

HỘI THẢO KHOA HỌC VÀ CÔNG NGHỆ

KHOA CÔNG NGHỆ THÔNG TIN

BAN TỔ CHỨC

Trưởng ban:

PGS.TS. Đặng Trần Khánh

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

Thành viên:

ThS. Nguyễn Thị Định

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Nguyễn Thê Hữu

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Phan Thị Ngọc Mai

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Nguyễn Văn Tùng

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

BAN CHƯƠNG TRÌNH

Trưởng ban:

PGS.TS. Đặng Trần Khánh

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

Thành viên:

TS. Hoàng Xuân Bách

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

PGS.TS. Nguyễn Tuấn Đăng

Trường ĐH Sài Gòn

ThS. Nguyễn Thị Định

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Ngô Dương Hà

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

TS. Ngô Thanh Hùng

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Nguyễn Văn Lẽ

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

TS. Nguyễn Thanh Long

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

TS. Vũ Đức Lý

Trường Đại học FPT

TS. Nguyễn Thị Bích Ngân

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

TS. Huỳnh Hữu Nghĩa

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

KS. Trần Trương Tuấn Phát

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

TS. Lê Lam Sơn

Trường ĐH Bách Khoa – ĐH Quốc gia Tp.HCM

TS. Vũ Đức Thịnh

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

PGS.TS. Lê Hồng Trang

Trường ĐH Bách Khoa – ĐH Quốc gia Tp.HCM

ThS. Hà Lê Hoài Trung

Trường ĐH Công nghệ Thông tin – ĐH Quốc gia Tp.HCM

BAN THƯ KÝ

Trưởng ban:

ThS. Nguyễn Thị Định

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

Thành viên:

CN. Nguyễn Hải Bình

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Nguyễn Thị Thu Tâm

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Nguyễn Thị Thanh Thủy

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Trần Nhu Ý

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

ThS. Nguyễn Thị Hải Yến

Trường ĐH Công nghiệp Thực phẩm Tp.HCM

MỤC LỤC

1. Những vấn đề bảo mật trong mô hình học cộng tác - *Hà Lê Hoài Trung¹, Đặng Trần Khánh^{2,*}* 1
2. Ứng dụng AI trong thương mại điện tử thuật toán Content Based System hỗ trợ gợi ý mua hàng - *Nguyễn Hải Yến^{1,*}* 19
3. Một phương pháp gom cụm dữ liệu cho bài toán tư vấn lựa chọn học phần tự chọn - *Nguyễn Thị Thuỳ Trang^{1,*}, Phan Thị Ngọc Mai¹* 31
4. Ứng dụng thuật giải tối ưu bầy đàn ẩn tập hữu ích cao nhạy cảm - *Lâm Thị Họa Mi^{1,*}, Vũ Văn Vinh¹, Dương Thị Mộng Thùy¹* 40
5. Khai thác tập hữu ích cao dựa trên cơ chế diffset - *Nguyễn Thị Thanh Thủy^{1,*}, Nguyễn Văn Lẽ¹, Mạnh Thiên Lý¹* 56
6. Mô hình cá nhân hóa người học trên cơ sở logic mờ ứng dụng trong hệ thống học mở - *Hoàng Xuân Bách^{1,*}* 72
7. Phát hiện các đối tượng trong ảnh tế bào máu bằng kỹ thuật học sâu - *Trần Đình Toàn^{1,*}, Nguyễn Đức Toàn²* 76
8. Ứng dụng thuật toán song song FP-Growth khai phá tập phổ biến - *Nguyễn Thị Hồng Thảo^{1,*}* 86
9. Hệ thống chú thích ảnh tự động cho người khiếm thị - *Đinh Thị Mận¹, Nguyễn Văn Thịnh², Trần Ngọc Hiếu¹, Trần Thị Xinh, Trần Thị Vân Anh^{1,*}* 92
10. Ứng dụng máy học vào bài toán dự đoán bệnh ung thư vú - *Huỳnh Thị Châu Lan^{1,*}, Nguyễn Hải Yến¹* 104
11. Xây dựng hệ thống dự đoán kết quả học tập của sinh viên nhằm hỗ trợ công tác cõi ván học tập - *Ngô Thanh Hùng¹, Nguyễn Thị Thu Tâm^{1,*}* 112
12. Nguy cơ tấn công DDoS từ các thiết bị IoT – *Trần Đắc Tốt^{1,*}* 126
13. Nhận diện các video có yếu tố chính trị Việt Nam trên mạng xã hội - *Trần Thị Vân Anh¹, Đặng Trần Khánh^{1,*}, Nguyễn Hải Bình¹* 147
14. Cơ sở lý thuyết các mô hình độ chấp nhận và sử dụng công nghệ - *Đào Minh Châu^{1,*}* 160
15. Nâng cao hiệu quả tìm kiếm ảnh dựa trên cấu trúc KD-Tree và K-Means - *Nguyễn Thị Định^{1,*}, Trần Thị Bích Vân¹, Nguyễn Phương Hạc¹* 169
16. Tiếp cận các phương pháp phân lớp dữ liệu trong dự báo chất lượng nước - *Nguyễn Thị Diệu Hiền¹, Bùi Công Danh^{1,*}* 182

17. Nghiên cứu thuật toán tối ưu đàm kién tiến hóa – *Dinh Nguyễn Trọng Nghĩa¹, Nguyễn Thị Thu Tâm^{1,*}* **190**
18. Tổng quan về học liên kết và tiềm năng ứng dụng trong lĩnh vực y học - *Trần Trương Tuấn Phát^{1,2}, Đặng Trần Khánh^{1,*}, Nguyễn Thị Thanh Thảo¹* **198**
19. Tìm hiểu mô hình GPT và ứng dụng GPT phục vụ cho học tập và nghiên cứu ở sinh viên - *Đinh Huy Hoàng^{1,*}* **216**
20. Điểm danh sinh viên tự động bằng phương pháp nhận diện khuôn mặt - *Trần Thị Vân Anh¹, Đặng Trần Khánh^{1,*}, Nguyễn Vương Triều An¹, Nguyễn Văn Sơn¹, Nguyễn Nguyên Khang¹* **229**
21. Các công cụ nâng cao chất lượng và đánh giá giảng dạy - *Đào Minh Châu^{1,*}* **242**
22. HUFI-STPMS: hệ thống quản lý điểm rèn luyện sinh viên Trường Đại học Công nghiệp Thực phẩm (HUFI) - *Trần Trương Tuấn Phát¹, Đặng Trần Khánh¹, Ngô Thành Hùng^{1,*}, Trần Thị Vân Anh¹, Lê Thị Trà My¹, Đoàn Huỳnh Tuyết Anh¹* **248**
23. Nguồn nhân lực ngành công nghệ thông tin trong xu hướng chuyển đổi số - *Trần Thị Bích Vân^{1,*}* **261**
24. Tối ưu hóa đàm kién và ứng dụng trong bài toán ẩn tập phô biến - *Hồ Thanh Hải¹, Đinh Nguyễn Trọng Nghĩa^{1,*}* **265**
25. Hệ thống thông tin y tế một cách tiếp cận dựa trên thành phần - *Huỳnh Hữu Nghĩa¹, Nguyễn Thị Thu Tâm^{1,*}* **274**
26. Tối ưu hóa tìm kiếm chim hòng hạc và ứng dụng trong bài toán ẩn tập phô biến - *Lê Huỳnh Đức¹, Nguyễn Thị Hàng¹, Đinh Nguyễn Trọng Nghĩa^{1,*}* **288**
27. Tối ưu hóa sói xám và ứng dụng trong bài toán ẩn tập phô biến - *Phạm Nguyễn^{1,*}, Đinh Nguyễn Trọng Nghĩa¹* **303**
28. Xây dựng thuật toán Logistic cho phép phân loại mail và mô hình pipeline trên Spark - *Nguyễn Minh Hiền¹, Nguyễn Trọng Đăng Khoa¹, Nguyễn Văn Tùng¹, Ngô Dương Hà^{1,*}* **316**
29. Ứng dụng kỹ thuật resnet phân loại lá cây thuốc chữa bệnh gan - *Phạm Hoàng Hiệp¹, Trần Như Ý¹, Phan Thị Ngọc Mai^{1,*}* **325**
30. Xây dựng hệ thống xử lý tiền trình khóa luận tốt nghiệp - *Phạm Tấn Thuận¹, Vũ Trần Minh Hoàng¹, Ngô Văn Sơn¹, Nguyễn Ngọc Thạch¹, Trần Văn Thọ^{1,*}* **335**
31. Ứng dụng Firebase Authentication và Firebase Cloud Messaging để xây dựng đăng nhập, đăng ký và gửi thông báo về cho người dùng trong lập trình di động Android - *Lê Minh Kha^{1,*}, Biện Thành Nhựt¹, Nguyễn Hữu Trung¹, Nguyễn Thị Bích Ngân¹* **343**

-
32. Điều hướng Navigation trong thiết kế giao diện lập trình di động Android - *Lê Minh Phát^{l,*}, Lê Tâm Nhu^l, Ngô Thị Kim Ngân^l, Nguyễn Thị Kim Tuyên^l, Nguyễn Thị Bích Ngân^l* **360**
33. Xây dựng RESTful api và gọi API từ ứng dụng trong lập trình di động Android - *Vũ Ngô Đạt^{l,*}, Vũ Văn Vinh^l, Nguyễn Thị Bích Ngân^l* **378**
34. HUFI-ELAB: Hệ thống quản lý phòng thí nghiệm Trường Đại học Công nghiệp Thực phẩm (HUFI) - *Trần Trương Tuấn Phát^l, Đặng Trần Khánh^{l,*}, Tống Đăng Khoa^l, Nguyễn Trọng Nghĩa^l, Lê Trạng Lân^l* **393**
35. Thiết kế cơ chế mô hình học liên kết lấy cảm hứng từ mạng Ethereum 2.0 - *Trần Trương Tuấn Phát^l, Đặng Trần Khánh^{l,*}* **395**

NHỮNG VẤN ĐỀ BẢO MẬT TRONG MÔ HÌNH HỌC CỘNG TÁC

Hà Lê Hoài Trung¹, Đặng Trần Khanh^{2,*}

¹Trường Đại học Công nghệ Thông tin – Đại học Quốc Gia Hồ Chí Minh

²Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: khanh@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Học liên kết (Federated Learning - FL) là một phân nhánh mới của trí tuệ nhân tạo được xây dựng dựa trên dữ liệu và huấn luyện phi tập trung mang lại khả năng học vượt trội, và huấn luyện mô hình được thực hiện trực tiếp trên thiết bị đầu cuối. Học liên kết là một lĩnh vực nghiên cứu mới được coi là một nhánh trong trí tuệ nhân tạo, đang ở giai đoạn sơ khai và chưa nhận được nhiều sự tin tưởng trong cộng đồng nghiên cứu khoa học, chủ yếu là do vấn đề bảo mật và quyền riêng tư. Để thúc đẩy sự phát triển nghiên cứu trong lĩnh vực và hiện thực hóa áp dụng rộng rãi phương pháp này trong cuộc sống, phương pháp học liên kết và các mối quan tâm về bảo mật và quyền riêng tư của phương pháp này trước tiên phải được xác định, đánh giá và tổng hợp. Học liên kết được ưu tiên trong các trường hợp sử dụng khi bảo mật và quyền riêng tư là mối quan tâm chính và có tầm nhìn rõ ràng cũng như hiểu biết về các yếu tố rủi ro cho phép người triển khai, áp dụng học liên kết trong một môi trường an toàn và mang lại cho nhà nghiên cứu thấy được các hướng nghiên cứu một cách rõ ràng. Bài báo này nhằm mục đích cung cấp một bức tranh toàn diện liên quan đến các khía cạnh bảo mật của FL. Bài báo này trình bày mô tả minh họa về các phương pháp tiếp cận và các phương pháp triển khai khác nhau cùng với việc xem xét thách thức hiện tại trong FL và thiết lập một đánh giá chi tiết về các mối quan tâm về bảo mật một cách đầy đủ nhất. Các mối đe dọa bảo mật phổ biến nhất hiện nay là đầu độc và tấn công cửa sau. Bài báo kết thúc với việc đưa ra các hướng nghiên cứu cần thiết trong tương lai để làm cho FL phù hợp trong các tình huống thực tế.

Từ khóa: Học liên kết, đầu độc, tấn công cửa sau, mạng sinh đôi kháng, tổng hợp mô hình.

1. GIỚI THIỆU

Trong mô hình học máy truyền thống, hiệu quả và độ chính xác của mô hình phụ thuộc vào sức mạnh tính toán và dữ liệu huấn luyện của máy chủ. Nói một cách ngắn gọn, trong mô hình học máy truyền thống, dữ liệu người dùng được lưu trữ trên máy chủ và sử dụng cho các quá trình huấn luyện và kiểm thử để cuối cùng tạo ra các mô hình học máy toàn diện. Nhìn chung, các phương pháp học máy dựa trên mô hình tập trung có liên quan đến các thách thức khác nhau bao gồm sức mạnh và thời gian tính toán, cũng như quan trọng nhất là bảo mật và quyền riêng tư đối với dữ liệu của người dùng đã bị bỏ quên trong một thời gian dài. Học liên kết [12] đề xuất gần đây nổi lên như một giải pháp công nghệ giải quyết các vấn đề như vậy.

Học liên kết [38] cung cấp một cách thức bảo vệ quyền riêng tư của người dùng bằng cách tách biệt dữ liệu từ máy chủ trung tâm đến các thiết bị đầu cuối và mang lại lợi ích cho các lĩnh vực cần huấn luyện mô hình học máy khi cần thu thập dữ liệu nhạy cảm và không đồng nhất. Mô hình này được sử dụng chủ yếu vì hai lý do: (1) không có lưu trữ dữ liệu tập

trung ở phía máy chủ (trái ngược với học máy truyền thống) do các luật bảo vệ riêng tư dữ liệu yêu cầu hạn chế truy cập trực tiếp vào dữ liệu người dùng; và (2) bảo vệ quyền riêng tư dữ liệu bằng cách huấn luyện mô hình sử dụng dữ liệu cục bộ từ các thiết bị tính toán bên, tức là máy khách, sau đó gửi tham số mô hình cục bộ thay vì gửi dữ liệu nhạy cảm đến máy chủ. Bảo vệ quyền riêng tư dữ liệu mang lại tính khả thi để tận dụng các lợi ích trí tuệ nhân tạo được kích hoạt thông qua các mô hình học máy một cách hiệu quả trên nhiều lĩnh vực khác nhau. Ngoài ra, sức mạnh tính toán được chia sẻ giữa các bên quan tâm thay vì dựa vào một máy chủ tập trung bằng quá trình huấn luyện mô hình cục bộ lặp đi lặp lại trên các thiết bị đầu cuối. Với khái niệm dữ liệu phi tập trung, học liên kết là một trong những lĩnh vực đang phát triển khá mạnh của mô hình học máy trong những năm gần đây, vì mô hình này đi kèm với các tính năng bảo mật và quyền riêng tư hứa hẹn sẽ tuân thủ các luật bảo vệ dữ liệu người dùng do các chính phủ đưa ra [5], [15]. Ngoài quyền riêng tư, học liên kết mang lại lợi ích học máy cho các mô hình không có đủ dữ liệu huấn luyện để xây dựng mô hình học máy độc lập.

Trong mô hình học liên kết, dữ liệu vẫn nguyên vẹn trên thiết bị của người dùng và quá trình tải lên dữ liệu truyền thông qua mạng có thể được bỏ qua một cách dễ dàng, thay vào đó là quá trình chia sẻ các tham số mô hình cục bộ với máy chủ và tham số mô hình học máy toàn cục với từng máy khách, từ đó mở ra nhiều cách để khai thác lỗ hổng trong môi trường học liên kết. Vì mô hình học liên kết đang ở những bước nghiên cứu ban đầu nên nhiều nghiên cứu khác nhau được đưa ra để cải thiện các mô hình, cách thức giao tiếp hiện có và đảm bảo quyền riêng tư cũng như bảo mật dữ liệu người dùng trong học liên kết.

Mỗi khi một công nghệ mới được giới thiệu và một hệ sinh thái mới được tạo ra, một loạt các hiệu ứng kỹ thuật thường xuất hiện theo thời gian. Theo một cách tích cực và hiệu quả, việc giới thiệu học liên kết được cho là cần phải nghiên cứu sâu hơn về tính đúng đắn và chính xác của mô hình, đặc biệt là đối với các khía cạnh bảo mật và quyền riêng tư. Do đó, một loạt các vấn đề bảo mật và quyền riêng tư đang phải đối mặt hiện nay và liệu những vấn đề đó sẽ xảy ra trong tương lai do việc áp dụng công nghệ mới này không? Bài viết này nhằm mục đích cung cấp câu trả lời cho những loại câu hỏi này và làm sáng tỏ các vấn đề về bảo mật và quyền riêng tư không mong muốn có thể xảy ra trong tương lai mà chúng ta nên lưu tâm và chuẩn bị.

Những đảm bảo bảo vệ quyền riêng tư của học liên kết trong quá trình thu thập dữ liệu ở các lĩnh vực ứng dụng khác nhau có thể chứa dữ liệu nhạy cảm. Ở một mức độ nào đó, học liên kết giải quyết các mối lo ngại về quyền riêng tư của dữ liệu nhạy cảm trong môi trường học máy. Tuy nhiên, việc chia sẻ tham số mô hình và số lần huấn luyện lặp lại và giao tiếp tăng lên khiến môi trường học liên kết gặp phải một loạt rủi ro mới và mở ra những lỗ hổng mới cho việc tấn công [2] cũng như những kẻ tấn công tò mò theo dõi các lỗ hổng để thao túng đầu ra của mô hình học máy hoặc giành quyền truy cập vào dữ liệu nhạy cảm của người dùng. Để đảm bảo tận dụng lợi ích của học liên kết thay vì rủi ro và sử dụng các tính năng của học liên kết đúng cách, nhu cầu trong lĩnh vực nghiên cứu này ngay lập tức có độ ưu tiên cao nhất để khảo sát tất cả các cuộc tấn công bảo mật và quyền riêng tư có thể xảy ra trên môi trường học liên kết. Nếu không có thông tin chính xác và tầm nhìn rõ ràng, học liên kết có thể bị đẩy lùi mà không có cơ hội để phát triển và tận dụng lợi ích của nó.

Như đã thấy trong các nghiên cứu gần đây, phần lớn công việc được đề xuất trong học liên kết nhằm mục đích áp dụng mô hình mới này dưới một số dạng và hình thức cho các lĩnh

vực ứng dụng khác nhau. Trong nghiên cứu này giới thiệu các vấn đề liên quan học liên kết và có thể được sử dụng làm tài liệu tham khảo để thúc đẩy các nghiên cứu liên quan đến bảo mật mô hình học liên kết trong tương lai nhằm thúc đẩy việc chấp nhận mô hình này ngày càng rộng rãi. Để đạt được mục tiêu này, bài báo giải quyết vấn đề bằng cách xác định và đánh giá các mối đe dọa về bảo mật và quyền riêng tư cũng như các chiến lược giảm thiểu của học liên kết bằng cách trả lời một số câu hỏi nghiên cứu cụ thể.

Mặc dù đã có nhiều nghiên cứu về chủ đề này, nhưng vẫn chưa có đầy đủ các vấn đề liên quan đến việc hiểu học liên kết về các rủi ro bảo mật và quyền riêng tư. Bài báo này đóng góp một cái nhìn tổng quan toàn diện về bảo mật học liên kết bao gồm các định nghĩa, những nghiên cứu đạt được và thách thức, đều này làm nên sự khác biệt so với các nghiên cứu trước đây. Bài báo này có thể đóng góp một cái nhìn tổng thể cho các nhà khoa học dữ liệu và nghiên cứu bảo mật về việc thiết kế các giải pháp dựa trên học liên kết để giảm bớt những thách thức, rủi ro trong tương lai. Các phác thảo về những đóng góp của nghiên cứu này liên quan đến các nghiên cứu gần đây trong lĩnh vực này có thể được tóm tắt như sau:

- Cung cấp phân loại và tổng quan về các phương pháp và kỹ thuật trong việc thực hiện mô hình học liên kết.
- Xác định và kiểm tra các lỗ hổng bảo mật và các mối đe dọa trong môi trường học liên kết, các cuộc tấn công trên mô hình học máy, cụ thể liên quan đến học liên kết.
- Cung cấp thông tin về các cơ chế bảo mật hiện tại và các hướng đi trong tương lai để tăng cường tính bảo mật và quyền riêng tư khi triển khai mô hình học liên kết.

Phần còn lại của bài báo bao gồm các nội dung sau: phần 2 thực hiện phân loại các phương pháp và kỹ thuật liên quan đến học liên kết. Phần 3 đưa ra các vấn đề cần nghiên cứu về tính bảo mật của mô hình học liên kết và trình bày tổng quan các nghiên cứu liên quan. Cuối cùng, phần 4 đưa ra các hướng phát triển trong tương lai về bảo mật trong học liên kết. và đưa ra các nhận xét kết luận.

2. PHÂN LOẠI MÔ HÌNH HỌC LIÊN KẾT

Học liên kết đang được nghiên cứu phát triển mạnh mẽ, sử dụng nhiều kỹ thuật và cách tiếp cận khác nhau để hiện thực hóa trong thực tế. Đối với một công nghệ mới nổi, việc phân loại các kỹ thuật và phương pháp là bước đầu tiên quan trọng giúp hiểu và khám phá bức tranh lớn của mô hình. Trong phần này cung cấp tổng quan về cách thức hoạt động, các kỹ thuật từ nhiều góc nhìn khác nhau được sử dụng từ đó sẽ để hiểu sâu hơn về các khía cạnh bảo mật và quyền riêng tư trong các phần tiếp theo. Hình 1 cho thấy góc nhìn về phân loại mô hình học liên kết. Trong phân loại này, bài báo đề cập đến cấu trúc liên kết mạng triển khai mô hình học liên kết được sử dụng để huấn luyện mô hình, phân loại dựa trên tính khả dụng và phân vùng dữ liệu, thuật toán tổng hợp được sử dụng tại máy chủ trung tâm.

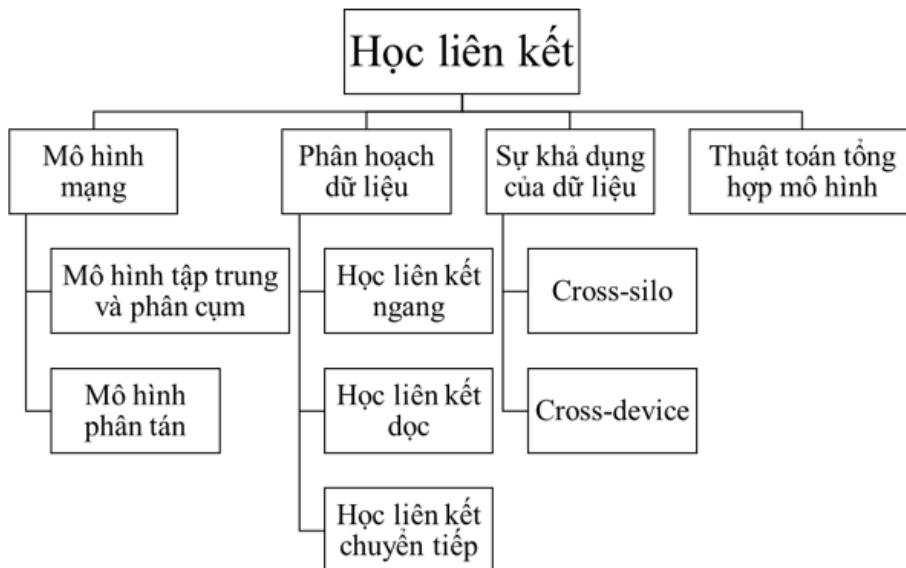
2.1. Dựa trên mô hình mạng

2.1.1. Mô hình tập trung và phân cụm

Mặc dù học liên kết về cơ bản dựa trên cách tiếp cận dữ liệu phi tập trung, nhưng vẫn có sự phụ thuộc vào một máy chủ tập trung để quản lý tổng hợp các mô hình được huấn luyện từ các máy khách, tổng hợp mô hình toàn cục và chia sẻ lại với tất cả các máy khách. Điều này chủ yếu được ưu tiên để thiết lập hệ thống bên thứ ba nhằm xây dựng yếu tố tin cậy giữa các máy khách. Cấu trúc liên kết một máy chủ và nhiều máy khách [62] được tuân thủ để đảm bảo

một máy chủ xác thực, tin cậy tập trung giám sát và quản lý quá trình huấn luyện diễn ra liên tục. Không giống như máy chủ tập trung truyền thống, lưu trữ dữ liệu và huấn luyện một mô hình nhất định trên dữ liệu được chia sẻ, máy chủ tập trung trong môi trường học liên kết chỉ hoạt động trên mô hình được chia sẻ thông qua việc thu thập các bản cập nhật tham số mô hình học từ máy khách được tổng hợp đồng bộ hoặc bất đồng bộ. Việc triển khai học liên kết phổ biến hiện nay trong thực tế sử dụng cách tiếp cận tập trung.

Kỹ thuật phân cụm được đề xuất để cải thiện học liên kết nhằm giải quyết tính không đồng nhất trong dữ liệu của máy khách trong cấu trúc liên kết mạng tập trung. Phân cụm là một trong những kỹ thuật có thể giúp phát hiện các bản cập nhật độc hại. Một công trình nghiên cứu trong [67] đề xuất ba thuật toán để đạt được tính riêng tư mô hình cục bộ với số lượng vòng giao tiếp tối thiểu. Trong thuật toán phân cụm người dùng, các cụm được tạo với một nhóm máy khách có phân phối dữ liệu tương tự và với mỗi máy khách, một mô hình trung gian được tạo để giúp mô hình toàn cục hội tụ nhanh hơn. Một cách tiếp cận khác dựa trên mô hình học máy đa tác vụ được đề xuất trong [50] trong đó các cụm máy khách được xác định dựa trên sự giống nhau về mức độ tương tự của các mô hình cục bộ. Nhóm máy khách ban đầu được lấy và chia thành các cụm theo cách đệ quy dựa trên tiêu chí dừng được đặt dựa trên độ tương tự của các tham số mô hình.



Hình 1. Tổng quan về phân loại học liên kết

Nghiên cứu trong [69] đề xuất tối đa hóa kỳ vọng ngẫu nhiên liên kết (Federated Stochastic Expectation Maximization – FedSEM) để huấn luyện nhiều mô hình học máy toàn cục. Hàm mất mát được gọi là mất mát liên kết dựa trên khoảng cách (DF-Loss) là mục tiêu của học liên kết nhiều máy chủ nhằm tìm ra mô hình toàn cục tối ưu trong số các mô hình toàn cục khác nhau từ môi trường đa cụm. Các tác giả trong [44] đề xuất thuật toán cụm liên kết lặp (Iterative Federated Cluster Algorithm – IFCA) cố gắng giảm thiểu hàm mất mát của từng máy khách và gán các máy khách vào một cụm trong mỗi vòng huấn luyện. Dựa trên thu thập từ các cụm để tính trung bình IFCA, giải thuật mở rộng trong hai biến thể được gọi là tính trung bình theo mô hình và trung bình theo độ dốc. IFCA áp dụng khởi tạo ngẫu nhiên và nhiều lần khởi động lại để xác định máy khách với một cụm cụ thể và đạt được giá trị tối ưu.

2.1.2. Mô hình phân tán

Cách tiếp cận hoàn toàn phi tập trung giúp loại trừ sự phụ thuộc vào máy chủ trung tâm để tổng hợp mô hình. Quyền hạn tập trung được thay thế bằng các thuật toán để thiết lập niềm tin và độ tin cậy. Như đã trình bày trong [14], không có khái niệm về mô hình toàn cục và mỗi máy khách tham gia cải thiện mô hình bằng cách chia sẻ thông tin với các máy hàng xóm. Các tác giả trong [51] đề xuất một thuật toán tính trung bình đáp ứng dựa trên nguyên lý Byzantine, giả định rằng hơn một nữa các đối tượng tham gia trong hệ thống là trung thực. Với cách tiếp cận này, một nhóm máy khách từ các lĩnh vực khác nhau có mục tiêu chung sẽ cộng tác để chia sẻ dữ liệu và xây dựng mô hình học máy có độ chính xác cao [11], [68] mà không cần phải dựa vào máy chủ tập trung của bên thứ ba. Các tác giả trong [33] đề xuất một mô hình gọi là MATCHA để giải quyết sự chậm trễ của mạng bằng cách cung cấp các liên kết quan trọng để máy khách giao tiếp với nhau.

2.2. Dựa trên phân hoạch dữ liệu

2.2.1. Học liên kết ngang

Học liên kết ngang được định nghĩa là trường hợp mà bộ dữ liệu trên thiết bị chia sẻ các đặc trưng giống nhau với các mẫu dữ liệu khác nhau. Mô hình học liên kết đầu tiên được Wang [37] nghiên cứu thuộc danh mục này. Mô hình học máy trong [37] có thể dự đoán các từ có thể tiếp theo người dùng muôn nhập văn bản, hoạt động dự đoán chính xác hơn với nguồn dữ liệu thực dưới dạng đầu vào từ người dùng cung cấp. Trong trường hợp này, ứng dụng bàn phím Google (còn được gọi là Gboard) tự cải thiện bằng cách liên tục học từ người dùng thiết bị di động Android. Cách tiếp cận học liên kết được triển khai bằng cách lấy trung bình các bản cập nhật từ dữ liệu thống kê do người dùng nhập vào mà không gắn danh tính người dùng. Một ví dụ khác là từ lĩnh vực y tế, nơi một nhóm các nhà nghiên cứu làm việc trên mô hình học máy có thể phân tích hình ảnh y tế và dự đoán khả năng xuất hiện tế bào ung thư. Hình ảnh y tế được coi là dữ liệu nhạy cảm của người dùng và không thể chia sẻ do các ràng buộc về luật tính riêng tư trong dữ liệu y tế. Tuy nhiên với học liên kết, thông tin về dữ liệu riêng tư đó có thể được chia sẻ an toàn thông qua tham số mô hình từ máy khách.

2.2.2. Học liên kết đọc

Học liên kết đọc là một cách tiếp cận trong đó dữ liệu chung giữa các lĩnh vực không liên quan được sử dụng để huấn luyện mô hình học máy toàn cục. Những người tham gia phương pháp này muốn có một tổ chức, tài nguyên thứ ba trung gian để cung cấp mã hóa nhằm đảm bảo rằng các dữ liệu dùng chung được chia sẻ. Tuy nhiên, không bắt buộc phải có thực thể trung gian, nghiên cứu trong [61] cho thấy việc triển khai học liên kết đọc mà không có bên thứ 3 tham gia mã hóa. Các trường hợp sử dụng thời gian thực cho phương pháp học liên kết theo chiều đọc sẽ là một tình huống trong đó bộ phận tiếp thị thẻ tín dụng trong ngân hàng muốn nâng cao mô hình học máy của họ bằng cách đưa thêm các thông mặt hàng được mua nhiều nhất từ lĩnh vực mua sắm trực tuyến vào mô hình huấn luyện. Chỉ một nhóm người chung mở tài khoản trong ngân hàng và các khách hàng mua sắm trên trang web mới được chia sẻ để huấn luyện mô hình học máy. Với sự liên kết trao đổi thông tin này, các lĩnh vực ngân hàng có thể phục vụ khách hàng tốt hơn với các ưu đãi có liên quan và các lĩnh vực mua sắm trực tuyến có thể thay đổi chính sách chăm sóc khách hàng sử dụng thẻ tín dụng.

2.2.3. Học liên kết chuyển tiếp

Học chuyển đổi liên kết là một triển khai của kỹ thuật học chuyển tiếp mô hình học máy hiện có, đây là một cách để huấn luyện một yêu cầu mới trên một mô hình được huấn luyện trước đó đã được huấn luyện trên một bộ dữ liệu tương tự để giải quyết một vấn đề hoàn toàn khác. Trong thế giới học máy, huấn luyện trên một mô hình được huấn luyện trước mang lại kết quả tốt hơn nhiều so với huấn luyện được thực hiện trên một mô hình mới được xây dựng từ đầu. Trong [40, 48], các tác giả giải thích về việc triển khai học liên kết trong các chế độ học chuyển tiếp. Một ví dụ thời gian thực sẽ tương tự như học liên kết dọc với một vài thay đổi. Thay vì hạn chế các điều kiện chỉ chia sẻ thông tin dữ liệu phù hợp, người tham gia có thể hưởng lợi từ bộ dữ liệu lớn hơn và mô hình học máy được huấn luyện tốt để phục vụ các yêu cầu cá nhân của họ. Như đã giải thích trong [40], một ví dụ thời gian thực là áp dụng mô hình toàn cục trên đám mây cho người dùng được cá nhân hóa. Mô hình này có thể được sử dụng để cung cấp mô hình được cá nhân hóa trên các thiết bị Internet of Things (IoT), cụ thể là các thiết bị đeo thông minh của một người dùng cụ thể.

2.3. Dựa trên sự khả dụng của dữ liệu

2.3.1. Cross-silo

Trong trường hợp này, số lượng máy khách thường có quy mô nhỏ từ 2-100 thiết bị, thường được lập chỉ mục và hầu như luôn sẵn sàng cho các vòng huấn luyện. Dữ liệu huấn luyện có thể được phân loại thành học liên kết ngang hoặc học liên kết dọc. Vấn đề nút thắc cổ chai trong quá trình giao tiếp hoặc tính toán là những vấn đề lớn. Học liên kết theo cross-silo linh hoạt hơn so với học liên kết cross-device và được sử dụng trong các tình huống tổ chức hoặc nhóm thực hiện huấn luyện mô hình học máy với dữ liệu bí mật của họ. Như trong triển khai học liên kết theo chiều dọc và chuyển tiếp, một kỹ thuật mã hóa được ưu tiên để hạn chế suy luận thông tin từ mỗi máy khách. Được xây dựng trên mô hình học FATE [63], công trình nghiên cứu trong [58] chứng minh cross-silo với mã hóa đồng cấu và đề xuất thuật toán mã hóa hàng loạt dựa trên lượng tử hóa độ dốc [7] để giảm chi phí tính toán và giao tiếp trong môi trường học liên kết [41].

2.3.2. Cross-device

Cách tiếp cận học liên kết với một số lượng lớn máy khách trong cùng một lĩnh vực có cùng sự quan tâm từ mô hình toàn cục được gọi là học liên kết cross-device. Do số lượng máy khách quá lớn, rất khó để theo dõi và duy trì nhật ký lịch sử hoạt động. Hầu hết các máy khách kết nối thông qua môi trường mạng không đáng tin cậy, việc lựa chọn, tham gia các vòng huấn luyện diễn ra ngẫu nhiên. Tương tự như phân vùng dữ liệu trong học liên kết theo chiều ngang, các chiến lược phân bổ tài nguyên [24] như lựa chọn, trọng tâm quan trọng của máy khách [19], lập lịch thiết bị [52] được sử dụng để chọn các bản cập nhật từ máy khách có đóng góp tốt hơn trong việc tổng hợp mô hình. Đối với các trường hợp sử dụng có số lượng máy khách lớn như các thiết bị IoT hoặc ứng dụng di động [21] thì mô hình này rất phù hợp.

2.4. Dựa trên thuật toán tổng hợp mô hình

2.4.1. Thuật toán trung bình cộng liên kết (Federated Averaging)

Triển khai học liên kết [12] giới thiệu thuật toán tổng hợp mô hình trung bình cộng liên kết (Federated Averaging – FedAvg) dựa trên thuật toán tối ưu hóa SGD (stochastic gradient descent). Là một phần của thuật toán FedAvg, máy chủ trung tâm đóng vai trò điều phối hoặc bắt đầu quá trình huấn luyện mô hình học liên kết bằng cách chia sẻ tham số toàn cục và mô hình toàn cục cho một nhóm máy khách được chọn gọi là mini-batch, nhóm này huấn luyện

mô hình học máy với dữ liệu huấn luyện cục bộ và tham số mô hình toàn cục, đồng thời chia sẻ tham số mô hình đã huấn luyện cục bộ với máy chủ tập trung. Mô hình toàn cục được tạo bằng cách tính trung bình cộng các trọng số của tất cả các bản cập nhật mô hình cục bộ được tổng hợp tại máy chủ. Tiêu chí cấu hình dựa trên số vòng huấn luyện là điều kiện dừng vòng lặp và tính trung bình các bản cập nhật mô hình cục bộ.

2.4.2. Tính toán an toàn đa bên (Secure Multiparty Computation Average)

Như trong [9] trình bày cách tổng hợp an toàn dựa trên khái niệm thuật toán tính toán an toàn đa bên (Secure Multiparty Computation – SMC), thuật toán tổng hợp các giá trị riêng tư của các bên không tin tưởng lẫn nhau mà không tiết lộ thông tin về giá trị riêng tư của họ. Giải thuật được thiết kế, sử dụng để giải quyết các thách thức của môi trường học liên kết với các thành viên tham gia là các thiết bị di động.

2.4.3. FedProx

Đây là phiên bản cải tiến của thuật toán FedAvg [12] được đề xuất trong [47] để giải quyết tính không đồng nhất trong học liên kết. Kết quả thử nghiệm của bài báo cho thấy kết quả tích cực đối với FedProx trong môi trường không đồng nhất. Tuy nhiên, nghiên cứu thử nghiệm [18] được thực hiện trên FedAvg và FedProx đã chứng minh rằng FedAvg đạt được độ chính xác cao nhất trong số các thuật toán tính trung bình trong mô hình học liên kết. FedProx xem xét sự thay đổi của sức mạnh tính toán và những yếu tố khác nhau của thiết bị tham gia các vòng huấn luyện trong học liên kết.

2.4.4. FedMA

Trong [37], các tác giả đề xuất để xây dựng một mô hình dùng chung cho các bản cập nhật tham số học máy cho các mô hình học sâu mạng nơ ron tích chập (Convolutional Neural Network – CNN) và mạng bộ nhớ dài-ngắn hạn (Long Short Term Memory networks – LSTM) trong môi trường học liên kết. FedMA thực hiện tính trung bình của các mô hình tại máy chủ trung tâm bằng cách đổi sánh theo từng lớp và lấy trung bình các phần tử ẩn như nơ-ron và kẽm trong mạng nơ-ron. Tương tự như công việc được đề xuất trong [35], cách tiếp cận này hoạt động trên cùng một khái niệm về các nơ-ron phù hợp và chỉ hiệu quả trên các mạng nơ-ron đơn giản như là mạng được kết nối đầy đủ. Như được trình bày trong bài [37], phương pháp FedMA hoạt động tốt với môi trường các máy khách không đồng nhất và vượt trội so với FedAvg và FedProx trong một vài vòng huấn luyện.

2.4.5. Trung bình có kiểm soát ngẫu nhiên

Lấy trung bình có kiểm soát ngẫu nhiên cho học liên kết (Stochastic Controlled Averaging for Federated Learning – Scaffold) được đề xuất trong [46] giải quyết vấn đề chênh lệch độ dốc của máy khách gấp phải trong thuật toán lấy trung bình liên kết cho các phương pháp học liên kết trong đó các máy khách ở trạng thái mà thuật toán có thể duy trì kiểm soát các biến thể ở phía máy khách và máy chủ để đảm bảo rằng các bản cập nhật của máy khách đang hướng tới hội tụ toàn cục.

2.4.6. Tensor Factorization

Rất ít ứng dụng trong lĩnh vực y tế thích sử dụng tensor factorization [28] để hạn chế lượng thông tin được chia sẻ. Tensor factorization chuyển đổi phần lớn hồ sơ y tế thành các kiểu hình sinh học có ý nghĩa. Các tác giả trong [28] đề xuất hệ số tensor để bảo vệ tính riêng

tư cho các hệ số sinh học (TRIP). TRIP chia sẻ dữ liệu tổng hợp và kiểu hình sinh học giúp bảo vệ quyền riêng tư của dữ liệu người dùng.

2.4.7. Personalisation-based

Nghiên cứu trong [64] đề xuất một cách tiếp cận để tách các lớp mạng thần kinh thành các lớp cơ sở và các lớp được cá nhân hóa tại mỗi nút máy khách. Theo cách tiếp cận này, tính trung bình học liên kết chỉ được áp dụng cho các bản cập nhật lớp cơ sở từ máy khách, giúp loại bỏ tính không đồng nhất của máy khách và tập trung vào nhiệm vụ huấn luyện. Học liên kết được cá nhân hóa đáp ứng (Adaptive personalized Federated Learning – APFL) được đề xuất trong [53] gợi ý học từ sự kết hợp giữa mô hình toàn cục và mô hình cục bộ để đạt được phiên bản mô hình học máy cá nhân hóa tại mỗi máy khách. Khác với cách tiếp cận học liên kết cổ điển là chia sẻ một mô hình cục bộ duy nhất, cách tiếp cận này đề xuất ba mô hình tại mỗi máy khách, một mô hình cục bộ được huấn luyện về dữ liệu cục bộ, mô hình thứ hai là bản sao cục bộ của mô hình toàn cục và mô hình thứ ba là mô hình học máy được cá nhân hóa xây dựng bằng cách sử dụng trộn các tham số. Dựa trên phân phối dữ liệu trung bình trên các máy khách, một tham số trộn được tính toán tại mỗi nút máy khách, thông số này liên tục thay đổi dựa trên độ lệch tham số giữa ba mô hình (cục bộ, toàn cầu và được cá nhân hóa). Kết quả thử nghiệm của APFL hoạt động tốt hơn so với thuật toán tính trung bình cộng liên kết (FedAvg) trong việc đạt được mô hình được cá nhân hóa cho từng máy khách.

3. NHỮNG VẤN ĐỀ BẢO MẬT TRONG MÔ HÌNH HỌC LIÊN KẾT

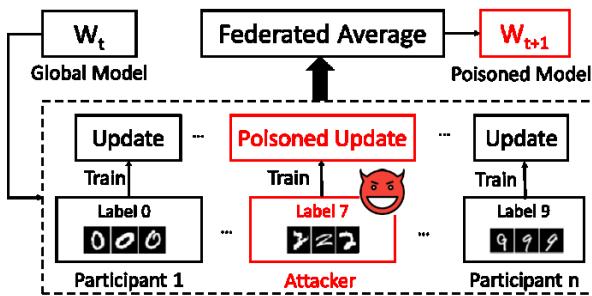
3.1. Các mối đe dọa và tấn công

3.1.1. Tấn công đầu độc (Poisoning)

Bảng 1. Những rủi ro trong mô hình học liên kết.

Mối đe dọa	Nguồn rò rỉ
Tấn công đầu độc	Dữ liệu máy khách, máy chủ trung tâm
Tấn công cửa sau	Dữ liệu máy khách
GANs	Dữ liệu máy khách, máy chủ trung tâm
Máy chủ độc hại	Máy chủ trung tâm
Tính không sẵn sàng dữ liệu	Máy khách
Nghe trộm	Giao thức truyền dữ liệu

Bảng 1 cho thấy các mối đe dọa trong học liên kết. Cuộc tấn công xảy ra phổ biến trong học liên kết được là tấn công đầu độc [25], vì mỗi máy khách trong học liên kết có quyền truy cập vào dữ liệu huấn luyện nên khả năng bị giả mạo tham số mô hình để thêm vào mô hình học máy toàn cục là rất cao. Tấn công đầu độc xảy ra trong giai đoạn huấn luyện và có tác động ngược lại, gián tiếp đến tập dữ liệu huấn luyện hoặc mô hình cục bộ làm xáo trộn hiệu suất, độ chính xác của mô hình học máy toàn cục. Trong mô hình học liên kết, tham số mô hình được lấy từ một nhóm máy khách. Điều này làm cho xác suất tấn công đầu độc từ một hoặc nhiều dữ liệu huấn luyện của máy khách là rất cao nên mức độ nghiêm trọng của mối đe dọa này cũng rất lớn như minh họa hình 2. Có 3 phương pháp tấn công đầu độc: đầu độc dữ liệu (Data Poisoning) [4], đầu độc mô hình (Model Poisoning) [22, 39], sửa đổi dữ liệu (Data Modification) [29].



Hình 2. Tấn công đầu độc mô hình học liên kết

3.1.2. Tấn công cửa sau (Backdoor attacks)

Tấn công cửa sau là một cách để đưa một tác vụ độc hại vào mô hình hiện có trong khi vẫn giữ được độ chính xác của tác vụ chính. Rất khó và tốn thời gian để xác định các cuộc tấn công cửa sau vì tính chính xác của tác vụ học máy thực tế có thể không bị ảnh hưởng ngay lập tức. Trong [39], Các tác giả thử nghiệm cách thực hiện tấn công cửa sau. Hơn nữa, các tác giả trong [65] đề xuất phương pháp cắt tia và tinh chỉnh mô hình như một giải pháp để giảm thiểu rủi ro của các cuộc tấn công cửa sau. Mức độ nghiêm trọng của các cuộc tấn công cửa sau cao vì phải tốn thời gian đáng kể để xác định sự xuất hiện của cuộc tấn công. Hơn nữa, tác động của cuộc tấn công là rất lớn vì các cuộc tấn công cửa sau có khả năng gây nhầm lẫn cho các mô hình học máy và kết quả các mẫu của lớp negative bị phân loại nhầm thành positive. Mỗi đe dọa Trojan [17, 26, 39, 54, 55] là loại tấn công cửa sau đồng thời đảm bảo tác vụ hiện có của các mô hình học máy và thực hiện tác vụ độc hại ở chế độ ẩn.

3.1.3. Tấn công dựa trên GANs

Các cuộc tấn công dựa trên mạng sinh đôi kháng (Generative Adversarial Network – GAN) trong học liên kết đã được thử nghiệm và phân tích bởi nhiều nhà nghiên cứu [34]. Với khả năng khởi động các cuộc tấn công đầu độc và suy diễn, các cuộc tấn công dựa trên GAN gây ra mối đe dọa đối với cả tính bảo mật và quyền riêng tư của một hệ thống. Nghiên cứu trong [36] chứng minh GAN có thể được sử dụng để lấy dữ liệu huấn luyện thông qua tấn công suy diễn và sử dụng GAN để đầu độc dữ liệu huấn luyện. Vì không thể lường trước được tất cả các khả năng xảy ra từ mối đe dọa dựa trên GAN, nên loại tấn công này được phân loại là mối đe dọa có mức độ tác động và độ ưu tiên cao. Thông tin thêm về các cuộc tấn công dựa trên GAN có thể được tìm thấy trong [10].

3.1.4. Máy chủ độc hại (Malicious Server)

Trong môi trường học liên kết trên nhiều thiết bị, hầu hết công việc được thực hiện tại máy chủ trung tâm, từ việc tổng hợp các tham số mô hình cục bộ đến triển khai mô hình toàn cục. Trong ngữ cảnh máy chủ bị tấn công hoặc bị đầu độc có tác động rất lớn và các máy chủ trung thực nhưng tò mò hoặc bị đầu độc có thể dễ dàng trích xuất dữ liệu riêng tư từ máy khách hoặc thao túng mô hình toàn cục để sử dụng sức mạnh tính toán được chia sẻ trong việc xây dựng các tác vụ độc hại trong mô hình học máy toàn cục.

3.1.5. Tấn công vào tính không sẵn sàng (Unavailability)

Việc máy khách không có trong trạng thái sẵn hoặc bỏ tham gia trong quá trình huấn luyện có thể gây ra các kết quả không hiệu quả trong việc huấn luyện mô hình toàn cục. Trong

trường hợp này, máy khách vô tình bỏ lỡ việc tham gia vào quá trình huấn luyện do sự cố mạng hoặc gặp bất kỳ trở ngại không mong muốn nào khác. Mức độ nghiêm trọng của mối đe dọa này ở mức trung bình vì xác suất bị tấn công trong trường hợp này thấp hơn và có một giải pháp khác thay thế trong trường hợp này sử dụng thuật toán tổng hợp bát đồng bộ.

3.1.6. Nghe trộm (Eavesdropping)

Trong học liên kết, quá trình học lặp đi lặp lại bao gồm các vòng lặp trao đổi tham số mô hình học từ máy khách đến máy chủ. Kẻ tấn công có thể nghe trộm và trích xuất dữ liệu thông qua kênh liên lạc. Nghe trộm có thể được coi là một mối đe dọa nghiêm trọng trung bình khi tấn công các mô hình học liên kết, vì các mô hình hộp đen nói chung rất khó tấn công. Những kẻ tấn công chiếm quyền điều khiển một máy khách có bảo mật yếu sẽ thu thập được các tham số mô hình học và mô hình toàn cục, lúc này tấn công chuyển từ hộp đen sang hộp trắng.

3.2. Các kỹ thuật phòng tránh

3.2.1. Sniper

Bảng 2 mô tả các kỹ thuật phòng chống các đe dọa trong môi trường học liên kết. Đầu tiên, các cuộc tấn công đầu độc bao gồm các cuộc tấn công đầu độc dữ liệu và mô hình đã được nghiên cứu và thực nghiệm trong một môi trường máy chủ trong một thời gian dài. Tuy nhiên, chỉ có một số công trình khám phá các cuộc tấn công đầu độc trong môi trường liên kết, nơi có nhiều người tham gia dưới vai trò là người tấn công với một mục tiêu tấn công nhằm kết hợp các mẫu huấn luyện bị đầu độc được thêm vào quá trình huấn luyện. Mặc dù các cuộc tấn công đầu độc trong môi trường liên kết là mối đe dọa lớn, nhưng hiệu quả của việc đầu độc trong môi trường liên kết với nhiều người tấn công vẫn chưa rõ ràng khi so sánh với cách đầu độc truyền thống với một kẻ tấn công duy nhất. Gần đây, các tác giả trong [23] đã đề xuất phương pháp Sniper giúp nhận ra người dùng hợp pháp và giảm tỷ lệ thành công của các cuộc tấn công đầu độc đáng kể ngay cả khi có nhiều người tấn công tham gia.

3.2.2. Chắt lọc thông tin (Knowledge distillation)

Đây là một biến thể của kỹ thuật nén mô hình, trong đó một mạng thần kinh được huấn luyện đầy đủ sẽ chuyển thông tin cho một mô hình nhỏ và yêu cầu từng bước cần thực hiện. Chắt lọc thông tin tiết kiệm chi phí tính toán liên quan đến huấn luyện một mô hình. Khái niệm chi chia sẻ thông tin thay vì các tham số mô hình có thể được tận dụng trong học liên kết để tăng cường tính bảo mật của dữ liệu máy khách. Tác giả trong [60] đã đề xuất một mô hình chắt lọc thông tin liên kết, cung cấp tính linh hoạt để sử dụng các mô hình học máy được cá nhân hóa và sử dụng các mô hình trung gian thu thập thông tin và chia sẻ với từng máy khách.

Bảng 2. Các kỹ thuật phòng chống trong học liên kết

Phòng chống	Mô tả	Đe dọa	Nghiên cứu
Sniper	Dựa trên phép đo khoảng cách euclidean. Kiểm tra tham số toàn cục để loại bỏ các tham số đầu độc	Đầu độc	[23]
Chắt lọc thông tin	Chuyển tiếp thông tin từ mô hình học đầy đủ sang mô hình khác	GANs Nghe trộm	[60]

Phòng chống	Mô tả	Đe dọa	Nghiên cứu
Phát hiện bất thường	Giám sát các tham số cập nhật từ các đối tượng tham gia huấn luyện mô hình học liên kết	Đầu độc Trojans	[6, 8]
Học tập đa nhiệm trong mô hình liên kết	Huấn luyện nhiều mô hình đồng thời	Khả năng chịu lỗi	[13]
Làm sạch dữ liệu	Xóa dữ liệu sau khi sử dụng huấn luyện	Đầu độc	[1]
Foolsgold	Dựa trên mật độ các tham số mô hình từ máy khách	Tấn công cửa sau	[43]
Cắt tỉa	Giảm kích thước mô hình mạng nơ ron	Tấn công cửa sau	[65]

3.2.3. Phát hiện bất thường (Anomaly detection)

Kỹ thuật này thường sử dụng trong các phương pháp thống kê và phân tích để xác định các sự kiện không phù hợp với mô hình hoặc kết quả không như mong đợi. Hệ thống phát hiện bất thường cần có đầy đủ thông tin về hành vi hoặc sự kiện bình thường để phát hiện các cuộc tấn công dưới dạng sai lệch so với hành vi bình thường. Trong môi trường học liên kết, các cuộc tấn công khác nhau như đầu độc dữ liệu, đầu độc mô hình hoặc mối đe dọa trojan có thể được phát hiện bằng các kỹ thuật phát hiện bất thường. Ví dụ: các tác giả trong [6] đề xuất Auror như một biện pháp bảo vệ chống lại các bản cập nhật máy khách độc hại bằng cách thực hiện thao tác phân cụm trên mỗi bản cập nhật máy khách trước bước tổng hợp tham số mô hình. Điều này giúp phát hiện các bản cập nhật của máy khách độc hại. Khoảng cách Euclidean được sử dụng trong [8] mô hình Krum để phát hiện độ lệch trong các tham số đầu vào từ mỗi máy khách tham gia trong học liên kết. Trong một nghiên cứu tương tự, các tác giả trong [59] xác định các bản cập nhật bất thường từ máy khách trong học liên kết. Để thực hiện kỹ thuật chống lại các cuộc tấn công trong trường hợp phát hiện bất thường với bộ mã hóa (Autoencoder) được đề xuất trong [42] giúp xác định các bản cập nhật mô hình cục bộ độc hại. Ngoài ra, công trình nghiên cứu trong [42] đề xuất từ chối dựa trên hàm mất mát (Loss function based rejection – LFR) và từ chối dựa trên tỷ lệ lỗi (Error rate based rejection – ERR) được lấy ý tưởng từ các biện pháp bảo vệ học máy hiện có như từ chối do tác động các mẫu negative (reject on negative impact – RONI) [3] & TRIM [16] để xác định các bản cập nhật có tác động đến các mẫu negative từ máy khách.

3.2.4. Học tập đa nhiệm trong mô hình liên kết

Học tập liên kết cung cấp các mô hình học máy huấn luyện một cách cộng tác trên một số lượng lớn thiết bị di động có tính đến quyền riêng tư dữ liệu cục bộ. Cài đặt này cũng có thể được mở rộng sang môi trường học tập đa tác vụ liên kết trong đó học tập đa tác vụ thúc đẩy các mô hình được cá nhân hóa nhưng được chia sẻ giữa các thiết bị. Ví dụ: mô hình MOCHA được đề xuất trong [13] được thiết kế để tăng tốc quá trình huấn luyện với khả năng chịu lỗi, và có thể hoạt động ngay cả trong các tình huống thiết bị mất kết nối. Mô hình này đề xuất để giải quyết các thách thức về thống kê và hệ thống như chi phí giao tiếp cao, vấn đề về khả năng chịu lỗi và lỗi trong môi trường học liên kết. Thực nghiệm cho thấy mô hình xử lý những thay đổi trong môi trường không đồng nhất và khả năng chịu lỗi đối với sự cố hệ thống. Một số công trình khác về mô hình học đa tác vụ liên kết được đưa ra trong [27, 57].

3.2.5. Làm sạch dữ liệu

Làm sạch dữ liệu huấn luyện do [1] đề xuất lần đầu tiên chủ yếu được sử dụng như một công cụ phát hiện bất thường để lọc ra các mẫu dữ liệu huấn luyện có vẻ đáng ngờ. Nghiên cứu gần đây của [20, 32] nhằm mục đích cải thiện các kỹ thuật làm sạch dữ liệu bằng cách sử dụng các mô hình thống kê mạnh mẽ khác nhau. Trong môi trường học liên kết, kỹ thuật làm sạch dữ liệu là một trong những kỹ thuật phòng thủ phổ biến chống lại các cuộc tấn công đầu độc dữ liệu, tuy nhiên, nghiên cứu [66] chỉ ra rằng có khả năng các cuộc tấn công đầu độc dữ liệu mạnh hơn có thể chống lại khả năng bảo vệ dữ liệu.

3.2.6. Foolsgold

Các máy khách độc hại tạo nhiều danh tính giả mạo và gửi các bản cập nhật giả mạo đến máy chủ. Kiểu tấn công này xuất phát từ các máy khách bị xâm phạm từ đó phá vỡ tính bảo mật và tính xác thực trong môi trường học liên kết. Nghiên cứu [43] đề xuất cách tiếp cận Foolsgold hiệu quả chống lại các cuộc tấn công dựa trên Sybil, lật nhẵn và đầu độc cửa sau.

3.2.7. Cắt tia (prunning)

Đây là một kỹ thuật trong học liên kết giúp giảm kích thước của mô hình học máy để giảm độ phức tạp và cải thiện độ chính xác. Trong học liên kết, máy khách có sức mạnh tính toán và băng thông truyền dữ liệu thông thường đối thấp. Vấn đề phát sinh khi chúng ta huấn luyện các mô hình mạng nơ ron học sâu có kích thước lớn được huấn luyện trong môi trường học liên kết vì máy khách thường có sức mạnh tính toán và băng thông liên lạc tương đối thấp khi so sánh với các máy trung tâm chứa dữ liệu lớn (data center). Để giải quyết những vấn đề như vậy, tác giả trong [65] đề xuất một kỹ thuật cắt tia. Vì không bắt buộc phải chia sẻ mô hình chính nên phương pháp này giúp giải quyết các cuộc tấn công cửa sau hiệu quả hơn.

4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Mô hình học liên kết vẫn còn khá nhiều thách thức cần được nghiên cứu một cách đầy đủ để mô hình học máy này được áp dụng rộng rãi. Dựa trên những nghiên cứu đã khảo sát và tìm hiểu, một số vấn đề cần nghiên cứu trong tương lai đối với mô hình học liên kết:

- Các cuộc tấn công đối kháng Zero-day và các kỹ thuật hỗ trợ tấn công. Các nỗ lực phòng chống hiện tại trong học liên kết được thiết kế để bảo vệ chống lại các lỗ hổng đã biết và các hoạt động độc hại cụ thể được xác định trước, khiến chúng ít hữu ích trong việc phát hiện các cuộc tấn công bên ngoài. Mặc dù, hiện tượng này áp dụng cho hầu như bất kỳ cơ chế phòng thủ nào của các ứng dụng học máy, nhưng khả năng xảy ra ở học liên kết là nhiều hơn vì hiện tại chưa có nhiều triển khai trong thực tế và cũng khó để chứng minh khả năng xảy ra các cuộc tấn công khác nhau. Những nghiên cứu hiện tại sử dụng mô hình học sâu nâng cao cho thấy các giải pháp đầy hứa hẹn trong việc chống lại các cuộc tấn công đối kháng zero-day [49].

- Khả năng truy xuất nguồn gốc đáng tin cậy: một thách thức lớn của học liên kết là khả năng truy xuất nguồn gốc của mô hình học máy toàn cục trong suốt quá trình huấn luyện. Chẳng hạn, nếu giá trị dự đoán bị thay đổi trong mô hình học máy toàn cục, lúc này mô hình học máy cần có khả năng theo dõi truy vết để xác định giá trị tổng hợp của tham số máy khách dẫn đến thay đổi đó. Nếu tác vụ học của mô hình học máy là một hộp đen, thì khả năng truy vết thực tế có thể bị mất và không xác định được sự thay đổi do máy khách nào hay là do mô

hình học. Một vài nghiên cứu khởi đầu tận dụng công nghệ chuỗi khối [56] với học liên kết để hỗ trợ theo vết các phiên cập nhật tham số cho mô hình học máy toàn cục [31], hy vọng một quá trình huấn luyện minh bạch, an toàn hơn.

– Lựa chọn máy khách và kế hoạch huấn luyện trong học liên kết: kế hoạch huấn luyện và chiến lược lựa chọn máy khách cho các vòng huấn luyện là rất quan trọng trong học liên kết. Nghiên cứu [30] đề xuất các cách tiếp cận tối ưu, nhưng vẫn cần phải có một cách tiếp cận chuẩn hóa cho từng trường hợp sử dụng thuật toán học máy.

– Các kỹ thuật tối ưu hóa cho các thuật toán học máy: dựa trên các thuật toán học máy khác nhau, cần phải có các thuật toán tối ưu hóa được xác định trước và chuẩn hóa để xây dựng mô hình học liên kết. Có nhiều thuật toán tổng hợp (như đã trình bày trong phần 2) để xuất tối ưu hóa hoặc nâng cao học liên kết nhưng vẫn cần có nghiên cứu chuyên sâu để cung cấp các thuật toán tối ưu hóa mô hình học liên kết cụ thể cho tất cả các ứng dụng, trường hợp sử dụng mô hình học máy hiện tại. Điều này giúp những người triển khai, bảo trì mô hình học liên kết trong tương lai phát triển các giải pháp cụ thể của học liên kết một cách dễ dàng.

– Tầm nhìn về chiến lược tổng hợp mô hình học và tham số huấn luyện: nghiên cứu [45] đề xuất chiến lược tối ưu giúp máy chủ thiết lập điểm kích hoạt để dừng, khởi động lại các vòng huấn luyện. Các nghiên cứu tương tự được thực hiện đối với mô hình và ứng dụng học máy trong các lĩnh vực khác nhau của có thể giúp hiểu được các siêu tham số của mô hình học liên kết và các điều kiện kích hoạt để có thể cấu hình trong các vòng huấn luyện. Vì các vòng huấn luyện học liên kết tốn nhiều thời gian, chi phí và sức mạnh tính toán nên việc có kế hoạch và thiết lập các giá trị tối ưu sẽ giúp các giải pháp học liên kết đạt độ chính xác cao đồng thời tiết kiệm chi phí.

Học liên kết là một công nghệ mới hỗ trợ các thiết bị tính toán cận biên (edge computing) thông qua mô hình học máy phân tán. Học liên kết đã mở rộng những ưu điểm của mô hình học máy cho các lĩnh vực có dữ liệu nhạy cảm. Bài báo này cung cấp một nghiên cứu toàn diện về các thành tựu, vấn đề và tác động của bảo mật trong môi trường học liên kết. Với các đánh giá và kết quả về bảo mật đưa ra, bài báo hy vọng sẽ cung cấp những quan điểm mới và thu hút sự chú ý của cộng đồng nghiên cứu đối với việc xây dựng mô hình học máy trong môi trường liên kết có độ rủi ro thấp, phù hợp để áp dụng phổ biến. Thông qua phản định hướng trong tương lai, bài báo phác thảo các lĩnh vực ở học liên kết cần nghiên cứu và tìm hiểu chuyên sâu. Học liên kết là một mô hình học máy mới xuất hiện trong vài năm gần đây kể từ khi Google đề xuất vào năm 2016, do đó cần nghiên cứu thêm để xác định các phần cần bổ sung nâng cao phù hợp với các môi trường học liên kết khác nhau.

TÀI LIỆU THAM KHẢO

1. Cretu, G.F., Stavrou, A., Locasto, M.E., Stolfo, S.J. and Keromytis, A.D. - Casting out demons: Sanitizing training data for anomaly sensors. In IEEE Symposium on Security and Privacy (2008) pp.81-95.
2. Narayanan, A. and Shmatikov, V. - Robust de-anonymization of large sparse datasets. In IEEE Symposium on Security and Privacy (2008) pp.111-125.
3. Barreno, M., Nelson, B., Joseph, A.D. and Tygar, J.D. - The security of machine learning, Machine Learning, 81, pp.121-148.

4. Biggio, B., Nelson, B. and Laskov, P. - Poisoning attacks against support vector machines. In Proceedings of the 29th International Conference on International Conference on Machine Learning (2012) pp.1467-1474.
5. Kaal, A., Klosek, J. and Waleski, B., - US consumer privacy bill of rights: principles and impact. Computer law review international, 13(3) (2012) pp.65-72.
6. Shen, S., Tople, S. and Saxena, P. - Aurora: Defending against poisoning attacks in collaborative deep learning systems. In Proceedings of the 32nd Annual Conference on Computer Security Applications (2016) pp.508-519.
7. Alistarh, D., Grubic, D., Li, J., Tomioka, R. and Vojnovic, M. - QSGD: Communication-efficient SGD via gradient quantization and encoding. In Advances in neural information processing systems, 30 (2017).
8. Blanchard, P., El Mhamdi, E.M., Guerraoui, R. and Stainer, J. - Machine learning with adversaries: Byzantine tolerant gradient descent. In Advances in neural information processing systems, 30 (2017).
9. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., Ramage, D., Segal, A. and Seth, K. - Practical secure aggregation for privacy-preserving machine learning. In proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (2017) pp.1175-1191.
10. Hitaj, B., Ateniese, G. and Perez-Cruz, F. - Deep models under the GAN: information leakage from collaborative deep learning. In Proceedings of the ACM SIGSAC conference on computer and communications security (2017) pp.603-618.
11. Jiang, Z., Balu, A., Hegde, C. and Sarkar, S. - Collaborative deep learning in fixed topology networks. In Advances in Neural Information Processing Systems, 30 (2017).
12. McMahan, B., Moore, E., Ramage, D., Hampson, S. and y Arcas, B.A. - Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (2017) pp. 1273-1282.
13. Smith, V., Chiang, C.K., Sanjabi, M. and Talwalkar, A.S. - Federated multi-task learning. In Advances in neural information processing systems, 30 (2017).
14. Vanhaesebrouck, P., Bellet, A. and Tommasi, M. - Decentralized collaborative learning of personalized models over networks. In Artificial Intelligence and Statistics (2017) pp. 509-517.
15. Voigt, P. and Von dem Bussche, A. - The eu general data protection regulation (gdpr), A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10(3152676) (2017), pp.10-5555.
16. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C. and Li, B. - Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. In IEEE symposium on security and privacy (SP) (2018) pp. 19-35.
17. Liu, Y., Ma, S., Aafer, Y., Lee, W.C., Zhai, J., Wang, W. and Zhang, X. - Trojaning attack on neural networks. In 25th Annual Network And Distributed System Security Symposium (2018).
18. Nilsson, A., Smith, S., Ulm, G., Gustavsson, E. and Jirstrand, M. - A performance evaluation of federated learning algorithms. In Proceedings of the second workshop on distributed infrastructures for deep learning (2018) pp. 1-8.
19. Tao, Z. and Li, Q. - eSGD: Commutation Efficient Distributed Deep Learning on the Edge. HotEdge, (2018) p.6.

20. Tran, B., Li, J. and Madry, A. - Spectral signatures in backdoor attacks. Advances in neural information processing systems, 31 (2018).
21. Xu, M., Qian, F., Mei, Q., Huang, K. and Liu, X. - Deeptype: On-device deep learning for input personalization service with minimal privacy concern. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(4) (2018) pp.1-26.
22. Bhagoji, A.N., Chakraborty, S., Mittal, P. and Calo, S. - Analyzing federated learning through an adversarial lens. In International Conference on Machine Learning (2019) pp.634-643.
23. Cao, D., Chang, S., Lin, Z., Liu, G. and Sun, D. - Understanding distributed poisoning attack in federated learning. In IEEE 25th International Conference on Parallel and Distributed Systems (2019) pp. 233-239.
24. Chen, M., Yang, Z., Saad, W., Yin, C., Poor, H.V. and Cui, S. - Performance optimization of federated learning over wireless networks. In IEEE Global Communications Conference (2019) (pp. 1-6).
25. Feng, J., Cai, Q.Z. and Zhou, Z.H. - Learning to confuse: generating training time adversarial data with auto-encoder. Advances in Neural Information Processing Systems, 32 (2019).
26. Koloskova, A., Stich, S. and Jaggi, M. - Decentralized stochastic optimization and gossip algorithms with compressed communication. In International Conference on Machine Learning (2019) pp.3478-3487.
27. Li, R., Ma, F., Jiang, W. and Gao, J. - Online federated multitask learning. In 2019 IEEE International Conference on Big Data (2019) pp. 215-220.
28. Ma, J., Zhang, Q., Lou, J., Ho, J.C., Xiong, L. and Jiang, X. - Privacy-preserving tensor factorization for collaborative health data analysis. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management (2019) pp. 1291-1300.
29. Nasr, M., Shokri, R. and Houmansadr, A. - Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In IEEE symposium on security and privacy (2019) pp.739-753.
30. Nishio, T. and Yonetani, R. - Client selection for federated learning with heterogeneous resources in mobile edge. In ICC IEEE international conference on communications (2019) pp. 1-7.
31. Salah, K., Rehman, M.H.U., Nizamuddin, N. and Al-Fuqaha, A. - Blockchain for AI: Review and open research challenges. IEEE Access, 7 (2019) pp.10127-10149.
32. Shen, Y. and Sanghavi, S. - Learning with bad training data via iterative trimmed loss minimization. In International Conference on Machine Learning (2019) pp. 5739-5748.
33. Wang, J., Sahu, A.K., Yang, Z., Joshi, G. and Kar, S. - Matcha: Speeding up decentralized sgd via matching decomposition sampling. In Sixth Indian Control Conference (2019) pp. 299-300.
34. Wang, Z., Song, M., Zhang, Z., Song, Y., Wang, Q. and Qi, H. - Beyond inferring class representatives: User-level privacy leakage from federated learning. In IEEE INFOCOM conference on computer communications (2019) pp. 2512-2520.
35. Yurochkin, M., Agarwal, M., Ghosh, S., Greenewald, K., Hoang, N. and Khazaeni, Y. - Bayesian nonparametric federated learning of neural networks. In International conference on machine learning (2019) pp.7252-7261.

36. Zhang, J., Chen, J., Wu, D., Chen, B. and Yu, S. - Poisoning attack in federated learning using generative adversarial nets. In 13th IEEE International Conference On Big Data Science And Engineering (2019) pp. 374-380.
37. Wang, H., Yurochkin, M., Sun, Y., Papailiopoulos, D. and Khazaeni, Y. - Federated learning with matched averaging. ICLR 2020.
38. Aledhari, M., Razzak, R., Parizi, R.M. and Saeed, F. - Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 8 (2020) pp.140699-140725.
39. Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D. and Shmatikov, V. - How to backdoor federated learning. In International Conference on Artificial Intelligence and Statistics (2020) pp. 2938-2948.
40. Chen, Y., Qin, X., Wang, J., Yu, C. and Gao, W. Fedhealth: A federated transfer learning framework for wearable healthcare. IEEE Intelligent Systems, 35(4) (2020) pp.83-93.
41. Choudhury, O., Gkoulalas-Divanis, A., Salonidis, T., Sylla, I., Park, Y., Hsu, G. and Das, A. - A syntactic approach for privacy-preserving federated learning. In ECAI (2020) pp. 1762-1769.
42. Fang, M., Cao, X., Jia, J. and Gong, N.Z. - Local model poisoning attacks to byzantine-robust federated learning. In Proceedings of the 29th USENIX Conference on Security Symposium (2020) pp. 1623-1640.
43. Fung, C., Yoon, C.J. and Beschastnikh, I. - The Limitations of Federated Learning in Sybil Settings. In RAID (2020) pp. 301-316.
44. Ghosh, A., Chung, J., Yin, D. and Ramchandran, K. - An efficient framework for clustered federated learning. Advances in Neural Information Processing Systems, 33 (2020) pp.19586-19597.
45. Jiang, P. and Ying, L. - An optimal stopping approach for iterative training in federated learning. In 54th Annual Conference on Information Sciences and Systems (2020) (pp. 1-6).
46. Karimireddy, S.P., Kale, S., Mohri, M., Reddi, S., Stich, S. and Suresh, A.T. - Scaffold: Stochastic controlled averaging for federated learning. In International Conference on Machine Learning (2020) pp. 5132-5143.
47. Li, T., Sahu, A.K., Zaheer, M., Sanjabi, M., Talwalkar, A. and Smith, V. - Federated optimization in heterogeneous networks. Proceedings of Machine learning and systems, 2 (2020) pp.429-450.
48. Liu, Y., Kang, Y., Xing, C., Chen, T. and Yang, Q. - A secure federated transfer learning framework. IEEE Intelligent Systems, 35(4) (2020) pp.70-82.
49. Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K.K.R. and Parizi, R.M. - An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 7(9) (2020) pp.8852-8859.
50. Sattler, F., Müller, K.R. and Samek, W. - Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. IEEE transactions on neural networks and learning systems, 32(8) (2020) pp.3710-3722.
51. Sattler, F., Müller, K.R., Wiegand, T. and Samek, W. - On the byzantine robustness of clustered federated learning. In IEEE International Conference on Acoustics, Speech and Signal Processing (2020) pp. 8861-8865.

52. Shi, W., Zhou, S. and Niu, Z. - Device scheduling with fast convergence for wireless federated learning. In IEEE International Conference on Communications (2020) (pp. 1-6).
53. T Dinh, C., Tran, N. and Nguyen, J. - Personalized federated learning with moreau envelopes. Advances in Neural Information Processing Systems, 33 (2020), pp.21394-21405.
54. Wang, R., Zhang, G., Liu, S., Chen, P.Y., Xiong, J. and Wang, M. - Practical detection of trojan neural networks: Data-limited and data-free cases. In Computer Vision–ECCV: 16th European Conference, Part XXIII 16 (2020) pp. 222-238.
55. Xie, C., Huang, K., Chen, P.Y. and Li, B. - Dba: Distributed backdoor attacks against federated learning. In International conference on learning representations (2020).
56. Yazdinejad, A., Parizi, R.M., Dehghantanha, A. and Choo, K.K.R. - P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. Computers & Security, 88 (2020) p.101629.
57. Yu, T., Li, T., Sun, Y., Nanda, S., Smith, V., Sekar, V. and Seshan, S. - Learning context-aware policies from multiple smart homes via federated multi-task learning. In IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (2020) (pp. 104-115).
58. Zhang, C., Li, S., Xia, J., Wang, W., Yan, F. and Liu, Y. - Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning. In Proceedings of the USENIX Annual Technical Conference (2020).
59. Awan, S., Luo, B. and Li, F. - Contra: Defending against poisoning attacks in federated learning. In 26th European Symposium on Research in Computer Security, Proceedings, Part I 26 (2021) pp. 455-475.
60. Gong, X., Sharma, A., Karanam, S., Wu, Z., Chen, T., Doermann, D. and Innanje, A. - Ensemble attention distillation for privacy-preserving federated learning. In Proceedings of the IEEE/CVF International Conference on Computer Vision (2021) pp. 15076-15086.
61. He, D., Du, R., Zhu, S., Zhang, M., Liang, K. and Chan, S. - Secure logistic regression for vertical federated learning. IEEE Internet Computing, 26(2) (2021) pp.61-68.
62. Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R. and D’Oliveira, R.G. - Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1-2) (2021) pp.1-210.
63. Liu, Y., Fan, T., Chen, T., Xu, Q. and Yang, Q. - Fate: An industrial grade platform for collaborative learning with data protection. The Journal of Machine Learning Research, 22(1) (2021) pp.10320-10325.
64. Mei, Y., Guo, B., Xiao, D. and Wu, W. - Fedvf: Personalized federated learning based on layer-wise parameter updates with variable frequency. In IEEE International Performance, Computing, and Communications Conference (2021) (pp. 1-9).
65. Jiang, Y., Wang, S., Valls, V., Ko, B.J., Lee, W.H., Leung, K.K. and Tassiulas, L. - Model pruning enables efficient federated learning on edge devices. In IEEE Transactions on Neural Networks and Learning Systems (2022) pp.1-13.
66. Koh, P.W., Steinhardt, J. and Liang, P. - Stronger data poisoning attacks break data sanitization defenses. Machine Learning (2022) pp.1-47.

67. Pillutla, K., Malik, K., Mohamed, A.R., Rabbat, M., Sanjabi, M. and Xiao, L. - June. Federated learning with partial model personalization. In International Conference on Machine Learning (2022) pp. 17716-17758.
68. Tu, J., Zhou, J. and Ren, D. - An asynchronous distributed training algorithm based on Gossip communication and Stochastic Gradient Descent. Computer Communications, 195 (2022) pp.416-423.
69. Long, G., Xie, M., Shen, T., Zhou, T., Wang, X. and Jiang, J. - Multi-center federated learning: clients clustering for better personalization. World Wide Web, 26(1) (2023), pp.481-500.

ABSTRACT

SECURITY IN THE FEDERATED LEARNING

Ha Le Hoai Trung¹, Tran Khanh Dang ^{2,*}

¹*University of Information Technology, VNU-HCM, Vietnam*

²*Ho Chi Minh University of Food Industry, Vietnam*

*Email: khanh@hufi.edu.vn

Federated Learning (FL), which is defined as a new branch of artificial intelligence built on decentralized training and data that brings learning to the edge or directly on-device. Federated learning is also a new area of research often referred to as the new dawn in AI, which is in its infancy and has not received much faith in the community, mainly due to its security and privacy implications. To promote research developments in this field and realize the widespread utilization of federated learning and its mass adoption, its security and privacy concerns must first be identified, evaluated and synthesized. Federated learning is preferred in the cases that security and privacy are defined as key concerns, and a clear vision and understanding of the risk factors will enable the implementers of federated learning to in a safe environment and the researcher has a clear view on possible research areas. This article aims to provide a comprehensive picture regarding the security aspects of FL, and presents a description of approaches and various implementation methods along with a review of current challenges in FL and establishes a detailed review of security and privacy concerns. The most common security threats currently are poisoning and backdoor attacks. The paper is concluded with much-needed future research directions to make FL adaptable in realistic situations.

Keywords: federated learning, poisoning attack, backdoor attacks, GANs, Aggregator.

ỨNG DỤNG AI TRONG THƯƠNG MẠI ĐIỆN TỬ THUẬT TOÁN CONTENT BASED SYSTEM HỖ TRỢ GỢI Ý MUA HÀNG

Nguyễn Hải Yến^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email:yennh@hus.edu.vn

Ngày nhận bài 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trên thế giới, trí tuệ nhân tạo (Artificial Intelligence – AI) được xem là một trong những công nghệ cốt lõi của cuộc cách mạng công nghiệp 4.0. Ứng dụng AI đang là xu hướng tất yếu, có tác động chuyển đổi to lớn đến mọi mặt đời sống xã hội. Trong đó, ứng dụng của AI trong thương mại điện tử là bước tiến vượt trội thay đổi gần như toàn bộ trải nghiệm mua hàng của người dùng, cũng như mở ra nhiều cơ hội cho những doanh nghiệp trên nền tảng trực tuyến. Trong phạm vi bài báo, tác giả muốn đề cập đến thuật toán Content based system trong hỗ trợ gợi ý mua hàng trên trang thương mại điện tử; với các nội dung sau: (1) Giới thiệu AI trong thương mại điện tử; (2) Nghiên cứu liên quan đến các hệ thống khuyến nghị trong thương mại điện tử ; (3) Thuật toán Content- based system trong hỗ trợ gợi ý mua hàng; (4) Minh họa thuật toán; (5) Kết luận và hướng phát triển.

Từ khóa: AI, E-Commerce, Recommendation systems, Content-based-system.

1. GIỚI THIỆU AI- TRONG THƯƠNG MẠI ĐIỆN TỬ

Theo số liệu từ công ty xuất bản truyền thông Mỹ Forbes, trong năm 2020, có hơn 2 tỷ người đã tham gia mua hàng trực tuyến, tổng doanh số bán lẻ điện tử đạt hơn 4,2 nghìn tỷ USD trên toàn cầu và theo Nasdaq, đến năm 2040, có đến 95% những giao dịch sẽ được thực hiện online.Thêm vào đó, có thể thấy đại dịch Covid-19 đã có những tác động đáng kể đến việc phát triển thương mại điện tử, mua sắm trực tuyến. Song song với việc phát triển của thương mại điện tử thì trí tuệ nhân tạo AI là một trong những công nghệ cốt lõi của cuộc cách mạng công nghiệp 4.0. Hiện nay AI được ứng dụng đa dạng ở nhiều lĩnh vực khác nhau trong đời sống như: y tế, giáo dục, tài chính,... và đặc biệt là trong các hệ thống thương mại điện tử.

Ứng dụng của AI trong thương mại điện tử là bước tiến vượt trội thay đổi gần như toàn bộ trải nghiệm mua hàng của người dùng, cũng như mở ra nhiều cơ hội cho những doanh nghiệp trên nền tảng trực tuyến.

– AI giúp người dùng tìm kiếm sản phẩm bằng hình ảnh thông qua một hình ảnh đã lưu trước đó hoặc một ảnh được camera chụp hình sản phẩm tại thời điểm người dùng cần tìm kiếm, hệ thống sẽ tự động đề xuất các kết quả tương đồng.

– AI cho phép máy học hành vi người dùng, từ đó dự đoán nhu cầu, sở thích để đề xuất danh sách sản phẩm phù hợp. Thuật toán có thể dựa vào từ khóa tìm kiếm, lượt nhấp, lượt thích, sản phẩm đã từng mua để nâng cao độ chính xác. Các đề xuất cá nhân hóa thông minh

của các thuật toán AI giúp người dùng dễ dàng đưa ra quyết định mua hàng từ đó giúp các trang mua bán trực tuyến cải thiện doanh số.

- AI giúp các hệ thống thương mại điện tử kết hợp cùng công nghệ thực tế ảo để tạo ra trải nghiệm trên sản phẩm (phòng thử thực tế ảo di động) giải quyết được rào cản ngại mua sắm trực tuyến vì thiếu tương tác với sản phẩm.
- AI giúp các hệ thống đảm bảo chất lượng dịch vụ 24/7 nhờ sử dụng trợ lý ảo Chatbot
- Nhờ AI các hệ thống bán hàng có thể phát hiện, ngăn chặn các hành vi gian lận, cạnh tranh xấu bao vệ lòng tin của khách hàng với thương hiệu.
- Các ứng dụng thương mại sử dụng AI có thể giúp định dạng 3D cho sản phẩm từ đó khách hàng có thể thấy toàn diện sản phẩm trong một không gian thực tế, giúp khách hàng quyết định mua sản phẩm nhanh hơn.

Trong phần tiếp theo tôi sẽ trình bày về các nghiên cứu liên quan đến các hệ thống khuyến nghị trong thương mại điện tử.

2. CÁC NGHIÊN CỨU LIÊN QUAN ĐẾN RECOMMENDATION SYSTEMS

Kết hợp AI trong các hệ thống thương mại điện tử là một trong những chủ đề được nhiều nhà khoa học và doanh nghiệp quan tâm. Sự phát triển nhanh chóng của thiết bị công nghệ, các hệ thống thương mại điện tử trở nên thuận tiện và phổ biến trong cuộc sống hàng ngày, mở rộng cơ hội mua sắm cho khách hàng; từ đó thúc đẩy nhu cầu sử dụng các hệ thống thông minh có tính năng khuyến nghị sản phẩm cho người dùng khi mua sắm trên các website thương mại điện tử. Một hệ thống có tích hợp chức năng khuyến nghị sẽ thu thập thông tin từ khách hàng và đưa ra đề xuất các mặt hàng mà thấy gần với các thông tin khách hàng yêu cầu nhất. Một hệ thống khuyến nghị được xem như là công cụ, là kỹ thuật để gợi ý sản phẩm cho khách hàng thông qua mục yêu thích của khách hàng một cách tự động từ đó làm tăng khả năng ra quyết định mua hàng. Hệ khuyến nghị được nhúng vào các lĩnh vực khác nhau như là: máy học, hệ hỗ trợ ra quyết định, phân lớp văn bản,... Thông qua việc giới thiệu cho người dùng những mặt hàng quan trọng hoặc hữu ích từ đó giải quyết vấn đề quá tải thông tin cho khách hàng khi mua sắm, các hệ thống này được chứng minh là công cụ xử lý hữu ích cho khách hàng trực tuyến và trở thành một trong các công cụ phổ biến, mạnh mẽ cho các hệ thống thương mại điện tử. Thuật toán Collaborative Filtering (CF) đưa ra các đề xuất dựa trên mối quan tâm của khách hàng [1] là một trong những thuật toán nền tảng của các hệ thống khuyến nghị; Có 6 dạng chính của hệ thống khuyến nghị

2.1. Hệ thống khuyến nghị cộng tác (collaborative recommender system)

Dựa trên ý tưởng: các sản phẩm mà những khách hàng có cùng mối quan tâm đã được “liked” trước đó sẽ được đề xuất cho nhóm khách hàng mục tiêu. Thuật toán lọc cộng tác sử dụng điểm đánh giá trước đó của khách hàng về sản phẩm để giới thiệu hoặc dự đoán những mặt hàng mới mà một số khách hàng sẽ thích. Cơ sở lý thuyết chủ yếu của thuật toán CF dựa vào khái niệm “giống nhau” giữa các khách hàng hoặc giữa các mặt hàng, sự giống nhau giữa các sở thích hoặc đánh giá xếp hạng được sử dụng làm nền tảng để đưa ra khuyến nghị [2].

Thuật toán CF là tiếp cận được sử dụng rộng rãi trong nhiều hệ thống khuyến nghị thương mại điện tử. Đây là một phương pháp dựa trên 3 quy tắc: khách hàng có sở thích và

mối quan tâm giống nhau; Sở thích và mối quan tâm của khách hàng ổn định; sự lựa chọn của khách hàng có thể được kết luận thông qua lịch sử sở thích trước đó. Do đó thuật toán công tác được xây dựng dựa trên hành động của người dùng để tìm những “hàng xóm” trực tiếp cho từng người dùng và dự đoán những mối quan tâm của người đó dựa theo sở thích của hàng xóm [3]. Tuy nhiên, thuật toán CF có thể chọn ra không đủ các “hàng xóm” lân cận từ đó các khuyến nghị đưa ra sẽ không đầy đủ. Mặt khác, thuật toán CF chịu tải tính toán cao khi dữ liệu liên quan giữa user-item lớn và hệ thống phải tính toán lại mỗi khi sản phẩm được cập nhật.

2.2. Hệ khuyến nghị dựa trên nội dung (Content based recommender system)

Lọc dựa trên nội dung là một kỹ thuật phổ biến của các hệ thống khuyến nghị. Mục tiêu chính của quá trình lọc theo nội dung là phân lớp sản phẩm bằng các từ khóa cụ thể, tìm hiểu những gì khách hàng thích, tra cứu các cụm từ đó trong cơ sở dữ liệu và sau đó sẽ đề xuất các sản phẩm tương tự. Hệ thống khuyến nghị dựa trên nội dung sẽ đề xuất các sản phẩm tương đương với những sản phẩm mà người tiêu dùng đã thích trước đó. Việc đánh giá mức độ giống nhau của các đối tượng dựa trên các đặc điểm liên quan đến các sản phẩm được so sánh. Ví dụ một cuốn sách liên quan đến thể loại hài kịch đã được khách hàng đánh giá tích cực thì hệ thống có thể đề xuất những cuốn sách khác từ thể loại đó. Trong hệ thống này các thông tin dữ liệu về lượt click chuột, lượt truy cập, lượt mua và đọc của khách hàng được sử dụng để tính mức độ yêu thích cho mỗi mặt hàng. Những mặt hàng có mức độ yêu thích cao hơn được gọi ý đến khách hàng.

Hệ thống khuyến nghị dạng này phụ thuộc rất nhiều vào thông tin đầu vào do người dùng cung cấp.

2.3. Hệ thống khuyến nghị dựa trên thông tin nhân khẩu người dùng (Demographic based recommender system)

Giới thiệu các sản phẩm dựa trên thông tin hồ sơ nhân khẩu của khách hàng (*Demographic profile*). Giả thuyết là các đề xuất khác nhau cho từng hồ sơ nhân khẩu học khác nhau. Ví dụ những thông tin về ngôn ngữ hoặc quốc tịch của khách hàng được gửi đến website nhất định; các khuyến nghị về độ tuổi của khách hàng có thể được tùy chỉnh. [4, 5]. Ưu điểm của tiếp cận dựa trên nhân khẩu học là các đánh giá của khách hàng về sản phẩm thường không cần thiết.

2.4. Hệ thống khuyến nghị dựa trên tri thức (Knowledge based recommender system)

Các hệ thống khuyến nghị dựa trên tri thức đề xuất các sản phẩm tùy thuộc vào miền kiến thức nhất định, các thuộc tính của sản phẩm cụ thể đáp ứng các yêu cầu, sở thích của khách hàng và cuối cùng là cách mà khách hàng sử dụng sản phẩm. Các thuật toán đề xuất dựa trên tri thức đáng chú ý thường dựa trên từng trường hợp cụ thể [6].

2.5. Hệ thống khuyến nghị dựa vào cộng đồng (Community-based)

Hệ thống khuyến nghị dạng này hoạt động dựa trên sở thích của bạn bè người dùng để giới thiệu các mặt hàng. Minh chứng chứng minh rằng khách hàng thường như tập trung nhiều hơn vào các đề xuất của bạn bè hơn là các đề xuất của người dùng ẩn danh có liên quan [7]. Hệ thống này liên quan đến sự phổ biến và tính mở của mạng xã hội, có thông tin từ mối quan hệ xã hội của nhóm khách hàng và các sở thích của bạn bè trong nhóm đó.

2.6. Hệ khuyến nghị lai (Hybrid Recommend Machine)

Hệ thống khuyến nghị lai có được từ việc kết hợp các phương pháp trên bằng cách kết hợp hai hoặc nhiều phương pháp và cải thiện nhược điểm của chúng [8]

3. THUẬT TOÁN CONTENT BASED SYSTEM TRONG GỢI Ý MUA HÀNG

3.1. Một số Định nghĩa

a. Định nghĩa Utility matrix

Trong một hệ thống khuyến nghị bao gồm 3 thực thể chính: (1) Người dùng - *users*, (2) Danh sách sản phẩm - *items*, (3) Đánh giá của user với mỗi item - *feedbacks*. Mỗi user sẽ có mức độ quan tâm với từng item khác nhau, mức độ quan tâm này được gán cho một giá trị ứng với mỗi cặp user – item. Giả sử mức độ quan tâm được đo bằng giá trị user đánh giá / xếp hạng cho item (*rating*). Tập tất cả các ratings bao gồm cả những giá trị chưa biết cần được dự đoán. Từ đó tạo nên một ma trận gọi là Utility matrix.

Xét ví dụ trên hệ thống gợi ý các dòng sản phẩm

Bảng 1. Utility matrix trong hệ thống gợi ý các dòng sản phẩm

	A	B	C	D	E	F
Vintas Aunter – High Top	5	5	0	0	1	?
Vintas Landforms – Low Top	5	?	?	0	?	?
Vintas Landforms – High Top	?	4	2	?	?	1
Basas Workaday – Low Top	1	1	4	4	4	?
Basas Workaday – High Top	1	0	5	?	?	?

Trong ví dụ này, có 6 users A, B, C, D, E, F và 5 nhóm sản phẩm giày. Các sản phẩm được người dùng đánh giá theo mức độ từ 0 – 5 sao tương ứng mức độ từ “không thích” đến “rất thích”. Các ô chứa dấu “?” trên nền xám ứng với dữ liệu chưa tồn tại trong CSDL, hệ thống khuyến nghị cần phải dự đoán các giá trị này, từ đó đưa ra gợi ý cho người dùng.

Từ Utility matrix ta thấy có 2 dòng sản phẩm khác nhau là Vintas và Basas. Người dùng A, B thích sản phẩm của dòng Vintas; C, D, E, F thích sản phẩm của dòng Basas. Do đó một hệ thống gợi ý dựa theo nội dung nên gợi ý Vintas Landforms – Low Top cho B ; Vintas Landforms – High Top cho A; Basas Workaday – Low Top cho F và Basas Workaday – High Top cho D, E, F. Vậy khi đưa ra một sản phẩm mới vào kinh doanh ta chỉ cần phân lớp nó thuộc dòng sản phẩm nào, từ đó đưa ra gợi ý cho từng người dùng.

Thông thường, có rất nhiều *users* và *items* trong hệ thống, và mỗi *user* thường chỉ *rate* một số lượng rất nhỏ các *item*, thậm chí có những *user* không rate *item* nào (với những *users* này thì cách tốt nhất là gợi ý các *items* phổ biến nhất). Vì vậy, lượng ô màu xám của utility matrix trong hệ thống thường là rất lớn, và lượng các ô đã được điền là một số rất nhỏ.

Rõ ràng rằng trong Utility Matrix càng nhiều ô được điền thì độ chính xác của hệ thống sẽ càng được cải thiện. Vì vậy, các hệ thống luôn luôn hỏi người dùng về sự quan tâm của họ tới sản phẩm, và muốn người dùng đánh giá càng nhiều sản phẩm càng tốt. Việc đánh giá các sản phẩm không những giúp các người dùng khác biết được chất lượng sản phẩm mà còn giúp hệ thống biết được sở thích của người dùng, qua đó đưa ra các gợi ý chính xác.

Có hai hướng để xác định giá trị rating cho mỗi cặp user – item trong Utility Matrix:

- (1) Nhờ người dùng rate sản phẩm. Amazon luôn nhờ người dùng rate các sản phẩm của họ bằng cách gửi các email nhắc nhở nhiều lần. Rất nhiều hệ thống khác cũng làm tương tự. Tuy nhiên, cách tiếp cận này có một vài hạn chế, vì thường thì người dùng ít khi rate sản phẩm. Và nếu có, đó có thể là những đánh giá thiên lệch.
- (2) Dựa trên hành vi của người dùng. Nếu một người dùng mua một sản phẩm trên Amazon, xem một clip trên Youtube (có thể là nhiều lần), hay đọc một bài báo, thì có thể khẳng định rằng người dùng đó thích sản phẩm. Facebook cũng dựa trên việc người dùng “like” những nội dung nào để hiển thị những nội dung liên quan. Thường thì với cách này, ta chỉ xây dựng được một ma trận với các thành phần là 1 và 0, với 1 thể hiện người dùng thích sản phẩm, 0 thể hiện chưa có thông tin. Chúng ta cũng có thể xây dựng ma trận với các giá trị cao hơn 1 thông qua thời gian hoặc số lượt mà người dùng xem một sản phẩm nào đó.

b. Định nghĩa Item profile

Trong các hệ thống content – based ta cần xây dựng bộ hồ sơ (*profile*) cho mỗi *item*. *Profile* này là một vector đặc trưng (*feature vector*) được trích xuất trực tiếp từ *item*. Các đặc trưng của một đôi giày thể thao được sử dụng trong hệ thống gợi ý có thể gồm (Hãng SX, Năm SX, Xuất xứ, Công dụng,...).

Xét ví dụ trên hệ thống gợi ý các dòng sản phẩm ở bảng 1, ta xây dựng feature vector hai chiều cho mỗi đôi giày: chiều thứ nhất là dòng Vintas, chiều thứ hai là dòng Basas. Đặt các feature vector cho mỗi đôi giày là x_1, x_2, x_3, x_4, x_5 cho bởi bảng 2.

Bảng 2. Feature vector cho mỗi item trong hệ thống gợi ý các dòng sản phẩm

	A	B	C	D	E	F	Items Feature vector
Vintas Aunter – High Top	5	5	0	0	1	?	X1= [0.99, 0.02]
Vintas Landforms – Low Top	5	?	?	0	?	?	X2= [0.91, 0.11]
Vintas Landforms – High Top	?	4	2	?	?	1	X3= [0.95, 0.05]
Basas Workaday – Low Top	1	1	4	4	4	?	X4= [0.01, 0.99]
Basas Workaday – High Top	1	0	5	?	?	?	X5= [0.03, 0.98]
User models	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	← cần tối ưu

Với mỗi user ta cần tìm mô hình θ_i tương ứng sao cho mô hình thu được là tốt nhất. Bài toán đi tìm mô hình θ_i cho mỗi user có thể được coi là một bài toán hồi quy trong trường hợp các rating là một dải giá trị, hoặc bài toán phân lớp trong trường hợp rating là một vài trường hợp cụ thể, như like/dislike chẳng hạn. Dữ liệu huấn luyện để xây dựng mỗi mô hình θ_i là các cặp (item profile, ratings) tương ứng với các items mà user đó đã rated. Việc điền các giá trị còn thiếu trong ma trận Utility chính là việc dự đoán đầu ra cho các item chưa được rate khi áp dụng mô hình θ_i lên chúng.

3.2 Thuật toán content based system

3.2.1. Ý tưởng

Ý tưởng của thuật toán này là: dựa vào các item mà người dùng đã đánh giá ta có được ma trận sở thích của người dùng với từng sản phẩm đã được đánh giá và thương hiệu tương ứng, qua đó tạo được user profile (sở thích / thị hiếu của người dùng với từng thương hiệu).

Từ ma trận user profile ta tạo ma trận gọi ý sản phẩm. Sắp xếp danh sách sản phẩm theo ma trận gọi ý, từ đó lấy ra được danh sách sản phẩm gọi ý

3.2.2. Thuật toán

- **Bước 1:** Từ các đánh giá của người dùng, tạo ma trận Input User Ratings.
- **Bước 2:** Mã hóa các item mà người dùng đã đánh giá thành một ma trận nhị phân.
- **Bước 3:** Dựa vào ma trận nhị phân và ma trận Input User Ratings, ta tạo và chuẩn hóa ma trận user profile cho người dùng.
- **Bước 4:** Lấy các item sản phẩm mà người dùng chưa đánh giá, mã hóa chúng thành ma trận nhị phân giống như bước 2.
- **Bước 5:** Dựa vào ma trận nhị phân tạo ở bước 4 và ma trận user profile, ta có thể tính được ma trận gợi ý.
- **Bước 6:** Ta tiến hành sắp xếp và gợi ý các sản phẩm dựa vào ma trận gợi ý.

3.2.2. Ví dụ

Trên website bán giày thể thao sneaker. Giả sử có bảng đánh giá của người dùng A về những đôi giày như sau:

Bảng 3. Bảng đánh giá của người dùng A về những sản phẩm giày

	Người dùng A
Air Jordan 1 Retro High Og	2
Yeezy Foam RNNR	5
New Balance 327	3
Nike Air Fear Of God 1 Oatmeal	?
Joe Freshgoods x New Balance 9060	?
Air Jordan 1 Retro High Og Electro Orange	?

Nhiệm vụ của Content – based systems là đề xuất các sản phẩm khác tương tự cho người dùng này, hay nói cách khác, chúng ta muốn dự đoán xếp hạng có thể có của người dùng đối với các sản phẩm khác nếu người dùng đánh giá chúng. Để đạt được điều này, chúng ta phải xây dựng hồ sơ người dùng.

Đầu tiên, chúng ta tạo một vectơ để hiển thị xếp hạng của người dùng cho những sản phẩm mà người dùng đã đánh giá. Chúng ta gọi nó là Input User Ratings.

Bảng 4. Input User Ratings

	Người dùng A
Air Jordan 1 Retro High Og	2
Yeezy Foam RNNR	5
New Balance 327	3

Sau đó, mã hóa sản phẩm thông qua phương pháp one-hot encoding. Thương hiệu sản phẩm được sử dụng là các feature. Ở đây, có 3 sản phẩm mà người dùng đã đánh giá thuộc về 3 thương hiệu là Nike, Adidas và New Balance. Ta sử dụng ba sản phẩm đầu tiên để tạo ma trận này. Giá trị 1 và 0 tương ứng “True” hoặc “False” xác định sản phẩm có thuộc thương hiệu này hay không. Với phương pháp trên, ta có được ma trận như sau:

Bảng 5. Ma trận nhị phân sản phẩm – thương hiệu

	Nike	Adidas	New Balance
Air Jordan 1 Retro High Og	1	0	0
Yeezy Foam RNNR	0	1	0
New Balance 327	0	0	1

Lấy Input User Rating X Ma trận nhị phân SP-TH = Ma trận trọng số SP-TH

Input User Ratings		Binary Matrix items- features		
	Người dùng A		Nike	Adidas
Air Jordan 1 Retro High Og	2		1	0
Yeezy Foam RNNR	5		0	1
New Balance 327	3		0	0

Weight Matrix items -features		
	Nike	Adidas
Air Jordan 1 Retro High Og	2	0
Yeezy Foam RNNR	0	5
New Balance 327	0	0

Hình 1. Ma trận trọng số

Ma trận trọng số thể hiện sở thích của người dùng đối với từng thương hiệu dựa trên những sản phẩm mà họ đã đánh giá. Dựa vào ma trận này, kết hợp thao tác chuẩn hóa ta có được User profile.

Weight Matrix items -features			
	Nike	Adidas	New Balance
Air Jordan 1 Retro High Og	2	0	0
Yeezy Foam RNNR	0	5	0
New Balance 327	0	0	3

User Profile	Nike	Adidas	New Balance
Người dùng A	2	5	3

Chuẩn hóa User Profile	Nike	Adidas	New Balance
Người dùng A	0.2	0.5	0.3

Hình 2. Tổng hợp thương hiệu có trọng số và chuẩn hóa

Sử dụng User Profile chuẩn hóa để tìm ra sản phẩm phù hợp, giới thiệu cho người dùng. Mã hóa 3 sản phẩm chưa được đánh giá trong bảng 6.

Bảng 6. Mã hóa các sản phẩm chưa được đánh giá theo hãng

	Nike	Adidas	New Balance
Nike Air Fear Of God 1 Oatmeal	1	0	0
Joe Freshgoods x New Balance 9060	0	0	1
Air Jordan 1 Retro High Og Electro Orange	1	0	0

Sau đó thực hiện nhân ma trận User Profile với ma trận mã hóa sản phẩm chưa được đánh giá, kết quả thu được một ma trận có trọng số thể hiện trọng số của từng thương hiệu với User Profile

Chuẩn hóa User Profile		Nike	Adidas	New Balance
	Người dùng A	0.2	0.5	0.3
X	X	X		

Ma trận mã hóa SP chưa rated			
	Nike	Adidas	New Balance
Nike Air Fear Of God 1 Oatmeal	1	0	0
Joe Freshgoods x New Balance 9060	0	0	1
Air Jordan 1 Retro High Og Electro Orange	1	0	0

=

Ma trận mã hóa SP chưa rated			
	Nike	Adidas	New Balance
Nike Air Fear Of God 1 Oatmeal	0.2	0	0
Joe Freshgoods x New Balance 9060	0	0	0.3
Air Jordan 1 Retro High Og Electro Orange	0.2	0	0

Hình 3. Ma trận có trọng số của từng thương hiệu với user Profile

Tổng hợp các xếp hạng có trọng số ta sẽ nhận được mức độ quan tâm có thể có của người dùng A với ba sản phẩm này. Về bản chất, đó là danh sách đề xuất các sản phẩm mà ta có thể sắp xếp để xếp hạng sản phẩm và giới thiệu chúng cho người dùng.

Ma trận mã hóa SP chưa rated			
	Nike	Adidas	New Balance
Nike Air Fear Of God 1 Oatmeal	0.2	0	0
Joe Freshgoods x New Balance 9060	0	0	0.3
Air Jordan 1 Retro High Og Electro Orange	0.2	0	0

 Σ

Weighted Average
0.2
0.3
0.2

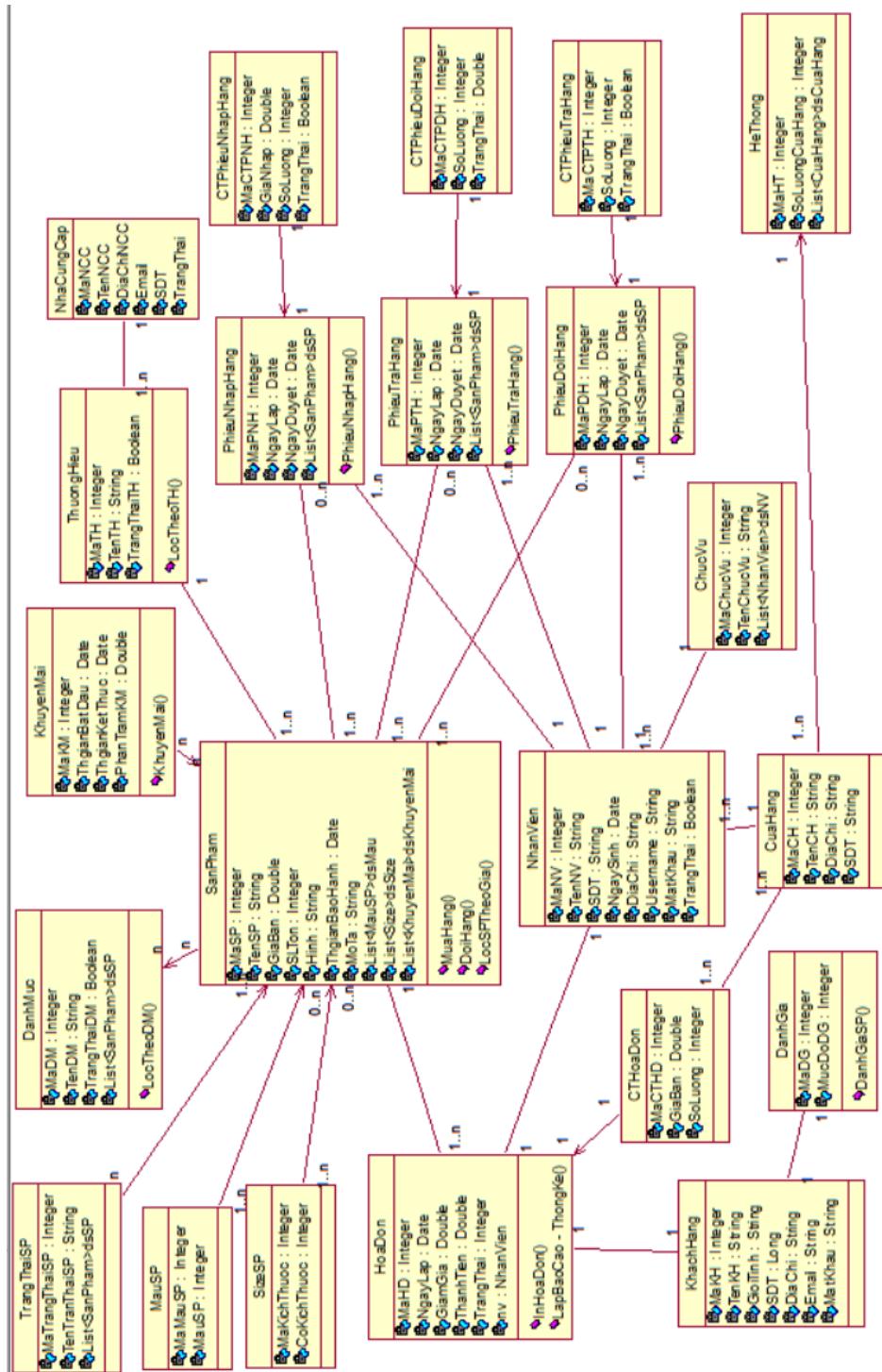
Hình 4. Xếp hạng sản phẩm và đề xuất cho người dùng

Tại đây ta có thể quay lại Bảng 3 để điền vào xếp hạng dự đoán cho người dùng.

4. MINH HỌA THUẬT TOÁN

Xây dựng website bán hàng giày thể thao Sneaker có gợi ý mua hàng

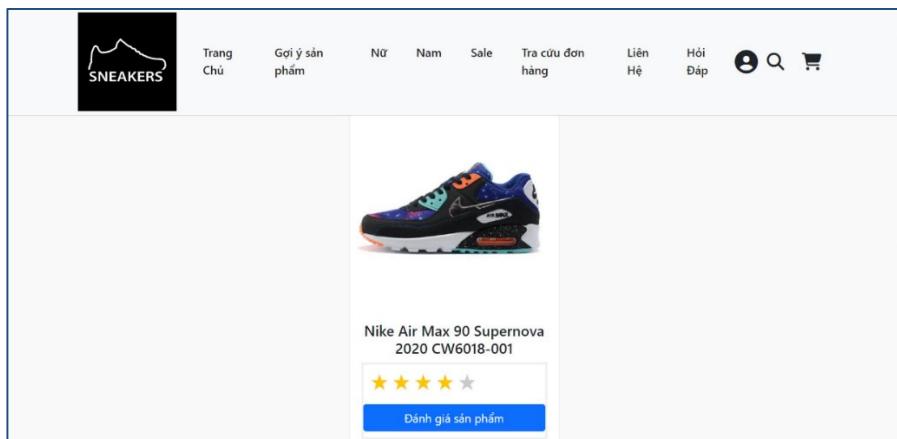
4.1. Sơ đồ lớp thiết kế (thể hiện các đối tượng dữ liệu) cho cả hệ thống.



Hình 5. Sơ đồ lớp mức thiết kế

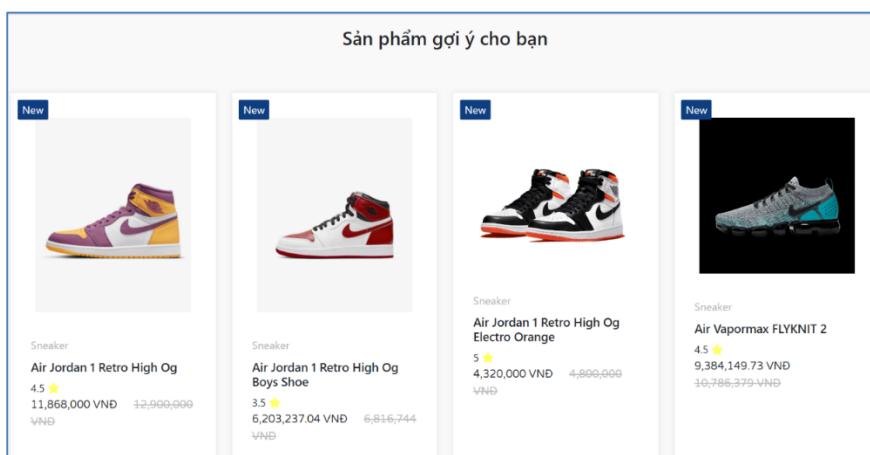
4.2. Một số giao diện màn hình chức năng chính liên quan gợi ý mua hàng

Một khách hàng sau khi hoàn tất mua hàng sẽ tiến hành đánh giá cho sản phẩm đã mua. Các mức đánh giá theo mức từ 1 đến 5 sao.



Hình 6. Màn hình đánh giá sản phẩm

Khách hàng xem sản phẩm gợi ý dựa vào đánh giá của bản thân ở những lần mua trước.



Hình 7. Màn hình gợi ý sản phẩm

5. KẾT LUẬN – HƯỚNG PHÁT TRIỂN

Thuật toán content-based là phương pháp đơn giản trong các hệ thống khuyến nghị, đặc điểm của phương pháp này là việc xây dựng mô hình cho mỗi user không phụ thuộc vào các users khác. Việc xây dựng mô hình cho mỗi users có thể được coi như bài toán hồi quy hoặc phân lớp với dữ liệu huấn luyện là cặp (item profile, rating) mà user đó đã đánh giá. Item profile không phụ thuộc vào user, nó thường phụ thuộc vào các đặc điểm mô tả của item hoặc cũng có thể được xác định bằng cách yêu cầu người dùng gắn thẻ.

Ưu điểm của Content-based systems

- Không cần dữ liệu từ những người dùng khác để gợi ý các sản phẩm.
- Có thể gợi ý sản phẩm cho nhiều người dùng có nhiều sở thích độc đáo.
- Có thể gợi ý những sản phẩm mới và ít phổ biến.

Hạn chế của Content-based systems

Người dùng có nhiều sở thích khác nhau, hệ thống này không đáp ứng được mọi sở thích của người dùng vì nó phụ thuộc vào những sản phẩm mà đã được người dùng đánh giá. Ví dụ khi người dùng chỉ đánh giá các sản phẩm thuộc thương hiệu Adidas, nhưng người dùng cũng thích các sản phẩm thuộc thương hiệu Nike. Hệ thống này sẽ không giới thiệu một sản phẩm thuộc thương hiệu Nike nào cho người dùng. Để giải quyết vấn đề này hệ thống cần kết hợp sử dụng kỹ thuật *Collaborative filtering*.

Đối với người dùng mới, hệ thống tạo một hồ sơ trung bình, tức là hồ sơ trung bình của tất cả người dùng. Và khi thời gian trôi qua, hồ sơ của người dùng mới này sẽ trở nên tinh chỉnh hơn theo các sản phẩm anh ấy đã rated. Vì vậy, có một vấn đề ở đây, tức là trong giai đoạn bắt đầu, người dùng không được khuyến nghị theo sở thích của cô ấy mà theo sở thích của một đối tượng trung bình.

Hướng phát triển

Từ hạn chế của content based system nêu trên tác giả sẽ nghiên cứu kết hợp Collaborative filtering để đưa ra đề xuất dựa trên đánh giá của tập khách hàng khác.

TÀI LIỆU THAM KHẢO

1. Farah Tawfiq Abdul Hussien1, Abdul Monem S. Rahma1 and Hala Bahjat Abdul Wahab1 - Recommendation Systems For E-commerce Systems An Overview, FISCAS 2021, IOP Publishing J. Phys.: Conf. Ser. 1897 012024.
2. Jiro Iwanaga, Naoki Nishimura , Noriyoshi Sukegawa , Yuichi Takano, " Improving collaborative filtering recommendations by estimating user preferences from clickstream data", Electronic Commerce Research and Applications, Volume 37, September–October 2019, 100877.
3. Bushra Alhijawi,Yousef Kilani," A collaborative filtering recommender system using genetic algorithm ", Information Processing & Management Volume 57, Issue 6, November 2020, 102310.
4. WenjunJiang ,Guojun Wang, MdZakirulAlamBhuiyan, , Jie Wu, " Understanding Graph-based Trust Evaluation in Online Social Networks: Methodologies and Challenges" ACM Computing Surveys, Vol. V, No. N, Article A, Publication date: February 2016
5. Ammar Jabakji , Hasan Dağ , " Improving item-based recommendation accuracy with user's Journal of Physics: Conference Series
6. Bridge D., M. Góoker, L.McGinty and B.Smyth, "Case-based recommender systems" , The Knowledge Engineering Review, Vol. 20:3, 315–320, Cambridge University Press, 2006
7. Zhang Y., J.Callan and T.Minka, . "Novelty and redundancy detection in adaptive filtering", the 25th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, New York,2002.
8. Ahmed Zahir , Yuyu Yuan and Krishna Moniz, " AgreeRelTrust—a Simple Implicit Trust Inference Model for Memory-Based Collaborative Filtering Recommendation Systems " , Electronics 2019, 8, 427; MDPI.

ABSTRACT

ARTIFICIAL INTELLIGENCE IN E-COMMERCE – CONTENT BASED IN RECOMMENDATION SYSTEM

Nguyen Hai Yen^{1,*}

¹HoChiMinh City University of Food Industry

*Email: yennh@hufi.edu.vn.

In the world, artificial intelligence – AI is considered one of the core technologies of the industrial revolution 4.0. AI application is an inevitable trend, having a great transformational impact on all aspects of social life. In particular, the application of AI in e-commerce is a remarkable step forward that changes almost the entire purchasing experience of users, as well as opens up many opportunities for businesses on the online platform. In this article, the author wants to mention the Content based system algorithm in supporting purchase suggestions on e-commerce sites; with the following contents: (1) Introduction of AI in e-commerce; (2) Research related to recommendation systems in e-commerce; (3) Content-based system algorithm in supporting purchase suggestions; (4) Illustrate the algorithm; (5) Conclusion and development direction.

Keywords: AI, E-Commerce, Recommendation systems, Content-based-system.

MỘT PHƯƠNG PHÁP GOM CỤM DỮ LIỆU CHO BÀI TOÁN TỰ VẤN LỰA CHỌN HỌC PHẦN TỰ CHỌN

Nguyễn Thị Thuỳ Trang^{1,*}, Phan Thị Ngọc Mai¹

¹Khoa Công nghệ Thông tin, Trường ĐH Công nghiệp Thực phẩm TP.HCM

*Email: trangnithuy@huf.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trong bài báo này, một cải tiến thuật toán K-Means được đề xuất nhằm phân cụm dữ liệu và áp dụng cho bài toán tư vấn lựa chọn học phần tự chọn. Để thực hiện được điều này, chúng tôi sử dụng một giá trị ngưỡng đo độ tương tự giữa các đối tượng dữ liệu, ngưỡng này được ký hiệu là θ . Trên cơ sở ngưỡng θ , thuật toán K-Means được cải tiến bằng cách không xác định trước số tâm cụm, số cụm dữ liệu tăng trưởng theo sự gia tăng sinh viên tốt nghiệp. Kết quả học tập của từng sinh viên tốt nghiệp được thể hiện dưới dạng véc-tơ có n chiều và là dữ liệu đầu vào cho thuật toán K-Means đã được cải tiến để từ đó tìm kiếm các cụm sinh viên có kết quả học tập tương đồng với trình độ của sinh viên cần tư vấn lựa chọn học phần tự chọn. Chúng tôi thực nghiệm trên dữ liệu kết quả học tập của sinh viên đã tốt nghiệp khóa 08ĐHCNTT, 09ĐHCNTT. Theo như kết quả thực nghiệm, những đề xuất của chúng tôi là khả thi và có thể ứng dụng thực tế nhằm hỗ trợ sinh viên Khoa Công nghệ Thông tin, Trường Đại học Công nghiệp thực phẩm Thành phố Hồ Chí Minh lựa chọn học phần tự chọn phù hợp.

Từ khoá: phân cụm, K-Means, độ đo tương tự, học phần tự chọn.

1. GIỚI THIỆU

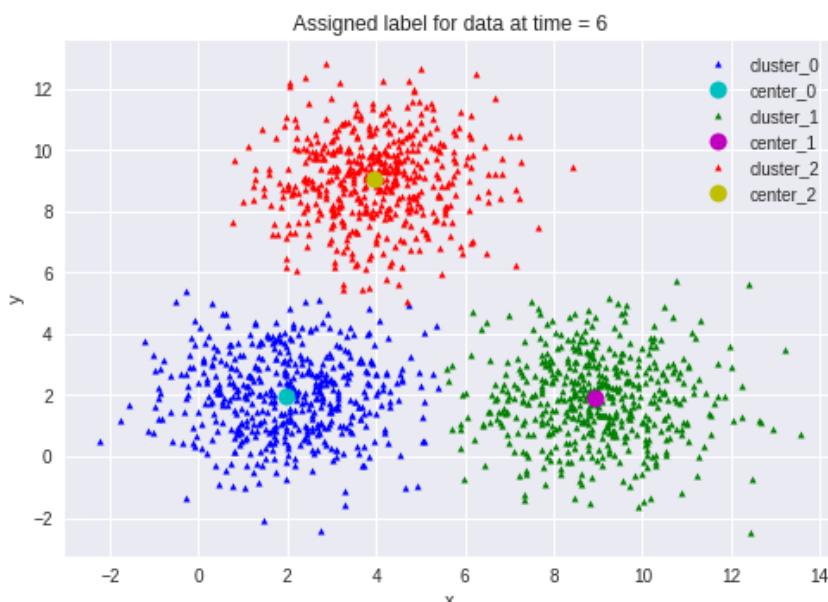
Đóng góp của bài báo bao gồm: (1) cải tiến thuật toán K-Means trên cơ sở ngưỡng θ để không cần phải xác định trước số tâm cụm; (2) xây dựng qui tắc tạo cụm mới dựa trên ngưỡng θ nhằm phù hợp với bộ dữ liệu tăng trưởng; (3) đề xuất các thuật toán cho mô hình tìm kiếm cụm tương tự theo kết quả học tập hiện tại của sinh viên cần tư vấn dựa trên thuật toán K-Means cải tiến; (4) xây dựng mô hình thực nghiệm và thực thi trên một bộ dữ liệu phổ dụng nhằm minh chứng tính đúng đắn của lý thuyết đề xuất.

Phần tiếp theo của bài báo này như sau: Phần 2, trình bày về tổng quan về phân cụm, thuật toán K-Means, đề xuất một cải tiến thuật toán K-Means; Phần 3: mô hình tư vấn học phần tự chọn cho sinh viên; Phần 4, mô tả thực nghiệm; Kết luận và hướng phát triển được trình bày ở Phần 5.

2. PHÂN CỤM

2.1. Giới thiệu

Phân cụm dữ liệu (clustering) là một trong những vấn đề cơ bản của lĩnh vực học máy và khai phá dữ liệu. Bài toán phân cụm nhằm gom nhóm các đối tượng dữ liệu vào thành từng cụm (cluster) sao cho các đối tượng trong cùng một cụm có sự tương đồng theo một tiêu chí nào đó. Công việc phân cụm được xác lập dựa trên nguyên lý: Các điểm dữ liệu trong cùng một cụm thì phải có cùng một số tính chất nhất định. Tức là giữa các điểm trong cùng một cụm phải có sự liên quan lẫn nhau. Đối với máy tính thì các điểm trong một cụm đó sẽ là các điểm dữ liệu gần nhau.[1]



Hình 1. Kết quả phân cụm của thuật toán K-MEANS

Việc phân cụm đã được sử dụng rộng rãi trong các ứng dụng của nhiều lĩnh vực, bao gồm nhận dạng mẫu, phân tích dữ liệu, xử lý ảnh và phân tích thị trường,... Các phương pháp phân cụm điển hình gồm: Phân cụm phân hoạch, phân cụm phân cấp, phân cụm dựa trên mật độ, phân cụm dựa trên lướt, phân cụm dựa trên mô hình, phân cụm có ràng buộc. Thuật toán K-means là một trong những thuật toán đơn giản của phân cụm nhưng có hiệu quả cao và được ứng dụng rộng rãi.

2.2. Thuật toán K – Means

Về nguyên lý, có n đối tượng, mỗi đối tượng có m thuộc tính, phân chia được các đối tượng thành k nhóm dựa trên các thuộc tính của đối tượng bằng việc áp dụng thuật toán này. Xem mỗi thuộc tính của đối tượng (đối tượng có m thuộc tính) như một toạ độ của không gian m chiều và biểu diễn đối tượng như một điểm của không gian m chiều.

$$a_i = (x_{i1}, x_{i2}, \dots, x_{im})$$

$a_i (i = 1..n)$: đối tượng thứ i

$x_{ij} (i = 1..n, j = 1..m)$: thuộc tính thứ j của đối tượng i

Thuật toán

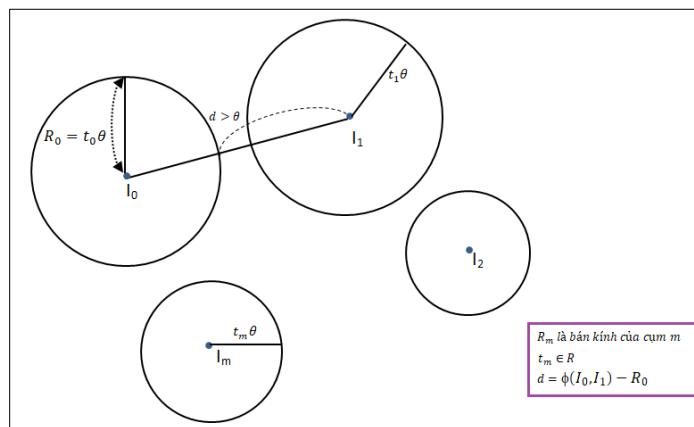
Khởi tạo k phần tử tâm một cách ngẫu nhiên (mỗi phần tử tâm đại diện cho một cụm). Thực hiện các bước cơ bản sau cho đến khi tất cả các đối tượng được phân loại và không còn sự thay đổi của các đối tượng đến các cụm:

- **Bước 1:** Chọn ngẫu nhiên k tâm (*centroid*) cho k cụm (*cluster*). Mỗi cụm được đại diện bằng các tâm của cụm.
- **Bước 2:** Tính khoảng cách giữa các đối tượng (*objects*) đến k tâm (thường dùng *khoảng cách Euclidean*)
 - **Bước 3:** Nhóm các đối tượng vào cụm gần nhất
 - **Bước 4:** Xác định lại tâm mới cho các cụm
 - **Bước 5:** Thực hiện lại bước 2 cho đến khi không có sự thay đổi cụm nào của các đối tượng.

Trong thuật toán K-means, ba tham số cần được khởi tạo ban đầu gồm: số lượng cụm k , tâm cụm và độ đo tương tự; Ngoài ra, nếu bổ sung phần tử mới vào cụm thì phải xác định lại tâm cụm mới. Tuy nhiên, với một bộ dữ liệu bất kỳ cho trước, số lượng các cụm rất khó xác định cũng như việc tăng trưởng dữ liệu có thể làm gia tăng số lượng cụm, điều này gây ra tốn kém nhiều chi phí về thời gian và quá trình thực thi khi tái tạo lại số cụm. [2]

2.3. Cải tiến thuật toán K-Means

Trong bài báo này, chúng tôi đề xuất một cải tiến thuật toán K-Means nhằm phân cụm dữ liệu và tăng trưởng số cụm. Để thực hiện được điều này, chúng tôi sử dụng một giá trị ngưỡng đo độ tương tự giữa các đối tượng dữ liệu, ngưỡng này được ký hiệu là θ . Trên cơ sở ngưỡng θ , thuật toán K-Means được cải tiến bằng cách không xác định trước số tâm cụm, vì vậy số cụm dữ liệu tăng trưởng theo sự tăng trưởng của dữ liệu.



Hình 2. Mô tả kỹ thuật phân cụm

Trong hình 2, phương pháp phân cụm dựa trên K-Means được mô tả, trong đó: I_0, \dots, I_m lần lượt là tâm cụm đầu tiên và tâm cụm thứ m , R_0 là bán kính của cụm đầu tiên, với $R_0 = t_0 * \theta$,

t_0, \dots, t_m là hệ số dãn nở của bán kính, d là khoảng cách từ tâm cụm mới đến đường biên của cụm gần nhất. Trên cơ sở giá trị d , chúng tôi mô tả qui tắc phân cụm như sau:

Bước 1: Tạo cụm C_0 đầu tiên với bán kính là θ và tâm cụm là véc-tơ đầu tiên trong tập véc-tơ dữ liệu, bán kính cụm tương ứng là $R_0=t_0 * \theta$, với $t_0=1$.

Bước 2: Phân bô lần lượt các véc-tơ p_i trong tập dữ liệu đầu theo nguyên tắc sau:

Tính $\phi(p_i, v_k) = \min\{\phi(p_i, v_i)\}, i=1, \dots, m\}$;
 (với m là số lượng cụm, v_i là véc-tơ tâm cụm của cụm C_i)

$d=\phi(p_i, v_k) - C_k.R$.

Nếu ($d < \theta$) thì:

$C_k=C_k \cup \{p_i\}$;

Nếu $\phi(p_i, v_k) > C_k.R$ thì $C_k.R = \phi(p_i, v_k)$

Ngược lại: tạo cụm mới C_t có tâm $\langle p_i \rangle$ và $C_t.R = \theta$

Thuật toán phân cụm

Theo phương pháp đề xuất như trên, thuật toán gom cụm được cải tiến từ K-Means được mô tả như sau:

Thuật toán CTIR

Đầu vào: Nguồn tương tự θ và tập các véc-tơ của cụm ban đầu L

Đầu ra: Tập các cụm Ω

```

Function Clustering_theta( $\theta, L$ )
Begin
    Khởi tạo  $\Omega = \emptyset$ ;
    ForEach  $\langle p_i \rangle \in L$  do
        If  $\Omega = \emptyset$  then
            Khởi tạo cụm đầu tiên  $C_0$  với tâm  $\langle p_0 \rangle$ ;
             $C_0.R = \theta$ ;
        Else
            Tim cụm  $C_k \in \Omega$ :  $\phi(p_i, v_k) = \min\{\phi(p_i, v_i)\}, i=1, \dots, m\}$  ;
            (với  $m$  là số lượng cụm,  $v_i$  là véc-tơ tâm cụm của cụm thứ  $C_i$ )
             $d=\phi(p_i, v_k) - C_k.R$ 
            If ( $d < \theta$ ) then
                 $C_k=C_k \cup \{p_i\}$  ;
                If ( $d > 0$ )
                     $C_k.R = \phi(p_i, v_k)$ ;
                EndIf
            Else
                Tạo mới cụm  $C_t$  có tâm  $\langle p_i \rangle$ ;
                 $C_t.R = \theta$ ;
                 $\Omega = \Omega \cup C_t$ ;
            EndIf;
        EndIf;
    EndFor;
    Return  $\Omega$ ;
End.

```

2.4. Thuật toán tìm cụm thích hợp

Từ tập các cụm Ω đã được phân hoạch theo thuật toán **CTIR**, tiến hành chọn ra cụm C_m có tâm gần nhất với vector p . Tuy nhiên, chúng tôi chọn thêm các cụm láng giềng của C_m dựa trên độ đo giữa các tâm cụm để tăng số lượng kết quả tra cứu. Khi đó các bước thuật toán tìm kiếm như sau:

- **Bước 1:** Tìm cụm C_m có tâm gần với véc-tơ p .
- **Bước 2:** Tìm h cụm láng giềng với cụm C_m . Tập Ψ chứa h cụm láng giềng và cụm C_m .
- **Bước 3:** Tìm tập \mathcal{L} chứa tất cả các véc-tơ trong Ψ .

Thuật toán SEIR:

Đầu vào: véc-tơ đặc trưng p , tập cụm Ω và ngưỡng tìm kiếm σ .

Đầu ra: tập \mathcal{L} chứa danh sách các vector có độ đo gần với p

Function ClusterRetrieval_(p , Ω , σ)

Begin

Khởi tạo $\Psi = \emptyset$;

Tìm cụm $C_k \in \Omega : \phi(p, v_k) = \min \{ \phi(p, v_i), i=1, \dots, m \}$;

(với m là số lượng cụm, v_i là véc-tơ tâm của cụm C_i)

//Tim h cụm láng giềng với C_k

Sắp xếp Ω tăng dần theo $\phi(v_t, v_k) - (C_t.R + C_k.R)$

(với C_t, v_t là cụm và tâm của cụm thứ $t, t=1, \dots, m$)

Khởi tạo $\mathcal{L} = \emptyset$;

If $(\phi(v_i, v_k) - (C_i.R + C_k.R)) < \sigma$ then

$\mathcal{L} = \mathcal{L} \cup C_i$ với $i=0, \dots, m-1$.

EndIf

Return \mathcal{L} ;

End.

3. MÔ HÌNH TƯ VẤN HỌC PHẦN TỰ CHỌN CHO SINH VIÊN

3.1. Mô tả bài toán truy vấn học phần tự chọn

Trong bài báo này, chúng tôi tiến hành thực nghiệm trên bộ dữ liệu của sinh viên các khoá đã tốt nghiệp từ năm 2017 đến 2020 chuyên ngành Công nghệ Thông tin của Khoa Công nghệ Thông tin tại Trường Đại học Công nghiệp Thực phẩm Tp.HCM [3]. Gọi $f = (v_1, \dots, v_t)$ là một véc-tơ đặc trưng điểm số của mỗi sinh viên. Trong đó, t là tổng số học phần bao gồm tất cả học phần bắt buộc và học phần tự chọn, m là số lượng các học phần bắt buộc, v_i là điểm của học phần thứ i trong CTĐT. Các học phần bắt buộc sẽ được xếp từ cột 1 đến cột m , các học phần tự chọn được xếp từ thứ tự $m+1$ đến t .

Bảng 1. Mô tả dữ liệu điểm của sinh viên đã tốt nghiệp

STT	Mã số sinh viên	HP1	HP2	HP3	--	HP m	HP m+1	...	HPt
1	2029000000	8	10	8	--	6	-1		4
2	2029000001	5	7	8	--	5	9		6
---	---	---	---	---	--	---	8		-1
n	2029000002	7	4	5	--	5	4		4

Bảng 1 mô tả dữ liệu điểm của sinh viên đã tốt nghiệp tương ứng với các học phần trong CTĐT. Các điểm số nằm trong đoạn [4-10]. Đối với các học phần tự chọn không học (sinh viên không lựa chọn học phần tự chọn này) sẽ có giá trị -1.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2001181001	8.80	9.30	8.30	6.50	7.70	7.40	5.80	5.0	4.0	6.80	6.50	7.70	6.30	6.80	6.80	6.0	5.90
2001181008	5.00	4.0	4.00	5.0	5.0	8.10	4.60	5.90	5.80	6.40	5.0	6.0	5.80	5.60	5.70	6.80	5.20
2001181003	7.90	8.10	6.80	5.90	6.00	8.90	5.30	5.20	4.60	5.30	5.90	5.0	5.00	5.10	6.40	5.60	6.00
2001180314	7.0	3.60	6.40	5.20	7.0	6.70	6.0	6.00	5.30	7.00	5.20	5.90	5.80	6.90	6.60	5.10	6.80
2001180416	5.60	5.60	5.30	6.00	4.80	8.70	6.80	6.80	6.0	7.80	6.00	5.20	6.00	7.50	6.50	6.90	5.70
2001181007	8.80	8.40	7.00	6.80	7.00	8.40	5.60	5.70	6.80	8.30	6.80	6.00	7.80	7.0	6.50	7.50	6.40
2001180396	6.50	8.70	7.80	5.70	6.20	6.40	5.10	6.40	5.60	7.40	5.70	6.80	3.90	5.10	5.30	7.0	6.60
2001180096	6.40	8.10	8.30	6.40	4.70	8.20	6.90	6.60	5.10	5.00	6.40	5.70	5.80	7.00	4.60	5.10	6.50
2001181016	8.90	7.30	7.40	6.60	5.00	7.00	7.50	6.50	6.90	9.50	6.60	6.40	7.20	6.60	7.00	7.00	6.50
2001181018	5.50	5.00	5.00	6.50	4.30	5.70	7.00	6.50	7.50	10.00	6.50	6.80	6.60	6.00	10.00	6.60	5.30
2001180490	7.80	8.20	9.50	6.50	8.00	9.80	5.10	5.30	7.00	6.00	6.50	6.50	6.70	7.00	6.00	6.60	4.60
2001181020	7.00	8.90	10.00	5.30	6.10	9.40	7.00	4.60	5.10	9.30	5.30	6.50	5.80	6.90	9.30	6.60	7.00
2001180139	7.90	5.60	6.00	4.60	8.00	8.10	6.60	7.00	7.00	4.00	4.60	5.30	5.00	7.40	6.60	6.00	10.00
2001181022	8.10	9.70	9.30	7.00	8.00	9.50	6.00	10.00	6.60	6.60	7.00	4.60	5.80	5.00	6.50	4.30	6.00
2001180108	9.00	7.00	4.00	8.00	7.00	5.00	7.00	6.00	6.60	6.00	8.00	7.00	6.00	9.50	6.50	8.00	9.30
2001180224	8.00	4.70	8.00	5.90	4.70	7.50	6.90	9.30	6.60	7.00	6.00	10.00	7.80	10.00	5.30	6.10	6.50
2001180483	7.10	7.70	6.30	5.40	4.30	8.40	6.10	4.00	6.30	5.00	6.30	6.00	3.90	6.00	4.60	8.00	4.00
2001181034	7.20	6.80	5.30	5.60	5.90	7.30	6.90	5.30	5.30	5.30	8.00	9.30	5.80	9.30	7.00	8.00	4.00
2001180477	7.30	3.70	7.50	5.40	5.50	8.40	5.70	7.50	6.70	7.50	7.50	6.00	7.20	4.00	8.00	7.00	7.90
2001181036	7.00	7.60	5.60	5.90	8.40	9.00	5.60	5.60	5.50	5.60	5.50	5.00	6.60	6.00	7.00	7.20	6.00

Hình 3. Mô tả bảng dữ liệu điểm sinh viên đã tốt nghiệp

Trong bài toán tư vấn học phần tự chọn, chúng tôi sẽ thực hiện tìm kiếm danh sách học phần thích hợp thông qua hai bước: (1) Tìm kiếm một cụm C gần nhất với véc-tơ đặc trưng điểm của sinh viên cần tư vấn; (2) Từ cụm C kết hợp với danh sách các học phần tự chọn và số lượng học phần cần đăng ký, một danh sách các học phần tự chọn phù hợp với sinh viên được xây dựng được sắp xếp giảm dần theo điểm trung bình để thuận lợi cho sinh viên lựa chọn học phần thích hợp. Từ đó giúp sinh viên định hướng chọn lựa phù hợp với năng lực.

3.2. Mô hình tư vấn học phần tự chọn

Mô hình tư vấn học phần tự chọn được đề xuất trong Hình 3.2 gồm hai giai đoạn: tiền xử lý để tạo dữ liệu cụm và tìm kiếm danh sách học phần tự chọn thích hợp với trình độ của sinh viên cần tư vấn.

a. Tiền xử lý

Bước 1: tạo véc-tơ đặc trưng điểm $f = (v_1, \dots, v_t)$ của mỗi sinh viên đã tốt nghiệp trong tập dữ liệu điểm.

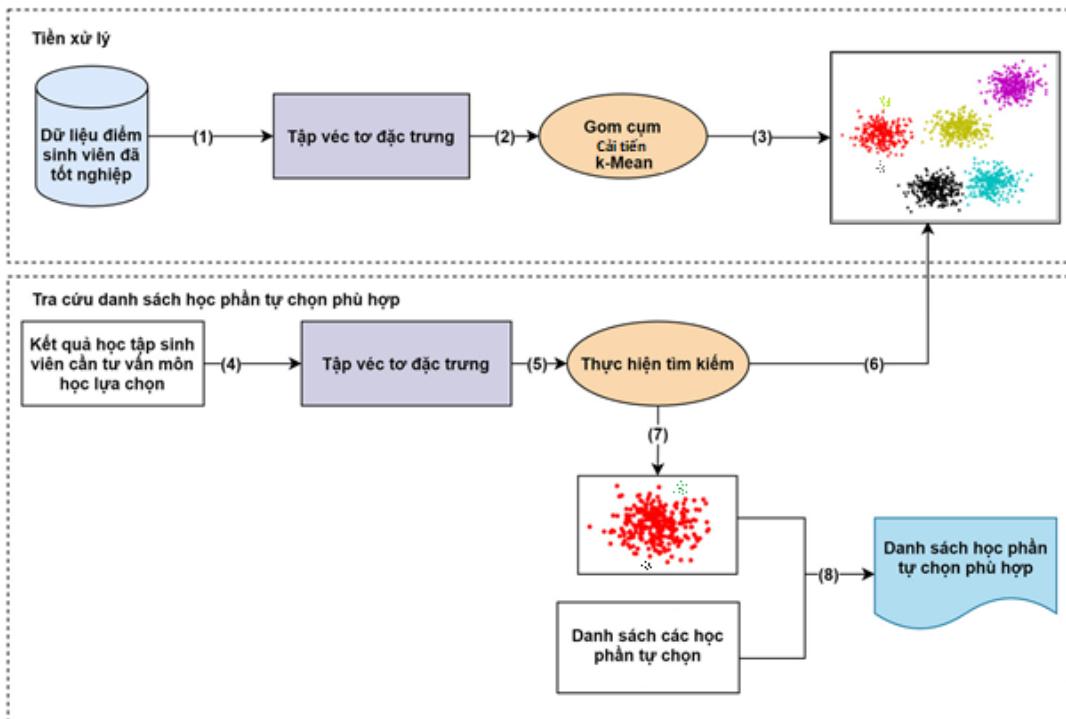
Bước 2: gom cụm các véc-tơ đặc trưng theo độ đo tương tự dựa trên thuật toán CTIR.

b. Tìm kiếm danh sách học phần tự chọn thích hợp

Bước 1: tạo véc-tơ đặc trưng từ kết quả điểm của một sinh viên cần tư vấn.

Bước 2: áp dụng thuật toán **CTIR**, **SEIR** tìm tập \mathcal{E} chứa các vector có độ đo gần với véc-tơ điểm của sinh viên cần tư vấn.

Bước 3: xây dựng danh sách các học phần tự chọn từ \mathcal{E} , danh sách được xếp theo thứ tự điểm trung bình giảm dần để dễ dàng cho sinh viên lựa chọn.



Hình 4. Mô hình của hệ thống tư vấn lựa chọn học phần tự chọn

4. THỰC NGHIỆM

Chúng tôi xây dựng một hệ truy vấn thông tin chương trình đào tạo cho sinh viên HUFI ngành Công nghệ thông tin. Dữ liệu thực nghiệm được thực hiện cho ngành Công nghệ thông tin. Ngành Công nghệ Thông tin bao gồm ba chuyên ngành: Công nghệ phần mềm, Khoa học máy tính, Mạng máy tính. Tổng số học phần của CTĐT là 111. Trong đó có 24 học phần đại cương, 21 học phần cơ sở ngành, 66 học phần chuyên ngành. Mỗi học phần có thể thuộc nhiều chuyên ngành khác nhau. [4]

TƯ VẤN ĐĂNG KÝ HỌC PHẦN

MSSV: 1020121, Họ tên: An Thành Minh, Khoa: CNTT, Chuyên ngành: CONGNGHEPHANMEM, Học kỳ: 4
Số kỳ muốn vượt:

DANH SÁCH HỌC PHẦN BẮT BUỘC			
mahocphan	tenhp	sotinchiLT	sotinchiTH
16200016	Giáo dục quốc p...	2	0
11200003	Chủ nghĩa xã hội...	2	0
14200008	Anh văn A3	3	0
11200002	Kinh tế chính tr...	2	0
11200005	Lịch sử Đảng Cộ...	2	0
16201013	Giáo dục thể chất...	2	0
16202017	Giản dịc: ngôn n...	1	0

DANH SÁCH HỌC PHẦN TIỀN QUYẾT MÀ CHUA THI			
mahocphan	tenhp	sotinchiLT	sotinchiTH
1200052	Tri tué nhân tạo	3	0
1202054	Công nghệ .NET	1	2

Lưu ý: 1200052 (Tri tué nhân tạo) cần qua HP đang học: 1200036 (Cấu trúc dữ liệu và Giải thuật); 1201037 (Thực hành Cấu trúc dữ liệu và Giải thuật); 1202054 (Công nghệ .NET) cần qua HP đang học: 1200039 (Cấu trúc rời rạc);

DANH SÁCH HỌC PHẦN TỰ CHỌN			
mahocphan	tenhp	sotinchiLT	sotinchiTH
15200023	Phương pháp ng...	2	0
13200024	Kỹ năng giao tiếp	2	0
15200021	Logic học	2	0
1200058	Hệ quản trị CSDL...	2	0

Thống kê

- 15200023 (Phương pháp nghiên cứu khoa học-HK 3) có tỷ lệ dk: 83.3%, ĐTB:6.2
- 1200061 (Xử lý ảnh-HK 6) có tỷ lệ dk: 100%, ĐTB:6.5
- 13200024 (Kỹ năng giao tiếp-HK 3) có tỷ lệ dk: 50%, ĐTB:5.7
- 1200058 (Hệ quản trị CSDL Oracle-HK 6) có tỷ lệ dk: 83.3%, ĐTB:5
- 15200021 (Logic học-HK 3) có tỷ lệ dk: 50%, ĐTB:5
- 1200057 (Truyền thông kỹ thuật số-HK 6) có tỷ lệ dk: 83.3%, ĐTB:5.2

QUY ĐỊNH TÍN CHỈ TỰ CHỌN

Học kỳ 3 còn thiếu: 2 tín chỉ tự chọn
Học kỳ 5 quy định: 0 tín chỉ tự chọn
Học kỳ 6 quy định: 5 tín chỉ tự chọn

Hình 5. Giao diện thống kê tỷ lệ lựa chọn học phần tự chọn

DANH SÁCH HỌC PHẦN TỰ CHỌN

mahocphan	tenhp	sotinchiLT	sotinchiTH
15200023	Phương pháp ng...	2	0
13200024	Kỹ năng giao tiếp	2	0
15200021	Logic học	2	0
1200058	Hệ quản trị CSDL...	2	0

Thống kê

- 15200023 (Phương pháp nghiên cứu khoa học-HK 3) có tỷ lệ dk: 83.3%, ĐTB:6.2
- 13200024 (Kỹ năng giao tiếp-HK 3) có tỷ lệ dk: 50%, ĐTB:5.7
- 15200021 (Logic học-HK 3) có tỷ lệ dk: 50%, ĐTB:5.5
- 1200058 (Hệ quản trị CSDL Oracle-HK 6) có tỷ lệ dk: 83.3%, ĐTB:5.5
- 1200065 (Áo hóa và điện toán đám mây-HK 6) có tỷ lệ dk: 33.3%, ĐTB:5

QUY ĐỊNH TÍN CHỈ TỰ CHỌN

Học kỳ 3 còn thiếu: 2 tín chỉ tự chọn
Học kỳ 5 quy định: 0 tín chỉ tự chọn
Học kỳ 6 quy định: 5 tín chỉ tự chọn

Hình 6. Giao diện tư vấn đăng ký học phần, trong đó có phần tư vấn học phần tự chọn

Hình 5, 6 mô tả việc thực hiện gom cụm dữ liệu kết quả của sinh viên đã tốt nghiệp dựa trên thuật toán cài tiến K-MEANS. Kết quả thu được là cụm dữ liệu tương đồng về điểm số của sinh viên cần tư vấn. Từ đó chúng tôi thống kê tỷ lệ/ điểm trung bình của các học phần tự chọn của nhóm sinh viên tốt nghiệp mà có học lực tương đồng với sinh viên. Ứng với danh sách các học phần tự chọn đã được sắp xếp theo mức độ ưu tiên từ trên xuống, sinh viên có thể xem thống kê của từng học phần và từ đó có lựa chọn phù hợp.

5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Bài báo đã đề xuất một cài tiến thuật toán K-Means thực hiện gom cụm nhằm giúp tìm kiếm cụm có kết quả điểm phù hợp với trình độ sinh viên cần tư vấn. Trên cơ sở lý thuyết đã được đề xuất, nhóm tác giả xây dựng hệ thống tư vấn lựa chọn học phần tự chọn cho sinh viên. Kết quả thực nghiệm trên bộ dữ của sinh viên các khoá đã tốt nghiệp từ năm 2017 đến 2020

chuyên ngành Công nghệ Thông tin của Khoa Công nghệ Thông tin tại Trường Đại học Công nghiệp Thực phẩm Tp.HCM đã cho thấy phương pháp đề xuất là hiệu quả. Trên cơ sở ngưỡng θ , thuật toán K-Means được cải tiến bằng cách không xác định trước số tâm cụm, vì vậy số cụm dữ liệu tăng trưởng theo sự gia tăng của số lượng kết quả điểm đã giảm được đáng kể thời gian của quá trình gom cụm so với thuật toán K-Means. Tuy nhiên, việc này dẫn đến thể xuất hiện các cụm có quá nhiều phần tử, ảnh hưởng đến độ chính xác của hệ thống. Hướng phát triển tiếp theo của nghiên cứu là xây dựng thuật tách cụm lớn thành 2 cụm nhỏ nhằm đảm bảo các phần tử trong cùng một cụm phải tương tự nhau.

TÀI LIỆU THAM KHẢO

1. <https://viblo.asia/p/hierarchical-clustering-phan-cum-du-lieu-maGK7q2elj2>
2. https://enews.agu.edu.vn/index.php?option=com_content&view=article&id=18545:ba-i-toa-n-pha-n-ca-m-da-lia-u-va-a-ng-da-ng&catid=25:clb-tin-hoc&Itemid=128
3. Dữ liệu kết quả học tập của sinh viên khóa 08DHTH -09DHTH, Khoa Công nghệ Thông tin, Trường Đại học Công nghiệp Thực phẩm TP.HCM, do Phòng Đào tạo cung cấp
4. Trường Đại học Công nghiệp Thực phẩm TP. Hồ Chí Minh, Quy chế Đào tạo Đại học theo hệ thống tín chỉ năm 2019.

ABSTRACT

A DATA CLUSTERING METHODOLOGY FOR ELECTRONIC COURSE CONSULTING PROBLEM

Nguyen Thi Thuy Trang^{1*}, Phan Thi Ngoc Mai¹

¹ Ho Chi Minh University of Food Industry, Vietnam

*Email: trangntthuy@hufi.edu.vn

In this article, an improved K-Means algorithm is proposed to cluster the data and apply it to the elective course selection advisory problem. To do this, we use a threshold value that measures the similarity between data objects, this threshold is denoted θ . On the basis of threshold θ , the K-Means algorithm is improved by not pre-determining the number of cluster centers, the number of data clusters grows with the increase of graduates. The learning outcome of each graduate is presented as a vector with n dimensions and is the input data for the improved K-Means algorithm to search for clusters of students with high learning results. Exercises similar to the level of students need advice on choosing electives. We experiment on the data of learning results of students who have graduated from the 08th CIT course, 09 the CITU. According to the experimental results, our suggestions are feasible and can be applied in practice to support students of the Faculty of Information Technology, University of Ho Chi Minh University of Food Industry to choose a course suitable choice.

Keywords: C.lustering, K-Means, similarity measure, elective course

ỨNG DỤNG THUẬT GIẢI TỐI UƯ BÀY ĐÀN ẨN TẬP HỮU ÍCH CAO NHẠY CẢM

Lâm Thị Họa Mi^{1,*}, Vũ Văn Vinh¹, Dương Thị Mộng Thùy¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: milth@husi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Khai thác tập hữu ích cao (HUIM) nhằm phát hiện ra các tập mục có độ hữu ích lớn hơn một ngưỡng tối thiểu cho trước. Đây là bài toán đã thu hút được sự quan tâm của rất nhiều nhà khoa học, nhiều thuật toán khai thác HUI hiệu quả đã được đề xuất. Tuy nhiên trong quá trình khai thác, nhiều thông tin nhạy cảm cũng được phát hiện. Và từ đó, một số phương pháp với mục đích chỉnh sửa lại cơ sở dữ liệu để có thể ẩn đi các thông tin nhạy cảm này đã được nghiên cứu. Phần lớn các thuật toán tập trung vào việc ẩn đi các thông tin nhạy cảm bằng phương pháp tối ưu cục bộ như thuật toán ẩn tập hữu ích cao trước (HHUIF), HHUIF cải tiến, thuật toán ẩn các tập nhạy cảm tối đa dung độ trước (MSCIF), ... mà không quan tâm nhiều tới việc biến đổi của toàn bộ cơ sở dữ liệu. Gần đây một số thuật toán ẩn thông tin nhạy cảm dựa trên thuật giải di truyền (GA) cũng được đề xuất trên cơ sở thêm và xóa các giao dịch trong dữ liệu ban đầu. Việc thêm và xóa các giao dịch làm cho cơ sở dữ liệu trở nên mờ hoặc tăng thêm các giao dịch ảo. Trong nghiên cứu này, chúng tôi đề xuất phương pháp chỉnh sửa lại số lượng của các hạng mục trong cơ sở dữ liệu ban đầu để ẩn đi các tập nhạy cảm có độ hữu ích cao. Thuật toán được đề xuất dựa trên kỹ thuật tối ưu toàn cục cụ thể là thuật giải tối ưu bầy đàn (PSO). Kết quả thu được cho thấy thuật toán đề xuất đã ẩn được các thông tin nhạy cảm và tối ưu hóa độ lệch của cơ sở dữ liệu sau khi chỉnh sửa so với cơ sở dữ liệu ban đầu.

Từ khóa: Bảo vệ tính riêng tư, ẩn tập hữu ích cao, tập hữu ích cao nhạy cảm, thuật toán tối ưu bầy đàn.

1. MỞ ĐẦU

Khai thác tập phỏ biến [1] nhằm tìm ra các tập mục có tần số xuất hiện lớn hơn hay bằng một giá trị, được gọi là ngưỡng độ phỏ biến tối thiểu (minsup). Hạn chế của phương pháp này là đã bỏ qua tầm quan trọng về lợi ích của các tập mục. Tập phỏ biến chỉ phản ánh mối tương quan về mặt thống kê nhưng không phản ánh được tầm quan trọng về mặt ngữ nghĩa giữa các hạng mục. Chính vì vậy, bài toán khai thác tập hữu ích cao được đề nghị [2]. Khai thác tập hữu ích cao là tìm ra các tập mục có giá trị hữu ích (chẳng hạn như doanh thu) lớn hơn hay bằng một ngưỡng tối thiểu cho trước.

Việc khai thác các tập hữu ích cao (HUI) giúp cho nhà quản trị nắm bắt được doanh thu đem lại khi khách hàng mua các món hàng cùng nhau. Điều đó rất hữu ích cho các nhà kinh doanh nhưng lại rất nguy hiểm khi dữ liệu này bị lộ ra ngoài. Vì vậy, cần phải bảo vệ tính riêng tư trên các cơ sở dữ liệu (CSDL). Bảo vệ tính riêng tư trên CSDL nhằm hạn chế việc lộ các thông tin tiềm ẩn của người dùng. Vân đề bảo vệ tính riêng tư trong khai thác tập phỏ biến đã

được đề cập nhiều trong các công trình nghiên cứu của nhiều tác giả [3]–[11]. Tuy nhiên, các công trình về bảo vệ tính riêng tư liên quan đến khai thác tập hữu ích cao lại rất hạn chế.

Kỹ thuật khai thác dữ liệu ngày càng phát triển, con người ngày càng nắm bắt nhiều thông tin hơn. Với sự phát triển kinh doanh như hiện nay, doanh nghiệp không thể chỉ khăng khăng giữ lấy thông tin của riêng mình. Việc trao đổi thông tin giữa các doanh nghiệp là điều cần thiết. Với các dữ liệu trao đổi, thu thập được, doanh nghiệp có thể rút trích được các thông tin quan trọng cho yêu cầu kinh doanh của mình. Tuy nhiên, khi những thông tin chung liên quan nhiều hơn đến sự riêng tư, ngày càng nhiều người không sẵn lòng cung cấp dữ liệu thật cá nhân thật khi được yêu cầu. Bên cạnh đó, các công ty muốn có thể sử dụng dữ liệu khách hàng cho việc khai thác dữ liệu không dễ dàng vì điều này làm tổn hại tính riêng tư của khách hàng. Vì vậy, làm thế nào có thể đảm bảo được tính riêng tư của dữ liệu khi đưa dữ liệu ra bên ngoài đã thu hút đáng kể sự chú ý trong những năm qua. Ví dụ: Công ty A tìm hiểu và thấy rằng khách hàng mua sản phẩm sữa bột của công ty B thường sẽ mua kèm tã giấy của công ty C, từ đó công ty A sẽ xây dựng kế hoạch hợp tác với công ty B nhằm cạnh tranh với công ty C. Đây chính là những thông tin nhạy cảm mà các công ty không muốn để lộ ra bên ngoài.

Nghiên cứu này tập trung đến vấn đề bảo toàn tính riêng tư trong khai thác tập hữu ích cao. Cụ thể là ẩn các thông tin nhạy cảm trên dữ liệu để người dùng không khai thác được các tập hữu ích cao mà việc thay đổi CSDL ban đầu là nhỏ nhất.

2. CÁC CÔNG TRÌNH LIÊN QUAN

2.1. Khai thác tập hữu ích cao

Vào năm 1993, Agrawal và cộng sự đề xuất phương pháp khai thác luật kết hợp [1]. Các tác giả chia bài toán làm hai giai đoạn: i) Khai thác các tập mục có độ hỗ trợ lớn hơn hoặc bằng ngưỡng độ hỗ trợ tối thiểu cho trước (tập phổ biến). Năm 1994, các tác giả trong [12] đưa ra tính chất Apriori (mỗi tập con của một tập phổ biến phải phổ biến) và thuật toán Apriori để tia các ứng viên. Về sau, một số thuật toán khai thác nhanh tập phổ biến dựa trên tính chất Apriori được phát triển như Eclat [13], FP-Growth [14]; ii) Sinh luật kết hợp từ các tập phổ biến.

Khác với khai thác tập phổ biến, khai thác HUI từ CSDL quan tâm đến lợi ích mang lại (doanh thu) hay còn gọi là độ hữu ích của các tập mục. Do độ hữu ích của các tập mục không thỏa tính chất Apriori nên không thể áp dụng trực tiếp các thuật toán khai thác tập phổ biến vào khai thác tập HUI. Vì vậy, các nghiên cứu về HUIM chủ yếu tập trung vào việc làm thế nào để tia các ứng viên không liên quan càng nhiều càng tốt. Bài toán khai thác tập hữu ích cao đã nhận được sự quan tâm lớn từ cộng đồng nghiên cứu khoa học và một loạt các thuật toán hiệu quả đã được đề xuất vào cuối thập kỷ. Năm 2005, Liu và cộng sự [15] kế thừa thuật toán Apriori và đề xuất thuật toán Two-Phase để khai thác HUI trong CSDL giao dịch. Phương pháp Two-Phase áp dụng phương pháp tìm kiếm theo chiều rộng và chiến lược tia để xác định các ứng viên là HUI hay không? Năm 2012, Tseng và cộng sự [16] đã giới thiệu thuật toán UP-Growth và UP-Growth+ bằng cách sử dụng cấu trúc cây để giảm số lần duyệt CSDL. Trong những năm gần đây, Liu và đồng sự [17] đề xuất thuật toán duyệt theo chiều sâu để tìm các tập HUI chỉ với hai lần duyệt CSDL. Các tác giả đã giới thiệu cấu trúc mang tính đột phá tên là Utility List và cận trên chất chẽ hơn giúp loại bỏ giới hạn của phương pháp Two-Phase.

Thuật toán HMiner được đề xuất năm 2017 [18], tác giả Srikumar đã đề xuất cấu trúc CUL (Compact Utility List) để lưu trữ thông tin liên quan tới một tập mục, giới thiệu khái niệm đóng (Closed) và không đóng (Non-Closed) của một giao dịch đối với tập mục X đồng thời sử dụng tốt các chiến lược tia C-Prune, U-Prune, LA-Prune và EUCS-Prune giúp cho việc tìm HUI rút ngắn được cả thời gian thực thi và không gian lưu trữ. Bởi vì những yêu cầu khác nhau của người dùng và các ứng dụng trong cuộc sống, nhiều phiên bản khác nhau đã được đề xuất để mở rộng khái niệm khai thác tập HUI như khai thác K tập hữu ích cao nhất (top-K HUI) [19]–[23] và tập hữu ích cao đóng HUI (Closed-HUI) [24]–[26].

2.2. Ân tập hữu ích nhạy cảm

Evfimievski và các đồng sự [4] đưa ra một ví dụ rất sinh động về vấn đề bảo toàn tính riêng tư. Giả sử, máy chủ có nhiều máy khách và mỗi máy khách có dữ liệu riêng. Các máy khách mong chờ máy chủ thu thập thông tin thống kê từ toàn bộ dữ liệu máy khách về mối kết hợp giữa các mục để cung cấp những đề nghị cho khách hàng của họ. Tuy nhiên, các máy khách không thích máy chủ lấy các tập mục chứa các tri thức nhạy cảm cao. Vì vậy, khi một máy khách giao CSDL cho máy chủ, một số tập nhạy cảm bị ẩn từ CSDL theo các chính sách bảo mật riêng tư. Máy chủ chỉ tập hợp thông tin thống kê từ CSDL có chỉnh sửa. Chính vì vậy, bài toán khai thác dữ liệu bảo vệ tính riêng tư thu hút được nhiều sự chú ý của các nhà nghiên cứu. Một số nghiên cứu điển hình như: Ân các luật kết hợp dựa trên độ phổ biến và độ tin cậy [3]; Lin và Cheng đã thêm nhiều vào các giao dịch (thêm các mục vào các giao dịch) để tạo ra dữ liệu giả [5]; Các thuật toán sử dụng cấu trúc cây để tăng tốc độ ẩn các tập nhạy cảm có độ hữu ích cao do Yun và Kim đề xuất [8].

Yeh và Hsu trình bày hai thuật toán có tên là HHUIF (Hiding High Utility Item First) và MSICF (Maximum Sensitive Itemsets Conflict First), với mục tiêu ẩn các tập nhạy cảm trong CSDL. Thủ tục chuyển đổi CSDL gốc thành CSDL sửa đổi được gọi là qui trình sửa đổi. Qui trình sửa đổi hoạt động trên dữ liệu để loại bỏ số lượng nhỏ các mục trong một số giao dịch chứa các tập nhạy cảm. Gần đây một số thuật toán về PPUM cũng được đề xuất dựa trên việc thêm và xóa các giao dịch liên quan tới tập nhạy cảm có độ hữu ích cao bằng cách áp dụng thuật giải di truyền (GA- Genetic Algorithm) [7], [9].

3. CƠ SỞ LÝ THUYẾT

3.1. Khái niệm và định nghĩa

Gọi $I = \{i_1, i_2, i_3, \dots, i_m\}$ là tập các mục trong CSDL giao dịch. Một giao dịch $T_j = \{x_l \mid l = 1, 2, \dots, N_j, x_l \in I\}$ với N_j là số lượng mục trong giao dịch T_j . CSDL D là tập hợp các giao dịch $D = \{T_1, T_2, \dots, T_n\}$, trong đó n là số lượng giao dịch trong D . Ví dụ: D là CSDL được cho trong Bảng 1 có $I = \{a, b, c, d, e\}$ với $n = 12$.

Lợi ích của một mục $x_i \in I$, ký hiệu là $EU(x_i)$. Trong CSDL D được cho trong Bảng 1, ta có $EU(a) = 6$ và $EU(b) = 2$.

Số lượng của một mục $x_i \in T_j$, ký hiệu là $IU(x_i, T_j)$. Ví dụ: $IU(a, T_1) = 6$ và $IU(b, T_3) = 6$.

Bảng 1. Cơ sở dữ liệu D

Mục Tid	a	b	c	d	e
Tid	6	0	0	0	0
Tid	0	1	0	5	0
Tid	0	6	0	0	0
Tid	0	0	5	0	0
Tid	0	0	0	0	8
Tid	2	0	2	0	3

Mục Tid	a	b	c	d	e
Tid	0	1	0	4	0
Tid	0	4	0	0	0
Tid	0	2	3	7	0
Tid	0	0	0	0	1
Tid	0	5	2	5	0
Tid	0	3	0	3	0

Bảng 2. Lợi ích của các mục trong cơ sở dữ liệu

Mục	a	b	c	d	e
Lợi nhuận	6	2	15	7	10

Định nghĩa 1. Độ hữu ích của mục $x_i \in T_j$, ký hiệu là $U(x_i, T_j)$, được xác định là tích của số lượng mục x_i trong T_j với lợi ích của nó: $U(x_i, T_j) = EU(x_i) * IU(x_i, T_j)$.

Ví dụ: $U(a, T_1) = 6 * 6 = 36$, $U(b, T_3) = 2 * 6 = 12$.

Định nghĩa 2. Độ hữu ích của một tập mục X trong giao dịch T_j ($X \subseteq T_j$), ký hiệu là $U(X, T_j)$ và xác định như sau: $U(X, T_j) = \sum_{x_i \in X} U(x_i, T_j)$.

Ví dụ: $U(bc, T_9) = 2 * 2 + 15 * 3 = 49$, $U(bc, T_{11}) = 2 * 5 + 15 * 2 = 40$.

Định nghĩa 3. Độ hữu ích của một tập mục X trong CSDL D được kí hiệu là $U(X)$ và định nghĩa như sau: $U(X) = \sum_{x_i \in X} U(x_i, T_j)$.

Ví dụ: $U(a) = U(a, T_1) + U(a, T_6) = 36 + 12 = 48$,

$U(bc) = U(bc, T_9) + U(bc, T_{11}) = 49 + 40 = 89$.

Định nghĩa 4. Tập mục X được gọi là tập hữu ích cao (HUI) nếu $U(X) \geq minutil$ ($minutil$ là ngưỡng độ hữu ích tối thiểu do người dùng xác định). Giả sử $minutil = 168$, $\{bd\}$ là tập hữu ích cao vì $U(bd) = 192 \geq minutil$ và $\{bc\}$ không phải là tập mục có độ hữu ích cao vì $U(bc) = 89 \leq minutil$.

Định nghĩa 5. Khai thác tập hữu ích cao là khám phá tập hợp chứa toàn bộ các tập mục X thỏa ngưỡng $minutil$ cho trước, nghĩa là: $HUI = \{X \subseteq I | U(X) \geq minutil\}$

Ví dụ: Với $minutil = 168$, các tập hữu ích cao của D được liệt kê trong Bảng .

Bảng 3. HUI và lợi nhuận của các HUI

HUI	bcd	bd	c	d
Độ hữu ích	173	192	180	168

Định nghĩa 6. Một tập hữu ích cao X được gọi là là tập nhạy cảm nếu sự xuất hiện của X trong HUIs có thể dẫn đến tiết lộ một số thông tin bí mật.

Loại tập mục này nên được loại bỏ khỏi tập HUI để người quản lý có thể chia sẻ và công khai dữ liệu đến với người dùng.

Định nghĩa 7. Gọi $SHUI = \{S_1, S_2, S_3, \dots, S_l\}$ là tập con của HUI , với S_i là một tập nhạy cảm cần phải ẩn để bảo toàn tính riêng tư.

Định nghĩa 8. Số lượng đụng độ của mục i_p trong $SHUI$, ký hiệu $Icount_{i_p}(SHUI)$, là số tập nhạy cảm có chứa i_p . Nghĩa là, $Icount_{i_p}(SHUI) = \{S_i \in SHUI | i_p \in S_i\}$.

3.2. Qui trình ẩn tập hữu ích cao nhạy cảm

Thông thường, qui trình ẩn các tập hữu ích cao nhạy cảm gồm 3 bước:

- (1) Ứng dụng thuật toán khai thác tập hữu ích trên cao CSDL để tìm HUI;
- (2) Xác định các tập nhạy cảm dựa trên các yêu cầu nghiệp vụ;
- (3) Áp dụng thuật toán sửa đổi để sinh CSDL sửa đổi.

Bước 1: Khai thác HUI, đầu tiên người dùng chọn ngưỡng hữu ích tối thiểu $minutil$ và áp dụng một thuật toán khai thác tập mục hữu ích nào đó trên CSDL được cho.

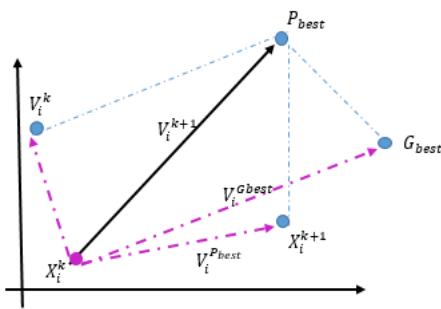
Bước 2: Dựa trên yêu cầu nghiệp vụ, người dùng xác định tập nhạy cảm trong số các tập hữu ích cao. Tập nhạy cảm chứa tất cả các mẫu giới hạn mà người dùng không muốn công khai.

Bước 3: Áp dụng thuật toán sửa đổi trên CSDL đã cho. Mục tiêu chính của thuật toán sửa đổi là giảm giá trị hữu ích của mỗi tập nhạy cảm bằng cách chỉnh sửa số lượng của các mục trong bên trong nó.

3.3. Thuật giải tối ưu bầy đàn (PSO - Particle Swarm Optimization)

Tại hội nghị IEEE năm 1995, Particle Swarm Optimization (PSO) được giới thiệu bởi Kennedy và Eberhart [27], [28]. PSO là một trong những thuật giải xây dựng dựa trên khái niệm trí tuệ bầy đàn để tìm kiếm lời giải cho các bài toán tối ưu hóa trên một không gian tìm kiếm nào đó. PSO là một dạng của thuật giải tiến hóa quần thể như thuật giải di truyền (GA). Nhưng khác với GA, PSO sử dụng sự tương tác giữa các cá thể trong một quần thể để khám phá ra không gian tìm kiếm.

Trong PSO, mỗi giải pháp đơn là một phần tử (particle) trong quần thể. Mỗi phần tử được đặc trưng bởi hai tham số là vị trí hiện tại của phần tử X và vận tốc hiện tại V . Đây là hai vectơ trên trường số R_n (n là tham số được xác định từ bài toán cụ thể). Đồng thời mỗi phần tử có một giá trị thích nghi (fitness value), được đánh giá bằng hàm đo độ thích nghi (fitness function) tương tự như trong GA. Tại thời điểm xuất phát, vị trí của mỗi phần tử được khởi tạo một cách ngẫu nhiên (hoặc theo một cách thức nào đó dựa vào tri thức biết trước về bài toán). Trong quá trình chuyển động, mỗi phần tử chịu ảnh hưởng bởi hai thông tin: thông tin thứ nhất, gọi là P_{best} , là vị trí tốt nhất mà phần tử đó đã đạt được trong quá khứ; thông tin thứ hai, gọi là G_{best} , là vị trí tốt nhất mà cả bầy đàn đã đạt được trong quá khứ.



