

ĐẠI HỌC BÁCH KHOA HÀ NỘI

# ĐỒ ÁN TỐT NGHIỆP

Nghiên cứu và đề xuất mô hình học liên kết hướng  
người dùng

ĐOÀN NGỌC KHÁNH  
khanh.dn180110@sis.hust.edu.vn

Ngành: Công nghệ thông tin

Giảng viên hướng dẫn: TS. Nguyễn Phi Lê \_\_\_\_\_

Chữ kí GVHD

Khoa: Khoa học máy tính

Trường: Công nghệ thông tin và Truyền thông

HÀ NỘI, 03/2023

# LỜI CẢM ƠN

Hơn bốn năm học đại học trôi qua thật nhanh mà cũng thật chậm. Chậm cho những giây phút đợi chờ, nhanh cho những khoảng khắc đáng nhớ mà ta đã không kịp trân trọng đúng mực. Bách Khoa đã cho tôi thật nhiều, cũng lấy đi thật nhiều, nhưng giúp tôi trưởng thành và khôn lớn. Bách Khoa là nền tảng, là bước ngoặt trong cuộc đời tôi.

Trước hết, con xin cảm ơn cha mẹ, chị gái, gia đình, và đặc biệt cảm ơn TS. Nguyễn Phi Lê. Mọi người đã luôn quan tâm, chăm sóc cho con, luôn giúp đỡ con những lúc khó khăn, lúc con đáng trách nhất.

Em xin cảm ơn cô Nguyễn Phi Lê và mọi anh chị em trong tập thể AIoT Lab. Cô là người tận tâm, chuyên cần, tận tình và thấu đáo. Cô đã chỉ dạy cho em rất nhiều, tạo cho em nhiều cơ hội học tập, tiếp xúc tốt đẹp. Được làm việc trong lab là được trao đổi với mọi người, giúp em xây dựng được hướng đi, cách nghĩ, cách làm việc.

Cảm ơn Bá Tân, Đức Long, Quang Điện, Hồng Sang, Việt Hoàng, Tiến Long, Phi Phúc, Trần Anh đã sát cánh trong suốt 4 năm đại học, cùng nhau vượt qua những khó khăn, những ngày vui và bao chuyện đáng nhớ. Cảm ơn những người bạn cấp ba vẫn luôn gắn bó với tôi.

Cuối cùng, xin được cảm ơn Bách Khoa.

# TÓM TẮT NỘI DUNG ĐỒ ÁN

Cách mạng công nghiệp lần thứ tư đem lại nhiều thay đổi lớn đối với nhân loại, đó là sự phổ biến của Internet kết nối vạn vật (IoT), dữ liệu lớn (BigData) và trí tuệ nhân tạo (AI). Các thiết bị di động với khả năng tính toán tương đối tốt ngày một phổ biến. Dữ liệu gia tăng với tốc độ hàm mũ, được lưu trữ, số hóa và trở thành tài nguyên phát triển các mô hình học máy, học sâu của trí tuệ nhân tạo. Việc huấn luyện các mô hình học sâu thông thường cần yêu cầu tập hợp dữ liệu lại trên cùng một thiết bị. Tuy nhiên, bên cạnh các nguồn dữ liệu mở, dữ liệu mang tính cá nhân, bảo mật chiếm đa số. **Học liên kết (federated learning)** ra đời như một giải pháp xây dựng mô hình học sâu từ nhiều thiết bị riêng biệt với bộ dữ liệu độc lập để đảm bảo hiệu quả tốt trên tập dữ liệu kiểm thử. **Học liên kết hướng người dùng (personalized federated learning)** là một ngữ cảnh khác khi mà mỗi thiết bị tham gia có một tập dữ liệu kiểm thử riêng bên cạnh việc có một tập dữ liệu huấn luyện riêng. Mục tiêu khi này là xây dựng cho mỗi thiết bị một mô hình riêng đạt hiệu quả cao trên bộ dữ liệu kiểm thử của chính nó. Trong những nghiên cứu gần đây về bài toán này, có một nghiên cứu mới nổi là **Personalized Federated Learning through Local Memorization** [1] đem lại hiệu quả tốt dựa trên kỹ thuật tương đối đơn giản đó là sử dụng kết hợp mô hình huấn luyện chung giữa các thiết bị với thuật toán  $K$  láng giềng gần nhất ( $KNN$ ) khi thực hiện dự đoán. Trong đồ án này, em đề xuất phương pháp huấn luyện sử dụng **học đối lập (contrastive learning)** khi huấn luyện mô hình nhằm cải thiện hiệu quả của phương pháp  $KNN$ , qua đó nâng cao hiệu quả của phương pháp trên.

