大规模在线教学中的网络安全研究

王家乾　张渊伟　侯丽媛
内蒙古开放大学　内蒙古呼和浩特　010011

摘　要：本文分析大规模在线教学在教育数字化转型中的安全挑战，聚焦数据保护、学术诚信与系统架构安全风险，提出构建技术与管理协同的防护体系，依托数据全生命周期加密、多模态生物识别、微服务架构等技术手段，结合零信任访问控制与用户行为规范，形成动态防御闭环，为在线教育可持续发展提供可信保障，实现开放共享与安全可控的动态平衡。

关键词：大规模在线教育；数据保护；学术诚信；系统安全

推进教育现代化，建设教育强国，数字化转型是关键之举，更是核心支撑。党的二十大报告也指出：“要推进教育数字化，建设全民终身学习的学习型社会、学习型大国。”[1]大规模在线教学作为教育数字化的重要体现，能够为有需求的学习者提供在线学习资源，实现了以“学习者”为中心的目标，消除了传统学习环境下的时空障碍[2]，使得优质教育资源得以广泛传播与共享，促进了个性化学习和终身学习理念的实践。

然而，随着在线教学规模的扩大，网络安全问题也日益凸显。一方面，教师和学生的信息隐私保护成为重点，包括个人信息、学习数据等敏感信息的安全存储与传输；另一方面，在线教学平台易遭受网络攻击，如DDoS攻击可能导致服务中断，影响在线教学的秩序。所以确保在线教学环境的安全稳定，完善技术防护措施、强化网络安全及学术诚信意识，对于推动教育数字化转型具有重要意义。

一、大规模在线教学的特征

大规模在线教学的核心特征在于其开放性与包容性。这类教学方式突破了传统教育的时空限制，向各地的学习者开放教学，例如国家开放大学打造的“一网一平台”，平台中课程内容覆盖学科广泛，可以满足不同领域学习者的需求，适合在职人士、全职家长等无法固定参与传统课堂的人群。大规模在线教学方式还实现了多样化教育资源的共享，单门课程可容纳数万甚至数十万学员，使优质教育资源得以跨越地域鸿沟，惠及更多人。这种模式不仅降低了教育门槛，还推动了教育公平，让更多人有机会接触优质的课程内容。

大规模在线教学的分布性与互动性则是体现了其独特的学习生态。尽管学习者分布在全国各地，但通过在线论坛、实时讨论区、协作项目等工具，学生之间可以互相交流、答疑解惑，甚至形成学习社群。教师与助教也会通过问答板块或直播答疑提供支持，形成“分布式”的教学网络。大规模在线教学方式通过持续的技术创新和模式优化，正不断拓展教育的边界，成为全国各地学习者知识共享与终身学习的重要载体。

二、大规模在线教学面临的安全挑战

大规模在线教学的形式广泛，例如中国大学MOOC，或国家开放大学的终身教育平台等，这些平台都面向着广泛的非传统学生群体，也由于大规模在线教学形式的开放性，导致了其面临着严峻的安全挑战。以下则对一些可能存在的安全问题进行分析。

（一）数据隐私与用户信息保护的困境

大规模在线教学平台需要收集、存储和处理海量用户数据，包括个人身份信息、学习记录、支付信息以及学习行为数据。这些数据的敏感性远超普通在线服务的普通日志数据，一旦泄露或滥用，可能导致严重的后果。例如，用户的身份信息可能被用于网络诈骗、身份盗用或精准广告推送；学习行为数据可能被第三方公司获取并用于商业分析，进一步侵犯个人隐私。

数据泄露的风险源于技术漏洞、外部攻击和人为失

课题或基金项目：内蒙古开放大学科学研究一般课题“大规模在线教学中的网络安全研究”（课题编号：IMOU-GSR2435）

作者简介：王家乾，出生年：1997.10，性别：男，民族：蒙古族，籍贯：内蒙古乌兰察布市察哈尔右翼前旗，单位：内蒙古开放大学，职称：讲师，学位：硕士研究生，主要研究方向：计算机技术。

误。例如2023年南昌公安监测发现，南昌的某高校3万余师生个人信息数据在境外互联网上被公开售卖，其原因是在开展数据处理活动中，未建立全流程数据安全管理制度，未采取技术措施保障数据安全，未履行数据安全保护义务，导致学校存储教职工信息、学生信息、缴费信息等3000余万条信息的数据库被黑客非法入侵。[3]人为失误则如用户使用简单密码、重复使用密码登录不同平台以及随意点击陌生网站链接等安全意识不足的个人行为，也是增加用户信息泄露风险的重要因素。