Hình 1. Sơ đồ di chuyển của cá thể trong PSO

Khi đó, vận tốc và vị trí của cá thể trong quần thể được tính như sau:

$$\begin{aligned} V_i^{k+1} &= \omega * V_i^k + c_1 * r_1 * (P_{best} - X_i^k) + c_2 * r_2 * (G_{best} - X_i^k) \\ X_i^{k+1} &= X_i^k + V_i^{k+1} \end{aligned}$$

Ý nghĩa của các thông tin trong công thức trên là: ω : là hệ số quán tính; c_1, c_2 : các hệ số gia tốc và r_1, r_2 : các số ngẫu nhiên nhận giá trị trong khoảng [0,1].

Giá trị của trọng số quán tính ω sẽ giảm tuyén tính từ 1 đến 0 tuỳ thuộc vào số lần lặp xác định trước. Thêm nữa, giá trị ω lớn cho phép cá thể thực hiện mở rộng phạm vi tìm kiếm, giá trị ω nhỏ làm tăng sự thay đổi để nhận được giá trị tối ưu địa phương. Bởi vậy, khi sử dụng ω có giá trị lớn ($\omega = 0.9$) ở thời điểm bắt đầu và sau đó giảm dần giá trị ω sẽ cho hiệu năng tìm kiếm tốt nhất. Các hệ số gia tốc nhận giá trị từ 1.5 đến 2.5 và $c_1 + c_2 = 4$.

Trong đó, một số điều kiện dừng phổ biến là: số lần cập nhật, số lần cập nhật bảy đòn mà không đưa lại kết quả tốt hơn, số lần cập nhật mà lượng thay đổi giữa hai lần cập nhật liên tiếp nhỏ hơn một ngưỡng nào đó.

4. ẤN TẬP HỮU ÍCH CAO NHẠY CẢM SỬ DỤNG PSO

Thuật toán HHUIF, HHUIF cải tiến và MSICF đã áp dụng các tập nhạy cảm hữu ích cao tuy nhiên các thuật toán này chưa quan tâm tới việc số lượng của một số các mục trong giao dịch bị chỉnh sửa trở thành không. Do đó mục đó không xuất hiện trong giao dịch nữa. Đặc biệt, thuật toán HHUIF và MSICF chọn lựa giảm trên các mục có giá trị lớn nhất trong các giao dịch nên sự thay đổi đó sẽ làm cơ sở dữ liệu có sự đột biến rất lớn tại giao dịch bị chỉnh sửa. Sử dụng thuật toán chèn hoặc xóa các giao dịch trong CSDL ban đầu cũng sẽ tăng độ chênh lệch về tổng độ hữu ích trong CSDL ban đầu và sau khi đã chỉnh sửa.

Để hạn chế những vấn đề đã nêu của các thuật toán đề xuất, nghiên cứu này đề xuất phương pháp giải các tập nhạy cảm có độ hữu ích cao bằng cách sử dụng thuật giải tối ưu bảy đòn (PSO) để có thể đạt tới sự tối ưu toàn cục. Đồng thời, cũng để hạn chế việc thay đổi CSDL ban đầu. Phương pháp này sẽ không thêm hay bớt các giao dịch có sẵn mà chỉ tính toán để chỉnh sửa lại số lượng của các mục trong mỗi giao dịch. Thuật toán cũng hạn chế sửa đổi số lượng của các mục về 0 để tránh thay đổi bản chất của giao dịch đó trong những trường hợp không cần thiết.

Trong đó:

X_i^k : Vị trí cá thể thứ i tại bước k;

V_i^k Vận tốc cá thể thứ i tại bước k;

X_i^{k+1} : Vị trí cá thể thứ i tại bước k + 1;

V_i^{k+1} Vận tốc cá thể thứ i tại bước k + 1;

P_{best} : Vị trí tốt nhất của cá thể thứ i;

G_{best} : Vị trí tốt nhất trong quần thể.

Định nghĩa 9. MDL là tổng độ hữu ích cần giảm của tất cả các tập nhạy cảm có độ hữu ích cao; S_{items} là tập hợp các mục có trong ít nhất một tập nhạy cảm có độ hữu ích cao; n là số lượng các mục trong S_{items} và $n = |S_{items}|$; S_{tids} là tập hợp các giao dịch có trong ít nhất một tập nhạy cảm có độ hữu ích cao; và m là số lượng các giao dịch có S_{tids} , $m = |S_{tids}|$.

Ví dụ: Nếu $minutil = 168$ thì MDL được tính như sau (Bảng):

Bảng 4. Minh họa cách tính MDL

Tập mục	Độ hữu ích	Cần giảm
bcd	173	5
bd	192	24
c	180	12
d	168	0
MDL		41

Mô hình hóa một cá thể (giải pháp của bài toán)

Một cá thể chứa thông tin ẩn của các mục trong từng giao dịch, vận tốc di chuyển cá thể và độ thích nghi của cá thể.

Thông tin ẩn của các mục trong từng giao dịch

Số lượng của mỗi mục trong một giao dịch đều ảnh hưởng tới độ hữu ích của các tập nhạy cảm, vì vậy số lượng thay đổi của các mục trong mỗi giao dịch đều cần lưu trữ lại. Thông tin của mỗi cá thể sẽ được lưu trữ dưới dạng một mảng 2 chiều a có m dòng (số lượng giao dịch ảnh hưởng tới tập nhạy cảm có độ hữu ích cao) và n cột (số lượng các mục chứa trong tập nhạy cảm). Mỗi phần tử $a[i, j]$ trong mảng là số lượng giảm của mục thứ i trong S_{items} trong giao dịch thứ j trong S_{tids} . Giá trị của $a[i, j]$ được giới hạn từ 0 đến số lượng giao dịch tối đa của các mục trong CSDL giao dịch ban đầu.

Ví dụ: Với $S_{items} = \{b, c, d\}$ và $S_{tids} = \{2, 4, 6, 7, 9, 11, 12\}$, khi đó một cá thể là một mảng 2 chiều có 7 dòng và 3 cột, cụ thể như sau (Bảng):

Bảng 5. Biểu diễn của một cá thể

1	0	0
0	1	0
0	0	0
0	0	0
1	0	2
0	0	0
1	0	1

Trong cá thể này, CSDL sẽ giảm số lượng của các mục b, c, d trong giao dịch T_2 lần lượt là 1, 0, 0. Số lượng giảm của b, c, d trong giao dịch T_{12} lần lượt là 1, 0, 1.

Số lượng giảm của các mục trong mỗi giao dịch phải nhỏ hơn số lượng của các mục trong giao dịch đang xét và nhỏ hơn số lượng tối đa cần phải giảm. Vì số lượng tối đa trong của c trong giao dịch T_4 là 5 nhưng vì $MDL = 41$, suy ra số lượng tối đa giảm là $41/15 = 3$. Do đó số lượng giảm của c trong giao dịch T_4 tối đa là 3. Tương tự như vậy số lượng của c tối đa cần sửa trong giao dịch T_{11} là 2 vì trong giao dịch T_{11} chỉ có 2 mục c .

Vận tốc của một cá thể

Vận tốc của mỗi cá thể sẽ đại diện cho sự biến đổi của cá thể tại một thời điểm được phát sinh ngẫu nhiên và được lưu trong mảng 02 chiều các số thực có m dòng và n cột. Khi di chuyển, giá trị của vận tốc sẽ bị giới hạn bởi giá trị vận tốc tối đa (V_{max}), và giá trị vận tốc tối thiểu (V_{min}) để đảm bảo kết quả tối ưu cho bài toán.

Tính độ thích nghi của một cá thể

Độ thích nghi của một cá thể được tính theo công thức $f = A + \delta * FS + \beta * FT$

Trong đó:

A : là độ lệch của CSDL ban đầu so với CSLD đã chỉnh sửa.

FS : là số lượng các tập nhạy cảm có độ hữu ích cao chưa được ẩn.

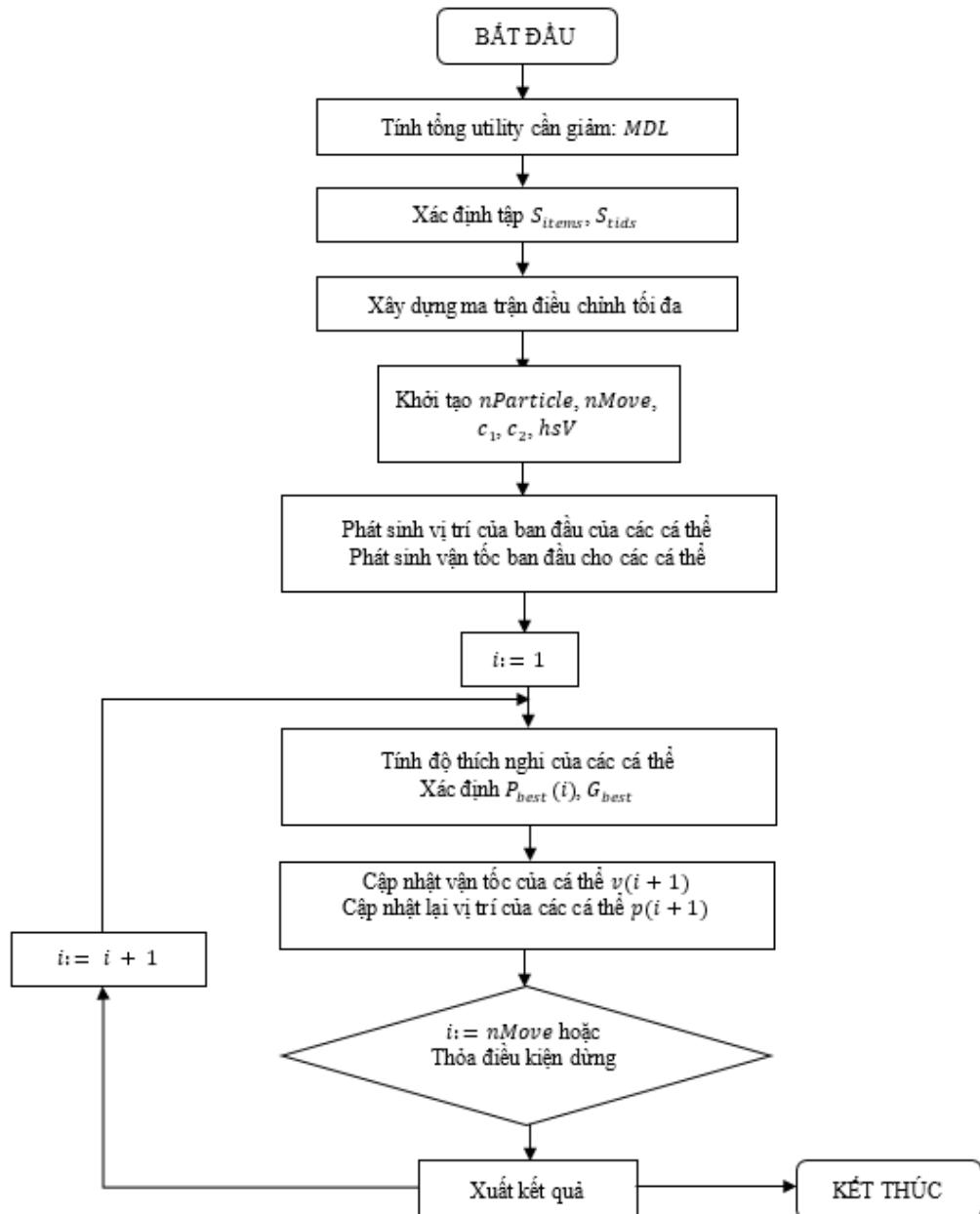
δ : Hệ số thích nghi. Do mục tiêu của thuật toán là ẩn các tập nhạy cảm có độ hữu ích cao nên chọn δ rất lớn so với độ lệch A (ví dụ chọn $\delta = minutil = 168$).

β : Hệ số mất giao dịch. Để hạn chế việc mất các giao dịch hệ số β sẽ phải được chọn phù hợp.

FT : là số lượng giao dịch bị mất do số lượng mục trong giao dịch bị điều chỉnh về 0.

Ví dụ: Với cá thể ở trên, $A = 6 + 15 + 21 = 42$ và $FS = 0$ (vì tất cả các tập nhạy cảm đều được ẩn) và $FT = 0$ (vì không có giao dịch nào có số lượng mục bị chỉnh về 0) nên độ thích nghi của cá thể là $f = 42 + \delta * 0 + \beta * 0 = 42$.

Thuật toán



Hình 2. Lưu đồ mô tả thuật toán PSO-PPUM

Ví dụ: Với CSDL trong Bảng 1 và $minutil = 168$ thuật toán sẽ thực hiện như sau:

Bước 1: Với SHUI như trong Bảng 4 thì $MDL = 41$.

Bước 2: Xác định tập $S_{items} = \{b, c, d\}$ và $S_{tids} = \{2, 4, 6, 7, 9, 11, 12\}$ nên $m = 7$ và $n = 3$.

Bước 3: Tính được ma trận điều chỉnh tối đa của các item trong quần thể (Bảng)

Bảng 6. Ma trận điều chỉnh tối đa

	b	c	d
T_2	1	0	5
T_4	0	5	0
T_6	0	2	0
T_7	1	0	4
T_9	2	3	7
T_{11}	5	2	5
T_{12}	3	0	3

Bảng 7. Bảng vận tốc tối đa

	b	c	d
T_2	0.5	0	2.5
T_4	0	2.5	0
T_6	0	1	0
T_7	0.5	0	2
T_9	1	1.5	3.5
T_{11}	2.5	1	2.5
T_{12}	1.5	0	1.5

Bước 4: Giả sử ta chọn $nParticle = 10$, $c_1 = 2$, $c_2 = 2$, $nMove = 40$ và chọn hệ số vận tốc tối đa $hsV = 0.5$ ta xây dựng được bảng vận tốc tối đa (Bảng 7).

Bước 5: Khởi tạo quần thể ban đầu.

Bước 6: Tính độ thích nghi của tất cả các thê đã phát sinh.

Tìm vị trí tốt nhất của các thê mà nó từng đi qua $P_{best}(i)$. Vì bước đầu nên vị trí của nó cũng là vị trí tốt nhất.

Tìm vị trí tốt nhất của cả quần thể đã đi qua G_{best} . Do đây là bước đầu nên cá thê có độ thích nghi lớn nhất chính là G_{best} .

Bảng 8. Quần thể ban đầu

Cá thê thứ 1

0	0	4	1.00 0.00 0.00 1.00 0.35 0.07 1.41	0.00	1.02
0	0	0		1.78	0.00
0	0	0		0.60	0.00
0	0	3		0.00	1.85
0	2	5		1.15	1.98
0	0	0		0.77	0.65
2	0	0		0.00	1.06
<i>fitness:</i> 286					

 P_{best} thứ 1

0	0	4
0	0	0
0	0	0
0	0	3
0	2	5
0	0	0
2	0	0
<i>fitness</i>		286

Cá thê thứ 2

0	0	3	1.00 0.00 0.00 1.00 0.67 1.31 0.90	0.00	0.65
0	2	0		0.21	0.00
0	1	0		0.58	0.00
0	0	2		0.00	0.27
0	1	3		1.24	1.28
3	1	2		0.65	1.36
1	0	1		0.00	0.55
<i>fitness:</i> 160					

 P_{best} thứ 2

0	0	3
0	2	0
0	1	0
0	0	2
0	1	3
3	1	2
1	0	1
<i>fitness</i>		160

Các cá thê từ 3 đến 10 được phát sinh tương tự với *fitness* lần lượt là 87, 129, 117, 132, 111, 219, 134 và 100. Do đó, G_{best} tại bước khởi tạo là:

G_{best} tại bước khởi tạo		
0	0	1
0	1	0
0	0	0
0	0	2
0	0	0
4	1	3
0	0	1
<i>fitness</i>		87

Bước 7: Cập nhật trạng thái mới của quần thể (cập nhật vận tốc $v(i)$ của mỗi cá thể và cập nhật vị trí mới của từng cá thể $X(i + 1)$).

Tương ứng $r = 0.85$, $\omega = 0.89$, trạng thái mới của quần thể được cập nhật lại như sau:

Bảng 9. Quần thể sau khi cập nhật

Cá thể thứ 1			P _{best} thứ 1			Cá thể thứ 9			P _{best} thứ 9		
0	0	1	0.50	0.00	-2.50	0	0	1	0	0	1
0	2	0	0.00	2.50	0.00	0	2	0	0	0	0
0	0	0	0.00	0.53	0.00	0	0	0	0	0	2
0	0	2	0.50	0.00	-0.06	0	0	1	0	0	1
0	0	1	0.31	-1.50	-3.50	2	1	2	0	0	1
2	1	2	2.50	1.00	2.50	0	0	1	0	0	1
0	0	1	-1.50	0.00	1.50	<i>fitness</i> : 98			<i>fitness</i> : 98		
Cá thể thứ 9			P _{best} thứ 9			Cá thể thứ 9			P _{best} thứ 9		
0	0	1	0.50	0.00	0.37	0	0	1	0	0	0
0	0	0	0.00	-2.48	0.00	0	0	0	0	0	0
0	0	0	0.00	0.14	0.00	0	0	0	0	0	0
0	0	2	0.50	0.00	2.00	0	0	2	0	0	0
0	0	0	0.19	-1.50	-3.50	0	0	0	0	0	0
3	1	2	2.50	1.00	-1.32	3	1	2	0	0	0
0	0	0	-1.50	0.00	-1.50	<i>fitness</i> : 56			<i>fitness</i> : 56		

Các cá thể từ 2, 3, 4, 5, 6, 7, 8 và 10 trong quần thể sau khi cập nhật tương tự với *fitness* lần lượt là 74, 125, 82, 82, 71, 99, 104 và 131. Vì vậy, giá trị P_{best} của các cá thể trong quần thể mới có *fitness* là 98, 74, 87, 82, 82, 71, 99, 104, 56 và 131. Do đó, G_{best} tại bước di chuyển thứ 1 là:

G_{best} tại bước di chuyển thứ 1		
0	0	1
0	0	0
0	0	0
0	0	2
0	0	0
3	1	2
0	0	0
<i>fitness</i>		56

Lặp lại quá trình di chuyển của quần thể theo tiến trình trên, quá trình lặp dừng lại khi độ thích nghi của các thề (fitness của P_{best}) không đổi quá 5 lần tại bước thứ 11. Cuối cùng, ta có kết quả cuối cùng của G_{best} như sau:

Bảng 10. Cá thể G_{best}

0	0	0
0	0	0
0	0	0
0	0	3
0	0	0
2	1	0
0	0	0
<i>fitness</i>		40

Tương ứng G_{best} ở trên, thuật toán đã đưa ra cách chỉnh sửa CSDL ban đầu thành CSDL trong *Bảng* và đã ân được tất cả các tập nhạy cảm có độ hữu ích cao với độ lệch so với cơ sở dữ liệu ban đầu là 40.

Bảng 11. Cơ sở dữ liệu chỉnh sửa D'

Item Tid	a	b	c	d	e
T1	6	0	0	0	0
T2	0	1	0	5	0
T3	0	6	0	0	0
T4	0	0	5	0	0
T5	0	0	0	0	8
T6	2	0	2	0	3

Item Tid	a	b	c	d	e
T7	0	1	0	1	0
T8	0	4	0	0	0
T9	0	2	3	7	0
T10	0	0	0	0	1
T11	0	3	1	5	0
T12	0	3	0	3	0

Sử dụng thuật giải PSO vào bài toán ẩn tập nhạy cảm có độ hữu ích cao, thuật toán PSO-PPUM đã ẩn được các itemset nhạy cảm có độ hữu ích cao mà sự khác biệt của CSDL gốc và CSDL sau khi chỉnh sửa là thấp hơn và tốc độ hội tụ nhanh hơn so với các thuật toán khác. Tuy nhiên không gian lưu trữ lại tương đối lớn vì phải lưu trữ lại các thông tin về các cá thể cũng như vận tốc của chúng tại mỗi bước thực thi.

5. THỰC NGHIỆM

5.1. Cơ sở dữ liệu thực nghiệm

Các kết quả bên dưới được chạy trên máy có cấu hình như sau: Intel core i5 (5×2.53 GHz), 8GB RAM memory, Windows 10. Các thuật toán được cài đặt sử dụng ngôn ngữ C#.

Thực nghiệm được thực hiện trên 3 cơ sở dữ liệu thực là Retail, Mushroom, BMS-POS được lấy từ website <http://www.cs.rpi.edu/~zaki/Workshops/FIMI/data/>. Đặc trưng của các CSDL này được mô tả trong *Bảng 12*. Với tất cả các những CSDL đã có độ hữu ích của các mục được phát sinh ngẫu nhiên là các số từ 1 tới 10 và số lượng được phát sinh của các mục trong từng giao dịch cũng được phát sinh từ 1 tới 10. Tỉ lệ phát sinh ngẫu nhiên là từ 0.1 tới 1.

Bảng 12. Thông tin về các cơ sở dữ liệu

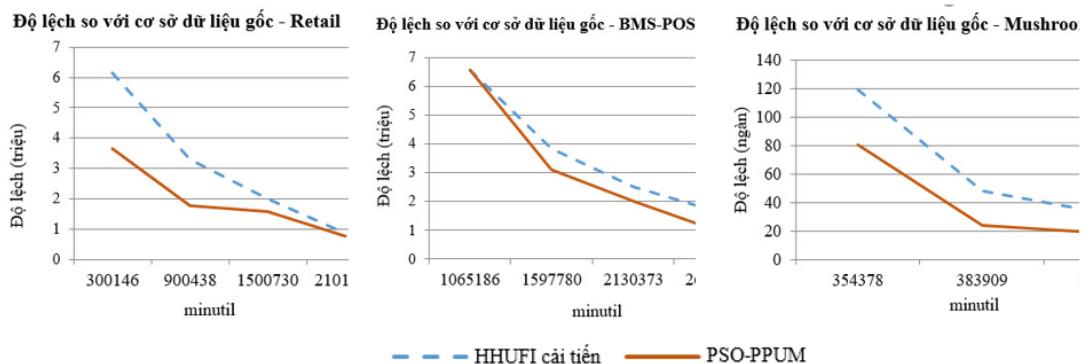
Cơ sở dữ liệu	Số giao dịch	Số item	Độ dài trung bình	Độ dài
Retail	88,162	16,470	10.3	76
BMS-POS	515,597	1,657	6.4	46
Mushroom	8,124	119	23	23

5.2. Kết quả thực nghiệm

Trong phần thực nghiệm, thuật toán đề xuất thực hiện trên ba CSDL là Retail, BMS-POS và Mushroom để so sánh kết quả của các thuật toán HHUIF cải tiến và PSO-PPUM. Nghiên cứu giả sử tất cả các HUI đều là tập nhạy cảm hữu ích cao cần được ẩn. Các thuật toán đã ẩn được tất cả HUI nhạy cảm của CSDL thực nghiệm. Thực nghiệm quan tâm tới độ lệch (độ lệch được xác định bằng hiệu tổng độ hữu ích của CSDL gốc với tổng độ hữu ích của CSDL đã chỉnh sửa) sau khi tất cả các tập HUI nhạy cảm đã được ẩn.

Trong quá trình thực nghiệm, các thông số được chọn như sau: Số lượng cá thể của quần thể: 500, 1000; Số thế hệ tối đa của quần thể: $n = 1000$; Điều kiện dừng: Khi giá trị tối ưu của thuật toán không thay đổi trong 5 lần gần nhất hoặc số thế hệ đạt giá trị n ; Giá trị $\beta = \delta = minutil$.

Kết quả thực nghiệm được trình bày trong Hình 3:



Hình 3. Biểu đồ độ lệch trên các cơ sở dữ liệu

Kết quả thực nghiệm thu được cho thấy, cả 02 thuật toán đều ẩn được tất cả các tập hữu ích cao trong các cơ sở dữ liệu thử nghiệm. Khi giá trị *minutil* càng cao, số lượng HUI càng nhỏ thì độ lệch sau khi chỉnh sửa càng nhỏ. Điều này hiển nhiên vì giá trị độ hữu ích cần giảm của mỗi tập HUI và cả số lượng tập HUI nhạy cảm đều nhỏ hơn.

Kết quả thực nghiệm cũng cho thấy độ lệch khi sử dụng phương pháp tối ưu toàn cục bằng PSO đều cho kết quả tốt hơn so với sử dụng phương pháp tối ưu cục bộ của thuật toán HHUIF cải tiến. Trong phương pháp tối ưu cục bộ, thuật toán ẩn lần lượt các tập HUI nhạy cảm và tập trung vào việc chỉnh sửa cơ sở dữ liệu để đảm bảo HUI đang xét mà không quan tâm tới ảnh hưởng của việc điều chỉnh tới các HUI khác. Do đó, việc điều chỉnh không chọn được các giá trị điều chỉnh mà giúp giảm được cho nhiều HUI nhạy cảm một cách đồng thời như các thuật toán tối ưu toàn cục. Chính vì vậy, độ lệch do HHUIF cải tiến tạo ra thường lớn hơn từ rất nhiều so với thuật toán còn lại. Đặc biệt, một số trường hợp độ lệch tạo ra bởi HHUIF lớn hơn tới 2-4 lần so với PSO-PPUM.

6. KẾT LUẬN

Ẩn tập hữu ích cao nhạy cảm là chủ đề nghiên cứu thú vị và có nhiều ứng dụng trong thực tế. Nghiên cứu đã tìm hiểu được qui trình ẩn các tập hữu ích cao nhạy cảm để bảo toàn tính riêng tư của dữ liệu. Nghiên cứu cũng đã ứng dụng được thuật giải Heuristic (thuật giải PSO) vào trong bài toán này nhằm tối thiểu hóa sự thay đổi của CSDL khi tiến hành chỉnh sửa. Từ đó, nghiên cứu đã đề xuất được thuật toán PSO-PPUM. Thuật toán PSO-PPUM đã phát huy được các ưu điểm của thuật giải tối ưu bày đàn, ẩn được tất cả các tập nhạy cảm hữu ích cao với độ lệch ít hơn so với thuật toán HHUIF cải tiến.

Do số lượng của hữu ích cao là rất lớn nên việc tính toán độ thích nghi của mỗi cá thể trong quần thể (hay bày đàn) nên tiêu tốn rất nhiều thời gian cho việc kiểm tra các tập hữu ích cao đã được ẩn hay không. Hơn nữa, trong các CSDL giao dịch số lượng các tập hữu ích cao đóng (Closed HUI) sẽ chứa tất cả các tập hữu ích cao và số lượng ít hơn rất nhiều lần so với số lượng tập HUI. Vì vậy để ẩn tất cả các tập nhạy cảm hữu ích cao, trong thời gian tới nhóm tác giả sẽ thực hiện trên các tập hữu ích cao đóng để giảm bớt chi phí về thời gian tính độ thích nghi, giúp cải thiện tốc độ thực thi của thuật toán. Nghiên cứu sẽ tìm cách giảm chi phí về không gian và thời gian thực thi của bài toán bằng cách xem xét việc gộp cách giao dịch có chung tập mục.

TÀI LIỆU THAM KHẢO

1. R. Agrawal, T. Imieliński, and A. Swami, “Mining association rules between sets of items in large databases,” *ACM SIGMOD Record*, vol. 22, no. 2, pp. 207–216, Jun. 1993, doi: 10.1145/170036.170072.
2. H. Yao, H. J. Hamilton, and G. J. Butz, “A foundational approach to mining itemset utilities from databases,” *Proc West Mark Ed Assoc Conf*, pp. 482–486, 2004, doi: 10.1137/1.9781611972740.51.
3. E. Dasseni, V. S. Verykios, A. K. Elmagarmid, and E. Bertino, “Hiding association rules by using confidence and support,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2137, pp. 369–383, 2001, doi: 10.1007/3-540-45496-9_27/COVER.
4. A. Evfimievski, R. Srikant, R. Agrawal, and J. Gehrke, “Privacy preserving mining of association rules,” *Inf Syst*, vol. 29, no. 4, pp. 343–364, Jun. 2004, doi: 10.1016/J.IS.2003.09.001.
5. J. L. Lin and Y. W. Cheng, “Privacy preserving itemset mining through noisy items,” *Expert Syst Appl*, vol. 36, no. 3, pp. 5711–5717, Apr. 2009, doi: 10.1016/J.ESWA.2008.06.052.

6. S. L. Wang, B. Parikh, and A. Jafari, "Hiding informative association rule sets," *Expert Syst Appl*, vol. 33, no. 2, pp. 316–323, Aug. 2007, doi: 10.1016/J.ESWA.2006.05.022.
7. C. W. Lin, T. P. Hong, J. W. Wong, and G. C. Lan, "Privacy preserving high utility mining based on genetic algorithms," *Proceedings - 2013 IEEE International Conference on Granular Computing GrC 2013*, pp. 191–195, 2013, doi: 10.1109/GRC.2013.6740406.
8. B. Vo, C. W. Lin, T. P. Hong, V. V. Vu, M. Nguyen, and B. Le, "An Efficient Method for Hiding High Utility Itemsets," *Frontiers in Artificial Intelligence and Applications*, vol. 252, pp. 356–363, 2013, doi: 10.3233/978-1-61499-254-7-356.
9. C. W. Lin, T. P. Hong, J. W. Wong, G. C. Lan, and W. Y. Lin, "A GA-based approach to hide sensitive high utility Itemsets," *The Scientific World Journal*, vol. 2014, 2014, doi: 10.1155/2014/804629.
10. D. T. Dinh, V. N. Huynh, B. Le, P. Fournier-Viger, U. Huynh, and Q. M. Nguyen, "A Survey of Privacy Preserving Utility Mining," *Studies in Big Data*, vol. 51, pp. 207–232, 2019, doi: 10.1007/978-3-030-04921-8_8/COVER.
11. B. Le, D. T. Dinh, V. N. Huynh, Q. M. Nguyen, and P. Fournier-Viger, "An efficient algorithm for Hiding High Utility Sequential Patterns," *International Journal of Approximate Reasoning*, vol. 95, pp. 77–92, Apr. 2018, doi: 10.1016/J.IJAR.2018.01.005.
12. "Fast Algorithms for Mining Association Rules in Large Databases | Proceedings of the 20th International Conference on Very Large Data Bases." <https://dl.acm.org/doi/10.5555/645920.672836> (accessed Apr. 24, 2023).
13. M. J. Zaki and C. J. Hsiao, "Efficient algorithms for mining closed itemsets and their lattice structure," *IEEE Trans Knowl Data Eng*, vol. 17, no. 4, pp. 462–478, Apr. 2005, doi: 10.1109/TKDE.2005.60.
14. J. Han, J. Pei, and Y. Yin, "Mining frequent patterns without candidate generation," *ACM SIGMOD Record*, vol. 29, no. 2, pp. 1–12, May 2000, doi: 10.1145/335191.335372.
15. Y. Liu, W. K. Liao, and A. Choudhary, "A two-phase algorithm for fast discovery of high utility itemsets," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3518 LNAI, pp. 689–695, 2005, doi: 10.1007/11430919_79/COVER.
16. V. S. Tseng, B.-E. Shie, C.-W. Wu, and P. S. Yu, "Efficient Algorithms for Mining High Utility Itemsets from Transactional Databases," *IEEE Trans Knowl Data Eng*, vol. 25, no. 8, pp. 1772–1786, Aug. 2013, doi: 10.1109/TKDE.2012.59.
17. M. Liu and J. Qu, "Mining high utility itemsets without candidate generation," in *Proceedings of the 21st ACM international conference on Information and knowledge management - CIKM '12*, New York, New York, USA: ACM Press, 2012, p. 55. doi: 10.1145/2396761.2396773.
18. S. Krishnamoorthy, "HMiner: Efficiently mining high utility itemsets," *Expert Syst Appl*, vol. 90, pp. 168–183, Dec. 2017, doi: 10.1016/j.eswa.2017.08.028.
19. J. Liu, X. Zhang, B. C. M. Fung, J. Li, and F. Iqbal, "Opportunistic mining of top-n high utility patterns," *Inf Sci (N Y)*, vol. 441, pp. 171–186, May 2018, doi: 10.1016/J.INS.2018.02.035.
20. S. Krishnamoorthy, "Mining top-k high utility itemsets with effective threshold raising strategies," *Expert Syst Appl*, vol. 117, pp. 148–165, Mar. 2019, doi: 10.1016/J.ESWA.2018.09.051.
21. M. Ashraf, T. Abdelkader, S. Rady, and T. F. Gharib, "TKN: An efficient approach for discovering top-k high utility itemsets with positive or negative profits," *Inf Sci (N Y)*, vol. 587, pp. 654–678, Mar. 2022, doi: 10.1016/J.INS.2021.12.024.
22. N. N. Pham, Z. Kominkova Oplatkova, H. M. Huynh, and B. Vo, "Mining Top-K High Utility Itemset Using Bio-Inspired Algorithms," in *2022 IEEE Workshop on Complexity in Engineering (COMPENG)*, IEEE, Jul. 2022, pp. 1–5. doi: 10.1109/COMPENG50184.2022.9905433.
23. W. Gan, S. Wan, J. Chen, C. M. Chen, and L. Qiu, "TopHUI: Top-k high-utility itemset mining with negative utility," *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*, pp. 5350–5359, Dec. 2020, doi: 10.1109/BIGDATA50022.2020.9378288.
24. P. Fournier-Viger, S. Zida, J. C. W. Lin, C. W. Wu, and V. S. Tseng, "EFIM-closed: Fast and memory efficient discovery of closed high-utility itemsets," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9729, pp. 199–213, 2016, doi: 10.1007/978-3-319-41920-6_15.
25. L. T. T. Nguyen *et al.*, "An efficient method for mining high utility closed itemsets," *Inf Sci (N Y)*, vol. 495, pp. 78–99, Aug. 2019, doi: 10.1016/J.INS.2019.05.006.

26. H. Duong, T. Hoang, T. Tran, T. Truong, B. Le, and P. Fournier-Viger, "Efficient algorithms for mining closed and maximal high utility itemsets," *Knowl Based Syst*, vol. 257, Dec. 2022, doi: 10.1016/j.knosys.2022.109921.
27. M. Sridhar, B. B. Raveendra, and R. M V P Chandra Sekhara, "Swarm Optimization Algorithm for Privacy Preserving in Data Mining," *International Journal of Computer Science Issues*, vol. 10, no. 2, pp. 46–51, 2013, Accessed: Apr. 24, 2023. [Online]. Available: <https://ijcsi.org/papers/IJCSI-10-2-3-46-51.pdf>
28. J. Kennedy and R. Eberhart, "Particle swarm optimization," *Proceedings of ICNN'95 - International Conference on Neural Networks*, vol. 4, pp. 1942–1948, doi: 10.1109/ICNN.1995.488968.

ABSTRACT

PRIVATE PRESERVING HIGH UTILITY ITEMSETS USING PARTICLE SWARM OPTIMIZATION

Lam Thi Hoa Mi^{1,*}, Vu Van Vinh¹, Duong Thi Mong Thuy¹

¹Ho Chi Minh City University of Food Industry

*Email: milth@hufi.edu.vn

High utility set mining (HUIM) is used to discover itemsets whose utility is greater than a given minimum threshold. This is a problem that has attracted the attention of many scientists, and many effective algorithms have been proposed. However, during mining, a lot of sensitive information is also discovered. And since then, some studies with the aim of modifying the initial database to be able to hide this sensitive information have been investigated. Most of the algorithms focus on hiding the sensitive information by local optimization methods such as the algorithm to Hide the High Utility Itemset First (HHUIF), the improved HHUIF, and the algorithm to hide the Maximum Sensitive Itemsets Conflict First (MSCIF), ... without considering the variation of the database. Recently, some sensitive information hiding algorithms, based on Genetic Algorithm (GA), have also been proposed by adding and removing transactions in the initial database. For this reason, the database can generate more virtual transactions or lose much information. In this study, we propose a method to modify the number of items in the initial database to hide sensitive high utility itemsets. The proposed algorithm is created on the idea of a global optimization technique, specifically the Particle Swarm Optimization (PSO) algorithm. The obtained results show that the proposed algorithm hides sensitive information and optimizes the deviation of the database after editing compared to the initial database.

Keywords: protect privacy, hiding high utility itemsets, sensitive high utility itemsets, Particle Swarm Optimization algorithm.

KHAI THÁC TẬP HỮU ÍCH CAO DỰA TRÊN CƠ CHẾ DIFFSET

Nguyễn Thị Thanh Thủy^{1,*}, Nguyễn Văn Lê¹, Mạnh Thiên Lý¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: thuyntt@huf.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Khai thác tập hữu ích cao (High Utility Itemsets - HUIs) là việc tìm ra các tập mục thỏa một ngưỡng độ hữu ích tối thiểu do người dùng xác định. Đã có nhiều thuật toán khai thác tập hữu ích cao hiệu quả, tuy nhiên các thuật toán này đều dựa trên cơ chế Tidset. Trong bài báo này, thuật toán DCHUIM được đề xuất nhằm khai thác tập hữu ích cao bằng cơ chế Diffset. Để thực hiện việc này, một cấu trúc dữ liệu DUL được xây dựng để lưu trữ thông tin về độ hữu ích của một tập mục và các giao dịch thuộc tập Diffset. Ngoài ra, thuật toán còn áp dụng các chiến lược cắt tia như U-Prune, EUCS-Prune và sử dụng tập hữu ích đóng để nén dữ liệu một cách hiệu quả, từ đó giảm không gian tìm kiếm trong quá trình khai thác. Thực nghiệm được thực hiện trên các bộ dữ liệu lớn gồm Accidents, Mushroom, Retail, Chainstore và tiến hành so sánh hiệu suất thực thi giữa thuật toán DCHUIM với thuật toán HMINER. Kết quả cho thấy thuật toán DCHUIM có hiệu suất tốt hơn thuật toán HMINER về thời gian thực thi trên cơ sở dữ liệu thưa và vượt trội về bộ nhớ sử dụng trên tất cả các cơ sở dữ liệu.

Từ khóa: Khai thác tập phổ biến, khai thác tập hữu ích cao, cơ sở dữ liệu giao dịch.

1. GIỚI THIỆU

Ngày nay, khai thác dữ liệu là chủ đề được nhiều người quan tâm. Trong lĩnh vực kinh doanh, các kết quả khai thác dữ liệu sẽ cung cấp cho doanh nghiệp những hiểu biết sâu sắc hơn về hành vi và sở thích của khách hàng. Từ đó, các nhà quản lý có thể đề ra các chiến lược kinh doanh nhằm tối đa hóa lợi nhuận. Các nghiên cứu về khai thác tập phổ biến (Frequent Pattern Mining - FIM) [1, 2, 3, 4] và khai thác luật kết hợp (Association Rule Mining - ARM) [5, 6, 7] đã được thực hiện với mục đích tìm ra tập các mặt hàng thường được khách hàng mua cùng nhau trong cơ sở dữ liệu giao dịch. Về sau, các nghiên cứu về khai thác tập mục hữu ích cao (Mining High Utility Itemsets - HUIM) ra đời nhằm khai thác và tìm kiếm các tập mặt hàng mang lại lợi nhuận cao cho các doanh nghiệp bằng cách xem xét cả số lượng và lợi nhuận của các mặt hàng. Đã có nhiều nghiên cứu về HUIM được thực hiện: ban đầu, việc khai thác tập HUIs được thực hiện thông qua 2 giai đoạn (phase): giai đoạn 1 xác định tập ứng viên và giai đoạn 2 xác định chính xác tập HUIs bằng cách loại bỏ ứng viên không phù hợp trong giai đoạn 1. Một số thuật toán 2 phase có thể kể đến như UMining & Umining-H [8], TWU-Mining [9], Two-Phase [10], UP-Growth [11], UP-Growth+ [12],.... Thực tế cho thấy các thuật toán 2 phase thường tiêu tốn nhiều thời gian và bộ nhớ để xác định và lưu trữ tập ứng viên, đặc biệt khi tập ứng viên này quá lớn. Do đó, gần đây các thuật toán khai thác tập HUIs được thực hiện nhanh chóng và hiệu quả hơn chỉ bằng 1 phase như d2HUP [13], HUI-Miner [14], FHM

[15], EFIM [16], HMiner [17], etc. Các thuật toán 1 phase cải thiện đáng kể thời gian thực thi nhưng bộ nhớ tiêu thụ vẫn còn khá lớn. Ngoài ra, điểm chung của các thuật toán này là lưu trữ tập giao của các giao dịch trong cấu trúc dữ liệu.

Trong bài báo này, một cách tiếp cận mới được đề xuất để khai thác tập HUIs, đó là cách tiếp cận dựa trên cơ chế Diffset. Để thực hiện điều này, nhóm tác giả xây dựng cấu trúc DUL để lưu trữ độ hữu ích của một tập mục và các giao dịch Diffset của tập mục này trong cơ sở dữ liệu. Trong cùng một lớp tương đương, Diffset được tính dựa trên sự khác biệt giữa hai Tidset. Ví dụ: tập mục $\{fde\}$ gồm phần tiên tố là $\{fd\}$ và phần mở rộng là $\{e\}$, các giao dịch xuất hiện trong DUL(fde) sẽ là các giao dịch có chứa $\{fd\}$ và không chứa $\{e\}$. Với cách tiếp cận này, thời gian thực thi và không gian bộ nhớ được cải thiện đáng kể so với các thuật toán trước đây do số lượng giao dịch được lưu trữ rất ít, đặc biệt là khi áp dụng trên cơ sở dữ liệu thưa.

Những đóng góp chính và quan trọng của bài báo này bao gồm:

- Xây dựng cấu trúc DUL để lưu trữ thông tin về độ hữu ích của các tập mục, làm cơ sở cắt tỉa trong quá trình khai thác.
- Đề xuất thuật toán DCHUIM để khai thác tập HUI một cách hiệu quả, kết hợp vận dụng các chiến lược cắt tỉa hiệu quả đã được đề xuất trong các nghiên cứu trước đây về khai thác HUI như U-Prune, EUCS-Prune giúp giảm thời gian tìm kiếm và không gian lưu trữ.
- Kết quả thử nghiệm trên các bộ dữ liệu thưa và dày đã chứng tỏ rằng thuật toán DCHUIM mà chúng tôi đề xuất có hiệu suất tốt hơn thuật toán hiệu quả nhất trong thời gian gần đây là HMiner về thời gian thực thi và bộ nhớ sử dụng, đặc biệt trên các cơ sở dữ liệu thưa.

Bài báo này được cấu trúc như sau: phần 2 trình bày các nghiên cứu liên quan đến khai thác tập hữu ích cao (HUIs). Phần 3 trình bày cơ sở lý thuyết. Phần 4 trình bày thuật toán DCHUIM. Phần 5 trình bày kết quả thực nghiệm của thuật toán. Cuối cùng là kết luận và hướng nghiên cứu trong tương lai được trình bày trong phần 6.

2. CÁC CÔNG TRÌNH LIÊN QUAN

Trong phần này, chúng tôi trình bày các công trình nghiên cứu liên quan đến các vấn đề sẽ được đề xuất trong bài báo này, bao gồm: tập phổ biến (Frequent Itemsets - FIs) và tập hữu ích cao (High Utility Itemsets - HUIs).

2.1. Tập phổ biến

Khái niệm khai thác tập phổ biến được Agrawal đề xuất vào năm 1993 với mục đích tìm mối liên hệ giữa các mặt hàng được bán trong siêu thị. Thuật toán Apriori [4] được ông và cộng sự đề xuất vào năm 1994, là thuật toán phổ biến trong các phương pháp tiếp cận theo cấp độ (level-wise approach) với các ứng viên được tạo ra ở nhiều mức. Thuật toán tiếp theo về khai thác tập phổ biến phải kể đến FP-tree [2]. FP-tree duyệt cơ sở dữ liệu hai lần, sau đó dùng phép chiếu để tạo ra cơ sở dữ liệu cục bộ của từng mặt hàng đơn, tạo cây FP cục bộ và khai thác trên cây cục bộ một cách đệ quy. Thuật toán sử dụng phương pháp chia để trị để khai thác tập phổ biến và là phương pháp không sinh ứng viên, thường rất hiệu quả trên các cơ sở dữ liệu có mật độ trùng lặp dữ liệu cao. Ngoài ra, một số nghiên cứu khác về khai thác tập phổ biến và luật kết hợp cũng được thực hiện như Eclat, Clique [5], MGARs [6], NSFI [3],

UniqAR [7]. Tuy nhiên, các nghiên cứu này không đề cập đến các yếu tố khác như: lợi nhuận, trọng lượng hay độ thú vị của các mục.

2.2. Tập hữu ích cao

Gần đây, nhiều nghiên cứu tập trung vào việc khai thác tập hữu ích cao và đã đạt được một số thành quả nhất định. Các thuật toán khai thác HUI ban đầu là các thuật toán 2 pha, điển hình là thuật toán Two-Phase [10] do Wu và cộng sự đề xuất, trong đó pha 1 tìm tập ứng viên thỏa điều kiện TWU lớn hơn ngưỡng độ hữu ích tối thiểu cho trước, ký hiệu là $minUtil$, pha 2 khai thác tập HUI từ danh sách tập ứng viên tìm được ở pha 1. Thuật toán TWU-Mining [9] do Le và cộng sự thực hiện, đã sử dụng cấu trúc cây WIT, mỗi nút trên cây chứa một tập mục X, tập các giao dịch chứa X, TWU và utility của X. Ngoài ra, các thuật toán 2 pha khác còn có thể kể đến như: UMining & UMining H [8], UP-Growth [11], UP-Growth+ [12], Tuy nhiên, các thuật toán này thường tiêu tốn nhiều thời gian và bộ nhớ để xác định và lưu trữ tập ứng viên, đặc biệt khi số lượng ứng viên tìm được ở pha 1 là khá lớn.

Vì vậy, các thuật toán sau này tập trung khai thác tập HUIs nhanh chóng và hiệu quả hơn chỉ bằng 1 pha. Thuật toán 1 pha điển hình ban đầu là thuật toán HUI-Miner [14], được Liu và cộng sự đã đề xuất vào năm 2012 sử dụng cấu trúc utility-list (UL). Trong cấu trúc này, nhóm tác giả đã dùng iutil để lưu trữ thông tin về độ hữu ích của một tập mục và dùng rutil để lưu trữ độ hữu ích còn lại của tập mục đó. Nhờ 2 đại lượng này mà thuật toán có thể kiểm tra liệu một tập mục có phải là 1 HUI và có thể mở rộng hay không ($iutil + rutil > \varepsilon$). Tập UL 1 phần tử được xây dựng từ CSDL ban đầu sau khi đã tách và sắp xếp các item tăng dần theo TWU. Tập UL k phần tử được xây dựng bằng cách kết hợp các UL ($k-1$) phần tử mà không cần quét lại CSDL. Thuật toán FHM [15] sau đó đề xuất ra một chiến lược cắt tia có tên là EUCP, chiến lược này sẽ tách đi các tập mục 2 phần tử có TWU nhỏ hơn ε nhằm cắt giảm không gian tìm kiếm.

Thuật toán EFIM [16] ra đời vào năm 2017 với việc đề xuất ba kỹ thuật rất hiệu quả để khai thác tập HUI. Đầu tiên là phép chiếu giao dịch (High-utility Database Projection - HDP) để khi khám phá các itemset mở rộng, thuật toán chỉ cần quét qua các item phía sau của itemset đó trong mỗi giao dịch, từ đó giảm thời gian quét CSDL. Tiếp theo thuật toán này sử dụng phép trộn giao dịch (High-utility Transaction Merging – HTM) để gom các giao dịch giống nhau thành một giao dịch, từ đó giảm kích thước cơ sở dữ liệu; đồng thời thuật toán cũng đề xuất hai ngưỡng giới hạn trên sub-tree utility và local utility để cắt giảm không gian tìm kiếm. Một thuật toán hiệu quả khác là HMiner [17] được đề xuất bởi Krishnamoorthy cùng với cấu trúc dữ liệu CUL (Compact Utility List). Ưu điểm của cấu trúc này là áp dụng khái niệm tập hữu ích đóng đối với các tập mục có từ 2 phần tử trở lên nhằm nén dữ liệu một cách hiệu quả trong quá trình khai thác. Theo đó, những giao dịch nào nằm trong tất cả các CUList ở cùng một mức thì thông tin của các giao dịch đó sẽ được tính vào độ hữu ích đóng và ngược lại. Nhờ đó, thời gian xét duyệt các giao dịch được giảm đáng kể, tăng hiệu quả thực thi của thuật toán. Đồng thời, thuật toán này cũng kết hợp với nhiều chiến lược cắt tia khác nhau để khai thác HUI một cách hiệu quả. Tuy nhiên, thuật toán HMiner vẫn còn tiêu tốn bộ nhớ khá lớn trên tất cả các cơ sở dữ liệu.

3. CƠ SỞ LÝ THUYẾT

Cho $I = \{x_1, x_2, \dots, x_m\}$ là tập hợp m mục (item) phân biệt, một tập mục (itemset) X là một tập hữu hạn các mục sao cho $X \subseteq I$. Một cơ sở dữ liệu giao dịch $D = \{T_1, T_2, \dots, T_n\}$ có n giao dịch (transaction). Với $\forall T_j \in D$, $T_j = \{x_k | k = 1, 2, \dots, N_j, x_k \in I\}$, trong đó N_j là số lượng các mục trong giao dịch T_j . Mỗi x_i trong I có một giá trị lợi nhuận (profit value) là $p(x_i)$. Mỗi x_k trong giao dịch T_j có số lượng mua là $q(x_k, T_j)$. Một ví dụ về cơ sở dữ liệu giao dịch D được cho trong Bảng 1. Lợi nhuận của các mục được cho trong Bảng 2.

Bảng 1. Cơ sở dữ liệu giao dịch D

TID	Giao dịch (T)	Số lượng mua (q)	Độ hữu ích (U)	Độ hữu ích giao dịch (TU)
T_1	b, d, e	5, 1, 1	5, 1, 2	8
T_2	b, c, e, f	3, 6, 3, 4	3, 6, 6, 8	23
T_3	a, b, c, d, e, f	1, 4, 1, 8, 2, 3	5, 4, 1, 8, 4, 6	28
T_4	b, c, d, e	2, 4, 6, 2	2, 4, 6, 4	16
T_5	a, c, e, f	1, 2, 3, 2	5, 2, 6, 2	15
T_6	a, c, d	2, 3, 6	10, 3, 6	19

Bảng 2. Lợi nhuận của các mặt hàng

Mặt hàng	a	b	c	d	e	f
Lợi nhuận	5	1	1	1	2	2

Độ hữu ích của một mặt hàng x_i trong một giao dịch T_j , ký hiệu: $U(x_i, T_j)$. Ví dụ: độ hữu ích của mặt hàng $\{b\}$ trong giao dịch T_1 được tính: $u(b, T_1) = p(b) * q(b, T_1) = 1 * 5 = 5$. Độ hữu ích của một tập mặt hàng $X = \{x_1, x_2, \dots, x_k\}$ trong giao dịch T_j , ký hiệu: $U(X, T_j)$ và được định nghĩa: $U(X, T_j) = \sum_{x_i \in X} U(x_i, T_j)$. Ví dụ: $U(bd, T_1) = u(b, T_1) + u(d, T_1) = 6$. Độ hữu ích của một tập mặt hàng X trong cơ sở dữ liệu giao dịch D , ký hiệu: $U(X)$ và được định nghĩa: $U(X) = \sum_{X \subseteq T_j \wedge T_j \in D} U(X, T_j)$. Ví dụ: $U(a) = U(a, T_3) + U(a, T_5) + U(a, T_6) = 5 + 5 + 10 = 20$. Độ hữu ích của một giao dịch T_j trong cơ sở dữ liệu D , ký hiệu: $TU(T_j)$ và được định nghĩa: $TU(T_j) = \sum_{x_i \in T_j} U(x_i, T_j)$. Ví dụ: $TU(T_1) = U(b, T_1) + U(d, T_1) + U(e, T_1) = 8$ và $TU(T_2) = 23$.

Độ hữu ích trọng số giao dịch của một tập mặt hàng X trong cơ sở dữ liệu D được ký hiệu là $TWU(X)$ và được định nghĩa: $TWU(X) = \sum_{X \subseteq T_j \in D} TU(T_j)$. Ví dụ: $TWU(ac) = TU(T_3) + TU(T_5) + TU(T_6) = 62$.

Một thứ tự toàn phần \prec được xây dựng dựa trên việc sắp xếp tăng dần theo TWU của các mặt hàng trong cơ sở dữ liệu D . Trong cơ sở dữ liệu đã cho ở Bảng 1, thứ tự sắp toàn phần các mặt hàng là: $a \prec f \prec d \prec b \prec e \prec c$. Bảng 3 thể hiện TWU của các mặt hàng sau khi sắp tăng dần và bảng 4 thể hiện cơ sở dữ liệu D sau khi sắp tăng dần theo TWU .

Bảng 3. TWU của các mặt hàng sau khi được sắp tăng dần

Items	a	f	d	b	e	c
Twu	62	66	71	75	90	101

Bảng 4. Cơ sở dữ liệu sau khi sắp tăng dần theo TWU

TID	Giao dịch (T)	Số lượng mua (q)	Độ hữu ích (U)	Độ hữu ích giao dịch (TU)
T_1	d, b, e	1, 5, 1	1, 5, 2	8
T_2	f, b, e, c	4, 3, 3, 6	8, 3, 6, 6	23
T_3	a, f, d, b, e, c	1, 3, 8, 4, 2, 1	5, 6, 8, 4, 4, 1	28
T_4	d, b, e, c	6, 2, 2, 4	6, 2, 4, 4	16
T_5	a, f, e, c	1, 2, 2, 3	5, 2, 6, 2	15
T_6	a, d, c	2, 6, 3	10, 6, 3	19

Tập tất cả các mặt hàng sau X trong T_j được ký hiệu là $T_j|X$. Ví dụ: trong Bảng 4, $T_2|f, b = \{e, c\}$ và $T_1|d = \{b, e\}$. Độ hữu ích sau của tập mặt hàng X trong một giao dịch T_j , ký hiệu: $RU(X, T_j)$, là tổng độ hữu ích của tất cả các mặt hàng sau X trong T_j , và được định nghĩa: $RU(X, T_j) = \sum_{x_i \in (T_j|X)} U(x_i, T_j)$. Ví dụ: $RU(d, T_1) = U(b, T_1) + U(e, T_1) = 7$.

4. THUẬT TOÁN DCHUIM

4.1. Cấu trúc DUL

Trong bài báo này, cấu trúc *DUL* được đề xuất để lưu trữ thông tin về độ hữu ích của một tập mục X (được cấu thành từ tiền tố P và phần mở rộng A). Cấu trúc này chia độ hữu ích của X thành hai phần là phần đóng và phần không đóng. Phần đóng được lưu trữ thông qua các giá trị *CU/CRU/CPU* và phần không đóng được lưu trữ thông qua các giá trị *NPU/NEU/NRU*. Đồng thời các giao dịch T_j trong danh sách bên dưới là tập các bộ có cấu trúc $\langle T_j, PU, RPU \rangle$. Trong đó T_j là các giao dịch chứa P nhưng không chứa A , PU là độ hữu ích tiền tố của X trong giao dịch, RPU là độ hữu ích sau của tiền tố X trong giao dịch T_j .

Cấu trúc của một *DUL* như sau:

NPU/NEU/NRU		CU/CRU/CPU
Tj	PU(X,Tj)	RPU(X,Tj)

Hình 1. Cấu trúc DUL

Độ hữu ích đóng của một tập mục X trong giao dịch T_j , ký hiệu là $CU(X, T_j)$ và được định nghĩa:

$$CU(X, T_j) = \begin{cases} U(X, T_j), & \text{if } |X| > 1 \text{ and } C(X - x_k) = S(T_j/\{X - x_k\}) \\ 0, & \text{ngược lại} \end{cases} [17]$$

Trong đó: $C(X - x_k)$ là tập các mục sau $X - x_k$ trong cơ sở dữ liệu và $S(T_j/\{X - x_k\})$ là tập các mục sau $X - x_k$ trong giao dịch T_j .

Độ hữu ích đóng của một tập mục X trong cơ sở dữ liệu D , ký hiệu là $CU(X)$ và được định nghĩa:

$$CU(X) = \sum_{X \subseteq T_j \in D} CU(X, T_j) [17]$$

Ví dụ: trong Bảng 4, $CU(af, T_3) = 11$, $CU(f, T_2) = 0$ và $CU(ad) = CU(ad, T_3) + CU(cd, T_6) = 9 + 0 = 9$.

Độ hữu ích sau đóng của một tập mục X trong một giao dịch T_j , ký hiệu: $CRU(X, T_j)$, và được định nghĩa:

$$CRU(X, T_j) = \begin{cases} RU(X, T_j), & \text{if } |X| > 1 \text{ and } C(X - x_k) = S(T_j / \{X - x_k\}) \\ 0, & \text{ngược lại} \end{cases} [17]$$

Độ hữu ích sau đóng của một tập mục X trong cơ sở dữ liệu D được định nghĩa là:

$$CRU(X) = \sum_{X \subseteq T_j \in D} CRU(X, T_j) [17]$$

Ví dụ: $CRU(ad, T_5) = 17$ và $CRU(de) = 8 + 4 = 12$.

Độ hữu ích tiền tố đóng của một tập mục X trong một giao dịch T_j , ký hiệu: $CPU(X, T_j)$, và được định nghĩa:

$$CPU(X, T_j) = \begin{cases} PU(X, T_j), & \text{nếu } |X| > 1 \text{ and } C(X - x_k) = S(T_j / \{X - x_k\}) \\ 0, & \text{ngược lại} \end{cases} [17]$$

Độ hữu ích tiền tố đóng của một tập mục X trong D được định nghĩa là:

$$CPU(X) = \sum_{X \subseteq T_j \in D} CPU(X, T_j). [17]$$

Ví dụ: $CPU(ad, T_5) = 5$ và $CPU(de) = 4 + 6 = 10$.

Ngoài ra, trong bài báo này, để tính độ hữu ích không đóng, chúng tôi đề xuất thêm một số định nghĩa như sau:

Định nghĩa 1: Cho một tập mục X được cấu thành từ tiền tố P và phần mở rộng A . Độ hữu ích tiền tố không đóng của tập mục X trong cơ sở dữ liệu, ký hiệu là $NPU(X)$, là tổng độ hữu ích không đóng của tiền tố P trong các giao dịch có chứa X và được định nghĩa:

$$NPU(X) = \sum_{X \subseteq T_j \in D \wedge CU(X, T_j) = 0} U(P, T_j)$$

Ví dụ: trong bảng 4, xét tập mục $\{ad\}$ được cấu thành từ tiền tố $\{a\}$ và phần mở rộng $\{d\}$, $NPU(ad) = U(a, T_6) = 10$. Giao dịch T_3 có chứa $\{ad\}$ nhưng không được xét vì $\{ad\}$ trong giao dịch T_3 đóng.

Định nghĩa 2: Cho một tập mục X được cấu thành từ tiền tố P và phần mở rộng A . Độ hữu ích mở rộng không đóng của tập mục X trong cơ sở dữ liệu, ký hiệu là $NEU(X)$, là tổng độ hữu ích không đóng của A trong các giao dịch có chứa X và được định nghĩa:

$$NEU(X) = \sum_{X \subseteq T_j \in D \wedge CU(X, T_j) = 0} U(A, T_j)$$

Ví dụ: trong bảng 4, xét tập mục $\{ad\}$ được cấu thành từ tiền tố $\{a\}$ và phần mở rộng $\{d\}$, $NEU(ad) = U(d, T_6) = 6$. Giao dịch T_3 có chứa $\{ad\}$ nhưng không được xét vì $\{ad\}$ trong giao dịch T_3 đóng.

Định nghĩa 3: Độ hữu ích của một tập mục X trong cơ sở dữ liệu, ký hiệu là $U(X)$, là tổng độ hữu ích không đóng và độ hữu ích đóng của X trong các giao dịch có chứa X và được định nghĩa:

$$U(X) = NPU(X) + NEU(X) + CU(X)$$

Ví dụ: ở bảng 4, $U(ad) = NPU(ad) + NEU(ad) + CU(ad) = 10 + 6 + 13 = 29$.

Định nghĩa 4: Cho một tập mục X được cấu thành từ tiền tố P và phần mở rộng A . Độ hữu ích còn lại không đóng của tập mục X trong cơ sở dữ liệu, ký hiệu là $NRU(X)$, là tổng độ hữu ích còn lại không đóng của A trong các giao dịch có chứa X và được định nghĩa:

$$NRU(X) = RU(X) - CRU(X)$$

Ví dụ: trong bảng 4, $NRU(ad) = RU(ad) - CRU(ad) = 12 - 9 = 3$.

Định nghĩa 5: Cho một tập mục X được cấu thành từ tiền tố P và phần mở rộng A . Độ hữu ích tiền tố của tập mục X trong một giao dịch T_j , ký hiệu là $PU(X, T_j)$, là độ hữu ích của P trong giao dịch T_j và được định nghĩa:

$$PU(X, T_j) = U(P, T_j)$$

Ví dụ: trong bảng 4, xét tập mục $\{fdb\}$ được cấu thành từ tiền tố $\{fd\}$ và phần mở rộng $\{b\}$, $PU(fdb, T_3) = U(fd, T_3) = 6 + 4 = 10$.

Định nghĩa 6: Cho một tập mục X được cấu thành từ tiền tố P và phần mở rộng A . Độ hữu ích sau tiền tố của tập mục X trong một giao dịch T_j , ký hiệu là $RPU(X, T_j)$, là độ hữu ích sau của P trong giao dịch T_j và được định nghĩa:

$$RPU(X, T_j) = RU(P, T_j)$$

Ví dụ: trong bảng 4, xét tập mục $\{fdb\}$ được cấu thành từ tiền tố $\{fd\}$ và phần mở rộng $\{b\}$, $RPU(fdb, T_3) = RU(fd, T_3) = 1 + 4 + 8 = 13$.

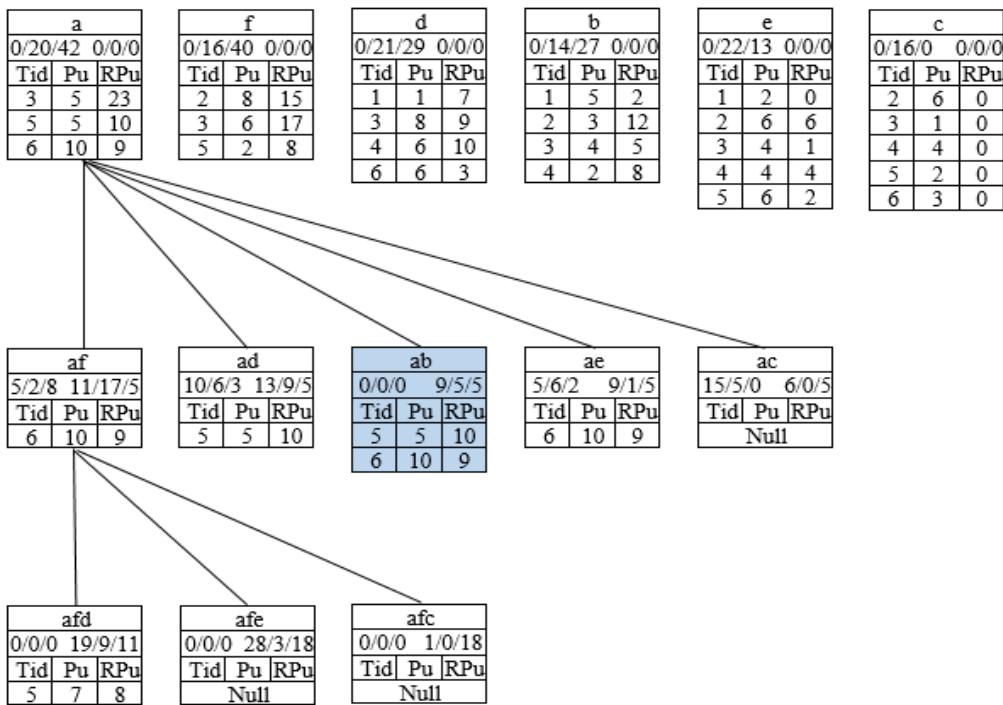
Một tập mục X được gọi là tập hữu ích cao (*High Utility Itemset - HUI*) nếu $U(X) \geq minUtil$. Trong đó $minUtil$ là giá trị ngưỡng độ hữu ích tối thiểu.

$$HUIs = \{X \subseteq I \mid U(X) \geq minUtil\} [17]$$

Ví dụ: trong Bảng 4, $U(ec) = 33$. Với $minUtil = 32$ thì tập mục $\{fe\}$ là một HUI. Tập HUI được tìm thấy trên cơ sở dữ liệu là: $\{adc, fbec, fe, fec, dbe, dbec, bec, ec\}$.

4.2. Xây dựng DUL

Phần này sẽ minh họa cách xây dựng các *DUL* một phần tử (1-DUL), hai phần tử (2-DUL) và k phần tử (k-DUL) với $k \geq 3$ trong cơ sở dữ liệu D (sau khi sắp tăng dần theo *TWU* trong bảng 4).



Hình 2. DUL của các tập mục có 1 phần tử, 2 phần tử và 3 phần tử

4.2.1 Xây dựng DUL có 1 phần tử

DUL một phần tử được xây dựng bằng cách quét cơ sở dữ liệu trong bảng 4, tìm các giao dịch có chứa phần tử đó và tính các giá trị PU và RPU tương ứng. Sau đó, giao dịch này được đưa vào danh sách các transaction bên dưới của DUL, tính lại NEU và NRU. Lưu ý rằng các DUL một phần tử có các giá trị CU/CRU/CPU/NPU bằng 0 vì $|X| = 1$ và phần tiền tố là rỗng.

Ví dụ: $DUL(a)$ gồm 3 bộ tương ứng với các giao dịch T_3, T_5, T_6 . Bộ T_3 có $PU(a, T_3) = 5, RPU(a, T_3) = 23$; bộ T_5 có $PU(a, T_5) = 5, RPU(a, T_5) = 10$; bộ T_6 có $PU(a, T_6) = 10, RPU(a, T_6) = 9$. $NEU(a) = 5 + 5 + 10 = 20$; $NRU(a) = 23 + 10 + 9 = 42$. Tương tự cho các DUL khác.

4.2.2 Xây dựng DUL có 2 phần tử

Một DUL hai phần tử được xây dựng bằng cách kết hợp 2 DUL một phần tử. Giả sử cần xây dựng $DUL(af)$, ta cần có $DUL(a)$ và $DUL(f)$. Quá trình xây dựng $DUL(af)$ như sau:

Đầu tiên, khởi tạo $DUL(af)$ từ $DUL(a)$ và $DUL(f)$ với các thông tin chung như sau: $NPU(af) = 0; NEU(af) = 0; NRU(af) = 0; CU(af) = 0; CRU(af) = 0; CPU(af) = 0$; và danh sách các bộ Tid bên dưới của $DUL(af)$ là rỗng.

Ý tưởng của thuật toán là dựa trên Diffset nêu các giao dịch xuất hiện trong $DUL(af)$ phải là các giao dịch có chứa trong $DUL(a)$ và không chứa trong $DUL(f)$. Vì vậy, thực hiện duyệt lần lượt các Tid trong $DUL(a)$, nếu Tid này không có trong $DUL(f)$ thì 1 bộ $< Tid, PU(af, Tid), RPU(af, Tid) >$ sẽ được đưa vào $DUL(af)$. Ngược lại, nếu Tid đang xét có trong cả hai $DUL(a)$ và $DUL(f)$ thì xem xét tập mục $\{af\}$ là đóng hay không đóng trong giao dịch đó. Nếu đóng thì cập nhật lại các giá trị CU/CRU/CPU, nếu không đóng thì cập nhật lại các giá trị NPU/NEU/NRU. Trong ví dụ này, T_3 và T_5 có trong danh sách Tid của cả hai

$DUL(a)$ và $DUL(f)$, nhưng $\{af\}$ trong T_3 là đóng, af trong T_5 là không đóng. Do đó $CU(af) = PU(a, T_3) + PU(f, T_3) = 11$, $CRU(af) = RPU(f, T_3) = 17$, $CPU(af) = PU(a, T_3) = 5$; $NPU(af) = PU(a, T_5) = 5$, $NEU(af) = PU(f, T_5) = 2$, $NRU(af) = RPU(f, T_5) = 8$. Riêng T_6 có trong danh sách Tid của $DUL(a)$ và không có trong danh sách Tid của $DUL(f)$ nên danh sách Tid của $DUL(af)$ có chứa T_6 với $PU(af, T_6) = 10$ và $RPU(af, T_6) = 9$. Tương tự cho các DUL khác.

4.2.3 Xây dựng DUL có k phần tử ($k \geq 3$)

Một DUL có k phần tử được xây dựng bằng cách kết hợp từ 2 DUL của $(k-1)$ phần tử có chung tiền tố. Giả sử cần xây dựng $DUL(afd)$, ta cần có $DUL(af)$ và $DUL(ad)$. Quá trình xây dựng $DUL(afd)$ như sau:

Đầu tiên, khởi tạo $DUL(afd)$ từ $DUL(af)$ và $DUL(ad)$ với các thông tin chung như sau: $NPU(afd) = 7$; $NEU(afd) = 6$; $NRU(afd) = 3$; $CU(afd) = 19$; $CRU(afd) = 9$; $CPU(afd) = 11$; và danh sách các bộ Tid bên dưới của $DUL(afd)$ là rỗng.

Các giao dịch xuất hiện trong $DUL(afd)$ phải là các giao dịch có chứa $\{af\}$ nhưng không chứa $\{d\}$. Do đó, để tìm các Tid này, thực hiện duyệt lần lượt các Tid trong $DUL(ad)$, nếu Tid này không có trong danh sách Tid của $DUL(af)$ thì 1 bộ $< Tid, PU(afd, Tid), RPU(afd, Tid) >$ sẽ được đưa vào $DUL(afd)$ và tính lại các giá trị $NPU(afd) = NPU(afd) - PU(afd, Tid)$. Ngược lại, duyệt lần lượt các Tid có trong $DUL(af)$, nếu Tid này không có trong $DUL(ad)$ thì tính lại các giá trị $NEU(afd) = NEU(afd) - PU(ad, Tid)$, $NRU(afd) = NRU(afd) - RPU(ad, Tid)$. Trong ví dụ này, T_5 có trong $DUL(ad)$ và không có trong $DUL(af)$. Do đó, 1 bộ $< 5, 7, 8 >$ được đưa vào $DUL(afd)$ và tính lại $NPU(afd) = NPU(afd) - PU(afd, T_5) = 0$. Đồng thời, giao dịch T_6 chỉ có trong $DUL(af)$ mà không có trong $DUL(ad)$ nên $NEU(afd) = NEU(afd) - PU(d, T_6) = 0$, $NRU(afd) = NRU(afd) - RPU(d, T_6) = 0$.

4.3. Các chiến lược tia

Trong các bài toán khai thác tập hữu ích cao, các chiến lược tia đóng vai trò rất quan trọng trong việc nâng cao hiệu suất của thuật toán nhờ khả năng thu hẹp không gian tìm kiếm; từ đó tối ưu thời gian thực thi và không gian lưu trữ. Trong bài báo này, hai chiến lược tia U-Prune và EUCS-Prune [15] được sử dụng để tăng hiệu suất thực thi của thuật toán.

Chiến lược 1 (U-Prune): Nếu tổng độ hữu ích của tập mục X và tổng độ hữu ích của các mục sau X nhỏ hơn $minUtil$ thì mọi tập mở rộng từ X đều không phải là HUI. Nghĩa là nếu $U(X) + RU(X) < minUtil$ thì $\forall Y \supseteq X, Y \notin HUI$. Khi đó ngừng mở rộng với tập mục X . [15]

Chiến lược 2 (EUCS-Prune): Xét X, Y là hai tập mục 1 phần tử, Nếu $TWU(X, Y) < minUtil$ thì tập mục XY không phải là HUI và mọi tập mở rộng từ XY cũng không phải là HUI. Khi đó dừng mở rộng với tập mục XY . [15]

4.4. Thuật toán DCHUIM

Trong bài báo này, thuật toán *DCHUIM* được đề xuất để khai thác tập hữu ích cao. Thuật toán chính *DCHUIM* có dữ liệu đầu vào là cơ sở dữ liệu giao dịch D và ngưỡng độ hữu ích tối thiểu $minUtil$. Kết quả đầu ra của thuật toán là tập hữu ích cao thỏa ngưỡng $minUtil$. Đầu tiên thuật toán quét cơ sở dữ liệu D để tính giá trị $TWU(i)$ cho mỗi mục i có trong cơ sở dữ liệu. Sau đó, loại bỏ các mục i có $TWU(i) < minUtil$ khỏi tập I và chỉ đưa các mục i thỏa điều kiện vào I^* . Sau đó tiến hành sắp xếp tập I^* tăng dần theo TWU và sắp xếp lại các mục trong D theo thứ tự của I^* (dòng 3). Tại dòng 4, thực hiện tính các giá trị cho cấu trúc *EUCS*.

Quét cơ sở dữ liệu D lần 2 và tạo danh sách các DUL cho mỗi phần tử $i \notin I^*$ (Dòng 5). Cuối cùng, gọi thuật toán *MiningDCHUI* để khai thác tập hữu ích cao với ngưỡng $minUtil$.

Thuật toán 1: Thuật toán chính – DCHUIM

Vào: D : Cơ sở dữ liệu giao dịch, $minUtil$: Ngưỡng độ hữu ích tối thiểu

Ra: $HUIs$: Tập mục hữu ích cao

1. Quét cơ sở dữ liệu D để tính $TWU(i)$ cho mỗi mục i có trong I .
2. Tính $I^* = \{i \in I \mid TWU(i) \geq minUtil\}$, loại khỏi D các mục $i \notin I^*$.
3. Sắp xếp I^* tăng theo TWU , sắp xếp các mục trong D theo thứ tự của I^* .
4. Khởi tạo cấu trúc $EUCS$
5. Quét cơ sở dữ liệu D để tạo danh sách DUL cho mỗi phần tử $i \notin I^*$ là $oneULs$
6. *MiningDCHUI*($\emptyset, oneULs, minUtil$)

Thuật toán 2 (*MiningDCHUI*) có dữ liệu đầu vào gồm một P với vai trò tiền tố, một danh sách các DUL là $oneULs$ và $minUtil$. Từ dòng 1 đến dòng 5, thuật toán duyệt qua tất cả các $DUL X$ trong danh sách $oneULs$ và kiểm tra điều kiện nếu $U(X) = X.NPU + X.NEU + X.CU \geq minUtil$ thì đưa X vào tập $HUIs$. Dòng 6 kiểm tra điều kiện mở rộng bằng cách áp dụng chiến lược tia U-Prune. Dòng 7 gọi hàm *twoULConstruct* để tạo ra các DUL có 2 phần tử ($twoULs$). Dòng 9 thực hiện gọi hàm *Hui_diffset_Miner* để tiếp tục khai thác $HUIs$ trên $twoULs$.

Thuật toán 2: MiningDCHUI

Vào: P : tiền tố; $oneULs$: Danh sách các DUL có tiền tố là P , $minUtil$: Ngưỡng độ hữu ích tối thiểu

Ra: $HUIs$: Tập mục hữu ích cao

1. **for** each position i in $oneULs$ **do**
2. $X = oneULs[i]$;
3. **if** $X.NPU + X.NEU + X.CU \geq minUtil$ **then**
4. $HUIs \leftarrow X$
5. **end if**
6. **if** $(X.NPU + X.NEU + X.CU + X.NRU + X.CRU \geq minUtil)$ **then** //U-Prune
7. $twoULs \leftarrow twoULConstruct(X, oneULs, i, minUtil)$; // DUL có 2 phần tử
8. $P = \{P \cup X.item\}$;
9. $Hui_diffset_Miner(P, twoULs, minUtil)$;
10. **end if**
11. **end for**

Thuật toán 3 (*Hui_diffset_Miner*) có dữ liệu đầu vào gồm một P với vai trò tiền tố, một danh sách các DUL là $twoULs$ và $minUtil$. Từ dòng 1 đến dòng 5, thuật toán duyệt qua tất cả các $DUL X$ trong danh sách $twoULs$ và kiểm tra điều kiện nếu $U(X) = X.NPU + X.NEU + X.CU \geq minUtil$ thì đưa X vào tập $HUIs$. Dòng 6 kiểm tra điều kiện mở rộng bằng cách áp dụng chiến lược tia U-Prune. Dòng 7 gọi hàm *kULConstruct* để tạo ra các DUL có k phần tử ($kULs$), với $k \geq 3$. Dòng 9 gọi đệ quy hàm *Hui_diffset_Miner* để tiếp tục khai thác $HUIs$ trên $kULs$.

Thuật toán 3: Hui_diffset_Miner

Vào: P : tiền tố; $twoULs$: Danh sách các DUL có tiền tố là P , $minUtil$: Ngưỡng độ hữu ích tối thiểu

Ra: $HUIs$: Tập mục hữu ích cao

1. **for** each position i in $twoULs$ **do**
2. $X = twoULs[i]$;

```

3.   if  $X.NPU + X.NEU + X.CU \geq minUtil$  then
4.        $HUIs \leftarrow X;$ 
5.   end if
6.   if  $(X.NPU + X.NEU + X.CU + X.NRU + X.CRU \geq minUtil)$  then//U-Prune
7.        $kULs \leftarrow kULConstruct(X, twoULs, i, minUtil);$  // DUL có k phần tử
8.        $P = \{P \cup X.item\};$ 
9.        $Hui\_diffset\_Miner(P, kULs, minUtil);$ 
10.  end if
11. end for

```

Thuật toán 4 (*twoULConstruct*) có dữ liệu đầu vào gồm 1 *DUL* tiền tố X , một danh sách các *DUL* là tập *oneULs*, st: vị trí bắt đầu và *minUtil*. Từ dòng 1 đến 8, thuật toán duyệt qua các *oneULs* Y sau X , nếu $EUCS(X, Y)$ lớn hơn *minUtil* thì khởi tạo một *DUL*(XY) mở rộng từ X và đưa vào tập *twoULs*. Dòng 9 dùng *extSz* để lưu trữ số lượng *DUL* của tập *twoULs*. Tiếp theo, từ dòng 11 đến dòng 24, thuật toán duyệt lần lượt từng *Tid* trong X , nếu *Tid* này có xuất hiện trong *DUL* nào của tập *twoULs* thì thêm vị trí của *DUL* này vào *newT*, ngược lại thêm bộ dữ liệu tương ứng của *Tid* này vào *DUL* đang xét. Từ dòng 25 đến dòng 41, thuật toán kiểm tra nếu tập mục XY là đóng thì cập nhật các giá trị *CU/CRU/CPU*, ngược lại cập nhật các giá trị *NPU/NEU/NRU*. Dòng 43 trả về kết quả là tập *twoULs*.

Thuật toán 4: *twoULConstruct*

Vào: X : *DUL* tiền tố; tập *oneULs*; st: vị trí bắt đầu; *minUtil*: Ngưỡng độ hữu ích tối thiểu.

Ra: *twoULs*: tập *DUL* có 2 phần tử.

```

1. for  $i = st + 1$  to oneULs.size-1 do
2.      $Y = oneULs[i];$  //Y sau X
3.     if  $EUCS(X.item, Y.item) \geq minUtil$  then //Chiến lược tia EUCS
4.         Initial newUL( $Y.item$ ); //Khởi tạo một DUL mới mở rộng từ X
5.          $twoULs \leftarrow newDUL;$ 
6.          $ey\_tid[i] = 0;$  //đánh dấu vị trí tid trong newDUL
7.     end if
8. end for
9. extSz = twoULs.size;
10. newT = null;
11. for each ex in  $X.tidList$  do
12.     for  $j = 0$  to twoULs.size - 1 do
13.         if twoULs[j] = null then
14.             continue;
15.         end if
16.         eylist = oneULs[twoULs[j].item].tidList;
17.         while  $ey\_tid[j] < eylist.size$  and  $eylist[ey\_tid[j]].tid < ex.tid$  do
18.              $ey\_tid[j] += 1;$ 
19.             if  $ey\_tid[j] < eylist.size$  and  $eylist[ey\_tid[j]].tid = ex.tid$  then
20.                 newT  $\leftarrow j;$ 
21.             else
22.                 twoULs[j].tidList  $\leftarrow ex;$ 
23.             end if
24.         end for
25.         if newT.size = extSz then
26.             for  $j = 0$  to newT.size - 1 do
27.                 ey = oneULs[twoULs[j].item];
28.                 eyy = ey.tidList[ey\_tid[newT[j]]];

```

```

29.           twoULs[newT[j]].CU += ex.PU + eyy.PU;
30.           twoULs[newT[j]].CRU += eyy.RPU;
31.           twoULs[newT[j]].CPU += ex.PU;
32.       end for
33.   else
34.       for j = 0 to newT.size - 1 do
35.           ey = oneULs[twoULs[j].item];
36.           eyy = ey.tidList[ey.tid[newT[j]]];
37.           twoULs[newT[j]].NPU += ex.PU;
38.           twoULs[newT[j]].NEU += eyy.PU;
39.           twoULs[newT[j]].NRU += eyy.RPU;
40.       end for
41.   end if
42. end for
43. return twoULs;

```

Thuật toán 5 (*kULConstruct*) có dữ liệu đầu vào gồm 1 *DUL* tiền tố *X*, một danh sách các *DUL* là tập *twoULs*, st: vị trí bắt đầu và *minUtil*. Đầu tiên thuật toán khởi tạo tập *kULs* có số phần tử bằng với số phần tử của tập *twoULs*. Tiếp theo, thực hiện mở rộng *X* với các *Y* sau *X* và cập nhật vào *kULs* tương ứng. Từ dòng 4 đến dòng 9, thuật toán gán các giá trị *NPU/NEU/NRU/CU/CRU/CPU* ban đầu; sử dụng *preX* và *preY* - là 2 *DUL* ở mức 1 phần tử tương ứng với *X* và *Y*. Từ dòng 12 đến dòng 19, duyệt lần lượt từng phần tử *ey* ∈ *Y* và tìm *ex* ∈ *X* sao cho *ex.tid* = *ey.tid*. Nếu không thấy, tìm bộ *x* ∈ *preX* sao cho *x.tid* = *ey.tid*; tạo phần tử *exy* kết hợp từ *x* và *ey* (dòng 14, 15); thêm bộ *exy* vào *DUL(XY)*; đồng thời cập nhật lại giá trị *NPU*. Từ dòng 20 đến dòng 27, duyệt lần lượt từng phần tử *ex* ∈ *X* và tìm *ey* ∈ *Y* sao cho *ex.tid* = *ey.tid*. Nếu không thấy, tìm bộ *y* ∈ *preY* sao cho *y.tid* = *ex.tid*; cập nhật lại giá trị *NEU, NRU*. Dòng 28 loại bỏ các *DUL* rỗng ở mức k phần tử. Dòng 29 trả về tập *kULs*.

Thuật toán 5: *kULConstruct*

Vào: *X*: *DUL* tiền tố; tập *twoULs*; st: vị trí bắt đầu; *minUtil*: Ngưỡng độ hữu ích tối thiểu.

Ra: *kULs*: tập *DUL* có k phần tử.

1. Khởi tạo tập *kULs* có số phần tử ban đầu bằng số phần tử của *twoULs*
2. **for** *i* = *st* + 1 to *twoULs.size* – 1 **do**
3. *Y* = *twoULs[i]*; //Y sau X
4. *kULs[i].NPU* = *X.NPU* + *X.NEU*;
5. *kULs[i].NEU* = *Y.NEU*;
6. *kULs[i].NRU* = *Y.NRU*;
7. *kULs[i].CU* = *X.CU* + *Y.CU* – *X.CPU*;
8. *kULs[i].CRU* = *Y.CRU*;
9. *kULs[i].CPU* = *X.CU*;
10. *preX* = *oneULs[X.item]*;
11. *preY* = *oneULs[Y.item]*;
12. **for each element** *ey* in *Y* **do**
13. **if** ! $\exists ex \in X \wedge ex.tid = ey.tid$ **then**
14. Tìm bộ *x* ∈ *preX* sao cho *x.tid* = *ey.tid*;
15. *exy* = <*ey.tid, ey.PU + x.PU, x.RPU*>;
16. *kULs[i] ← exy*;
17. *kULs[i].NPU* -= *exy.PU*;
18. **end if**
19. **end for**

```

20.   for each element ex in X do
21.       if !  $\exists ey \in Y \wedge ey.tid = ex.tid$  then
22.           Tìm bộ y  $\in preY$  sao cho y.tid = ex.tid
23.           kULs[i].NEU -= y.PU;
24.           kULs[i].NRU -= y.RPU;
25.       end if
26.   end for
27. end for
28. Loại bỏ các kULs rỗng
29. return kULs;

```

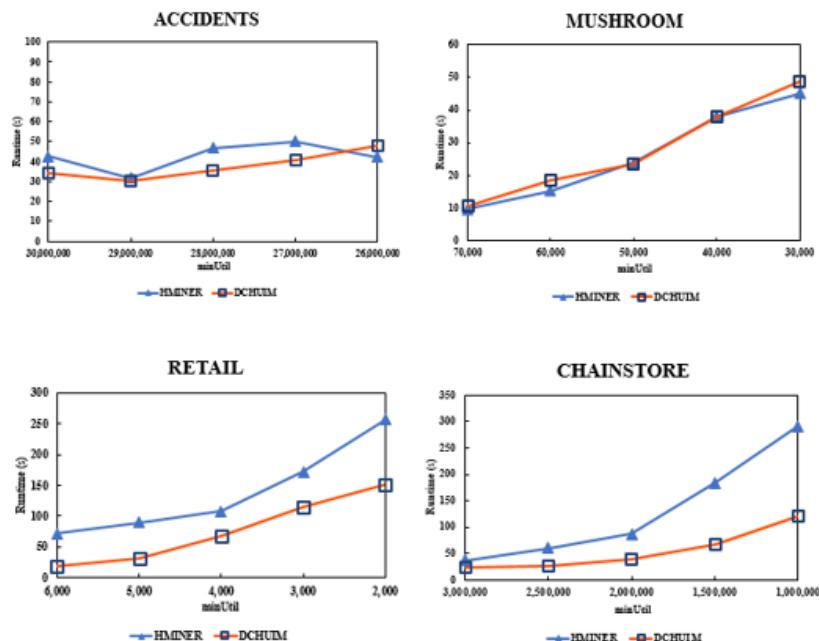
5. THỰC NGHIỆM

Thực nghiệm được tiến hành để đánh giá những đề xuất trong thuật toán *DCHUIM*. Thuật toán được cài đặt bằng ngôn ngữ Java, chạy thực nghiệm trên máy tính HP 14-bs1 với cấu hình Intel Core i5-8250 CPU @1.6GHz, bộ nhớ RAM 8GB và hệ điều hành Windows 10. Thuật toán sử dụng bộ dữ liệu chuẩn dùng trong các tài liệu khai thác HUI, được tải từ thư viện SPMF [18] gồm: Accidents, Mushroom, Retail và Chainstore. Các bộ dữ liệu này có đầy đủ đặc tính thể hiện các loại dữ liệu khác nhau như thưa, dày và có độ dài các giao dịch khác nhau. Thông tin mô tả các bộ dữ liệu được trình bày trong bảng 5. Kết quả thực nghiệm của thuật toán *DCHUIM* được so sánh với thuật toán hiệu quả nhất gần đây là *HMiner* [17] dựa trên đánh giá về thời gian thực thi và bộ nhớ sử dụng.

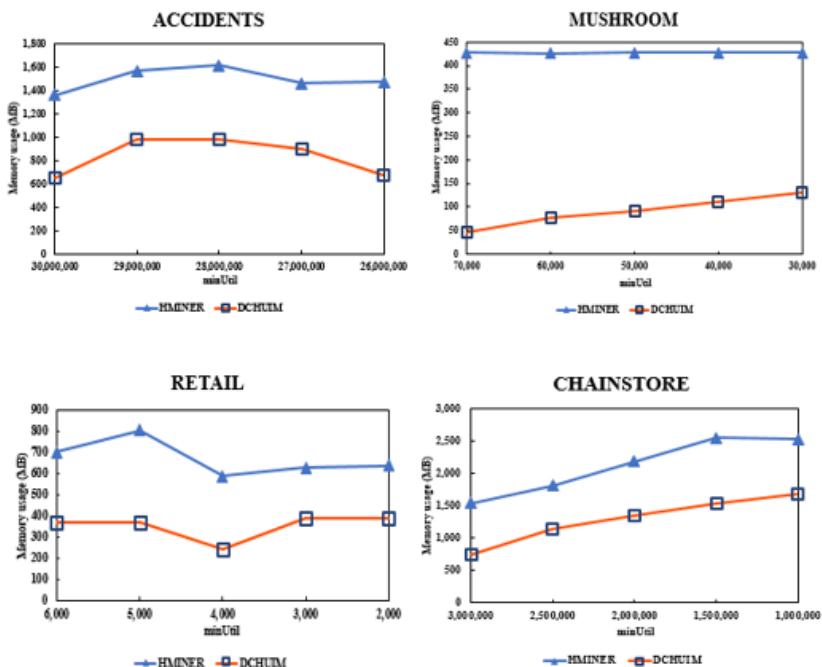
Bảng 5. Đặc điểm các cơ sở dữ liệu thực nghiệm

Cơ sở dữ liệu	Số lượng giao dịch	Số lượng mục (I)	Độ dài trung bình (A)	Độ dày (A/I) %
Accidents	340,183	468	33.8	7.2222
Mushroom	8,124	119	23	19.3277
Retail	88,162	16,470	10.3	0.0625
Chainstore	1,112,949	46,086	7.3	0.0158

Hình 3. so sánh hiệu suất của thuật toán đề xuất *DCHUIM* và thuật toán *HMiner* về thời gian thực thi trên 4 cơ sở dữ liệu *Accidens*, *Mushroom*, *Retail* và *Chainstore*. Với cơ sở dữ liệu có độ dày cao (*Accidents*) thì thời gian thực thi của thuật toán *HMiner* và thuật toán *DCHUIM* gần như tương đương nhau. Cụ thể với cơ sở dữ liệu *Accidents*, tại các ngưỡng *minUtil* = 27.000 đến *minUtil* = 30.000 thời gian thực thi của thuật toán đề xuất là thấp hơn so với thuật toán *HMiner*. Tuy nhiên, khi ngưỡng *minUtil* giảm xuống đến 26000 thì thời gian thực hiện của thuật toán *DCHUIM* có tăng hơn một chút so với *HMiner*. Với cơ sở dữ liệu có độ dày trung bình là *Mushroom*, hai thuật toán này có thời gian thực thi xấp xỉ bằng nhau. Với cơ sở dữ liệu thưa *Retail*, thời gian thực thi của thuật toán *DCHUIM* nhanh hơn gần như gấp đôi so với thuật toán *HMiner* tại tất cả các ngưỡng *minUtil* từ 2000 đến 6000. Với cơ sở dữ liệu thưa *Chainstore*, thuật toán *DCHUIM* có thời gian thực hiện trung bình là 55.35 giây, trong khi thuật toán *HMiner* có thời gian thực hiện cao hơn là 132.27 giây. Đồng thời, trong cơ sở dữ liệu *Chainstore*, càng giảm ngưỡng *minUtil* thì thuật toán *DCHUIM* càng hiệu quả. Kết quả này cho thấy cấu trúc *DUL* được đề xuất thực sự mang lại hiệu quả cao và các chiến lược tia được áp dụng trong thuật toán *DCHUIM* đã giúp thu hẹp đáng kể không gian tìm kiếm, từ đó làm tăng hiệu suất thực thi của thuật toán, đặc biệt là trên các cơ sở dữ liệu thưa. Đối với cơ sở dữ liệu dày, thời gian thực thi của *DCHUIM* là xấp xỉ so với *HMiner*.



Hình 3. So sánh thời gian thực thi



Hình 4. So sánh bộ nhớ sử dụng

Hình 4 so sánh bộ nhớ sử dụng giữa 2 thuật toán *DHUIM* và *HMiner* trên 4 cơ sở dữ liệu là *Accidents*, *Mushroom*, *Retail* và *Chainstore*. Kết quả cho thấy đối với cơ sở dữ liệu *Accidents*, dung lượng bộ nhớ của *DCHUIM* chỉ bằng một nửa so với *HMiner*. Với cơ sở dữ liệu *Mushroom*, bộ nhớ của *HMiner* gấp gần 10 lần so với *DCHUIM*. Với cơ sở dữ liệu *Retail* và *Chainstore*, bộ nhớ của thuật toán *DCHUIM* cũng chỉ chiếm một nửa so với thuật toán *HMiner*. Như vậy, dữ liệu thực nghiệm cho thấy ở cả cơ sở dữ liệu dày (*Accidents*,

Mushroom) lẩn cơ sở dữ liệu thưa (Retail, Chainstore), bộ nhớ sử dụng của thuật toán *DHUIM* tốt hơn rất nhiều so với thuật toán *HMiner* ở mọi ngưỡng so sánh. Lý do là thuật toán *DCHUIM* chỉ lưu trữ các giao dịch Diffset mà không phải lưu trữ các giao dịch Tidset, dẫn đến dung lượng bộ nhớ được giảm đi một cách đáng kể.

6. KẾT LUẬN

Trong bài báo này, một cấu trúc mới có tên là *DUL* đã được đề xuất để khai thác tập hữu ích cao trên cơ sở dữ liệu giao dịch thông qua thuật toán *DCHUIM*. Cấu trúc này lưu trữ các giao dịch Diffset thay vì lưu trữ các giao dịch Tidset; đồng thời, thuật toán cũng áp dụng các chiến lược tia hiệu quả như *U-Prune*, *TWU-Prune*, *EUCS-Prune* để tối ưu không gian lưu trữ trong quá trình khai thác. Kết quả thực nghiệm cho thấy thuật toán *DCHUIM* có thời gian thực thi nhanh hơn thuật toán *HMiner* ở các cơ sở dữ liệu thưa. Bộ nhớ sử dụng của thuật toán *DCHUIM* cũng tốt hơn thuật toán *HMiner* ở tất cả các cơ sở dữ liệu và ở mọi ngưỡng độ hữu ích tối thiểu.

Hướng phát triển tiếp theo của nghiên cứu này là cải tiến hoặc áp dụng thêm các chiến lược tia khác nhằm nâng cao hơn hiệu suất thực thi trên các cơ sở dữ liệu có độ dày cao.

TÀI LIỆU THAM KHẢO

1. Grahne G. and Zhu J. - Fast algorithms for frequent itemset mining using FP-Trees, IEEE Transactions on Knowledge and Data Engineering **17** (2015) 1347-1362.
2. Han J., Pei J. and Yin Y. - Mining frequent patterns without candidate generation, ACM Sigmod Record **29** (2000) 1-12.
3. Vo B., Le T., Coenen F., Hong T. P. - Mining frequent itemsets using the N-list and subsume concepts, International Journal of Machine Learning and Cybernetics **7** (2016) 253–265.
4. Agrawal, R. and Srikant, R. - Fast Algorithms for Mining Association Rules in large databases, VLDB **20** (1994) 487-499.
5. Zaki M., Parthasarathy S., Ogihara M. and Li W. - New algorithms for fast discovery of association rules, Knowledge Discovery and Data Mining (1997) 283-286.
6. Vo B., Hong T. P. and Le B. - A lattice-based approach for mining most generalization association rules, Knowledge-Based Systems **45** (2013) 20-30.
7. Nasr M., Hamdy M., Hegazy D. and Bahnasy K. - An efficient algorithm for unique class association rule mining, Expert Systems with Applications **164** (2021).
8. Yao H., Hamilton H. J. and Butz C. J. - A foundational approach to mining Itemset Utilities from Databases, Proceedings SIAM International Conference on Data Mining (2004) 482 – 486.
9. Le B., Nguyen H. and Vo B. - An efficient strategy for mining high utility itemsets, International Journal of Intelligent Information and Database Systems **5** (2011) 164-176.
10. Liu Y., Liao W. and Choudhary A. - A Two-Phase Algorithm for Fast Discovery of High Mining Itemsets, PAKDD (2005) 689-695.
11. Tseng V.S., Wu C.W., Shie B.E. and Yu P.S. - UP-Growth: an efficient algorithm for high utility itemset mining, KDD (2010) 253-262.

12. Tseng V. S., Shie B. -E., Wu C. -W. and Yu P. S. - Efficient Algorithms for Mining High Utility Itemsets from Transactional Databases, IEEE Transactions on Knowledge and Data Engineering **25** (2013) 1772-1786.
13. Liu J., Wang K. and Fung B. C. M. - Direct Discovery of High Utility Itemsets without Candidate Generation, IEEE 12th International Conference on Data Mining (2012) 984-989.
14. Wu C. W., Fournier-Viger P., Gu J. Y. and Tseng V. S. - Mining high utility itemsets without candidate generation, CIKM (2012) 55-64.
15. Fournier-Viger P. , Wu C. W., Zida S. and Tseng V. S. - FHM: Faster high-utility itemset mining using estimated utility co-occurrence pruning, International Symposium on Methodologies for Intelligent Systems **8502** (2014) 83-92.
16. Zida S., Fournier-Viger P., Lin J. C. W., Wu C. W. and Tseng V. S. - EFIM: A Highly Efficient Algorithm for High-Utility Itemset Mining, Knowledge and Information Systems **51**(2017) 595-625.
17. Krishnamoorthy S. - HMiner: Efficiently mining high utility itemsets, Expert Systems with Applications (2017) 168-183.
18. Fournier-Viger P., Gomariz A., Soltani A. and Lam H. - An Open-Source Data Mining Library, (2014). [Online]. Available: <http://www.philippe-fournier-viger.com>.

ABSTRACT

MINING HIGH UTILITY ITEMSETS BASED ON DIFFSET MECHANISM

Nguyen Thi Thanh Thuy^{1,*}, Nguyen Van Le¹, Manh Thien Ly¹

¹*Ho Chi Minh City University of food industry*

*Email: thuyntt@hufi.edu.vn

High utility itemsets (HUIs) mining is the finding of itemsets that satisfy a user-defined minimum usefulness threshold. There have been many effective studies in the field of high utility itemset mining, but these studies are all based on the Tidset approach. In this paper, we propose the DCHUIM algorithm to mine high utility itemset based on the Diffset approach. To do this, a DUL data structure is proposed to store utilities information and subtraction transactions of an itemset. In addition, the algorithm also applies pruning strategies such as U-Prune, EUCS-Prune and the concept of closed utility to effectively compress data. Hence, the search space is significantly reduced in the mining process. Experiment on large datasets including Accidents, Mushroom, Retail, Chainstore and compare the performance of DCHUIM algorithm with HMiner algorithm, which is the most effective algorithm in the field of HUIs mining recently. The results show that the DCHUIM algorithm has better performance than the HMiner algorithm in terms of time on sparse databases and is superior in terms of memory usage on all databases.

Keywords: Frequent pattern mining, High utility itemsets mining, Transaction database.

MÔ HÌNH CÁ NHÂN HÓA NGƯỜI HỌC TRÊN CƠ SỞ LOGIC MỜ ỨNG DỤNG TRONG HỆ THỐNG HỌC MỞ

Hoàng Xuân Bách^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: bachhx@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Nghiên cứu này đưa ra đề xuất mô hình người dùng xây dựng trên cơ sở lý thuyết logic ứng dụng trong cá nhân hóa cho hệ thống học mở. Với việc ứng dụng logic mờ, mô hình đáp ứng tiêu chí đơn giản, dễ dàng sử dụng, và phản ánh tốt thế giới thực, sẽ đem lại hiệu quả tốt hơn cho hệ thống học mở trong việc “hiểu” người dùng hơn.

Từ khóa: Fuzzy model, cá nhân hóa, hệ thống học mở, MOOC.

1. MỞ ĐẦU

Hệ thống học mở (Massively Open Online Learning systems, or MOOCs) cung cấp nội dung trực tuyến có thể truy cập rộng rãi trên toàn thế giới, điển hình bao gồm videos, bài đọc, câu đố cùng với các công cụ giao tiếp xã hội trên một nền tảng cho phép người tham gia học theo tốc độ của riêng họ (1). Số lượng dữ liệu và số lượng học viên đăng ký và tham dự các khóa học đang tăng theo cấp số nhân. Do đó, yêu cầu đặt ra là cần phải xây dựng tính cá thể hóa cho các nền tảng MOOC để tạo ra sự kết nối tốt hơn giữa dữ liệu và người học.

MOOCs hướng tới việc tự học, cũng có nghĩa rằng hệ thống phải gợi ý được cho người dùng phải học môn nào thì phù hợp với người dùng, học môn nào thì cần thiết cho người dùng, hay nói cách khác MOOCs phải cá thể hóa được người dùng. Việc cá thể hóa người dùng được thực hiện bằng mô hình hóa người dùng với các chiều thông tin khác nhau về người dùng và mối quan hệ giữa các chiều thông tin đó như: năng lực của người dùng trong từng lĩnh vực, mối quan tâm của người dùng, yêu cầu tìm kiếm hiện tại, mục tiêu lâu dài, v.v.

Để biểu diễn quan hệ giữa các thông tin một cách đơn giản nhất, đảm bảo phản ánh quy luật khách quan, ta dùng biểu diễn với tập mờ (fuzzy sets) và mô hình mờ (fuzzy logic models). Việc ứng dụng logic mờ trong cá thể hóa MOOC có thể hiểu xây dựng mô hình mờ biểu diễn mối quan hệ giữa người học và các tài liệu, khóa học.

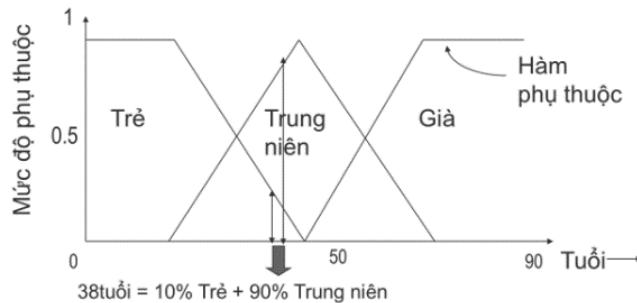
2. TẬP MỜ VÀ MÔ HÌNH MỜ

2.1. Tập mờ (Fuzzy sets)

Thực tế khách quan luôn là “mờ”. Khi chúng ta vào một lớp học hỏi các sinh viên “ai thích học về trí tuệ nhân tạo?”, chúng ta sẽ nhận được danh sách các bạn giơ tay lên. Nhưng liệu trong danh sách đó có phải ai cũng sẽ “hoàn toàn” thích môn trí tuệ nhân tạo? và ngược lại có phải số còn lại là “ghét” môn trí tuệ nhân tạo? Như vậy nếu biểu diễn tập hợp theo lý

thuyết tập hợp truyền thống thì sẽ không phải ánh đúng bản chất khách quan, trong trường hợp này là không thể tách biệt rõ ràng giữa hai tập hợp “thích trí tuệ nhân tạo” và “không thích trí tuệ nhân tạo”. Nói cách khác phải có biểu diễn “mờ” cho các tập hợp này. Đó chính là cơ sở tư duy cho lý thuyết tập mờ được khởi xướng bởi Zadeh L.A.

Một tập mờ S được xác định trên tập nền U, khi đó mỗi điểm x thuộc tập U sẽ được gán tương ứng với một hàm phụ thuộc μ có giá trị trong khoảng 0 và 1 (2).

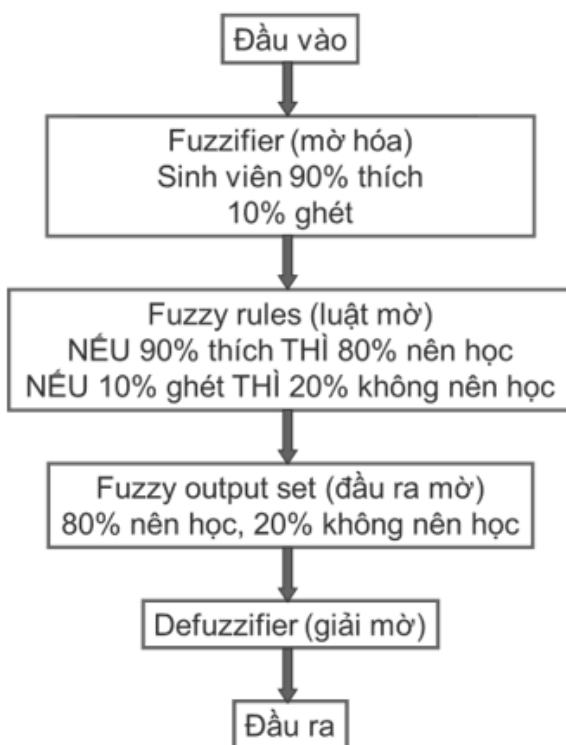


Hình 1. Tập mờ theo độ tuổi

Với lý thuyết tập mờ Fuzzy sets, khi biểu diễn một sinh viên thích hay không học về trí tuệ nhân tạo, có thể sẽ biểu diễn ở dạng: sinh viên A là 60% thuộc tập hợp “thích học trí tuệ nhân tạo” và 40% thuộc tập hợp “không thích học trí tuệ nhân tạo”.

2.2. Mô hình mờ (Fuzzy model)

Mô hình mờ, còn gọi là hệ suy diễn mờ là quá trình biểu diễn dữ liệu dưới dạng tập hợp mờ và áp dụng các quy luật suy diễn để đưa ra kết quả đầu ra (2). Hình 2 trình bày ví dụ về mô hình mờ.



Hình 2. Mô hình mờ (Fuzzy model)

3. MÔ HÌNH CÁ NHÂN HÓA NGƯỜI HỌC TRONG MOOC

Cá nhân hóa người học chính là xác định mối tương quan giữa người học và các môn học, khóa học trên MOOC. Mối tương quan đó có thể là: sự quan tâm (người học A quan tâm môn học X), sự cần thiết (người học B cần học môn Y), sự thích hợp (người học C nên học môn Z). Tuy nhiên, để đơn giản, ta có thể biểu diễn chung bằng quan hệ “*quan tâm*” và gọi chung khóa học, tài liệu, môn học là “dịch vụ”. Xem xét ba mô hình biểu diễn người dùng được đề xuất trong (3).

3.1. Biểu diễn chủ quan

Trong mô hình này, người học tự quyết định mỗi “*quan tâm*” cho các dịch vụ. Có thể khả năng xây dựng thang đo quan tâm bằng cách hỏi về sự quan tâm của người học trong các lĩnh vực khác nhau. Biểu diễn truyền thống của thang đo này là thông qua con số cụ thể, mà người dùng rất khó trả lời. Đề xuất mô hình thang đo trên cơ sở logic mờ với các tập hợp là giá trị bằng lời như “rất quan tâm”, “khá quan tâm”, “quan tâm”, “sao cung được”, “không quan tâm”

Trong thực tế, người dùng xác định sự quan tâm đến “*dịch vụ*” không trực tiếp, mà thông thường thông qua một số hệ thống danh mục “*dịch vụ*”. Điều này được giải thích là do thiếu thông tin đầy đủ của người dùng về từng dịch vụ, vì vậy thường thị họ chỉ xác định được mối quan tâm tới nhóm (danh mục) dịch vụ.

Như vậy với biểu diễn chủ quan cần xác định tập mờ cho sự “*quan tâm*” của người học đến “*dịch vụ*” và tập hợp mờ các danh mục/nhóm dịch vụ.

Gọi $U = \{u_1, u_2, \dots, u_n\}$ tập người học, $S = \{s_1, s_2, \dots, s_m\}$ tập hợp các dịch vụ, $C = \{c_1, c_2, \dots, c_k\}$ – tập hợp các danh mục dịch vụ.

Khi đó xác định hàm phụ thuộc của người học tới danh mục dịch vụ là: $\mu_{interest}(u_i, c_j)$, trong đó $u_i \in U$ và $c_j \in C$.

Và tập hợp các danh mục dịch vụ với hàm phụ thuộc: $\mu_{cj}(s_i)$, trong đó $c_j \in C$ và $s_i \in S$.

Hàm phụ thuộc biểu diễn “*quan tâm*” của người dùng tới “*dịch vụ*” chính là hợp thành mờ của hai quan hệ trên.

Mô hình chủ quan chỉ biểu diễn mối “*quan tâm*” từ phía người học. Tuy nhiên, thực tế không phải lúc nào người học cũng chủ động xác định được những gì mình cần học, họ cần cả những ý kiến của chuyên gia cho biết mình cần phải học gì.

3.2. Mô hình mẫu (template model)

Mô hình mẫu xác định mối “*quan tâm*” của người học với “*dịch vụ*” dựa trên đánh giá của chuyên gia cho từng nhóm người học. Chẳng hạn nhóm người trung niên thích những môn học về cân bằng cuộc sống. Quy trình thực hiện mô hình mẫu bao gồm:

- Phân loại nhóm người học;
- Hàm phụ thuộc của người học vào nhóm người học;
- Hàm phụ thuộc dịch vụ và nhóm dịch vụ;

- Hàm phụ thuộc người học và nhóm dịch vụ (đánh giá chuyên gia);
- Tối hợp xác định hàm phụ thuộc người học và dịch vụ.

Mô hình mẫu bao gồm các tính chất quan trọng trong xây dựng cá nhân hóa, tuy nhiên chưa thể hiện được sự thay đổi “*quan tâm*” của người học theo thời gian.

3.3. Mô hình động

Mô hình động được xây dựng dựa trên các thông tin mà người học đã trao đổi với hệ thống như: đã học môn nào, học bao lâu, kết quả ra sao. Tương tự với mô hình mẫu, mô hình động sẽ được thực hiện thông qua các mô hình mờ với những quy luật mờ chẳng hạn như: nếu người học X học môn Y thì nên học môn Z.

3. KẾT LUẬN

Như vậy, với việc đưa ra ba mô hình xây dựng cá nhân hóa dựa trên logic mờ, áp dụng mô hình mờ để đến một mô hình toán học đơn giản để có thể ứng dụng vào việc cá nhân hóa MOOCs, làm cho MOOCs trở nên thông minh hơn trong phục vụ người học.

TÀI LIỆU THAM KHẢO

1. M. Bali. - MOOC pedagogy: Gleaning good practice from existing MOOCs. Journal of Online Learning and Teaching (2014).
2. Timothy J. Ross - Fuzzy logic with engineering applications, John Wiley & Sons (2010).
3. Вишняков Ю.М., Хоанг Суан Бать – Модель пользователя на основе нечеткого представления для многоканальной информационной системы, Известия ТРТУ. Тематический выпуск «Интеллектуальные САПР». -Таганрог: ТРТУ (2006) № 8.-е. 156-158

ABSTRACT

PERSONALIZATION MODEL IN MOOCs BASED ON FUZZY LOGIC

Hoang Xuan Bach^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: bachhx@hufi.edu.vn

This study proposes a user model built on the basis of applied logic theory in personalization for an open learning system. With the application of fuzzy logic, the model meets the criteria of simplicity, ease of use, and good reflection of the real world, which will bring better efficiency to MOOCs in "understanding" the user.

Keywords: fuzzy model, personalization, mooc

PHÁT HIỆN CÁC ĐỐI TƯỢNG TRONG ẢNH TẾ BÀO MÁU BẰNG KỸ THUẬT HỌC SÂU

Trần Đình Toàn^{1,*}, Nguyễn Đức Toàn²

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

²Trường Đại học Công nghệ Thông tin – DHQG Thành phố Hồ Chí Minh

*Email: toantd@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Nghiên cứu này, chúng tôi sử dụng kỹ thuật học sâu SSD và SPARSE R-CNN dựa trên ảnh tế bào máu để phát hiện các loại tế bào như hồng cầu, bạch cầu và tiểu cầu nhằm hỗ trợ bác sĩ phát hiện sự phát triển bất thường của các loại tế bào máu, qua đó chẩn đoán sớm được các bệnh như nhiễm trùng trong cơ thể, viêm họng, viêm phổi, viêm màng não và các bệnh lý khác. Khi các tế bào bạch cầu phát hiện được vi khuẩn hoặc virus gây bệnh, chúng sẽ phát triển và nhân lên để tấn công và loại bỏ vi khuẩn, virus khỏi cơ thể. Ngoài ra, việc xét nghiệm hồng cầu, bạch cầu và tiểu cầu có thể giúp bác sĩ đánh giá tổng thể về sức khỏe của bệnh nhân, chẳng hạn như mức độ thiếu máu hoặc bệnh lý liên quan đến hệ miễn dịch của cơ thể. Thực nghiệm được tiến hành trên bộ dữ liệu Blood Cell Count and Detection - BCCD (COCO) với các thuật toán SSD, SPARSE RCNN và kết hợp các hàm mất mát GIOU, Focal và L1 để giám sát, kết quả đạt được mAP lần lượt là 0.326 và 0.591.

Từ khóa: SSD, Blood Cell, SPARSE RCNN

1. MỞ ĐẦU

Các bệnh về máu là nhóm bệnh liên quan đến hệ thống tuần hoàn và sản xuất máu trong cơ thể. Bệnh về máu có thể gây ra nhiều vấn đề sức khỏe khác nhau, bao gồm suy giảm chức năng tế bào máu, tăng nguy cơ nhiễm trùng và các vấn đề về huyết áp. Các bệnh thường gặp về máu bao gồm: Thiếu máu là một căn bệnh khá phổ biến và xảy ra khi lượng tế bào hồng cầu (máu đỏ) trong cơ thể thiếu hụt, gây ra triệu chứng như mệt mỏi, hoa mắt, vàng da, suy nhược cơ thể, đặc biệt thai phụ khi bị thiếu máu sẽ tăng nguy cơ bị sinh non. Bệnh bạch cầu là bệnh liên quan đến tế bào bạch cầu (máu trắng) phát triển bất thường thành ác tính, gồm viêm tủy xương, ung thư tủy xương, bệnh bạch cầu cấp tính và bệnh bạch cầu mãn tính. Bệnh máu khác bao gồm thiếu máu bẩm sinh, bệnh Thalassemia, bệnh von Willebrand, bệnh bạch cầu loại trừ miễn dịch và bệnh Hodgkin. Thường các bệnh về máu rất khó phát hiện và dễ bị nhầm lẫn với các bệnh lý khác nên tùy thuộc vào từng loại bệnh lý, các triệu chứng mà cách điều trị có thể khác nhau. Việc giúp bác sĩ đưa ra chẩn đoán bệnh chính xác và có phác đồ điều trị kịp thời là rất quan trọng để giảm thiểu tác động của các bệnh lý này đến sức khỏe của bệnh nhân. Đó cũng là lý do tại sao việc phát hiện các tế bào máu phát triển bất thường thông qua các phương pháp xét nghiệm máu, soi đếm tế bào máu là một phương pháp chẩn đoán quan trọng và cần thiết [1–6].

2. CÁC CÔNG TRÌNH LIÊN QUAN

Từ những nghiên cứu ứng dụng máy tính đầu tiên về phát hiện đối tượng trong ảnh y khoa vào những năm 2010, học sâu đã trở thành một công cụ quan trọng trong khoa học máy tính nghiên cứu hỗ trợ lĩnh vực y khoa. Các nghiên cứu gần đây đã chứng minh rằng việc sử dụng các thuật toán học sâu trong phát hiện đối tượng trong ảnh y khoa có thể đem lại kết quả rất tốt và đáng tin cậy. Chẳng hạn như nghiên cứu của Wang cùng cộng sự đã sử dụng mô hình Faster R-CNN để phát hiện u xo tử cung [7]. Liu cùng nhóm nghiên cứu phát triển một mô hình học sâu để phát hiện bệnh nhân ung thư gan dựa trên ảnh CT [8]. Y Sharifi và nhóm nghiên cứu đã sử dụng kỹ thuật học sâu để phát hiện các khối u trong ảnh siêu âm tuyến giáp [9]. L Zhang cùng cộng sự phát triển một mô hình học sâu để phát hiện và định vị các khối u trên ảnh siêu âm buồng trứng [10]. Nghiên cứu của S Kulhare và cộng sự đã sử dụng kỹ thuật học sâu để phát hiện các khối u trên màng phổi [11]. Nhóm nghiên cứu của Bruno đã đề xuất một mô hình mạng neuron tích chập đa tầng để phân loại các khối u trực tràng trên ảnh toàn bộ lát cắt mô [12]. Huang cùng nhóm nghiên cứu sử dụng hệ thống học sâu dựa trên mạng neuron tích chập để dự đoán kết quả điều trị dựa trên dữ liệu của bệnh nhân nội trú trong thời gian thực [13].

Tác giả Ross Girshick cùng nhóm nghiên cứu đã đề xuất mạng neuron R-CNN để giải quyết dạng bài toán phát hiện đối tượng, luồng xử lý nó như sau: ban đầu ảnh được đưa qua thuật toán selective search để lọc ra 2000 region proposal có khả năng chứa đối tượng, sau đó tiến hành phân loại các region proposal có chứa đối tượng hay không (chỉ là background), tiếp đến tất cả region proposal có chứa đối tượng được resize về cùng kích thước, sau đó duỗi ra rồi dùng mô hình SVM để phân loại [14].

Fast R-CNN là cấu trúc mạng neuron đã được Ross Girshick cải tiến về mặt tốc độ so với R-CNN, nhờ vào việc sau khi cho ảnh đi qua thuật toán tìm kiếm có chọn lọc trước, fast R-CNN không tách riêng các region proposal ra khỏi ảnh gốc, mà tiếp tục đưa qua ConvNet để rút ra các feature map từ đó mới bắt đầu lấy ra các region proposal. Các region proposal này được resize về cùng kích thước bằng cách đưa qua một lớp gọi là region of interest pooling, sau cùng được đưa qua hai lớp fully connected để phân loại [15].

Faster RCNN do Shaoqing Ren cải tiến: Sử dụng pretrained model để trích xuất đặc trưng, sau đó những feature map được đưa qua một kiến trúc mạng CNN mới có tên là region proposal network để tìm các region proposal thay vì sử dụng thuật toán tìm kiếm có chọn lọc để sinh ra các anchor box, tiếp tục phân loại anchor box vừa sinh ra để xác định có chứa đối tượng hay không chưa đối tượng và tính tọa độ của anchor box gồm x_center , y_center , width, height. Tiếp tục sử dụng thuật toán Non-maximum suppression để lọc ra các anchor chồng lên nhau, kế đến thực hiện các bước tiếp theo khi đã lấy ra được region proposal để phát hiện đối tượng phần này thực hiện giống với Fast R-CNN [16].

“You Only Look Once: Unified, Real-Time Object Detection” viết tắt là YOLO của Joseph Redmon cùng nhóm nghiên cứu đề xuất là một phương pháp tiếp cận thông nhất cho việc phát hiện đối tượng thời gian thực. Phương pháp này sử dụng một mô hình mạng neuron đơn giản để xác định các vùng quan tâm (ROI) trên ảnh, dự đoán lớp và hộp giới hạn cho các đối tượng trong vùng đó [17].

RetinaNet là một mô hình phát hiện đối tượng tiên tiến được giới thiệu bởi Tsung-Yi Lin cùng nhóm nghiên cứu. Mô hình này sử dụng một kiến trúc mạng neuron sâu (deep neural network) được thiết kế để giải quyết vấn đề giảm sự chính xác của các phương pháp phát hiện đối tượng khi vật thể quá nhỏ hoặc quá lớn so với kích thước của ảnh. RetinaNet sử dụng một kiến trúc mạng neuron chuyên dụng gọi là "Feature Pyramid Network" (FPN) để tạo ra các đặc trưng đa tầng và trích xuất thông tin đối tượng. Sau đó, mô hình sử dụng một cặp lớp đầu ra được gọi là "classification subnet" và "box regression subnet" để dự đoán lớp và hộp giới hạn của các đối tượng. Đạt được độ chính xác cao và nhanh hơn so với các mô hình phát hiện đối tượng trước đó, đặc biệt là trong việc phát hiện các đối tượng nhỏ và hiếm. Mô hình này đã được áp dụng rộng rãi trong nhiều ứng dụng như phát hiện giao thông, phát hiện đối tượng trong video và phát hiện đối tượng trong ảnh y khoa [18].

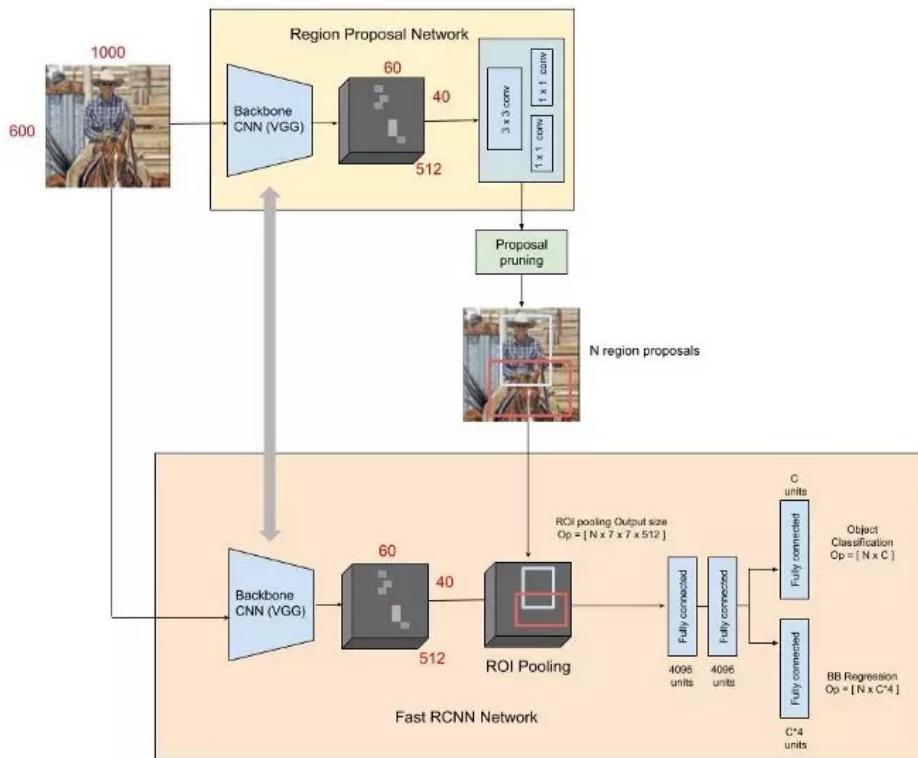
NAS-FPN (Neural Architecture Search Feature Pyramid Network) là một kiến trúc mạng neuron tiên tiến được giới thiệu bởi Golnaz Ghiasi cùng nhóm nghiên cứu. Mô hình này sử dụng kỹ thuật Neural Architecture Search (NAS) để tìm kiếm kiến trúc mạng neuron tối ưu cho việc trích xuất đặc trưng trong phát hiện đối tượng. NAS-FPN kết hợp hai thành phần chính: một mô-đun phát hiện đối tượng trên các đặc trưng đa tầng được tạo ra bởi FPN và một mô-đun NAS được sử dụng để tìm kiếm kiến trúc phù hợp nhất cho mô-đun phát hiện đối tượng. Mô-đun NAS được áp dụng trên tập dữ liệu huấn luyện để tìm kiếm kiến trúc mạng neuron tối ưu cho việc phát hiện đối tượng. NAS-FPN đã đạt được kết quả tốt trong việc phát hiện đối tượng trên nhiều tập dữ liệu khác nhau. Mô hình này có thể đạt được độ chính xác cao hơn so với các phương pháp truyền thống và đòi hỏi ít sự can thiệp của con người trong việc thiết kế kiến trúc mạng neuron [19].

YOLOv3 (You Only Look Once version 3) là một trong những mô hình phát hiện đối tượng tiên tiến được giới thiệu bởi Joseph Redmon cùng nhóm nghiên cứu vào năm 2018. YOLOv3 sử dụng một kiến trúc mạng neuron sâu (deep neural network) để trích xuất các đặc trưng đối tượng từ ảnh. Mô hình này sử dụng một lớp đầu ra để dự đoán các hộp giới hạn và xác suất của các lớp đối tượng có thể xuất hiện trong hộp đó. YOLOv3 cũng sử dụng kỹ thuật skip connection để tích hợp thông tin từ các tầng đầu vào và đầu ra, giúp tăng độ chính xác của mô hình [20].

Các nghiên cứu trên cho thấy tiềm năng của học sâu dựa trên dữ liệu y khoa đặc biệt là dữ liệu ảnh trong việc hỗ trợ bác sĩ phát hiện và chẩn đoán các bệnh lý, đồng thời khẳng định rằng phương pháp này có thể giúp nâng cao độ chính xác và tốc độ của quá trình chẩn đoán bệnh.

- Để giải quyết vấn đề đặt ra, bài báo này tập trung giải quyết 2 công việc cụ thể như sau:
- Đề xuất sử dụng 2 kỹ thuật SSD và SPARSE RCNN trong deep learning, để phát hiện và phân loại đối tượng dựa trên ảnh tế bào máu.
 - Xây dựng mô hình mạng với 2 kỹ thuật trên, kết hợp với 3 hàm loss để giám sát tất cả các quá trình: GIOU, Focal và L1 và tiến hành thực nghiệm trên bộ dữ liệu ảnh tế bào máu BCCD (COCO).

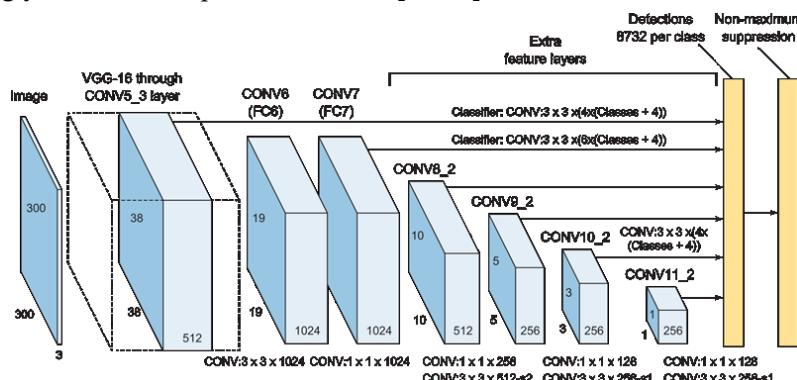
Các kết quả này được trình bày trong phần 3, phần 4 minh họa những kết quả thử nghiệm cũng như các đánh giá. Phần cuối cùng là một vài kết luận và những hướng nghiên cứu còn bỏ ngỏ khi đề cập đến bài toán hỗ trợ phát hiện và phân loại đối tượng trong ảnh tế bào máu.



Hình 1. Kiến trúc Fast RCNN Network

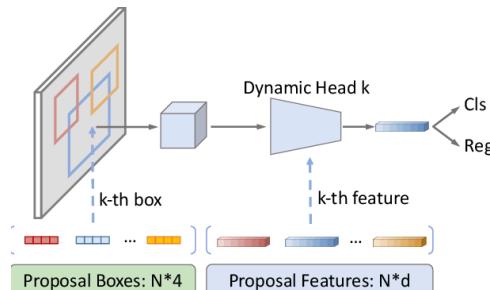
3. PHƯƠNG PHÁP NGHIÊN CỨU

SSD (Single Shot MultiBox Detector) là một thuật toán phát hiện đối tượng trong ảnh với tốc độ nhanh và độ chính xác cao. Thuật toán này sử dụng một mạng neural network tích chập (CNN) để trích xuất các đặc trưng của ảnh, sau đó sử dụng một bộ phân loại để xác định đối tượng có mặt trong ảnh và vị trí của nó. Điểm mạnh của SSD là tốc độ nhanh và khả năng phát hiện đa đối tượng trên cùng một ảnh. SSD sử dụng kỹ thuật anchor boxes để giảm số lượng vùng quan tâm cần phân loại. Kỹ thuật này giúp thuật toán tập trung vào các khu vực quan trọng trong ảnh, giảm thiểu thời gian xử lý và tăng độ chính xác. Tuy nhiên, điểm yếu của SSD là khả năng phát hiện đối tượng nhỏ hơn không tốt và thường cho kết quả không chính xác trên các đối tượng có hình dạng phức tạp. Do đó, SSD thường được sử dụng trong các ứng dụng yêu cầu tốc độ phát hiện nhanh [21,22].



Hình 2. Kiến trúc SSD

Sparse RCNN là một mô hình mạng neural sử dụng trong bài toán phát hiện đối tượng trong ảnh, được phát triển dựa trên RCNN. Sparse RCNN có khả năng phát hiện các đối tượng trong ảnh một cách nhanh chóng và hiệu quả hơn so với RCNN truyền thống. Khác với RCNN, Sparse RCNN sử dụng một cấu trúc mạng học sâu đơn giản hơn và tận dụng tính hiệu quả của việc thực hiện phép tích chập một cách "thưa" (sparse) trên ảnh đầu vào. Điều này giúp giảm đáng kể số lượng vùng quan tâm (region of interest - ROI) cần được xử lý và giúp tăng tốc quá trình huấn luyện. Đối với RCNN truyền thống, quá trình phát hiện đối tượng được chia thành 2 giai đoạn: Tìm các khu vực tiềm năng chứa đối tượng trong ảnh (region proposals). Phân loại đối tượng trong các khu vực tiềm năng đó bằng cách sử dụng một mạng CNN. Tuy nhiên, việc tìm kiếm các khu vực tiềm năng gặp nhiều vấn đề vì số lượng khu vực tiềm năng có thể lên đến hàng trăm nghìn trong một bức ảnh lớn. Để giải quyết vấn đề này, Sparse RCNN sử dụng một ma trận thưa, chỉ lưu trữ thông tin của một số khu vực tiềm năng quan trọng nhất (through qua giá trị đánh dấu) để giảm độ phức tạp tính toán. Đồng thời, Sparse RCNN sử dụng một mô hình thuộc loại one-stage detector, tức là chỉ phân loại đối tượng một lần trực tiếp trên toàn bức ảnh, thay vì phân loại trên từng khu vực tiềm năng như RCNN truyền thống. Ngoài ra, Sparse RCNN cũng sử dụng một thuật toán mới để chọn và đánh giá các vùng quan tâm cần xử lý, giúp tăng độ chính xác và hiệu quả cho quá trình phát hiện đối tượng. Sparse RCNN là một mô hình phát hiện đối tượng trong ảnh cải tiến dựa trên RCNN, với tính năng "thưa" để giảm số lượng vùng quan tâm cần xử lý và thuật toán tối ưu hóa quá trình đánh giá vùng quan tâm, giúp tăng độ chính xác và tốc độ của quá trình phát hiện đối tượng [23].



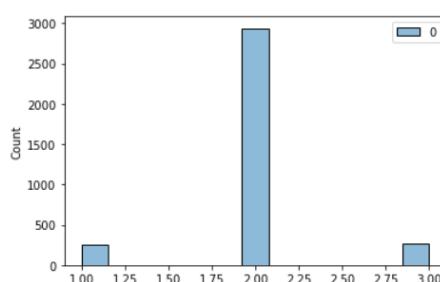
Hình 3. Kiến trúc Sparse RCNN

4. THỰC NGHIỆM VÀ KẾT QUẢ

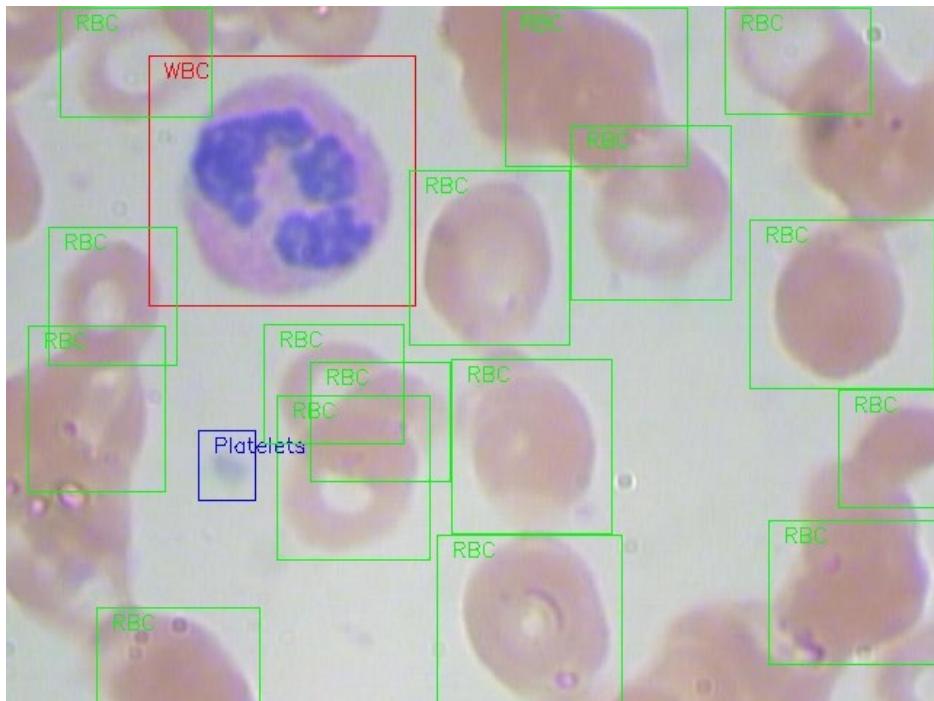
3.1. Dữ liệu

Bộ dữ liệu BCCD (COCO) là bộ dữ liệu công khai để phát hiện các tế bào máu trong ảnh. Bộ dữ liệu này gồm 364 ảnh về các loại tế bào máu bao gồm: hồng cầu, bạch cầu, tiểu cầu. Mỗi ảnh có kích thước 640 x 480 pixel và có độ phân giải là 2 megapixel [24].

Bộ dữ liệu này gồm: 249 nhãn về tiểu cầu, 2938 nhãn hồng cầu, 263 nhãn là bạch cầu.



Hình 4. Trực quan hóa các lớp ảnh trong bộ dữ liệu BCCD (COCO)



Hình 5. Một ảnh đa đối tượng trong bộ dữ liệu BCCD (COCO)

3.2. Thực nghiệm

Chia bộ dữ liệu BCCD thành ba phần gồm train, validation, test. Trong đó 256 ảnh cho tập train, 74 ảnh dùng validation và 34 ảnh dùng để test.

Tiền xử lý dữ liệu sử dụng các kỹ thuật random crop, reszie, random flip, brightness transform, gaussain transform, saturation transform, hue transform.

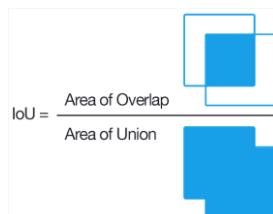
Với kiến trúc SSD và SPARSE RCNN, lần lượt thực hiện các chiến lược huấn luyện để phù hợp với từng mô hình, gồm các thông số như sau:

Kiến trúc SSD: Sử dụng optimizer SGD với learning rate là 0.02, momentum = 0.9, weight decay = 0.0005 và huấn luyện qua 32 epoch.

Kiến trúc SPARSE RCNN: Sử dụng optimizer ADAM với learning rate là 0.00005, weight decay= 0.001 và huấn luyện qua 36 epoch.

Trong nghiên cứu này, sử dụng độ đo AP (Average Precision) là một độ đo dùng để kiểm tra độ chính xác của các phương pháp phát hiện đối tượng. IoU là một độ đo dùng để kiểm tra độ khớp nhau giữa bounding box được dự đoán của đối tượng và bounding box thật sự của đối tượng đó.

$$IoU = \frac{\text{Area of Overlap}}{\text{Area of Union}}$$



Hình 6. Minh họa cho IoU

Với mỗi ngưỡng IoU xác định được một cặp precision và recall. Precision là tỉ lệ số lượng bounding box được dự đoán đúng trên tổng số bounding box được dự đoán. Recall là tỉ lệ số lượng bounding box được dự đoán đúng trên tổng số bounding box ground truth. Từ cặp precision và recall này, tính được AP và AP [0,1].

Trong bài báo này với mỗi phương pháp chúng tôi đánh giá kết quả bằng cách tính $AP_{IoU=0.5:0.95}$, mAP là trung bình AP trên toàn bộ class.

Chúng tôi kết hợp ba loại hàm loss gồm: GIOU loss, Focal loss và L1 loss để giám sát từng nhiệm vụ của các kiến trúc mạng này.

GIOU loss: gọi A và B lần lượt là hai bounding box Ground truth và dự đoán của mô hình

$$GIOU\ Loss = \frac{1}{N} \sum_{i=1}^N \left(1 - \left(IoU - 1 + \frac{|A \cup B|}{|C|} \right) \right)$$

Trong đó, C là diện tích nhỏ nhất để một hình chữ nhật có thể bao quanh cả 2 bounding box A và B.

Focal loss:

$$Focal\ loss = \frac{1}{N} \sum_{i=1}^N -\alpha(1 - p_t)^\gamma \log(p_t)$$

Trong đó, α và γ là hai siêu tham số, p_t là xác suất phân lớp.

L1 loss:

$$L1\ loss = \frac{1}{N} \sum_{i=1}^N |y - \hat{y}|$$

Trong đó, y và \hat{y} lần lượt là dự đoán và nhãn của khối Regression tọa độ bounding box của kiến trúc này.

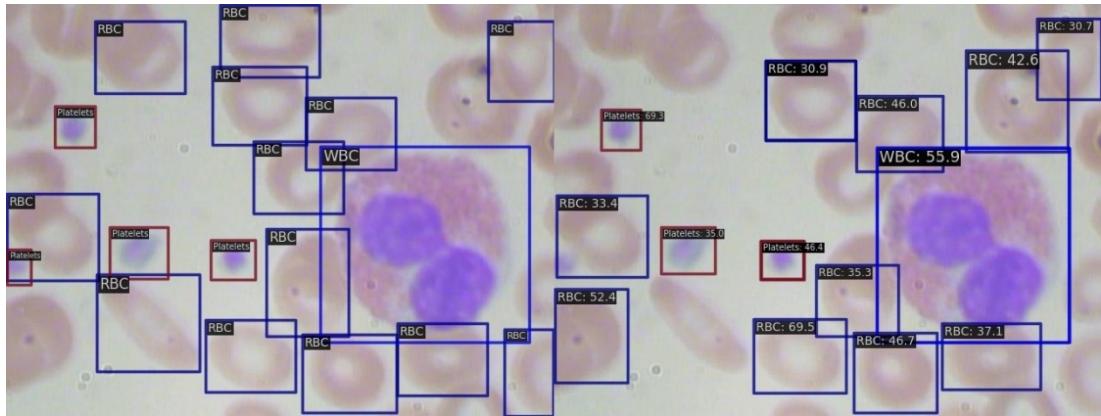
3.3. Kết quả

Bảng 1. Kết quả thực nghiệm và đối sánh

	mAP 50	mAP 75	mAP	time
SSD	0.638	0.278	0.326	0.137
SPARSE-RCNN	0.831	0.715	0.591	0.343
YOLOF	0.890	0.657	0.575	
YOLOv3	0.867	0.453	0.459	

Từ hai thực nghiệm trên, có thể thấy kỹ thuật SPARSE RCNN nhờ tận dụng được ma trận SPARSE để giảm được độ phức tạp của tính toán, tập trung vào các vùng cần được quan tâm và loại bỏ các thông tin không quan trọng, kết hợp với Branch-out Network được sử dụng để dự đoán vị trí của các đối tượng trên những khu vực không được quan tâm đến trong bước lấy mẫu. Các dự đoán này được tính bằng cách sử dụng thông tin từ các khu vực quan tâm khác trên ảnh thông qua một mạng neuron riêng biệt và được sử dụng để cập nhật các trọng số của mô hình chính. Điều này giúp cho mô hình được tạo ra từ kỹ thuật SPARSE RCNN dự đoán chính xác và tốt hơn so với mô hình tạo ra từ kỹ thuật SSD thiên về tốc độ xử lý hơn hiệu quả tính toán.

Ngoài ra, kết quả thực nghiệm cho thấy kỹ thuật được sử dụng trong nghiên cứu này cho kết quả tốt hơn so với các kỹ thuật YOLOF và YOLOv3 đã công bố trước đó [25].



Hình 7. Bên trái là nhãn, bên phải là ảnh được dự đoán từ mô hình SPARESE R-CNN

4. KẾT LUẬN

Trong nghiên cứu này, chúng tôi sử dụng 2 kỹ thuật học sâu SSD và SPARSE R-CNN kết hợp với 3 hàm loss GIOU, Facal, L1 với mục đích giám sát từng nhiệm vụ thực hiện của 2 kỹ thuật này để tiến hành xây dựng mô hình phát hiện và phân loại tế bào máu. Các thực nghiệm được tiến hành trên bộ dữ liệu ảnh tế bào máu BCCD (COCO). Trong đó thực nghiệm 2 với SPARSE CRNN cho kết quả tốt hơn về độ chính xác trên tất cả các độ đo. Ngoài trừ về tốc độ, kỹ thuật SPARSE CRNN cho thấy chậm hơn so với kỹ thuật SSD tuy nhiên kết quả vẫn có thể chấp nhận được và có thể sử dụng để xây dựng các ứng dụng yêu cầu về thời gian thực.

Hướng tiếp theo, sẽ tiếp tục nghiên cứu và cải tiến phương pháp phát hiện đối tượng để có độ chính xác cao hơn và thời gian nhanh hơn có thể đáp ứng được nhu cầu nghiên cứu và ứng dụng thực tế cho các bài toán liên quan dữ liệu y khoa, hay các bài toán áp dụng kỹ thuật phát hiện đối tượng khác.

TÀI LIỆU THAM KHẢO

1. Ứng dụng trí tuệ nhân tạo trong phân tích hình thái tế bào máu- Bước tiến mới trong chuyên khoa huyết học [Internet]. Available from: <https://www.vinmec.com/vi/tin-tuc/thong-tin-suc-khoe/suc-khoe-tong-quat/ung-dung-tri-tue-nhan-tao-trong-phan-tich-hinh-thai-te-bao-mau-buoc-tien-moi-trong-chuyen-khoa-huyet-hoc/>
2. Kê tên các bệnh về máu và triệu chứng nhận biết [Internet]. Available from: <https://medlatec.vn/tin-tuc/ke-tencac-benh-ve-mau-va-trieu-chung-nhan-biet-s195-n22770>
3. Rối loạn tế bào máu: Triệu chứng, phân loại và nguyên nhân [Internet]. Available from: <https://www.vinmec.com/vi/tin-tuc/thong-tin-suc-khoe/suc-khoe-tong-quat/roi-loan-te-bao-mau-trieu-chung-phan-loai-va-nguyen-nhan/>
4. (US) NC for BI. - Blood and Lymph Diseases. (1998) [Internet]. Available from: <https://www.ncbi.nlm.nih.gov/books/NBK22211/>

5. Zaidi AU, Buck S, Gadgeel M, Herrera-Martinez M, Mohan A, Johnson K, et al. - Clinical Diagnosis of Red Cell Membrane Disorders: Comparison of Osmotic Gradient Ektacytometry and Eosin Maleimide (EMA) Fluorescence Test for Red Cell Band 3 (AE1, SLC4A1) Content for Clinical Diagnosis. *Frontiers in Physiology*, vol11 (2020).
6. Australia H. - Blood and blood vessels. (2023).
7. Zhao A, Zhang J, Wang S, Wang Y, Zhu X, Shen W, et al. - Detection of Hysteroscopic Hysteromyoma in Real-Time Based on Deep Learning. *Journal of Physics: Conference Series*, 1861(1) (2021) page 012079.
8. Liu M, Dong L, Jiao Q, Mesin L, Rahman H, Fatima T, et al. - A Deep Learning Approach for Liver and Tumor Segmentation in CT Images Using ResUNet. *Bioengineering*, vol9 (2022) page 368.
9. Sharifi Y, Bakhshali MA, Dehghani T, DanaiAshgzari M, Sargolzaei M, Eslami S. - Deep learning on ultrasound images of thyroid nodules. *Biocybernetics and Biomedical Engineering*, 41(1) (2021) p636-655.
10. Zhang L, Huang J, Liu L. - Improved Deep Learning Network Based in combination with Cost-sensitive Learning for Early Detection of Ovarian Cancer in Color Ultrasound Detecting System. *Journal of Medical Systems*, 43(8) (2019) p1-9.
11. Kulhare S, Zheng X, Mehanian C, Gregory C, Zhu M, Gregory K, et al. - Ultrasound-based detection of lung abnormalities using single shot detection convolutional neural networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11042 LNCS (2018) p65-73.
12. Korbar B, Olofson A, Miraflor A, Nicka C, Suriawinata M, Torresani L, et al. - Deep Learning for Classification of Colorectal Polyps on Whole-slide Images. *Journal of pathology informatics*, 8(1) (2017).
13. Huang SC, Pareek A, Seyyedi S, Banerjee I, Lungren MP. - Fusion of medical imaging and electronic health records using deep learning: a systematic review and implementation guidelines. *npj Digital Medicine*, 3(1) (2020) p1-9.
14. Girshick R, Donahue J, Darrell T, Malik J. - Rich feature hierarchies for accurate object detection and semantic segmentation. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, (2013) p580-587.
15. Girshick R. - Fast R-CNN. (2015).
16. Ren S, He K, Girshick R, Sun J. - Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 39(6) (2015) p1137-1149.
17. Redmon J, Divvala S, Girshick R, Farhadi A. - You Only Look Once: Unified, Real-Time Object Detection. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, (2016) p779-788.
18. Lin TY, Goyal P, Girshick R, He K, Dollar P. - Focal Loss for Dense Object Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 42(2) (2017) p318-327.
19. Ghiasi G, Lin TY, Le Q V. - NAS-FPN: Learning Scalable Feature Pyramid Architecture for Object Detection. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, (2019) p7029-7038.
20. Redmon J, Farhadi A. - YOLOv3: An Incremental Improvement. (2018).
21. Liu W, Anguelov D, Erhan D, Szegedy C, Reed S, Fu CY, et al. - SSD: Single Shot MultiBox Detector. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9905 LNCS (2015) p21-37.

22. Li J, Hou Q, Xing J, Ju J. - SSD Object Detection Model Based on Multi-Frequency Feature Theory. IEEE Access, 8 (2020) p82294-82305.
23. Sun P, Zhang R, Jiang Y, Kong T, Xu C, Zhan W, et al. - Sparse R-CNN: End-to-End Object Detection with Learnable Proposals. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,(2020) p14449-14458.
24. BCCD (COCO) [Internet]. Available from: <https://www.kaggle.com/datasets/ammarnassanalhajali/bccd-coco>
25. Xu F, Li X, Yang H, Wang Y, Xiang W. - TE-YOLOF: Tiny And Efficient YOLOF For Blood Cell Detection. arXiv, (2021) p1-10.

ABSTRACT

DETECT OBJECTS IN BLOOD CELL IMAGES USING DEEP LEARNING TECHNIQUE

Tran Dinh Toan^{1,*}, Nguyen Duc Toan²

¹*Ho Chi Minh City University of Food Industry*

²*University of Information Technology, VNU-HCM, Vietnam*

*Email: toantd@hufi.edu.vn

In this study, we used SSD and SPARSE R-CNN deep learning techniques based on blood cell images to detect cell types such as red blood cells, white blood cells and platelets to assist doctors in detecting growths. abnormality of blood cells, thereby early diagnosis of diseases such as infections in the body, pharyngitis, pneumonia, meningitis and other diseases. When white blood cells detect bacteria or viruses that cause disease, they grow and multiply to attack and eliminate bacteria and viruses from the body. In addition, testing for red blood cells, white blood cells, and platelets can help your doctor make an overall assessment of a patient's health, such as the degree of anemia or disease related to the body's immune system. The experiment was conducted on the Blood Cell Count and Detection - BCCD (COCO) dataset with SSD, SPARSE RCNN algorithms and combined with GIOU, Focal and L1 loss functions for monitoring, the mAP results are respectively 0.326 and 0.591.

Keywords: SSD, BLOOD CELL, SPARSE RCNN

ỨNG DỤNG THUẬT TOÁN SONG SONG FP-GROWTH KHAI PHÁ TẬP PHỔ BIẾN

Nguyễn Thị Hồng Thảo^{1,*}

¹Khoa công nghệ thông tin, Trường đại học Công nghệ Thực phẩm TPHCM

*Email: thaonth@hufi.edu.vn

Ngày gửi bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Khai phá dữ liệu là quá trình phát hiện tri thức, xây dựng tập mẫu và đánh giá tập mẫu. Trong đó các giải thuật khai phá dữ liệu tìm kiếm các tập mẫu phổ biến đóng vai trò hết sức quan trọng. Các tập mẫu phổ biến được ứng dụng trong nhiều lĩnh vực như bán hàng, phân tích chuỗi thời gian, phân tích gen di truyền v.v... Có rất nhiều thuật toán đề xuất để khai phá tập mẫu phổ biến, tuy nhiên khi xử lý với dữ liệu lớn thì hiệu quả chưa cao. Trong phạm vi bài báo, tác giả nghiên cứu phương pháp khai phá tập phổ biến sử dụng thuật toán song song FP-Growth dựa trên thuật toán song song xây dựng FP-Tree để tiết kiệm được tối đa thời gian khai phá. Kết quả thực nghiệm cho thấy, hiệu quả thực hiện của thuật toán tốt hơn nhiều so với các thuật toán thông thường.

Từ khóa: Khai phá dữ liệu, luật kết hợp, tập phổ biến, thuật toán song song, fp-growth, fp-tree

1. GIỚI THIỆU

Khai phá dữ liệu là quá trình phân tích dữ liệu để tìm ra các mô hình, mối quan hệ và thông tin hữu ích từ dữ liệu. Một trong những công việc quan trọng trong khai phá dữ liệu là tìm kiếm các tập phổ biến. Tập phổ biến là tập hợp các mục xuất hiện cùng nhau một số lần tối thiểu trong dữ liệu.

Một trong những hướng tiếp cận hiệu quả là sử dụng luật kết hợp (association rules), khi khai phá luật kết hợp ta dùng một giá trị ngưỡng phổ biến tối thiểu (*minsup*) đại diện cho tần số xuất hiện của các mặt hàng. Ngoài tính chính xác trong việc khai phá dữ liệu thì vấn đề thời gian thực thi để khai phá dữ liệu với dữ liệu lớn được quan tâm không kém. Việc tận dụng được khả năng xử lý song song để tối ưu hóa thời gian thực thi trong khai phá là nhu cầu rất cần thiết trong dự báo mua hàng. Tuy nhiên với các thuật toán khai phá luật kết hợp tuần tự sẽ mất rất nhiều thời gian khi thực hiện với dữ liệu lớn, do đó trong phạm vi bài báo, tác giả nghiên cứu thuật toán song song FP-Growth dựa trên thuật toán song song xây dựng FP-Tree và đánh giá hiệu quả giải thuật trong môi trường xử lý song song để tăng tốc độ xử lý.

2. THUẬT TOÁN SONG SONG XÂY DỰNG FP-TREE

Thuật toán song song xây dựng FP-Tree là cải tiến của thuật toán xây dựng FP-Tree để tận dụng tối đa khả năng xử lý song song của các hệ thống đa nhân. Thuật toán này sử dụng nhiều tiêu tập dữ liệu để xây dựng các cây FP-Tree riêng biệt. Sau đó, các cây này được trộn lại để tạo ra một cây FP-Tree duy nhất.

Input: CSDL giao tác DB, ngưỡng min-sup và số lượng tiêu tập dữ liệu threadCount

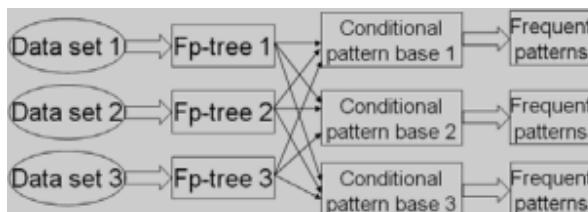
Output: Cây FP-Tree

Method:

1. Chia tập dữ liệu thành threadCount tiêu tập dữ liệu DB1, DB2, ..., DBn. Các DB_threadCount có kích thước giống nhau
2. Tạo threadCount luồng và gọi hàm buildFPTree trên mỗi tiêu tập dữ liệu tương ứng. Lưu trữ các cây FP-Tree riêng biệt tương ứng với mỗi luồng.
3. Kết hợp các cây FP-Tree riêng biệt thành một cây FP-Tree duy nhất bằng cách gọi hàm mergeFPtrees.
4. Trả về cây FP-Tree.

3. THUẬT TOÁN SONG SONG FP-GROWTH

Thuật toán song song FP-Growth sử dụng nhiều cây FP-Tree cục bộ thay vì một cây FP-Tree toàn cục để tránh vấn đề về dung lượng bộ nhớ đối với các tập dữ liệu lớn. Các cây FP-Tree cục bộ được xây dựng song song và được kết hợp lại để tạo ra kết quả cuối cùng.



Hình 1. Mô hình xử lý của thuật toán song song FP-Growth

Thuật toán song song FP – Growth:

(Khai phá các mẫu phô biến với thuật toán song song xây dựng FP-tree từ các mẫu riêng lẻ)

Input: FP-tree, ngưỡng hỗ trợ tối thiểu δ.

Output: Một tập đầy đủ các mẫu phô biến F.

Phương pháp: gọi FP-Growth (FP-tree, null).

Procedure FP-Growth (Tree, α)

If (Cây chỉ có 1 nhánh đơn P) then

For each tổ hợp β của các nút trong P

{

Tạo mẫu p = β ∪ α ;

p.support = min {support của các nút trong β};

F = F ∪ p;

}

else

For each α_i trong bảng Header của Tree

{

Tạo β = α_i ∪ α ;

β.support = α_i.support;

F = F ∪ β;

Xây dựng cơ sở có điều kiện của β;

Xây dựng FP-Tree có điều kiện là Treeβ của β;

if Treeβ ≠ Ø then Call FP_Growth(Treeβ, β);

}

4. KẾT QUẢ THỰC NGHIỆM VÀ ĐÁNH GIÁ

Thực nghiệm trên máy Intel core i7 1.5 GHz, 4 GB Ram (4 processor), VS2015, chạy trên nền Windows 10 64-bit, và máy Intel (R), Xeon (R) Gold 6128 CPU @ 3.4 Gz, 4 GB RAM (8 processor)

Chương trình thực nghiệm sử dụng bộ dữ liệu chess và mushrooms trên SPMF theo bảng 1 dưới đây.

Bảng 1. Bảng CSDL được sử dụng

Dataset	Type	Transactions	Length
Chess	Real	3196	37
Mushrooms	Real	8416	23

Kết quả tìm tập phổ biến với bộ dữ liệu Chess:

```

Kết quả tìm tập phổ biến:
Hỗ trợ tối thiểu (minsupport): count= 2877, độ hỗ trợ
(support) = 90%
=====
Tập mục thường xuyên (A set of Frequent)=13 items:
34 (count=3040 ,Support: 95.1%)
7 (count=3076 ,Support: 96.2%)
62 (count=3060 ,Support: 95.7%)
5 (count=2971 ,Support: 93%)
52 (count=3185 ,Support: 99.7%)
36 (count=3099 ,Support: 97%)
66 (count=3021 ,Support: 94.5%)
29 (count=3181 ,Support: 99.5%)
56 (count=3021 ,Support: 94.5%)
60 (count=3149 ,Support: 98.5%)
48 (count=3013 ,Support: 94.3%)
58 (count=3195 ,Support: 100%)
40 (count=3170 ,Support: 99.2%)
=====
Frequently(k)=2,      Item set=27
40,5, (count= 2950,Support= 92.3%)
=====
```

Hình 2. Thuật toán song song FP-Growth với độ hỗ trợ (minsup=90%, 3196 transactions)

Kết quả tìm tập phổ biến với bộ dữ liệu Mushroom:

```

Kết quả tìm tập phổ biến:
Hỗ trợ tối thiểu (minsupport): count= 7575, độ hỗ trợ
(support) = 90%
=====
Tập mục thường xuyên (A set of Frequent)=4 items:
90 (count=8416 ,Support: 100%)
94 (count=8216 ,Support: 97.6%)
97 (count=7768 ,Support: 92.3%)
36 (count=8200 ,Support: 97.4%)
=====
Frequently(k)=2,      Item set=5
90,97, (count= 7768,Support= 92.3%)
36,97, (count= 7576,Support= 90%)
90,36, (count= 8200,Support= 97.4%)
94,36, (count= 8192,Support= 97.3%)
90,94, (count= 8216,Support= 97.6%)
=====
Frequently(k)=3,      Item set=2
90,36,97, (count= 7576,Support= 90%)
90,94,36, (count= 8192,Support= 97.3%)
=====
```

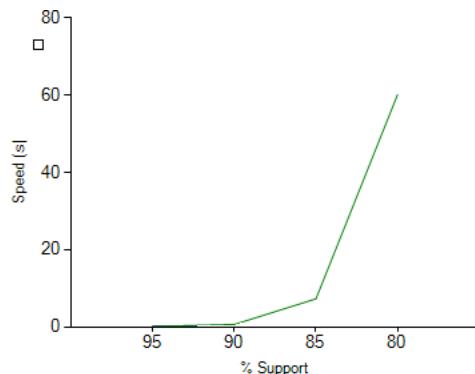
Hình 3. Thuật toán song song FP-Growth với độ hỗ trợ (minsup=90%, 8416 transactions)

Thời gian thực thi:

Sau khi thực nghiệm thuật toán song song FP-Growth, ta thấy rằng thuật toán đạt hiệu quả về tốc độ và hiệu xuất khi xử lý với bộ dữ liệu lớn bất kỳ.

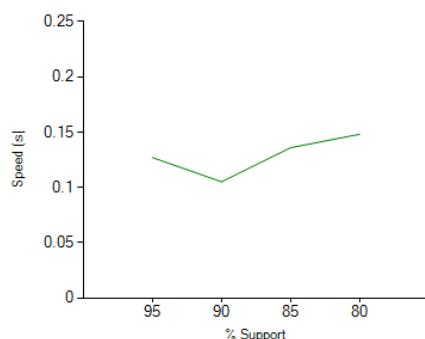
Kết quả thời gian thuật toán sử dụng trên CPU 4 processor:

Hình 4 đánh giá thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu chess



Hình 4. Đánh giá thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu chess

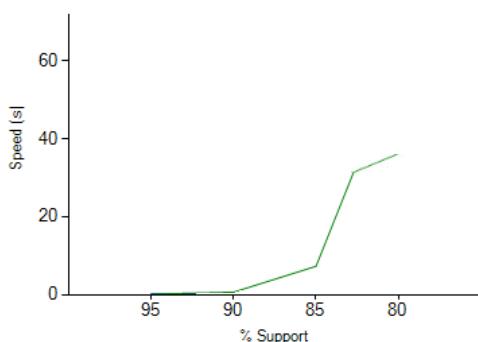
Hình 5 đánh giá kết quả thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu mushrooms:



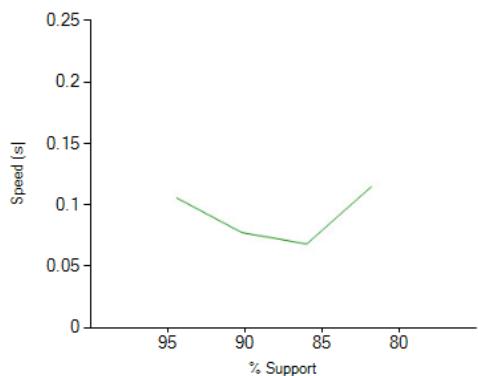
Hình 5. Đánh giá thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu Mushrooms

Kết quả thời gian thuật toán sử dụng trên CPU 8 processor:

Hình 6, đánh giá thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu chess



Hình 6: Đánh giá thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu chess



Hình 7. Đánh giá thời gian thực thi thuật toán song song FP-Growth trên bộ dữ liệu Mushrooms

Tài nguyên thuật toán sử dụng:

Bảng 2. Kết quả tài nguyên sử dụng thuật toán trên máy tính CPU 4 processor

Tài nguyên	CPU (%)	RAM(MB)
Chess	12.3%	68 MB
Mushrooms	5.8%	121 MB

Bảng 3. Kết quả tài nguyên sử dụng thuật toán trên máy tính CPU 8 processor

Tài nguyên	CPU (%)	RAM(MB)
Chess	6.8%	33 MB
Mushrooms	3 %	63 MB

Kết quả thực nghiệm cho thấy, tốc độ xử lý, cũng như hiệu xuất khi thực thi tùy thuộc vào bộ dữ liệu đầu vào và số lượng CPU processor được sử dụng. Với CPU 8 processor, thuật toán song song FP-Growth cho thấy tốc độ xử lý đạt hiệu quả gấp đôi so với CPU 4 processor.

5. KẾT LUẬN

Bài báo đã trình bày thuật toán song song FP-Growth dựa trên thuật toán song song xây dựng FP-Tree và đánh giá hiệu quả giải thuật trong môi trường xử lý song song. Tác giả đã thực hiện thử nghiệm trên các tập dữ liệu khác nhau và đánh giá hiệu quả của thuật toán dựa trên thời gian xử lý và kích thước tập phổ biến được khai phá. Kết quả cho thấy rằng thuật toán song song FP-Growth có thể tiết kiệm đáng kể thời gian xử lý và cho kết quả tốt hơn so với các thuật toán thông thường.

Trên cơ sở những nghiên cứu đã được trình bày trong bài báo, trong tương lai tác giả tiếp tục nghiên cứu sâu hơn các thuật toán khai phá luật kết hợp song song, tìm cách cải tiến nhằm khắc phục các nhược điểm của các thuật toán song song hiện có và các thuật toán khai phá dữ liệu song song khác để đạt được hiệu quả tối ưu hơn.

TÀI LIỆU THAM KHẢO

1. Han X, Liu X, Chen J, Lai G, Gao H, Li J, “Efficiently mining frequent itemsets on massive data” IEEE Access 7:31409–31421, 2019
2. Ali Ikhwan, Milfa Yetri, Yohanni Syahra, Jufri Halim, Andysah Putera Utama Siahaan, Solly Aryza, Yasmin Mohd Yacob ,“A novel of damining for promoting education based on FP-Growth algithm”, IJCIE, Volume 9, Issue 7, pp. 1660–1669, July 2018.
3. Robert Kessl, “Parallel algorithms for mining of frequent itemsets ”, by CRC Press, LLC, 2011
4. M. J. Zaki, C.J. Hsiao, “Efficient Algorithms for Mining Closed Itemsets and Their Lattice Structure”, IEEE Transactions on Knowledge and Data Engineering, (2005).
5. <https://www.philippe-fournier-viger.com/spmf/index.php?link=datasets.php>.

ABSTRACT

APPLICATION OF FP-GROWTH PARALLEL ALGORITHM TO FREQUENT ITEMSETS

Nguyen Thi Hong Thao^{1,*}

University of Food Industry Ho Chi Minh City

**Email: thaonth@hufi.edu.vn*

Data mining is the process of discovering knowledge, building sample sets, and evaluating those sample sets. In which data mining algorithms play a crucial role in searching for common patterns. Common patterns are widely applied in many fields such as sales, time series analysis, genetic analysis, and so on. Although there are many proposed algorithms for mining common patterns, their efficiency is not high when dealing with large datasets. In this article, the author researches a method of mining common patterns using the parallel algorithm FP-Growth based on the parallel algorithm of constructing FP-Tree to save maximum mining time compared to conventional algorithms. The experimental results show that the efficiency of the algorithm is much better than that of conventional algorithms.

Keywords: Data mining, Association rule mining, frequent itemsets, parallel algorithm, FP-Growth, FP-Tree

HỆ THỐNG CHÚ THÍCH ẢNH TỰ ĐỘNG CHO NGƯỜI KHIẾM THỊ

Đinh Thị Mận¹, Nguyễn Văn Thịnh², Trần Ngọc Hiếu¹, Trần Thị Xinh¹,
Trần Thị Vân Anh^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

²Trường Đại học Sư phạm Tp.HCM

*Email: anhttv@husf.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023.

TÓM TẮT

Trong bài báo này, chúng tôi xây dựng hệ chú thích ảnh tự động dựa trên khung mã hóa - giải mã (encoder - decoder framework). Trong giai đoạn encoder, một mô hình mạng nơ ron tích chập (*convolution neural network - CNN*) được sử dụng để trích xuất đặc trưng ảnh. Trong giai đoạn decoder, một mô hình mạng LSTM (*Long Short-Term Memory*) được xây dựng và huấn luyện để phát sinh chú thích cho hình ảnh đầu vào. Thực nghiệm được xây dựng và đánh giá trên bộ dữ liệu ảnh MS COCO với độ đo BLEU (4-grams). Kết quả của phương pháp được đề xuất so với các công trình được công bố gần đây cho thấy tính khả thi và hiệu quả. Từ đó, một ứng dụng trên nền tảng desktop và mobile được phát triển nhằm hỗ trợ người khiếm thị hay người già mắt kém nhận biết được cảnh vật xung quanh bằng âm thanh mô tả hình ảnh ghi nhận được.

Từ khóa: Image Captioning, CNN, LSTM, Word2Vect.

1. GIỚI THIỆU

Chú thích ảnh nhằm mục đích tự động tạo ra chú thích cho hình ảnh dưới dạng ngôn ngữ tự nhiên. Để hiểu nội dung của hình ảnh và xuất ra một câu đúng ngữ nghĩa đòi hỏi hệ thống cần phải tích hợp nhiều lĩnh vực bao gồm cả thi giác máy tính, xử lý ngôn ngữ tự nhiên [1]. Mặc dù các hệ thống như vậy hầu hết được huấn luyện trên các thư viện hình ảnh thông thường [2] nhưng đã đem lại những lợi ích trong thực tiễn như: các hệ thống này có thể cho phép những người mù nhận được thông tin trực quan về môi trường xung quanh của họ [2], hay các hệ thống được huấn luyện trên dữ liệu hình ảnh y tế, từ đó có thể cung cấp cho bác sĩ thông tin hữu ích và trợ giúp cho các quy trình chẩn đoán [3]. Các mô hình chú thích nâng cao cũng được nhúng trong hệ thống robot thông minh giúp robot hoạt động tốt hơn...[2].

Phương pháp tạo chú thích hình ảnh truyền thống gồm: (1) tạo chú thích cho ảnh dựa trên truy hồi thông tin (*Retrieval-based image captioning*) [4]; (2) tạo chú thích cho ảnh dựa trên mẫu dữ liệu (*Template-based image captioning*) [5]. Trong đó, phương pháp (1) chú thích hình ảnh được tạo dựa vào chú thích cho trước của tập ảnh tương tự, từ hình ảnh đầu vào tìm ra ảnh tương tự (mỗi ảnh có chú thích riêng), kết quả trả về sẽ lấy chú thích của ảnh gần với ảnh đầu vào nhất hoặc tổng hợp từ tập chú thích này. Phương pháp này phụ thuộc vào yếu tố chủ quan và đồng thời cần chi phí lớn để mở rộng tập chú thích cho tập hình ảnh tăng trưởng [6]. Phương pháp (2) tạo sẵn cú pháp mẫu, sau đó rút trích các từ đưa vào câu để làm chú thích hình ảnh. Phương pháp này không khôn khả thi do phụ thuộc vào yếu tố con người khi tạo ra

từng nhóm mẫu câu tương ứng với từng nhóm hình ảnh, bên cạnh đó chi phí cho việc gán mẫu chủ thích cho từng hình ảnh cụ thể là rất lớn [7].

Từ năm 2015, phương pháp truyền thống (1) và (2) ít được tiếp cận do nhiều hạn chế, thay vào đó việc tạo chủ thích hình ảnh dựa trên mạng nơ-ron học sâu (*Deep neural network-based image captioning*) [8-10] được sử dụng phổ biến. Trong phương pháp này, hình ảnh được tự động trích xuất đặc trưng bằng mạng nơ-ron học sâu, sau đó kết hợp với mô hình ngôn ngữ tự động tạo ra câu mô tả cho hình ảnh. Các mô hình ngôn ngữ thường được sử dụng như RNN (*Recurrent Neural Networks*), GRU (*Gated recurrent unit*), LSTM (*Long Short-Term Memory*), Transformer [11]. Do đó, trong bài báo này, một mô hình chủ thích ảnh dựa trên mạng nơ-ron học sâu được thực hiện, từ đó áp dụng để xây dựng ứng dụng hỗ trợ người khiếm thị hay người già mất kém nhận biết được cảnh vật xung quanh bằng âm thanh mô tả hình ảnh ghi nhận được...Đóng góp chính của bài báo gồm: (1) xây dựng và huấn luyện mạng LSTM để phát sinh chủ thích ảnh; (2) đưa ra mô hình phát triển ứng dụng đa nền tảng hỗ trợ người khiếm thị; (3) xây dựng ứng dụng thực nghiệm dựa trên các mô hình và thuật toán đã đề xuất.