## MỤC LỤC

<b>CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....</b>	<b>1</b>
1.1 Đặt vấn đề.....	1
1.1.1 Học liên kết (Federated Learning) .....	1
1.1.2 Học liên kết hướng người dùng (Personalized Federated Learning)	
3	
1.2 Các giải pháp hiện tại và hạn chế .....	4
1.3 Mục tiêu và định hướng giải pháp .....	4
1.4 Đóng góp của đề án .....	4
1.5 Bố cục đề án .....	4
<b>CHƯƠNG 2. NỀN TẢNG LÝ THUYẾT .....</b>	<b>6</b>
2.1 Kiến thức cơ bản về học máy và học sâu .....	6
2.1.1 $K$ láng giềng gần nhất .....	6
2.1.2 Thuật toán Robbins-Monro và tối ưu trong học sâu .....	6
2.1.3 Mạng tích chập , kĩ thuật kết nối tắt và mô hình MobileNet V2 .....	8
2.2 Học liên kết, học liên kết hướng người dùng và nghiên cứu <i>Personalized Federated Learning through Local Memorization</i> .....	12
2.2.1 Học liên kết .....	12
2.2.2 Học liên kết hướng người dùng.....	14
2.2.3 Nghiên cứu <i>Personalized Federated Learning through Local Memorization</i>	
14	
2.3 Học đối lập (contrastive learning).....	15
2.3.1 Contrastive Loss .....	16
2.3.2 Triplet Loss .....	16
2.3.3 NT-Xent Loss .....	16

<b>CHƯƠNG 3. PHƯƠNG PHÁP ĐỀ XUẤT.....</b>	<b>18</b>
3.1 Tổng quan giải pháp.....	18
3.2 Học đối lập theo biểu diễn cục bộ.....	18
3.3 Học đối lập kết hợp biểu diễn cục bộ và toàn cục.....	20
3.4 Phương pháp tối ưu tránh bề mặt nhọn.....	22
3.5 Kỹ thuật lấy mẫu ngẫu nhiên có trọng số (weighted random sampling).....	24
<b>CHƯƠNG 4. ĐÁNH GIÁ THỰC NGHIỆM.....</b>	<b>26</b>
4.1 Dữ liệu và phương pháp chia dữ liệu cho bài toán học liên kết.....	26
4.1.1 Dữ liệu.....	26
4.1.2 Phương pháp chia dữ liệu cho bài toán học liên kết.....	27
4.1.3 Mô tả về các trường hợp chia dữ liệu.....	30
4.2 Các tham số đánh giá.....	32
4.3 Phương pháp thí nghiệm.....	33
4.3.1 Bộ dữ liệu CIFAR-10.....	33
4.3.2 Bộ dữ liệu CIFAR-100.....	34
4.4 Quan sát về trạng thái thí nghiệm.....	35
4.5 Đánh giá kết quả thí nghiệm.....	37
<b>CHƯƠNG 5. KẾT LUẬN .....</b>	<b>42</b>
5.1 Kết luận.....	42
5.2 Hướng phát triển trong tương lai .....	42
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>45</b>