（二）学术诚信与身份验证的漏洞

大规模在线教育的开放性特征，不可避免的会导致学术诚信问题。在这种开放的在线学习场景中，由于学习者的地理分布广泛且身份验证困难，使得替考舞弊、智能代写、辅助刷课等行为形成灰色产业链，这些技术性作弊手段已对教育评价的客观性构成威胁，破坏了教育的公平性。另外，生成式人工智能的快速发展也正在突破文献检测系统的识别边界，当前的文献检测系统即便是专业的人工智能生成内容检测，在应对生成式人工智能生成的内容时，也面临语义缺失、特征模糊化等技术瓶颈，这导致学术诚信的问题会更容易发生。

而身份验证技术的局限性进一步加剧了这些问题。尽管人脸识别、屏幕监控、远程监考系统等技术被广泛应用，但仍会受到技术条件限制。例如静态人脸识别可能被高仿真照片或视频破解，屏幕监控可能因网络延迟或设备故障失效等。另外在设备配置不足与网络基础设施薄弱的地区，用户只能选择低安全级别的认证方式，从而留下安全漏洞。[4]

（三）系统安全与基础框架的长期隐患

大规模在线教学平台的运行依赖于复杂的底层技术架构，包括服务器集群、数据库、学习管理系统以及与第三方工具的集成，这些系统之间相互关联，一旦出现安全漏洞就可能引发大规模服务中断或数据泄露。例如将学习管理系统作为核心枢纽，其代码中的漏洞或第三方插件如果被攻击者利用并加以攻击，会导致学习管理系统出现瘫痪或死机，造成教学进程滞后。

技术系统的复杂性与老旧架构的矛盾也构成潜在风险。学习平台在快速扩张规模的过程中，如果代码漏洞或架构缺陷未被充分修复就进行多次的快速迭代，短时间内可能不会造成影响，但长期如此就会导致系统被攻破的风险大大提升。另外学习平台如果为提升用户体验引入的前沿技术，其复杂功能本身就存在新型风险，如果存在漏洞，则可能在数据交互过程中泄露用户隐私。

因此，大规模在线教学的安全挑战是多维度、系统性的，且因开放性、分布性等特征使其愈发复杂。这些安全问题涉及到技术漏洞、用户行为、政策监管及社会信任等层面，成为了制约大规模在线教学可持续发展的核心挑战。

三、网络安全技术赋能路径以及防护对策体系

在智能时代，在线教育既有历史的继承又有创新的发展，在线教学变革要契合社会多样化、个性化人才培养的诉求。[5]如今教育正处于一个深度信息化的“大变局”时期，技术与教育已呈现融合创新态势。因此大规模在线教学的网络安全挑战需要从多维度构建防护体系，可以通过自动化、智能化手段加强数据保护与系统安全架构，规范学术行为，重点针对存储、访问以及权限进行实时监管，强化预防、发现、消除风险隐患的能力和手段。[6]

（一）构建数据保护体系，强化信息防护

在大规模在线教学系统中，数据保护需通过系统化的策略降低敏感信息暴露风险，重点可以围绕数据全生命周期管理，采用加密、脱敏等技术手段保障存储与传输安全，例如在数据传输过程中使用端到端加密技术，在存储时采用AES–256等高强度加密算法，确保即使数据被截取也无法被直接读取。从权限角度看，还应建立权限分级管理制度，对敏感数据实施零信任架构强化访问控制，确保最小权限原则。例如，平台需在用户注册时明确告知数据用途，并提供最小必要原则下的数据收集选项[7]。还需要建立数据安全事件应急响应机制，制定网络安全预案并定期开展攻防演练，确保在遭受攻击时能快速隔离风险、追溯泄露路径，这样就可以强化事前预防、事中监测与事后响应的闭环管理，形成覆盖全流程的信息保护体系。

除了大规模在线教学平台技术因素之外，降低人为因素导致的数据泄露风险也需用户的意识提升与行为规范双向发力。常态化开展用户网络安全培训，对用户采用模拟钓鱼攻击、密码强度测试等互动形式，引导用户摒弃简单密码、重复使用密码等高风险行为，减少非技术因素导致的数据泄露风险。

（二）强化学术诚信环境，遏制作弊行为

大规模在线教育中一直存在着学生身份验证的问题，这也是导致学术诚信问题发生的重要因素。针对远程身份验证，可通过融合生物识别、行为分析等技术手段，提升身份认证的可靠性，从而确保考试与作业提交的真实性。例如学习平台可以部署多模态生物识别系统，将人脸动态活体检测、动态验证码、键鼠行为分析相结合，

或在远程考试中同步调用摄像头以及多种输入设备传感器数据，捕捉学生面部表情、操作行为及环境声音，结合AI算法判断，实时比对用户是否存在代考行为。[8]