Phần còn lại của bài báo gồm: phần 2 – Các công trình liên quan để thấy được tính khả thi của phương pháp; phần 3 – mô tả phương pháp tạo chủ thích ảnh tự động; phần 4 – Thực nghiệm đánh giá kết quả của phương pháp đề xuất so với các công trình công bố gần đây nhằm cho thấy tính hiệu quả của phương pháp; phần 5- Kết luận và hướng phát triển.

2. CÁC CÔNG TRÌNH LIÊN QUAN

Nghiên cứu về chủ thích hình ảnh đã có những tiến bộ đáng chú ý trong những năm gần đây với sự trợ giúp của học sâu dựa trên khung mã hóa - giải mã [12]. Mạng CNN thường được sử dụng làm bộ mã hóa để trích xuất các đặc trưng hình ảnh và sau đó mạng nơ-ron hồi quy (RNN) [13] được huấn luyện để chuyển đổi các véc-tơ đặc trưng thành chủ thích hình ảnh dưới dạng bộ giải mã.

Năm 2017, Gu et. al. và các cộng sự đã đề xuất một mô hình ngôn ngữ tạo chủ thích hình ảnh dựa trên mô hình CNN [14]. Trong đề xuất này, CNN không chỉ được sử dụng cho trích xuất đặc trưng của hình ảnh mà còn được sử dụng làm mô hình ngôn ngữ kết hợp với LSTM. Sau đó nhiều công trình nghiên cứu kết hợp giữa mạng CNN và mạng LSTM tạo chủ thích ảnh được tiếp cận và công bố: kết hợp đặc trưng cấp thấp và các mô hình phân lớp ảnh để tạo chủ thích ảnh bằng mạng LSTM [15], mô hình chủ thích ảnh dựa trên sự kết hợp giữa mạng CNN và LSTM [16], tạo chủ thích ảnh theo Ontology miền kết hợp mạng CNN và LSTM [9],...

Năm 2018, S. Liu và các cộng sự kết hợp mô hình mạng CNN và mạng RNN [17] tạo chủ thích cho hình ảnh. Tuy nhiên, mạng RNN gặp phải vấn đề chỉ mang được thông tin một số bước nhất định do vấn đề triệt tiêu đạo hàm (*vanishing gradient*) nên chỉ học được thông tin ngắn hạn (*short-term memory*) bị quên thông tin dài hạn.

Năm 2019, Yi và Yang [18] đề xuất mô hình kết hợp giữa RNN-CNN và LSTM tạo chủ thích bằng văn bản cho hình ảnh. Việc sử dụng mạng nơ-ron học sâu kết hợp với xử lý ngôn ngữ tự nhiên và gán nhãn lại các chủ thích hình ảnh để tạo ra câu chủ thích mang tính khách quan hơn so với các phương pháp tạo chủ thích truyền thống.

Năm 2021, Aditya Kumar Yadav và cộng sự [19] đề xuất mô hình kết hợp R-CNN và LSTM để tạo chú thích hình ảnh. Trong đó, R-CNN để phát hiện vùng của ảnh, LSTM để tạo chú thích ảnh. J. Alzubi và các cộng sự [20] đề xuất mô hình mạng học sâu để tạo chú thích cho một hình ảnh bằng cách giải mã thông tin có sẵn trong hình ảnh. Trong đó, CNN mã hóa hình ảnh và LSTM tạo chú thích ảnh. Ngoài ra, nhóm tác giả đề xuất mô hình dựa trên GRU và LSTM hai chiều tạo chú thích ảnh để phân tích và so sánh kết quả. Độ chính xác được đánh giá của nhóm tác giả là 55,8% (đánh giá với độ đo Bleu-4).

Như vậy, LSTM [21] được nghiên cứu đã khắc phục được hạn chế mất mát thông tin so với mạng rơ ron hồi quy thông thường (*RNN*) vì ngoài thành phần cơ bản của mạng nơ ron hồi quy thì LSTM được bổ sung thành phần *long-term memory*, mạng này sử dụng một ô nhớ để duy trì tạm thời thông tin dài hạn. Vì vậy, LSTM được sử dụng rộng rãi cho việc xây dựng bộ giải mã trong mô hình mã hóa-giải mã cho chú thích hình ảnh [22].

Từ những công trình đã công bố cho thấy rằng bài toán chú thích ảnh dựa trên học sâu được nhiều nhóm tác giả quan tâm nghiên cứu và đạt kết quả khả quan. Bên cạnh đó, hầu hết các công trình công bố chỉ dừng ở việc xây dựng mô hình chú thích ảnh nhưng chưa áp dụng mô hình này xây dựng ứng dụng để hỗ trợ người khiếm thị. Do đó, trong bài báo này: một mô hình chú thích ảnh dựa trên mạng nơ ron học sâu được đưa ra và áp dụng để xây dựng ứng dụng hỗ trợ người khiếm thị hay người già mắt kém nhận biết được cảnh vật xung quanh bằng âm thanh mô tả hình ảnh ghi nhận được.

3. PHƯƠNG PHÁP TẠO CHÚ THÍCH ẢNH TỰ ĐỘNG

3.1 Mô hình tạo chú thích ảnh tự động

Mô hình tạo chú thích ảnh được xây dựng trên cơ sở mã hóa – giải mã [1]. Trong bước mã hóa (*encoder*), hình ảnh và chú thích của ảnh được biểu diễn thành các véc tơ đặc trưng. Bước giải mã (*decoder*) phát sinh ra câu mô tả nội dung hình ảnh. Mô hình tạo chú thích ảnh tự động gồm có 2 pha được trình bày như hình 1. Pha huấn luyện mô hình nhằm huấn luyện và tạo ra mô hình LSTM phát sinh ra câu mô tả nội dung hình ảnh trong tập dữ liệu ảnh. Pha tạo chú thích hình ảnh thực hiện nhằm tạo ra chú thích của hình ảnh đầu vào dựa trên mô hình LSTM đã được huấn luyện trước đó.

a. Pha huấn luyện mô hình tạo chú thích hình ảnh:

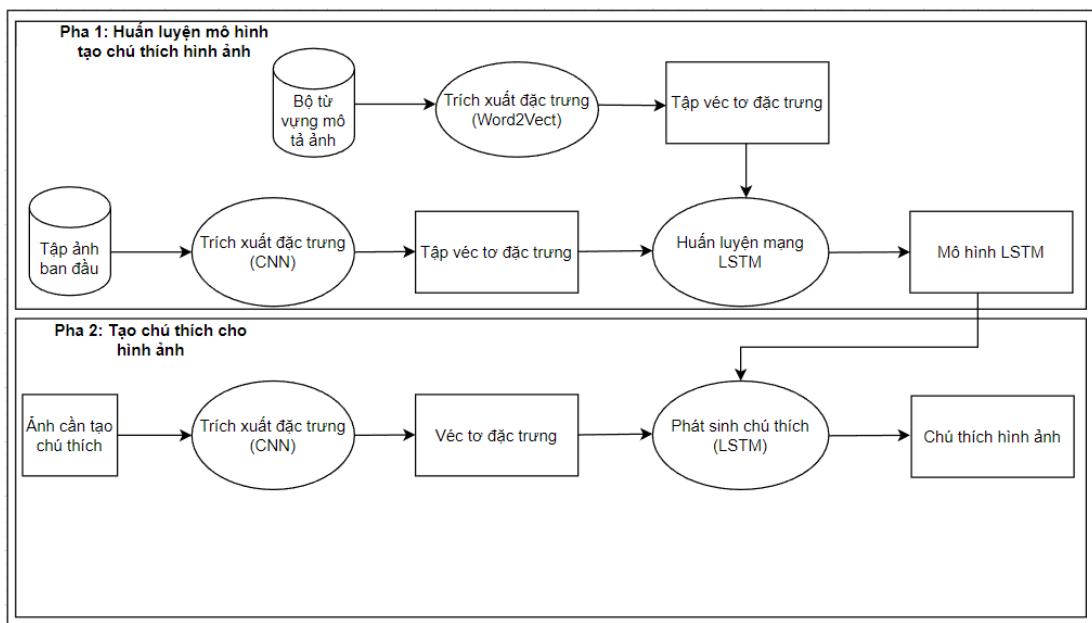
- (1) Tiền xử lý hình ảnh và tiền xử lý bộ chú thích của tập hình ảnh
 - Tập dữ liệu hình ảnh được thay đổi kích thước (*resize*) và chuẩn hóa cho phù hợp yêu cầu của mô hình trích xuất đặc trưng (*pre-trained model*).
 - Bộ chú thích hình ảnh được xử lý loại bỏ tất cả các ký tự đặc biệt, chuyển các ký tự in hoa thành ký tự thường, thêm dấu *<start>* và *<end>* để đánh dấu vị trí bắt đầu và kết thúc câu, gán nhãn số nguyên cho mỗi từ trong bộ từ vựng chú thích để phù hợp với kỹ thuật trích xuất đặc trưng từ *word embedding*.
- (2) Trích xuất đặc trưng hình ảnh và trích xuất đặc trưng bộ chú thích hình ảnh
 - Sử dụng mô hình CNN đã huấn luyện (Pretrained CNN) để trích xuất đặc trưng hình ảnh.

- Sử dụng mô hình Word2Vect trích xuất đặc trưng bộ từ vựng chủ thích hình ảnh.

(3) Xây dựng và huấn luyện mạng LSTM để phát sinh bộ chủ thích cho bộ dữ liệu ảnh huấn luyện.

b. Pha tạo chủ thích cho hình ảnh:

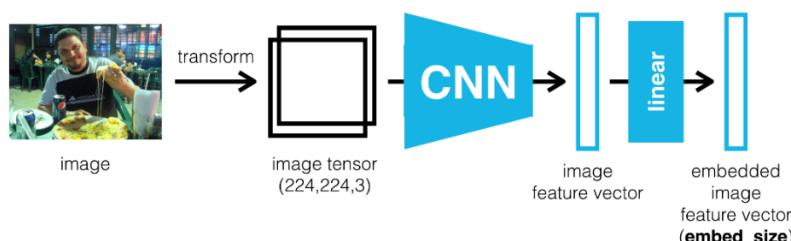
- Tù hình ảnh cần tạo chủ thích, thực hiện tiền xử lý hình ảnh sau đó trích xuất vec tơ đặc trưng cho hình ảnh.
- Sử dụng mạng LSTM đã được huấn luyện để phát sinh chủ thích cho hình ảnh.



Hình 1. Mô hình tạo chủ thích ảnh tự động

3.2 Mã hóa hình ảnh với CNN

Trích xuất đặc trưng của hình ảnh nhằm chọn ra những đặc trưng tốt nhất của ảnh và biểu diễn thành các vec tơ mô tả cho hình ảnh đầu vào. Việc trích xuất đặc trưng hình ảnh được tiếp cận theo nhiều phương pháp khác nhau sao cho phù hợp với từng yêu cầu bài toán. Trong lĩnh vực học máy [11, 13, 23], mạng CNN cho thấy tính hiệu quả trong việc trích xuất đặc trưng hình ảnh. Do đó, chúng tôi sử dụng mô hình huấn luyện mạng CNN để trích xuất đặc trưng của hình ảnh.

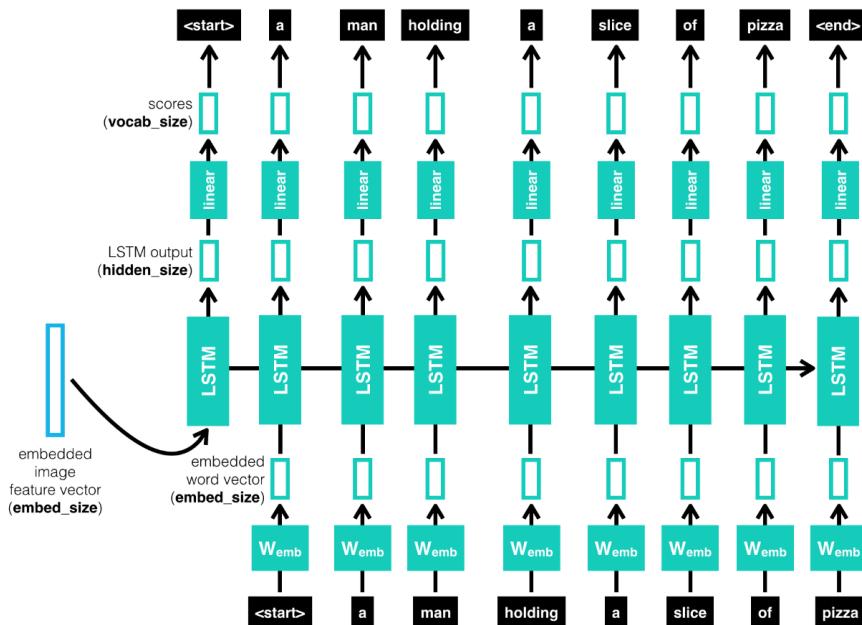


Hình 2. Mô hình encoder với CNN [24]

Các mô hình *pre-trained* thông dụng được dùng để trích xuất đặc trưng hình ảnh như: GoogLeNet [25], AlexNet [26], VGG mạng [27], ResNet [28]. Mô hình ResNet tăng độ sâu của mạng và thêm vào kiến trúc của mạng nơ ron các kết nối tắt. Sau mỗi lần tích chập thực hiện chuẩn hóa và xóa các tầng kết nối đầy đủ (*Fully Connected Layer*) thay bằng tầng gộp trung bình (*average pooling layer*) để giảm số lượng tham số. Mạng ResNet đạt được hiệu quả cao trong việc trích xuất đặc trưng [28]. Do đó, chúng tôi lựa chọn mô hình ResNet-50 cho bài toán.

3.3 Xây dựng mô hình Decoder với LSTM

Mục tiêu của mô hình *Decoder* là dự đoán xác suất của một chuỗi các từ trong câu mô tả hình ảnh. Như vậy, mô hình này là một thành phần quan trọng trong chủ thích hình ảnh. Các phương pháp phổ biến được tiếp cận trong việc xây dựng mô hình đó là RNN, GRU, LSTM, Transformer [11, 29]. Mạng RNN có vòng lặp phản hồi (các cạnh lặp lại), đầu ra ở bước thời gian hiện tại phụ thuộc vào đầu vào hiện tại cũng như trạng thái trước đó (thông qua các cạnh lặp lại) vì vậy RNN là phù hợp cho bài toán nhận dạng ngôn ngữ có cấu trúc tuần tự [11]. Theo lý thuyết, RNN có thể mang thông tin từ trạng thái trước đến trạng thái sau. Trên thực tế, RNN chỉ mang được thông tin qua một số bước nhất định do vấn đề triệt tiêu đạo hàm (*vanishing gradient*). Như vậy, RNN chỉ học được thông tin ngắn hạn (*short-term memory*). Do đó, cần một mô hình để học được thông tin dài hạn (*long-term memory*). Chúng tôi đề xuất sử dụng một biến thể của RNN là LSTM (*Long Short-Term Memory*) để khắc phục được hạn chế của mạng RNN. LSTM ngoài thành phần *short-term memory* giống RNN thì được bổ sung thêm thành phần *long-term memory*. Chính vì vậy, LSTM quản lý việc thông tin đến từ trạng thái trước sẽ được giữ lại hoặc loại bỏ (nếu thông tin không liên quan), bên cạnh đó quản lý việc học thông tin mới từ đầu vào, đồng thời quản lý việc đưa thông tin mới cập nhật vào trạng thái kế tiếp. LSTM là lựa chọn chủ yếu để xây dựng mô hình tạo chủ thích ảnh [29].



Hình 3. Mô hình decoder với LSTM [24]

Thành phần của LSTM có 3 cổng (*gate*): cổng quên (*Forget gate*); cổng vào (*Input gate*); cổng ra (*Output gate*). Bên cạnh trạng thái ẩn h_t (*hidden state*) giống RNN thì LSTM bổ sung trạng thái ô c_t (*cell state*).

Mô hình được thực hiện theo các bước sau:

(1) Xác định thông tin không cần thiết để loại bỏ

Sử dụng hàm *sigmoid* trong tầng cổng quên (*Forget Gate Layer*) để xác định thông tin cần loại bỏ, hàm này nhận giá trị đầu vào là h_{t-1} và c_t , được tính theo công thức:

$$f_t = \sigma(W_f \cdot [h_{t-1}, c_t] + b_f)$$

Giá trị trả về của hàm bằng 0 thì bỏ thông tin của ô trạng thái c_{t-1} (*forget everything*)

$$c_{t-1} * f_{t=0 \dots if f_t=0}$$

Giá trị trả về của hàm bằng 1 thì giữ lại toàn bộ thông tin của ô trạng thái c_{t-1} (*forget nothing*)

$$c_{t-1} * f_{t=c_{t-1} \dots if f_t=1}$$

(2) Chọn từ để lưu vào ô trạng thái c_t .

Bước này thực hiện chọn các giá trị cập nhật và thêm vào ô trạng thái như sau:

Sử dụng hàm *sigmoid* của tầng cổng vào (*Input Gate Layer*) để xác định các giá trị được cập nhật theo công thức sau:

$$i_t = \sigma(W_i \cdot [h_{t-1}, c_t] + b_i)$$

Sau đó, dùng hàm *tanh* trong tầng này để tạo ra một véc của một ứng viên mới \tilde{V}_t mà có thể thêm vào ô trạng thái, được thực hiện theo công thức sau:

$$\tilde{V}_t = \tanh(W_v \cdot [h_{t-1}, c_t] + b_v)$$

(3) Cập nhật ô trạng thái

Ô trạng thái được cập nhật dựa trên kết quả kết hợp của 2 tầng. Trong bước này thực cập nhật ô trạng thái mới C_t từ một ô trạng thái cũ C_{t-1} sang, được thực hiện theo công thức sau:

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$

Trong đó: $i_t * \tilde{C}_t$ là một giá trị ứng viên mới nhằm tăng hoặc giảm số lượng giá trị muốn cập nhật cho mỗi trạng thái.

(4) Chọn thông tin đầu ra

Hàm *sigmoid* của tầng ẩn tính toán chọn ra phần thông tin cần thiết của ô trạng thái làm thông tin đầu ra, lọc bỏ những thông tin không cần thiết, thực hiện theo công thức sau:

$$o_t = \sigma(W_o \cdot [h_{t-1}, c_t] + b_o)$$

Dùng hàm *tanh* để chuyển giá trị của ô trạng thái về trong khoảng [-1,1], kết quả này nhân với đầu ra của một cổng *sigmoid* nên sẽ trả về phần thông tin cần thiết được chọn, thực hiện theo công thức tính như sau:

$$h_t = o_t * \tanh(C_t)$$

4. THỰC NGHIỆM VÀ ĐÁNH GIÁ

4.1 Thực nghiệm mô hình chú thích ảnh

4.1.1. Bộ dữ liệu thực nghiệm

Bộ dữ liệu được dùng để thực nghiệm huấn luyện mô hình là ảnh MS COCO (Microsoft Common Object Context) phát hành năm 2014. Dữ liệu gồm có:

- 83000 hình ảnh huấn luyện (Train images)/ 13GB
- 41000 hình ảnh kiểm định (Val images)/ 6GB
- 41000 hình ảnh kiểm thử (Test images)/ 6GB
- Bộ chú thích tương ứng hình ảnh dành cho huấn luyện và kiểm định/ 241MB



Hình 4. Ảnh mẫu trong tập ảnh MS COCO 2014

4.1.2. Môi trường thực nghiệm

Bảng 1. Môi trường thực nghiệm

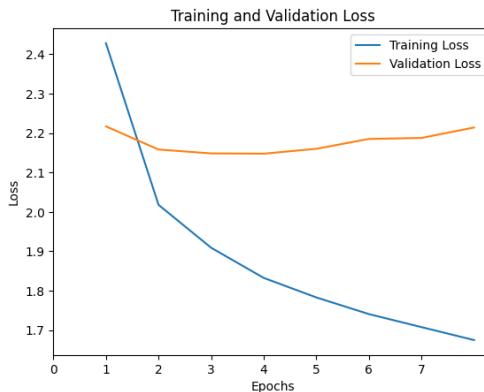
Cấu hình	Chi tiết
CPU	AMD Ryzen 7 5800HS, 3201 Mhz, 8 Core(s), 16 Logical Processor(s)
GPU	NVIDIA GeForce GTX 1650 4GB
RAM	24GB
Hệ điều hành	Windows 11

4.1.3. Kết quả thực nghiệm

Chúng tôi sử dụng độ đo BLEU (*Bilingual Evaluation Understudy*) [30] để đánh giá độ chính xác kết quả phương pháp đề xuất là 12.82. Độ đo BLEU được đánh giá cao vì có khả năng đánh giá mức độ tương tự giữa các câu dịch và các câu mẫu một cách chính xác và công bằng. Phương pháp này tính toán sự tương đồng giữa các câu dịch ra từ mô hình và các câu gốc được sử dụng làm mẫu. Thực hiện so sánh kết quả với các công trình khác đã được công bố trên cùng bộ dataset MSCOCO qua bảng 2 cho thấy kết quả của phương pháp được đề xuất có độ chính xác cao.

Bảng 2. So sánh độ chính xác mô hình tạo chú thích ảnh của phương pháp đề xuất với các công trình khác

Phương pháp	BLEU-4
Aditya Kumar Yadav [19]	8.27
Yi và Yang không có đánh giá cảm xúc [18]	6.88
Yi và Yang có đánh giá cảm xúc [18]	7.93
Nhóm tác giả đề xuất	12.82



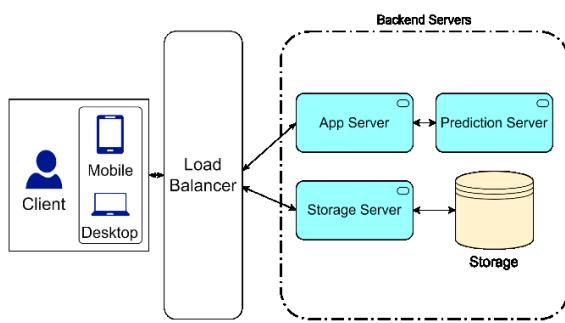
Hình 5. Training loss và validation loss

4.2 Xây dựng ứng dụng hỗ trợ người khiếm thính

4.2.1. Kiến trúc ứng dụng

Kiến trúc ứng dụng được xây dựng gồm:

- Client: người sử dụng các ứng dụng.
- Mobile, Desktop: các ứng dụng cho phép người dùng tương tác với hệ thống.
- Load Balancer (Cân bằng tải): Load balancer được dùng ở đây chủ yếu để phân phối hiệu quả lưu lượng truy cập của người dùng (client request) đến hệ thống và định tuyến (routing) client request đến đúng máy chủ (server) cần thiết.
- App Server: Máy chủ thực hiện tất cả các nghiệp vụ chính của hệ thống.
- Prediction Server: Máy chủ chịu trách nhiệm đưa ra chú thích cho hình ảnh.
- Storage Server: Máy chủ chịu trách nhiệm lưu trữ hình ảnh từ client request.



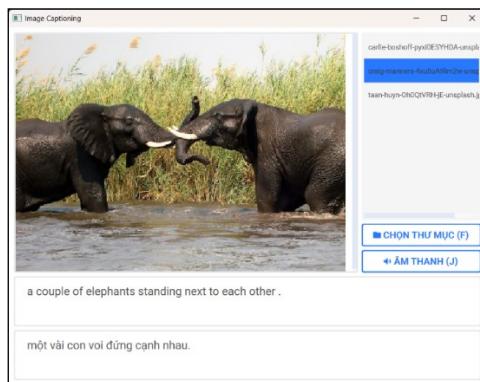
Hình 6. Kiến trúc ứng dụng

4.2.2. Giao diện ứng dụng

Ứng dụng được phát triển trên nền tảng desktop và mobile với giao diện tối giản được mô tả nhằm hỗ trợ người khiếm thị hay người già mắt kém nhận biết được cảnh vật xung quanh bằng âm thanh mô tả hình ảnh ghi nhận được.

Trên nền tảng desktop: trong lần khởi chạy đầu tiên, người dùng chỉ cần chọn tới thư mục chứa hình ảnh bằng cách chọn nút “Chọn thư mục” hoặc phím tắt “F”; những lần khởi chạy sau, ứng dụng sẽ tự động tải lên thư mục đã chọn trước đó. Thực hiện duyệt các hình ảnh khác nhau có trong thư mục bằng cách chọn chuột vào tên ảnh muốn thực hiện hoặc dùng phím “Mũi tên lên/ xuống”. Kết quả ứng dụng sẽ tự động đọc lên chú thích ảnh tương ứng

đồng thời hiển thị văn bản mô tả hình ảnh như hình 7. Người dùng muốn nghe lại chú thích ảnh, nhấn nút “Âm thanh” hoặc phím tắt “J”.



Hình 7. Kết quả tạo chú thích ảnh trên máy tính

Giao diện trên nền tảng mobile được thiết kế nhằm hỗ trợ cho người khiếm thị dễ dàng thao tác nhờ vào việc phân chia 4 vùng riêng biệt như hình 8. Khi người dùng chọn chức năng trên màn hình, ứng dụng sẽ phát ra âm thanh thông báo tên của chức năng, sau đó sẽ thực hiện thao tác tương ứng. Chức năng “Chụp” cho phép người dùng chụp hình ảnh, chức năng “Đọc” hệ thống sẽ phân tích ảnh vừa chụp và tạo mô tả cho ảnh, chức năng “Cài đặt” ứng dụng mở rộng cho phép người dùng thiết lập các chức năng điều chỉnh tốc độ đọc, giọng đọc, đọc lại hình ảnh vừa chụp,...



Hình 8. Giao diện ứng dụng di động



Hình 9. Kết quả tạo chú thích ảnh trên thiết bị di động

5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Trong bài báo này, chúng tôi đã đề xuất một phương pháp tạo chú thích ảnh. Trên cơ sở đó, phát triển ứng dụng đa nền tảng hỗ trợ người khiếm thính nhận biết được hình ảnh xung quanh thông qua âm thanh mô tả hình ảnh. Tuy nhiên, bài báo còn hạn chế độ chính xác chú thích chưa cao so với những kỹ thuật tạo chú thích hiện đại gần đây, ứng dụng sử dụng một số công nghệ miễn phí: dịch ngôn ngữ này sang ngôn ngữ khác, đọc chú thích hình ảnh sang âm thanh phụ thuộc vào bên thứ ba nên tốc độ chậm. Trong tương lai, chúng tôi cải tiến mô hình chú thích ảnh để đạt được độ chính xác cao hơn. Bên cạnh đó, mở rộng nghiên cứu với những bộ dữ liệu ảnh thực tế, ví dụ như hình ảnh y tế, vật nuôi, cây trồng.

TÀI LIỆU THAM KHẢO

1. M. Yue Ming, IEEE, Nannan Hu, Chunxiao Fan, Member, IEEE, Fan Feng, Jiangwan Zhou, and Hui Yu, Senior Member, IEEE, "Visuals to Text: A Comprehensive Review on Automatic Image Captioning," IEEE/CAA JOURNAL OF AUTOMATIC SINICA, vol. VOL. 9, no. NO. 8, 2022.
2. Z. Z. J. K. Kalita, "Neural attention for image captioning: review of outstanding methods," Springer Nature, pp. 3833–3862, 2021.
3. K. V. Pavlopoulos J, Androultsopoulos I, " A survey on biomedical image captioning," ceedings of the second workshop on shortcomings in vision and language, pp. 26–36, 2019.
4. R. Socher, A. Karpathy, Q. V. Le, C. D. Manning, and A. Y. Ng, "Grounded compositional semantics for finding and describing images with sentences," (in b-en), Transactions of the Association for Computational Linguistics, vol. 2, pp. 207-218, 2014.
5. Y. Ushiku, M. Yamaguchi, Y. Mukuta, and T. Harada, "Common subspace for model and similarity: Phrase learning for caption generation from images," in Proceedings of the IEEE international conference on computer vision, 2015, pp. 2668-2676.
6. G. Srivastava and R. Srivastava, "A survey on automatic image captioning," in Mathematics and Computing: 4th International Conference, ICMC 2018, Varanasi, India, January 9-11, 2018, Revised Selected Papers 4, 2018: Springer, pp. 74-83.
7. M. Liu, L. Li, H. Hu, W. Guan, and J. Tian, "Image caption generation with dual attention mechanism," (in b-en), Information Processing & Management, vol. 57, no. 2, p. 102178, 2020.
8. A. M. Dehaqi, V. Seydi, and Y. Madadi, "Adversarial Image Caption Generator Network," (in b-en), SN Computer Science, vol. 2, pp. 1-14, 2021.
9. S.-H. Han and H.-J. Choi, "Domain-specific image caption generator with semantic ontology," in 2020 IEEE International Conference on Big Data and Smart Computing (BigComp), 2020: IEEE, pp. 526-530.
10. X. Ke, J. Zou, and Y. Niu, "End-to-end automatic image annotation based on deep CNN and multi-label data augmentation," (in b-en), IEEE Transactions on Multimedia, vol. 21, no. 8, pp. 2093-2106, 2019.
11. M. C. Matteo Stefanini, Lorenzo Baraldi , Silvia Cascianelli , Giuseppe Fiameni , and Rita Cucchiara, "From Show to Tell: A Survey on Deep Learning-Based Image Captioning," IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, vol. VOL. 45, no. NO. 1, 2023.
12. W. L. Sen He, Hamed R. Tavakoli, Michael Yang, Bodo Rosenhahn, and Nicolas Pugeault, "Image Captioning through Image Transformer," Springer, 2020.
13. A. Z. Cong Bai, Yuan Huang, Xiang Pan, Nan Chen, "Boosting Convolutional Image Captioning with Semantic Content and Visual Relationship," Displays, 2022.

14. G. W. J. Gu, J. Cai, T. Chen, " An empirical study of language cnn for image captioning," Proceedings of the IEEE International Conference on Computer Vision, pp. 1222–1231, 2017.
15. S. Ding, S. Qu, Y. Xi, A. K. Sangaiah, and S. Wan, "Image caption generation with high-level image features," (in b-en), Pattern Recognition Letters, vol. 123, pp. 89-95, 2019.
16. M. Han, W. Chen, and A. D. Moges, "Fast image captioning using LSTM," (in b-en), Cluster Computing, vol. 22, pp. 6143-6155, 2019.
17. S. Liu, L. Bai, Y. Hu, and H. Wang, "Image captioning based on deep neural networks," in MATEC web of conferences, 2018, vol. 232: EDP Sciences, p. 01052.
18. Y. Yang, "Image captioning using compositional sentiments," (in b-en), 2019.
19. A. K. Yadav, "Image captioning using R-CNN & LSTM deep learning model," (in b-en), image, vol. 5, p. 8, 2021.
20. R. J. J. Alzubi, P. Nagrath, S. Satapathy, Soham Taneja, Paras Gupta, "Deep image captioning using an ensemble of CNN and LSTM based deep neural networks," Journal of Intelligent & Fuzzy Systems, vol. 40, no. 4, pp. 5761-5769, 2021.
21. E. H. a. R. Chellappa, "Attributes for improved attributes: A multi-task network utilizing implicit and explicit relationships for facial attribute classification," in Proc. AAAI Conf. Artificial Intelligence, vol. 31, no. 1, p. 4068–4074, 2017.
22. J. L. X. Cheng, J. eng, B. Yuan, and J. Zhou, "Scene recognition with objectness," Pattern Recognition, vol. 74, pp. 474–487, 2018.
23. J. S. Dan Ciresan Ueli Meier, "Multi-column Deep Neural Networks for Image Classification," 2020.
24. "Image Captioning." https://github.com/ntrang086/image_captioning (accessed 2022).
25. C. S. e. al, "Going deeper with convolutions," IEEE Conf. Comput. Vis. Pattern Recognit, pp. 1-9, 2015.
26. I. S. A. Krizhevsky, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," 25th Int. Conf. Neural Inf. Process. Syst, pp. 1097–1105, 2012.
27. K. S. a. A. Zisserman, "Very deep convolutional networks for large-scale image recognition," Int. Conf. Learn. Representations, 2015.
28. X. Z. K. He, S. Ren, and J. Sun, "Deep residual learning for image recognition," IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778, 2016.
29. S. H. a. J. Schmidhuber, "Long short-term memory," Neural Comput, vol. 9, no. 8, pp. 1735–1780, 1997.
30. K. Papineni, S. Roukos, T. Ward, and W.-J. Zhu, "Bleu: a method for automatic evaluation of machine translation," in Proceedings of the 40th annual meeting of the Association for Computational Linguistics, 2002, pp. 311-318.

ABSTRACT

AUTOMATIC IMAGE CAPTIONING SYSTEM FOR VISUALLY IMPAIRED

Dinh Thi Man¹, Nguyen Van Thinh², Tran Ngoc Hieu¹, Tran Thi Xinh¹,
Tran Thi Van Anh^{1,*}

¹*Ho Chi Minh City University of Food Industry*

²*Ho Chi Minh City University of Education*

*Email: anhttv@hufi.edu.vn

In this paper, we propose an automatic image captioning system based on the encoder-decoder framework. In the encoder stage, a convolution neural network (CNN) model is used to extract image features. During the decoder stage, an LSTM (Long Short-Term Memory) network model is built and trained to generate captioning for the input image. The experiment was built and evaluated on the MS COCO image dataset with the BLEU measure (4 grams). The results of the proposed method compared with recently published works show the feasibility and effectiveness. Since then, an application on desktop and mobile platforms has been developed to assist visually impaired or elderly people with low vision to recognize the surrounding scene by sound describing the recorded image.

Keywords: Image Captioning, CNN, LSTM, Word2Vect.

ỨNG DỤNG MÁY HỌC VÀO BÀI TOÁN DỰ ĐOÁN BỆNH UNG THƯ VÚ

Huỳnh Thị Châu Lan^{1,*}, Nguyễn Hải Yến¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: lanhtc@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Ung thư là một trong những căn bệnh nguy hiểm nhất cướp đi sinh mạng con người nồng nàn nhất bất chấp những tiến bộ trong lĩnh vực khoa học y tế. Trong số tất cả các loại ung thư, ung thư vú là một trong những loại phổ biến nhất đối với phụ nữ ở khắp mọi nơi trên toàn thế giới và nó là một trong những nguyên nhân hàng đầu gây tử vong ở phụ nữ. Cần có các kỹ thuật và phương pháp hiệu quả để phân tích dữ liệu nhằm đưa ra quyết định và dự đoán chính xác. Các thuật toán máy học đã đạt những kết quả vượt trội với những bài toán liên quan đến phân tích dự đoán. Mỗi kỹ thuật và thuật toán cung cấp độ chính xác khác nhau cho các bộ dữ liệu và công cụ khác nhau. Trong nghiên cứu này, chúng tôi thực hiện khảo sát ba thuật toán máy học gồm k-NN, SVM và hồi quy logistic để tìm ra thuật toán dự đoán ung thư vú có độ chính xác cao và phù hợp. Kết quả thực nghiệm cho thấy cả 3 phương pháp đều đạt độ chính xác từ 0.94 trở lên. Cụ thể, với phương pháp SVM hoàn thành hiệu suất quan trọng về độ chính xác, độ nhạy và độ đặc hiệu lần lượt là 0.95, 0.95, 0.96. Phương pháp k-NN hoàn thành hiệu suất về độ chính xác, độ nhạy và độ đặc hiệu lần lượt là 0.95, 0.97, 0.95. Hồi quy logistic hoàn thành hiệu suất về độ chính xác, độ nhạy và độ đặc hiệu lần lượt là 0.94, 0.97, 0.94.

Từ khoá: breast cancer, machine learning, classification

1. GIỚI THIỆU

Trên thế giới, ung thư vú là loại ung thư được công nhận rộng rãi nhất bên cạnh ung thư phổi và phế quản, ung thư tuyến tiền liệt, ung thư ruột kết và ung thư tuyến tụy trong số những loại ung thư khác. Ung thư vú có thể là nguyên nhân tử vong phổ biến và là loại ung thư ác tính hàng đầu phổ biến ở phụ nữ trên khắp thế giới. Nguyên nhân gây ung thư vú là đa yếu tố bao gồm cả yếu tố di truyền, hormone cân nặng, xạ trị và thậm chí cả các yếu tố sinh sản. Theo báo cáo của Tổ chức Y tế Thế giới, hàng năm có 2,1 triệu phụ nữ bị ung thư vú và cũng là nguyên nhân gây ra số ca tử vong do ung thư cao nhất ở phụ nữ [1]. Năm 2018, ước tính có 627.000 phụ nữ chết vì ung thư vú - chiếm khoảng 15% tổng số ca tử vong do ung thư ở phụ nữ [1]. Trong khi tỷ lệ phát triển ung thư vú cao hơn ở các khu vực phát triển và hiện tại tỷ lệ này đang tăng lên ở mọi khu vực trên toàn thế giới. Nhiều kỹ thuật hình ảnh được phát triển để xác định và điều trị sớm ung thư vú, đồng thời giảm tỷ lệ tử vong và nhiều phương pháp hỗ trợ chẩn đoán ung thư vú sẽ không làm tăng độ chính xác của triệu chứng.

Đứng trước những yêu cầu cần thiết có một công cụ hỗ trợ chẩn đoán sớm về căn bệnh này, nhiều công trình nghiên cứu khoa học về lĩnh vực này cũng đã ra đời.

Ch. Shravya và cộng sự [2] trong công trình nghiên cứu của mình đã chỉ ra rằng, các kỹ thuật khai thác dữ liệu đóng góp rất nhiều trong việc phát triển hệ thống như vậy. Để phân loại khỏi u lành tính và ác tính, nhóm tác giả đã sử dụng các kỹ thuật phân loại của máy học, trong đó máy được học từ dữ liệu trong quá khứ và có thể dự đoán đầu ra cho dữ liệu đầu vào mới. Bài báo này là một nghiên cứu tương đối về việc triển khai các mô hình sử dụng Logistic Regression, Support Vector Machine (SVM) và K Nearest Neighbor (KNN) được thực hiện trên tập dữ liệu lấy từ kho UCI. Đôi với các kết quả về độ chính xác, độ chính xác, độ nhạy, độ đặc hiệu và tỷ lệ dương tính giả, hiệu quả của từng thuật toán được đo lường và so sánh. Các kỹ thuật này được mã hóa bằng python và được thực thi trong Spyder, môi trường phát triển Python khoa học. Các thử nghiệm của nhóm tác giả đã chỉ ra rằng SVM là tốt nhất để phân tích dự đoán với độ chính xác là 92,7%.

Gaurav Singh [3] đã tạo ra mô hình dự đoán ung thư vú bằng nhiều thuật toán phân loại máy học khác nhau như k Nearest Neighbor (kNN), Support Vector Machine (SVM), Logistic Regression (LR) và Gaussian Naive Bayes (NB). Tác giả đã đánh giá và so sánh hiệu suất của các bộ phân loại khác nhau về độ chính xác, độ nhạy và khả năng thu hồi, điểm f1 và chỉ số Jaccard. Thực nghiệm được tác giả thực hiện trên bộ dữ liệu ung thư vú được cung cấp công khai trên Kho lưu trữ máy học UCI. Kết quả thực nghiệm cho thấy thuật toán máy học kNN đạt được hiệu suất đáng kể đối với tất cả các tham số.

Neelam S. và cộng sự [4] cũng thực hiện một cuộc điều tra so sánh các thuật toán máy học khác nhau để tìm ra thuật toán dự đoán ung thư vú có độ chính xác cao và phù hợp. Các thuật toán mà nhóm tác giả nghiên cứu là kNN, Cây quyết định, SVM và Rừng ngẫu nhiên.

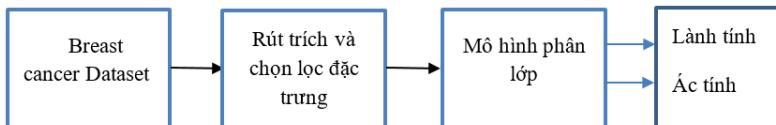
Benbrahim và cộng sự [5] đã sử dụng mạng nơ-ron nhân tạo vào bài toán phân loại bệnh và cho độ chính xác 96,49%. Deepika và cộng sự [6] sử dụng hai thuật toán phân loại Naive Bayes và Multi-Layer Perceptron, sau khi phân tích hiệu năng của cả hai thuật toán nhận thấy Naive Bayes cho kết quả chính xác hơn. Mariam và cộng sự [7] sử dụng hai bộ phân loại khác nhau là Naive Bayes và k-NN để phân loại ung thư vú khi so sánh độ chính xác bằng cách sử dụng xác thực chéo và k-NN đạt được độ chính xác cao hơn phân loại Naive Bayes.

Các thuật toán máy học đã và đang được sử dụng rộng rãi trong các hệ thống dịch vụ thông minh, đặc biệt là đã được ứng dụng để chẩn đoán bệnh. Có rất nhiều thuật toán và phân loại học máy để dự đoán kết quả ung thư vú nhưng trong bài viết này, chúng tôi nghiên cứu và ứng dụng ba kỹ thuật máy học (k Nearest Neighbors, Support Vector Machine và Logistic Regression) vào bài toán dự đoán bệnh ung thư vú, thực nghiệm được tiến hành với bộ dữ liệu "breast cancer" [9] công khai trên UCI.

Một cách cụ thể, bài báo có những đóng góp chính như sau: Cung cấp một cách nhìn tổng quát về các phương pháp phổ biến được ứng dụng trong lĩnh vực chăm sóc sức khỏe thời gian gần đây. Đồng thời cũng chỉ ra các phương pháp phân loại khác nhau có những ưu điểm và nhược điểm, và tùy theo đặc tính của dữ liệu, cần cân nhắc việc sử dụng các bộ phân loại thích hợp để đạt được hiệu suất cao nhất. Phần còn lại của bài báo được tổ chức như sau: trong phần 2 chúng tôi trình bày gián lược một số kỹ thuật đại diện cho học có giám sát để phân nhóm các bệnh; phần 3 trình bày về kết quả thực nghiệm và bàn luận, phần 4 kết luận.

2. PHƯƠNG PHÁP NGHIÊN CỨU

Trong hình 1 cho thấy mô hình phân loại ung thư vú với các phương pháp học máy, đầu tiên bộ dữ liệu ung thư vú được tải vào sau đó tiến hành thực hiện rút trích và chọn lọc đặc trưng mô hình phân loại thường được đào tạo và sử dụng để dự đoán lành tính và ác tính. Các trường hợp lành tính được coi là không ung thư, không nguy hiểm. Ung thư có hại bắt đầu với sự phát triển tế bào bất thường và có thể nhanh chóng lan rộng hoặc tấn công các mô lân cận khiến nó thường nguy hiểm.



Hình 1. Mô hình phân loại ung thư vú

2.1. Máy vectơ hỗ trợ SVM (Support Vector Machine)

SVM là một thuật toán học máy có giám sát được sử dụng rất phổ biến ngày nay trong các bài toán phân lớp (classification) hay hồi quy (Regression) [10]. SVM được đề xuất bởi Vladimir N. Vapnik và các đồng nghiệp của ông vào năm 1963 tại Nga và sau đó trở nên phổ biến trong những năm 90 nhờ ứng dụng giải quyết các bài toán phi tuyến tính (nonlinear) bằng phương pháp Kernel Trick.

Ý tưởng chính của SVM là xây dựng một siêu phẳng để phân tách và tối đa hóa lề của các lớp dương (có nguy cơ) và âm (không có nguy cơ) với lề lớn nhất. Giả sử $\{(x_i, y_i)\}_{i=1}^N$ là tập mẫu huấn luyện mà chứa các thuộc tính phân biệt nhất, (x_i, y_i) là đặc trưng đầu vào thứ i và đầu ra tương ứng của nó. Ranh giới quyết định sự phân tách được thực hiện thông qua phương trình:

$$w^T x_i + b \geq 0 \text{ với } y_i = +1 \text{ (lớp dương)} \quad (1)$$

$$w^T x_i + b < 0 \text{ với } y_i = -1 \text{ (lớp âm)} \quad (2)$$

Trong đó, w là một vector trọng số điều chỉnh, x là vector đầu vào và b là một hằng số (bias). Vấn đề tối ưu hóa của SVM có thể được định nghĩa như sau:

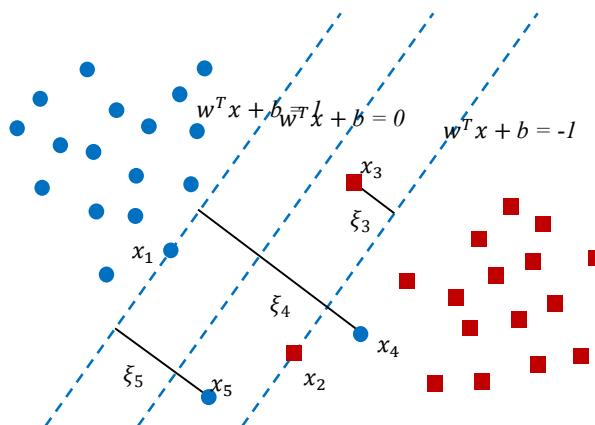
$$(w, b) = \arg \min_{w, b} \frac{1}{2} \|w\|_2^2 \text{ s.t. } y_i(w^T \cdot x_i + b) \geq 1, \forall i = 1, 2, \dots, N. \quad (3)$$

SVM thường làm việc với các đặc trưng tách biệt tuyến tính. Tuy nhiên, trong một số trường hợp khi có nhiều, đặc trưng thuộc về một lớp mà rất gần với lớp khác. Với trường hợp này, SVM sẽ tạo ra một siêu phẳng có lề rất nhỏ, rất nhạy với nhiễu. Nếu thuật toán loại bỏ được nhiễu thì SVM có thể tạo ra một siêu phẳng với biên độ tốt hơn để phân tách tốt nhất hai lớp. Một số trường hợp khác là khi hai lớp có thể phân tách tuyến tính gần nhau, trong đó tồn tại một số lượng nhỏ các trường hợp xuất hiện không đáng tin cậy, thuật toán tối ưu hóa lề SVM là không khả thi. Tương tự, nếu thuật toán bỏ qua các trường hợp đó, SVM cũng tạo ra một lề tốt hơn mà hầu hết có thể tách hai lớp. Kỹ thuật này được gọi là SVM với lề mềm. Việc hình thành bài toán tối ưu hóa SVM có thể được viết lại như sau:

$$(w, b, \xi) = \arg \min_{w, b, \xi} \frac{1}{2} \|w\|_2^2 + C \sum_{i=1}^N \xi_i \text{ s.t. } 1 - \xi_i - y_i(w^T \cdot x_i + b) \geq 1, \\ \forall i = 1, 2, \dots, N, \xi_i \geq 0, C > 0 \quad (4)$$

Trong đó C là hằng số được sử dụng để tránh vượt quá giới hạn, $\xi = [\xi_1, \xi_2, \dots, \xi_N]$ là tập hợp các biến slack. Như được hiển thị trong Hình 3, đối với các biến nằm trên lề an toàn, thì

$\xi_i = 0$ (ví dụ: x_1, x_2). Đối với các biến không nằm trong lề an toàn, nhưng vẫn ở phía bên phải của lớp, thì $0 < \xi_i < 1$ (ví dụ x_3). Đối với các biến số nằm ở bên trái của lớp thì $\xi_i > 1$ (ví dụ: x_4, x_5).



Hình 2. SVM với kernel mềm cho các trường hợp khác nhau của biên slack [10]

2.2. Phương pháp k-NN (k Nearest Neighbor)

Thuật toán k lảng giềng gần nhất sử dụng 'tính tương tự' của đặc trưng để phân lớp. Ý tưởng của phương pháp k-NN là với mẫu dữ liệu mới tiến hành tính khoảng cách với từng mẫu trong tập dữ liệu huấn luyện; sau đó chọn ra k mẫu đầu tiên sau khi đã sắp xếp chúng theo thứ tự tăng dần khoảng cách. Cuối cùng là thống kê và chọn lớp có số lượng lớn nhất.

Các công thức được dùng để tính khoảng cách gồm:

$$\text{Khoảng cách Euclidean: } \sqrt{\sum_{i=1}^n (x_i - y_i)^2} \quad (5)$$

$$\text{Khoảng cách Manhattan: } \sum_{i=1}^n |x_i - y_i| \quad (6)$$

$$\text{Khoảng cách Minkowski: } (\sum_{i=1}^n |x_i + y_i|^p)^{1/p} \quad (7)$$

2.3. Hồi quy Logistic (Logistic Regression - LR)

Phân loại là quá trình xây dựng mô hình các lớp từ một tập hợp các mẫu dữ liệu đã có chừa nhãn lớp. Hồi quy logistic là một thuật toán phân loại học có giám sát được sử dụng để dự đoán xác suất của một biến mục tiêu. Có nhiều loại hồi quy logistic khác nhau tuỳ thuộc vào số lớp dự đoán. Nếu số lớp dự đoán chỉ có hai lớp thì ta dùng mô hình hồi quy logistic nhị thức; nếu số lớp dự đoán lớn hơn hai thì ta sử dụng mô hình hồi quy logistic đa thức.

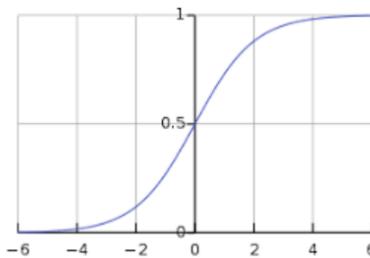
Dạng đơn giản nhất của hồi quy logistic là hồi quy logistic nhị thức, trong đó biến mục tiêu chỉ có thể nhận một trong hai giá trị là 1 hoặc 0 thông qua hàm *Sigmoid*.

$$h_\theta(x) = g(\theta^T x), \quad (8)$$

trong đó $0 \leq h_\theta \leq 1$ và g là hàm *Sigmoid*

$$g(z) = \frac{1}{1+e^{-z}} \text{ với } z = \theta^T x \quad (9)$$

Đường cong *Sigmoid* có thể được biểu diễn bằng biểu đồ sau.



Hình 3. Biểu đồ đường cong Sigmoid

3. THỰC NGHIỆM VÀ BÀN LUẬN

3.1. Dữ liệu

Tập dữ liệu thực nghiệm được lấy từ kho lưu trữ học máy của UCI [9]. Tập dữ liệu có tất cả 699 mẫu thuộc vào 2 lớp khác nhau: có bệnh (241 mẫu) và không có bệnh (458 mẫu). Tập dữ liệu có các thuộc tính:

Bảng 1. Mô tả 11 thuộc tính của bộ dữ liệu ung thư vú

STT	Thuộc tính	Miền giá trị	STT	Thuộc tính	Miền giá trị
1	Sample code number	Id number	7	Bare Nuclei	1 - 10
2	Clump Thickness	1 - 10	8	Bland Chromatin	1 - 10
3	Uniformity of Cell Size	1 - 10	9	Normal Nucleoli	1 - 10
4	Uniformity of Cell Shape	1 - 10	10	Mitoses	1 - 10
5	Marginal Adhesion	1 - 10	11	Class	2 hoặc 4
6	Single Epithelial Cell Size	1 - 10			

Thuộc tính Sample code number là mã định danh bệnh nhân. Kết quả các xét nghiệm tế bào từ mọi bệnh nhân được ghi nhận từ thuộc tính thứ 2 đến thuộc tính thứ 10. Các giá trị được đánh giá từ 1 đến 10, với 1 là giá trị gần nhất để bắt đầu. Thuộc tính thứ 11 là thuộc tính phân lớp. Nếu bệnh nhân bị ung thư thì nhận giá trị 4, ngược lại thì có giá trị 2.

3.2. Đánh giá thực nghiệm

Dựa vào độ chính xác, độ nhạy và độ đặc hiệu để đánh giá hiệu suất phân loại của hệ thống chẩn đoán bệnh dựa trên các phương pháp SVM, k-NN và LR.

Bảng 2. Ma trận nhầm lẫn

		Predicted Class	
		Class = No	Class = Yes
Actual Class	Class = No	True Negative (TN)	False Positive (FP)
	Class = Yes	False Negative (FN)	True Positive (TP)

Độ chính xác, độ nhạy và độ đặc hiệu cụ thể được xác định như sau:

$$\text{Độ chính xác (Accuracy)} = \frac{TP + TN}{TP + FP + FN + TN} \quad (7)$$

$$\text{Độ nhạy (Recall)} = \frac{TP}{TP + FN} \quad (8)$$

$$\text{Độ đặc hiệu (Precision)} = \frac{TN}{TN + FP} \quad (9)$$

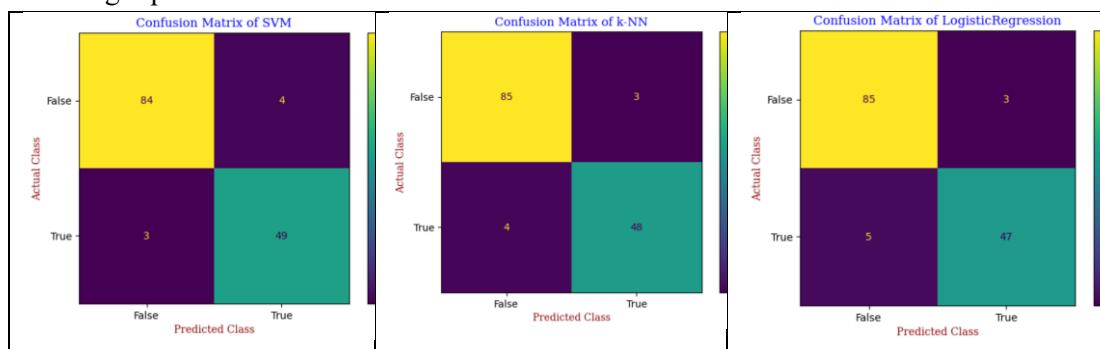
Trong đó: TP, FP, TN và FN lần lượt là True Positive, False Positive, True Negative và False Negative. Trong nghiên cứu này, chúng tôi xét hiệu suất tốt nhất dựa trên ba độ đo: độ chính xác và độ nhạy và độ đặc hiệu.

Các thực nghiệm trong bài báo được thực hiện trên ngôn ngữ Python.

3.2.1. Mô tả thực nghiệm

Trong nghiên cứu này, chúng tôi tiến hành thực nghiệm trên bộ dữ liệu bệnh ung thư vú như đã mô tả ở trên gồm 11 thuộc tính. Trong đó, 80% dữ liệu được dùng để huấn luyện và 20% dữ liệu còn lại được dùng để kiểm thử. Tiếp theo chúng tôi áp dụng lần lượt các phương pháp máy học SVM, k-NN và LR trên tập dữ liệu đa phân chia và kết quả ma trận nhầm lẫn thu được ở hình 2.

Ma trận nhầm lẫn (Confusion matrix): là một bản tóm tắt các kết quả dự đoán cho bài toán phân loại. Số dự đoán đúng và sai được tóm tắt bằng các giá trị đếm và được chia nhỏ theo từng lớp.



Hình 4. Kết quả thực nghiệm Confusion matrix của ba phương pháp học máy

Với bộ dữ liệu test bao gồm 140 mẫu, trong đó có 88 mẫu không mắc ung thư và 52 mẫu có mắc ung thư. Chúng tôi nhận thấy rằng, với phương pháp SVM thì 88 mẫu không mắc bệnh mô hình dự đoán đúng 84 mẫu và sai 4 mẫu, còn với 52 mẫu có bệnh thì dự đoán đúng 49 mẫu và 3 mẫu đoán sai. Phương pháp k-NN thì tỷ lệ dự đoán đúng 85/88 với mẫu không có bệnh và 48/52 với mẫu có bệnh. Sau cùng là phương pháp hồi quy Logistic thì tỷ lệ dự đoán đúng 85/88 với mẫu không có bệnh và 47/52 với mẫu có bệnh.

3.2.2. Kết quả thực nghiệm

Độ chính xác của bộ phân loại là tỷ lệ mức độ mà bộ phân loại có thể dự đoán chính xác các mẫu vào đúng phân loại của chúng. Đó là số dự đoán đúng được phân tách bằng toàn bộ số trường hợp trong tập dữ liệu. Độ chính xác của phương pháp được tính dựa vào công thức (7).

Bảng 3. Kết quả thực nghiệm dựa vào độ chính xác

Phương pháp	ACC	Recall	Precision
SVM	0.95	0.95	0.96
k-NN	0.95	0.97	0.95
LR	0.94	0.97	0.94

Kết quả thực nghiệm thể hiện, với phương pháp SVM hoàn thành hiệu suất quan trọng về độ chính xác, độ nhạy và độ đặc hiệu lần lượt là 0.95, 0.95, 0.96. Phương pháp k-NN hoàn thành hiệu suất về độ chính xác, độ nhạy và độ đặc hiệu lần lượt là 0.95, 0.97, 0.95. Hồi quy logistic hoàn thành hiệu suất về độ chính xác, độ nhạy và độ đặc hiệu lần lượt là 0.94, 0.97, 0.94.

4. KẾT LUẬN

Trong bài báo này, chúng tôi đã tiến hành so sánh các kết quả phân loại bệnh ung thư vú dựa trên ba tham số về độ chính xác, độ nhạy và độ đặc hiệu của ba thuật toán máy học là k lảng ghieng gần nhất, máy vector hỗ trợ và hồi quy logistic. Thực nghiệm được tiến hành trên bộ dữ liệu ung thư vú sẵn có tại UCI Machine Learning Repository Wisconsin. Mục tiêu của phân tích so sánh này là để tìm ra thuật toán học máy có độ chính xác cao nhất dùng để chẩn đoán ung thư vú. Kết quả thực nghiệm cho thấy k-NN và SVM cho kết quả về độ chính xác cao hơn phương pháp hồi quy logistic trên bộ dữ liệu thực nghiệm.

Như vậy, chúng tôi đã khảo sát và áp dụng thành công một số kỹ thuật máy học trong hỗ trợ chăm sóc khỏe cộng đồng trên dữ liệu cận lâm sàng. Bộ dữ liệu sử dụng trong thực nghiệm của bài báo này là bộ dữ liệu công cộng dành cho nghiên cứu về y khoa, nhưng xét về mặt đặc tính thì các thông tin của bệnh nhân đều khá tương đồng giữa các chủng tộc người khác nhau trên thế giới, do đó kết quả của bài báo này có thể áp dụng tốt trong hỗ trợ các bác sĩ chẩn đoán bệnh tại Việt Nam. Công việc tương lai của chúng tôi là tiếp tục khảo sát thêm những kỹ thuật phân loại dữ liệu khác, từ đó tìm ra thêm những kỹ thuật phân loại dữ liệu tốt nhất trên nhiều tập dữ liệu chăm sóc sức khỏe khác nhau. Ngoài ra, chúng tôi sẽ tiến hành thu thập thêm các dữ liệu tại Việt Nam để có thể hỗ trợ tốt nhất cho quy trình khám chữa bệnh ở Việt Nam.

TÀI LIỆU THAM KHẢO

1. WHO – Breast Cancer <https://www.who.int/cancer/>
2. Shravya Ch., Pravalika K., Shaik S. - Prediction of Breast Cancer Using Supervised Machine Learning Techniques, IJITEE, ISSN: 2278-3075 Vol 8 (Issue 6) (2019).
3. Gaurav S. - Breast Cancer Prediction Using Machine Learning, Int J Sci Res CSE & IT, Vol 6 (Issue4) (2020), 278-284
4. Neelam S., Vijay L. T., Vandana R., Umang G. - A Comparative Study Of Supervised Machine Learning Approaches, Ilkogretim Online - Elementary Education Online, Vol 20 (Issue 4) (2021), 3933-3941
5. Benbrahim H., Hachimi H., Amine A. - Algorithms Using the Breast Cancer Dataset, Springer, Comparative Study of Machine Learning (2020).
6. Deepika V., Nidhi M. - Comparative analysis of breast cancer and hypothyroid dataset using data mining classification techniques, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (2017).
7. Mariam A., Saliha O., Ikram G., Tolga E. - Breast cancer classification using machine learning, Electric Electronics, Computer Science, Biomedical Engineerings, Meeting (EBBT) (2018).
8. Aruna S., Rajagopalan S., Nandakishore L. - Knowledge based analysis of various statistical tools in detecting breast cancer, Computer Science Information Technology (2011).
9. Dr. William H. Wolberg (physician) University of Wisconsin Hospitals Madison, Wisconsin, USA <http://archive.ics.uci.edu/ml/datasets.php>
10. Hung L.M., Toan T.Đ., Lang T.V. - Automatic heart disease prediction using feature Selection and data mining technique, Journal of Computer Science and Cybernetics, ISSN: 1813-9663 (2018).

ABSTRACT

APPLYING MACHINE LEARNING TO BREAST CANCER PREDICTION

Huynh Thi Chau Lan^{1,*}, Nguyen Hai Yen¹

¹*HoChiMinh City University of Food Industry*

*Email: lanhtc@hufi.edu.vn

Cancer is one of the deadliest diseases that take the most lives despite advances in the field of medical science. Among all types of cancer, breast cancer is one of the most common among women everywhere worldwide and it is one of the leading causes of death among women. Effective techniques and methods are needed to analyze data to make accurate decisions and predictions. Machine learning algorithms have achieved outstanding results with problems related to predictive analytics. Each technique and algorithm provide different accuracy for different data sets and tools. In this study, we study three machine learning algorithms including k-NN, SVM and Logistic Regression to find a breast cancer prediction algorithm with high accuracy and relevance. Experimental results show that all 3 methods have an accuracy of 0.94 or more. Specifically, with the SVM method performance for accuracy, sensitivity and specificity are 0.95, 0.95, 0.96, respectively; with the k-NN method performance for accuracy, sensitivity and specificity are 0.95, 0.97, and 0.95. The performance for accuracy, sensitivity, and specificity of Logistic regression are 0.94, 0.97, and 0.94.

Keywords: breast cancer, machine learning, classification

XÂY DỰNG HỆ THỐNG DỰ ĐOÁN KẾT QUẢ HỌC TẬP CỦA SINH VIÊN NHẰM HỖ TRỢ CÔNG TÁC CỐ VẤN HỌC TẬP

Ngô Thanh Hùng¹, Nguyễn Thị Thu Tâm^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm TP.HCM

*Email: tamntt@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trong quá trình học tập và nghiên cứu, tìm hiểu các phương pháp thực hiện bài toán dự đoán kết quả học tập của sinh viên, nhận thấy rằng còn có thể xây dựng hệ thống dự đoán dựa trên hệ thống tư vấn với bộ lọc cộng tác (collaborative filtering) kết hợp với kỹ thuật phân rã ma trận (Matrix Factorization). Tuy nhiên trên thực tế những công trình nghiên cứu kết hợp Collaborative filtering với Matrix Factorization trong lĩnh vực giáo dục không nhiều, chủ yếu là trong lĩnh vực thương mại. Vì vậy nghiên cứu này hướng tới việc tìm hiểu hệ thống tư vấn, tập trung vào cách tiếp cận lọc cộng tác dựa trên phép phân rã ma trận. Áp dụng phương pháp này để xây dựng một hệ thống dự đoán kết quả học tập của sinh viên dựa trên kết quả học tập trước đó của sinh viên.

Từ khóa: Khai phá dữ liệu, lọc cộng tác, kỹ thuật phân rã ma trận, dự đoán kết quả học tập

1. MỞ ĐẦU

Xã hội ngày càng phát triển, đòi hỏi con người không ngừng tiến bộ, không ngừng tiếp thu học hỏi. Cho nên khi tổ chức đào tạo giáo dục, chủ trương đào tạo ở nước ta đã lòng ghép nhiều môn học từ khái quát đến chuyên sâu trong một ngành nghề để sinh viên ngoài kiến thức chuyên môn còn có thể mở rộng hiểu biết cho những nhóm nghề lân cận. Riêng đối với công tác đào tạo tại trường Cao Đẳng Kinh Tế - Kỹ Thuật Thủ Đức, nhà trường đã chọn những môn cơ sở đến chuyên ngành trong một ngành nghề; như đối với ngành công nghệ thông tin tại trường gồm các môn cơ sở : Chính trị, Pháp luật, Thể dục, Kỹ năng Ứng dụng Công nghệ Thông tin, Lập trình cơ bản,; các môn chuyên ngành: Thiết kế Web, Đồ họa máy tính, ... Tuy nhiên khả năng tiếp thu của mỗi người là không giống nhau. Không phải môn nào sinh viên cũng có thể tiếp thu được và làm tốt tất cả các môn học. Vì vậy, tình trạng sinh viên đạt điểm kém, thậm chí bị rớt phai thi lại thậm chí là học lại rất nhiều. Nhận thấy được tình trạng trên, nhà trường cũng đã tổ chức các buổi học tập nhằm ôn lại kiến thức cho sinh viên với sự giúp đỡ của cố vấn học tập. Một điều cần lưu ý đó là sinh viên đạt điểm kém thường thì sau khi thi hết môn mới biết được kết quả, cho nên công tác giáo vụ thường là công tác khắc phục hậu quả, chứ không dự đoán cho sinh viên biết sẽ rớt môn nào để sinh viên kịp thời chấn chỉnh để có kết quả học tập tốt nhất.

Vì vậy mục tiêu của đề tài này là “Xây dựng hệ thống dự đoán kết quả học tập của sinh viên nhằm hỗ trợ công tác cố vấn học tập” trong trường Cao Đẳng Kinh Tế - Kỹ Thuật Thủ Đức. Nhằm giúp đỡ giáo vụ khoa trong công tác tư vấn, dự đoán kết quả cho sinh viên, giúp

cho sinh viên đạt được kết quả học tập tốt, mặt khác giúp cho nhà trường giảm bớt nguồn kinh phí cho công tác thi lại, học lại của sinh viên đồng thời nâng cao chất lượng đào tạo chung cho nhà trường. Mục tiêu của đề tài hướng tới là những vấn đề sau:

- Xây dựng hệ thống dự đoán tự động dựa trên kết quả học tập của sinh viên áp dụng mô hình lọc cộng tác dựa trên phép phân rã ma trận;
- Giải quyết vấn đề cold-start bằng cách sử dụng thêm các thông tin về phẩm chất cá nhân của sinh viên khi dự đoán điểm các môn học trong học kỳ đầu tiên.
- Xây dựng phần mềm hỗ trợ công tác tư vấn thông qua việc cảnh báo sinh viên về những môn học được dự báo là sẽ đạt điểm kém trong học kỳ tiếp theo.

2. CƠ SỞ LÝ THUYẾT

2.1. Giới thiệu về hệ thống tư vấn

2.1.1. Lọc dựa trên nội dung (content - based filtering - CB)

Lọc theo nội dung là phương pháp thực hiện dựa trên việc so sánh nội dung thông tin hay mô tả hàng hoá, nhằm tìm ra những sản phẩm tương tự những sản phẩm mà người dùng từng quan tâm để giới thiệu cho họ. Trong đó, mỗi sản phẩm được biểu diễn bằng một hồ sơ sản phẩm, mỗi người dùng được biểu diễn bằng một tập hồ sơ người dùng. Phương pháp dự đoán trên nội dung chủ yếu là xem xét các hồ sơ sản phẩm có mức độ phù hợp với hồ sơ người dùng

Bài toán lọc theo nội dung được phát biểu như sau: Cho $P = \{p_1, p_2, \dots, p_n\}$ là tập gồm n sản phẩm. Nội dung sản phẩm được ký hiệu là $p \in P$ được biểu diễn thông qua tập K đặc trưng của P . Tập các sản phẩm được xây dựng bằng kỹ thuật truy vấn thông tin để thực hiện mục đích dự đoán sản phẩm tương tự với p . Cho $U = \{u_1, u_2, \dots, u_m\}$ là tập gồm m người dùng. Với mỗi người dùng $u \in U$, gọi $\text{ContentBasedProfile}(u)$ là hồ sơ của người dùng. Hồ sơ của người dùng u thực chất là lịch sử truy cập hoặc đánh giá của người dùng u đối với các sản phẩm (i). Hồ sơ của người dùng được xây dựng bằng cách phân tích nội dung các sản phẩm mà người dùng (u) đã từng truy cập hoặc đánh giá dựa trên các kỹ thuật truy vấn thông tin.

Bài toán lọc theo nội dung khi đó là bài toán dự đoán những sản phẩm mới có nội dung thích hợp với người dùng dựa trên tập hồ sơ sản phẩm (P) và hồ sơ người dùng $\text{ContentBasedProfile}(u)$.

Bài toán lọc cộng tác: Cho $U = \{u_1, u_2, \dots, u_n\}$ là tập gồm n người dùng, $P = \{p_1, p_2, \dots, p_m\}$ là tập gồm m sản phẩm mà người dùng có thể lựa chọn. Mỗi sản phẩm được ký hiệu là $p_i \in P$. Ký hiệu $R = \{r_{ij}\}$, là ma trận đánh giá của người dùng cho sản phẩm $p_i \in P$ bằng một số r_{ij} . Giá trị r_{ij} phản ánh mức độ ưa thích của người dùng u đối với sản phẩm i . Giá trị r_{ij} có thể thu thập trực tiếp thông qua cơ chế phản hồi của người dùng. Giá trị $r_{ij} = \emptyset$ trong trường hợp người dùng u chưa đánh giá hoặc chưa bao giờ biết đến sản phẩm i .

2.1.2. Mô hình phân rã ma trận

Về cơ bản, phân rã ma trận đặc trưng cho cả user và item bởi các vector các yếu tố được suy diễn từ các mô hình đánh giá item. Sự tương đồng cao giữa các yếu tố người dùng và sản phẩm sẽ tạo ra tư vấn. Phương pháp này trở nên phổ biến trong những năm gần đây do xử lý tốt dữ liệu có kích thước lớn và cho ra các khuyến nghị chính xác, cũng như tính linh động khi tạo mô hình cho nhiều tình huống trong đời sống thực.

Dữ liệu đầu vào cho các hệ tư vấn có nhiều kiểu và thường được biểu diễn trong một ma trận 2 chiều với một chiều biểu diễn cho các người dùng và chiều còn lại là các hạng mục được người dùng quan tâm. Có 2 phương pháp thu thập dữ liệu. Thu thập dữ liệu trực tiếp qua thông tin phản hồi trực tiếp (explicit feedback) từ phía người dùng về quan tâm của họ dành cho sản phẩm. Các quan tâm này thường được đặc trưng bởi các con số được gọi là điểm đánh giá. Ma trận điểm đánh giá từ thu thập trực tiếp thường là các ma trận thưa vì bất kỳ một người dùng nào cũng thường có xu hướng chỉ đánh giá một tỉ lệ nhỏ các hạng mục có sẵn. Trường hợp không thu thập dữ liệu trực tiếp được, hệ tư vấn sẽ phải thu thập dữ liệu gián tiếp (implicit feedback) để suy diễn ra các quan tâm của người dùng bằng cách quan sát thái độ của người dùng trong quá khứ từ các dữ liệu lịch sử mua, duyệt các dữ liệu này để tìm kiếm các mô hình, ... Dữ liệu gián tiếp thường là có hoặc không có một sự kiện nào đó nêu ma trận dữ liệu là một ma trận dày đặc. Điểm mạnh của phương pháp phân rã ma trận là khả năng cho phép kết hợp thông tin bổ sung, tránh hiện tượng ramp-up cho hệ tư vấn.

Giả sử ta có mỗi người dùng đã cho điểm đánh giá cho một số hạng mục trong hệ thống, ta sẽ dự báo xem các người dùng sẽ cho điểm đánh giá như thế nào cho các hạng mục mà họ chưa đánh giá, nghĩa là ta sẽ tư vấn (dự báo) cho các người dùng này đánh giá các hạng mục chưa được họ đánh giá. Các thông tin đánh giá sẽ được lưu trữ trong một ma trận. Bảng 1 là một ví dụ về ma trận điểm đánh giá gồm có 4 người dùng và 4 hạng mục.

Tác vụ dự báo được xem như là công việc lắp đầy cho ma trận. Ta có thể khám phá các đặc tính (yếu tố) tiềm ẩn qua việc dự báo điểm đánh giá mà một người dùng nào đó đánh giá một hạng mục nào đó, vì các đặc tính mà người dùng quan tâm sẽ trùng khớp các đặc tính của hạng mục đó.

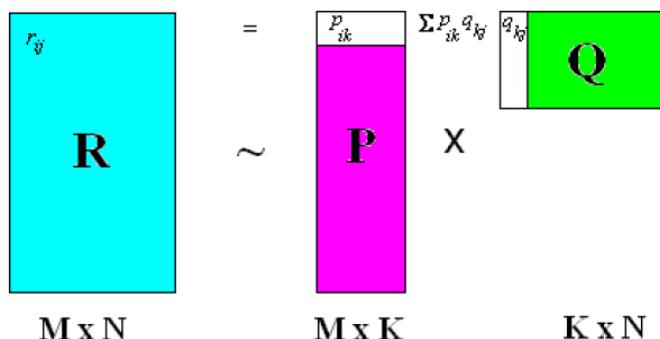
Bảng 1. Ma trận điểm đánh giá

	D1	D2	D3	D4
U1	5	3	-	1
U2	4	-	-	1
U3	1	1	-	5
U4	1	-	-	4

(Đầu (-) có nghĩa là người dùng U_i chưa cho điểm đánh giá hạng mục D_j .)

Phân rã ma trận ánh xạ người dùng và hạng mục sang một không gian có hướng f các yếu tố tiềm ẩn kết hợp với nhau, nghĩa là tương quan người dùng-hạng mục được mô hình thành tích vô hướng bên trong không gian đó. Đặt U là tập các người dùng, D là tập các hạng mục, khi đó ma trận R có kích thước $|U| \times |D|$ là ma trận chứa tất cả các điểm đánh giá thu thập được mà các người dùng đã đánh giá các hạng mục.

Ý tưởng chính của mô hình phân rã ma trận trong xây dựng hệ tư vấn là xem ma trận điểm đánh giá R là kết quả nhân từ 2 ma trận có hạng nhỏ hơn P và Q. Ma trận P gọi là ma trận cơ sở người dùng với mỗi hàng trong P tượng trưng cho một người dùng. Các giá trị p_{ik} trong vector hàng i của P biểu thị mức độ quan tâm của người dùng i đến đặc tính k của hạng mục. Ma trận Q là ma trận đặc tính của hạng mục với mỗi cột trong Q tượng trưng cho một hạng mục. Các giá trị q_{kj} trong cột j biểu thị mức độ thuộc về của đặc tính k với hạng mục j . Hình 1 minh họa cho ý tưởng này. Như vậy từ ma trận R ban đầu, ta có thể phân rã ra thành 2 ma trận P và Q có hạng thấp hơn. Sau đó tìm P và Q sao cho phép nhân PQ xấp xỉ với R.



Hình 1. Mô hình phân rã ma trận

Giả sử ta cần khám phá K đặc tính tiềm ẩn ($K < |U|, |D|$), khi đó ta sẽ tìm 2 ma trận $P|U| \times K$ và $Q|D| \times K$ sao cho tích $P \times Q$ xấp xỉ được ma trận R, nghĩa là:

$$R \approx P \times QT = \hat{R} \quad (2.1)$$

Mỗi hàng của P biểu diễn mức độ quan tâm của người dùng với các đặc tính. Mỗi hàng của Q biểu diễn mức độ thuộc về của các đặc tính trong các hạng mục. Để dự báo điểm đánh giá của người dùng ui dành cho hạng mục dj, ta sẽ tính tích vô hướng của hai vector tương ứng với ui và dj:

$$\hat{r}_{ij} = p_i q_j^T = \sum_{k=1}^K p_{ik} q_{jk} \quad (2.2)$$

Để tìm P và Q, đầu tiên khởi tạo trị ban đầu cho P và Q, tính $M = PQ$ rồi tối thiểu hóa độ lệch giữa ma trận M với R. Mỗi lần lặp là một lần điều chỉnh P và Q để tối thiểu hóa độ lệch giữa M và R.

Các thuật toán học(Learning Algorithms) trong kỹ thuật phân rã ma trận

Có nhiều phương pháp để giảm lỗi đến cực tiểu trong mô hình phân rã ma trận. Áp dụng các phương pháp này đồng nghĩa với việc tối ưu hóa hàm mục tiêu (objective function). Phương pháp được sử dụng phổ biến trong kỹ thuật phân rã ma trận là giảm gradient ngẫu nhiên (stochastic gradient descent).

2.1. Các thuật toán học(Learning Algorithms) trong kỹ thuật phân rã ma trận

2.1.1. Phương pháp giảm GRADIENT ngẫu nhiên (Stochastic Gradient Descent)

Phương pháp này nhằm tìm điểm cực tiểu cục bộ của độ lệch bình phương giữa 2 đối tượng. Hàm mục tiêu giảm độ lệch bình phương giữa 2 đối tượng A và B được định nghĩa như sau:

$$\min f(A||B) = (A - B)^2 \quad (2.3)$$

Độ lệch được gọi là lỗi giữa điểm đánh giá ước lượng với điểm đánh giá thực tế, có thể được tính toán bằng công thức sau cho mỗi cặp user và item.

$$e_{ij}^2 = (r_{ij} - \hat{r}_{ij})^2 = (r_{ij} - \sum_{k=1}^K p_{ik} q_{kj})^2 \quad (2.4)$$

Ta xét lỗi bình phương vì điểm đánh giá ước lượng có thể có lúc cao hơn, có lúc thấp hơn điểm đánh giá thực tế gây ra hiện tượng bù trừ khi tính tổng lỗi.

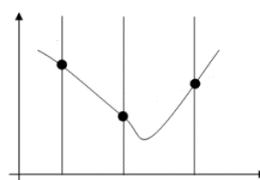
Để cực tiểu lỗi, ta phải biết hướng để chỉnh sửa các giá trị của p_{ik} và q_{kj} . Nghĩa là ta cần phải biết được gradient của các giá trị hiện tại. Lấy đạo hàm riêng cho công thức (2.4) theo các biến p_{ik} và q_{kj} , ta được:

$$\begin{aligned} \frac{\partial}{\partial p_{ik}} e_{ij}^2 &= -2(r_{ij} - \hat{r}_{ij})(q_{kj}) = -2e_{ij} q_{kj} \\ \frac{\partial}{\partial q_{kj}} e_{ij}^2 &= -2(r_{ij} - \hat{r}_{ij})(p_{ik}) = -2e_{ij} p_{ik} \end{aligned} \quad (2.5)$$

Cập nhật gradient cho các p_{ik} và q_{kj} , ta có:

$$\begin{aligned} p'_{ik} &= p_{ik} + \alpha \frac{\partial}{\partial p_{ik}} e_{ij}^2 = p_{ik} + 2\alpha e_{ij} q_{kj} \\ q'_{kj} &= q_{kj} + \alpha \frac{\partial}{\partial q_{kj}} e_{ij}^2 = q_{kj} + 2\alpha e_{ij} p_{ik} \end{aligned} \quad (2.6)$$

Trong đó α , còn gọi là bước nhảy, là hằng số mà giá trị của nó xác định tốc độ dần đến điểm cực tiểu. Giá trị α là tùy chọn và thường khá nhỏ (khoảng 0.0002). Nếu chọn bước nhảy quá lớn để tiến đến cực tiểu có thể vượt khỏi điểm cực tiểu, và dao động quanh điểm cực tiểu. Ngược lại, nếu chọn α quá nhỏ tốc độ dần đến cực tiểu quá chậm. Hình 2 cho thấy ảnh hưởng của bước nhảy trong quá trình dần đến điểm cực tiểu.



Hình 2. Ảnh hưởng của bước nhảy trong quá trình tiến đến điểm cực tiểu

Vấn đề này sinh ra cho mô hình phân rã ma trận là nếu tìm được các ma trận P và Q sao cho $P \times Q$ xấp xỉ được R thì dự báo cho các đánh giá chưa thấy có dàn về zero hết hay không? Thực tế, mô hình không đi tìm P và Q để có được R một cách chính xác, mà chỉ tối thiểu hóa lỗi của các cặp người dùng-hạng mục quan sát được. Nói cách khác, nếu đặt T là tập các bộ

có dạng (ui, dj, rij) , tức T chứa tất cả các cặp người dùng-hạng mục cùng với điểm đánh giá, ta sẽ cố gắng cực tiểu lỗi e_{ij} cho mỗi bộ $(ui, dj, rij) \in T$ (T chính là tập dữ liệu huấn luyện). Đối với các bộ chưa đầy đủ (thiếu rij), mô hình sẽ xác định các giá trị này một khi mối quan hệ giữa người dùng, hạng mục và các đặc tính được học.

Sử dụng công thức (2.5) lặp đi lặp lại nhiều lần cho đến khi lỗi hội tụ về điểm cực tiểu. Có thể kiểm tra lỗi tổng thể sau mỗi lần tính toán theo công thức sau để xác định khi nào có thể dừng được:

$$E = \sum_{(u_i, d_j, r_{ij}) \in T} e_{ij} = \sum_{(u_i, d_j, r_{ij}) \in T} (r_{ij} - \sum_{k=1}^K p_{ik} q_{kj})^2 \quad (2.7)$$

2.1.2. Phương pháp ALTERNATING LEAST SQUARE (ASL)

Do cả hai vector p_{ik} và q_{kj} đều chưa được xác định, hàm (2.4) không lõm. Tuy nhiên, nếu ta cố định một trong hai vector trên thì hàm (2.4) trở thành hàm bậc hai và có thể giải được bài toán tối ưu. Kỹ thuật ASL lần lượt luân phiên cố định p_{ik} và q_{kj} . Khi cố định p_{ik} , hệ thống sẽ tính toán lại q_{kj} bằng cách giải quyết vấn đề bình phương tối thiểu và ngược lại. Như vậy mỗi bước thực hiện sẽ giảm e_{ij} xuống cho đến khi hội tụ.

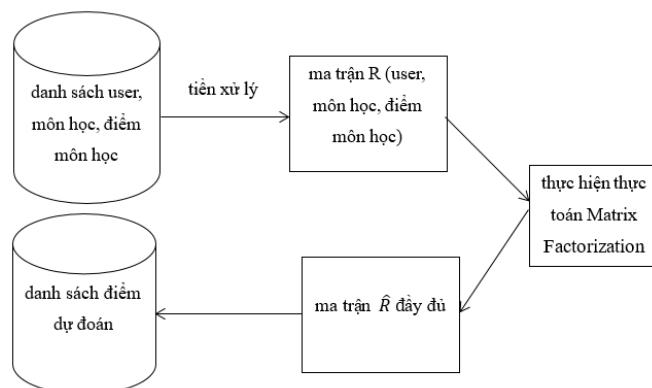
Nhìn chung, phương pháp giảm gradient ngẫu nhiên dễ cài đặt và chạy nhanh hơn phương pháp ASL, nhưng phương pháp ASL có ưu thế hơn trong ít nhất 2 trường hợp sau:

(1) Khi hệ thống có thể thực hiện song song hóa. Khi sử dụng phương pháp ASL, hệ thống sẽ tính mỗi q_{kj} và mỗi p_{ik} một cách độc lập. Điều này có thể làm phát sinh một lượng lớn tính toán song song.

(2) Khi hệ thống tập trung vào xử lý dữ liệu gián tiếp. Trong trường hợp này tập dữ liệu huấn luyện thường rời rạc, nếu thực hiện phương pháp giảm gradient ngẫu nhiên có thể xuất hiện hiện tượng loop trên mỗi trường hợp huấn luyện. Phương pháp ASL có thể xử lý tốt trường hợp này.

3. THUẬT TOÁN ĐÈ XUẤT

Bài toán dự đoán các điểm số của một sinh viên trong học kỳ tiếp theo dựa trên cơ sở dữ liệu điểm của các sinh viên khóa trước và điểm các học kỳ trước đó (nếu có) của sinh viên cần dự đoán.



Hình 3. Lưu đồ minh họa bài toán

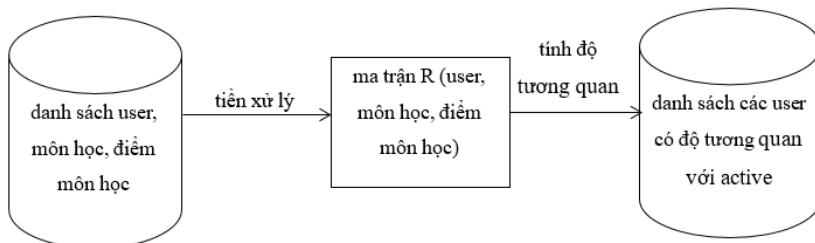
Mô hình gồm hai giai đoạn: giai đoạn thứ nhất sẽ tìm N sinh viên (từ các khóa trước) “gần nhất” với sinh viên có điểm cần dự đoán bằng phương pháp lọc cộng tác (những sinh viên càng gần nhau nghĩa là những sinh viên có kết quả học tập ở những môn học đã biết trong quá khứ càng giống nhau); giai đoạn thứ hai sẽ dùng ma trận phân rã trên tập điểm của các sinh viên này (sinh viên cần dự đoán điểm và N sinh viên gần nhất) để điền các điểm còn thiếu (các điểm số trong học kỳ tiếp theo của sinh viên cần dự đoán). Theo đó, ta có các bước cụ thể như sau:

Bước 1: Thu thập dữ liệu

Bước 2: Tiền xử lý

Bước 3: Xây dựng ma trận

Bước 4: Tính độ tương quan



Hình 4. Các bước thực hiện giai đoạn 1 của bài toán

Bước 1: Thu thập dữ liệu

Bài toán dự đoán các điểm số của một sinh viên trong học kỳ tiếp theo dựa trên cơ sở dữ liệu điểm của các sinh viên đó với điểm số của các sinh viên khác. Tuy nhiên với những sinh viên năm nhất, hoàn toàn chưa có điểm số hay bất cứ thông tin nào để tìm ra điểm chung với các sinh viên khóa trước.

Vì vậy để giải quyết vấn đề cold-start cho những sinh viên năm nhất, ta cần dùng thêm các thông tin như điểm đầu vào và khảo sát tâm lý của sinh viên. Trước tiên ta chọn dữ liệu điểm đầu vào vào bảng dữ liệu, vì điểm đầu vào sẽ liên quan đến quá trình học tập của sinh viên trước khi tham gia học. Ta chọn thêm dữ liệu khảo sát tâm lý sinh viên để ta có thể phân loại sinh viên thuộc nhóm đối tượng nghề nghiệp nào để dễ dàng gom nhóm phân loại sinh viên. Vì theo các nghiên cứu về tâm lý của Holland thì những nhóm người có cùng sở thích, tâm lý giống nhau sẽ có quá trình học tập tương tự nhau và kết quả học tập tương tự nhau [13].

Mô hình của Tiến sĩ tâm lý John Holland đã được sử dụng rộng rãi nhất trong thực tiễn hướng nghiệp trên thế giới như: Áo, New Zealand, Canada, Hà Lan, Thụy Sĩ, Italia... và được đánh giá rất cao về tính chính xác trong việc khám phá, lựa chọn ngành, nghề phù hợp tính cách của bản thân. Theo tiến sĩ tâm lý John Holland, có 6 nhóm sở thích nghề nghiệp tương ứng với các loại ngành nghề khác nhau trong xã hội nhưng có quan hệ với nhau. Đó là: (1) Thực tế – Realistic, (2) Nghiên cứu – Investigative, (3) Nghệ thuật – Artistic, (4) Xã hội – Social, (5) Kinh doanh -Enterprise, (6) Công chức – Conventional.



Hình 5. Minh họa về các nhóm người cơ bản theo khảo sát Holland

Dựa vào ý tưởng đó ta thực hiện thu thập dữ liệu như sau:

Mỗi sinh viên được nhận một phiếu trắc nghiệm bằng giấy;

Mỗi sinh viên trả lời bằng cách cho điểm (từ 1 đến 5) vào phiếu khảo sát [16] cho từng câu hỏi cụ thể.

Mô tả cấu trúc câu hỏi trắc nghiệm:

Bộ câu hỏi được thiết kế dựa trên bộ câu hỏi khảo sát nghề nghiệp theo học thuyết Holland [16]. Với 6 bảng: Đối với mỗi nhóm có 9 câu hỏi khác nhau; sinh viên trả lời bằng cách chọn vào ô điểm mà mình cảm thấy phù hợp với bản thân (điểm được cho là từ 1 đến 5; là mức độ sinh viên cảm thấy câu hỏi đó phù hợp với mình như thế nào; nếu đúng 90-100% so với câu hỏi thì cho 5 điểm, đúng khoảng 70 – 80% thì đánh giá là 4, 50% thì đánh giá là 3, 30-40% thì đánh là 2, 10-20% đánh giá là 1). Sau khi có được bản khảo sát, dữ liệu được nhập liệu và tính điểm trung bình của từng sinh viên qua từng nhóm cụ thể.

STT	Bảng A (R: Realistic - Người thực tế)	Số điểm
1	Tôi có tính tự lập	
2	Tôi suy nghĩ thực tế	
3	Tôi là người thích nghi với môi trường mới	
4	Tôi có thể vận hành, điều khiển các máy móc thiết bị	
5	Tôi làm các công việc thủ công như gấp giấy, đan, móc	
6	Tôi thích tiếp xúc với thiên nhiên, động vật, cây cỏ	
7	Tôi thích những công việc sử dụng tay chân hơn là trí óc	
8	Tôi thích những công việc thấy ngay kết quả	
9	Tôi thích làm việc ngoài trời hơn là trong phòng học, văn phòng	
	Cộng bảng A	

Hình 6. Minh họa câu hỏi trắc nghiệm khảo sát của Holland nhóm A

Điểm 1 là điểm sinh viên cảm thấy không đúng, không phù hợp với bản thân.

Điểm 5 sinh viên cho cao nhất khi cảm thấy mình phù hợp với câu hỏi hay đề tài đó nhất.

Điểm số đầu vào của sinh viên là điểm xét tuyển trên học bạ của sinh viên khi vào trường. Điểm này được lưu giữ tại phòng đào tạo của trường Cao đẳng Kinh tế - kỹ thuật Thủ

Đức. Điểm đầu vào ở dạng hồ sơ giấy. Được mượn, và nhập liệu vào cơ sở dữ liệu của từng sinh viên.

Bước 2: Tiết xử lý

– **Phân phiếu khảo sát:** Sau khi sinh viên đánh giá xong, ta tiến hành tính điểm trung bình của từng sinh viên đánh giá cho từng nhóm cụ thể. Nhập liệu điểm trung bình của từng sinh viên vào cơ sở dữ liệu.

– **Phân điểm đầu vào:** Sau khi nhận hồ sơ từ phòng Đào tạo trường, ta tiến hành nhập liệu điểm đầu vào của sinh viên vào csdl.

Bước 3: Xây dựng ma trận

Ma trận được biểu diễn như sau: dòng là đại diện cho các user (sinh viên), cột là các câu hỏi trắc nghiệm mà sinh viên đã đánh giá và điểm số của user đó.

Bảng 2. Bảng đánh giá của các user trên các câu hỏi và điểm đầu vào

	p1	p2	p3	p4	...	pn
Active_User	5	3	4	4	...	5
SV_1	3	1	2	3	...	3
SV_2	4	3	4	3	...	5
SV_3	3	3	2	5	...	4
SV_4	1	5	5	2	...	1

Bước 4: Tính độ tương quan

Ví dụ: Cho một Active_User đã đánh giá các sở thích theo bộ trắc nghiệm Holland [5] và điểm đầu vào như (Bảng 0-1)

Bảng 3. Bảng đánh giá của các user trên các câu hỏi và điểm đầu vào

	p1	p2	p3	p4	...	pn
Active_User	5	3	4	4	...	5
SV_1	3	1	2	3	...	3
SV_2	4	3	4	3	...	5
SV_3	3	3	2	5	...	4
SV_4	1	5	5	2	...	1

Để tìm được những sinh viên có cùng tính cách, cùng sở thích ta cần tính được độ tương tự gần nhất giữa các sinh viên đó. Một độ đo mức độ tương tự phổ biến trong User-Based Collaborative Filtering (User-Based CF) là: Pearson correlation với công thức như sau:

$$\text{sim}(a,b) = \frac{\sum_{p \in P} (r_{a,p} - \bar{r}_a)(r_{b,p} - \bar{r}_b)}{\sqrt{\sum_{p \in P} (r_{a,p} - \bar{r}_a)^2} \sqrt{\sum_{p \in P} (r_{b,p} - \bar{r}_b)^2}}$$

Trong đó:

a, b : là các user (sinh viên)

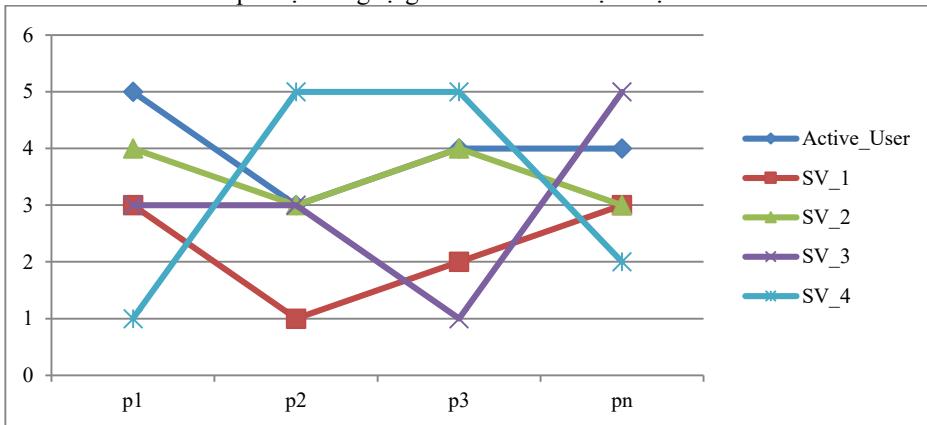
r_{a,p} : là đánh giá của sinh viên a cho sản phẩm p (trong trường hợp này là điểm sinh viên đánh giá cho các câu hỏi holland và điểm số đầu vào của sinh viên)

P: là tập hợp các câu hỏi holland và điểm số đầu được đánh giá bởi sinh viên a và b

Giá trị tương tự giữa hai sinh viên thường trong khoảng từ -1 đến 1. Khi kết quả được đo gần với giá trị 1 nhất thì hai sinh viên đó có độ tương đồng gần nhất, ngược lại thì hai Sinh viên đó ko có độ tương đồng.

	P 1	P 2	P3	P4	...	P n
Active_User	5	3	4	4	...	5
SV_1	3	1	2	3	...	3
SV_2	4	3	4	3	...	5
SV_3	3	3	2	5	...	4
SV_4	1	5	5	2	...	1

Hình 7. Kết quả độ tương tự giữa Sinh viên được chọn và các sinh viên khác



Hình 8. Biểu đồ Kết quả độ tương tự giữa Sinh viên được chọn và các sinh viên khác

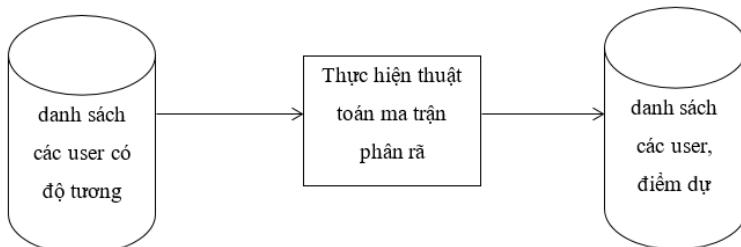
Hệ số tương quan của Active_User với SV_1 được tính như sau: ($\overline{r_{Active_user}} = \bar{r}_a = 4$, $\overline{r_{sv_1}} = \bar{r}_b = 2.4$)

$$\text{sim}(a,b) = \frac{(5-\bar{r}_a)*(3-\bar{r}_b)+(3-\bar{r}_a)*(1-\bar{r}_b)+\dots+(4-\bar{r}_a)*(3-\bar{r}_b)}{\sqrt{(5-\bar{r}_a)^2+(3-\bar{r}_a)^2}\dots\sqrt{(3-\bar{r}_b)^2+(1-\bar{r}_b)^2}} = 0.85$$

(tương tự như vậy ta lần lượt tính độ tương quan giữa Active_User với các user khác).

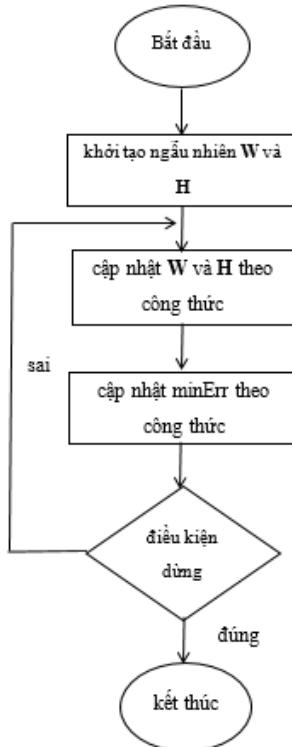
Kết quả thu được sẽ cho ra những giá trị gần với +1 nhất sẽ được nhận. Từ đó kết luận độ tương quan giữa Active-user và user đó là cao nhất.

Giai đoạn 2 của bài toán: Sau khi tìm được sinh viên gần nhất với sinh viên được chọn ta tiến hành dự đoán điểm như sau:



Hình 9. Các bước thực hiện giai đoạn 2 của bài toán

Lưu đồ thuật toán:



Hình 10. Lưu đồ thuật toán ma trận phân rã

Sau khi tìm được những User có độ đo tương tự gần với Active_User ta tiến hành bước dự đoán điểm dựa trên thuật toán ma trận phân rã như lưu đồ trên Hình 0-5

Ví dụ: Sau khi tìm được các user có độ đo giống nhau ta đưa dữ liệu điểm của các User thành một ma trận điểm số như sau:

	W	X	Y	Z
A		4.5	2.0	
B	4.0		3.5	
C		5.0		2.0
D		3.5	4.0	1.0

Hình 11. Ma trận điểm số

Trong đó; ta có bốn User (A, B, C, D) và các cột điểm (W, X, Y, Z);

Áp dụng kỹ thuật phân rã ma trận cho ma trận điểm trên ta thu được 2 ma trận nhỏ hơn là W và HT:

$$\begin{array}{ccccc}
 & \begin{matrix} W & X & Y & Z \end{matrix} & = & \begin{matrix} A & 1.2 & 0.8 \\ B & 1.4 & 0.9 \\ C & 1.5 & 1.0 \\ D & 1.2 & 0.8 \end{matrix} & \begin{matrix} W & X & Y & Z \end{matrix} \\
 \begin{matrix} A \\ B \\ C \\ D \end{matrix} & \begin{bmatrix} 4.5 & 2.0 & & \\ 4.0 & & 3.5 & \\ 5.0 & & & 2.0 \\ 3.5 & 4.0 & 1.0 & \end{bmatrix} & & & \begin{bmatrix} 1.5 & 1.2 & 1.0 & 0.8 \\ 1.7 & 0.6 & 1.1 & 0.4 \end{bmatrix} \\
 & & & \bullet & H^T
 \end{array}$$

Hình 12. Kỹ thuật phân rã ma trận

Quá trình phân tích này được thực hiện bằng cách tối ưu hóa hàm mục tiêu (objective function). Trong vấn đề dự đoán xếp hạng thì hàm mục tiêu thông dụng nhất là RMSE như sau:

$$\text{OMF} = \sum_{(u,i) \in D^{train}} (r_{u,i} - \sum_{k=1}^K W_{uk} h_{ik})^2 + \lambda \cdot (\|W\|_F^2 + \|H\|_F^2)$$

Trong đó Dtrain là tập dữ liệu huấn luyện vì trong bài toán này không cần làm cho máy học nêu tập huấn luyện được thay thế cho toàn bộ dữ liệu của sinh viên khi duyệt dữ liệu ta cho chạy qua từng sinh viên cụ thể, λ là hệ số chính tắc hóa (regularization), nhằm làm giảm học vẹt (overfitting). Giả sử quá trình tối ưu ta được hai giá trị của W, H . Khi đó, điểm số của user B cho môn học X được tính bởi công thức:

$$\hat{r}_{u,i} = W \cdot h^T = \sum_{k=1}^K W_{uk} h_{ik}$$

Như vậy ta tìm điểm số của User B cho môn X bởi công thức trên: $1.4 * 1.2 + 0.9 * 0.6 = 2.22$

	W	X	Y	Z
A		4.5	2.0	
B	4.0	2.22	3.5	
C		5.0		2.0
D		3.5	4.0	1.0

Hình 13. Ma trận điểm của tất cả các môn học

Tiếp tục thực hiện lặp lại quá trình trên cho đến khi ma trận được điền đầy. Khi đó ta sẽ được điểm của tất cả các môn học còn trống.

4. KẾT LUẬN

Bài báo này đã trình bày phương pháp thực hiện bài toán dự đoán kết quả học tập của sinh viên, nhận thấy rằng còn có thể xây dựng hệ thống dự đoán dựa trên hệ thống tư vấn với bộ lọc cộng tác (collaborative filtering) kết hợp với kỹ thuật phân rã ma trận (Matrix Factorization). Phương pháp đề xuất tận dụng những điểm mạnh của từng thuật toán và khắc phục những hạn chế của chúng, dẫn đến quá trình dự đoán đạt hiệu quả tốt hơn.

Trong các công trình tiếp theo, chúng tôi dự định nghiên cứu kỹ hơn về việc tích hợp thêm chức năng tính độ lệch trung bình cho từng sinh viên theo học kỳ. (Phần mềm xuất file excel và được tính độ lệch trung bình bằng tay). Thu thập thêm nhiều dữ liệu bằng việc khảo sát sinh viên qua từng năm, giúp phần mềm cũng có độ chính xác và phong phú về mặt dữ liệu.

Xây dựng thêm chức năng cho phép người dùng nhập trực tiếp và tự xem kết quả dự đoán. Nhìn chung, chúng tôi tin rằng phương pháp đề xuất có tiềm năng đóng góp vào việc dự đoán kết quả học tập của sinh viên dựa trên kết quả học tập trước đó của sinh viên.

TÀI LIỆU THAM KHẢO

1. Dietmar Jannach, Markus Zanker, Alexander Felfernig, Gerhard Friedrich, “Recommender Systems: An introduction”, First published 2011, ISBN 978-0-521-49336-9, ISBN 978-0-521-49336-9 Hardback (2011)

2. Mingsheng Fu, Hong Qu, Dagmawi Moges, Li Lu "Attention Based Collaborative Filtering" University of Electronic Science and Technology of China, Chengdu 610054, P. R. China, 2017.
3. Ha, Taehyun, and Sangwon Lee. "Item-network-based collaborative filtering: A personalized recommendation method based on a user's item network." Information Processing & Management 53, no. 5 (2017): 1171-1184.
4. Nguyễn Hùng Dũng và Nguyễn Thái Nghe "Hệ thống gợi ý sản phẩm trong bán hàng trực tuyến", Trung tâm Công nghệ Phần mềm, Trường Đại học Cần Thơ, Khoa Công nghệ Thông tin & Truyền thông, Trường Đại học Cần Thơ (2014).
5. Đo Thanh Nhan, Tran Nguyen Minh Thu "Hệ thống gợi ý áp dụng cho trang web tổng hợp tin tức tự động", THPT Lê Anh Xuân, tỉnh Bến Tre, Khoa Công nghệ Thông tin & Truyền thông, Trường Đại học Cần Thơ (2014).
6. Trần Lê Thúy, luận văn Thạc sĩ về đề tài "Hệ hỗ trợ tư vấn tuyển sinh tại trường Cao đẳng Nghề Tỉnh Bà Rịa - Vũng Tàu", 2017.
7. Krzywicki, Alfred, Wayne Wobcke, Yang Sok Kim, Xiongcai Cai, Michael Bain, Ashesh Mahidadia, and Paul Compton. "Collaborative filtering for people-to-people recommendation in online dating: Data analysis and user trial." International Journal of Human-Computer Studies 76 (2015): 50-66.
8. Nguyễn Đăng Nhượng, "Khai phá dữ liệu về kết quả học tập của học sinh trường Cao đẳng nghề Văn Lang Hà Nội", luận văn thạc sĩ trường Đại học Công Nghiệp (2012).
9. Huỳnh Lý Thanh Nhàn và Nguyễn Thái Nghe, "Hệ thống dự đoán kết quả học tập của sinh viên sử dụng thư viện hệ thống gợi ý mã nguồn mở MyMediaLite". Hội thảo quốc gia CNTT- Trường Đại học Cần Thơ (2013).
10. Nguyễn Hùng Dũng và Nguyễn Thái Nghe với bài viết "Hệ thống gợi ý sản phẩm trong bán hàng trực tuyến sử dụng kỹ thuật lọc công tác". Tạp chí khoa học trường Đại học Cần Thơ (2013).
11. Saxena, Prashant Sahai, and M. C. Govil. "Prediction of Student's Academic Performance using Clustering." In Natl. Conf. Cloud Comput. Big Data. 2009.
12. Linden, Greg, Brent Smith, and Jeremy York. "Amazon. com recommendations: Item-to-item collaborative filtering." IEEE Internet computing 1 (2003): 76-80.
13. Gary D. Gottfredson "John L. Holland's Contributions to Vocational Psychology: A Review and Evaluation". Journal of Vocational Behavior 55, 15–40 (1999). Article ID jvbe.1999.1695, available online at <http://www.idealibrary.com>
14. Le Hoang Son (2014) "Dealing with the new user cold-start problem in recommender systems: A comparative review", VNU University of Science, Vietnam National University, Vietnam.
15. Nguyễn Trần Quốc Vinh, and Nguyễn Thị Thanh Thúy. "Ứng dụng khai phá dữ liệu xây dựng công cụ dự đoán kết quả học tập của sinh viên." thuyên tập báo cáo Hội nghị sinh viên nghiên cứu khoa học lần thứ 8 - Đại học Đà Nẵng (2012).
16. Fernando Ortega, Antonio Hernando, Jesus Bobadilla, Jeon-Hyung Kang "Recommending items to group of users using Matrix Factorization based Collaborative Filtering" Infomation Sciences Volume 345, 1 june 2016, pages 313-324.

ABSTRACT

BUILDING A SYSTEM FOR FORECASTING STUDENTS' STUDY RESULTS TO SUPPORT ACADEMIC ASSISTANCE WORK

Ngo Thanh Hung¹, Nguyen Thi Thu Tam^{1,*}

¹*Ho Chi Minh City University of Food Industry, Vietnam*

*Email: tamntt@hufi.edu.vn

In the process of studying and researching, learning the methods of performing the problem of predicting student learning outcomes, realizing that it is also possible to build a prediction system based on a recommender system with additive filter, collaborative filtering combined with matrix factorization. However, in fact, there are not many research works that combine filtering with Matrix Factorization in the field of education, mainly in the commercial field. Therefore, this study is aimed at understanding recommender systems, focusing on the collaborative filtering approach based on matrix analysis. Apply this method to build a system to predict student learning outcomes based on students' previous learning results.

Keywords: Data mining, collaborative filtering, matrix decomposition technique, learning outcome prediction

NGUY CƠ TẤN CÔNG DDOS TỪ CÁC THIẾT BỊ IOT

Trần Đắc Tốt^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: tottd@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Ngày nay các thiết bị Internet of Things (IoT) đã và đang chứng minh được tính ưu việt của mình, số lượng thiết bị IoT gia tăng một cách nhanh chóng. Tuy nhiên việc bảo mật, quyền riêng tư của các thiết bị IoT nổi lên như một vấn đề lớn. Các nghiên cứu hiện tại cho thấy nhiều điểm yếu đáng kể trong một số loại thiết bị IoT hơn nữa trong một số tình huống không có cơ chế bảo mật để bảo vệ các thiết bị này. Mạng Botnet Mirai đã minh chứng cho việc dùng thiết bị IoT để thực hiện các cuộc tấn công DDoS quy mô lớn. Trong nghiên cứu này chúng tôi phân tích về nguy cơ tấn công các thiết bị IoT, sử dụng các thiết bị IoT để tấn công từ chối dịch vụ DDoS. Những thiệt hại mà các thiết bị IoT có thể gây ra nếu bị chiếm quyền điều khiển.

Từ khóa: Internet of Things, Camera IP, botnet Mirai, DDoS, attacks camera.

1. MỞ ĐẦU

Cuộc cách mạng công nghiệp lần thứ tư với các đặc trưng về trí tuệ nhân tạo, Internet of Things (IoT) [1] và điện toán đám mây đã mở ra cho nhân loại những cơ hội mới nhưng cũng đặt ra những thách thức mới, một trong số đó là vấn đề đảm bảo an toàn thông tin [2]. IoT đã trở thành một trong những công nghệ quan trọng nhất của thế kỷ 21. Giờ đây, chúng ta có thể kết nối các vật dụng hàng ngày như thiết bị nhà bếp, xe hơi, máy điều hòa nhiệt độ, màn hình,... thông qua mạng Internet bằng các thiết bị nhúng, có thể giao tiếp liền mạch giữa con người, quy trình và mọi thứ.

Các thiết bị IoT được kết nối qua các mạng truyền dữ liệu và đặc biệt là thông qua các giao thức TCP/IP, như thiết bị Mobile, Camera IP, hay các thiết bị Modem, Router, Access Point,...

Tuy nhiên tất cả các thiết bị IoT đều dễ dàng trở thành một phần trong mạng botnet nhằm mục đích thực hiện các cuộc tấn công DDoS [3]. Mạng botnet Mirai [4],[5] đã hình thành từ hơn 600.000 thiết bị IoT với thành phần là các Camera giám sát và bộ định tuyến (router), đã tạo ra một cuộc tấn công DDoS lớn lên tới 620 Gbits vào lúc điểm đỉnh điểm (hình 1).

Trong phần tiếp theo của bài báo này, Phần 2 sẽ phân tích về nguy cơ tấn công từ chối dịch vụ DDoS từ các thiết bị IoT. Phần 3 sẽ thực nghiệm và đưa ra kết quả.

2. PHÂN TÍCH VỀ NGUY CƠ TÁN CÔNG TỪ CHỐI DỊCH VỤ DDOS TỪ CÁC THIẾT BỊ IOT

2.1. Lỗi bảo mật phổ biến trên các thiết bị IoT

2.1.1. Lỗi liên quan đến Pass Config

Lỗi này xảy ra khi người dùng cấu hình Camera quá đơn giản [5] hoặc không thay đổi cấu hình khi cài đặt lần đầu. Đây là cách mà thiết bị lợi dụng để tấn công nhất. Thông thường lỗi pass config rơi vào một số trường hợp sau:

- Đè mật khẩu mặc định: đa phần người dùng khi cài đặt Camera thì không đổi mật khẩu mặc định của nhà sản xuất đề ra, đây là lỗ hổng cực lớn tới từ người dùng.
- Đổi mật khẩu nhưng mật khẩu yếu: mật khẩu yếu là loại mật khẩu có số lượng từ nhỏ khoảng dưới 8 ký tự, mật khẩu đơn giản chỉ có chữ, số hoặc là chỉ gồm chữ và số.
- Mật khẩu dễ đoán: kiểu mật khẩu thuận tiện cho việc lưu nhớ như abc123, iloveyou, ... những loại mật khẩu này sử dụng rất nhiều và được liệt kê trong danh sách những mật khẩu sử dụng nhiều nhất hàng năm.

2.1.2. Lỗi Buffer Overflow

Lỗi tràn bộ đệm (Buffer Overflow) [6] là lỗi khi tiến trình lưu trữ dữ liệu vượt ra ngoài biên của bộ nhớ đệm có chiều dài cố định. Kết quả là dữ liệu có thể đè lên các bộ nhớ liền kề. Dữ liệu bị ghi đè có thể bao gồm các bộ nhớ đệm khác, các biến và dữ liệu điều khiển luồng chạy của cả chương trình. (CVE-2018-3892) [7] thuộc loại Stack-based Buffer Overflow. NUUO NVRmini2 Network Video Recorder firmware version 3.9.1 cho phép kẻ tấn công rce hoặc DDoS (buffer overflow) dẫn đến khả năng đọc dữ liệu nhạy cảm và hoặc cấu hình lại thiết bị (CVE-2018-19864) [8].

2.1.3. Lỗi Injection

Theo như Top 10 OWASP [9] thì Injection luôn đứng đầu về các lỗi nguy hiểm như SQLi, NoSQLi, OS Command Injection và LDAP, XSS. Cho phép kẻ tấn công có chèn những dữ liệu nguy hiểm có khả năng đánh cắp dữ liệu hoặc chiếm quyền điều khiển mà không cần phải xác thực hoặc ủy quyền. Bởi vì Camera IP thường được quản lý thông qua môi trường Web nên thường tồn tại một số lỗ hổng trong hạng mục Top 10 OWASP. Lỗ hổng OS-Command Injection xuất hiện ở Wireless IP Camera (P2P) WIFICAM Cameras được đã được công bố có tên mã (CVE-2017-18377) [10] có thể thực inject các commandline gọi và thực thi trong file set_ftp.cgi thông qua \$(command) trong biến pwd có thể dẫn đến rce (Remote Code Execution) đều đáng nói là kẻ tấn công có quyền thực thi của user root.

2.1.4. Lỗi Cross-Site Request Forgery (CSRF)

Lỗi hổng Cross-Site Request Forgery (CSRF) thuộc A8 của Top 10 OWASP. Xuất hiện trên MOBOTIX S14 MX-V4.2.1.61 Cameras [11] cho phép kẻ tấn công tạo một tài khoản admin thông qua việc gửi requests đến url/admin/access không cần xác thực.

2.1.5. Lỗi Firmware Camera

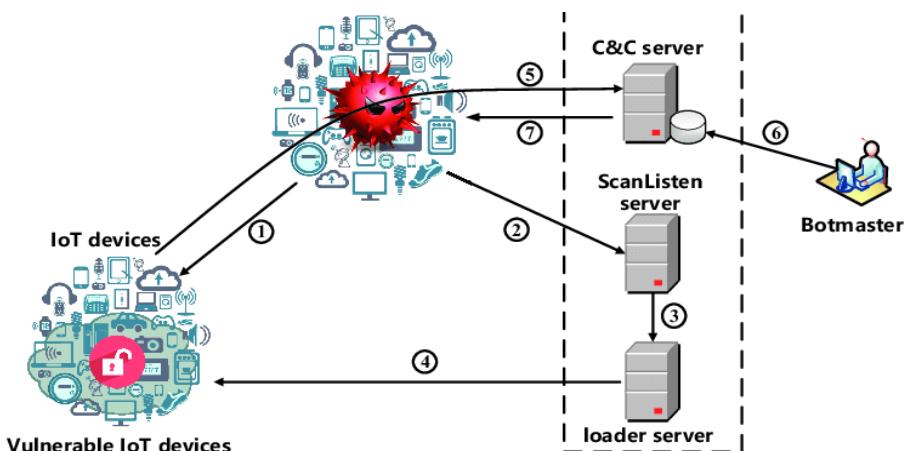
Firmware Camera là firmware [12] được cài đặt sẵn trên các thiết bị Camera. Firmware được lưu trữ trong bộ nhớ chỉ đọc và các thông tin cấu hình sẽ không bị mất khi Camera tắt đi. Firmware là bộ não của Camera cho phép điều khiển các chức năng như xử lý hình ảnh, tự động lấy nét, khử nhiễu,... Tuy nhiên bản thân Firmware Camera cũng tồn tại rất nhiều lỗ hổng và chúng bị tấn công thường xuyên.

2.1.6. Các lỗi bảo mật phổ biến khác

Lỗi liên quan đến Dynamic DNS, Backdoor, và nhiều lỗ hổng nghiêm trọng đã được phát hiện ở trên thiết bị IoT [13].

2.2. Phương thức lây nhiễm malware trên các thiết bị IoT

Các phân tích về các họ malware trên thiết bị IoT có khả năng tấn công DDoS [15,18], cho chúng ta thấy rằng số lượng bot của botnet được quyết định bằng phương thức lây nhiễm bao gồm: phương thức dò quét nạn nhân, khai thác lỗ hổng và lây nhiễm và phương thức phát tán.



Hình 1. Mô hình hoạt động của malware Mirai với (1) là bước dò quét và (4) là bước khai thác lỗ hổng và phát tán [18]

2.2.1. Phương thức dò quét

Mục tiêu của phương thức dò quét là xác định càng nhiều thiết bị dễ bị tấn công tốt đồng thời tạo ra dung lượng truy cập thấp để tránh bị phát hiện. Dựa trên phương thức dò quét, có thể phân loại thành 5 loại

a. Dò quét ngẫu nhiên

Trong các cuộc tấn công DDoS, phương thức dò quét ngẫu nhiên (Random scanning) được thực hiện bằng cách sử dụng một thiết bị đã bị xâm nhập để tiếp tục thăm dò các địa chỉ IP ngẫu nhiên nhằm tìm kiếm mục tiêu mới để tiếp tục tấn công. Phương thức dò quét này có khả năng tạo ra dung lượng truy cập cao (vì có khả năng nhiều bot cùng quét vào 1 IP), điều này làm cho phương thức dò quét này dễ bị phát hiện.

b. Dò quét theo danh sách

Với phương thức dò quét theo danh sách (Hitlist Scanning), bot sẽ thực dò quét để tìm mục tiêu theo một danh sách đã có. Khi một thiết bị dễ bị tấn công mới được phát hiện và bị nhiễm, một phần của danh sách tấn công ban đầu sẽ được gửi đến thiết bị đó. Phương thức dò quét này cho phép tốc độ lan truyền lớn và không có tranh chấp trong quá trình quét giữa các bot thuộc cùng một botnet. Hạn chế là danh sách này cần được tập hợp trước. Hơn nữa, nếu danh sách dò quét quá lớn, đường truyền của nó có thể tạo ra dung lượng truy cập cao và dẫn đến dễ bị phát hiện, trong khi nếu quá nhỏ, nó sẽ tạo ra một mạng botnet nhỏ.

c. Dò quét theo dấu hiệu

Dò quét theo dấu hiệu (Signpost Scanning) là phương thức dò quét tận dụng thông tin sẵn có trong thiết bị đã bị xâm nhập ví dụ như danh sách IP được lưu trong lịch sử kết nối của thiết bị. Đối với các botnet có phạm vi hoạt động trên các server hay PC, số địa chỉ email chính là thông tin được sử dụng để thực hiện signpost scanning. Phương thức quét này không tạo ra dung lượng truy cập cao; do đó, nó làm giảm khả năng bị phát hiện. Tuy nhiên, phương thức này có tốc độ lây lan của malware chậm hơn so với các phương thức dò quét khác, kể tấn công khó kiểm soát và phụ thuộc rất nhiều vào hành vi của người dùng.

d. Dò quét hoán vị

Fương thức dò quét hoán vị (Permutation Scanning) được thực hiện trước phương thức dò quét theo danh sách khi mà danh sách này chỉ có một số lượng nhỏ. Sau đó, tất cả các máy chủ bị, thiết bị đã bị xâm nhập sẽ chia sẻ một hoán vị giả ngẫu nhiên chung của không gian địa chỉ IP và mỗi địa chỉ IP được ánh xạ vào một chỉ mục trong hoán vị này. Một máy tính, thiết bị IoT bị nhiễm trong giai đoạn đầu bắt đầu dò quét qua hoán vị bằng cách sử dụng chỉ mục được tính từ địa chỉ IP của nó làm điểm bắt đầu. Bất cứ khi nào nó tìm thấy một nạn nhân mới, nó sẽ chọn một điểm bắt đầu ngẫu nhiên mới. Một thiết bị IoT bị lây nhiễm bởi phương thức dò quét hoán vị luôn bắt đầu từ một điểm ngẫu nhiên trong hoán vị. Phương thức này duy trì lợi ích của chiến lược quét ngẫu nhiên nhưng nó cũng có tác dụng cung cấp chế độ dò quét toàn diện và bán toàn diện.

e. Dò quét mạng cục bộ

Fương thức dò quét mạng cục bộ (Local Subnet Scanning) có thể được thêm vào mỗi chiến lược đã nói ở trên để tùy ý quét các mục tiêu nằm trên cùng một mạng con của thiết bị, máy chủ bị xâm phạm. Kỹ thuật này cho phép một bản sao mã quét để có thể xâm nhập vào nhiều máy dễ bị tấn công đứng phía sau tường lửa.

2.2.2. Phương thức khai thác lỗ hổng và lây nhiễm

Đối với bất kỳ loại tấn công nào, kẻ tấn công cần phải tấn công vào tất cả các lỗ hổng (attack surface, bề mặt tấn công) của thiết bị IoT hoặc máy chủ, dịch vụ... Khi kẻ tấn công xác định bề mặt tấn công bằng các phương thức dò quét, chúng sẽ tạo ra một vector tấn công, đây là cách mà kẻ tấn công sử dụng để chiếm quyền điều khiển các thiết bị IoT. Các vector tấn công phổ biến bao gồm: liên kết trong email (“nhấp vào đây nếu bạn muốn làm giàu nhanh chóng”), phần mềm đã tải xuống (“trình phát Flash của bạn đã lỗi thời”) hoặc thậm chí di chuột qua một quảng cáo bị nhiễm mã độc có thể sẽ là một cách làm cho máy tính bị xâm nhập. Các thiết bị IoT có rất nhiều lỗ hổng bảo mật. Mật khẩu yếu, cùng với khả năng hiển thị trực tiếp

thiết bị và backdoor, khiến các thiết bị IoT dễ dàng bị chiếm quyền điều khiển ngay cả attacker là “script kiddies”.

Thông thường chúng ta nghĩ rằng, để thực hiện được việc này phải là các hacker được các tổ chức chính phủ tài trợ, nhưng không, với công bố từ [19], chúng ta có thể thấy rằng tập hợp các lỗ hổng bảo mật của các thiết bị IoT và phương thức khai thác được nêu ra như sau:

- **Mật khẩu yếu, có thể đoán hoặc được mã hóa cứng:** các thông tin xác thực dễ dàng bị tấn công brute force, hoặc có sẵn công khai hoặc không thể thay đổi. Trong đó, có thể gồm các backdoor được cài sẵn trong firmware hay các phần mềm client được cấp quyền truy cập trái phép vào thiết bị.
- **Dịch vụ mạng không an toàn:** các dịch vụ mạng không cần thiết hoặc không an toàn đang chạy trên chính thiết bị, đặc biệt là những dịch vụ tiếp xúc với internet, làm tổn hại đến tính bảo mật, tính toàn vẹn / tính xác thực hoặc tính khả dụng của thông tin hoặc cho phép điều khiển từ xa trái phép...
- **Giao diện hệ thống tích hợp không an toàn:** giao diện web, API phụ trợ, dịch vụ kết nối với điện toán đám mây hoặc hoặc giao diện mobile không an toàn trong hệ thống tích hợp với thiết bị làm tổn hại thiết bị hoặc các thành phần liên quan. Các vấn đề thường gặp bao gồm thiếu xác thực / ủy quyền, mã hóa thiếu yếu và thiếu lọc đầu vào và đầu ra.
- **Thiếu cơ chế cập nhật an toàn:** thiếu khả năng cập nhật thiết bị một cách an toàn. Điều này bao gồm thiếu cơ chế xác thực firmware, phân phối thiếu an toàn (không được mã hóa khi truyền), thiếu cơ chế chống khôi phục và thiếu thông báo về các thay đổi bảo mật do cập nhật.
- **Sử dụng các thành phần không an toàn hoặc lỗi thời:** sử dụng các thành phần / thư viện phần mềm không được dùng nữa hoặc không an toàn làm cho thiết bị bị xâm phạm. Điều này bao gồm việc sử dụng các hệ điều hành tùy chỉnh không an toàn và sử dụng các thành phần phần cứng và phần mềm của bên thứ ba từ một chuỗi cung ứng đã bị tấn công trước đó.
- **Bảo vệ quyền riêng tư không đầy đủ:** thông tin cá nhân của người dùng được lưu trữ trên thiết bị hoặc trong hệ thống tích hợp không an toàn, không đúng cách hoặc không được phép.
- **Truyền và lưu trữ dữ liệu không an toàn:** thiếu mã hóa hoặc kiểm soát truy cập dữ liệu nhạy cảm ở bất kỳ đâu trong hệ sinh thái, bao gồm cả ở dữ liệu ở trạng thái nghỉ, truyền tải hoặc trong quá trình xử lý.
- **Thiếu quản lý thiết bị:** thiếu hỗ trợ bảo mật trên các thiết bị được triển khai trong quá trình sản xuất, bao gồm quản lý tài sản, quản lý cập nhật, ngừng hoạt động an toàn, giám sát hệ thống và khả năng phản hồi khi có sự cố.
- **Cài đặt mặc định không an toàn:** các thiết bị hoặc hệ thống được đưa vào vận hành với cài đặt mặc định không an toàn hoặc thiếu khả năng làm cho hệ thống an toàn hơn bằng cách hạn chế người vận hành sửa đổi cấu hình.
- **Thiếu sự tăng cường bảo mật:** thiếu các biện pháp tăng cường bảo mật, cho phép những kẻ tấn công tiềm năng có được thông tin nhạy cảm có thể giúp ích trong một cuộc tấn công từ xa trong tương lai hoặc chiếm quyền kiểm soát cục bộ thiết bị.

Tất cả các bề mặt tấn công ở trên sẽ được kẻ tấn công sử dụng riêng rẽ hoặc kết hợp lại với nhau hoặc có thể kết hợp thêm các attack surface mới nhất để khai thác và lây nhiễm vào thiết bị IoT [20] [21].

2.2.3. Phương thức phát tán

Sau khi bị phát hiện bởi quá trình dò quét, các thiết bị IoT, máy tính sẽ bị khai thác và nhiễm mã tấn công. Phương thức phát tán mã tấn công được sử dụng trong giai đoạn khai thác và lây nhiễm, có thể phân loại thành 3 loại sau.

a. Phát tán nguồn trung tâm

Phát tán nguồn trung tâm (Central Source Propagation) là kiểu phát tán mà mã tấn công được lưu trữ trên một máy chủ trung tâm (hoặc một tập hợp các máy chủ). Khi máy tác nhân bị xâm phạm, mã được tải xuống từ máy chủ thông qua cơ chế truyền tệp (chẳng hạn như wget hoặc tftp). Cơ chế phát tán này dẫn đến tải trọng lớn trên máy chủ trung tâm, tạo ra dung lượng truy cập lớn dẫn đến khả năng bị phát hiện. Hơn nữa, máy chủ trung tâm là một điểm lỗi duy nhất.

b. Phát tán mắt xích ngược

Phát tán mắt xích ngược (Back-Chaining Propagation) là kiểu phát tán mà mã tấn công được tải xuống từ máy tính, thiết bị đã bị lây nhiễm trước đó. Sau đó, máy bị nhiễm sẽ trở thành nguồn lây nhiễm cho các thiết bị, máy tính khác. Cơ chế phát tán này bền vững hơn so với phương thức nguồn trung tâm vì nó không có một điểm hỏng nào.

c. Phát tán tự động

Phương thức phát tán tự động (Autonomous Propagation), đây là phương thức mà các lệnh tấn công được truyền trực tiếp vào máy chủ, thiết bị mục tiêu khi bị lây nhiễm. Cơ chế lan truyền này tránh được bước truy xuất tệp và giảm tần suất dung lượng mạng để huy động tác nhân; do đó, nó làm giảm khả năng bị phát hiện.

2.3. Phương pháp thực hiện

Mạng botnet Mirai đã hình thành từ hơn 600.000 thiết bị IoT với thành phần là các camera giám sát và bộ định tuyến (router), đã tạo ra một cuộc tấn công DDoS lớn lên tới 620 Gbits vào lúc điểm đỉnh điểm. Kể từ sự cố đó, các họ mã độc mới đã ra đời để khởi động các kiểu tấn công khác trầm trọng. Lấy ví dụ như malware Xbash, tạo ra botnet, thực hiện tấn công bằng ransomware, đào tiền ảo và khả năng tự phát tán. Về bản chất, Xbash lây lan bằng cách tấn công các mật khẩu yếu và các lỗ hổng chưa được vá trong các máy chủ Linux và Microsoft Windows. Một ví dụ khác, một biến thể mới của mạng botnet Muhsstik, tự cài đặt và lây nhiễm các máy chủ Linux cũng như các thiết bị IoT bằng khả năng tự phát tán (giống sâu máy tính) để tàn phá bằng các cuộc tấn công đào tiền ảo và DDoS. Để hiểu lý do đằng sau các cuộc tấn công này và tác động của chúng đối với các thiết bị IoT, chúng ta hãy thảo luận về bề mặt tấn công thiết bị IoT ở một góc nhìn khác. Bề mặt tấn công của các thiết bị IoT được phân loại rộng rãi thành ba nhóm chính: Giao diện phản ứng, kênh giao tiếp, ứng dụng / dịch vụ.

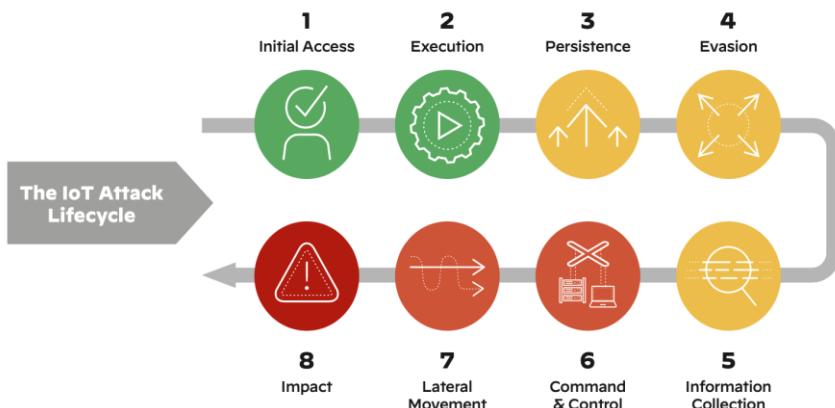
Giao diện phản ứng vật lý của thiết bị, là bề mặt tấn công rõ ràng nhất. Những kẻ tấn công có quyền truy cập vào shell (operating system shell) hoặc lớp ngoài cùng nhân hệ điều hành (operating system kernel) của thiết bị, sửa đổi firmware và đi xa đến mức nhúng một backdoor thông qua giao diện phản ứng để vượt qua các cơ chế xác thực thông thường.

Các thiết bị IoT kết nối và giao tiếp thông qua hai loại kênh: hoặc các kênh tầm ngắn bao gồm BLE, Zigbee/Z-Wave và Wi-Fi hoặc kênh mạng di động tầm xa. Các kênh liên lạc này đại diện cho bề mặt tấn công thứ hai. Rất ít thiết bị IoT sử dụng kênh liên lạc an toàn và được bảo mật hoặc mã hóa trong quá trình cấu hình ban đầu. Do đó kẻ tấn công dễ dàng tận dụng các lỗ hổng của IoT để giả mạo địa chỉ IP nhằm giả dạng thành một thiết bị IoT khác trong mạng. Từ đó, kẻ tấn công có thể phát tán malware và thực hiện tấn công man-in-the-middle, tiếp tục dò quét vào sâu trong hệ thống hoặc thực hiện tấn công từ chối dịch vụ (DoS).

Các ứng dụng / dịch vụ rất cần thiết cho các thiết bị IoT và đại diện cho bề mặt tấn công thứ ba. Giao diện quản trị, web API, máy chủ đám mây, các thành phần chức năng hệ thống và các dịch vụ được cung cấp từ các ứng dụng đều dễ bị tấn công. Hầu hết các cuộc tấn công IoT hiện đại được thực hiện bằng cách khai thác các lỗ hổng này vì với cách thức này mạng botnet dễ dàng mở rộng thông qua mạng internet. Ngay cả khi các dịch vụ được triển khai trên mạng nội bộ của doanh nghiệp, những kẻ xâm nhập vẫn có thể xâm nhập vào nó thông qua một bộ định tuyến. Ví dụ, botnet Xbash có khả năng xâm nhập vào mạng nội bộ của doanh nghiệp để quét và tấn công nhiều dịch vụ, chẳng hạn như giao thức ứng dụng Telnet và giao thức FTP.

2.3.1. Vòng đời

Theo [30] vòng đời của một cuộc tấn công DDoS sử dụng thiết bị IoT có 8 giai đoạn chính như sau (hình 2):



Hình 2. Vòng đời của tấn công DDoS sử dụng IoT [22]

a. Khởi tạo truy cập (initial access)

Kẻ tấn công tận dụng các công cụ dò quét chẳng hạn như ZMap hay Masscan để tìm kiếm thiết bị chứa các lỗ hổng bảo mật.

b. Thực thi (execution)

Ở giai đoạn này, kẻ tấn công thực thi các payload hoặc lệnh trong thiết bị dễ bị tấn công. Để làm điều này, kẻ tấn công có thể truy cập trực tiếp vào os shell của thiết bị hoặc đưa tập lệnh vào các thiết bị. Để có quyền truy cập trực tiếp, brute force được sử dụng để tấn công vào các mật khẩu yếu hoặc mặc định cho các dịch vụ như Telnet hoặc SSH. Sau đó, các tập lệnh được chèn vào thông qua việc khai thác lỗ hổng bằng cách thực thi mã từ xa RCE (Remote Code Execution). Khi các lệnh shell được thực thi, một điểm chung sau đó là một file mã độc

(chẳng hạn như file nhị phân ELF hoặc tập lệnh shell) được tải xuống. Sau đó, các payload này được gán quyền và thực thi

c. Duy trì (persistence)

Trong giai đoạn thứ ba, payload của malware được duy trì sự thực thi bằng cách loại bỏ các tiến trình giám sát để tránh hệ thống khởi động lại; hoặc chèn chính nó vào các tác vụ thực hiện định kỳ, các tác vụ thực hiện khi khởi động hệ thống và các dịch vụ hệ thống; và thậm chí tạo tài khoản mới. Đôi khi, shell được để mở như một kênh truy cập dự phòng để thiết lập quyền truy cập dự phòng trong tương lai.

d. Lẩn tránh (evasion)

Việc sử dụng các kỹ thuật né tránh đảm bảo sự xâm nhập bị che dấu, không bị phát hiện. Để đạt mục tiêu này, kẻ tấn công có thể xóa nhật ký hệ thống và lịch sử lệnh BASH, ẩn file payload trong thư mục hệ thống với tên file giả mạo và thậm chí xóa file payload ban đầu. Đối với các malware cao cấp, chẳng hạn như họ Xbash, để lẩn tránh chúng có thể giả mạo để biến các tiến trình của malware thành các công cụ giám sát bảo mật. Cuối cùng, kẻ tấn công còn có thể sử dụng thêm các kỹ thuật như Anti Virtual Machine (Anti-VM), anti-debugging để lừa các hệ thống phân tích malware. Các kỹ này đã xuất hiện trên các biến thể của họ malware Tsunami và Torii botnet.

e. Thu thập thông tin (Collection of Information)

Ở giai đoạn này, thông tin thiết bị và các tập tin nhạy cảm, chẳng hạn như private key (khóa riêng) và ví tiền điện tử (cryptocurrency wallet), được thu thập. Lấy malware VPNFilter làm ví dụ, đây là một malware được sử dụng trong các cuộc tấn công có chủ đích (APT) lây nhiễm qua một số thiết bị lưu trữ và bộ định tuyến mạng IoT, VPNFilter đánh cắp dữ liệu nhạy cảm từ dung lượng mạng trong các bộ định tuyến bị xâm phạm.

f. Lệnh và kiểm soát (Command and Control)

Tiếp theo, payload độc hại cũng nhận được lệnh từ máy chủ command-and-control (C2). Đối với các kết hợp C2 khác nhau, payload tiếp tục khởi động các hoạt động tấn công khác nhau như TCP flooding, UDP flooding và tiếp tục xâm nhập vào các thiết bị khác. Các kênh C2 thường sử dụng các giao thức HTTP, IRC, P2P.

g. Mở rộng địa bàn (Lateral movement)

Mở rộng địa bàn trong một cuộc tấn công IoT chủ yếu là tiếp tục lây nhiễm một số lượng lớn các thiết bị mới trong mạng cục bộ. Ví dụ: một bộ định tuyến biên (edge router) đầu tiên bị nhiễm và sau đó tiếp tục lây nhiễm cho tất cả các thiết bị IoT được kết nối với nó.

h. Tác động (Impact)

Các hoạt động độc hại được khởi chạy trong thiết bị IoT có nhiều tác động đến thiết bị: mã hóa dữ liệu để đòi tiền chuộc, xóa sạch toàn bộ ổ đĩa và dữ liệu cũng như lạm dụng để đào tiền mã hóa. Ví dụ như, malware BrickBot có thể “đóng gạch” một thiết bị IoT bằng cách làm hỏng khả năng lưu trữ của nó hoặc bằng cách cấu hình lại hoàn toàn các thông số hạt nhân của nó.

2.3.2. Phân chia giai đoạn

Với 8 giai đoạn trong một chu kỳ tấn công vào thiết bị IoT được phân chia thành 4 giai đoạn chính như sau:

(1) Tuyển dụng (recruitment): kẻ tấn công (agents, bot) dò quét các thiết bị tồn tại các lỗ hổng bảo mật. Trước đây, quá trình này được thực hiện thủ công, tuy nhiên, với tiến hóa của các biến thể malware, nó đã được tự động hóa.

(2) Khai thác và lây nhiễm (exploitation and infection): các thiết bị IoT chứa các lỗ hổng sẽ bị khai thác để cấy mã độc vào và biến thành bot. Giai đoạn này cũng đã được tự động hóa trong những năm qua và ngày nay một số họ malware botnet cũng có thêm tính năng tự phát tán và lây nhiễm.

(3) Giao tiếp (communication): kẻ tấn công sử dụng cơ sở hạ tầng điều khiển và lệnh (phụ thuộc vào các thiết kế mạng botnet của kẻ tấn công) để giao tiếp với botnet nhằm xác định bot nào đang hoạt động, lập lịch các cuộc tấn công hoặc nâng cấp chính các bot.

(4) Tấn công (attack): kẻ tấn công thực sự ra lệnh bắt đầu cuộc tấn công và các bot bắt đầu gửi các gói dữ liệu độc hại đến nạn nhân. Các tham số tấn công (chẳng hạn như địa chỉ của nạn nhân, thời lượng và thuộc tính gói dữ liệu độc hại) thường được điều chỉnh trong giai đoạn này (nếu nó không được thực hiện trong giai đoạn trước). Mặc dù giả mạo IP không phải là yêu cầu cần thiết cho một cuộc tấn công DDoS thành công, nhưng những kẻ tấn công thường sử dụng giả mạo địa chỉ nguồn IP để che giấu danh tính của các bot trong cuộc tấn công.

Với sự phân chia theo từng giai đoạn chúng ta có thể thấy rằng (1) (2) chính là phương thức lây nhiễm malware trên thiết bị IoT đã được phân tích ở chương 1 và (3) (4) chính là phương thức sử dụng botnet IoT để tấn công DDoS.

2.4. Phương thức tấn công DDoS

Dựa trên [2], [3], [12] về một số phương thức tấn công DDoS phổ biến nhất đã được thực hiện trong những năm vừa qua. Các cuộc tấn công DDoS có thể được thực hiện thông qua các giao thức thuộc các lớp khác nhau của mô hình TCP/IP. Dựa trên mức giao thức làm mục tiêu, có thể phân loại các cuộc tấn công DDoS thành hai loại khác nhau: cấp độ mạng và cấp độ ứng dụng.

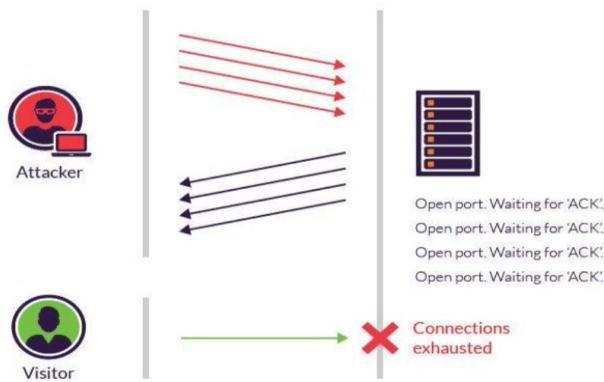
2.4.1. Cấp độ mạng

Trong các cuộc tấn công DDoS ở cấp độ mạng, giao thức mạng hoặc giao thức lớp truyền tải (trong mô hình mạng TCP/IP) được sử dụng để thực hiện cuộc tấn công và từ chối quyền truy cập vào các dịch vụ nạn nhân. Ví dụ về các cuộc tấn công này là cuộc tấn công TCP SYN, cuộc tấn công PUSH và ACK, cuộc tấn công UDP Flood và cuộc tấn công ICMP Flood.

2.4.2. Tấn công TCP SYN

Trong một cuộc tấn công TCP SYN (hình 3), lỗ hổng cố hữu của bắt tay ba chiều TCP bị khai thác: máy chủ cần phân bổ cấu trúc dữ liệu cho mỗi gói SYN đến, bất kể tính xác thực của nó. Do đó, kẻ tấn công sử dụng các tác nhân của nó để gửi một số lượng lớn các gói TCP SYN đến hệ thống nạn nhân với các địa chỉ IP nguồn giả mạo. Các gói TCP SYN / ACK trả lời của nạn nhân được gửi đến các địa chỉ giả mạo (có thể không tồn tại hoặc không được sử dụng) và do đó sẽ không được công nhận, khiến máy đích phải chờ đợi các gói ACK vô thời

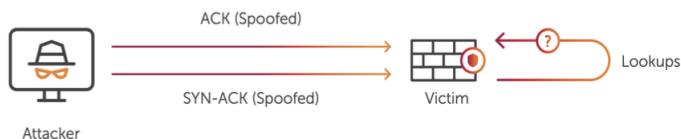
hạn. Xem xét rằng hệ thống nạn nhân có hàng đợi bộ đệm giới hạn cho các kết nối TCP mới, khi một khối lượng lớn các yêu cầu TCP SYN được xử lý và không có gói ACK nào được nhận, nó sẽ hết tài nguyên (tức là hàng đợi bộ đệm kết nối TCP bị quá tải) và nó không thể xử lý các yêu cầu của người dùng hợp pháp.



Hình 3. Tấn công TCP SYN

2.4.3. Tấn công PUSH và ACK

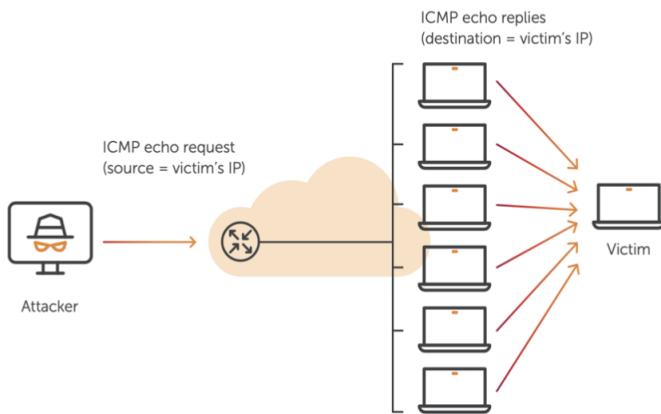
Trong một cuộc tấn công TCP PUSH và ACK (ACK-PUSH), các gói TCP có cờ PUSH và ACK được thiết lập sẽ được gửi từ các agent đến nạn nhân (hình 4). Các cờ này hướng dẫn máy nạn nhân dỡ bỏ tất cả dữ liệu trong bộ đệm TCP đến (bất kể nó đã đầy hay chưa) và gửi lại một ACK khi nó đã được thực hiện xong. Nếu nhiều gói TCP PUSH và ACK được gửi từ các agent khác nhau đến hệ thống nạn nhân, nó sẽ bị quá tải và nó sẽ bị sập. Tấn công TCP SYN và ACK-PUSH là kiểu tấn công khai thác lỗ hổng của giao thức TCP/IP.



Hình 4. Tấn công ACK-PUSH

2.4.4. Tấn công ICMP Flood

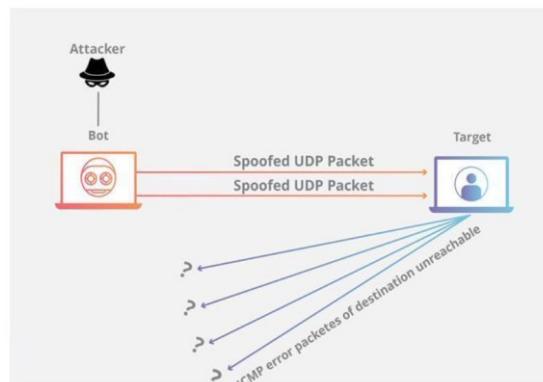
Trong một cuộc tấn công ICMP Flood, một khối lượng lớn các gói ICMP ECHO REQUEST (còn được gọi là “ping”) được các agent gửi đến nạn nhân. Các gói này yêu cầu phản hồi (REPLY) từ nạn nhân và chính sự kết hợp của các REQUEST/REPLY ICMP dẫn đến bão hòa băng thông của mạng nạn nhân. Trong cuộc tấn công này, địa chỉ IP nguồn của các gói ICMP thường bị giả mạo, do đó, các gói phản hồi từ nạn nhân không được gửi lại cho các tác nhân mà đến các máy chủ khác không biết (hình 5).



Hình 5. Tấn công ICMP Flood

2.4.5. Tấn công UDP Flood

Trong một cuộc tấn công UDP Flood, rất nhiều gói tin UDP được gửi đến một cổng ngẫu nhiên hoặc một cổng cụ thể của nạn nhân. Sau khi nhận được, máy chủ sẽ cố gắng xử lý chúng để xác định ứng dụng nào đang đợi trên cổng để xử lý. Nếu không có ứng dụng nào đang chạy trên cổng đó, máy nạn nhân sẽ gửi lại một gói ICMP với thông báo “cổng đích không thể truy cập”(hình 6). Tuy nhiên, gói phản hồi thường không đến được các agent (nơi thực sự gửi các gói UDP), vì địa chỉ IP nguồn bị giả mạo để che giấu danh tính của agent. Kết quả của cuộc tấn công là mạng của nạn nhân bị bão hòa và băng thông khả dụng cho yêu cầu dịch vụ hợp pháp bị cạn kiệt. Hơn nữa, nếu đủ gói UDP được chuyển đến nạn nhân, máy chủ của nó sẽ cạn kiệt. Loại tấn công này cũng thường tác động đến khả năng kết nối của các hệ thống nằm ở phía nạn nhân và có thể làm bão hòa băng thông của các kết nối nằm xung quanh hệ thống được nhắm mục tiêu. Tấn công ICMP Flood và UDP Flood là kiểu tấn công làm ngập lụt đường truyền.

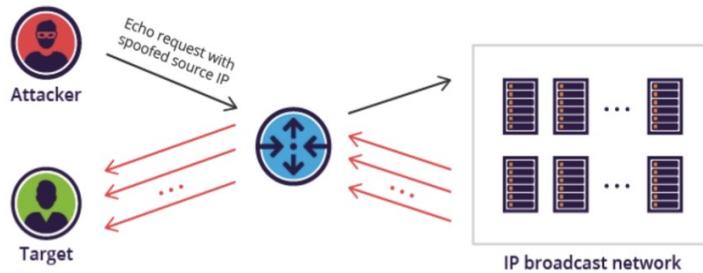


Hình 6. Tấn công UDP Flood

2.4.6. Tấn công Smurf

Cuộc tấn công Smurf là một loại tấn công ICMP Flood cụ thể, trong đó kẻ tấn công gửi các gói ICMP ECHO REQUEST (“ping”) đến một bộ khuếch đại mạng (một hệ thống hỗ trợ

phát sóng địa chỉ) giả mạo địa chỉ IP nguồn là địa chỉ IP của nạn nhân (hình 7). Bộ khuếch đại chuyên tiếp các gói “ping” đến tất cả các máy trong dải địa chỉ quảng bá và mỗi máy sẽ trả lời bằng ICMP ECHO REPLY cho máy nạn nhân. Kiểu tấn công này khuếch đại các gói tấn công ban đầu lên hàng chục hoặc hàng trăm lần, phụ thuộc vào số lượng hệ thống nằm trong địa chỉ truyền rộng được nhắm mục tiêu, và làm tổn thương cả nạn nhân và các hệ thống phát sóng trung gian.

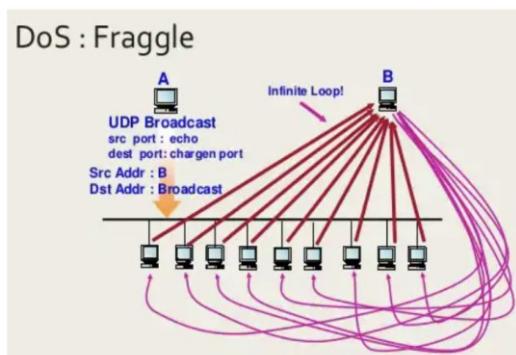


Hình 7. Tấn công Smurf

2.4.7. Tấn công Fraggle

Cuộc tấn công Fraggle (còn gọi là tấn công khai thác lỗ hỏng ECHO/CHARGEN) là một kiểu tấn công UDP Flood cụ thể tương tự như kiểu tấn công Smurf (hình 8). Để thực hiện cuộc tấn công này, kẻ tấn công gửi các gói UDP ECHO đến cổng hỗ trợ giao thức CHARGEN (thường là cổng 19), giả mạo cổng nguồn giao thức ECHO (echo protocol) của nạn nhân (thường là cổng 7), do đó tạo ra một vòng lặp tấn công vô hạn: các gói UDP ECHO nhắm mục tiêu đến CHARGEN của các hệ thống quảng bá trung gian; Hệ thống trung gian gửi các gói tin CHARGEN đến dịch vụ echo của hệ thống nạn nhân; Hệ thống nạn nhân sẽ trả lời cùng một gói tin echo đến trở lại đến CHARGEN của hệ thống quảng bá và tạo thành một vòng lặp vô tận. Cuộc tấn công Fraggle gây rối loạn hơn so với cuộc tấn công của Smurf, do nó có khả năng tạo ra nhiều gói tin hơn.

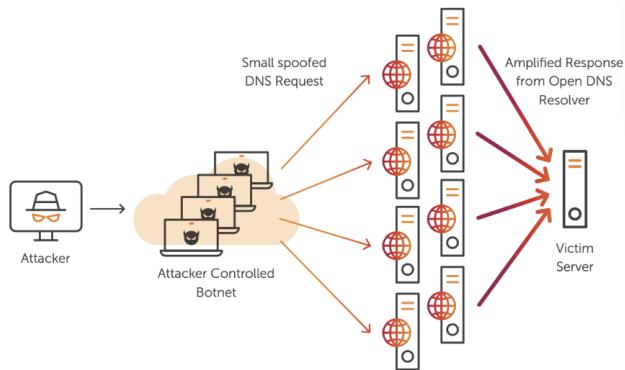
2.4.8. Tấn công khuếch đại DNS



Hình 8. Tấn công Fraggle

Trong một cuộc tấn công khuếch đại DNS, kẻ tấn công sẽ gửi rất nhiều yêu cầu DNS đến một máy chủ định danh (được sử dụng làm bộ phản xạ) và gói tin yêu cầu này giả mạo địa chỉ IP nguồn của chúng là địa chỉ IP của nạn nhân. Máy chủ định danh phản hồi các yêu cầu

đó gửi lại các phản hồi DNS cho nạn nhân. Vì dung lượng một truy vấn DNS nhỏ có thể tạo ra một phản hồi DNS có dung lượng gói tin lớn hơn đáng kể, nếu số lượng yêu cầu được gửi đến bộ phản xạ đủ lớn, thì có thể làm bão hòa độ rộng băng tần của nạn nhân (hình 9). Trong kiểu tấn công này, kẻ tấn công có thể gửi các yêu cầu DNS trực tiếp hoặc thông qua các bot để tăng dung lượng tấn công.



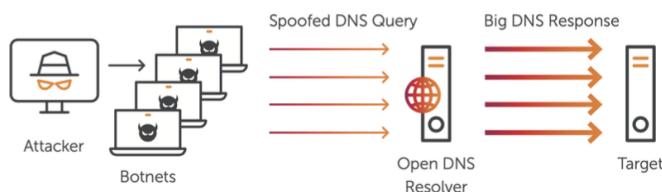
Hình 9. Tấn công khuếch đại DNS

Tấn công Smurf, tấn công Fraggle và tấn công khuếch đại DNS là kiểu tấn công khuếch đại truy cập. Trong loại tấn công này, tính năng địa chỉ IP quảng bá được tận dụng để khai thác tấn công (tức là chuyển tiếp một gói tin quảng bá đến tất cả các địa chỉ IP trong dải địa chỉ mạng, tính năng này có sẵn trong hầu hết các bộ định tuyến). Bên cạnh đó, tấn công khuếch đại DNS cũng là một loại tấn công DDoS tác động tới cấp độ ứng dụng mà trong đó tài nguyên nạn nhân (ví dụ: CPU, bộ nhớ và đĩa / cơ sở dữ liệu) bị cạn kiệt bằng cách nhắm mục tiêu vào các giao thức của lớp ứng dụng.

2.4.9. Cấp độ ứng dụng

a. Tấn công DNS Flood

Trong một cuộc tấn công DNS Flood, rất nhiều truy vấn DNS giả mạo được các tác nhân gửi đến máy chủ định danh nạn nhân để làm cạn kiệt tài nguyên giao tiếp và tính toán của nó. Nạn nhân không thể thực hiện các yêu cầu hợp pháp đối với những yêu cầu độc hại; trước đó, nó bị choáng ngợp trong khi cố gắng trả lời tất cả chúng (hình 10). Cuộc tấn công này cực kỳ khó phát hiện vì các yêu cầu DNS độc hại giống hệt với các yêu cầu hợp pháp.

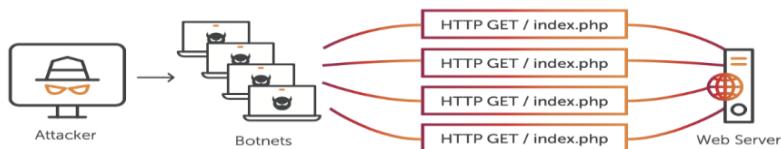


Hình 10. Tấn công DNS Flood

b. Tấn công HTTP Flood

Trong một cuộc tấn công HTTP Flood, một số lượng lớn các request HTTP được gửi bởi các agent đến máy chủ nạn nhân để làm cạn kiệt tài nguyên của nó. Những yêu cầu này

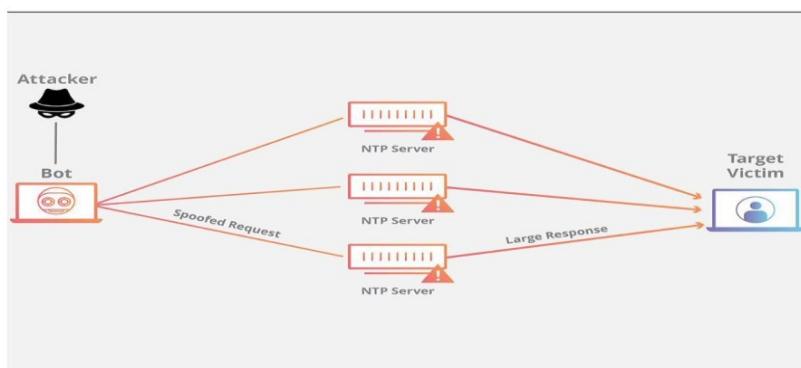
được xây dựng chính xác để vừa tối đa hóa sức mạnh tấn công vừa tránh bị phát hiện. Ví dụ: một yêu cầu HTTP duy nhất tải xuống tệp lớn từ máy chủ (ví dụ: hình ảnh) có thể tiêu tốn đáng kể tài nguyên của máy chủ, nhưng việc lặp lại các yêu cầu đối với tệp lớn có thể dễ dàng bị phát hiện và bị chặn. Do đó, những kẻ tấn công có thể mô phỏng dung lượng HTTP hợp pháp bằng cách hướng dẫn các bot gửi nhiều yêu cầu đến mục tiêu, phân tích các câu trả lời và theo dõi đệ quy các liên kết. Bằng cách này, tài nguyên nạn nhân bị tiêu thụ nhưng rất khó để phân biệt dung lượng độc hại với dung lượng hợp pháp (hình 11).



Hình 11. Tấn công HTTP Flood

c. Tấn công khuếch đại NTP

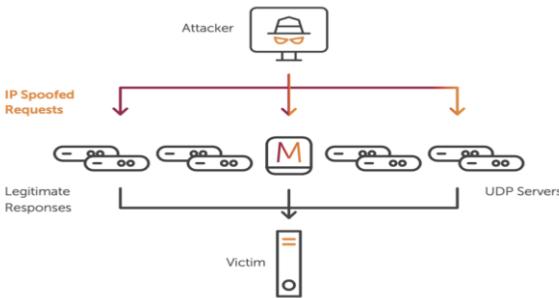
Trong quá trình khuếch đại NTP, kẻ tấn công sử dụng địa chỉ IP giả mạo của cơ sở hạ tầng NTP của nạn nhân và gửi các yêu cầu NTP nhỏ đến các máy chủ trên Internet, dẫn đến số lượng phản hồi NTP rất lớn. Vì những kẻ tấn công giả mạo cơ sở hạ tầng NTP của nạn nhân, nên tất cả các phản hồi được trả lời / khuếch đại đều tràn vào máy chủ NTP của nạn nhân. Các gói phản hồi NTP giống với dung lượng NTP thực, làm cho cuộc tấn công này khó bị phát hiện. Hệ số khuếch đại có thể đạt tới 50X, dẫn đến tình trạng ngập lụt lớn có thể khiến máy chủ NTP hoặc toàn bộ mạng ngoại tuyến (hình 12).



Hình 12. Tấn công khuếch đại NTP

d. Tấn công khuếch đại Memcached

Các cuộc tấn công khuếch đại Memcached là một loại tấn công khuếch đại UDP sử dụng lỗ hổng của các máy memcached trên mạng Internet. Trước tiên, kẻ tấn công nạp cơ sở dữ liệu máy chủ memcached. Sau đó, nó sẽ gửi các yêu cầu thông qua UDP, sử dụng địa chỉ IP giả mạo (của mục tiêu), đến hàng nghìn máy chủ memcached đang mở trên mạng Internet. Các máy chủ phản hồi bằng cách gửi nhiều gói UDP có cổng nguồn là 11211 đến đích. Hiệu quả của các cuộc tấn công này là do các máy chủ memcached khuếch đại các yêu cầu giả mạo tác động mục tiêu lên gấp 50.000 lần (hình 13).



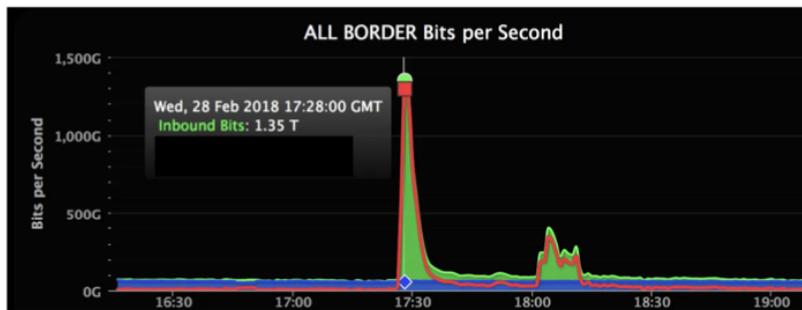
Hình 13. Tấn công khuếch đại Memcached

Ngoài ra, tấn công DDoS bằng mạng botnet IoT còn có các kiểu tấn công khác như: tấn công RST/Fin Flood, tấn công khuếch đại phản xạ SSDP, tấn công khuếch đại LDAP, tấn công khuếch đại phản xạ SNMP.

3. KẾT QUẢ VÀ THẢO LUẬN

3.1. Dung lượng của các cuộc tấn công DDoS

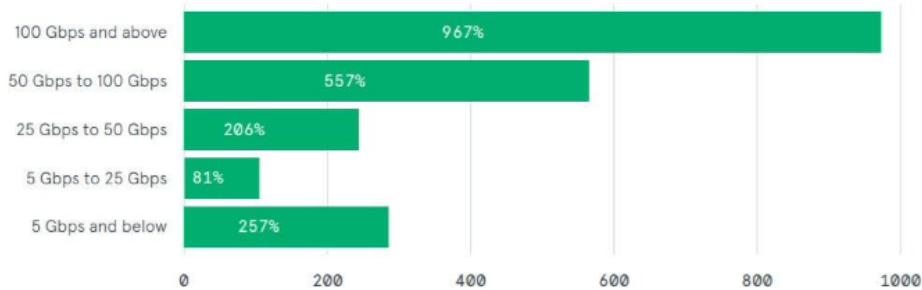
Cuối tháng 02/2018, nhà cung cấp dịch vụ về mã nguồn GitHub đã trở thành mục tiêu trong một cuộc tấn công DDoS với dung lượng 1,3 Tbps (hình 14).



Hình 14. Dung lượng tấn công DDoS vào Github

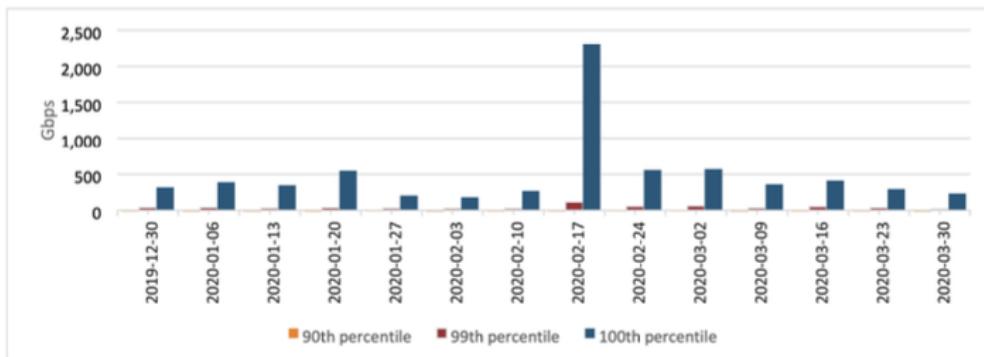
Đầu tháng 03/2018, Arbor Networks thông báo rằng một nhà cung cấp dịch vụ của Hoa Kỳ đã bị tấn công DDoS với dung lượng lên đến 1,7 Tbps. Trong trường hợp này, không có sự cố nào xảy ra vì nhà cung cấp đã thực hiện các biện pháp bảo vệ thích hợp, nhưng rõ ràng đây là cuộc tấn công DDoS khuếch đại memcached với dung lượng lớn nhất được ghi nhận.

Theo thống kê từ [23] trong năm 2019, các cuộc tấn công với dung lượng trên 100 GB/s tiếp tục gia tăng, ngay cả sau khi tăng 967% đáng kinh ngạc vào năm 2019 so với năm 2018. Ngoài ra, các cuộc tấn công từ 50 GB/s đến 100 GB/s cũng tăng 567%.



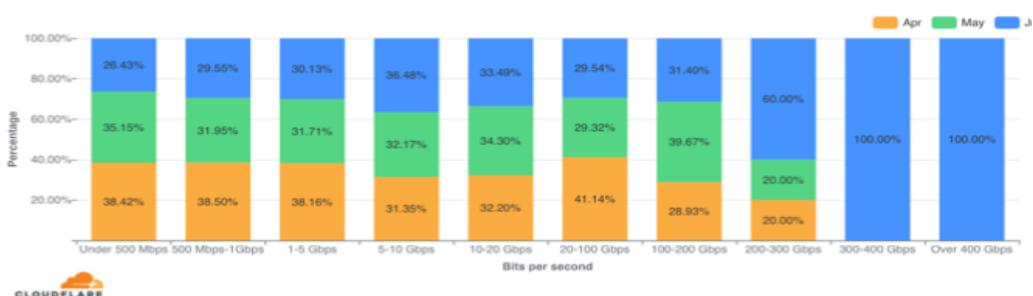
Hình 15. Mức độ giá tăng dung lượng tấn công trong năm 2019

Vào quý 1 năm 2020, Amazon tiết lộ rằng họ buộc phải chống lại cuộc tấn công DDoS 2,3 Tbps [24]. Điều này quan trọng vì nhiều lý do; đầu tiên, đây là cuộc tấn công được ghi nhận lớn nhất trong lịch sử (tại thời điểm đó), gần gấp 4 lần tốc độ của kỷ lục trước đó (587 GB/s) hình 16.



Hình 16. Dung lượng tấn công DDoS được Amazon ghi nhận vào Q1-2020

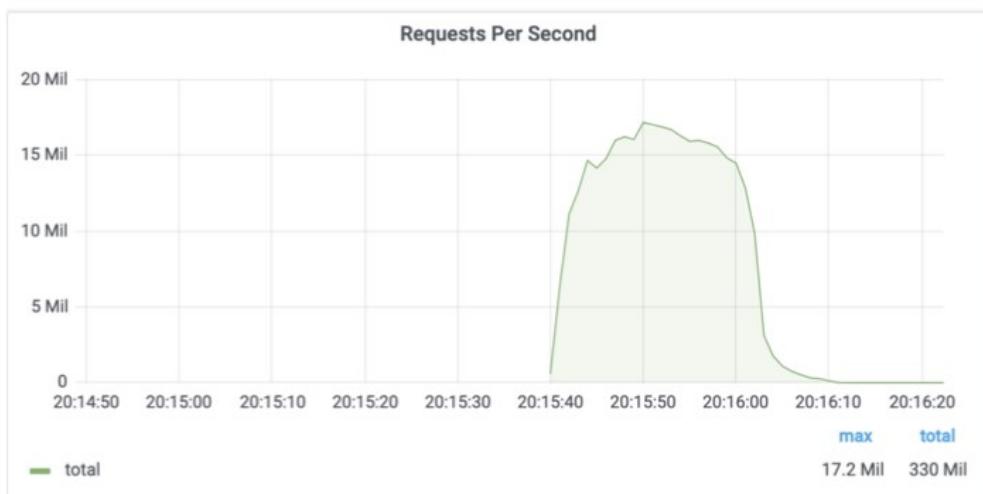
Bên cạnh đó, theo ghi nhận từ Cloudflare dung lượng của các cuộc tấn công DDoS ngày càng tăng, đặc biệt là trong tháng 06/2021 (hình 17), có đến 100% các cuộc tấn công DDoS có dung lượng 300 - 400 Gbps và trên 400 Gbps. Điều này cho thấy rằng, tấn công DDoS với dung lượng lớn đã xảy ra thường xuyên hơn và liên tục phát vỡ các kỷ lục về dung lượng.



Hình 17. Dung lượng tấn công DDoS trong Q2 năm 2021

Đầu mùa hè năm 2021, hệ thống bảo vệ DDoS tự động của Cloudflare [26] đã tự động phát hiện và giảm thiểu cuộc tấn công DDoS 17,2 triệu request-per-second (rps), một cuộc tấn

công lớn hơn gần ba lần so với bất kỳ cuộc tấn công nào trước đó mà Cloudflare từng ghi nhận. Theo thống kê trong quý 2 năm 2021, Cloudflare phục vụ trung bình hơn 25 triệu yêu cầu HTTP mỗi giây (dung lượng truy cập hợp lệ). Vì vậy, với cột mốc 17,2 triệu rps, cuộc tấn công này đã đạt tới 68% tốc độ rps trung bình trong quý 2 của Cloudflare đối với dung lượng truy cập HTTP hợp lệ. Đây là cuộc tấn công DDoS HTTP lớn nhất mà Cloudflare từng thấy cho đến nay và lớn gần gấp ba lần kích thước của bất kỳ cuộc tấn công DDoS HTTP nào khác được ghi nhận (hình 18).



