ĐẠI HỌC QUỐC GIA TP. HCM
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

# BÁO CÁO TỔNG KẾT
ĐỀ TÀI KHOA HỌC VÀ CÔNG NGHỆ SINH VIÊN NĂM 2021

*Tên đề tài tiếng Việt:*

## BẢO VỆ TÍNH RIÊNG TƯ TRONG CỘNG TÁC DỮ LIỆU CHO ỨNG DỤNG CHẨN ĐOÁN BỆNH SỬ DỤNG MÔ HÌNH FEDERATED LEARNING

*Tên đề tài tiếng Anh:*

## COLLABORATIVE FEDERATED LEARNING FOR PROTECTING THE DATA PRIVACY OF DISEASE PREDICTION APPLICATIONS

Khoa/ Bộ môn: Mạng máy tính và Truyền thông

Thời gian thực hiện: 06 tháng

Cán bộ hướng dẫn: ThS. Nguyễn Thanh Hoà

Tham gia thực hiện


| TT | Họ và tên, MSSV | Chịu trách nhiệm | Điện thoại | Email |
|---|---|---|---|---|
| 1. | Đoàn Thanh Phương | Chủ nhiệm | 0944022034 | 18521267@gm.uit.edu.vn |
| 2. | Phạm Trần Tiến Đạt | Tham gia | 0934993860 | 18520585@gm.uit.edu.vn |
| 3. | Lê Đăng Dũng | Tham gia | 0363789095 | 18520633@gm.uit.edu.vn |


**Thành phố Hồ Chí Minh – Tháng 12 /2021**

**Mẫu F6**

**ĐẠI HỌC QUỐC GIA TP. HCM**
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

| | |
|---|---|
| **Ngày nhận hồ sơ** | |
| **Mã số đề tài** | |
| ***(Do CQ quản lý ghi)*** | |

# BÁO CÁO TỔNG KẾT

*Tên đề tài tiếng Việt:*

**BẢO VỆ TÍNH RIÊNG TƯ TRONG CỘNG TÁC DỮ LIỆU CHO ỨNG DỤNG CHẨN ĐOÁN BỆNH SỬ DỤNG MÔ HÌNH FEDERATED LEARNING**

*Tên đề tài tiếng Anh:*

**COLLABORATIVE FEDERATED LEARNING FOR PROTECTING THE DATA PRIVACY OF DISEASE PREDICTION APPLICATIONS**

*Ngày ... tháng ..... năm ....*
**Cán bộ hướng dẫn**
*(Họ tên và chữ ký)*

**Nguyễn Thanh Hoà**

*Ngày ... tháng ..... năm ....*
**Sinh viên chủ nhiệm đề tài**
*(Họ tên và chữ ký)*

**Đoàn Thanh Phương**

# THÔNG TIN KẾT QUẢ NGHIÊN CỨU

## 1. Thông tin chung:

- Tên đề tài:

**BẢO VỆ TÍNH RIÊNG TƯ TRONG CỘNG TÁC DỮ LIỆU CHO ỨNG DỤNG CHẨN ĐOÁN BỆNH SỬ DỤNG MÔ HÌNH FEDERATED LEARNING**

- Chủ nhiệm: **Đoàn Thanh Phương**

- Thành viên tham gia:

  - **Phạm Trần Tiến Đạt**
  - **Lê Đăng Dũng**

- Cơ quan chủ trì: Trường Đại học Công nghệ Thông tin.
- Thời gian thực hiện: 06 tháng.

## 2. Mục tiêu:

Sự phát triển của các nghiên cứu về trí tuệ nhân tạo (AI), đặc biệt là những tiến bộ trong các kỹ thuật học máy (ML - Machine Learning) và học sâu (DL - Deep Learning) đã dẫn đến nhiều sự đổi mới đột phá trong nhiều lĩnh vực của đời sống xã hội như ô tô không người lái, thành phố thông minh hay ứng dụng để giải quyết các vấn đề trong lĩnh vực y khoa như chẩn đoán bệnh, theo dõi sức khoẻ [1, 2].

Machine Learning và Deep Learning đang trở thành phương pháp tiếp cận và khám phá tri thức trên thực tế trong nhiều ngành, nhưng các ứng dụng ML đòi hỏi một lượng lớn dữ liệu để đào tạo các ra mô hình đạt độ chính xác cao. Trong lĩnh vực y khoa, một trong những thách thức lớn nhất khi triển khai ứng dụng ML là đảm bảo quyền riêng tư của dữ liệu [3]. Việc có thể tập hợp được dữ liệu trong lĩnh vực y tế từ nhiều nguồn khác nhau đối mặt với nhiều khó khăn vì đây là các dữ liệu chứa nhiều thông tin nhạy cảm [4]. Bên cạnh đó, nhiều đạo luật, quy định mới đã được thông qua để kiểm soát việc chia sẻ dữ liệu trong khi vẫn duy trì tính bảo mật và quyền riêng tư của người dùng, ví dụ như quy định chung về bảo vệ dữ liệu chung (GDPR) và Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế năm 1996 (HIPAA) [2]. Ngoài

ra, chi phí để thu thập và xử lý dữ liệu tập trung cũng đặt ra thách thức lớn cho việc triển khai các ứng dụng ML [4].

Để giải quyết những vấn đề trên, mô hình học máy Federated Learning (FL – học cộng tác) đã được đề xuất và nổi lên như một giải pháp đầy hứa hẹn. Khái niệm về FL lần đầu được nhóm nghiên cứu của Google giới thiệu vào năm 2016. Đây là mô hình học máy mà trong đó nhiều thiết bị cùng cộng tác để giải quyết một bài toán học máy, dưới sự điều phối của một máy chủ trung tâm hoặc nhà cung cấp dịch vụ. Dữ liệu thô (raw data) của mỗi thiết bị tham gia chỉ được lưu trữ cục bộ trên thiết bị đó mà không được chia sẻ hoặc chuyển đi. Mô hình này sẽ đảm bảo được tính riêng tư cho dữ liệu cá nhân của mỗi thiết bị tham gia vào hệ thống [5].

Hiện nay mô hình Federated learning đang được các doanh nghiệp, công ty công nghệ lớn quan tâm, hợp tác phát triển và ứng dụng rộng rãi trong lĩnh vực y tế [6]. Nổi bật trong đó là dự án nghiên cứu áp dụng FL cho lĩnh vực y khoa của Owkin. Bên cạnh đó, nhiều nghiên cứu về ứng dụng mô hình Federated Learning trong việc học phát hiện và chẩn đoán bệnh từ hồ sơ bệnh án điện tử và dữ liệu khối u não cũng đã được công bố trong thời gian gần đây như [7, 8]. Đặc biệt, Vaid và cộng sự đã nghiên cứu ứng dụng FL trong việc cải thiện khả năng dự đoán tử vong ở bệnh nhân COVID-19 [9].

Với những tiềm năng đầy hứa hẹn của FL trong lĩnh vực y khoa, nhóm tác giả quyết định nghiên cứu, thực hiện đề tài "**Bảo vệ tính riêng tư trong cộng tác dữ liệu cho ứng dụng chẩn đoán bệnh sử dụng mô hình Federated Learning**" với mục tiêu nghiên cứu và đánh giá về khả năng ứng dụng của Federated Learning trong việc chẩn đoán bệnh trong khi vẫn đảm bảo được quyền riêng tư về dữ liệu của bệnh nhân.

**3. Tính mới và sáng tạo:**

Những năm gần đây đã chứng kiến sự gia tăng quan tâm liên quan đến phân tích dữ liệu chăm sóc sức khỏe, ngày càng có nhiều dữ y tế từ nhiều nguồn khác nhau bao gồm các tổ chức y tế, cá nhân bệnh nhân, công ty bảo hiểm và ngành công nghiệp dược phẩm. Dữ liệu chăm sóc sức khỏe thường bị phân mảnh vì tính chất phức tạp của hệ thống và quy trình chăm sóc sức khỏe [10]. Ví dụ, các bệnh viện khác nhau

chỉ có thể truy cập vào hồ sơ lâm sàng của quần thể bệnh nhân của chính họ. Những hồ sơ này rất nhạy cảm với thông tin sức khỏe của các cá nhân.

Các quy định nghiêm ngặt, chẳng hạn như Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế (HIPAA) [11], đã được phát triển để điều chỉnh quá trình truy cập và phân tích dữ liệu đó. Điều này tạo ra một thách thức lớn cho các công nghệ khai thác dữ liệu và học máy (ML) hiện đại, chẳng hạn như học sâu, thường đòi hỏi một lượng lớn dữ liệu đào tạo.