面对生成式人工智能的安全威胁需要筑牢安全防线，学习平台可以通过前沿机器学习方式整合多种学习平台数据来训练AI识别模型，捕捉生成文本的语义断层与风格异常，或引入水印技术检测文本中的模式特征，识别非人类创作痕迹，对作业、论文等内容进行实时比对与异常检测，从而有效识别抄袭、AI代写等违规行为。

另外技术手段也需要与管理制度协同作用，平台可以通过分层认证流程、匿名举报渠道、透明规则以及案例公示等方式，形成技术与管理协同的监督网络，完善学术诚信体系，推动大规模在线教育的建设，为教育公平性提供保障。

（三）完善系统安全架构，降低长期隐患

面对网络环境复杂化与攻击手段智能化，要解决系统架构的复杂性问题，可以通过零信任架构与自动化防御技术增强系统健壮性。例如采用微服务架构与容器化技术，将系统拆分为独立模块，降低单一环节被攻击导致的连锁风险。另外针对系统迭代更新产生的漏洞或缺陷，可以构建平台问题可视化系统，对未修复漏洞进行优先级标记与跟踪，及时解决系统隐患。针对涉及AI的新型功能模块，需在训练阶段采用联邦学习框架与差分隐私技术清洗数据[9]，特别是增强非结构数据的分类分级工作，实施分级管控，对训练数据进行来源追溯与使用审计，确保数据流转可查可控。

除预防安全隐患外，应急预案也是关键，平台需要明确数据泄露、服务中断等场景的响应流程。例如可以通过多区域数据中心同步备份数据，并设置好自动切换机制，以备在安全问题发生后能够及时进行应对处理，服务器被攻击时，系统自动切换至备用节点，可以确保服务的连续性，减少意外因素导致的教学进程滞后。

大规模在线教学的网络安全防护需通过技术赋能与体系化对策构建综合防御体系。通过构建数据保护体系、强化学术诚信环境与完善系统安全架构的路径，为大规模在线教学提供坚实的安全防护。网络安全体系的建设应始终服务于教育质量提升与教育公平保障，为在线教育生态的发展提供支撑，保障在线教育的可信度与可持续发展。

四、结论与展望

大规模在线教学作为教育数字化转型的一部分，通过突破时空限制、整合优质资源、支持个性化学习，已成为推动教育现代化的重要载体。通过技术创新与制度优化形成网络安全的动态防御，方能实现教育公平与安全可信的结合，但大规模在线教育因其自身的特殊性，仍会面临技术碎片化、政策执行差异及用户意识不足等安全隐患。

大规模在线教学的安全防护体系需在技术迭代、政策协同与生态共建三个维度持续深化发展。随着量子加密、边缘计算等新兴技术的发展，数据隐私保护将向动态化、智能化方向演进，分布式智能身份验证也有望突破学术诚信监管的局限性。同时也需要加快构建覆盖政府、学校、企业的协同治理机制，推动《数据安全法》《个人信息保护法》在教育场景的落地实施，建立网络安全责任追溯与跨域联防联控体系，着力培育“技术–教育–社会”三元融合的教育生态，开展全民数字素养提升工程，形成多方共建共治的安全文化，才能为教育数字化构筑坚实的安全堡垒，最终构建更安全、更包容的数字教育生态。

参考文献

[1] 习近平.高举中国特色社会主义伟大旗帜为全面建设社会主义现代化国家而团结奋斗[N].人民日报，2022-10-26（001）.

[2] 何如珍.在线学习环境下的网络信息安全[J].电子技术与软件工程，2021，（07）：257-258.

[3] 内蒙古工业大学，网络空间安全研究所，《2023年网络安全事件处罚案例》.

[4] 张孝存，蒲菲.地方高校学生在线学习体验的影响因素及改进路径[J].西部素质教育，2023，9（04）：9-12.

[5] 王开，汪滢.智能时代”因材施教”的回归与超越——基于教学范式变革的历史考察[J].河南大学学报：社会科学版，2021，61（6）：114-122.

[6] 孔祥宇.后疫情时代高校在线开放课程网络安全与管理探析[J].中国信息安全，2022，（06）：87-89.

[7] 敖颜思文.在线教育平台用户个人信息保护与开发研究[J].河南广播电视大学学报，2022，35（01）：55-60.

[8] 杨柳群.高校在线评估中学术诚信及测试安全研究[J].高教学刊，2023，9（35）：22-25+30.

[9] 何泽平，许建，戴华，等.联邦学习应用技术研究综述[J].信息网络安全，2024，24（12）：1831-1844.