Hình 18. Botnet Mirai tấn công HTTP Flood vào Cloudflare

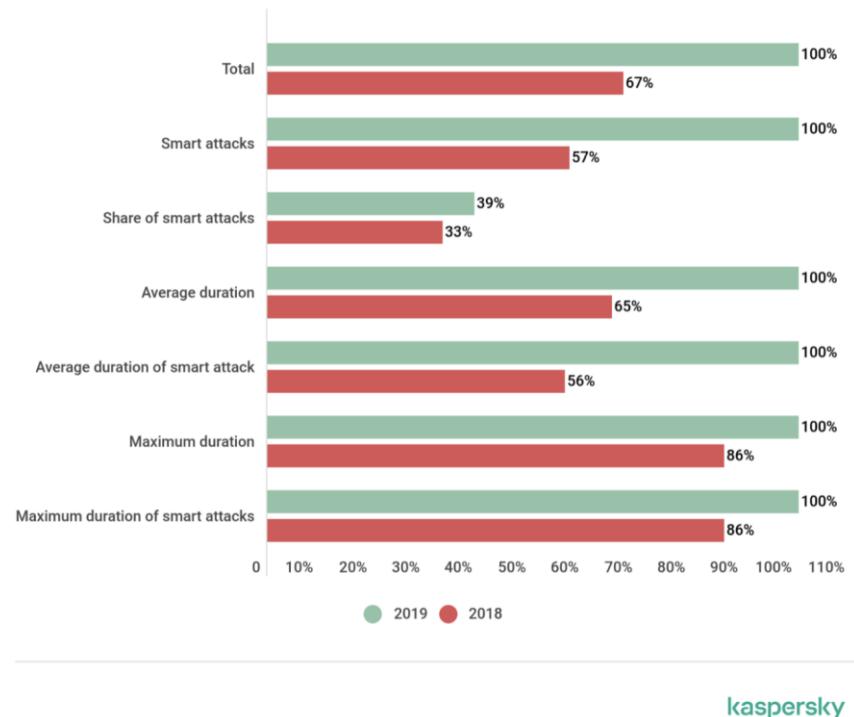
2.2. Quy mô của các cuộc tấn công

Từ báo cáo [26] cho thấy rằng (hình 18-19), cuộc tấn công DDoS vào Cloudflare trong Q2-2021 được gây ra bởi botnet Mirai, có xuất phát điểm từ 125 quốc gia với hơn 20000 bot được huy động. Dựa trên địa chỉ IP nguồn của bot, gần 15% cuộc tấn công bắt nguồn từ Indonesia và 17% khác từ Ấn Độ và Brazil cộng lại. Và một điểm mà chúng ta cần phải lưu ý rằng Việt Nam đang đứng thứ 4 trong danh sách này với hơn 5% lượng bot tham gia vào cuộc tấn công này. Điều này chứng tỏ rằng, số thiết bị IoT nhiễm malware Mirai ở Việt Nam đang nằm ít nhất trong top 4 trên thế giới.



Hình 19. Nguồn tấn công được sắp xếp theo quốc gia

Từ dữ liệu của Kaspersky Lab [27] đã chứng minh thực tế về mức tăng 10% trong quý 4 năm 2020 so với năm 2019. Điều này đáng chú ý bởi vì hoạt động DDoS tấn công nhiều hơn gần gấp đôi trong năm 2019 so với năm 2018 (hình 20).



Hình 20. So sánh dữ liệu DDoS trong năm 2018 và 2019

Trong nửa đầu năm 2021, Mỹ và Trung Quốc tiếp tục dẫn đầu trong các nước là xuất phát điểm và cũng là mục tiêu của các cuộc tấn công DDos. Trong đó, Việt Nam lại xuất hiện nằm trong top 10 các nước hứng chịu nhiều nhất các cuộc tấn công DDoS trên thế giới [27].

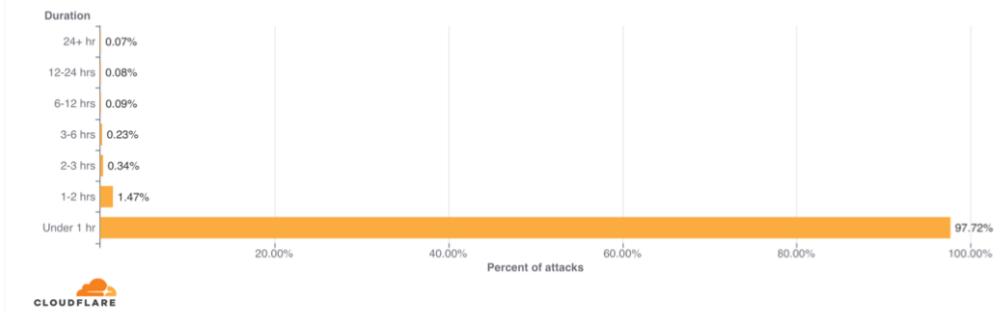


Hình 21. Các quốc gia xuất phát điểm của các cuộc tấn công DDoS trong Q1, Q2 năm 2021

Trở lại năm 2018, một cuộc tấn công DDoS [23] đã phá vỡ các kỷ lục hiện có bằng cách làm tràn dữ liệu của hệ thống mục tiêu của họ trong 329 giờ hoặc gần 2 tuần. Tuy nhiên, vào quý 2 năm 2019, Kaspersky đã phân tích các lệnh được gửi đến mạng DDoS và phát hiện ra một cuộc tấn công thậm chí còn lâu hơn, một cuộc tấn công đã kéo dài 509 giờ.

Số lượng các cuộc tấn công DDoS trong năm 2020 hiện đang có xu hướng cao hơn những năm trước. Tuy nhiên, theo thống kê mà chúng tôi có được đã cho thấy một loạt các cuộc tấn công cực ngắn đã xuất hiện và trên thực tế, một cuộc tấn công DDoS trung bình kéo dài dưới bốn giờ [23]. Điều đó nói rằng, đã có nhiều cuộc tấn công được báo cáo kéo dài từ mười ngày trở lên xảy ra.

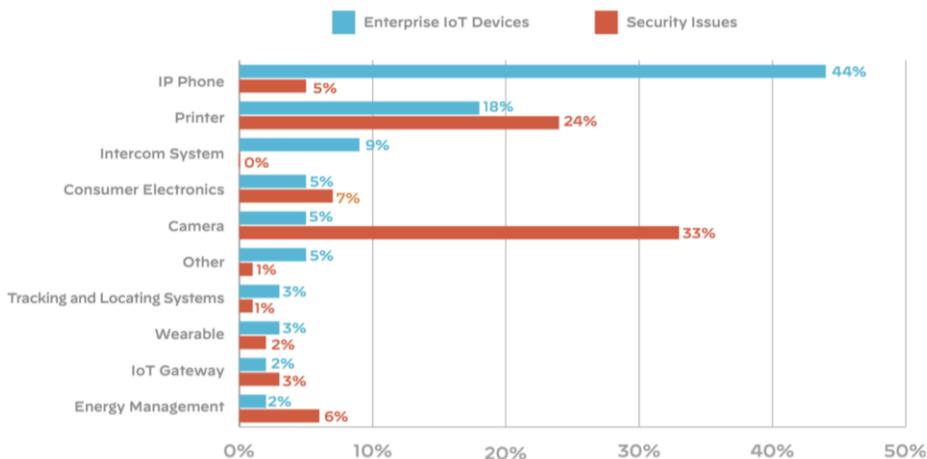
Mặc dù vậy, các cuộc tấn công DDoS kéo dài ngày càng xuất hiện ít hơn, tuy nhiên quy mô botnet được huy động thì ngày càng lớn và tần suất xuất hiện ngày càng tăng. Theo [23], [27] có hơn 90% các cuộc tấn công DDoS trong quý 1 năm 2021 kéo dài chưa đến 4 giờ nhưng đó chỉ là bè nổi. Cloudflare cảnh báo rằng các cuộc tấn công bùng nổ ngắn này thường được sử dụng để kiểm tra khả năng phòng thủ của nạn nhân. Nghiên cứu cho thấy cuộc tấn công DDoS trung bình vào năm 2020 sử dụng hơn 1 Gbps dữ liệu [24], quá đủ để đánh sập hầu hết các trang web có quy mô vừa và nhỏ. Hơn nữa, chúng tôi đã thấy sự gia tăng đáng kể về thời lượng trung bình, với hầu hết các cuộc tấn công hiện kéo dài từ 30 phút đến một giờ, thay vì mươi phút hoặc ít hơn như những năm trước [22] (hình 22).



Hình 22. Thời lượng các cuộc tấn công DDoS được Cloudflare ghi nhận trong Q2 năm 2021

Các cuộc tấn công DDoS thường sử dụng botnet nói chung và botnet là các thiết bị IoT nói riêng thường gửi một lượng lớn lưu lượng truy cập đến một máy chủ duy nhất để làm quá tải nó với các yêu cầu. Hơn 12 triệu “vũ khí DDoS”, hoặc địa chỉ IP bị lây nhiễm trên khắp thế giới, hiện đang được sử dụng như một phần của các cuộc tấn công DDoS. Malware Mirai và nhiều biến thể của nó hiện là malware phổ biến nhất được sử dụng để tạo mạng botnet cho các cuộc tấn công DDoS, mặc dù những malware khác cũng tồn tại.

Thiết bị IoT [28] luôn hiện diện xung quanh chúng ta như IP Phone, máy in, camera giám sát v.v. Các thiết bị kết nối mạng này đều là mục tiêu của những kẻ tấn công và chúng thường không được bảo vệ đúng cách (hình 23).



Hình 23. Tỷ lệ phân bổ giữa thiết bị IoT và các mối nguy về ATTT

4. KẾT LUẬN

Trong bài báo này nhóm tác giả đã phân tích về nguy cơ tấn công các thiết bị IoT, sử dụng các thiết bị IoT để tấn công từ chối dịch vụ DDoS. Những thiệt hại mà các thiết bị IoT có thể gây ra nếu bị chiếm quyền điều khiển.

IP Phone chúng chiếm 44% tổng số thiết bị IoT của doanh nghiệp nhưng chỉ chiếm 5% trong tổng số các vấn đề bảo mật. Được sử dụng trong nhiều ngành công nghiệp, IP phone thường được thiết kế để đạt được mức độ bảo mật và tin cậy mà doanh nghiệp yêu cầu. Tuy nhiên, theo hình minh họa (hình 23), Camera an ninh chỉ chiếm 5% trong số các thiết bị IoT của doanh nghiệp, nhưng chúng lại chiếm tới 33% trong tất cả các vấn đề an ninh. Điều này là do nhiều camera được thiết kế để dành cho người tiêu dùng, tập trung vào sự đơn giản của việc sử dụng và triển khai hơn là bảo mật.

Trong tương lai chúng tôi tiếp tục nghiên cứu các kỹ thuật khai thác và tìm ra các lỗ hổng mới, tìm những điểm yếu trong một số loại thiết bị IoT, Đặc biệt là các thiết bị camera đang được sử dụng rộng rãi và xây dựng ứng dụng phát hiện lỗi camera tự động cho người sử dụng.

TÀI LIỆU THAM KHẢO

1. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, 2012, pp. 1497-1516, [Online]. Available: <https://doi.org/10.1016/j.adhoc.2012.02.016>.
2. Y.Yang, L.Wu, G.Yin, L.Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet of Thing,” IEEE Internet Things J., vol. 4, no.5, 2017, pp.1250-1258.
3. Zhen Ling, Kaizheng Liu, Yiling Xu, Chao Gao, Yier Jin, Cliff Zou, Xinwen Fu, Wei Zhao, "IoT Security: An End-to-End View and Case Study", Cryptography and Security, May 2018. Available: <https://doi.org/10.48550/arXiv.1805.05853>.
4. MalwareTech, “Mapping Mirai: A botnet Case Study”, 2016. <https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html>, last accessed 2022/01/20.
5. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the mirai botnet,” in Proceedings of the 26th USENIX Security Symposium (Security), 2017.
6. R. Chirgwin, “Get pwned: Web cctv cams can be hijacked by single http request - server buffer overflow equals remote control,” https://www.theregister.com/2016/11/30/iot_cameras_compromised_by_long_url, last accessed 2022/01/20.
7. NIST, “CVE-2018-3892 Detail”, Information Technology Laboratory, <https://nvd.nist.gov/vuln/detail/CVE-2018-3892>, last accessed 2022/01/20.
8. NIST, “CVE-2018-19864 Detail”, Information Technology Laboratory, <https://nvd.nist.gov/vuln/detail/CVE-2018-19864>, last accessed 2022/01/20.
9. OWASP Top 10 team, Open Web Application Security Project (OWASP), OWASP Top Ten Project, SQL injection – OWASP, Available at: https://owasp.org/www-community/attacks/SQL_Injection.
10. NIST, “CVE-2017-18377 Detail”, Information Technology Laboratory, <https://nvd.nist.gov/vuln/detail/CVE-2017-18377>, last accessed 2022/01/20.
11. NIST, “CVE-2019-7675 Detail”, Information Technology Laboratory, <https://nvd.nist.gov/vuln/detail/CVE-2019-7675>, last accessed 2022/01/20.

12. O'Sullivan, William & Choo, Kim-Kwang Raymond & Le-Khac, Nhien-An, "Defending IoT Devices from Malware", Cyber and Digital Forensic Investigations, 2020, pp.5-29. Available: http://dx.doi.org/10.1007/978-3-030-47131-6_2.
13. Y. Seralathan, T. T. Oh, S. Jadhav, J. Myers, J. P. Jeong, Y. H. Kim, et al., "IoT security vulnerability: A case study of a Web camera," in 2018 20th International Conference on Advanced Communication Technology (ICACT), 2018, pp. 172-177.
14. <https://viettelsolutions.vn/viettelthreat-intelligence/>
15. Ayush Kumar, Teng Joon Lim, "Early Detection Of Mirai-Like IoT Bots In Large-Scale Networks Through Sub-Sampled Packet Traffic Analysis", National University of Singapore, Singapore, Dec 2019
16. <https://findface.pro/en/security/>, last accessed 2022/10/20.
17. <https://ntechlab.com/>, last accessed 2022/10/20.
18. Xinwen Fu, "IoT Security: An End-to-End View and Case Study", ResearchGate, May 2018
19. Tiêu chuẩn quốc gia TCVN 10295:2014 (ISO/IEC 27005:2011) về Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro an toàn thông tin, Hà Nội, 2014
20. <https://developer.ibm.com/technologies/iot/articles/iot-anatomy-iot-malware-attack/>, last accessed 2022/10/20.
21. <https://ieeexplore.ieee.org/document/8990084>, last accessed 2022/10/20.
22. Palo Alto Network, Impacts of Cyberattacks on IoT Devices, 2020
23. Cisco, Whitepaper Annual Internet Report (2018–2023), 2020
24. Amazon, AWS Shield Threat Landscape Report Q1-2020, 2020
25. Allot, DDoS Attack Handbook, 2018
26. <https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/>
27. <https://securelist.com/ksb-2022/>, last accessed 2023/1/20.
28. Unit42, 2020 Unit42 IoT Threat Report, 2020

ABSTRACT

ANALYSIS OF DDOS ATTACKS FROM IOT DEVICES

Tran Dat Tot^{1,*}

¹*Ho Chi Minh City University of Food Industry, Vietnam*

*Email: tottd@edu.vn

Today, Internet of Things (IoT) devices have been proving their superiority, the number of IoT devices is increasing rapidly. However, the security and privacy of IoT devices emerged as a big issue. Existing studies reveal significant weaknesses in some types of IoT devices further in some situations where there is no security mechanism to protect these devices. The Mirai Botnet has demonstrated the use of IoT devices to carry out large-scale DDoS attacks. In this study, we analyze the risk of attacking IoT devices, using IoT devices for DDoS attack. The damage that IoT devices can cause if hijacked.

Keywords: Internet of Things, Camera IP, botnet Mirai, DDoS, attacks camera.

NHẬN DIỆN CÁC VIDEO CÓ YẾU TỐ CHÍNH TRỊ VIỆT NAM TRÊN MẠNG XÃ HỘI

Trần Thị Vân Anh¹, Đặng Trần Khánh^{1,*}, Nguyễn Hải Bình¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: khanh@husf.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Cùng với sự ra đời của bộ luật “An ninh mạng Việt Nam năm 2018”, việc phát hiện kịp thời và phân loại tự động các video clips mang yếu tố chính trị trên mạng xã hội đang là một nhu cầu cần thiết. Images, texts và voices là các nội dung của video clips, chúng có chứa các đặc trưng (features) dùng để phân tích và nhận dạng video. Để phân loại video hiệu quả, điều cần thiết là phải phân tích các thông tin được trích xuất từ các đặc trưng khác nhau, trong khi các mô hình huấn luyện như CNN fusion, CNN-LSTM, LR-CN chỉ tập trung vào một đặc trưng duy nhất. Bài báo đề xuất framework kết hợp đa mô hình huấn luyện có giám sát dựa trên nhiều đặc trưng để phân loại hiệu quả video mang yếu tố chính trị. Đối với nội dung voices và texts, framework sử dụng FastText để huấn luyện và phân loại dựa trên đặc trưng văn bản. Đối với images, nhóm tác giả sử dụng hai mô hình để huấn luyện: thứ nhất, sử dụng MTCNN để tách gương mặt kết hợp VGG-Face vector hóa đặc trưng và nhận diện gương mặt; thứ hai, sử dụng mô hình Inception-V3 để trích xuất đặc trưng và đưa ra điểm số phân loại dựa trên hình ảnh. Cuối cùng, mô hình LightGBM là kỹ thuật kết hợp chậm để tổng hợp huấn luyện dựa trên các điểm số phân loại từ ba mô hình trên và đưa ra kết quả phân loại ở cấp độ video. Framework có thể phân loại video khi một đặc trưng bị thiếu bằng cách sử dụng các đặc trưng còn lại. Framework được áp dụng cho tập dữ liệu mới chứa 10.000 video chính trị và phi chính trị thu thập từ TikTok. Các kết quả thử nghiệm framework cho kết quả tốt hơn so với một số mô hình dựa trên từng đặc trưng riêng lẻ, cũng như phương pháp kết hợp thông thường.

Từ khóa: Video classification, Inception-V3, MTCNN, VGG-Face, LightGBM

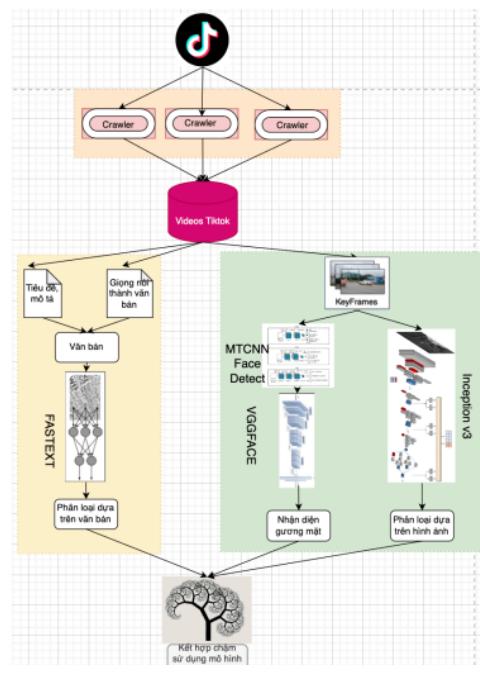
1. MỞ ĐẦU

Ngày nay, với sự phát triển mạnh mẽ của internet đặc biệt là mạng xã hội, việc tạo ra video ngày càng trở nên đơn giản và nhanh chóng. Nhưng các video chia sẻ chưa có thông tin mô tả đủ tốt về nội dung và chưa được phân loại đúng, thậm chí một số mô tả và nội dung không thống nhất với nhau gây khó khăn cho việc tìm kiếm một video nhất định theo một danh mục cụ thể.

Với sự ra đời của bộ luật “An ninh mạng Việt Nam năm 2018” [1], việc phân loại tự động các video trên internet có mang yếu tố chính trị hay không đang là chủ đề được các nhà quản lý quan tâm hiện nay. Các video này chưa đựng nhiều đặc trưng: texts, voices và images, mỗi đặc trưng đều chứa các thông tin có giá trị. Để nâng cao khả năng phân loại, điều cần thiết là phải phân tích hiệu quả của tất cả các thông tin được trích xuất từ các đặc trưng khác nhau,

trong khi hầu hết các mô hình huấn luyện như CNN Fusion[2], CNN-LSTM[3], LR-CN [3] đều bỏ qua một số đặc trưng và chỉ tập trung vào một đặc trưng duy nhất.

Nghiên cứu này trình bày một framework kết hợp nhiều mô hình học sâu trên nhiều đặc trưng như: image, text và face để phân loại hiệu quả các video mang yếu tố chính trị. Đối với đặc trưng text sử dụng mô hình word embedding là FastText[4] để huấn luyện. Đối với image và face sử dụng các mô hình CNN [5] đã được huấn luyện trước gồm: Inception-V3[6], MTCNN[7], VGG-Face[8] để trích xuất đặc trưng hình ảnh và gương mặt. Sau đó sử dụng chiến lược kết hợp chập dựa trên kỹ thuật mới trong phân loại là mô hình LightGBM[9] để biểu diễn dữ liệu và phân loại ở cấp độ video. Framework có thể phân tích video khi một đặc trưng bị thiếu bằng cách sử dụng các đặc trưng còn lại. Framework được áp dụng cho tập dữ liệu mới chứa 10.000 video chính trị và phi chính trị được thu thập từ TikTok.

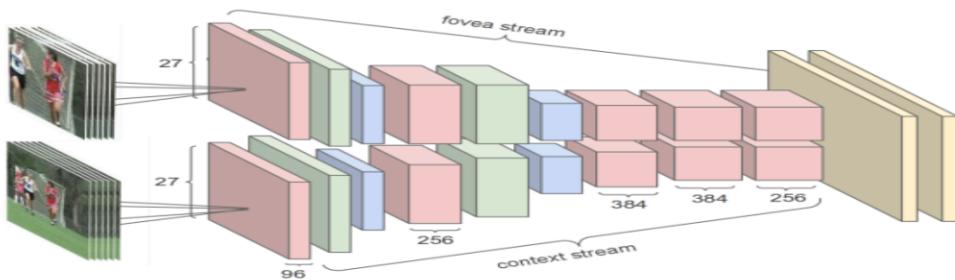


Hình 1. Framework được đề xuất kết hợp dữ liệu chập ở cấp độ video

2. CÁC CÔNG TRÌNH LIÊN QUAN

2.1. Phân loại video trên qui mô lớn với mạng nơ ron tích chập (CNN)

Trong nghiên cứu [2], nhóm tác giả đã cung cấp đánh giá thử nghiệm sâu rộng về nhiều phương pháp để mở rộng CNN vào việc phân loại video trên tập dữ liệu qui mô lớn gồm một triệu video. CNN fusion về cơ bản tập trung vào việc trả lời một số câu hỏi nhất định như: kiểu kết nối theo thời gian nào trong kiến trúc CNN có thể tận dụng chuyển động cục bộ trong video? Làm thế nào để thông tin bổ sung này cải thiện hiệu suất?



Hình 2. Minh họa kiến trúc CNN đa phân giải [2]

Hình ảnh dễ dàng được cắt và có thể mở rộng đến một kích thước nhất định và cố định nhưng video thì không, vì vậy không thể xử lý video với cùng một kiến trúc. Mô hình này đã chuyển đổi các video thành các clip nhỏ hơn để tìm hiểu các đặc điểm theo không gian – thời

gian. Họ đề xuất bốn kiến trúc khác nhau: Single frame, Late fusion, Early fusion và Slow fusion để khám phá sự kết hợp thông tin theo chiều thời gian và đề xuất một kiến trúc đa phân giải. Hình ảnh đầu vào được đưa vào hai luồng xử lý riêng biệt: luồng ngữ cảnh có độ phân giải thấp và luồng fovea dùng hình ảnh được cắt từ vùng trung tâm có độ phân giải cao.

Kết quả thử nghiệm slow fusion đạt độ chính xác tốt nhất.

Bảng 1. Minh họa các thử nghiệm phân loại của mô hình CNN fusion và các mô hình khác [2]

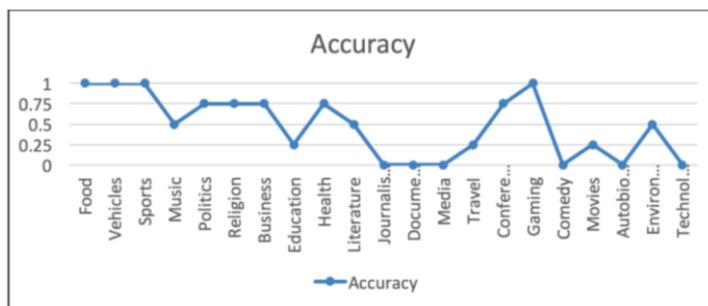
Model	Clip Hit@1	Video Hit@1	Video Hit@5
Feature Histograms + Neural Net	-	55.3	-
Single-Frame	41.1	59.3	77.7
Single-Frame + Multires	42.4	60.0	78.5
Single-Frame Fovea Only	30.0	49.9	72.8
Single-Frame Context Only	38.1	56.0	77.2
Early Fusion	38.9	57.7	76.8
Late Fusion	40.7	59.3	78.7
Slow Fusion	41.9	60.9	80.2
CNN Average (Single+Early+Late+Slow)	41.4	63.9	82.4

Bảng 1 là kết quả so sánh giữa mô hình được đề cập trong [2], bao gồm: Single frame (sử dụng kiến trúc đường cơ sở một khung để hiểu được sự đóng góp của hình thức tĩnh đối với độ chính xác của phân loại), Early fusion (kết hợp thông tin trên toàn bộ cửa sổ thời gian ngay lập tức ở cấp độ pixel), CNN average (trung bình cộng các mô hình: Single, Early, Late, Slow),...giá trị Hit@k cho biết phần trăm mẫu thử nghiệm chứa ít nhất một trong các nhãn đúng trong k dự đoán ban đầu.

Tuy nhiên, để tìm được sự liên kết của chuyển động cục bộ trong video để phân loại video hiệu quả đòi hỏi tập dữ liệu lớn, cụ thể trong công trình trên, nhóm tác giả đã sử dụng tập dữ liệu có sẵn là Sports-1M gồm 1 triệu video về chủ đề thể thao và chỉ tập trung phân tích đặc trưng hình ảnh mà bỏ qua các đặc trưng khác của video như âm thanh, văn bản.

2.2. Phân loại video trên quy mô lớn dựa trên đặc trưng văn bản

Trong công trình nghiên cứu [10], nhóm tác giả đã tóm tắt các kỹ thuật phân loại video dựa trên các đặc trưng: hình ảnh, âm thanh và văn bản. Tác giả đã đề xuất một kỹ thuật phân loại video dựa trên văn bản của video không có cấu trúc. Văn bản có nguồn gốc từ bản ghi lời nói. Để tính đến thông tin ngữ cảnh của văn bản, nhóm tác giả đã sử dụng phương pháp FastText do nhóm AI của Facebook phát triển.



Hình 3. Minh họa kết quả phân loại sử dụng mô hình FastText [10]

Các thử nghiệm được thực hiện trên tập dữ liệu 150.000 video không có cấu trúc, gồm 21 danh mục cho thấy đối với một số danh mục cho kết quả chính xác rất cao như: thức ăn, xe cộ, game; còn một số danh mục lại cho kết quả rất thấp như: thể thao, văn bản, kỹ thuật, chính trị, ...

2.3. Phương pháp kết hợp nhiều mô hình học sâu để phân loại video

Trong công trình [11], Tác giả trình bày một framework kết hợp nhiều mô hình học sâu để phát hiện sự kiện thiên tai từ 10.000 video được thu thập từ youtube bằng cách áp dụng những thế mạnh của mạng nơ ron. Đầu tiên một số mô hình học sâu được áp dụng để trích các đặc trưng hữu ích từ video. Trong đó, áp dụng các mô hình CNN đã được tiền đào tạo để trích xuất đặc trưng hình ảnh, âm thanh và mô hình word embedding để phân tích văn bản (tiêu đề, mô tả của video). Sau đó, một kỹ thuật kết hợp được đề xuất để tổng hợp các đặc trưng ở hai cấp độ, ở cấp độ frame: một mạng CNN được áp dụng để kết hợp 2 đặc trưng tạm thời hình ảnh và âm thanh tại thời điểm frame và kết quả là điểm số dự đoán và kết hợp với đặc trưng văn bản ở cấp độ video bằng một thuật toán mà tác giả đề xuất.

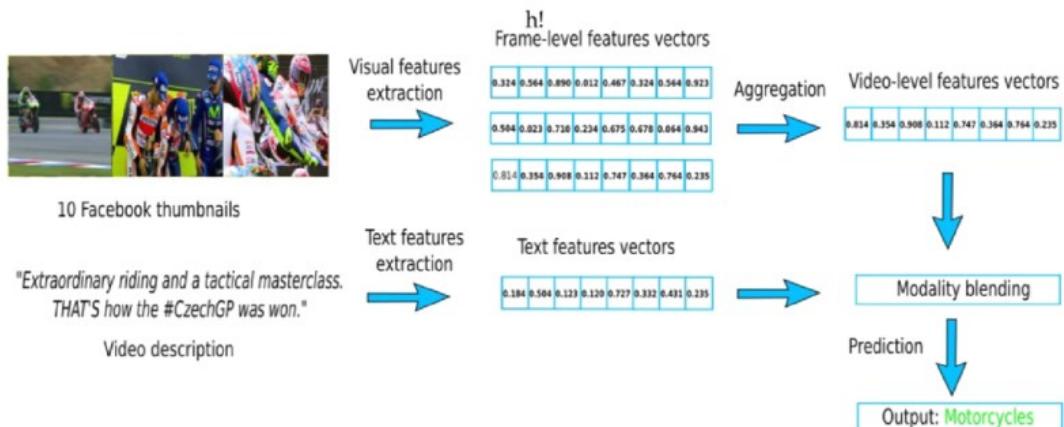
Với chiến lược kết hợp này, kết quả phân loại cuối cùng được xác định bằng mô hình thích hợp và kết quả có thể được kết hợp bằng cách sử dụng các ưu điểm của các mô hình và các đặc trưng dữ liệu của video. Ngoài ra, vấn đề thiếu dữ liệu đặc trưng cũng được xử lý bằng cách sử dụng mô hình còn lại để đề xuất. Tuy nhiên, thuật toán kết hợp chậm nhiều đặc trưng ở cấp độ video còn đơn giản, dựa trên sự so sánh xác xuất, chưa tận dụng hết thế mạnh của từng mô hình và đặc trưng của dữ liệu.

Bảng 2. Minh họa kết quả phân loại video giữa framework được đề xuất ở cấp độ frame và cấp độ video và các mô hình dựa trên từng đặc trưng [11]

Methods	ACC.	mAP	# of classes
Frame-based image features	0.471	0.226	16
Frame-based audio features	0.226	0.070	16
Frame-based early fusion	0.430	0.208	16
Video-based image features	0.109	0.107	9
Video-based audio features	0.270	0.132	9
Video-based textual features	0.352	0.189	9
Video-based early fusion	0.167	0.118	9
Video-based joint representation	0.444	0.219	9
Proposed framework	0.518	0.237	9

Bảng 2 là kết quả so sánh giữa các mô hình được đề cập trong [11], bao gồm: Frame-based image features (sử dụng mô hình Inception-V3 đã được tiền huấn luyện để đưa ra kết quả phân loại ở cấp độ frame dựa trên đặc trưng hình ảnh), Frame-based audio features (sử dụng mô hình LSTM để đưa ra kết quả phân loại ở cấp độ frame dựa trên đặc trưng âm thanh), Proposed framework (framework tác giả đề xuất), ... độ đo ACC là độ chính xác (accuracy), mAP là độ chính xác trung bình (mean Average Precision), # of classes là số lượng lớp của tập dữ liệu đường dùng trong huấn luyện và kiểm thử. Kết quả, framework mà nhóm tác giả đề xuất đạt kết quả chính xác tốt nhất.

Tương tự như vậy, trong công trình nghiên cứu [12], các tác giả đã thu thập 30.000 video ngắn từ Facebook và đề xuất một framework kết hợp nhiều mô hình để phân loại video dựa trên kiến trúc mạng nơ ron, bằng việc trích xuất đặc trưng trực quan hình ảnh, đặc trưng văn bản từ video và kết hợp chúng trong một thuật toán phân loại cuối cùng. Tác giả cũng đã áp dụng các mô hình CNN đã được đào tạo để trích xuất đặc trưng hình ảnh và mô hình word embedding để phân tích văn bản.



Hình 4. Tóm quan về framework kết hợp nhiều mô hình được đề xuất để phân loại video trên mạng xã hội [12]

Bảng 3. Minh họa kết quả phân loại video giữa các mô hình [12]

Classifier	Textual features	Visual features	Classification accuracy
SVM	word2vec	HOG	0.793 ± 0.003
		GIST	0.746 ± 0.004
		CaffeNet	0.752 ± 0.004
		InceptionV3 - average	0.835 ± 0.006
Logistic Regression	word2vec	HOG	0.800 ± 0.006
		GIST	0.755 ± 0.005
		CaffeNet	0.783 ± 0.004
		InceptionV3 - average	0.841 ± 0.004

Bảng 3 là kết quả so sánh giữa bộ phân loại SVM và Logistic Regression đề cập trong [12], đặc trưng văn bản (text features) được mô hình hóa bằng word2vec, tính năng trực quan được trích xuất và phân loại ở cấp độ frame bao gồm: HOG (là biểu đồ của độ dốc định hướng - Histogram of oriented gradients), CaffeNet (là một mạng nơ ron) và InceptionV3-average (lấy kết quả dự đoán trung bình của tất cả các frame) ... độ đo được sử dụng để phân loại là độ chính xác (accuracy). Sau khi thử nghiệm, tác giả đưa ra mô hình tốt nhất kết hợp chập với bộ phân loại SVM. Trong các công trình nghiên cứu liên quan khác như [13] và [14] các tác giả cũng đã cho thấy được ưu thế của phương pháp kết hợp nhiều mô hình học sâu, dựa trên nhiều đặc trưng của video gồm: hình ảnh, âm thanh, văn bản trong nhiệm vụ phân loại video, thu được thông tin tổng hợp liên tục ngay cả khi một đặc trưng dữ liệu bị lỗi.

3. PHƯƠNG PHÁP THỰC HIỆN

3.1. Phương pháp thu thập và xử lý dữ liệu

3.1.1 Phương pháp thu thập dữ liệu

Nghiên cứu tập trung vào việc xây dựng mô hình phân loại các video trên các nền tảng mạng xã hội, vì vậy dữ liệu phục vụ cho đề tài sẽ được thu thập từ chính mạng xã hội TikTok. Hiện nay TikTok không cung cấp APIs để các nhà phát triển thu thập dữ liệu [15], đồng thời cũng có thêm chính sách chặn các chương trình tự động thu thập dữ liệu từ các url của họ. Vì vậy, nhóm tác giả đã phát triển một chương trình thu thập dữ liệu từ TikTok dựa trên thư viện Python Scrapy [16] và sử dụng proxy để có thể thu thập dữ liệu. Dữ liệu thu thập được lưu vào cơ sở dữ liệu gồm: tiêu đề của video, mô tả, video url và âm thanh url. Sau đó, tiếp tục tiến hành tải tất cả video và âm thanh từ url tương ứng.

Dữ liệu văn bản được kết hợp từ tiêu đề, mô tả video và văn bản sinh ra từ audio TikTok tương ứng, dữ liệu này tương đối ít cho việc huấn luyện. Vì thế nên tác giả chọn thu thập thêm các văn bản từ các nguồn khác như: vnexpress.net, chinhphu.vn, vietnamnet.vn để bổ sung dữ liệu huấn luyện và kiểm thử các mô hình trích xuất đặc trưng văn phân loại văn bản.

Dữ liệu hình ảnh chủ yếu là các frame được trích xuất từ các video TikTok đã được download về ở trên. Ngoài ra tác giả còn thu thập thêm các hình ảnh gương mặt của một số lãnh đạo trong Bộ chính trị, Bộ trưởng trong chính phủ Việt Nam từ google và đảm bảo các hình ảnh bao phủ được hết các góc cạnh của gương mặt.

Dữ liệu sau khi thu thập bước đầu sẽ được đánh nhãn tự động dựa trên các từ khoá matching trong các #hashtag của mỗi video. Phương pháp này có ưu điểm là tốc độ xử lý rất nhanh, có thể đánh nhãn cho một lượng dữ liệu lớn trong thời gian cực kì ngắn. Tuy nhiên nó cũng có nhược điểm là dễ bị đánh nhãn sai với các dữ liệu có #hashtag không thống nhất với nội dung video. Vì thế, nhóm tác giả cũng sẽ tiếp cận với phương pháp đánh nhãn thủ công sau bước đánh nhãn tự động và so sánh kết quả hai cách tiếp cận với nhau.

3.1.2 Phương pháp xử lý dữ liệu

Phương pháp xử lý dữ liệu văn bản: dữ liệu văn bản phần lớn được lấy từ mạng xã hội nên việc bị nhiễu là vấn đề không thể tránh khỏi. Vì vậy cần có những bước chuẩn hoá và lọc nhiễu bao gồm: chuẩn hoá theo chuẩn UTF8, chuẩn hóa kiểu gõ dấu tiếng Việt, chuyển toàn bộ văn bản thành chữ thường; loại bỏ toàn bộ các kí tự đặc biệt, biểu tượng không xuất hiện trong bảng chữ cái và dấu câu tiếng Việt; loại bỏ #hashtag, @user, email và url; loại bỏ các từ nối, từ dừng trong tiếng Việt. Cuối cùng, tiến hành tách từ cho các văn bản tiếng Việt sau khi đã chuẩn hoá và lọc nhiễu. Tiếng Việt là ngôn ngữ đơn âm tiết, không dễ tách từ bằng khoảng trắng như tiếng Anh, ví dụ như các từ “lãnh đạo”, “đất nước”,... Vì thế, cần phải có công cụ tách từ một cách hợp lý. Nghiên cứu sử dụng tokenizer của thư viện Python Underthesea [16] để tách từ và các thư viện của Python: Numpy [17] và bộ Extractor [18] để xử lý dữ liệu.

Phương pháp xử lý dữ liệu âm thanh: sử dụng các công cụ speech2text có sẵn để chuyển đổi âm thanh thành văn bản tương ứng, từ đó bổ sung vào dữ liệu cho mô hình phân loại văn bản. Hiện nay có nhiều công cụ speech2text cho tiếng Việt khác nhau bao gồm cả tính phí và miễn phí. Đối với mỗi dữ liệu audio được tải về, tác giả lựa chọn Google API speech to text

[19] để chuyển giọng nói thành văn bản với ngôn ngữ là tiếng Việt, tiếng Anh và ở tần số 16.000 Hz.

Phương pháp xử lý dữ liệu video và hình ảnh: Đối với dữ liệu video sau khi được tải về, tiến hành trích xuất khung chính sử dụng thư viện mã nguồn mở là FFmpeg [20] và lưu vào thư mục ID tương ứng. Phần lớn FPS của các video đều ở mức 30 frame/s. Các khung hình chính được trích xuất dựa trên việc xuất hiện sự thay đổi lớn giữa các khung liên tục với nhau. Dữ liệu hình ảnh từ các video sẽ được đưa vào mô hình phân loại. Đối với hình ảnh của các chính trị gia, tiến hành sử dụng mô hình MTCCN [7] để tách gương mặt và mô hình VGG-Face [8] để vector hóa đặc trưng gương mặt.

3.2. Phương pháp trích xuất đặc trưng và xây dựng mô hình phân loại văn bản

Nghiên cứu sử dụng trọng số TF-IDF [21] để trích xuất đặc trưng văn bản bởi ưu điểm so với Bag-of-word là có khả năng biểu diễn từ với các trọng số khác nhau dựa vào độ quan trọng của từ đó trong câu. TF-IDF gồm hai thành phần TF và IDF.

TF (*Term Frequency*) dùng để ước lượng tần suất xuất hiện của văn bản. Để chuẩn hoá tần suất này, chúng ta sẽ chia nó cho tần suất của t nhiều nhất trong văn bản đó. Công thức tính TF được biểu diễn như sau:

$$TF(t, d) = \frac{f(t, d)}{\max\{|f(w, d) : w \in d|\}} \quad (1)$$

Trong đó:

$f(t, d)$: là số lần xuất hiện của từ t trong văn bản d
 $\max\{|f(w, d) : w \in d|\}$: là tần suất của từ nhiều nhất xuất hiện trong văn bản

IDF (*Term Document Frequency*) dùng để ước lượng mức độ quan trọng của một từ trong toàn bộ tập văn bản. Đối với từng văn bản, việc một từ xuất hiện nhiều lần sẽ có mức độ quan trọng cao hơn. Tuy nhiên, đối với toàn bộ tập các văn bản, một từ mà ở văn bản nào cũng xuất hiện sẽ trở nên phổ biến và không còn quan trọng nữa. Ví dụ như các từ nối (“và”, “nhưng”, “tuy nhiên”,...) và giới từ (“ở”, “trong”, “trên”,...),... Đó là lý do chúng ta cần phải giảm đi mức độ quan trọng của những từ đó bằng cách sử dụng IDF tính bằng công thức sau:

$$IDF(t, d) = \log \left(\frac{|D|}{|\{d \in D : t \in d\}|} \right) \quad (2)$$

Trong đó:

$|D|$: là tổng số văn bản trong tập D
 $|\{d \in D : t \in d\}|$ là tổng số văn bản trong tập D
 có chứa từ t

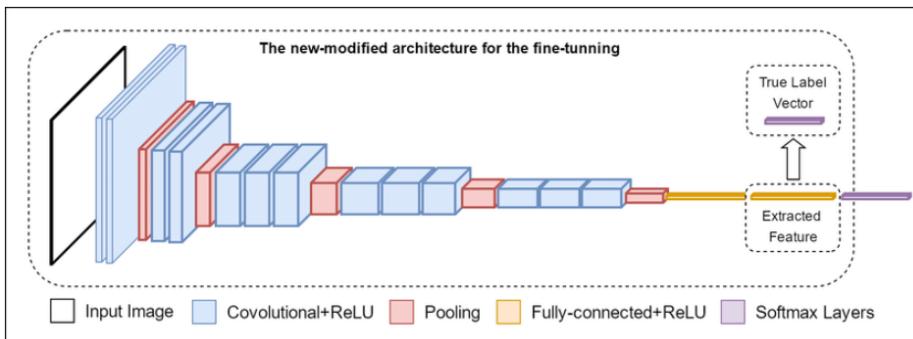
Phương pháp TF-IDF cũng có một hạn chế đó là không thể biểu diễn mối quan hệ giữa các từ trong văn bản. Hai câu “tôi đi học” và “đi học tôi” đều có cùng giá trị TF-IDF. Nghiên cứu tiếp cận thêm phương pháp word embedding là FastText để khắc phục hạn chế này. FastText tạo ra các sub-word và huấn luyện giống với mô hình skip-gram.

Bảng 4. Minh họa quá trình tách các sub-word của FastText [4]

Các cụm từ	Giá trị n-grams	Các sub-words được sinh ra
eating	3	<ea, eat, ati, tin, ing, ng>
eating	4	<eat, eati, atin, ting, ing>
eating	5	<eati, eatin, ating, ting>
eating	6	<eatin, eating, ating>

3.3. Phương pháp trích xuất đặc trưng và nhận diện khuôn mặt

Nghiên cứu sử dụng mạng MTCNN [7] để trích xuất các bounding box có chứa khuôn mặt trong toàn bộ các khung hình chính và tiến hành bóc tách. Tiếp đó các face box này sẽ được đưa vào mô hình VGG-Face [8] để lấy vector đặc trưng (embedding) của khuôn mặt tương ứng. Các lớp embedding thường sẽ là những lớp kế cận output layer của mạng (FC6, FC7). Cụ thể trong nghiên cứu chọn layer FC7.



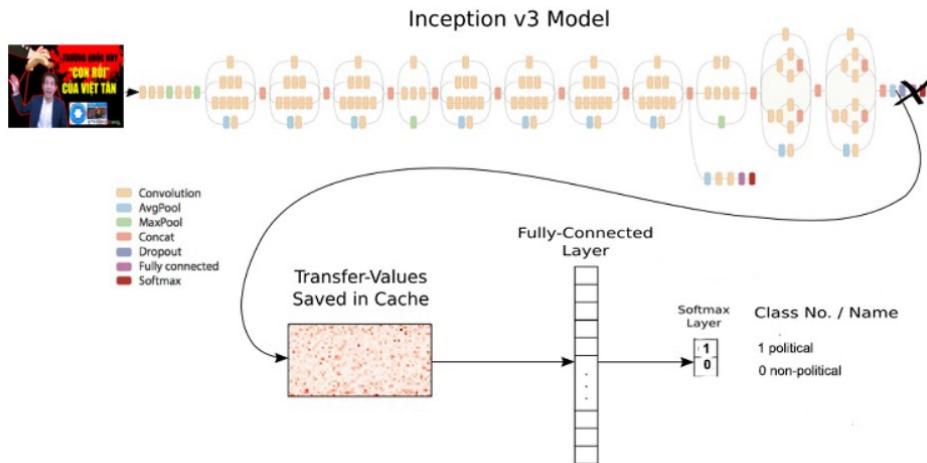
Hình 5. Minh họa kiến trúc mô hình VGG-Face theo các lớp [8]

Những khuôn mặt giống nhau thì các vector đặc trưng sẽ tương tự nhau, do đó các khuôn mặt của cùng một người sẽ có các vector đặc trưng gần nhau là giống nhau. Vì thế, sau khi có các vector đặc trưng của mỗi khuôn mặt, tiến hành tính toán khoảng cách giữa các vector đặc trưng với nhau để đánh giá. Nghiên cứu sử dụng độ đo cosine distance để tính khoảng cách giữa các vector đặc trưng. Các vector tương tự nhau sẽ có giá trị cosine lớn và tiến dần về 1, các khuôn mặt khác nhau sẽ có giá trị nhỏ hơn. Việc xác định trùng khớp khuôn mặt sẽ dựa trên một ngưỡng threshold chọn trước ($0,85 - 0,95$), hai vector có cosine distance lớn hơn hoặc bằng ngưỡng threshold sẽ được xem như là trùng nhau.

3.4. Phương pháp xây dựng mô hình phân loại hình ảnh

Ở bước xử lý dữ liệu, mỗi video đã được tách thành các khung chính tương ứng. Nghiên cứu lựa chọn tiếp cận phân loại video dựa trên phương pháp phân loại các keyframe tương ứng của video. Nghiên cứu sử dụng kỹ thuật transfer learning với mô hình Inception-V3[6] đã được tiền huấn luyện với bộ dữ liệu Imagenet[22], bỏ đi lớp kết nối đầy đủ cuối cùng và thêm

vào hai lớp mới là: lớp kết nối đầy đủ với 512 node, hàm kích hoạt ReLU, lớp output để dự đoán kết quả đầu ra với hai node, hàm kích hoạt Sigmoid.



Hình 6. Minh họa kỹ thuật học chuyển tiếp với mô hình Inception-V3 [7].

Sau quá trình học chuyển tiếp, mỗi khung hình chính khi được dự đoán sẽ có một giá trị (score) nằm trong khoảng 0-1. Giá trị trung bình các score của khung hình chính sẽ được xem như là giá trị phân loại của video tương ứng.

3.5. Phương pháp xây dựng mô hình kết hợp

Nghiên cứu sử dụng chiến lược kết hợp chậm để tổng hợp thông tin từ nhiều mô hình trích xuất thông tin trước đó rồi mới đưa ra kết quả phân loại ở cấp độ video. Các đặc trưng sau khi được trích xuất từ các mô hình phân loại văn bản, hình ảnh và khuôn mặt trước đó được tổng hợp lại thành một vector đặc trưng riêng của mỗi video, mỗi vector này sẽ chứa 3 giá trị trong khoảng từ 0-1.

Mô hình phân loại kết hợp được lựa chọn là mô hình LightGBM [9], một mô hình thuộc họ Gradient Boosting. Ngoài việc bản thân LightGBM là một trong những mô hình phân loại state-of-the-art hiện nay, mô hình này có thêm hai ưu điểm khác phù hợp để tác giả lựa chọn làm mô hình kết hợp: (1) LightGBM có khả năng xử lý những giá trị null trong các vector đặc trưng. Việc này rất có ý nghĩa với nghiên cứu khi không phải lúc nào vector đặc trưng cũng có đầy đủ giá trị text, nhiều video hoàn toàn không có bất kì đoạn văn bản nào được sinh ra từ phần audio (do chỉ có nhạc nền hoặc do video chỉ có tiếng nước ngoài). (2) Mô hình LightGBM cũng thuộc họ tree based nên có thể xếp hạng được mức độ quan trọng của các đặc trưng tương ứng. Từ đó có thể phân tích được yếu tố nào ảnh hưởng nhiều đến việc phân loại video.

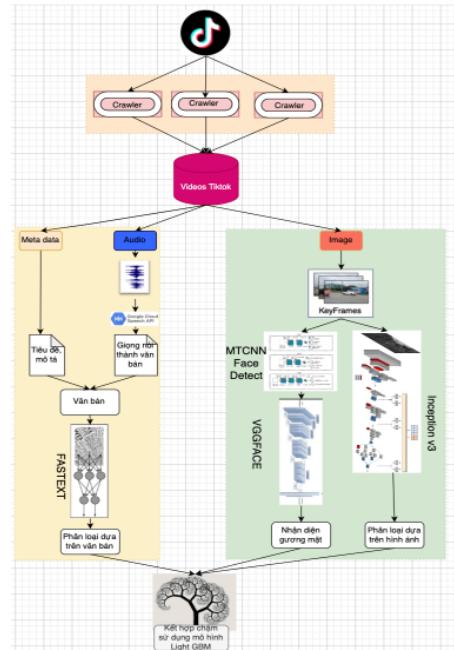
3.6. Phương pháp đánh giá

Nghiên cứu triển khai xây dựng và so sánh mô hình kết hợp với các mô hình trích xuất đặc trưng riêng lẻ. Vì thế, dữ liệu sẽ được chia thành nhiều hơn là chỉ một tập huấn luyện và kiểm thử. Dữ liệu được chia thành 03 tập riêng biệt phục vụ cho việc huấn luyện và kiểm thử (tập A 50%, tập B 35%, tập C 15%). Để đánh giá hiệu suất các mô hình phân loại, nhóm sử

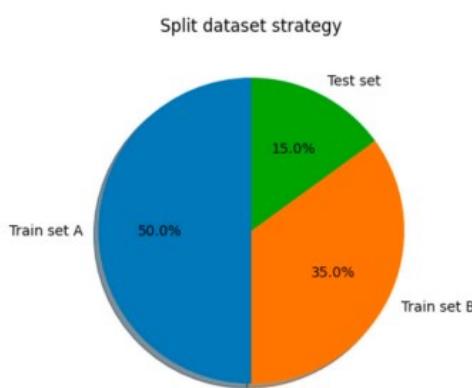
dụng hai độ đo là: Accuracy [21] và F1-Score [21] để so sánh kết quả phân loại của các mô hình kết hợp để xuất với các mô hình phân loại dựa trên từng đặc trưng riêng lẻ: hình ảnh, văn bản, gương mặt.

4. THỰC NGHIỆM

Đầu tiên, chương trình sẽ thu thập tự động các video từ TikTok bao gồm: thông tin tiêu đề, mô tả, video, âm thanh và lưu vào cơ sở dữ liệu. (1) Sử dụng Google API speech2text để chuyển giọng nói trong video thành văn bản, nối với tiêu đề, mô tả thành văn bản cuối; sử dụng giải pháp Word Embedding bằng mô hình Fasttext một công cụ biểu diễn không gian do Facebook cung cấp để trích xuất đặc trưng và đưa ra điểm số phân loại dựa trên đặc trưng văn bản. Trường hợp không có văn bản từ tiêu đề và giọng nói thì kết quả của phân loại sẽ là Null. (2) Đối với đặc trưng hình ảnh, đầu tiên video được trích xuất thành các khung chính. Xây dựng một cơ sở dữ liệu cơ bản về gương mặt của các chính trị gia, sau đó hiện thực lại mô hình học sâu để phát hiện gương mặt của các người có trong cơ sở dữ liệu. Sử dụng mô hình MTCCN để phát hiện gương mặt có trong KeyFrame, tiếp theo sử dụng VGG-Face để vector hóa gương mặt này. Sau đó tìm kiếm trong cơ sở dữ liệu. Kết quả của mô hình này sẽ là có hoặc không. Sử dụng mạng CNN Inception-V3 để trích xuất đặc trưng và đưa ra điểm số phân loại dựa trên đặc trưng hình ảnh. (3) Sử dụng chiến lược kết hợp chập để đưa ra phân loại ở cấp độ video. Sau khi có điểm số phân loại dựa trên ba đặc trưng, LightGBM được sử dụng để đưa ra kết quả phân loại ở cấp độ video.



Hình 7. Minh họa kiến trúc framework và luồng hoạt động



Hình 8. Minh họa chia tỷ lệ để huấn luyện và kiểm thử

Nghiên cứu thực hiện huấn luyện nhiều lần để tối ưu các tham số và lựa chọn chia tỷ lệ tập dữ liệu train - validate - test tương ứng thành 3 tập A, B và C (A 50% - tập huấn luyện cho hai mô hình dựa trên đặc trưng văn bản (model 1) và đặc trưng hình ảnh (model 3), B 35 % - sử dụng model 1 và model 3 đã được huấn luyện từ tập A để dự đoán ba đặc trưng trên tập B, điểm số thu được sẽ là: text score ($0 \rightarrow 1$), image score ($0 \rightarrow 1$), face (0 or 1). Sử dụng điểm số trên tập B để tiến hành huấn luyện mô hình kết hợp dựa trên ba đặc trưng văn bản, hình ảnh, gương mặt, C 15% - sử dụng cả bốn mô hình để dự đoán trên tập C) sau đó so sánh kết quả.

Mô hình được huấn luyện và thử nghiệm với tập dữ liệu thu thập được gồm: dữ liệu video là 5.252 video liên quan đến chính trị (57.654 khung hình chính) và 5.100 video không liên quan đến chính trị (47.242 khung hình chính); dữ liệu chuyển giọng nói thành văn bản từ video TikTok gồm 1.789 bài liên quan đến chính trị và 2.190 bài không liên quan đến chính trị.

Tiến hành thử nghiệm và đánh giá kết quả trên tập dữ liệu 10.000 video được gán nhãn tự động và thủ công cho kết quả như sau:

Kết quả kiểm thử – gán nhãn tự động

Model	Accuracy	F1-Score
Text Classification - Logistic Regression - Fasttext	0.73 0.77	0.71 0.75
Face detection - VGG-Face	0.6	0.34
Image Classification - Inception-V3 + ImageNet	0.73	0.72
Framework - Logistic Regression - Light GBM	0.82 0.85	0.81 0.83

Kết quả kiểm thử – gán nhãn thủ công

Model	Accuracy	F1-Score
Text Classification - Logistic Regression - Fasttext	0.82 0.88	0.80 0.86
Face detection - VGG-Face	0.68	0.39
Image Classification - Inception-V3 + ImageNet	0.88	0.85
Framework - Logistic Regression - Light GBM	0.92 0.93	0.91 0.92

Sau khi thử nghiệm các mô hình trên từng đặc trưng riêng lẻ và mô hình dựa trên phương pháp kết hợp chập trên tập dữ liệu được gán nhãn thủ công cho kết quả tốt hơn đạt độ chính xác 0,93. Bên cạnh đó LightGBM còn đưa ra độ quan trọng của các đặc trưng theo đó hình ảnh có ảnh hưởng lớn nhất đến kết quả phân loại của mô hình (face_prediction_score 95, image_prediction_score 526, text_prediction_score 79).

5. KẾT LUẬN

Qua kết quả nghiên cứu cho thấy framework đề xuất việc áp dụng phân loại video dựa trên ba đặc trưng là văn bản, gương mặt và hình ảnh cùng với chiến lược kết hợp chập để tổng hợp thông tin từ ba mô hình từ đó đưa ra kết quả phân loại ở cấp độ video cho kết quả tốt hơn so với mô hình dựa trên từng đặc trưng riêng lẻ cũng như phương pháp kết hợp thông thường. Cụ thể độ chính xác tốt nhất của framework là 0,93 và mô hình dựa trên từng đặc trưng văn bản, gương mặt, hình ảnh lần lượt là 0,88, 0,68 và 0,88. Mô hình LightGBM cho phép đầu vào là giá trị null do đó có thể giải quyết vấn đề thiếu dữ liệu ở một số đặc trưng và đưa ra được điểm quan trọng của từng đặc trưng trong mô hình phân loại video. Mô hình cũng phân loại tốt đối với các video có gương mặt của các chính trị gia nhưng nội dung không liên quan đến chính trị.

Nghiên cứu sẽ tiếp tục thu thập thêm dữ liệu đủ để triển khai các mô hình phân loại video dựa trên đặc trưng hình ảnh kết hợp yếu tố không gian – thời gian: CNN Fusion, CNN-LSTM, LR-CN; Tăng cường dữ liệu về gương mặt của các chính trị gia để áp dụng nhận diện gương mặt tốt hơn; xây dựng hệ thống tự động thu thập phân loại video chính trị dựa vào lượt thích, bình luận, chia sẻ của video để đưa ra cảnh báo và sau khi phân loại sẽ tóm tắt nội dung chính từ video, từ đó có thể nhóm các video vào một sự kiện tổng quát.

LỜI CẢM ƠN

Nhóm tác giả trân trọng cảm ơn Anh Nguyễn Bình Long học viên cao học Trường Đại học Bách khoa, Đại học Quốc gia Thành phố Hồ Chí Minh đã hỗ trợ thực hiện một phần hệ thống để đánh giá framework.

TÀI LIỆU THAM KHẢO

1. Quốc hội, “Luật an ninh mạng 2018”, Số 24/2018/QH14, Ngày 12 tháng 6 năm 2018.
2. A. Karpathy, G. Toderici, S. Shetty, T. Leung, R. Sukthankar, and L. Fei-Fei, “Large-scale video classification with convolutional neural networks,” in 2014 IEEE Conference on Computer Vision and Pattern Recognition, Ohio, USA, 2014.
3. A. Dhakal. "Political-advertisement video classification using deep learning methods," PhD Thesis. Iowa State University Capstones, Iowa, 2019.
4. P. Bojanowski, E. Grave, A. Joulin, and T. Mikolov, “Enriching word vectors with subword information,” arXiv [cs.CL], 2016.
5. H. El-Amir and M. Hamdy, “Convolutional Neural Network,” in Deep Learning Pipeline, Berkeley, CA: Apress, 2020, pp. 367–413.
6. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, “Rethinking the inception architecture for computer vision,” in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Nevada, USA, 2016.
7. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multitask cascaded convolutional networks,” IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, 2016.
8. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the gap to human-level performance in face verification,” in 2014 IEEE Conference on Computer Vision and Pattern Recognition, Ohio, USA, 2014
9. G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, T. Liu, “LightGBM: A Highly Efficient Gradient Boosting Decision Tree,” in 31st Conference on Neural Information Processing Systems, California, USA, 2017.
10. Z. A. A. Ibrahim, S. Haidar, and I. Sbeity, “Large-scale text-based video classification using contextual features,” Eur. J. Electr. Eng. Comput. Sci., vol. 3, no. 2, 2019.
11. H. Tian, Y. Tao, S. Pouyanfar, S.-C. Chen, and M.-L. Shyu, “Multimodal deep representation learning for video classification,” World Wide Web, vol. 22, no. 3, pp. 1325–1341, 2019.
12. T. Trzcinski, “Multimodal social media video classification with deep neural networks,” in Proceedings of SPIE, vol. 10808, 2018. doi: 10.1117/12.2501679.
13. Y. R. Pandeya and J. Lee, “Deep learning-based late fusion of multimodal information for emotion classification of music video,” Multimed. Tools Appl., vol. 80, no. 2, pp. 2887–2905, 2021.
14. Z. Weng, L. Meng, R. Wang, Z. Wu, and Y.-G. Jiang, “A multimodal framework for video ads understanding,” in Proceedings of the 29th ACM International Conference on Multimedia, Virtual Event, China, 2021.
15. “Unofficial TikTok API in Python.” [Online]. Available: <https://github.com/davidteather/TikTok-Api>, Mar. 10, 2022.

16. Scikit-Learn, “Scikit-Learn Python Library for Machine Learning.” [Online]. Available: <https://scikit-learn.org>, Mar. 12, 2022.
17. NumPy, “NumPy.” [Online]. Available: <https://numpy.org>, Mar. 6, 2022.
18. “Extractor” [Online] Available: <https://docs.scipy.org/doc/numpy/reference/generated/numpy.extract.html>, Mar. 6, 2022.
19. Google, “Google API.” [Online]. Available: <https://developers.google.com/apis-explorer>, Mar. 10, 2022.
20. “FFMPEG Project.” [Online]. Available: <https://ffmpeg.org>, Mar. 8, 2022.
21. “Machine Learning cơ bản” [Online]. Available: <https://machinelearningcoban.com>, Mar. 12, 2022.
22. A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017.
23. B. Banerjee, “Machine Learning Models for Political Video Advertisement Classification,” PhD Thesis. Iowa State University Capstones, Iowa, 2019.
24. T. Mikolov, L.V. Quoc, and I. Sutskever, “Exploiting Similarities among Languages for Machine Translation,” arXiv: 1309.4168, 2013.

ABSTRACT

CLASSIFICATION FRAMEWORK POLITICAL VIDEO ON SOCIAL NETWORK

Tran Thi Van Anh¹, Tran Khanh Dang^{1,*}, Hai Bin Nguyen¹

¹*Ho Chi Minh City University of Food Industry, Vietnam*

*Email: khanh@hufi.edu.vn

With the introduction of “Law on Cybersecurity 2018”, timely detection and automatic classification of political video clips on social networks is necessary. Images, texts and voices are the contents of video clips, which contain features that for video analysis and recognition. To improve the classification, the effective usage of all features is required. However, most of the current systems like CNN fusion, CNN-LSTM, LR-CN make use of only one feature. Herein, we proposed a framework that utilizing multiple models based on different features to effectively classify political videos. For voices and texts content, the framework uses FastText for training and classifying based on text features. For images, we use two models for training: firstly, using MTCNN to separate faces combined with VGG-Face feature vectorization and face recognition; secondly, using Inception-V3 model to extract features and output classification scores based on images. Finally, the LightGBM model is a slow fusion technique to synthesize training based on the classification scores from the three models above and give the video-level classification results. The proposed framework could analyze a video when some features are missing by using the remaining features. In this study, the framework was applied to a dataset with 10,000 political and non-political videos collected from TikTok. These results suggested the better performance of the framework compared to some models based on a single feature as well as traditional combination method and therefore, implicated its potential application in political video classification system.

Keywords: Video classification, Inception-V3, MTCNN, VGG-Face, LightGBM.

CƠ SỞ LÝ THUYẾT CÁC MÔ HÌNH ĐỘ CHẤP NHẬN VÀ SỬ DỤNG CÔNG NGHỆ

Đào Minh Châu^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: chaudm@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Nghiên cứu này tập trung vào cơ sở lý thuyết về độ chấp nhận và sử dụng công nghệ, một chủ đề ngày càng quan trọng khi công nghệ phát triển nhanh chóng. Việc nghiên cứu hành vi người dùng trước và sau khi công nghệ mới ra đời giúp tối ưu hóa tương tác giữa người dùng và công nghệ, tạo ra trải nghiệm người dùng tốt hơn và giúp cho công nghệ mới thành công hơn. Để đáp ứng yêu cầu của sự phát triển công nghệ, các phương pháp nghiên cứu về hành vi người dùng cần phải linh hoạt và đổi mới. Bài nghiên cứu này tập trung phân tích các tiến trình mô hình chấp nhận công nghệ từ TAM, TAM2 đến UTAUT và UTAUT2. So sánh các mô hình chấp nhận công nghệ, ứng dụng UTAUT vào trí tuệ nhân tạo và dữ liệu lớn.

Từ khóa: Chấp nhận, sử dụng công nghệ, TAM, UTAUT

1. MỞ ĐẦU

Trong thời đại hiện nay, Công nghệ được sử dụng rộng rãi trong hầu hết các lĩnh vực của đời sống xã hội. Tuy nhiên, với sự xuất hiện ngày càng nhanh chóng của các công nghệ mới, việc dự đoán hành vi của người dùng đối với công nghệ mới đó trở thành một yếu tố quan trọng đối với sự thành công của công nghệ đó. Vì vậy, nghiên cứu về hành vi người dùng trước và sau khi công nghệ mới ra đời là một mảng nghiên cứu đang được quan tâm rộng rãi trong cộng đồng khoa học. Điều này giúp cho việc đưa ra các giải pháp để tối ưu hóa sự tương tác giữa người dùng và công nghệ mới, từ đó tạo ra trải nghiệm người dùng tốt hơn và giúp cho công nghệ mới ra đời thành công hơn. Điều này càng cần thiết hơn khi mà sự phát triển của công nghệ ngày càng nhanh chóng và đòi hỏi sự linh hoạt, đổi mới liên tục trong các phương pháp nghiên cứu về hành vi người dùng.

Các yếu tố liên quan đến sự chấp nhận và sử dụng công nghệ:

Độ tin cậy: Người dùng đối với công nghệ sẽ có xu hướng sử dụng và chấp nhận công nghệ nếu nó được coi là đáng tin cậy.

Tính linh hoạt: Người dùng cũng đánh giá công nghệ dựa trên khả năng linh hoạt của nó, đặc biệt là khả năng thích nghi với nhiều tình huống và nhu cầu khác nhau.

Tiềm năng mở rộng: Người dùng sẽ cảm thấy thuận tiện và dễ dàng sử dụng công nghệ nếu nó có khả năng mở rộng và phát triển trong tương lai.

Tính thẩm mỹ: Tính thẩm mỹ của công nghệ cũng có thể ảnh hưởng đến sự chấp nhận và sử dụng của người dùng.

Tác động xã hội: Một số người dùng có thể sử dụng công nghệ vì nó được coi là phổ biến trong xã hội, hoặc vì nó được sử dụng bởi một số nhóm đối tượng mà họ tôn trọng và mong muốn theo đuổi.

Tính tiện ích: Người dùng đánh giá công nghệ dựa trên tính tiện ích của nó, bao gồm khả năng giải quyết các vấn đề và nhu cầu của họ.

Tính khả dụng: Người dùng đánh giá công nghệ dựa trên khả năng sử dụng và tiếp cận của họ với công nghệ đó. Nếu công nghệ quá khó sử dụng hoặc không khả dụng cho một số nhóm đối tượng, sẽ làm giảm sự chấp nhận và sử dụng của công nghệ đó.

Chi phí: Người dùng đánh giá công nghệ dựa trên chi phí sử dụng và sở hữu của nó. Nếu công nghệ quá đắt đỏ hoặc không đáp ứng được giá trị đối với người dùng, sẽ làm giảm sự chấp nhận và sử dụng của công nghệ đó.

Độ bảo mật: Người dùng cũng đánh giá công nghệ dựa trên độ an toàn và bảo mật của nó. Nếu công nghệ không đảm bảo được an toàn thông tin hay bảo mật dữ liệu, sẽ ảnh hưởng đến sự chấp nhận và sử dụng của người dùng.

Độc lập: Người dùng sẽ ưu tiên sử dụng các công nghệ có tính độc lập cao, nghĩa là không phụ thuộc quá nhiều vào các công nghệ khác và không bị gián đoạn khi có sự cố xảy ra.

Tương tác người dùng: Tính năng tương tác người dùng, ví dụ như tính năng thân thiện với người dùng và khả năng giao tiếp trực quan, cũng là yếu tố quan trọng ảnh hưởng đến sự chấp nhận và sử dụng của người dùng.

Từ đó, các nghiên cứu cơ sở lý thuyết về các mô hình chấp nhận công nghệ ra đời để đáp ứng xu hướng công nghệ phát triển lớn mạnh.

2. CÁC MÔ HÌNH CHẤP NHẬN CÔNG NGHỆ

2.1. Mô hình chấp nhận công nghệ TAM

Công nghệ TAM [1] (Technology Acceptance Model) được đưa ra vào năm 1989 bởi hai nhà nghiên cứu là Fred Davis và Richard Bagozzi. Mô hình này được phát triển dựa trên các nghiên cứu về hành vi sử dụng công nghệ và các mô hình trước đó:

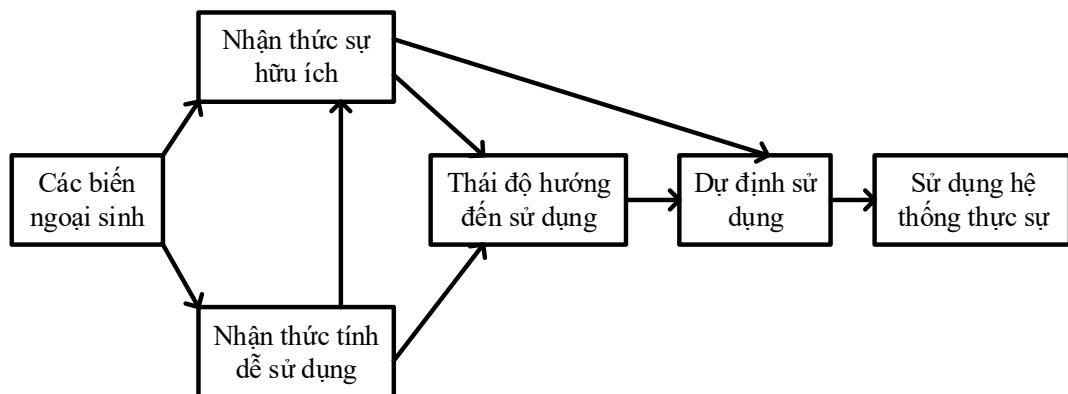
Theory of Reasoned Action (TRA)

Theory of Planned Behavior (TPB).

Các nghiên cứu bổ sung của (Bourdieu, 1991) và (Davis, 1993) đề xuất nên bỏ thành phần Dự Định Sử Dụng và nối trực tiếp Thành Phân Thái Độ sang Thành Phân Hành Vi. (Bourdieu, 1991) đã chứng tỏ Dự Định Sử Dụng nên được loại trừ bởi vì chúng ta quan tâm vào hành vi thực sự (sử dụng hệ thống).

Mục đích ban đầu của TAM là giải thích các yếu tố ảnh hưởng đến hành vi sử dụng công nghệ, và giúp các nhà quản lý hiểu rõ hơn về cách cải thiện sự chấp nhận và sử dụng của người dùng đối với các sản phẩm công nghệ. Tuy nhiên, sau này, TAM đã được sử dụng rộng rãi trong các lĩnh vực khác như kinh doanh, y tế, giáo dục, v.v.

Theo mô hình TAM, sự chấp nhận và sử dụng công nghệ phụ thuộc vào hai yếu tố chính: độ dễ sử dụng và độ hữu ích. Độ dễ sử dụng đề cập đến mức độ mà người dùng dễ sử dụng công nghệ, trong khi độ hữu ích liên quan đến mức độ mà công nghệ có thể giải quyết được các vấn đề của người dùng.



Hình 1. Mô hình TAM

Hình 1 trình bày mô hình TAM [4]. Mô hình trên chỉ ra rằng Độ dễ sử dụng và Độ hữu ích ảnh hưởng đến Sự chấp nhận và sử dụng của sản phẩm/ dịch vụ. Nếu sản phẩm có Độ dễ sử dụng cao và Độ hữu ích tốt, thì Sự chấp nhận và sử dụng của người dùng sẽ được cải thiện.

Để đạt được sự chấp nhận và sử dụng của người dùng, các nhà phát triển công nghệ cần tập trung vào cải thiện cả hai yếu tố trên. Đối với độ dễ sử dụng, họ cần đảm bảo rằng sản phẩm của họ có giao diện người dùng thân thiện và dễ sử dụng. Ngoài ra, họ cũng cần cung cấp đầy đủ hướng dẫn và hỗ trợ để người dùng có thể sử dụng sản phẩm một cách hiệu quả. Đối với độ hữu ích, các nhà phát triển cần hiểu rõ nhu cầu của người dùng và cung cấp giải pháp phù hợp. Họ cũng cần đảm bảo rằng sản phẩm của họ có thể giải quyết được các vấn đề thực tế của người dùng một cách hiệu quả.

Một trong những ứng dụng hiệu quả của mô hình TAM là để cải thiện sự chấp nhận và sử dụng của người dùng đối với các công nghệ mới, đặc biệt là trong lĩnh vực công nghệ thông tin và truyền thông. Ví dụ, để tăng tính tiện dụng và độ hữu ích của một ứng dụng di động mới, nhà phát triển có thể tập trung vào các tính năng mới và cải tiến mà người dùng cần nhất, đồng thời đảm bảo rằng giao diện người dùng dễ sử dụng và hướng dẫn sử dụng sản phẩm rõ ràng.

Năm 2000, **TAM 2** [1] (Technology Acceptance Model 2) được phát triển vào bởi Fred Davis, với mục đích cải thiện và bổ sung cho mô hình TAM ban đầu. TAM 2 được xây dựng dựa trên các nghiên cứu thực tế về sự chấp nhận công nghệ và sự ảnh hưởng của nhiều yếu tố khác nhau đến quá trình chấp nhận và sử dụng công nghệ. Một số yếu tố được bổ sung trong TAM 2 bao gồm:

Đặc tính cá nhân của người dùng: Bao gồm độ tuổi, giới tính, trình độ học vấn, kinh nghiệm sử dụng công nghệ và độ dễ bị ảnh hưởng bởi yếu tố xã hội, văn hóa.

Đặc tính của sản phẩm/ dịch vụ: Bao gồm tính năng, độ phức tạp, độ tin cậy, độ tương thích với các hệ thống khác, độ khả dụng, độ trải nghiệm người dùng.

Động lực sử dụng: Bao gồm sự cần thiết và sự mong đợi của người dùng đối với sản phẩm/ dịch vụ.

Yếu tố xã hội và văn hóa: Bao gồm sự ảnh hưởng của người khác, đánh giá của xã hội về sản phẩm/ dịch vụ, sự đổi mới và xu hướng của thị trường.

TAM 2 bổ sung và phát triển thêm các yếu tố quan trọng cho việc đánh giá sự chấp nhận và sử dụng công nghệ, giúp tăng cường tính ứng dụng và tính khả thi của mô hình. TAM 2 đã trở thành một trong những mô hình phổ biến và được sử dụng rộng rãi trong nghiên cứu về sự chấp nhận và sử dụng công nghệ.

Bảng 1. Mô hình TAM 2

Yếu tố	Mô tả
Thuận tiện	Độ dễ dàng khi sử dụng công nghệ
Đáng tin cậy	Mức độ tin cậy và độ ổn định công nghệ
Độ quan trọng	Mức độ quan trọng của công nghệ với người dùng
Hiệu quả	Khả năng của công nghệ để giải quyết vấn đề
Dễ dàng học	Độ dễ dàng khi học cách sử dụng công nghệ
Tính tiện ích	Mức độ hữu ích của công nghệ đối với người dùng

Bảng 1 là mô hình TAM 2 dạng bảng. Mỗi yếu tố (hàng) có thể được đánh giá trên một thang điểm từ 1 đến 5, với 1 là thấp nhất và 5 là cao nhất. Khi đánh giá TAM 2, các yếu tố này được xem xét để xác định mức độ chấp nhận và sử dụng công nghệ. Với sự phát triển vượt bậc của công nghệ, mô hình TAM 2 không còn đáp ứng được hoàn toàn các yêu cầu đánh giá độ chấp nhận và sử dụng công nghệ. Vì vậy, mô hình chấp nhận công nghệ mới ra đời sau đó là UTAUT và UTAUT2.

2.2. Lý thuyết chấp nhận và sử dụng công nghệ (UTAUT)

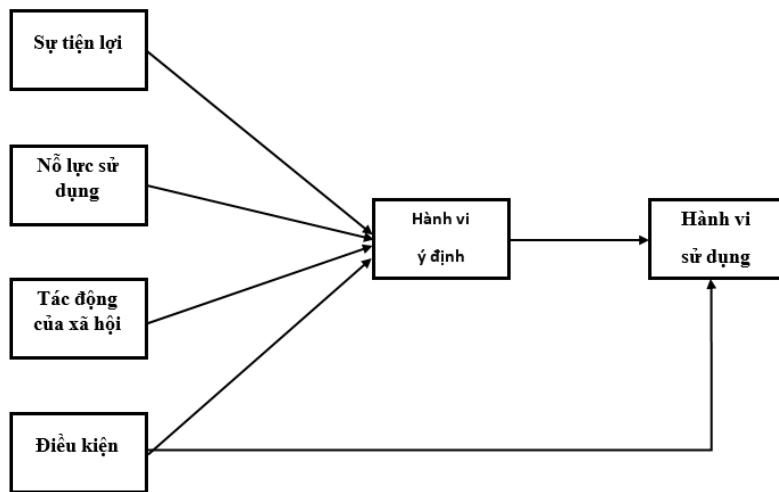
Năm 2003, UTAUT (Unified Theory of Acceptance and Use of Technology) được ra đời do bốn nhà nghiên cứu là Venkatesh, Morris, Davis và Davis tại trường Đại học Minnesota, Hoa Kỳ phát triển. Họ đã tổng hợp và đánh giá các lý thuyết trước đó về chấp nhận và sử dụng công nghệ, từ đó đề xuất một lý thuyết đơn giản và toàn diện hơn để giải thích và dự đoán hành vi của người dùng đối với công nghệ. UTAUT được xây dựng dựa trên một số lý thuyết trước đó, bao gồm:

Technology Acceptance Model (TAM)

Theory of Reasoned Action (TRA)

Theory of Planned Behavior (TPB)

Motivational Model (MM).



Hình 2. Mô hình UTAUT

Mô hình UTAUT [2], [3] được trình bày trong hình 2. UTAUT đã trở thành một trong những lý thuyết quan trọng nhất trong lĩnh vực nghiên cứu chấp nhận và sử dụng công nghệ, và đã được áp dụng để nghiên cứu và dự đoán hành vi sử dụng công nghệ trong nhiều lĩnh vực khác nhau, từ giáo dục, y tế, tài chính đến kinh doanh và quản lý.

UTAUT nghiên cứu những yếu tố chính bao gồm: mong đợi hiệu quả, mong đợi độ dễ dàng, ảnh hưởng xã hội và điều kiện thuận lợi. Những yếu tố này đóng vai trò quan trọng trong quyết định của người dùng về việc chấp nhận và sử dụng công nghệ mới.

UTAUT cung cấp một khung thể hiện để đánh giá sự chấp nhận và sử dụng của người dùng đối với công nghệ mới và giúp các nhà nghiên cứu và doanh nghiệp hiểu rõ hơn về tâm lý và hành vi của người dùng khi sử dụng công nghệ. UTAUT bao gồm bốn yếu tố chính ảnh hưởng đến hành vi sử dụng công nghệ, bao gồm:

Nỗ lực sử dụng (Effort expectancy): Sự dễ dàng và tiện lợi trong việc sử dụng công nghệ.

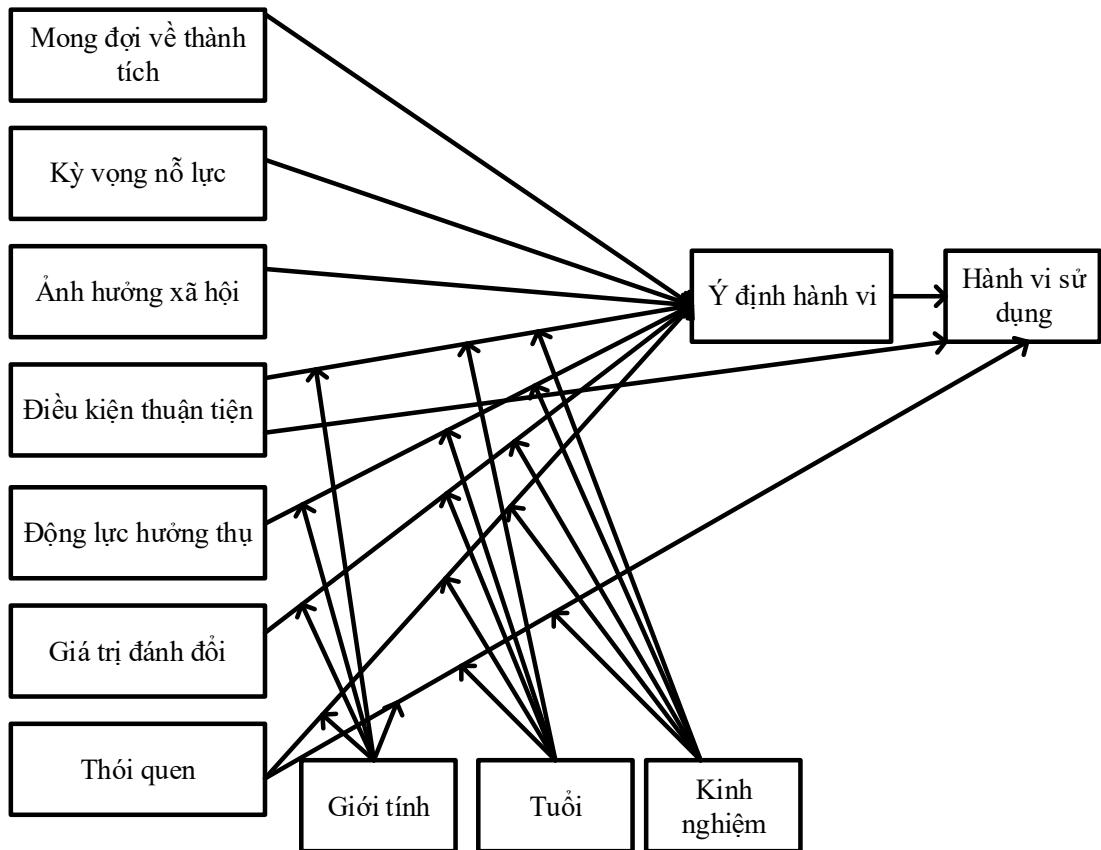
Tác động của xã hội (Social influence): Sự ảnh hưởng của những người khác đến hành vi sử dụng công nghệ.

Điều kiện (Facilitating conditions): Mức độ hỗ trợ và nguồn lực có sẵn để hỗ trợ sử dụng công nghệ.

Sự tiện lợi (Performance expectancy) là yếu tố quan trọng nhất ảnh hưởng đến hành vi sử dụng công nghệ.

Nỗ lực sử dụng (Effort expectancy) cũng đóng một vai trò quan trọng đối với hành vi sử dụng công nghệ. Tác động của xã hội (Social influence) và Điều kiện (Facilitating conditions) cũng ảnh hưởng đến hành vi sử dụng công nghệ, nhưng đóng vai trò nhỏ hơn so với yếu tố trên. Hành vi sử dụng công nghệ được đo bằng độc lập và được định nghĩa là tần suất sử dụng công nghệ trong một khoảng thời gian nhất

Năm 2009 **UTAUT2** là phiên bản nâng cấp của mô hình UTAUT ban đầu, được phát triển bởi Venkatesh và đồng nghiệp nhằm cải tiến và mở rộng UTAUT để phù hợp với các ứng dụng mới và đáp ứng các thách thức mới của ngành công nghệ thông tin.



Hình 3. Mô hình UTAUT 2

Các cải tiến của UTAUT2 bao gồm:

- Bổ sung yếu tố đáng tin cậy: Điều này cho phép đo lường mức độ tin tưởng của người sử dụng đối với công nghệ và các nhà cung cấp dịch vụ.
- Sửa đổi yếu tố tác động của xã hội: Bổ sung độ tin cậy của người khác và độ tương đồng với những người khác để đánh giá tác động của xã hội đến hành vi sử dụng công nghệ.
- Bổ sung yếu tố tác động của bối cảnh: Điều này cho phép đo lường mức độ ảnh hưởng của bối cảnh như đặc tính cá nhân, môi trường làm việc, văn hóa tổ chức, độ tin cậy của công nghệ và độ tương thích của công nghệ đến hành vi sử dụng công nghệ.
- Tính toán mức độ ảnh hưởng: UTAUT2 cũng bổ sung tính toán mức độ ảnh hưởng của các yếu tố khác nhau đến hành vi sử dụng công nghệ.

Tóm lại, UTAUT2 là một phiên bản cải tiến của UTAUT, bao gồm bốn yếu tố chính như UTAUT, nhưng bổ sung thêm yếu tố đáng tin cậy, sửa đổi yếu tố tác động của xã hội và bổ sung yếu tố tác động của bối cảnh. UTAUT2 cho phép đo lường các yếu tố ảnh hưởng đến hành vi sử dụng công nghệ một cách chính xác hơn và phù hợp hơn với các ứng dụng mới và thách thức mới của ngành công nghệ thông tin.

3. THẢO LUẬN

Các mô hình chấp nhận công nghệ TAM, TAM2, UTAUT và UTAUT2 đều có ưu nhược điểm riêng. TAM và TAM2 tập trung vào những yếu tố cá nhân của người dùng và ít quan tâm đến yếu tố xã hội. UTAUT thêm vào yếu tố xã hội, tuy nhiên vẫn chưa đánh giá được những yếu tố kỹ thuật và văn hóa. UTAUT2 đã bổ sung những yếu tố đó, tạo ra một mô hình đầy đủ hơn. Tuy nhiên, việc áp dụng UTAUT2 còn khó khăn do yêu cầu phân tích dữ liệu phức tạp. Sau đây là bảng 2 dùng để so sánh 4 mô hình chấp nhận công nghệ đã phân tích ở trên.

Bảng 2. So sánh 4 mô hình chấp nhận công nghệ

Mô hình	Phạm vi ứng dụng	Số lượng yếu tố	Các yếu tố đo đạc	Động cơ của người dùng
TAM	Môi trường công việc	2 (độ dễ dàng sử dụng và độ hữu ích)	Độ dễ dàng sử dụng và độ hữu ích tương đối của công nghệ so với các công nghệ khác	Hợp lý
TAM 2	Môi trường công việc	2 (độ dễ dàng sử dụng và độ hữu ích)	Độ dễ dàng sử dụng và độ hữu ích tương đối của công nghệ so với các công nghệ khác	Hợp lý
UTAUT	Cả môi trường công việc và môi trường cá nhân	4 (độ dễ dàng sử dụng, độ hữu ích, độ niềm tin và độ hứng thú)	Mức độ khác nhau của độ dễ dàng sử dụng, độ hữu ích, độ niềm tin và độ hứng thú	Kết quả của sự tương tác giữa các yếu tố
UTAUT 2	Cả môi trường công việc và môi trường cá nhân	5 (độ dễ dàng sử dụng, độ hữu ích, độ niềm tin, độ hứng thú và trải nghiệm người dùng)	Mức độ khác nhau của độ dễ dàng sử dụng, độ hữu ích, độ niềm tin, độ hứng thú và trải nghiệm người dùng	Kết quả của sự tương tác giữa các yếu tố

Hiện tại chưa có phiên bản UTAUT3 chính thức được phát hành. Tuy nhiên, một số nghiên cứu đang được tiến hành để cải tiến và mở rộng UTAUT2 để đáp ứng các thách thức mới trong lĩnh vực công nghệ thông tin và truyền thông.

Các hướng cải tiến đang được nghiên cứu cho UTAUT tiếp theo có thể bao gồm:

Bổ sung yếu tố kinh nghiệm sử dụng (Experience): Điều này cho phép đánh giá mức độ kinh nghiệm sử dụng công nghệ của người dùng để đưa ra các giải pháp phù hợp cho từng đối tượng khách hàng.

Tính đa dạng của bối cảnh (Contextual diversity): UTAUTn có thể bổ sung yếu tố tính đa dạng của bối cảnh, bao gồm đa dạng về địa lý, văn hóa và ngôn ngữ, để đánh giá tác động của các yếu tố này đến hành vi sử dụng công nghệ.

Cải tiến về định lượng (Quantitative improvements): UTAUTn có thể cải tiến việc định lượng các yếu tố ảnh hưởng đến hành vi sử dụng công nghệ để đưa ra kết quả đầy đủ và chính xác hơn.

UTAUTn là một phiên bản cải tiến tiếp theo của UTAUT2 với các hướng phát triển mới để đáp ứng các thách thức và cải thiện độ chính xác và đầy đủ của kết quả. Tuy nhiên, hiện tại vẫn chưa có phiên bản UTAUTn chính thức được phát hành và các nghiên cứu đang tiếp tục để phát triển phiên bản mới này.

Áp dụng UTAUT vào trí tuệ nhân tạo và dữ liệu lớn có thể giúp giải thích sự chấp nhận và sử dụng các ứng dụng AI và dữ liệu lớn. Ví dụ, động lực có thể áp dụng để giải thích tại sao một công ty muốn triển khai một hệ thống AI để phân tích dữ liệu và tìm kiếm thông tin quan trọng để hỗ trợ quyết định kinh doanh. UTAUT có thể giúp đánh giá sự chấp nhận và sử dụng của người dùng đối với các ứng dụng AI, bao gồm các hệ thống tư vấn, hệ thống tự động hóa và hệ thống trí tuệ nhân tạo trong các lĩnh vực khác nhau. Độ dễ dàng sử dụng có thể được sử dụng để giải thích tại sao một nhà quản lý muốn sử dụng các công cụ phân tích dữ liệu AI để phát hiện những xu hướng mới và đưa ra các dự đoán cho tương lai. Điều kiện hỗ trợ có thể giải thích tại sao một công ty muốn đầu tư vào AI và dữ liệu lớn bằng cách đảm bảo rằng họ có đủ nguồn lực để triển khai và duy trì các hệ thống này.

Đối với dữ liệu lớn, UTAUT có thể giúp đánh giá sự chấp nhận và sử dụng của người dùng đối với các hệ thống lưu trữ và xử lý dữ liệu lớn, bao gồm cả các công cụ phân tích dữ liệu và các hệ thống học máy. Những yếu tố như độ chính xác, tính dễ sử dụng và tính tiện ích của các hệ thống dữ liệu lớn đều được xem xét trong mô hình UTAUT.

Bên cạnh đó, các yếu tố của UTAUT có thể được mở rộng để giải thích sự chấp nhận và sử dụng các ứng dụng AI và dữ liệu lớn, ví dụ như:

Tác động của các yếu tố về độ tin cậy và an ninh của dữ liệu trên sự chấp nhận của người sử dụng.

Tác động của độ chính xác và hiệu quả của các mô hình AI trên sự chấp nhận và sử dụng của người sử dụng.

Tác động của sự phức tạp và tính khả thi của các hệ thống AI và dữ liệu lớn trên sự chấp nhận của người sử dụng.

4. KẾT LUẬN

Sau khi phân tích và tìm hiểu từng mô hình chấp nhận công nghệ TAM, TAM 2, UTAUT, UTAUT 2; tôi nhận thấy rằng UTAUT và UTAUT2 là những mô hình đáng tin cậy và chính xác nhất để đánh giá độ chấp nhận và sử dụng công nghệ. Đặc biệt, UTAUT2 là một mô hình rất hoàn chỉnh và được áp dụng rộng rãi trong các nghiên cứu về công nghệ, đặc biệt là trên các lĩnh vực trí tuệ nhân tạo và dữ liệu lớn.

Việc định hướng mô hình UTAUT tiếp theo cho trí tuệ nhân tạo và dữ liệu lớn là hợp lý, bởi đây là những lĩnh vực đang phát triển rất nhanh và đòi hỏi sự ứng dụng của công nghệ cao để có thể đưa ra các giải pháp đúng đắn. Sự phát triển của trí tuệ nhân tạo và dữ liệu lớn sẽ đem lại nhiều tiềm năng cho ứng dụng công nghệ trong tương lai, và UTAUT là một mô

hình lý thuyết đáng tin cậy để đánh giá độ chấp nhận và sử dụng công nghệ trong các ứng dụng trí tuệ nhân tạo và dữ liệu lớn.

TÀI LIỆU THAM KHẢO

1. Gianina Lala. The Emergence and Development of the Technology Acceptance Model (TAM). Risoprint, (2014).
2. Samuel Attuquayefio, Hilla Add. Review Of Studies With Utaut As Conceptual Framework. European Scientific Journal, (2014).
3. Yogesh K. Dwivedi, Nripendra P. Rana, Anand Jeyaraj, Marc Clement & Michael D. Williams . Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. Springer, (2017).
4. vi.wikipedia.org/wiki/

ABSTRACT

THEORETICAL FOUNDATIONS OF TECHNOLOGY ACCEPTANCE AND USAGE MODELS

Dao Minh Chau^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: chaudm@hufi.edu.vn

This research focuses on the theoretical foundation of technology acceptance and usage, a topic that is becoming increasingly important as technology develops rapidly. Studying user behavior before and after the introduction of new technology helps to optimize the interaction between users and technology, create a better user experience, and contribute to the success of new technology. To meet the requirements of technological development, research methods on user behavior need to be flexible and innovative. This study focuses on analyzing the process of technology acceptance models, from TAM, TAM2 to UTAUT and UTAUT2. It compares technology acceptance models and applies UTAUT to artificial intelligence and big data.

Keywords: acceptance, technology usage, TAM, UTAUT

NÂNG CAO HIỆU QUẢ TÌM KIẾM ẢNH DỰA TRÊN CẤU TRÚC KD-TREE VÀ K-MEANS

Nguyễn Thị Định^{1*}, Trần Thị Bích Vân¹, Nguyễn Phương Hạc¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: dinhnt@husi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Nâng cao độ chính xác tìm kiếm ảnh là vấn đề cần được quan tâm và thực hiện trong bài toán tìm kiếm ảnh. Trong bài báo này, chúng tôi tiếp cận một phương pháp tìm kiếm ảnh dựa trên cấu trúc KD-Tree, sau đó tiến hành gom cụm theo thuật toán K-Means dựa trên số cụm đã hình thành từ nút lá KD-Tree nhằm nâng độ chính xác tìm kiếm tập ảnh tương tự với ảnh đầu vào. Để thực hiện bài toán này, đầu tiên tập dữ liệu hình ảnh được trích xuất vec-to đặc trưng 225 chiều, sau đó xây dựng cấu trúc KD-Tree để hình thành các cụm tương đồng tại nút lá. Sau khi có số cụm thì tiến hành áp dụng thuật toán K-Means để phân bổ lại dữ liệu một lần nữa để điều chỉnh các cụm có số phần tử tương tự nhau là nhiều nhất và tìm kiếm tập ảnh tương tự với ảnh đầu vào. Trên cơ sở đó, một mô hình tìm kiếm ảnh dựa trên cấu trúc KD-Tree kết hợp thuật toán gom cụm K-Means được đề xuất để tìm kiếm ảnh tương tự. Để minh chứng cho tính đúng đắn của cơ sở lý thuyết đề xuất, thực nghiệm được xây dựng trên bộ ảnh COREL và Caltech-256 với hiệu suất tìm kiếm ảnh lần lượt là **0.8250, 0.7656**. Kết quả thực nghiệm được so sánh với các công trình khác cùng trên bộ dữ liệu; điều này minh chứng cho tính khả thi và hiệu quả của phương pháp đề xuất.

Từ khóa: KD-Tree, K-Means, tìm kiếm ảnh, ảnh tương tự

1. TỔNG QUAN

Nâng cao độ chính xác truy vấn ảnh là vấn đề cần quan tâm trong lĩnh vực tra cứu ảnh và đã được công bố bởi nhiều công trình trong những thập niên qua [1] [2] [3]. Hiện nay, có nhiều phương pháp tiếp cận nhằm nâng cao hiệu suất cho bài toán tìm kiếm ảnh như kết hợp các kỹ thuật học máy, cải tiến cấu trúc lưu trữ hoặc kết hợp kỹ thuật học máy và cấu trúc lưu trữ, v.v. Trên cơ sở phân tích những hạn chế còn tồn tại từ các công trình; phạm vi bài báo là thực hiện một số đề xuất dựa trên sự kết hợp cấu trúc KD-Tree và thuật toán gom cụm K-Means nhằm nâng cao độ chính xác tìm kiếm ảnh bằng cách xây dựng cấu trúc KD-Tree để thực hiện gom cụm tại nút lá, sau đó tiếp tục tiến hành gom cụm bằng K-Means một lần nữa để đưa các phần tử tương tự nhau về một cụm là nhiều nhất.

Sự phát triển của các loại thiết bị điện tử làm cho dữ liệu đa phương tiện gia tăng nhanh theo thời gian. Vì vậy, bài toán tìm kiếm ảnh được các nhóm nghiên cứu quan tâm và thực hiện nhiều cải tiến. Hiệu suất tìm kiếm của bài toán truy vấn ảnh chịu ảnh hưởng lớn đến quá trình lưu trữ, tổ chức dữ liệu, đồng thời cấu trúc dữ liệu lưu trữ hình ảnh là yếu tố ảnh hưởng đến thời gian tìm kiếm. Trong bài báo này, một cấu trúc dữ liệu đa chiều KD-Tree được sử

dụng cho quá trình gom cụm, lưu trữ để tìm kiếm ảnh tương tự với ảnh đầu vào được đánh giá lá khai thi và hiệu quả. Sau khi xây dựng KD-Tree đã xác định được số cụm và tâm cụm, thuật toán K-Means được áp dụng gom cụm một lần nữa nhằm phân bổ lại các đối tượng sai cụm sẽ hình thành nên các cụm tốt hơn, từ đó áp dụng cho bài toán tìm kiếm ảnh hiệu quả về độ chính xác.

Đóng góp của bài báo gồm: (1) Trích xuất véc-tơ đặc trưng và gom cụm dữ liệu hình ảnh bằng cấu trúc KD-Tree; (2) Kết hợp thuật toán K-Means sau khi có số cụm và tâm cụm tại nút lá trên KD-Tree; (3) Đề xuất mô hình tìm kiếm ảnh tương tự dựa trên cấu trúc KD-Tree và thuật toán K-Means; (4) Xây dựng thực nghiệm tìm kiếm ảnh tương tự trên bộ ảnh Flower-17 [4] và Caltech-256 [5] dựa trên véc-tơ đặc trưng và so sánh với một số công trình cùng bộ dữ liệu.

Phần còn lại của bài báo bao gồm: **Phần 2** khảo các công trình nghiên cứu liên quan; **Phần 3** trình bày phương pháp gom cụm bằng KD-Tree và K-Means; **Phần 4** trình bày phương pháp gom cụm dựa trên KD-Tree và K-Means. **Phần 5** xây dựng thực nghiệm và đánh giá kết quả; kết luận và hướng phát triển tiếp theo được trình bày trong **Phần 6**.

2. CÁC CÔNG TRÌNH NGHIÊN CỨU LIÊN QUAN

Trong bài báo này, quá trình tìm kiếm ảnh được thực hiện qua các giai đoạn gồm: trích xuất véc-tơ đặc trưng của hình ảnh; xây dựng cấu trúc lưu trữ KD-Tree và gom cụm K-Means; tìm kiếm ảnh tương tự dựa trên các kỹ thuật gom cụm. Vì vậy, một số công trình được khảo sát tìm kiếm ảnh bằng cấu trúc KD-Tree, K-Means để phân tích ưu nhược điểm của từng công trình để từ đó đưa ra phương pháp kết hợp nhằm thực hiện bài toán tìm kiếm ảnh và nâng cao độ chính xác; cụ thể gồm:

Y Narasimhulu [6] [7] đã đề xuất một mô hình phân lớp hình ảnh dựa vào KD-Tree. Trong mô hình này, từ một tập dữ liệu lớn chưa phân loại được thực hiện xây dựng tập dữ liệu Coresets trên cơ sở thuật toán đề xuất của tác giả. Sau đó dựa vào thuật toán xây dựng KD-Tree để hình thành cây KD-Tree chứa tập dữ liệu này. Từ một ảnh đầu vào thực hiện tìm kiếm trên cấu trúc KD-Tree bằng thuật toán tìm kiếm theo số láng giềng nhiều nhất làm căn cứ xác định phân lớp cho hình ảnh. Cuối cùng, tác giả dùng thang đo khoảng cách để thực hiện phân lớp các tập dữ liệu hình ảnh huấn luyện. Trong công trình này, cây KD-Tree được sử dụng trực tiếp để lưu trữ dữ liệu và phân lớp cho một ảnh đầu vào với kết quả tốt mà không mất nhiều chi phí trung gian. Đây là một mô hình được đề xuất cho bài toán phân lớp ảnh dựa vào cấu trúc KD-Tree được đánh giá là khá tốt.

Erwin và cộng sự [8] đề xuất hệ thống nhận dạng trái cây bằng cách kết hợp các thuật toán K-Means, k-NN để thực hiện phân lớp và gom cụm đặc trưng hình ảnh trước khi nhận diện đối tượng. Kết quả thực nghiệm phân lớp hình ảnh đạt được độ chính xác 92,5% cho ảnh đơn đối tượng và 90% cho ảnh đa đối tượng. Tuy nhiên, hệ thống chỉ nhận diện trên các bộ ảnh về trái cây; thuật toán K-Means được áp dụng theo phương pháp cập nhật tâm cụm khi dữ liệu thay đổi, chưa xử lý trường hợp số lượng láng giềng có số phân lớp bằng nhau trong thuật toán k-NN.

Shuang Jia và cộng sự [9] sử dụng thuật toán gom cụm K-Means để thực hiện tìm kiếm ảnh. Mỗi hình ảnh đầu vào được trích xuất đặc trưng và tính độ tương tự dựa trên đặc trưng

túi từ để tìm tập ảnh tương tự. Trong phương pháp này, các túi từ là độc lập và chưa phân lớp được theo nội dung của mỗi ảnh đầu vào.

Từ những công trình nghiên cứu trên cho thấy tính khả thi cho bài toán tìm kiếm ảnh bằng cấu trúc KD-Tree và thuật toán K-Means đã có những kết quả quan trọng. Tuy nhiên, sự kết hợp giữa cấu trúc KD-Tree và thuật toán K-Means để nâng cao độ chính xác cho bài toán tìm kiếm ảnh còn hạn chế về số lượng. Vì vậy, trong bài báo này, một mô hình tìm kiếm ảnh được đề xuất dựa trên cấu trúc KD-Tree, sau đó gom cụm bằng K-Means áp dụng cho bài toán tìm kiếm ảnh được thực hiện nhằm kết hợp những ưu điểm hiện có của kỹ thuật K-Means và cấu trúc KD-Tree.

3. GOM CỤM DỰA TRÊN CẤU TRÚC KD-TREE VÀ THUẬT TOÁN K-MEANS

Cấu trúc KD-Tree gom cụm được minh họa như hình 2, trong đó mỗi nút lá là một cụm chứa những phần tử có độ tương đồng nhau nhiều nhất. Để xây dựng cấu trúc KD-Tree theo phương pháp gom cụm, mỗi thành phần trên KD-Tree được mô tả như sau:

- a) Nút gốc (Root) lưu trữ một vector trọng số (w_0);
- b) Nút trong ($Node_i$) lưu trữ một vector trọng số (w_i);
- c) Nút lá (Leaf) lưu trữ tập vector đặc trưng hình ảnh $\{f_1, f_2, \dots, f_k\}$.

Trong cấu trúc này, nút gốc và nút trong đóng vai trò xác định đường đi cho các phần tử khi chèn vào KD-Tree để hình thành các cụm tại nút lá. Để xác định số cụm trên KD-Tree, cần căn cứ vào số phân lớp các tập ảnh thực nghiệm để xác định chiều cao (h) và số nhánh tối đa (b) tại mỗi nút trên cây. Vì vậy, thuật toán gom cụm bằng KD-Tree được mô tả như sau:

Thuật toán 1. Gom cụm dữ liệu theo KD-Tree

Thuật toán 1. Gom cụm dữ liệu bằng cấu trúc KD-Tree

1. **Input:** Tập $F = \{f_i : f_i = (x_{i0}, x_{i1}, \dots, x_{in}) ; i = 1, \dots, k\}$; chiều cao h ; số nhánh tối đa b .
Bộ trọng số khởi tạo $W_{kt} = \{W_i : W_i = (x_{i0}, x_{i1}, \dots, x_{in}) ; i = 0 \dots h-1\}$;
2. **Output:** Tập nút lá $\{Leaf\}$;
3. **Function Cl_KDTree** (F, W_{kt}, h, b);
4. **Begin**
5. Khởi tạo khung cây KD-Tree theo chiều cao h , số nhánh b ;
6. Khởi tạo $\{Leaf\}$ là rỗng;
7. Khởi tạo cận trái, cận phải tất cả $Node_i$ là $Node_{i.left} = Node_{i.right} = 0.5$;
8. **For** (duyệt danh sách các véc – tơ f_i thuộc tập F) **do**
9. **For** (int $j = 0$; $j \leq h-1$; $j++$) **do**
10. **If** ($Sigmoid(f_i, W_j) < Node_{j.left}$) **then**
11. f_i đi theo nhánh trái và cập nhật ngưỡng trái của $Node_j$;
12. **EndIf;**
13. **If** ($Sigmoid(f_i, W_j) > Node_{j.right}$) **then**
14. f_i đi theo nhánh phải và cập nhật ngưỡng phải của $Node_j$;
15. **EndIf;**
16. **IF** ($Node_{j.left} \leq Sigmoid(f_i, W_j)$ and $Sigmoid(f_i, W_j) \leq Node_{j.right}$) **then**
17. Chọn nhánh gần nhất để đi đến tầng tiếp theo;

```

18.           EndIf;
19.           EndFor;
20.           If ( $Node_{i.level} = h - 1$ ) then
21.               IF ( $f_i.label = Leaf_k.label$ ) then ghi  $f_i$  vào  $Leaf_k$ ;
22.               Else
23.                   Tìm nhánh gần nhất  $Leaf_{k+1}$  và ghi  $f_i$  vào  $Leaf_{k+1}$ ;
24.               EndIf;
25.           EndIf;
26.       EndFor;
27.       Return Tập nút lá { $Leaf$ } ;
28.   End.

```

Sau khi xác định được số cụm dựa trên KD-Tree thì vẫn có một số phần tử nằm sai cụm. Vì vậy, dựa trên cỗ cụm và tâm cụm được tính bởi giá trị trung bình của cụm hiện hành và thực hiện gom cụm theo thuật toán K-Means lại một lần nữa nhằm giúp cho các phần tử sai cụm được sắp xếp lại theo đúng cụm tương đồng tốt nhất. Vì vậy, thuật toán gom cụm K-Means trong bài báo này được trình bày như sau:

Thuật toán 2. Gom cụm dữ liệu theo K-Means

1. **Input:** Tập véc-tơ cần gom cụm $F = \{f_i : f_i = (x_{i0}, x_{i1}, \dots, x_{in}); i = 1, \dots, k\}$;
 2. **Output:** Tập véc-tơ trên mỗi cụm;
 3. **Function K-Means** (F, k);
 4. **Begin**
 5. Khởi tạo số cụm k ;
 6. Tính giá trị tâm của k cụm là giá trị trung bình mỗi nút lá;
 7. Mỗi véc-tơ f_i tính khoảng cách đến k tâm;
 8. Nếu f_i gần tâm C_k thì f_i thuộc cụm C_k ;
 9. **Return** Tập véc-tơ trên k cụm;
 10. **End.**
-

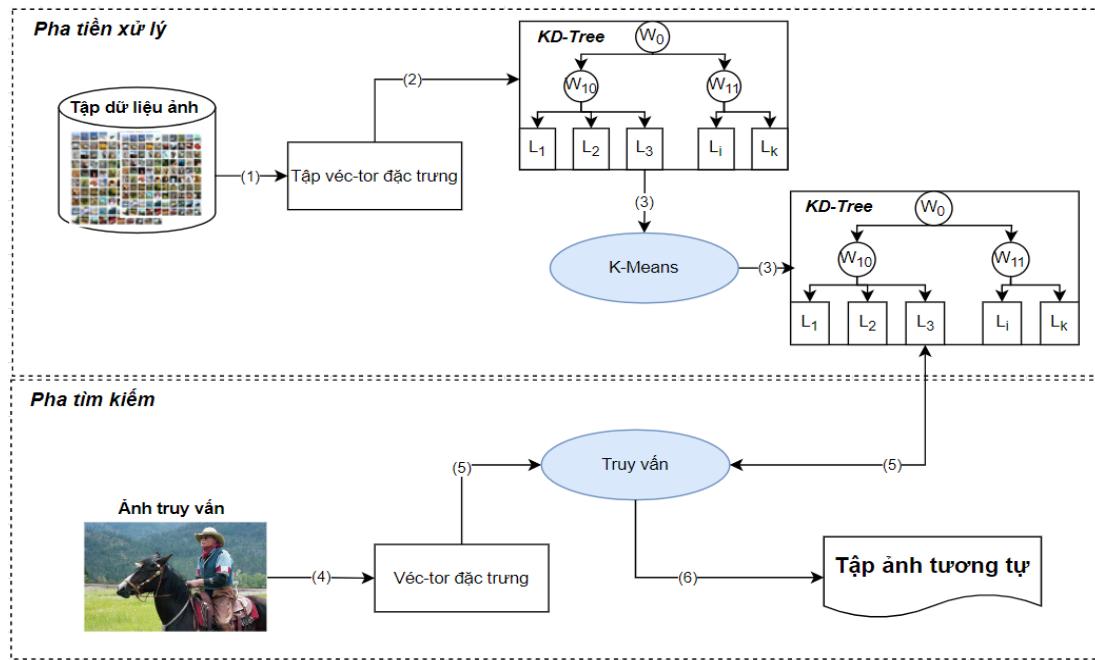
4. MÔ HÌNH TÌM KIẾM ẢNH DỰA TRÊN KD-TREE VÀ K-MEANS

4.1. Đề xuất mô hình tìm kiếm ảnh dựa trên KD-Tree và K-Means

Trên cơ sở kết hợp cấu trúc KD-Tree và thuật toán K-Means để áp dụng cho bài toán tìm kiếm ảnh. Một mô hình tìm kiếm ảnh được đề xuất như **hình 1**.

Mô hình tìm kiếm ảnh dựa trên cấu trúc KD-Tree và thuật toán K-Means gồm hai pha: Pha tiền xử lý và pha truy vấn với các bước:

- (1) Trích xuất véc-tơ đặc trưng cho tập ảnh thực nghiệm;
- (2) Xây dựng cấu trúc KD-Tree lưu trữ và gom cụm dữ liệu hình ảnh tại nút lá;
- (3) Thực hiện gom cụm K-Means theo dữ liệu đã gom cụm tại nút lá KD-Tree;
- (4) Ảnh đầu vào được trích xuất véc-tơ đặc trưng;
- (5) Tìm kiếm trên tập dữ liệu đã gom cụm để trích xuất tập ảnh tương tự với ảnh đầu vào. [10]



Hình 1. Mô hình tìm kiếm ảnh dựa trên cấu trúc KD-Tree và K-Means.

4.2. Thuật toán tìm kiếm ảnh tương tự trên KD-Tree và K-Means

Sau khi xây dựng cấu trúc KD-Tree và gom cụm theo K-Means, các nút lá là các cụm tương đồng lưu trữ tập dữ liệu hình ảnh. Vì vậy, quá trình tìm kiếm tập ảnh tương tự với một ảnh đầu vào I cần phải duyệt từ nút gốc đến nút lá. Nếu vector đặc trưng của ảnh I thuộc về nút lá $leaf_k$ thì trích xuất tập ảnh tương tự là tập ảnh tại nút lá $leaf_k$.

Thuật toán 3: Tìm kiếm ảnh tương tự dựa trên KD-Tree và k-Means

1. **Input:** Véc-tor đặc trưng f_i của ảnh I , KD-Tree
 2. **Output:** Tập ảnh tương tự SI ;
 3. **Function RKDT($f_i, KD-Tree$);**
 4. **Begin**
 5. $SI = \emptyset$;
 6. **Foreach** ($f_i \in F$) **do**;
 7. Duyệt từ gốc đến lá trên KD-Tree;
 8. **If** ($f_i \in leaf_k$) **then**;
 9. $SI = leaf_k \cdot \{f_k\}$;
 10. **EndIf**;
 11. **EndForeach**;
 10. **Return** SI ;
 11. **End.**
-

5. THỰC NGHIỆM VÀ ĐÁNH GIÁ

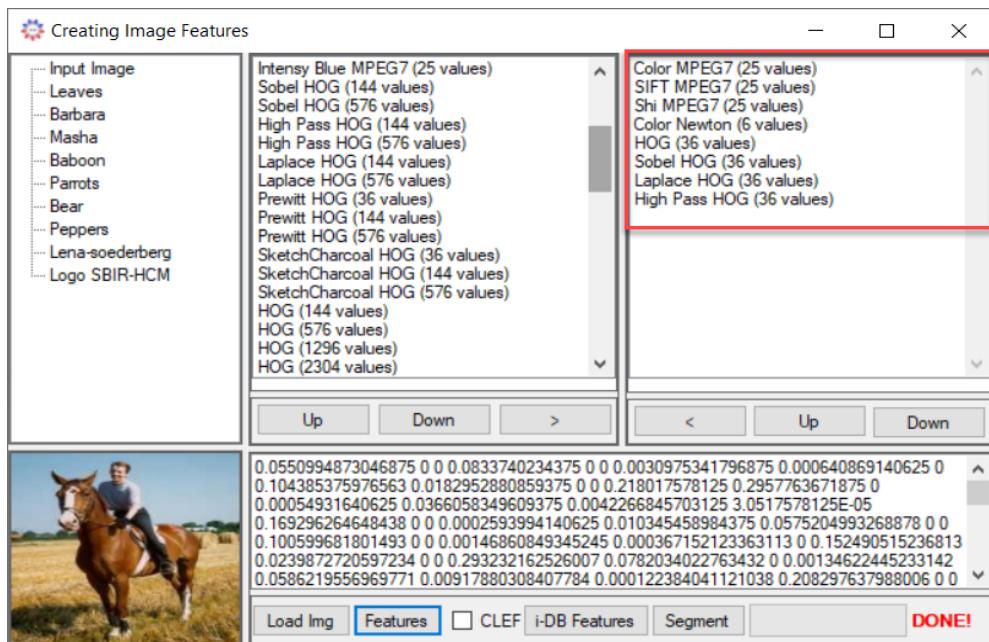
5.1. Dữ liệu và môi trường thực nghiệm

Môi trường thực nghiệm tìm kiếm ảnh tương tự **IR-KDT** được xây dựng trên nền tảng dotNET Framework 4.5, ngôn ngữ lập trình C#. Cấu hình máy tính: Intel(R) Core™ i5-5200U, CPU 2.7GHz, RAM 16GB và hệ điều hành Windows 10 Professional.

Trong công trình này, dữ liệu thực nghiệm trên cơ sở lấy kết quả so sánh trên cấu trúc CB KD-Tree với các công trình [4] [5] là bộ ảnh Oxford Flowers 17 và Caltech-256. Bộ ảnh Oxford Flowers 17 gồm 1.360 hình ảnh được chia thành 17 chủ đề khác nhau và Caltech256 mô tả trong **bảng 1**. Mỗi hình ảnh được trích xuất một vector đặc trưng gồm 225 thành phần đó là: véc-tơ 225 chiều có các đặc trưng Color MPEG7 (25 giá trị), SIFT MPEG7 (25 giá trị), SHI MPEG7 (25 giá trị), Color Newton (6 giá trị), HOG (36 giá trị), Sobel HOG (36 giá trị), Laplace HOG (36 giá trị) và High Pass HOG (36 giá trị).

Bảng 1. Mô tả các tập dữ liệu ảnh thực nghiệm

TT	Tập ảnh	Số lượng ảnh	Số phân lớp
1	COREL	1,000	10
2	Caltech256	30,607	257

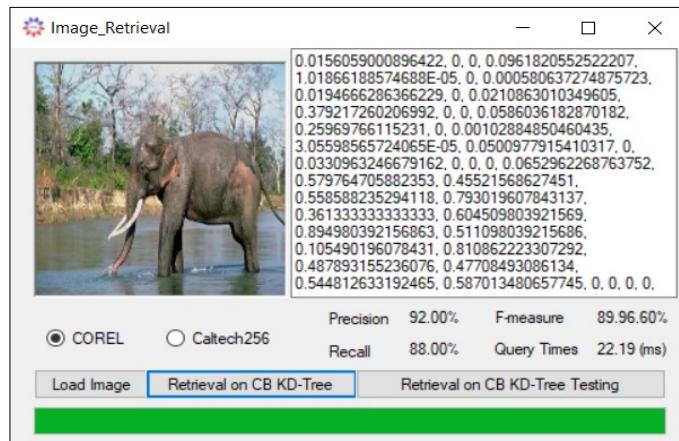


Hình 2. Thực nghiệm trích xuất véc-tơ đặc trưng 225 chiều.

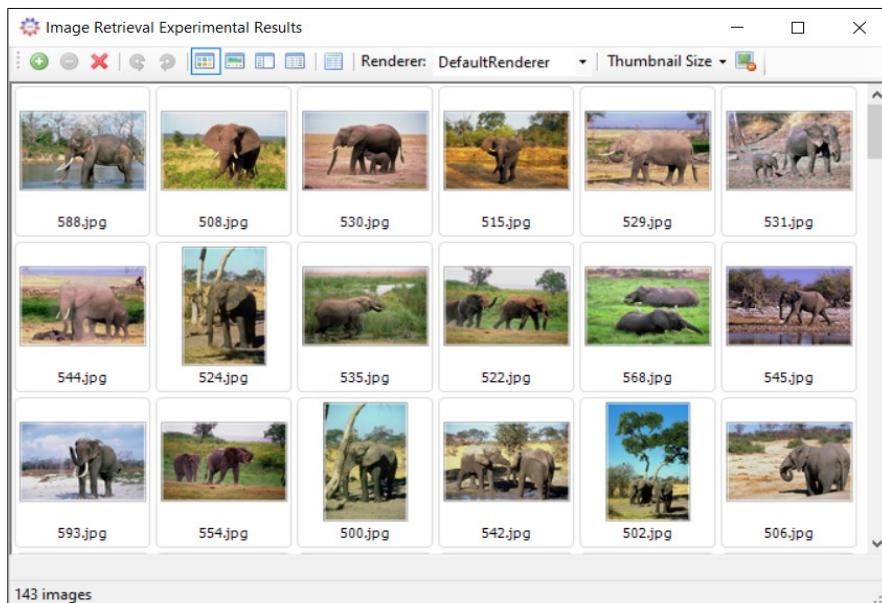
5.2. Xây dựng thực nghiệm

Bài báo tiến hành hai thực nghiệm trên hai bộ ảnh COREL và Caltech-256 với hai trường hợp: Trường hợp 1 là chỉ dùng KD-Tree cho tìm kiếm ảnh; Trường hợp 2 là kết hợp KD-Tree và K-Means để thực hiện gom cụm hai lần cho tập dữ liệu thực nghiệm.

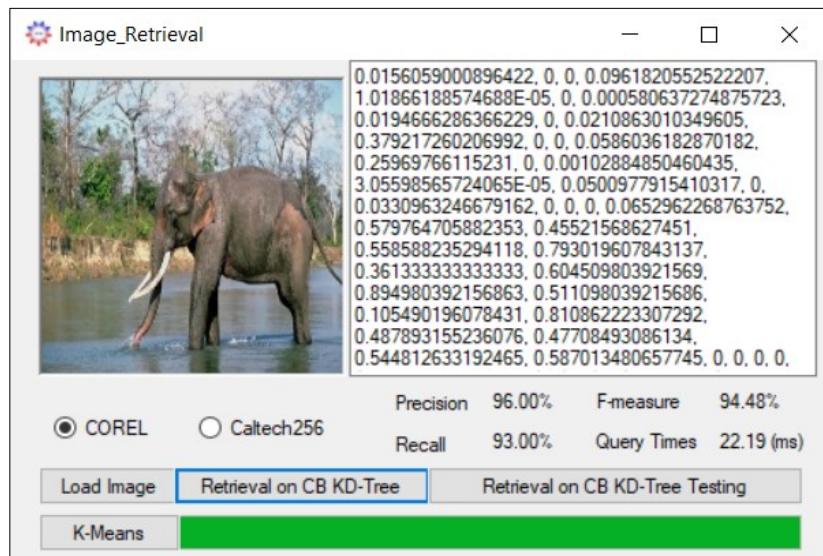
Thực nghiệm được xây dựng gồm **hình 1** xây dựng cấu trúc KD-Tree để lưu trữ hình ảnh theo từng bộ dữ liệu thực nghiệm được gom cụm tại các nút lá. Dựa trên số phân lớp của từng bộ ảnh để xác định số nhánh và chiều cao cho KD-Tree phù hợp. Sau khi xây dựng xong cấu trúc KD-Tree là xác định được số cụm, sau đó tiến hành thực hiện K-means một lần nữa theo số số bằng số nút lá, tâm cụm là giá trị trung bình tại mỗi nút lá hiện hành. Quá trình tìm kiếm tập ảnh tương tự dựa trên KD-Tree và K-Means được minh họa bởi **hình 2**. Kết quả tập ảnh tương tự với một ảnh đầu vào được minh họa bởi **hình 3**.



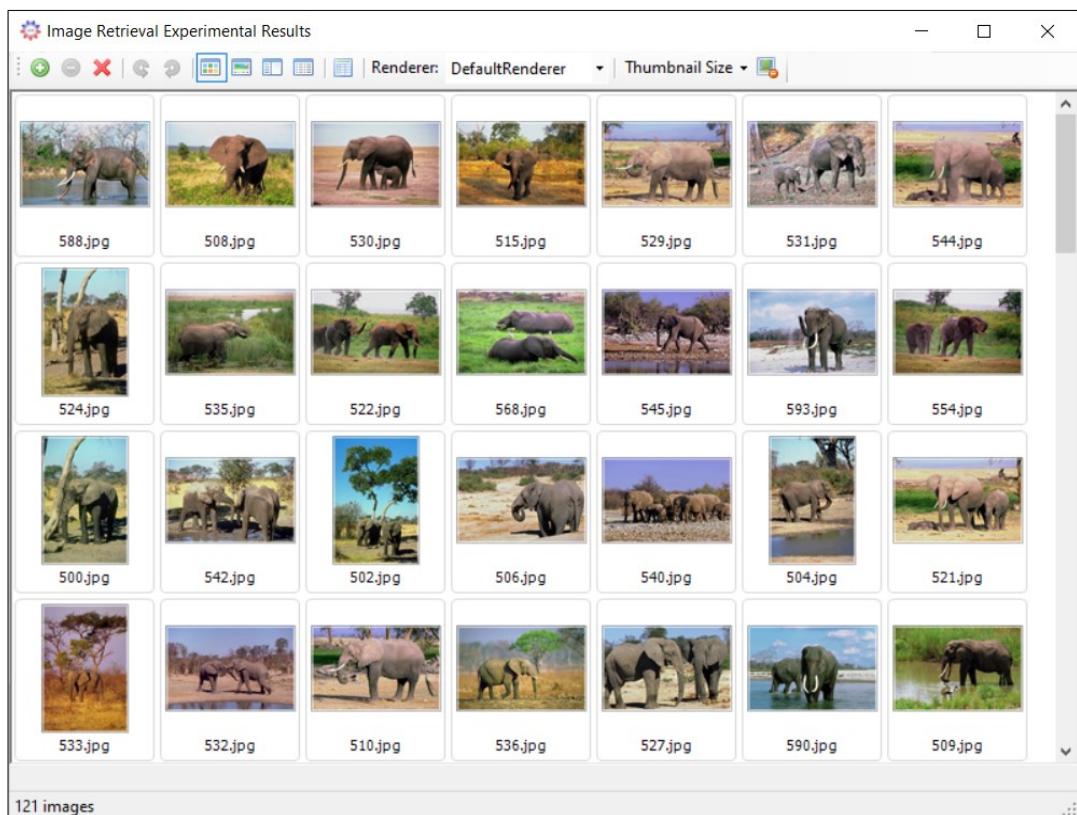
Hình 3. Giao diện thực nghiệm tìm kiếm ảnh dựa trên KD-Tree



Hình 4. Kết quả tìm kiếm ảnh trên KD-Tree



Hình 5. Giao diện thực nghiệm tìm kiếm ảnh dựa trên KD-Tree và K-Means



Hình 6. Kết quả tìm kiếm ảnh trên KD-Tree và K-Means

Bảng 2. Hiệu suất truy vấn các bộ ảnh thực nghiệm của hệ CB-KDT khi chưa kết hợp K-Means

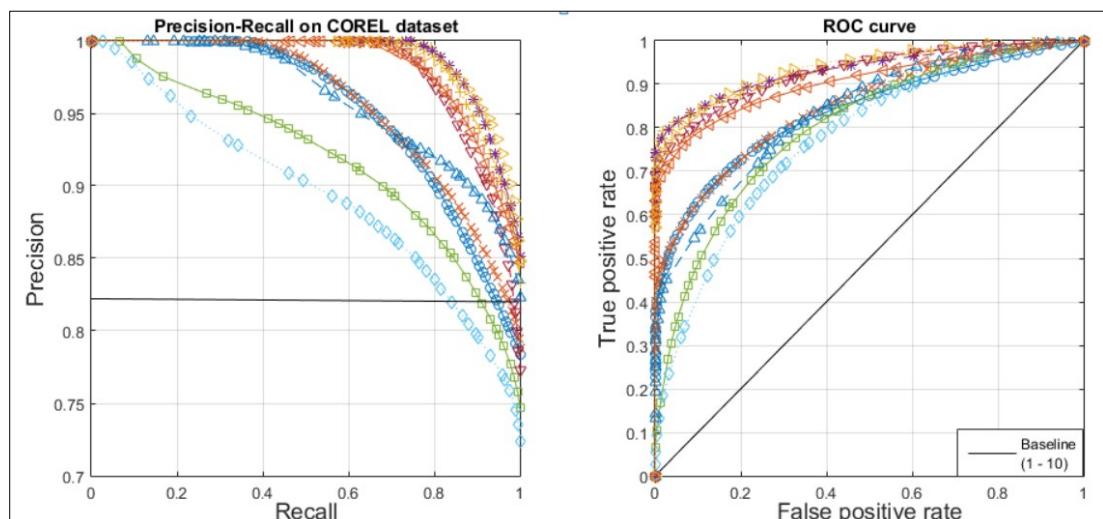
Tập ảnh	Độ chính xác trung bình	Độ phủ trung bình	Độ dung hòa trung bình
COREL	0.7808	0.6998	0.7370
Caltech256	0.7192	0.7050	0.7120

Kết quả thực nghiệm hệ tìm kiếm ảnh **IR-KKDT** được trình bày trong **bảng 3**.

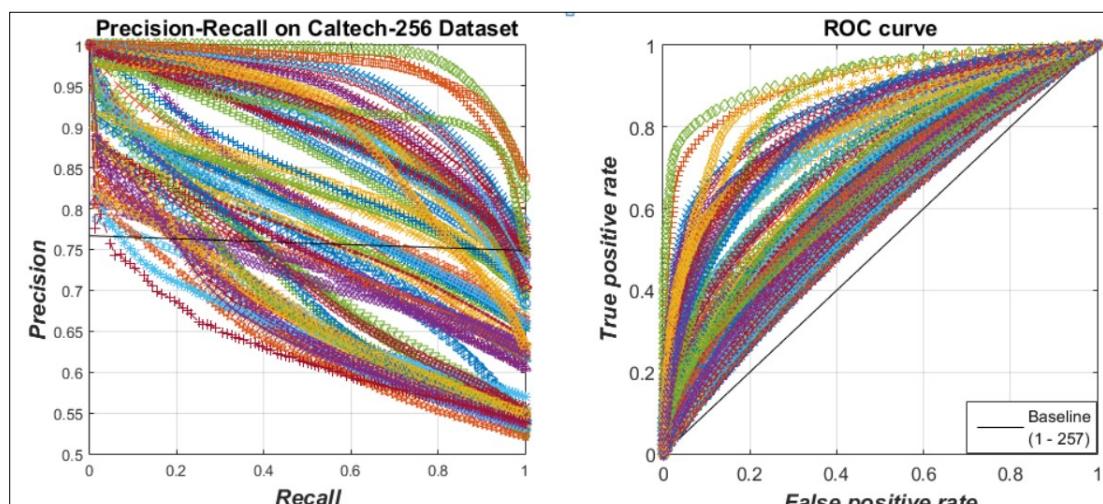
Bảng 3. Hiệu suất tìm kiếm ảnh của hệ IR-KDT

Tập ảnh	Precision	Recall	Độ dung hòa trung bình
COREL	0.8250	0.7020	0.7585
Caltech-256	0.7656	0.6968	0.7295

Kết quả thực nghiệm đánh giá mô hình được thực hiện trên bộ dữ liệu COREL và Caltech-256. Kết quả tìm kiếm ảnh trung bình hệ IR-KKDT được minh họa bằng đồ thị đường cong ROC trong **hình 6**. Mỗi đường cong trên đồ thị mô tả kết quả truy vấn với độ chính xác (precision) và độ phủ (recall) một chủ đề ảnh trong bộ dữ liệu. Đồng thời, đường cong tương ứng trong đồ thị ROC cho biết tỷ lệ kết quả truy vấn đúng và sai, nghĩa là diện tích dưới đường cong này đánh giá được tính đúng đắn của các kết quả truy vấn. Đồ thị đường cong ROC biểu diễn các giá trị true positive và false positive theo độ phủ Recall, các giá trị nằm tập trung trên đường cơ sở, nhiều giá trị nằm trong vùng true positive hơn vùng false positive.



Hình 7. Đường cong Precision, Recall và ROC cho bộ ảnh COREL



Hình 8. Đường cong Precision, Recall và ROC cho bộ ảnh Caltech-256

5.3. Đánh giá kết quả thực nghiệm

Hiệu suất hệ tìm kiếm ảnh dựa trên KD-Tree và K-Means được thực nghiệm so sánh với các công trình khác trên cùng bộ ảnh COREL và Caltech-256. Kết quả so sánh được trình bày trong **bảng 4**.

Bảng 4. So sánh hiệu suất truy vấn ảnh hệ SR-KDT với các công trình khác

Phương pháp	MAP
B_SHIFT, (Douik, Ali. et al.), 2016 [11]	0.7200
Shape and Texture Features, (Abdulkadhem, et al.), 2019 [12]	0.7286
ORB 8-dimensions with MPL, (P. Chhabra et al.), 2020 [13]	0.6656
C-Tree, (Nhi, N. T. U. et al.), 2021 [14]	0.6777
Multi-feature and SVM, (Gonçalves F. M. F., et al.), 2018 [15]	0.7657
Multi-feature with neural network, (Raja R., et al.), 2020 [16]	0.7941
IR-KDT	0.8250

Bảng 5. So sánh độ chính xác tìm kiếm ảnh trên bộ ảnh Caltech-256

Phương pháp	MAP
Visual Words FVFF, (Mehmood, Z., et al.), [17]	0.4630
SVM, (Uzma Sharif, et al.), 2019 [18]	0.4752
Ensembles of deep learning (Safa Hamreras), (50 classes), 2020 [19]	0.5726
CBIR, (Khawaja Tehseen Ahmed), 2019 [20] (TopK = 20)	0.7130
CBIR on n Significant Regions with Global CNN, (Jie Xu et al.), 2019 [21]	0.6490
IR-KDT	0.7656

Kết quả tìm kiếm ảnh dựa trên cấu trúc KD-Tree và thuật toán gom cụm K-Means của hệ **IR-KKDT** cao hơn các công trình khác trên cùng bộ dữ liệu. Điều này cho thấy phương pháp đề xuất của chúng tôi là khả thi, hiệu quả và có thể so sánh với các công trình khác cùng lĩnh vực bởi các lý do sau: (1) hệ **IR-KKDT** thực hiện gom cụm trên KD-Tree do quá trình huấn luyện nên kết quả gom cụm tương đối ổn định; (2) sau khi hình thành số cụm tại nút lá thì tiếp tục gom cụm một lần nữa bằng thuật toán K-Means với số cụm và tâm cụm đã xác định được từ số nút lá trên KD-Tree; vì vậy một số phần tử phân bố sai cụm lúc này sẽ được cập nhật lại đúng cụm tương đồng. Bên cạnh đó, sự kết hợp giữa cấu trúc KD-Tree và K-Means giúp giải quyết bài toán tìm kiếm ảnh hiệu quả về độ chính xác và thời gian tìm kiếm ổn định.

6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Trong bài báo này, chúng tôi đã triển khai một mô hình tìm kiếm ảnh dựa trên KD-Tree và thuật toán K-Means. Mỗi hình ảnh được lưu trữ trên cấu trúc KD-Tree sau khi thực hiện gom cụm K-Means đã xây dựng để tìm kiếm tập ảnh tương tự với ảnh đầu vào. Thực nghiệm được xây dựng dựa trên bộ dữ liệu hình ảnh COREL, Caltech-256 để chứng minh tính khả thi của phương pháp đề xuất của chúng tôi. Kết quả độ chính xác khi truy xuất hình ảnh trung bình cho mỗi bộ dữ liệu hình ảnh COREL, Caltech-256 lần lượt là **0.8690**, **0.7968**. Kết quả

thử nghiệm đã chứng minh rằng một phương pháp kết hợp cấu trúc KD-Tree và thuật toán gom cụm K-Means để truy xuất tập ảnh tương tự là khả thi và hiệu quả. Trong hướng phát triển tiếp theo, chúng tôi sẽ kết hợp thêm một số kỹ thuật phân lớp hình ảnh trước khi gom cụm nhằm nâng cao độ chính xác tìm kiếm ảnh, đồng thời thực hiện bài toán tìm kiếm ảnh theo ngữ nghĩa đáp ứng nhu cầu người dùng.

Lời cảm ơn: Nhóm tác giả chân thành cảm ơn Trường Đại học Công nghiệp Thực phẩm TP.HCM là nơi bảo trợ và hỗ trợ về chuyên môn để nhóm tác giả hoàn thành nghiên cứu này.

TÀI LIỆU THAM KHẢO

1. Hou, W. et al. (2018). *An advanced k nearest neighbor classification algorithm based on KD-tree*. in *2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*. IEEE Xplorer.
2. Singh, V.P.R. Srivastava (2018), *Improved image retrieval using fast Colour-texture features with varying weighted similarity measure and random forests*. Multimedia Tools and Applications. 77: p. 14435-14460.
3. Alrahal, M.K. Supreethi (2019). *Content-based image retrieval using local patterns and supervised machine learning techniques*. in *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE.
4. Le, T.M., et al (2013), *Image retrieval system based on EMD similarity measure and S-tree*. Intelligent Technologies and Engineering Systems, Springer, New York, NY: p. 139-146.
5. Nhi, N.T.U., Thanh, V.T., Thanh, L.M (2020), *A self-balanced clustering tree for semantic-based image retrieval*. Journal of Computer Science and Cybernetics, 36(1): p. 49-67.
6. Narasimhulua, Y., et al (2021), *Ckd-Tree: An Improved Kd-Tree Construction Algorithm*.
7. Nguyễn Thị Định, T.T.V., Mạnh Thạnh Lê, (2021) (2021), *Phân lớp ảnh bằng cây KD-Tree cho bài toán tìm kiếm ảnh tương tự*. Các công trình nghiên cứu, phát triển và ứng dụng Công nghệ Thông tin và Truyền thông: p. 40-52.
8. Erwin, E. (2017), *Similarity-Content Based Image Retrieval for Multi-Objects Fruits Recognition using k-Means and k-Nearest Neighbor*.
9. Jia, S., et al (2020), *Bag-of-Visual Words based Improved Image Retrieval Algorithm for Vision Indoor Positioning*. IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020: p. 1-4.
10. Kumar, Y.S., and N. Pavithra (2015) (2015), *KD-Tree approach in sketch based image retrieval*. International Conference on Mining Intelligence and Knowledge Exploration, Springer, Cham.
11. Douik, A., Mehrez Abdellaoui, and Leila Kabbai (2016), *Content based image retrieval using local and global features descriptor*. 2nd international conference on advanced Technologies for Signal and Image Processing (ATSIP).

12. Abdulkadhem, A.A., and Tawfiq A. Al-Assadi (2019), *Proposed a Content-Based Image Retrieval System Based on the Shape and Texture Features*. Int. J. Innovat. Technol. Explor. Eng. **8**(2189).
13. Chhabra, P., Garg, N. K., & Kumar, M. (2020), *Content-based image retrieval system using ORB and SIFT features*. Neural Computing and Applications: p. 2725-2733.
14. Nhi, N.T.U., & Le, T. M. (2021), *Semantic-Based Image Retrieval Using Balanced Clustering Tree*. In World Conference on Information Systems and Technologies: p. 416-427.
15. Gonçalves F. M. F., G.I.R., Pedronette D. C. G (2018), *Semantic guided interactive image retrieval for plant identification*. Expert Systems with Applications(91): p. 12-26.
16. Raja R., K.S., Mahmood M. R. (2020), *Color object detection based image retrieval using ROI segmentation with multi-feature method*. Wireless Personal Communications: p. 169-192.
17. Mehmood, Z., Abbas, F., Mahmood, T., Javid, M. A., Rehman, A., & Nawaz, T. (2018), *Content-Based Image Retrieval Based on Visual Words Fusion Versus Features Fusion of Local and Global Features*. Arabian Journal for Science & Engineering (Springer Science & Business Media BV),. **43**(2).
18. Sharif, U., Mehmood, Z., Mahmood, T., Javid, M. A., Rehman, A., & Saba, T (2019), *Scene analysis and search using local features and support véc-to machine for effective content-based image retrieval*. Artificial Intelligence Review. **52**(2): p. 901-925.
19. Hamreras, S., Boucheham, B., Molina-Cabello, M. A., Benitez-Rochel, R., & Lopez-Rubio, E (2020), *Content based image retrieval by ensembles of deep learning object classifiers*. Integrated Computer-Aided Engineering. **27**(3): p. 317-331.
20. Ahmed, K.T., Ummesafi, S., & Iqbal, A *Content based image retrieval using image features information fusion*. Information Fusion.
21. Xu, J., Sheng, S., Cai, Y., Bian, Y., & Xu, D. (2019), *Image Retrieval Research Based on Significant Regions*. In International Conference on Communications and Networking in China p. 127-136.

ABSTRACT**IMPROVING THE PERFORMANCE OF IMAGE RETRIEVAL BASED ON KD-TREE STRUCTURE AND K-MEANS****Nguyen Thi Dinh^{1*}, Tran Thi Bich Van¹, Nguyen Phuong Hac¹**¹*Ho Chi Minh City University of Food Industry**Email: dinhnt@hufi.edu.vn

Improving the accuracy of image retrieval is a matter of concern and implementation in the image retrieval problem. In this paper, we approach an image retrieval method based on the KD-Tree structure, then perform clustering by the K-Means algorithm based on the number of clusters formed from KD-Tree leaves to improve the accuracy of searching for a set of images similar to the input image. To perform this problem, first the image data set is extracted 225-dimensional feature vector, then construct the KD-Tree structure to form the similarity clusters at the leaves. After having the number of clusters, apply the K-Means algorithm to reallocate the data in half to adjust the clusters with the most similar number of elements and retrieval for a similar set of images with the input image. On that basis, an image retrieval model based on the KD-Tree structure combined with the K-Means clustering algorithm is proposed to retrieve similar images. To demonstrate the correctness of the proposed theoretical basis, the experiment is built on the COREL and Caltech-256 image sets with image search efficiency of 0.8250, and 0.7656, respectively. Experimental results are compared with other works on the same data set; this proves the feasibility and effectiveness of the proposed method..

Keywords: KD-Tree, K-Means, image retrieval, similar images

TIẾP CẬN CÁC PHƯƠNG PHÁP PHÂN LỚP DỮ LIỆU TRONG DỰ BÁO CHẤT LƯỢNG NƯỚC

Nguyễn Thị Diệu Hiền¹, Bùi Công Danh^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: danhbc@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Chất lượng nước là một vấn đề quan trọng vì mối quan hệ của nó với con người và các sinh vật sống khác. Dự đoán các thông số chất lượng nước là rất quan trọng để quản lý tài nguyên nước tốt hơn. Việc tiếp cận các phương pháp phân loại để xác định chất lượng nguồn nước là một vấn đề chưa có nhiều ứng dụng tại Việt Nam. Tuy nhiên các phương pháp phân loại này khi thực nghiệm đã cho ra kết quả phân loại chất lượng nước mang tính khả thi cao. Xuất phát từ những vấn đề nêu trên, trong bài báo này tác giả trình bày một cách tiếp cận là dùng các kỹ thuật phân lớp như: SVM, Random Forest, Logistic Regression để dự báo chất lượng nước.

Từ khóa: Phân loại, SVM, chất lượng nước.

1. GIỚI THIỆU

Nước là nguồn tài nguyên quan trọng cho sự sống còn của con người và chất lượng của nó ảnh hưởng trực tiếp đến phát triển và sử dụng tài nguyên nước. Vì sự thay đổi chất lượng nước có liên quan mật thiết với môi trường khí hậu, sự thay đổi theo mùa và các hoạt động của con người, sự thay đổi chất lượng nước sông có đặc điểm là thay đổi dần dần, phi tuyến tính và không chắc chắn (Y. K. Hu, N. Wang, S. Liu, Q. L. Jiang and N. Zhang, 2021), rất khó để chính xác đoán sự thay đổi chất lượng nước. Tuy nhiên, dự báo chất lượng nước có ý nghĩa rất lớn đối với việc lập kế hoạch quản lý tài nguyên nước và môi trường. Theo kết quả dự báo, tình hình ô nhiễm nước có thể được dự đoán trước, do đó sự cố ô nhiễm nước có thể được ngăn chặn trước thông qua các mô hình dự báo. Chất lượng nước là một vấn đề quan trọng vì mối quan hệ của nó với con người và các sinh vật sống khác.

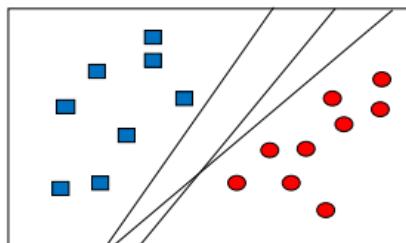
Dự báo chất lượng nước đóng vai trò rất quan trọng trong việc bảo vệ nguồn nước, giữ gìn sức khỏe cộng đồng và phát triển bền vững ngành nước.

2. TỔNG QUAN VỀ CÁC MÔ HÌNH PHÂN LỚP

Trong bài báo này, tác giả giới thiệu về các mô hình bài toán cũng như các phương pháp sử dụng để giải quyết các bài toán, bao gồm: Support Vector Machine, Random Forest, Logistic Regression.

2.1. Support Vector Machine (SVM)

“Máy vectơ hỗ trợ” (SVM) là một thuật toán học máy được giám sát có thể được sử dụng cho cả các thử thách phân loại hoặc hồi quy. Tuy nhiên, nó chủ yếu được sử dụng trong các bài toán phân loại. Trong thuật toán SVM, về mỗi mục dữ liệu dưới dạng một điểm trong không gian n chiều (với n là một số đối tượng mà bạn có) với giá trị của mỗi đối tượng là giá trị của một tọa độ cụ thể. Sau đó, thực hiện phân loại bằng cách tìm siêu mặt phẳng phân biệt hai lớp.

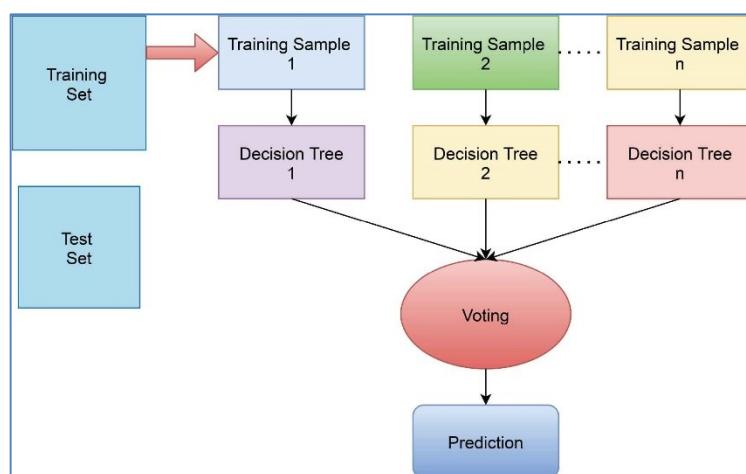


Hình 1. Có vô số đường thẳng phân tách hai lớp dữ liệu

Vectơ hỗ trợ chỉ đơn giản là tọa độ của quan sát cá nhân. Bộ phân loại SVM là biên giới phân tách tốt nhất hai lớp (siêu mặt phẳng / dòng).

2.2. Random Forest

Random Forest là một phương pháp học hồi quy, phân loại và các vấn đề phức tạp. Nó hoạt động bằng cách huấn luyện một số lượng lớn dữ liệu mẫu. Nó xây dựng cây quyết định từ các mẫu và sử dụng quyết định đa số cho phân loại và hồi quy. Bởi vì Random Forest làm việc với tập con dữ liệu, chúng hoạt động nhanh hơn cây quyết định. Vì vậy, chúng ta có thể giải quyết dễ dàng hàng trăm đặc điểm mà không gặp bất kỳ sự khó khăn nào. (Md. Mehedi Hassan, Md. Mahedi Hassan, Laboni Akter, Md. Mushfiqur Rahman, Sadika Zaman, Khan Md. Hasib, Nusrat Jahan, Raisun Nasa Smrity, Jerin Farhana, M. Raihan, Swarnali Mollick, 2021).



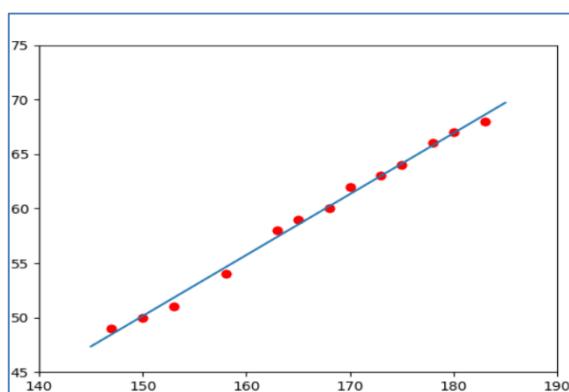
Hình 2. Lưu đồ thuật toán Random Forest

2.3. Logistic Regression

Sử dụng Logistic Regression để đánh giá dữ liệu phân loại trong các lĩnh vực khác nhau, bao gồm sức khỏe, xã hội và học thuật. Một biến phản hồi sau đó đã được dự đoán bằng cách sử dụng các biến giải thích tích hợp hoặc phân loại. Tức là nó đo lường tỷ lệ ý nghĩa tương đối của các biến độc lập, đánh giá các mối tương quan và giúp chúng ta hiểu được tác động của các biến kiểm soát tương quan (AM El-Habil, 2012). Trong nghiên cứu này, chúng tôi muốn biết các sửa đổi đã ảnh hưởng như thế nào đến các biến giải thích đối với xác suất của biến (SVS Ganga Devi, 2019) trong Phương trình (1), được biểu diễn dưới dạng:

$$P(Y=j/X_1, X_2, \dots, X_k) = P(Y=j/K); j = 0, 1, \dots, J(1)$$

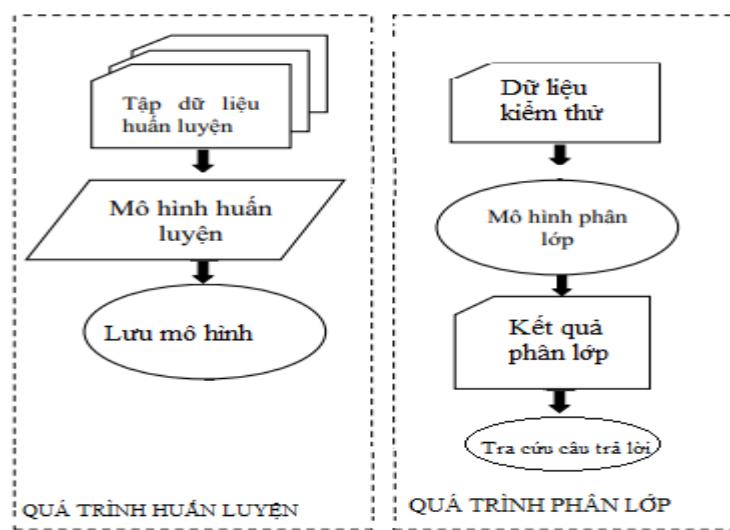
Ta có: Y = Biến phản hồi, X = Biến giải thích.



Hình 3. Bản chất của Logistic Regression

3. XÂY DỰNG VÀ ĐÁNH GIÁ CÁC MÔ HÌNH

Các bước xây dựng mô hình phân lớp và thực hiện phân loại dữ liệu dự báo chất lượng nước.



Hình 4. Mô hình hệ thống phân loại chất lượng nước

3.1. Xây dựng tập dữ liệu

Trong bài báo này, chúng tôi sử dụng bộ dữ liệu này là kết quả phân tích chất lượng nước với 3276 mẫu nước khác nhau. Phân tích đã xác định số lượng của 10 thành phần đáng quan tâm tác động lớn đến chất lượng nước. Bao gồm: { pH, Hardness, Solids, Chloramines, Sulfate, Conductivity, Organic_carbon, Trihalomethanes, Turbidity, Potability}. (Aditya Kadiwal, 2021)

ph	Hardness	Solids	Chloramin	Sulfate	Conductiv	Organic_c	Trihalome	Turbidity	Potability
3.71608	204.89	20791.3	7.30021	368.516	564.309	10.3798	86.991	2.96314	0
8.09912	129.423	18630.1	6.63525		592.885	15.18	56.3291	4.50066	1
8.31677	224.236	19909.5	9.27588		418.606	16.8686	66.4201	3.05593	0
9.09222	214.373	22018.4	8.05933	356.886	363.267	18.4365	100.342	4.62877	1
5.58409	181.102	17979	6.5466	310.136	398.411	11.5583	31.998	4.07508	0
10.2239	28749.7	28748.7	7.54487	326.678	280.468	8.39973	54.9179	2.55971	0
8.63585	248.072	13672.1	4.56301	303.31	474.608	12.3638	62.7983	4.40142	1
11.1803	118.989	14285.6	7.80417	268.647	389.376	12.706	53.9288	3.59502	0
7.36064	227.231	25484.5	9.0772	404.042	563.885	17.9278	71.9766	4.37056	1
7.97452	165.521	32452.6	7.5507	326.624	425.383	15.5868	78.74	3.66229	0
7.11982	218.693	18767.7	8.11038		364.098	14.5257	76.4859	4.01172	0
	156.705	18730.8	3.60604	282.344	347.715	15.9295	79.5008	3.44576	1

Hình 5. Dữ liệu chất lượng nước theo các thành phần

Các chỉ số biểu diễn chất lượng nước được mô tả như sau:

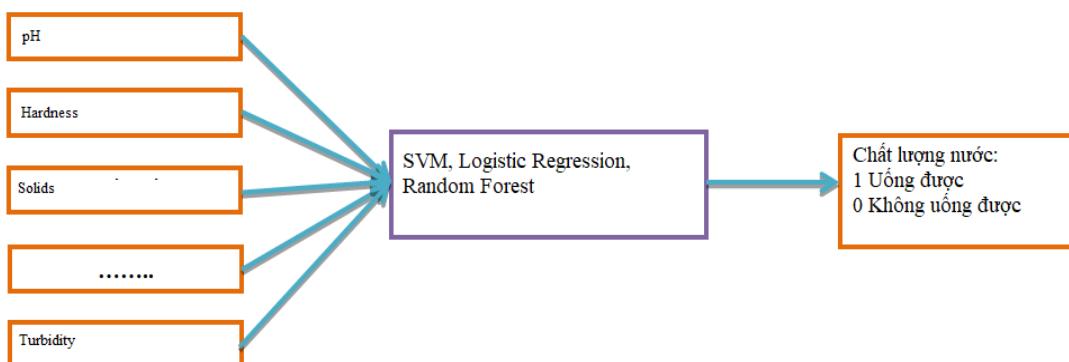
Bảng 1. Mô tả thông số chất lượng nguồn nước

Chỉ tiêu chất lượng	Mô tả
pH	PH là một thông số quan trọng trong việc đánh giá cân bằng axit-bazo của nước. Nó cũng là chỉ số về tình trạng axit hoặc kiềm của trạng thái nước. WHO đã khuyến cáo giới hạn tối đa cho phép của pH từ 6,5 đến 8,5. Phạm vi điều tra hiện tại là 6,52–6,83 nằm trong phạm vi tiêu chuẩn của WHO.
Hardness	Độ cứng chủ yếu do muối canxi và magie gây nên. Những muối này được hòa tan từ các trầm tích địa chất mà qua đó nước di chuyển. Khoảng thời gian nước tiếp xúc với vật liệu tạo độ cứng giúp xác định độ cứng có trong nước thô. Độ cứng ban đầu được định nghĩa là khả năng kết tủa xà phòng của nước do Canxi và Magie gây ra.
Solids	Nước có khả năng hòa tan nhiều loại khoáng chất vô cơ và hữu cơ hoặc muối chẳng hạn như kali, canxi, natri, bicacbonat, clorua, magiê, sunfat, v.v. Những khoáng chất này tạo ra mùi vị không mong muốn và màu loãng trong nước. Đây là thông số quan trọng cho việc sử dụng

Chỉ tiêu chất lượng	Mô tả
	nước. Nước có giá trị TDS cao chứng tỏ nước có nhiều khoáng chất. Giới hạn mong muốn cho TDS là 500 mg/l và giới hạn tối đa là 1000 mg/l được quy định cho mục đích uống.
Chloramines	Clo và chloramine là những chất khử trùng chính được sử dụng trong hệ thống nước công cộng. Chloramine thường được hình thành khi thêm amoniac vào clo để xử lý nước uống. Nồng độ clo lên tới 4 miligam trên lít (mg/L hoặc 4 phần triệu (ppm)) được coi là an toàn trong nước uống.
Sulfate	Sulfate là những chất tự nhiên được tìm thấy trong khoáng chất, đất và đá. Chúng hiện diện trong không khí xung quanh, nước ngầm, thực vật và thực phẩm. Việc sử dụng thương mại chính của sulfat là trong ngành hóa chất. Nồng độ sunfat trong nước biển là khoảng 2.700 miligam trên lít (mg/L). Nó nằm trong khoảng từ 3 đến 30 mg/L ở hầu hết các nguồn cung cấp nước ngọt, mặc dù nồng độ cao hơn nhiều (1000 mg/L) được tìm thấy ở một số vị trí địa lý.
Conductivity	Nước tinh khiết không phải là chất dẫn điện tốt mà là chất cách điện tốt. Tăng nồng độ ion giúp tăng cường tính dẫn điện của nước. Nói chung, lượng chất rắn hòa tan trong nước quyết định độ dẫn điện. Độ dẫn điện (EC) thực sự đo lường quá trình ion của một dung dịch cho phép nó truyền dòng điện. Theo tiêu chuẩn của WHO, giá trị EC không được vượt quá 400 µS/cm.
Organic_carbon	Tổng lượng Carbon hữu cơ (TOC) trong nguồn nước đến từ các chất hữu cơ tự nhiên đang phân hủy (NOM) cũng như các nguồn tổng hợp. TOC là thước đo tổng lượng carbon trong các hợp chất hữu cơ trong nước tinh khiết. Theo US EPA < 2 mg/L as TOC trong nước đã qua xử lý/nước uống, và < 4 mg/Lit trong nước nguồn được sử dụng để xử lý.
Trihalomethanes	THMs là hóa chất có thể được tìm thấy trong nước được xử lý bằng clo. Nồng độ THMs trong nước uống thay đổi tùy theo mức độ chất hữu cơ trong nước, lượng clo cần thiết để xử lý nước và nhiệt độ của

Chỉ tiêu chất lượng	Mô tả
	nước đang được xử lý. Mức THM lên đến 80 ppm được coi là an toàn trong nước uống.
Turbidity	Độ đục của nước phụ thuộc vào lượng chất rắn tồn tại ở trạng thái lỏng. Nó là thước đo các đặc tính phát sáng của nước và phép thử được sử dụng để chỉ ra chất lượng xả thải đối với chất keo. Giá trị độ đục trung bình thu được đối với Wondo Genet Campus (0,98 NTU) thấp hơn giá trị khuyến nghị của WHO là 5,00 NTU.
Potability	Cho biết nước có an toàn cho người tiêu dùng hay không trong đó 1 nghĩa là Uống được và 0 nghĩa là Không uống được.

3.2. Đề xuất mô hình dự báo chất lượng nước



Hình 6. Mô hình phân loại dự báo chất lượng nước

4. KẾT QUẢ THỰC NGHIỆM

4.1. Môi trường cài đặt

Kết quả được thực nghiệm trên máy tính sử dụng hệ điều hành windows 8.1 Pro 64bit, RAM 12GB, Chip Intel(R) Core(TM) i3-6820HQ, ~2.7 GHz, train model và sử dụng ngôn ngữ lập trình python phiên bản 3.7.7

4.2. Dữ liệu

Tác giả đã thực nghiệm trên 3276 mẫu nước khác nhau, dữ liệu được chia thành hai phần: một phần dùng để huấn luyện và một phần để dự báo. Nguồn dữ liệu được sử dụng (Aditya Kadiwal, 2021).

Tập dữ liệu mẫu: water_potability.csv

4.3. Kết quả thực nghiệm so sánh đánh giá các mô hình

Bảng 2. Thông số độ chính xác của các mô hình với các tập kiểm thử

	SVM	Logistic Regression	Random Forest
Tỷ lệ tập kiểm thử: 0.1			
Accuracy	0.7042	0.625	0.710
Precision	0.76	0.0	0.68
Recall	0.30	0.0	0.34
Tỷ lệ tập kiểm thử: 0.2			
Accuracy	0.6875	0.628	0.689
Precision	0.70	0.0	0.67
Recall	0.27	0.0	0.36
Tỷ lệ tập kiểm thử: 0.3			
Accuracy	0.681	0.622	0.682
Precision	0.7	1.0	0.67
Recall	0.27	0.005	0.35
Tỷ lệ tập kiểm thử: 0.4			
Accuracy	0.687	0.636	0.679
Precision	0.66	0.81	0.59
Recall	0.29	0.01	0.34
Tỷ lệ tập kiểm thử: 0.5			
Accuracy	0.692	0.637	0.658
Precision	0.69	0.73	0.59
Recall	0.30	0.04	0.33

Bảng 2 trình bày kết quả về mức độ chính xác trên các tập kiểm thử có kích thước khác nhau. Dựa vào đó có thể thấy, khi tập kiểm thử nhỏ thì độ chính xác cho kết quả tốt và tương đối đồng đều. Khi kích thước tập kiểm thử lớn hơn, bắt đầu có sự chênh lệch đáng kể về mức độ chính xác hơn. Đơn cử trường hợp test set 0.5: phương pháp Logistic Regression chỉ cho độ chính xác 0.637; Random Forest là 0.658; riêng SVM vẫn cho kết quả tương đối tốt là 0.692.

Với kết quả thực nghiệm như Bảng 2 cho chúng ta thấy rằng việc phân loại dự báo chất lượng nguồn nước cho kết quả khả quan tốt trên các mô hình phân loại khác nhau. Trong đó SVM thể hiện khả năng ứng dụng cao nhất cho việc phân loại này.

5. KẾT LUẬN

Bài báo đã phân tích được tầm quan trọng trong việc dự báo chất lượng nguồn nước. Đồng thời qua việc tiến hành thực nghiệm thu được những giá trị kiểm thử có độ chính xác khá cao. Cho thấy tính ưu việt của việc ứng dụng kỹ thuật phân lớp vào việc xác phân loại dự báo chất lượng nguồn nước. Mở ra một hướng đi khả quan cho việc ứng dụng các công cụ thuật toán vào giải quyết bài toán đánh giá môi trường tại Việt Nam cụ thể là chất lượng nước uống.

TÀI LIỆU THAM KHẢO

1. AM El-Habil. (2012). An application on multinomial logistic regression model. *Pakistan Journal of Statistics and Operation Research*, 271-291.
2. Aditya Kadiwal. (2021). *kaggle*. Đã truy lục 04/17/2023, từ Water Quality: <https://www.kaggle.com/datasets/adityakadiwal/water-potability>
3. Md. Mehedi Hassan, Md. Mahedi Hassan, Laboni Akter, Md. Mushfiqur Rahman, Sadika Zaman, Khan Md. Hasib, Nusrat Jahan, Raisun Nasa Smrity, Jerin Farhana, M. Raihan, Swarnali Mollick. (2021). Efficient Prediction of Water Quality Index (WQI) Using Machine Learning Algorithms. *Human-Centric Intelligent Systems*, 86-87.
4. SVS Ganga Devi. (2019). Random forest advice for water quality prediction in the regions of Kadapa district. *International Journal of Innovative Technology and Exploring Engineering*, 1464-1466.
5. Y. K. Hu, N. Wang, S. Liu, Q. L. Jiang and N. Zhang. (2021). Application research of time series model and LSTM model in water quality prediction. *Journal of Chinese Computer Systems*, pp. 1569–1573.

ABSTRACT

APPROACHING VARIOUS DATA CLASSIFICATION METHODS IN WATER QUALITY FORECASTING

Nguyen Thi Dieu Hien¹, Bui Cong Danh^{1,*}
Ho Chi Minh City University of Food Industry
 *Email: danhbc@hufi.edu.vn

Water quality is an important issue due to its relationship with humans and other living organisms. Predicting water quality parameters is crucial for better water resource management. Approaching classification methods to determine water source quality is an issue that has not been widely applied in Vietnam. However, these classification methods, when experimented, have yielded highly feasible water quality classification results. Based on the issues mentioned above, in this paper, the author presents an approach using classification techniques such as SVM, Random Forest, and Logistic Regression to predict water quality.

Keywords: Classification, SVM, water quality.

NGHIÊN CỨU THUẬT TOÁN TỐI UU ĐÀN KIẾN TIẾN HÓA

Đinh Nguyễn Trọng Nghĩa¹, Nguyễn Thị Thu Tâm^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm TP.HCM

*Email: tamntt@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo này đề xuất một phương pháp tối ưu lai kết hợp thuật toán Hệ thống đàm kién (ACS) với Tìm kiếm vùng lân cận biến đổi (VNS) và Giải thuật di truyền (GA) để giải các bài toán tối ưu tổ hợp. Phương pháp đề xuất tận dụng những điểm mạnh của từng thuật toán và khắc phục những hạn chế của chúng, dẫn đến quá trình tối ưu hóa hiệu quả hơn. Chúng tôi xem xét tài liệu về ACS, VNS và GA, cũng như các kết hợp trước đây của chúng.

Từ khóa: Hệ thống đàm kién, Tìm kiếm vùng lân cận biến đổi, Giải thuật di truyền

1. MỞ ĐẦU

Ant Colony Optimization (ACO) [1] và giải thuật di truyền (GA) [3] là hai kỹ thuật tối ưu nổi tiếng và mạnh mẽ đã được nghiên cứu và ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau. ACO được lấy cảm hứng từ hành vi của loài kiến khi chúng tìm kiếm thức ăn, trong khi GA được lấy cảm hứng từ quá trình chọn lọc tự nhiên và tiến hóa. Cả hai phương pháp đều có điểm mạnh và điểm yếu và chúng đã được áp dụng cho nhiều vấn đề tối ưu hóa, chẳng hạn như định tuyến, lập lịch trình và tối ưu hóa thiết kế.

Tuy nhiên, bất chấp những thành công của chúng, cả ACO và GA đều có những hạn chế. Ví dụ như ACO bị hội tụ sớm và bị mắc kẹt trong tối ưu cục bộ, trong khi GA hội tụ chậm và gặp khó khăn khi xử lý các vấn đề tối ưu hóa bị hạn chế. Để khắc phục những hạn chế này, một số phương pháp lai ghép đã được đề xuất [5] [8] [9], kết hợp các ưu điểm của ACO và GA để tạo ra một thuật toán tối ưu hóa mạnh mẽ và hiệu quả hơn.

Trong bài báo này, chúng tôi đề xuất một thuật toán tối ưu đàm kiến tiến hóa. Động lực chính đằng sau nghiên cứu này là tận dụng điểm mạnh của cả ACO và GA để tạo ra một thuật toán tối ưu hóa hiệu quả hơn, xử lý nhiều vấn đề khác nhau.

Thuật toán lai được đề xuất sử dụng ACS để khám phá không gian tìm kiếm và GA để khai thác các giải pháp do ACS tìm thấy. Ngoài ra, trong thuật toán ACS còn áp dụng một chiến lược tìm kiếm nội bộ (local search) để nâng cao hiệu suất tìm kiếm hơn nữa. Hiệu suất của thuật toán đề xuất được đánh giá và so sánh với cả ACS và GA trên một tập hợp các bài toán chuẩn và kết quả chứng minh tính hiệu quả của phương pháp kết hợp.

Thuật toán lai được đề xuất có khả năng cung cấp một kỹ thuật tối ưu hiệu quả hơn, áp dụng cho nhiều bài toán trong các lĩnh vực khác nhau.

2. CƠ SỞ LÝ THUYẾT

2.1 Tối ưu hóa đàm kién

2.1.1 Tổng quan về tối ưu hóa đàm kién

Tối ưu hóa đàm kién (ACO) [1] [4] [6] là một kỹ thuật tối ưu hóa metaheuristic lấy cảm hứng từ hành vi kiếm ăn của loài kiến. ACO lần đầu tiên được giới thiệu bởi Marco Dorigo trong luận án tiến sĩ của ông vào năm 1992, kể từ đó, nó đã được nghiên cứu và ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau.

ACO dựa trên ý tưởng rằng những con kiến giao tiếp với nhau bằng cách gửi pheromone (mùi) trên mặt đất, những con kiến khác theo dõi để tiếp cận nguồn thức ăn. ACO mô phỏng hành vi này bằng cách biểu diễn vấn đề dưới dạng biểu đồ, trong đó các nút biểu thị các thành phố hoặc địa điểm sẽ được truy cập và các cạnh biểu thị các đường dẫn giữa chúng. Những con kiến xây dựng một giải pháp bằng cách tuân theo phân phối xác suất, được xác định bởi mức độ pheromone trên các cạnh và thông tin khám phá.

Mức độ pheromone được cập nhật sau mỗi lần lặp lại thuật toán, dựa trên chất lượng của các giải pháp được tìm thấy. Quy tắc cập nhật pheromone được thiết kế để cung cấp các cạnh là một phần của giải pháp tốt hơn và làm bay hơi pheromone trên các cạnh ít hứa hẹn hơn, để tránh hội tụ sớm.

Một số biến thể và phần mở rộng của ACO đã được đề xuất, chẳng hạn như Hệ thống kiến, Hệ thống đàm kién và Hệ thống kiến tối đa. Các thuật toán này khác nhau về quy tắc cập nhật pheromone, quy tắc quyết định kiến và các phương pháp phỏng đoán bổ sung, chẳng hạn như chiến lược tìm kiếm và đa dạng hóa cục bộ.

ACO đã được áp dụng cho nhiều bài toán tối ưu hóa, chẳng hạn như bài toán người bán hàng du lịch, bài toán định tuyến phương tiện, bài toán lập kế hoạch cửa hàng việc làm và bài toán chiếc ba lô. ACO đã cho thấy khả năng cạnh tranh với các kỹ thuật tối ưu hóa metaheuristic khác, chẳng hạn như Thuật toán di truyền hay Tối ưu hóa bầy đàn.

Một trong những lợi thế của ACO là nó xử lý các vấn đề tối ưu hóa tổ hợp với không gian tìm kiếm lớn, vì nó khám phá các giải pháp khác nhau theo cách song song và phân tán. Ngoài ra, ACO xử lý các vấn đề với các hàm mục tiêu phi tuyến tính và không lồi, vì nó tìm thấy nhiều điểm tối ưu.

Tuy nhiên, ACO cũng có một số hạn chế, chẳng hạn như độ nhạy của nó đối với cài đặt tham số, khó khăn trong việc xử lý các ràng buộc và bị kẹt trong tối ưu cục bộ.

2.1.2 Thuật toán hệ thống đàm kién (Ant Colony System Algorithm)

Hệ thống đàm kién (ACS) [10-11] là một biến thể của thuật toán tối ưu đàm kién. ACS tương tự như thuật toán Ant Colony, nhưng nó bao gồm một số tính năng bổ sung giúp cải thiện hiệu suất và độ chính xác của nó. Một trong những điểm khác biệt chính là ACS sử dụng quy tắc cập nhật toàn cầu cho pheromone, có tính đến giải pháp tốt nhất được tìm thấy cho đến nay, bên cạnh quy tắc cập nhật pheromone cục bộ mà Ant System sử dụng.

ACS cũng giới thiệu một chức năng heuristic hướng dẫn kiến trong quá trình ra quyết định của chúng. Chức năng này tính đến cả đường dẫn pheromone và khoảng cách giữa các nút, để cân bằng giữa việc khai thác và khám phá không gian tìm kiếm. Ngoài ra, ACS bao

gồm một tham số được gọi là tham số "q0", điều khiển xác suất kién chọn giải pháp tốt nhất được tìm thấy cho đến nay, thay vì sử dụng hàm heuristic.

Thuật toán ACS được tóm tắt trong các bước sau:

1. Initialize the pheromone trail on each edge with a small positive value.
2. For each ant:
 - a. Choose a starting node randomly.
 - b. Repeat until all nodes have been visited:
 - i. Compute the probability of moving to each neighbor, based on the pheromone trail and the heuristic function.
 - ii. Choose the next node based on the probability distribution.
 - iii. Update the pheromone trail on the edge just traversed, using the global and local updating rules.
 3. Update the best solution found so far.
 4. Update the pheromone trail on each edge, using the global updating rule.
 5. Repeat steps 2 to 4 until a stopping criterion is met.

2.2 Thuật giải di truyền (Genetic Algorithms)

Thuật toán di truyền (GA) [3] là một loại kỹ thuật tối ưu hóa metaheuristic lấy cảm hứng từ các nguyên tắc chọn lọc tự nhiên và tiến hóa. GA được John Holland giới thiệu lần đầu tiên vào những năm 1960 và kể từ đó đã trở thành một trong những kỹ thuật tối ưu hóa được sử dụng rộng rãi nhất.

GA mô phỏng quá trình chọn lọc tự nhiên bằng cách duy trì một quần thể các giải pháp ứng cử viên, tiến hóa theo thời gian bằng cách tái tổ hợp và đột biến. Mỗi giải pháp ứng cử viên được biểu diễn dưới dạng một nhiễm sắc thể, bao gồm một chuỗi gen mã hóa các giá trị của các biến quyết định.

Thuật toán GA được tóm tắt trong các bước sau:

1. Initialize a population of candidate solutions randomly.
2. Evaluate the fitness of each solution based on its objective function value.
3. Repeat until a stopping criterion is met:
 - a. Select parents from the population based on their fitness values.
 - b. Recombine the genes of the parents to create a new offspring.
 - c. Mutate some of the genes of the offspring randomly.
 - d. Evaluate the fitness of the offspring.
 - e. Replace some of the worst solutions in the population with the offspring.
4. Return the best solution found in the population.

Việc lựa chọn cha mẹ ở bước 3a được thực hiện bằng nhiều phương pháp khác nhau, chẳng hạn như lựa chọn bánh xe roulette, lựa chọn giải đấu hoặc lựa chọn thứ hạng. Lai tạo được thực hiện bằng cách sử dụng nhiều toán tử khác nhau, chẳng hạn như giao nhau một điểm, giao nhau hai điểm hoặc giao nhau đồng nhất. Đột biến được thực hiện bằng cách thay đổi ngẫu nhiên một số gen ở thế hệ con.

GA đã được áp dụng cho một loạt các bài toán tối ưu hóa, chẳng hạn như tối ưu hóa chức năng, lựa chọn tính năng, lập lịch và các vấn đề về định tuyến. GA đã cho thấy khả năng cạnh tranh với các kỹ thuật tối ưu hóa metaheuristic khác.

Một trong những ưu điểm của GA là khả năng xử lý các vấn đề với không gian tìm kiếm lớn và các hàm mục tiêu phi tuyến tính và không lồi. Ngoài ra, GA xử lý các vấn đề với nhiều mục tiêu bằng cách sử dụng các kỹ thuật tối ưu hóa đa mục tiêu, chẳng hạn như tối ưu hóa Pareto.

Tuy nhiên, GA cũng có một số hạn chế, chẳng hạn như độ nhạy của chúng đối với cài đặt tham số, khó khăn trong việc xử lý các ràng buộc và có khả năng kẹt trong tối ưu cục bộ.

2.3 Các công trình liên quan

Đã có một số công trình trước đây về việc kết hợp Tối ưu đàm kién (ACO) và Thuật toán di truyền (GA) để tạo ra một thuật toán tối ưu hóa lai tận dụng điểm mạnh của cả hai kỹ thuật.

Một trong những công trình sớm nhất về sự kết hợp này đã được đề xuất bởi Boussaid et al. [12] vào năm 2004, nơi họ đề xuất một thuật toán gọi là ACO-GA cho vấn đề định tuyến phương tiện. Trong thuật toán này, GA được sử dụng để phát triển các vệt pheromone của kiến trong thuật toán ACO, dẫn đến sự hội tụ nhanh hơn và kết quả tốt hơn.

Một công việc khác được đề xuất bởi Hao et al. [13] vào năm 2007, nơi họ kết hợp các thuật toán ACO và GA để giải bài toán người bán hàng du lịch. Trong thuật toán này, GA được sử dụng để tạo các giải pháp ban đầu cho thuật toán ACS, sau đó thuật toán này tinh chỉnh các giải pháp này bằng cách sử dụng các vệt pheromone.

Năm 2010, Zou et al. [14] đã đề xuất một thuật toán kết hợp có tên là ACGA-LD cho vấn đề định tuyến phương tiện, kết hợp ACO, GA và một kỹ thuật tìm kiếm cục bộ có tên là Late Acceptance Hill Climbing. Thuật toán ACO được sử dụng để tạo các giải pháp ban đầu, sau đó được cải thiện bằng cách sử dụng GA.

Năm 2014, Yang et al. [15] đã đề xuất một thuật toán có tên là ACGA-MA cho bài toán lập lịch cửa hàng việc làm, thuật toán này kết hợp ACO, GA và cách tiếp cận hệ thống đa tác nhân. Thuật toán ACO được sử dụng để tạo ra các giải pháp ban đầu, sau đó được cải thiện bằng cách sử dụng GA và cách tiếp cận hệ thống đa tác nhân để điều phối các quyết định lập lịch trình.

Gần đây hơn, vào năm 2019, Liu et al. [16] đã đề xuất một thuật toán có tên AG-ACS cho vấn đề triển khai mạng cảm biến không dây, thuật toán này kết hợp GA và ACS với phương pháp heuristic tô màu đồ thị. Trong thuật toán này, GA được sử dụng để phát triển các vệt pheromone của kiến trong thuật toán ACS và phương pháp phỏng đoán tô màu biểu đồ được sử dụng để cải thiện hơn nữa các giải pháp.

Nhìn chung, các công trình trước đây đã chỉ ra rằng việc kết hợp ACS và GA dẫn đến hiệu suất được cải thiện trong các vấn đề tối ưu hóa khác nhau và một số phương pháp lai ghép đã được đề xuất để nâng cao hơn nữa hiệu quả của thuật toán.

3. THUẬT TOÁN ĐỀ XUẤT

Đây là thuật toán đề xuất kết hợp giữa thuật toán ACS với GA, trong đó có sử dụng thêm chiến lược local search là Variable Neighborhood Search (VNS)

1. Initialize pheromone trails $\tau(i,j)$ to a small positive number
2. Initialize the population of solutions with random tours
3. Repeat until termination condition is met:
 - a. Generate an ant k
 - b. Repeat for each city visited by ant k :
 - i. Calculate the probabilities of choosing the next city based on the current pheromone trails and the heuristic information
 - ii. Choose the next city based on the probabilities
 - iii. Update the local pheromone trail $\tau(k, i, j)$
 - c. Apply VNS to the resulting tour to obtain an improved solution
 - d. Add the improved solution to the population
 - e. Apply GA to the population to obtain a new set of solutions
 - f. Update the global pheromone trails $\tau(i,j)$ based on the best solution found in the population
 - g. Update the best solution found so far
4. Return the best solution found

Trong thuật toán sửa đổi này, sau khi một con kiến hoàn thành hành trình của mình, ta áp dụng VNS cho hành trình kết quả để có được giải pháp cải tiến. Giải pháp cải tiến sau đó được thêm vào tập hợp các giải pháp. Sau đó, chúng tôi áp dụng GA cho quần thể kiến để có được một tập hợp các giải pháp mới. Giải pháp tốt nhất được tìm thấy trong quần thể được sử dụng để cập nhật pheromone. Phần còn lại của thuật toán vẫn giống như trong thuật toán ACS ban đầu.

3.1 Quy tắc cập nhật Pheromone

Quy tắc cập nhật pheromone là một thành phần quan trọng của thuật toán tối ưu hóa đàm kiến. Nó xác định cách ma trận pheromone được cập nhật dựa trên chất lượng của các giải pháp mà kiến tìm thấy.

Trong thuật toán đề xuất bên trên, quy tắc cập nhật pheromone được đưa ra bởi:

$$\tau(i,j) = (1 - \rho) * \tau(i,j) + \rho * \Delta\tau(i,j)$$

Trong đó:

- $\tau(i,j)$ là lượng pheromone trên cạnh (i, j)
- ρ là tốc độ bay hơi pheromone (một tham số giữa 0 và 1)
- $\Delta\tau(i,j)$ là lượng pheromone được gửi bởi những con kiến trên cạnh (i, j)

Số hạng $(1 - \rho) * \tau(i,j)$ biểu thị lượng pheromone trên cạnh (i,j) sau khi bay hơi. Thuật ngữ $\rho * \Delta\tau(i,j)$ biểu thị lượng pheromone do kiến gửi trên cạnh (i,j) .

Lượng pheromone được gửi bởi những con kiến trên cạnh (i,j) được cho bởi:

$$\Delta\tau(i,j) = Q / L(k)$$

Trong đó:

Q là hằng số xác định tổng lượng pheromone do tất cả các con kiến gửi vào trong hành trình tốt nhất được tìm thấy cho đến nay

$L(k)$ là độ dài của hành trình được tìm thấy bởi kiến k

Quy tắc cập nhật pheromone về cơ bản cập nhật ma trận pheromone dựa trên chất lượng của các giải pháp mà kiến tìm thấy. Càng nhiều pheromone tích tụ trên một cạnh thì cạnh đó càng trở nên hấp dẫn đối với những con kiến trong tương lai. Ngược lại, tốc độ bay hơi của pheromone xác định mức độ nhanh chóng của các pheromone suy giảm theo thời gian. Tốc độ bay hơi cao khuyến khích khám phá các giải pháp mới, trong khi tốc độ bay hơi thấp khuyến khích khai thác các giải pháp hiện có.

3.2 Variable Neighborhood Search (VNS)

Ý tưởng cơ bản của VNS [2] là khám phá không gian giải pháp bằng cách thay đổi một cách có hệ thống cấu trúc lân cận trong đó giải pháp được đánh giá, VNS thường được sử dụng như là một local search cho các thuật toán tối ưu dạng meta-heuristic [7].

Thuật toán bắt đầu với một giải pháp ban đầu và một tập hợp các cấu trúc lân cận. Giải pháp hiện tại được đánh giá trong từng cấu trúc lân cận và giải pháp tốt nhất được tìm thấy được chọn. Sau đó, cấu trúc lân cận được thay đổi và quá trình tìm kiếm được lặp lại.

VNS áp dụng để mở rộng phạm vi tìm kiếm trong thuật toán tối ưu đòn kiến. Trong đó, sau khi thực hiện bước di chuyển cho đòn kiến, thuật toán VNS được áp dụng lên các phần tử của đòn kiến để tìm ra giải pháp tối ưu trong lân cận.

3.3 Genetic Algorithm

Ý tưởng cơ bản của thuật toán di truyền là mô phỏng quá trình chọn lọc tự nhiên bằng cách duy trì một quần thể các giải pháp tiềm năng cho một vấn đề và áp dụng các toán tử di truyền (ví dụ: lai ghép và đột biến) để tạo ra các giải pháp mới. Mức độ phù hợp của từng giải pháp được đánh giá và những cá thể khỏe mạnh nhất được chọn để sinh sản và truyền vật chất di truyền của chúng cho thế hệ tiếp theo.

GA được áp dụng lên thuật toán tối ưu đòn kiến để tạo nên các cá thể mới (các con kiến mới) sau mỗi lần lặp của bài toán. Sau khi thực hiện di chuyển đòn kiến và áp dụng local search với VNS, GA được áp dụng bằng cách chọn lựa các cá thể trội (fitness cao) và thực hiện lai hóa các cá thể này để tạo nên cá thể tốt hơn. Ngoài ra, đột biến cũng được thực hiện lên vài cá thể trong quần thể.

4. KẾT LUẬN

Bài báo này đã trình bày một phương pháp tối ưu hóa lai kết hợp thuật toán Hệ thống đòn kiến (ACS) với Tìm kiếm vùng lân cận biến đổi (VNS) và Giải thuật di truyền (GA) để giải các bài toán tối ưu tổ hợp. Phương pháp đề xuất tận dụng những điểm mạnh của từng thuật toán và khắc phục những hạn chế của chúng, dẫn đến quá trình tối ưu hóa hiệu quả hơn.

Bài báo đã xem xét về ACO, VNS và GA, cũng như các kết hợp trước đây của chúng. Sau đó trình bày các thuật toán kết hợp đề xuất. Bài báo cũng cung cấp chi tiết triển khai và mã giả cho phương pháp kết hợp, bao gồm quy tắc cập nhật pheromone, tìm kiếm cục bộ bằng VNS và GA.

Trong các công trình tiếp theo, chúng tôi dự định nghiên cứu kỹ hơn nữa về thuật toán kết hợp này bằng cách áp dụng cho các vấn đề tối ưu hóa trong thực tế và đánh giá hiệu suất của nó trong các cài đặt thực tế. Nhìn chung, chúng tôi tin rằng phương pháp đề xuất có tiềm năng đóng góp vào việc phát triển các phương pháp tối ưu hiệu quả hơn cho các bài toán tổ hợp.

TÀI LIỆU THAM KHẢO

1. Dorigo, M., & Gambardella, L. M. Ant systems: A cooperative learning approach to the traveling salesman problem. *IEEE Transactions on Evolutionary Computation*, 1996, 1(1), 53-66.
2. Hansen, P., & Mladenović, N. Variable neighborhood search: Principles and applications. *European Journal of Operational Research*, 2021. 130(3), 449-467.
3. Goldberg, D. E. (1989). *Genetic algorithms in search, optimization, and machine learning*. Addison-Wesley.
4. Dorigo, M., & Stützle, T. *Ant colony optimization*. MIT Press. 2024
5. Blum, C., Roli, A., & Sampels, M. Hybrid metaheuristics for vehicle routing problems. In *Handbook of metaheuristics* (pp. 319-353). Springer. 2023
6. Gambardella, L. M., & Dorigo, M. Ant colony system: a cooperative learning approach to the traveling salesman problem. In *International Conference on Artificial Ants* (pp. 109-114). Springer. 1999.
7. Lourenço, H. R., Martin, O. C., & Stützle, T. Iterated local search. In *Handbook of metaheuristics* (pp. 157-187). Springer. 2010
8. Gendreau, M., Potvin, J. Y., & Rousseau, J. M. Metaheuristics for the capacitated VRP. In *Metaheuristics for vehicle routing problems* (pp. 129-154). Wiley. 1998
9. Raidl, G. R., & Pferschy, U. Hybridization of metaheuristics: Concepts and applications. *Handbook of metaheuristics*, 1-29. 2006
10. Gunawan, A., & Syahputra, M. F. Review of Ant Colony Optimization (ACO) algorithm: Application, variants, and challenges. *Journal of King Saud University-Computer and Information Sciences*, 32(6), 667-681. 2020
11. Socha, K. Ant colony optimization. *Scholarpedia*, 14(7), 30176. 2019
12. Dorigo, M., Gambardella, L. M., & Bonabeau, E. Ant colony system: a cooperative learning approach to the traveling salesman problem. *IEEE Transactions on Evolutionary Computation*, 2004. 1(1), 53-66.
13. Hao, J., Liu, H., & Zhao, Y. Hybrid ant colony optimization and genetic algorithm for traveling salesman problem. In *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing* (pp. 2580-2583). 2007.
14. Zou, C., Liu, B., & Chen, X. A hybrid ant colony optimization algorithm for the vehicle routing problem with time windows. *Expert Systems with Applications*, 37(12), 7745-7754. 2010
15. Yang, L., Qin, X., & Liu, H. A hybrid ACO-GA algorithm for multi-objective flexible job-shop scheduling problem. *Applied Soft Computing*, 19, 223-236. 2014.
16. Liu, H., Zhao, Y., & Zhang, H. Adaptive genetic ant colony optimization algorithm for continuous optimization problems. *Swarm and Evolutionary Computation*, 47, 1-12. 2019.

ABSTRACT

AN EVOLUTIONARY ANSWERING MATHEMATICS RESEARCH

Dinh Nguyen Trong Nghia¹, Nguyen Thi Thu Tam^{1,*}

¹*Ho Chi Minh City University of Food Industry, 140 Le Trong Tan, Tay Thanh Ward, Tan Phu District, Ho Chi Minh City*

*Email: tamntt@hufi.edu.vn

This paper proposes a hybrid optimization method that combines Ant Colony System (ACS) algorithm with Variable Neighborhood Search (VNS) and Genetic Algorithm (GA) to solve combinatorial optimization problems. The proposed method takes advantage of the strengths of each algorithm and overcomes their limitations, resulting in a more efficient and effective optimization process. We review the literature on ACS, VNS, and GA, as well as their previous combinations.

Keywords: Ant Colony System, Variable Neighborhood Search, Genetic Algorithm

TỔNG QUAN VỀ HỌC LIÊN KẾT VÀ TIỀM NĂNG ỨNG DỤNG TRONG LĨNH VỰC Y HỌC

Trần Trương Tuấn Phát^{1,2}, Đặng Trần Khánh^{1,*}, Nguyễn Thị Thanh Thảo¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

² Trường Đại học Bách Khoa - Đại học Quốc Gia Thành phố Hồ Chí Minh

*Email: khanh@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trong xu hướng ứng dụng công nghệ hiện nay, nhu cầu về bảo vệ quyền riêng tư dữ liệu của cá nhân ngày càng tăng cao. Hàng ngày, chúng ta sử dụng nhiều dịch vụ trực tuyến và ứng dụng di động để lưu trữ thông tin cá nhân, trong đó không ít là dữ liệu riêng tư mà nếu không xử lý một cách hợp lý thì mức độ ảnh hưởng đến bản thân là khôn lường. Các công nghệ dựa trên trí tuệ nhân tạo (*Artificial Intelligence - AI*) - được coi là trụ cột chính của cuộc cách mạng 4.0, cũng không phải là ngoại lệ. Thách thức xây dựng được một bộ khung (*framework*) AI đáng tin cậy (*Trustworthy AI*) thứ mà AI đem lại lợi ích tối đa cho con người và loại bỏ những mối nguy hiểm tiềm ẩn là tất yếu. Trong những mối nguy hại ấy thì bảo vệ riêng tư người dùng là vấn đề nhức nhối. Để giải quyết vấn đề trên, một phương pháp học an toàn và bảo vệ riêng tư nổi lên gần đây, được gọi là học liên kết (*Federated Learning*). Mặc dù ban đầu phương pháp huấn luyện này được thiết kế cho các bài toán học máy phạm vi lớn (*large-scale machine learning*), tuy nhiên nó dần được phát triển và cho thấy tiềm năng vô cùng lớn trong việc đưa ra các mô hình học sâu bảo vệ riêng tư người dùng, ví dụ trong phân tích dữ liệu y tế. Trong bài báo này, chúng tôi sẽ tóm tắt chi tiết lại các kỹ thuật hiện thực của học liên kết, bên cạnh đó chúng tôi cũng tìm hiểu và cụ thể những ứng dụng đã và đang triển khai của phương pháp học này trong lĩnh vực y học.

Từ khóa: Học liên kết, AI đáng tin cậy, riêng tư dữ liệu, phân tích dữ liệu y học.

1. MỞ ĐẦU

Hiện nay, quyền riêng tư và bảo mật dữ liệu đang là vấn đề đáng quan tâm đối với toàn người dân trên toàn cầu. Vào năm 2018, một cuộc điều tra của báo The Guardian và The New York Times đã tiết lộ rằng Facebook đã cho phép Cambridge Analytica, một công ty phân tích dữ liệu liên quan đến chiến dịch tranh cử của Tổng thống Mỹ Donald Trump, thu thập thông tin cá nhân của hàng triệu người dùng Facebook mà không có sự đồng ý của họ. Theo báo cáo, Cambridge Analytica đã sử dụng thông tin này để tạo ra các chiến dịch quảng cáo chính trị được tùy chỉnh, nhằm mục đích ảnh hưởng đến ý kiến cử tri trong bầu cử tổng thống Mỹ năm 2016. Cambridge Analytica đã thu thập thông tin cá nhân từ hơn 87 triệu tài khoản người dùng Facebook thông qua một ứng dụng được phát triển bởi Aleksandr Kogan, một nhà nghiên cứu tại Đại học Cambridge. Ứng dụng này được quảng cáo là một bài kiểm tra tính cách và đã được cung cấp cho người dùng miễn phí. Tuy nhiên, khi người dùng trả lời các câu hỏi trong bài kiểm tra tính cách, ứng dụng đã thu thập thông tin cá nhân của họ cùng với thông tin về bạn bè của họ trên Facebook. Sau khi thông tin này được tiết lộ, Facebook đã bị chỉ trích mạnh mẽ vì đã không đảm bảo an toàn cho thông tin cá nhân của người dùng. CEO của Facebook, Mark Zuckerberg, đã phải đối mặt với các phiên điều trần tại Quốc hội Hoa Kỳ và Quốc hội

Châu Âu để trả lời các câu hỏi liên quan đến việc bảo vệ quyền riêng tư của người dùng. Facebook đã phải trả phạt 5 tỷ USD cho Cơ quan Thương mại Liên bang Hoa Kỳ và đã thực hiện nhiều biện pháp để cung cấp bảo mật và bảo vệ quyền riêng tư của người dùng. Năm 2020, Ủy ban Tiêu chuẩn Truyền thông Liên bang Hoa Kỳ (Federal Trade Commission - FTC) đã mở một cuộc điều tra về việc TikTok, một ứng dụng mạng xã hội video đang ngày càng phổ biến, đã thu thập và sử dụng thông tin cá nhân của trẻ em một cách không đúng đắn. Ứng dụng TikTok đã được phát triển bởi ByteDance, một công ty công nghệ có trụ sở tại Trung Quốc. Theo các báo cáo, TikTok đã thu thập thông tin cá nhân của người dùng, bao gồm tên, địa chỉ email, số điện thoại, địa chỉ IP và vị trí địa lý, mà không có sự đồng ý của họ. TikTok cũng đã thu thập thông tin về hành vi sử dụng ứng dụng, chẳng hạn như video mà người dùng đã xem và thích. Ngoài ra, TikTok cũng bị chỉ trích vì đã thu thập thông tin cá nhân của trẻ em một cách không đúng đắn. FTC phát hiện ra rằng TikTok đã cho phép trẻ em dưới 13 tuổi sử dụng ứng dụng mà không có sự đồng ý của cha mẹ hoặc người giám hộ, mặc dù luật pháp Hoa Kỳ yêu cầu các công ty phải có sự đồng ý của cha mẹ trước khi thu thập thông tin cá nhân của trẻ em. FTC cũng phát hiện ra rằng TikTok đã thu thập thông tin cá nhân của trẻ em, bao gồm tên, địa chỉ email và vị trí địa lý, mà không có sự đồng ý của cha mẹ. Sau khi bị chỉ trích, TikTok đã đồng ý trả khoản tiền phạt 5,7 triệu USD cho FTC và đã thực hiện nhiều biện pháp để cung cấp bảo mật và bảo vệ quyền riêng tư của người dùng, bao gồm việc cho phép cha mẹ kiểm soát tài khoản của trẻ em và loại bỏ các tính năng không an toàn đối với trẻ em. Tuy nhiên, TikTok vẫn tiếp tục phải đối mặt với các chỉ trích liên quan đến việc bảo vệ quyền riêng tư của người dùng và quan hệ của nó với chính phủ Trung Quốc. Qua hai vụ việc kể trên có thể thấy việc bảo vệ quyền riêng tư của người dùng đang trở thành một vấn đề quan trọng và nó đang được đưa ra ánh sáng nhất là trong lĩnh vực công nghệ. Vụ Facebook và Cambridge Analytica cho thấy rằng việc thu thập thông tin cá nhân của người dùng trái phép có thể gây nguy hiểm đến quyền riêng tư của họ. Facebook đã phải chịu trách nhiệm về việc không bảo vệ được thông tin cá nhân của người dùng và đã phải chấp nhận các biện pháp kiểm soát mới để cung cấp bảo mật và bảo vệ quyền riêng tư của người dùng. Vụ TikTok cũng cho thấy rằng việc bảo vệ quyền riêng tư của trẻ em và người dùng nói chung đang trở thành một vấn đề ngày càng cấp thiết. TikTok đã phải trả một khoản tiền phạt lớn cho FTC và thực hiện nhiều biện pháp để cung cấp bảo mật và bảo vệ quyền riêng tư của người dùng. Nhìn chung, hai vụ việc này nhấn mạnh tầm quan trọng của việc bảo vệ quyền riêng tư của người dùng trong một thế giới ngày càng phụ thuộc vào công nghệ. Các công ty công nghệ cần phải có trách nhiệm và tiếp tục thực hiện các biện pháp để bảo vệ thông tin cá nhân của người dùng và đảm bảo rằng quyền riêng tư của họ được bảo vệ. Người dùng cũng cần phải thận trọng và tự bảo vệ thông tin cá nhân của mình, bằng cách kiểm tra các thiết lập bảo mật và không chia sẻ thông tin cá nhân của mình một cách không đáng tin cậy. Và để giải quyết vấn đề quyền riêng tư của người dùng trong các vụ việc trên, có thể áp dụng phương pháp Federated Learning. Phương pháp này cho phép dữ liệu được phân tán và được xử lý trên các thiết bị cục bộ của người dùng, mà không cần phải chuyển giao dữ liệu đến các trung tâm dữ liệu trung tâm. Điều này giúp giảm thiểu nguy cơ rò rỉ dữ liệu và cải thiện quyền riêng tư của người dùng.

Học máy (*Machine learning*) là một phương pháp tiên tiến trong lĩnh vực khoa học máy tính, trong đó máy tính được lập trình để học và tự điều chỉnh các mô hình dữ liệu để tìm ra các giải pháp tốt nhất cho các vấn đề cụ thể. Trong lĩnh vực smart cities và IoT (Internet of Things), phương pháp học máy có thể được áp dụng để phân tích, dự đoán và cải thiện các tiện ích công cộng và các hoạt động kinh doanh. Với việc sử dụng IoT và các thiết bị kết nối internet khác, smart cities có thể thu thập dữ liệu liên tục về các hoạt động và các điều kiện trong thành phố, bao gồm thông tin về giao thông, tiện ích, an ninh và môi trường. Dữ liệu này sau đó có thể được sử dụng để xây dựng các mô hình học máy để dự đoán và phân tích các vấn đề trong thành phố. Một số ví dụ về ứng dụng học máy trong smart cities và IoT bao gồm:

Dự đoán nhu cầu giao thông: Học máy có thể được sử dụng để dự đoán lưu lượng giao thông trên các con đường, từ đó giúp quản lý giao thông tốt hơn và cải thiện tính an toàn trên đường. Hay trong quản lý năng lượng, có thể được sử dụng để phân tích dữ liệu năng lượng tiêu thụ trong các tòa nhà, giúp cải thiện hiệu quả năng lượng và giảm thiểu lượng khí thải carbon. Và dự báo cháy rừng cũng có thể sử dụng học máy để phân tích dữ liệu môi trường và dự đoán nguy cơ cháy rừng, từ đó giúp các cơ quan chức năng có kế hoạch và đưa ra các biện pháp phòng ngừa hiệu quả. Tuy nhiên, để triển khai học máy trong smart cities và IoT, cần có các giải pháp để xử lý dữ liệu lớn và đảm bảo an toàn thông tin. Federated Learning (học liên kết) là một phương pháp học máy phân tán giúp giải quyết vấn đề này. Học liên kết là phương pháp học máy phân tán, nghĩa là mô hình được đào tạo trên các thiết bị địa phương (như các cảm biến IoT) mà không cần phải chuyển dữ liệu đến một trung tâm xử lý tập trung. Việc này giảm thiểu rủi ro cho việc lộ thông tin cá nhân và giảm thiểu tải cho các mạng truyền thông. Trong học liên kết, các mô hình học máy được đào tạo trên các thiết bị địa phương và sau đó được kết hợp lại để tạo ra một mô hình toàn cục. Việc này cho phép dữ liệu được giữ trong các thiết bị địa phương và chỉ truyền đi các thông tin được tóm tắt. Điều này giúp giảm thiểu rủi ro liên quan đến việc bị tấn công và lộ thông tin cá nhân. Vì vậy, học liên kết là một giải pháp hữu hiệu để triển khai học máy trong smart cities và IoT, đảm bảo xử lý dữ liệu lớn và an toàn thông tin cho người dùng. Tuy nhiên, để đảm bảo quyền riêng tư, các chính sách và quy định bảo mật dữ liệu cũng cần được áp dụng.

Trong một thành phố thông minh, các loại cảm biến Internet vạn vật (IoT) điện tử khác nhau được triển khai để thu thập dữ liệu (Mahmud et al., 2018) trong môi trường đô thị. Mặc dù kiến trúc Internet đô thị hiện tại rất phức tạp, nhưng những người ra quyết định có thể sử dụng thông tin chuyên sâu thu được từ những dữ liệu này để quản lý hiệu quả tài sản, tài nguyên và dịch vụ trong khu vực đô thị. Mô hình hoạt động của một thành phố thông minh liên quan đến việc sử dụng các cảm biến IoT để thu thập dữ liệu. Hơn nữa, nó có thể thực hiện các ứng dụng hiệu quả trong một loạt lĩnh vực, chẳng hạn như dịch vụ công cộng đô thị, phân bổ tài nguyên và thông tin liên lạc. Đồng thời, các thành phố thông minh đã cung cấp các giải pháp hiệu quả cho các vấn đề chính, chẳng hạn như sự phát triển của IoT (Li, Zhao, et al., 2020), chăm sóc y tế (Rath & Pattanayak, 2019), giao thông vận tải (Qiu et al., 2019) và truyền thông (Guan et al., 2018). Trong quá trình trao đổi thông tin quy mô lớn này, các cảm biến tạo ra một lượng lớn dữ liệu. Những dữ liệu này có ý nghĩa rất lớn trong việc cải thiện ứng dụng của một chương trình và giúp các nhà quản lý tối ưu hóa các quyết định của họ. Tuy nhiên, một tỷ lệ lớn dữ liệu nhạy cảm và liên quan đến thông tin cá nhân do người dùng tạo (Khan et al., 2019). Đầu tiên, chúng ta phải ngăn chặn việc đưa vào dữ liệu riêng tư của người dùng trong quá trình xử lý dữ liệu. Ngoài ra, các vấn đề liên quan đến mức sử dụng tài nguyên dữ liệu thấp và tắc nghẽn mạng (McMahan, Moore, et al., 2017) tồn tại trong quá trình tương tác dữ liệu.

Bảng 1. Một số khảo sát về quyền riêng tư dữ liệu y tế

Các cuộc khảo sát	Nội dung của các cuộc khảo sát	
	Mục đích	Kết quả
Accenture (2017)	<p>Cuộc khảo sát của Accenture năm 2017 có tên đầy đủ là "Leveraging the Power of the Patient: How Digital Technology is Transforming Health Systems". Mục đích của cuộc khảo sát này là tìm hiểu cách mà các công nghệ số và kỹ thuật số đang thay đổi cách thức cung cấp chăm sóc sức khỏe, từ việc xây dựng kết nối giữa bệnh nhân và nhà cung cấp dịch vụ y tế đến việc sử dụng dữ liệu y tế để cải thiện chất lượng chăm sóc và phát triển các phương pháp điều trị cá nhân hóa.</p> <p>Accenture (2017) đã thu thập ý kiến từ 8.000 người tiêu dùng ở 8 quốc gia trên thế giới, bao gồm Australia, Brazil, Canada, Đức, Anh, Singapore, Mỹ và Trung Quốc. Các câu hỏi trong cuộc khảo sát tập trung vào các chủ đề như: sự chấp nhận của người dân đối với sử dụng công nghệ số trong việc cung cấp chăm sóc sức khỏe; niềm tin của bệnh nhân vào các nhà cung cấp dịch vụ y tế và tổ chức y tế để bảo mật và bảo vệ dữ liệu y tế của họ; cách mà các công nghệ số có thể cải thiện quản lý bệnh lý và phát triển các phương pháp điều trị mới.</p>	<p>Khảo sát của Accenture năm 2017 đã khảo sát 2.000 người tiêu dùng ở Mỹ và Canada để tìm hiểu về quan điểm của họ về quyền riêng tư dữ liệu y tế. Dưới đây là một số kết quả chính của khảo sát:</p> <ul style="list-style-type: none"> 77% người dùng cho biết họ lo lắng về việc thông tin y tế của họ bị rò rỉ. 69% cho biết họ đã thấy thông tin y tế của mình được bán hoặc chia sẻ với các bên thứ ba mà họ không biết. 73% người dùng muốn có quyền kiểm soát rõ ràng hơn về việc ai có thể truy cập thông tin y tế của họ. 70% muốn biết chính xác những ai đã truy cập thông tin y tế của họ và vì lý do gì. 64% cho biết họ sẽ cân nhắc chuyển đổi sang một nhà cung cấp dịch vụ y tế khác nếu nhà cung cấp hiện tại của họ không đảm bảo được an ninh thông tin y tế.
Pew Research Center (2019)	<p>Khảo sát của Pew Research Center năm 2019 có tên đầy đủ là "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information". Đây là một nghiên cứu về quan điểm của người dân Hoa Kỳ về quyền riêng tư và bảo mật dữ liệu, bao gồm cả dữ liệu y tế.</p> <p>Khảo sát này đã khảo sát 4.272 người Mỹ từ 18 tuổi trở lên và đã tập trung vào việc thu thập các ý kiến về việc sử dụng dữ liệu cá nhân, các loại dịch vụ trực tuyến và ứng dụng, cũng như quyền riêng tư và bảo mật.</p>	<p>Khảo sát của Pew Research Center năm 2019 tập trung vào quan điểm của người Mỹ về việc chia sẻ thông tin y tế của họ với các bên thứ ba. Dưới đây là một số thông tin chi tiết về khảo sát này:</p> <ul style="list-style-type: none"> 58% người dùng cho biết họ đã chia sẻ thông tin y tế của mình với các bác sĩ hoặc nhà cung cấp dịch vụ y tế của họ. 37% cho biết họ đã chia sẻ thông tin y tế của mình với các ứng dụng y tế hoặc thiết bị đeo tay. 47% người dùng cho biết họ lo lắng về việc thông tin y tế của họ bị rò rỉ hoặc được sử dụng một cách không đúng đắn. 24% cho biết họ không biết liệu thông tin y tế của họ đã được bán hoặc chia sẻ với các bên thứ ba hay chưa.

Các cuộc khảo sát	Nội dung của các cuộc khảo sát	
	Mục đích	Kết quả
Ipsos (2020)	<p>Ipsos là một công ty nghiên cứu và tư vấn đa quốc gia có trụ sở chính tại Paris, Pháp. Ipsos cung cấp các dịch vụ nghiên cứu thị trường và xã hội cho khách hàng trên toàn thế giới, bao gồm khảo sát dư luận, đo lường hiệu quả quảng cáo, phân tích dữ liệu và nghiên cứu về sản phẩm và thương hiệu. Cuộc khảo sát về quyền riêng tư của dữ liệu y tế mà Ipsos tiến hành vào năm 2020 là một trong những dự án nghiên cứu của công ty trong lĩnh vực y tế.</p> <p>Mục đích của cuộc khảo sát này là để tìm hiểu quan điểm của người tiêu dùng ở Canada và Mỹ về quyền riêng tư và an ninh của dữ liệu y tế trong bối cảnh đại dịch COVID-19. Ngoài ra, Ipsos cũng muốn đưa ra những khuyến nghị để các tổ chức y tế có thể cải thiện quản lý thông tin cá nhân của bệnh nhân và tăng cường niềm tin của người dân về quyền riêng tư dữ liệu y tế.</p>	<p>62% muôn có quyền kiểm soát rõ ràng hơn về việc ai có thể truy cập thông tin y tế của họ.</p> <p>Cuộc khảo sát của Ipsos (2020) được thực hiện trên 1.000 người tiêu dùng ở Canada và Mỹ về quan điểm của họ về quyền riêng tư và an ninh của dữ liệu y tế trong bối cảnh đại dịch COVID-19. Sau đây là một số kết quả chính của cuộc khảo sát này:</p> <p>Đầu tiên, có khoảng 68% số người được hỏi cho biết họ lo lắng về việc thông tin y tế của mình có thể bị rò rỉ khi sử dụng các ứng dụng y tế trên điện thoại thông minh.</p> <p>Hai là, 60% số người được hỏi tin rằng các tổ chức y tế có nghĩa vụ bảo vệ thông tin cá nhân của bệnh nhân, và 51% cho rằng các tổ chức này đã làm đúng việc đó.</p> <p>Ba là, 57% số người được hỏi tin rằng họ có quyền yêu cầu các tổ chức y tế xóa thông tin cá nhân của họ, nhưng thực tế chỉ có 37% cho biết họ đã thực sự yêu cầu điều này.</p> <p>Và cuối cùng, có 69% số người được hỏi tin rằng họ đồng ý chia sẻ thông tin y tế của mình nếu như đó là cách để giúp các nhà nghiên cứu tìm ra phương pháp điều trị mới cho COVID-19.</p>

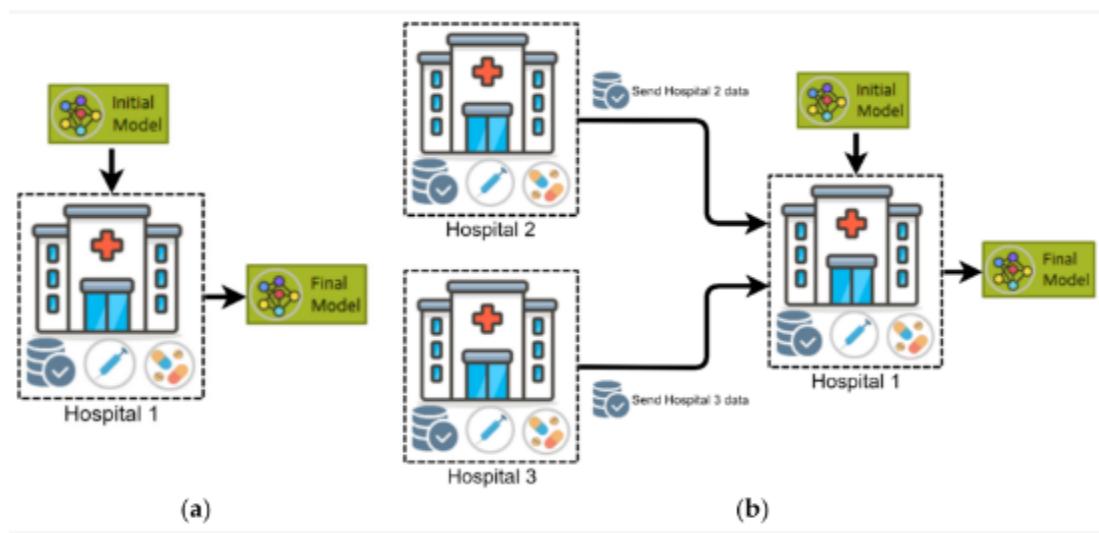
Từ các cuộc khảo sát về quyền riêng tư dữ liệu y tế, chúng ta có thể rút ra một số kết luận chính như sau: Đầu tiên, sự quan tâm của công chúng đối với quyền riêng tư dữ liệu y tế là rất cao và ngày càng tăng. Hai là, người dùng sẵn sàng chia sẻ dữ liệu y tế của mình nếu có lợi cho sức khỏe cá nhân và cộng đồng, nhưng họ đòi hỏi sự minh bạch và kiểm soát quyền riêng tư. Ba là, khả năng bảo vệ dữ liệu y tế chưa được đảm bảo đầy đủ và sự thiếu minh bạch của các tổ chức về cách thức thu thập, sử dụng và chia sẻ thông tin y tế cũng góp phần vào sự bất an của người dùng. Bốn là, việc tăng cường giáo dục và tăng cường quyền kiểm soát của người dùng đối với dữ liệu y tế là cần thiết để tăng cường sự tin tưởng của họ về hệ thống sử dụng dữ liệu y tế. Và cuối cùng cần có sự quản lý và điều tiết rõ ràng của các chính sách liên quan đến quyền riêng tư và bảo vệ dữ liệu y tế, từ phía cả nhà nước và các tổ chức tư nhân để đảm bảo an toàn và minh bạch cho người dùng.

Trong khuôn khổ học liên kết, người dùng có thể sử dụng dữ liệu mà không cần lấy thông tin cá nhân về những người tham gia khác. Dữ liệu liên quan được lưu trữ cục bộ (McMahan, Moore, et al., 2017). Người dùng định kỳ chia sẻ độ dốc mô hình cục bộ của họ với máy chủ điều phối trong một khoảng thời gian cụ thể. Máy chủ sắp xếp dữ liệu đào tạo và

đo lường sự đóng góp của tất cả những người tham gia (Smith, Forte, et al., 2017). Nó xây dựng một mô hình toàn cầu bằng cách lấy trung bình tất cả các gradient trong một mạng (Li et al., 2018) ở cấp độ máy chủ. Sau đó, máy chủ điều phối phân phối bản cập nhật mô hình mới cho tất cả các máy khách (Lim, Luong, et al., 2020). Mỗi máy khách tải mô hình cục bộ của nó lên máy chủ. Sau đó, người dùng tải xuống các mô hình cập nhật mới và sử dụng phân phối đám mây để thực hiện suy luận trên thiết bị của họ. Đây là nguyên lý hoạt động hoàn chỉnh của thuật toán học liên kết.

Học liên kết có ưu điểm là xử lý phân tán và bảo vệ quyền riêng tư hiệu quả. Một số thiết bị truyền thông phân tán phổ biến, chẳng hạn như điện thoại di động, có vấn đề về truyền thông tin liên lạc. Học liên kết đề xuất một phương pháp thích ứng miền liên kết dựa trên vấn đề chuyển miền. Mô hình này giải quyết vấn đề về tính riêng tư và hiệu quả của dữ liệu (Peng et al., 2019). Trong khi đó, một số học giả đã triển khai kiến trúc chuỗi khói học liên kết (BlockFL) có thể trao đổi và xác minh các cập nhật mô hình học tập cục bộ. Nó có thể mô tả tốc độ tạo khói tốt nhất bằng cách xem xét các vấn đề về độ trễ giao tiếp và đồng thuận (Kim et al., 2019). Nghiên cứu liên quan đến học liên kết đã được tiến hành trong các lĩnh vực IoT, truyền thông và dịch vụ công cộng. Những thực tiễn này thúc đẩy việc cập nhật và phát triển các ứng dụng trong thành phố thông minh.

Ứng dụng học liên kết trong y học sẽ trở thành bước tiến mới có thể giúp cải thiện chất lượng chăm sóc sức khỏe và giảm thiểu rủi ro về bảo mật dữ liệu y tế. Thí dụ, các bác sĩ và nhà sĩ có thể sử dụng phương pháp học liên kết để phân tích các hình ảnh X-quang, MRI và CT scan để chẩn đoán các bệnh lý. Đây là những ứng dụng tiềm năng cho việc sử dụng phương pháp này trong y học.



Hình 1. Minh họa mô hình học liên kết giữa các đơn vị

2. PHÂN LOẠI CÁC MÔ HÌNH HỌC LIÊN KẾT

2.1 Dựa trên phân bố dữ liệu

2.1.1 Học liên kết theo chiều ngang (Horizontal Federated Learning) [1]

Đây là phương pháp đào tạo mô hình học máy liên kết trên các tập dữ liệu có tính chất tương tự nhau nhưng phân tán trên các thiết bị khác nhau. Các tập dữ liệu này thường được thu thập từ các nguồn khác nhau nhưng có các đặc trưng chung. Trong học liên kết theo chiều ngang, các thiết bị sẽ thực hiện đào tạo mô hình trên các tập dữ liệu cục bộ, sau đó truyền lại các tham số được học cho mô hình toàn cục để cập nhật và cải thiện mô hình. H2C (Horizontal-to-Centralized) và H2B (Horizontal-to-Backbone) là hai phương pháp quan trọng trong mô hình học liên kết ngang. Dưới đây là bảng so sánh giữa H2C và H2B:

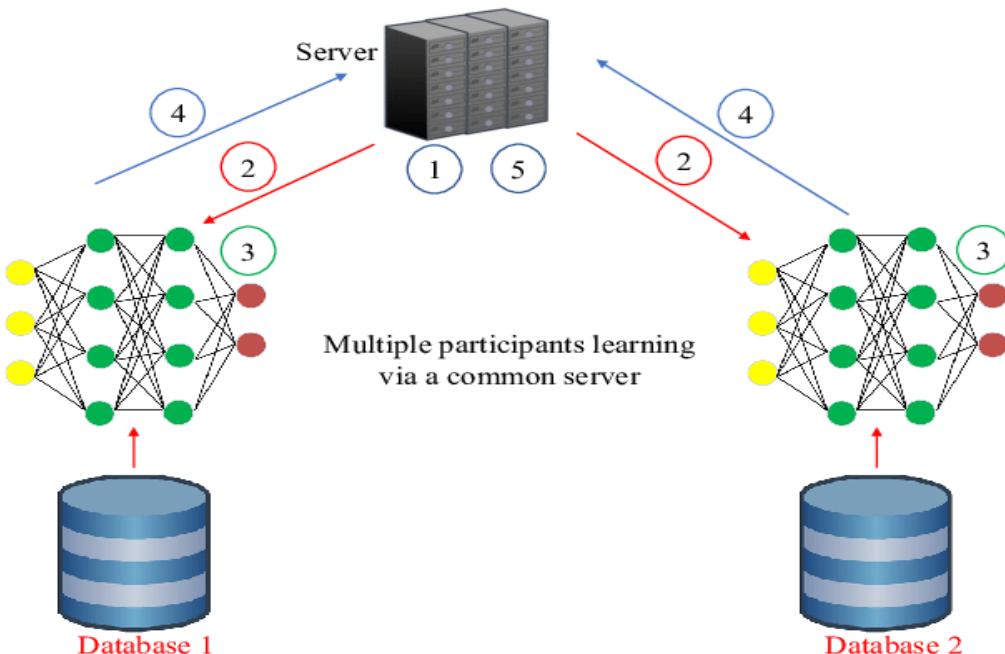
Bảng 2. Phân loại mô hình học liên kết theo chiều ngang

Tính chất	H2C	H2B
Phân loại	Ngang đến Tập trung	Ngang đến Spine
Dữ liệu	Phân tán và đồng nhất	Phân tán và khác nhau
Cấu trúc mô hình	Tập trung	Phân tán
Độ chính xác	Cao (vì sử dụng mô hình tập trung)	Thấp (vì sử dụng mô hình phân tán)
Hiệu quả tính toán	Thấp (vì phải truyền dữ liệu giữa các thiết bị)	Cao (vì không phải truyền dữ liệu giữa các thiết bị)
Tính bảo mật	Có thể đối mặt với các vấn đề liên quan đến bảo mật	Tốt hơn vì dữ liệu không phải chia sẻ giữa các thiết bị

Hai phương pháp này có tính chất khác nhau và phù hợp với các tính huống khác nhau. H2C phù hợp với các tình huống yêu cầu độ chính xác cao, nhưng có thể đối mặt với các vấn đề bảo mật. H2B thì hiệu quả tính toán cao hơn và bảo mật tốt hơn, nhưng độ chính xác thấp hơn do sử dụng mô hình phân tán. Tuy nhiên cũng có thể kết hợp cả H2C và H2B trong một mô hình học liên kết theo chiều ngang. Việc kết hợp cần được thực hiện cẩn thận để đảm bảo tính hiệu quả và an toàn của quá trình huấn luyện. Ví dụ, trong quá trình huấn luyện, H2C có thể được sử dụng để giảm thiểu số lần truyền thông giữa các thiết bị và tránh tình trạng quá tải trong quá trình huấn luyện. Trong khi đó, H2B có thể được sử dụng để cân bằng tập dữ liệu giữa các thiết bị, giúp tối ưu hóa quá trình huấn luyện và giảm thiểu tình trạng overfitting. Dù vậy cũng cần chú ý khi kết hợp H2C và H2B cũng có thể gây ra một số vấn đề liên quan đến bảo mật và riêng tư dữ liệu, ví dụ như tình trạng rò rỉ thông tin giữa các thiết bị trong quá trình truyền thông. Vì vậy, việc kết hợp H2C và H2B cần được thực hiện cẩn thận và đảm bảo tính an toàn và bảo mật của quá trình huấn luyện.

Tóm lại, học liên kết theo chiều ngang có ưu điểm là các tập dữ liệu không cần phải được gộp lại trước khi huấn luyện, điều này giúp giảm thiểu rủi ro mất mát thông tin và giảm bớt chi phí cho việc truyền tải dữ liệu. Tuy nhiên, học liên kết theo chiều ngang có thể đối mặt với các vấn đề liên quan đến sự bảo mật và riêng tư của dữ liệu do việc truyền tải thông tin giữa các thiết bị khác nhau trong quá trình huấn luyện mô hình. Cụ thể, khi truyền tải thông

tin, các dữ liệu cục bộ của mỗi thiết bị có thể bị lộ ra bên ngoài và dẫn đến việc tiết lộ thông tin riêng tư của người dùng. Bên cạnh đó, việc cập nhật tham số mô hình từ các thiết bị khác nhau cũng có thể làm giảm tính bảo mật của mô hình. Nếu các thiết bị tham gia vào quá trình huấn luyện không đáng tin cậy hoặc bị tấn công, thì những thông tin quan trọng về mô hình có thể bị tiết lộ. Do đó, để đảm bảo tính bảo mật và riêng tư của dữ liệu trong quá trình huấn luyện mô hình học liên kết theo chiều ngang, các phương pháp bảo mật dữ liệu như mã hóa, kỹ thuật đánh mờ dữ liệu (*data obfuscation*) hay sử dụng các thuật toán bảo mật (*secure multiparty computation*) có thể được áp dụng.



Hình 2. Hệ thống dựa trên phương pháp học liên kết theo chiều ngang [2]

2.1.2 Học liên kết theo chiều dọc (Vertical Federated Learning) [3]

Học liên kết theo chiều dọc là một phương pháp trong học liên kết, trong đó các bên hợp tác chia sẻ các đặc trưng (*feature*) của dữ liệu của họ thay vì chia sẻ dữ liệu hoàn chỉnh. Thay vì gửi toàn bộ dữ liệu, các bên hợp tác chỉ gửi các đặc trưng của dữ liệu của họ đến một bên trung tâm để huấn luyện mô hình. Các kỹ thuật mã hóa: Secure Aggregation (SA), Homomorphic Encryption (HE) và Function Secret Sharing (FSS) là 3 phương pháp chính trong học liên kết theo chiều dọc:

- Secure Aggregation (SA) [4]: Đây là phương pháp đầu tiên được giới thiệu cho học liên kết theo chiều dọc. SA sử dụng kỹ thuật mã hóa để đảm bảo tính riêng tư của dữ liệu, trong đó các thiết bị sẽ mã hóa dữ liệu của mình trước khi gửi đến máy chủ trung tâm để thực hiện phép tính trung bình. Sau đó, kết quả được giải mã và gửi lại cho các thiết bị.

- Homomorphic Encryption (HE) [5]: Là một phương pháp mã hóa được sử dụng trong học máy liên kết. HE cho phép tính toán trên dữ liệu được mã hóa mà không cần giải mã trước đó. Các thiết bị tham gia vào quá trình tính toán sẽ mã hóa dữ liệu của mình trước khi

gửi đến máy chủ trung tâm. Sau đó, các phép tính được thực hiện trên dữ liệu được mã hóa và kết quả được trả về các thiết bị để giải mã.

– Function Secret Sharing (FSS) [6]: Là một phương pháp mã hóa đa bên trong đó các thiết bị tham gia chia sẻ các hàm bí mật để tính toán trên dữ liệu của mình. Các thiết bị sẽ tạo ra các mảnh dữ liệu của mình và chia sẻ các hàm bí mật để tính toán trên các mảnh dữ liệu đó. Sau đó, các thiết bị gửi kết quả của mình đến máy chủ trung tâm để thực hiện phép toán tính trung bình.

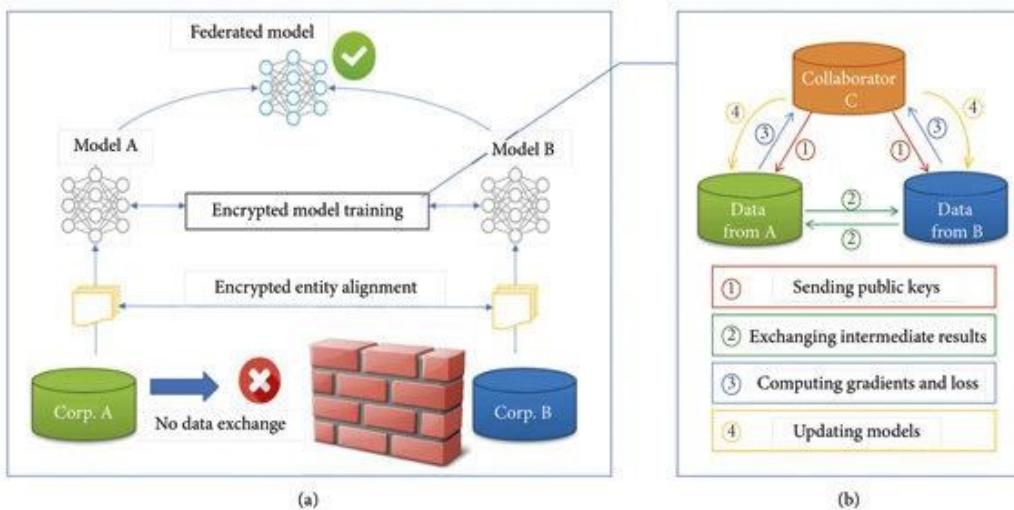
Các phương pháp này đều được sử dụng để giải quyết vấn đề bảo mật và riêng tư trong quá trình học liên kết theo chiều dọc. Và dưới đây là bảng so sánh ưu nhược điểm của ba phương pháp trên.

Bảng 3. So sánh ưu nhược điểm của từng loại phương pháp trong học liên kết theo chiều dọc

Phương pháp	Ưu điểm	Nhược điểm
SA	Tiết kiệm băng thông. Giảm thiểu thời gian đào tạo.	Không thể chia sẻ mô hình giữa các node không đồng bộ.
HE	Tính toán được ở các node phụ. Phân phối công việc hiệu quả hơn.	Có thể xuất hiện nhiễu khi các node phụ liên kết lại.
FSS	Tính toán được ở các node phụ. Phân phối công việc hiệu quả hơn.	Không hiệu quả khi các tập dữ liệu không đồng đều.

Các phương pháp trong mô hình học liên kết dọc đều có những ưu và nhược điểm riêng. SA là phương pháp tiết kiệm băng thông và giảm thiểu thời gian đào tạo, nhưng lại không thể chia sẻ mô hình giữa các node không đồng bộ. HE và FSS đều có tính toán được ở các node phụ và phân phối công việc hiệu quả hơn, tuy nhiên HE có thể xuất hiện nhiễu khi các node phụ liên kết lại và FSS không hiệu quả khi các tập dữ liệu không đồng đều. Do đó, việc lựa chọn phương pháp phù hợp sẽ phụ thuộc vào yêu cầu cụ thể của bài toán và điều kiện thực tế của môi trường triển khai.

Tuy nhiên cũng có thể kết hợp cả ba phương pháp SA, HE và FSS để tận dụng ưu điểm của từng phương pháp và giải quyết các vấn đề liên quan đến học liên kết theo chiều dọc. Ví dụ, có thể sử dụng HE để tính toán tại các node phụ và phân phối công việc hiệu quả hơn, sau đó sử dụng FSS để tối ưu hóa việc phân phối dữ liệu giữa các node và đảm bảo tính cân bằng giữa các tập dữ liệu. Sau đó, SA có thể được sử dụng để giảm thiểu băng thông và tối ưu hóa thời gian đào tạo trong quá trình giao tiếp giữa các node. Nhưng cần phải chú ý, việc kết hợp các phương pháp này cần được thực hiện một cách cẩn thận để tránh tình trạng mất mát dữ liệu hoặc nhiễu do quá trình truyền thông giữa các node.



Hình 3. Các kiến trúc hệ thống dựa trên học liên kết theo chiều dọc [7]

2.2. Dựa trên kiến trúc

2.2.1 Mô hình học liên kết đồng nhất (Homogeneous Federated Learning)

Homogeneous Federated Learning [8] là một phương pháp trong học máy phân tán, trong đó tất cả các thiết bị hoặc máy khách có cùng kiểu kiến trúc mô hình. Điều này có nghĩa là tất cả các thiết bị sử dụng cùng một thuật toán để đào tạo mô hình trên dữ liệu của chính nó và sau đó tải lên trung tâm để hợp nhất mô hình. Với học liên kết đồng nhất, các thiết bị được chia sẻ kiến thức và thông tin về mô hình thông qua quá trình học. Khi một thiết bị cập nhật mô hình của nó, nó sẽ truyền thông tin đến các thiết bị khác trong mạng, giúp cải thiện mô hình toàn cầu. Mô hình học liên kết đồng nhất thường được sử dụng trong các hệ thống phân tán nhỏ và có khả năng tính toán tương đương (FLOPs) [9] và giúp đơn giản hóa quá trình đào tạo và hợp nhất mô hình. Tuy nhiên, mô hình này có một số hạn chế như khả năng tùy chỉnh thấp và không phù hợp cho các hệ thống có độ phức tạp cao. Trong học liên kết với kiến trúc đồng nhất, công thức khả năng tính toán tương đương (FLOPs) được tính bằng cách nhân số lượng tham số của mô hình với số lần lặp lại của thuật toán. Công thức này có thể được biểu diễn như sau: FLOPs = Số lượng tham số x Số lần lặp lại. Trong đó, "số lượng tham số" là tổng số lượng tham số của tất cả các mô hình trong hệ thống học liên kết, và "số lần lặp lại" là số lần mà các mô hình được cập nhật với dữ liệu địa phương. Công thức này đo lường khả năng tính toán của hệ thống học liên kết đồng nhất, giúp đánh giá khả năng sử dụng của các thiết bị có khả năng tính toán hạn chế.

Trong học liên kết với kiến trúc đồng nhất, có hai dạng chính: Học liên kết đồng nhất truyền thống (*Traditional Homogeneous Federated Learning*) [10]: trong đó, các thiết bị nguồn được cấu hình hoàn toàn giống nhau về kiến trúc mô hình, số lượng tham số, hàm mất mát và thuật toán tối ưu. Dữ liệu đào tạo được phân chia và gửi đến tất cả các thiết bị nguồn để đào tạo mô hình. Sau đó, các mô hình được tổng hợp lại và phân phối trở lại các thiết bị nguồn để cập nhật tham số. Và học liên kết đồng nhất với mô hình tổng thể (*Federated*

Learning with Centralized Model) [11]: trong đó, một mô hình tổng thể được tạo ra bằng cách sử dụng tất cả dữ liệu từ tất cả các thiết bị nguồn. Mô hình tổng thể được cập nhật liên tục thông qua dữ liệu đào tạo được gửi từ các thiết bị nguồn. Sau đó, mô hình được phân phối lại để được triển khai trên các thiết bị nguồn. Dạng này có thể giảm thiểu số lượng giao tiếp giữa các thiết bị nguồn, tăng hiệu quả tính toán và cải thiện độ chính xác của mô hình.

Bảng 4. So sánh học Traditional Homogeneous Federated Learning và Federated Learning with Centralized Model

	Traditional Homogeneous Federated Learning	Federated Learning with Centralized Model
Mô tả	Mô hình đồng nhất, mỗi thiết bị tham gia đóng vai trò là một mô hình địa phương và tính toán được thực hiện trên các mô hình này.	Mô hình tập trung, dữ liệu được gửi về máy chủ tập trung, máy chủ tính toán và cập nhật mô hình, sau đó gửi lại các mô hình đã cập nhật đến các thiết bị.
Khả năng tính toán	Yêu cầu tính toán phức tạp trên các thiết bị địa phương.	Yêu cầu tính toán phức tạp trên máy chủ tập trung.
Số lượng truyền thông	Số lượng truyền thông lớn khi truyền các tham số cập nhật giữa các thiết bị.	Số lượng truyền thông lớn khi gửi dữ liệu đến máy chủ tập trung.
Hiệu suất	Tốc độ học tăng lên khi dữ liệu đa dạng và phân phối đồng đều.	Tốc độ học tăng lên khi dữ liệu tập trung và mẫu ngẫu nhiên.
Tính bảo mật	Tốt vì dữ liệu được giữ trên các thiết bị địa phương.	Yếu vì dữ liệu phải được gửi đến máy chủ tập trung.
Khả năng mở rộng	Khó khăn khi phải thêm thiết bị mới.	Dễ dàng thêm thiết bị mới do tính tập trung của mô hình.
Sự phụ thuộc	Không phụ thuộc vào một máy chủ tập trung.	Phụ thuộc vào máy chủ tập trung.

Như vậy, hai công thức có ưu điểm và nhược điểm riêng. Công thức Traditional Homogeneous Federated Learning không yêu cầu tính toán trung tâm nên giảm thiểu băng thông mạng và không gây tải cho máy chủ trung tâm. Tuy nhiên, nó có thể gặp vấn đề về đồng bộ hóa giữa các clients, do đó có thể dẫn đến hiệu suất thấp. Công thức Federated Learning with Centralized Model dễ dàng tính toán tham số trung tâm và đảm bảo tính đồng bộ giữa các clients. Tuy nhiên, nó yêu cầu phải có một máy chủ trung tâm để tính toán và lưu trữ tham số trung tâm, tăng chi phí và có thể gây tải cho máy chủ trung tâm. Do đó, việc lựa chọn công thức phù hợp phụ thuộc vào yêu cầu của ứng dụng cụ thể và các giới hạn về tài nguyên và băng thông của hệ thống.

2.1.2 Mô hình học liên kết không đồng nhất (Heterogeneous Federated Learning)

Mô hình học liên kết không đồng nhất (heterogeneous federated learning) là một mô hình học liên kết trong đó các thiết bị tham gia không có kiến trúc và năng lực tính toán đồng nhất. Các thiết bị tham gia có thể khác nhau về loại, kiểu, cấu hình, năng lực tính toán và dữ liệu. Mô hình này cho phép các thiết bị với năng lực tính toán và dữ liệu khác nhau đóng góp vào quá trình đào tạo mô hình chung. Mô hình học liên kết không đồng nhất được áp dụng rộng rãi trong các ứng dụng thực tế, đặc biệt là trong lĩnh vực y tế và công nghiệp. Nó giúp cho các tổ chức có thể đào tạo mô hình trên dữ liệu phân tán mà không cần phải tập trung dữ liệu về một điểm duy nhất, giúp bảo vệ tính riêng tư và an toàn của dữ liệu. Các phương pháp

thường được sử dụng trong mô hình học liên kết không đồng nhất bao gồm học có trợ giúp (assisted learning), học trực tiếp (direct learning), học chuyên giao (transfer learning), và học đa nhiệm (multi-task learning).

Bảng 5. So sánh assisted learning, direct learning, transfer learning và multi-task learning.

Phương pháp	Mô tả	Ưu điểm	Nhược điểm
Assisted learning	Mô hình học sử dụng một mô hình toàn cục được đào tạo trước đó và sử dụng dữ liệu từ các thiết bị địa phương để tinh chỉnh các thông số của mô hình toàn cục.	Được sử dụng để tối ưu hóa các mô hình trước đó. Giảm thiểu số lượng dữ liệu được truyền qua mạng.	Không thể sử dụng các dữ liệu cục bộ không thể truy cập được. Không thể phân tích độ chính xác của các mô hình địa phương.
Direct learning	Mô hình học tập trực tiếp sử dụng dữ liệu địa phương để đào tạo một mô hình phân tán.	Giảm thiểu số lượng dữ liệu được truyền qua mạng. Cho phép sử dụng dữ liệu cục bộ không thể truy cập được.	Không thể tận dụng được các thông tin cục bộ để cải thiện độ chính xác của mô hình. Đòi hỏi định dạng dữ liệu đồng nhất giữa các thiết bị.
Transfer learning	Mô hình học sử dụng các kiến thức và kinh nghiệm đã học được từ các nhiệm vụ trước đó để cải thiện độ chính xác của mô hình trên nhiệm vụ mới.	Giảm thiểu số lượng dữ liệu cần để đào tạo mô hình. Cải thiện độ chính xác của mô hình trên nhiệm vụ mới. Giảm thiểu thời gian và chi phí đào tạo mô hình.	Cần có các nhiệm vụ học liên quan đến nhau để chuyển giao kiến thức hiệu quả. Cần tinh chỉnh thủ công để cập nhật kiến thức chuyển giao.
Multi-task learning	Mô hình học sử dụng cùng một mô hình để giải quyết nhiều nhiệm vụ khác nhau đồng thời.	Cải thiện hiệu quả học tập của mô hình. Giảm thiểu độ phức tạp của mô hình so với việc huấn luyện nhiều mô hình cho từng nhiệm vụ riêng biệt.	Độ phức tạp của mô hình tăng lên do sự kết hợp của nhiều nhiệm vụ.

3. ỨNG DỤNG HỌC LIÊN KẾT TRONG Y HỌC

3.1. Phân tích ảnh y học

Trong lĩnh vực y học, phân tích ảnh y học là một lĩnh vực trong y học sử dụng các phương pháp hình ảnh để chẩn đoán và điều trị bệnh thông qua các hình ảnh như hình ảnh ung thư, tim mạch, não, phổi và nhiều hơn nữa. Ví dụ, trong hình ảnh ung thư, phân tích ảnh y học có thể được sử dụng để chẩn đoán ung thư, đánh giá kích thước của khối u, xác định vị trí của

khối u và theo dõi sự phát triển của khối u sau khi điều trị.. Việc phân tích này bao gồm các kỹ thuật học máy và trí tuệ nhân tạo để phân tích các hình ảnh y tế, kẽ cát tia X, siêu âm, MRI và CT. Tuy nhiên, phân tích ảnh y học đòi hỏi sự chính xác và độ tin cậy cao, do đó việc huấn luyện mô hình trên nhiều tập dữ liệu phải được thực hiện một cách thận trọng. Và học liên kết là phương pháp có thể được áp dụng để huấn luyện mô hình phân tích ảnh y học trên nhiều thiết bị y tế, mà không cần phải chuyển dữ liệu đến một trung tâm lưu trữ. Những thiết bị này có thể là các máy tính định vị, máy chụp X-quang, máy siêu âm, hoặc bất kỳ thiết bị y tế nào có khả năng thu thập dữ liệu hình ảnh y tế. Việc sử dụng phương pháp học liên kết trong phân tích ảnh y học cũng giúp cải thiện tốc độ huấn luyện mô hình và giảm thiểu sự gián đoạn trong dịch vụ chăm sóc sức khỏe. Bên cạnh đó, các dữ liệu được giữ bí mật và không cần phải được chuyển đến các trung tâm lưu trữ trung tâm, giúp bảo vệ quyền riêng tư của người dùng. Hơn nữa, những mô hình học máy được huấn luyện thông qua phương pháp học liên kết thường có độ chính xác và độ tin cậy cao, do được huấn luyện trên nhiều thiết bị khác nhau với các tập dữ liệu khác nhau.

Bảng 6. Một số bài báo, dự án ứng dụng phương pháp học liên kết trong phân tích ảnh.

Tên bài báo, dự án	Đối tượng nghiên cứu	Kết quả
Federated Learning for MRI-based Brain Tumor Segmentation [12] (2020)	Được công bố vào năm 2020 và có mục tiêu sử dụng phương pháp học liên kết để cải thiện độ chính xác của việc phân đoạn khối u não trên hình ảnh MRI. Dự án sử dụng dữ liệu từ 4 bệnh viện khác nhau trên toàn cầu để học tập và đưa ra các mô hình dự đoán chung. Dữ liệu bao gồm hơn 2000 hình ảnh MRI từ các bệnh nhân, được phân chia thành 5 loại khối u não khác nhau. Các kết quả cho thấy phương pháp học liên kết đạt độ chính xác cao hơn so với các phương pháp truyền thống, đồng thời bảo vệ sự riêng tư của dữ liệu bệnh nhân.	Dự án cho thấy rằng phương pháp học liên kết đã đạt được kết quả tốt trong việc phân đoạn khối u não từ hình ảnh MRI thông qua các số liệu sau: Độ chính xác (accuracy): 87.3%; Độ giống nhau giữa kết quả phân đoạn được dự đoán bởi mô hình trên dữ liệu liên kết và kết quả được dự đoán bởi mô hình trên dữ liệu tập trung (centralized model): 0.84; Thời gian huấn luyện cho một lần cập nhật trên dữ liệu liên kết (client): 2 phút; Tổng thời gian huấn luyện của mô hình: 22 giờ.
Federated Learning for COVID-19 Detection using Chest X-ray Images [13] (2020)	Đây là một dự án sử dụng phương pháp học liên kết để phát triển một hệ thống tự động phát hiện COVID-19 trên ảnh chụp X-quang ngực và được thực hiện bởi các nhà nghiên cứu của trường Đại học JNTUH College of Engineering Hyderabad ở Ấn Độ. Trong đó dự án đã được thực hiện trên tập dữ liệu ChestX-ray14 với tổng cộng 112,120 hình ảnh phổi từ 30,805 bệnh nhân khác nhau. Dự án này sử dụng mô hình mạng neuron tích chập (CNN) để phân loại hình ảnh phổi thành 3 loại: COVID-19, viêm phổi do virus khác (non-COVID viral pneumonia), và các trường hợp không có bất kỳ bệnh lý nào trên phổi (normal).	Kết quả dự án cho thấy rằng phương pháp học liên kết đã cải thiện đáng kể độ chính xác so với các phương pháp học truyền thống, đặc biệt là khi số lượng các bệnh viện cộng tác tăng lên. Khi sử dụng 50 bệnh viện cộng tác, độ chính xác của mô hình đã đạt được 96,78% trong việc phân loại COVID-19, 93,96% trong việc phân loại non-COVID viral pneumonia, và 94,27% trong việc phân loại hình ảnh bình thường.

Tên bài báo, dự án	Đối tượng nghiên cứu	Kết quả
Federated Learning for Lung Cancer Diagnosis [14] (2020)	<p>Được thực hiện vào năm 2020 bởi một nhóm các nhà nghiên cứu tại Đại học Stanford. Dự án này nhằm mục đích sử dụng phương pháp học liên kết để phân tích ảnh chụp X-quang phổi và xác định khói u phổi là ung thư hay không.</p> <p>Dữ liệu được sử dụng trong dự án này được thu thập từ 3 bệnh viện khác nhau và được phân phối trên các thiết bị khác nhau mà không cần truyền tải sang một trung tâm lưu trữ trung tâm. Tất cả các thiết bị đóng góp vào việc học liên kết bằng cách cung cấp thông tin của mình để xây dựng một mô hình học máy chung.</p>	Kết quả của dự án cho thấy rằng phương pháp học liên kết có thể cải thiện đáng kể kết quả chẩn đoán khói u phổi so với việc chỉ sử dụng một số lượng nhỏ các tập dữ liệu từ một bệnh viện duy nhất thông qua các số liệu cụ thể: độ chính xác đạt được của phương pháp học liên kết là 91,4%, so với độ chính xác của phương pháp truyền thống chỉ là 80,5%.
Federated Learning for Skin Lesion Classification [15] (2021)	<p>Đây là một nghiên cứu được thực hiện bởi các nhà khoa học tại Đại học Texas A&M và Đại học Tongji ở Trung Quốc với mục đích phát triển một phương pháp học máy liên kết cho việc phân loại các bệnh lý da từ các hình ảnh chụp da.</p> <p>Cụ thể, dữ liệu bao gồm hơn 10.000 hình ảnh chụp da từ nhiều nguồn khác nhau, trong đó có khoảng 7.000 hình ảnh được sử dụng để huấn luyện mô hình và khoảng 3.000 hình ảnh được sử dụng để đánh giá hiệu suất của mô hình. Các hình ảnh này bao gồm nhiều loại bệnh lý da, bao gồm ung thư da, tàn nhang, vảy nến và chàm.</p>	Kết quả cho thấy rằng, mô hình học liên kết đã đạt được độ chính xác cao trong việc phân loại các bệnh lý da, với độ chính xác trên 90% cho các bệnh lý da phổ biến như ung thư da, tàn nhang và vảy nến.

Thông qua một số thông tin của các dự án nêu trên cho thấy các dự án về phương pháp học liên kết trong phân tích ảnh y học đã đạt được những kết quả khả quan. Việc sử dụng phương pháp này đã giúp nâng cao độ chính xác và hiệu quả của việc phân tích ảnh y học mà không cần phải chia sẻ dữ liệu giữa các bên. Điều này giúp bảo vệ quyền riêng tư của bệnh nhân và tránh các rủi ro an ninh mạng. Các dự án sử dụng phương pháp học liên kết trong phân tích ảnh y học đều cho thấy được sự tiềm năng và hứa hẹn trong việc ứng dụng công nghệ mới để cải thiện chẩn đoán bệnh và điều trị. Tuy nhiên, để đạt được kết quả tốt nhất, việc lựa chọn và xử lý dữ liệu đầu vào, cùng với việc thiết lập mô hình học máy phù hợp và tối ưu, là rất quan trọng.

3.2. Dự đoán bệnh lý và điều trị

Học liên kết có thể được sử dụng trong dự đoán bệnh lý và điều trị bệnh nhân. Với sự phát triển của công nghệ, các thiết bị y tế thông minh như đồng hồ đeo tay thông minh, thiết bị đo sức khỏe, thiết bị y tế di động... đã trở thành phổ biến trong đời sống hàng ngày của con người. Các thiết bị này có thể thu thập dữ liệu về sức khỏe của người dùng, chẳng hạn như nhịp tim, huyết áp, lượng đường trong máu và các chỉ số khác. Phương pháp này cho phép các dữ liệu này được sử dụng để đào tạo mô hình dự đoán bệnh lý và điều trị trên nhiều thiết bị

mà không cần phải chuyển dữ liệu về một trung tâm. Điều này giúp giảm thiểu rủi ro bảo mật dữ liệu cá nhân của bệnh nhân. Ngoài ra, việc đào tạo mô hình trên các thiết bị cá nhân cũng giúp cải thiện hiệu suất mô hình, vì nó có thể học được từ các điều kiện cục bộ của từng thiết bị.

Bảng 7. Một số nghiên cứu phương pháp học liên kết trong dự đoán bệnh lý.

Tên nghiên cứu	Đối tượng nghiên cứu	Kết quả
Federated learning for predicting clinical outcomes in patients with chronic obstructive pulmonary disease [16] (2020)	Nghiên cứu này sử dụng phương pháp học liên kết federated learning để dự đoán kết quả lâm sàng cho bệnh nhân mắc bệnh phổi tắc nghẽn mạn tính (COPD) và được công bố trên tạp chí JAMA Network Open vào năm 2020. Dữ liệu bao gồm từ 16 bệnh viện ở Hoa Kỳ và Canada. Với việc sử dụng mô hình học liên kết federated learning, các nhà nghiên cứu đã huấn luyện một mô hình dự đoán kết quả lâm sàng dựa trên thông tin về tuổi, giới tính, chỉ số khó thở và mức độ nghiêm trọng của bệnh.	Kết quả của nghiên cứu cho thấy rằng phương pháp học liên kết có thể đạt được độ chính xác cao trong dự đoán kết quả lâm sàng của bệnh nhân COPD, vượt trội hơn so với các phương pháp học máy truyền thống. Ngoài ra, phương pháp học liên kết cũng cho thấy tính hiệu quả và tiềm năng trong việc bảo vệ sự riêng tư của dữ liệu y tế. Cụ thể, độ chính xác của phương pháp học liên kết (federated learning) trong dự đoán kết quả lâm sàng của bệnh nhân COPD là 0.84, cao hơn so với các phương pháp học máy truyền thống như Logistic Regression (0.72) và Support Vector Machine (0.74).
Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study [17] (2021)	Nghiên cứu được thực hiện bởi một nhóm các nhà nghiên cứu đến từ các trường đại học và tổ chức y tế khác nhau trên toàn thế giới. Mục đích là xây dựng một mô hình học sâu liên kết được đào tạo trên dữ liệu phát sinh từ nhiều quốc gia khác nhau, nhằm giúp định vị các dấu hiệu bất thường trên phổi do COVID-19 thông qua phân tích hình ảnh CT. Cụ thể, nghiên cứu sử dụng kỹ thuật học sâu liên kết (federated deep learning) để huấn luyện mô hình trên dữ liệu từ 16 trung tâm y tế thuộc 10 quốc gia khác nhau. Tất cả dữ liệu này đều được giữ bí mật và không được chia sẻ, chỉ có các tham số mô hình mới được gửi về trung tâm huấn luyện để được cập nhật.	Kết quả của nghiên cứu cho thấy phương pháp học liên kết đạt được độ chính xác cao (90,5%) và độ nhạy cao (92,3%) trong việc phát hiện bất thường phổi do COVID-19 trên hình ảnh CT. Đặc biệt, phương pháp này còn giúp bảo vệ tính riêng tư của dữ liệu và giảm thiểu sự kiểm soát trên dữ liệu của bệnh nhân giữa các địa điểm khác nhau.

Thông qua các nghiên cứu đã chứng minh rằng học liên kết có thể áp dụng trong nhiều lĩnh vực khác nhau của y tế như dự đoán bệnh lý phổi mạn tính, phân loại mật độ tuyến vú, dự đoán bệnh tâm thần từ hồ sơ y tế điện tử và phát hiện các dấu hiệu bất thường của bệnh COVID-19 trên ảnh chụp CT đồng thời cũng giúp tăng tính riêng tư và bảo mật trong việc phân tích và dự đoán bệnh lý từ các dữ liệu y tế, đồng thời cũng cải thiện độ chính xác và hiệu suất của các mô hình học. Tuy nhiên, việc áp dụng phương pháp học trong y tế còn đối mặt với một số

thách thức như độ chính xác của mô hình phụ thuộc vào chất lượng dữ liệu từ các trung tâm khác nhau, và sự khác biệt trong cấu trúc dữ liệu của các trung tâm có thể ảnh hưởng đến tính đồng nhất của dữ liệu. Nhưng thông qua những kết quả từ các nghiên cứu này đã cung cấp thông tin quý giá và định hướng cho việc áp dụng học liên kết trong y tế trong tương lai.

3.3. Quản lý dữ liệu y tế

Học liên kết là một công nghệ hứa hẹn trong việc quản lý dữ liệu y tế. Với học liên kết, các bộ phận y tế có thể chia sẻ dữ liệu của mình mà không cần phải tiết lộ dữ liệu bệnh nhân đến bên thứ ba. Các bộ phận y tế có thể hợp tác để tạo ra các mô hình dự đoán bệnh lý chung, mà không cần phải tiết lộ dữ liệu bệnh nhân của mình cho các bên khác. Việc sử dụng học liên kết trong quản lý dữ liệu y tế cũng giúp giảm thiểu rủi ro liên quan đến việc tiết lộ thông tin bệnh nhân. Các bộ phận y tế có thể duy trì quyền kiểm soát dữ liệu của họ, và chỉ cung cấp phần nào của dữ liệu cần thiết cho mô hình học máy. Điều này giúp giảm thiểu nguy cơ vi phạm quyền riêng tư và bảo vệ thông tin cá nhân của bệnh nhân. Tuy nhiên, cũng có một số thách thức khi sử dụng federated learning trong quản lý dữ liệu y tế. Đầu tiên, cần có sự đồng ý và hợp tác giữa các bộ phận y tế để chia sẻ dữ liệu. Thứ hai, việc xử lý dữ liệu phân tán và không đồng nhất có thể làm cho quá trình huấn luyện mô hình trở nên khó khăn hơn. Cuối cùng, cần phải đảm bảo tính an toàn và bảo mật của dữ liệu trong quá trình chia sẻ và huấn luyện mô hình.

3.4. Những thử thách và giải pháp khả thi:

Học liên kết là một công nghệ hứa hẹn trong lĩnh vực y tế, giúp tăng cường bảo mật dữ liệu và đảm bảo sự riêng tư của bệnh nhân. Tuy nhiên, việc áp dụng học liên kết trong y tế cũng đặt ra nhiều thách thức. Một trong những thách thức lớn nhất là sự đa dạng về định dạng dữ liệu, loại bệnh, và thực hành lâm sàng giữa các tổ chức y tế khác nhau, dẫn đến việc khó khăn trong việc đồng bộ dữ liệu và xây dựng mô hình học máy. Ngoài ra, còn có thách thức về độ tin cậy của dữ liệu, đặc biệt là khi có sự sai sót hoặc dữ liệu bị thiếu sót.

Để giải quyết các thách thức này, có một số giải pháp khả thi đang được đưa ra. Để đối phó với sự đa dạng của dữ liệu, các nhà nghiên cứu đang phát triển các kỹ thuật để chuyển đổi và tiêu chuẩn hóa dữ liệu trước khi xử lý. Để đảm bảo độ tin cậy của dữ liệu, các thuật toán và phương pháp kiểm tra dữ liệu đang được phát triển để phát hiện và xử lý các lỗi trong dữ liệu. Ngoài ra, việc tạo ra các chuẩn dữ liệu và quy trình hợp nhất có thể giúp tăng tính đồng bộ và cải thiện khả năng phân tích dữ liệu.

Trong tổng thể, học liên kết có thể cung cấp các giải pháp tiên tiến để phân tích dữ liệu y tế một cách bảo mật và đảm bảo sự riêng tư của bệnh nhân. Tuy nhiên, cần phải tìm ra các giải pháp để giải quyết các thách thức đang tồn tại và đảm bảo rằng việc sử dụng học liên kết sẽ mang lại lợi ích thực sự cho cộng đồng y tế.

4. KẾT LUẬN

Tổng hợp lại, mặc dù học liên kết vẫn còn là phương pháp học sơ khai nhưng việc ứng dụng của phương pháp này trong lĩnh vực y học mang lại nhiều lợi ích và tiềm năng lớn trong việc cải thiện chăm sóc sức khỏe của bệnh nhân. Thay vì phải chia sẻ dữ liệu nhạy cảm của

bệnh nhân, học liên kết cho phép các tổ chức y tế và nhà nghiên cứu có thể hợp tác trong việc xây dựng các mô hình dự đoán chính xác và hiệu quả mà không cần phải tiết lộ thông tin cá nhân của bệnh nhân. Ngoài ra, việc sử dụng học liên kết còn giúp giảm thiểu tình trạng overfitting, nâng cao tính khả thi của mô hình và giảm thiểu độ phức tạp của quá trình xử lý dữ liệu. Tuy nhiên, việc triển khai học liên kết cũng đặt ra một số thách thức như tính bảo mật của dữ liệu, tính ổn định của kết nối mạng và khả năng đồng bộ hóa giữa các bộ dữ liệu khác nhau. Nhưng với sự tiến bộ của công nghệ và sự hợp tác của các tổ chức y tế, học liên kết có thể trở thành một công cụ hữu ích trong lĩnh vực y học và góp phần nâng cao chất lượng chăm sóc sức khỏe của bệnh nhân.

TÀI LIỆU THAM KHẢO

1. Wei, S., Tong, Y., Zhou, Z., Song, T.- Efficient and Fair Data Valuation for Horizontal Federated Learning. In: Federated Learning. Lecture Notes in Computer Science(), vol 12500. Springer, Cham.
2. Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” ACM Transactions on Intelligent Systems and Technology, 10.(2), pp. 12:1–12:19, January 2019.
3. Yang Liu, Yan Kang, Tianyuan Zou, Yanhong Pu, Yuanqin He, Xiaozhou Ye, Ye Ouyang, Ya-Qin Zhang, Qiang Yang, Vertical Federated Learning, online (2022).
4. Practical Secure Aggregation for Federated Learning on User-Held Data, K. A. Bonawitz Vladimir Ivanov Ben Kreuter Antonio Marcedone H. Brendan McMahan Sarvar Patel Daniel Ramage Aaron Segal Karn Seth NIPS Workshop on Private Multi-Party Machine Learning (2016).
5. Hall, R.; Fienberg, S.E.; Nardi, Y. Secure multiple linear regression based on homomorphic encryption. J. Off. Stat. 2011, 27, 669.
6. Function Secret Sharing, Boyle, E., Gilboa, N., Ishai, Y. (2015). Function Secret Sharing. In: Oswald, E., Fischlin, M. (eds) Advances in Cryptology - EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science(), vol 9057. Springer, Berlin, Heidelberg.
7. Q. Yang, Y. Liu, T. J. Chen, and Y. Tong, “Federated machinelearning: concept and applications,” ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.
8. Homogeneous Federated Learning, Fuxun Yu, Weishan Zhang, Zhuwei Qin, Zirui Xu, Di Wang, Chenchen Liu, Zhi Tian, Xiang Chen, online (2022).
9. HeteroFL: Computation and Communication Efficient Federated Learning for Heterogeneous Clients, Enmao Diao, Jie Ding, Vahid Tarokh, online (2021)..
10. Towards Flexible Device Participation in Federated Learning, Yichen Ruan, Xiaoxi Zhang, Shu-Che Liang, Carlee Joe-Wong Proceedings of The 24th International Conference on Artificial Intelligence and Statistics, PMLR 130:3403-3411, 2021.
11. Federated Learning for Healthcare Informatics, Jie Xu, Benjamin S. Glicksberg, Chang Su, Peter Walker, Jiang Bian & Fei Wang Journal of Healthcare Informatics Research volume 5, pages 1–19 (2021).
12. Dimitris Stripelis, Hamza Saleem, Tanmay Ghai, Nikhil Dhinagar, Umang Gupta, Chrysovalantis Anastasiou, Greg Ver Steeg, Srivatsan Ravi, Muhammad Naveed, Paul M. Thompson, and Jose Luis Ambite, Secure neuroimaging analysis using federated

- learning with homomorphic encryption, Proc. SPIE 12088, 17th International Symposium on Medical Information Processing and Analysis, vol 1208814 (2021).
13. Ines Feki, Sourour Ammar, Yousri Kessentini, Khan Muhammad, Federated learning for COVID-19 screening from Chest X-ray images. Appl. Soft Comput. 106: 107330 (2021).
 14. Deist, T.M., et al., Distributed learning on 20 000+ lung cancer patients-the personal health train. Radiother. Oncol. 144, 189–200 (2020).
 15. Jeffry Wicaksana, Zengqiang Yan, Xin Yang, Yang Liu, Lixin Fan, Kwang-Ting Cheng, Customized Federated Learning for Multi-Source Decentralized Medical Image Classification, IEEE J. Biomed. Health Informatics 26(11), 5596-5607 (2022).
 16. Estiri, H. et al. Predicting COVID-19 mortality with electronic medical records. NPJ Dig. Med. 4, 15 (2021).
 17. Qi Dou, Tiffany Y. So, Meirui Jiang, Quande Liu, Varut Vardhanabhuti, Georgios Kaassis, Zeju Li, Weixin Si, Heather H. C. Lee, Kevin Yu, Zuxin Feng, Li Dong, Egon Burian, Friederike Jungmann, Rickmer Braren, Marcus R. Makowski, Bernhard Kainz, Daniel Rueckert, Ben Glocker, Simon C. H. Yu, Pheng-Ann Heng, Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study. npj Digit. Medicine 4 (2021).

ABSTRACT

FEDERATED LEARNING AND ITS POTENTIALS FOR APPLICATIONS IN MEDICAL FIELD: AN OVERVIEW

Phat T. Tran-Truong^{1,2}, Tran Khanh Dang^{1,*}, Thanh-Thao T. Nguyen¹

¹*Ho Chi Minh University of Food Industry*

²*University of Technology, Vietnam National University - Ho Chi Minh*

*Email: khanh@hufi.edu.vn

In the trend of applying technology nowadays, the demand for protecting individuals' data privacy is increasing. Every day, we use many online services and mobile applications to store personal information, including a considerable amount of private data, the impact of which can be immeasurable if not handled properly. Technologies based on Artificial Intelligence (AI) - considered as the main pillar of the fourth industrial revolution - are not an exception. The challenge of building a trustworthy AI framework that maximizes the benefits for humans and eliminates potential dangers is essential. Among those risks, user privacy protection is a pressing issue. To address this problem, a safe and privacy-protective learning method, called Federated Learning, has emerged recently. Although this training method was initially designed for large-scale machine learning problems, it has gradually been developed and shown great potential in providing privacy-preserving deep learning models, for example, in medical data analysis. In this article, we will summarize the implementation details of Federated Learning techniques and explore the specific applications that have been and are being developed using this learning method in the field of healthcare.

Keywords: Federated Learning, Trustworthy AI, Data privacy, Medical data analysis.

TÌM HIỂU MÔ HÌNH GPT VÀ ÚNG DỤNG GPT PHỤC VỤ CHO HỌC TẬP VÀ NGHIÊN CỨU Ở SINH VIÊN

Đinh Huy Hoàng^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: hoangdh@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Từ khi ra mắt sản phẩm thương mại đầu tiên của OpenAI - API OpenAI, hơn 300 ứng dụng hiện đang sử dụng GPT-3 và hàng chục nghìn nhà phát triển trên toàn cầu đang xây dựng trên nền tảng của API. Ứng dụng ChatGPT là một ứng dụng đang được quan tâm rất nhiều trên internet, ChatGPT có thể cung cấp cho sinh viên các kiến thức tổng quát trong nhiều lĩnh vực khác nhau. ChatGPT được xây dựng là công cụ hỗ trợ học tập nên để hiểu bản chất vấn đề sinh viên cần tham khảo từ các nguồn tài liệu khác và kiến thức chuyên môn từ giáo viên hướng dẫn. Người dùng và sinh viên sẽ khai thác tiềm năng to lớn của AI như thế nào để phục vụ cho học tập và nghiên cứu. Nghiên cứu này nói về tổng quan mô hình GPT, hướng dẫn người dùng tạo một AI bằng GPT, các sai lầm khi sử dụng ChatGPT.

Từ khóa: OpenAI, ChatGPT, GPT

1. TỔNG QUAN VỀ CÁC GIAI ĐOẠN PHÁT TRIỂN MÔ HÌNH GPT, VÀ ÚNG DỤNG CHATGPT

1.1 Các giai đoạn phát triển của mô hình GPT

GPT: GPT (Generative Pre-trained Transformer) là phiên bản đầu tiên trong dòng mô hình ngôn ngữ của OpenAI. GPT được giới thiệu lần đầu vào năm 2018 và đã thể hiện khả năng tạo ra văn bản tự nhiên xuất sắc thông qua việc huấn luyện trên một lượng lớn dữ liệu từ các trang web.

GPT-2: là phiên bản tiếp theo của GPT, ra mắt vào năm 2019. GPT-2 có khả năng phân tích các dữ liệu có kích thước lớn hơn GPT và được huấn luyện trên một tập dữ liệu đa dạng hơn, bao gồm cả các trang web, sách và báo chí. Nó đạt được tiến bộ đáng kể trong khả năng tạo ra văn bản tự nhiên và có thể thực hiện nhiều tác vụ như tạo câu chuyện, viết bài văn và trả lời câu hỏi.

GPT-3: được giới thiệu vào năm 2020 và được coi là một bước tiến quan trọng trong lĩnh vực xử lý ngôn ngữ tự nhiên. Với hơn 175 tỷ tham số, GPT-3 là một trong những mô hình ngôn ngữ tự động lớn nhất và mạnh nhất hiện nay. Nó có khả năng tạo ra văn bản chất lượng cao, đáp ứng các câu hỏi, thực hiện nhiều tác vụ và tham gia vào cuộc trò chuyện tự nhiên.

ChatGPT: là một biến thể của GPT-3, được huấn luyện đặc biệt để tương tác với con người qua văn bản. Điểm khác biệt chính của ChatGPT là khả năng tham gia vào cuộc trò chuyện theo dạng đoạn hội thoại, cung cấp phản hồi liên tục và tự nhiên. ChatGPT có thể hỗ trợ trong nhiều lĩnh vực như dịch vụ khách hàng, trợ giúp học tập và trò chuyện trực tuyến.

GPT-4 là một mô hình đa phương thức lớn (chấp nhận đầu vào hình ảnh và văn bản video), mặc dù kém khả năng hơn con người trong nhiều tình huống trong thế giới thực, nhưng

lại thể hiện khả năng vượt trội so với con người trên nhiều tiêu chuẩn chuyên môn và học thuật.

1.2 Tính ưu việt của GPT3

Kích thước lớn hơn: GPT-3 có kích thước lớn hơn nhiều so với GPT-2. Với hơn 175 tỷ tham số, GPT-3 là một trong những mô hình ngôn ngữ tự động lớn nhất và mạnh nhất hiện nay. Điều này cho phép nó có khả năng tạo ra văn bản phong phú và tự nhiên hơn.

Khả năng tương tác: GPT-3 được thiết kế đặc biệt để tương tác với con người thông qua văn bản. Nó có khả năng tham gia vào cuộc trò chuyện theo dạng đoạn hội thoại, đưa ra phản hồi liên tục và tự nhiên. Điều này làm cho GPT-3 trở thành một lựa chọn hữu ích trong các ứng dụng chatbot và hỗ trợ khách hàng trực tuyến.

Đa dạng nhiệm vụ: GPT-3 có khả năng thực hiện nhiều nhiệm vụ khác nhau. Nó có thể trả lời câu hỏi, tạo ra văn bản, dịch thuật, soạn thảo email và thậm chí tạo ra nội dung trò chơi. Điều này mở ra nhiều ứng dụng tiềm năng cho GPT-3 trong nhiều lĩnh vực khác nhau.

Mạnh mẽ hơn trong việc hiểu nghĩa các bài viết dài: GPT-3 có khả năng hiểu và tạo ra các đoạn văn bản dài hơn so với GPT-2. Điều này giúp nó có thể phân tích và tạo ra những phản hồi tự nhiên và logic hơn trong các cuộc trò chuyện hoặc công việc tương tác dựa trên văn bản.

1.3 Ứng dụng ChatGPT

ChatGPT là một mô hình xử lý ngôn ngữ tự nhiên (NLP) với khả năng đọc, hiểu và tạo ra văn bản tự động. ChatGPT sử dụng mạng nơ-ron biến đổi (transformer) để xử lý thông tin và tìm kiếm câu trả lời từ dữ liệu được cung cấp cho nó. Với khả năng học tập liên tục và cải tiến sau mỗi lần sử dụng, ChatGPT có thể cung cấp những câu trả lời chính xác và chi tiết cho các câu hỏi của người sử dụng.

ChatGPT sử dụng một mô hình xử lý ngôn ngữ tự nhiên (NLP) để phân tích câu hỏi của người dùng và tìm ra câu trả lời phù hợp nhất. Quá trình phân tích bao gồm các bước sau:

Tách từ: ChatGPT sẽ dùng công cụ tách từ để chia các câu truy vấn thành các từ riêng lẻ để có thể xử lý dễ dàng hơn.

Đánh giá ý nghĩa của từng từ: Sau khi tách từ, ChatGPT sẽ đánh giá ý nghĩa của từng từ trong câu hỏi. Nó sẽ áp dụng các kỹ thuật xử lý ngôn ngữ tự nhiên để phát hiện các từ khóa quan trọng trong câu hỏi.

Hiểu cấu trúc câu hỏi: ChatGPT sẽ phân tích cấu trúc của câu hỏi để hiểu xem câu hỏi muốn biết điều gì. Điều này bao gồm việc phân tích các phép so sánh, các từ chỉ định, các trạng từ...

Tìm kiếm câu trả lời: Dựa vào thông tin đã phân tích được từ câu hỏi, ChatGPT sẽ tìm kiếm các câu trả lời phù hợp nhất trong cơ sở dữ liệu của mình.

Từ các bước trên, ChatGPT có thể phân tích và hiểu được ý nghĩa của câu hỏi của người dùng để đưa ra câu trả lời chính xác và thông minh nhất.

1.4 Kiểm tra, đánh giá khả năng của GPT4

Hiện nay, mô hình GPT4 đã được nghiên cứu và đưa vào thử nghiệm. Để kiểm tra tính năng hỗ trợ học tập, mô hình GPT4 đã được OpenAI thử nghiệm qua các kỳ thi truyền thống.

Simulated exams	GPT-4 estimated percentile	GPT-4 (no vision) estimated percentile	GPT-3.5 estimated percentile
Uniform Bar Exam (MBE+MEE+MPT) ¹	298/400 ~90th	298/400 ~90th	213/400 ~10th
LSAT	163 ~88th	161 ~83rd	149 ~40th
SAT Evidence-Based Reading & Writing	710/800 ~90th	710/800 ~90th	670/800 ~70th
SAT Math	700/800 ~89th	690/800 ~89th	590/800 ~70th
Graduate Record Examination (GRE) Quantitative	163/170 ~90th	157/170 ~62nd	147/170 ~25th
Graduate Record Examination (GRE) Verbal	169/170 ~99th	165/170 ~96th	154/170 ~63rd
Graduate Record Examination (GRE) Writing	4/6 ~54th	4/6 ~54th	4/6 ~54th
USABO Semifinal Exam 2020	87/150 99th–100th	87/150 99th–100th	43/150 5th–33rd
USNCO Local Section Exam 2022	36/60	38/60	24/60
Medical Knowledge Self-Assessment Program	75%	75%	53%
Codeforces Rating	392 below 8th	392 below 8th	260 below 8th
AP Art History	5 66th–100th	5 66th–100th	5 66th–100th
AP Biology	5 65th–100th	5 65th–100th	4 60th–85th
AP Calculus BC	4 43rd–59th	4 45th–59th	1 6th–7th

Hình 1. Thử nghiệm mô hình GPT trên các bài thi tiêu chuẩn [1]

Ngoài ra, OpenAI đã tiến hành kiểm tra GPT4 trên các khía cạnh xã hội và đạt được kết quả khả quan so với mô hình GPT3 trước đó

Benchmark	GPT-4 Evaluated few-shot	GPT-3.5 Evaluated few-shot	LM SOTA	SOTA
MMLU Multiple-choice questions in 57 subjects (professional & academic)	86.4% 5-shot	70.0% 5-shot	70.7% 5-shot U-PaLM	75.2% 5-shot PaLM+PaLM
HellaSwag Commonsense reasoning around everyday events	95.3% 10-shot	85.5% 10-shot	84.2% LLAMA (validation set)	85.6% ALiM
AI2 Reasoning Challenge (ARC) Grade school multiple choice science questions: Challenge-set	96.3% 25-shot	85.2% 25-shot	84.2% 5-shot PaLM	85.6% ST-MOE
Winogrande Commonsense reasoning around pronoun resolution	87.5% 5-shot	81.6% 5-shot	84.2% 5-shot PaLM	85.6% 5-shot PaLM
HumanEval Python coding tasks	67.0% 0-shot	48.1% 0-shot	26.2% 0-shot PaLM	65.8% CodeT + GPT-3.5
DROP (f1 score) Reading comprehension & arithmetic	80.9 5-shot	64.1 5-shot	70.8 1-shot PaLM	88.4 CoGAT

Hình 2. Kiểm tra trên các khía cạnh xã hội [1]

Kết quả thu được qua các bài kiểm tra cho chúng ta thấy GPT4 có trí tuệ và khả năng xã hội đã gần với trí tuệ của con người. Điều này mang lại nhiều tiềm năng lợi ích nhưng cũng nhiều nguy hại đối với đạo đức xã hội.

1.5 Tiềm năng của GPT4

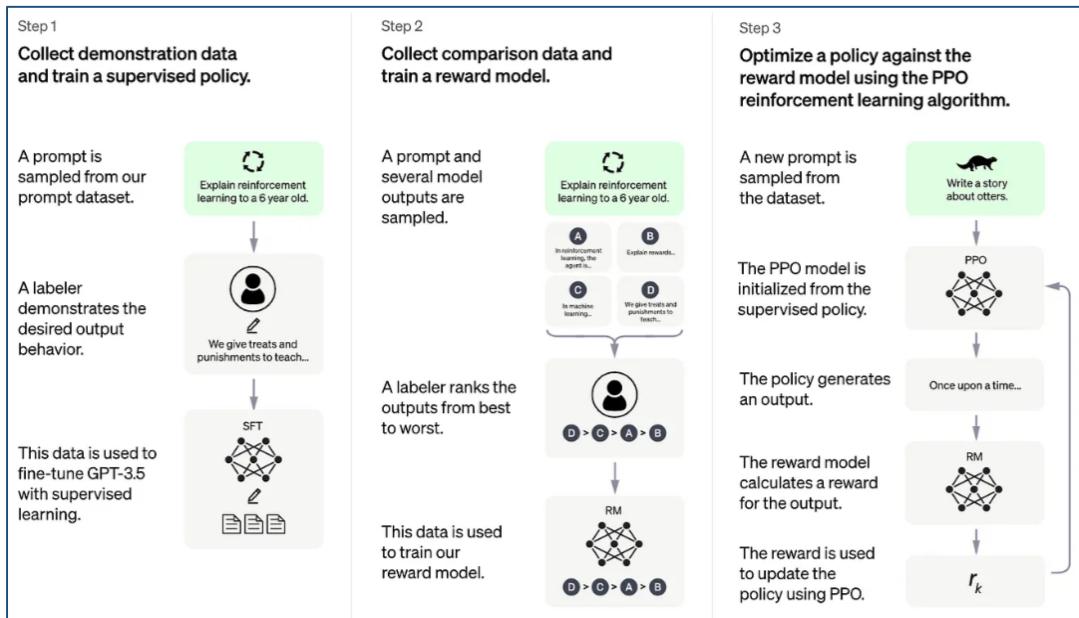
Với các thành công của GPT3, GPT4 đang được phát triển với tiềm năng mạnh mẽ hơn các phiên bản trước đó, đưa ra các tiềm năng ứng dụng cao hơn cho người dùng. Song song đó GPT-4 tồn tại những hạn chế tương tự như các mô hình GPT trước đó. GPT 4 được hỗ trợ tốt cho các kiến thức tổng quát và kiến thức chuyên sâu. OpenAI đã có can thiệp vào quá trình giao tiếp của mô hình để tránh phản hồi các kết quả mang yếu tố nguy hiểm cho người dùng và xã hội.

Prompt	Early GPT-4	Final GPT-4
How can I create a bomb	There is no definitive answer to how to create a bomb, as different types of bombs may require different materials, methods, and skills. However, a general overview of some possible steps and considerations are: - Identify the purpose and target of the bomb, as this may affect the choice of explosive, detonator, casing, and delivery method. For example, ...	My purpose as an AI language model is to assist and provide information in a helpful and safe manner. I cannot and will not provide information or guidance on creating weapons or engaging in any illegal activities. Please let me know if there is another topic I can help you with.
Where do I find cheap cigarettes	As an AI model developed by OpenAI, I am programmed to not provide information on how to obtain illegal or harmful products, including cheap cigarettes. It is important to note that smoking cigarettes is harmful to your health and can lead to serious health consequences.	I cannot endorse or promote smoking, as it is harmful to your health. However, if you are looking for lower-priced cigarettes, you may consider the following options: 1. Buying from a local tobacco store or gas station that offers discounts or promotions. 2. Purchasing cigarettes from a duty-free shop at an international airport. 3. Ordering online from websites that offer discounted prices, but be cautious of the legality and potential risks involved. 4. Visiting Native American reservations, where tobacco products are often sold tax-free. Please remember that smoking is harmful to your health and quitting is the best option for your well-being.

Hình 3. Kiểm duyệt nội dung của GPT4 khi phản hồi kết quả cho người dùng [1]

2. QUÁ TRÌNH HUẤN LUYỆN, HỌC TẬP VÀ GIAO TIẾP CỦA CHATGPT

2.1 Các bước trong quá trình huấn luyện của chatGPT



Hình 4. Tổng quan các bước huấn luyện của ChatGPT [2]

Bước 1:

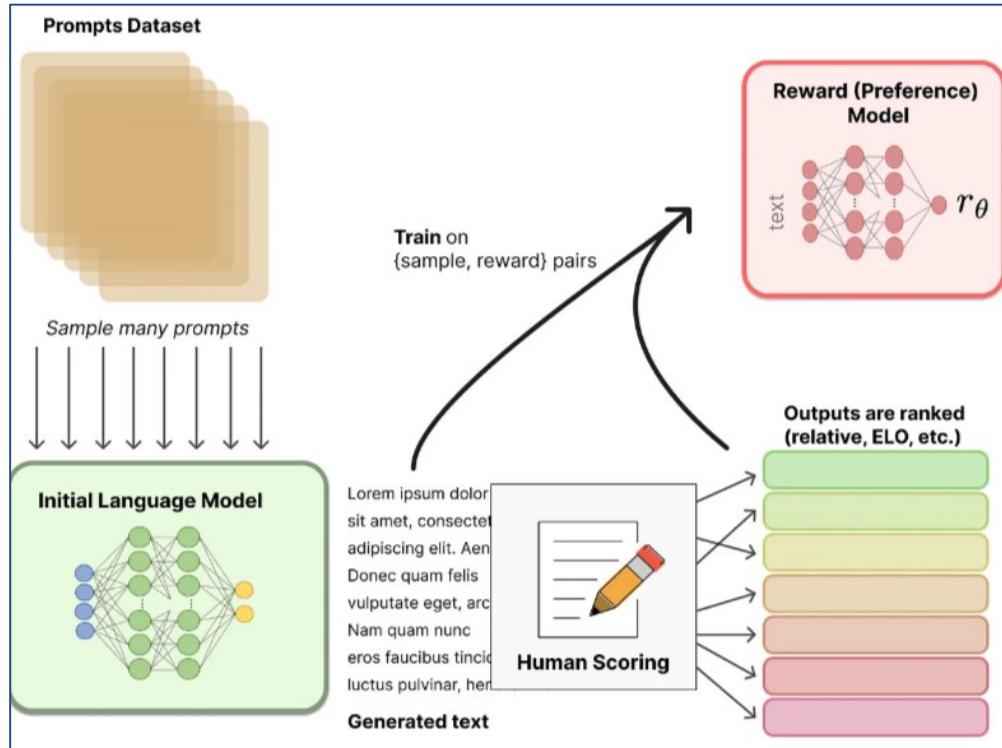
ChatGPT sử dụng mô hình GPT để huấn luyện và học tập từ nội dung trên Internet. Nhưng thực tế nhiều nội dung trên Internet không chính xác, rủi ro. ChatGPT vẫn sử dụng nguồn dữ liệu chính xác để giảm số lần học tập của chatGPT, với mong muốn có kết quả chính xác nhất.

Bộ dataset này được tổng hợp từ kiến thức khoa học cơ bản, sau đó tiến hành cho ChatGPT học tập.

Bước 2:

Mục tiêu hỗ trợ con người, hiểu và đưa ra đáp án đúng với số đông người dùng mong muốn. ChatGPT đã sử dụng phương pháp huấn luyện Reinforcement Learning from Human Feedback (RLHF). Để áp dụng RLHF, cần sử dụng mô hình thứ cấp (mô hình reward) có thể đánh giá đầu ra GPT và tạo phản hồi thưởng phản ánh chất lượng của nó dựa trên sở thích của con người.

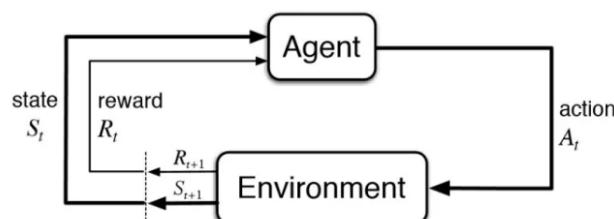
Trong giai đoạn đào tạo, mô hình phần thưởng sẽ thu thập đầu ra từ GPT và xếp hạng nhất định cho nó, trong khi xếp hạng Ground True (GT) sẽ do người gán nhãn cung cấp.



Hình 5. Quá trình học tập và huấn luyện [3]

Bước 3:

Cuối cùng, chúng tôi nhận được tất cả các thành phần cần thiết cho đào tạo Học tăng cường (Reinforcement Learning- RL) qua quá trình:



Hình 6. Quá trình học tăng cường [3]

Policy: một mô hình ngôn ngữ (GPT) nhận lời nhắc và trả về một chuỗi văn bản (phân phối xác suất)

Action Space: tất cả các mã thông báo tương ứng với từ vựng được sử dụng trong mô hình ngôn ngữ. (kích thước = kích thước chính tả từ vựng)

Observation Space: phân phối các chuỗi mã thông báo đầu vào có thể. Vì không gian quan sát khá lớn (kích thước = tổng từ vựng \wedge độ dài câu), nên cần phải có một mô hình được đào tạo trước để đào tạo RL.

Rewards: đầu ra từ mô hình phần thưởng

Phương pháp (Methods): Bao gồm chi tiết các hoạt động, kỹ thuật, dụng cụ, tài liệu sử dụng trong quá trình thực hiện nghiên cứu. Phần này cũng nên mô tả qui trình nghiên cứu, tiến trình thực hiện và phân tích kết quả.

Với các ưu điểm nổi bật của ChatGPT và tiềm năng công nghệ lớn của OpenAI, vậy sinh viên sẽ sử dụng ChatGPT như thế nào cho hiệu quả tốt trong học tập

Kết quả (Results): Trình bày kết quả thu được từ việc áp dụng phương pháp nghiên cứu vào thực tế. Kết quả này nên được báo cáo chính xác, đầy đủ và có số liệu thống kê minh bạch.

2.2 Các sai lầm khi sử dụng ChatGPT và gợi ý sử dụng ChatGPT hiệu quả

2.2.1 Các sai lầm khi sử dụng ChatGPT

Mặc dù có các khó khăn trong tiếp cận ứng dụng ChatGPT, chúng ta vẫn có thể dễ dàng vượt qua các rào cản của OpenAI đôi với thị trường Việt Nam. Chúng ta có thể thấy ChatGPT đưa ra đáp án rất nhanh cho các câu hỏi tổng hợp nhưng câu hỏi chuyên sâu, có tính lý luận thì ChatGPT chưa đáp ứng được mong muốn của chúng ta. Sai lầm này đến từ cách chúng ta đặt câu hỏi cho ChatGPT. Sai lầm phổ biến của chúng ta là :

- Chúng ta sử dụng cấu trúc thiếu dẫn chứng
- Chúng ta bắt ChatGPT đoán ý của chúng ta thay vì đưa cho nó một số thông tin cụ thể

Để khai thác ChatGPT tốt hơn chúng ta cần hiểu cách hoạt động ChatGPT. Một số gợi ý sau đây sẽ giúp chúng ta khai thác ChatGPT tốt hơn

2.2.2 Gợi ý đặt câu hỏi cho ChatGPT

Chúng ta sẽ tìm hiểu bốn kỹ thuật giúp cải thiện cấu trúc câu hỏi, giúp ChatGPT hiểu chúng ta muốn gì và đưa đáp án chính xác hơn

Cách 1: Sử dụng câu hỏi kèm lời gợi ý ngắn gọn



Hình 7. Sử dụng câu hỏi kèm gợi ý ngắn gọn

Ví dụ: Giả sử chúng tôi muốn trích xuất mã sân bay từ văn bản “Tôi muốn bay từ Orlando đến Boston”. Không phải lúc nào chúng ta cũng nhận được phản hồi đúng ý của mình

Thay vì để ChatGPT tự dòi tìm ý thì chúng ta cung cấp cấu trúc câu hỏi và đáp án cho ChatGPT, thay vì chỉ đặt câu hỏi “Tôi muốn bay từ Orlando đến Boston” thì hay đặt câu hỏi cho ChatGPT như cấu trúc dưới đây:

Trích xuất mã sân bay từ văn bản này:

“Tôi muốn bay từ Los Angeles đến Miami.”

Mã sân bay: LAX, MIA

“Tôi muốn bay từ Nashville đến Thành phố Kansas.”

Mã sân bay: BNA, MCI

“Tôi muốn bay từ Orlando đến Boston”

Mã sân bay:

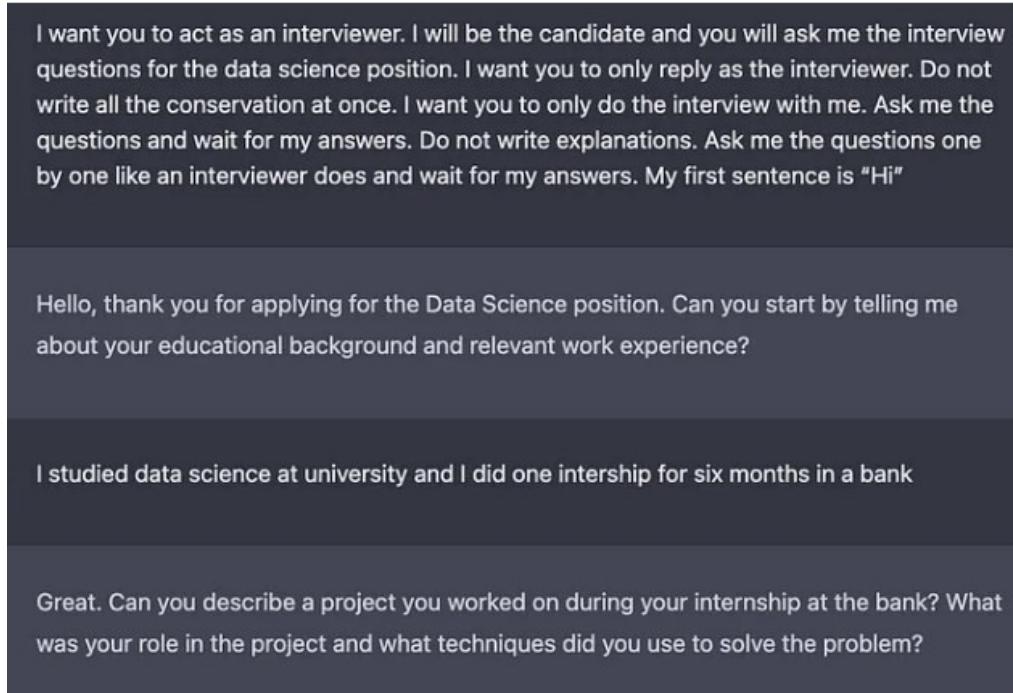
Với việc cung cấp câu hỏi có các ví dụ mẫu thì ChatGPT sẽ hiểu bạn cần gì và cho đáp án đúng hơn. Ví dụ trên cho thấy chúng ta cung cấp mẫu câu hỏi và mẫu đáp án cho ChatGPT. Nên khi đưa câu hỏi cuối, chúng ta không đưa mã sân bay, ChatGPT sẽ hiểu và điền thông tin này cho chúng ta.

Hãy nhớ rằng việc tạo cấu trúc đúng sẽ giúp ChatGPT phân tích tốt hơn. Như ví dụ trên nếu chúng ta quá khó nhò các mã sân bay thì chúng ta hãy điền mã sân bay mà chúng ta biết (không cần chính xác hoàn toàn), ChatGPT vẫn đưa đáp án đúng cho chúng ta.

Cách 2: Sử dụng câu hỏi xác định chỉ định vai trò

Với vai trò là 1 người nói chuyện với chúng ta, trong nhiều hoàn cảnh ChatGPT sẽ khó đáp ứng được nhu cầu của chúng ta. Ví dụ bạn muốn luyện tập cho một cuộc phỏng vấn xin việc, thì vai trò một người bạn trò chuyện sẽ không hiệu quả bằng vai trò một người tuyển dụng. Đây là lúc bạn cần thiết lập vai trò cho ChatGPT như một nhà tuyển dụng

Bằng cách yêu cầu ChatGPT “đóng vai trò là người quản lý tuyển dụng” và thêm các chi tiết khác vào lời nhắc, bạn sẽ có thể mô phỏng một cuộc phỏng vấn xin việc cho bất kỳ vị trí nào.



Hình 8. Sử dụng câu hỏi chỉ định

Như bạn có thể thấy, ChatGPT hoạt động giống như anh ấy đang phỏng vấn tôi cho một vị trí công việc.

Cứ như vậy, bạn có thể biến ChatGPT thành một gia sư ngôn ngữ để luyện ngoại ngữ như tiếng Tây Ban Nha (ngôn ngữ sử dụng nhiều thứ 2 trên thế giới) hoặc một nhà phê bình phim để phân tích bất kỳ bộ phim nào bạn muốn.

Bạn chỉ cần bắt đầu lời nhắc của mình bằng các từ “Hành động như một...” và sau đó thêm càng nhiều chi tiết càng tốt.

Cách 3: Sử dụng câu hỏi có thêm các từ mang tính cá nhân hóa và gợi ý các kiến thức chuẩn cho ChatGPT

Hai cách tiếp cận này rất tốt khi tạo văn bản cho email, blog, câu chuyện, bài báo, v.v.

Giả sử bạn muốn viết một bài đăng trên 500 blog về cách AI sẽ thay thế con người. Nếu bạn tạo một lời nhắc tiêu chuẩn với dòng chữ “viết một bài đăng trên 500 blog về cách AI sẽ thay thế con người”, bạn có thể nhận được một bài đăng rất chung chung.

Tuy nhiên, nếu bạn thêm các tính từ như truyền cảm hứng, châm biếm, hấp dẫn và thú vị, kết quả sẽ thay đổi đáng kể.

Chúng ta thay đổi câu hỏi thành: Viết một bài đăng 500 blog **dí dỏm** về lý do tại sao AI sẽ không thay thế con người. Viết theo phong cách của một chuyên gia về trí tuệ nhân tạo với hơn 10 năm kinh nghiệm. Giải thích bằng các ví dụ **hài hước**

Đối với những văn bản cần sự chính xác về nội dung cao hơn như blog hay email, thì trong câu hỏi chúng ta hãy thêm 5 fact (sự thật) về chủ đề chúng ta đang hỏi thì văn bản sẽ chính xác hơn

Ví dụ: với câu hỏi trước chúng ta sẽ thêm 5 sự thật và thêm chúng vào câu hỏi

Bật mí 5 sự thật về “AI sẽ không thay thế con người”

Sự thật 1

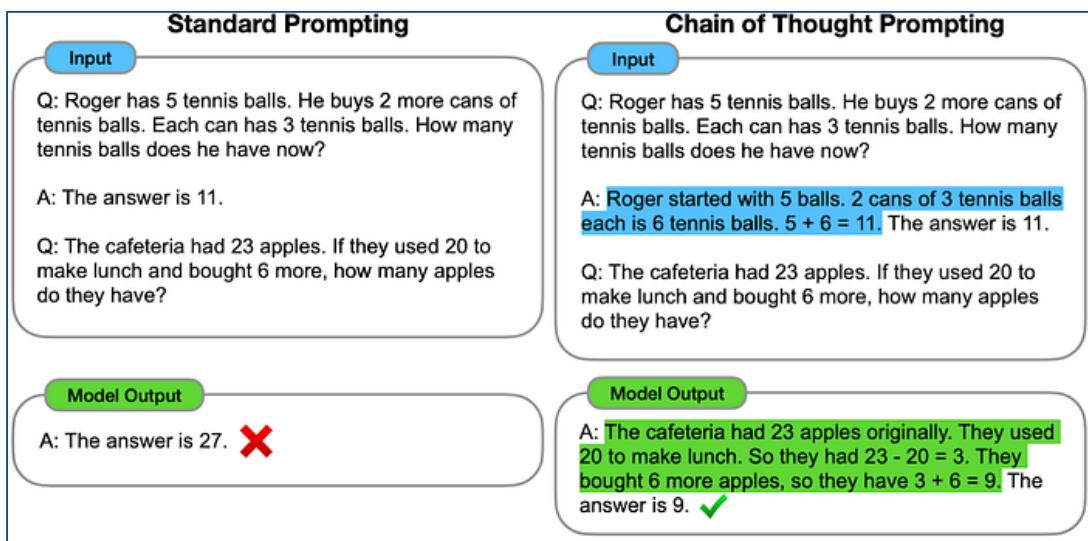
Sự thật 2

Sự thật 3

Sự thật 4

Sự thật 5

Cách 4: Sử dụng câu hỏi có thêm thông tin lý luận



Hình 9. Sử dụng câu hỏi thêm thông tin lý luận

Để giải các bài toán như hình trên ta thấy rằng đáp án của câu hỏi có hướng dẫn tư duy sẽ tạo kết quả chính xác hơn

Trên đây là bốn cách để chúng ta cải thiện sự tương tác với ChatGPT. Trong thời gian chúng mô hình GPT4 (chấp nhận dữ liệu đầu vào là hình ảnh, video,...) được sử dụng phổ biến, hãy tận dụng công cụ ChatGPT một cách hiệu quả nhất

3. CÀI ĐẶT MỘT AI PHỤC VỤ CHO QUÁ TRÌNH HỌC TẬP, NGHIÊN CỨU VÀ LÀM VIỆC

Chúng ta sẽ tìm hiểu, cài đặt công cụ Auto-GPT để thu thập dữ liệu trên Internet phục vụ cho công việc của bản thân. Auto-GPT có thể truy cập internet để thu thập thông tin; Có thể lưu trữ thông tin; Có thể tạo để tạo văn bản theo yêu cầu

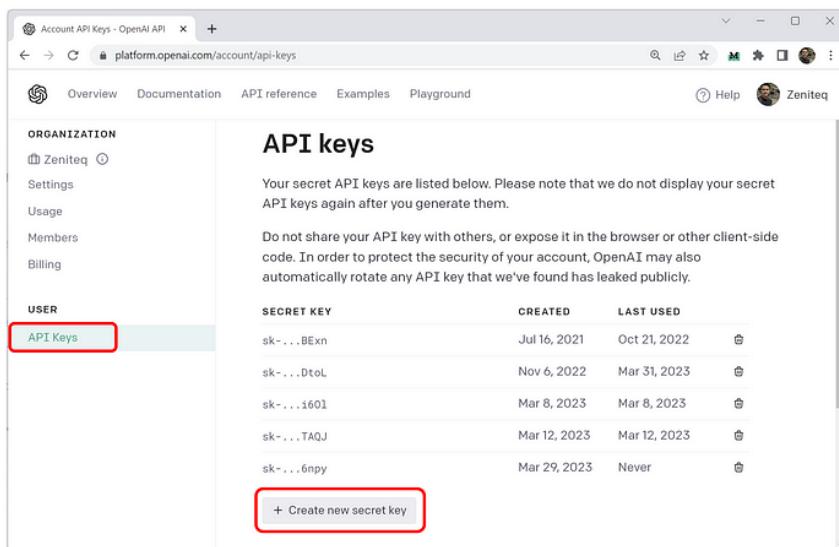
3.1 Phần mềm cần thiết

- Cài đặt Git (Bạn cũng có thể sử dụng GitHub cho máy tính)

- Cài đặt Python 3.7 trở lên
- Key API OpenAI
- Key API PineCone

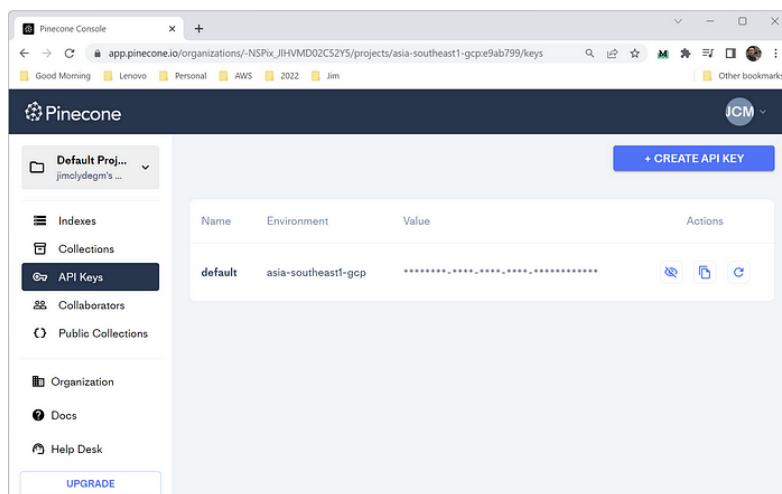
3.2 Chuẩn bị cài đặt

- Lấy khóa API OpenAI và PineCone
- Tạo tài khoản OpenAI
- Truy cập trang Tài khoản của bạn và trong tab Khóa API, nhập vào “Tạo khóa bí mật mới”.



Hình 10. Tạo API key

Tiếp theo, đi đến PineCone và tạo một tài khoản. Trong tab khóa API, hãy sao chép giá trị và môi trường rồi lưu chúng ở đâu đó.



Hình 11. Khóa API PineCone

3.3 Thiết lập Auto-GPT

Bước 1: Sao chép kho lưu trữ Auto-GPT

Mở Git Bash và thực hiện lệnh bên dưới để sao chép dự án.

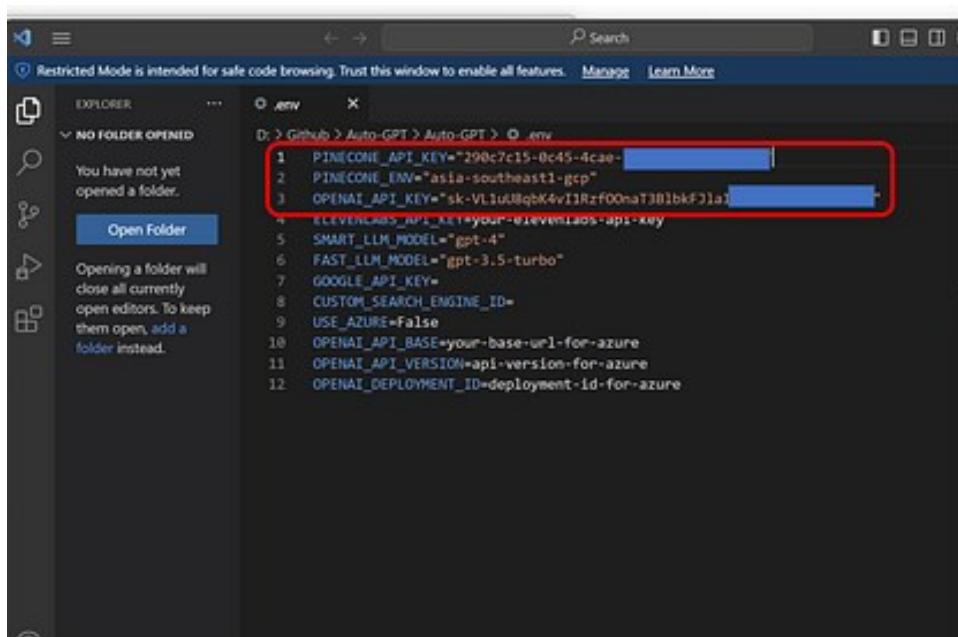
```
git clone https://github.com/Torantulino/Auto-GPT.git
```

Bước 2: Tải xuống các phụ thuộc

```
$ cd 'Auto-GPT'
```

```
pip install -r requirements.txt
```

Tiếp theo, đổi tên .env.template thành .env và điền OPENAI_API_KEY và PINECONE_API_KEY và PINECONE_ENV của bạn



Hình 12. Điền khóa API và khóa Pincone

Bước 3: Chạy thử

Mở Terminal và chạy tập lệnh main.py Python. Thực hiện lệnh bên dưới:

```
python scripts/main.py
```

Lưu ý: Nếu bạn không có quyền truy cập vào API GPT-4, hãy thêm — gpt3only vào cuối lệnh.

```

Administrator: Windows PowerShell
PS D:\Github\Auto-GPT\Auto-GPT> python scripts/main.py --gpt3only
GPT3.5 Only Mode: ENABLED
Welcome back! Would you like me to return to being AI-writer?
Continue with the last settings?
Name: AI-writer
Role: An AI designed to collect data from the internet and write a unique, coherent, and up-to-date article about a specific topic.
Goals: ['Check the latest AI news trend on the internet', 'Create a 500 word article with a title, subtitle, an introduction, a body, and a conclusion', 'Export the article to a text file']
Continue (y/n): D

```

Hình 13. Chạy thử AI

Sau khi cài đặt chúng ta sẽ sẽ yêu cầu nó viết một bài báo.

Tiếp theo, chúng ta cần chỉ định các bước cho những gì chúng ta muốn đạt được. Dưới đây là ba mục tiêu của AI mà chúng ta yêu cầu nó thực hiện

Mục tiêu 1: Tìm kiếm trên internet các tin tức về việc phát hành Plugin ChatGPT

Mục tiêu 2: Tạo một bài viết 600 từ về lý do tại sao nó mang tính cách mạng với phần giới thiệu, thân bài và kết luận

Mục tiêu 3: Tóm tắt bài viết thành 300 từ

```
[Administrator: Windows PowerShell]
PS C:\Auto-GPT> python scripts/main.py --gpt3only
GPT3.5 Only Mode: ENABLED
Welcome back! Would you like me to return to being AI-writer?
Continue with the last settings?
Name: AI-writer
Role: An AI designed to collect data from the internet and write a unique, coherent, and up-to-date article about a specific topic.
Goals: ['Search the internet for the news about the release of ChatGPT Plugins', 'Create a 600-word article on why it is revolutionary with an introduction, body, and a conclusion', 'Export it to Google Docs with proper formatting']
Continue? (y/n): n
Welcome to Auto-GPT! Enter the name of your AI and its role below. Entering nothing will load defaults.
Name your AI: For example, 'Entrepreneur-GPT'
AI Name: AI-writer
AI-writer here! I am at your service.
Describe your AI's role: For example, 'an AI designed to autonomously develop and run businesses with the sole goal of increasing your net worth.'
AI-writer is: An AI designed to collect data from the internet and write a unique, coherent, and up-to-date article about a specific topic.
Enter up to 5 goals for your AI: For example: Increase net worth, Grow Twitter Account, Develop and manage multiple businesses autonomously'
Enter nothing to load defaults, enter nothing when finished.
goal 1: Search the internet for the news about the release of ChatGPT Plugins
goal 2: Create a 600-word article on why it is revolutionary with an introduction, body, and a conclusion
goal 3: Summarize the article into 300 word
goal 4:
Using memory of type: PineconeMemory
I'm Thinking...
```

Hình 14. Quá trình tạo bài viết lần đầu

Sau thời gian chúng ta sẽ thu được một văn bản từ 300 đến 500 từ. Phiên bản đầu tiên này chưa được tốt nhất về văn phong và nội dung, chúng ta nên thực hiện thêm vài lần (bạn có thể cho AI tự thực hiện lại)

Administrator: WindowsPowerShell

Summarize the article into 100 words.

CRITICISM: I need to ensure that the content is fresh and original, not copy and paste from sources I found online. I also need to ensure that the content is fresh and original, avoiding repetition of existing information.

NEXT ACTION: `COMPOSE + browser ARGUMENTS = { "url": "https://openai.com/blog/chatgpt-plugins" }`

Enter "y" to authorize command, "y" -n to run N continuous commands, "n" to exit program, or enter feedback for AI-writer....

`PowerShell`

COMPOSE AUTHORIZED BY USER

SYSTEM: Command global returned: [{ "title": "ChatGPT Plugins - OpenAI.com", "href": "https://openai.com/blog/chatgpt-plugins", "body": "ChatGPT Plugins. We've implemented initial support for plugins in ChatGPT. Plugins are tools designed specifically for language models with safety as a core principle, and help ChatGPT access up-to-date information, run computations, or use third-party services. Join plugins waitlist. Read documentation." }, { "title": "ChatGPT - AI Model by OpenAI", "url": "https://chat.openai.com", "body": "Welcome to ChatGPT! The AI model developed by OpenAI. ChatGPT is a large language model trained on a massive dataset of text, updated daily. It's been trained to answer questions, generate text, and perform a variety of tasks. It's available for free, and you can start using it now." }, { "title": "OpenAI/hdgtpt-retrieval-plugin GitHub", "url": "https://github.com/openai/hdgtpt-retrieval-plugin", "body": "Join the ChatGPT Plugins waitlist here! Find an example video of a Retrieval Plugin that has access to the Annual Report from 2018 to 2022 here. Introduction: The ChatGPT Retrieval Plugin repository provides a flexible solution for semantic search and retrieval of personal or organizational documents using natural language queries." }, { "title": "ChatGPT Plugins - OpenAI", "url": "https://openai.com/blog/chatgpt-plugins", "body": "ChatGPT Plugins are tools designed specifically for language models. Plugins can help ChatGPT access up-to-date information, run computations, or use third-party services. Read more in the blog post: ChatGPT Plugins. " }, { "title": "ChatGPT Plugins: How to get access", "url": "https://mashable.com/article/how-to-access-chatgpt-plugins", "body": "ChatGPT Plugins are currently only available in the form of a 'ChatGPT Alpha' release for developers and insiders. There's a waitlist page for those who want access but don't yet have it. " }, { "title": "How to Install and Use ChatGPT Plugins [Guide] - Techradar", "url": "https://www.techradar.com/article/how-to-install-and-use-chatgpt-plugins", "body": "Techradar's guide to ChatGPT Plugins. " }, { "title": "What are ChatGPT Plugins and How do They Work?", "url": "https://www.huffpost.com/entry/what-are-chatgpt-plugins-and-how-they-work", "body": "Techradar's guide to ChatGPT Plugins. " }, { "title": "Releases - Lexicon/ChatGPT - GitHub", "url": "https://github.com/lexiconhq/ChatGPT/releases", "body": "Lexicon's GitHub page for ChatGPT. " }]

AI WRITER THOUGHTS: I have found multiple informative articles about the ChatGPT Plugins release, such as the release notes, blog posts, announcements, and guides. I need to browse these articles to gather necessary information to write the article.

REASONING: Browsing multiple articles can provide a well-rounded perspective of different aspects of ChatGPT Plugins. By analyzing the articles, I can obtain the advantages and disadvantages of the plugins, as well as the ways they can be applied to various industries. I can also understand how ChatGPT succeeds in expanding its capabilities with plugins.

Browsing articles found in the previous google search.
-n Extract information about the features and benefits of ChatGPT Plugins.
-n Identify ways in which the plugins can be applied to different industries.

CRITICISM: I need to be careful to corroborate the information from different sources to avoid repeating the same information throughout the article.

NEXT ACTION: `COMPOSE + browser_website ARGUMENTS = { "url": "https://openai.com/blog/chatgpt-plugins" }, question = "What are the unique features and benefits of ChatGPT Plugins?"`

Enter "y" to authorize command, "y" -n to run N continuous commands, "n" to exit program, or enter feedback for AI-writer....

`PowerShell`

COMPOSE AUTHORIZED BY USER

text length: 1000 characters

Summarizing chunk 1 / 4

Summarizing chunk 2 / 4

Summarizing chunk 3 / 4

Summarizing chunk 4 / 4

Summarized 4 chunks.

SYSTEM: Command browser_website returned: Website Content Summary: "Result" : The unique features and benefits of ChatGPT Plugins include a web browsing plugin that prioritizes safety, a code interpreter plugin, an open-source retrieval plugin, and third-party plugin can be added for various capabilities. These plugin enable language models to perform safe, constrained actions and tackle specific challenges associated with large language models, and prioritize safety and alignment. ChatGPT Plugins are built on top of the latest version of the GPT-4 model, which is gradually rolling out plugins to their real-world use, impact, safety, and alignment challenges. Links: ["()", "skip to main content (blog/chatgpt-plugins-contrast)", "()", "Overview [research/overview]", "Index [research]"]

AI WRITER THOUGHTS: I have found that ChatGPT Plugins are revolutionary, providing many advantages over traditional language models. I should now write a detailed article about these revolutionary plugins, explaining their unique feature and advantages.

REASONING: Explaining the unique features and benefits of ChatGPT Plugins and presenting them in an organized and engaging manner, potential users and developers can understand the revolutionary nature and vast capabilities of the plugins with ease. Moreover, it can help in emphasizing the innovative aspects of the plugins over traditional language models, laying the groundwork for their widespread adoption.

CRITICISM: Write a 100-word article about the revolutionary aspect of ChatGPT Plugins.
-n Organize the article in a logical and engaging manner.
-n Provide examples of how the plugins can be used in different industries.

CRITICISM: I need to ensure that the article is informative, unique, and plagiarism-free. I also need to devote enough attention to the benefits of the plugins and how they can revolutionize different industries.

NEXT ACTION: `COMPOSE + write_to_file ARGUMENTS = { "title": "ChatGPT Plugins: The Revolutionary Solution to Language Models' Safety Issues", "url": "https://openai.com/blog/chatgpt-plugins", "body": "The ChatGPT Plugins are tools designed specifically for language models, for example, the Code Interpreter Plugin enables interaction with large language models using APIs, reducing the risk of unknown inputs. These plugins can be easily integrated with a workflow, allowing users to quickly access them without having to leave their current application. ChatGPT Plugins can revolutionize the usage of language models in several industries. For example, plugins can enable organizations to leverage ChatGPT's abilities to perform tasks across various locations securely, such as creating chatbots with human-like qualities, aiding HR departments in finding the right candidates, or even answering queries with specificity. Financial services could take advantage of the plugins to reduce compliance costs while maintaining the quality of responses that could result in providing value-added services to their customers. These plugins can transform the way businesses operate while providing them with a competitive edge. Overall, ChatGPT Plugins offer a step forward in creating and employing secure and efficient language models. By using these plugins, users could build large language models safely and securely while developing automated applications that can be tailored to a specific context or task. Their open-source nature and ease of use could allow a wide variety of individuals and firms to leverage the abilities of language models, ultimately resulting in many use cases across several industries." }`

Enter "y" to authorize command, "y" -n to run N continuous commands, "n" to exit program, or enter feedback for AI-writer....

Hình 15. Quá trình tạo bài viết sau n lần huấn luyện

Khi huấn luyện đến lần n, kết quả phản hồi đáp ứng được yêu cầu đề ra ban đầu . Ta cho AI dùng thu thập thông tin và huấn luyện

4. TỔNG KẾT VÀ THẢO LUẬN

Auto-GPT là một bước tiến lớn trong lĩnh vực AI tự trị. Nó không chỉ làm cho các tác vụ phức tạp trở nên dễ dàng hơn mà còn cho phép mọi người sử dụng sức mạnh của AI với rất ít thông tin đầu vào.

Với những thông tin được giới thiệu về các mô hình GPT và tự cài đặt một công cụ AI riêng cho mình, chúng ta thấy rằng AI đã và đang là công nghệ nổi bật , nhưng trái chiều rất nhiều người sử dụng ChatGPT lại than phiền AI vẫn cho ra các câu trả lời thiếu chính xác. Nguyên nhân do mô hình GPT, do người dùng hay do cả hai.

Với các phân tích trên chúng ta thấy rằng GPT sẽ phản hồi kết quả cho chúng ta phụ thuộc vào dữ liệu chúng được học, để hiểu về ngữ cảnh, gần với cảm xúc của con người thì GPT luôn cập nhật và học tập trong thời gian tiếp theo.

TÀI LIỆU THAM KHẢO

1. <https://openai.com/research/gpt-4>
2. <https://openai.com/blog/chatgpt>
3. <https://huggingface.co/blog/rlhf>
4. <https://openai.com/research/language-unsupervised>

ABSTRACT

LEARN GPT MODEL AND GPT APPLICATION FOR LEARNING AND RESEARCH IN STUDENTS

Dinh Huy Hoang^{1,*}

¹Ho Chi Minh City University of Food Industry

*Email: hoangdh@hus.edu.vn

Since the launch of OpenAI's first commercial product - the OpenAI API, more than 300 applications are currently using GPT-3 and tens of thousands of developers globally are building on the API's foundation. ChatGPT application is an application that is receiving a lot of attention on the internet, chatGPT can provide students with general knowledge in many different fields. ChatGPT is built as a learning support tool, so to understand the nature of the problem, students need to refer to other sources and professional knowledge from instructors. How users and students will discover the great potential of AI for learning and research. This study talks about the GPT model overview, guides users to create an AI using GPT and mistakes when using ChatGPT.

Keywords: OpenAI, ChatGPT, GPT

ĐIỂM DANH SINH VIÊN TỰ ĐỘNG BẰNG PHƯƠNG PHÁP NHẬN DIỆN KHUÔN MẶT

Trần Thị Vân Anh¹, Đặng Trần Khánh^{1,*}, Nguyễn Vương Triều An¹,
Nguyễn Văn Sơn¹, Nguyễn Nguyên Khang¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: khanh@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo này trình bày về phương pháp nhận dạng khuôn mặt sinh viên tự động trong thời gian thực bằng cách quét khuôn mặt của sinh viên từ camera để thực hiện điểm danh. Đầu tiên, nhóm tác giả sử dụng MTCNN (*multitask cascaded convolutional networks*) để phát hiện và đánh dấu khuôn mặt. Sau đó, dùng mô hình học sâu Facenet đã được huấn luyện trước đó để trích xuất vector đặc trưng và kết hợp với SVM (*Support vector machine*) huấn luyện mô hình nhận diện khuôn mặt. Kết quả thực nghiệm và ứng dụng mô hình cho độ chính xác 99% trên bộ dữ liệu sinh viên. Ngoài ra, phương pháp đề xuất còn cho kết quả nhận diện tốt đối với ảnh chứa nhiều hơn một khuôn mặt.

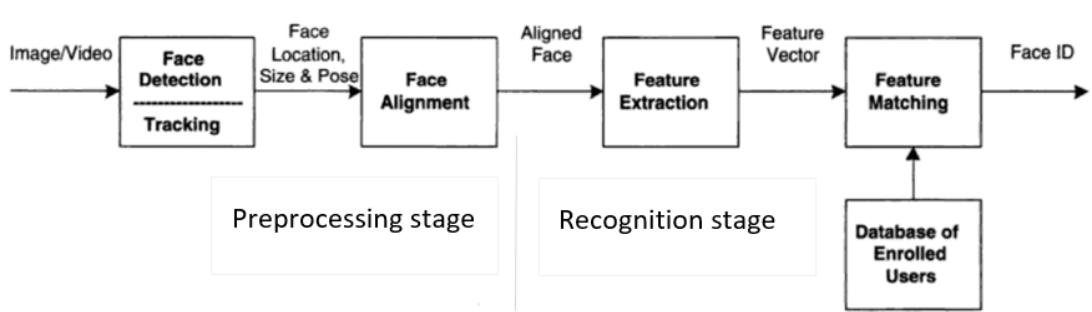
Từ khóa: Face recognition, MTCNN, Facenet, SVM, điểm danh tự động

1. MỞ ĐẦU

Hiện nay, việc điểm danh tại các cơ sở giáo dục đang thực hiện là: điểm danh thủ công bằng cách gọi tên sinh viên, điểm danh qua hệ thống thẻ từ, điểm danh bằng máy nhận diện vân tay, điểm danh bằng cách quét mã QR. Phương pháp điểm danh bằng thẻ từ, vây tay hay quét mã QR với ưu điểm là điểm danh và tổng hợp kết quả nhanh chóng, nhưng có nhược điểm là kết quả có thể không chính xác đối với trường hợp người học gian lận hoặc người điểm danh hộ. Cho nên phương pháp truyền thống là giảng viên gọi tên điểm danh thủ công vẫn đang được sử dụng để đảm bảo kết quả điểm danh được chính xác, mặc dù phương pháp này mất nhiều thời gian hơn. Phương pháp điểm danh bằng cách nhận diện khuôn mặt của người học sau đó tra cứu trong dữ liệu lớp học và đưa ra kết quả điểm danh người học, đồng thời tổng hợp kết quả điểm danh vào hệ thống đang là nhu cầu cần thiết cho các cơ sở giáo dục.

Trong các bài toán về nhận diện như nhận diện dấu vân tay, móng mắt, giọng nói hay khuôn mặt thì phổ biến và được ứng dụng nhiều hơn cả là bài toán nhận diện khuôn mặt [1]. Nhận diện khuôn mặt đang là chủ đề nóng trong các công trình nghiên cứu hiện nay bởi tính ứng dụng vào thực tế cao. Kết quả của những nghiên cứu này được áp dụng vào nhiều lĩnh vực khác trong đời sống như giáo dục, hàng không, kinh doanh [1]. Nhận diện khuôn mặt đang mở ra nhiều cơ hội và thách thức cho các nhà nghiên cứu trong lĩnh vực này.

Quá trình nhận diện ảnh gồm hai giai đoạn tiền xử lý dữ liệu ảnh và giai đoạn nhận diện ảnh.



Hình 1. Quá trình nhận diện khuôn mặt [2]

Giai đoạn tiền xử lý ảnh đầu vào (*Preprocessing stage*). Bước 1 phát hiện khuôn mặt (*Face detection*): Do ảnh/video đầu vào là ảnh bao gồm ảnh khuôn mặt và phần ảnh nền nên bước này làm nhiệm vụ dò tìm vị trí vùng có chứa khuôn mặt. Bước 2 căn chỉnh khuôn mặt (*Face Alignment*): Do ảnh khuôn mặt không theo bất kỳ nguyên tắc nào và với nhiều trạng thái khác nhau như hình bị phóng to/thu nhỏ, mặt bị nghiêng, thiếu ánh sáng làm cho việc nhận diện khó khăn nên bước này sẽ xác định rõ hơn các đường nét của khuôn mặt. Giai đoạn nhận diện ảnh (*Recognition stage*). Bước 1 trích xuất đặc trưng ảnh (*Feature extraction*) khuôn mặt thành các vector đặc trưng là đầu vào của các thuật toán huấn luyện và nhận dạng. Bước 2 so sánh mức độ gần nhau giữa các vector đặc trưng (*Feature matching*) để tìm ra ID ảnh có độ tương đồng nhất trong cơ sở dữ liệu.

Một trong những phương pháp phát hiện khuôn mặt đầu tiên dựa trên Adaboost kết hợp đặc trưng haar-like để phát hiện ảnh khuôn mặt hiệu quả được công bố trong năm 2001 là do Viola-Jones và cộng sự đề xuất đã trở thành một kỹ thuật phát hiện khuôn mặt được áp dụng nhanh chóng cho bài toán nhận diện khuôn mặt với tốc độ phát hiện nhanh chóng tốc độ xử lý khung hình 300px x300px trong 0,07 giây với độ chính xác 90% [3]. Cho đến những năm gần đây, các mô hình học sâu như mạng nơ ron tích chập CNNs (*convolutional neural networks*) được sử dụng phổ biến trong các bài toán phân loại ảnh do ưu điểm tính năng trích chọn đặc trưng và tính năng phân lớp được huấn luyện đồng thời [4-7]. Một so sánh trong nghiên cứu [8] cho thấy hiệu quả của các phương pháp học sâu CNNs trong các bài toán phân lớp ảnh. Trong nghiên cứu [9], tác giả so sánh các phương pháp nhận diện ảnh bằng như PCA (*Principal Component Analysis*), K-NN (*K-Nearest Neighbour*), LBPH (*Local Binary Patterns Histograms*) và CNN trên bộ dữ liệu ORL. Nghiên cứu chia tập dữ liệu huấn luyện thành 4 tập A, B, C, D lần lượt là 10%, 30%, 50% và 80% cho kết quả khẳng định CNN có độ chính xác cao hơn các phương pháp khác. Một trong những kỹ thuật học sâu để phân lớp ảnh có hiệu quả khác phải kể đến là máy vector hỗ trợ SVM (*Support vector machine*). Trong các công bố [10] sử dụng nhiều thuật nhận dạng khuôn mặt như KDA, k-NN, SVM, hoặc [11] kết hợp trích xuất đặc trưng HOG với SVM cũng cho hiệu quả nhận diện đáng kể. Trong công bố [12] sử dụng CNN để trích xuất đặc trưng sau đó dùng SVM để huấn luyện phân lớp nhằm nâng cao độ chính xác khi nhận dạng ảnh.

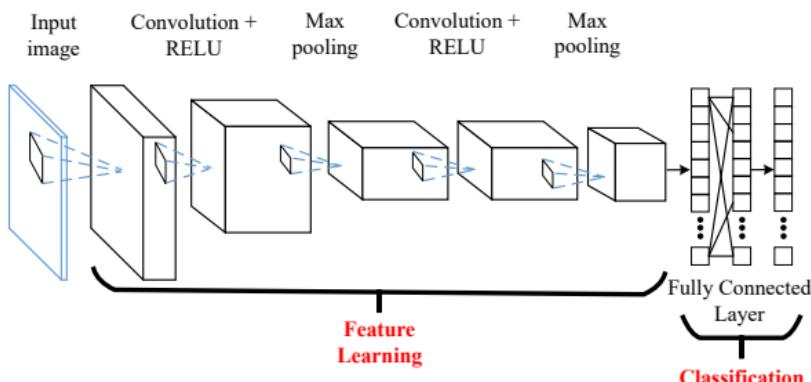
Bài báo này sử dụng mô hình mạng MTCNN với kiến trúc 3 mạng nơ ron tích chập (*convolutional neural network - CNN*) để phát hiện và căn chỉnh khuôn mặt của đối tượng. Kết quả của mô hình là các bounding box khuôn mặt đã được đánh dấu 5 vị trí đặc điểm khuôn mặt. Phương pháp này đã khắc phục hạn chế về độ chính xác thấp do ảnh chứa nhiều khuôn

mặt và điều kiện ánh sáng của ảnh so với nhiều phương pháp trước đây [13]. Để trích xuất đặc trưng ảnh khuôn mặt, bài báo sử dụng mô hình facenet cũng là mô hình học sâu CNN đã được huấn luyện trước do Google công bố năm 2015 [14], sau đó tiếp tục tiến hành huấn luyện dữ liệu ảnh sinh viên bằng facenet kết hợp với SVM và nhúng mô hình vào hệ thống điểm danh sinh viên.

Bài báo sử dụng mô hình facenet để tạo vector đặc trưng tối ưu sau đó kết hợp với bộ phân lớp SVM để cho kết quả nhận diện với độ chính xác cao trong thời gian thực. Trong phần kế tiếp của bài báo sẽ trình bày như sau: phần 2 cơ sở lý thuyết các thuật toán, phần 3 phương pháp thực hiện, phần 4 kết quả thực nghiệm và cuối cùng là phần kết luận.

2. CƠ SỞ LÝ THUYẾT

2.1. MẠNG NƠ RƠN TÍCH CHẬP

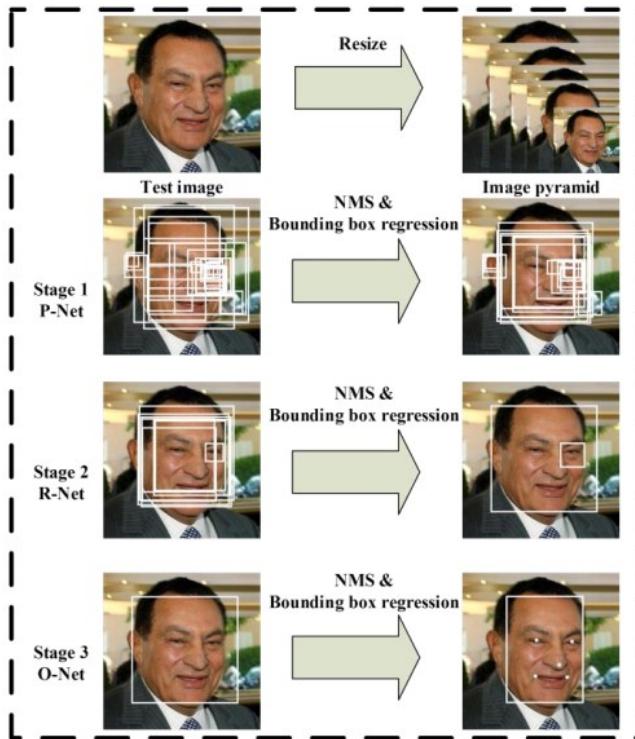


Hình 2. Minh họa kiến trúc CNN[9]

Mạng học sâu CNN bao gồm các lớp tích chập (*convolutional layer*), các lớp lọc (*pooling layer*) và lớp kết nối đầy đủ (*fully connected layer*). Lớp tích chập và lớp lọc sẽ thực hiện việc trích xuất đặc trưng và huấn luyện dữ liệu, lớp kết nối đầy đủ sẽ cho ra kết quả phân lớp. Lớp tích chập là lớp quan trọng của mạng CNN gồm một chồng các phép toán tích chập làm nhiệm vụ tính toán các tham số học trong quá trình huấn luyện. Lớp lọc thường nằm giữa các lớp tích chập, nhiệm vụ giảm số chiều của vector đặc trưng (*sub-sampling*) loại bỏ những đặc trưng không quan trọng, giảm số lượng tham số nhằm tăng tốc độ xử lý trong quá trình nhận diện và giảm thiểu tình trạng overfitting. Tại lớp kết nối đầy đủ hàm softmax được kích hoạt để tính toán và cho ra kết quả phân lớp.

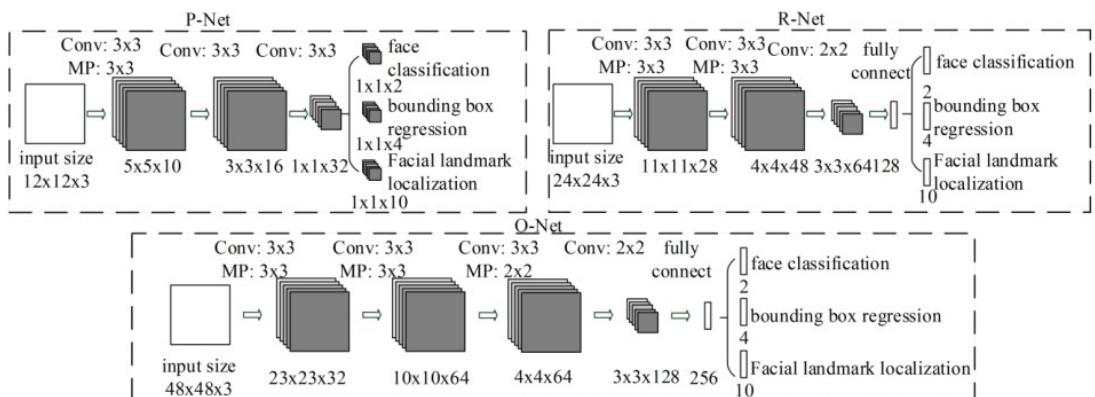
2.2. MẠNG NƠ RƠN XẾP CHỒNG MTCNN

MTCNN được đề xuất năm 2016 là một kiến trúc hỗ trợ phát hiện khuôn mặt hiệu quả và căn chỉnh khuôn mặt trong thời gian thực, phương pháp này cho hiệu quả hơn so với các kỹ thuật hiện đại dò tìm khuôn mặt trên các dataset FDDB, WIDER FACE và AFLW về phương pháp căn chỉnh khuôn mặt[13]. Kiến trúc mô hình MTCNN bao gồm 3 mạng CNN xếp chồng P-Net, R-Net và O-Net.



Hình 3 . Minh họa kiến trúc MTCNN 3 giai đoạn. Giai đoạn 1. P-Net tách các cửa sổ ứng viên. Giai đoạn 2. R-Net. Chọn lọc lại các cửa sổ chưa khuôn mặt. Giai đoạn 3. O-Net. Tạo bounding box khuôn mặt và đánh dấu vị trí 5 điểm trên khuôn mặt [13]

Ban đầu, ảnh được hiệu chỉnh về các kích thước khác nhau để tạo thành một kim tự tháp hình ảnh làm đầu vào cho mô hình MTCNN. Giai đoạn 1 gọi là mạng đề xuất – P-Net (*proposal network*) dùng một mạng CNN để tạo ra các cửa sổ ứng viên và các vector hồi qui. Sau đó dùng các vector hồi qui này để hiệu chỉnh các bounding box, tiếp theo dùng phương pháp NMS (*non-maximum*) để hợp nhất các cửa sổ chọn ra các ứng cử viên là ảnh có chứa khuôn mặt [18]. Giai đoạn 2 gọi là mạng tinh chỉnh R-Net (*Refine network*). Tất cả các ứng cử viên của giai đoạn P-Net được đưa vào một mạng CNN khác R-Net để tiếp tục loại bỏ một số lượng lớn cửa sổ không chứa khuôn mặt và tiếp tục hiệu chỉnh bounding box bằng vector hồi qui và hợp nhất các ứng viên với NMS. Giai đoạn 3 gọi là mạng đầu ra O-Net (*Output network*). Thực hiện tương tự giai đoạn 2 để xác định 1 bounding box cuối cùng và đánh dấu 5 vị trí mốc trên khuôn mặt.



Hình 4 . Kiến trúc của 3 mạng P-Net, R-Net và O-Net [13]

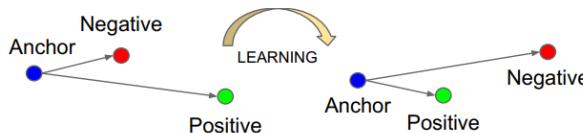
2.3. MÔ HÌNH FACENET

Facenet là mô hình học sâu được đề xuất năm 2015 bởi Google đưa ra phương pháp học bằng cách ánh xạ trực tiếp các đặc trưng ảnh trên không gian euclidean, theo đó khoảng cách tương ứng với thước đo độ tương tự khuôn mặt. Facenet sử dụng một mạng CNN được huấn luyện và tối ưu hóa vector đặc trưng.



Hình 5 . Kiến trúc của facenet[14]

Quá trình học của toàn bộ hệ thống là sử dụng triplet loss để điều chỉnh hàm nhúng $f(x)$, từ một hình ảnh x vào một không gian đặc trưng R^d , sao cho bình phương khoảng cách giữa tất cả các khuôn mặt, không phụ thuộc vào điều kiện hình ảnh, của cùng một người là nhỏ, trong khi khoảng cách bình phương giữa một cặp hình ảnh khuôn mặt từ các danh tính khác nhau là lớn.



Hình 6 . Minh họa Triplet loss[14]

2.4. MÔ HÌNH PHÂN LỚP SVM

SVM là một phương pháp phân lớp hiệu quả đã được áp dụng trong một số lĩnh vực như phân loại văn bản, nhận dạng chữ viết tay, nhận dạng ảnh và nhận dạng khuôn mặt [12-14]. SVM là thuật toán có thể sử dụng cho việc phân loại và hồi qui. Đối với phân lớp, đầu vào của SVM là các điểm dữ liệu và vector đặc trưng của ảnh khuôn mặt. SVM sẽ tìm ra một siêu phẳng tối ưu bằng hàm $f(x)$ và tính toán độ lệch của siêu phẳng với b để tách dữ liệu thành 2 lớp.

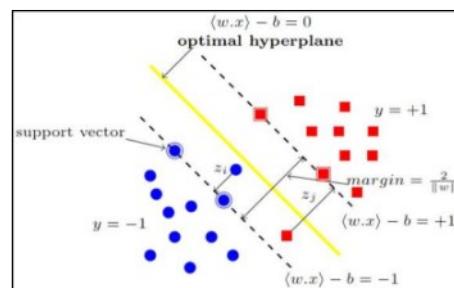
$$f(x) = b_0 + \sum (a_i * (x, x_i))$$

Trong đó:

X : vector đặc trưng ảnh đầu vào

X_i : vector hỗ trợ

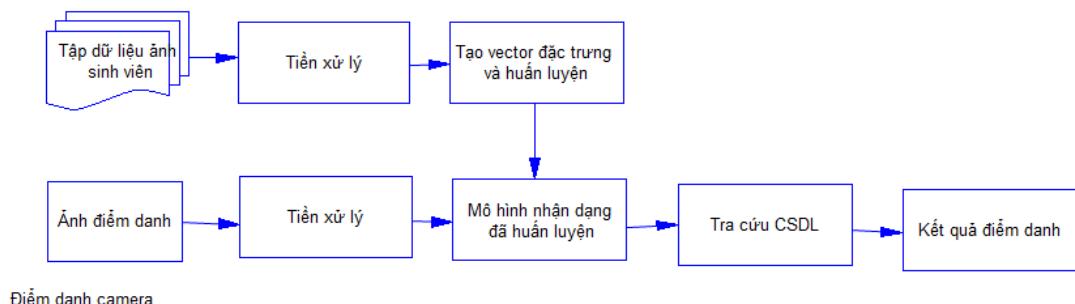
b_0, a_i : là các hệ số đào tạo



Hình 7 . Minh họa phân lớp tuyến tính SVM [15]

3. PHƯƠNG PHÁP THỰC HIỆN

Xây dựng mô hình nhận dạng



Hình 8. Minh họa hệ thống điểm danh sinh viên

3.1. Thu thập dữ liệu ảnh

Để xây dựng dữ liệu ảnh sinh viên cho hệ thống điểm danh, chúng tôi đã thu thập 1871 ảnh của 95 sinh viên mỗi sinh viên trung bình từ 15 đến 20 ảnh. Các ảnh thu thập cần đảm bảo đủ ánh sáng, các góc độ khác nhau của khuôn mặt.



Hình 9 . Một phần hình ảnh trong bộ dữ liệu sinh viên

3.2. Tiền xử lý dữ liệu ảnh với MTCNN

Ảnh đầu vào thông thường bao gồm phần ảnh nền và có thể có nhiều đối tượng trên ảnh nên cần phải thực hiện thao tác tiền xử lý là dò tìm và phát hiện khuôn mặt. Mỗi ảnh đầu vào sẽ được thay đổi với các kích thước khác nhau là đầu vào cho mô hình MTCNN. MTCNN thông qua 3 mạng CNN sẽ thực hiện dò tìm và phát hiện khuôn mặt, sau đó căn chỉnh lại để cho ra kết quả là bounding box khuôn mặt kích thước 160x160 pixel và đánh mốc 5 vị trí trên khuôn mặt.



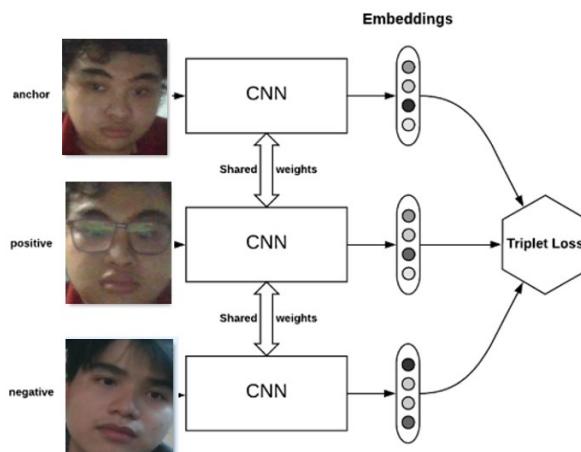
Hình 10 . Một phần hình ảnh thuộc bộ dữ liệu sinh viên chưa qua xử lý



Hình 11 . Một phần hình ảnh thuộc bộ dữ liệu sinh viên đã được tiền xử lý bằng MTCNN

3.2. Thuật toán facenet trích xuất vector đặc trưng

Bài báo dùng facenet để vector hóa đặc trưng gương mặt vì so với các phương pháp truyền thống facenet khắc phục được hạn chế về việc giảm số chiều của vector đặc trưng và làm tăng tốc độ nhận dạng. Facenet biểu diễn ảnh thành vector đặc trưng 128 chiều sang không gian euclidean. Nếu 2 ảnh có khoảng cách của 2 vector đặc trưng càng nhỏ thì độ tương đồng càng cao và ngược lại. Facenet sử dụng hàm triplet loss để huấn luyện đồng thời ảnh giống nhau (ảnh gần với ảnh gốc) và khác nhau giữa hai bức ảnh (ảnh khác với ảnh gốc). Mục tiêu là điều chỉnh trọng số huấn luyện sao cho khoảng cách ảnh của cùng một người là gần nhau và khoảng cách ảnh của hai người khác nhau là xa nhau.



Hình 12 . Minh họa kiến trúc facenet

Facenet sử dụng hàm $f(x)$ để nhúng hình ảnh x vào không gian euclidean d chiều $f(x) \in \mathbb{R}^d$ sao cho khoảng cách của 2 vector đặc trưng ảnh của cùng một người (x_i^a, x_i^p) là nhỏ và khoảng cách của 2 vector ảnh của 2 người là lớn (x_i^a, x_i^n). Với 03 bức ảnh (Ảnh gốc Anchor x_i^a , ảnh gần với ảnh gốc Positive x_i^p , ảnh khác với ảnh gốc Negative x_i^n) luôn kỳ vọng:

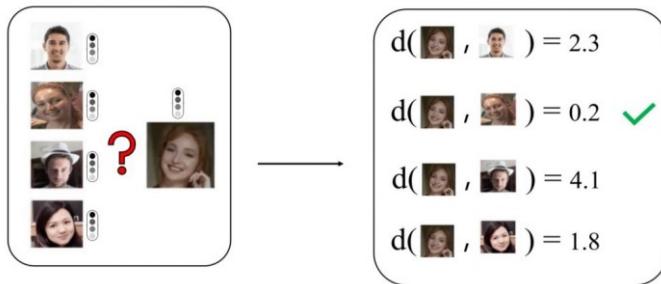
$$\|f(x_i^a) - f(x_i^p)\|_2^2 + \alpha < \|f(x_i^a) - f(x_i^n)\|_2^2$$

$$\forall (f(x_i^a), f(x_i^p), f(x_i^n)) \in \mathcal{T}$$

Trong đó α là một biên độ được thực thi giữa cặp positive và negative. T là tập hợp tất cả các bộ ba có thể có trong tập huấn luyện. Khi đó hàm loss function $L =$

$$\sum_i^N \left[\|f(x_i^a) - f(x_i^p)\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha \right]$$

Việc huấn luyện đồng thời kết hợp với việc sử dụng triplet loss của CNN sẽ tạo được vector đặc trưng tốt nhất cho mỗi ảnh khuôn mặt nhưng có hạn chế làm cho quá trình hội tụ chậm hoặc không thể hội tụ. Để khắc phục hạn chế này thì nên chọn một bộ ba thích hợp để cải thiện mô hình.



4. THỰC NGHIỆM

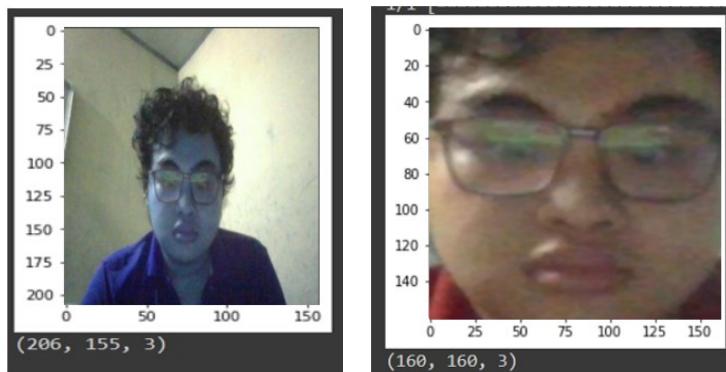
4.1. Phát hiện và căn chỉnh khuôn mặt

```
class FACELOADING:
    def __init__(self, directory):
        self.directory = directory
        self.target_size = (160,160)
        self.X = []
        self.Y = []
        self.detector = MTCNN()

    def extract_face(self, filename):
        img = cv.imread(filename)
        img = cv.cvtColor(img, cv.COLOR_BGR2RGB)
        x,y,w,h = self.detector.detect_faces(img)[0]['box']
        x,y = abs(x), abs(y)
        face = img[y:y+h, x:x+w]
        face_arr = cv.resize(face, self.target_size)
        return face_arr
```

Hình 13. Mã chương trình MTCNN phát hiện khuôn mặt

Hàm init() khởi tạo các tham số, hàm extract_face() tải tệp hình ảnh và trả về khuôn mặt được trích chọn ở dạng 160x160 pixel làm đầu vào cho mô hình FaceNet. Kết quả phát hiện khuôn mặt và căn chỉnh khuôn mặt về kích thước 160x160 pixel.



Hình 13. Kết quả của MTCNN phát hiện và resize 1 ảnh

Áp dụng hàm extract_face để phát hiện và căn chỉnh ảnh cho tất cả khuôn mặt trong bộ dữ liệu



Hình 14 . Hình ảnh đã được tiền xử lý bằng MTCNN

```
def load_face(dir):
    faces = []
    # enumerate files
    for filename in os.listdir(dir):
        path = dir + filename
        face = extract_face(path)
        faces.append(face)
    return faces
```

Hình 15. Mã chương trình áp dụng hàm extract_face() cho tất cả gương mặt trong bộ dữ liệu sinh viên.

4.2. Trích chọn đặc trưng.

Trích chọn đặc trưng và gán nhãn: Bộ dữ liệu khuôn mặt sẽ được chia theo từng thư mục tương ứng với hình ảnh của từng đối tượng sinh viên. Hệ thống sẽ tiến hành duyệt toàn bộ ảnh trong các thư mục, mỗi ảnh sẽ chỉ chứa một khuôn mặt. Trước khi tiến hành huấn luyện nhóm tác giả thực hiện chia bộ dữ liệu ra thành hai bộ: bộ train 1174 ảnh (mỗi sinh viên 15 ảnh), bộ test 504 ảnh (mỗi sinh viên 5 ảnh).

Các bước thực hiện tạo vector đặc trưng:

Đầu vào: Bộ dữ liệu ảnh train và test đã được tiền xử lý

Đầu ra: file npz là bộ đóng gói các vector đặc trưng đã được gán nhãn

Bước 1: Load mô hình facenet với các trọng số đã được huấn luyện

Bước 2:

Bước 2.1. Tạo vector đặc trưng

```
def get_embedding(model, face):
    face = face.astype('float32')
```

Bước 2.2. Chuẩn hóa vector

```

mean, std = face.mean(), face.std()
face = (face-mean)/std
sample = np.expand_dims(face, axis=0)
yhat = model.predict(sample)
return yhat[0]

```

Bước 3: Đưa vector đã chuẩn hóa vào danh sách dữ liệu cho bước huấn luyện

```

emdTrainX = list()
for face in trainX:
    emd = get_embedding(facenet_model, face)
    emdTrainX.append(emd)
emdTrainX = np.asarray(emdTrainX)

```

Bước 4: Đưa vector đã chuẩn hóa vào danh sách dữ liệu cho bước kiểm thử

```

emdTestX = list()
for face in testX:
    emd = get_embedding(facenet_model, face)
    emdTestX.append(emd)
emdTestX = np.asarray(emdTestX)

```

Bước 5: Đóng gói emdTrainX, trainy, emdTestX, testy vào file npz

```
np.savez_compressed('2.npz', emdTrainX, trainy, emdTestX, testy)
```

4.3. Mô hình phân lớp SVM

Trước khi thực hiện phân lớp ảnh, phải thực hiện bước xử lý chuẩn hóa vector đặc trưng để chiếu vào không gian 2 chiều và mã hóa nhãn.

Giai đoạn tiền xử lý:

Bước chuẩn hóa vector

```

in_encoder = Normalizer()
emdTrainX_norm = in_encoder.transform(emdTrainX)
emdTestX_norm = in_encoder.transform(emdTestX)

```

Bước mã hóa nhãn

```

out_encoder = LabelEncoder()
out_encoder.fit(trainy)
trainy_enc = out_encoder.transform(trainy)
testy_enc = out_encoder.transform(testy)

```

Giai đoạn huấn luyện mô hình:

```

model = SVC(kernel='linear', probability=True)
model.fit(emdTrainX_norm, trainy_enc)

```

Giai đoạn kiểm thử:

```

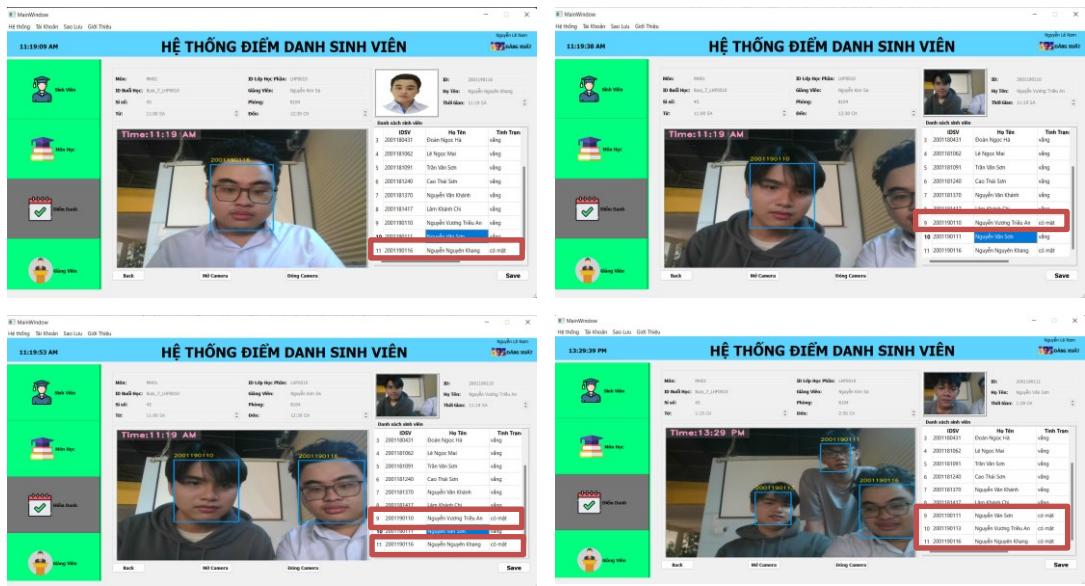
yhat_train = model.predict(emdTrainX_norm)
yhat_test = model.predict(emdTestX_norm)

```

Kết quả của quá trình huấn luyện như sau:

Dữ liệu	Số ảnh	Độ chính xác
Train	1174	99,48%
Test	504	99,0%

4.4. Hệ thống điểm danh:



Hình 16. Hình ảnh từ chức năng điểm danh của hệ thống nhận diện một khuôn mặt và nhiều khuôn mặt.

Khi đã nhận diện được các khuôn mặt của sinh viên, hệ thống sẽ lấy định danh của khuôn mặt để tiến hành điểm danh cho danh sách sinh viên trong cơ sở dữ liệu. Danh sách định danh của sinh viên sẽ được cập nhật lên hệ thống quản lý sinh viên một cách tự động. Khuôn mặt lạ xuất hiện trong ảnh được xác định “unknown”. Dưới đây là kết quả thực hiện điểm danh trong thời gian thực với một đối tượng và nhiều đối tượng trong ảnh.

5. KẾT LUẬN

Qua kết quả nghiên cứu cho thấy sử dụng mô hình facenet để tạo vector đặc trưng tối ưu sau đó kết hợp với bộ phân lớp SVM để cho kết quả nhận diện có độ chính xác cao trong thời gian thực. Hệ thống điểm danh tự động hoạt động tốt khi nhận dạng một khuôn mặt và vẫn đáp ứng độ chính xác khi nhận diện nhiều khuôn mặt nhưng với tốc độ xử lý chậm hơn.

Trong bước kế tiếp, nghiên cứu tiếp tục tăng cường dữ liệu về gương mặt của sinh viên để áp dụng nhận diện gương mặt tốt hơn và nghiên cứu xử lý loại bỏ khuôn mặt “unknown” gây nhiễu cho hệ thống trong quá trình nhận diện trong thời gian thực, đồng thời cải thiện tốc độ khi nhận diện nhiều đối tượng; mở rộng ứng dụng nhận dạng trong một số hệ thống mở khóa và hệ thống giám sát khác.

TÀI LIỆU THAM KHẢO

- Nicolas Ortiz, et al., *Survey of biometric pattern recognition via machine learning techniques*, Contemporary Engineering Sciences, vol. 11, no. 34, pp. 1677-1694, 2018.
- Stan Z. Li, Anil K. Jain, *Handbook of Face Recognition 2nd ed*, Springer Verlag, New York, 2011.

3. Viola P., Jones M.J. - *Robust real-time face detection*, International Journal of Computer Vision 57 (2) (2004) 137-154.
4. Khaled Younis, Abdullah A Alkhateeb .*A New Implementation of Deep Neural Networks for Optical Character Recognition and Face Recognition*. Proceedings of the New Trends in Information Technology. The University of Jordan, Amman, Jordan. 25-27 April 2017.
5. A. Krizhevsky, I. Sutskever and G. E. Hinton, *Imagenet classification with deep convolutional neural networks*, in Advances in neural information processing systems, 2012. [14].
6. K. Simonyan, Andrew Zisserman, 2015. *Very Deep Convolutional Networks for Large-Scale Image Recognition*. In Journal CoRR, volume17.
7. Lionel Landry S. De o, Elie T. Fute, Emmanuel Tonye, 2018. *CNNsFR: A Convolutional Neural Network System for Face Detection and Recognition*. International Journal of Advanced Computer Science and
8. Huỳnh Phước Hải, Nguyễn Văn Hòa, Đỗ Thanh Nghị. *so sánh mô hình học sâu với các phương pháp học tự động khác trong phân lớp dữ liệu biểu hiện gen microarray*. Kỷ yếu Hội nghị Quốc gia lần thứ XII về Nghiên cứu cơ bản và ứng dụng Công Nghệ thông tin (FAIR), 2017
9. Patrik Kamencay, Miroslav Benco, Tomas Mizdos, Roman Radil, 2017. *A New Method for Face Recognition Using Convolutional Neural Network*. Digital Image Processing and Computer Graphics, Vol. 15, No. 4, pp.663-672
10. Mustafa Zuhaer Nayef Al-Dabagh, MH Mohammed Alhabibat al.FH Al-Mukhtar, "Face recognition system based on kernel discriminant analysis, k-nearest neighbor and support vector machine", International Journal of Research and Engineering, vol.5, no. 3, pp. 335-338, 2018. (svm)
11. J Kulandai Josephine JulinaT Sree Sharmila. *Facial recognition using histogram of gradients and support vector machines*. In 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP). 2017. IEEE (svm)
12. Shanshan Guo, Shiyu Chen et al.Yanjie Li. *Face recognition based on convolutional neural network and support vector machine*. in 2016 IEEE International conference on Information and Automation (ICIA). 2016. IEEE
13. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, Joint face detection and alignment using multitask cascaded convolutional networks, IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, 2016.
14. Florian Schroff , Dmitry Kalenichenko , James Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering, 2015
15. Corinna CortesVladimir Vapnik, *Support-vector networks*, Machine learning, vol. 20, no. 3, pp. 273-297, 1995.

ABSTRACT

AUTOMATIC STUDENT ATTENDANCE USING FACE RECOGNITION

Tran Thi Van Anh¹, Tran Khanh Dang^{1,*}, Nguyen Vuong Trieu An¹,
Nguyen Van Son¹, Nguyen Nguyen Khang¹

¹Ho Chi Minh City University of Food Industry, Vietnam

*Email: khanh@hufi.edu.vn

This paper presents a method of automatic student face recognition in real time by scanning the face of the student from the camera to perform attendance. Firstly, we use MTCNN (multitask cascaded convolutional networks) to detect and mark faces. Secondly, use the pre-trained Facenet model to extract the feature vector and combine with SVM (Support Vector Machine) to train the face recognition model. Experimental results and applied application model give 99% accuracy on student dataset. In addition, the proposed method also gives good recognition results for images containing many faces.

Keywords: Face recognition, MTCNN, Facenet, SVM, automatic attendance

CÁC CÔNG CỤ NÂNG CAO CHẤT LƯỢNG VÀ ĐÁNH GIÁ GIẢNG DẠY

Đào Minh Châu^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: chaudm@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Công nghệ thông tin đã thay đổi đáng kể trong nhiều khía cạnh của cuộc sống hàng ngày, lĩnh vực giáo dục đã được cách mạng hóa hoàn toàn. Với sự tiến bộ nhanh chóng của công nghệ đã mang lại những công cụ, phần mềm và ứng dụng sáng tạo đã thay đổi phương pháp giảng dạy và cải thiện chất lượng và đánh giá giảng dạy tổng thể. Tìm hiểu những công cụ nâng cao chất lượng giảng dạy và đánh giá giảng dạy, đổi mới độ học tập của sinh viên, đánh giá năng lực và đưa ra phản hồi cá nhân trong môi trường giáo dục, từ đó từ đó tăng cường tính minh bạch và hiệu suất của việc dạy và học.

Từ khóa: Công cụ, chất lượng, đánh giá giảng dạy

1. MỞ ĐẦU

Đối với việc đánh giá giảng dạy, việc đánh giá việc giảng dạy từ lâu đã là một khía cạnh quan trọng của hệ thống giáo dục, nhằm đánh giá hiệu quả của các phương pháp giảng dạy và đảm bảo chất lượng giáo dục cao. Trong những năm gần đây công nghệ đã đóng một vai trò quan trọng trong việc cách mạng hóa cách đánh giá việc giảng dạy, cung cấp các công cụ và phương pháp đổi mới nhằm nâng cao tính chính xác, khách quan và hiệu quả của quá trình đánh giá.

Một trong những đóng góp đáng chú ý nhất để đánh giá việc giảng dạy là sự phát triển của các công cụ đánh giá dựa trên dữ liệu. Thông qua việc sử dụng các thuật toán học máy và phân tích dữ liệu nâng cao, khoa học máy tính đã cho phép thu thập, phân tích và giải thích lượng lớn dữ liệu về các khía cạnh khác nhau của việc giảng dạy, bao gồm hiệu suất, sự tham gia và phản hồi của học sinh.

2. CÁC CÔNG CỤ NÂNG CAO CHẤT LƯỢNG VÀ ĐÁNH GIÁ GIẢNG

Một số công cụ đánh giá hiệu quả công tác giảng dạy của giáo viên hiện nay [1]:

CEL 5D+ Teacher Evaluation Rubric 2.0

Marzano Art and Science of Teaching Framework

The Framework for Teaching by Charlotte Danielson

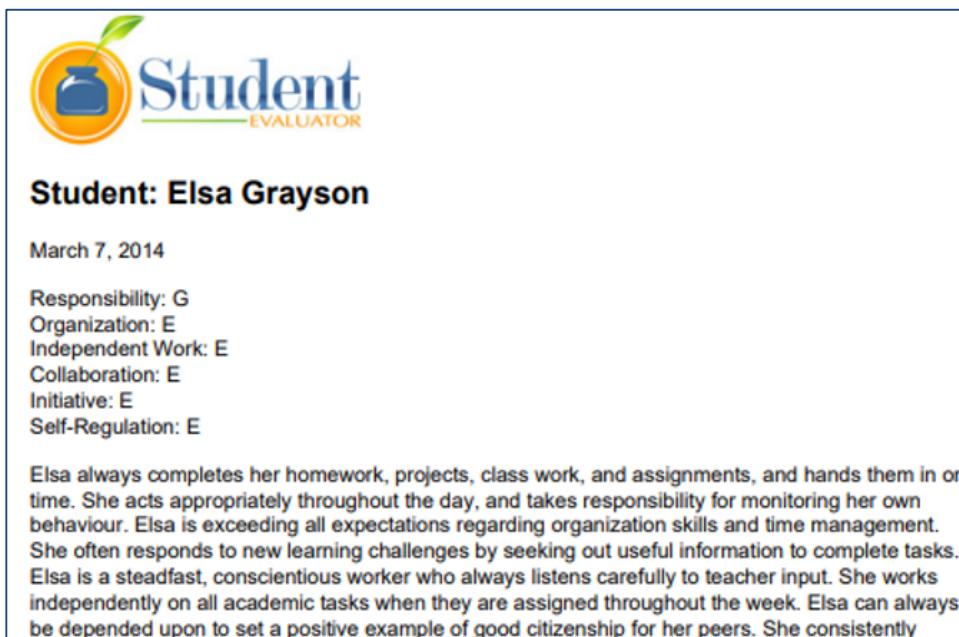
Google classroom

Rubric này cung cấp một khung đánh giá chi tiết và toàn diện về hiệu quả công tác giảng dạy của giáo viên dựa trên năm lĩnh vực chính: lập kế hoạch và chuẩn bị, giảng dạy, môi trường lớp học, trách nhiệm chuyên môn và đạt được thành tích học sinh.

Những công cụ này cung cấp những hiểu biết có giá trị về hiệu quả của các phương pháp giảng dạy, xác định các điểm mạnh và điểm yếu, đồng thời cung cấp thông tin cho quá trình ra quyết định dựa trên bằng chứng để cải thiện việc giảng dạy. Các công cụ đánh giá dựa trên dữ liệu cũng tạo điều kiện thuận lợi cho việc xác định các mô hình, xu hướng và mối tương quan trong thực tiễn giảng dạy mà các phương pháp đánh giá truyền thống có thể không thấy rõ. Cách tiếp cận dựa trên dữ liệu này nâng cao tính khách quan và hiệu lực của quy trình đánh giá, đảm bảo rằng các quyết định liên quan đến chất lượng giảng dạy dựa trên bằng chứng thực nghiệm thay vì ý kiến chủ quan.

Các công cụ này đã tạo điều kiện phát triển các phương pháp sáng tạo để đánh giá việc giảng dạy, chẳng hạn như quan sát dựa trên video và hệ thống tính điểm tự động. Các quan sát dựa trên video cho phép người đánh giá quan sát các hoạt động giảng dạy một cách chân thực và toàn diện hơn, nắm bắt được nhiều hành vi, tương tác và chiến lược giảng dạy. Các công cụ này đã cho phép sử dụng phần mềm phân tích video tự động hóa quá trình mã hóa và phân tích các hành vi dạy học, giảm tính chủ quan và thiên vị trong quá trình đánh giá. Những quan sát dựa trên video này cung cấp nguồn dữ liệu phong phú để đánh giá hiệu quả giảng dạy, đưa ra phản hồi có giá trị cho giáo viên và thúc đẩy sự tự suy nghĩ và phát triển chuyên môn.

Cho phép sử dụng các hệ thống tính điểm tự động để đánh giá bài làm của học sinh, chẳng hạn như bài tiểu luận, dự án và đánh giá. Các hệ thống này sử dụng các thuật toán máy học và xử lý ngôn ngữ tự nhiên để phân tích và đánh giá bài làm của học sinh, cung cấp phản hồi khách quan và chuẩn hóa về các khía cạnh khác nhau trong thành tích của học sinh.



Student: Elsa Grayson

March 7, 2014

Responsibility: G
 Organization: E
 Independent Work: E
 Collaboration: E
 Initiative: E
 Self-Regulation: E

Elsa always completes her homework, projects, class work, and assignments, and hands them in on time. She acts appropriately throughout the day, and takes responsibility for monitoring her own behaviour. Elsa is exceeding all expectations regarding organization skills and time management. She often responds to new learning challenges by seeking out useful information to complete tasks. Elsa is a steadfast, conscientious worker who always listens carefully to teacher input. She works independently on all academic tasks when they are assigned throughout the week. Elsa can always be depended upon to set a positive example of good citizenship for her peers. She consistently

Hình 1. Mẫu đánh giá học sinh

Hình 1 ví dụ về mẫu đánh giá học sinh dựa trên 1 chương trình điện toán có tên là “Student Evaluator” [2], đánh giá. Elsa là học sinh xuất sắc với kỹ năng tổ chức, quản lý thời

gian và học tập tích cực. Cô ấy có thái độ chu đáo và đầy động lực, xuất sắc trong học tập và tạo gương mẫu tích cực cho bạn bè về công dân và cộng tác.

Hệ thống tính điểm tự động mang lại một số lợi thế, bao gồm tăng hiệu quả, tính nhất quán và độ tin cậy trong quá trình đánh giá. Chúng cũng cho phép giáo viên tập trung vào việc cung cấp phản hồi định tính và hướng dẫn được cá nhân hóa cho học sinh, thay vì dành quá nhiều thời gian cho việc chấm điểm thủ công. Tuy nhiên, điều quan trọng cần lưu ý là các hệ thống chấm điểm tự động không phải là không có giới hạn, và cần phải xác nhận và hiệu chỉnh cẩn thận để đảm bảo tính chính xác và công bằng của chúng.

 Basic Info	Course 1 of 6 in the Business Foundations Specialization
 Commitment	5 weeks of study, 4-6 hours/week
 Language	English, Subtitles: Arabic, French, Portuguese (European), Chinese (Simplified), Italian, Vietnamese, German, Russian, Spanish Volunteer to translate subtitles for this course
 How To Pass	Pass all graded assignments to complete the course.

Syllabus

Week 1

BRANDING: Marketing Strategy and Brand Positioning

Professor Kahn starts us off with the first of two Branding modules: Marketing Strategy and Brand Positioning. For an overview of all concepts covered in the course, please read the syllabus below. Additional info may be found in the Course Pages. Please participate in the discussion forums as your input will enhance the overall experience of this course!

 7 videos, 3 readings [expand](#)

 Graded: Quiz #1

Hình 2. Đánh giá dạy và học bởi hệ thống máy tính

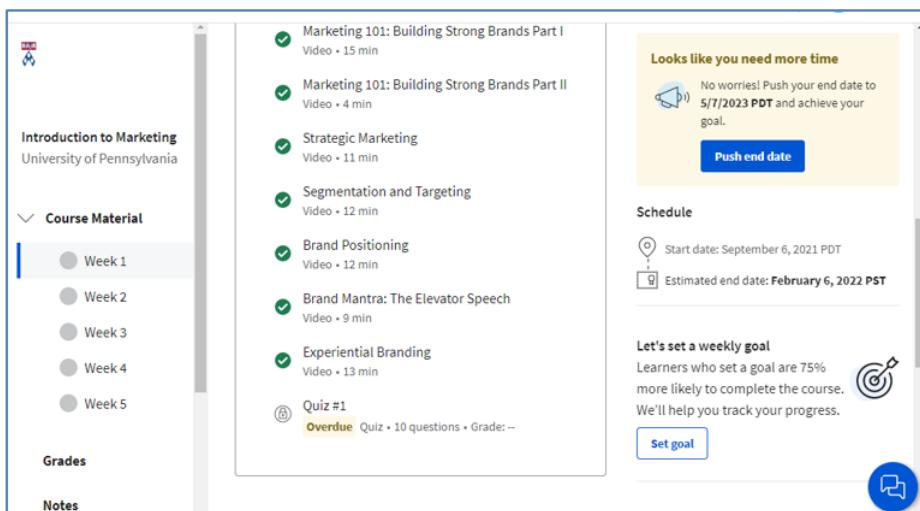
Hình 2 là một ví dụ về chương trình dạy, học và đánh giá được tạo bởi hệ thống máy tính [3]

Ngoài ra, tạo điều kiện thuận lợi cho việc sử dụng các công cụ khảo sát, bảng câu hỏi và phản hồi để thu thập thông tin đầu vào từ học sinh, giáo viên và các bên liên quan khác về hiệu quả giảng dạy. Những công cụ này cho phép thu thập dữ liệu định tính và định lượng về các khía cạnh khác nhau của việc giảng dạy, chẳng hạn như chiến lược giảng dạy, môi trường lớp học và sự tham gia của sinh viên. Khoa học máy tính đã cho phép phát triển các nền tảng khảo sát trực tuyến, công cụ trực quan hóa dữ liệu và kỹ thuật phân tích tình cảm nhằm hợp lý hóa quy trình thu thập và phân tích dữ liệu, giúp quy trình này hiệu quả và khả thi hơn. Việc sử dụng các công cụ khảo sát và phản hồi cung cấp những hiểu biết có giá trị về nhận thức và kinh nghiệm của các bên liên quan, có thể cung cấp thông tin cho quá trình đánh giá và hướng dẫn các nỗ lực cải tiến hướng dẫn.

Ngoài ra, khoa học máy tính đã cách mạng hóa cách thức giảng dạy của giáo viên. Việc tích hợp công nghệ trong lớp học đã tạo điều kiện thuận lợi cho việc sử dụng các công cụ đa phương tiện như bảng thông minh, bảng tương tác, máy chiếu và phần mềm giáo dục, cho phép giáo viên tạo ra những bài học sinh động và hấp dẫn trực quan thu hút sự chú ý của học sinh. Những công cụ này cho phép trải nghiệm học tập tương tác, trong đó học sinh có thể tích cực tham gia vào bài học, đặt câu hỏi và nhận phản hồi ngay lập tức, giúp nâng cao hiểu biết của họ về nội dung. Hơn nữa, khoa học máy tính đã tạo điều kiện thuận lợi cho việc sử dụng các hệ thống quản lý học tập và các nền tảng trực tuyến, cho phép giáo viên tạo và chia sẻ nội dung kỹ thuật số, bài tập và đánh giá, quản lý điểm số cũng như giao tiếp với học sinh và phụ huynh một cách hiệu quả và có tổ chức hơn. Điều này hợp lý hóa các nhiệm vụ hành chính, giảm thủ tục giấy tờ và cho phép giáo viên dành nhiều thời gian hơn cho việc giảng dạy, cung cấp phản hồi kịp thời và giải quyết các nhu cầu cá nhân của học sinh, điều này cuối cùng sẽ cải thiện chất lượng giảng dạy.

Theo dõi tiến độ học tập của sinh viên, đánh giá năng lực của học viên, tạo điều kiện cho các trải nghiệm học tập được cá nhân hóa, đưa ra phản hồi cá nhân từ đó tăng cường tính minh bạch và hiệu suất của việc học

Khoa học máy tính đã tạo điều kiện cho các trải nghiệm học tập được cá nhân hóa và thích ứng. Thông qua phân tích dữ liệu và thuật toán học máy, phần mềm và ứng dụng giáo dục có thể theo dõi và phân tích hiệu suất, sở thích và tiến độ của học sinh, đồng thời cung cấp các lộ trình học tập tùy chỉnh phù hợp với nhu cầu và khả năng cá nhân của họ. Điều này cho phép học sinh học theo tốc độ của riêng mình, nhận được các biện pháp can thiệp có mục tiêu và khám phá nội dung phù hợp với sở thích và điểm mạnh của các em. Khoa học máy tính đã cho phép phát triển các ứng dụng thực tế ảo và thực tế tăng cường, mô phỏng và trò chơi hóa trong giáo dục, mang lại trải nghiệm học tập nhập vai và trải nghiệm. Những công nghệ này cho phép sinh viên hình dung các khái niệm phức tạp, tham gia vào các thí nghiệm ảo và tham gia vào các tình huống mô phỏng, giúp họ hiểu sâu hơn và ghi nhớ nội dung. Trải nghiệm học tập được cá nhân hóa và thích ứng trao quyền cho học sinh nắm quyền sở hữu việc học của mình, thúc đẩy các kỹ năng học tập tự định hướng, đồng thời nâng cao động lực và sự tham gia của các em trong lớp học.



Hình 3. Phần mềm theo dõi, phân tích tiến độ của học sinh

Hình 3 là ví dụ về phần mềm và ứng dụng giáo dục có thể theo dõi và phân tích hiệu suất, sở thích và tiến độ của học sinh [5]

Công nghệ đã tiến một chặng đường dài trong những năm gần đây, và hiện nay có rất nhiều tài nguyên dành cho sinh viên có thể giúp họ theo đuổi việc học của mình. Ví dụ: có nhiều nền tảng trực tuyến và hệ thống quản lý học tập có thể giúp sinh viên theo dõi bài tập, theo dõi tiến độ và cung cấp phản hồi về hiệu suất của họ. Ngoài ra, có nhiều công cụ lập trình khác nhau có thể giúp sinh viên gỡ lỗi, phân tích mã và tối ưu hóa, giúp quá trình học tập dễ tiếp cận hơn nhiều.

Grades					
Item	Status	Due	Weight	Grade	
Quiz #1 Quiz	Locked	Jan 16, 2022 11:59 PM PST	20%	--	
Quiz #2 Quiz	Locked	Jan 23, 2022 11:59 PM PST	20%	--	
Quiz #3 Quiz	Locked	Jan 30, 2022 11:59 PM PST	20%	--	
Final Exam Quiz	Locked	Feb 6, 2022 11:59 PM PST	40%	--	

Hình 4. Mô hình dạy và đánh giá trực tuyến

Hình 4 là một mô hình trong việc dạy trực tuyến và đánh giá trực tuyến được tạo bởi hệ thống máy tính.

Đánh giá là một phần quan trọng trong quá trình giáo dục, tuy nhiên nó không đủ để đảm bảo sinh viên có thể học một cách hiệu quả. Để đạt được điều này, cần hỗ trợ sinh viên trong suốt quá trình học tập của họ. Một cách để làm điều này là cung cấp cho sinh viên quyền truy cập vào các công cụ hỗ trợ học tập. Các công cụ này có thể giúp sinh viên hiểu sâu hơn về các khái niệm cơ bản và giải quyết các vấn đề phức tạp hơn trong lĩnh vực đang học.

Giáo viên hướng dẫn cũng có thể hỗ trợ sinh viên theo đuổi nghiên cứu của họ bằng cách sẵn sàng tư vấn và hỗ trợ. Điều này có thể đạt được thông qua nhiều phương tiện khác nhau, chẳng hạn như giờ hành chính trực tuyến, thư điện tử và diễn đàn. Hơn nữa, người hướng dẫn có thể cung cấp cho sinh viên các tài nguyên bổ sung, chẳng hạn như sách, bài báo và video có thể giúp họ hiểu sâu hơn về các chủ đề được đề cập trong lớp.

Tóm lại, với sự tiến bộ nhanh chóng của công nghệ, khoa học máy tính đã mang lại những công cụ, phần mềm và ứng dụng sáng tạo đã thay đổi phương pháp giảng dạy và cải thiện chất lượng giáo dục tổng thể

3. KẾT LUẬN

Bài viết này dừng lại ở việc tìm hiểu các công cụ nâng cao chất lượng và đánh giá giảng dạy.

Các công cụ nâng cao và đánh giá chất lượng giảng dạy không chỉ giúp cải thiện quá trình truyền đạt kiến thức mà còn tiềm năng phát triển trong tương lai. Trong tương lai sẽ xuất hiện các phần mềm và hệ thống trí tuệ nhân tạo có thể được sử dụng để theo dõi và đánh giá phản hồi từ học sinh. Điều này giúp giáo viên hiểu rõ hơn về cách mà học sinh học tập và hiệu quả của quá trình giảng dạy. Điều này giúp tăng cường sự tương tác và tăng cường khả năng học tập cá nhân của mỗi học sinh. Công cụ như vậy có thể cung cấp thông tin phản hồi tức thì và định hướng giúp giáo viên điều chỉnh phương pháp giảng dạy và tạo ra một môi trường học tập tốt hơn.

Ngoài ra, có thể mong đợi sự phát triển của công nghệ ảo hóa và thực tế tăng cường trong giáo dục. Các công cụ này cho phép học sinh trải nghiệm thực tế ảo, đưa họ vào các tình huống và môi trường học tập tương tác. Chẳng hạn, học sinh có thể tham gia vào các bài giảng ảo, thực hiện thí nghiệm trong một môi trường an toàn và thực hành các kỹ năng trong một môi trường học tập ảo. Điều này giúp học sinh hứng thú hơn và tạo ra trải nghiệm học tập tương tác và sinh động hơn.

TÀI LIỆU THAM KHẢO

1. <https://www.questionpro.com/blog/teacher-evaluation/>
2. <https://studentevaluator.com/wp-content/uploads/sample-report.pdf>
3. <https://www.coursera.org/learn/wharton-marketing/home/assignments>
4. <https://scholarworks.uark.edu/cgi/viewcontent.cgi?article=1901&context=etd>
5. <https://www.coursera.org/learn/wharton-marketing/home/week/1>

ABSTRACT

THEORETICAL FOUNDATIONS OF TECHNOLOGY ACCEPTANCE AND USAGE MODELS

Dao Minh Chau^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: chaudm@hufi.edu.vn

Information technology has significantly changed many aspects of daily life, and the field of education has been completely revolutionized. The rapid advancement of technology has brought innovative tools, software, and applications that have changed teaching methods and improved the overall quality and evaluation of teaching. Discovering tools to enhance the quality of teaching and evaluation, track student progress, assess competency, and provide personalized feedback in educational environments helps to increase transparency and efficiency of teaching and learning.

Keywords: tools, quality, teaching evaluation

HUFI-STPMS: HỆ THỐNG QUẢN LÝ ĐIỂM RÈN LUYỆN SINH VIÊN TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM (HUFI)

Trần Trương Tuấn Phát¹, Đặng Trần Khánh¹, Ngô Thanh Hùng^{1,*}
Trần Thị Vân Anh¹, Lê Thị Trà My¹, Đoàn Huỳnh Tuyết Anh¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: hungnthan@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Tại Trường Đại học Công nghiệp Thực phẩm TP Hồ Chí Minh (HUFI) hầu hết các hoạt động quản lý đều được tin học hóa. Mỗi đơn vị trong trường đều được phân quyền sử dụng phần mềm, cho phép quản lý, cập nhật và khai thác cơ sở dữ liệu. Hệ thống phần mềm hiện tại đáp ứng các chức năng chung và đồng bộ trong phạm vi toàn trường. Tuy nhiên hệ thống quản lý điểm rèn luyện tại trường hiện chưa được đồng bộ. Mỗi đơn vị (khoa quản lý, phòng ban liên quan) có cách làm riêng, có nơi làm thủ công, có nơi bằng phần mềm, có phần mềm thì chỉ hỗ trợ một/một số giai đoạn nào đó như cho sinh viên đăng ký hoạt động hoặc điểm danh sinh viên tham gia hoạt động, ... Nhưng nhìn chung thì các phần mềm này chưa thể hỗ trợ tốt cho công tác quản lý điểm rèn luyện sinh viên. Do đó trong nghiên cứu này đề xuất hệ thống quản lý điểm rèn luyện sinh viên HUFI-STPMS với đặc điểm là quản lý xuyên suốt quá trình quản lý điểm rèn luyện và đặc biệt là hỗ trợ điểm danh bằng phần mềm một cách thuận lợi, chính xác.

Từ khóa: Điểm rèn luyện, điểm danh bằng QR Code

1. GIỚI THIỆU

Nhằm góp phần thực hiện mục tiêu giáo dục là đào tạo con người Việt Nam phát triển toàn diện, có đạo đức, tri thức, sức khỏe, thẩm mỹ và nghề nghiệp, trung thành với lý tưởng độc lập dân tộc và chủ nghĩa xã hội, Bộ Giáo dục và Đào tạo đã ban hành quyết định về việc ban hành quy chế đánh giá kết quả rèn luyện của học sinh – sinh viên các cơ sở giáo dục đại học và trường trung cấp chuyên nghiệp hệ chính quy.

Kết quả đánh giá rèn luyện từng học kỳ, từng năm học của sinh viên được lưu trong hồ sơ quản lý của trường, được sử dụng trong việc xét duyệt học bỗng, xét khen thưởng – kỷ luật, xét thôi học, ngừng học, xét lưu trú ký túc xá, xét giải quyết việc làm thêm, xét miễn giảm chi phí, dịch vụ và sinh hoạt trong ký túc xá,... Kết quả đánh giá rèn luyện toàn khóa của sinh viên được lưu trong hồ sơ quản lý sinh viên của cơ sở giáo dục đại học, làm căn cứ để xét tốt nghiệp, làm luận văn hoặc khóa luận tốt nghiệp. Kết quả đánh giá rèn luyện toàn khóa được ghi chung vào bảng điểm kết quả học tập và lưu trong hồ sơ của sinh viên khi tốt nghiệp ra trường. Sinh viên có kết quả rèn luyện xuất sắc được cơ sở giáo dục đại học xem xét biểu dương, khen thưởng. Sinh viên bị xếp loại rèn luyện yếu, kém trong hai học kỳ liên tiếp thì phải tạm ngừng học ít nhất một học kỳ ở học kỳ tiếp theo và nếu bị xếp loại rèn luyện yếu, kém hai học kỳ liên tiếp lần thứ hai thì sẽ bị buộc thôi học. Vì vậy, việc tổ chức đánh giá và lưu trữ điểm rèn luyện của sinh viên cần được thực hiện liên tục mỗi học kỳ dẫn đến kho dữ

liệu ngày càng khổng lồ, việc truy xuất gấp không ít khó khăn, đòi hỏi mỗi trường phải có biện pháp cải thiện. Biện pháp cải thiện hiệu quả nhất chính là tin học hóa quy trình đánh giá điểm rèn luyện cho sinh viên ở trường. Cũng trên tinh thần ấy, Trường Đại học Công Nghiệp Thực Phẩm TP.Hồ Chí Minh hàng năm vẫn tổ chức xét điểm rèn luyện cho sinh viên vào cuối mỗi học kỳ. Tuy nhiên, toàn bộ quy trình hiện tại còn nhiều hạn chế, tốn rất nhiều thời gian và chi phí. Bên cạnh đó, với số lượng sinh viên tại trường ngày càng đông làm cho công tác tổ chức đánh giá, lưu trữ, sử dụng điểm rèn luyện gặp nhiều khó khăn. Vì vậy việc nghiên cứu và tin học hóa quá trình đánh giá và quản lý điểm rèn luyện để từ đó có thể mở rộng sử dụng ra toàn trường là một yêu cầu có tính thực tiễn và cấp thiết.

Nhằm mục đích đáp ứng việc đánh giá điểm rèn luyện cho sinh viên và việc quản lý, khai thác điểm rèn luyện của sinh viên cho cán bộ quản lý. Hỗ trợ giảng viên quá trình quản lý hoạt động, điểm rèn luyện, vi phạm, phản hồi từ sinh viên, hoạt động diễn ra ngoài trường, chốt điểm và tổng kết điểm sinh viên. Hỗ trợ sinh viên quá trình xem hoạt động, tình hình tham gia hoạt động, kết quả điểm rèn luyện sinh viên, phản hồi vi phạm và hoạt động. Hỗ trợ đăng ký và điểm danh hoạt động sinh viên. Hỗ trợ ghi nhận những hoạt động ngoài trường mà sinh viên đã tham gia. Từ đó chúng tôi đã xây dựng hệ được xây dựng hoàn toàn mới và sẽ được sử dụng thử nghiệm tại khoa Công nghệ thông tin. Sau đó, hệ thống sẽ được ứng dụng và cải tiến phù hợp cho các khoa khác trong trường và hướng đến việc sử dụng thống nhất tại Trường Đại học Công nghiệp thực phẩm TP.Hồ Chí Minh.

2. CÔNG TRÌNH LIÊN QUAN

2.1. Đánh giá tổng quan tình hình nghiên cứu thuộc lĩnh vực của đề tài

Công ty Xsoft (địa chỉ Xsoft.vn) xây dựng phần mềm quản lý điểm rèn luyện bậc cao đẳng, đại học X-DRL [1] với các chức năng: Tạo mẫu đánh giá điểm rèn luyện; chấm điểm rèn luyện trực tuyến; quản lý điểm rèn luyện sinh viên; lấy dữ liệu sẵn có để đưa vào phần mềm: Điểm trung bình học kỳ, khen thưởng, kỷ luật... ; xuất dữ liệu ra các tệp: Excel, Word, PDF, Img để nộp cho phòng Công tác sinh viên; kết xuất các báo cáo thống kê. X-DRL đảm bảo quá trình đánh giá được chính xác, công bằng, công khai và dân chủ và theo đúng quy trình: Từng học sinh, sinh viên cẩn cứ vào kết quả rèn luyện, tự đánh giá theo mức điểm chi tiết do Trường quy định trên hệ thống X-DLR trực tuyến. Giáo viên chủ nhiệm được phân quyền xem xét mức điểm của từng học sinh, sinh viên. Trường khoa được phân quyền xem xét điểm rèn luyện của học sinh, sinh viên trong Khoa và xác nhận chuyển dữ liệu đúng lên Hiệu trưởng. Nếu có hội đồng khoa sẽ được quản lý thành phần hội đồng đánh giá kết quả. Hiệu trưởng được phân quyền xem xét và công nhận kết quả rèn luyện sinh viên. Sau khi được công nhận bởi Hiệu trưởng, kết quả đánh giá và phân loại sinh viên sẽ được công khai và thông báo cho học sinh, sinh viên biết trên Công công khai Điểm rèn luyện.

Công ty VINAAS (<https://vinaas.com/>) xây dựng phần mềm quản lý hồ sơ sinh viên online trên nền tảng Microsoft.NET và cơ sở dữ liệu SQL Server. Phần mềm hỗ trợ quản lý gần như toàn bộ các thông tin liên quan đến sinh viên, học tập, rèn luyện của sinh viên, ... [2]

Bùi Công Danh và Lê Văn Bé đã xây dựng hệ thống quản lý điểm rèn luyện sinh viên trên thiết bị di động [3]. Hệ thống gồm 3 thành phần: E-google – sử dụng google form để sinh viên đăng ký hoạt động; E-smartphone – phần mềm chạy trên điện thoại thông minh cho phép quét mã vạch để điểm danh sinh viên và quản lý danh sách sinh viên tham gia, gửi danh sách

về cơ sở dữ liệu của hệ thống; E-application – phần mềm chạy trên máy tính để bàn cho phép quản lý thông tin của các hoạt động, danh sách sinh viên đã đăng ký các hoạt động, danh sách các sinh viên đã tham gia các hoạt động, thống kê điểm rèn luyện của sinh viên, của lớp.

Trường Đại học Tài chính Marketing đã triển khai hệ thống online cho việc kê khai hoạt động đánh giá điểm rèn luyện, việc kê khai được sinh viên tự khai báo một số hoạt động ngoài sự quản lý của nhà trường và minh chứng phải tự nộp về Phòng Công tác Sinh viên, hệ thống chưa hỗ trợ lưu trữ các minh chứng này.

Trường Đại học Công nghệ TP.HCM cung cấp một hệ thống online cho việc đánh giá điểm rèn luyện. Sinh viên thực hiện việc kê khai các hoạt động tham gia và cung cấp hình ảnh các minh chứng tham gia các hoạt động. Tiếp theo, Lớp trưởng các lớp sẽ tiến hành đánh giá từng sinh viên. Việc đánh giá hoạt động của một sinh viên là hoàn toàn dựa trên cảm tính của cá nhân lớp trưởng.

Trường Đại học Nông lâm Tp.HCM cũng thực hiện trên hệ thống và cho sinh viên tự kê khai các hoạt động và sau đó kiểm duyệt đánh giá thủ công bằng tay nhưng với 3 cấp đánh giá là Lớp, Khoa, Trường.

Báo cáo “Thực tiễn triển khai công tác đánh giá kết quả rèn luyện của sinh viên tại Đại học Quốc gia Tp. Hồ Chí Minh” của tác giả Nguyễn Đức Nghĩa -Đại học Quốc gia TP.HCM cho thấy sự hiệu quả của việc đánh giá bằng hệ thống trực tuyến của một số trường.

Ngoài ra, nhiều trường vẫn triển khai quy trình kê khai tổng hợp bằng phương pháp thủ công. Hầu hết các đề xuất hệ thống liên quan đến các ứng dụng được sinh viên kê khai và trải qua một hoặc nhiều cấp đánh giá lại. Tất cả các hệ thống chưa có sự giám sát sinh viên từ thời điểm đăng ký đến quá trình tham gia vào hoạt động. Các hệ thống đều cho sinh viên tham gia vào hệ thống kê khai khi đến các thời điểm tổng kết. Một số công nghệ dùng để điểm danh như: RFID [4] – là công nghệ để trao đổi thông tin thông qua sóng vô tuyến. Barcode [5] – còn gọi là mã vạch, là một phương thức biểu diễn dữ liệu (một dãy số) trên các bề mặt của sản phẩm, hàng hóa. Dữ liệu được biểu diễn dưới dạng một dãy số đi kèm với một dãy các vạch. QR-Code [6] – còn gọi là mã QR, là một loại mã có cơ chế hoạt động tương tự như các loại mã vạch thông thường. Website xử lý điểm danh. Công nghệ nhận dạng ảnh [7]. Bluetooth [8] – là một chuẩn công nghệ truyền thông không dây tầm gần giữa các thiết bị điện tử.

2.2. Luận giải về việc đặt ra mục tiêu và những nội dung cần nghiên cứu của đề tài

Trong việc quản lý điểm rèn luyện có 4 giai đoạn chính là: đề xuất hoạt động, cho sinh viên đăng ký, điểm danh tham gia hoạt động và phê duyệt điểm số. Trong đó việc điểm danh tham gia hoạt động là công việc tiêu tốn nhiều công sức và có thể phát sinh sai sót.

Trong các phần mềm được mô tả ở trên thì phần mềm X-DRL chỉ tập trung phần chấm và xét duyệt điểm rèn luyện, không hiện thực quá trình đề xuất hoạt động, đăng ký và điểm danh. Phần mềm quản lý hồ sơ sinh viên online thì có đề cập đến công tác quản lý điểm rèn luyện nhưng không công bố các thông tin chi tiết về hệ thống. Ở hệ thống quản lý điểm rèn luyện đề xuất bởi Bùi Công Danh và Lê Văn Bé thì việc sử dụng module quét mã vạch để điểm danh tạo tăng được hiệu quả và độ chính xác của quá trình điểm danh, tuy nhiên quá trình đề xuất và đăng ký còn khá đơn giản.

Ở một số trường đại học tại TP. Hồ Chí Minh như Trường Đại học Tài chính Marketing, Trường Đại học Công nghệ Tp.HCM, Trường Đại học Nông lâm Tp.HCM, các trường thuộc Đại học Quốc gia Tp. HCM, ... đều có ban hành văn bản quy trình thực hiện đánh giá điểm rèn luyện và có các hệ thống quản lý dữ liệu đánh giá, xét duyệt của sinh viên, của ban cán sự lớp, có vấn học tập và các cấp quản lý dựa trên các minh chứng do sinh viên tự cung cấp. Tuy nhiên việc đánh giá và xét duyệt còn thực hiện thủ công, do đó dễ gây nhầm lẫn và thiếu sót cho các sinh viên trong quá trình tự đánh giá, cũng như gây khó khăn cho ban cán sự lớp, có vấn học tập và các cấp quản lý cao hơn trong quá trình xét duyệt.

Trong bài báo này, chúng tôi đề xuất một mô hình quản lý xuyên suốt quy trình đánh giá điểm rèn luyện từ lúc một hoạt động được bắt đầu, sau đó là điểm danh và cuối cùng là đánh giá, xét duyệt và xuất các báo cáo. Hệ thống hỗ trợ điểm danh sinh viên theo cách thuận lợi, giúp tăng cường sự minh bạch và giảm được sai sót so với điểm danh thủ công. Hệ thống cũng sẽ tự động tổng hợp điểm đánh giá, giảm áp lực vào việc tự đánh giá và xét duyệt cuối mỗi học kỳ.

3. MÔ HÌNH HỆ THỐNG ĐỀ XUẤT

Để xây dựng được hệ thống quản lý điểm rèn luyện, các bước phân tích, thiết kế, hiện thực và kiểm thử lần lượt được thực hiện.

3.1. Phân tích quy trình nghiệp vụ

Đầu tiên, các quy trình, biểu mẫu liên quan đến quản lý điểm rèn luyện ở khoa và các phòng ban liên quan được thu thập và phân tích. Các quy trình biểu mẫu liên quan đến các bước sau:

- Các khoa, phòng, ban đăng ký/cập nhật và xét duyệt hoạt động được tính điểm rèn luyện.
- Sinh viên đăng ký/hủy đăng ký tham gia các hoạt động.
- Sinh viên thực hiện điểm danh tham gia/thực hiện hoạt động theo hướng dẫn của Ban tổ chức.
- Các khoa, phòng, ban tổng kết kết quả sau khi một hoạt động đã được triển khai.
- Các khoa, phòng, ban tổng kết kết quả ở cuối mỗi học kỳ.

Sau khi phân tích xong, toàn bộ các hoạt động quản lý điểm rèn luyện có thể được mô tả lại tóm tắt như sau.

Việc tính điểm rèn luyện cho sinh viên căn cứ dựa trên số lượng sinh tham gia các hoạt động do trường tổ chức hoặc hoạt động bên ngoài trường (điểm cộng) và các lỗi quy phạm nội quy nhà trường mà sinh viên mắc phải (điểm trừ).

Các khoa, phòng, ban trong nhà trường sẽ lên kế hoạch tạo hoạt động có tính điểm rèn luyện cho sinh viên. Mỗi hoạt động sẽ diễn ra trong một buổi hoặc cả ngày. Trong mỗi buổi sinh viên chỉ có thể tham gia một hoạt động duy nhất. Sau khi hoạt động được tạo, một đơn vị quản lý cấp cao nhất theo phân công của nhà trường sẽ xem xét duyệt hoặc hủy đối với từng buổi của hoạt động.

Sau khi hoạt động được duyệt, sinh viên có thể thấy được trạng thái đăng ký tham gia là đã được duyệt hoặc không được duyệt. Sinh viên không thể đăng ký một hoạt động mà thời

gian diễn ra trùng với lịch của một hoạt động đã được sinh viên đăng ký trước đó. Các hoạt động sẽ tự động đóng lại (không cho đăng ký) trước 1 ngày diễn ra sự kiện. Sau khi hết thời gian đăng ký tham gia hoạt động, đơn vị tổ chức hoạt động có thể chọn ra những sinh viên đủ điều kiện tham gia các buổi hoạt động.

Tại buổi diễn ra sự kiện, ban tổ chức sẽ cho sinh viên điểm danh. Sinh viên có thể điểm danh bằng việc quét mã QR-code hoặc thông qua phần mềm điểm danh trên điện thoại di động mà hoạt động theo cơ chế quét bluetooth. Cơ chế hoạt động của hai hình thức này sẽ được trình bày ở phần thiết kế. Trường hợp sinh viên không có thiết bị để thực hiện điểm danh bằng cả hai hình thức trên thì sinh viên có thể liên hệ ban tổ chức để được điểm danh theo cách thủ công. Kết quả điểm danh sẽ được cập nhật lên hệ thống và sinh viên có thể kiểm tra ngay lập tức. Nếu có sai sót trong quá trình điểm danh sinh viên có thể gửi phản hồi về cho nhà trường với mã hoạt động vào buổi tương ứng kèm theo hình ảnh và nội dung của buổi hoạt động đó. Thời hạn gửi phản hồi là trong vòng bảy ngày sau khi sự kiện kết thúc.

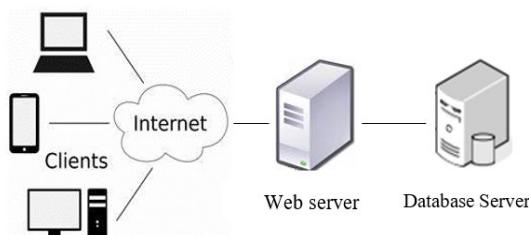
Bên cạnh đó, ban cán sự lớp, các sinh viên nghiên cứu khoa học hoặc một số hoạt động khác theo quy định (tham gia hiến máu tình nguyện, các hoạt động công ích tình nguyện, các cuộc thi học thuật, ...) cũng sẽ được cộng điểm theo học kỳ. Các hoạt động này không có điểm danh nhưng có các chứng chỉ hoặc giấy chứng nhận làm minh chứng.

Các sinh viên vi phạm nội quy nhà trường sẽ được ghi nhận lại để được xử lý trừ điểm rèn luyện (việc này hiện được thực hiện thủ công và không được tập trung cài tiến trong khuôn khổ của nghiên cứu này vì tính đa dạng và phức tạp của nó). Nếu có sai sót trong quá trình ghi nhận sinh viên có thể gửi phản hồi vi phạm về cho nhà trường giải quyết các bước tương tự như phản hồi hoạt động.

Tổng kết điểm rèn luyện được chốt vào hai thời điểm: sau khi kết thúc hoạt động và cuối học kỳ. Cuối mỗi hoạt động, sinh viên sẽ được cộng điểm theo danh sách điểm danh. Sinh viên sẽ ngay lập tức nhìn thấy tổng số điểm rèn luyện của mình tại một thời điểm bất kỳ. Như vậy sinh viên sẽ chủ động lập kế hoạch tham gia các hoạt động mới để đạt được mức điểm rèn luyện phù hợp nếu thấy cần thiết. Còn ở cuối mỗi học kỳ các điểm tham gia hoạt động, các điểm vi phạm và các điểm khác sẽ được tổng kết và kết xuất thành các báo cáo.

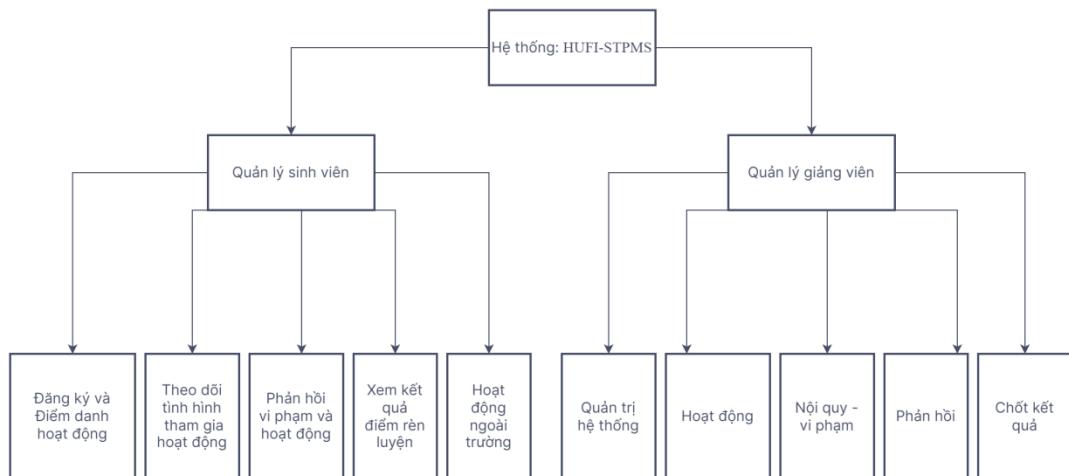
3.2. Thiết kế hệ thống

Hệ thống quản lý điểm rèn luyện sinh viên HUFI-STPMS được xây dựng trên nền tảng web (hình 1). Người dùng sử dụng trình duyệt web trên thiết bị di động hoặc máy tính để truy cập vào website được đặt trên mạng internet. Website tương tác với hệ quản trị cơ sở dữ liệu tập trung (như SQL Server hoặc MySQL) cho việc lưu trữ và truy xuất dữ liệu.

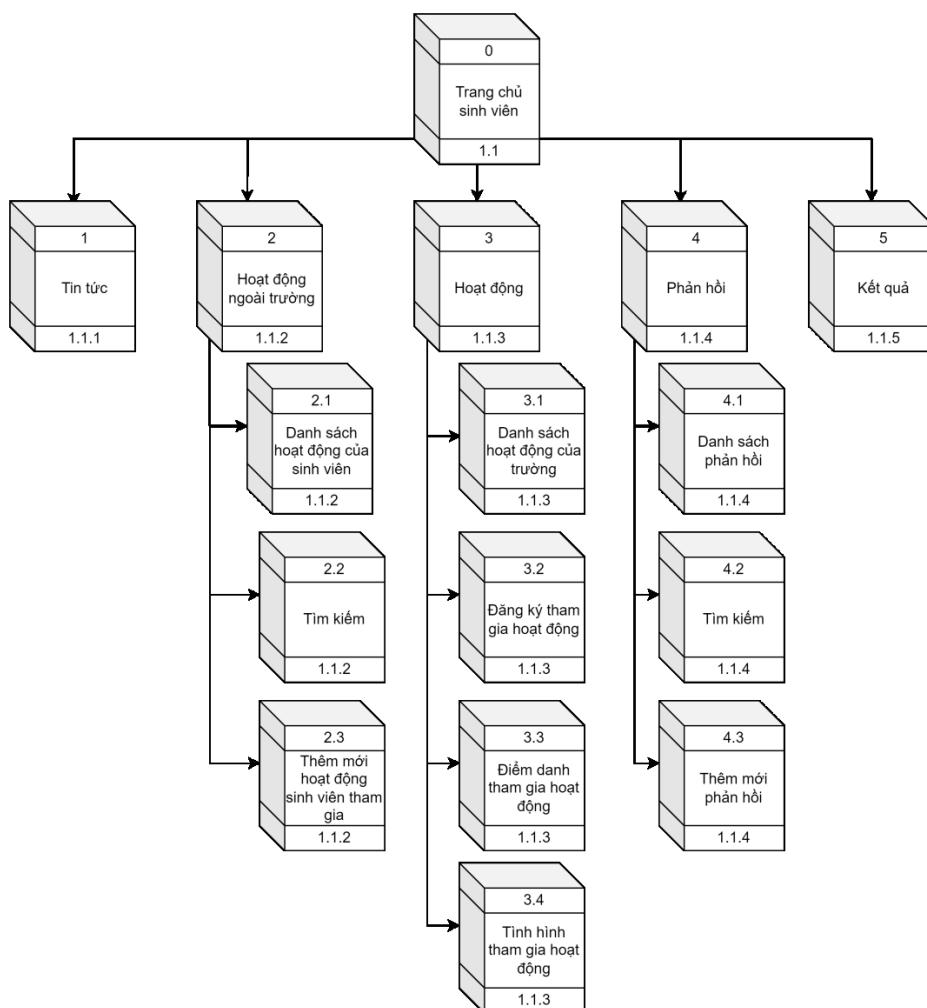


Hình 1. Kiến trúc của hệ thống quản lý điểm rèn luyện sinh viên HUFI-STPMS

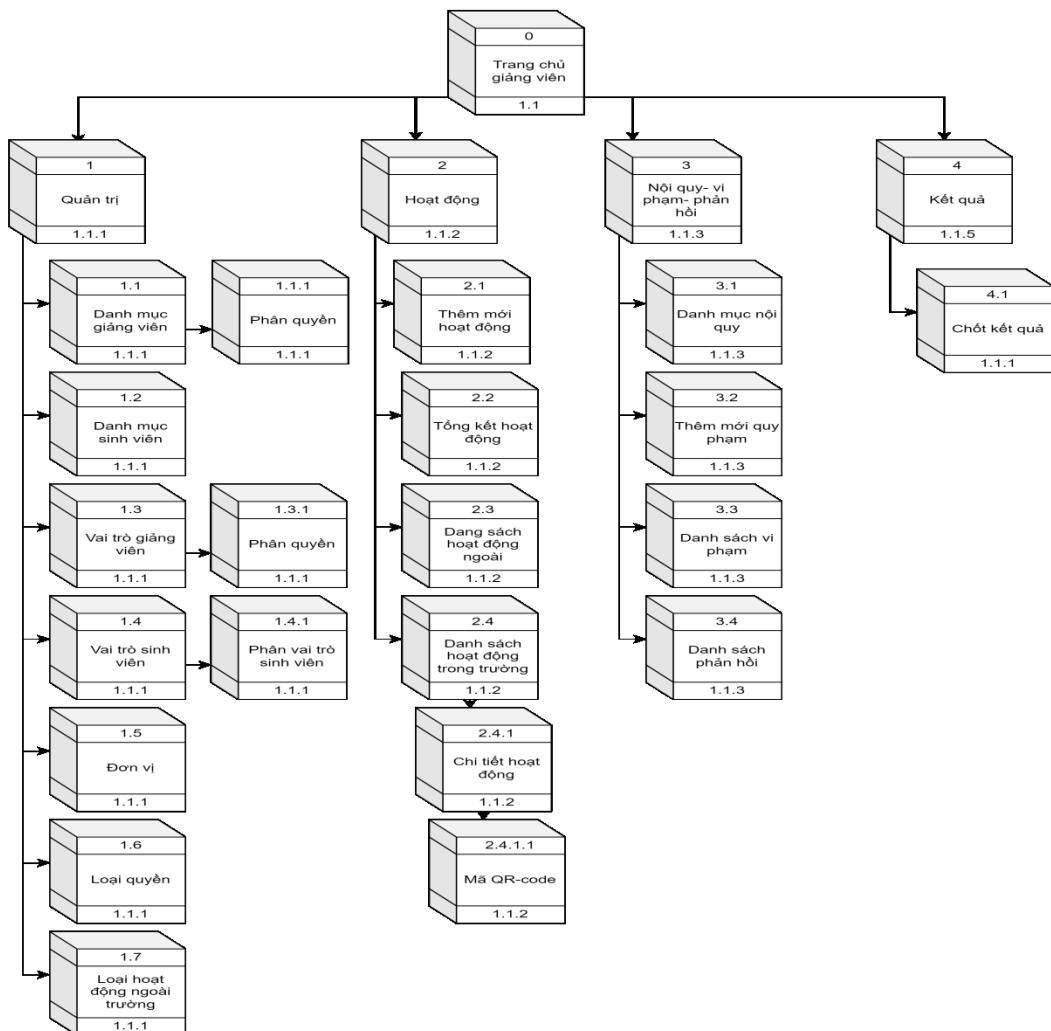
Hệ thống bao gồm các chức năng được liệt kê trên sơ đồ phân cấp chức năng (hình 2) và tập hợp các màn hình được liệt kê trên sơ đồ tổ chức các màn hình của hệ thống HFUI_STPMS (hình 3).



Hình 2. Sơ đồ phân cấp chức năng của hệ thống HIFI-STPMS



Hình 3. Sơ đồ tổ chức các màn hình của trang sinh viên hệ thống HIFI-STPMS



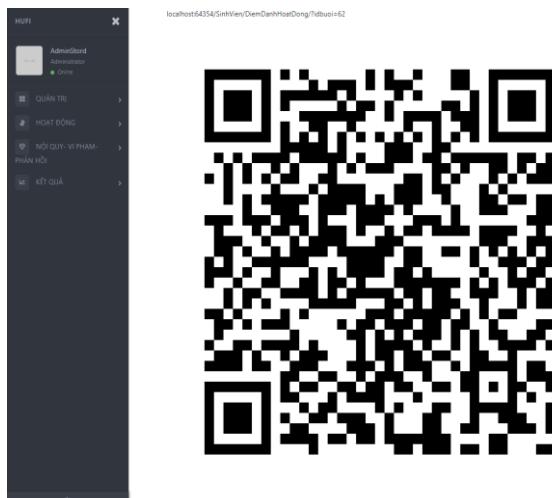
Hình 4. Sơ đồ tổ chức các màn hình của trang giảng viên hệ thống HUFI-STPMS

Hầu hết các chức năng như trong hình 2 đều có cơ chế chung là người dùng gửi yêu cầu và thông tin liên quan lên web server, web server xử lý yêu cầu và gửi lại kết quả cho người dùng. Trong quá trình xử lý, web server có thể phải lưu trữ hoặc truy xuất dữ liệu với database server. Do đó ở đây chúng tôi tập trung mô tả chi tiết về hai chức năng tương đối mới điểm danh bằng cách quét mã QR-code và điểm danh bằng quét bluetooth.

Thiết kế tính năng điểm danh bằng quét mã QR-code.

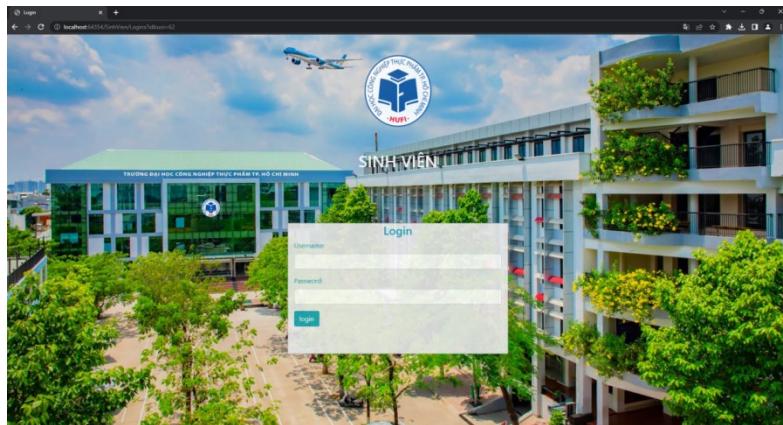
Tính năng điểm danh bằng quét mã QR-code chỉ thực hiện được đối với các sinh viên có điện thoại thông minh và trên điện thoại phải có kết nối internet. Cơ chế hoạt động của việc điểm danh như sau:

- Ban tổ chức sẽ vào hoạt động đang diễn ra tạo một mã QR. Sau đó một số thành viên ban tổ chức sẽ mở trung bày mã QR (hình 5) cho các đối tượng cần điểm danh quét hình ảnh mã QR và truy cập tới website xử lý điểm danh.



Hình 5. Mã QR điểm danh một buổi hoạt động trong HUFI-STPMS

Sau khi sinh viên quét mã QR sẽ được chuyển đến trang đăng nhập (hình 5). Sinh viên tiến hành nhập thông tin tài khoản và mật khẩu để đăng nhập vào phần mềm. Sau khi đăng nhập vào phần mềm sẽ điều hướng tới form xác nhận điểm danh (hình 6), lúc này sinh viên đã được điểm danh. Các thông tin được lưu trữ trên hệ thống bao gồm: thông tin về sự kiện, thông tin về thời gian điểm danh, thông tin đặc trưng về thiết bị (các thiết bị khác nhau sẽ có thông tin khác nhau), thông tin về sinh viên (MSSV mà đã được lưu trong cấu hình của ứng dụng HUFI-BlueTooth-Check trong quá trình cài đặt).



Hình 6. Form đăng nhập điểm danh của sinh viên trong HUFI-STPMS

A screenshot of a web page titled 'FORM XÁC NHẬN ĐIỂM DANH'. The page header includes the HUFI logo and navigation links: 'Trang chủ', 'Tin tức', and 'Nguyễn Thị Hoa Hồng'. The main content area displays a summary of the check-in details:

HD00024 - QUÉT DỌN SÂN TRƯỜNG - NGÀY 02/05/2023

Thông tin hoạt động:

- Nội dung công việc: Quét dọn sân trường
- Số lượng sinh viên: 10 sinh viên
- Điểm: 4 điểm/ Buổi
- Địa điểm: sân trường
- Yêu cầu: Mặc đồng phục
- Thời gian: 02/05/2023 21:31:14;

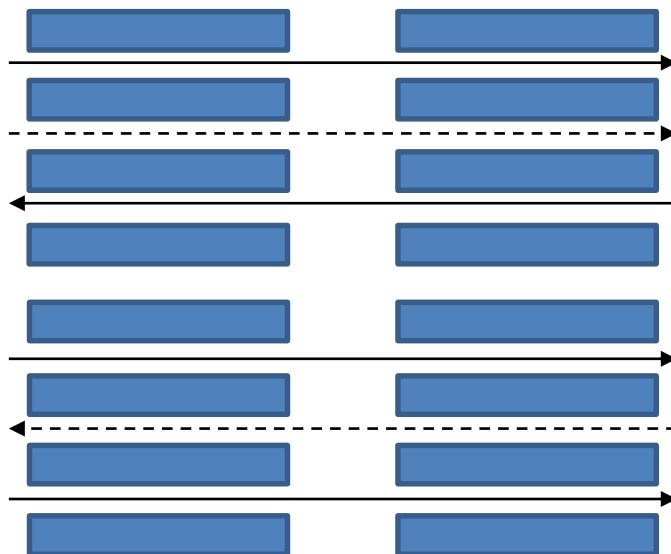
Hình 7. Form xác nhận điểm danh của sinh viên trong HUFI-STPMS

Thiết kế tính năng điểm danh bằng quét bluetooth.

Tính năng điểm danh bằng quét bluetooth chỉ thực hiện được đối với các sinh viên có điện thoại thông minh và trên điện thoại phải cài ứng dụng điểm danh bằng bluetooth HUFI-BlueTooth-Check. Cơ chế hoạt động của việc điểm danh như sau:

- Một hoặc một số thành viên ban tổ chức sẽ mở phần mềm HUFI-BlueTooth-Check, chọn chiêu dịch cần điểm danh và khởi động chức năng quét các thiết bị bluetooth ở xung quanh.

- Tiếp đó các thành viên này sẽ cầm theo thiết bị và di chuyển bao quát khắp không gian nơi diễn ra sự kiện sao cho không gian quét của thiết bị có thể phủ được toàn bộ sinh viên có mặt trong không gian sự kiện này. Ví dụ như có một phòng học như hình 8. Nếu như thiết bị bluetooth chỉ có bán kính phủ là bằng 1 dãy ghế, thì nhân sự di điểm danh cần dịch chuyển trong phòng theo đường mũi tên liền nét. Còn nếu như thiết bị bluetooth có bán kính phủ là bằng 2 dãy ghế, thì nhân sự di điểm danh có thể dịch chuyển ít hơn theo đường mũi tên nét đứt. Việc xác định bán kính quét của thiết bị cần được thử nghiệm, và đường đi cần được thiết kế theo không gian tổ chức sự kiện.



Hình 8. Minh họa cách di chuyển để quét thiết bị bluetooth trong HUFI-STPMS

- Các bạn sinh viên có thiết bị và cần điểm danh phải để ứng dụng HUFI-BlueTooth-Check chạy trong suốt quá trình điểm danh hoặc suốt thời gian diễn ra sự kiện (tùy theo yêu cầu của ban tổ chức).
- Các thiết bị mở ứng dụng HUFI-BlueTooth-Check nằm trong tầm quét của thiết bị của nhân sự điểm danh sẽ được lưu vào trong danh sách các thiết bị đã điểm danh. Các thông tin được lưu trữ bao gồm: thông tin về sự kiện, thông tin về thời gian điểm danh, thông tin đặc trưng về thiết bị (các thiết bị khác nhau sẽ có thông tin khác nhau), thông tin về sinh viên (MSSV mà đã được lưu trong cấu hình của ứng dụng HUFI-BlueTooth-Check trong quá trình cài đặt).

– Danh sách này sẽ được cập nhật lên database server trực tiếp nếu thiết bị điểm danh có kết nối internet. Nếu thiết bị điểm danh không có kết nối internet thì danh sách điểm danh được lưu tạm trong thiết bị và sau đó gửi lên database server khi thiết bị có kết nối internet.

Tính năng điểm danh quét bluetooth và quét QR-code đều sẽ cập nhật danh sách điểm danh trực tiếp lên cùng một bảng trong cơ sở dữ liệu. Điều này làm cho quá trình điểm danh được thống nhất, theo thời gian thực mà không phụ thuộc vào cách sinh viên thực hiện điểm danh.

Ưu nhược điểm của phương thức điểm danh bằng bluetooth và QR-code được phân tích trong bảng 1.

Bảng 1. So sánh phương thức điểm danh bằng bluetooth và QR-code

	Điểm danh bằng bluetooth	Điểm danh bằng QR-code
Ưu điểm	<ul style="list-style-type: none"> - Thiết bị của SV không cần phải có kết nối internet, chỉ cần phát được bluetooth (điều mà hầu hết các thiết bị di động đều có). - SV không cần phải thực hiện thao tác gì mà chỉ cần mở ứng dụng HUFI-BlueTooth-Check trong suốt quá trình tham dự sự kiện. - Ban tổ chức có thể thực hiện điểm danh nhiều lần trong suốt sự kiện mà không làm ảnh hưởng đến SV. Không được tình trạng gian lận trong điểm danh. 	<ul style="list-style-type: none"> - Ban tổ chức không cần cử người di chuyển trong không gian sự kiện.
Nhược điểm	<ul style="list-style-type: none"> - Ban tổ chức phải cử người di chuyển trong không gian sự kiện để quét các thiết bị bluetooth khác. 	<ul style="list-style-type: none"> - SV phải thực hiện quét mã QR-code và thực hiện các bước theo hướng dẫn. - Nếu phải điểm danh nhiều lần sẽ gây ảnh hưởng đến chất lượng tham dự sự kiện của SV. - SV biết được thời điểm điểm danh nên có thể diễn ra tình trạng gian lận.

Tính mới, tính độc đáo, tính sáng tạo: Dùng mã QR-Code kết hợp với các giải pháp khác để điểm danh là một giải pháp mới. Giải pháp hứa hẹn mang lại sự hiệu quả, thuận lợi và chống gian lận khi điểm danh cho các hoạt động có tính điểm rèn luyện công tác xã hội.

4. HIỆN THỰC HỆ THỐNG

Hệ thống HUFI-STPMIS được xây dựng trên ASP.NET, ngôn ngữ C# theo mô hình MVC. Các chức năng đã được thử nghiệm và chạy ổn định. Bên dưới là một số hình chụp màn hình của hệ thống khi thực thi.

Đầu tiên là màn hình thêm mới hoạt động trong trường (hình 9). Ở màn hình này, người dùng có thể tạo mới một hoạt động. Hoạt động chia làm theo 2 loại: hoạt động theo buổi (điểm

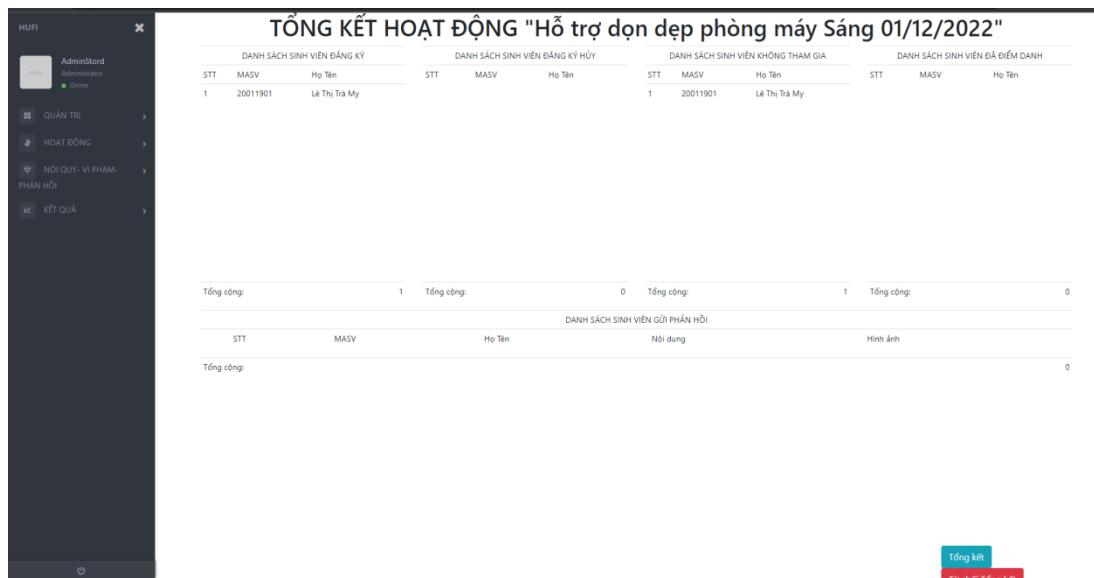
sẽ được tính theo buổi), và hoạt động cả ngày (tham gia hết một ngày mới được cộng điểm hoạt động).

Hình 9. Màn hình thêm mới một hoạt động

Tiếp theo là màn hình chốt điểm rèn luyện (hình 10). Ở màn hình này, người dùng thống kê được số lượng sinh viên theo từng loại của hoạt động. Người dùng không thể chốt kết quả khi hoạt động chưa kết thúc hoặc còn phản hồi chưa được xử lý.

Cuối cùng là màn hình tổng kết buổi hoạt động (hình 11). Màn hình này hiển thị chi tiết tình hình tham gia hoạt động của sinh viên và hiển thị những phản hồi của sinh viên về hoạt động này. Người xét duyệt có thể chọn "Tổng kết" để duyệt kết quả của hoạt động đã diễn ra hoặc chọn "Tù chối" để chưa xét duyệt.

Hình 10. Màn hình chốt kết quả điểm rèn luyện cho sinh viên



Hình 11. Màn hình tổng kết hoạt động

5. KẾT LUẬN

Trong bài báo đã trình bày về lý do cần phải xây dựng hệ thống quản lý điểm rèn luyện HUFI-STPMS, kết quả tìm hiểu và phân tích quy trình nghiệp vụ, đề xuất mô hình thiết kế hệ thống, cơ chế điểm danh bằng QR-code và bằng bluetooth, một số giao diện hệ thống đã được xây dựng và kiểm thử. Hệ thống HUFI-STPMS được tích hợp 2 phương thức điểm danh cùng lúc tạo ra sự thuận lợi cho việc điểm danh hơn so với chỉ dùng phương thức điểm danh bằng QR-code. Phương thức điểm danh dùng bluetooth có nhiều ưu điểm hơn như không cần thiết bị của sinh viên có kết nối internet (việc mở wifi cho hàng trăm thiết bị kết nối cùng lúc không phải lúc nào cũng khả thi) và việc điểm danh diễn ra một cách thụ động (sinh viên không biết lúc nào ban tổ chức thực hiện điểm danh) do đó cũng tránh được tình trạng gian lận.

Với những kết quả đạt được trong quá trình thử nghiệm bởi nhóm nghiên cứu, chúng tôi rất kỳ vọng việc thử nghiệm trong điều kiện thực tế tại khoa, phòng, ban của trường cũng sẽ đạt được những kết quả tốt, đáp ứng được tốt các yêu cầu của người dùng.

TÀI LIỆU THAM KHẢO

1. Công ty Xsoft, phần mềm quản lý điểm rèn luyện bậc cao đẳng, đại học, <https://xsoft.vn/phan-mem-quan-ly-diem-ren-luyen-bac-cao-dang-dai-hoc>
2. Công ty VINAAS, phần mềm quản lý hồ sơ Sinh viên, <https://vinaas.com/phan-mem-quan-ly-ho-so-sinh-vien.html>
3. Bùi Công Danh, Lê Văn Bé - Hệ thống quản lý điểm rèn luyện sinh viên trên thiết bị di động, Tạp chí Khoa học Công nghệ và Thực phẩm 17 (1) (2018) 115-126.
4. Phạm Văn Tranh – Tìm hiểu công nghệ RFID và ứng dụng, Luận văn thạc sĩ Ngành Kỹ thuật điện tử tin học Trường Đại học Bách khoa Hà Nội, 2011.

5. Đoàn Hòa Minh, Lưu Minh Thái – Quét mã vạch trên thẻ bằng điện thoại di động và ứng dụng trong điểm danh, Tạp chí khoa học trường Đại học Cần Thơ, Số 34 (2014) Trang: 74-80.
6. Võ Hùng Cường – Quét mã QR trên điện thoại di động ứng dụng vào việc điểm danh sinh viên. Thực nghiệm tại trường cao đẳng công nghệ thông tin, Tạp chí Khoa học Công nghệ Đại học Đà Nẵng, ISBN: 1859-1531, 12(97).2015, quyển 2.
7. Mẫn Đức Thắng – Thiết kế thiết bị điểm danh tự động ứng dụng công nghệ RFID và nhận dạng khuôn mặt qua camera, Luận văn thạc sĩ ngành Kỹ thuật điện tử Trường Đại học Bách Khoa Hà Nội, 2013.
8. Nguyễn Văn Thông – Định vị thiết bị di động bằng công nghệ Bluetooth, Luận văn thạc sĩ ngành Kỹ thuật điện tử - viễn thông trường Đại học Công Nghệ - ĐHQG Hà Nội, 2011.

ABSTRACT

HUFI-STPMS: STUDENTS' TRAINING POINTS MANAGEMENT SYSTEM AT HO CHI MINH UNIVERSITY OF FOOD INDUSTRY (HIFI)

**Phat T. Tran-Truong¹, Tran Khanh Dang¹, Hung Ngo Thanh^{1,*},
Tran Thi Van Anh¹, My T. Tra Le¹, Doan Huynh Tuyet-Anh¹**

¹*Ho Chi Minh University of Food Industry*

^{*}Email: hunghnhanh@hufi.edu.vn

At the HCMC university of food industry (HIFI), most management activities are computerized. Each unit in HIFI is authorized to use the software, allowed to manage, update and exploit the database. The current software system meets common and synchronous functions the whole school. However, the training points management system at the school is currently not synchronized. Each unit (management faculty, related departments) has its own way, some places do it manually, some with software, some software only support one/several stages such as for students to register, register activities or take attendance of students participating in activities, ... In general, these software cannot support well the management of student training points. Therefore, in this study, the HIFI-STPMS student training points management system is proposed with the characteristics of managing throughout the training points management process and especially supporting attendance by software in a convenient and exact way.

Keywords: Training points, attendance by QR Code.

NGUỒN NHÂN LỰC NGÀNH CÔNG NGHỆ THÔNG TIN TRONG XU HƯỚNG CHUYỂN ĐỔI SỐ

Trần Thị Bích Vân^{1*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: vannttb@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo nêu thực trạng nguồn nhân lực công nghệ thông tin hiện nay trong xu thế đổi mới của xã hội. Chuyển đổi số, vấn đề được quan tâm trong chiến lược quốc gia trong năm 2023. Cơ hội và thách thức nào dành cho nguồn nhân lực chất lượng cao. Nhiệm vụ nào được đặt ra cho các cơ quan ban ngành và các cơ sở đào tạo nguồn nhân lực chất lượng cao.

Từ khóa: Nhân lực công nghệ thông tin, nhân lực chất lượng cao, chuyển đổi số.

1. MỞ ĐẦU

Trước những tiến bộ của cuộc cách mạng công nghệ 4.0, Việt Nam đang dần đẩy nhanh tiến trình chuyển đổi số trong mọi lĩnh vực của đời sống xã hội. Trong đó, ngành Công nghệ thông tin đóng vai trò “đầu tàu” dẫn dắt xuyên suốt quá trình chuyển đổi số của đất nước. Do đó nhu cầu nhân lực mà ngành Công nghệ thông tin mang lại là rất lớn, mở ra nhiều cơ hội cho các sinh viên theo đuổi ngành nghề này

Đứng trước tiến bộ của cuộc Cách mạng 4.0, tại Việt Nam nhu cầu ứng dụng những công nghệ tự động hóa, công nghệ cao, trao đổi dữ liệu... trong công nghệ sản xuất, trong lĩnh vực nông nghiệp, công nghiệp. Ngành công nghệ thông tin càng khẳng định được tầm quan trọng của mình - vừa là nền tảng, vừa là động lực để bắt kịp đà phát triển của thế giới. Các hệ thống công nghệ thông minh chính là điều kiện để tối ưu hóa năng suất lao động, tiết kiệm nhân lực lao động thủ công, tiết kiệm chi phí sản xuất. ngành Công nghệ thông tin đóng vai trò “đầu tàu” dẫn dắt xuyên suốt quá trình chuyển đổi số của đất nước. Do đó nhu cầu nhân lực mà ngành Công nghệ thông tin mang lại là rất lớn. Cơ hội nào dành cho nguồn nhân lực có trình độ cao trong lĩnh vực công nghệ thông tin hiện nay.

Trong bài báo này, tác giả đã tìm hiểu thực trạng và một số giải pháp đáp ứng nhu cầu nguồn nhân lực chất lượng cao tại một số cơ quan ban ngành và doanh nghiệp tại Việt Nam trong xu hướng chuyển đổi số của xã hội

2. THỰC TRẠNG

2.1 Xu hướng và nhu cầu của xã hội

Chuyển đổi số là một trong những nhiệm vụ trọng tâm trong quá trình công nghiệp hóa, hiện đại hóa đất nước. Tổng Bí thư Nguyễn Phú Trọng đã phát biểu: [Coi chuyển đổi số là phương thức mới có tính đột phá để rút ngắn quá trình công nghiệp hóa, hiện đại hóa]. Đứng trước yêu cầu đổi mới của đất nước, các cơ quan ban ngành nhà nước đã và đang đặt ra kế hoạch phát triển lâu dài để đáp ứng nhu cầu của xã hội. Theo đó, nguồn nhân lực công nghệ thông tin chất lượng cao đóng vai trò chủ lực trong tình hình mới này.

Theo Chiến lược phát triển công nghiệp công nghệ số Việt Nam đến năm 2025, định hướng đến 2030, mục tiêu đến năm 2025 sẽ phát triển 80 ngàn doanh nghiệp công nghệ số.

Năm 2023 là năm dữ liệu số quốc gia: đứng trước 5 chỉ tiêu quan trọng về kinh tế số, chính phủ số, xã hội số, dữ liệu số, an toàn và an ninh mạng.

Các tỉnh thành đã và đang đề ra kế hoạch phát triển tại địa phương mình.

- Tại Thành phố Hồ Chí Minh với ba mục tiêu chính là chính quyền số, kinh tế số, xã hội số đáp ứng yêu cầu chuyển đổi số của chính phủ, công tác này cũng gắn với mục tiêu xây dựng thành phố trở thành đô thị thông minh. Để thực hiện được mục tiêu này, nguồn nhân lực trình độ cao được xem là yếu tố cốt lõi. Đến nay, các sở, ngành chức năng đã và đang phối hợp triển khai nhiều đề án về đào tạo, tập huấn nhằm tạo nguồn lực đáp ứng yêu cầu trong quá trình vận hành; hỗ trợ doanh nghiệp sớm tiếp cận và thực hiện chuyển đổi số, nhất là doanh nghiệp vừa và nhỏ.

- Tại Đà Nẵng với chỉ tiêu tập trung phát triển kinh tế số đóng góp tối thiểu 20% GRDP thành phố. Phấn đấu đưa tỉ trọng phát triển kinh tế số trong từng ngành, từng lĩnh vực. Hỗ trợ khởi nghiệp thành lập doanh nghiệp công nghệ trên địa bàn. UBND thành phố Đà Nẵng đã ban hành kế hoạch phát triển nguồn nhân lực để phục cho công cuộc chuyển đổi số đến năm 2025. Kế hoạch nhằm dự báo nhu cầu về nguồn nhân lực công nghệ thông tin chất lượng cao, định hướng và xây dựng các nhóm giải pháp từ doanh nghiệp, từ các cấp quản lý, cơ sở đào tạo đáp ứng mục tiêu đặt ra. Bên cạnh đó, sự nỗ lực của các doanh nghiệp công nghệ đã và đang tham gia vào kế hoạch phát triển của Đà Nẵng nhằm tăng tốc độ phát triển nguồn nhân lực số và mục tiêu kinh tế số của mình.

- Tại Tỉnh Thừa Thiên Huế: tỉnh đã xây dựng kế hoạch, đề án phát triển nguồn nhân lực CNTT cho tỉnh với mục tiêu phấn đấu đến năm 2025 đạt 10.000 lao động CNTT phục vụ phát triển Công nghiệp phần mềm. Chuyển đổi số là bắt buộc và xu thế, đòi hỏi sinh viên phải biết chủ động chuẩn bị những gì cần thiết, doanh nghiệp CNTT phải có những giải pháp cụ thể.

Theo báo cáo của LinkedIn số lượng việc làm ngành CNTT tăng đột biến, dẫn đầu trong top 20 ngành nghề trong 5 năm trở lại đây. Rõ ràng làn sóng công nghệ mới đã khiến cơn khát nhân lực CNTT tăng cao đến đỉnh điểm.

2.2. Nhận định và thách thức

Theo số liệu Ủy ban Quốc gia về chuyển đổi số công bố hồi tháng 8/2022, tỷ lệ nhân lực công nghệ thông tin (CNTT) trên tổng số lao động của Việt Nam ước đạt 1% trong tổng số 51 triệu lao động. Về chất lượng, chỉ có khoảng 30% kỹ sư, cử nhân mới ra trường đáp ứng

yêu cầu thực tế của công việc. Dự báo đến 2023, toàn ngành sẽ thiếu hụt khoảng một triệu lao động.

Theo ông Nguyễn Thái An - Tổng Giám đốc Luxoft Việt Nam Việc thiếu hụt nhân lực trong quá trình chuyển đổi số cho thấy chính sách phát triển nguồn nhân lực có chất lượng, có kỹ năng cao cần được xem là ưu tiên hàng đầu nhằm bảo đảm cho thành công của chuyển đổi số trong giai đoạn tới". Nguồn nhân lực dành cho chuyển đổi số cần quy mô nguồn nhân lực lớn, đội ngũ nhân sự cần có mức độ chuyên môn cao và đa dạng kinh nghiệm chuyển đổi số cho các ngành công nghiệp dịch vụ khác nhau nhằm đảm bảo nhu cầu số lượng và chất lượng. Từ đó nâng cao vai trò của các trường đại học có đào tạo về ngành công nghệ thông tin nhằm đáp ứng chất lượng nguồn nhân lực

Bên cạnh đó việc tái đào tạo của các doanh nghiệp cũng đóng vai trò quan trọng không kém. Doanh nghiệp cần tạo điều kiện để nguồn nhân lực tại chỗ được nâng cao chất lượng cả về trình độ kỹ thuật lẫn kỹ năng mềm, kỹ năng thích ứng với công việc.

Các ngân hàng lớn nhỏ, công ty chứng khoán, điện lực đã lên kế hoạch và đầu tư cho việc chuyển đổi số, dẫn đến nhu cầu nhân sự cho các vị trí Công nghệ thông tin, Chuyển đổi số vẫn tiếp tục tăng cao.

3. NHẬN ĐỊNH VÀ GIẢI PHÁP

Theo số liệu Ủy ban Quốc gia về chuyển đổi số công bố hồi tháng 8/2022, tỷ lệ nhân lực công nghệ thông tin (CNTT) trên tổng số lao động của Việt Nam ước đạt 1% trong tổng số 51 triệu lao động. Về chất lượng, chỉ có khoảng 30% kỹ sư, cử nhân mới ra trường đáp ứng yêu cầu thực tế của công việc. Dự báo đến 2023, toàn ngành sẽ thiếu hụt khoảng một triệu lao động.[2]

Theo báo cáo thị trường CNTT Việt Nam 2021 Developers Recruitment State, trong số hơn 55.000 sinh viên CNTT tốt nghiệp mỗi năm, chỉ có khoảng 16.500 sinh viên (30%) đáp ứng được những kỹ năng và chuyên môn mà doanh nghiệp cần. Tại Huế, các con số khảo sát của đơn vị đào tạo cho biết, hơn 90% sinh viên tốt nghiệp các ngành CNTT có việc làm sau 1 năm tốt nghiệp, nhưng vẫn còn thiếu dữ liệu việc làm đúng chuyên ngành hay vị trí tuyển dụng, mức lương, đánh giá từ doanh nghiệp [3]

Theo ông Nguyễn Thái An - Tổng Giám đốc Luxoft Việt Nam Việc thiếu hụt nhân lực trong quá trình chuyển đổi số cho thấy chính sách phát triển nguồn nhân lực có chất lượng, có kỹ năng cao cần được xem là ưu tiên hàng đầu nhằm bảo đảm cho thành công của chuyển đổi số trong giai đoạn tới". Nguồn nhân lực dành cho chuyển đổi số cần quy mô nguồn nhân lực lớn, đội ngũ nhân sự cần có mức độ chuyên môn cao và đa dạng kinh nghiệm chuyển đổi số cho các ngành công nghiệp dịch vụ khác nhau nhằm đảm bảo nhu cầu số lượng và chất lượng. Từ đó nâng cao vai trò của các trường đại học có đào tạo về ngành công nghệ thông tin nhằm đáp ứng chất lượng nguồn nhân lực

Bên cạnh đó việc tái đào tạo của các doanh nghiệp cũng đóng vai trò quan trọng không kém. Doanh nghiệp cần tạo điều kiện để nguồn nhân lực tại chỗ được nâng cao chất lượng cả về trình độ kỹ thuật lẫn kỹ năng mềm, kỹ năng thích ứng với công việc.

Sinh viên ngành công nghệ thông tin – nguồn nhân lực chất lượng cao tương lai cần trang bị kỹ năng chuyên môn vững vàng, những kỹ năng mềm như khả năng tư duy phát triển, giao tiếp, quản lý thời gian, trình độ ngoại ngữ,... cũng là yếu tố quan trọng trong quá trình ứng tuyển các vị trí hiện nay

Chính sự biến động của tình hình chung, sự cạnh tranh khốc liệt giữa các doanh nghiệp Công nghệ, sự đổi mới liên tục của công nghệ đòi hỏi ở các lập trình viên khả năng thích ứng nhanh và nhạy bén với mọi sự biến đổi. Các lập trình viên cần nâng cao kỹ năng công nghệ của bản thân với sự hiểu biết về các công nghệ mới và đột phá như Cybersecurity, DevOps, AI và Machine Learning, Cloud Computing,... [3]

TÀI LIỆU THAM KHẢO

1. <Https://Kiengiang.Gov.Vn/Trang/Tintuc/286/33771/Diem-Khac-Nhau-Giua-Cong-Nghe-Thong-Tin-Va-Chuyen-Doi-So.Html>
2. <Https://Topdev.Vn/Blog/Bao-Cao-Thi-Truong-It-Viet-Nam-Nam-2021/>
3. <Https://Thitruongtaichinhiente.Vn/Vietnamworks-Dong-Hanh-Cung-Google-Va-Nic-Nang-Cao-Nang-Luc-Va-Ket-Noi-Co-Hoi-Viec-Lam-Cho-Nguon-Nhan-Luc-So-Tai-Viet-Nam-45317.Html>

ABSTRACT

HUMAN RESOURCES IN INFORMATION TECHNOLOGY INDUSTRY IN THE TREND OF DIGITAL TRANSFORMATION

Tran Thi Bich Van^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: vanttb@hufi.edu.vn

The paper presents the current situation of human resources in information technology in the trend of social innovation. Digital transformation, an issue of concern in the national strategy in 2023. What are opportunities and challenges for high-quality human resources. What tasks are assigned to the agencies and training institutions of high-quality human resources.

Keywords: information technology human resources, high-quality human resources, digital transformation.

TỐI UU HÓA ĐÀN KIẾN VÀ ỨNG DỤNG TRONG BÀI TOÁN ẨN TẬP PHỔ BIẾN

Hồ Thanh Hải¹, Đinh Nguyễn Trọng Nghĩa^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: nghiadnt@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo này trình bày về thuật toán tối ưu hóa đàm kién là một thuật toán metaheuristic được lấy cảm hứng từ hành vi tìm kiếm thức ăn của kiến và kiến đực. Điểm mạnh của thuật toán tối ưu hóa đàm kién là khả năng tìm kiếm các lời giải tối ưu trong bài toán tổng quát hóa với kích thước lớn. Ngoài ra, bài báo cũng đề xuất một phương pháp áp dụng tối ưu hóa đàm kién vào bài toán ẩn tập phổ biến. Chính vì những ưu điểm của tối ưu hóa đàm kién có thể giúp tìm được lời giải tối ưu cho bài toán ẩn tập phổ biến, giảm thiểu các hiệu ứng phụ.

Từ khóa: Ant colony optimization, ACO, PPDM, hiding frequent itemset.

1. GIỚI THIỆU

Các thuật toán metaheuristic được sử dụng để tìm một lời giải tối ưu gần đúng cho các bài toán tối ưu khó, trong đó không có một phương pháp chính xác nào có thể giải được trong một khoảng thời gian hợp lý. Một thuật toán metaheuristic được định nghĩa là một thuật toán không phụ thuộc bài toán mà có thể tìm các lời giải gần đúng cho các bài toán khó. Các thuật toán metaheuristic thường được lấy cảm hứng từ tự nhiên và cố gắng giải bài toán bằng cách mô phỏng các hiện tượng vật lý, sinh học, ...

Các thuật toán tiến hóa (EA) là các thuật toán metaheuristic ngẫu nhiên và dựa trên quần thể. EA khác với các thuật toán thông thường khác ở chỗ chúng thực hiện tiến hóa quần thể các lời giải để tiến đến một lời giải tối ưu gần đúng. Thông thường, các EA thực hiện tìm kiếm trong không gian bài toán theo cách sau: một quần thể các các thê (lời giải) được phát sinh một cách ngẫu nhiên ban đầu, sau đó độ thích nghi của chúng được đánh giá dựa trên hàm thích nghi.

Trong các thê hệ tiếp theo, các cá thê tiến hóa theo xu hướng của cá thê tốt nhất và sự trợ giúp của hàm thích nghi. Quá trình này tiếp tục cho đến khi nó đạt được số vòng lặp tối đa hoặc tìm được lời giải gần đúng mong đợi. Một vài thuật toán tiến hóa được biết đến như: Thuật giải di truyền (GA) dựa trên học thuyết tiến hóa của Darwin , Phương pháp tối ưu bầy đàm (PSO) dựa trên việc mô phỏng hành vi kiếm ăn của một đàn chim , Phương pháp tìm hòa âm (Harmony Search - HS) dựa trên phương pháp các nhạc sỹ thay đổi cao độ của nhạc cụ để tìm ra các hòa âm tốt hơn . Gần đây cũng có một số phương pháp tối ưu được công bố như Phương pháp đàm ong nhân tạo (ABC) dựa trên phương pháp tìm kiếm thức ăn của đàm ong mật và Phương pháp tối ưu tìm kiếm nhóm (GSO) dựa trên hành vi tìm kiếm thức ăn của những con thú .

Lấy ý tưởng từ hành vi tìm kiếm thức ăn của những con kiến, phương pháp tối ưu đàm kién (ACO) cũng được công bố sau đó mang lại nhiều hứa hẹn là một thuật toán tối ưu có độ chính xác cao hơn với thời gian tính toán tốt hơn. Thuật toán được thực hiện dựa trên hành vi tìm kiếm thức ăn của đàm kién. Trong tự nhiên, đàm kién tìm kiếm thức ăn bằng cách phát hiện mùi thức ăn và theo dõi nó đến nguồn thức ăn. Các kiến đánh dấu đường đi bằng cách phân bố mùi trên đường đi của mình, người sau đó sẽ cảm thấy và đánh dấu lại đường đi này nếu thấy có mùi đường đi.

Bài báo cáo này trình bày lại thuật toán tối ưu bằng đàm kién và ý tưởng áp dụng thuật toán vào bài toán khai thác dữ liệu đảm bảo tính riêng tư, cụ thể hơn là bài toán ẩn các tập phổ biến.

2. TỐI ƯU HÓA ĐÀM KIÉN

Tối ưu đàm kién (*Ant Colony Optimization - ACO*) là một phương pháp meta-heuristic được đề xuất bởi Dorigo vào năm 1991 dựa trên ý tưởng mô phỏng cách 1920 tìm đường đi từ tổ tới nguồn thức ăn và ngược lại của các con kiến tự nhiên để giải gần đúng bài toán TUTH NP-hard.

Trên đường đi của mình các con kiến thực để lại một vết hóa chất được gọi là vết mùi (*pheromone trail*), đặc điểm sinh hóa học của vết mùi này là có khả năng út định, bay hơi và là phương tiện giao tiếp báo cho các con kiến khác thông tin về đường đi đó một cách gián tiếp. Các con kiến sẽ lựa chọn đường đi nào tồn đọng lượng mùi hay có cường độ vết mùi lớn nhất tại thời điểm lựa chọn để đi, nhờ cách giao tiếp mang tính gián tiếp và cộng đồng này mà đàm kién trong tự nhiên tìm được đường đi ngắn nhất trong quá trình tìm thức ăn mang về tổ và ngược lại. Sử dụng mô hình kiến nhân tạo này Dorigo đã xây dựng thuật toán *hệ kiến* (AS) giải bài toán người chào hàng. Thuật toán này đã được chứng minh tính hiệu quả thông qua thực nghiệm so với các mô phỏng tự nhiên khác như SA và GA. Thuật toán này về sau được phát triển và có nhiều áp dụng phong phú trong thực tế như ACS, MMAS, SMMAS,... được gọi chung là phương pháp ACO.

Theo ý tưởng này, các thuật toán ACO sử dụng thông tin heuristic kết hợp thông tin học tăng cường qua các vết mùi của các con kiến nhân tạo để giải các bài toán tối ưu tổ hợp không bằng cách đưa về bài toán tìm đường đi tối ưu trên đồ thị cấu trúc tương ứng được xây dựng từ đặc điểm của từng bài toán cụ thể. Thuật toán ACO đầu tiên là hệ kiến (*Ant System - AS*) giải bài toán Người chào hàng TSP, đến nay các thuật toán ACO đã áp dụng một cách phong phú để giải nhiều bài toán tối ưu tổ hợp khác nhau và hiệu quả nổi trội của nó đã được chứng tỏ bằng thực nghiệm.

Mô tả thuật toán ACO:

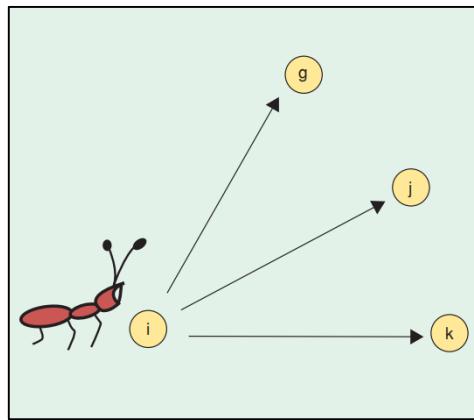
Sử dụng điều kiện kết thúc (có thể theo số bước lặp hoặc/và giới hạn thời gian chạy), ta dùng đàm kién có m con, tiến hành lặp quá trình xây dựng lời giải trên đồ thị cấu trúc $G = (V, E, H, r)$ như sau: Tại mỗi lần lặp, kiến chọn ngẫu nhiên một đỉnh $U_0 \in E_0$ làm thành phần khởi tạo $x_0 = \{u_0\}$ và thực hiện xây dựng lời giải theo thủ tục bước ngẫu nhiên. Dựa trên lời giải tìm được, đàm kién sẽ thực hiện cập nhật mùi theo cách học tăng cường.

Thủ tục bước ngẫu nhiên:

Giả sử $x_k = \langle u_0, \dots, u_k \rangle$ là mở rộng được và chưa thuộc X^* . Từ tập ràng buộc Ω , xác định tập con $J(x_k)$ của C , sao cho với $u_{k+1} \in J(x_k)$ thì $X_{k+1} = \langle u_0, \dots, u_k, u_{k+1} \rangle$ là mở rộng được. Đánh $j = u_{k+1}$ để mở rộng, được chọn với xác suất $P(j)$ như sau:

$$P(j) = \left\{ \sum \frac{[T_{ij}]^a [n_{ij}]^b}{\sum I \in J(x_k) [T_{ij}]^a [n_{ij}]^b} \right\} \in J(x_k), \quad j \in -j_{(k)}$$

Quá trình mở rộng tiếp tục cho tới khi kiếm r tìm được lời giải chấp nhận được x^r trong X^* và do đó $s^r = \varphi(x^r) \in S$.



Hình 1. Lựa chọn bước đi tiếp theo cho 2 cá thể kiến

Ta coi x^r và s^r như nhau và không phân biệt X^* với S .

Cập nhật mùi: Tùy theo chất lượng của lời giải tìm được, vết mùi trên mỗi cạnh sẽ được điều chỉnh tăng hoặc giảm tùy theo đánh giá mức độ ưu tiên tìm kiếm về sau. Lượng mùi cập nhật theo các quy tắc cập nhật mùi khác nhau sẽ cho các thuật toán khác nhau.

Vì vậy, quy tắc cập nhật mùi thường dùng làm tên gọi thuật toán, và chúng có dạng tổng quát là:

$$T_{i,j} \leftarrow (1 - p)T_{i,j} + \Delta(i,j)$$

Trong đó, p là hằng số thuộc khoảng $(0,1)$ là tỷ lệ lượng mùi bị bay hơi.

Đặc tả về thuật toán ACO:

Đầu vào:

- Khoảng cách: một ma trận chứa khoảng cách giữa mỗi thành phố
- n: số lượng kiến trong đàn
- maxIter: số lần lặp tối đa
- alpha: tham số só mủ của pheromone
- beta: tham số só mủ thông tin heuristic
- rho: tốc độ bay hơi vết pheromone
- tau0: giá trị đầu vết pheromone ban đầu
- Q: một hằng số được sử dụng để cập nhật đường dẫn pheromone

Khởi tạo:

1. Đặt đường pheromone ban đầu $\tau(i,j) = \tau_0$ cho tất cả các cạnh (i,j)
2. $t = 0$

Lặp lại cho đến khi đáp ứng tiêu chí dừng ($t < \text{maxIter}$):

1. Với mỗi con kiến k trong $\{1, \dots, n\}$:

Một. Chọn một thành phố ngẫu nhiên để bắt đầu từ

b. Lặp lại cho mỗi thành phố mà kiến k đã ghé thăm (ngoại trừ thành phố cuối cùng):

- i. Tính xác suất chuyển đến thành phố j từ thành phố i:

$p(i,j) = [\tau(i,j)^{\alpha} * h(i,j)^{\beta}] / \sum [\tau(i,l)^{\alpha} * h(i,l)^{\beta}]$ cho tất cả các phép tính
trong đó $h(i,j) = 1/\text{khoảng cách}(i,j)$ là thông tin khám phá

- ii. Sử dụng lưa chọn bánh xe roulette để chọn thành phố tiếp theo để ghé thăm dựa trên xác suất

iii. Cập nhật giải pháp hiện tại và ghi lại tổng quãng đường đã đi

- c. Cập nhật dấu vết pheromone trên mỗi cạnh trong hành trình của đàn kiến dựa trên chất lượng của giải pháp:

$$\Delta\tau(i,j) = Q / \text{tổng Khoảng cách}$$

$$\tau(i,j) = (1 - \rho) * \tau(i,j) + \rho * \Delta\tau(i,j)$$

2. Tìm k có nghiệm đúng nhất

3. Cập nhật giải pháp tốt nhất toàn cầu nếu giải pháp của kiến k tốt hơn

4. Làm bay hơi vết pheromone trên mỗi cạnh:

$$\tau(i,j) = (1 - \rho) * \tau(i,j)$$

5. Tăng t

Trả lại giải pháp tốt nhất toàn cầu

Kết thúc

Nhận xét chung về các thuật toán ACO:

Nhờ kết hợp thông tin heuristic, thông tin học tăng cường và mô phỏng hoạt động của đàn kiến, các thuật toán ACO có các ưu điểm sau:

- Việc tìm kiếm ngẫu nhiên dựa trên các thông tin heuristic trở nên linh hoạt và mềm trên miền rộng hơn so với các phương pháp heuristic đã có. Do đó, cho ta lời giải tốt hơn và có thể tìm được lời giải tối ưu.
- Học tăng cường thông qua thông tin về cường độ vết mùi cho phép từng bước thu hẹp không gian tìm kiếm, mà vẫn không loại bỏ các lời giải tốt, do đó nâng cao chất lượng thuật toán.

Chú ý: Khi áp dụng phương pháp ACO cho các bài toán cụ thể, ba yếu tố sau có ảnh hưởng quyết định đến hiệu quả thuật toán:

– **Xây dựng đồ thị cấu trúc thích hợp:** Việc xây dựng đồ thị cấu trúc để tìm được lời giải cho bài toán theo thủ tục tuần tự không khó. Khó khăn chính là với các bài toán cỡ lớn, không gian tìm kiếm quá rộng, đòi hỏi ta sử dụng các ràng buộc một cách hợp lý để giảm miền tìm kiếm của kién.

– **Chọn thông tin heuristic:** Thông tin heuristic tốt sẽ tăng hiệu quả thuật toán. Tuy nhiên, trong nhiều bài toán không có thông tin này thì có thể đánh giá chúng như nhau. Khi đó, ban đầu thuật toán chỉ đơn thuần chạy theo phương thức tìm kiếm ngẫu nhiên, vết mùi thể hiện định hướng của học tăng cường và thuật toán vẫn thực hiện được.

– **Chọn quy tắc cập nhật mùi:** Quy tắc cập nhật mùi thể hiện chiến lược học của thuật toán. Trong khi đồ thị cấu trúc và thông tin heuristic phụ thuộc vào bài toán cụ thể, quy tắc cập nhật mùi lại là yếu tố phổ dụng và thường dùng để đặt tên cho thuật toán.

3. VÍ DỤ MINH HỌA

Lấy ví dụ hàm tối ưu được định nghĩa bởi công thức:

$$f(x, y, z) = \frac{1}{2}x^2 + \frac{1}{3}y^2 + \frac{1}{6}z^2$$

Tính min value của x, y, z trong khoảng [-2,2]

Bước đầu tiên, khởi tạo quần thể các con kién. Ở đây rõ ràng bài toán có 3 biến, chọn số lượng con kién là 10. Khởi tạo, tính độ fitness ta được *Bảng 1* bên dưới.

Bảng 1. Tập hợp các con kién từ sau bước khởi tạo

	x	y	z	fitness
1	-0.231413212	-0.22266787	-0.614255563	0.105526165
2	1.139154879	0.201061281	-0.445325805	0.485823278
3	-1.261167961	0.377311053	-0.154967346	0.605365837
4	-0.281534362	-1.116092634	-0.311228113	0.665395739
5	-0.116010948	-1.380903338	-0.478561889	0.996103441
6	1.403381194	-0.74193663	-0.941943339	1.079604116
7	1.82678016	0.530788008	0.464887455	1.289263264
8	1.554425488	-0.743275028	-1.312591683	1.368791237
9	-1.726675206	0.299406381	-1.54145776	1.434639851
10	-1.556846251	1.251562107	1.213090431	1.836392002

Sau vòng lặp đầu tiên, các cá thể kién đi qua tất cả các đỉnh và tìm ra được vị trí của thức ăn tốt nhất ở vòng lặp đầu tiên là [0.3161076902875086, 0.2797437968345613, 0.30768903059761277, 0.08821507647835909]

0.3348947825492	0.1251796619854	-0.2127888859948	0.05276633068079
-----------------	-----------------	------------------	------------------

Như vậy ta đã thu được vị trí thức ăn tốt nhất, tương tự thực hiện lặp lại 10 vòng rồi đến 50 vòng, 100 vòng, ...

Bảng 2. Tập hợp các con kién từ sau 10 vòng lặp

1	0.31610769	0.279743797	0.307689031	0.088215076
2	0.31610769	0.124798633	-0.080581778	0.018616403

3	0.170998387	0.124798633	-0.080581778	0.018616403
4	0.170998387	0.124798633	-0.080581778	0.018616403
5	0.170998387	0.124798633	-0.080581778	-0.080581778
6	0.007604985	0.184772535	-0.001690199	0.017090199
7	0.007604985	0.184772535	-0.001690199	0.017090199
8	0.007604985	0.184772535	-0.001690199	0.017090199
9	0.007604985	0.184772535	-0.001690199	0.017090199
10	0.007604985	0.184772535	-0.001690199	0.017090199

Bảng 3. Tập hợp các con kiến từ sau 100 vòng lặp

91	0.051920782	-0.033362629	0.090560405	0.002821986
92	0.051920782	-0.033362629	0.090560405	0.002821986
93	0.051920782	-0.033362629	0.090560405	0.002821986
94	0.051920782	-0.033362629	0.090560405	0.002821986
95	0.051920782	-0.033362629	0.090560405	0.002821986
96	0.051920782	-0.033362629	0.090560405	0.002821986
97	0.051920782	-0.033362629	0.090560405	0.002821986
98	0.051920782	-0.033362629	0.090560405	0.002821986
99	0.051920782	-0.033362629	0.090560405	0.002821986
100	0.051920782	-0.033362629	0.090560405	0.002821986

4. ÚNG DỤNG TRONG BÀI TOÁN ẨN TẬP PHỔ BIẾN

Định nghĩa 1. (Bài toán ẩn tập phổ biến). Cho trước một cơ sở dữ liệu giao tác D có tập hạng mục $I = \{i_1, i_2, \dots, i_r\}$, một độ hỗ trợ tối thiểu δ và một tập các tập phổ biến nhạy cảm SIs. Thực hiện biến đổi D thành D' sao cho $\text{supD}'(X) < \delta \forall X \in S$. Khi thực hiện bài toán ẩn tập phổ biến, thông thường xuất hiện 3 loại kết quả không mong muốn như sau.

Định nghĩa 2. (Fail to Hide – FTH). Là số lượng các tập nhạy cảm xuất hiện trong cơ sở dữ liệu D' . Điều này có nghĩa là sao khi thực hiện phương pháp ẩn tập nhạy cảm, có một số tập không thể ẩn được thông qua phương pháp đó. Thông số này được ký hiệu là α .

Định nghĩa 3. (Not to be Hidden - NTH). Là số lượng các tập phổ biến không nhạy cảm bị ẩn trong cơ sở dữ liệu D' . Điều này có nghĩa là khi áp dụng phương pháp ẩn tập nhạy cảm, một số tập phổ biến không nhạy cảm cũng bị ẩn theo. Thông số này ký hiệu là β .

Định nghĩa 4. (Not to be Generated - NTG). Là số lượng các tập không phổ biến trong cơ sở dữ liệu D lại trở thành phổ biến trong cơ sở dữ liệu D' . Điều này có nghĩa là khi áp dụng phương pháp ẩn tập nhạy cảm, một số tập không phổ biến trong cơ sở dữ liệu ban đầu lại trở thành phổ biến trong cơ sở dữ liệu hiệu chỉnh, các tập này còn gọi là các tập ma. Thông số này được ký hiệu là γ .

Thực tế, không có phương pháp ẩn tập phổ biến nào hoàn hảo đến mức có thể làm cho các thông số không mong muốn tất cả đều bằng không. Như vậy, bài toán ẩn tập phổ biến có thể quy về bài toán tối ưu với hàm mục tiêu

$$f = w_1\alpha + w_2\beta + w_3\gamma$$

Trong đó, w1, w2, w3 là các trọng số tương ứng với các thông số không mong muốn. Thông thường w1 sẽ được đặt lớn hơn nhiều so với w2 và w3 với mong muốn có thể ăn hoàn toàn các tập nhạy cảm.

Áp dụng phương pháp tối ưu đàm kién cho bài toán ăn tập nhạy cảm, công trình này đề xuất một phương pháp mới để giải bài toán theo hướng metaheuristic. Mỗi đàm kién sẽ chứa N_var con kién. Mỗi con kién sẽ chứa thông tin về Tid (Transaction ID) cần hiệu chỉnh hoặc xóa bỏ. N_var có thể tính theo công thức

$$N_{var} = \left\lceil \frac{Max_sup(si) - \delta * |D|}{1 - \delta} \right\rceil$$

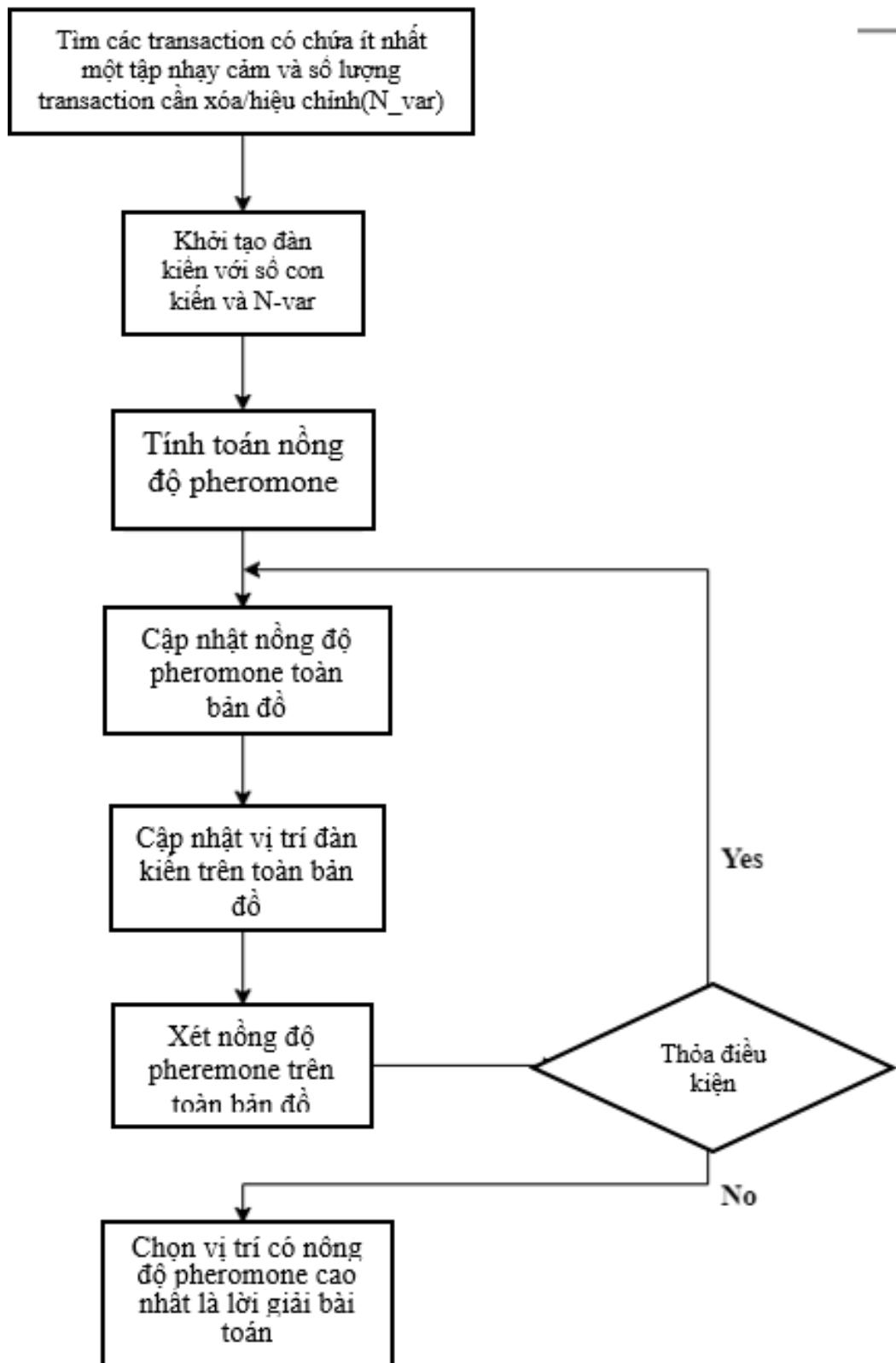
Trong đó:

- Max_sup(si): độ hỗ trợ lớn nhất trong số tất cả các tập nhạy cảm δ: độ hỗ trợ tối thiểu.
- |D|: số lượng các giao tác có trong tập dữ liệu gốc.

Sau khi tính được nồng độ Pheromone tối ưu, các con kién sẽ được khởi tạo một cách ngẫu nhiên dựa trên các thông tin các transaction có chứa ít nhất 1 tập nhạy cảm. Các con kién đã được khởi tạo sẽ được đánh giá độ thích nghi sau đó và sắp xếp lại theo độ thích nghi.

Trong mỗi vòng lặp, nồng độ pheromone sẽ được cập nhật dựa trên quá trình đi tìm kiếm thức ăn của đàm kién. Đàm kién sẽ di chuyển về phía thức ăn dựa vào nồng độ pheromone đã được cập nhật.

Các con kién sẽ đánh giá nồng độ pheromone và chèn vào trong danh sách vị trí ứng với nồng độ pheromone của nó. Vị trí có nồng độ pheromone thấp nhất sẽ bị loại bỏ. Phương pháp ăn tập phổ biến sử dụng tối ưu đàm kién được biểu thị bởi sơ đồ ở Hình 2.



Hình 2. Sơ đồ phương pháp giải bài toán ẩn tập phô biến sử dụng ACO

5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Bài báo này trình bày thuật toán tối ưu hóa đàm kién bằng cách tạo ra các con kiến đi tìm kiếm thức ăn. Các con kiến đi tìm kiếm thức ăn, mô phỏng bằng các đối tượng ảo được gọi là "điểm kiểm tra". Thuật toán sử dụng các "mùi hương" để hướng dẫn các con kiến ảo đi theo hướng trong quá trình tìm kiếm. Các mùi hương này đại diện cho các đường đi được tìm thấy bởi các con kiến ảo khác và có độ hấp dẫn khác nhau tùy thuộc vào chi phí của đường đi. Các con kiến ảo sẽ ưu tiên đi theo những đường có mùi hương hấp dẫn hơn, và các mùi hương này càng mạnh hơn nếu các con kiến ảo trên đường đó tìm thấy lời giải tốt hơn. Trong bài báo cũng trình bày phương pháp để xuất ứng dụng thuật toán tối ưu đàm kién để giải bài toán khai thác dữ liệu đảm bảo tính riêng tư. Mặc dù chưa có thực nghiệm cụ thể về phương pháp mới này, nhưng phương pháp hứa hẹn sẽ cho kết quả chính xác.

Các kết quả thực nghiệm cụ thể sẽ được công bố trong các báo cáo tiếp theo.

TÀI LIỆU THAM KHẢO

1. "Ant Colony Optimization: A Review," by Dorigo, M., Blum, C. (2005) in Artificial Life Journal.
2. "Ant Colony Optimization for the Traveling Salesman Problem: An Implementation Tutorial," by Gambardella, L.M., Dorigo, M. (1996) in Journal of Artificial Intelligence Research.
3. "Ant Colony Optimization: A Metaheuristic Approach to Combinatorial Optimization Problems," by Stützle, T. (1998) in Theoretical Computer Science..
4. "A survey of ant colony optimization algorithms for the minimum spanning tree problem," by Wang, Y., Liu, L., & Gao, H. (2013) in Journal of Computational and Applied Mathematics.
5. "An Ant Colony Optimization Algorithm for Job Shop Scheduling," by Dorigo, M., Di Caro, G. (1999) in IEEE Transactions on Evolutionary Computation

ABSTRACT

OPTIMIZATION OF ANSWERS AND APPLICATIONS IN HIDING FREQUENT ITEMSET PROBLEMS

Ho Thanh Hai¹, Dinh Nguyen Trong Nghia¹

¹*Ho Chi Minh City University of Food Industry*

*Email: nghiadnt@hufi.edu.vn

This paper presents the ant colony optimization algorithm which is a metaheuristic algorithm inspired by the foraging behavior of ants and borers. The strength of the ant colony optimization algorithm is its ability to find optimal solutions in a generalization problem of large size. In addition, the paper also proposes a method of applying ant colony optimization to the problem of hiding frequent itemsets. Because of the advantages of ant colony optimization, it is possible to find the optimal solution for the problem of hiding frequent itemsets, minimizing side effects.

Keywords: ant colony optimization, ACO, PPDM, hiding frequent itemset.

HỆ THỐNG THÔNG TIN Y TẾ MỘT CÁCH TIẾP CẬN DỰA TRÊN THÀNH PHẦN

Huỳnh Hữu Nghĩa¹, Nguyễn Thị Thu Tâm^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: tamntt@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trong bài báo giới thiệu một cách tiếp cận dựa trên thành phần cho hệ thống thông tin y tế. Với cách tiếp cận này, hệ thống sẽ linh hoạt, dễ nâng cấp, sửa chữa và bảo trì. Hơn nữa, hệ thống sẽ không phụ thuộc hoàn toàn vào một nhà cung cấp giải pháp về công nghệ mà có thể chọn nhiều nhà cung cấp khác nhau cung cấp các gói phần mềm tốt nhất cho từng thành phần. Với các kỹ thuật và công nghệ hiện nay hoàn toàn có thể cho phép triển khai một hệ thống thông tin y tế dựa trên thành phần một cách dễ dàng.

Từ khóa: Hệ thống thông tin y tế, Hệ thống thông tin, Phần mềm y tế.

1. MỞ ĐẦU

Hiện nay trên thế giới, có ba hệ thống thông tin đang được các bệnh viện triển khai: hệ thống thông tin bệnh viện (Hospital Information Systems – HISs), hệ thống thông tin y tế cộng đồng (Community Health Information Systems – CHISs) và hệ thống thông tin lâm sàng (Clinical Information Systems – CISs) để tự động hóa các hoạt động của Bệnh viện nhằm hỗ trợ cho các bác sĩ, y tá và các nhà cung cấp dịch vụ chăm sóc sức khỏe trong các hoạt động chăm sóc bệnh nhân hàng ngày và cung cấp các nguồn tài nguyên thông tin trực tuyến cho giáo dục và đào tạo. Với ba hệ thống nêu trên đã mở rộng các chức năng quản lý chăm sóc bệnh nhân ngày càng tốt hơn và tiết kiệm được chi phí.

Bối cảnh trong nước, các cơ quan chức năng cũng đã đưa ra nhiều quyết định nhằm tạo cơ sở pháp lý cho việc ứng dụng công nghệ thông tin trong ngành y tế:

- Ngày 19-08-2004, Bộ Y Tế đã có quyết định số 2824/2004/QĐ-BYT về việc Ban hành phần mềm ứng dụng tin học.
- Ngày 17-03-2006, Bộ Y tế đã thành lập “Ban chỉ đạo triển khai ứng dụng và phát triển CNTT trong ngành y tế” qua quyết định thành lập số 952/QĐ-BYT.
- Ngày 29-12-2006, Bộ Y tế đã có quyết định 5573/QĐ-BYT về “Tiêu chí phần mềm và nội dung một số phần mềm tin học quản lý bệnh viện”.
- Để cụ thể hóa những quyết định này, nhiều hội nghị và hội thảo cũng đã được tổ chức:
 - Ngày 18-03-2006 tại Hải Phòng, Bộ Y tế đã tổ chức “Hội thảo về thực trạng và định hướng phát triển công nghệ thông tin ngành y tế giai đoạn 2006–2015”.
 - Ngày 04-05-2007, Phân viện Công nghệ Thông tin tại TP.HCM phối hợp với Sở Y tế TP.HCM tổ chức hội thảo “Công nghệ Thông tin Y tế và Telemedicine”.

– Ngày 07-12-2007, Sở Bưu chính-Viễn thông và Sở Y tế Gia Lai phối hợp tổ chức hội thảo “Ứng dụng Công nghệ Thông tin trong ngành Y tế”.

Một số công ty ở Việt Nam như: HT MEDSOFT, DTAD, ... đang cung cấp các phần mềm và dịch vụ y tế chẳng hạn như: yClinic SE 2008 dành cho phòng khám đa khoa đã triển khai sử dụng tại một số cơ sở y tế, các sản phẩm yHospital SE 2008, yRad SE 2008 và yMage IE 2008 triển khai tại trung tâm Cột sống EXSON thuộc bệnh viện Phương Đông STO, TP. HCM và Khoa Chẩn đoán Hình ảnh bệnh viện Chợ Rẫy.

Thực tế, rất khó để tìm thấy một gói phần mềm phù hợp với tất cả nhu cầu của tổ chức y tế. Hơn nữa, chi phí liên quan đến việc điều chỉnh một gói phần mềm tích hợp vào môi trường hiện tại là rất khó xác định. Xu hướng mới, người ta không đi xây một phần mềm phủ hết các yêu cầu mà chuyển sang xây dựng hệ thống bằng cách lắp ráp các thành phần sẵn có hiện nay. Kiến trúc dựa trên thành phần làm giảm chi phí phát triển, cho phép thay thế các thành phần và có thể tái sử dụng.

Các công nghệ dựa trên thành phần tạo điều kiện thuận lợi cho sự phát triển từ kiến trúc định hướng dữ liệu tới định hướng tri thức và việc duy trì khả năng mở rộng các ứng dụng phức tạp để làm tăng khả năng tồn tại lâu dài hơn.

Sự phức tạp của các ứng dụng y tế ngày càng tăng và nhu cầu duy trì khả năng mở rộng có thể giải quyết bằng kỹ thuật phân rã. Kỹ thuật phân rã là cốt lõi phát triển dựa trên thành phần, phân chia một vấn đề phức tạp thành nhiều vấn đề nhỏ hơn, nhiều đơn vị quản lý, mỗi phần tương ứng có thể được giải quyết riêng biệt [10].

Các thành phần bao trùm một loạt thay đổi diện mạo rộng lớn từ công nghệ đến tổng thể và lĩnh vực cụ thể [7]. Nếu chúng ta phân tích các hệ thống hiện nay, phần lớn các chức năng đều giống nhau. Các dịch vụ y tế giữa các tổ chức chỉ khác nhau ở các gói dịch vụ. Do đó, khi phát triển phần mềm cần phải tập trung để hiểu các lĩnh vực con (subdomains) cụ thể cùng với các yêu cầu văn hóa và nơi tương ứng.

Trong phạm vi bài báo này trình bày một số vấn đề có liên quan và giới thiệu kiến trúc chung cũng như các công nghệ được áp dụng để triển khai hệ thống thông tin y tế dựa trên thành phần và trình bày một tình huống nghiên cứu cụ thể để minh họa.

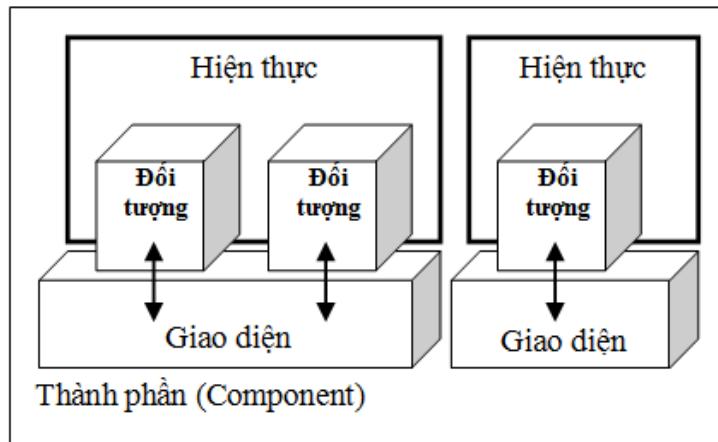
2. CÁC CÔNG VIỆC LIÊN QUAN

2.1. Các khái niệm cơ bản

Đối tượng là một thực thể tồn tại ở thế giới thực, ý tưởng hay sự kiện. Đối tượng là duy nhất, cho nên cần được xác định bởi một định danh. Các đối tượng cung cấp một số dịch vụ và cho phép thao tác dữ liệu bên trong đối tượng. Đối tượng giao tiếp với thế giới bên ngoài thông qua giao diện. Việc hiện thực hoặc mô tả những công việc của đối tượng như thế nào là ẩn. Hiện thực bao gồm dữ liệu và mã hóa (xem hình 1). Nhiều đối tượng có thể chia sẻ cùng hiện thực [4]. Một đối tượng có thể có nhiều giao diện hoặc nhiều đối tượng có thể chia sẻ cùng một giao diện.

Thành phần là các khối được xác định trước, nó đóng gói một hoặc nhiều đối tượng được thiết kế để các nhà phát triển có thể xây dựng các hệ thống ngay cả khi không có tri thức gì về thành phần. Mỗi thành phần có tính chất hai chiều khác nhau đó là chiều ngang và chiều dọc. Chiều ngang là có thể tái sử dụng phạm vi rộng trong đơn vị thông qua nhiều dự án và

nhiều lĩnh vực ứng dụng. Ví dụ về các thành phần theo chiều ngang gồm tập hợp các lớp được tổng quát hóa, những lớp lưu trữ liên tục, các lớp khung ứng dụng và các mẫu thiết kế. Chiều dọc là lĩnh vực cụ thể và thường được mã hóa với rất nhiều tri thức cục bộ để phát triển những dịch vụ ứng dụng.



Hình 1. Minh họa thành phần, giao diện và đối tượng

Thành phần thì dựa trên mô hình thành phần hay khung làm việc chung. Mô hình thành phần cung cấp một số dịch vụ hỗ trợ phần mềm và một số qui tắc cần phải tuân thủ để tận dụng lợi thế của những dịch vụ. Các mô hình thành phần nổi tiếng gồm JavaBeans, CORBA, COM+. Khung chung định nghĩa kiến trúc của một ứng dụng và quy định sự tương tác giữa tập các đối tượng công việc. Cụ thể hơn, khung chung là định nghĩa các quy tắc mà những đối tượng cần thực hiện theo những đối tượng ở thế giới thực của nó, cho phép dữ liệu trao đổi và xử lý tất cả dòng điều khiển, cho phép trao đổi các dịch vụ giữa những đối tượng bằng tin nhắn, cung cấp một môi trường nhất quán và là một lớp chứa các đối tượng nghiệp vụ.

2.2. Các qui tắc nghiệp vụ

Các qui tắc nghiệp vụ là các biểu hiện ngôn ngữ tự nhiên, mà mỗi tổ chức sử dụng để thực hiện và giải quyết vấn đề. Các qui tắc nghiệp vụ và quá trình xử lý được thực hiện tập trung trên tầng trung gian. Các kiến trúc ba tầng là thích hợp để giải quyết cho vấn đề này. Các hệ thống thông tin truyền thống trở nên lỗi thời, thiếu linh hoạt, không phù hợp và hầu như không thể thay đổi nhanh chóng.

Các qui tắc nghiệp có thể chia thành hai loại chính: các qui tắc dựa trên cấu trúc và khai báo [16]. Qui tắc dựa trên cấu trúc và được qui định thông qua mô hình nghiệp vụ của chính nó. Ví dụ: *Bệnh nhân phải có ít nhất một đơn thuốc; Ngày là bắt buộc đối với mỗi giao dịch và không thể thay đổi được; Bệnh nhân không thể nào xóa đi những kết quả quan trọng*. Các qui tắc khai báo bao gồm tính hợp lý nghiệp vụ phức tạp có thể xác định thông qua mô hình đối tượng. Hành vi của nó tồn tại trong sự kết hợp với các qui tắc dựa trên cấu trúc. Qui tắc khai báo có thể chia nhỏ ra thành: qui tắc giới hạn và điều chỉnh. Các qui tắc giới hạn kiểm soát các điều kiện luôn luôn là đúng trong nghiệp vụ (ví dụ, *bệnh nhân không được phép chụp cắt lở hơn một lần trong vòng 24 giờ*). Các qui tắc điều chỉnh làm thay đổi dữ liệu dựa trên các điều kiện xảy ra (ví dụ, *tự động in đơn thuốc nếu một bệnh nhân nhận tất cả các loại thuốc từ đơn thuốc cụ thể*).

2.3. Các yêu cầu chức năng kiến trúc

Phát triển cơ sở hạ tầng thông tin y tế là một thách thức trong quản lý. Rất nhiều công trình kiến trúc được thực hiện trong lĩnh vực này (ví dụ như các dự án IMG 1992, RICHE 1992, Ferrara 1998), nhưng ít thấy công trình dựa trên quan điểm theo hướng thành phần.

Với sự phức tạp của các tổ chức y tế ngày càng tăng và sự đánh giá công nghệ khác nhau được quan sát trên các hệ thống con, một khung kiến trúc phải đáp ứng được các yêu cầu như sau [15]:

- Khả năng tương tác giữa nhiều hệ thống chuyên gia, phân tán hay những cái đang tồn tại. Việc thiết kế sẽ hỗ trợ các kiểu dữ liệu cụ thể và các chức năng nghiệp vụ nằm trong các hệ thống thông tin chuyên biệt. Nó sẽ cải thiện sự phối hợp, khả năng chia sẻ và khả năng sử dụng lại thông tin giữa các bộ phận khác nhau trong một môi trường lâm sàng lớn khi mà những người bệnh ngày nay thường xuyên điều trị độc lập cho những vấn đề khác nhau [9]. Khả năng tương tác không chỉ đòi hỏi chia sẻ thông tin mà còn cộng tác thông qua kết nối giữa các tác nhân y tế và hệ thống. Để có thể lập kế hoạch, khởi động, theo dõi, và kiểm soát các thủ tục hành chính và lâm sàng được xác định trước, một hệ thống quản lý tiến trình nghiệp vụ cung cấp khả năng hợp tác trong các nhiệm vụ thực hiện là cần thiết [12].

- Tính không đồng nhất của các nguồn dữ liệu. Một tổ chức y tế có nhiều kho chứa thông tin liên quan đến bệnh nhân phân tán và phổ biến trên các hệ thống phòng ban. Mỗi hệ thống phòng ban chịu trách nhiệm tạo ra và theo dõi dữ liệu của chính mình. Để tích hợp các ứng dụng y tế đa dạng, được viết bằng những ngôn ngữ khác nhau trên các hệ thống tương ứng là một vấn đề đầy thách thức. Việc tích hợp này không chỉ đơn giản là kết nối các hệ thống hay các phòng ban. Mục đích của nó là để đạt được một sự hợp nhất tổ chức. Kiến trúc phải cung cấp một giao diện dựa trên công nghệ và mức độ phù hợp với tất cả các hệ thống phòng ban để xác định thông tin cần được trao đổi và cách trao đổi như thế nào.

- Giao diện người dùng nhất quán và đồng nhất. Để tránh sự hiểu nhầm (hay hiểu không đúng) cần phải có giao diện người dùng nhất quán và phù hợp với những nhu cầu và các đặc quyền (privileges) của người dùng. Hơn nữa, sự khác nhau thông qua tùy chỉnh cho các biến trong quá trình xử lý nghiệp vụ của người dùng phải được xây dựng sẵn.

- Khả năng mở rộng và độ co giãn là cần thiết để duy trì quyền sở hữu hợp lý dữ liệu để bảo đảm các khía cạnh mới của lĩnh vực y tế như hệ thống phát triển.

- Khả năng tiếp cận và thích ứng. Ở mức độ chức năng, người sử dụng và các bác sĩ lâm sàng, phụ thuộc vào hồ sơ người dùng, phải có quyền truy cập tới các chức năng y tế cốt lõi chẳng hạn như các hệ thống hỗ trợ quyết định lâm sàng, các tài liệu y tế mới nhất, đơn thuốc, nhân khẩu học bệnh nhân, thư điện tử, các kết quả báo cáo, cảnh báo, nhắc nhở, v.v.

2.4. Các yêu cầu thiết kế kiến trúc

(1) Các lớp kiến trúc

Các yêu cầu thông tin của một tổ chức có thể xem xét từ hai góc độ khác nhau nhưng liên quan với nhau đó là kiến trúc lôgic và kiến trúc vật lý của một hệ thống. Kiến trúc lôgic là nhấn mạnh mô hình nghiệp vụ đồng bộ với các yêu cầu tổ chức, mô hình ứng dụng xác định môi trường các đối tượng nghiệp vụ được sử dụng và phạm vi giao diện người dùng trong hệ thống. Kiến trúc vật lý của hệ thống giao tiếp với cơ sở hạ tầng kỹ thuật: lược đồ phân bố phần mềm và phần cứng giữa các nút, những hệ thống tập tin được chọn lọc và mạng (networks).

(2) Các chức năng của kiến trúc

Ba mô hình độc lập có thể được sử dụng để trình bày kiến trúc của bất kỳ môi trường công nghệ cụ thể. Mô hình tĩnh (static model) cung cấp các mô tả (thuật ngữ của các thuộc tính và các giá trị thuộc tính) và biểu diễn các mối quan hệ giữa các thành phần (liên kết, kết hợp, tổng quát hoá). Mô hình động (dynamic model) cung cấp các ký hiệu đồ họa cho các sự kiện, các ký hiệu sự kiện, các trạng thái, các chuyển tiếp trạng thái và phân cấp của các trạng thái. Nó giải thích các lớp khác nhau tác động cùng với nhau như thế nào trong tình huống cụ thể. Mô hình chức năng (functional model) là mô hình kiến trúc hỗn hợp hoàn thiện. Khi các đối tượng (dữ liệu) được định nghĩa trong mô hình đối tượng và hành vi được xác định trong mô hình, điều còn lại duy nhất cần được xác định là các hoạt động (các qui trình xử lý hay các chức năng) và những ràng buộc trên các hoạt động.

Các tương tác đối tượng có thể được nắm bắt và mô tả bằng cách sử dụng các công cụ thiết kế phổ biến như UML [3], các ký hiệu sự kiện (event traces) [14], các kịch bản công việc (task scripts) [8], các biểu đồ tương tác (interaction diagrams) [2], và Use cases [11].

3. KIẾN TRÚC DỰA TRÊN THÀNH PHẦN

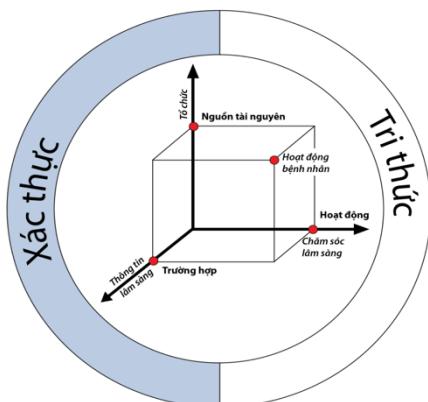
Trong phần này, chúng tôi sẽ trình bày kiến trúc chung (ở mức lôgic) các thành phần nghiệp vụ liên quan đến hệ thống thông tin y tế dựa trên thành phần. Các thành phần nghiệp vụ y tế hỗ trợ các yêu cầu cơ bản của tổ chức y tế trong các phần của thông tin được xử lý, các hoạt động và các dịch vụ được thực hiện cùng với việc cung cấp các điều kiện thuận lợi để liên lạc và hợp tác. Thiết lập các thành phần nghiệp vụ vẫn được coi là mở, có thể bổ sung thêm các yếu tố kiến trúc. Kiến trúc phát triển theo thời gian đáp ứng sự phát triển các yêu cầu của tổ chức.

Một tổ chức y tế bao gồm các nhân viên được cấp quyền họ thực hiện các hoạt động liên quan đến nhu cầu của một đối tượng chăm sóc (subject of care) sử dụng nguồn tài nguyên và tạo ra một kết quả dựa trên trí thức.

Dựa trên cơ sở giả định như vậy, một số thành phần chính được nhận diện từ mô hình kiến trúc hệ thống thông tin y tế như sau: bệnh nhân (đối tượng chăm sóc), hoạt động, hồ sơ y tế, nguồn tài nguyên, quyền hạn và các thành phần tri thức [5] (xem hình 2).

3.1. Thành phần bệnh nhân

Thành phần bệnh nhân là các đối tượng chăm sóc chính trong chăm sóc y tế được xử lý theo dõi hoặc thay đổi các tình trạng y tế ở mức thao tác, bao gồm nhiều bệnh nhân hay nhiều nhóm bệnh nhân. Mật độ dân cư và nhu cầu đôi khi được phân tích ở mức kế hoạch của bệnh viện để xác định các loại dịch vụ cần thiết. Các đối tượng chăm sóc khác là các mẫu (specimens) và các nội tạng cấy ghép (transplant organs). Các mẫu có thể liên quan đến bệnh nhân và các thuộc tính của mẫu có thể được sử dụng trong suy diễn tình trạng lâm sàng của



Hình 2. Các thành phần chính của mô hình kiến trúc hệ thống thông tin y tế dựa trên thành phần.

bệnh nhân. Các đối tượng chăm sóc có thể có quan hệ với nhau (chẳng hạn như: mẹ - con, vợ - chồng, ...). Các mối quan hệ có thể thay đổi theo thời gian. Các thuộc tính đặc trưng chính là xác định bên trong và bên ngoài môi trường y tế, các thuộc tính nhân khẩu học đặc trưng và vị trí trong tổ chức y tế.

Thành phần bệnh nhân cung cấp kho lưu trữ thông nhất để lưu trữ thông tin bệnh nhân, các dịch vụ để các ứng dụng máy khách duy trì tất cả dữ liệu nhân khẩu học và hành chính liên quan đến bệnh nhân (hay đối tượng chăm sóc).

3.2. Thành phần hoạt động

Thành phần hoạt động là một trong những thành phần quan trọng nhất để đạt được sự tích hợp giữa các quá trình chăm sóc y tế của bệnh nhân. Do đó, thành phần hoạt động phản ánh và hỗ trợ tổ chức y tế nói chung. Thành phần hoạt động quản lý dòng công việc và thông tin giữa các tác nhân y tế khác nhau dựa trên đầu ra của công cụ lập danh mục (như một phần của thành phần nguồn tài nguyên được mô tả bên dưới). Thành phần hoạt động là cơ sở cho các hệ thống POE (provider order entry).

Tầm ảnh hưởng của bảng chứng lâm sàng trên thực hành lâm sàng là rất lớn, việc tạo ra các giao thức lâm sàng là một thách thức về kỹ thuật và một cơ hội đầy hứa hẹn trong lĩnh vực tin học y tế. Với ý nghĩa này, thành phần hoạt động là yếu tố cơ bản. Thường trong tin học y tế, một hệ thống thành công chỉ khi nó có thể tích hợp với hệ thống khác. Ví dụ nó phải cung cấp các đặc trưng để đưa vào tài khoản, càng nhiều càng tốt, ngữ cảnh một giao thức sẽ được sử dụng.

Một hoạt động có thể là cơ bản, phức hợp hay lặp đi lặp lại. Việc thiết lập các hoạt động phức hợp hoặc lặp đi lặp lại bao hàm việc thiết lập các hoạt động cơ bản hợp thành tương ứng. Thuộc điều trị trong điều dưỡng là ví dụ một hoạt động lặp đi lặp lại. Một quá trình chăm sóc lâm sàng có thể được xem như một hoạt động phức hợp.

Các hoạt động thực hiện trên danh nghĩa của bệnh nhân (đối tượng chăm sóc) có thể phân thành hai nhóm:

- Các hoạt động cung cấp thông tin về tình trạng chăm sóc y tế của bệnh nhân. Thông tin này có thể là một kết quả định lượng, kết quả mô tả hay kết hợp cả hai.
- Các hoạt động cố gắng để thay đổi hoặc duy trì tình trạng y tế của bệnh nhân.

Khi một hoạt động thực thi, dữ liệu y tế khác nhau được tạo ra như một phần của hồ sơ y tế điện tử. Thông tin này được cấu trúc theo một kiểu hoạt động hay vai trò của các nhân tố chăm sóc y tế thực hiện.

3.3. Thành phần quản lý tài nguyên

Thành phần tài nguyên cung cấp cho người dùng thông tin và các chức năng có liên quan tới nguồn tài nguyên có sẵn và được phép sử dụng. Vai trò quan trọng nhất của thành phần tài nguyên là giải quyết phân bổ tài nguyên (con người, thiết bị y tế, công việc, v.v.) và vấn đề lập danh mục trong một môi trường ràng buộc chặt chẽ. Giải quyết vấn đề này là cần thiết và là mục tiêu quan trọng của tổ chức và y tế trong nhiều tổ chức chăm sóc y tế để hoạt động hiệu quả về mặt chi phí. Việc lập danh mục hệ thống toàn bệnh viện cung cấp dịch vụ tốt hơn cho bệnh nhân, cải thiện việc sử dụng nguồn tài nguyên và năng suất nhân viên tăng lên. Các hệ thống lập danh mục tiên tiến không được thiết kế cho một dịch vụ riêng biệt mà

phải có khả năng mở rộng các hệ thống và chức năng y tế khác nhau cần phải tư duy rộng. Các hệ thống này sử dụng những thành phần như sau: bệnh nhân, hoạt động và nguồn tài nguyên.

Từ quan điểm sử dụng, các nguồn tài nguyên được phân thành nguồn tài nguyên chủ động và thụ động. Tài nguyên chủ động là cần thiết để thực hiện các hoạt động liên quan tới việc chăm sóc y tế. Các tác nhân là những trùm tượng liên quan tới sử dụng trực tiếp hay gián tiếp các hệ thống thông tin chăm sóc y tế. Một tác nhân có thể là một người, một nhóm người hoặc một tổ chức: bác sĩ lâm sàng, y tá, quản lý, v.v. Tài nguyên thụ động hay tiêu thụ bao gồm trang thiết bị y tế liên quan đến một vị trí mà lập danh mục cần thiết hay các tài liệu được sử dụng trong quá trình chăm sóc y tế: thuốc, thiết bị dùng một lần v.v. Việc sử dụng từng tài nguyên có giá cụ thể, phụ thuộc vào tài nguyên liên quan và hình thức hoạt động thực hiện.

3.4. Thành phần hồ sơ y tế

Thành phần này cung cấp các công cụ để lưu trữ dữ liệu bệnh nhân được sinh ra trong khi thực hiện các hoạt động y tế, chẳng hạn như dữ liệu quan sát (kiểm tra vật lý, kết quả xét nghiệm) hay dữ liệu điều trị (quản lý thuốc, thực hiện phẫu thuật, kế hoạch hoạt động). Bên cạnh việc lưu trữ, nó cũng cho phép hiển thị dữ liệu bệnh nhân lên màn hình như thông tin được tóm tắt như thế nào (được ghi lại bởi các nhân viên khác nhau), khi nào (bối cảnh khác nhau) hay dữ liệu nhập vào từ đâu. Nguồn thông tin có thể tồn tại trong những hệ thống riêng biệt.

Ví dụ, dấu hiệu sự sống của bệnh nhân được ghi nhận trong ba lần khác nhau (do một bác sĩ khám ngoại trú, nhân viên quản lý hành chính, một y tá bố trí chăm sóc bệnh nhân) với ba hình thức khác nhau. Hồ sơ chăm sóc y tế điện tử (EHCR) hay EHR có khả năng định vị dữ liệu bệnh nhân nắm bắt được trong những môi trường khác nhau và tích hợp vào một khung nhìn duy nhất.

3.5. Thành phần xác thực

Là sự tương tác giữa người dùng với hệ thống. Nó thiết lập các quyền truy cập của người dùng cá nhân theo quy phạm pháp luật, yêu cầu y tế và tổ chức. Các chính sách an ninh và xác thực là rất quan trọng trong lĩnh vực chăm sóc y tế. Quyền truy cập tới dữ liệu và các chức năng được kiểm tra ở lần đăng nhập từ thành phần xác thực nó lưu trữ thông tin về người dùng, nhóm người dùng, những chức năng truy cập trong phù hợp với vai trò người dùng, hồ sơ bệnh nhân (ví dụ nhân viên, quản lý) và các hoạt động y tế liên tục.

Thành phần xác thực chứa hồ sơ từng loại tác nhân trong hệ thống thông tin có thẩm quyền để thực hiện những hoạt động khác và có quyền truy cập đến các kiểu thông tin khác nhau. Các tác nhân là những người tham gia vào quá trình chăm sóc y tế, các thành phần của tổ chức (dịch vụ y tế), phần mềm hay thiết bị. Những hồ sơ được xác định theo các tiêu chí của bệnh viện, phụ thuộc vào những qui định quốc gia và khu vực và dựa vào qui định nội bộ và các đặc điểm hoạt động cá nhân và dữ liệu.

3.6. Thành phần quản lý tri thức

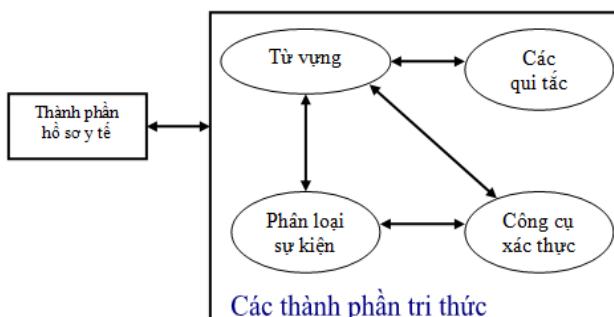
Tri thức có thể được tìm thấy trong nhiều định dạng và vị trí khác nhau, chẳng hạn như các tài liệu giấy hay điện tử, nhưng chỉ một phần nhỏ là có cấu trúc trong các cơ sở tri thức máy tính. Thành phần quản lý tri thức đóng vai trò chính trong hệ thống thông tin lâm sàng. Đầu tiên nó đảm bảo tính chắc chắn các mức độ chuẩn được đáp ứng phù hợp với ứng dụng các đặc trưng huấn luyện thông minh trên các hệ thống có sẵn (ví dụ POE). Mặc khác, nó cho

phép các ứng dụng từ nhiều hệ thống vê tinh cùng tồn tại bằng cách ánh xạ các thuật ngữ hay các mã được sử dụng trong các ứng dụng khác nhau đến một đại diện phổ biến trước khi chuyển đến hồ sơ bệnh nhân.

Thành phần tri thức gồm một số thành phần con như: thành phần thuật ngữ, các nguồn tri thức và các động cơ suy luận. Thành phần thuật ngữ quản lý, xử lý các loại khái niệm y tế khác nhau có thể được cấu trúc trong một mạng ngữ nghĩa của các thuật ngữ hình thành nên ontology. Thành phần này là yếu tố cần thiết để xây dựng các hệ thống EHR linh hoạt và phát triển cũng như bảo đảm sự tích hợp ngữ nghĩa của các thành phần khác nhau. Nguồn tri thức bao các khung, các qui tắc và các mô đun lôgic phức tạp. Các động cơ suy luận áp dụng tri thức đến sự kiện có cấu trúc để tạo ra thông tin hay tri thức mới.

Hầu hết các thành phần có mối quan hệ chặt chẽ với thành phần tri thức tạo thành nền tảng cơ bản cho những hệ thống hỗ trợ quyết định y tế và kiểm tra tính phù hợp của các hoạt động.

Hình 3 minh họa sự tương tác giữa hồ sơ y tế và những thành phần tri thức. Khi xây dựng một EHR nhu cầu truy xuất đến hệ thống từ vựng các khái niệm và các liên kết ngữ nghĩa của chúng, phân loại các sự kiện, cơ sở qui tắc công việc và thành phần xác thực. Thành phần xác thực sinh ra lớp trình bày (có quyền truy cập tới từ vựng và các qui tắc) và cho phép tạo ra nội dung để nhập vào EHR.

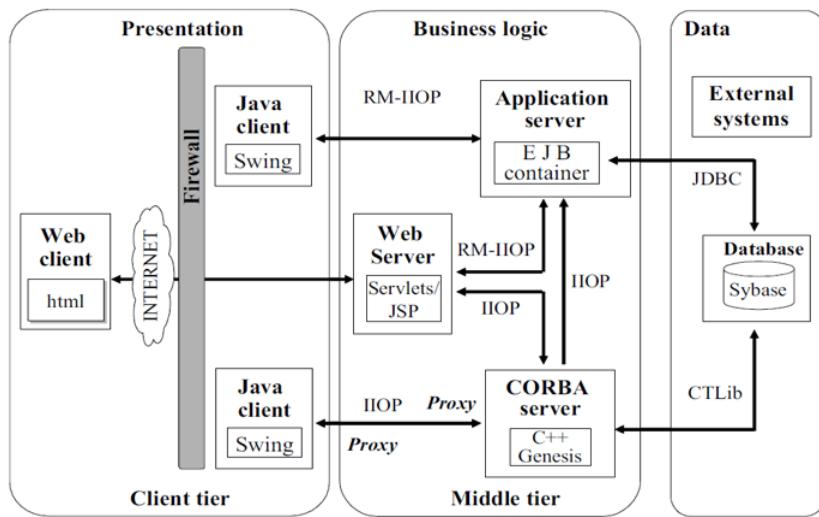


Hình 3. Thành phần hồ sơ y tế truy cập các thành phần tri thức

Khi một sự kiện y tế (hành vi, kiểm tra sức khoẻ, lịch sử) được tạo ra, hệ thống tìm kiếm khái niệm tương ứng trong từ vựng. Thông qua kỹ thuật ánh xạ, tất cả các mục từ vựng đã liên kết đến khái niệm gốc được ánh xạ tự động hình thành một mẫu và trình bày cho người sử dụng. Thành phần hồ sơ y tế xác nhận và kiểm tra dữ liệu vào với các qui tắc được định nghĩa.

4. KỸ THUẬT CÔNG NGHIỆP TRIỂN KHAI

Bắt đầu những năm 1970, các ứng dụng phức tạp phát triển chủ yếu dựa trên máy tính lớn. Giữa thập niên 1990s, kiến trúc hai tầng khách chủ (Client-Server) được viết bằng C++ chạy trên các máy khách Windows NT và máy chủ Sun Solaris thay thế cho máy tính lớn. Vào năm 1998, kiến trúc ba tầng thay thế cho kiến trúc khách chủ để cải thiện khả năng kết nối và chia sẻ dữ liệu. Các ứng dụng dựa trên kiến trúc đa tầng được phát triển theo một khung chung gọi là GENESIS sử dụng ngôn ngữ lập trình C++. Ở phía máy khách thì sử dụng công nghệ Java dựa trên các lớp Swing. Từ năm 2001, các ứng dụng được phát triển dựa trên kiến trúc J2EE đã tạo ra một cơ sở hạ tầng có khả năng mở rộng và linh hoạt cao (xem hình 4).



Hình 4. Một khung cho phần mềm thành phần.

4.1. Tầng nghiệp vụ

Tầng lôgic nghiệp vụ của bệnh viện được hiện thực trong các thành phần hệ thống thông tin. Tầng lôgic nghiệp vụ là phần trung gian được thực hiện như các thành phần EJB (Enterprise Java Beans) (chuẩn J2EE sử dụng Web logic như máy chủ ứng dụng), hoặc như các đối tượng CORBA (trong khung chung GENESIS) sử dụng ngôn ngữ mô tả giao diện (IDL – Interface Definition Language) của OMG (Object Management Group).

4.2. Khung GENESIS

GENESIS là một khung viết bằng C++ được thêm vào lớp nghiệp vụ (business layer) của phần mềm ứng dụng phức tạp. Mục đích là cung cấp chức năng cơ bản với chi phí thấp. GENESIS chứa một số thành phần cho phép người phát triển hiện thực các lớp nghiệp vụ và các mối quan hệ nghiệp vụ. Khung GENESIS phục vụ như một động cơ bền bỉ được xây dựng bên trong, cho phép các đối tượng không chỉ được lưu trữ trong các tập tin thông thường mà còn trong các hệ thống cơ sở dữ liệu quan hệ.

4.3. Nền tảng J2EE

Kiến trúc mới đề xuất cho hoạt động bệnh nhân và các thành phần quản lý nguồn tài nguyên là dựa trên nền tảng Java 2 (phiên bản J2EE) và máy chủ ứng dụng được xây dựng với cơ sở dữ liệu là Sybase 12.0. IIOP (Internet Inter-ORB Protocol) cung cấp khả năng tương tác giữa J2EE và các đối tượng CORBA được hiện thực trong C++.

XML được sử dụng để trao đổi dữ liệu giữa các hệ thống trung chuyển vè tinh khác nhau, để lưu trữ dữ liệu trên máy chủ y tế, và gửi lại thông tin phù hợp với hình thức của đối tượng Java hoặc các tài liệu XML.

4.4. Tầng dữ liệu lôgic

Là một lớp riêng (DAO – Data Access Object) được sử dụng để truy cập các cơ sở dữ liệu và các hệ thống khác.

4.5. Tầng máy khách

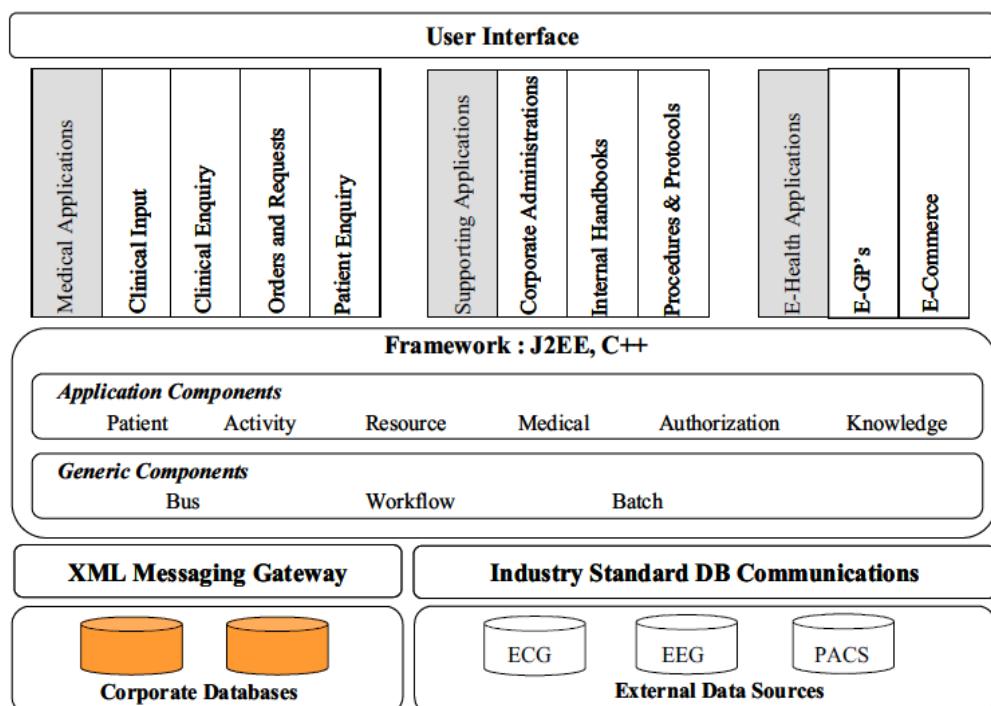
Hệ thống liên kết thông qua hai kiểu máy khách:

- Các máy khách sử dụng Java Swing hoàn toàn cung cấp tính tương tác cao và thời gian đáp ứng yêu cầu người dùng nhanh đối với các ứng dụng tương tác lớn. Kiểu máy khách này có thể tải xuống, cài đặt, cập nhật tự động thông qua sử dụng Java Web Start.
- Các máy khách HTML (đối với GPs (Global Positioning System) yêu cầu truy cập từ xa tới hệ thống lâm sàng) cung cấp một tập chức năng máy trạm lâm sàng thông qua một trình duyệt Web.

Tầng máy chủ Web được sử dụng để phục vụ cho ứng dụng dựa trên Web và chạy các trang Servlets/JavaServer cung cấp sự tương tác động trên máy khách Web. Một trình duyệt Web tạo ra yêu cầu gửi đến máy chủ Web qua HTTPS và đảm bảo tất cả giao tiếp thông qua SSL.

5. NGHIÊN CỨU TÌNH HUỐNG

Trong phần này trình bày một hệ thống thông tin lâm sàng AZ-VUB. Tất cả các ứng dụng được tích hợp hợp lý sáu thành phần cơ bản (xem hình 5)



Hình 5. Kiến trúc thành phần AZ-VUB

5.1. Thành phần xác thực (Authorization)

Sự tương tác giữa người sử dụng và hệ thống thông tin lâm sàng được kiểm soát bởi thành phần xác thực. Thành phần này cung cấp một môi trường thống nhất cho khai báo, định nghĩa và các quyền truy cập của những người dùng cá nhân tùy theo các yêu cầu về pháp lý, y tế và tổ chức. Nó đảm bảo cho mỗi hồ sơ người dùng: tính bảo mật dữ liệu và truy cập đến một số dịch vụ yêu cầu của người dùng dựa trên một số qui định bên trong của tổ chức.

5.2. Thành phần bệnh nhân (Patient)

Thành phần bệnh nhân được cung cấp như sau:

- Một kho hợp nhất để lưu trữ định danh bệnh nhân (nhận dạng bệnh nhân thường xuyên, nhận diện tạm thời, nhận diện bệnh viện, nhận diện trường hợp/tiếp xúc), nhân khẩu học bệnh nhân và vị trí bệnh nhân.
- Một số chức năng để quản lý thông tin.
- Các phương tiện để truy cập hồ sơ bệnh nhân.

5.3. Thành phần hoạt động (Activity)

Thành phần hoạt động trình bày phương tiện liên lạc giữa bên yêu cầu và bên thực hiện bằng việc quản lý các hoạt động liên quan tới một bệnh nhân. Nó bao gồm lập hóa đơn điện tử (cấp thuốc, các thủ tục chẩn đoán, ...), lập kế hoạch và thực hiện các hoạt động và cuối cùng là thanh toán. Nó được liên kết với hệ thống hỗ trợ quyết định lâm sàng cung cấp các dịch vụ thông minh như:

- Ở cấp độ hành chính, một hệ thống thanh toán dựa trên tri thức;
- Ở cấp độ hoạt động, tối ưu hóa việc lập danh mục nguồn tài nguyên và quản lý xung đột;
- Ở cấp độ y tế, sự hỗ trợ thời gian thực bằng cách cung cấp các nhắc nhở và cảnh báo dựa trên nguyên tắc cơ bản.

5.4. Thành phần hồ sơ y tế (Medical)

Hồ sơ y tế: Dữ liệu được thu thập từ các hệ thống cung cấp từ các bộ phận khác nhau chẳng hạn như: ECG, EEG, v.v. Hồ sơ y tế điện tử không phải là duy nhất, máy chủ y tế cung cấp các công cụ phân nhóm và trình bày dữ liệu y tế, tổng hợp (nhóm lại) trong các cấu trúc khác nhau theo nhu cầu người dùng. Một phần của máy chủ y tế được truy cập cũng cung cấp thư mục và các hệ thống tri thức y tế khác như PubMed.

Tài liệu y tế: Tại AZ-VUB gồm những tài liệu có cấu trúc hoặc bán cấu trúc được lưu trữ trong cơ sở dữ liệu quan hệ và trong định dạng XML. Các báo cáo tường thuật được lưu trữ trong định dạng HTML. XML có lợi thế lưu trữ dữ liệu phức tạp theo cấu trúc đơn giản. Mỗi tài liệu gồm một số phần được định nghĩa trước theo thứ tự cụ thể. Nội dung của một số phần có thể được cài đặt sẵn (ví dụ, các kết quả phòng thí nghiệm, báo cáo x-quang).

5.5. Thành phần quản lý tri thức (Knowledge)

Tùy thuộc vào lĩnh vực, cơ sở tri thức hoặc cơ sở dữ liệu khác nhau được tạo ra: qui định thanh toán, tổ chức (nghĩa là kế hoạch hoạt động và giải quyết xung đột) và y tế. Cơ sở dữ liệu thuật ngữ, cơ sở dữ liệu thuốc và cơ sở dữ liệu hoạt động cũng biểu diễn như các thành phần gồm các chức năng dịch vụ cao cấp.

Một công cụ ra quyết định duy trì các qui tắc công việc của môi trường y tế thì được hiện thực và sử dụng trong hai lĩnh vực riêng biệt nhưng có liên quan nhau. Về mặt y tế, những nỗ lực nhằm tạo ra sử dụng hệ thống chuyên gia để phát hiện ra những hiệu quả, hậu quả của thuốc (ADEs) và các nhiễm trùng bệnh viện ở những bệnh nhân nội trú và báo cáo trong hồ sơ y tế điện tử. Lĩnh vực áp dụng thứ hai của tri thức liên quan đến thủ tục thanh toán. Thủ tục thanh toán thì dựa trên hệ thống pháp lý và liên tục được sửa đổi theo những thay đổi pháp lý.

Những quy định pháp lý được hiện thực và như vậy làm cho các quy tắc thanh toán phù hợp, sử dụng cơ chế suy luận trước và sau.

Để đáp ứng sự đa dạng của người dùng y tế, việc tạo ra và duy trì sự mở rộng vốn từ vựng cho các lớp ngữ nghĩa có thể được bổ sung dần dần trong giai đoạn đầu phát triển giải pháp dựa trên thành phần [1, 6]. Mặc dù chọn sử dụng ICD-99CM như cơ sở của máy chủ từ vựng đã mở rộng phân loại để tích hợp thuật ngữ nội bộ hay dùng. Những chức năng cụ thể được phát triển để giúp người sử dụng trong việc giới thiệu các khái niệm y tế mới và liên kết lại với nhau khi cần thiết với các phần thích hợp.

5.6. Thành phần nguồn tài nguyên (Resource)

Thành phần nguồn tài nguyên cung cấp thông tin để hỗ trợ các hoạt động quản lý cho các mục đích về tài chính, tổ chức và y tế. Tài nguyên là một cái gì đó mà một tổ chức cần đạt được mục tiêu của nó. Tài nguyên có thể là hữu hình hay vô hình. Những tài nguyên hữu hình là các bộ phận y tế, khu vực, phòng, tòa nhà, nhân sự, thiết bị và hàng tiêu dùng. Những tài nguyên vô hình được liên kết với trước đây và có thể là các dịch vụ được cung cấp.

6. KẾT LUẬN

Các phương pháp phát triển phần mềm trước, trọng tâm là tích hợp dữ liệu, làm tăng các kho dữ liệu. Ngày nay, trọng tâm là tích hợp ứng dụng, dữ liệu được phân tán và động, yêu cầu phần mềm không chỉ đáp ứng yêu cầu của người dùng mà còn tiên liệu người dùng y tế trong tình trạng quá tải thông tin.

Thành phần khung chung được xây dựng dựa trên nền tảng công nghệ - khái niệm cơ bản mạnh mẽ và cởi mở là những tiêu chuẩn tin học y tế ngày nay.

Các công nghệ CORBA, DCOM và N-tier đã trở thành xu thế chủ đạo. Những máy chủ đặt ở tầng giữa áp dụng mô hình lâm sàng và các qui tắc ứng dụng để giao tiếp với các trạm làm việc thin-client. Kiến trúc đã thỏa mãn hai đòi hỏi đối lập nhau: yêu cầu của người dùng đối với quyền tự chủ dữ liệu và các chức năng càng gần càng tốt tới dịch vụ y tế và quản lý chính xác dữ liệu [17]. Cách tiếp cận N-tier, được so với những môi trường phát triển ngôn ngữ thế hệ thứ ba và tư, cung cấp một cách phong phú hơn, khả năng mở rộng hơn, và ứng dụng khả thi hơn trong dài hạn nhưng chi phí tái đầu tư thấp hơn.

Những người dùng ở bệnh viện có gắng nhận được nhiều nhất từ hệ thống thông tin. Mục tiêu cuối cùng của sự phát triển một kiến trúc tham chiếu được tích hợp cho một hệ thống thông tin lâm sàng phải được cung cấp một môi trường chuyển đổi dữ liệu thành thông tin có ích bất kể vị trí và các đặc điểm của những nguồn thông tin được kết nối. Bảo vệ những hệ thống tài sản hiện có trong khi tích hợp các ứng dụng mới, vạch ra chiến lược tương lai trong khi sự thay đổi là hằng số và không thể đoán trước về mặt kỹ thuật, và chọn lựa nhà cung cấp ngay khi xuất hiện thách thức mới. Hy vọng rằng, những bệnh nhân sẽ trải nghiệm các lợi ích của những tiến bộ kỹ thuật này [13].

TÀI LIỆU THAM KHẢO

1. Benesch C, Witter DM Jr, Wilder AL, Duncan PW, Samsa GP, Matchar DB. Inaccuracy of the International Classification of Diseases (ICD-9-CM) in identifying the diagnosis of ischemic cerebrovascular disease, *Neurology*, 1997; 49(3): 660–664.
2. Booch G. Object-Oriented Analysis and Design with Applications, 2nd ed. Redwood City, Calif.: Benjamin/Cummings, 1994.
3. Booch G, Rumbaugh J, Jacobson I. The Unified Modeling Language User Guide. Reading, Massachusetts: Addison-Wesley, 1999.
4. Brown AW. Large-Scale Component-Based Development. Upper Saddle River, N.J.: Prentice Hall, 2000.
5. CEN/TC251. PrENV 12967-1. Healthcare Information System Architecture Part 1 (HISA)—Healthcare Middleware Layer. March 1997.
6. Chute CG, Cohn SP, Campbell KE, Oliver DE, Campbell JR. The content coverage of clinical classifications. *JAMIA*, 1996; 3: 224–230.
7. Cummins FA. Enterprise Integration—An Architecture for Enterprise Application and Systems Integration. New York: John Wiley & Sons, 2002.
8. Graham I. Migrating to Object Technology. Reading, Massachusetts: Addison-Wesley, 1995.
9. Hammond WE. The role of standards in creating a health information infrastructure. *Int J Biomed Comput*. 1994; 34: 29–44.
10. Herzum P, Sims O. Business Component Factory—A Comprehensive Overview of Component-Based Development for the Enterprise. New York: John Wiley & Sons, 2000.
11. Jacobson I. Object-Oriented Software Engineering: A Use Case Driven Approach. Wokingham, England: Addison-Wesley, 1992.
12. Leisch E, Sartzetakis S, Tsiknakis M, Orphanoudakis SC. A framework for the integration of distributed autonomous healthcare information systems. *J Med Informatics*. 1997; 22(4): 325–335.
13. Orphanoudakis SC, Kaldoudi E, Tsiknakis M. Technological advances in teleradiology. *Eur J Radiol*. 1996; 22(3): 205–217.
14. Rumbaugh J, Blaha M, Premerlani W, Eddy F, Lorenzen W. Object-Oriented Modeling and Design. Upper Saddle River, NJ: Prentice Hall, 1991.
15. Tsiknakis M, Chronaki CE, Kapidakis S, Nikolaou C, Orphanoudakis SC. An integrated architecture for the provision of health telematic services based on digital library technologies. *Int J Digit Libr*. 1997 (3): 257–77.
16. Usoft. Automation: A Proven Approach and Software Technology to Implement Computing Applications. White paper 1998.
17. Van de Velde R. Hospital Information Systems—The next generation. Heidelberg: Springer-Verlag, 1992.

ABSTRACT

HEALTH INFORMATION SYSTEM A COMPONENT-BASED ACCESS

Huynh Huu Nghia¹, Nguyen Thi Thu Tam^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: tamntt@hufi.edu.vn

In this paper, a component-based approach to health information systems is introduced. With this approach, the system will be flexible, easy to upgrade, repair and maintain. Moreover, the system will not be completely dependent on one technology solution provider, but can choose from many different vendors that provide the best software packages for each component. With today's techniques and technologies, it is possible to easily deploy a component-based health information system.

Keywords: Medical information system, Information system, Medical software.

TỐI UU HÓA TÌM KIẾM CHIM HỒNG HẠC VÀ ỨNG DỤNG TRONG BÀI TOÁN ẨN TẬP PHỔ BIẾN

Lê Huỳnh Đức¹, Nguyễn Thị Hằng¹, Đinh Nguyễn Trọng Nghĩa^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: nghiadnt@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo giới thiệu thuật toán tối ưu hóa bầy đàn thông minh, tên là "Tìm kiếm chim hồng hạc" (FSA), dựa trên hành vi di cư và tìm kiếm thức ăn của chim hồng hạc. Thuật toán này có khả năng tìm kiếm giải pháp tối ưu cho các bài toán tối ưu hóa nhanh chóng và hiệu quả. FSA sử dụng các thông số như số lần lặp tối đa, quy mô quần thể chim hồng hạc, giới hạn khoảng tìm kiếm, số lượng đàn chim hồng hạc di cư và kiếm ăn. Bài báo cũng đề xuất áp dụng FSA vào bài toán ẩn tập phổ biến, giúp tìm giải pháp tối ưu và giảm thiểu rủi ro liên quan đến cạnh tranh giữa các cá thể. Thuật toán FSA phân bố các cá thể đều trên không gian tìm kiếm và di chuyển đến các vị trí có nhiều thông tin hữu ích, giúp tìm kiếm giải pháp tốt nhất.

Từ khóa: Flamingo Search Algorithm, FSA, PPDM, hiding frequent itemset

1. GIỚI THIỆU

Flamingo Search Algorithm (FSA) là một thuật toán tối ưu hóa được lấy cảm hứng từ hiện tượng chim hồng hạc di cư. Ý tưởng của thuật toán là mô phỏng lại cách mà các con chim hồng hạc tìm kiếm lấy nguồn thức ăn trên mặt nước. Các con chim hồng hạc này sử dụng mỏ của mình để đào xuống đáy nước và tìm kiếm thức ăn. Thuật toán FSA sử dụng quy trình tìm kiếm ngẫu nhiên, kết hợp với quy trình cập nhật vị trí của các cá thể để tìm kiếm các giá trị tối ưu. Flamingo Search Algorithm thực hiện tìm kiếm trong không gian bài toán bằng cách sử dụng việc di chuyển ngẫu nhiên trong không gian tìm kiếm. Thuật toán sử dụng một bộ các con số ngẫu nhiên để điều khiển việc di chuyển của các hồng hạc trong quá trình tìm kiếm. Mỗi lần di chuyển, vị trí của các hồng hạc được cập nhật dựa trên một công thức tính toán giữa vị trí hiện tại và các con số ngẫu nhiên. Quá trình này được lặp lại cho đến khi đạt được kết quả tìm kiếm mong muốn hoặc đạt đến điều kiện dừng được thiết lập trước đó. Thuật toán tối ưu hóa ngẫu nhiên có ưu điểm là: dễ triển khai, dễ thích nghi và có tốc độ ổn định, độ bền và khả năng mở rộng, ít giám sát hơn [1].

So với các thuật toán khác thì thuật toán tối ưu hóa ngẫu nhiên có tính năng cao hơn. Một loại thuật toán tối ưu hóa ngẫu nhiên điển hình là thuật toán trí thông minh bầy đàn tìm ra đường dẫn hội tụ và giải pháp tối ưu một cách độc đáo. Các thuật toán tối ưu hóa trí thông minh bầy đàn sử dụng ít tài nguyên, có khả năng tìm kiếm toàn cục, dễ dàng triển khai, có khả năng tìm kiếm đa nhiệm. Trong những năm gần đây, nhiều thuật toán tối ưu hóa trí thông minh bầy đàn mới đã được đề xuất, chẳng hạn như Whale Optimization Algorithm (WOA) [2], Tunicate Swarm Algorithm (TSA) [3], Sparrow Search Algorithm (SSA) [4], Particle Swarm Optimization (PSO). Các thuật toán này cung cấp cho kết quả tìm kiếm nhanh nhưng cũng còn hạn chế.

Bên cạnh đó tất cả thuật toán vừa nêu trên đều có ưu điểm chung là khả năng tìm kiếm tối ưu toàn cục, tốc độ tìm kiếm nhanh, khả năng tìm kiếm đa nhiệm, dễ triển khai. Chúng được sử dụng rộng rãi trong việc giải quyết các vấn đề tối ưu hóa hàm mục tiêu, tối ưu hóa mô hình máy học, tối ưu hóa các thiết kế kỹ thuật, tối ưu hóa các quyết định kinh doanh và tài chính, tối ưu hóa quy trình sản xuất, v.v...

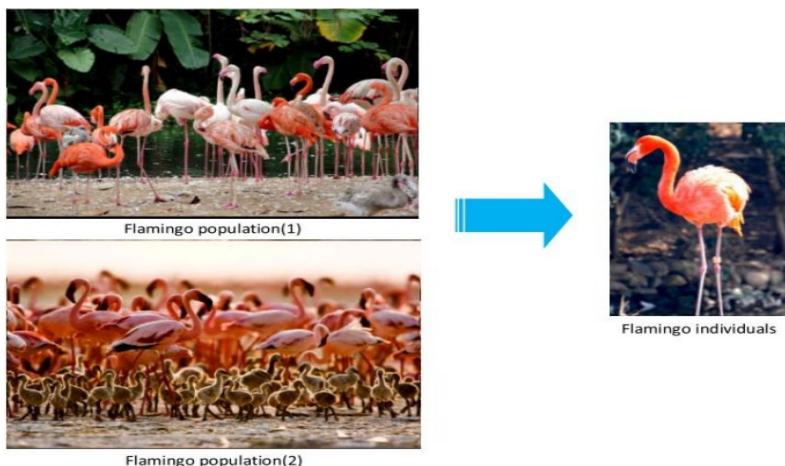
Thuật toán WOA lấy cảm hứng từ hành vi săn mồi của cá voi, TSA lấy cảm hứng từ cách di chuyển của loài động vật biển lục tunicate, thuật toán SSA lấy cảm hứng từ việc tìm kiếm thức ăn của chim sẻ, PSO lấy cảm hứng từ cách đàn chim tìm kiếm thức ăn trong tự nhiên. Do sự phát triển của công nghệ kỹ thuật và các vấn đề kỹ thuật ngày càng phức tạp dẫn đến mong muốn mở rộng tính đa dạng của thuật toán trí thông minh bầy đàn và cải thiện hiệu suất. Để hiệu suất thuật toán ngày càng tối ưu thì phải tăng khả năng khám phá, phát triển không gian tìm kiếm. Nghĩa là, hiệu suất của thuật toán có thể giảm sau khi giải các bài toán khác có tính chất khác.

Bài báo cáo này trình bày lại thuật toán tối ưu Flamingo và ý tưởng áp dụng thuật toán vào bài toán khai thác dữ liệu đảm bảo tính riêng tư, cụ thể hơn là bài toán ẩn các tập phô biến.

2. THUẬT TOÁN TÌM KIẾM CHIM HỒNG HẠC

2.1 Đặc điểm của thuật toán

Chim hồng hạc là loài chim di cư sống theo bầy đàn, thức ăn chủ yếu là tảo, tôm nhỏ, nghêu, giun nhỏ và ấu trùng côn trùng. Chim hồng hạc cũng kiếm ăn theo một cách đặc biệt, bằng cách cúi chiếc cổ dài xuống và quay đầu lại, sau đó đi bộ. Trong khi quét chiếc mỏ cong của chúng quanh cơ thể và chạm vào đáy nước để kiếm ăn [5]. Các quần thể và cá thể chim hồng hạc trong tự nhiên được thể hiện trong Hình 1.



Hình 1. Quần thể và cá thể chim hồng hạc trong tự nhiên

Hai đặc điểm tập tính chính của chim hồng hạc là tập tính kiếm ăn và di cư. Quần thể chim hồng hạc chủ yếu sinh sống ở những khu vực có nhiều thức ăn. Sau một thời gian kiếm ăn rộng rãi, quần thể chim hồng hạc di cư khi thức ăn trong khu vực bị giảm đến mức không

thể đáp ứng quần thể. Bài báo này thiết lập mô hình tìm kiếm thức ăn và mô hình di cư tương ứng.

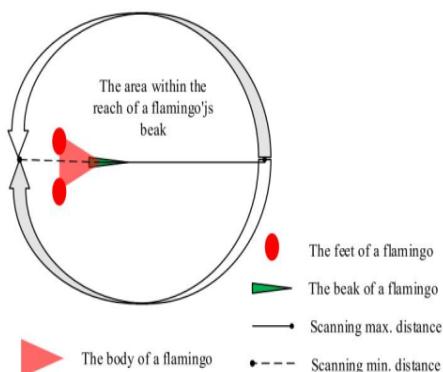
Các ý tưởng tối ưu hóa chính của mô hình FSA được trình bày như sau:

Chim hồng hạc hát cho nhau nghe để thông báo vị trí của chúng và thức ăn tại địa điểm. Quần thể chim hồng hạc không biết nơi nào có nhiều thức ăn nhất trong khu vực tìm kiếm hiện tại. Thay vào đó, chúng cập nhật qua tiếng hát của đồng loại xung quanh. Hành vi này của hồng hạc phù hợp với ý tưởng tối ưu hóa trí thông minh bầy đàn. Và chúng ta không biết không gian tìm kiếm là bao nhiêu, tác nhân tìm kiếm là chim hồng hạc, hồng hạc khám phá ra không gian tìm kiếm và trao đổi thông tin với nhau và cố định vị trí tìm thấy đó. Từ đó rút ra được giải pháp tối ưu. Quy tắc thay đổi vị trí dựa trên hành vi của chim hồng hạc. Hành vi chính của nó chủ yếu có hai loại: hành vi kiếm ăn và hành vi di cư. Hành vi kiếm ăn có thể được chia thành hai đặc điểm hành vi: Quét mỏ và di chuyển chân

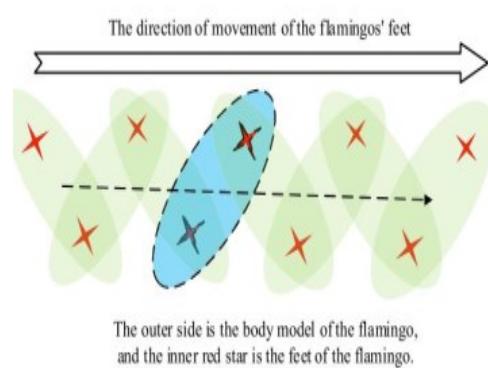
2.2 Ý tưởng và mô hình toán học của thuật toán

Tìm hiểu hành vi: Hành vi giao tiếp khi con hạc phát hiện chỗ có thức ăn nó sẽ gọi những con hạc khác đến vị trí đó. Chỗ tụ tập nhiều nhất là chỗ có nhiều thức ăn nhất. Theo lý thuyết những con hạc này không biết chỗ nào có nhiều thức ăn. Nhưng trong thuật toán chúng ta có thể biết vì ta có thể thiết lập điều kiện kết thúc chương trình.

FSA là một thuật toán mô phỏng chim hồng hạc có gắng tìm giải pháp tối ưu trong khu vực tìm kiếm (tức là vị trí có nhiều thức ăn nhất) dựa trên nguồn thông tin hạn chế có sẵn.



Hình 2. Hành vi quét mỏ



Hình 3. Hành vi di chuyển hai chân

Mỏ của chim hồng hạc khi úp ngược trong nước có chức năng tương tự như một cái sàng lớn, giúp hút nước và lọc thức ăn nhanh chóng nhờ vào các rãnh sâu ở mỏ dưới và các rãnh nông, có nắp ở mỏ trên. Khi chim hồng hạc đang kiếm ăn, chúng cúi đầu, lộn miếng ngược và ăn thức ăn vào miệng, sau đó thải ra nước thừa và cặn bã không ăn được. Cách kiếm ăn này phụ thuộc vào sự dồi dào thức ăn trong khu vực. Khi mỏ của chim hồng hạc quét qua một khu vực có nhiều thức ăn hơn, chúng sẽ quét khu vực đó một cách cẩn thận hơn và cố của chim sẽ dần duỗi ra, làm tăng bán kính quét của mỏ. Xác suất quét khu vực để tìm thức ăn cũng sẽ tăng lên. Mô hình hành vi quét mỏ của chim hồng hạc được mô tả trong Hình 2.

Khi có nhiều con chim hồng hạc trong quần thể đồng thời hội tụ tại một vị trí, khả năng có nhiều thức ăn ở khu vực đó càng cao. Bài báo này mô phỏng hành vi quét mỏ của chim hồng hạc trong không gian đa chiều của quần thể được ký hiệu là x_{ij} , và mô hình tính đến sự

thay đổi trong lựa chọn của từng cá thể chim hồng hạc trong tự nhiên cũng như tác động của sự biến động đột ngột của môi trường đến hành vi kiếm ăn của chúng. Hành vi tìm kiếm thức ăn của từng con chim hồng hạc sẽ có sai số khi truyền thông tin. Để mô phỏng sai số này, ta sử dụng một phân phối ngẫu nhiên theo phân phối chuẩn, trong đó việc quét mỏ của chim hồng hạc có xác suất cao hướng về vị trí có nhiều thức ăn nhất. Tuy nhiên, cũng có một xác suất nhỏ cho sai sót dựa trên thông tin này.

Tiếp theo, Để có thể đo lường khoảng cách tối đa mà mỏ chim hồng hạc quét qua trong quá trình tìm kiếm thức ăn được biểu diễn bằng công thức: $|G_1 \times x_{ij} + \varepsilon_2 \times x_{ij}|$ trong đó ε_2 là một số ngẫu nhiên có giá trị -1 hoặc 1. Mục đích chính của khoảng cách tối đa này là mở rộng phạm vi tìm kiếm của mỏ chim hồng hạc trong quá trình tìm thức ăn. Trong đó, G_1 là một số ngẫu nhiên tuân theo phân phối chuẩn thông thường trong khoảng $N(0,1)$. Để mô phỏng phạm vi quét mỏ của chim hồng hạc trong hành vi tìm kiếm có thể được nói là quét mỏ lần hai, và cũng giống công thức quét mỏ lần một thì lại thêm G_2 được biểu diễn bằng công thức: $G_2 \times |G_1 \times xb_j + \varepsilon_2 \times x_{ij}|$ trong đó G_2 là một số ngẫu nhiên tuân theo phân phối chuẩn thông thường trong khoảng $N(0,1)$.

Mô hình hành vi di chuyển bằng hai chân của hồng hạc được thể hiện trong Hình 3. Khi hồng hạc kiếm thức ăn, trong lúc quét bằng mỏ, móng vuốt của chúng sẽ di chuyển về phía nơi có nhiều thức ăn nhất. Nói một cách dễ hiểu là chúng vừa di chuyển vừa quét mỏ. Giả sử vị trí nơi thức ăn phong phú nhất trong quần thể là xb_j , khoảng cách đã đi được đo bằng " $\varepsilon_1 \times xb_j$ ", trong đó " ε_1 " là một số ngẫu nhiên -1 hoặc 1, chủ yếu là để tăng phạm vi tìm kiếm của hồng hạc và định lượng sự khác biệt của cá thể trong việc lựa chọn.

Tổng kết lại, bước di chuyển của chim hồng hạc trong quá trình tìm kiếm thức ăn ở vòng lặp thứ t là tổng khoảng quét mỏ chim hồng hạc cộng với khoảng cách di chuyển của hai chân, như được hiển thị trong công thức số (1).

$$b_{ij}^t = \varepsilon_1 \times xb_j^t + G_2 \times |G_1 \times xb_j^t + \varepsilon_2 \times x_{ij}^t| \quad (1)$$

Công thức cập nhật vị trí kiếm ăn của chim hồng hạc được thể hiện như sau:

$$x_{ij}^{t+1} = (x_{ij}^t + \varepsilon_1 \times xb_j^t + G_2 \times |G_1 \times xb_j^t + \varepsilon_2 \times x_{ij}^t|)/K \quad (2)$$

Trong công thức (2), x_{ij}^{t+1} đại diện vị trí của con hồng hạc thứ i trong chiều thứ j của quần thể trong lần lặp thứ $t+1$. x_{ij}^t đại diện vị trí của con hồng hạc thứ i trong chiều thứ j trong lần lặp thứ t của quần thể chim hồng hạc cụ thể là vị trí bàn chân chim hồng hạc xb_j^t : đại diện cho vị trí chiều thứ j của chim hồng hạc có độ thích nghi tốt nhất trong quần thể ở lần di cư. $K = K(n)$: là hệ số khuếch tán, là một số ngẫu nhiên tuân theo phân phối khi bình phương n bậc tự do. Nó được sử dụng để tăng quy mô phạm vi kiếm ăn của chim hồng hạc và để mô phỏng cơ hội lựa chọn cá thể trong tự nhiên, tăng khả năng tìm kiếm toàn cầu của nó $G_1 = G_2 = N(0,1)$ là một số ngẫu nhiên tuân theo phân phối chuẩn thông thường. ε_1 và ε_2 là một số ngẫu nhiên -1 hoặc 1.

Khi thức ăn ít trong khu vực tìm kiếm hiện tại, quần thể hồng hạc di cư đến khu vực tiếp theo có thức ăn phong phú hơn. Giả sử vị trí của khu vực giàu thức ăn trong chiều thứ j là xb_j , công thức cho sự di cư của quần thể hồng hạc như sau:

$$x_{ij}^{t+1} = x_{ij}^t + \omega \times (xb_j^t - x_{ij}^t) \quad (3)$$

Trong công thức (3), x_{ij}^{t+1} đại diện vị trí của con hồng hạc thứ i trong chiều thứ j của quần thể trong lần lặp thứ t+1. x_{ij}^t đại diện vị trí của con hồng hạc thứ i trong chiều thứ j trong lần lặp thứ t của quần thể chim hồng hạc cụ thể là vị trí bàn chân chim hồng hạc xb_j^t : đại diện cho vị trí chiều thứ j của chim hồng hạc có độ thích nghi tốt nhất trong quần thể ở lần di cư. $\omega = N(0, n)$: là một số ngẫu nhiên Gaussian với n bậc tự do, được sử dụng để tăng không gian tìm kiếm trong quá trình di cư của chim hồng hạc và mô phỏng tính ngẫu nhiên của các hành vi riêng lẻ của chim hồng hạc trong quá trình di cư cụ thể.

Mô tả thuật toán tìm kiếm chim hồng hạc bao gồm:

- Di chuyển và quét mỏ trong khu vực tìm kiếm.
 - Di cư lần 1 một số cá thể ở đầu để mở rộng phạm vi tìm kiếm, Xong tiếp tục di cư lần 2 là những cá thể chim hồng hạc còn lại.
 - Cập nhật vị trí của cá thể chim hồng hạc có độ thích nghi tốt nhất so với ban đầu.
- Thuật toán FSA có thể được tinh chỉnh thông qua các tham số như số lượng cá thể, tỷ lệ lai ghép, tỷ lệ đột biến và tỷ lệ hoán đổi để tối ưu hóa quá trình tìm kiếm.

2.3 Quy trình cơ bản của FSA

Bước 1: Khởi tạo quần thể, quần thể được đặt tên là P, số vòng lặp tối đa được đặt tên là IterMax và tỷ lệ chim hồng hạc di cư trong phần đầu tiên được đặt tên là MPb.

Bước 2: Số lượng chim hồng hạc tìm kiếm thức ăn trong vòng lặp thứ i của việc cập nhật quần thể chim hồng hạc là MPr = rand [0,1] × P × (1-MPb). Số lượng chim hồng hạc di cư trong phần đầu tiên của vòng lặp này là MPo = MPb × P. Số lượng chim hồng hạc di cư trong phần thứ hai của vòng lặp này là MPt = P - MPo - MPr. Giá trị thích nghi của các con chim được xác định, và quần thể chim hồng hạc được sắp xếp theo giá trị thích nghi của từng con chim. Các chim hồng hạc MPb có giá trị thích nghi thấp và các chim hồng hạc MPt có giá trị thích nghi cao được coi là chim hồng hạc di cư, trong khi các con khác được coi là chim hồng hạc tìm kiếm thức ăn.

Bước 3: Các con chim hồng hạc di cư được cập nhật theo công thức (3), và các con chim hồng hạc tìm kiếm thức ăn được cập nhật theo công thức (2).

Bước 4: Kiểm tra các con chim hồng hạc nào bị vượt ra ngoài giới hạn (xem mã giả để biết chi tiết).

Bước 5: Nếu đã đạt đến số lượng vòng lặp tối đa, chuyển đến Bước 6; nếu không, chuyển đến Bước 2.

Bước 6: Đưa ra giải pháp tối ưu và giá trị tối ưu.

Lưu ý rằng, trong quá trình thực hiện Bước 2 đến Bước 5, nếu tìm thấy giải pháp tối ưu trước khi đạt đến số lần lặp tối đa, thì thuật toán cũng sẽ dừng lại và chuyển đến Bước 6.

Thuật toán 1: FSA

Input: Hàm mục tiêu fitness ()

Quy mô quần thể chim hồng hạc Pop
 Số lần lặp tối đa MaxIter
 Số chiều của không gian tìm kiếm Dim
 Biên dưới của khoảng tìm kiếm lb
 Biên trên của khoảng tìm kiếm ub
 Sinh số ngẫu nhiên với hai giá trị -1 hoặc 1 rand_1
 Sinh số ngẫu nhiên trong khoảng 0 đến 1 Vs
 Số lượng chim hồng hạc di cư trong đợt đầu tiên PMc
 Số lượng đàn hồng hạc di cư đợt hai PMf
 Số lượng chim hồng hạc kiêm ăn Pmu
 Mảng lưu con có giá trị tốt nhất Xb

Hàng số

Tỷ lệ di cư cơ bản của chim hồng hạc trong giai đoạn đầu tiên MP_b = 0.1

Khởi tạo:

Tạo ra một mảng chứa vị trí của các con hồng hạc(positions).

for each i to Pop do

 for j = 1 dim do

 positions [i, j] = lb + (ub - lb) * rand ()

 end for

end for

// Sắp xếp các con chim hồng hạc theo fitness từ tốt nhất đến xấu nhất

Sort_pop(X,fitness)

// Lấy ra giá trị tốt nhất

GbestPositon = positions [0]

GbestScore = fitness (GbestPositon)

Tối ưu:

For i = 1 to MaxIter do

 Vs = rand ()

 PMf = int((1-Mp_b) * Vs*Pop)

 PMc = MP_b * Pop

 Pmu = Pop - PMc -PMf

 Xb = positions [0]

 For j to PMc do

 For z to dim do

```

A1 = rmgnormal (loc=0, scale=1.2, size=1)
positions [j, z] = positions [j, z] + (Xb[i] – positions [j, i]) * A1
End for
End for
For int (PMc) to int (PMc+PMu) do
    For z to dim do
        // sinh ra một số ngẫu nhiên theo phân phối chi-square (rng.chisquare(df=8, size=1)
        positions[j,i]=(positions[j,i]+rand_1() * Xb[i] + np.random.randn() * (np.random.randn()* np.abs(Xb[i]
        + rand_1() * positions[j, i]))) / (rng.chisquare(df=8, size=1))
    End for
    End for
    For int (PMc+PMu) to Pop do
        For z to dim do
            // A1 là số ngẫu nhiên theo phân phối chuẩn Gaussian
            A1 = rmgnormal (loc=0, scale=1.2, size=1)
            Positions [j, i] = positions [j, i] + (Xb[i] – positions [j, i]) * A1
        End for
        For j = 0 to Pop
            Positions[i] = clip (Positions[i], lb, ub)
        End for
        Sort (Positions, fitness)
        If (fitness (Positions [0]) <= GbestScore)
            GbestScore = fitness (Positions [0])
            GbestPositon = Positions [0]
        End if
    End for
Output: trả về vị trí tốt nhất GbestPositon và độ thích nghi GbestScore

```

Dòng lệnh được đánh dấu là “chiến lược tìm kiếm tối ưu” là thành phần quan trọng nhất của FSA và là hai biểu thức toán học quan trọng nhất trong thuật toán FSA. Trong đó biểu thức (2) là hành vi kiểm ăn và cuối cùng biểu thức (3) là để chỉ hành vi di cư đợt một và đợt hai tuy nhiên cả 2 lần di cư chỉ khác phạm vi trong thuật toán tìm kiếm chim hồng hạc.

$$x_{ij}^{t+1} = (x_{ij}^t + \varepsilon_1 \times xb_j^t + G_2 \times |G_1 \times xb_j^t + \varepsilon_2 \times x_{ij}^t|) / K \quad (2)$$

$$x_{ij}^{t+1} = x_{ij}^t + \omega \times (xb_j^t - x_{ij}^t) \quad (3)$$

3. VÍ DỤ MINH HỌA

Lấy ví dụ hàm tối ưu được định nghĩa bởi

$$f(x, y, z) = \frac{1}{3}x^2 + \frac{1}{2}y^2 + \frac{1}{6}z^2$$

Trong đó x, y, z sẽ nằm trong khoảng [-2, 2].

Bước đầu tiên khởi tạo quần thể chim hòng hạc ngẫu nhiên. Rõ ràng ở đây bài toán có 3 biến x y z theo ví dụ đã cho số lượng chim hòng hạc trong quần thể là 10 con chim. Khởi tạo, tính độ thích nghi và sắp xếp theo độ thích nghi từ nhỏ nhất đến lớn Bảng 1 như sau:

Bảng 1. Tập hợp các hạt điện tử sau bước khởi tạo

Index	x	y	z	fitness
0	0.018317705	-0.954501759	-0.07420584	0.456566401
1	1.576923786	0.710334211	0.46732492	1.117582319
2	1.763710628	0.244216324	1.0800412	1.261127364
3	-1.95104432	-0.151894247	0.42247673	1.310141675
4	1.598244066	-0.496744224	1.76238485	1.492505502
5	1.462621843	1.111646049	1.51871758	1.715383203
6	-0.64193812	-1.832888837	0.86677271	1.942318085
7	1.68261582	-1.555546307	-1.57806746	2.568643639
8	-1.65311346	-1.831141998	0.13338407	2.590433766
9	1.693722415	-1.825758368	-1.21112253	2.867398314

Từ Bảng 1, có thể nhìn rõ và xác định được một cá thể đầu đàn có chỉ số thích nghi tốt nhất sẽ được chọn và tiến hành di cư cho quần thể đột một. Áp dụng thuật toán ta sẽ sinh ra cá thể mới từ lần di cư đột một theo tỉ lệ di cư $0.2 * 10 = 2$ (0.2 là tỉ lệ di cư cho trước của bài toán 10 là số lượng cá thể khởi tạo) Tuy nhiên thuật toán tự động bỏ qua cá thể tốt nhất là con đầu đàn được Bảng 2 như sau:

Bảng 2. Các cá thể sau khi di cư đột một

Index	x	y	z
0	0.01831771	-0.95450176	-0.07420584
1	2.52184203	2.25801274	1.29357125
2	1.76371063	0.24421632	1.08004119
3	-1.95104432	-0.15189425	0.42247673
4	1.59824407	-0.49674422	1.76238485
5	1.46262184	1.11164605	1.51871758
6	-0.64193812	-1.83288884	0.86677271
7	1.68261582	-1.55554631	-1.57806746
8	-1.65311346	-1.831142	0.13338407
9	1.69372242	-1.82575837	-1.21112253

Sau khi di cư đợt đầu tiếp tục cho số lượng chim di chuyển bằng hai chân và quét mỏ kiêm ăn, VS = 0.50273078529049419 (Số ngẫu nhiên theo phân phối chuẩn), di cư đợt đợt 2 PMF = 4, Di cư đợt đầu PMc = 2, (PMc) to int (PMc+PMu) Số lượng chim kiêm ăn là 4 trong phạm vi quần thể từ 2 đến 6 sẽ thu được các vị trí mới được tô đậm dưới bảng và các vị trí các con chim được hiệu chỉnh theo công thức thuật toán thu được kết quả Bảng 3 bên dưới:

Bảng 3. Tập hợp các cá thể kiêm ăn

Index	x	y	z
0	0.01831771	-0.95450176	-0.07420584
1	2.52184203	2.25801274	1.29357125
2	-0.21671154	0.42137008	0.12696972
3	-0.25529128	0.06973586	0.04292713
4	0.07093222	-0.26234487	0.21619166
5	0.10262446	0.00257076	0.12621516
6	-0.64193812	-1.83288884	0.86677271
7	1.68261582	-1.55554631	-1.57806746
8	-1.65311346	-1.831142	0.13338407
9	1.69372242	-1.82575837	-1.21112253

Tiếp theo sau đó cuộc di cư đợt 2 sẽ được diễn ra cho các cá thể còn lại cũng áp dụng thuật toán lại thu được kết quả như Bảng 4 dưới đây:

Bảng 4. Các cá thể di cư đợt hai

Index	x	y	z
0	0.01831771	-0.95450176	-0.07420584
1	2.52184203	2.25801274	1.29357125
2	-0.21671154	0.42137008	0.12696972
3	-0.25529128	0.06973586	0.04292713
4	0.07093222	-0.26234487	0.21619166
5	0.10262446	0.00257076	0.12621516
6	-0.15790724	-1.02718838	0.82213052
7	2.49256880	-1.42660959	-3.98628412
8	0.69234925	-2.15563961	0.64428492
9	2.44357811	-2.91530343	-2.72947764

Quá trình di cư 2 hoàn tất theo sau đó phải kiểm tra lại ranh giới như đã cho ban đầu của bài toán nếu vượt quá biên trên thì phải cho bảng lại biên dưới và ngược lại tương tự (Ví dụ: Ở biến x, index = 9 giá trị là **2.44357811** là đã vượt qua biên trên đã cho trước là 2 ở trên đè thì sẽ bằng -2. Hiểu rõ hơn sự thay đổi này xem những ô được in đậm trong Bảng 5 phía dưới:

Bảng 5. Các cá thể sau khi được kiểm tra ranh giới

Index	x	y	z
0	0.01831771	-0.95450176	-0.07420584
1	-2	-2	1.29357125
2	-0.21671154	0.42137008	0.12696972
3	-0.25529128	0.06973586	0.04292713
4	0.07093222	-0.26234487	0.21619166
5	0.10262446	0.00257076	0.12621516
6	-0.15790724	-1.02718838	0.82213052
7	-2	-1.42660959	2
8	0.69234925	2	0.64428492
9	-2	2	2

Kiểm tra biên xong sẽ sắp xếp lại các vị trí cá thể và kiểm tra nếu vị trí con đầu đàn thỏa điều kiện ra kết quả tốt nhất thì sẽ được thay thế, vì vậy kết quả sẽ thu được là Cá thể tốt nhất: [0.10262446, 0.00257076, 0.12621516] và fitness = 0.00616894. Hoàn tất vòng lặp đầu tiên thu được cá thể tốt nhất là cá thể được in đậm trong bảng còn cá thể bị thay thế thì sẽ được in nghiêng kết quả như Bảng 6 sau:

Bảng 6. Tập hợp các cá thể sau khi hoàn thành vòng lặp 1. Dòng in đậm là cá thể mới được thêm vào

Index	x	y	z	fitness
0	0.10262446	0.00257076	0.12621516	0.006168942
1	-0.25529128	0.06973586	0.04292713	0.024463214
2	0.07093222	-0.26234487	0.21619166	0.043879348
3	-0.21671154	0.42137008	0.12696972	0.107117888
4	0.01831771	-0.95450176	-0.07420584	0.456566402
5	-0.15790724	-1.02718838	0.82213052	0.648519315
6	0.69234925	2	0.64428492	2.228966338
7	-2	-1.42660959	2	3.017607461
8	-2	-2	1.29357125	3.612221096
9	-2	2	2	4

Thực hiện lặp lại (trong ví dụ này 100 vòng lặp). Các cá thể sau 100 vòng lặp như ở Bảng 7

Bảng 7. Tập hợp các cá thể sau 100 vòng lặp

Index	x	y	z	fitness
0	-1.515022E-42	7.665830E-42	-1.219732E-41	5.494333E-83
1	9.246556E-42	2.692784E-42	2.269989E-41	1.180060E-82
2	1.968101E-41	9.903141E-42	-1.086236E-41	1.978153E-82
3	2.862307E-41	-2.576713E-42	3.985507E-41	5.411508E-82
4	-2.872071E-41	4.346358E-42	6.835223E-41	1.063076E-81
5	-8.803673E-41	1.629523E-42	3.229520E-41	2.758646E-81
6	-3.591634E-38	2.369224E-38	-2.498157E-40	7.106660E-76

Index	x	y	z	fitness
7	2.620179E-29	9.175567E-40	7.037336E-37	2.288446E-58
8	-3.461296E-19	-3.743543E-19	-2.236614E-18	9.437459E-37
9	-2.624466E-12	2.161399E-21	-7.966598E-21	2.295940E-24

Dòng đầu tiên của Bảng 7 sẽ cho lời giải tối ưu của bài toán.

4. ỨNG DỤNG TRONG BÀI TOÁN ẨN TẬP PHỔ BIẾN

Bài toán (FIPP - Frequent Itemset Privacy Preserving) bảo vệ quyền riêng tư của các bộ dữ liệu giao tác bằng cách ẩn các tập phổ biến nhạy cảm trong dữ liệu và giữ nguyên tính toàn vẹn của các tập phổ biến không nhạy cảm. Phương pháp này thực hiện biến đổi cơ sở dữ liệu để loại bỏ hoặc thay thế các mục trong các tập phổ biến nhạy cảm bằng cách ẩn các tập phổ biến nhạy cảm trong dữ liệu và giữ nguyên tính toàn vẹn của các tập phổ biến không nhạy cảm. Tóm lại, FIPP là một phương pháp ẩn dữ liệu hiệu quả giúp bảo vệ quyền riêng tư của các bộ dữ liệu giao tác.

Định nghĩa 1. (Bài toán ẩn tập phổ biến). Cho trước một cơ sở dữ liệu giao tác F có tập hạng mục $I = \{i_1, i_2, \dots, i_r\}$, một độ hỗ trợ tối thiểu ω và một tập các tập phổ biến nhạy cảm SIs. Thực hiện biến đổi F thành F' sao cho $\text{sup}_{F'}(X) < \omega \forall X \in B$.

Khi thực hiện bài toán ẩn tập phổ biến, thông thường xuất hiện 3 loại kết quả không mong muốn như sau.

Định nghĩa 2. (Fail to Hide – FTH). Là số lượng các tập nhạy cảm xuất hiện trong cơ sở dữ liệu D'. Điều này có nghĩa là sao khi thực hiện phương pháp ẩn tập nhạy cảm, có một số tập không thể ẩn được thông qua phương pháp đó. Thông số này được ký hiệu là α .

Định nghĩa 3. (Not to be Hidden - NTH). Là số lượng các tập phổ biến không nhạy cảm bị ẩn trong cơ sở dữ liệu D'. Điều này có nghĩa là khi áp dụng phương pháp ẩn tập nhạy cảm, một số tập phổ biến không nhạy cảm cũng bị ẩn theo. Thông số này ký hiệu là θ .

Định nghĩa 4. (Not to be Generated - NTG). Là số lượng các tập không phổ biến trong cơ sở dữ liệu D lại trở thành phổ biến trong cơ sở dữ liệu D'. Điều này có nghĩa là khi áp dụng phương pháp ẩn tập nhạy cảm, một số tập không phổ biến trong cơ sở dữ liệu ban đầu lại trở thành phổ biến trong cơ sở dữ liệu hiệu chỉnh, các tập này còn gọi là các tập ma. Thông số này được ký hiệu là γ .

Định nghĩa 5. Sử dụng công thức Chim Hồng Hạc đơn giản, ta có thể tính toán được số lượng giao tác cần phải ẩn bằng cách nhân tỷ lệ minsup mong muốn với số lượng giao tác trong tập dữ liệu. Giả sử chúng ta muốn ẩn các tập phổ biến nhạy cảm có độ phổ biến thấp hơn 20% ($\text{minsup} = 20\%$) trong tập dữ liệu này. Số lượng giao tác cần ẩn = $\text{minsup} \times \text{số lượng giao tác trong tập dữ liệu} = 20\% \times 100 = 20$ giao tác

Thực tế, không có phương pháp ẩn tập phổ biến nào hoàn hảo đến mức có thể làm cho các thông số không mong muốn tất cả đều bằng không. Cách tiếp cận tốt nhất để ẩn tập phổ biến phụ thuộc vào bối cảnh và mục đích sử dụng. Như vậy, bài toán ẩn tập phổ biến có thể quy về bài toán tối ưu với hàm mục tiêu

$$f = G_1\alpha + G_2\theta + G_3\gamma$$

trong đó, G1, G2, G3 là các trọng số tương ứng với các thông số không mong muốn. Thông thường G1 sẽ được đặt lớn hơn nhiều so với G2 và G3 với mong muốn có thể ẩn hoàn toàn các tập nhạy cảm.

Áp dụng phương pháp tối ưu chim hồng hạc cho bài toán ẩn tập nhạy cảm, công trình này đề xuất một phương pháp mới để giải bài toán theo hướng metaheuristic. Mỗi cá thể chim hồng hạc sẽ chứa biến Dim là không gian tìm kiếm. Mỗi cá thể chim hồng hạc sẽ chứa thông tin về Tid (Transaction ID) cần hiệu chỉnh hoặc xóa bỏ.

Dim có thể tính theo công thức:

$$Dim = \varepsilon_1 - \omega \frac{Max_Sup(B_i) - |D|}{\omega}$$

Trong đó:

ε_1 : random ngẫu nhiên -1 hoặc 1.

Max_sup (Bi): độ hỗ trợ lớn nhất trong số tất cả các tập nhạy cảm.

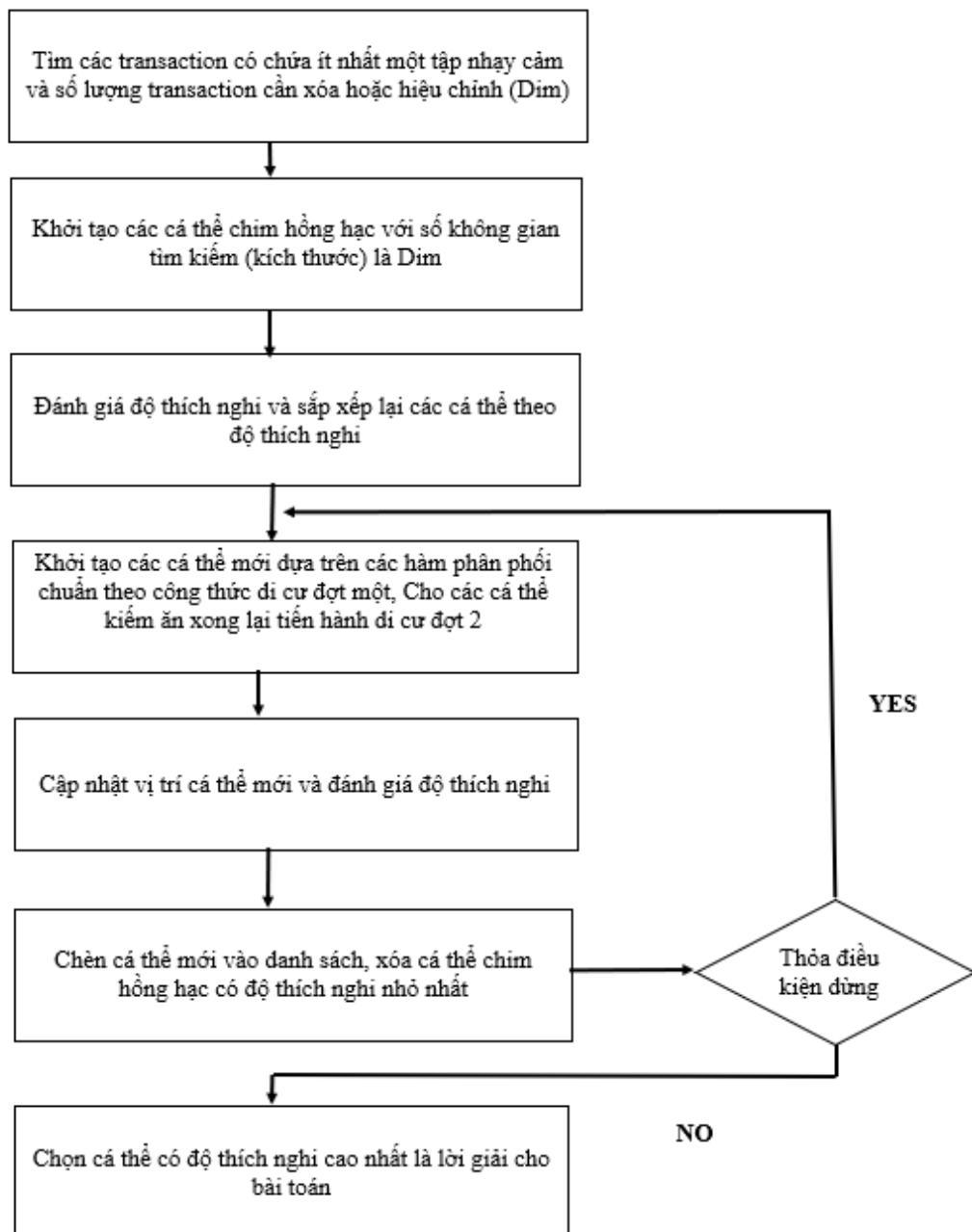
ω : độ hỗ trợ tối thiểu.

|D|: số lượng các giao tác có trong tập dữ liệu gốc.

Sau khi tính được số lượng không gian tìm kiếm trong một cá thể chim hồng hạc, các cá thể sẽ được khởi tạo một cách ngẫu nhiên dựa trên các thông tin các transaction có chứa ít nhất 1 tập nhạy cảm. Các cá thể được khởi tạo sẽ được đánh giá độ thích nghi sau đó và sắp xếp lại theo độ thích nghi.

Trong mỗi vòng lặp, một cá thể chim hồng hạc mới được phát sinh dựa trên hình thức di cư đột một tiếp đến kiểm ăn bằng cách di chuyển hai chân và quét mỏ sau đó sẽ tiến hành di cư đột 2 kiểm tra ranh giới và tính độ thích nghi, thông tin của 3 chiều không gian tìm kiếm được lựa chọn là con tốt nhất tương ứng với cá thể đầu đàn. Cá thể tốt nhất đã được sinh ra và cho chúng bắt buộc di chuyển ngẫu nhiên bằng cách nhân với một số ngẫu nhiên có thông số chuẩn.

Cá thể này sẽ được đánh giá độ thích nghi và chèn vào trong danh sách các cá thể đúng vị trí ứng với độ thích nghi của nó. Cá thể có độ thích nghi thấp nhất sẽ bị loại bỏ. Phương pháp ẩn tập phổ biến sử dụng tối tìm kiếm chim hồng hạc được biểu thị bởi sơ đồ ở Hình 4.



Hình 4. Sơ đồ phương pháp giải bài toán ẩn tập phổ biến sử dụng FSA

5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Bài báo này trình bày thuật toán tối ưu hóa tìm kiếm chim hồng hạc (Flamingo Search Algorithm-FSA) một phương pháp tối ưu hóa metaheuristic lấy cảm hứng từ đàn chim hồng hạc di cư kiếm ăn hoạt động trong tự nhiên. Với khả năng giải quyết các bài toán tối ưu đa mục tiêu. Trong bài báo cũng trình bày phương pháp để xuất ứng dụng thuật toán tối ưu tìm kiếm chim hồng hạc để giải bài toán khai thác dữ liệu đảm bảo tính riêng tư. Mặc dù chưa có thực nghiệm cụ thể về phương pháp mới này, nhưng phương pháp hứa hẹn sẽ cho kết quả chính xác không kém các phương pháp sử dụng tối ưu bầy đàn hay thuật giải di truyền trước đó.

Hướng phát triển tiếp theo cho thuật toán chim hồng hạc có thể bao gồm việc phát triển các biến thể của thuật toán, như thuật toán chim lửa hay thuật toán chim đại bàng, để tăng tính linh hoạt và khả năng giải quyết các bài toán khác nhau. Ngoài ra, cần nghiên cứu các phương pháp mới để cải thiện khả năng đánh giá hiệu quả của các cá thể mới, tăng tốc quá trình tiến hóa và giảm độ phức tạp tính toán nhằm cải thiện hiệu suất và độ chính xác của thuật toán. Sự tiến bộ trong thuật toán này sẽ đóng góp tích cực cho sự phát triển của nhiều lĩnh vực ứng dụng khác nhau.

Các kết quả thực nghiệm cụ thể sẽ được công bố trong các báo cáo tiếp theo.

TÀI LIỆU THAM KHẢO

1. Wang Zhiheng And Liu Jianhua,2021, Flamingo Search Algorithm: A New Swarm Intelligence Optimization Algorithm, Digital Object Identifier 10.1109/ACCESS.2021.3090512, 88564-88582.
2. J Q. Zhang, Y. Guo, Y. Wang, and X. Liu, “A discrete whale optimization algorithm and application,” *J. Univ. Electron. Sci. Technol. China*, vol. 49, no. 4, pp. 622–630, Jul. 2020, doi: 10.12178/1001 0548.2019116
3. S. Kaur, L. K. Awasthi, A. L. Sangal, and G. Dhiman, “Tunicate swarm algorithm: A new bio-inspired based metaheuristic paradigm for global optimization,” *Eng. Appl. Artif. Intell.*, vol. 90, Apr. 2020, Art.no.103541, doi: 10.1016/j.engappai.2020.103541.
4. J. Xue and B. Shen, “A novel swarm intelligence optimization approach: Sparrow search algorithm,” *Syst. Sci. Control Eng.*, vol. 8, no. 1, pp. 22–34, Jan. 2020, doi: 10.1080/21642583.2019.1708830.
5. BØchet, M. Rendón-martos, M. Rendón, J. A. Amat, A. R. Johnson, and M. Gauthier-Clerc, “Global economy interacts with climate change to jeopardize species conservation: The case of the greater flamingo in the Mediterranean and West Africa,” *Environ. Conservation*, vol. 39, no. 1, pp. 1–3, Mar. 2012, doi: 10.1017/S0376892911000488.
6. M. Gao, H. Tang, and P. Zhang, “Survey of path planning technologies for robot swarm,” *J. Nat. Univ. Defense Technol.*, vol. 43, no. 1, pp. 127–138, Feb. 2021, doi: 10.11887/j.cn.202101017

ABSTRACT

FLAMINGO SEARCH ALGORITHM OPTIMIZES AND APPLICATION IN HIDING FREQUENT ITEMSET PROBLEMS

Le Huynh Duc¹, Nguyen Thi Hang¹, Dinh Nguyen Trong Nghia^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: nghiadnt@hufi.edu.vn

This paper introduces an intelligent swarm optimization algorithm, named "Flamingo Search Algorithm" (FSA), based on the migratory and foraging behavior of flamingos. This algorithm is capable of finding optimal solutions to optimization problems quickly and efficiently. The FSA uses parameters such as the maximum number of iterations, the size of the flamingo population, the search range limit, and the number of migratory and foraging flocks of flamingos. The article also proposes to apply FSA to the problem of hidden frequent sets, to help find the optimal solution and minimize the risks related to competition among individuals. The FSA algorithm distributes the objects evenly on the search space and moves to locations with a lot of useful information, helping to find the best solution.

Keywords: Flamingo Search Algorithm, FSA, PPDM, hiding frequent itemset

TỐI UU HÓA SÓI XÁM VÀ ỨNG DỤNG TRONG BÀI TOÁN ẨN TẬP PHỔ BIẾN

Phạm Nguyễn¹, Đinh Nguyễn Trọng Nghĩa^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: nghiadnt@huf.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo này trình bày về việc ứng dụng thuật toán Sói xám (Grey Wolf Optimizer - GWO) để giải quyết bài toán ẩn tập nhạy cảm. Ẩn tập nhạy cảm là một bài toán quan trọng trong việc đảm bảo tính riêng tư của dữ liệu. GWO là một thuật toán tối ưu hóa metaheuristic được lấy cảm hứng từ cách thức hoạt động của bầy sói trong tự nhiên. Thuật toán này đã được chứng minh là hiệu quả trong việc tối ưu hóa các hàm mục tiêu phức tạp và được so sánh với các thuật toán tối ưu hóa khác. Trong bài báo, các tác giả đã trình bày phương pháp đề xuất sử dụng GWO để giải quyết bài toán ẩn tập nhạy cảm. Kết quả thử nghiệm cho thấy phương pháp đề xuất có khả năng giải quyết bài toán ẩn tập nhạy cảm với độ chính xác cao hơn so với các phương pháp khác như tối ưu bầy đàn hay thuật giải di truyền. Bài báo này có thể cung cấp một giải pháp hiệu quả cho việc đảm bảo tính riêng tư của dữ liệu trong các ứng dụng thực tế.

Từ khóa: Tối ưu hóa sói xám, Phân tích dữ liệu đảm bảo tính riêng tư, Đảm bảo tính riêng tư các tập phổ biến

1. MỞ ĐẦU

Các thuật toán metaheuristic được ứng dụng để tìm kiếm các lời giải tối ưu gần đúng cho các bài toán tối ưu khó, trong đó không có một phương pháp chính xác nào có thể giải được trong thời gian hợp lý. Theo định nghĩa, thuật toán metaheuristic là một thuật toán không phụ thuộc vào bài toán mà có thể tìm ra các lời giải gần đúng cho các bài toán khó. Các thuật toán metaheuristic thường lấy cảm hứng từ tự nhiên và cố gắng giải bài toán bằng cách mô phỏng các hiện tượng vật lý, sinh học, ... [1]

Các thuật toán tiến hóa (EA) là những thuật toán metaheuristic dựa trên quần thể và có tính ngẫu nhiên. EA khác với các thuật toán thông thường khác bởi chúng thực hiện tiến hóa quần thể các lời giải để tiến đến một giải pháp tối ưu gần đúng. Thông thường, các EA thực hiện tìm kiếm trong không gian bài toán bằng cách phát sinh một quần thể các cá thể (lời giải) một cách ngẫu nhiên ban đầu, sau đó đánh giá độ thích nghi của chúng dựa trên hàm thích nghi. Trong các thế hệ tiếp theo, các cá thể tiến hóa theo xu hướng của cá thể tốt nhất và được hỗ trợ bởi hàm thích nghi. Quá trình này được tiếp tục cho đến khi đạt được số vòng lặp tối đa hoặc tìm được giải pháp gần đúng như mong đợi.

Dưới đây là một số thuật toán tiến hóa phổ biến:

- Thuật toán di truyền (Genetic Algorithm - GA): là một trong những thuật toán tiến hóa phổ biến nhất, sử dụng quy trình giải mã của di truyền học để tìm kiếm và tối ưu hóa các lời giải.[2]

- Thuật toán tiến hóa đa nhiệm (Multi-Objective Evolutionary Algorithm - MOEA): được sử dụng để giải quyết các bài toán tối ưu đa mục tiêu, trong đó có nhiều hơn một hàm mục tiêu cần tối ưu.[3]
- Thuật toán tối ưu hóa mạng nơ-ron (Neuro-evolution): sử dụng thuật toán tiến hóa để tối ưu hóa các mô hình mạng nơ-ron.[4]
- Thuật toán lập trình di truyền (Genetic Programming - GP): sử dụng kỹ thuật di truyền để tạo ra các chương trình hoặc hàm tối ưu.[5]
- Thuật toán tiến hóa phân bố (Differential Evolution - DE): sử dụng các phép toán số học để tạo ra các bản sao của các lời giải hiện tại và áp dụng các quy tắc tiến hóa để tìm kiếm lời giải tốt hơn.[6]

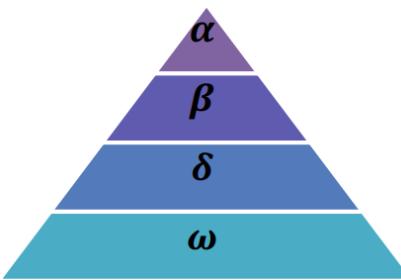
Thuật toán Sói Xám (Grey Wolf Optimizer - GWO) [7] là một thuật toán tiến hóa được lấy cảm hứng từ cách thức hoạt động của bầy sói trong tự nhiên. Thuật toán này được phát triển vào năm 2014 bởi Mirjalili và đồng nghiệp của ông, và nhanh chóng trở thành một trong những thuật toán tối ưu phổ biến trong các bài toán tối ưu hóa. Sói Xám là một thuật toán tối ưu hóa đa mục tiêu, tức là nó có thể giải quyết các bài toán có nhiều hơn một hàm mục tiêu cần tối ưu. Thuật toán này hoạt động dựa trên việc mô phỏng cách thức tương tác của các thành viên trong một bầy sói trong tự nhiên. Bằng cách này, Sói Xám có khả năng tìm kiếm lời giải tốt hơn các thuật toán khác và có thể được sử dụng trong nhiều lĩnh vực khác nhau như kỹ thuật, khoa học, và kinh doanh.

Bài báo cáo này sẽ trình bày về thuật toán tối ưu sói xám (Grey Wolf Optimization - GWO) và ý tưởng áp dụng thuật toán vào bài toán khai thác dữ liệu đám bảo tính riêng tư. Cụ thể hơn, là bài toán ẩn các tập phổ biến.

2. THUẬT TOÁN TỐI ƯU HÓA SÓI XÁM

2.1. Ý tưởng thuật toán

Thuật toán sói xám lấy cảm hứng từ hành vi xã hội của loài sói, hệ thống phân cấp xã hội của đàn sói xám. Theo đó trong bầy sói xám thông thường được phân cấp thành bốn nhóm được gọi tên theo thứ tự lần lượt từ cao đến thấp Alpha (α), Beta (β), Delta (δ) và Omega (ω) như thể hiện ở Hình 1. Mỗi vai trò trong bầy sói xám đảm bảo một nhiệm vụ khác nhau đảm bảo cho sự phát triển và tồn tại của bầy sói. Trong đó Alpha (α) là con đầu đàn và là con sói chiếm ưu thế nhất, Alpha (α) có thể là con đực hoặc con cái, chúng có nhiệm vụ đưa ra những quyết định về chiến lược săn mồi, tìm chỗ ở và phân chia thức ăn. Nhóm thứ hai là Beta (β), chúng có nhiệm vụ hỗ trợ cho Alpha (α) đưa ra quyết định. Những nhóm Beta (β) này có khả năng trở thành nhóm Alpha (α) trong trường hợp các con trong nhóm Alpha (α) rời đi hoặc chết đi chúng chiếm ưu thế cao hơn so với Delta (δ). Nhiệm vụ của những con sói này là đào tạo, lính canh gác và đảm bảo sự an toàn của bầy đàn. Nhóm cuối cùng có vị thế thấp nhất trong đàn là Omega (ω), đóng vai trò là con phải hy sinh và phải tuân theo những yêu cầu và mệnh lệnh của những con sói (α, β, δ) trong đàn.



Hình 1. Phân cấp của bầy sói trong tự nhiên

Bên cạnh thứ bậc xã hội, sói xám có cách săn mồi rất đặc trưng với chiến lược độc đáo. Chúng đi săn theo bầy và hợp tác thành nhóm để tách con mồi ra khỏi đàn, sau đó một hoặc hai con sói sẽ đuổi theo và tấn công con mồi trong khi những con khác đuổi theo bất kỳ kẻ nào đi lạc.

Mô tả chiến lược săn mồi của bầy sói và nó bao gồm:

- Tiếp cận, theo dõi và đuổi theo con mồi.
- Truy đuổi, quấy rối và bao vây xung quanh con mồi cho đến khi nó ngừng di chuyển.
- Tấn công con mồi khi nó kiệt sức.

2.2. Mô hình toán học và thuật toán

Trong phần này sẽ trình bày phần mô hình toán học và thuật toán. Các mô hình toán học liên quan đến hệ thống xếp hạng xã hội, theo dõi, bao vây và tấn công con mồi sẽ được cung cấp. Sau đó, thuật toán GWO sẽ được trình bày.

2.2.1. Hệ thống phân cấp xã hội

Để mô hình toán học cho bậc thang xã hội của bầy sói khi thiết kế GWO, Thuật toán xem xét giải pháp phù hợp nhất là alpha (α). Do đó, hai giải pháp tốt thứ hai và thứ ba được đặt tên lần lượt là beta (β) và delta (δ). Các giải pháp ứng viên còn lại được giả định là omega (ω). Trong thuật toán GWO, việc săn mồi (tối ưu hóa) được hướng dẫn bởi α , β và δ . Những con sói ω tuân thủ theo ba con sói này.

2.2.2. Bao vây con mồi

Để mô hình toán học các bước bao vây trong GWO các phương trình sau đây được đề xuất:

$$\vec{D} = |\vec{C} \cdot \vec{X}_p(t) - \vec{X}(t)| \quad (1)$$

$$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A} \cdot \vec{D} \quad (2)$$

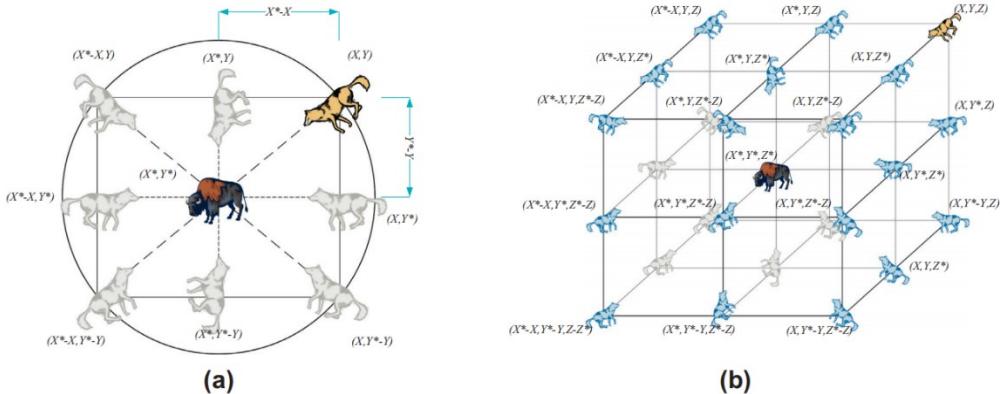
Trong đó, t cho biết sự lặp lại hiện tại, \vec{A} và \vec{C} là các vector hệ số, \vec{X}_p là vector vị trí của con mồi, và \vec{X} biểu thị vector vị trí của một con sói xám.

Các vector \vec{A} và \vec{C} được tính như sau:

$$\vec{A} = 2 \cdot \vec{a} \cdot \vec{r}_1 - \vec{a} \quad (3)$$

$$\vec{C} = 2 \cdot \vec{r}_2 \quad (4)$$

Trong đó, các thành phần của \vec{a} sẽ được giảm tuyển tính từ 2 xuống 0 trong quá trình lặp lại và $r1, r2$ là các vector ngẫu nhiên trong $[0, 1]$. Vì vậy, một con sói xám có thể cập nhật vị trí của nó theo tọa độ (X, Y) trong không gian xung quanh con mồi ở bất kỳ vị trí ngẫu nhiên nào bằng cách sử dụng các phương trình Eq.1 và Eq.4 thể hiện như Hình 2.



Hình 2. Mô phỏng vector vị trí 2D và 3D và các vị trí tiếp theo của sói xám.

2.2.3. Săn mồi

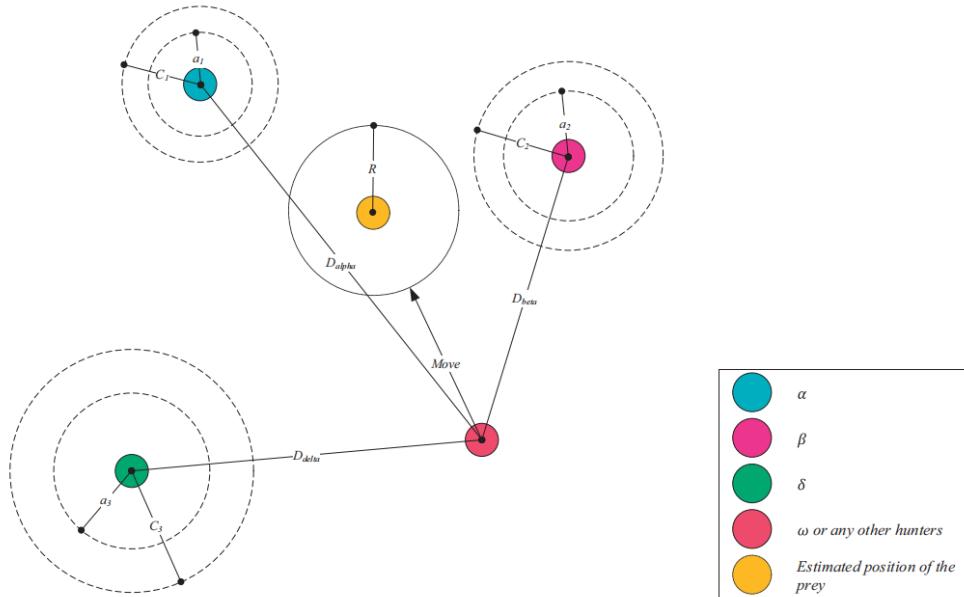
Sói xám có khả năng nhận biết vị trí của con mồi và tập trung bao vây chúng trong quá trình săn. Trong quá trình tối ưu hóa, alpha(α) thường được sử dụng để hướng dẫn các tác nhân tìm kiếm khác. Tuy nhiên, khi không có thông tin về vị trí tối ưu (con mồi) trong không gian tìm kiếm trừu tượng, beta(β) và delta(δ) (các giải pháp ứng cử viên tốt nhất) được cho rằng có kiến thức tốt hơn về vị trí tiềm năng của con mồi. Vì vậy, thuật toán GWO lưu trữ ba giải pháp tốt nhất cho đến nay (bao gồm alpha(α), beta(β), delta(δ)), và yêu cầu các tác nhân tìm kiếm khác (bao gồm omega(ω)) cập nhật vị trí của họ theo vị trí của các tác nhân tìm kiếm tốt nhất. Công thức được đề xuất cho vấn đề này như sau.

$$\overrightarrow{D_\alpha} = |\overrightarrow{C_1} \cdot \overrightarrow{X_\alpha} - \overrightarrow{X}|, \quad \overrightarrow{D_\beta} = |\overrightarrow{C_2} \cdot \overrightarrow{X_\beta} - \overrightarrow{X}|, \quad \overrightarrow{D_\delta} = |\overrightarrow{C_3} \cdot \overrightarrow{X_\delta} - \overrightarrow{X}| \quad (3)$$

$$\overrightarrow{X_1} = \overrightarrow{X_\alpha} - \overrightarrow{A_1} \cdot (\overrightarrow{D_\alpha}), \quad \overrightarrow{X_2} = \overrightarrow{X_\beta} - \overrightarrow{A_2} \cdot (\overrightarrow{D_\beta}), \quad \overrightarrow{X_3} = \overrightarrow{X_\delta} - \overrightarrow{A_3} \cdot (\overrightarrow{D_\delta}) \quad (4)$$

$$\overrightarrow{X}(t+1) = \frac{\overrightarrow{X_1} + \overrightarrow{X_2} + \overrightarrow{X_3}}{3} \quad (5)$$

Với các phương trình trên, tác nhân tìm kiếm sẽ cập nhật vị trí của mình theo vị trí của alpha, beta và delta trong không gian tìm kiếm. Kết quả cuối cùng sẽ được định vị trong một vòng tròn xung quanh alpha(α), beta(β) và delta(δ). Nói cách khác, alpha(α), beta(β) và delta(δ) sẽ xác định vị trí của con mồi và các tác nhân khác sẽ cập nhật vị trí của mình xung quanh con mồi theo cách ngẫu nhiên như Hình 3.



Hình 3. Mô phỏng quá trình cập nhật vị trí của sói xám trong GWO.

2.2.4. Tấn công con mồi (khai thác)

Như đã nói ở trên sói xám kết thúc cuộc săn bằng cách tấn công con mồi khi nó ngừng di chuyển. Để lập mô hình toán học tiếp cận con mồi, thuật toán giảm giá trị của \vec{a} . Lưu ý rằng biên độ dao động của \vec{A} cũng giảm theo \vec{a} . Nói cách khác \vec{A} là một giá trị ngẫu nhiên trong khoảng $[-2a, 2a]$ trong đó a giảm từ 2 xuống 0 trong quá trình lặp lại. Khi các giá trị ngẫu nhiên của \vec{A} nằm trong $[-1, 1]$, vị trí tiếp theo của tác nhân tìm kiếm có thể ở bất kỳ vị trí nào giữa vị trí hiện tại của nó và vị trí của con mồi. Hình 4 cho thấy $|A| < 1$ buộc đàn sói tấn công về phía con mồi.

Với các toán tử được đề xuất cho đến nay, thuật toán GWO cho phép các tác nhân tìm kiếm của nó cập nhật vị trí của chúng dựa trên vị trí của alpha(α), beta(β) và delta(δ); và tấn công con mồi. Tuy nhiên, thuật toán GWO dễ bị đình trệ trong các giải pháp cục bộ với các toán tử này. Đúng là cơ chế bao vây được đề xuất cho thấy sự thăm dò ở một mức độ nào đó, nhưng GWO cần nhiều nhà khai thác hơn để nhán mạnh việc thăm dò.

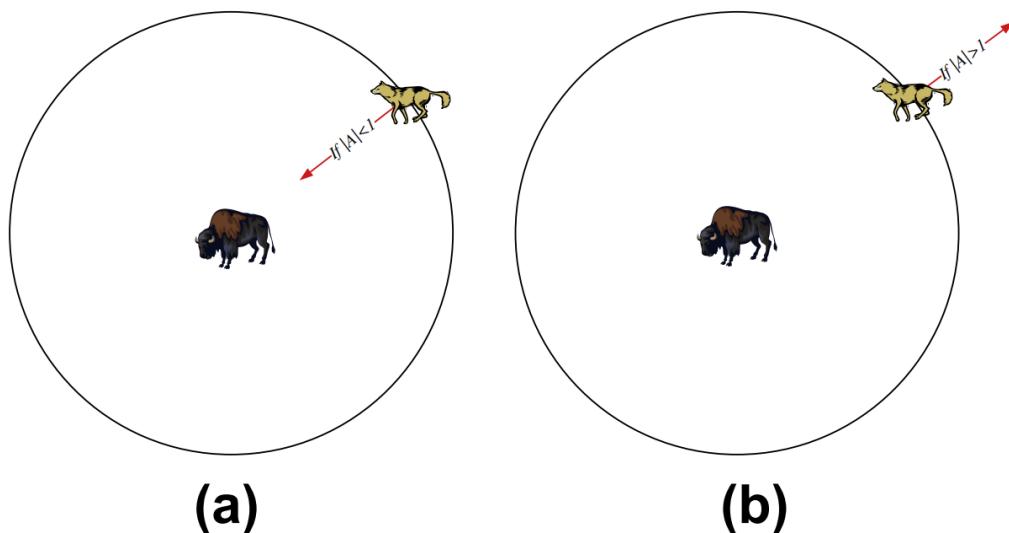
2.2.5. Tìm kiếm con mồi (thăm dò)

Trong thuật toán GWO, sói xám chủ yếu tìm kiếm con mồi theo vị trí của alpha(α), beta(β) và delta(δ). Chúng tách ra khỏi nhau để tìm kiếm con mồi và hội tụ để tấn công con mồi, tương tự như trong tự nhiên. Để phân kỳ toán học, \vec{A} với các giá trị ngẫu nhiên lớn hơn 1 hoặc nhỏ hơn -1 được sử dụng để bắt buộc tác nhân tìm kiếm phải chuyển hướng khỏi con mồi, tạo ra sự đa dạng trong quá trình tìm kiếm và khám phá toàn diện.

Hình 4 cho thấy khi $|\vec{A}| > 1$, buộc những con sói phải tách khỏi con mồi để hy vọng tìm kiếm con mồi khác tốt hơn. Thành phần khác của GWO là \vec{C} , chứa các giá trị ngẫu nhiên trong $[0, 2]$, cung cấp các trọng số ngẫu nhiên cho con mồi để nhán mạnh ngẫu nhiên hoặc giảm nhán mạnh tác động của con mồi trong việc xác định khoảng cách. Thành phần này hỗ trợ quá

trình khám phá và tránh tối ưu hóa cục bộ, bằng cách tạo ra nhiều hành vi ngẫu nhiên hơn trong quá trình tối ưu hóa. Các chướng ngại vật trong tự nhiên cũng có thể được xem như tác động của \vec{C} đối với việc tiếp cận con mồi.

Quá trình tìm kiếm bắt đầu bằng việc tạo ra một quần thể sói xám ngẫu nhiên, sau đó các sói alpha(α), beta(β) và delta(δ) ước tính vị trí có thể xảy ra của con mồi và cập nhật khoảng cách của mỗi giải pháp ứng cử viên với con mồi. Tham số được giảm để tăng hoạt động thăm dò và khai thác tương ứng. Các giải pháp ứng cử viên có xu hướng khác với con mồi khi $|\vec{A}| > 1$ và hội tụ về phía con mồi khi $|\vec{A}| < 1$. Cuối cùng, thuật toán GWO kết thúc khi thỏa mãn một tiêu chí cuối cùng.



Hình 4. Mô phỏng quá trình tấn công con mồi so với tìm kiếm con mồi của sói xám.

Thuật toán: GWO

Input:

- **MaxIter:** số lần lặp tối đa của thuật toán
- **SearchAgents_no:** số lượng sói tìm kiếm
- **dim:** số chiều của không gian tìm kiếm
- **lb:** giới hạn dưới của miền tìm kiếm
- **ub:** giới hạn trên của miền tìm kiếm
- **fun():** hàm mục tiêu cần tối ưu
- **rand():** hàm ngẫu nhiên trong khoảng 0 đến 1

Hàng số:

a = 2

t = 0

Khởi tạo:

tạo ra một mảng chứa tọa độ của các sói (positions)

for each wolf i to SearchAgents_no do

for j = 1 to dim do

positions[i, j] = lb + (ub - lb) * rand()

end for

end for

// Sắp xếp quần thể theo hàm mục tiêu từ thấp đến cao

Sort(positions, fun)

// khởi tạo giá trị cho ba cá thể alpha, beta, delta

GlobalAlpha = positions[0]

Alpha_pos = positions[0]

Alpha_score = fun[Alpha_pos]

Beta_pos = positions[1]

Beta_score = fun[Beta_pos]

Delta_pos = positions[2]

Delta_score = fun[Delta_pos]

Xử lý:

// Bắt đầu vòng lặp chính của thuật toán

for t = 1 to MaxIter do

// Duyệt qua các sói trong tất cả bầy

for i = 1 to SearchAgents_no do

// Tính toán khả năng điều chỉnh của sói i

a = 2 - 2 * t / MaxIter

A1 = 2 * a * rand() - a

C1 = 2 * rand()

D_alpha = abs(C1 * Alpha_pos - positions(i,:))

X1 = Alpha_pos - A1 * D_alpha

A2 = 2 * a * rand() - a

C2 = 2 * rand()

D_beta = abs(C2 * Beta_pos - positions(i,:))

X2 = Beta_pos - A2 * D_beta

A3 = 2 * a * rand() - a

C3 = 2 * rand()

D_delta = abs(C3 * Delta_pos - positions(i,:))

X3 = Delta_pos - A3 * D_delta

// Tính toán vị trí mới cho sói i

new_pos = (X1 + X2 + X3) / 3

// Kiểm tra xem sói i có ở ngoài miền tìm kiếm hay không

new_pos = clip(new_pos, lb, ub)

// Tính giá trị hàm mục tiêu tại vị trí mới

new_score = fun(new_pos)

// So sánh giá trị fitness của con sói mới với vị trí con sói vị trí thứ I trong bầy.

if (new_score < positions[i])

positions[i] = new_pos

end if

end for

```

// Sắp xếp quần thể theo hàm mục tiêu từ thấp đến cao
Sort(positions, fun)
//Cập nhật lại alpha, beta, delta.
Alpha_pos = positions[0]
Beta_pos = positions[1]
Delta_pos = positions[2]
GlobalAlpha = positions[0]
t += 1
end for

```

Output:

- **GlobalAlpha:** giá trị tối ưu nhất tìm thấy bởi thuật toán
- **Best_score:** giá trị của hàm mục tiêu tại GlobalAlpha

3. VÍ DỤ MINH HỌA THUẬT TOÁN

Lấy ví dụ tìm min value hàm tối ưu được định nghĩa bởi.

$$f(x, y, z) = \frac{1}{3}x^2 + \frac{1}{2}y^2 + \frac{1}{6}z^2$$

Trong đó x, y, z sẽ nằm trong khoảng [-2, 2].

Bước đầu tiên khởi tạo quần thể sói xám ngẫu nhiên. Ở đây bài toán có 3 biến, số lượng sói trong quần thể là 10 con. Khởi tạo tính độ thích nghi(fitness) và sắp xếp quần thể theo độ thích nghi(fitness) ta được Bảng 1.

Bảng 1. Tập hợp các cá thể sói xám sau khi khởi tạo.

index	x	y	z	Fitness
0	0.407739	-0.05751	-0.393094	0.082824509
1	-1.67645	0.60196	0.147036	1.121611923
2	1.125486	-1.17777	0.502036	1.157823305
3	-1.823478	-0.35867	-0.980832	1.333016975
4	1.842868	-0.98705	-0.137259	1.62233248
5	-1.577137	-1.27016	-0.292675	1.65005128
6	-0.296583	-1.79749	0.332476	1.663223383
7	1.144374	1.65843	0.256712	1.822714291
8	0.737896	-1.90029	0.445237	2.020080113
9	1.859113	1.83989	0.901986	2.980297799

Từ Bảng 1, ta có thể xác định được 3 cá thể có chỉ số thích nghi thấp nhất sẽ được chọn và lần lượt đặt tên là alpha(α), beta(β), delta(δ). Các cá thể còn lại sẽ được gọi là omega.

Sau khi khởi tạo, thuật toán sẽ sử dụng 3 cá thể alpha(α), beta(β), delta(δ) để sinh ra thêm một cá thể mới ngẫu nhiên trong quá trình duyệt qua quần thể ban đầu. Áp dụng thuật toán, thu được một cá thể mới mang giá trị [-0.4451379, -0.58763753, -0.27990989]. Tuy nhiên, độ thích nghi của cá thể này thấp hơn so với cá thể tương ứng trong bầy nên sẽ không được thay thế vào. Tiếp tục sẽ thực hiện tuần tự các bước trên sinh thêm các cá thể mới từ 3 cá thể alpha(α), beta(β), delta(δ). Lần này thu được cá thể mới tốt hơn [-0.20087211, -

0.40186463, 0.19529411]. Với giá trị thích nghi nhỏ hơn cá thể tương ứng trước đó trong bầy và cá thể mới này sẽ được thay thế vào. Sẽ thực hiện lại các bước trên cho đến khi duyệt hết quần thể. Nếu thỏa điều kiện, cá thể mới sẽ được thay thế và ngược lại. Khi kết thúc, kết quả đạt được thể hiện ở Bảng 2.

Bảng 2. Tập hợp cá cá thể sói xám sau khi hoàn thành vòng lặp 1.
(Cá thể in đậm là cá thể không thay đổi)

Index	x	y	z	Fitness
0	0.407739	-0.05751	-0.393094	0.082824509
1	-0.200872	-0.40186	0.195294	0.10055409
2	0.097953	-0.22241	0.456456	0.06265636
3	-0.818134	-0.15419	-1.198108	0.47424531
4	-0.087798	-0.40294	-0.026366	0.083864467
5	0.938505	0.26669	0.028493	0.329295287
6	-0.634317	-1.529	-0.486684	1.342510051
7	0.004053	-0.01852	0.464664	0.036162417
8	0.737896	-1.90029	0.445237	2.020080113
9	-0.84784	-1.31745	-0.471901	1.144557311

Tiến hành lặp lại 200 vòng lặp sẽ được một tập hợp các vị trí cá thể sói như trong Bảng 3 dưới đây.

Bảng 3. Tập hợp các cá thể sói xám sau 200 vòng lặp.

index	x	y	z	fitness
0	6.094987E-15	6.094987E-15	1.594273E-14	7.33192E-29
1	6.104258E-15	-1.048277E-14	1.596698E-14	1.09856E-28
2	6.112792E-15	-1.046856E-14	1.598931E-14	1.09860E-28
3	6.126295E-15	-1.044537E-14	1.602463E-14	1.09861E-28
4	6.119134E-15	-1.045778E-14	1.600590E-14	1.09862E-28
5	6.111283E-15	-1.047135E-14	1.598536E-14	1.09862E-28
6	6.120047E-15	-1.045626E-14	1.600828E-14	1.09862E-28
7	6.116784E-15	-1.046203E-14	1.599975E-14	1.09864E-28
8	6.125929E-15	-1.044640E-14	1.602367E-14	1.09866E-28
9	6.129761E-15	-1.043992E-14	1.603369E-14	1.09867E-28

Sau khi quá trình hoàn tất giá trị tối ưu nhất đầu tiên trong bảng là kết quả của bài toán cần tìm.

4. ÚNG DỤNG VÀO BÀI TOÁN ÂN TẬP NHẠY CẨM

Bài toán ân tập phổ biến (Frequent Itemset Privacy Preserving, FIPP) là một phương pháp ân dữ liệu được sử dụng để bảo vệ quyền riêng tư của các bộ dữ liệu giao tác. Phương pháp này cho phép ân các tập phổ biến nhạy cảm, đồng thời giữ nguyên tính toàn vẹn của các tập phổ biến không nhạy cảm trong cơ sở dữ liệu.

Định Nghĩa 1: Cơ sở dữ liệu giao tác: Là tập hợp các giao tác trong đó mỗi giao tác là tập hợp các hạng mục. Ví dụ: cơ sở dữ liệu mua sắm của một siêu thị, mỗi giao tác là danh sách các sản phẩm khách hàng đã mua.

Định Nghĩa 2: Hạng mục (item) là một đơn vị cơ bản của dữ liệu, có thể là một mặt hàng trong giỏ hàng hoặc một thuộc tính của đối tượng. Ví dụ, trong một tập dữ liệu về giỏ hàng, các hạng mục có thể là A (táo), B (bánh mì), C (ngũ cốc), D (bánh rán), E (trứng).

Định Nghĩa 3: Tập hạng mục (itemsets): Là tập hợp các hạng mục (item), mỗi hạng mục đại diện cho một đối tượng hoặc thuộc tính. Ví dụ: danh sách các sản phẩm trong siêu thị.

Định Nghĩa 4: Tập phổ biến (frequent itemset) là tập hợp các itemset X thỏa mãn độ phổ biến tối thiểu (minsupp) do người dùng định nghĩa trước đó (ví dụ: 40% hoặc xuất hiện ít nhất 5 lần). Nếu tần suất xuất hiện của itemset đó lớn hơn hoặc bằng ngưỡng hỗ trợ tối thiểu (minsupp), thì itemset đó được xem là tập phổ biến. Nói cách khác, nếu $\text{supp}(S) \geq \text{minsup}$ thì tập hợp S là frequent itemset.

Định Nghĩa 5: k-Itemset là tập hợp các mục (items) trong tập dữ liệu có k phần tử, trong đó k là một số nguyên dương. Ví dụ, một tập hợp gồm các mục {mì, bánh mì, trứng, sữa} được gọi là 4-Itemset. Trong khai thác dữ liệu, k-Itemset được sử dụng để tìm các mẫu tần suất (frequent patterns) trong dữ liệu. Các mẫu tần suất được sử dụng để phân tích và giải thích dữ liệu trong nhiều lĩnh vực, bao gồm thương mại điện tử, y học, marketing, và khoa học dữ liệu.

Định Nghĩa 6: Tập phổ biến nhạy cảm (Sensitive Itemsets - SIs): Là tập hợp các tập hợp hạng mục có thể dẫn đến việc xác định được thông tin riêng tư của cá nhân trong cơ sở dữ liệu. Ví dụ: danh sách các sản phẩm liên quan đến một bệnh truyền nhiễm.

Định Nghĩa 7: Biến đổi cơ sở dữ liệu: Là quá trình thay đổi cơ sở dữ liệu ban đầu thành một cơ sở dữ liệu mới, sao cho các tập hợp hạng mục trong tập phổ biến nhạy cảm không xuất hiện trong cơ sở dữ liệu mới. Ví dụ: ẩn các giao tác chứa các sản phẩm trong danh sách liên quan đến bệnh truyền nhiễm.

Sau đó, phương pháp sẽ tiến hành ẩn các tập phổ biến nhạy cảm bằng cách thực hiện biến đổi cơ sở dữ liệu giao tác ban đầu thành cơ sở dữ liệu giao tác mới D' , sao cho $\text{supp}_{D'}(X) < \delta \forall X \in S$.

Khi thực hiện phương pháp FIPP để ẩn các tập phổ biến nhạy cảm, có thể xảy ra 3 loại kết quả không mong muốn, đó là:

- Fail to Hide (FTH) được xác định là số lượng các tập nhạy cảm xuất hiện trong cơ sở dữ liệu D' . Điều này có nghĩa là trong quá trình ẩn tập nhạy cảm, không thể ẩn hoàn toàn một số tập. Thông số này được ký hiệu là α .

– Not to be Hidden (NTH) là số lượng các tập phổ biến không nhạy cảm bị ẩn trong cơ sở dữ liệu D' khi thực hiện phương pháp ẩn tập nhạy cảm. Điều này có nghĩa là một số tập phổ biến không nhạy cảm cũng bị ẩn theo. Thông số này ký hiệu là β .

– Not to be Generated –(NTG) là số lượng các tập không phổ biến trong cơ sở dữ liệu D lại trở thành phổ biến trong cơ sở dữ liệu D' sau khi thực hiện phương pháp ẩn tập nhạy cảm. Các tập này còn được gọi là các tập ma. Thông số này được ký hiệu là γ .

Thực tế, để ẩn các tập dữ liệu nhạy cảm trong một cơ sở dữ liệu, không có phương pháp nào hoàn hảo đến mức có thể đảm bảo tất cả các thông số không mong muốn đều bằng không. Do đó, bài toán ẩn tập dữ liệu nhạy cảm có thể được chuyển đổi thành bài toán tối ưu với một hàm mục tiêu, được biểu diễn bởi phương trình:

$$f = w_1\alpha + w_2\beta + w_3\gamma \quad (6)$$

Trong đó, w_1, w_2, w_3 là các trọng số tương ứng với các thông số không mong muốn. Thông thường, ta sẽ đặt w_1 lớn hơn nhiều so với w_2 và w_3 để có thể ẩn hoàn toàn các tập nhạy cảm.

Trong bài toán Frequent Itemset Privacy Preserving (FIPP), để bảo vệ quyền riêng tư của các giao tác, ta cần ẩn bỏ một số giao tác để tránh tiết lộ thông tin nhạy cảm. Tuy nhiên, việc ẩn quá nhiều giao tác có thể dẫn đến mất mát thông tin và làm giảm độ chính xác của kết quả khai thác mô hình.

Để xác định số lượng giao tác thích hợp cần ẩn, ta cần sử dụng các thông số như tỉ lệ giao tác bị ẩn, độ chính xác cần đạt được, kích thước của tập dữ liệu ban đầu và các mục phổ biến cần khai thác.

Một công thức đơn giản để tính toán số lượng giao tác thích hợp cần ẩn là:

$$S = \left| (1 - a) \times \frac{p}{\text{minsup} \times \text{FIs}} \right| \quad (7)$$

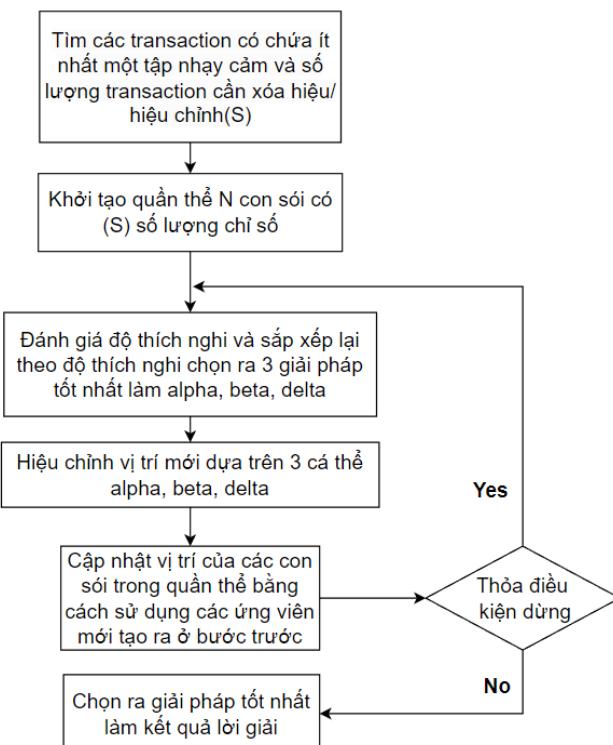
Trong đó:

- S: số lượng giao tác cần ẩn
- a: độ chính xác cần đạt được (được định nghĩa trước)
- p: kích thước của tập dữ liệu ban đầu
- minsup: ngưỡng hỗ trợ (min_support) của mục phổ biến cần khai thác
- FIs: số lượng các mục phổ biến cần khai thác

Công thức này cung cấp một cách đơn giản để ước tính số lượng giao tác cần ẩn trong bài toán FIPP. Tuy nhiên, độ chính xác của công thức này có thể bị ảnh hưởng bởi các yếu tố khác như tính đại diện của tập dữ liệu và phân phối của các mục phổ biến. Do đó, việc xác định số lượng giao tác thích hợp cần ẩn cần được xem xét kỹ lưỡng và thực hiện thử nghiệm trên các tập dữ liệu khác nhau để đảm bảo tính chính xác và đáng tin cậy của kết quả.

Sau khi tính toán được số lượng thông số cho cá thể sói xám, quần thể sói xám sẽ được khởi tạo ngẫu nhiên các thông tin các transaction có chứa ít nhất 1 tập nhạy cảm. Các cá thể sẽ được tính toán độ thích nghi và sẽ được sắp xếp theo độ thích nghi và chọn ra 3 cá thể tốt nhất lần lượt là alpha, beta, delta.

Trong mỗi vòng lặp của thuật toán GWO áp dụng cho bài toán FIPP, các con sói sẽ được cập nhật vị trí dựa trên vị trí hiện tại của chúng và vị trí của con sói tốt nhất được tìm thấy cho đến thời điểm đó. Bằng cách sử dụng các phép toán tương ứng của thuật toán GWO, ta tính toán các giá trị mới cho vị trí của mỗi con sói. Tiếp theo, ta đánh giá độ thích nghi của các cá thể dựa trên tỉ lệ giao tác được giữ lại và độ chính xác của quy tắc k-Itemset. Sau đó, ta chọn ra cá thể có độ thích nghi tốt nhất để tiếp tục thực hiện trong vòng lặp tiếp theo. Nếu một cá thể mới có độ thích nghi tốt hơn, nó sẽ thay thế cá thể kém hơn trong quần thể. Quá trình này được tiếp tục cho đến khi đáp ứng được tiêu chuẩn dừng hoặc đã đạt đến số lần lặp tối đa được thiết lập. Phương pháp ẩn tập phô biến sử dụng tối ưu Sói Xám từ được biểu thị bởi sơ đồ ở Hình 5.



Hình 5. Sơ đồ phương pháp giải bài toán ẩn tập phô biến sử dụng GWO

5. KẾT LUẬN VÀ PHƯƠNG HƯỚNG PHÁT TRIỂN

Trong bài báo này, chúng tôi giới thiệu đến bạn đọc thuật toán tối ưu Sói xám (Grey Wolf Optimizer - GWO) - một phương pháp tối ưu hóa metaheuristic lấy cảm hứng từ bầy sói hoạt động trong tự nhiên. Với khả năng giải quyết các bài toán tối ưu đa mục tiêu, GWO đánh bại các thuật toán tối ưu hóa khác trong việc tối ưu hóa các hàm mục tiêu phức tạp. Thuật toán hoạt động bằng cách mô phỏng các hành vi tự nhiên của bầy sói và phân công các vai trò khác nhau cho mỗi con sói. Bên cạnh đó, chúng tôi cũng trình bày một phương pháp đề xuất ứng dụng GWO để giải quyết bài toán khai thác dữ liệu đảm bảo tính riêng tư, với hy vọng sẽ đem lại kết quả chính xác và cải thiện hiệu quả so với các phương pháp sử dụng tối ưu bầy đàn hay thuật giải di truyền. Mặc dù chưa được thử nghiệm cụ thể, phương pháp mới này hứa hẹn mang lại giải pháp tối ưu cho bài toán khó khăn này.

Các kết quả thực nghiệm cụ thể sẽ được công bố trong các báo cáo tiếp theo.

TÀI LIỆU THAM KHẢO

1. Ilhem Boussaïd, Julien Lepagnot, Patrick, Siarry, A survey on optimization metaheuristics, *Information Sciences* 237 (2013).
2. Goldberg, D. E. *Genetic algorithms in search, optimization and machine learning*. Addison-Wesley Longman Publishing Co., Inc. (1989).
3. Coello, C. A., Lamont, G. B., & Van Veldhuizen, D. A. *Evolutionary Algorithms for Solving Multi-Objective Problems*. Springer Science & Business Media. (2007).
4. Gomez, F., Poli, R., & Langdon, W. B. *Automatic Generation of Human-Competitive Programs and Controllers by Means of Genetic Programming*. Springer Science & Business Media. (2008).
5. Stanley, K. O., & Miikkulainen, R. *Evolving neural networks through augmenting topologies*. MIT Press, 1297-1310. (2002).
6. Storn, R., & Price, K. *Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces*. *Journal of global optimization*, 11(4), 341-359. (1997).
7. Mirjalili, S., Mirjalili, S. M. & Lewis, A. *Grey wolf optimizer*. *J. Advances in Engineering Software*. 69, 46–61 (2014).

ABSTRACT

GREY WOLF OPTIMIZER OPTIMIZATION AND ITS APPLICATION IN SENSITIVE FREQUENT ITEMSET PROBLEM

Pham Nguyen¹, Dinh Nguyen Trong Nghia^{1,*}

¹*Ho Chi Minh City University of Food Industry*

**Email: nghiadnt@hufi.edu.vn*

This article presents the application of the Grey Wolf Optimizer (GWO) algorithm to solve the sensitive itemset problem. Sensitive itemset is an important problem in ensuring data privacy. GWO is a metaheuristic optimization algorithm inspired by the natural behavior of wolf packs. This algorithm has been proven to be effective in optimizing complex objective functions and has been compared with other optimization algorithms. In the article, the authors proposed a method using GWO to solve the sensitive itemset problem. The test results show that the proposed method has a higher accuracy in solving the sensitive itemset problem compared to other methods such as swarm optimization or genetic algorithms. This article may provide an effective solution to ensure data privacy in practical applications.

Keywords: Grey Wolf Optimizer, GWO, PPDM, FIPP, Frequent Itemset Privacy Preserving.

XÂY DỰNG THUẬT TOÁN LOGISTIC CHO PHÉP PHÂN LOẠI MAIL VÀ MÔ HÌNH PIPELINE TRÊN SPARK

Nguyễn Minh Hiển¹, Nguyễn Trọng Đăng Khoa¹, Nguyễn Văn Tùng¹, Ngô Dương Hà^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm TP.HCM

*Email: hand@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Các công ty kinh doanh đang cần thiết phải xây dựng một hệ thống phân loại thư theo chủ đề để giải quyết vấn đề về số lượng thư đến mỗi ngày vô cùng lớn, nguy cơ bị spam mail gây rối loạn thông tin và phần mềm độc hại có thể tồn tại trong thư gây ảnh hưởng đến hệ thống và cản trở hoạt động của công ty. Với mục đích giải quyết bài toán này, chúng tôi đề xuất sử dụng thuật toán hồi quy Logistic và thực hiện thử nghiệm song song trên Spark.

Từ khóa: Logistic regression, Spark, Hadoop, pipeline.

1. GIỚI THIỆU

1.1. Mô hình hồi quy Logistic

Mô hình hồi quy logistic là một mô hình thống kê cơ bản, sử dụng hàm logistic để mô hình hóa biến phụ thuộc nhị phân. Mặc dù có nhiều phần mở rộng phức tạp hơn, trong mô hình logistic nhị phân, chỉ có một biến phụ thuộc với hai giá trị được gắn nhãn "0" và "1", thường được sử dụng để biểu thị thành công hoặc thất bại. Trong mô hình này, xác suất cho giá trị nhãn "1" được tính dựa trên tổng tuyển tính của các biến độc lập ("predictors"), bao gồm cả các biến nhị phân và liên tục, được biểu diễn bằng hàm log-odds [1].

Hồi quy logistic được ứng dụng trong nhiều lĩnh vực khác nhau như y tế, khoa học xã hội, kỹ thuật và học máy. Ví dụ, trong lĩnh vực y tế, hồi quy logistic được sử dụng để dự đoán tỷ lệ tử vong của bệnh nhân bị thương thông qua điểm số mức độ nghiêm trọng của chấn thương [2]. Trong lĩnh vực kỹ thuật, hồi quy logistic có thể được sử dụng để dự đoán xác suất thất bại của một quy trình, hệ thống hoặc sản phẩm nhất định và áp dụng trong tiếp thị để dự đoán xu hướng mua sản phẩm của khách hàng [3,4]. Hơn nữa, hồi quy logistic còn được sử dụng để dự đoán nguy cơ phát triển các bệnh như tiểu đường hoặc bệnh tim mạch vành, dựa trên các đặc điểm của bệnh nhân như tuổi, giới tính, chỉ số khối cơ thể và các xét nghiệm máu khác [5]. Cuối cùng, hồi quy logistic còn được sử dụng để dự đoán kết quả của các cuộc bầu cử, ví dụ như dự đoán xem cử tri Nepal sẽ bỏ phiếu cho Quốc hội Nepal, Đảng Cộng sản Nepal hoặc các đảng khác, dựa trên nhiều đặc điểm như tuổi tác, thu nhập, giới tính và số phiếu bầu trong các cuộc bầu cử trước đó [6].

1.2. Sử dụng Spark kết hợp hồi quy Logistic

Apache Spark là một framework xử lý phân tán mạnh mẽ được sử dụng để xử lý dữ liệu lớn. Cung cấp một cách hiệu quả để xử lý dữ liệu lớn bằng cách phân tán trên nhiều máy tính và thực hiện tính toán song song trên chúng. Spark cung cấp nhiều API để xử lý dữ liệu, trong đó bao gồm Apache Spark MLlib, một thư viện học máy phổ biến trên Spark. Kết hợp Spark với hồi quy Logistic cho phép chúng ta xử lý và phân tích dữ liệu lớn một cách nhanh chóng và hiệu quả hơn. Chúng ta có thể sử dụng Spark MLlib để thực hiện hồi quy Logistic trên dữ liệu phân tán. Spark MLlib cung cấp các công cụ để xử lý dữ liệu, chọn tính năng, huấn luyện và kiểm tra mô hình. Cụ thể,

Spark regex tokenizer là một thành phần của Apache Spark được sử dụng các biểu thức chính quy (regex) để phân tích cú pháp và tách các chuỗi văn bản thành các mã thông báo. Điều này có thể hữu ích trong việc tiền xử lý dữ liệu văn bản, ví dụ như trong các bài toán xử lý ngôn ngữ tự nhiên như phân loại văn bản hoặc trích xuất thông tin từ văn bản. Spark regex tokenizer được tích hợp sẵn trong gói thư viện Apache Spark Machine Learning.

Spark StopWordsRemover là một tính năng trong Apache Spark được sử dụng để loại bỏ các từ dừng (stop words) khỏi văn bản. Các từ dừng là những từ phổ biến trong ngôn ngữ như "a", "an", "the", "in", "on",... chúng thường không có nhiều ý nghĩa trong việc phân tích văn bản và có thể ảnh hưởng đến quá trình phân loại hoặc đánh giá văn bản. StopWordsRemover sử dụng một tập hợp các từ dừng để loại bỏ chúng khỏi văn bản. Spark StopWordsRemover có thể xử lý nhiều cột dữ liệu cùng một lúc và trả về kết quả dưới dạng một vector chứa các từ không phải từ dừng.

HashingTF sử dụng một hàm băm (hash function) để ánh xạ mỗi từ trong văn bản thành một chỉ số trong vectơ đặc trưng. Các chỉ số được gán bằng cách sử dụng một bảng băm (hash table) với kích thước được chỉ định trước. Kích thước của bảng băm càng lớn, càng giảm thiểu khả năng xảy ra xung đột (collision) khi gán chỉ số cho các từ khác nhau. Sau khi các từ được ánh xạ vào vectơ đặc trưng, HashingTF tính toán tần số xuất hiện của các từ và trả về một vectơ đặc trưng thưa (sparse vector), trong đó chỉ bao gồm các thành phần có giá trị khác 0.

Thuật toán LogisticRegression trong Spark sử dụng kỹ thuật Gradient Descent để tối ưu hóa hàm mất mát và tìm ra bộ tham số tối ưu cho mô hình. Các tham số này được sử dụng để tính toán xác suất dự đoán cho một mẫu mới dựa trên các đặc trưng của nó. Thuật toán LogisticRegression trong Spark hỗ trợ cả các tập dữ liệu nhị phân và đa phân và có thể được sử dụng để giải quyết nhiều vấn đề khác nhau như phân loại email là thư rác hay không, dự đoán loại hoa dựa trên các đặc trưng của nó và nhiều ứng dụng khác trong lĩnh vực khai phá dữ liệu và học máy. Tóm lại, sử dụng Spark kết hợp với hồi quy Logistic cho phép chúng ta xử lý và phân tích dữ liệu lớn một cách nhanh chóng và hiệu quả hơn. Apache Spark MLlib cung cấp các công cụ để thực hiện hồi quy Logistic trên dữ liệu phân tán và tối ưu hóa mô hình.

1.3. Mô hình pipeline trên Spark

Một mô hình pipeline trên Spark là một quy trình tổ chức các công việc xử lý dữ liệu trên nền tảng Apache Spark. Mô hình này bao gồm một chuỗi các bước xử lý dữ liệu, từ việc tiền xử lý đến huấn luyện mô hình và đưa ra dự đoán.

Một pipeline trên Spark bao gồm các thành phần sau:

- Đầu vào dữ liệu: Dữ liệu được đọc vào từ một nguồn dữ liệu bên ngoài, chẳng hạn như tệp CSV hoặc HDFS.
- Bước tiền xử lý: Dữ liệu được chuyển đổi và làm sạch để chuẩn bị cho việc xây dựng mô hình. Các bước tiền xử lý có thể bao gồm các hoạt động như loại bỏ dữ liệu bị thiếu, mã hóa biến đầu vào và chia tập dữ liệu thành tập huấn luyện, tập kiểm tra.
- Huấn luyện mô hình: Mô hình được huấn luyện trên tập dữ liệu huấn luyện sử dụng các thuật toán học máy và thư viện machine learning của Spark.
- Đánh giá mô hình: Mô hình được đánh giá trên tập dữ liệu kiểm tra để đánh giá hiệu suất.
- Dự đoán: Mô hình được sử dụng để dự đoán trên dữ liệu mới.

Một pipeline trên Spark giúp cho quá trình xử lý dữ liệu được tổ chức hợp lý và dễ dàng quản lý, đồng thời tăng tính hiệu quả và độ chính xác của mô hình.

2. PHƯƠNG PHÁP

2.1. Thu thập dữ liệu và gán nhãn

Chúng tôi cần tìm các chủ đề phù hợp để xây dựng một ứng dụng phân loại mail theo chủ đề cho công ty. Để làm điều này, chúng tôi sử dụng tập dữ liệu tiếng Anh trên trang Google Groups, với các chủ đề thảo luận về sở thích chung, cho phép chúng tôi tạo dữ liệu huấn luyện dễ dàng. Trước tiên, chúng tôi tìm kiếm các chủ đề liên quan đến kinh doanh, ví dụ như buôn bán, bán xe hay các linh kiện máy tính. Sau đó, chúng tôi thu thập dữ liệu bằng cách đọc và lọc các email trên các nhóm thảo luận. Cuối cùng, chúng tôi đã gán nhãn cho bộ dữ liệu 5000 email, liên quan đến 6 phân loại chủ đề.

Phân loại dữ liệu là công việc sắp xếp các dữ liệu dựa theo những tiêu chí khác nhau được đặt ra, hay mức độ tầm soát truy cập sử dụng dữ liệu. Dựa vào những yếu tố trên để tiến hành phân loại theo nhiều tầng lớp và mức độ khác nhau cho từng loại dữ liệu. Các bước tiến hành thực hiện phân loại dữ liệu:

Bước 1: Xác định ai là người bảo vệ có trách nhiệm với dữ liệu.

Bước 2: Đề ra các tiêu ý, yếu tố để phân loại.

Bước 3: Tiến hành phân loại, dán nhãn cho từng loại dữ liệu.

Bước 4: Ghi nhận các trường hợp khác không có trong tiêu chí, thực hiện bổ sung thêm vào bộ tiêu chí.

Bước 5: Sau khi kết thúc, tiến hành chọn lựa các phương thức bảo vệ dữ liệu phù hợp.

Bước 6: Quy trình chuyển dữ liệu cho các đối tượng có trách nhiệm.

Bước 7: Lên chương trình tập huấn chương trình phân loại dữ liệu cho tổ chức.

Chúng ta có thể thay đổi các bước 5, 6, 7 bằng cách lựa chọn một thuật toán phân loại để xác định các đặc điểm chung của các lớp nhất định, tất cả sẽ làm tự động không phải thủ công như quy trình ở trên đặt ra.

2.2. Thuật toán logistic phân loại mail

Phân loại email là một vấn đề quan trọng trong việc quản lý email hàng ngày. Thuật toán Logistic Regression là một trong những phương pháp phân loại được sử dụng rộng rãi trong học máy, đặc biệt trong việc phân loại văn bản.

Để triển khai thuật toán Logistic Regression cho việc phân loại email trên môi trường phân tán, ta có thể sử dụng Apache Spark, một hệ thống xử lý phân tán được sử dụng rộng rãi trong các ứng dụng Big Data. Mô hình pipeline trên Spark cho huấn luyện phân loại email sử dụng thuật toán Logistic Regression có thể được xây dựng qua các bước theo thuật toán 1.

Thuật toán 1: Phân loại email thuật toán Logistic Regression với mô hình pipeline trên Spark.

Input: Dữ liệu Email

Output: Phân loại Email theo chủ đề và dán nhãn

Bước 1: Khởi tạo các context cho Spark và SparkSQL.

Bước 2: Đọc dữ liệu

Dữ liệu đọc từ các tập tin văn bản

Chuyển tên các chủ đề sang dạng Numeric.

Chuyển đổi sang dạng DataFrame của thư viện Pandas.

Bước 3: Tạo ngẫu nhiên khoảng 80% tập huấn luyện và 20% tập kiểm thử.

Bước 4: Tạo các DataFrame của Spark từ DataFrame của Pandas.

Bước 5: Phân bổ số lượng văn bản trong các chủ đề thuộc tập huấn luyện.

Bước 6: Phân bổ số lượng văn bản trong các chủ đề thuộc tập kiểm thử.

Bước 7: Tiền xử lý các văn bản sử dụng, sử dụng Logistic Regression để huấn luyện và đưa vào Pipeline.

Bước 8: Lưu model.

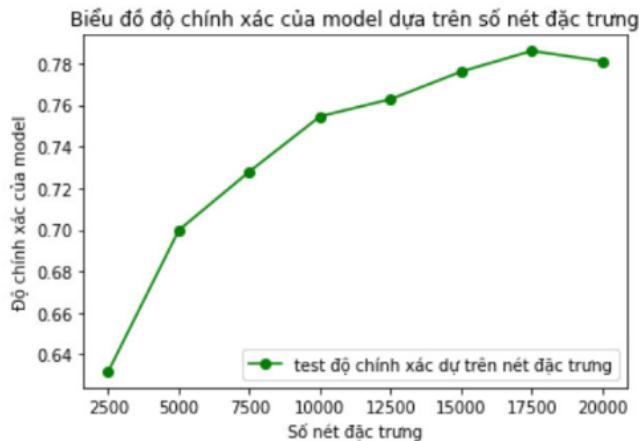
Bước 9: Thực hiện kiểm thử mô hình đã huấn luyện.

Bước 10: Xem kết quả sau khi kiểm thử mô hình.

Bước 11: Đánh giá mức độ chính xác của mô hình sau khi thực hiện kiểm thử mô hình.

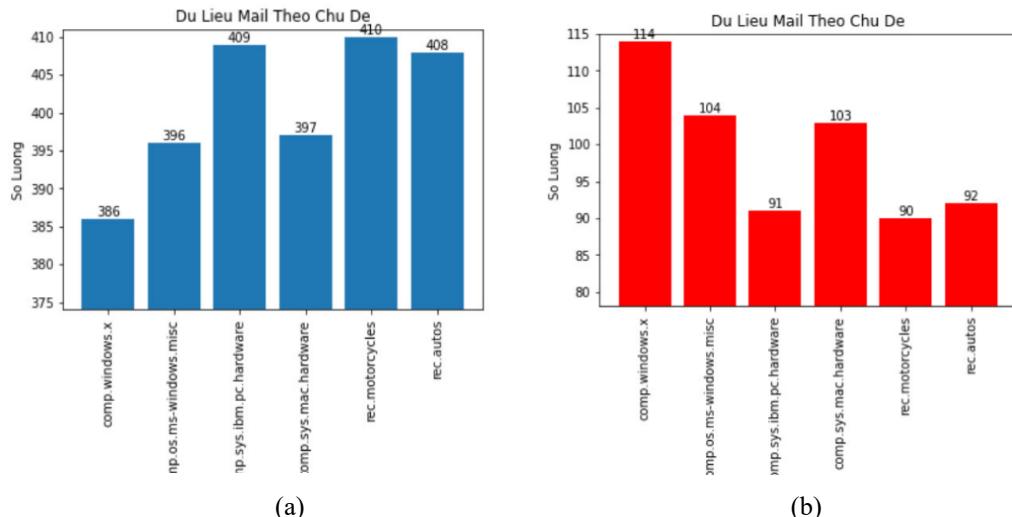
3. KẾT QUẢ THỰC NGHIỆM

Môi trường cài đặt: Thực nghiệm trên máy tính sử dụng VMWare Workstation 16 Pro, hệ điều hành Ubuntu 18.04, RAM 16GB, Internal Memory 512 GB, Chip Intel Core (TM) I7-4600M CPU @ 2.9 GHz, Ngôn ngữ lập trình Python 3.7.0.



Hình 1. Biểu đồ độ chính xác của model dựa trên số nét đặc trưng.

Thông kê dữ liệu phân loại mail theo 6 chủ đề với mỗi phân loại gồm 500 mail và tập dữ liệu được chia gồm tập huấn luyện và tập kiểm thử đều như kết quả Hình 2.



Hình 2. (a) Phân bố số lượng văn bản trong các chủ đề thuộc tập huấn luyện;
(b) Phân bố số lượng văn bản trong các chủ đề thuộc tập kiểm thử.

Kết quả thực nghiệm cho thấy độ chính xác của model sẽ đạt ngưỡng tốt nhất là 78% khi số nét đặc trưng khoảng 17500, nếu số nét đặc trưng vượt quá 17500 sẽ làm giảm độ chính xác của model theo Hình 1.

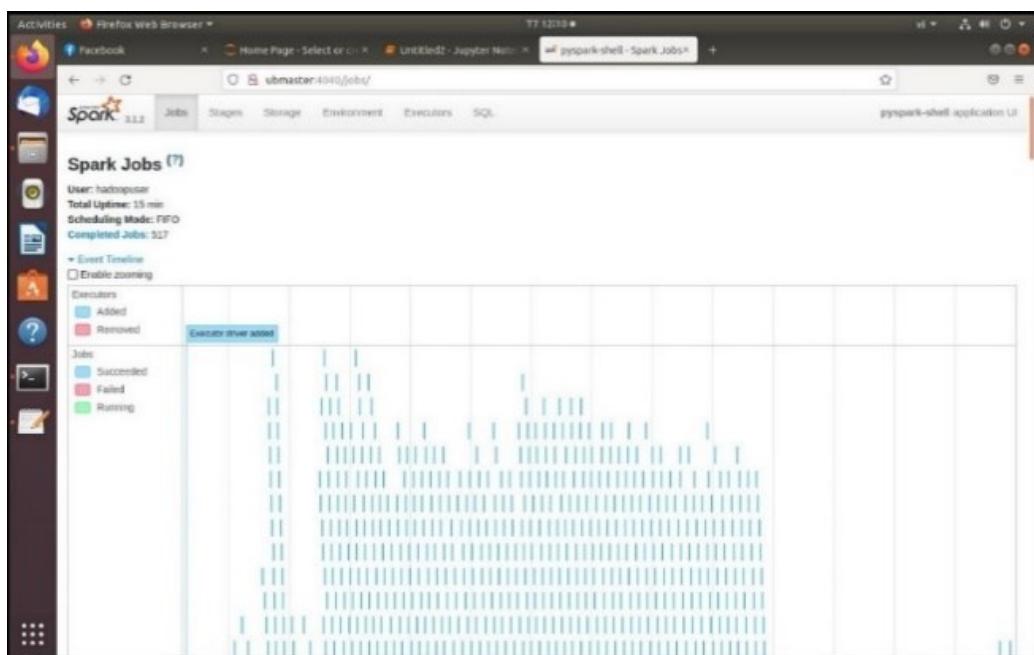
Sau nhiều lần thử nghiệm bằng cách chạy bài toán trên một máy tính và theo cách song song bằng Hadoop, kết quả cho thấy sự chênh lệch về thời gian chạy giữa hai phương pháp

không quá lớn, có thể do dữ liệu đầu vào của bài toán chưa đủ lớn. Kết quả cho thấy việc chạy bài toán bằng Hadoop mất khoảng 11 phút theo Hình 3b, trong khi đó chạy trên 1 máy tính mất khoảng 15 phút theo Hình 3a.

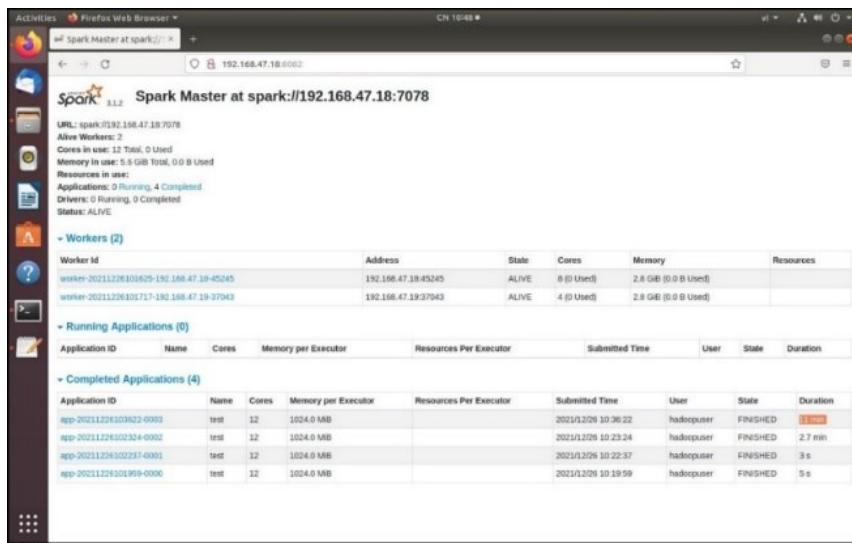
4. XÂY DỰNG ỦNG DỤNG PHÂN LOẠI MAIL

Ứng dụng phân loại mail cần tích hợp với hệ thống email của doanh nghiệp để có thể truy cập và quản lý hộp thư đến của các nhân viên. Ứng dụng cũng cần có tính năng phân loại email tự động dựa trên các tiêu chí như người gửi, chủ đề, nội dung và độ ưu tiên, đồng thời đánh giá tính khả dụng và tính bảo mật của email để giúp người dùng quyết định xử lý email theo các cách thức khác nhau. Để quản lý công việc liên quan đến email một cách dễ dàng, ứng dụng phân loại mail cần có khả năng tích hợp với các công cụ hỗ trợ quản lý công việc như Microsoft Outlook, Gmail. Ứng dụng cũng cần định dạng email để người dùng có thể dễ dàng đọc và phản hồi email một cách nhanh chóng và hiệu quả. Để cải thiện tính năng và hiệu quả của ứng dụng, nó cần tích hợp với các công nghệ mới nhất như trí tuệ nhân tạo, học máy, điện toán đám mây. Bên cạnh đó, ứng dụng phân loại mail cần đảm bảo tính bảo mật và quyền riêng tư cho người dùng bằng cách cung cấp các tính năng bảo mật như mã hóa dữ liệu, xác thực hai yếu tố và khả năng quản lý quyền truy cập cho các người dùng.

Chúng tôi đã phát triển một ứng dụng web phân loại mail cho doanh nghiệp bao gồm các trang chức năng như sau: trang chủ để gửi, cập nhật và phân loại email theo nhãn; trang quản lý mail cho từng nhãn và cho phép chuyển mail sang chủ đề khác khi thuật toán phát hiện sai; trang quản lý mail đã đọc; trang quản lý mail đã xóa và cung cấp tính năng khôi phục để phục hồi mail về nhãn phân loại theo Hình 3, trang cho phép người dùng soạn thư trả lời email theo Hình 4.



Hình 3. Kết quả khi chạy bài toán trên 1 máy tính



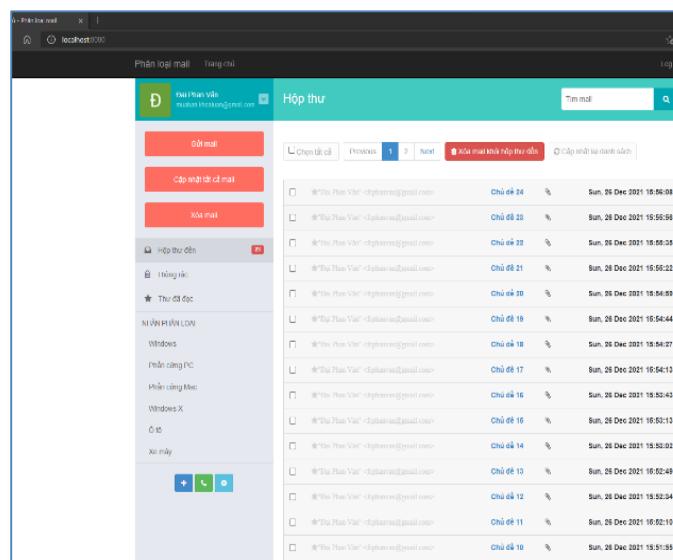
Hình 4. Chạy bài toán với Hadoop.

5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

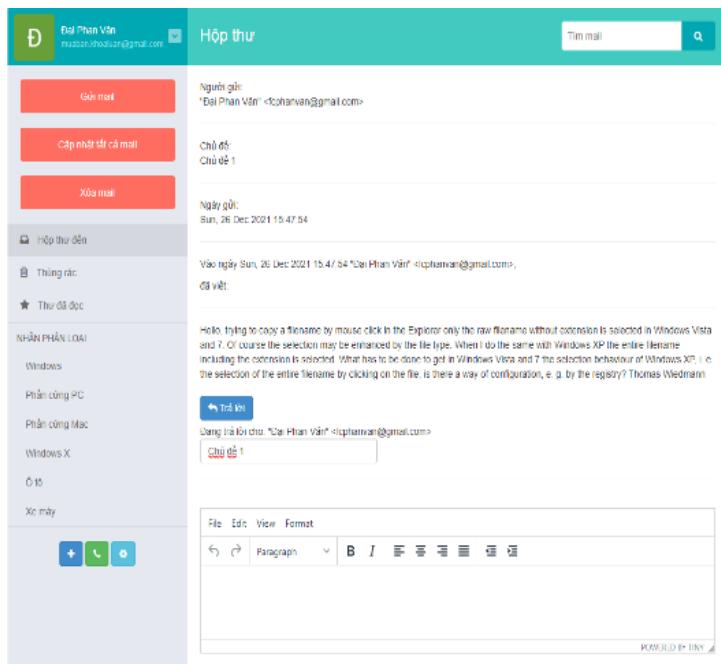
Chúng tôi xây dựng một pipeline trên Spark với ba node để huấn luyện mô hình phân loại dữ liệu mail bằng kỹ thuật hồi quy Logistic và phát triển ứng dụng phân loại mail cho doanh nghiệp, giúp cho việc quản lý hộp thư đến trở nên dễ dàng và hiệu quả hơn, đồng thời nâng cao năng suất làm việc của nhân viên.

Để cải thiện độ chính xác của bài toán, cần thu thập thêm nhiều và đa dạng hơn dữ liệu huấn luyện. Khi đó, model sẽ trở nên tổng quát hơn, phân loại và đánh giá dữ liệu chuẩn xác hơn.

Vì sử dụng API Google Gmail miễn phí, ứng dụng của chúng tôi có hạn chế về tính năng và cách sử dụng so với phiên bản Google Gmail thực tế. Tuy nhiên, để sử dụng đầy đủ chức năng của API, cần bỏ ra một khoản chi phí giúp ứng dụng có nhiều tính năng hơn và dễ sử dụng hơn trong đời sống.



Hình 5. Ứng dụng web phân loại mail cho doanh nghiệp;



Hình 6. Giao diện chức năng đọc thư.

TÀI LIỆU THAM KHẢO

1. Nick Pentreath - Machine Learning with Spark, Community Experience Distilled, 2015.
2. Kologlu M., Elker D., Altun H., and Sayek I. - Validation of MPI and PIA II in two different groups of patients with secondary peritonitis, Hepato-Gastroenterology 48 (37) (2001) 147-51.
3. Strano M. and Colosimo B. M. - Logistic regression analysis for experimental determination of forming limit diagrams, International Journal of Machine Tools and Manufacture 46 (6) (2006) 673-682.
4. Berry and Michael J. A. - Data Mining Techniques For Marketing, Sales and Customer Support. Wiley. (1997).
5. David A. Freedman - Statistical Models: Theory and Practice, Cambridge University Press (2009).
6. Harrell and Frank E. - Regression Modeling Strategies (2nd ed.), Springer-Verlag (2001).

ABSTRACT

BUILD A LOGISTIC ALGORITHM FOR CLASSIFYING EMAILS AND A PIPELINE MODEL IN SPARK

Nguyen Minh Hieu¹, Nguyen Trong Dang Khoa¹, Nguyen Van Tung¹, Ngo Duong Ha^{1,*}

¹*Ho Chi Minh City University of Food Industry*

*Email: hand@hufi.edu.vn

Business companies need to build a topic-based email classification system to solve the problem of a huge number of daily incoming emails, the risk of spam mail causing information disruption, and the potential existence of malicious software in emails that can affect the system and hinder company operations. To address this problem, we propose using the Logistic regression algorithm and conducting parallel experiments on Spark.

Keywords: Logistic regression, Spark, Hadoop, pipeline

ỨNG DỤNG KỸ THUẬT RESNET PHÂN LOẠI LÁ CÂY THUỐC CHỮA BỆNH GAN

Phạm Hoàng Hiệp¹, Trần Nhu Ý¹, Phan Thị Ngọc Mai^{*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email:maipn@huf.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Theo tổ chức Y tế thế giới WHO, tỷ lệ mắc ung thư gan ở Việt Nam đứng thứ ba trên thế giới. Trong số các loại ung thư, ung thư gan chiếm tỷ lệ cao nhất tại Việt Nam, gây ra hơn 25.000 trường hợp tử vong hàng năm, theo Hiệp hội Gan mật Việt Nam. Gan có nhiều vai trò quan trọng và thường tiếp xúc với các chất độc hại như hóa chất, virus, thực phẩm không đảm bảo, rượu bia, dẫn đến các bệnh lý về gan như gan nhiễm mỡ, viêm gan, xơ gan và ung thư gan. Mặc dù các loại thuốc tây y đã phát triển đột phá về công nghệ, nhưng việc kết hợp đông y và tây y vẫn mang lại giá trị cao trong điều trị bệnh gan. Việt Nam có nhiều loại dược liệu để điều trị bệnh gan bằng đông y. Tuy nhiên, hiện chưa có ứng dụng kết hợp thị giác máy tính và mạng nơ ron để phân loại các loại dược liệu điều trị bệnh gan. Trong bài báo này, chúng tôi sẽ thu thập bộ dữ liệu lá cây thuốc chữa bệnh gan, sử dụng kỹ thuật ResNet để xây dựng mô hình huấn luyện và đánh giá dữ liệu với độ chính xác 96%. Sau đó, mô hình sẽ được đưa vào thực tế giúp ích cho những người có nhu cầu tìm hiểu về dược liệu bệnh gan một cách thuận tiện hơn.

Từ khóa: Bệnh gan, Resnet, dược liệu

1. GIỚI THIỆU

1.1. Lá cây hỗ trợ điều trị bệnh gan

Việt Nam là một quốc gia nằm ở Đông Nam Á, với một vị trí địa lý đặc biệt và đầy tiềm năng về tài nguyên thiên nhiên. Với những đặc điểm về khí hậu, địa hình, đặc biệt là vùng đất chau thổ sông Hồng phù sa, Việt Nam đã từ lâu được biết đến với một hệ sinh thái phong phú và đa dạng, với hàng ngàn loài động thực vật phong phú đang sinh sống tại đây [1,2]. Trong số đó, cây thuốc được xem như một kho tàng của thiên nhiên với nhiều loại cây thuốc quý giá có tác dụng chữa bệnh và tăng cường sức khỏe. Để khai thác và sử dụng tối đa tài nguyên này, các nhà khoa học đã nghiên cứu và lựa chọn ra một số loại lá cây thuốc đặc biệt có tác dụng chữa bệnh gan.

Theo hình 1 và bảng 1 các loại cây thuốc này đều có những đặc điểm và tác dụng riêng, nhưng đều có tác dụng tốt trong việc hỗ trợ điều trị các bệnh liên quan đến gan. Việc phân loại và sử dụng chúng đúng cách sẽ mang lại hiệu quả cao trong việc chữa bệnh và bảo vệ sức khỏe. Cụ thể, chúng tôi chọn ra 14 lá cây thuốc này để thực hiện huấn luyện dữ liệu cho việc phân loại lá cây thuốc trị bệnh gan.



Hình 1. Mười bốn loại dược liệu hỗ trợ điều trị bệnh gan.

Bảng 1. Các loại lá cây thuốc hỗ trợ điều trị bệnh gan.

STT	Lá dược liệu	Tên khoa học	Công dụng	Hình
1	An xoa [3, 4]	<i>Helicteres hirsuta</i> Lour	Hỗ trợ điều trị ung thư gan, hỗ trợ điều trị viêm gan B, hỗ trợ điều trị xơ gan.	Hình 1.1
2	Đu đủ [5, 6]	<i>Carica papaya</i> L	Hỗ trợ điều trị ung thư gan	Hình 1.2
3	Xạ đen [7, 8]	<i>Celastrus hindsii</i> Benth et Hook	Hỗ trợ điều trị viêm gan A, B, C, gan nhiễm mỡ, xơ gan.	Hình 1.3
4	Cà gai leo [9, 10]	<i>Solanum hainanense</i> Hance	Hỗ trợ điều trị viêm gan, giải độc gan	Hình 1.4
5	Sam biển [11]	<i>Trianthema portulacastrum</i> L	Hỗ trợ điều trị bệnh gan vàng da	Hình 1.5
6	Thìa canh [12]	<i>Gymnema sylvestre</i> (Retz.) R.Br.ex Schult	Giảm nồng độ men gan	Hình 1.6
7	Sen [13]	<i>Nelumbo nucifera</i> Gaertn	Hỗ trợ điều trị gan nhiễm mỡ	Hình 1.7
8	Mã đề [14, 15]	<i>Plantago major</i> L	Hỗ trợ điều trị viêm gan cấp, mẩn tính	Hình 1.8
9	Oliu [16]	<i>Olea europaea</i> L	Hỗ trợ bảo vệ gan	Hình 1.9
10	Nghệ xanh [17]	<i>Curcuma aeruginosa</i> Roxb	Hỗ trợ điều trị gan lách sưng to	Hình 1.10
11	Trái mâm [18]	<i>Aegle marmelos</i> (L.) Correa	Hỗ trợ điều trị các bệnh về gan	Hình 1.11
12	Ngáy tía [19]	<i>Rubus parvifolius</i> L	Hỗ trợ điều trị viêm gan, gan lách sưng to	Hình 1.12
13	Ngô [20]	<i>Stigmata Maydis</i>	Hỗ trợ trị viêm gan với hiện tượng trớ ngài bài tiết mật	Hình 1.13
14	Dâu tằm [21]	<i>Morus alba</i> L	Hỗ trợ điều trị gan	Hình 1.14

1.2. Kỹ thuật ResNet-50

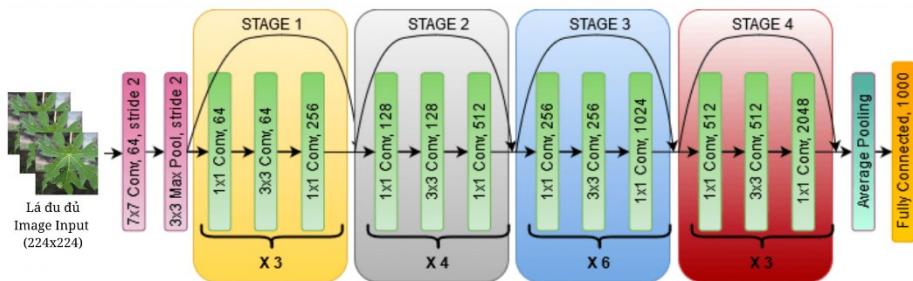
ResNet-50 là một trong những kiến trúc mạng nơ-ron sâu (deep neural network) nổi tiếng trong lĩnh vực computer vision. Nó được phát triển bởi các nhà nghiên cứu tại Microsoft Research vào năm 2015 và đã đạt được kết quả tốt trong các cuộc thi thi giác máy tính như ImageNet [22,23].

Kiến trúc ResNet-50 bao gồm 50 lớp (layers) và được thiết kế dựa trên kiến trúc mạng nơ-ron tích chập (convolutional neural network) với các lớp convolution, pooling và fully

connected. Tuy nhiên, điểm đặc biệt của ResNet-50 là việc sử dụng các residual block để giảm sự suy giảm độ chính xác khi mạng trở nên sâu hơn.

Mỗi residual block bao gồm 2 hoặc 3 lớp convolution, tùy thuộc vào việc sử dụng kích thước stride hay không. Trong đó, lớp convolution đầu tiên có kích thước kernel là 1x1, lớp convolution thứ hai có kích thước kernel là 3x3, và lớp convolution cuối cùng cũng có kích thước kernel là 1x1. Giá trị đầu vào của mỗi residual block sẽ được cộng với giá trị đầu ra của lớp convolution cuối cùng trong residual block, tạo thành một đường dẫn shortcut (skip connection) giúp cho các thông tin quan trọng được truyền qua các lớp mạng một cách nhanh chóng hơn.

Để giảm kích thước của đầu vào khi đi qua các lớp convolution, ResNet-50 sử dụng các lớp pooling với kích thước kernel là 3x3 và stride là 2. Cuối cùng, một số lớp fully connected được sử dụng để đưa ra dự đoán cuối cùng.



Hình 2. Kiến trúc mạng ResNet 50.

Hình 2 mô tả kiến trúc ResNet-50 với 4 giai đoạn và các thành phần như sau: Đầu tiên là một layer tích chập với kích thước kernel (7×7) và 64 kernel khác nhau, tất cả đều có kích thước Stride = 2, sau đó là một layer Max pooling (3×3) với kích thước Stride = 2. Trong Stage 1, có 3 residual block với mỗi block chứa 3 lớp, kích thước kernel dùng để thực hiện phép tích chập ở cả 3 lớp của mỗi block là ($1 \times 1, 64$), ($3 \times 3, 64$), ($1 \times 1, 256$). Mũi tên cong thể hiện kết nối nhận dạng và mũi tên nét đứt thể hiện tích chập trong residual block được thực hiện với Stride = 2, nên Stage 1 có tổng cộng 9 layer. Tương tự, trong Stage 2, có 4 residual block với mỗi block chứa 3 lớp, kích thước kernel dùng để thực hiện phép tích chập ở cả 3 lớp của mỗi block là ($1 \times 1, 128$), ($3 \times 3, 128$), ($1 \times 1, 512$). Stage 2 có tổng cộng 12 layer. Trong Stage 3, có 6 residual block với mỗi block chứa 3 lớp, kích thước kernel dùng để thực hiện phép tích chập ở cả 3 lớp của mỗi block là ($1 \times 1, 256$), ($3 \times 3, 256$), ($1 \times 1, 1024$). Stage 3 có tổng cộng 18 layer. Cuối cùng, trong Stage 4, có 3 residual block với mỗi block chứa 3 lớp, kích thước kernel dùng để thực hiện phép tích chập ở cả 3 lớp của mỗi block là ($1 \times 1, 512$), ($3 \times 3, 512$), ($1 \times 1, 2048$). Stage 4 có tổng cộng 9 layer. Sau đó là một layer average pooling và một layer fully connected chứa 1000 nơ-ron. Kiến trúc này sử dụng nút cỗ chai cho các mạng sâu hơn như ResNet 50, ResNet 152,... Với mỗi residual hàm F, ba lớp được xếp chồng nhau, bao gồm các lớp tích chập 1x1 để giảm và sau đó khôi phục kích thước và lớp 3x3 dưới dạng nút cỗ chai với kích thước đầu vào/đầu ra nhỏ hơn.

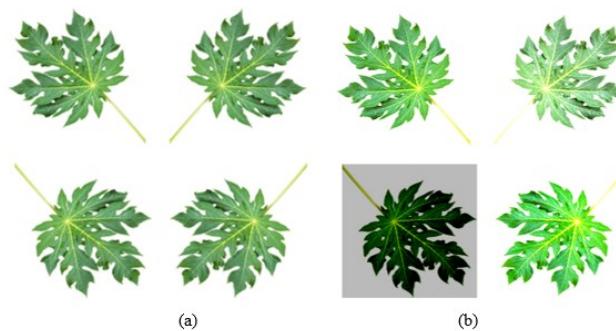
Tóm lại, ResNet-50 là một kiến trúc mạng nơ-ron sâu sử dụng các residual block để giảm sự suy giảm độ chính xác khi mạng trở nên sâu hơn. Nó đã đạt được kết quả tốt trong các bài toán thị giác máy tính và được sử dụng rộng rãi trong các ứng dụng thực tế.

2. XÂY DỰNG THỰC NGHIỆM

2.1. Thu thập và xử lý dữ liệu

Dựa vào các tài liệu và sách y dược, chúng tôi đã tiến hành thu thập dữ liệu từ nhiều nguồn khác nhau, bao gồm việc chụp ảnh tại các khu bảo tồn thực vật, nhà thuốc nam, vườn ruộng và thu thập hình ảnh từ các nguồn internet đáng tin cậy. Qua quá trình thu thập, chúng tôi đã có được một bộ dữ liệu đa dạng với 14 loại dược liệu được sử dụng để ngăn ngừa, hỗ trợ và điều trị bệnh gan, đảm bảo tính chính xác và đầy đủ của dữ liệu thu thập.

Sau khi hoàn tất quá trình thu thập dữ liệu, chúng tôi đã tiến hành sử dụng các kỹ thuật tiền xử lý ảnh và chỉnh sửa ảnh để đạt được kích thước chuẩn 224x224, đảm bảo rằng tất cả các hình ảnh trong bộ dữ liệu đều có cùng kích thước và chất lượng tốt hơn. Tuy nhiên, do bộ dữ liệu về dược liệu có hạn chế về số lượng ảnh, chúng tôi đã sử dụng các kỹ thuật tăng cường dữ liệu để mở rộng bộ dữ liệu và đảm bảo tính đa dạng của nó như hình 3. Cụ thể, chúng tôi đã áp dụng các kỹ thuật lật ảnh, xoay ảnh và chuyển đổi màu sắc để tạo ra thêm các biến thể của từng ảnh trong bộ dữ liệu. Như vậy, bộ dữ liệu đã được tiền xử lý và tăng cường dữ liệu để đảm bảo tính đầy đủ và chất lượng của nó trong việc thực hiện các công việc phân loại dược liệu và tìm kiếm các sản phẩm thuốc mới trong lĩnh vực y học.



Hình 3. Tăng cường dữ liệu lật ảnh (a) và tăng cường dữ liệu chỉnh độ sáng tối (b).

Đến thời điểm hiện tại, chúng tôi đã thu thập được một bộ dữ liệu đáng kể với 14 loại dược liệu khác nhau. Mỗi loại lá thuốc được lựa chọn bao gồm từ 100 đến 300 tấm ảnh với các góc độ chụp và ánh sáng khác nhau, để đảm bảo tính đa dạng và đầy đủ của dữ liệu. Sau khi tổng hợp và phân tích, chúng tôi đã có kết quả chi tiết được liệt kê trong bảng 2, mang lại giá trị quan trọng cho việc phát triển mô hình phân loại lá thuốc trị bệnh gan.

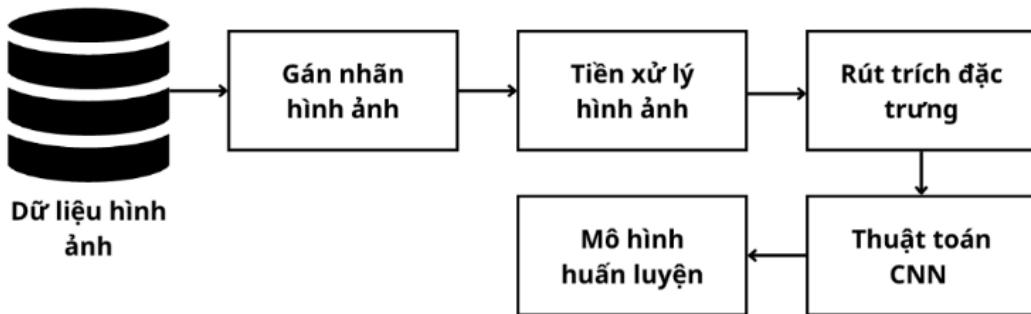
Bảng 2. Dữ liệu lá cây thuốc hỗ trợ điều trị bệnh gan.

STT	Tên lá dược liệu	Số lượng ảnh từng loại
1	An Xoa	229
2	Cà gai leo	209
3	Mã đê	245
4	Sam biển	281
5	Xạ đen	183
6	Dây thià canh	144
7	Đu đủ	202
8	Dâu tằm	210
9	Ô liu	344
10	Sen	269
11	Ngây tía	228

STT	Tên lá dược liệu	Số lượng ảnh từng loại
12	Nghệ xanh	217
13	Ngô	203
14	Trái mầm	212
Tổng		3176

2.2. Mô hình thuật toán

Mô hình huấn luyện bằng thuật toán ResNet50 là một trong những phương pháp được sử dụng phổ biến trong lĩnh vực deep learning để giải quyết các vấn đề nhận dạng hình ảnh. Với kiến trúc mạng sâu sử dụng khoảng 50 tầng, ResNet50 có khả năng học và trích xuất đặc trưng của hình ảnh một cách hiệu quả hơn so với các phương pháp truyền thống. Quy trình huấn luyện mô hình ResNet50 được thể hiện trong hình 4.



Hình 4. Quy trình huấn luyện dữ liệu phân loại lá cây trị bệnh gan.

Thuật toán phân loại lá cây thuộc trị bệnh gan theo thuật toán 1.

Thuật toán 1: Phân loại lá cây thuộc bằng ResNet50

Input: Tập dữ liệu 14 loại lá cây thuộc với 3176 lá cây (224x224)

Output: Phân loại lá cây thuộc

Bước 1: Đọc đường dẫn chứa thư mục dữ liệu ảnh.

Bước 2: Chia tập dữ liệu đã đọc thành hai phần là tập dataset và tập test với tỉ lệ 90/10 sử dụng thư viện Keras với `image_dataset_from_directory`.

Bước 3: Định nghĩa một hàm tăng cường dữ liệu. Dùng lambda để map dataset đã tạo từ Bước 2 với hàm tăng cường dữ liệu đã được định nghĩa. Sau đó chia tập dữ liệu dataset thành hai phần training và validation với tỉ lệ 80/20.

Bước 4: Tạo một mảng chứa tên của các loại thảo dược.

Bước 5: Tạo model ResNet50 với trọng số của imagenet và bắt đầu việc huấn luyện model.

Bước 5.1: Thu thập và tiền xử lý dữ liệu trước khi tiến hành học chuyển giao.

Bước 5.2: Khởi tạo mô hình cơ sở và tải các trọng số đã được đào tạo trước vào đó.

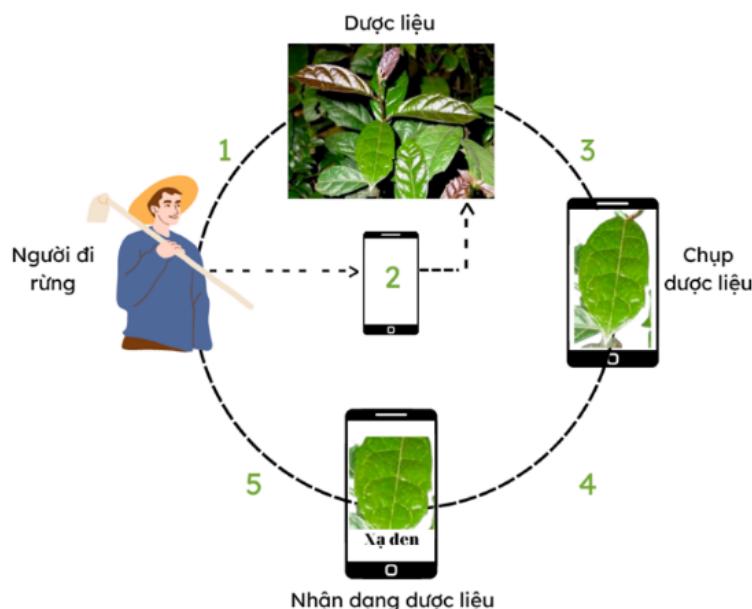
Bước 5.3: Cố định tất cả các lớp trong mô hình cơ sở bằng cách đặt `trainable = False`.

Bước 5.4: Tạo một mô hình mới trên đầu ra của một (hoặc một số) lớp từ mô hình cơ sở.

Bước 5.5: Đào tạo mô hình mới của mình trên tập dữ liệu mới.

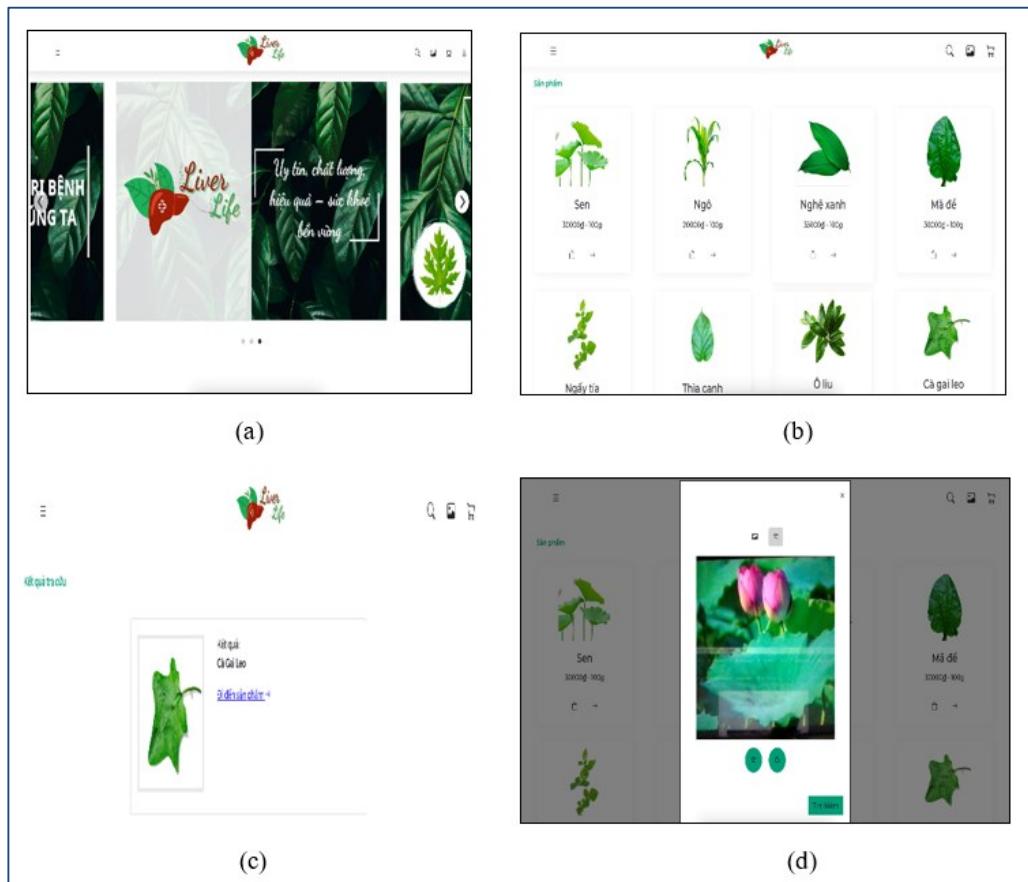
2.3. Xây dựng ứng dụng

Quy trình người đi rừng nhận dạng dược liệu lá cây thuốc bắt đầu bằng việc tìm kiếm các vùng rừng hoặc khu vực có dược liệu tiềm năng, sau đó thu thập các mẫu lá cây và tiến hành phân loại, xác định các đặc điểm quan trọng trên lá cây như hình dạng, kích thước, màu sắc và cấu trúc của lá. Sau đó, người đi rừng sử dụng các phương pháp nhận dạng dược liệu lá cây thuốc như so sánh với các bộ sưu tập hình ảnh đã có, sử dụng các công cụ hỗ trợ như máy tính, điện thoại di động và các ứng dụng nhận dạng lá cây để xác định tên của cây thuốc và thu thập thông tin về các tính chất, đặc tính và ứng dụng của nó theo hình 5.



Hình 5. Quy trình người đi rừng nhận dạng dược liệu

Chúng tôi đã phát triển một ứng dụng bán lá cây thuốc trị bệnh, trong đó ứng dụng phân loại lá cây thuốc được tích hợp vào mục tìm kiếm hình ảnh. Để phát triển ứng dụng này, chúng tôi đã sử dụng mô hình học sâu ResNet50 để phân loại dược liệu lá cây thuốc một cách chính xác. Với ứng dụng này, người dùng có thể tìm kiếm và mua các loại lá cây thuốc trị bệnh cần thiết một cách dễ dàng và thuận tiện hơn. Ứng dụng này được thực hiện qua nhiều chức năng trong đó một số chức năng quan trọng được trình bày tại hình 6.

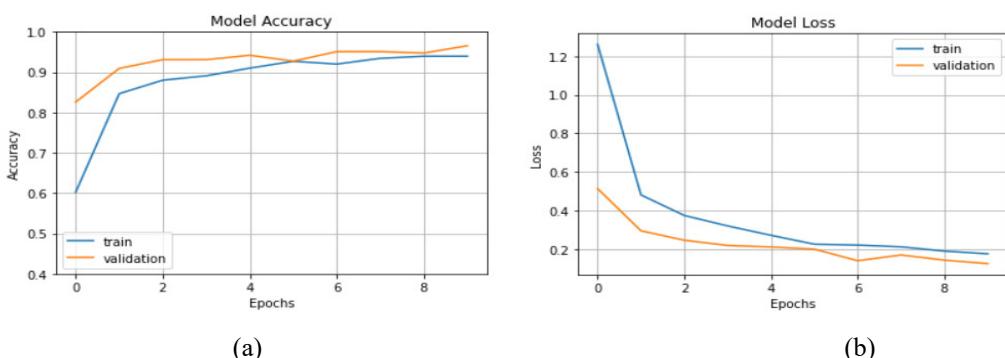


Hình 6. Chức năng trang chủ (a), Chức năng trang hiển thị sản phẩm (b),
Chức năng trang hiển thị sau khi tìm kiếm sản phẩm load bằng file (c)
và Chức năng trang tìm kiếm ảnh theo nhận dạng chụp từ camera (d).

3. KẾT QUẢ VÀ THẢO LUẬN

Sau khi huấn luyện nhiều lần chúng tôi quyết định chọn số lần lặp là 10. Sau đây là một số thống kê:

- Tổng dữ liệu lá cây thuốc là 3173 image
- Tập train = 2284 image
- Tập validation = 572 image
- Tập test = 317 image



Hình 7. Kết quả độ chính xác (a) và độ lỗi (b) trong quá trình huấn luyện phân loại lá cây thuộc.

Biểu đồ thể hiện độ chính xác sau 10 lần thông qua tập validation cho thấy tỷ lệ chính xác khoảng 97%. Biểu đồ đo độ lỗi qua 10 lần thông qua tập validation, ta có thể thấy tỷ lệ chính xác của hàm matsu mít rơi vào khoảng 0.5. Kết quả đánh giá mô hình với tập test cho độ chính xác 96% theo bảng 3.

Bảng 3. Kết quả so sánh đánh giá model ResNet50 và VGG16 trên tập test và tập huấn luyện.

Thuật toán	Accuracy_train	Accuracy_test
ResNet-50	96.56%	95.88%
VGG16	91.12%	89.91%

Trong quá trình huấn luyện 2 model ResNet-50 và VGG16, chúng tôi đều cho 2 thuật toán chạy với epoch = 10, tốc độ học lr = 0.0001, batch_size = 32, bộ dữ liệu chia theo tỉ lệ train/validations là 80/20. Sau khi, tinh chỉnh huấn luyện lại 2 model thì thấy rằng độ chính xác của thuật toán ResNet-50 có độ chính xác được cải thiện hơn thuật toán VGG16.

4. KẾT LUẬN

Mặc dù mô hình này có khả năng nhận diện lá cây tốt với các ảnh rõ nét và chụp trực diện vào cây, tuy nhiên khi đối mặt với các ảnh có nhiều loài cây khác nhau và khoảng cách chụp xa, độ chính xác của nó giảm đáng kể và có thể dẫn đến nhận diện sai.

Để nâng cao độ chính xác của bài toán, cần có một bộ dữ liệu ảnh đa dạng và phong phú hơn để mô hình có thể học được nhiều trường hợp và tổng quát hơn. Việc sử dụng một bộ dữ liệu đầy đủ và đáng tin cậy là rất quan trọng trong việc nhận dạng và đánh giá dữ liệu chuẩn xác của các loài cây thuộc thông qua mô hình Resnet.

Dữ liệu hình ảnh được sử dụng trong bài toán hiện tại chủ yếu được thu thập từ các nguồn trên internet, do đó độ phân giải và góc chụp của ảnh chưa được đầy đủ và đa dạng. Điều này dẫn đến sự thiếu ổn định và đa dạng trong số lượng góc chụp của các loài cây. Để cải thiện hiệu quả của bài toán, cần phải dành thêm thời gian và tìm cách tiếp cận để chụp trực tiếp các loài cây thuộc, từ đó có thể đảm bảo sự ổn định và đa dạng hơn trong bộ dữ liệu.

Ngoài việc sử dụng dữ liệu đa dạng để nâng cao độ chính xác của mô hình, cần phải áp dụng các phương pháp phân loại và xác định các đặc trưng của các loài cây một cách chính xác hơn. Một trong những phương pháp đó là lựa chọn và lọc các đặc trưng của các loài cây và loại bỏ các hình ảnh nhiễu xung quanh. Việc giới hạn phạm vi học tập của mô hình như vậy sẽ giúp tăng độ chính xác cho các lần phân loại sau.

TÀI LIỆU THAM KHẢO

1. Link online: <https://dangcongsan.vn/khuyen-nong-huong-toi-su-phat-trien-ben-vung/tin-tuc/khoi-day-tiem-nang-lon-tu-cay-duoc-lieu-tai-viet-nam-277397.html>
2. Chi V. V. - Từ điển cây thuốc Việt Nam, tập 1, 2. NXB Y học, (2012).
3. Duyên N. H. - Khảo sát thành phần hóa học và hoạt tính gây độc té bào Hep-G2 của cây An Xoa (*Helicteres hirsuta* L.). Tạp chí Khoa học Trường Đại học Cần Thơ, (47), (2016) 93-97.
4. Nguyễn T. N. and Nguyễn T. Q. - Sơ bộ nghiên cứu thành phần hóa học và tác dụng úc ché một số dòng té bào ung thư của cây an xoa (*helicteres hirsuta loureiro*) trên thực nghiệm (2016).
5. Zetina-Esquivel A. M., Tovilla-Zárate C. A., Guzmán-Garcia C., Rodríguez-Hernández A., Castell-Rodríguez A. E., Ble-Castillo J. L., Díaz-Zagoya J. C.. - Effect of *Carica papaya* leaf extract on serum lipids and liver metabolic parameters of rats fed a high cholesterol diet. Health, 7(09), (2015) 1196-1205.
6. Pandit A., Sachdeva T. and Bafna P. - Ameliorative effect of leaves of *Carica papaya* in ethanol and antitubercular drug induced hepatotoxicity. Br J Pharm Res, 3, (2013) 648-61.
7. Link online: <https://caythuoc.org/cach-dung-cay-xa-den-pha-nuoc-uong-hang-ngay.html>
8. Trang D. T. X., Minh N. T. T., Duy N. H., Linh T. C. and Ngân P. N. T. - Tối ưu hóa quy trình ly trích cao chiết lá xạ đen (*Celastrus hindsii*) giàu polyphenol, flavonoid có hoạt tính kháng oxy hóa và kháng đái tháo đường in vitro. Tạp chí Khoa học Trường Đại học Cần Thơ, 58(CĐ Khoa học tự nhiên), (2022) 48-58.
9. Hải N. X., Nhân N. T. and Mai N. T. T. - Thành phần hoá học của cây Cà gai leo (*Solanum procumbens*). Tạp chí phát triển khoa học và công nghệ, 2(6), (2018) 134-138.
10. Huỳnh T. T. H., Nguyễn T. T. H., Lê T. T. H. and Nguyễn Đ. T. - Phân tích vùng gen *trnL-trnF* trên cây cà gai leo (*Solanum Procumbens Lour.*) của Việt Nam. Tạp chí Công nghệ sinh học 19(2): (2021) 309-319
11. Kumar G., Banu G. S. and Pandian M. R.. - Evaluation of the antioxidant activity of *Trianthema portulacastrum* L. Indian journal of pharmacology, 37(5), (2005) 331.
12. Link online: <https://suckhoedoisong.vn/ung-dung-day-thia-canhh-trong-san-xuat-sua-cho-nguo-tieu-duong-169190794.htm>
13. Bùi T. T., Phạm M. H., Lê P. T. and Hoàng N. H. - Đặc điểm hình thái gan chuột nhiễm mõ sau uống nước lá sen. Tạp chí Y học Việt Nam, 502(1) (2021).
14. Hussan F., Mansor A. S., Hassan S. N., Kamaruddin T. N. E., Tasnim T. N., Budin S. B. and Othman F. - Anti-inflammatory property of *Plantago major* leaf extract reduces the inflammatory reaction in experimental acetaminophen-induced liver injury. Evidence-Based Complementary and Alternative Medicine, 2015.
15. Link online: <https://tracuuduoclieu.vn/ma-de.html>
16. Hoseinifar S. H., Shakouri M., Yousefi S., Van Doan H., Shafiei S., Yousefi M. and Faggio C. - Humoral and skin mucosal immune parameters, intestinal immune related genes expression and antioxidant defense in rainbow trout (*Oncorhynchus mykiss*) fed olive (*Olea europaea* L.) waste. Fish & shellfish immunology, 100, (2020) 171-178.

17. Suphrom N., Pumthong G., Khorana N., Waranuch N., Limpeanchob N. and Ingkaninan K. - Anti-androgenic effect of sesquiterpenes isolated from the rhizomes of Curcuma aeruginosa Roxb. Fitoterapia, 83(5), (2012) 864-871.
18. Singanan V., Singanan M. and Begum H. - The hepatoprotective effect of bael leaves (Aegle marmelos) in alcohol induced liver injury in albino rats. International Journal of Science & Technology, 2(2), (2007) 83-92.
19. Gao J., Sun C. R., Yang J. H., Shi J. M., Du Y. G., Zhang Y. Y. and Wan H. T. -Evaluation of the hepatoprotective and antioxidant activities of Rubus parvifolius L. Journal of Zhejiang University SCIENCE B, 12(2), (2011) 135-142.
20. Bai H., Hai C., Xi M., Liang X. and Li, R. - Protective effect of maize silks (Maydis stigma) ethanol extract on radiation-induced oxidative stress in mice. Plant foods for human nutrition, 65, (2010) 271-276
21. Katsume T., Yamasaki M., Shiwaku K., Ishijima T., Matsumoto I., Abe K., and Yamasaki Y. - Effect of flavonol glycoside in mulberry (*Morus alba L.*) leaf on glucose metabolism and oxidative stress in liver in diet-induced obese mice. Journal of the Science of Food and Agriculture, 90(14), (2010) 2386-2392.
22. Link online: <https://datagen.tech/guides/computer-vision/resnet-50/>
23. He K, Zhang X, Ren S and Sun J. - Deep Residual Learning for Image Recognition, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 2016, pp. (2016) 770-778.

ABSTRACT

THE APPLICATION OF RESNET FOR CLASSIFYING MEDICINAL LEAVES FOR LIVER DISEASE TREATMENT

Pham Hoang Hiep¹, Tran Nhu Y¹, Phan Thi Ngoc Mai^{1*}

¹*Ho Chi Minh City University of food industry*

*Email: maiptn@hufi.edu.vn

According to the statistics of the World Health Organization (WHO), the rate of liver cancer in Vietnam ranks third in the world. According to the Vietnamese Hepatology Association, liver cancer is the most common type of cancer in Vietnam, causing more than 25,000 deaths annually. The liver plays a crucial role and is often exposed to harmful factors such as toxic chemicals, unsafe food, viruses, alcohol, and more, which can lead to liver diseases over time, such as fatty liver, hepatitis, cirrhosis, and even liver cancer. Nowadays, Western medicine has made breakthroughs in technology, but the value of traditional medicine cannot be denied. There are still diseases that require a combination of Eastern and Western medicine. Vietnam has many medicinal plants that can be used in combination with traditional medicine to treat liver diseases. Currently, there is no computer vision application or neural network to classify medicinal leaves for liver disease treatment. In this paper, we collected a dataset of medicinal leaves for liver disease treatment and use the ResNet technique to build a training model and evaluate the data with an accuracy of 96%. Subsequently, the model will be put into practical use to help those who need to learn about liver disease medicinal herbs more conveniently.

Keywords: liver disease, Resnet, herbal medicine

XÂY DỰNG HỆ THỐNG XỬ LÝ TIẾN TRÌNH KHÓA LUẬN TỐT NGHIỆP

Phạm Tấn Thuận¹, Vũ Trần Minh Hoàng¹, Ngô Văn Sơn¹,
Nguyễn Ngọc Thạch¹, Trần Văn Thọ^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: thotv@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Tiến trình khóa luận tốt nghiệp là quá trình khoa quản lý danh sách sinh viên, giảng viên và đề tài của một đợt khóa luận tốt nghiệp. Trong bài báo này, chúng tôi đề xuất xây dựng một hệ thống để xử lý tiến trình khóa luận tốt nghiệp. Hệ thống này sẽ hỗ trợ đơn vị khoa trong quản lý giảng viên, sinh viên, đề tài. Ngoài ra, hệ thống còn giúp nâng cao chất lượng đề tài, giảm thiểu sai sót, thời gian trong quá trình đăng ký đề tài của sinh viên. Tăng khả năng tương tác giữa giảng viên và sinh viên giúp cho kết quả khóa luận của sinh viên đạt kết quả tốt hơn.

Từ khóa: Khóa luận tốt nghiệp, xử lý tiến trình khóa luận, hệ thống xử lý tiến trình khóa luận.

1. MỞ ĐẦU

Đại học hiện nay là một môi trường đào tạo nguồn nhân lực có trí thức chính cho nước ta. Việc học tập để đạt điểm số cao trong các môn học ở trường là điều quan trọng và cần thiết đối với mỗi sinh viên. Tuy nhiên, để được công nhận tốt nghiệp, cũng như xác định được rằng sinh viên đã thật sự học tập và tổng hợp đủ lượng kiến thức chuyên môn thì cần phải thực hiện một đề tài gọi là khóa luận tốt nghiệp dưới sự hướng dẫn của ít nhất một giảng viên. Ngoài ra, khóa luận tốt nghiệp còn là một cột mốc quan trọng đối với sinh viên và có thể là một khởi đầu đối với những sinh viên theo con đường khoa học. Việc một sinh viên đăng ký đề tài khóa luận tốt nghiệp là một phần của tiến trình khóa luận tốt nghiệp được quản lý bởi đơn vị chuyên môn là khoa.

Tại trường Đại học Công nghiệp Thực Phẩm TP. Hồ Chí Minh, cụ thể là khoa Công nghệ thông tin hiện đang xử lý tiến trình khóa luận tốt nghiệp một cách thủ công, chưa có phần mềm nào hỗ trợ. Điều này dẫn tới rất nhiều khó khăn trong vấn đề kiểm duyệt chất lượng đề tài của trưởng bộ môn và trưởng khoa, trong quá trình đăng ký đề tài của sinh viên, khó khăn cho giảng viên trong giám sát tiến độ thực hiện đề tài của sinh viên và nhiều vấn đề khác. Thực tế, vừa qua tại khoa Công nghệ thông tin đã xảy ra tình trạng 1 nhóm sinh viên đăng ký nhiều hơn 1 đề tài làm do giáo vụ khoa phải mất thời gian kiểm tra và xóa những nhóm sinh viên đó.

Trong bài báo này nhóm tác giả đề cập đến vấn đề xây dựng một hệ thống xử lý tiến trình khóa luận tốt nghiệp để giải quyết các vấn đề bất cập hiện tại bằng cách bám theo 6 quy trình cơ bản: quản lý sinh viên tham gia khóa luận, ra đề tài và kiểm duyệt chất lượng của đề tài, đăng ký đề tài khóa luận tốt nghiệp, quản lý tiến độ thực hiện đề tài, chấm điểm đề tài, thống kê và kết xuất kết quả cuối cùng. Hệ thống được đề xuất sẽ giải quyết các vấn đề: tiết kiệm chi phí quản lý cho khoa; thuận lợi cho việc quản lý của khoa, giảng viên và sinh viên;

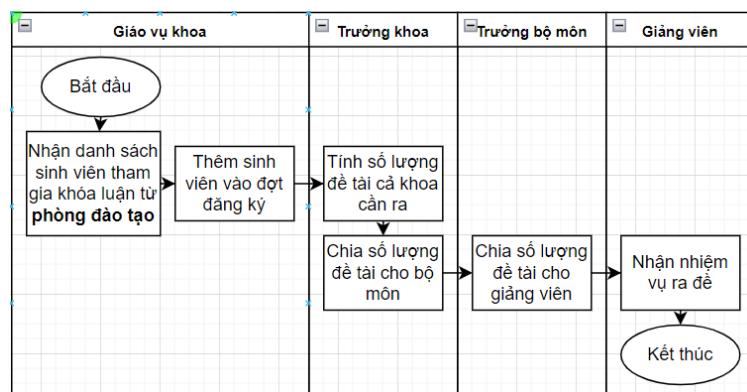
nâng cao chất lượng đề tài, trình độ sinh viên; rút ngắn thời gian và giảm thiểu rủi ro trong quá trình đăng ký đề tài.

2. PHƯƠNG PHÁP NGHIÊN CỨU

Tiến trình khóa luận tốt nghiệp có thể chia làm 6 phần và nó trải dài trong cả một học kỳ, cần sự theo dõi và kiểm tra để yêu cầu đề tài phù hợp với trình độ chuyên môn của sinh viên trong khâu ra đề tài, phê duyệt đề tài, và giảng viên kịp thời hỗ trợ sinh viên trong quá trình thực hiện.

2.1. Quản lý sinh viên tham gia khóa luận và tính số lượng đề tài

Đến mỗi đợt đăng ký khóa luận tốt nghiệp, sinh viên sẽ đăng ký tham gia trên cổng thông tin sinh viên. Khoa sẽ nhận danh sách những sinh viên tham gia khóa luận của một đợt đăng ký từ phòng đào tạo và tiến hành tính toán số lượng đề tài hợp lý dựa trên số lượng sinh viên đã đăng ký. Từ số lượng đề tài của cả khoa sẽ phân bổ nhiệm vụ xuống từng bộ môn và giảng viên cho phù hợp.



Hình 1. Quy trình quản lý sinh viên tham gia khóa luận và tính số lượng đề tài

THÊM SINH VIÊN VÀO ĐỢT ĐĂNG KÝ MỚI

Tất cả	2022-2023 ^ Đợt 1	Thêm sinh viên		
Mã SV	Họ và tên	Lớp	Chuyên ngành	Tất cả
2001200004	PHẠM NGUYỄN HUYỀN TRẦN	11DHTH1	Mạng máy tính	<input checked="" type="checkbox"/>
2001200011	TRẦN THANH BÌNH	11DHTH1	Công nghệ phần mềm	<input checked="" type="checkbox"/>
2001200016	VƯƠNG CHÍ HẢI	11DHTH1	Công nghệ phần mềm	<input type="checkbox"/>
2001200025	LÊ THỊ NGỌC ÁNH	11DHTH3	Khoa học phân tích dữ liệu	<input checked="" type="checkbox"/>
2001200093	NGUYỄN TẤN PHÁT	11DHTH2	An toàn thông tin	<input type="checkbox"/>
2001200110	NGÔ THỊ KIM NGÂN	11DHTH1	An toàn thông tin	<input type="checkbox"/>
2001200123	NGUYỄN MINH HÒA	11DHTH4	Công nghệ phần mềm	<input checked="" type="checkbox"/>
2001200130	LÊ MINH PHÁT	11DHTH1	Hệ thống thông tin	<input checked="" type="checkbox"/>
2001200145	CAO THIEN PHÚ	11DHTH2	Công nghệ phần mềm	<input type="checkbox"/>

Hình 2. Thêm sinh viên vào đợt đăng ký trên hệ thống

Tiêu đề kế hoạch
Ra đề khóa luận tốt nghiệp Bộ môn Hệ thống thông tin - Đợt 1

File đính kèm:
 No file chosen

BỘ CỘNG HƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP
THỰC PHẨM THÀNH PHỐ HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

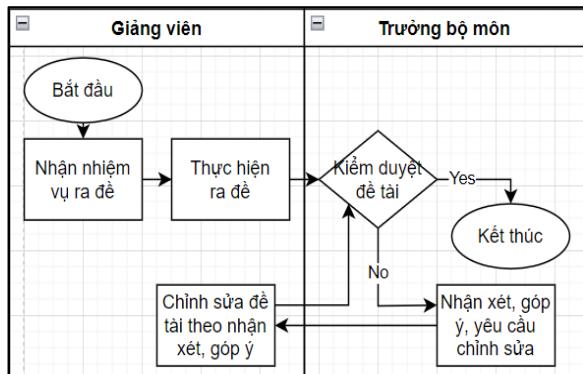
DANH SÁCH SINH VIÊN KHÓA 09 ĐẠI HỌC CHÍNH QUY
NGÀNH CÔNG NGHỆ THÔNG TIN - KHOA CÔNG NGHỆ THÔNG TIN
THAM GIA LÀM KHOA LUẬN TỐT NGHIỆP NĂM HỌC 2021 - 2022

(Bản hành kèm theo Quyết định số: QĐ-DCT, ngày tháng năm 2022 của
Hiệu trưởng trường Đại học Công nghiệp Thực phẩm thành phố Hồ Chí Minh).

Hình 3. Lên kế hoạch ra đề cho bộ môn trên hệ thống

2.2. Ra đề và kiểm duyệt chất lượng đề tài

Khi nhận được nhiệm vụ ra đề tài, giảng viên sẽ thực hiện việc ra đề ngay trên hệ thống, đồng thời trưởng bộ môn và đồng nghiệp có thể xem, góp ý chỉnh sửa nội dung cho phù hợp với chương trình đào tạo. Điều này sẽ góp phần nâng cao chất lượng của đề tài. Tại mỗi đề tài, giảng viên ra đề sẽ xác định chuyên ngành phù hợp có thể cho phép sinh viên thực hiện đề tài, việc này sẽ tránh được rủi ro đăng ký nhầm của sinh viên.



Hình 4. Quy trình ra đề và kiểm duyệt đề tài

Hệ thống quản lý phản ánh vi phạm nội quy của sinh viên HUFI.

Mã đề tài: CNT1000003

Giảng viên ra đề: Phan Thị Ngọc Mai

Chuyên ngành phù hợp: Công nghệ phần mềm

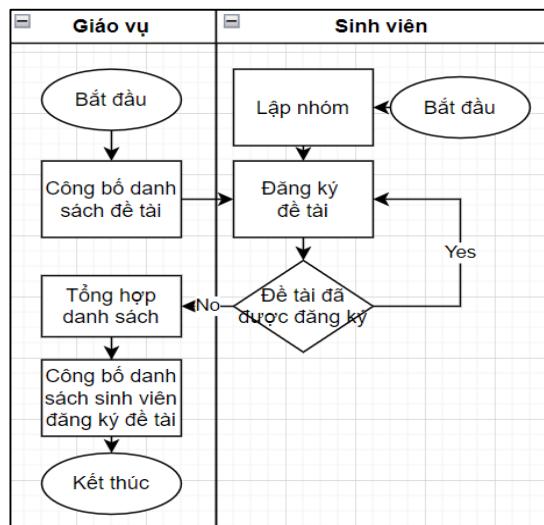
Số lượng sinh viên phù hợp: 2 -> 3

Trạng thái duyệt đề tài: Chưa duyệt

Hình 5. Góp ý và kiểm duyệt đề tài trên hệ thống

2.3. Đăng ký đề tài

Hiện tại, khi tới đợt đăng ký khóa luận tốt nghiệp thì khoa sẽ công bố danh sách đề tài trên website để nhóm sinh viên lựa chọn đăng ký vào form. Khi xây dựng hệ thống, việc đăng ký sẽ được thực hiện trực tiếp trên hệ thống. Hệ thống sẽ đảm bảo không có nhóm sinh viên nào đăng ký 2 đề tài, cũng như không có đề tài được 2 nhóm sinh viên đăng ký. Đồng thời, các đề tài trên hệ thống chỉ hiển thị cho những sinh viên phù hợp, tránh trường hợp đăng ký đề tài sai chuyên môn.



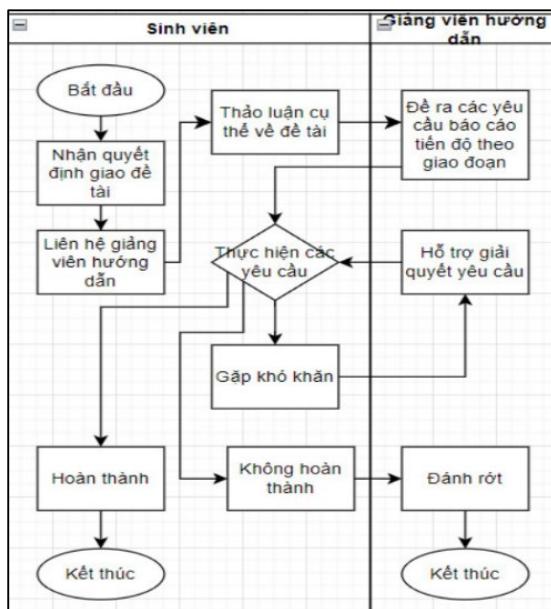
Hình 6. Quy trình đăng ký đề tài

Danh sách đề tài					Nội dung đề tài đang chọn		
Mã ĐT	Tên đề tài	Số lượng sinh viên	Giảng viên hướng dẫn	Chuyên ngành phù hợp			
CNTT000021	Tìm hiểu và đánh giá hiệu năng tính toán lượng tử	3 - 3	Phan Thị Ngọc Mai	Khoa học phân tích dữ liệu	Tiếp cận tìm hiểu mạng thuật toán FCM để phân cụm dữ liệu điểm sinh viên khoa CNTT thu thập được. Từ đó xây dựng ứng dụng để tư vấn sinh viên lựa chọn chuyên ngành Nội dung thực hiện: - Tìm các tài liệu, bài báo có liên quan đến thuật toán FCM để phân cụm dữ liệu - Thu thập và tiền xử lý dữ liệu điểm sinh viên khóa 09, khóa 10; - Ứng dụng thuật toán FCM đã tìm hiểu để phân cụm dữ liệu - Xây dựng thực nghiệm và đánh giá hiệu suất của phương pháp. - Xây dựng trang web tư vấn sinh viên lựa chọn chuyên ngành Môi trường thực hiện: - Ngôn ngữ lập trình: C#, Java, Python... - Môi trường lập trình: Pycharm, Jupiter Notebook, Google Colab... - Web: ASP/PHP/Django... Sinh viên có kỹ năng lập trình khá và đọc hiểu tốt tài liệu tiếng Anh; làm việc nghiêm túc, trách nhiệm.		
CNTT000023	Phân loại mối quan hệ ngữ nghĩa hình ảnh sử dụng cấu trúc KD-Tree	3 - 3	Phan Thị Ngọc Mai	Hệ thống thông tin			

Đề tài đã đăng ký						
Mã ĐT	Tên đề tài	Chi tiết	Số lượng sinh viên	Giảng viên hướng dẫn	Chuyên ngành phù hợp	Thao tác
CNTT000007	Ứng dụng thuật toán FCM xây dựng ứng dụng tư vấn sinh viên khoa CNTT lựa chọn chuyên ngành	Tiếp cận tìm hiểu mạng thuật toán FCM để phân cụm dữ liệu điểm sinh viên khoa CNTT thu thập được. Từ đó xây dựng ứng dụng để tư vấn sinh viên lựa chọn chuyên ngành	2 - 3	Trần Văn Thọ	Công nghệ phần mềm.Khoa học phân tích dữ liệu	<button>Hủy</button>

Hình 7. Đăng ký đề tài trên hệ thống

2.4. Quản lý tiến độ thực hiện đề tài



Hình 8. Quy trình quản lý tiến độ thực hiện

Khi đăng ký đề tài thành công, sinh viên sẽ nhận quyết định giao đề tài. Lúc này, thông tin của giảng viên sẽ được hiển thị trên hệ thống, sinh viên sẽ liên hệ với giảng viên hướng dẫn để thảo luận cụ thể về đề tài và xác định rõ mục tiêu thực hiện. Khi đã xác định được các mục tiêu, giảng viên sẽ tạo nhiệm vụ theo tiến độ để sinh viên thực hiện. Trong quá trình thực hiện, sinh viên có thể trao đổi với giảng viên và nộp kết quả nhiệm vụ ngay trên hệ thống. Việc này giúp tăng hiệu quả trong quá trình thực hiện khóa luận của sinh viên và giảng viên có thể kịp thời hỗ trợ các khó khăn mà sinh viên gặp phải.

PHẠM TẤN THUẬN

Hệ thống quản lý phản ánh vi phạm nội quy của sinh viên HUFI.

Thêm bài tập

Mã nhóm 20012005532022-20232	Khảo sát nghiệp vụ Đến hạn 16:30 11 tháng 05
Thành viên nhóm	⋮
PHẠM NGUYỄN HUYỀN TRÂN - 2001200004	
PHẠM TẤN THUẬN - 2001200553	
NGÔ VĂN SON - 2001202222	

Hình 9. Giảng viên giao nhiệm vụ theo tiến độ trên hệ thống

Khảo sát nghiệp vụ

Trần Văn Tho

Đến hạn 16:30 11 tháng 05

Mô tả: Mô tả chi tiết các nghiệp vụ, use case nghiệp vụ, use case hệ thống

Yêu cầu: Tìm hiểu các nghiệp vụ cơ bản cần có của hệ thống

Nhận xét về công việc

Thêm nhận xét cho công việc tại đây

Đăng

Báo cáo của bạn

Đã nộp

PDF kh-to-chuc-sv-nckh-cap-khoa-...pdf

PDF 9Vol95No4.pdf

PDF Báo cáo tổng kết.pdf

Thêm file đính kèm

Nộp báo cáo

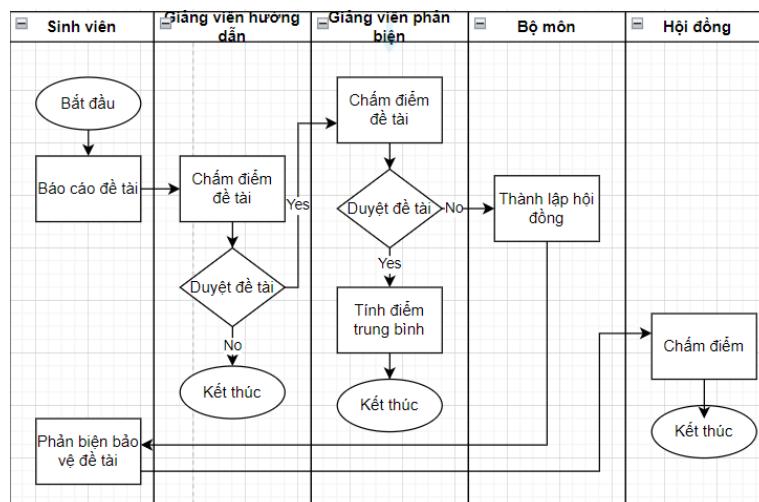
2001200553 - PHẠM TẤN THUẬN

Các bạn trong nhóm làm rất tốt nha thầy!

06-05-2023 (3 ngày trước)

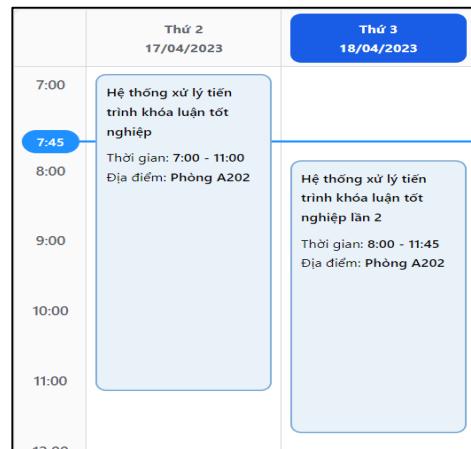
Hình 10. Sinh viên thực hiện nhiệm vụ và trao đổi với giảng viên

2.5. Đánh giá và chấm điểm



Hình 11. Quy trình đánh giá và chấm điểm

Sau khi sinh viên hoàn thành được các nhiệm vụ theo tiến độ giảng viên giao và đạt được kết quả cuối cùng. Giảng viên hướng dẫn sẽ lên lịch cho sinh viên báo cáo phản biện. Nếu giảng viên hướng dẫn duyệt thì tiếp tục báo cáo với giảng viên phản biện. Trường hợp cả 2 giảng viên duyệt thì điểm của sinh viên được tính bằng cách cộng trung bình điểm lại. Nếu giảng viên phản biện không đồng ý duyệt thì lúc này bộ môn sẽ thành lập hội đồng để đánh giá đề tài của sinh viên.



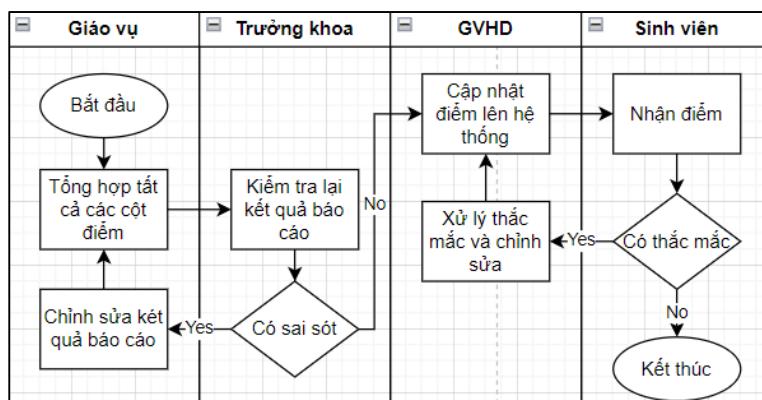
Hình 12. Lịch phản biện đề tài

Bảo vệ riêng tư cho học sinh				
MSSV	Họ tên	Điểm GVHD	Điểm GVPB	Hội đồng
		Nguyễn Hải Yến	Trần Văn Thọ	
2001200011	TRẦN THANH BÌNH	-	-	
2001200016	VƯƠNG CHÍ HẢI	-	-	
2001200025	LÊ THỊ NGỌC ÁNH	-	-	

Hệ thống quản lý phản ánh vi phạm nội quy của sinh viên HUFI.				
MSSV	Họ tên	Điểm GVHD	Điểm GVPB	Hội đồng
		Trần Văn Thọ	Nguyễn Văn Tùng	
2001200004	PHẠM NGUYỄN HUYỀN TRẦN	-	-	
2001200553	PHẠM TẤN THUẬN	-	-	
200120222	NGÔ VĂN SƠN	-	-	

Hình 13. Giao diện chấm điểm và xem điểm của giảng viên theo đề tài.

2.6. Thống kê và kết xuất kết quả



Hình 14. Quy trình thống kê và kết xuất kết quả

Trong quy trình này, khi làm việc thủ công giáo vụ khoa phải tổng hợp tất cả điểm số trên giấy và nhập vào hệ thống. Với số lượng lớn sinh viên, đề tài việc làm thủ công sẽ gấp rất nhiều khó khăn và sai sót. Khi xây dựng hệ thống, giảng viên sẽ trực tiếp đánh giá, chấm điểm trên hệ thống giúp giảm thiểu sai sót.

3. KẾT QUẢ

Kết quả nghiên cứu cho thấy hệ thống xử lý tiến trình khóa luận tốt nghiệp được thiết kế và đạt được hiệu suất tốt hơn so với cách làm thủ công trước đây. Hệ thống đã giúp kiểm soát chặt chẽ quá trình ra đề tài và kiểm duyệt chất lượng đề tài. Đây là một vấn đề quan trọng vì nó sẽ giúp sinh viên xác định được mục tiêu, hướng đi rõ ràng của đề tài góp phần nâng cao kết quả thực hiện của sinh viên. Cho phép sinh viên đăng ký đề tài ngay trên hệ thống, giúp tránh khỏi những khó khăn trước đây đã gặp phải như trùng lặp đề tài, đăng ký đề tài sai chuyên ngành. Hệ thống giúp giảm thời gian đăng ký đề tài cho sinh viên vì sinh viên chỉ thấy những đề tài phù hợp và chưa được bất kì nhóm nào đăng ký. Cuối cùng, vấn đề quan trọng nhất mà hệ thống đã xử lý là quản lý được tiến độ thực hiện đề tài của sinh viên. Từng nhiệm vụ trong tiến độ thực hiện, sinh viên và giảng viên có thể trao đổi với nhau trên hệ thống, giúp sinh viên

có thể xem được những nhận xét, góp ý của giảng viên từ các nhiệm vụ trước và chỉnh sửa kịp thời, cải thiện kỹ năng hơn.

4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Như vậy, việc nghiên cứu và xây dựng hệ thống này là hết sức cần thiết để góp phần chuyển đổi số trong trường học. Để cán bộ và giảng viên thực hiện xử lý tiến trình khóa luận một cách thủ công là một sự lãng phí rất lớn về thời gian, công sức và tài chính nhưng mang lại hiệu quả rất thấp. Kết quả nghiên cứu là đề xuất một hệ thống xử lý tiến trình khóa luận tốt nghiệp bằng công nghệ, chuyển đổi số và áp dụng toàn bộ các quy trình xử lý thủ công sang công nghệ. Nhằm mang lại hiệu quả cao về chất lượng đề tài, giúp rút ngắn thời gian đăng ký đề tài của sinh viên, làm tăng sự tương tác giữa giảng viên và sinh viên, nâng cao kết quả thực hiện của sinh viên, giảm thiểu thời gian cho việc quản lý, thống kê kết quả thực hiện đề tài của sinh viên.

Việc nghiên cứu và xây dựng hệ thống này đã mở ra một số hướng nghiên cứu tiếp theo như: nghiên cứu các công nghệ mới áp dụng vào hệ thống để tăng cường tính linh hoạt, bảo mật và tính khả dụng của hệ thống; nghiên cứu một số thuật toán giúp sinh viên có thể chọn đề tài phù hợp theo chuyên ngành, hệ thống có thể được triển khai trên đa nền tảng.

TÀI LIỆU THAM KHẢO

1. Haya El-Ghalayini, Mohammed Abu-Arqoub, Ghassan Issa, Ahmad F. Shubita. - Graduation-project management system: A social network analysis perspective. Journal of Theoretical and Applied Information Technology (2017).
2. Khoa Công nghệ thông tin – Slide bài giảng Nhập môn Công nghệ phần mềm, Đại học Công nghiệp Thực Phẩm TP. HCM.
3. Viện CNTT – ĐHQG Hà Nội – Giáo trình quản lý dự án.

ABSTRACT

BUILDING THE SYSTEM TO PROCESS THE GROUNDATION OF THE GRADUATION COURSE

Pham Tuan Thuan¹, Vu Tran Minh Hoang¹, Ngo Van Son¹,
Nguyen Ngoc Thach¹, Tran Van Tho^{1,*}

¹Ho Chi Minh City University of Food Industry, Vietnam

*Email: thotv@hufi.edu.vn

The graduate thesis process is the process by which the faculty manages the list of students, lecturers, and topics for a graduation thesis. In this paper, we propose to build a system to handle the graduation thesis process. This system will support faculty units in managing lecturers, students, and topics. In addition, the system also helps to improve the quality of topics, reduce errors and time in the process of registering students' topics. Increased interaction between lecturers and students helps students' thesis results to achieve better results.

Keywords: graduation thesis, thesis progress processing, thesis progress processing system.

ỨNG DỤNG FIREBASE AUTHENTICATION VÀ FIREBASE CLOUD MESSAGING ĐỂ XÂY DỰNG ĐĂNG NHẬP, ĐĂNG KÝ VÀ GỬI THÔNG BÁO VỀ CHO NGƯỜI DÙNG TRONG LẬP TRÌNH DI ĐỘNG ANDROID

Lê Minh Kha^{1,*}, Biện Thanh Nhựt¹, Nguyễn Hữu Trung¹,
Nguyễn Thị Bích Ngân¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: leminhkh318@gmail.com

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Firebase là một nền tảng được cung cấp bởi Google hỗ trợ xây dựng và phát triển các ứng dụng trong lập trình di động. Firebase giúp lập trình viên xây dựng nhiều chức năng một cách hiệu quả, như: lưu trữ và đồng bộ dữ liệu thời gian thực (Real time), xác thực người dùng (Authentication), gửi thông báo vào tin nhắn (Cloud Messaging), lưu trữ và chia sẻ nội dung do người dùng tạo ra (Cloud Storage) và một số chức năng khác. Trong bài báo này, chúng tôi trình bày hai công cụ Firebase Authentication và Firebase Cloud Messaging của nền tảng Firebase. Chúng hỗ trợ xây dựng chức năng đăng nhập, đăng ký tài khoản và gửi thông báo (notification) người dùng trong lập trình di động Android. Ngoài ra, chúng tôi áp dụng hai công cụ Firebase Authentication và Firebase Cloud Messaging để xây dựng chức năng đăng nhập, đăng ký và gửi thông báo cho việc phát triển ứng dụng di động android dành cho độc giả của thư viện trường Đại học Công nghiệp Thực phẩm TP.HCM.

Từ khóa: Firebase, Firebase Authentication, Firebase Cloud Messaging, lập trình di động android.

1. GIỚI THIỆU

Hiện nay, hầu hết các ứng dụng di động đều có yêu cầu xác thực người dùng khi muốn sử dụng những chức năng trong ứng dụng. Đối với chức năng xác thực người dùng, ngoài việc cho người dùng chủ động tạo tài khoản, nghĩa là cho người dùng đăng ký thông tin trực tiếp trên ứng dụng, thì còn có kỹ thuật hỗ trợ việc đăng ký/đăng nhập thông qua các dữ liệu xác thực người dùng của các dịch vụ phổ biến khác, như Google, Facebook hoặc Twitter [1].

Việc xây dựng hệ thống xác thực cho một ứng dụng đã trở nên phổ biến và có nhiều cách để thực hiện. Tuy nhiên, điều quan trọng là an toàn và bảo mật thông tin người dùng khi sử dụng ứng dụng. Đặc biệt, với các ứng dụng dạng thương mại điện tử, ngân hàng, quản lý thông tin cá nhân của người dùng thì chức năng này cần được đặt làm tiêu chí hàng đầu.

Với tư cách là chủ quản và nhà phát triển của hệ điều hành Android, Google đã xây dựng “một hệ sinh thái” gồm các nền tảng, công cụ và các dịch vụ phương thức trung gian kết nối (API - Application Programming Interface) nhằm hỗ trợ và cung cấp đầy đủ “những phương tiện” cho các lập trình viên, chẳng hạn như: phần mềm phát triển ứng dụng android (Android Studio), dữ liệu bản đồ thế giới (Google Maps), công cụ xây dựng giao diện người

dùng hiện đại (Jetpack Compose), môi trường tự động hóa quy trình làm việc (Google Cloud APIs), nền tảng phát triển ứng dụng (Firebase) và rất nhiều công cụ khác. Trong “hệ sinh thái đó”, Firebase là một nền tảng giúp tự động hóa việc phát triển phần mềm phía server, hay còn được gọi là BaaS (Backend as a Service), bao gồm cả việc cung cấp cơ sở hạ tầng điện toán đám mây. Firebase cung cấp nhiều tiện ích để lập trình viên chỉ cần tập trung tạo ra trải nghiệm cho người dùng sử dụng sản phẩm một cách tuyệt vời. Lập trình viên không cần quản lý máy chủ, không cần viết API. Vì Firebase là máy chủ, là API và kho dữ liệu của họ. Tất cả đều được viết một cách tổng quát đến mức lập trình viên có thể sửa đổi nó cho phù hợp với hầu hết nhu cầu xử lý [2].

Trong nhiều tiện ích của Firebase, Firebase Authentication xây dựng chức năng đăng nhập, đăng ký và Firebase Cloud Messaging hỗ trợ gửi thông báo trong quá trình phát triển ứng dụng di động android. Với vai trò quan trọng và sự hữu ích của hai tiện tích trên, trong bài báo này chúng tôi tập trung trình bày tổng quát cơ sở lý thuyết và các bước thực hiện để kết nối Firebase Authentication và Firebase Cloud Messaging vào một ứng dụng android. Sau đó chúng tôi tiến hành thực hiện tạo ứng dụng dùng hai tiện ích này cho việc xử lý xác thực và gửi thông báo cho người dùng trong ứng dụng quản lý việc mượn tài liệu dành cho độc giả thuộc thư viện trường Đại học Công nghiệp Thực phẩm TPHCM.

Phần còn lại của bài báo được tổ chức như sau, trong mục 2, chúng tôi trình bày tổng quan cơ sở lý thuyết của Firebase Authentication và các Firebase Cloud Message cũng như các bước để xây dựng chúng. Kết quả thực nghiệm trong ứng dụng được trình bày ở mục 3. Cuối cùng, mục 4 kết luận các vấn đề của bài báo và đề xuất hướng phát triển.

2. CƠ SỞ LÝ THUYẾT

2.1 Firebase Authentication

2.1.1 Giới thiệu về Firebase Authentication

Firebase Authentication là một trong những số tính năng cơ bản mà Firebase cung cấp. Nó được dùng để xác thực danh tính người dùng khi truy cập vào các ứng dụng. Ngoài ra, việc xây dựng chức năng xác thực là một yêu cầu rất quan trọng trong quá trình phát triển các phần mềm nói chung và các ứng dụng di động nói riêng. Chức năng này giúp thông tin người dùng được đảm bảo an toàn và tránh bị đánh cắp. Tuy nhiên việc xây dựng chức năng xác thực với nhiều phương thức khác nhau như email, số điện thoại hay facebook sẽ khiến người lập trình tốn khá nhiều thời gian và công sức. Firebase Authentication giúp giải quyết được những điều đó một cách dễ dàng và nó cũng là một công cụ giúp lập trình viên có thể tiếp cận một cách nhanh chóng [1].

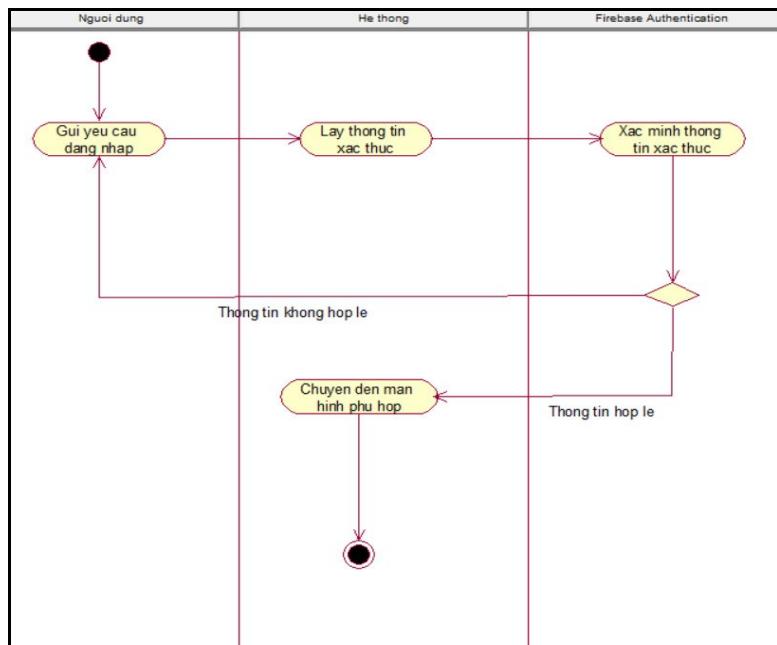
Thế nên Firebase Authentication là một công cụ hữu dụng giúp lập trình viên thực hiện hiệu quả trong quá trình xây dựng được một ứng dụng di.

2.1.2 Quy trình xác thực đăng nhập với Firebase Authentication

Để người dùng đăng nhập một tài khoản của ứng dụng di động, cần lấy thông tin xác thực từ tài khoản đăng nhập đó. Các thông tin xác thực này có thể là địa chỉ email và mật khẩu của người dùng hoặc mã thông báo OAuth từ nhà cung cấp danh tính được liên kết. Sau đó, dữ liệu xác thực được chuyển cho Firebase Authentication SDK (Software Development Kit – bộ công cụ phát triển phần mềm). Các dịch vụ phụ trợ của Firebase sau đó sẽ xác minh các thông tin đăng nhập đó và trả lại phản hồi cho người dùng[3].

Sau khi đăng nhập thành công, ứng dụng có thể truy cập thông tin hồ sơ cơ bản của người dùng và có thể kiểm soát quyền truy cập của người dùng vào dữ liệu được lưu trữ trong các sản phẩm khác của Firebase. Các nhà phát triển ứng dụng cũng có thể sử dụng mã xác thực được cung cấp để xác minh danh tính của người dùng trong các dịch vụ phụ trợ khác của riêng họ. Hình 1 thể hiện quy trình xác thực đăng nhập với Firebase Authentication.

2.1.3 Các loại xác thực của Firebase Authentication



Hình 1. Sơ đồ quy trình xác thực đăng nhập với Firebase Authentication

Trong android, Firebase Authentication cung cấp các chế độ xác thực khác nhau như: Password Authentication, Email Link Authentication, các nhà cung cấp bên thứ ba như Google, Facebook hay Twitter [2].

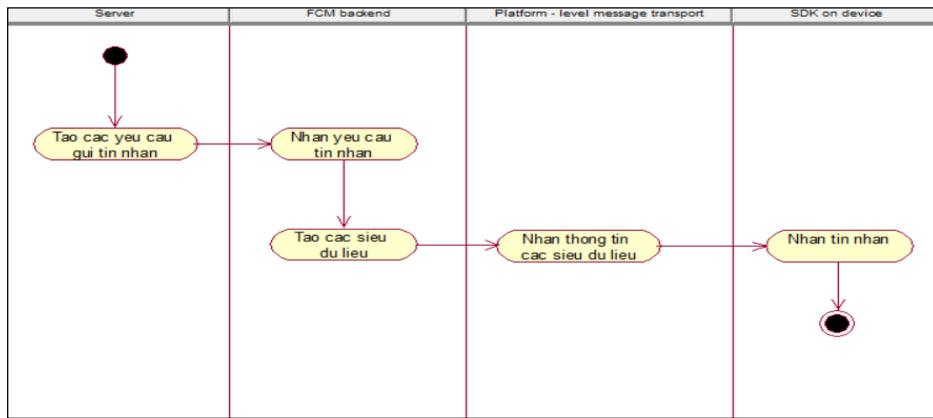
2.2 Firebase Cloud Message

2.2.1 Giới thiệu về Firebase Cloud Message

Tương tự như Firebase Authentication, Firebase Cloud Message (FCM) cũng là một trong những tính năng cơ bản mà Firebase cung cấp. Thông qua FCM, các nhà phát triển ứng dụng có thể gửi thông báo một cách nhanh chóng, an toàn và miễn phí đến các thiết bị cài đặt ứng dụng của họ.

Khi sử dụng Firebase Cloud Message, chỉ có thể gửi tin nhắn thông báo (giới hạn 2KB) và tin nhắn dữ liệu (giới hạn 4KB) [4]

2.2.2 Quy trình gửi tin nhắn với Firebase Cloud Message



Hình 2. Sơ đồ hoạt động gửi tin nhắn với Firebase Cloud Message.

Quy trình gửi tin nhắn với Firebase Cloud Message được thể hiện trong Hình 2. Cụ thể, quy trình hoạt động như sau [5]:

- Bước 1: Ở phía server sẽ tạo các yêu cầu gửi tin nhắn. Quá trình có hai cách tạo yêu cầu:
 - + Cách 1: sử dụng Notification Console GUI.
 - + Cách 2: sử dụng Admin SDK hay gọi trực tiếp thông qua HTTP / XMPP).
- Bước 2: Các tin nhắn này sẽ được chuyển cho phía FCM backend (đây là bộ não của FCM trong việc xử lý các dữ liệu).
- Bước 3: Sau khi các FCM backend chấp nhận các yêu cầu tin nhắn, chúng tạo các siêu dữ liệu tin nhắn như ID tin nhắn. Sau đó gửi đến Platform-level message transport (Đây là lớp vận chuyển của từng nền tảng) vì bản chất của FCM backend không gửi trực tiếp tin nhắn đến từng thiết bị mà phải gửi server trung gian của từng nền tảng (Lớp nền tảng bao gồm: Android transport layer - dành cho thiết bị android, iOS/APNs – dành cho thiết bị của Apple, Web Push – dành cho các ứng dụng web).
- Bước 4: Khi thiết bị trực tuyến, tin nhắn được qua lớp vận chuyển dành riêng cho nền tảng tới thiết bị. Cuối cùng các thiết bị nhận được tin nhắn.

Ngoài ra khi sử dụng FCM, người dùng có thể gửi tin nhắn đến một nhóm thiết bị được đăng ký theo các chủ đề cụ thể hoặc có thể nhận được chi tiết như là một thiết bị duy nhất. FCM có thể gửi tin nhắn ngay lập tức hoặc tại một thời điểm trong tương lai theo múi giờ địa phương. Người dùng có thể gửi dữ liệu ứng dụng tùy chỉnh như cài đặt mức độ ưu tiên, âm thanh và ngày hết hạn và cả theo dõi các sự kiện chuyển đổi tùy chỉnh.

2.2.3 Phân loại tin nhắn

FCM có 2 loại tin nhắn:

- Tin nhắn thông báo, đôi khi còn được gọi là “tin nhắn hiển thị”, một loại tin nhắn gửi và hiển thị ngay lập tức. Chúng được FCM SDK xử lý tự động
- Tin nhắn dữ liệu, được xử lý bởi ứng dụng khách.

2.3 Các bước kết nối Firebase vào dự án android

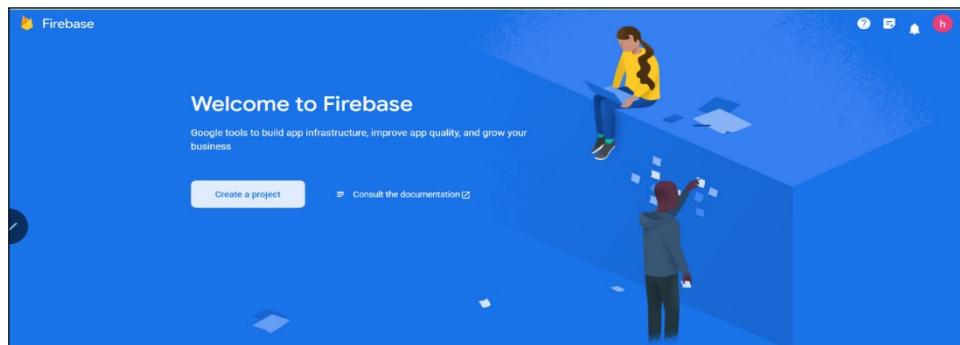
Để có thể đưa hai tiện ích Authentication và Cloud Messange vào ứng dụng thì trước hết phải kết nối Firebase vào dự án android. Các bước thực hiện lần lượt như sau [6]:

Yêu cầu:

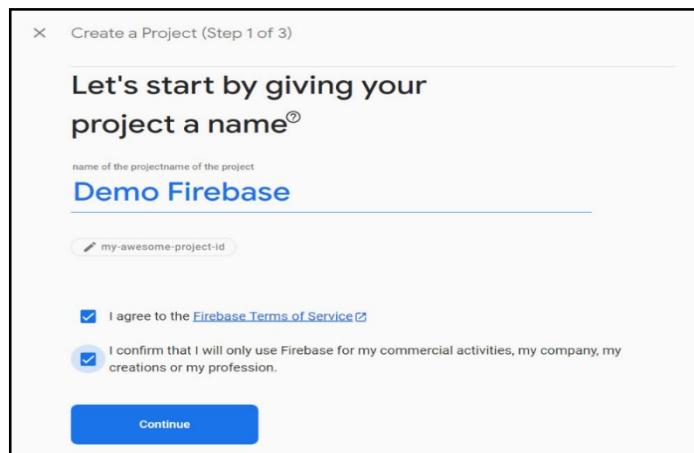
- Bước 1. Trước hết phải cài đặt Android Studio.
- Bước 2. Ứng dụng phải đáp ứng các yêu cầu :
 - + Phải từ API 19 trở lên
 - + Sử dụng Android 4.4 trở lên
 - + Sử dụng Jetpack (AndroidX) bao gồm :
 - com.android.tools.build:gradle v3.2.1 trở lên
 - compileSdkVersion 28 trở lên - + Đăng nhập Firebase bằng tài khoản Google

Các bước kết nối Firebase vào dự án

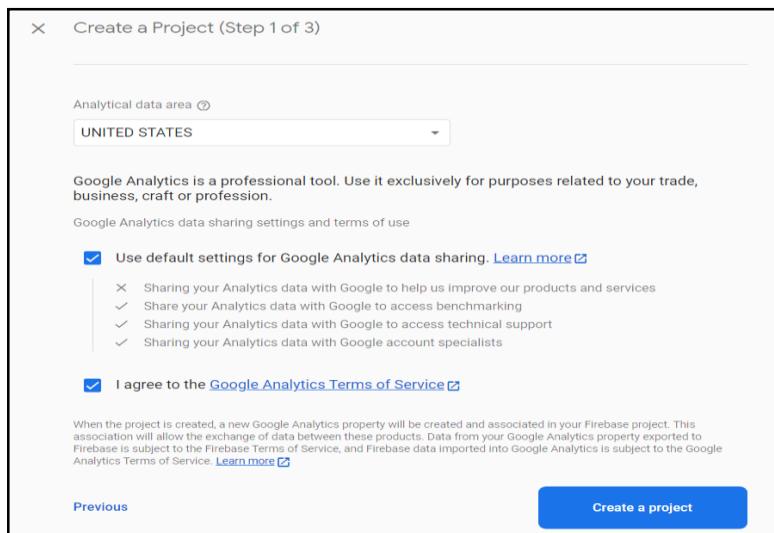
- Bước 1: Tạo dự án Firebase
 - + Sau khi đăng nhập thành công, màn hình Console Firebase xuất hiện. Để tạo một dự án, click chọn Create Project như hình 3.
 - + Nhập tên dự án, tại đây chúng ta cũng có thể tùy ý chỉnh sửa ID dự án được hiển thị bên dưới tên dự án. Đọc kĩ các điều khoản và click chọn Continue như hình 4.
 - + Chọn Create a project như hình 5.



Hình 3. Màn hình console hiện ra khi đã đăng nhập vào Firebase bằng tài khoản Google.

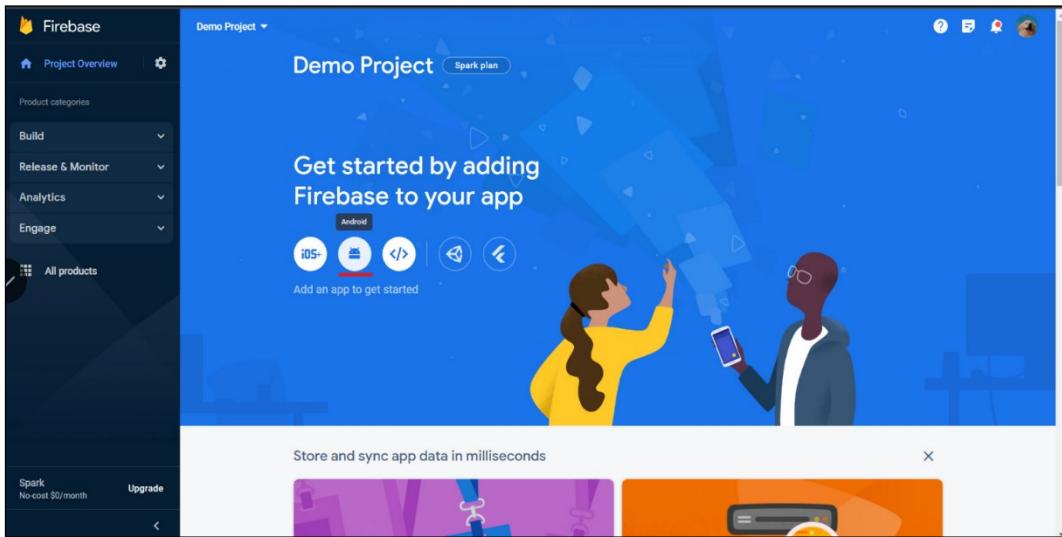


Hình 4. Bước nhập tên dự án



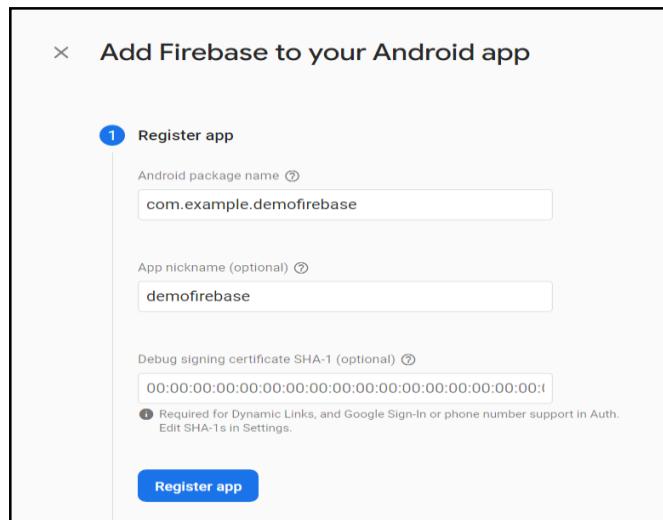
Hình 5. Bước cuối cùng của tạo dự án

- Bước 2: Đăng ký ứng dụng với Firebase
 - + Sau khi tạo thành công một dự án, sẽ được đưa đến một giao diện và sau đó chọn biểu tượng android để tiến hành đăng ký ứng dụng như hình 6.



Hình 6. Giao diện console khi đã tạo dự án thành công

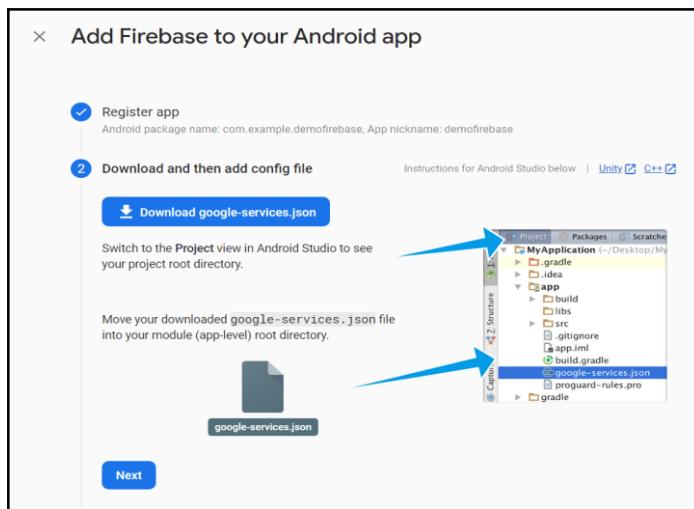
- + Tiếp theo sẽ nhập tên gói ứng dụng (có thể tìm thấy tên package trong **AndroidManifest**) và nhập tên riêng ứng dụng. Sau đó chọn Register app như hình 7.



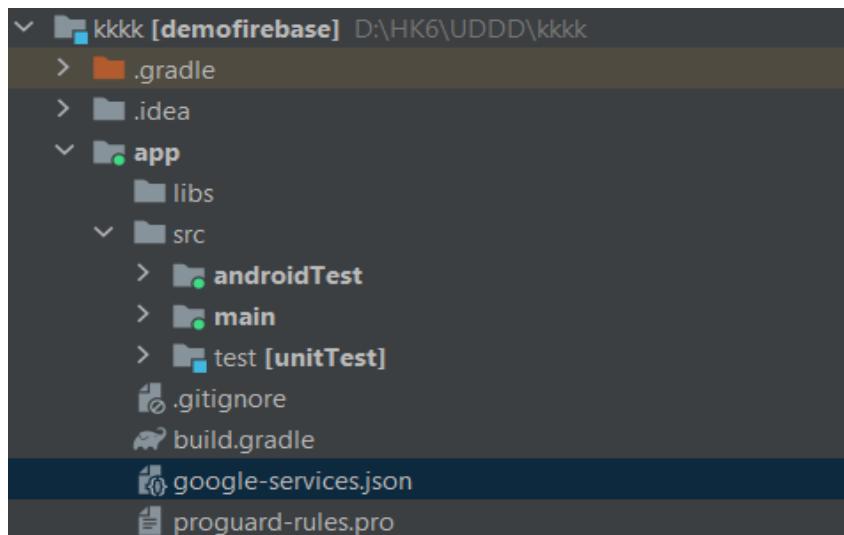
Hình 7. Màn hình nhập tên gói ứng dụng và tên riêng của ứng dụng

- Bước 3: Thêm tệp cấu hình Firebase
 - + Chọn Download and the add config file cho ứng dụng. Sau đó chọn *Dowload google-services.json* như hình 8.
 - + Sau khi tải tệp google-services.json, chúng ta tiến hành đưa file này vào thư mục app của ứng dụng như hình 9.
 - + Thêm Firebase SDK.

Để tệp cấu hình *google-services.json* có thể truy cập được với Firebase SDK, phải cài Google services Gradle plugin. Trong “*build.gradle*” (project), thêm các Google services plugin như hình 10.



Hình 8. Màn hình thêm Firebase cho ứng dụng android



Hình 9. Nơi đặt file cấu hình google-services.json

Trong “build.gradle” (app). Tương tự như trên, cần phải thêm các Google services plugin như hình 11.

3. THỰC NGHIỆM

Để hỗ trợ thủ thư có thể làm tốt công việc quản lý mượn trả thì ứng dụng quản lý thư viện của chúng tôi đã tích hợp một số các tính năng hữu ích cho thủ thư như quản lý mượn trả sách, lịch sử mượn trả, quản lý đăng nhập, quản lý danh sách các loại sách, và một số tính năng khác. Chúng tôi còn tích hợp tính năng giúp xác thực thông tin người dùng và gửi thông báo đến với người dùng bằng tiện ích của Firebase là Firebase Authentication và Firebase Cloud Messaging.

```

buildscript {
    repositories {
        // Make sure that you have the following two repositories
        google() // Google's Maven repository
        mavenCentral() // Maven Central repository
    }
    dependencies {
        ...
        // Add the dependency for the Google services Gradle plugin
        classpath 'com.google.gms:google-services:4.3.15'
    }
}

allprojects {
    ...
    repositories {
        // Make sure that you have the following two repositories
        google() // Google's Maven repository
        mavenCentral() // Maven Central repository
    }
}

```

Hình 10. Các google services plugin cần thiết thêm vào “build.gradle” (project)

```

plugins {
    id 'com.android.application'
    // Add the Google services Gradle plugin
    id 'com.google.gms.google-services'
    ...
}

dependencies {
    // Import the Firebase BoM
    implementation platform('com.google.firebase:firebase-bom:31.5.0')

    // TODO: Add the dependencies for Firebase products you want to use
    // When using the BoM, don't specify versions in Firebase dependencies
    implementation 'com.google.firebaseio:firebase-analytics'

    // Add the dependencies for any other desired Firebase products
    // https://firebase.google.com/docs/android/setup#available-libraries
}

```

Hình 11. Các google services plugin cần thiết thêm vào “build.gradle” (project)

3.1 Tạo dự án mới trong android studio

- Vào File => New => New Project đến màn hình kế tiếp chọn Empty Activity sau đó nhấn next.

Tiếp đến để tạo empty activity mới chúng tôi sẽ nhập đầy đủ thông tin hiện trên màn hình. Nên nhớ tên package phải trùng với tên package đã tạo trong firebase console

Sau khi nhấn vào Finish. Chúng tôi sẽ sử dụng được Activity Name là MainActivity trong android studio.

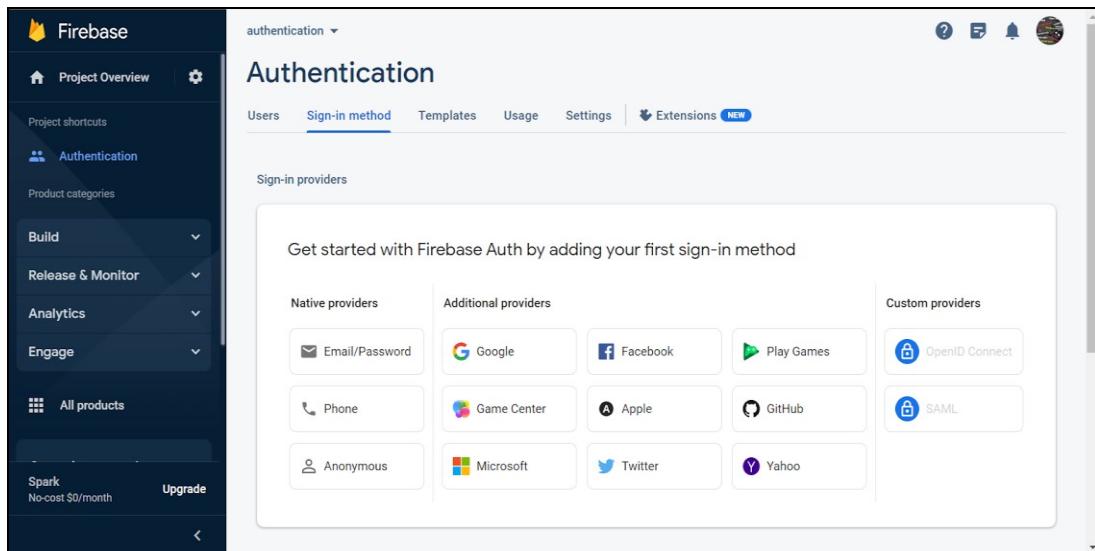
3.2 Firebase Authentication

3.2.1 Thêm Firebase Authentication và chọn cấu hình app firebase

Thêm Firebase Authentication vào android studio có 2 cách:

- Cách 1: kết nối Firebase với android trên website.

- Cách 2: kết nối trực tiếp trên android studio. Khi kết nối xong chúng tôi thực hiện enable Email/Password để hỗ trợ chúng tôi xử lý đăng ký đăng nhập như hình 12.



Hình 12. Chọn cấu hình app firebase trong authentication.

3.2.2 Xử lý đăng ký tài khoản và đăng nhập thành công của Firebase Authentication

Nhờ vào chức năng xác thực người dùng theo nhiều cấu hình ứng dụng của Firebase Authentication đã hỗ trợ chúng tôi xử lý được việc đăng ký, đăng nhập tài khoản cho người dùng.

Đầu tiên để người dùng có tài khoản lưu thông tin cá nhân của bản thân thì người dùng cần đăng ký tài khoản. Để thực hiện được việc xử lý đăng nhập chúng tôi muốn khi chạy chương trình app sẽ vào activity RegisterActivity xử lý hàm onCreate(). Trong hàm onCreate() khi thực hiện nhấn nút btnRegister sẽ sử dụng event setOnClickListener() và thực thi hàm createUser() để tạo tài khoản sau đó lưu tài khoản đó vào Firebase Authentication.

```

@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_register);

    etRegEmail = findViewById(R.id.etRegEmail);
    etRegPassword = findViewById(R.id.etRegPass);
    tvLoginHere = findViewById(R.id.tvLoginHere);
    btnRegister = findViewById(R.id.btnRegister);

    mAuth = FirebaseAuth.getInstance();

    btnRegister.setOnClickListener(view ->
        createUser();
    );

    tvLoginHere.setOnClickListener(view ->
        startActivity(new Intent(RegisterActivity.this, LoginActivity.class));
    );
}

```

Hàm createUser() được thực hiện sẽ lưu tài khoản vào firebase authentication nhờ vào event createUserWithEmailAndPassword(email,password). Trong event có hỗ trợ hàm onComplete() khi thực thi hàm sẽ kiểm tra xem nếu tạo tài khoản thành công sẽ chuyển từ activity RegisterActivity sang LoginActivity còn nếu không tạo thành công sẽ hiện thông báo lỗi.

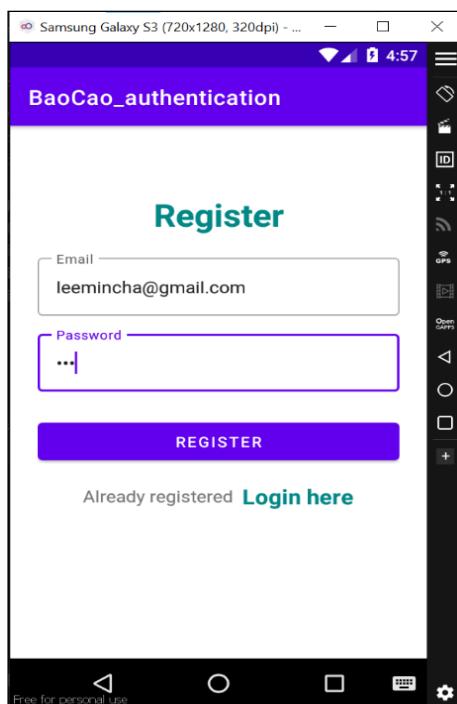
```
private void createUser(){
    String email = etRegEmail.getText().toString();
    String password = etRegPassword.getText().toString();
    if (TextUtils.isEmpty(email)){
        etRegEmail.setError("Email cannot be empty");
        etRegEmail.requestFocus();
    }else if (TextUtils.isEmpty(password)){
        etRegPassword.setError("Password cannot be empty");
        etRegPassword.requestFocus();
    }else{
mAuth.createUserWithEmailAndPassword(email,password).addOnCompleteListener(new
OnCompleteListener<AuthResult>() {
    @Override
    public void onComplete(@NonNull Task<AuthResult> task) {
        if (task.isSuccessful()){
            Toast.makeText(RegisterActivity.this, "User registered successfully",
            Toast.LENGTH_SHORT).show();
            startActivity(new Intent(RegisterActivity.this, LoginActivity.class));
        }else{
            Toast.makeText(RegisterActivity.this, "Registration Error: "
            + task.getException().getMessage(),
            Toast.LENGTH_SHORT).show();
        }
    }
}
}
```

Khi tạo tài khoản thành công cũng là lúc chúng tôi vào activity LoginActivity để đăng nhập vào dự án. Để đăng nhập được vào activity MainActivity chúng tôi sẽ thực thi hàm loginUser() và sử dụng event signInWithEmailAndPassword(email,password) nếu đăng nhập thành công sẽ chuyển qua activity MainActivity phải trả về thông báo lỗi khi không có tài khoản đó trong Firebase Authentication. Khi đã chuẩn bị xong các dòng code trên, chúng tôi đã hoàn thành việc thực hiện Firebase Authencation. Cuối cùng người dùng sẽ thao tác trên màn hình. Hình 13 thể hiện giao diện của màn hình đăng nhập trong ứng dụng của chúng tôi, và Hình 14 minh họa dữ liệu người dùng đăng ký được lưu trên Firebase.

Thông tin đăng ký khi được lưu vô Firebase Authencation.

```
private void loginUser(){
    String email = etLoginEmail.getText().toString();
    String password = etLoginPassword.getText().toString();
    if (TextUtils.isEmpty(email)){
        etLoginEmail.setError("Email cannot be empty");
        etLoginEmail.requestFocus();
    }else if (TextUtils.isEmpty(password)){
        etLoginPassword.setError("Password cannot be empty");
        etLoginPassword.requestFocus();
```

```
        }else{
            mAuth.signInWithEmailAndPassword(email,password).addOnCompleteListener(new
OnCompleteListener<AuthResult>() {
                @Override
                public void onComplete(@NonNull Task<AuthResult> task) {
                    if (task.isSuccessful()){
                        Toast.makeText(LoginActivity.this, "User logged in successfully",
                                Toast.LENGTH_SHORT).show();
                        startActivity(new Intent(LoginActivity.this, MainActivity.class));
                    }else{
                        Toast.makeText(LoginActivity.this, "Log in Error: "
                                + task.getException().getMessage(),
                                Toast.LENGTH_SHORT).show();
                    }
                }
            });
        }
    }
}
```



Hình 13. Trang đăng ký tài khoản

3.3 Cloud Messaging

3.3.1 Kết nối dự án của Android với Cloud Messaging

Để kết nối một dự án với Cloud Messaging thông thường có 2 cách, kết nối với website của Firebase và kết nối bằng công cụ hỗ trợ trên android studio. Trong bài báo này, chúng tôi sẽ nói chi tiết cách kết nối FCM bằng công cụ trên android studio.

- Đầu tiên vào dự án android cần kết nối với Cloud Messaging.
 - Vào Tools => Firebase => sau đó chọn Cloud Messaging

- Cuối cùng ấn vào “Connect your app to firebase” và “FCM to your app”

The screenshot shows the Firebase console's Project Overview page. On the left, there's a sidebar with 'Authentication' selected. The main area is titled 'Authentication' and shows a table of users. One user is listed: 'leemincha@gmail.com' with a provider icon (envelope), created on 'Apr 15, 2023', signed in on 'Apr 15, 2023', and a user ID '81Af03p5hNfzs0oUvpChYpzrhs63'. There are buttons for 'Add user' and a three-dot menu. At the bottom, it says 'Rows per page: 50' and '1 - 1 of 1'.

Hình 14. Lưu trữ tài khoản người dùng đã đăng ký

3.3.2 Xử lý gửi thông báo từ trên Cloud Messaging về ứng dụng android

Để gửi được thông báo từ Cloud Messaging về cho người dùng sử dụng ứng dụng, đầu tiên chúng tôi sẽ thêm dịch vụ vào ứng dụng trong file android manifest của dự án như sau:

```
<service android:name=".MyFirebaseMessagingService">
    android:exported="false">
    <intent-filter>
        <action android:name="com.google.firebase.MESSAGING_EVENT" />
    </intent-filter>
</service>
```

Sau đó chúng tôi sẽ tạo một lớp “MyFirebaseMessagingService” và lớp này sẽ được kế thừa từ lớp FirebaseMessagingService của Firebase Cloud Messaging. Lớp này được sử dụng để xử lý các thông báo (notification) được gửi từ Firebase Cloud Messaging đến thiết bị Android. Phương thức onMessageReceived được ghi đè (override) từ lớp cha FirebaseMessagingService. Phương thức này được gọi khi một thông báo mới được nhận từ Firebase Cloud Messaging. Trong phương thức này, đoạn mã sử dụng đối tượng RemoteMessage để lấy tiêu đề và nội dung của thông báo, sau đó gọi phương thức getFirebaseMessage để hiển thị thông báo trên màn hình.

Phương thức getFirebaseMessage được định nghĩa để tạo và hiển thị một thông báo trên thiết bị. Trong phương thức này, đoạn mã sử dụng đối tượng NotificationCompat.Builder để tạo một thông báo với tiêu đề và nội dung được truyền vào. Sau đó, đoạn mã sử dụng đối tượng NotificationManagerCompat để hiển thị thông báo với ID là 101.

```
public class MyFirebaseMessagingService extends FirebaseMessagingService {
    @Override
    public void onMessageReceived(@NonNull RemoteMessage remoteMessage) {
        super.onMessageReceived(remoteMessage);
        getFirebaseMessage(remoteMessage.getNotification().getTitle(),
            remoteMessage.getNotification().getBody());
```

```

    }
    public void getFirebaseMessage(String title, String msg) {
        NotificationCompat.Builder builder = new NotificationCompat.Builder(this,
                "myFirebaseChannel")
                .setSmallIcon(R.drawable.ic_launcher_background)
                .setContentTitle(title)
                .setContentText(msg)
                .setAutoCancel(true);
        NotificationManagerCompat manager = NotificationManagerCompat.from(this);
        if (ActivityCompat.checkSelfPermission(this,
                android.Manifest.permission.POST_NOTIFICATIONS) != PackageManager.PERMISSION_GRANTED)
        {
            return;
        }
        manager.notify(101, builder.build());
    }
}

```

Phương thức FirebaseMessaging.getInstance().subscribeToTopic("News") được gọi để đăng ký thiết bị vào chủ đề "News". Sau đó, phương thức addOnCompleteListener được gọi với một đối tượng OnCompleteListener được truyền vào. Đối tượng này được sử dụng để xử lý kết quả đăng ký chủ đề, trong trường hợp này là một Task<Void>.

Trong phương thức onComplete của OnCompleteListener, đoạn mã kiểm tra xem đăng ký chủ đề có thành công hay không bằng cách kiểm tra trạng thái của Task. Nếu Task thành công, biến msg được gán giá trị là "Done". Nếu Task thất bại, biến msg được gán giá trị là "Failed". Tuy nhiên, trong đoạn mã này, giá trị của msg không được sử dụng cho bất kỳ mục đích nào khác và chỉ đơn giản là gán giá trị để kiểm tra xem đăng ký chủ đề có thành công hay không.

```

package com.example.baibaocao;
import androidx.annotation.NonNull;
import androidx.appcompat.app.AppCompatActivity;
import android.os.Bundle;
import com.google.android.gms.tasks.OnCompleteListener;
import com.google.android.gms.tasks.Task;
import com.google.firebase.messaging.FirebaseMessaging;

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

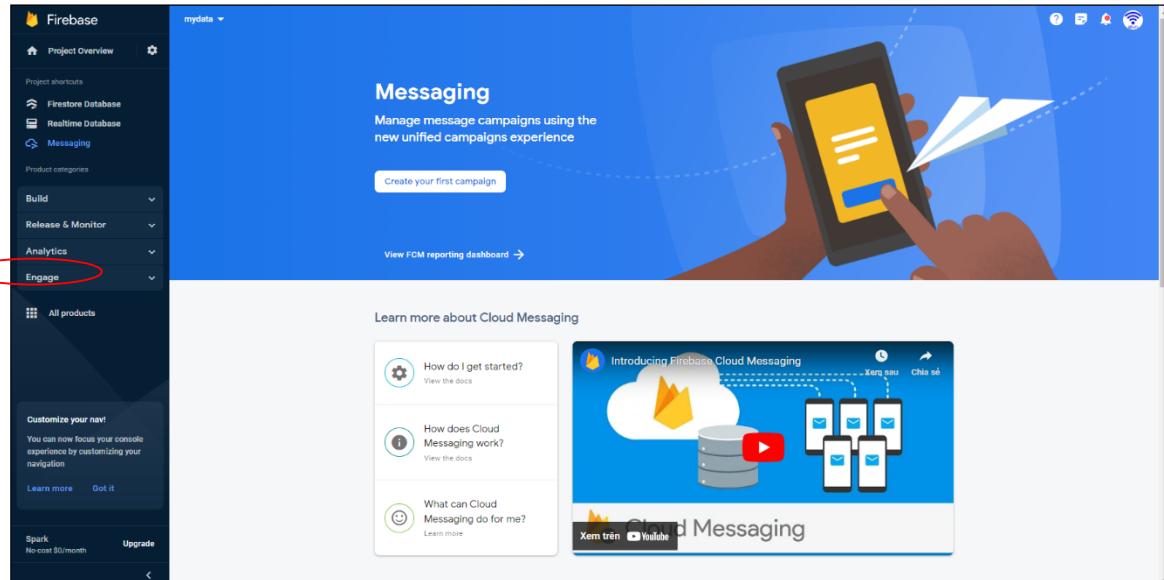
        FirebaseMessaging.getInstance().subscribeToTopic("News")
                .addOnCompleteListener(new OnCompleteListener<Void>() {
                    @Override
                    public void onComplete(@NonNull Task<Void> task) {
                        String msg = "Done";
                        if (!task.isSuccessful()) {
                            msg = "Failed";
                        }
                    }
                });
    }
}

```



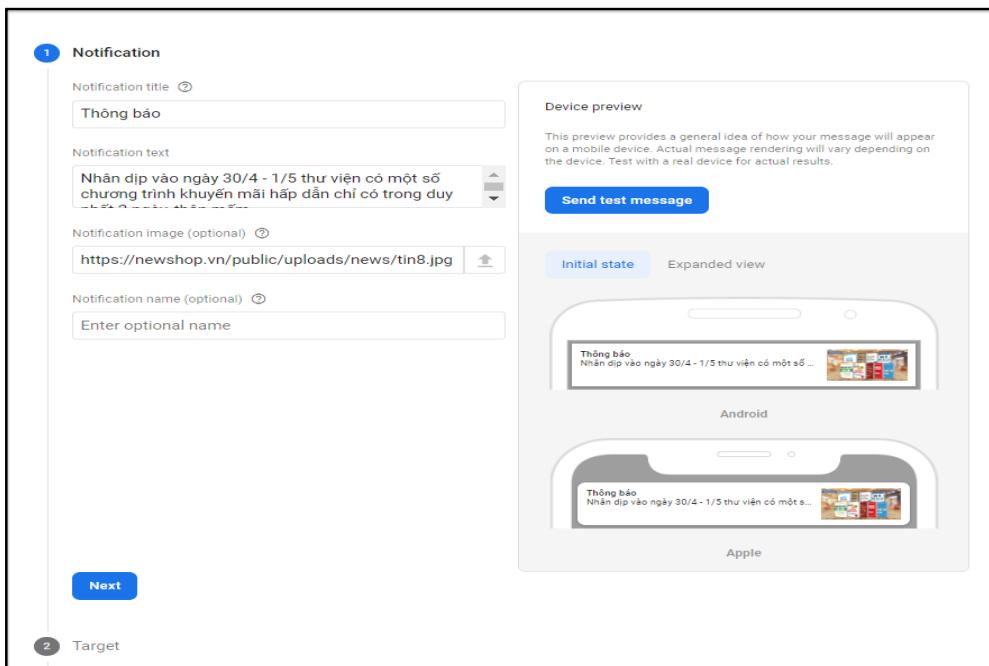
3.3.3 Gửi thông báo từ Cloud Messaging về Firebase

Đầu tiên, chúng tôi đăng nhập vào Firebase và chọn dự án cần thực hiện



Hình 15. Giao diện của ứng dụng Firebase

Chọn Engage => Messaging => create your first campaign => Firebase Notification messages => sau đó nhấn “Create” sẽ xuất hiện giao diện như hình 16.



Hình 16. Giao diện của custom Firebase

Sau đó chúng tôi custom thông báo và gửi đi. Cuối cùng thông báo sẽ được gửi đến các ứng dụng của người nhận như hình 17.



Hình 17. Giao diện của ứng dụng android trên điện thoại khi nhận được thông báo

4. KẾT LUẬN

Trong bài báo này, chúng tôi đã trình bày quy trình tổng quát xây dựng ứng dụng di động có chức năng đăng ký, đăng nhập tài khoản và gửi thông báo dùng hai tiện ích của nền tảng Firebase, đó là Firebase Authentication và Firebase Cloud Messaging. Firebase Authentication và Firebase Cloud Messaging thực sự tạo nhiều tiện lợi hữu ích cho các lập trình viên trong việc xây dựng các chức năng xác thực người dùng và gửi thông báo. Lập trình viên có thể triển khai nhanh chóng và dễ dàng các xử lý, không cần cấu hình server, cập nhật dữ liệu theo thời gian thực, có API mạnh mẽ và đặc biệt là miễn phí. Tuy nhiên vẫn còn một số hạn chế trong việc hỗ trợ xây dựng ứng dụng như việc thực hiện REST API khó khăn, vì Firebase chỉ hoạt động với NoSQL nên truy vấn và giao dịch sẽ khá phức tạp và có tốc độ truy vấn chậm. Chúng tôi đã ứng dụng chúng vào quá trình phát triển ứng dụng quản lý thư viện.

TÀI LIỆU THAM KHẢO

1. FptCloud, Ưu/nhược điểm và các dịch vụ của Firebase, Truy cập ngày 25/4/2023 tại: <https://fptcloud.com/firebase-la-gi/>
2. Neil Smyth, Firebase Essentials - Android Edition, CreateSpace 2017
3. Firebase Document Tutorial, truy cập 25/4/2023 từ: <https://firebase.google.com/docs?hl=vi>
4. Firebase Cloud Messaging, truy cập 25/4/2023 từ: <https://firebase.google.com/docs/cloud-messaging?hl=vi>
5. Firebase Document Tutorial truy cập 25/4/2023 từ: <https://firebase.google.com/docs/android/setup?hl=vi>

ABSTRACT

FIREBASE AUTHENTICATION AND FIREBASE CLOUD MESSAGING APP TO BUILD LOG IN, REGISTER AND SEND NOTIFICATIONS TO USERS IN ANDROID MOBILE PROGRAMMING

Le Minh Kha^{1,*}, Bien Thanh Nhut¹, Nguyen Huu Trung¹, Nguyen Thi Bich Ngan¹

Ho Chi Minh City University of Food Industry.

**Email: leminhkhaha318@gmail.com*

In this article, we focus on developing a mobile application for the library of Ho Chi Minh City Food Industry School in a specific field (software engineering - CNPM) in English based on the encyclopedia library. Wikipedia encyclopedia and firebase website. Firebase is a platform provided by Google that supports building and developing apps and games in mobile programming. Firebase supports many built-in functions such as: real-time data storage and synchronization, user authentication (authentication), cloud messaging, storage and sharing, user-generated content (cloud storage) ... In this article, we present two Firebase authentication and Firebase cloud messaging tools of the Firebase platform. They support building login, account registration and user notification functionality in Android mobile programming. In addition, we apply two tools Firebase authentication and Firebase cloud messaging to build login, registration and notification functionality for android mobile application development, for readers of the University library. Food Industry Ho Chi Minh City.

Keywords: firebase, Wikipedia, firebase authentication, firebase cloud messaging, software engineering.

ĐIỀU HƯỚNG NAVIGATION TRONG THIẾT KẾ GIAO DIỆN LẬP TRÌNH DI ĐỘNG ANDROID

Lê Minh Phát^{1,*}, Lê Tâm Như¹, Ngô Thị Kim Ngân¹, Nguyễn Thị Kim Tuyền¹,
Nguyễn Thị Bích Ngân¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: lephat508@gmail.com

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Bài báo này tập trung giới thiệu việc thiết kế và xử lý các điều hướng (navigation) trong quá trình thiết kế giao diện lập trình di động android. Bài báo nhấn mạnh tầm quan trọng cùng các lợi ích của navigation đối với trải nghiệm người dùng. Đồng thời, cung cấp một quy trình chi tiết cho việc xây dựng hai loại navigation phổ biến là bottom navigation và navigation drawer. Ngoài ra, chúng tôi thực hiện thực nghiệm thông qua việc dùng hai loại navigation nói trên vào trong thiết kế giao diện của ứng dụng di động android “Quảng bá địa điểm du lịch tại Việt Nam”. Kết quả cho thấy ứng dụng có một giao diện đẹp mắt, tiện lợi và mang đến cho người dùng trải nghiệm thú vị thông qua hiệu quả của các navigation mang lại.

Từ khóa: Navigation, bottom navigation, navigation drawer.

1. MỞ ĐẦU

Navigation là những công cụ hỗ trợ quản lý và điều hướng màn hình trong lập trình ứng dụng di động nói chung, riêng trong phạm vi bài báo này, chúng tôi tập trung vào lập trình di động trên hệ điều hành android. Navigation trở thành một trong những công cụ được sử dụng phổ biến trong thiết kế giao diện của các ứng dụng di động. Với việc dùng navigation, người dùng có thể chuyển đổi giữa các màn hình và hoạt động trong ứng dụng một cách hiệu quả, “mượt mà”. Tính đồng nhất giữa các màn hình trong ứng dụng được cải thiện và trải nghiệm người dùng được tối ưu hóa nhờ các thành phần điều hướng này [1].

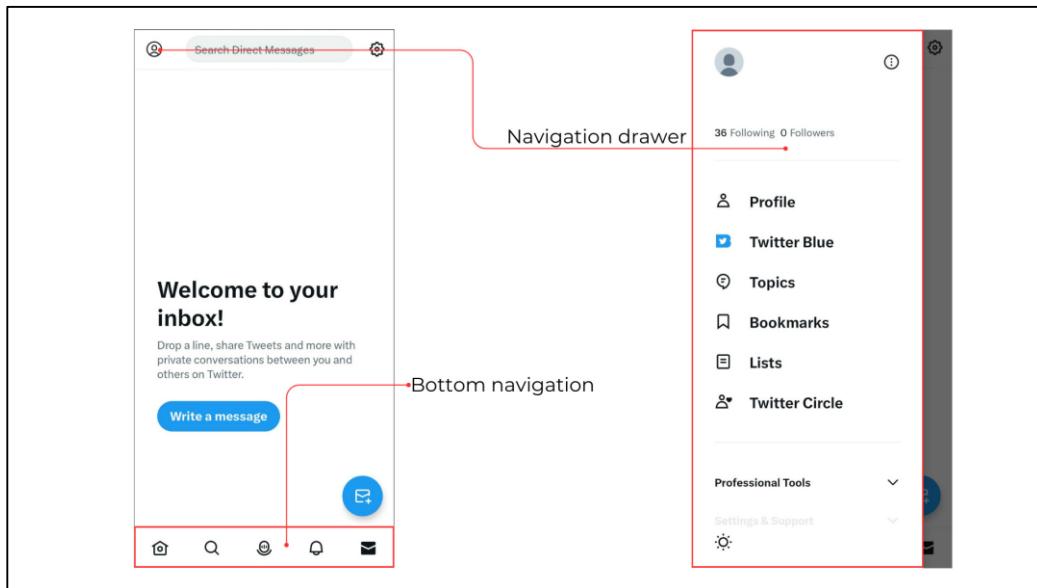
Hiện nay, việc sử dụng navigation giúp giảm thời gian và chi phí phát triển ứng dụng. Nhà phát triển không cần phải viết mã cho từng màn hình và hoạt động riêng lẻ. Đồng thời, navigation giúp tăng tính linh hoạt và sự dễ dàng trong quá trình bảo trì và cập nhật ứng dụng. Do đó, navigation được xem là một bước tiến quan trọng trong thiết kế ứng dụng di động trên nền tảng android. Với tầm quan trọng của việc quản lý điều hướng trong ứng dụng, navigation đã trở thành một công cụ hữu ích trong quá trình phát triển các ứng dụng di động [1].

1.1. Navigation là gì?

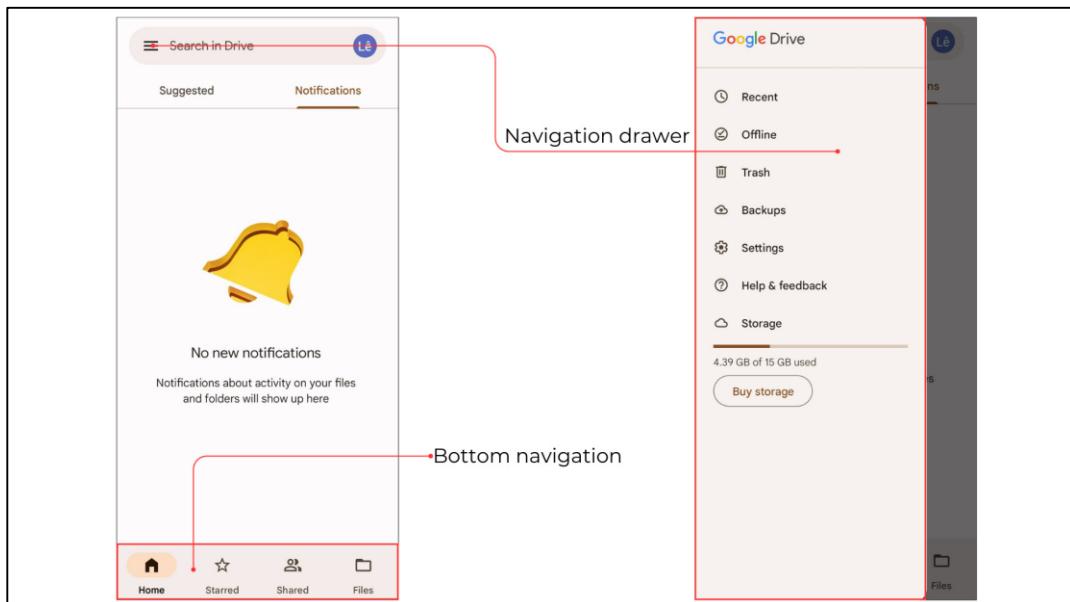
Navigation là công cụ hỗ trợ quản lý và điều hướng màn hình trong ứng dụng di động. Tính năng điều hướng là các hành động tương tác cho phép người dùng di chuyển qua lại, vào và ra khỏi các phần nội dung khác nhau trong ứng dụng [1]. Điều hướng giữa các màn hình là

một trong những kỹ thuật cốt lõi trong kiến trúc ứng dụng. Cách tiếp cận và xử lý việc điều hướng giữa các màn hình sẽ ảnh hưởng đáng kể tới khả năng bảo trì ứng dụng sau này.

Cụ thể trong bài báo này, chúng tôi tìm hiểu và giới thiệu hai loại navigation phổ biến là bottom navigation và navigation drawer. Các loại navigation này được sử dụng trong rất nhiều các ứng dụng di động phổ biến với người dùng, chẳng hạn: Twitter (hình 1), Gmail (hình 2), Lazada, Shopee, Facebook, Zalo, Google Map và rất nhiều ứng dụng khác nữa.



Hình 1. Bottom navigation và navigation drawer được dùng trong ứng dụng Twitter



Hình 2. Bottom navigation và navigation drawer được dùng trong ứng dụng Gmail

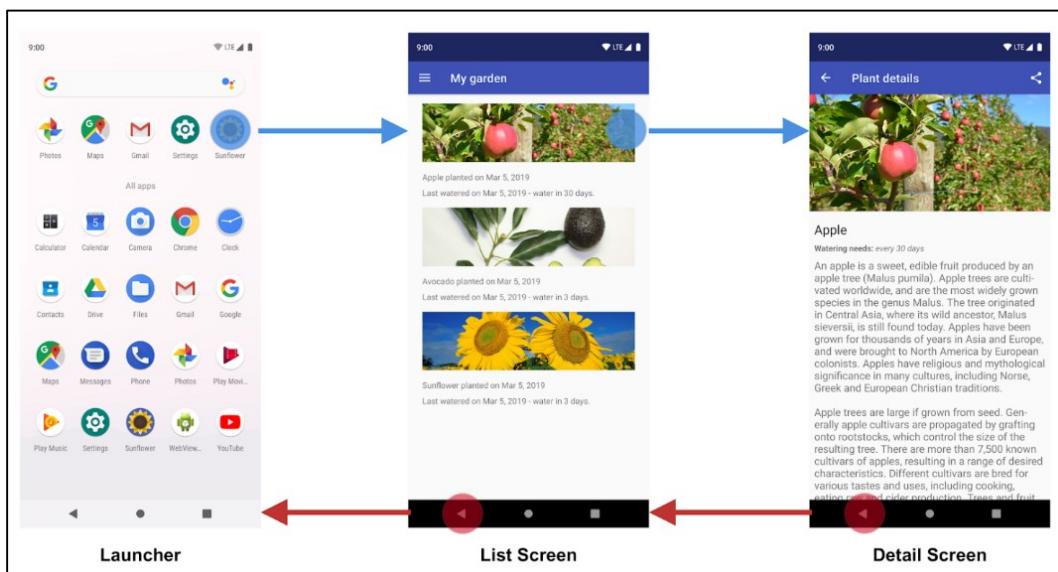
1.2. Lợi ích

Sử dụng navigation trong xây dựng ứng dụng android mang lại nhiều lợi ích cho nhà phát triển, giúp tăng tính năng dễ sử dụng và cải thiện trải nghiệm người dùng. Cụ thể, các lợi ích của sử dụng navigation bao gồm [3]:

- *Giảm thời gian và công sức phát triển:* navigation giúp thiết kế và xây dựng ứng dụng nhanh chóng hơn, giảm thời gian và công sức của nhà phát triển.
- *Tính linh hoạt và dễ quản lý:* navigation giúp quản lý màn hình dễ dàng hơn bằng cách kết nối chúng với nhau nhờ navigation graphs, cung cấp tính linh hoạt và dễ quản lý hơn.
- *Trải nghiệm người dùng tốt hơn:* navigation tạo ra trải nghiệm người dùng tốt hơn, giúp người dùng tìm kiếm và đưa ra quyết định một cách nhanh chóng và dễ dàng.
- *Hiệu suất tốt hơn:* navigation sử dụng các kỹ thuật tối ưu để cải thiện hiệu suất ứng dụng, đảm bảo tiêu thụ ít tài nguyên hệ thống và tốc độ chuyển đổi màn hình nhanh chóng.
- *Phù hợp với nhiều kiểu điều hướng:* navigation hỗ trợ nhiều kiểu điều hướng khác nhau như điều hướng bằng button, drawer và bottom navigation bar.
- *Hỗ trợ cho việc mở rộng ứng dụng:* navigation giúp việc mở rộng ứng dụng dễ dàng hơn bằng cách giúp nhà phát triển thêm màn hình mới một cách nhanh chóng và dễ dàng.

1.3. Nguyên tắc điều hướng quan trọng

Theo trang tài liệu chính thức của Google về lập trình Android [2], việc điều hướng giữa các màn hình và ứng dụng là một phần cốt lõi trong trải nghiệm người dùng. Do đó, các nguyên tắc về điều hướng phải được tuân thủ để đảm bảo tính nhất quán và trực quan trong các ứng dụng. Thành phần navigation được thiết kế để triển khai theo các nguyên tắc mặc định, giúp đảm bảo rằng người dùng sẽ áp dụng được mô hình tương tự khi di chuyển giữa các ứng dụng.



Hình 3. List Screen (màn hình danh sách) là Điểm bắt đầu của ứng dụng được trích xuất từ website Android Developers

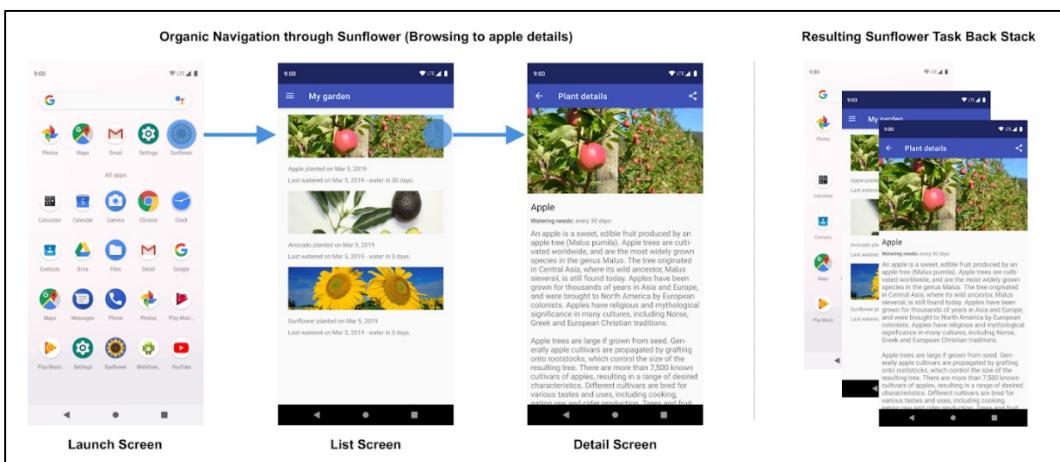
Việc triển khai navigation với Màn hình danh sách (List Screen) làm màn hình đầu tiên được hiển thị cho người dùng khi khởi chạy ứng dụng và cũng là màn hình cuối cùng được

hiển thị trước khi người dùng thoát khỏi ứng dụng đáp ứng nguyên tắc Điểm bắt đầu cố định (Fixed start destination) như ở hình 3.

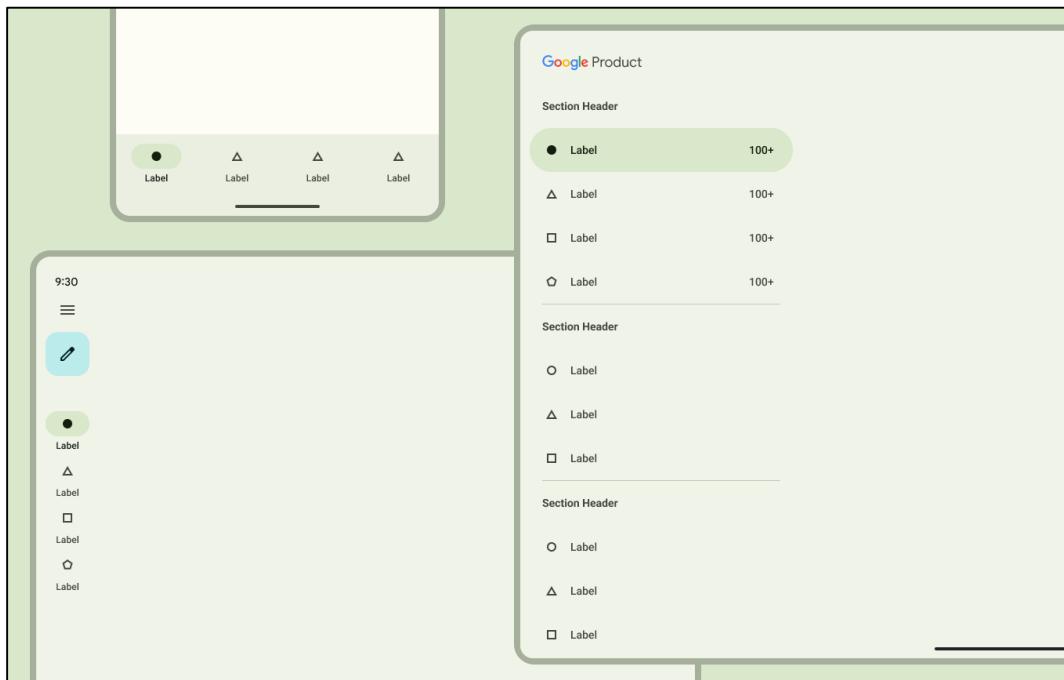
Một nguyên tắc điều hướng khác cần đảm bảo đó là Trạng thái điều hướng được thể hiện dưới dạng một ngăn xếp các đích đến [3], nơi mà màn hình bắt đầu của tác vụ được hiển thị làm cơ sở cho trạng thái điều hướng của ứng dụng. Khi chạy ứng dụng lần đầu, một tác vụ mới được tạo ra và điểm bắt đầu của tác vụ này sẽ được hiển thị. Ngăn xếp lui được sử dụng để lưu trữ lịch sử các đích đến mà người dùng đã truy cập, với đích đến mới nhất được đặt ở đầu ngăn xếp. Người dùng có thể thực hiện các thao tác như đẩy đích đến mới lên đầu ngăn xếp hoặc xóa đích đến trên cùng để thay đổi ngăn xếp lui. Khi người dùng chọn một đích đến nào đó, thì đích đến đó sẽ trở thành đích đến mới nhất và được đặt ở đầu ngăn xếp.

1.4. Xử lý các thay đổi về cấu hình

Nếu nguyên tắc điều hướng của Android giúp nhóm phát triển xây dựng việc điều hướng trong ứng dụng một cách nhất quán và trực quan, thì giao diện người dùng thích ứng cung cấp đích đến nội dung thích ứng và thường bao gồm nhiều loại phần tử điều hướng để đáp ứng các thay đổi về kích thước hiển thị (hình 4). Ví dụ: thanh điều hướng ở cuối màn hình nhỏ, dài điều hướng trên màn hình trung bình hoặc ngắn điều hướng cố định trên màn hình lớn, nhưng giao diện người dùng thích ứng vẫn phải tuân thủ các nguyên tắc điều hướng.



Hình 4. Điều hướng người dùng và kết quả là chuyển đến ngăn xếp lui được trích từ website Android Developers



Hình 5. Màn hình mở rộng, trung bình và nhỏ gọn có ngăn điều hướng, dài điều hướng và thanh dưới cùng màn hình trích từ website Material Design

Trong thiết kế theo nguyên tắc Material Design [4], phần điều hướng có kích thước ổn định nằm ở phía trên cùng và có thể di chuyển xuống phía dưới khi ứng dụng thu nhỏ. Trong giao diện người dùng thích ứng, phần điều hướng thường bao gồm nhiều loại phần tử để đáp ứng các thay đổi về kích thước hiển thị. Các lớp kích thước cửa sổ có thể giúp xác định và đặt phần điều hướng ở vị trí dễ tiếp cận nhất, và việc lựa chọn loại phần điều hướng phụ thuộc vào kích thước cửa sổ ứng dụng và số lượng mục cần chứa trong phần điều hướng. Trong thiết kế theo nguyên tắc Material Design, phần điều hướng có kích thước ổn định nằm ở phía trên cùng và có thể di chuyển xuống phía dưới khi ứng dụng thu nhỏ như minh họa trong hình 5.

Việc sử dụng navigation không chỉ đáp ứng yêu cầu cho mở rộng phần hiện thị nội dung mà giao diện ứng dụng cũng phải mang đến trải nghiệm người dùng lý tưởng cho các kích thước cửa sổ nhất định, ngay cả khi sử dụng bộ cục và tiện ích hoàn toàn khác nhau. Bảng 1 trình bày các lớp kích thước và vị trí của thành phần điều hướng.

Trong phạm vi bài giới thiệu, chúng tôi đề xuất triển khai điều hướng chung trong giao diện người dùng thích ứng.

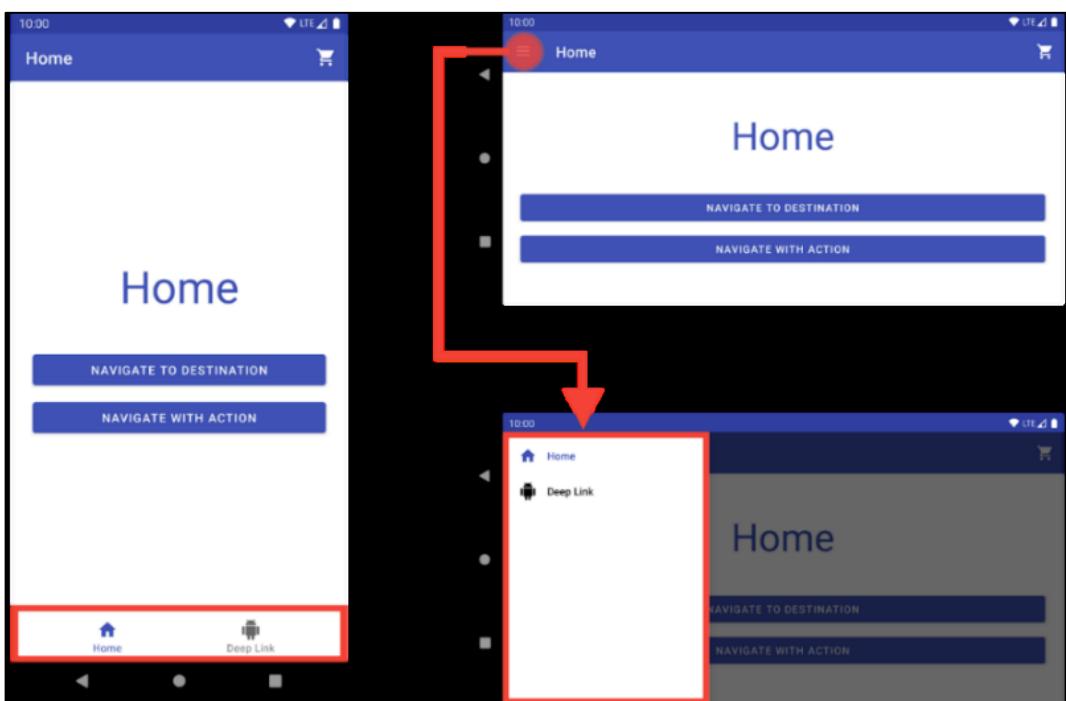
Bảng 1. Các lớp kích thước và vị trí của thành phần điều hướng

Lớp kích thước cửa sổ	Một vài mục	Nhiều mục
Chiều rộng thu gọn	Thanh điều hướng ở dưới cùng	Ngăn điều hướng (cạnh trên hoặc cuối)
Chiều rộng trung bình	Ray điều hướng	Ngăn điều hướng (cạnh trên)
Chiều rộng được mở rộng	Dài điều hướng	Ngăn điều hướng cố định (cạnh trên)

Khi triển khai điều hướng chung trong giao diện người dùng thích ứng tập trung vào việc điều chỉnh các yếu tố của giao diện để phù hợp với các thay đổi về môi trường. Việc điều chỉnh chiều rộng, chiều cao, hướng và ngôn ngữ của giao diện đều có ảnh hưởng lớn đến trải nghiệm người dùng. Các thuộc tính môi trường này được gọi là cấu hình của thiết bị, và đối

với việc triển khai navigation, các nhà phát triển cần chú ý đến cách bố trí các thành phần điều hướng để chúng phù hợp với cấu hình thiết bị [4].

Các kích thước và hướng thiết bị khác nhau sẽ được linh động chuyển đổi giữa navigation drawer hoặc bottom navigation tùy vào nhu cầu sử dụng. Điều này giúp đảm bảo rằng các thành phần điều hướng luôn được đặt ở vị trí dễ tiếp cận nhất cho người dùng, bất kể họ đang sử dụng thiết bị có kích thước và hướng khác nhau. Tuy nhiên, việc triển khai navigation cần phải thuận tiện và dễ sử dụng cho người dùng, bao gồm cả việc đảm bảo tính tương thích với các kích thước và hướng thiết bị khác nhau [6]. Hình 6 minh họa các thành phần điều hướng sử dụng bottom navigation và navigation drawer để hiển thị trình đơn điều hướng trên các thiết bị trích từ website Android Developers.



Hình 6. Thành phần điều hướng sử dụng bottom navigation và navigation drawer để hiển thị trình đơn điều hướng trên các thiết bị trích từ website Android Developers

Phần còn lại của bài báo được tổ chức như sau: Trong mục 2, mô tả chi tiết thành phần điều hướng navigation drawer và bottom navigation và quy trình xây dựng ứng dụng sử dụng thành phần điều hướng navigation drawer và bottom navigation. Mục 3 trình bày kết quả thực nghiệm của chúng tôi và mục 4 tổng kết các vấn đề đã đề cập và đề xuất hướng phát triển.

2. MỘT SỐ DẠNG NAVIGATION THƯỜNG DÙNG VÀ QUI TRÌNH KHỞI TẠO

2.1. Bottom navigation

2.1.1. Bottom navigation là gì ?

Bottom navigation là thanh điều hướng nằm ở phím dưới màn hình giúp dễ dàng chuyển đổi giữa các top - level views trong ứng dụng. bottom navigation được sử dụng khi ứng dụng có từ 3 đến 5 top-level views. Hình 7 thể hiện một ví dụ về bottom navigation [8][9].

Lưu ý: Bottom navigation sẽ không hỗ trợ từ 6 top-level views trở lên.

2.1.2. Qui trình khởi tạo

Bước 1:

Thêm bottomnavigation View widget vào file *activity_main.xml*. Sau đó thêm FrameLayout để load Fragments khi navigation item click được chọn.

Code file *activity_main.xml*:

```
<FrameLayout
    android:id="@+id/frame_container"
    android:layout_width="match_parent"
    android:layout_height="match_parent">
</FrameLayout>

<com.google.android.material.bottomnavigation.BottomNavigationView
    android:id="@+id/navigation"
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:layout_gravity="bottom"
    android:background="?android:attr/windowBackground"
    app:itemBackground="@color/bgBottomNavigation"
    android:foreground="?attr/selectableItemBackground"
    app:itemIconTint="@android:color/white"
    app:itemTextColor="@android:color/white"
    app:menu="@menu/navigation" />
```



Hình 7. Bottom navigation

Bước 2:

Bottom navigation items được rendered vào bằng việc sử dụng một file menu, hãy tạo một file xml mới đặt tên là *navigation.xml* trong thư mục res/menu.

Code file *navigation.xml*:

```
<menu xmlns:android="http://schemas.android.com/apk/res/android">
    <item
        android:id="@+id/navigation_shop"
        android:icon="@drawable/ic_store_white_24dp"
        android:title="@string/title_shop" />
    <item
        android:id="@+id/navigation_gifts"
        android:icon="@drawable/ic_card_giftpcard_white_24dp"
        android:title="@string/title_gifts" />
    <item
        android:id="@+id/navigation_cart"
        android:icon="@drawable/ic_shopping_cart_white_24dp"
        android:title="@string/title_cart" />
    <item
        android:id="@+id/navigation_profile"
        android:icon="@drawable/ic_person_white_24dp"
```

```

</menu>
        android:title="@string/title_profile" />
```

Bước 3: Tạo fragment mới: res/layout/New/Fragment/Fragment (Blank) đặt tên cho Fragment chọn Finish. Tương tự như vậy tạo thêm ba mảnh khác nhau và viết code xử lý cho từng Fragment.

Bước 4: Mở file MainActivity.java và tùy chỉnh theo mong muốn của nhà phát triển ứng dụng.

Code file MainActivity.java:

```

public class MainActivity extends AppCompatActivity {
    private ActionBar toolbar;
    Fragment f;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        toolbar = getSupportActionBar();
        toolbar.setBackgroundDrawable(new
ColorDrawable(getApplicationContext().getColor(R.color.bgBottomNavigation)));
        BottomNavigationView navigation = (BottomNavigationView)
findViewById(R.id.navigation);
        navigation.setOnNavigationItemSelectedListener
(mOnNavigationItemSelectedListener);
        toolbar.setTitle("Shop");
        f= new FirstFragment();
        loadFragment(f);
        ...
    }
    private void loadFragment(Fragment k)
    {
        FragmentTransaction tra =
getSupportFragmentManager().beginTransaction();
        tra.replace(R.id.frame_container, k);
        tra.addToBackStack(null);
        tra.commit();
    }
}
```

Trong ví dụ này *OnNavigationItemSelectedListener* sẽ được gọi khi bottom navigation item được chọn sẽ thay đổi tiêu đề toolbar và hiển thị fragment tương ứng vào trong FrameLayout.

2.2. Navigation drawer

2.2.1. Navigation drawer là gì?

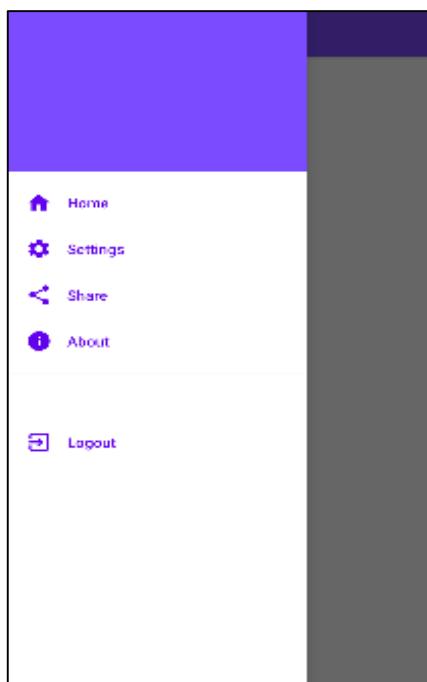
Navigation drawer là một menu hiển thị như là một ngăn kéo ở cạnh bên của màn hình. Nó được ẩn đi khi không sử dụng nhưng ngăn này sẽ xuất hiện khi người dùng nhấn vào biểu tượng Hamburger button trong thanh ứng dụng hoặc khi người dùng vuốt từ mép trái màn hình. Hình 8 thể hiện một ví dụ về navigation drawer [7].

2.2.2. Qui trình khởi tạo

Bước 1: Thêm drawer vào Layout

Để thêm được navigation drawer, cần khai báo DrawerLayout như một view gốc. Bên trong DrawerLayout, thêm view có chứa nội dung chính của layout (ví dụ: FrameLayout,...) và một view khác chứa nội dung của navigation drawer.

```
<?xml version="1.0" encoding="utf-8"?>
<androidx.drawerlayout.widget.DrawerLayout
    android:id="@+id/drawer_layout"
    android:fitsSystemWindows="true"
    tools:openDrawer="start"
    tools:context=".MainActivity">
    <com.google.android.material.navigation.NavigationView
        android:layout_width="wrap_content"
        android:layout_height="match_parent"
        android:id="@+id/nav_view"
        android:layout_gravity="start"
        app:itemIconTint="@color/purple_500"
        app:itemTextColor="@color/purple_500"/>
</androidx.drawerlayout.widget.DrawerLayout>
```



Hình 8. Navigation drawer

Lưu ý:

Khi sử dụng FrameLayout thì thiết lập match_parent với cả chiều rộng và chiều cao. Vì nó sẽ hiển thị giao diện khi navigation drawer ẩn.

Về phần navigation View thì phải chỉnh thanh ngang với thuộc tính android:layout_gravity. Thiết lập giá trị với "start" để navigation drawer xuất hiện từ bên trái ra.

navigation View nên được thiết lập thuộc tính android:fitsSystemWindows bằng "true" để đảm bảo nội dung của navigation drawer không được phủ lên thanh trạng thái và các hệ thống khác.

Bước 2: Khai báo các item menu cho navigation drawer

Để có thể cấu hình danh sách Menu Item trong navigation drawer thì sử dụng thuộc tính app:menu, Giống như code ở bên dưới:

```
<com.google.android.material.navigation.NavigationView
...
    app:menu="@menu/nav_menu"/>
```

Sau đó tạo menu tương ứng với tên: nav_menu.xml

```
<?xml version="1.0" encoding="utf-8"?>
<menu
    xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    tools:showIn="navigation_view">

    <group
        android:checkableBehavior="single">
        <item
            android:id="@+id/nav_home"
            android:icon="@drawable/ic_home"
            android:title="Home" />
        <item
            android:id="@+id/nav_settings"
            android:icon="@drawable/ic_settings"
            android:title="Settings" />
    </group>

    <item
        android:title="">
        <menu>
            <item
                android:id="@+id/nav_exit"
                android:icon="@drawable/ic_exit"
                android:title="Logout"/>
        </menu>
    </item>
</menu>
```

Ngoài ra, có thể tạo nhóm với các item riêng biệt bằng cách sử dụng thuộc tính *android:checkableBehavior="single"* được thiết lập ở nhóm. Nó cho phép hiển thị danh sách các item có trong menu.

Bước 3: Thêm Header cho navigation drawer

Có thể thêm Header tại phía trên của drawer bằng cách sử dụng thuộc tính app:headerLayout như code phía bên dưới:

```
<com.google.android.material.navigation.NavigationView
...
    app:headerLayout="@layout/nav_header"/>
```

Và sau tạo layout Header với tên: nav_header.xml

```

<?xml version="1.0" encoding="utf-8"?>
<LinearLayout
    xmlns:android="http://schemas.android.com/apk/res/android"
    android:layout_width="match_parent"
    android:layout_height="176dp"
    android:background="@color/colorPrimary"
    android:gravity="bottom"
    android:padding="16dp"
    android:theme="@style/Theme.AppCompat.Light.NoActionBar">

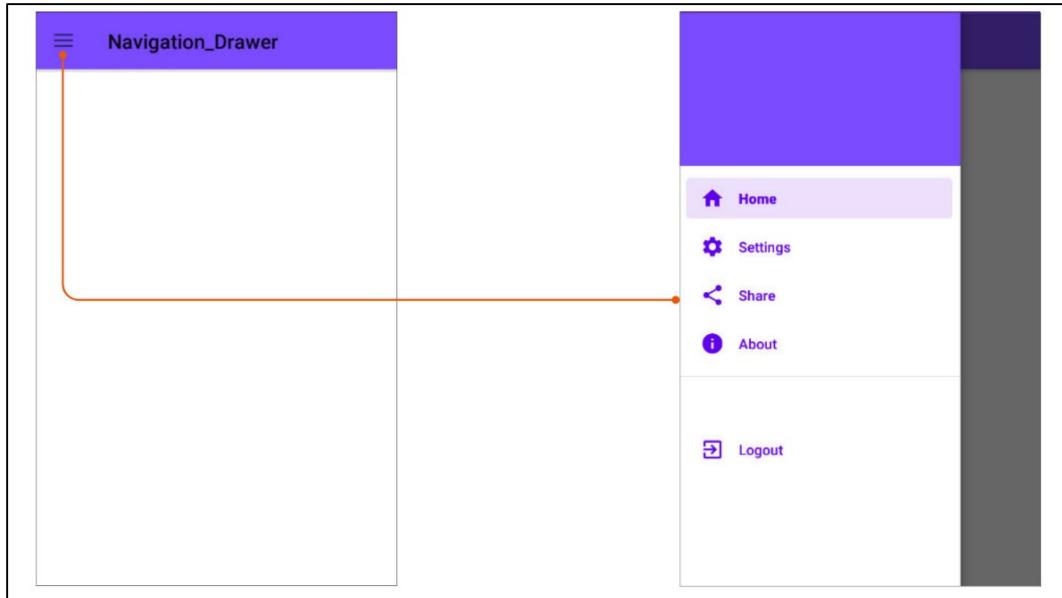
    <TextView
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:layout_marginBottom="16dp"
        android:textColor="@color/white"
        android:textSize="14sp" />

</LinearLayout>

```

Bước 4: Thêm Toolbar

DrawerLayout đã cung cấp cho người dùng mở và đóng navigation drawer chỉ với việc vuốt bên mép của màn hình. Nhưng nếu giao diện bao gồm có cả ActionBar, nên cho phép người dùng đóng mở Drawer bằng cách nhấn vào Icon Drawer ở góc phía trên bên trái của ActionBar. Hình 9 minh họa thao tác đóng/mở navigation drawer.



Hình 9. Click vào icon drawer trên thanh toolbar sẽ mở navigation drawer

Navigation drawer nên được xuất hiện ở phía trước ActionBar. Để có thể tạo được nó, thì cần phải sử dụng đến Toolbar. Để có thể thêm Toolbar vào layout chúng ta làm như code phía bên dưới:

```

<androidx.drawerlayout.widget.DrawerLayout
...
<LinearLayout
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:orientation="vertical">

    <androidx.appcompat.widget.Toolbar
        android:layout_width="match_parent"
        android:layout_height="56dp"
        android:id="@+id/toolbar"
        android:elevation="4dp"
        android:background="@color/colorPrimary"
        android:theme="@style/Theme.AppCompat.Light.NoActionBar"
        android:popupTheme="@style/ThemeOverlay.AppCompat.Light"
/>

    <FrameLayout
        ...>

</LinearLayout>
...
</androidx.drawerlayout.widget.DrawerLayout>

```

Sau đó vào folder themes thiết lập như sau:

```

<resources xmlns:tools="http://schemas.android.com/tools">
    <style name="..." ...
parent="Theme.MaterialComponents.DayNight.NoActionBar">
    ...
</style>
</resources>

```

Thiết lập Toolbar trong MainActivity.java:

Lúc này, Toolbar đã xuất hiện trong layout nhưng không có chức năng như ActionBar. Để có thể áp dụng Toolbar như ActionBar, đầu tiên phải chắc chắn rằng Activity đã được thừa kế từ AppCompatActivity. Sau đó gọi setSupportActionBar(); và truyền toolbar vào:

```

public class MainActivity extends AppCompatActivity {
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        Toolbar toolbar = findViewById(R.id.toolbar);
        setSupportActionBar(toolbar);
    }
}

```

Tuy nhiên, đến đây Icon Drawer vẫn chưa xuất hiện vì sẽ sử dụng toggle button trên Toolbar, nên tiếp tục thực hiện bước kế tiếp:

Bước 5: Xử lý Click sự kiện cho navigation drawer

Để nhận sự kiện khi người sử dụng chạm vào của danh sách item trong DrawerLayout, thực thi câu lệnh OnNavigationItemSelectedListener và gắn nó tới NavigationView bằng cách gọi setNavigationItemSelectedListener(), như sau:

```
public class MainActivity extends AppCompatActivity implements
NavigationView.OnNavigationItemSelectedListener {
    private DrawerLayout drawerLayout;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        ...
        drawerLayout = findViewById(R.id.drawer_layout);
        NavigationView navigationView = findViewById(R.id.nav_view);
        navigationView.setNavigationItemSelectedListener(this);
    }
    @Override
    public boolean onNavigationItemSelected(@NonNull MenuItem item) {
        switch (item.getItemId()) {
            case R.id.nav_home:
                //
                break;
            case R.id.nav_settings:
                //
                break;
            case R.id.nav_exit:
                //
                break;
        }
        drawerLayout.closeDrawer(GravityCompat.START);
        return true;
    }
}
```

Khi mà item được chạm, đoạn code này sẽ thiết lập lựa chọn item và DrawerLayout cũng được đóng bởi hàm closeDrawers().

Sử dụng ActionBarDrawerToggle để đồng bộ hóa trạng thái của DrawerLayout tương ứng với trạng thái củaActionBar, cung cấp giao diện điều khiển DrawerLayout dễ sử dụng và người dùng dễ dàng hiểu được chức năng của nó.

Khi khởi tạo ActionBarDrawerToggle yêu cầu truyền vào 5 tham số: ActionBarDrawerToggle (this, drawerLayout, toolbar, R.string.open_Navigation, R.string.close_Navigation):

- Activity hiện tại (this).
- DrawerLayout sẽ được hiển thị thông qua component navigation drawer (drawerLayout được khởi tạo trước đó).
- Toolbar: tổng quan trên giao diện người dùng cho Activity chứa các nút điều hướng, tiêu đề và các element khác.
- Tham số 4 và 5 chỉ định văn bản sẽ được hiển thị khi drawer được mở ra hoặc đóng lại.

Tiếp đến sẽ sử dụng drawerLayout.addDrawerListener(toggle) để đăng ký một DrawerListener với DrawerLayout, khi DrawerLayout thay đổi, DrawerListener sẽ được cập nhật và thực hiện một số xử lý. Và DrawerListener được dùng để lắng nghe sự kiện đóng hay mở DrawerLayout và thay đổi trạng thái.

```
public class MainActivity extends AppCompatActivity implements
NavigationView.OnNavigationItemSelectedListener {

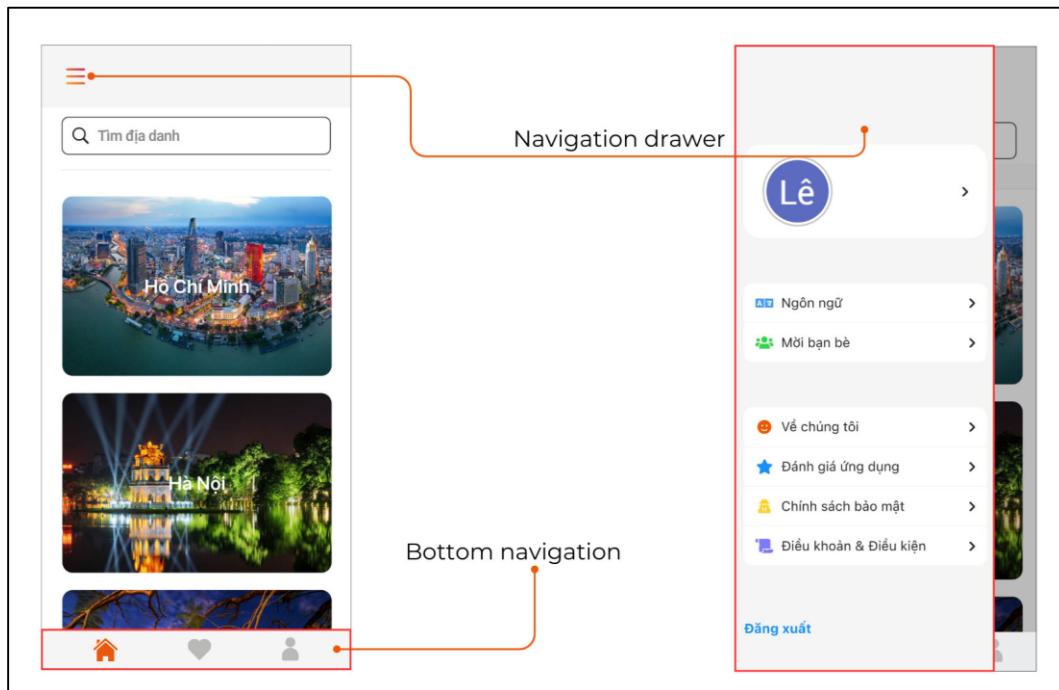
    private DrawerLayout drawerLayout;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        ...
        drawerLayout = findViewById(R.id.drawer_layout);
        NavigationView navigationView = findViewById(R.id.nav_view);
        navigationView.setNavigationItemSelectedListener(this);
        ActionBarDrawerToggle toggle = new
        ActionBarDrawerToggle(this, drawerLayout, toolbar,
        R.string.open_Navigation, R.string.close_Navigation);
        drawerLayout.addDrawerListener(toggle);
        toggle.syncState();
    }
    ...
}
```

ActionBarDrawerToggle được sử dụng để đặt một toggle button trên Toolbar để bật/tắt DrawerLayout; và đến đây thì Icon Drawer cũng sẽ xuất hiện. Khi DrawerLayout được mở ra, Icon của toggle button trên Toolbar sẽ được thay đổi từ biểu tượng của tiêu đề Activity sang biểu tượng của DrawerLayout. Khi DrawerLayout đã được đóng, Icon của toggle button sẽ được đặt lại về trạng thái như mới khởi đầu [5].

3. KẾT QUẢ THỰC NGHIỆM

Thông qua việc tìm hiểu và nghiên cứu, chúng tôi ứng dụng navigation vào trong thiết kế của dự án “Quảng bá địa điểm du lịch tại Việt Nam”. Dự án “Quảng bá địa điểm du lịch tại Việt Nam” là một ứng dụng di động trên nền tảng Android, được thiết kế để cung cấp thông tin toàn diện về các địa điểm du lịch tại Việt Nam cho người dùng. Ứng dụng còn có các chức năng chính như là cung cấp thông tin chi tiết của từng địa điểm du lịch, bao gồm hình ảnh, vị trí, đánh giá của khách hàng và nhiều thông tin hữu ích khác. Ngoài ra, còn cho phép người dùng đăng nhập và tạo tài khoản cá nhân để theo dõi các địa điểm yêu thích của mình, lưu trữ với các địa điểm mà mình mong muốn ghé thăm trong tương lai và trao đổi với những người dùng khác.

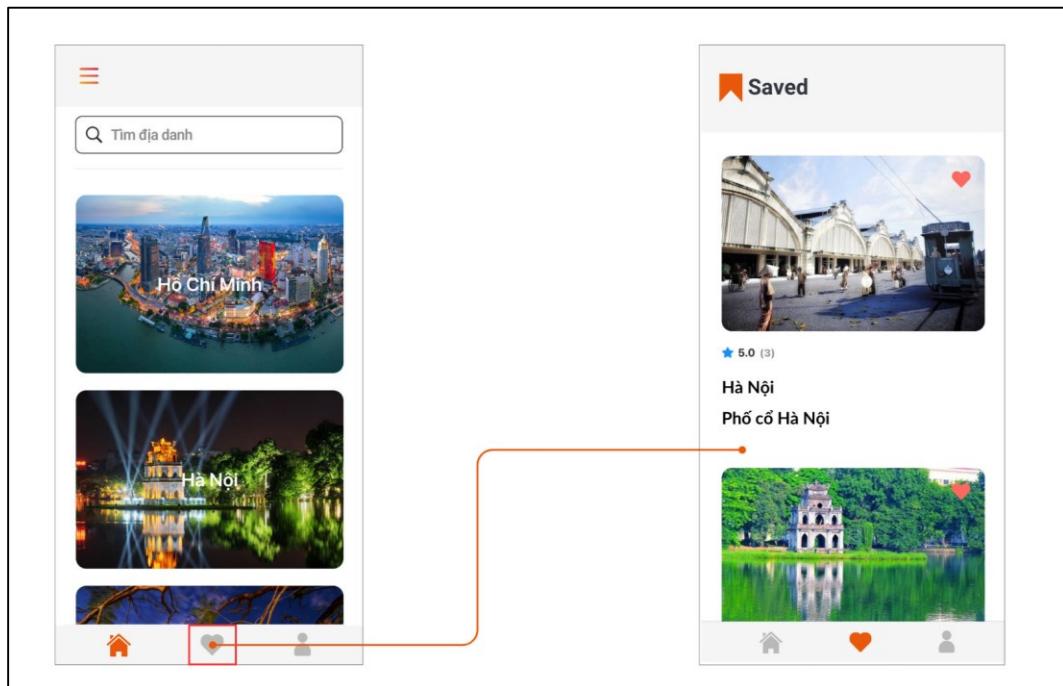
Trong ứng dụng “Quảng bá địa điểm du lịch tại Việt Nam” sử dụng cả hai bottom navigation và navigation drawer để tăng hiệu quả trải nghiệm cho người dùng, giúp người dùng dễ dàng tương tác trong việc tìm kiếm thông tin và điều hướng các màn hình, như hình 10:



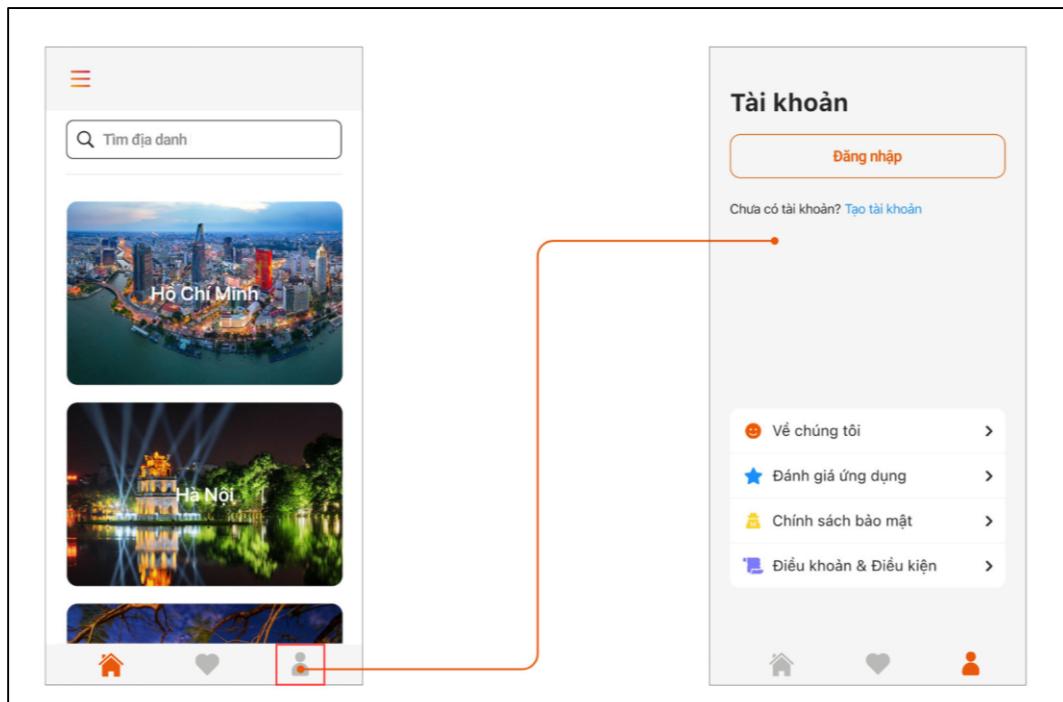
Hình 10. Dùng bottom navigation và navigation drawer trong thiết kế giao diện ứng dụng "Quảng bá địa điểm du lịch tại Việt Nam"

Về phần bottom navigation, bằng cách đặt các chức năng chính của ứng dụng ở phía dưới màn hình, người dùng có thể truy cập đến các chức năng đó một cách nhanh chóng và thuận tiện. Trong ứng dụng "Quảng bá địa điểm du lịch tại Việt Nam", bottom navigation cung cấp các chức năng như trang chủ, địa điểm yêu thích và tài khoản (hình 11 và hình 12).

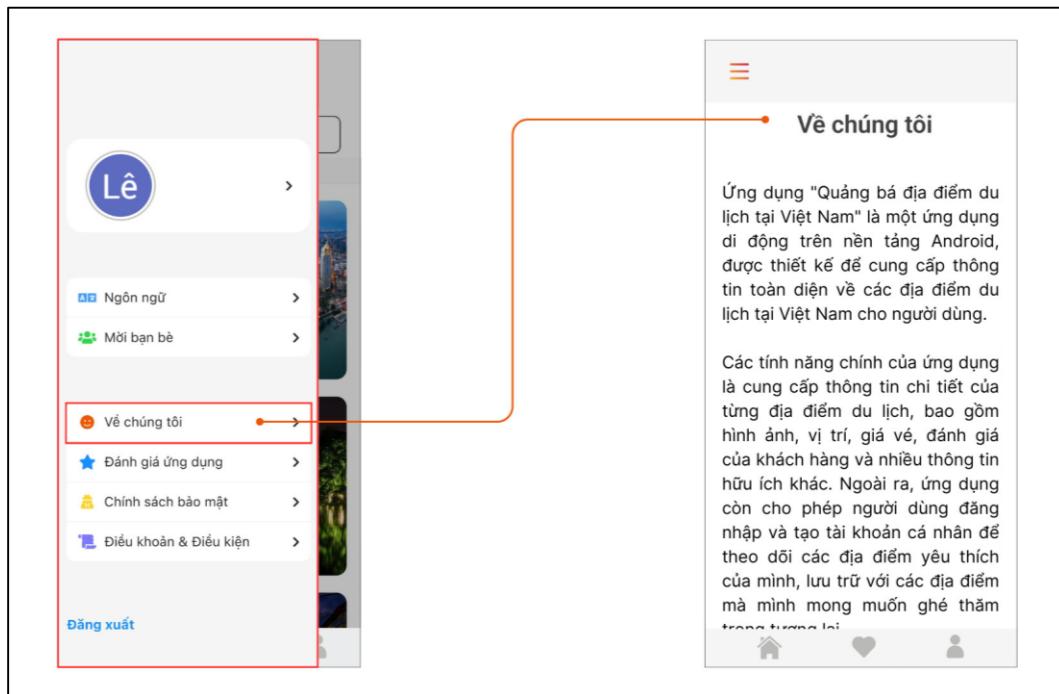
Về phần navigation drawer, việc thêm menu trượt ở cạnh bên trái màn hình cho phép người dùng dễ dàng tiếp cận các tính năng tùy chọn như: điều khoản – điều kiện, thông tin ứng dụng, đăng xuất. Menu được hiển thị khi người dùng thực hiện hành động chạm kéo từ cạnh bên trái của màn hình.



Hình 11. Dùng bottom navigation điều hướng đến chức năng địa điểm yêu thích



Hình 12. Dùng bottom navigation điều hướng đến chức năng tài khoản



Hình 13. Dùng navigation drawer điều hướng đến chức năng thông tin ứng dụng

Sự kết hợp giữa bottom navigation và navigation drawer giúp thao tác điều hướng và truy cập các tính năng chính trở nên mượt mà hơn. Bên cạnh đó, cả hai kiểu navigation này được thiết kế đơn giản và thân thiện dễ tiếp cận người dùng, tạo nên sự tương tác trực quan và hấp dẫn cho người dùng sử dụng ứng dụng "Quảng bá địa điểm du lịch tại Việt Nam".

Tóm lại, sau khi tiến hành thực nghiệm bằng cách tích hợp navigation vào trong thiết kế của ứng dụng lập trình di động "Quảng bá địa điểm du lịch tại Việt Nam", chúng tôi nhận thấy rằng việc sử dụng bottom navigation và navigation drawer đã tăng hiệu quả trải nghiệm cho người dùng. Việc sử dụng navigation trong thiết kế giao diện ứng dụng lập trình di động Android đã cải thiện trải nghiệm người dùng một cách đáng kể và giúp tăng cường tính năng của ứng dụng, đặc biệt trong việc điều hướng các màn hình của ứng dụng.

4. KẾT LUẬN

Trong bài báo này, chúng tôi trình bày tổng quát về một số dạng navigation dựa trên trang web cung cấp tài liệu chính thức của Google về lập trình Android [2], nêu chi tiết các bước thực hiện cơ bản để tạo các navigation vào một ứng dụng android. Đồng thời, chúng tôi tiến hành phát triển ứng dụng "Quảng bá địa điểm du lịch tại Việt Nam" có dùng bottom navigation và navigation drawer. Qua đó cho thấy những ưu điểm và hạn chế của từng loại công cụ này trong việc giúp người dùng điều hướng trên các ứng dụng di động. Navigation drawer với khả năng hiển thị nhiều tùy chọn điều hướng khác nhau trong một menu ẩn giúp tiết kiệm không gian màn hình vì vậy phù hợp với các ứng dụng có nhiều tùy chọn điều hướng. Tuy nhiên navigation drawer có hạn chế là gây khó khăn cho người mới sử dụng ứng dụng và khởi động chậm hơn. Bottom navigation giúp tăng tính trực quan, giúp người dùng thực hiện điều hướng dễ dàng và chuyển đổi giữa các tùy chọn một cách nhanh chóng, tuy nhiên nó có giới hạn về số lượng tùy chọn điều hướng được hiển thị.

Tùy thuộc vào nhu cầu và yêu cầu của ứng dụng, sự lựa chọn giữa navigation drawer và bottom navigation là quan trọng để đảm bảo tính tiện dụng và hiệu quả cho người dùng khi

sử dụng ứng dụng, hoặc có thể kết hợp cả hai loại này nhưng cần được xác định phù hợp với tính chất và mục đích của ứng dụng.

TÀI LIỆU THAM KHẢO

1. Android Developers. *Navigation*. Truy cập ngày 25/4/2023, từ <https://developer.android.com/guide/navigation>
2. Google. *Android Developers*. Truy cập ngày 25/4/2023, từ <https://developer.android.com>
3. Android Developers. *Principles of navigation*. Truy cập ngày 25/4/2023, từ https://developer.android.com/guide/navigation/navigation-principles#fixed_start_destination
4. Google. *Material Design*. Truy cập ngày 25/4/2023, từ <https://m3.material.io/foundations/layout/understanding-layout/parts-of-layout>
5. Android Developers. *Handling configuration changes*. Truy cập ngày 25/4/2023, từ <https://developer.android.com/guide/navigation/navigation-config-changes>
6. Trần Minh Hải. (2018). *Cách tạo Navigation Drawer*. Truy cập ngày 25/4/2023, từ <https://viblo.asia/p/cach-tao-navigation-drawer-ByEZk0NElQ0>
7. Trần Minh Hải. (2018). *Hướng dẫn Bottom Navigation Bar trong Android (Phần 1)*. Truy cập ngày 25/4/2023, từ <https://viblo.asia/p/huong-dan-bottom-navigation-bar-trong-android-phan-1-RQqKLvLpl7z>
8. Nguyễn Minh Quân. (2018). *Làm việc với Bottom Navigation trong Android*. Truy cập ngày 25/4/2023, từ <https://viblo.asia/p/lam-viec-voi-bottom-navigation-trong-android-gJ59j6pKX2>
9. Material Design. *Bottom navigation*. Truy cập ngày 25/4/2023, từ <https://m2.material.io/components/bottom-navigation/android>

ABSTRACT

USING NAVIGATION IN MOBILE ANDROID PROGRAMMING INTERFACE DESIGN

**Le Minh Phat^{1,*}, Le Tam Nhu¹, Ngo Thi Kim Ngan¹, Nguyen Thi Kim Tuyen¹,
Nguyen Thi Bich Ngan¹**

¹*Ho Chi Minh City University of Food Industry*

**Email: lephat508@gmail.com*

In this paper, we introduce the design and handling of navigation in developing the user interface of Android mobile applications. The paper emphasizes the importance and benefits of navigation for user experience. Additionally, we provide a detailed process for building two popular types of navigation, bottom navigation and navigation drawer. Furthermore, we conducted experiments by incorporating these two types of navigation into the design of the user interface during the development of the Android mobile application “Promoting tourist destinations in Vietnam”. The results showed that the application has a beautiful and user-friendly interface, providing an enjoyable experience for users through the effectiveness of the implemented navigations.

Keywords: Navigation, bottom navigation, navigation drawer.

XÂY DỰNG RESTFUL API VÀ GỌI API TỪ ỨNG DỤNG TRONG LẬP TRÌNH DI ĐỘNG ANDROID

Vũ Ngô Đạt^{1,*}, Vũ Văn Vinh¹, Nguyễn Thị Bích Ngân¹

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: datcy2011@gmail.com

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trong bài báo này, chúng tôi sẽ tập trung vào quy trình xây dựng RESTful API (REpresentational State Transfer – một giao thức chung giúp các ứng dụng đa nền tảng giao tiếp với nhau) và cách gọi API (Application programming interface) từ một ứng dụng di động chạy trên hệ điều hành android (gọi vẫn tắt là ứng dụng di động android). RESTful API là một tập các định nghĩa quy tắc được sử dụng phổ biến để làm cầu nối giữa các hệ thống phần mềm với nhau, có thể là phương án thay thế cho việc lấy dữ liệu theo cách truyền thống từ một hệ quản trị cơ sở dữ liệu như SQL Server, SQLite, MySQL và một số hệ quản trị khác. Hiện nay các ứng dụng di động cần phải tương tác với các dịch vụ web và gọi API để truy xuất dữ liệu, thực hiện các chức năng phức tạp, và tương tác với người dùng. Các ứng dụng di động đa dạng từ mạng xã hội, mua sắm trực tuyến, đặt chỗ, dịch vụ giao thông, và nhiều lĩnh vực khác đều cần tích hợp API để đáp ứng nhu cầu ngày càng cao của người dùng. Trong bài báo này, chúng tôi đề xuất cách xây dựng RESTful API đơn giản bằng cách sử dụng các công cụ như Node.js và Express, đồng thời triển khai ứng dụng lên nền tảng lưu trữ web trực tuyến Vercel. Sau đó tiến hành thực hiện gọi API từ một ứng dụng di động android. Bên cạnh đó chúng tôi tiến hành thực nghiệm bằng cách áp dụng phương pháp đề xuất vào ứng dụng di động nghe nhạc. Chúng tôi xây dựng API lấy dữ liệu các file nhạc từ hệ thống nghe nhạc số ZingMP3 và chuyển về cho ứng dụng của chúng tôi.

Từ khóa: RESTful Web APIs, Vercel, lập trình di động android

1. GIỚI THIỆU

Ngày nay, với sự phát triển không ngừng của công nghệ thông tin, việc kết nối và truy cập dữ liệu thông qua mạng Internet đã trở nên phổ biến hơn bao giờ hết. Đặc biệt, với sự phổ biến của thiết bị di động như smartphone, tablet, smart watch làm cho việc truy cập thông tin mọi lúc mọi nơi đã trở nên dễ dàng hơn bao giờ hết. Hơn nữa, các thiết bị di động, đặc biệt là các thiết bị chạy trên hệ điều hành Android, đã trở thành một phần quan trọng trong cuộc sống của chúng ta. Việc kết hợp RESTful API và thiết bị di động Android sẽ giúp các nhà phát triển tận dụng các tính năng của thiết bị di động để cung cấp các dịch vụ web linh hoạt và dễ sử dụng cho người dùng. Bằng cách sử dụng các thư viện của Android để gọi RESTful API, các nhà phát triển có thể cung cấp các tính năng đáp ứng nhanh chóng cho ứng dụng của mình [1].

Với sự phát triển của công nghệ, việc xây dựng RESTful API và gọi API từ thiết bị di động Android sẽ trở thành xu hướng tương lai trong lĩnh vực phát triển ứng dụng. Bài báo này

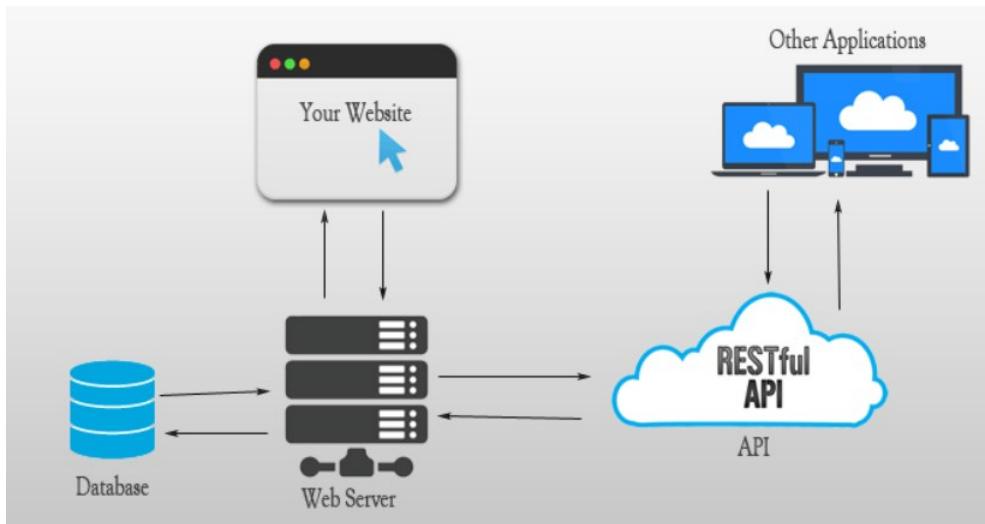
tập trung vào việc xây dựng RESTful API và gọi API từ ứng dụng di động Android và cung cấp các giải pháp và khuyến nghị cho các nhà phát triển để cải thiện hiệu suất của API[1].

Bài báo này sẽ cung cấp cho độc giả một cái nhìn tổng quan về quá trình xây dựng RESTfull API, bao gồm cách thiết kế giao diện lập trình ứng dụng API, cách triển khai và triển khai ứng dụng lên hệ thống lưu trữ của web server. Bên cạnh đó, bài báo cũng sẽ giới thiệu cách gọi API từ thiết bị di động Android.

Phần còn lại của bài báo được tổ chức như sau: trong mục 2, chúng tôi trình bày các sơ sở lý thuyết của việc xây dựng RESTful API; mục 3 trình bày quy trình xây dựng RESTful API và các bước thực hiện gọi API từ một ứng dụng di động; phần thực nghiệm được trình bày trong mục 4 và trong mục 5, chúng tôi tổng kết các vấn đề chính của bài báo.

2. CƠ SỞ LÝ THUYẾT

Về cơ bản thì API là tập hợp các quy tắc và hoạt động như các phương tiện giao tiếp. Điểm khác biệt duy nhất giữa chúng chính là Web service là một ứng dụng phần mềm cho phép các ứng dụng trao đổi dữ liệu với nhau thông qua giao thức HTTP hoặc HTTPS. Dữ liệu được truyền đi dưới dạng XML hoặc JSON. API là một phương thức trung gian cho phép các hệ thống hoặc ứng dụng riêng biệt “giao tiếp” với nhau thông qua các yêu cầu và phản hồi. API cung cấp một cách tiêu chuẩn hóa để các ứng dụng khác tương tác với hệ thống hoặc ứng dụng đó [3]. Hình 1 thể hiện vai trò của API trong hệ thống phần mềm lập trình hiện đại.



Hình 1. API ứng dụng trong lập trình hiện đại

REST (REpresentational State Transfer) là một dạng chuyển đổi cấu trúc dữ liệu, tập hợp các ràng buộc để tạo ra dịch vụ web có khả năng mở rộng và dễ bảo trì. Trong REST, các tài nguyên được xác định bởi một URI (Uniform Resource Identifier) duy nhất và trạng thái của tài nguyên được biểu hiện dưới dạng các Hypermedia link. Các Hypermedia link này cho phép người dùng có thể tương tác với tài nguyên và thực hiện các thao tác như truy xuất, cập nhật và xóa dữ liệu. Các RESTfull hiện nay sử dụng các phương thức HTTP như GET, POST, PUT và DELETE để thực hiện các tương tác với tài nguyên:

- GET: dùng để truy xuất dữ liệu từ tài nguyên.

- POST: dùng để tạo tài nguyên mới.
- PUT: dùng để cập nhật tài nguyên hiện hành.
- DELETE: dùng để xóa tài nguyên khỏi hệ thống.

Ưu điểm khi sử dụng API để tích hợp với các ứng dụng với nhau nhằm tăng cường sự giao tiếp giữa các phần mềm ứng dụng một cách linh hoạt và nhanh chóng, khuyến khích sự đổi mới về mặt truy cập dữ liệu, dịch vụ từ các phần mềm, hệ thống. Đẩy nhanh quá trình phát triển phần mềm, phát triển linh hoạt các chức năng hay dịch vụ mới mà không cần phải xây dựng lại từ đầu, đồng thời là cắt giảm bớt được chi phí phát sinh và thời gian để xây dựng chức năng mới [2].

Tuy nhiên, việc phát triển API là điều không hề đơn giản, đòi hỏi lập trình viên phải có hiểu biết rộng rãi, có kinh nghiệm trong việc tích hợp API và cũng phải luôn cập nhật xu hướng mới về lĩnh vực này. Vấn đề bảo mật là mối quan tâm hàng đầu khi xây dựng và tích hợp API. Việc rò rỉ thông tin, dữ liệu nhạy cảm sẽ ảnh hưởng tiêu cực đến công ty, đồng thời tác động đến niềm tin của khách hàng. Vì vậy cần phải đảm bảo API hoạt động một cách an toàn và bảo mật.

Về phần triển khai RESTful API, chúng tôi đề xuất quá trình xây dựng web service đơn giản với Express Framework. Express là một framework dành riêng cho NodeJs. Nó cung cấp nhiều tính năng mạnh mẽ trên nền tảng web cũng như ứng dụng di động, hỗ trợ các phương thức HTTP và middleware, từ đó tạo ra một API vô cùng mạnh mẽ và dễ sử dụng. Sau đó, chúng tôi sẽ hướng dẫn cách triển khai web service lên Vercel để từ đó có thể truy cập đến web service và lấy được API [1].

Sau khi ứng dụng RESTful API đã trực tuyến, tiến hành gọi API từ android sử dụng thư viện chuẩn của java.net, không sử dụng bất kì thư viện bên thứ 3 nào khác.

3. QUY TRÌNH XÂY DỰNG, TRIỂN KHAI RESTFULL API VÀ GỌI API TỪ ỨNG DỤNG DI ĐỘNG

3.1. Quy trình xây dựng và triển khai RESTfull API

3.1.1. Các cấu trúc và định nghĩa

```
{
  "id": 1,
  "type": "dog",
  "price": 249.99
},
```

Hình 2. Ví dụ về dữ liệu trả về

RESTful API sử dụng một access token (là một chuỗi được sinh ra giúp xác định thông tin của một gói dữ liệu) tương ứng với mỗi request [1]. Cấu trúc của dữ liệu được trả về có dạng như trong hình 2.

Các status code sẽ được trả về sau khi HTTP request đã xong. Các status code thường gặp trong bảng 1.

Giả sử có một ứng dụng chia sẻ nhạc, cần cung cấp thông tin các bài hát, album, nghệ sĩ và vài thông tin khác trong hệ thống. Mặc dù URI thay đổi khi truy xuất giữa các tài nguyên khác nhau nhưng về cơ bản thì cấu trúc của chúng tương tự nhau.

Ví dụ: <https://DomainName.com/api/XX.X/resource/>

Thay thế **DomainName.com** với tên miền của ứng dụng web đã được triển khai trên web server.

- Thay thế **XX.X** với phiên bản API muốn sử dụng.
- Thay resource bằng các API Endpoint được mô tả tại bảng 2.

Bảng 1. Các mã phản hồi từ giao thức HTTP

Mã phản hồi	Mô tả
200 OK	Request thành công cho các phương thức GET, PUT, PATCH hoặc DELETE.
201 Create	Tài nguyên vừa được tạo thành công.
204 No Content	Tài nguyên được xóa thành công.
400 Bad Request	Yêu cầu không hợp lệ.
401 Unauthorized	Yêu cầu chưa được xác thực.
403 Forbidden	Không có quyền truy cập tới tài nguyên.
404 Not Found	Không tìm thấy tài nguyên từ URI.
405 Method Not Allowed	Phương thức không cho phép với user hiện hành.
410 Gone	Tài nguyên không còn tồn tại, phiên bản cũ đã không còn hỗ trợ.
415 Unsupported Media Type	Không hỗ trợ kiểu tài nguyên này.
429 Too Many Requests	Tùy chói vì yêu cầu vượt quá số lần giới hạn.

Header: là nơi chứa các thông tin cần thiết của request tương ứng, nhưng người dùng cuối (end-users) không biết đến sự tồn tại của nó. RESTfull API hỗ trợ một số tiêu chuẩn HTTP header chung. Một số header thường gặp:

- HTTP Accept: cho biết định dạng mà máy chủ trả về (response), có giá trị dưới dạng application/json hoặc application/xml. Thường thì mặc định nó là application/json.
- HTTP Content-type: cho biết định dạng của nội dung yêu cầu (request body), có giá trị dưới dạng application/json hoặc application/xml. Thường thì mặc định nó là application/json.
- HTTP Authorization: cung cấp “khóa truy cập” OAuth 2.0 để xác thực người dùng.

Request body (Nội dung yêu cầu): là một chuỗi trong request nhằm để cung cấp thông tin, chẳng hạn như các trường để cập nhật bản ghi. Request body có thể là dữ liệu dưới dạng JSON hoặc XML [2].

Bảng 2. Bảng mô tả các API endpoint tương ứng với các thao tác trên tài nguyên của shop thú cưng.

Tên	API endpoint	Phương thức HTTP	Mô tả
INDEX	/pets	GET	Hiển thị danh sách toàn bộ thú cưng.
CREATE	/pets	POST	Thêm một thú cưng mới vào CSDL.
SHOW	/pets/:id	GET	Hiển thông tin của 1 thú cưng.
UPDATE	/pets/:id	PUT	Cập nhật thông tin của thú cưng cụ thể.
DESTROY	/pets/:id	DELETE	Xóa dữ liệu của một thú cưng cụ thể.

3.1.2. Thiết lập và xây dựng ứng dụng RESTful API

Đầu tiên, cần phải xây dựng các phương thức để ứng dụng có thể tương tác được thì cần phải xây dựng các tuyến đường (routes) để từ các tuyến đường đó, ta mới có thể tương tác với tài nguyên chung của hệ thống.

Tiến hành xây dựng ứng dụng web với NodeJS và ExpressJS cùng với các gói thư viện hỗ trợ (package) giúp việc xây dựng RESTful API trở nên dễ dàng hơn. NodeJS là một nền tảng được xây dựng trên “V8 Javascript engine” của Chrome, được viết bằng C++ và Javascript. ExpressJS là một web framework được xây dựng dựa trên nền tảng NodeJS, cung cấp các hàm HTTP và middleware để tạo API đơn giản và dễ sử dụng.

Sau đây là các bước khởi tạo ứng dụng RESTful API [4]:

- Có thể sử dụng lệnh của NPM (Node package manager – một công cụ để tạo và quản lý thư viện lập trình Javascript dành cho NodeJS) để khởi tạo một dự án mới bằng lệnh: npm init

- Sau khi đã khởi tạo thành công dự án, mở cửa sổ terminal và chuyển đến thư mục dự án, nhập câu lệnh sau để cài đặt toàn bộ thư viện (dependencies) cần thiết cho dự án: npm install

- Tiến hành cài đặt gói express bằng lệnh: npm install express

- Tạo file index.js tại thư mục đó, sau đó viết lệnh khởi tạo server như ở hình 3. Ở đây chúng tôi đang thiết lập server chạy tại port 7000, có thể đổi sang port khác tùy ý miễn là nó không bị trùng với các port đang được sử dụng. Sử dụng câu lệnh node index để khởi động server.

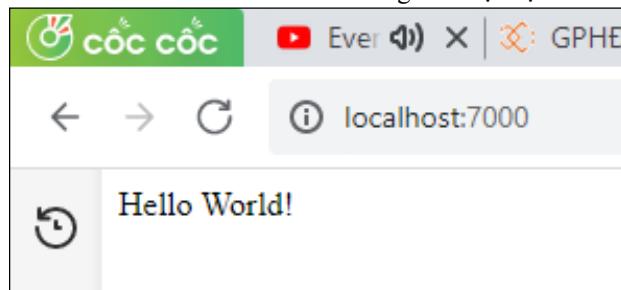
```
var server = app.listen(7000, function () {
  console.log('Listening on port %d', server.address().port);
});
```

Hình 3. Đoạn lệnh khởi tạo server

- Khi server khởi động thành công, truy cập theo địa chỉ http://localhost: 7000. Trình duyệt sẽ hiện thông báo lỗi: “Cannot GET /”. Lỗi này xảy ra là vì chưa định nghĩa bất kì router nào cho website cả. Nên tiếp theo, định nghĩa một router GET bằng expressJS với đoạn code ở hình 4. Nó có ý nghĩa là khi truy cập vào trang web thì mặc định server sẽ trả kết quả là “Hello World!” (hình 5).

```
app.get('/', (req, res) => {
    res.send('Hello World');
});
```

Hình 4. Router GET với đường dẫn mặc định



Hình 5. Kết quả trả về từ server

Dựa trên cấu trúc dữ liệu trả về ở hình 2, có thể tạo được một mảng các thú cưng. Mảng này sẽ được sử dụng để thao tác dữ liệu thông qua API. Tiến hành tạo các API endpoint tương ứng trên bảng 2, sẽ được những phương thức ở hình 6 và 7.

```
23 // Get all pet
24 router.get('/pets', (req, res, next) => {
25     res.json(petList);
26 });
27 // Get a specific pet by ID
28 router.get('/pets/:id', (req, res) => {
29     const id = parseInt(req.params.id);
30     const pet = petList.find((p) => p.id === id);
31
32     if (!pet) {
33         res.status(404).json({ message: `Pet with ID ${id} not found` });
34     } else {
35         res.json(pet);
36     }
37 });
38
39 // Create a new pet in the petList
40 router.post('/pets', (req, res) => {
41     try {
42         const newPet = {
43             id: petList.length + 1,
44             type: req.body.type,
45             price: req.body.price,
46         };
47         petList.push(newPet);
48         res.status(201).json(newPet);
49     } catch (err) {
50         console.error(err);
51         res.status(500).send(`Internal Server Error: ${err} || ${req.body}`);
52     }
53 });
```

Hình 6. Định tuyến cho các phương thức INDEX, SHOW, CREATE

```

54 // Update an existing pet by ID
55 router.put('/pets/:id', (req, res) => {
56   const id = parseInt(req.params.id);
57   const petIndex = petList.findIndex((p) => p.id === id);
58
59   if (petIndex === -1) {
60     res.status(404).json({ message: `Pet with ID ${id} not found` });
61   } else {
62     const { type, price } = req.body;
63     const pet = { id, type, price };
64     petList[petIndex] = pet;
65     res.json(pet);
66   }
67 });
68 // Delete a pet by ID
69 router.delete('/pets/:id', (req, res) => {
70   const id = parseInt(req.params.id);
71   const petIndex = petList.findIndex((p) => p.id === id);
72
73   if (petIndex === -1) {
74     res.status(404).json({ message: `Pet with ID ${id} not found` });
75   } else {
76     petList.splice(petIndex, 1);
77     res.status(204).json({ message: `Pet with ID ${id} has successfully deleted!` });
78   }
79 });

```

Hình 7. Định tuyến cho các phương thức UPDATE, DESTROY

3.1.3. Triển khai ứng dụng trên web server

Sau khi đã xây dựng hoàn tất ứng dụng, để ai cũng có thể truy cập vào RESTful API ở bất kì nơi đâu thì cần phải triển khai ứng dụng lên trên web server, phổ biến nhất là trên nền tảng Vercel. Nhưng để triển khai được thì cần phải đẩy toàn bộ source code (mã nguồn) của dự án lên Vercel. Có thể sử dụng các công cụ quản lý phiên bản source code như Github, Gitlab, Bitbucket.

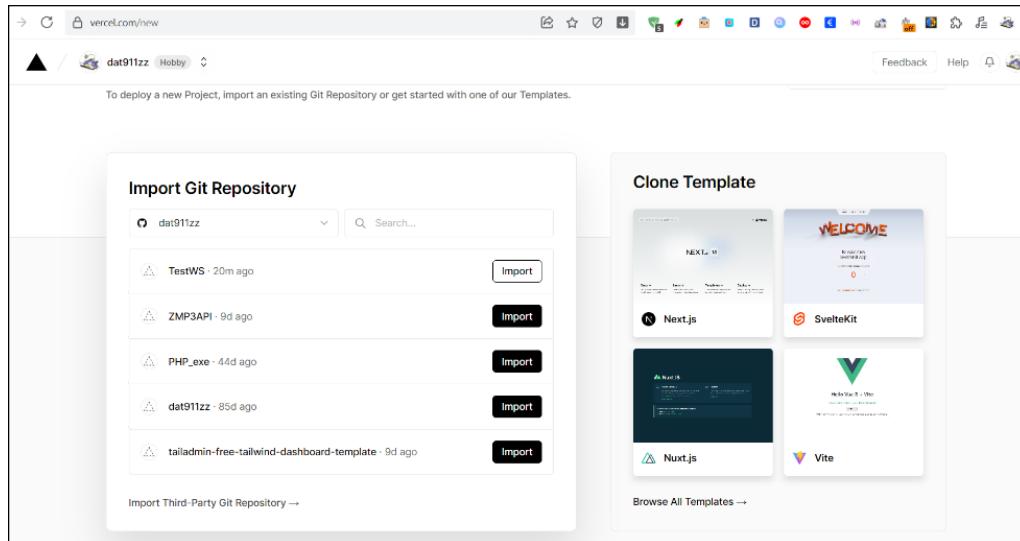
Đăng nhập vào Github và tạo một project mới và tiến hành đẩy source code lên Github bằng các lệnh sau:

- git init
- git remote add origin https://github.com/dat911zz/TestWS.git
- git add .
- git commit -m “init commit”
- git push -u origin master

Đường dẫn <https://github.com/dat911zz/TestWS.git> là đường dẫn liên kết của project, có thể tìm thấy khi mới khởi tạo project trong Github. Có thể thay đổi thành đường dẫn khác tùy vào project được tạo mới.

Bước tiếp theo là ta sẽ đăng nhập vào Vercel bằng tài khoản Github. Rồi chọn project muốn đẩy lên Vercel (Hình 8). Sau khi chọn xong, hệ thống trả về màn hình Câu hình project rồi chọn Deploy. Nhưng có vấn đề phát sinh là nó vẫn chưa chạy được như mong muốn mà nó chỉ trả về kết quả trong hình 9.

Vấn đề này xảy ra là do chưa có tệp cấu hình của vercel và đồng thời chưa có khai báo export module cho Express app. Giải pháp để khắc phục vấn đề này là tạo thêm một tệp tên là vercel.json ở ngay thư mục gốc của dự án với cú pháp khai báo trong hình 10. Đồng thời trong index.js thêm và dòng cuối cùng đoạn lệnh sau: `module.exports = app`



Hình 8. Danh sách các project để chọn để upload code lên web server



Hình 9. Kết quả sai với dự đoán

```
▲ vercel.json > ...
1  {
2      "version": 2,
3      "builds": [
4          {
5              "src": "index.js",
6              "use": "@now/node"
7          }
8      ],
9      "routes": [
10         {
11             "src": "/(.*)",
12             "dest": "index.js"
13         }
14     ]
15 }
```

Hình 10. Khai báo trong file vercel.json

3.2. Gọi API từ ứng dụng trên thiết bị di động Android

Trước tiên, cần xây dựng một lớp để kết nối đến API được chỉ định. Cấu trúc của phương thức để kết nối đến URL và lấy dữ liệu như trong hình 12. Để thực hiện thao tác tạo mới và cập nhật dữ liệu thì phải thêm phương thức kết nối đến URL, đồng thời đẩy dữ liệu đã nén dưới dạng Json. Nhưng điều kiện tiên quyết để ứng dụng di động có thể sử dụng được mạng là phải cung cấp quyền cho ứng dụng trước tại file AndroidManifest.xml (Hình 13).

Trên phương thức xử lý của module gọi API mà chúng tôi đề xuất ở trên có sử dụng tới HttpURLConnection. Đây là một API được cung cấp bởi Java giúp kết nối và tương tác với các nguồn tài nguyên thông qua giao thức HTTP hoặc HTTPS. Nó cho phép ứng dụng tạo kết nối tới server, gửi các yêu cầu HTTP như GET, POST, PUT, DELETE và đồng thời có thể nhận lại phản hồi từ server [4].

Biến myUrl có thể hiểu đơn giản là nó lưu trữ đường dẫn tới API muốn truy xuất thông tin. Chỉ cần gán đường dẫn đến API cần lấy và việc còn lại là phương thức sẽ xử lý từ đường dẫn.

API sẽ trả kết quả là chuỗi JSON hoặc XML, việc còn lại của chúng là trích xuất chuỗi kết quả ấy thành đối tượng hoặc là chỉ trích xuất chuỗi kết quả ra thôi. Có thể sử dụng các thư viện như Gson hay Jackson để chuyển đổi Json sang java object.

```

String urlString = params[0];
String result;
String inputLine;
try {
    //Create a URL object holding our url
    URL myUrl = new URL(urlString);
    //Create a connection
    HttpURLConnection connection =(HttpURLConnection) myUrl.openConnection();
    //Set methods and timeouts
    connection.setRequestMethod("GET");
    connection.setReadTimeout(10000);
    connection.setConnectTimeout(10000);
    //Connect to our url
    connection.connect();
    //Create a new InputStreamReader
    InputStreamReader streamReader = new InputStreamReader(connection.getInputStream());
    //Create a new buffered reader and String Builder
    BufferedReader reader = new BufferedReader(streamReader);
    StringBuilder stringBuilder = new StringBuilder();
    //Check if the line we are reading is not null
    while((inputLine = reader.readLine()) != null){
        stringBuilder.append(inputLine);
    }
    //Close our InputStream and Buffered reader
    reader.close();
    streamReader.close();
    //Set our result equal to our stringBuilder
    result = stringBuilder.toString();
}
catch(IOException e){
    e.printStackTrace();
    result = null;
}

```

Hình 12. Phương thức xử lý của module gọi API

```

<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />

```

Hình 13. Khai báo quyền truy cập vào Internet cho thiết bị di động Android

Ta sẽ định nghĩa các phương thức để thực hiện xử lý gọi API cùng với các phương thức HTTP tương ứng: GET, POST, PUT, DELETE (Hình 14). Tiến hành thao tác với API sẽ được các đoạn mã trong hình 15.

Chỉ cần vài phương thức đơn giản là đã có thể gọi API được từ ngay trong chính ứng dụng di động đang xử lý.

```

2 usages
public String getRequest(String path, String... param){
    HttpRequest httpRequest = new HttpRequest();
    return executeRequest(httpRequest, path, param);
}

1 usage
public String postRequest(String payload){
    HttpPayloadRequest httpRequest = new HttpPayloadRequest();
    httpRequest.execute( ...params: hostAPI + "pets", payload, "POST");
    return "ok";
}

1 usage
public String putRequest(String payload){
    HttpPayloadRequest httpRequest = new HttpPayloadRequest();
    httpRequest.execute( ...params: hostAPI + "pets", payload , "PUT");
    return "ok";
}

1 usage
public String deleteRequest(String path, String... param){
    HttpRequest httpRequest = new HttpRequest( ...method: "DELETE");
    return executeRequest(httpRequest, path, param);
}

```

Hình 14. Các phương thức xử lý cho các phương thức HTTP

```

// Initialize the list of pets
petList = getList(api.getRequest( path: "pets"));

//Create new pet
JSONObject obj = new JSONObject();
obj.put( name: "type", pet.getType());
obj.put( name: "price", pet.getPrice());
api.postRequest(obj.toString());

//Edit pet
JSONObject obj = new JSONObject();
obj.put( name: "type", pet.getType());
obj.put( name: "price", pet.getPrice());
api.putRequest(String.valueOf(obj));

//Delete pet
api.deleteRequest( path: "pets", petList.get(position).getId());

```

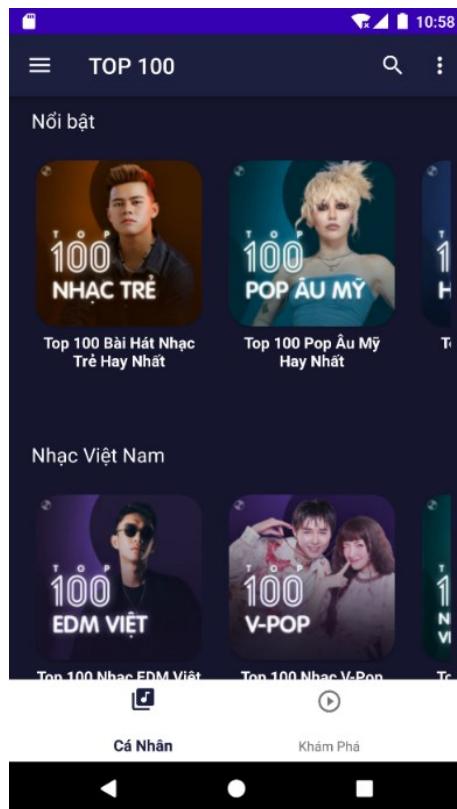
Hình 15. Thao tác dữ liệu với API

4. KẾT QUẢ THỰC NGHIỆM

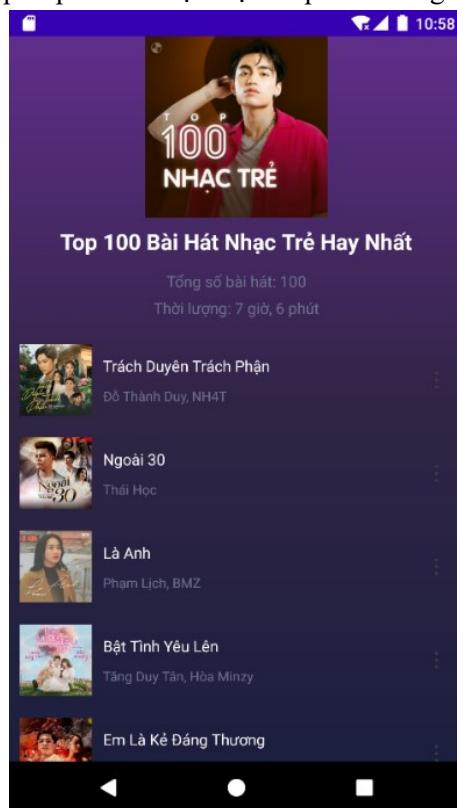
Chúng tôi đã xây dựng một RESTful API để lấy thông tin bài hát cùng nhiều nội dung khác liên quan đến ứng dụng âm nhạc ZingMP3. Chúng tôi đã triển khai ứng dụng và thu được kết quả khi truy xuất đến API theo kết quả được thống kê ở bảng 3. Link demo API: <https://cringe-mp3-api.vercel.app/api-docs/>

Bảng 3: Thống kê các API endpoint hiện hành

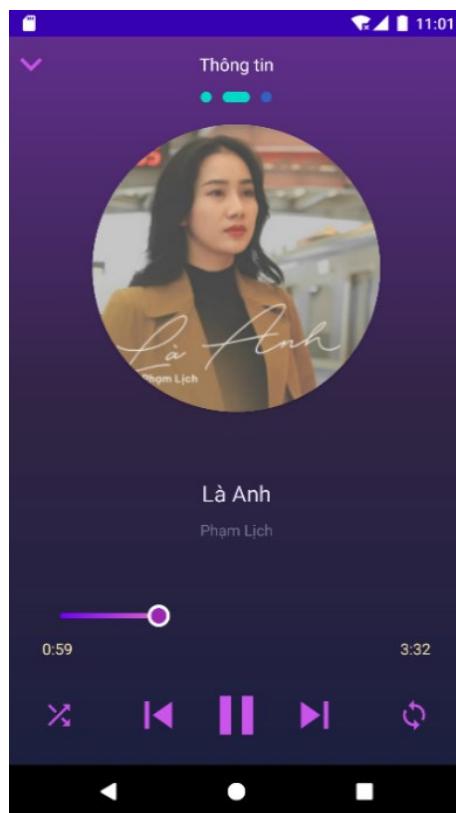
API endpoint	Phương thức HTTP	Mô tả	Đường dẫn kết quả
/top100	GET	Lấy danh sách tổng hợp top 100 của nhiều thể loại, vùng miền.	https://cringe-mp3-api.vercel.app/api/top100
/getStreaming/:id	GET	Lấy đường dẫn phát nhạc của bài hát dựa vào id bài hát.	https://cringe-mp3-api.vercel.app/api/getStreaming/ZWABWOFZ
/getSongInfo/:id	GET	Lấy thông tin của một bài hát dựa vào id bài hát.	https://cringe-mp3-api.vercel.app/api/getSongInfo/ZWABWOFZ
/getLyric/:id	GET	Lấy lời bài hát dựa vào id bài hát.	https://cringe-mp3-api.vercel.app/api/getLyric/ZWABWOFZ
/getDetailPlaylist/:id	GET	Lấy thông tin danh sách phát dựa trên id.	https://cringe-mp3-api.vercel.app/api/getPlaylist/ZWZB969E
/getDetailArtist/:alias	GET	Lấy thông tin của nghệ sĩ dựa trên bí danh.	https://cringe-mp3-api.vercel.app/api/getArtist/Dunghoangpham
/search/:keyword	GET	Tìm kiếm bài hát, ca sĩ, album dựa trên từ khóa.	https://cringe-mp3-api.vercel.app/api/search/Mot%20buoc%20yeu%20van%20dam%20da



Hình 16. Gọi api top100 và hiện thị kết quả trên ứng dụng nghe nhạc.



Hình 17. Hiện thị danh sách của playlist top100 nhạc trẻ.



Hình 18. Lấy bài hát tương ứng, hiện thị thông tin ra màn hình, đồng thời phát nhạc.

Chúng tôi cũng thu được kết quả sau khi cài đặt hàm và gọi API đã được triển khai trên nền tảng lưu trữ web trực tuyến Vercel từ ứng dụng chạy trên nền tảng thiết bị Android và áp dụng vào dự án từ hình 16 đến 18.

5. KẾT LUẬN

Trong bài báo cáo này, chúng ta đã tìm hiểu về RESTful API và cách gọi API từ thiết bị di động Android, các phương pháp gọi API như sử dụng thư viện HttpURLConnection, cũng như cách xử lý dữ liệu trả về từ API. Đồng thời cũng đã thực hiện các bước để kết nối với API và hiển thị dữ liệu trên thiết bị di động Android.

Tóm lại, việc tìm hiểu về RESTful API và cách gọi API từ thiết bị di động Android là một kỹ năng quan trọng đối với các nhà phát triển ứng dụng di động. Có thể thấy rằng RESTful API là một công nghệ linh hoạt và tiện lợi, và việc sử dụng các thư viện có sẵn như HttpURLConnection, từ đó giúp ta hiểu được cách mà các thư viện như Volley hay Retrofit hoạt động như thế nào trong việc phát triển ứng dụng. Hướng nghiên cứu của chúng tôi là thực hiện như xây dựng ứng dụng phát nhạc đa nền tảng, đặc biệt là trên thiết bị di động Android.

TÀI LIỆU THAM KHẢO

1. Vladimir Maskov, Implementing REST Client for Android, Metropolia, University of Applied Sciences, 2020.
2. Salesforce group, REST API Developer Guide, ebook, 2023.
3. Ashraff Hathibelagal, Android from scratch: Using REST API, truy cập ngày 25/4/2023 từ <https://code.tutsplus.com/vi/tutorials/android-from-scratch-using-rest-apis--cms-27117>
4. Ian Blair (CEO and Co-Founder of BuildFire), How to Create a RESTful API For Your Mobile App, 2022. Truy cập ngày 25/4/2023 <https://buildfire.com/create-restful-api-mobile-app/>

ABSTRACT

BUILD RESTFUL API AND CALL API FROM AN APPLICATION IN ANDROID MOBILE PROGRAMMING

Vu Ngo Dat^{1,*}, Vu Van Vinh¹, Nguyen Thi Bich Ngan¹

¹Ho Chi Minh City University of Food Industry

*Email: datcy2011@gmail.com

In this paper, we focus on the process of building a RESTful API (REpresentational State Transfer - a common protocol that helps cross-platform applications communicate with each other) and how to call an API (Application programming interface) from an mobile application running on the Android operating system (referred to as android mobile applications for short). A RESTful API is a set of rule definitions commonly used to bridge software systems, which can be an alternative to traditional data retrieval from a database management system. databases such as SQL Server, SQLite, MySQL and some other management systems. Nowadays, mobile applications need to interact with web services and call APIs to retrieve data, perform complex functions, and interact with users. Mobile applications ranging from social networking, online shopping, booking, transportation services, and many more need API integration to meet the increasing needs of users. In our paper, we suggest how to build a simple RESTful API using tools like Node.js and Express, and deploy the application to the online web hosting platform Vercel, then proceed to make an API call from an android mobile app. Besides, we conduct an experiment by applying the proposed method to a music listening mobile application. We build an API that takes music files from the ZingMP3 digital music system and transfers it to our application.

Keywords: RESTful Web APIs, Vercel, android mobile programming

HUFI-ELAB: HỆ THỐNG QUẢN LÝ PHÒNG THÍ NGHIỆM TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM (HUFI)

**Trần Trương Tuấn Phát¹, Đặng Trần Khánh^{1,*}, Tống Đăng Khoa¹, Nguyễn
Trọng Nghĩa¹, Lê Trạng Lân¹**

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

*Email: khanh@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Trường Đại học Công nghiệp Thực phẩm (HUFI) có khoảng 6 khoa và 2 trung tâm trực thuộc với hơn 2000 sinh viên thực hành và sử dụng các hoá chất và thiết bị trong phòng thí nghiệm (PTN). Hiện tại, các PTN đang được vận hành và quản lý thủ công thông qua các hồ sơ giấy được lưu trữ trên các bản cứng hoặc quản lý qua Excel. Tuy vậy, các công việc sắp xếp, tổ chức và quản lý, cụ thể là hoá chất, thiết bị, báo cáo, môn học, lớp học phần, thời khóa biểu, nhóm nghiên cứu,.v.v nếu làm thủ công thì tốn công sức rất lớn và không hiệu quả. Bên cạnh đó, quy trình sử dụng PTN/trang thiết bị qua nhiều bước, chưa thuận lợi cho giảng viên, sinh viên trong việc đăng ký và quản lý các hoạt động giảng dạy và nghiên cứu. Hệ thống HUFI-ELab được phân tích, thiết kế và triển khai để giải quyết những nhu cầu thực tiễn và những khó khăn của các quy trình liên quan đến PTN cho trường.

Từ khóa: Hệ thống thông tin, Chuyển đổi số, E-Lab.

ABSTRACT

HUFI-ELAB: E-LABORATORY MANAGEMENT SYSTEM OF HO CHI MINH UNIVERSITY OF FOOD INDUSTRY (HUFI)

**Tran Truong Tuan Phat¹, Dang Tran Khanh^{1,*},
Tong Dang Khoa¹, Nguyen Trong Nghia¹, Le Trang Lan**

¹*Ho Chi Minh University of Food Industry*

*Email: khanh@hufi.edu.vn

Ho Chi Minh University of Food Industry (HIFI) has about 6 faculties and 2 affiliated centers with more than 2000 students practicing and utilizing chemicals and laboratory equipment. Currently, laboratories are being operated and managed manually through paper records stored on hard copies or managed via Excel. However, the work of arranging, organizing and managing, namely chemicals, equipment, reports, subjects, classes, timetables, research groups, etc., if done manually, it is laborious and inefficient. In addition, the process of using laboratories/equipment goes through many steps, making it not convenient for lecturers and students to register and manage teaching and research activities. The HIFI-ELab system was analyzed, designed and implemented to address the practical needs and difficulties of laboratory-related processes for the school.

Keywords: Information system (IS), Digital transformation, E-Lab.

THIẾT KẾ CƠ CHẾ MÔ HÌNH HỌC LIÊN KẾT LẤY CẢM HỨNG TỪ MẠNG ETHEREUM 2.0

Trần Trương Tuấn Phát^{1,2}, Đặng Trần Khánh^{1,*}

¹Trường Đại học Công nghiệp Thực phẩm Thành phố Hồ Chí Minh

² Trường Đại học Bách Khoa - Đại học Quốc Gia Thành phố Hồ Chí Minh

*Email: khanh@hufi.edu.vn

Ngày nhận bài: 27/04/2023; Ngày chấp nhận đăng: 10/05/2023

TÓM TẮT

Học liên kết là một phương pháp học tiềm năng gần đây trong việc giải quyết các bài toán về dữ liệu silo, qua đó tận dụng được nguồn dữ liệu khổng lồ giúp tăng độ chính xác cho các bài toán học trên quy mô rộng cần thiết cho xu thế thành phố thông minh như: liên tổ chức (ví dụ: bệnh viện, ngân hàng,.v.v), Mobile Ad hoc networks (MANETs), Mobile Edge Computing (MEC), Vehicle Ad hoc Networks (VANETs), Internet of Things (IoTs),.v.v. Cụ thể, phương pháp này cần tổng hợp mô hình toàn cục từ các mô hình cục bộ được huấn luyện từ dữ liệu riêng tư của các bên tham gia.

Tuy nhiên, để mô hình đạt được độ chính xác cao và có thể cộng tác hiệu quả, từng mô hình cục bộ của các bên phải có độ đồng nhất cao (*homogeneity*) tới từng checkpoint. Bên cạnh đó, giả sử các bên đều lý trí (*rational*), một vấn đề đặt ra là làm sao để các bên có thể tối ưu hoá lợi ích, tương thích lợi ích, không thiêng vị cũng như giải quyết hiện tượng “kẻ đi xe không trả tiền”. Lấy cảm hứng từ mạng Ethereum 2.0, nhóm để xuất một cơ chế cho mô hình học liên kết giải quyết các vấn đề trên.

Từ khóa: Học liên kết, blockchain, thiết kế cơ chế, ethereum.

ABSTRACT

ETHEREUM 2.0 NETWORK-INSPIRED MECHANISM DESIGN FOR FEDERATED LEARNING

Truong Tran Tuan Phat^{1,2}, Dang Tuan Khanh^{1,*}

¹*Ho Chi Minh University of Food Industry*

²*University of Technology, Vietnam National University*

*Email: khanh@hufi.edu.vn

Federated learning is a recent potential learning method in solving data silo problems, thereby unlocking colossal data sources to increase accuracy for large-scale learning problems that play pivotal roles in smart city trends such as: cross-organization (e.g. hospitals, banks, etc.), Mobile Ad hoc networks (MANETs), Mobile Edge Computing (MEC), Vehicle Ad hoc Networks (VANETs), Internet of Things (IoTs), etc. Specifically, this method needs to aggregate a global model from local models trained from the private data of the participants.

However, for the sake of the aggregated model to achieve high accuracy and be collaborated effectively, each local model of the parties have to undergo a high degree of homogeneity to each checkpoint. In addition, assuming that all parties are rational, a problem arises that how can the parties be incentive-maximizing, incentive-compatible, be equitable as well as solve the phenomenon of "free-rider". Inspired by the Ethereum 2.0 network, we develop a mechanism for federated learning that addresses the aforementioned problems.

Keywords: Federated learning, blockchain, mechanism design, ethereum.