce/zhengceku/202504/content_7019045.htm, 2025-04-11.

[4] 魏顺平, 袁亚兴, 吴淑苹, 等. 基于云服务的教育信息化精准扶贫模式研究——以国家开放大学扶贫实践为例[J]. 中国电化教育, 2020(9): 74-81.

[5] European Parliament and Council of the European Union (2026) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] 中关村网络安全与信息化产业联盟数据安全治理专业委员会. 数据安全治理白皮书 5.0 [R]. 北京: 中关村网络安全与信息化产业联盟, 2023.

[7] International Organization for Standardization (2022) Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements: ISO/IEC 27001:2022. International Organization for Standardization.

[8] 国家市场监督管理总局, 中国国家标准化管理委员会. GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型[S]. 北京: 中国标准出版社, 2019.

[9] 吴信东, 董丙冰, 堵新政, 等. 数据治理技术[J]. 软件学报, 2019, 30(9): 2830-2856.