## DANH MỤC HÌNH VẼ

Hình 1.1	Sơ đồ hoạt động thuật toán FedAvg . . . . .	1
Hình 1.2	Mô hình hoạt động tại mỗi vòng của thuật toán FedAvg . . . . .	2
Hình 1.3	Hệ thống học liên kết truyền thống (trái) và hệ thống học liên kết hướng người dùng (phải) . . . . .	3
Hình 2.1	Thuật toán KNN . . . . .	6
Hình 2.2	Batch, mini-batch và stochastic gradient descent . . . . .	8
Hình 2.3	Ảnh dưới dạng 3 kênh màu . . . . .	8
Hình 2.4	Phép tích chập trên ảnh . . . . .	9
Hình 2.5	Mạng tích chập LeNet . . . . .	10
Hình 2.6	Luồng hoạt động kết nối tắt . . . . .	10
Hình 2.7	Mô hình mạng ResNet18 . . . . .	11
Hình 2.8	Tích chập tách biệt chiều sâu . . . . .	12
Hình 2.9	Học đối lập với khoảng cách Euclid . . . . .	15
Hình 2.10	Học đối lập với độ tương đồng cosine . . . . .	16
Hình 3.1	Luồng tính toán hàm mục tiêu của học đối lập theo biểu diễn cục bộ . . . . .	19
Hình 3.2	Hiện tượng thiếu nhất quán của không gian biểu diễn (inconsistency of representation space) (a) và sai lệch về biểu diễn (misalignment of representations) (b) . . . . .	20
Hình 3.3	Phương pháp SimCLR . . . . .	21
Hình 3.4	Luồng tính toán hàm mục tiêu của học đối lập kết hợp biểu diễn cục bộ và toàn cục . . . . .	21
Hình 3.5	Đồ thị hàm mục tiêu trên tập huấn luyện (đen) và kiểm thử (đỏ), các điểm cực tiểu "nhọn" và "phẳng" [19] . . . . .	22
Hình 3.6	Hướng cập nhật của SAM so với gradient descent thông thường	25
Hình 4.1	Bộ dữ liệu CIFAR-10 . . . . .	26
Hình 4.2	Bộ dữ liệu CIFAR-100 với chia tiết phân tầng về lớp . . . . .	27
Hình 4.3	Biểu diễn mật độ của phân phối Dirichlet đối xứng bậc 3 . . . . .	28
Hình 4.4	(CIFAR-10) Tỷ lệ về số mẫu xuất hiện trong từng thiết bị . . . . .	30
Hình 4.5	(CIFAR-10) Số lượng thiết bị theo số lượng nhãn xuất hiện trong tập dữ liệu huấn luyện . . . . .	31
Hình 4.6	(CIFAR-10) Histogram về kích thước các tập dữ liệu huấn luyện	31

Hình 4.7 (CIFAR-100) Histogram về kích thước các tập dữ liệu huấn luyện . . . . .	32
Hình 4.8 (CIFAR-100) Histogram về kích thước các tập dữ liệu huấn luyện . . . . .	32
Hình 4.9 Hàm mục tiêu và độ chính xác trong quá trình huấn luyện (CIFAR-10). . . . .	36
Hình 4.10 Hàm mục tiêu và độ chính xác trong quá trình huấn luyện (CIFAR-100). . . . .	36
Hình 4.11 Độ chính xác của mô hình khi chưa áp dụng $KNN$ (CIFAR-10). . . . .	37
Hình 4.12 Độ chính xác của mô hình khi chưa áp dụng $KNN$ (CIFAR-10). . . . .	38
Hình 4.13 Độ chính xác tốt nhất đạt được (CIFAR-10). . . . .	39
Hình 4.14 Độ chính xác tốt nhất đạt được (CIFAR-100). . . . .	39
Hình 4.15 Độ chính xác trung bình đạt được (CIFAR-10). . . . .	40
Hình 4.16 Độ chính xác trung bình đạt được (CIFAR-100). . . . .	40
Hình 4.17 Trung bình độ tương đồng và chênh lệch giữa các cặp cùng nhãn và khác nhãn (CIFAR-10). . . . .	41
Hình 4.18 Trung bình độ tương đồng và chênh lệch giữa các cặp cùng nhãn và khác nhãn (CIFAR-100). . . . .	41

## DANH MỤC BẢNG BIỂU

Bảng 4.1	Các tham số trong thí nghiệm gốc của nghiên cứu <b>kNN-Per</b> (CIFAR-10). . . . .	33
Bảng 4.2	Các tham số trong thí nghiệm học đối lập theo biểu diễn cục bộ (CIFAR-10). . . . .	34
Bảng 4.3	Các tham số trong thí nghiệm học đối lập kết hợp biểu diễn cục bộ và toàn cục (CIFAR-10). . . . .	34
Bảng 4.4	Các tham số trong thí nghiệm gốc của nghiên cứu <b>kNN-Per</b> (CIFAR-100). . . . .	34
Bảng 4.5	Các tham số trong thí nghiệm học đối lập kết hợp theo biểu diễn cục bộ (CIFAR-100). . . . .	35
Bảng 4.6	Các tham số trong thí nghiệm học đối lập kết hợp biểu diễn cục bộ và toàn cục (CIFAR-100). . . . .	35