FL là một mô hình với sự gia tăng phổ biến gần đây vì nó có nhiều hứa hẹn về việc học tập với dữ liệu nhạy cảm bị phân mảnh và có nhiều hứa hẹn về phân tích dữ liệu chăm sóc sức khỏe. Theo báo cáo của Nature, Federated Learning cũng đã được chứng minh là hữu ích trong kỹ thuật liên quan đến hình ảnh y tế và MRI (chụp cộng hưởng từ). Ngoài chẩn đoán chính xác hơn, Federated Learning còn hứa hẹn sẽ cải thiện việc chăm sóc sức khỏe cho tất cả mọi người, không phân biệt chuyên môn.

Nắm bắt xu hướng đó, nhóm thực hiện đề tài với mục tiêu xây dựng mô hình FL hiệu quả để bảo vệ các dữ liệu nhạy cảm trong chăm sóc y tế, chăm sóc sức khỏe nói riêng và các lĩnh vực khác nói chung.

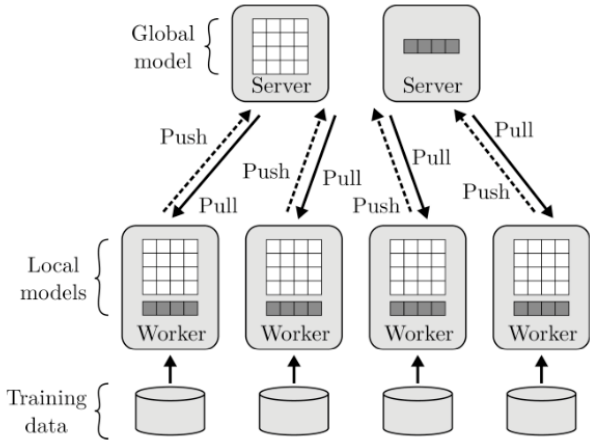
## 4. Tóm tắt kết quả nghiên cứu:

### 4.1. Nghiên cứu cơ sở lý thuyết và khảo sát các nghiên cứu liên quan

#### 4.1.1 Mô hình học máy phân tán

Mô hình học máy phân tán là mô hình đề cập đến các thuật toán và hệ thống học máy đa bên được thiết kế để cải thiện hiệu suất, tăng độ chính xác và mở rộng quy mô kích thước dữ liệu đầu vào lớn hơn. Việc tăng kích thước dữ liệu đầu vào có thể khiến cho nhiều thuật toán giảm đáng kể lỗi học tập và thường có hiệu quả so với việc sử dụng các phương pháp phức tạp hơn.

Mô hình học máy phân tán cho phép các công ty, nhà nghiên cứu và những người trong bộ phận đưa ra quyết định sáng suốt và kết luận rút ra từ một lượng lớn dữ liệu.




Hình 4.1.1. Mô hình học máy phân tán [1]

Trong mô hình học máy phân tán thì tất cả dữ liệu sẽ được đưa lên máy chủ trung tâm và đây cũng là một trong những thử thách lớn của mô hình này. Vì những dữ liệu có thể chứa thông tin nhạy cảm của người dùng cuối hoặc tổ chức. Việc di chuyển dữ liệu thô từ các thiết bị cá nhân hoặc trung tâm dữ liệu của nhiều tổ chức sang máy chủ hoặc trung tâm dữ liệu tập trung có thể gây rò rỉ thông tin tức thì hoặc tiềm ẩn. Điều này làm cho việc tổng hợp dữ liệu từ các thiết bị phân tán, nhiều khu vực hoặc tổ chức hầu như không thể.

Chính vì những thách thức trên mà mở ra tiềm năng vô cùng lớn cho mô hình học máy Federated Learning.

### 4.1.2. Mô hình học hợp tác

#### a. Giới thiệu

Học hợp tác - Federated Learning (FL) là mô hình học máy mà trong đó nhiều thiết bị (clients) cùng hợp tác để giải quyết một vấn đề học máy, dưới sự điều phối của một server trung tâm hoặc nhà cung cấp dịch vụ. Dữ liệu thô (raw data) của mỗi thiết bị tham gia chỉ được lưu trữ cục bộ trên thiết bị đó mà không được chia sẻ hoặc chuyển đi, thay vào đó, chúng sẽ chia sẻ các cập nhật chứa các dữ liệu đã được tổng hợp nhằm phục vụ cho quá trình học của cả hệ thống.

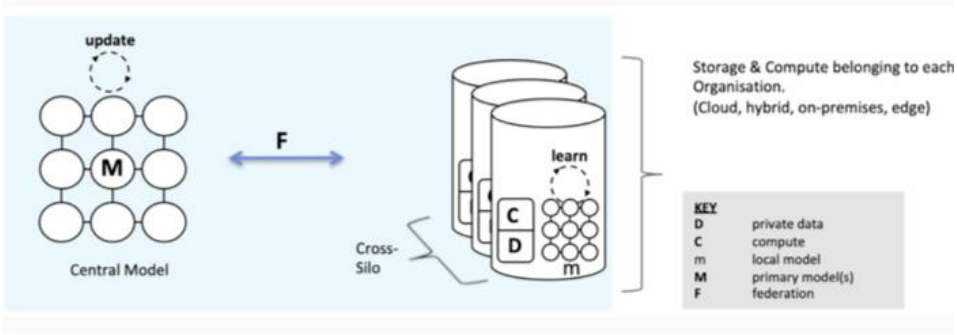
[1] https://medium.com/@karan.sapolia/3lc-speeding-up-distributed-machine-learning-48fec3038330

Mô hình này sẽ đảm bảo được tính riêng tư cho dữ liệu cá nhân của mỗi thiết bị tham gia vào hệ thống [5].

**b. Phân loại**

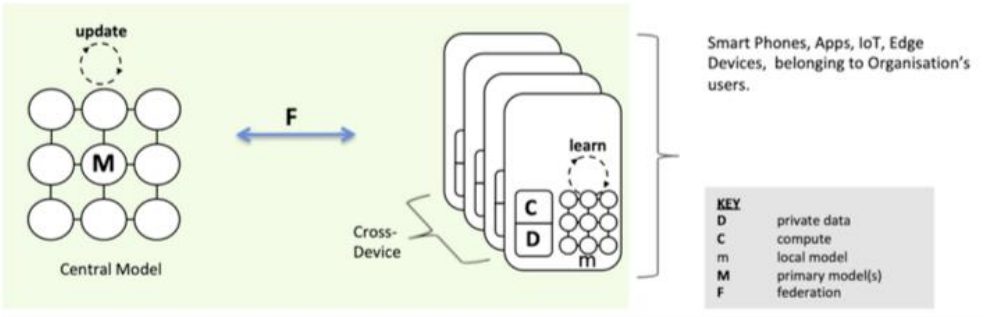
Kỹ thuật học hợp tác được chia làm **2 loại**:

**Cross Silo** là một dạng biến thể của mô hình học hợp tác, cho phép huấn luyện mô hình tại các vùng silo đã được phân chia. Thành phần tham gia là các tổ chức (như bệnh viện hoặc các trung tâm tài chính) hoặc các trung tâm dữ liệu được phân phối theo địa lý. Số lượng thiết bị tham gia vào mô hình là 1 − 100 thiết bị [5].




Hình 4.1.2. Kỹ thuật Cross Silo [2]

**Cross Device** là một dạng biến thể khác của mô hình học hợp tác, nó là dạng mô hình học máy dưới sự tham gia của một số lượng lớn thiết bị đầu cuối kết nối vào mạng (thiết bị IoT). Số lượng thiết bị rơi vào khoảng 1010 thiết bị [5].

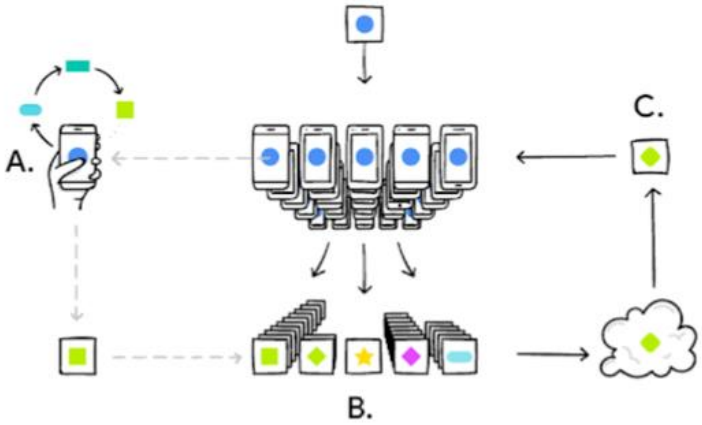



Hình 4.1.3. Kỹ thuật Cross Device

**c. Thuật toán**

[2] https://blog.openmined.org/federated-learning-types/

Như đã nói ở phần khái niệm, học hợp tác cho phép chúng ta có thể tải mô hình học máy về ngay trên thiết bị của mình, cải thiện mô hình đó bằng cách huấn luyện thông qua dữ liệu nằm trên thiết bị, tóm tắt các thay đổi dưới dạng một bản cập nhật nhỏ cho mô hình tổng thể. Chỉ bản cập nhật này được mã hóa và gửi lên cho máy chủ, nơi nó được tập hợp và tính trung bình với các bản cập nhật của các người dùng, thiết bị khác để cải thiện mô hình chung ban đầu. Một điều hiển nhiên là dữ liệu huấn luyện cho mô hình vẫn nằm trên thiết bị của chúng ta và không có một bản cập nhật riêng lẻ nào của từng thiết bị được lưu trữ trên hệ thống máy chủ [5].




Hình 4.1.4. Mô hình Federated Learning [3]

Thiết bị của ta (A) quản lý dữ liệu cục bộ trên thiết bị. Sau khi dùng dữ liệu đó để huấn luyện mô hình, ta được một bản cập nhật nhỏ để góp vào mô hình tổng thể, bản cập nhật này được tập hợp với các bản cập nhật của các thiết bị khác và tính trung bình (B) để tạo nên một bản cập nhật chung cho mô hình tổng thể (C). Quá trình này lại được lặp lại khi các thiết bị tải xuống mô hình tổng thể sau khi được áp dụng bản cập nhật (C).

### d. Ứng dụng

Học hợp tác được sử dụng trong rất nhiều các ứng dụng của cuộc sống, chủ yếu là các ứng dụng dành cho trải nghiệm người dùng, ứng dụng trong lĩnh vực thị giác máy tính và ứng dụng trong lĩnh vực y tế [12]. Các ví dụ điển hình:

[3] https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

**Trải nghiệm người dùng:**

- *Google Keyboard Query Suggestion*: Gboard - đưa ra các từ gợi ý khi thực hiện tìm kiếm [13].
- *Mobile Keyboard Prediction*: ứng dụng dự đoán từ tiếp theo mà người dùng mong muốn nhập [14].
- *Ranking Browser History Suggestions*: ứng dụng đánh giá và gợi ý các dữ liệu lịch sử duyệt web khi người dùng thực hiện tìm kiếm [15].

**Thị giác máy tính:**

- *Visual Object Detection*: Công nghệ phát hiện vật thể.

**Y tế:**

- *Patient Clustering To Predict Mortality and Hospital Stay Time*: Phân loại bệnh nhân, dự đoán tỉ lệ tử vong và thời gian nằm viện.
- *Drug Discovery*: Phân tích và nghiên cứu các loại thuốc mới.

**e. Các hạn chế và mối đe dọa**

Học hợp tác được ứng dụng nhiều là vậy nhưng nó cũng đặt ra rất nhiều thách thức cho chúng ta. Không chỉ là các vấn đề về cơ sở hạ tầng thiết bị, công nghệ giao tiếp giữa các thiết bị tham gia trong hệ thống mà còn cả vấn đề về bảo mật, quyền riêng tư cũng như trải nghiệm của người dùng. Các vấn đề, hạn chế cần quan tâm trong học hợp tác:

- **Vấn đề công nghệ giao tiếp**: Giao tiếp là nút thắt quan trọng trong hầu hết các hệ thống công nghệ có sử dụng mạng lưới làm nền tảng giao tiếp. Song song với việc gửi và nhận dữ liệu trên hàng triệu thiết bị thì tốc độ giao tiếp là một vấn đề nan giải đối với hệ thống này. Với số lượng hàng triệu thiết bị tham gia vào hệ thống thì đòi hỏi hệ thống phải đủ mạnh và đủ nhanh để có thể xử lí tập trung hàng triệu yêu cầu trong một khoảng thời gian. Điều này dẫn tới chi phí hiện thực hóa hệ thống rất đắt đỏ, tốn rất nhiều thời gian và nhân lực [16].

- **Hệ thống không đồng nhất**: Những thiết bị tham gia khác nhau hoàn toàn về phần cứng (phần cứng CPU, GPU, RAM), kiến trúc, nền tảng kết nối (5G, 4G, 3G) và cả nguồn cấp (Pin, nguồn điện), ... [16]. Do đó không thể đảm bảo rằng những thiết bị tham gia vào hệ thống sẽ đáp ứng hoàn toàn yêu cầu mà hệ thống đặt ra và trong một vòng lặp huấn luyện nào đó, nó sẽ bị bỏ lại vì vấn đề kết nối và năng lượng.
- **Dữ liệu không đồng nhất trên các thiết bị**: Hàng triệu thiết bị tham gia vào hệ thống đồng nghĩa với việc sẽ có hàng triệu những cấu trúc và thành phần dữ liệu khác nhau được tạo ra từ người dùng. Điều đó đặt ra một vấn đề lớn cho hệ thống khi muốn tạo ra một mô hình có mối liên hệ sâu sắc nhất tới các cấu trúc và thành phần dữ liệu của từng thiết bị để các thiết bị tải về và cải thiện. Điều này thực sự rất khó khăn và đặt ra thách thức lớn [16].
- **Quyền riêng tư**: Quyền riêng tư là một vấn đề nhức nhối trong thời đại công nghệ số, và ngày càng là vấn đề nóng hổi của các tổ chức và cá nhân, đó cũng là vấn đề được quan tâm lớn nhất trong mô hình học hợp tác. Trong lúc huấn luyện, các thiết bị chỉ gửi đi những bản cập nhật của mô hình, tuy vậy, mô hình học hợp tác cũng có những rủi ro về mặt dữ liệu đối với cá nhân và tổ chức do trong lúc giao tiếp có thể tiết lộ các thông tin nhạy cảm cho bên thứ ba hoặc ngay chính máy chủ trung tâm [17].

## 4.2. Thiết kế và triển khai mô hình thực nghiệm Federated Learning

### 4.2.1. Phân tích Mô hình Cross Silo

Mô hình thực nghiệm được nhóm tác giả xây dựng là mô hình học hợp tác theo dạng cross-silo với hai thành phần chính là người sở hữu dữ liệu (Data Owner) và người nghiên cứu dữ liệu (Data Scientist).

#### a. Data Owner

Trong mô hình này, sau khi các Data Owner đã thiết lập kết nối thành công với Data Scientist, các Data Owner sẽ tiến hành xử lý tập dữ liệu của

mình cho phù hợp với đầu vào của mô hình. Sau khi xử lý dữ liệu, mô hình DL sẽ được khởi tạo và thực hiện các bước chuẩn bị cho bước huấn luyện.

Bước vào quá trình huấn luyện, các bước lan truyền tiến (Forward propagation), tính loss (loss function), lan truyền ngược (Backward propagation) và tối ưu hoá mô hình sẽ được lần lượt thực hiện, các bước này sẽ được thực hiện với từng mẫu có trong tập dữ liệu. Song song đó, quá trình thẩm định sẽ diễn ra để kiểm tra tỉ lệ dự đoán chính xác của mô hình cũng như giá trị loss thực tế khi thực hiện trên tập dữ liệu thử nghiệm, quá trình thẩm định sẽ được thực hiện sau khi một epoch huấn luyện kết thúc. Tiếp đến, các tham số của mô hình (weight, bias của từng lớp) sẽ được rút trích ra và gửi đến Data Scientist. Sau bước này các Data Owner sẽ tạm nghỉ để đợi Data Scientist tạo ra bản cập nhật. Các Data Owner sẽ hoạt động trở lại khi nhận được bản cập nhật.

Bản cập nhật sẽ được cập nhật vào mô hình và thực hiện thẩm định với tập dữ liệu thử nghiệm. Các kết quả của quá trình thẩm định sẽ được lưu lại và các giai đoạn từ giai đoạn huấn luyện sẽ được lặp lại cho đến khi đủ số lượng round nhất định.

**b. Data Scientist**

Khi các Data Owner đã hoàn tất quá trình huấn luyện và gửi các tham số mô hình, Data Scientist sẽ lấy các tham số này về và tiến hành tính trung bình. Sau khi quá trình tính toán hoàn tất, Scientist sẽ gửi bản cập nhật cho các Owner. Quá trình này sẽ được lặp lại với số round nhất định.

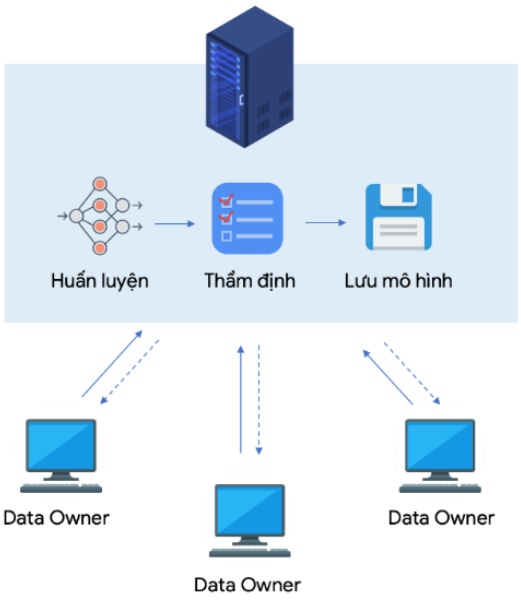
### 4.2.2. Triển khai mô hình

**a. Mô hình học máy phân tán truyền thống**

Ý tưởng của học máy phân tán (distributed learning) là sử dụng nhiều nút cùng đảm nhiệm việc thực hiện các thuật toán ML hoặc DL để cải thiện hiệu suất, đảm bảo tính riêng tư, tăng lượng dữ liệu huấn luyện và có thể phát triển những mô hình phức tạp hơn. Mô hình dưới đây là một ví dụ về mô hình học máy phân tán truyền thống, bao gồm ba nút tính toán và một máy chủ huấn luyện, thậm định và tổng hợp. Dữ liệu của ba Data Owner sẽ

được huấn luyện cục bộ, sau đó các nút này sẽ gửi kết quả học tập về phía máy chủ tổng hợp để tiến hành tính trung bình và đưa ra kết quả học tập cuối cùng cho toàn bộ các nút.

Các giai đoạn chính trong mô hình học máy phân tán truyền thống:



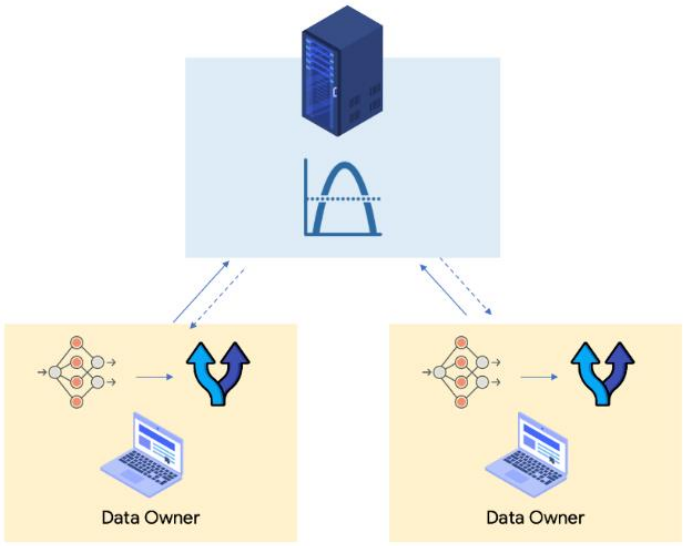

Hình 4.2.1. Mô hình máy học phân tán truyền thống

1. Dữ liệu từ các Owner sẽ được gửi đến Scientist.
2. Data Scientist gộp các dữ liệu của Owner và tiến hành huấn luyện mô hình DL.
3. Data Scientist thẩm định mô hình với tập dữ liệu kiểm tra của mình.
4. Data Scientist lưu lại mô hình DL.
5. Data Scientist gửi mô hình DL cho các Owner.

Với giải pháp này học này, mô hình có thể đảm bảo tính riêng tư của dữ liệu. Học máy phân tán có thể được phân thành hai loại: scalabilitymotivated (thúc đẩy khả năng mở rộng) và privacy-motivated (đảm bảo quyền riêng tư). Scalability- otivated là mô hình được thiết kế để giải quyết nhu cầu mở rộng và tập trung tối ưu khả năng tính toán của các nút trong hệ thống học máy. Ngược lại, privacy-motivated tập trung giải quyết các nhu cầu về đảm bảo tính riêng tư của người dùng bởi vì tính riêng tư dữ liệu của người dùng hiện đang là mối quan tâm toàn cầu.

### 4.2.2. Mô hình học hợp tác

Mô hình học hợp tác (FL) giải quyết những vấn đề liên quan đến quyền riêng tư của dữ liệu và giúp giảm chi phí trong quá trình huấn luyện mô hình học máy. Trong quá trình tham gia vào hệ thống FL, dữ liệu của mỗi nút tham gia được lưu trữ cục bộ và sẽ không chia sẻ hay chuyển đi với bất kì thực thể nào.




