

BẢO MẬT DỮ LIỆU VÀ AN TOÀN THÔNG TIN TRONG GIÁO DỤC MỞ

Lâm Văn Ân¹, Nguyễn Đình Tường¹, Nguyễn Minh Dũng¹, Phạm Quang Huy¹

Email: anl@hou.edu.vn. ORCID: 0009-0005-4064-3486

Ngày tòa soạn nhận được bài báo: 06/07/2026

Ngày hoàn thành đánh giá: 05/10/2026

Ngày bài báo được duyệt đăng: 19/10/2026

DOI: 10.59266/houjs.2026.1514

Tóm tắt: Bài viết phân tích các nguy cơ về bảo mật dữ liệu và an toàn thông tin trong giáo dục mở, đồng thời đề xuất một khung nguyên tắc gắn với các cơ chế kỹ thuật có thể kiểm tra. Đặc tính mở làm phát sinh ba căng thẳng: giữa tiếp cận nội dung và bảo vệ quyền sử dụng; giữa cá nhân hóa và quyền riêng tư của người học; giữa liên thông, mở rộng quy mô và chủ quyền dữ liệu. Bài viết phân biệt tài nguyên giáo dục mở, nội dung hạn chế và dữ liệu người học; xây dựng ma trận rủi ro bốn lớp; đồng thời đề xuất ba nguyên tắc thiết kế bảo mật gắn với quản trị khóa, URL ký số có phạm vi, mã giả hóa, nhật ký kiểm toán, phân tầng hạ tầng và quyền quyết định của con người khi sử dụng AI. Phương pháp là phân tích tài liệu có cấu trúc trong giai đoạn 2018-2025, kết hợp đối chiếu các nghiên cứu học thuật, khung tham chiếu an toàn thông tin và tài liệu kiến trúc công khai. Bài viết không tuyên bố hiệu quả thực nghiệm mà cung cấp một kiến trúc tham chiếu và các tiêu chí để kiểm chứng trong LMS cụ thể.

Từ khóa: giáo dục mở, an toàn thông tin, bảo mật dữ liệu, dữ liệu người học, phân tích học tập, trí tuệ nhân tạo có trách nhiệm

I. Mở đầu

Giáo dục mở mở rộng quyền tiếp cận học liệu, khóa học, dữ liệu học tập và các công cụ hỗ trợ học tập vượt ra ngoài lớp học truyền thống. Tuy nhiên, “mở” không đồng nghĩa với công khai mọi dữ liệu hoặc bỏ qua kiểm soát truy cập. Một hệ sinh thái giáo dục mở thường đồng thời chứa tài nguyên giáo dục mở (OER), tài liệu có điều kiện sử dụng, tài khoản định danh và dữ liệu hành vi học tập. Nếu các

lớp dữ liệu này bị xử lý như nhau, chính sách mở có thể làm tăng nguy cơ vi phạm bản quyền, lộ thông tin cá nhân và thao túng kết quả phân tích học tập.

Các nghiên cứu tổng quan gần đây cho thấy tính mở của OER có ít nhất hai phương diện: mở về pháp lý và mở về kỹ thuật; một tài nguyên có giấy phép mở nhưng vẫn có thể khó truy cập, khó tái sử dụng hoặc thiếu siêu dữ liệu (Sousa và cộng sự, 2023). Trong phân tích học tập,

¹ Trường Đại học Mở Hà Nội, Hà Nội, Việt Nam

rủi ro lại phát sinh trên toàn bộ vòng đời dữ liệu, từ thu thập, liên kết, suy luận đến chia sẻ và lưu giữ (Liu và Khalil, 2023). Vì vậy, bài viết này tập trung vào ba vấn đề:

- 1) Tiếp cận mở và bảo vệ quyền sử dụng nội dung;
- 2) Cá nhân hóa và quyền riêng tư của người học;
- 3) Liên thông, mở rộng quy mô và chủ quyền dữ liệu.

Mục tiêu của bài viết là đưa các vấn đề trên thành các nguyên tắc có thể kiểm tra bằng cơ chế kỹ thuật. Bài viết đóng góp: một ma trận rủi ro bốn lớp; ba nguyên tắc thiết kế bảo mật gắn với kiểm soát cụ thể; kiến trúc tham chiếu cho một hệ thống quản lý học tập mở; và một khung quản trị ngăn cho mô hình AI cá nhân hóa. Đây là phân tích tài liệu và thiết kế tham chiếu, không phải đánh giá thực nghiệm một hệ thống triển khai thực tế.