## DANH MỤC THUẬT NGỮ VÀ TỪ VIẾT TẮT

Thuật ngữ	Ý nghĩa
$KNN$	Thuật toán $K$ láng giềng gần nhất ( $KNN$ )
$KNN$ -Per	Nghiên cứu <b>Personalized Federated Learning through Local Memorization</b>
FedAvg	Thuật toán FedAvg trong học liên kết
FedProx	Thuật toán FedProx trong học liên kết
SAM	Phương pháp tối ưu tránh điểm cực tiểu có bề mặt nhọn (Sharpness Aware Minimization)

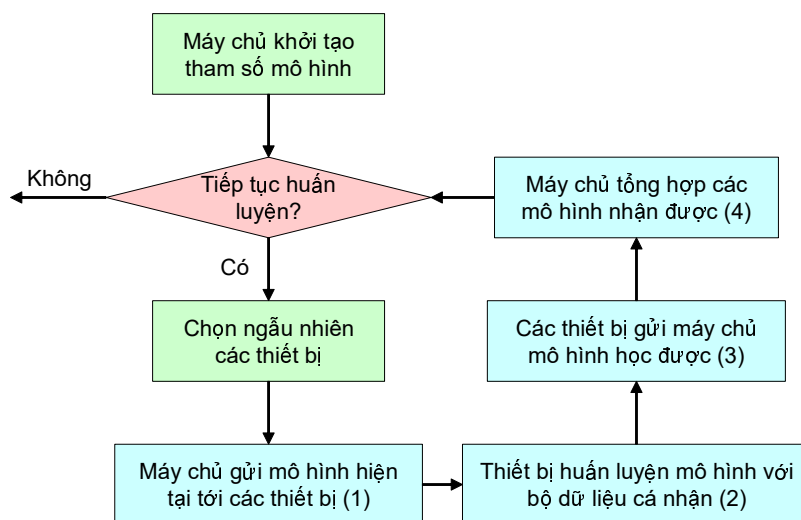
# CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI

## 1.1 Đặt vấn đề

### 1.1.1 Học liên kết (Federated Learning)

Học liên kết được Google giới thiệu vào năm 2017. Với hướng tiếp cận xây dựng các mô hình học máy trước đó, chúng ta cần tập trung dữ liệu lại trên một thiết bị hay trung tâm dữ liệu, và bài toán hướng đến là tập trung nâng cao hiệu quả mô hình. Học liên kết tồn tại một máy chủ (server), cho phép nhiều thiết bị kết nối với máy chủ, như điện thoại di động với khả năng tính toán tương đối tốt, tham gia huấn luyện một mô hình học sâu chung bằng những bộ dữ liệu trên từng thiết bị đó.

Thuật toán đầu tiên được đề xuất giải quyết bài toán học liên kết đó là **FedAvg** [2]. Đây cũng là hình mẫu chung cho nhiều thuật toán về sau phát triển. Như học sâu thông thường, ban đầu máy chủ sẽ khởi tạo một bộ tham số mô hình. Quá trình học mô hình sẽ tồn tại nhiều vòng, gọi là vòng kết nối (communication round). Tại mỗi vòng, máy chủ sẽ chọn một hay một vài thiết bị ngẫu nhiên, gửi bộ tham số mô hình hiện tại về cho các thiết bị đó. Các thiết bị này sẽ tiến hành huấn luyện mô hình dữ liệu trên bộ dữ liệu của chúng với một số ít vòng lặp, sau đó gửi lại máy chủ mô hình thu được. Máy chủ sẽ tổng hợp lại các mô hình này theo phương pháp trung bình cộng có trọng số, trong đó trọng số tỷ lệ thuận với lượng dữ liệu huấn luyện của các thiết bị tham gia. Đây sẽ là bộ tham số mới của mô hình tại vòng này. Vòng mới sẽ được bắt đầu tương tự cho đến khi mô hình hội tụ.



**Hình 1.1:** Sơ đồ hoạt động thuật toán FedAvg

Tồn tại bốn thách thức lớn đối với học liên kết [3]: