KIỂM SOÁT TRUY CẬP ĐỘNG CHO HỆ THỐNG QUẢN LÝ HỌC TẬP DỰA TRÊN MÃ HÓA THUỘC TÍNH

Nguyễn Thị Khánh Quyên[1], Nguyễn Minh Dũng[1], Lâm Văn Ân[1]
Email: nguyenkhanhquyen@hou.edu.vn

Ngày tòa soạn nhận được bài báo: 03/06/2025
Ngày phản biện đánh giá: 02/12/2025
Ngày bài báo được duyệt đăng: 23/12/2025

DOI: 10.59266/houjs.2025.1092

Tóm tắt: *Trong bối cảnh giáo dục số phát triển mạnh mẽ, việc chia sẻ tài nguyên học tập qua các Hệ thống quản lý học tập (LMS) đặt ra thách thức lớn về bảo mật và an toàn dữ liệu. Các mô hình kiểm soát truy cập truyền thống, đặc biệt là RBAC, cho thấy nhiều hạn chế về linh hoạt và khả năng quản lý khi phải đáp ứng nhu cầu truy cập phức tạp, thường xuyên thay đổi trong môi trường giáo dục hiện đại. Bài báo này đề xuất một kiến trúc lý thuyết mới dựa trên Ciphertext-Policy Attribute-Based Encryption (CP-ABE) nhằm khắc phục những vấn đề trên. Kiến trúc cho phép xây dựng cơ chế kiểm soát truy cập động, chi tiết và an toàn hơn. Đóng góp chính của nghiên cứu gồm: (1) đề xuất mô hình kiến trúc mới với CP-ABE để kiểm soát truy cập trong LMS; (2) định nghĩa rõ ràng các thực thể và thuật toán cốt lõi của mô hình; và (3) phân tích các ưu điểm về bảo mật, chống thông đồng và khả năng mở rộng. Kết quả chứng minh mô hình có tiềm năng mang lại giải pháp chia sẻ học liệu an toàn, linh hoạt và hiệu quả hơn so với các phương pháp hiện hành.*

Từ khóa*: mã hóa thuộc tính, kiểm soát truy cập động, hệ thống quản lý học tập, CP-ABE, bảo mật giáo dục*

I. Đặt vấn đề

Cuộc cách mạng công nghiệp lần thứ tư đã thúc đẩy một quá trình chuyển đổi số sâu rộng trong mọi lĩnh vực, trong đó giáo dục được xác định là một trong những ưu tiên hàng đầu. Tại Việt Nam, theo kế hoạch của Chính phủ và Bộ Giáo dục và Đào tạo, đến năm 2025 ngành giáo dục sẽ được số hóa ở mức độ cao với việc ứng dụng mạnh mẽ trí tuệ nhân tạo và công nghệ thông tin. Các cơ sở giáo dục, đặc biệt là các trường đại học hiện đang sử dụng rộng rãi các hệ thống quản lý học tập để lưu trữ, quản lý và chia sẻ khối lượng khổng lồ tài nguyên học tập số (Wagman, 2021).

Tuy nhiên, những lợi ích này cũng đi kèm với những rủi ro an ninh mạng nghiêm trọng. Trong môi trường giáo dục, việc chia sẻ và quản lý dữ liệu trong môi trường số đặt ra các thách thức lớn về bảo vệ dữ liệu cá nhân của người dùng và tài sản trí tuệ của giảng viên. Nếu một sự cố

[1] Trường Đại học Mở Hà Nội

rò rỉ dữ liệu xảy ra thì có thể gây ra những thiệt hại nặng nề về tài chính và uy tín cho tổ chức đó (Styra, 2022). Do đó, việc xây dựng một cơ chế kiểm soát truy cập an toàn, hiệu quả và linh hoạt cho học liệu số không chỉ là một yêu cầu kỹ thuật mà còn là một nhiệm vụ chiến lược vô cùng cấp thiết.

Hiện nay, một mô hình kiểm soát truy cập phổ biến nhất trong các hệ thống thông tin, bao gồm cả LMS, là kiểm soát truy cập dựa trên vai trò (RBAC). RBAC đơn giản hóa việc quản lý quyền hạn bằng cách gán quyền cho các vai trò như "Giảng viên", "Sinh viên", "Quản trị viên" thay vì cho từng người dùng riêng lẻ. Tuy nhiên đây là một mô hình tĩnh nên khó đáp ứng các tình huống chia sẻ cần sự chi tiết và thay đổi liên tục. Vấn đề hạn chế thứ hai chính là phân tích vai trò người dùng, để đáp ứng các nhu cầu chi tiết, quản trị viên buộc phải tạo ra vô số vai trò mới, dẫn đến việc làm cho hệ thống trở nên phức tạp, khó quản lý và bảo trì. Thứ ba là vấn đề quản lý tập trung, quyền truy cập và vai trò của người dùng có thể thay đổi theo thời gian và việc duy trì RBAC đòi hỏi sự cập nhật liên tục. Những hạn chế này dẫn đến câu hỏi nghiên cứu cốt lõi: làm thế nào để xây dựng một kiến trúc kiểm soát truy cập cho LMS cho phép người sở hữu dữ liệu có thể tự định nghĩa và thực thi các chính sách truy cập phức tạp, chi tiết trên chính tài nguyên số của họ một cách an toàn và hiệu quả, đồng thời khắc phục được sự cứng nhắc của mô hình RBAC.

Mục tiêu nghiên cứu của bài báo là thiết kế một kiến trúc lý thuyết toàn diện, lấy CP-ABE làm trung tâm, để cung cấp một cơ chế kiểm soát truy cập động, chi tiết và an toàn cho các tài nguyên học tập số trên hệ thống LMS.

II. Cơ sở lý thuyết

Để nhận diện rõ giá trị của nghiên cứu, cần nhìn lại quá trình phát triển của các mô hình kiểm soát truy cập cùng công nghệ mã hóa dựa trên thuộc tính. Trải qua nhiều giai đoạn, các mô hình này đã tiến hóa từ dạng cơ bản đến phức tạp.

Mô hình sớm nhất là DAC (Discretionary Access Control) - kiểm soát truy cập tùy quyền. Trong đó, chủ sở hữu tài nguyên trực tiếp quyết định ai có quyền truy cập và mức độ quyền hạn. Tuy nhiên, khi hệ thống mở rộng với nhiều người dùng và tài nguyên, DAC trở nên khó quản lý.

Đối lập với DAC là MAC (Mandatory Access Control) - kiểm soát truy cập bắt buộc. Ở đây, chủ sở hữu không quyết định quyền truy cập mà hệ thống hoặc một cơ quan có thẩm quyền định sẵn qua các nhãn an ninh. MAC đảm bảo an toàn cao, nhưng cứng nhắc và chỉ thích hợp cho các hệ thống yêu cầu bảo mật nghiêm ngặt.

Tiếp đến là RBAC (Role-Based Access Control) - kiểm soát dựa trên vai trò. Quyền hạn được gán cho vai trò, sau đó gán vai trò cho người dùng. Cách này đơn giản hóa quản lý trong tổ chức có phân cấp rõ ràng. Song, trong môi trường giáo dục - nơi tồn tại nhiều nhóm người dùng với quyền thay đổi liên tục theo khoa, năm học, điểm số, tình trạng ghi danh - RBAC bộc lộ hạn chế lớn. Sự phụ thuộc vào danh tính và vai trò tĩnh khiến RBAC khó đáp ứng yêu cầu truy cập thường xuyên biến đổi.