II. Cơ sở lý thuyết

Rủi ro bảo mật trong giáo dục mở được phân tích theo các tầng kỹ thuật của một hệ thống LMS/OER điển hình. Trong nghiên cứu này, Ba nhóm dữ liệu và nội dung cần được phân biệt gồm: (1) tài nguyên giáo dục mở (OER); (2) tài liệu hạn chế, chẳng hạn nội dung thương mại, để

kiểm tra chưa công bố, video có điều kiện bản quyền hoặc tài liệu chỉ dành cho một nhóm học viên; (3) dữ liệu người học, bao gồm thông tin định danh, thông tin nhân khẩu học, nhật ký truy cập, kết quả học tập, dữ liệu thiết bị và các biến suy luận như ‘nguy cơ bỏ học’... Ba nhóm này có mục đích xử lý và mức bảo vệ khác nhau.

Bảo mật từ khâu thiết kế đặt các mục tiêu bí mật, toàn vẹn, sẵn sàng và khả năng truy vết vào kiến trúc ngay từ đầu. Quyền riêng tư từ khâu thiết kế bổ sung các nguyên tắc giảm thiểu dữ liệu, giới hạn mục đích, minh bạch, quyền can thiệp và thời hạn lưu giữ. Hai cách tiếp cận liên quan nhưng không đồng nhất: mã hóa một tệp giúp bảo mật nội dung, song không tự quyết định dữ liệu nào được phép thu thập hay bao lâu được lưu giữ.

Đối với phân tích học tập, cần coi dữ liệu là một dòng chảy có các điểm chuyển giao. Mỗi điểm phải trả lời bốn câu hỏi: dữ liệu nào được thu thập; ai được truy cập; mục đích nào được phép; và khi nào dữ liệu phải xóa hoặc chuyển sang dạng tổng hợp. Tổng quan của Liu và Khalil (2023) và Prinsloo và cộng sự (2023) nhấn mạnh rằng rủi ro không chỉ nằm ở cơ sở dữ liệu mà còn ở việc liên kết nhiều nguồn và suy luận các thuộc tính nhạy cảm từ dữ liệu tưởng như vô hại.

Bảng 1: Ma trận rủi ro và cơ chế kiểm soát trong giáo dục mở

Tầng	Rủi ro chính	Điểm kiểm soát	Biện pháp kỹ thuật
Nội dung học liệu	Phát tán, quay lén hoặc giả mạo học liệu	Quyền truy cập và tính toàn vẹn	DRM, watermark, URL có thời hạn và chữ ký số
Danh tính và phân quyền	Xác thực yếu, dùng chung tài khoản, quyền truy cập tồn dư	Danh tính và phạm vi quyền	Xác thực phù hợp, phân quyền theo vai trò và theo tài nguyên
Dữ liệu hành vi	Dùng sai mục đích, lưu quá hạn, tái định danh	Mục đích và vòng đời dữ liệu	Giảm thiểu dữ liệu, giả danh hóa, tự động xóa theo thời hạn
Hạ tầng vận hành	Mất mát, lộ lọt dữ liệu, DDoS và ransomware...	Khả năng phục hồi sau thảm họa	Quản lý khóa độc lập, sao lưu có kiểm thử, WAF và giám sát tập trung

Nguồn: tác giả

III. Phương pháp nghiên cứu

Bài viết sử dụng phương pháp phân tích tài liệu có cấu trúc trong giai đoạn 2018-2025; một số văn bản chính sách ban hành sau đó chỉ được dùng để đối chiếu định hướng. Phương pháp này được lựa chọn vì mục tiêu là xây dựng khung thiết kế và quản trị, không phải ước lượng hiệu quả can thiệp. Các nhóm nguồn gồm: (i) bài báo bình duyệt và bài tổng quan về OER, phân tích học tập, quyền riêng tư và công bằng thuật toán; (ii) tiêu chuẩn, khung quản trị an toàn thông tin và AI; (iii) tài liệu kiến trúc công khai của các nền tảng giáo dục quy mô lớn.

Để kiểm tra tính nhất quán, bài viết sử dụng hai lớp phân tích. Lớp thứ nhất là lập bản đồ STRIDE cho tài sản và luồng dữ liệu, kết hợp LINDDUN (Wuyts và cộng sự, 2020) cho các nguy cơ riêng tư như liên kết, nhận diện, không biết và không tuân thủ. Lớp thứ hai là đối chiếu các kiểm soát với các nhóm chức năng của NIST Cybersecurity Framework 2.0 và các yêu cầu quản trị dữ liệu của ISO/IEC 27001: 2022. Việc đối chiếu chỉ nhằm kiểm tra độ bao phủ của đề xuất.

Ba trường hợp so sánh trong mục 4.4 được dùng như minh họa kiến trúc, không phải nghiên cứu tình huống đánh giá hiệu quả. DIKSHA và Moscow Electronic School được xem xét qua tài liệu kiến trúc/chính thức công khai, với cùng ba tiêu chí: phân tầng dịch vụ và dữ liệu; hỗ trợ liên thông hoặc ngoại tuyến; và cơ chế quản trị truy cập.

IV. Kết quả nghiên cứu và thảo luận

4.1. Nguyên tắc thiết kế bảo mật gắn với cơ chế kỹ thuật cụ thể

Từ ma trận rủi ro và đối chiếu tài liệu, bài viết đề xuất ba nguyên tắc. Nguyên tắc thứ nhất bảo vệ chủ quyền

và vòng đời dữ liệu; nguyên tắc thứ hai phân biệt mức mở và giảm thiểu dữ liệu; nguyên tắc thứ ba duy trì trách nhiệm của con người khi sử dụng AI. Mỗi nguyên tắc dưới đây đều được diễn đạt thành yêu cầu có thể kiểm tra trong thiết kế và vận hành.

4.1.1. Chủ quyền dữ liệu và quản trị công gắn với kiến trúc lưu trữ và mã hóa có kiểm soát khóa độc lập

Chủ quyền dữ liệu không chỉ là nơi đặt máy chủ mà là quyền quyết định dữ liệu nào được thu thập, ai được dùng, dùng cho mục đích gì, trong bao lâu và được chuyển đi đâu. Hệ thống nên lập danh mục tài sản dữ liệu, gắn chủ sở hữu và phân loại mức nhạy cảm. Dữ liệu định danh và dữ liệu học tập chi tiết cần được lưu ở vùng tin cậy cao; dữ liệu OER công khai có thể nằm ở vùng phân phối rộng hơn.

Cơ chế kỹ thuật cần tách biệt nơi lưu trữ dữ liệu với quyền kiểm soát truy cập dữ liệu, mã hóa dữ liệu khi lưu trữ với khóa do đơn vị giáo dục quản lý, thông qua một hệ thống quản lý khóa độc lập. Mã hóa dựa trên thuộc tính (ABE) có thể phù hợp khi chính sách truy cập phụ thuộc vào vai trò, khóa học hoặc địa bàn; tuy nhiên, tổng quan của Kumar và cộng sự (2018) cho thấy các vấn đề thu hồi, chi phí tính toán và mở rộng vẫn phải được kiểm thử. Vì vậy, ABE chỉ nên áp dụng cho tài liệu hạn chế, không trở thành điều kiện mặc định đối với OER.

4.1.2. Bảo mật từ khâu thiết kế và ẩn danh hóa gắn với kiểm soát nội dung số và giảm thiểu dữ liệu

Hệ thống cần tách ba chính sách: OER được phép tải và tái sử dụng theo giấy phép; nội dung hạn chế được cấp quyền theo phạm vi; dữ liệu người học được thu thập tối thiểu theo mục đích. Với

OER, chữ ký nội dung, kiểm tra toàn vẹn, siêu dữ liệu giấy phép và quản lý phiên bản thường phù hợp hơn DRM. Với nội dung hạn chế, URL ký số phải ràng buộc tài nguyên, người dùng/nhóm, thao tác, thời hạn, nonce hoặc cơ chế chống phát lại; chỉ đặt thời hạn ngắn không đủ để bảo đảm kiểm soát.

Bí danh thay thế định danh trực tiếp nhưng vẫn cho phép tái liên kết có kiểm soát; còn ẩn danh hóa dữ liệu hướng tới loại bỏ khả năng tái nhận diện hợp lý. Trong hỗ trợ người học có nguy cơ bỏ học, việc sử dụng bí danh sẽ phù hợp hơn: mô hình chỉ nhận mã giả, còn bằng ảnh xạ được mã hóa và đặt trong kho riêng; chỉ cán bộ được ủy quyền mới có thể mở đường dẫn tái liên kết, và mọi lần mở phải được ghi log.

4.1.3. Trách nhiệm trong kỷ nguyên AI gắn với ràng buộc kỹ thuật và quyền quyết định của giáo viên

Các yêu cầu “dán nhãn AI rõ ràng” và “giáo viên có quyền kiểm soát cuối cùng” phải được thể hiện trong cả giao diện người dùng lẫn kiến trúc hệ thống:

Mọi đầu ra từ mô hình AI cần được gắn cờ nguồn gốc ở tầng dữ liệu, không chỉ ở giao diện hiển thị.

Thiết kế luồng phê duyệt bắt buộc có bước xác nhận của giáo viên trước khi bất kỳ đầu ra AI nào (đặc biệt là đánh giá/chấm điểm) được coi là chính thức.

Đối với các mô hình phân tích dự đoán (ví dụ dự đoán nguy cơ bỏ học từ dữ liệu hành vi LMS), cần có ràng buộc kỹ thuật giới hạn phạm vi người có quyền xem kết quả dự đoán, tránh việc một chỉ số dự đoán rủi ro trở thành nhãn dán gắn với học sinh trong toàn bộ hồ sơ học tập.

Về kỹ thuật, hệ thống cần phân quyền theo vai trò, lưu phiên bản mô hình và đầu vào, kiểm soát truy cập API, phát hiện thay đổi dữ liệu và ghi lại quyết định cuối cùng của giáo viên. Kiểm tra công bằng phải được thực hiện theo nhóm có ý nghĩa giáo dục; không nên suy luận rằng một mô hình có độ chính xác chung cao là công bằng. Nghiên cứu về tính công bằng trong phân tích dự đoán cho thấy hiệu năng có thể khác đáng kể giữa các nhóm, do đó cần báo cáo cả dương tính giả, âm tính giả và độ thu hồi.

4.2. Ứng dụng AI có trách nhiệm trong giáo dục mở qua trường hợp dự đoán nguy cơ bỏ học

Phần này xem xét một ứng dụng ngày càng phổ biến trong các nền tảng LMS: mô hình dự đoán nguy cơ bỏ học dựa trên dữ liệu hành vi. Trường hợp này cho thấy ngay cả một ứng dụng hữu ích cũng cần khung quản trị kỹ thuật chặt chẽ để có thể triển khai an toàn.

Khác với AI tạo sinh, mô hình dự đoán bỏ học thuộc nhóm AI phân tích. Mục tiêu là phát hiện sớm học sinh, sinh viên có nguy cơ thôi học để nhà trường hỗ trợ kịp thời. Vì mục tiêu này có vẻ tích cực, ứng dụng thường không được xem xét đầy đủ trong các đánh giá rủi ro bảo mật.

4.2.1. Rủi ro đặc thù của loại mô hình này

Nhãn dán cố định: một khi hệ thống gắn nhãn “nguy cơ cao” cho một học sinh, nhãn đó có xu hướng tồn tại trong hồ sơ lâu hơn mức cần thiết và có thể ảnh hưởng đến cách nhìn nhận học sinh đó - kể cả khi thực tế đã thay đổi.

Sai lệch dữ liệu đầu vào: nếu dữ liệu huấn luyện mô hình phản ánh bất bình đẳng sẵn có (ví dụ học sinh vùng sâu vùng

xa có tần suất truy cập thấp do hạ tầng mạng kém, không phải do thiếu động lực học), mô hình có thể tái tạo và khuếch đại chính bất bình đẳng dưới vỏ bọc “khách quan vì AI tính toán”.

Phạm vi truy cập kết quả dự đoán: nếu không giới hạn chặt, chỉ số dự đoán rủi ro có thể bị truy cập bởi những bên không có trách nhiệm hỗ trợ trực tiếp học sinh, đi ngược lại mục đích ban đầu của mô hình.

Thiếu cơ chế phản hồi của con người: một dự đoán sai có thể ít gây hại nếu chỉ dẫn đến một cuộc trao đổi hỗ trợ. Rủi ro sẽ nghiêm trọng hơn nếu hệ thống tự động kích hoạt biện pháp can thiệp mang tính chế tài mà không qua đánh giá của con người.

4.2.2. Khung quản trị kỹ thuật đề xuất

Để triển khai mô hình dự đoán bỏ học theo tinh thần «AI có trách nhiệm», hệ thống cần ít nhất bốn lớp kiểm soát:

Giới hạn phạm vi dữ liệu đầu vào chỉ sử dụng dữ liệu cần thiết: mô hình chỉ nên sử dụng các đặc trưng hành vi học tập trực tiếp liên quan đến tiến trình học.

4.3.1. Nguyên tắc thiết kế tổng thể về phân tầng và cô lập



Hình 1. Kiến trúc tham chiếu bốn vùng cho nền tảng học tập số

Kiểm định công bằng định kỳ: đánh giá lại hiệu suất mô hình theo từng nhóm để phát hiện sớm hiện tượng mô hình dự đoán kém chính xác hơn đối với một số nhóm học sinh nhất định.

Kiểm soát truy cập kết quả dự đoán ở tầng ứng dụng: chỉ hiển thị chỉ số rủi ro cho các vai trò có trách nhiệm hỗ trợ trực tiếp, trong một cửa sổ thời gian phù hợp với chu kỳ học tập, không lưu trữ vĩnh viễn trong hồ sơ tổng thể của học sinh.

Bắt buộc xác nhận của con người trước hành động can thiệp.

4.3. Kiến trúc hạ tầng tham chiếu

Kiến trúc tham chiếu được xây dựng cho một LMS mở có CDN, kho OER, kho nội dung hạn chế, dịch vụ danh tính, kho phân tích và bảng điều khiển giáo viên. Ranh giới tin cậy được đặt giữa mạng phân phối công khai, lớp dịch vụ ứng dụng, vùng dữ liệu nhạy cảm và vùng quản trị khóa/giám sát. Mục tiêu là giảm quyền mặc định và ngăn sự cố ở một vùng lan sang vùng khác.

Kiến trúc tham chiếu không đặt toàn bộ hệ thống trong một vùng tin cậy duy nhất. Hạ tầng được chia thành các vùng cô lập theo độ nhạy cảm của dữ liệu, với ranh giới kiểm soát truy cập rõ ràng với 4 vùng chính.

Vùng 1 - Lớp truy cập công khai:

Gồm máy chủ ứng dụng LMS/OER, mạng phân phối nội dung. Đây là vùng có bề mặt tấn công lớn nhất vì tiếp xúc trực tiếp với internet. Vì vậy, hệ thống cần khả năng tự động điều chỉnh tài nguyên để chịu tải tăng đột biến và giảm tác động của tấn công mạng.

Vùng 2 - Lớp dữ liệu vận hành:

Gồm cơ sở dữ liệu chính của LMS, hệ thống lưu trữ phiên làm việc và bộ nhớ đệm. Vùng này được cô lập khỏi Vùng 1 bằng tường lửa nội bộ, chỉ chấp nhận kết nối từ lớp ứng dụng qua những cổng và giao thức được cho phép.

Vùng 3 - Lớp nội dung và khóa mã hóa: Gồm kho học liệu, hệ thống quản lý khóa mã hóa và dịch vụ DRM hoặc watermarking. Đây là vùng được cô lập chặt nhất và vận hành theo nguyên tắc phân tách quyền: đơn vị vận hành hạ tầng không đồng thời nắm khóa giải mã nội dung.

Vùng 4 - Lớp phân tích và AI:

Gồm quy trình xử lý dữ liệu hành vi phục vụ các mô hình phân tích và dự đoán, chẳng hạn mô hình dự đoán nguy cơ bỏ học. Vùng này chỉ nhận dữ liệu đã được ẩn danh hóa, nó không được truy vấn ngược trực tiếp vào cơ sở dữ liệu vận hành.

4.3.2. Giám sát bảo mật xuyên suốt các vùng

Giám sát cần kết hợp các lớp. Ở biên, CDN/WAF và giới hạn tốc độ giúp

giảm lưu lượng bất thường; autoscaling chỉ đáp ứng tải hợp lệ và không thay thế bảo vệ DDoS. Ở ứng dụng, cần phát hiện đăng nhập bất thường, lạm dụng API, thay đổi quyền và truy cập vượt mục đích. Ở dữ liệu, cần theo dõi truy vấn lớn, tải xuống hàng loạt, mở bảng ánh xạ và sử dụng khóa ngoài quy trình. Ở vùng quản trị, log phải chuyển tới hệ thống tập trung, kiểm soát sửa/xóa và có bản sao chỉ-ghi hoặc cơ chế chứng minh toàn vẹn; SIEM là công cụ phân tích, không tự thân làm cho log bất biến.

Mỗi sự kiện cần gắn chủ thể, thời điểm, tài nguyên, thao tác, kết quả và lý do nghiệp vụ khi cần. Chính sách lưu log phải cân bằng điều tra với giảm thiểu dữ liệu. Hệ thống cần chỉ số RTO/RPO, bản sao mã hóa, kiểm tra khôi phục và diễn tập tình huống mất khóa, lộ token, sửa nội dung và DDoS. Quy trình ứng cứu phải nêu rõ ai cô lập dịch vụ, ai thông báo, ai quyết định khôi phục và cách bảo toàn bằng chứng.

4.4. Kinh nghiệm quốc tế

Hai nền tảng dưới đây được dùng để minh họa cách các hệ sinh thái lớn giải quyết bài toán quy mô, liên thông và đa dạng người dùng. Do nguồn công khai chủ yếu là tài liệu nền tảng, chúng không được trình bày như bằng chứng thực nghiệm về hiệu quả bảo mật.

4.4.1. Ấn Độ và nền tảng DIKSHA với hạ tầng liên bang đa ngôn ngữ và kết nối ngoại tuyến trực tuyến

Tài liệu công khai của DIKSHA/Sunbird cho thấy nền tảng hướng tới kiến trúc mô-đun, hỗ trợ nhiều bang, ngôn ngữ và kịch bản kết nối khác nhau. Điểm có thể tham khảo là tách dịch vụ, chuẩn hóa

siêu dữ liệu và thiết kế để tích hợp thay vì khóa toàn bộ hệ sinh thái vào một ứng dụng. Tuy nhiên, tài liệu nền tảng không đủ để kết luận về mức độ bảo vệ dữ liệu trong mọi bang. Khi vận dụng, cần bổ sung ma trận chủ thể-quyền, quy tắc lưu trữ theo địa bàn, mã hóa khóa độc lập và kiểm tra ngoại tuyến: dữ liệu tạm trên thiết bị phải có thời hạn, xóa từ xa hoặc cơ chế đồng bộ an toàn.

4.4.2. Nga và hệ sinh thái tích hợp Moscow Electronic School

Moscow Electronic School được giới thiệu như một hệ sinh thái kết hợp học liệu số, kế hoạch bài dạy, hoạt động lớp học và các dịch vụ cho nhà trường. Bài học có thể rút ra là cần một lớp danh tính và quyền truy cập thống nhất, đồng thời duy trì quyền quyết định của giáo viên trong quy trình sư phạm. Nhưng việc tích hợp nhiều nguồn làm tăng rủi ro liên kết hồ sơ và mở rộng mục đích. Vì vậy, kiến trúc tham chiếu nên tách kho nội dung, dữ liệu định danh và dữ liệu phân tích; mọi API liên thông phải có phạm vi, thời hạn, nhật ký và cơ chế thu hồi. Đây là suy luận thiết kế từ mô tả công khai, không phải đánh giá độc lập nền tảng.

V. Kết luận

Bảo mật dữ liệu và an toàn thông tin không phải phần việc bổ sung sau khi đã quyết định ai vận hành nền tảng học tập số. Đây là điều kiện thiết kế cần được tích hợp ngay từ đầu, bắt kể nền tảng do Nhà nước, khu vực tư nhân hay mô hình hợp tác công tư vận hành.

Giáo dục mở chỉ bền vững khi mức độ mở của nội dung được thiết kế song song với mức độ bảo vệ của dữ liệu. Bài viết đã phân biệt OER, nội dung hạn chế

và dữ liệu người học; chuyển ba vấn đề cốt lõi thành ba nguyên tắc; và gắn chúng với phân vùng hạ tầng, quản trị khóa, URL ký số, mã giả hóa, nhật ký hệ thống, giám sát và quyền quyết định của con người.

Giới hạn của nghiên cứu là chưa có dữ liệu vận hành, thử nghiệm xâm nhập, khảo sát chuyên gia hoặc đánh giá tác động theo thời gian. Vì vậy, các kiểm soát được đề xuất cần được kiểm chứng trong một LMS cụ thể bằng threat model, kiểm thử tải và bảo mật, đánh giá công bằng theo nhóm, thử khôi phục và đánh giá khả năng sử dụng của giáo viên. Hướng nghiên cứu tiếp theo là xây dựng bộ chỉ số tối thiểu cho quyền riêng tư, tính mở, tính liên thông và khả năng phục hồi; đồng thời đánh giá liệu các biện pháp bảo mật có vô tình tạo thêm rào cản tiếp cận hay không.

Tài liệu tham khảo

- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection-Information security management systems-Requirements*.
- Kumar, P. P., Kumar, P. S., & Alphonse, P. J. A. (2018). Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. *Journal of Network and Computer Applications*, 108, 37-52. <https://doi.org/10.1016/j.jnca.2018.02.009>
- Liu, Q., & Khalil, M. (2023). Understanding privacy and data protection issues in learning analytics using a systematic review. *British Journal of Educational Technology*, 54, 1715-1747. <https://doi.org/10.1111/bjet.13388>
- Moscow State Pedagogical University. (n.d.). *Moscow Electronic School and digital educational resources*. <https://en.mgpu.ru/institutes/institute-of-education-content-methods-and-technology/>

- National Council of Educational Research and Training. (n.d.). *DIKSHA open-source software and platform documentation*. <https://diksha.gov.in/help/diksha-oss/>
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. <https://doi.org/10.6028/NIST.AI.100-1>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. <https://doi.org/10.6028/NIST.CSWP.29>
- Prinsloo, P., Slade, S., & Khalil, M. (2023). Multimodal learning analytics-in-between student privacy and encroachment: A systematic review. *British Journal of Educational Technology*, 54, 1566-1586. <https://doi.org/10.1111/bjet.13373>
- Sunbird. (n.d.). *Architecture design*. <https://project-sunbird.github.io/architecture/design/>
- Sousa, L., Pedro, L., & Santos, C. (2023). A systematic review of systematic reviews on open educational resources: An analysis of the legal and technical openness. *The International Review of Research in Open and Distributed Learning*, 24(3), 18-33. <https://doi.org/10.19173/irrodl.v24i3.7196>
- Wuyts, K., Sion, L., & Joosen, W. (2020). LINDDUN GO: A lightweight approach to privacy threat modeling. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 302-309). IEEE. <https://doi.org/10.1109/EuroSPW51379.2020.00047>

DATA PROTECTION AND INFORMATION SECURITY IN OPEN EDUCATION

Lam Van An¹, Nguyen Dinh Tuong¹, Nguyen Minh Dung¹, Pham Quang Huy¹

Abstract: *This paper analyzes data security and information security risks in open education and proposes a principles-based framework linked to testable technical mechanisms. The open nature of education creates three tensions: between content access and the protection of usage rights; between personalization and learner privacy; and between interoperability, scalability, and data sovereignty. The paper distinguishes open educational resources, restricted materials, and learner data; develops a four-layer risk matrix; and proposes three security-by-design principles associated with key management, scoped signed URLs, pseudonymization, audit logging, infrastructure segmentation, and human decision-making in the use of AI. The study employs structured document analysis covering the period from 2018 to 2025, combined with a comparison of academic studies, information-security reference frameworks, and publicly available architecture documents. Rather than claiming empirical effectiveness, the paper provides a reference architecture and criteria for validation in a specific learning management system (LMS).*

Keywords: open education, information security, data security, learner data, learning analytics, responsible AI

¹ Hanoi Open University, Hanoi, Vietnam