Một bước tiến vượt bậc là Mã hóa dựa trên thuộc tính (Attribute-Based Encryption - ABE) do Sahai và Waters đề xuất năm 2005. Đây là dạng mật mã khóa công khai tiên tiến, cho phép gắn điều kiện kiểm soát truy cập trực tiếp vào

dữ liệu đã mã hóa. Trong ABE, khóa bí mật của người dùng và bản mã đều gắn với thuộc tính; giải mã chỉ thành công khi thuộc tính trong khóa phù hợp chính sách trên bản mã.

ABE có hai biến thể chính:

KP-ABE (Key-Policy ABE): bản mã gắn với thuộc tính, còn khóa bí mật chứa chính sách. Người dùng chỉ giải mã được khi thuộc tính của bản mã đáp ứng chính sách trong khóa.

CP-ABE (Ciphertext-Policy ABE): ngược lại, bản mã chứa chính sách do người mã hóa xác định, trong khi khóa bí mật gắn với thuộc tính người dùng. Giải mã thành công khi tập thuộc tính khớp chính sách.

Các nghiên cứu gần đây, như Li và cộng sự (2018), đã chỉ ra tiềm năng rộng lớn của ABE, đặc biệt trong điện toán đám mây, giúp giải quyết các vấn đề về bảo mật và quyền riêng tư khi chia sẻ dữ liệu.

III. Phương pháp nghiên cứu

Nghiên cứu này nhằm mục đích tạo ra một kiến trúc mới - cụ thể là một kiến trúc lý thuyết cho hệ thống kiểm soát truy cập. Do đó, phương pháp luận phù hợp nhất là DSR - Nghiên cứu khoa học thiết kế (Design Science Research). Đây là mô hình nghiên cứu được công nhận rộng rãi trong các ngành kỹ thuật và hệ thống thông tin, tập trung vào việc giải quyết các vấn đề thực tiễn thông qua việc thiết kế và đánh giá các giải pháp mới hữu ích và sáng tạo.

Trong nghiên cứu này, nhóm tác giả áp dụng quy trình DSR do Peffers và cộng sự (2007) đề xuất. Quy trình bao gồm sáu bước chính: (1) nhận diện vấn đề và tạo động lực, (2) xác định mục tiêu giải pháp, (3) thiết kế và phát triển, (4) trình diễn, (5) đánh giá và (6) truyền thông. Tuy nhiên, do đặc thù mang tính lý thuyết, nghiên cứu tập trung chủ yếu vào bốn bước: 1, 2, 3 và 5.

Bước 1: Nhận diện vấn đề. Giai đoạn này tập trung phân tích một cách hệ thống các hạn chế của mô hình RBAC trong môi trường giáo dục. Quá trình bao gồm khảo sát tài liệu, phân tích các tình huống thực tế trong LMS và tham khảo ý kiến từ chuyên gia trong giáo dục cũng như bảo mật thông tin.

Bước 2: Xác định mục tiêu. Mục tiêu được định nghĩa dưới dạng yêu cầu chức năng và phi chức năng cho kiến trúc mới. Yêu cầu chức năng gồm khả năng biểu diễn chính sách phức tạp, đảm bảo quyền kiểm soát cho chủ sở hữu dữ liệu và tính mở rộng. Yêu cầu phi chức năng liên quan đến bảo mật, hiệu năng và khả năng sử dụng.

Bước 3: Thiết kế và phát triển. Nghiên cứu xây dựng kiến trúc dựa trên CP-ABE, định nghĩa các thực thể, mô tả giao thức tương tác và xác định thuật toán mật mã cốt lõi. Công đoạn này đòi hỏi hiểu biết chuyên sâu về mật mã học, đặc biệt các lược đồ ABE, cũng như kinh nghiệm trong thiết kế hệ thống phân tán.

Bước 5: Đánh giá. Kiến trúc được phân tích ở mức lý thuyết nhằm làm rõ các đặc tính bảo mật và hiệu năng. Hoạt động này bao gồm chứng minh tính an toàn dựa trên giả định mật mã được chấp nhận, phân tích độ phức tạp tính toán và so sánh với mô hình hiện có, đồng thời xem xét khả năng triển khai thực tế và tích hợp với LMS hiện hành.

IV. Kết quả và thảo luận

4.1. Kiến trúc hệ thống đề xuất

Kiến trúc kiểm soát truy cập được đề xuất dựa trên CP-ABE bao gồm bốn thực

thể logic chính, mỗi thực thể có vai trò và trách nhiệm riêng biệt trong việc đảm bảo tính bảo mật và hiệu quả của hệ thống:

Cơ quan quản lý thuộc tính (Attribute Authority - AA): Đây là một thực thể được tin cậy trong hệ thống, chịu trách nhiệm định nghĩa toàn bộ không gian thuộc tính (ví dụ: các khoa, các vai trò, các năm học), tạo ra các tham số công khai và khóa chủ của hệ thống. AA cấp phát khóa bí mật cho mỗi người dùng dựa trên các thuộc tính mà họ sở hữu.

Người sở hữu dữ liệu (Data Owner): Đây có thể là đơn vị quản lý hệ thống LMS. Họ là người tạo ra học liệu, định nghĩa chính sách truy cập cho học liệu đó, và thực hiện việc mã hóa trước khi tải lên hệ thống.

Người dùng dữ liệu (Data User): Là các sinh viên hoặc các bên liên quan khác. Họ yêu cầu truy cập học liệu và sử dụng khóa bí mật của mình để giải mã nếu các thuộc tính của họ thỏa mãn chính sách.

Hệ thống lưu trữ (Storage System): Là LMS hoặc một dịch vụ lưu trữ đám mây. Thực thể này được xem là «bán tin cậy» hoặc «không tin cậy». Nó chỉ có nhiệm vụ lưu trữ các bản mã (ciphertext) mà không thể đọc được nội dung bên trong.

Mô hình CP-ABE được xây dựng dựa trên bốn thuật toán mật mã cơ bản sau:

Setup(λ) → (PK, MK): Thuật toán khởi tạo hệ thống. Nó nhận đầu vào là một tham số an toàn λ, và tạo ra Khóa Công khai (Public Key - PK) và Khóa Chủ (Master Key - MK).

Encrypt(PK, M, P) → CT: Thuật toán mã hóa. Nó nhận đầu vào là khóa công khai PK, một thông điệp M (học liệu), và một cấu trúc truy cập P (chính sách). Thuật toán này mã hóa M theo chính sách P và tạo ra một bản mã CT.

KeyGen(MK, S) → SK: Thuật toán tạo khóa. Nó nhận đầu vào là khóa chủ MK và một tập hợp các thuộc tính S mô tả một người dùng. Thuật toán tạo ra một Khóa bí mật (Secret Key - SK) tương ứng với tập thuộc tính S.

Decrypt(CT, SK) → M hoặc ⊥: Thuật toán giải mã. Nó nhận đầu vào là bản mã CT và một khóa bí mật SK. Nếu tập thuộc tính S liên kết với SK thỏa mãn chính sách P được nhúng trong CT, thuật toán sẽ trả về thông điệp gốc M. Ngược lại, nó trả về lỗi (⊥).

4.2. Luồng hoạt động của hệ thống

Kiến trúc hệ thống gồm 2 luồng hoạt động chính:

Luồng chia sẻ tài liệu (do Giảng viên thực hiện):

– Giảng viên chuẩn bị một học liệu (M).

– Giảng viên định nghĩa một chính sách truy cập (P) cho học liệu đó.

– Hệ thống LMS gọi thuật toán Encrypt(PK, M, P) để tạo ra bản mã CT.

– Hệ thống tính toán giá trị băm của CT, ví dụ Hash(CT), để đảm bảo tính toàn vẹn.

– LMS lưu trữ CT và Hash(CT).

Luồng truy cập tài liệu (do Sinh viên thực hiện):

– Sinh viên yêu cầu truy cập học liệu.

– LMS trả về bản mã CT tương ứng.

– Sinh viên sử dụng khóa bí mật SK của mình (đã được AA cấp trước đó, tương ứng với các thuộc tính của sinh viên, ví dụ: S = {Vai trò: Sinh viên, Khoa: CNTT, Năm học: 3}) để thực hiện giải mã.

– Sinh viên gọi thuật toán Decrypt (CT, SK). Vì tập thuộc tính S của sinh viên

thỏa mãn chính sách P, thuật toán sẽ trả về thông điệp gốc M. Nếu một sinh viên khác với tập thuộc tính không phù hợp cố gắng giải mã, thuật toán sẽ thất bại.

4.3. Phân tích an toàn của mô hình

Mô hình được đề xuất bảo đảm an toàn nhờ nền tảng mật mã CP-ABE. Dữ liệu được mã hóa trước khi lưu trữ, vì vậy ngay cả khi máy chủ LMS bị tấn công, kẻ xấu cũng không thể truy cập nội dung nếu không có khóa bí mật hợp lệ với các thuộc tính phù hợp chính sách. Tính bảo mật này được chứng minh dựa trên những giả định toán học phức tạp như Bilinear Diffie-Hellman (DBDH), vốn được cộng đồng mật mã học thừa nhận rộng rãi.

Một đặc điểm quan trọng khác của ABE là khả năng chống thông đồng. Điều này ngăn cản việc nhiều người dùng kết hợp khóa bí mật để giải mã dữ liệu khi mỗi người đều không đủ quyền riêng lẻ. Ví dụ, một sinh viên có thuộc tính "Khoa: Tiếng Anh" và một sinh viên khác có thuộc tính "Năm học: 3" không thể kết hợp khóa để truy cập tài liệu yêu cầu cả hai thuộc tính "Khoa: Tiếng Anh" AND "Năm học: 3". Đặc tính này được bảo đảm bởi thiết kế toán học của ABE, khi mỗi khóa bí mật đều gắn giá trị ngẫu nhiên riêng.

Ngoài ra, mô hình còn bảo vệ tính toàn vẹn dữ liệu thông qua việc lưu trữ giá trị băm kèm bản mã, giúp người dùng dễ dàng kiểm tra dữ liệu có bị thay đổi trong quá trình lưu trữ hay không. Nhờ vậy, hệ thống trở nên toàn diện và an toàn hơn.

4.4. So sánh với mô hình RBAC

So với RBAC, kiến trúc dựa trên CP-ABE mang lại những lợi thế hơn về nhiều khía cạnh.

Thứ nhất là khả năng kiểm soát truy cập chi tiết và linh hoạt. CP-ABE cho phép biểu diễn các chính sách truy cập phức tạp dưới dạng các biểu thức logic (AND, OR, NOT) trên các thuộc tính. Nếu RBAC cần tạo ra hàng chục hoặc hằng trăm vai trò để biểu diễn một chính sách phức tạp, thì CP-ABE chỉ cần biểu diễn cùng một chính sách bằng một biểu thức logic đơn giản.

Thứ hai là việc trao quyền kiểm soát cho người sở hữu dữ liệu. Đây là thay đổi mang tính cách mạng so với RBAC. Người tạo ra học liệu, nội dung số có toàn quyền định nghĩa chính sách truy cập cho chính tài liệu đó tại thời điểm mã hóa. Điều này tuân thủ chặt chẽ hơn nguyên tắc sở hữu trí tuệ và loại bỏ sự phụ thuộc vào quản trị viên hệ thống.

Thứ ba là khả năng mở rộng cũng là một lợi thế quan trọng khác. Trong mô hình CP-ABE, việc thêm một người dùng mới chỉ yêu cầu AA cấp một khóa bí mật duy nhất cho người đó dựa trên các thuộc tính của họ. Việc thêm một tài liệu mới không ảnh hưởng đến các khóa đã cấp. Điều này giúp hệ thống dễ dàng mở rộng mà không cần phải định nghĩa lại toàn bộ cấu trúc vai trò và quyền hạn như trong RBAC.

4.5. Thách thức và hạn chế

Mặc dù có nhiều ưu điểm như đã nêu ở phần trên, mô hình kiến trúc hệ thống đề xuất cũng đối mặt với một số thách thức và hạn chế cần được xem xét. Một trong những thách thức lớn nhất là vấn đề thu hồi thuộc tính hiệu quả. Trong các lược đồ ABE truyền thống, việc thu hồi quyền truy cập của một người dùng hoặc một thuộc tính là rất khó khăn. Trong RBAC, quản trị hệ thống có thể loại bỏ vai trò của người dùng một cách rất đơn giản thì trong ABE, quản trị viên phải tạo và phân phối lại khóa cho tất cả người dùng khác, điều này sẽ không hiệu quả trong một hệ thống lớn.

Bên cạnh đó, hiệu suất tính toán là một thách thức lớn. Các phép toán mật mã trong ABE, đặc biệt là các phép ghép cặp song tuyến (bilinear pairings) đòi hỏi nhiều tài nguyên tính toán hơn so với các phép toán trong RBAC. Điều này có thể ảnh hưởng đến thời gian phản hồi của hệ thống, đặc biệt trong các môi trường có nhiều người dùng đồng thời. Muốn giải quyết vấn đề này cần đầu tư cho phần cứng và tối ưu hóa các kỹ thuật của hệ thống.

Một vấn đề khác cũng cần được xem xét là vấn đề ký quỹ khóa (key escrow). Trong kiến trúc hiện tại, cơ quan quản lý thuộc tính có quyền truy cập vào tất cả các khóa bí mật, nếu cơ quan này bị xâm nhập, toàn bộ hệ thống có thể bị ảnh hưởng.

Thêm một thách thức thực tế khác là độ phức tạp trong việc triển khai và tích hợp với các hệ thống hiện tại. Việc chuyển từ mô hình RBAC sang CP-ABE đòi hỏi những thay đổi đáng kể trong kiến trúc hệ thống, chi phí đầu tư cao cũng như đào tạo người dùng để sử dụng các tính năng mới.

V. Kết luận

Như vậy, Nghiên cứu này đã giới thiệu một kiến trúc kiểm soát truy cập tiên tiến dựa trên CP-ABE, nhằm khắc phục các hạn chế cố hữu của RBAC như sự cứng nhắc, thiếu linh hoạt và phụ thuộc vào quản trị viên. Kiến trúc đề xuất mang lại cơ chế kiểm soát truy cập chi tiết, linh hoạt, đồng thời cho phép biểu diễn chính sách phức tạp một cách hiệu quả hơn. So sánh với RBAC cho thấy CP-ABE vượt trội ở khả năng mở rộng và quản lý quyền truy cập, phù hợp với môi trường giáo dục vốn đa dạng và thường xuyên thay đổi.

Bằng việc áp dụng các thuật toán mật mã hiện đại, hệ thống đảm bảo mức độ bảo mật mạnh mẽ, có khả năng chống thông đồng và bảo vệ dữ liệu ngay cả khi máy chủ lưu trữ bị xâm nhập. Điều này có ý nghĩa đặc biệt quan trọng đối với giáo dục số, nơi việc bảo vệ tài sản trí tuệ của giảng viên và thông tin cá nhân của sinh viên là ưu tiên hàng đầu.

Tuy nhiên, nghiên cứu cũng chỉ ra nhiều thách thức cần giải quyết như vấn đề thu hồi thuộc tính hiệu quả, chi phí tính toán cao và khó khăn khi triển khai thực tế. Trong tương lai, các hướng nghiên cứu có thể tập trung phát triển cơ chế thu hồi thuộc tính không cần tái tạo khóa, tối ưu hóa hiệu năng, và xây dựng giao diện người dùng trực quan để giảm độ phức tạp. Xa hơn, việc phát triển mô hình ABE phi tập trung, kỹ thuật che giấu chính sách nhằm bảo vệ thông tin nhạy cảm, cùng các lược đồ ABE kháng lượng tử để thích ứng với công nghệ mới cũng là những hướng đi triển vọng.

Nghiên cứu này đóng góp vào nền tảng lý thuyết cho việc phát triển các hệ thống kiểm soát truy cập thế hệ mới trong giáo dục số. Mặc dù còn một số thách thức cần giải quyết, những kết quả ban đầu cho thấy tiềm năng lớn của việc áp dụng công nghệ mật mã tiên tiến vào giải quyết các vấn đề thực tế trong môi trường giáo dục hiện đại.

Lời cảm ơn: Nghiên cứu này được tài trợ bởi đề tài cấp Trường Đại học Mở Hà Nội, mã số MHN2025-03.65.

Tài liệu tham khảo

[1]. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *2007 IEEE Symposium on Security and Privacy (SP '07)*, 321-334.

[2]. Chase, M., & Chow, S. S. M. (2009). Improving Privacy and Security in Multi-authority Attribute-based Encryption. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 121-130.

[3]. Cheung, L., & Newport, C. (2007). Provably Secure Ciphertext Policy ABE. *Cryptology ePrint Archive, Paper 2007/183*.

[4]. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 89-98.

[5]. Han, J., Qin, B., & Xiang, Y. (2019). A Survey on Attribute-based Encryption Schemes Suitable for the Internet of Things. *Cryptology ePrint Archive, Paper 2019/1428*.

[6]. Li, J., Lin, X., Zhang, Y., & Han, J. (2018). A survey on attribute-based encryption for cloud computing. *International Journal of Information Security, 17*(1), 1-16.

[7]. Narayanan, A. (2021). CESCR: CP-ABE for efficient and secure sharing of data in collaborative ehealth with revocation and no dummy attribute. *PLOS ONE*, *16*(5), e0250992.

[8]. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77.

[9]. Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. In R. Cramer (Ed.), *Advances in Cryptology -- EUROCRYPT 2005* (pp. 457-473). Springer.

[10]. Styra. (2022, December 1). What is Fine-Grained Access Control? https://www.styra.com/blog/what-is-fine-grained-access-control/

[11]. Wagman, K. B. (2021, October 27). *Nurturing Digital Safety: Unpacking Privacy and Security Challenges for Young Children in Emergency Remote Learning*. ACM CSCW.

[12]. Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. *Public Key Cryptography*, 53-70.

[13]. Zahid, M., & Arshad, M. (2019). The Inadequacies of Role-Based Access Control Model. *Symmetry, 11*(5), 669.

DYNAMIC ACCESS CONTROL FOR LEARNING MANAGEMENT SYSTEMS BASED ON ATTRIBUTE-BASED ENCRYPTION

Nguyen Thi Khanh Quyen[1], Nguyen Minh Dung[1], Lam Van An[1]

Abstract: *In the context of the strong digital transformation of the education sector, sharing learning resources on Learning Management Systems (LMS) poses significant challenges in terms of safety and security. Traditional access control models, particularly Role-Based Access Control (RBAC), reveal many limitations in flexibility and manageability when facing the complex and dynamic data-sharing requirements of modern educational environments. This paper proposes a theoretical architecture to address these issues using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This architecture establishes a dynamic, fine-grained, and secure access control mechanism, allowing data owners (lecturers) to fully define complex access policies directly on their digital resources. The main contributions of this paper include: (1) proposing a new theoretical architectural model centered on CP-ABE for access control in LMS; (2) formally defining the entities and core algorithms of the model; and (3) analyzing the security properties and theoretical advantages of the architecture, including confidentiality, collusion resistance, and scalability. The results indicate that the proposed model has great potential in providing a more secure, flexible, and efficient solution for learning resource sharing compared to existing approaches.*

Keywords: *attribute-based encryption, dynamic access control, learning management system, CP-ABE, educational security*

[1] Hanoi Open University