Hình 4.2.2. Mô hình máy học hợp tác

Các giai đoạn chính trong mô hình FL Cross Silo:

1. Dữ liệu từ các Owner sẽ được dùng để huấn luyện mô hình DL.
2. Data Owner trích xuất các tham số mô hình.
3. Data Owner gửi các tham số đến Scientist để tổng hợp.
4. Data Scientist gửi bản cập nhật được tạo ra từ việc tính trung bình cho các Owner.
5. Data Owner cập nhật vào mô hình DL của mình.

Với cách tiếp cận trên, mô hình học máy hợp tác đã giải quyết những vấn đề liên quan đến quyền riêng tư của dữ liệu. Sau khi hoàn thành quá trình huấn luyện mô hình cục bộ, các nút sẽ thực hiện gửi những cập nhật của mô hình cục bộ cho máy chủ trung tâm hoặc nhà cung cấp dịch vụ. Việc chỉ gửi những cập nhật của mô hình thay vì khối lượng lớn dữ liệu

gốc đã giúp giảm chi phí truyền thông giữa các nút và máy chủ trung tâm một cách đáng kể.

## 4.3. Ứng dụng Federated Learning trong phát hiện và chẩn đoán bệnh.

### 4.3.1. Tập dữ liệu thực nghiệm

Về tập dữ liệu thực nghiệm, qua quá trình khảo sát các tập dữ liệu về phát hiện và chẩn đoán bệnh. Nhóm tác giả quyết địch tiến hành các thực nghiệm dựa trên 2 tập dữ liệu khác nhau là ECG Heartbeat Categorization và Brain Tumor Classification (MRI).

**ECG Heartbeat Categorization**: là tập dữ liệu nổi tiếng trong phân loại nhịp tim. Tất cả các mẫu đều được xử lý chọn lọc các thuộc tính phù hợp và chèn thêm các số 0 vào. Trong đó bao gồm 5 nhãn tương ứng với các trường hợp Normal, Artial Premature, Premature ventricular contraction, Fusion of ventricular and normal, Fusion of paced and normal.

- Tổng số mẫu: 109446
- Số lượng nhãn: 5
- Tập huấn luyện: 76612 (70%)
- Tập dữ liệu kiểm tra: 32834 (30%)

**Brain Tumor Classification (MRI):** là tập dữ liệu về khối u trong não. Một khối u não được coi là một trong những căn bệnh nguy hiểm, ở trẻ em và người lớn. Trong tập dữ liệu này bao gồm một lượng lớn dữ liệu hình ảnh chụp cắt lớp của được tạo ra thông qua công nghệ chụp X quang. Các hình ảnh chụp cắt lớp khối u não được phân loại thành 4 nhãn như sau: Benign Tumor, Malignant Tumor, Pituitary Tumor, No Tumor.

- Tổng số mẫu: 3264
- Số lượng nhãn: 4
- Tập huấn luyện: 2284 (70%)
- Tập dữ liệu kiểm tra: 980 (30%)

### 4.3.2. Cấu hình thực nghiệm

Để chứng minh tính hiệu quả của mô hình Federated Learning trong việc phát hiện và chẩn đoán bệnh. Nhóm tác giả thực nghiệm trên mô hình học máy tập trung và mô hình Federated Learning. Môi trường nhóm tác giả thực nghiệm như sau:

- Một máy ảo Ubuntu Linux 18.04(64-bit), CPU 6 Cores, RAM 16GB, Ổ đĩa HDD dung lượng 60GB
- Google Colab Notebook

Chi tiết hơn về 2 thực nghiệm chính để chứng minh độ hiệu quả của các mô hình Federated Learning:

**Thực nghiệm 1:** So sánh giữa mô hình Centralize Learning và Federated Learning trên tập dữ liệu ECG Heartbeat Categorization.

Để so sánh sự khác nhau khi huấn luyện trên Centralize Learning và Federated Learning. Trong thực nghiệm này, nhóm tác giả sử dụng cùng một model ANN để huấn luyện. Model bao gồm 4 lớp fully connected với đầu vào là một Vector có độ dài 187 tương ứng với mỗi mẫu dữ liệu, đầu ra là Vector có độ dài 5 tương ứng với 5 nhãn trong tập dữ liệu ECG Heartbeat Categorization. Các thông số cài đặt riêng cho từng mô hình huấn luyện như sau:

- Centralize Learning: huấn luyện qua 50 vòng, dữ liệu huấn luyện gồm 76612 mẫu (70%), tập kiểm tra gồm 32834 mẫu (30%)
- Federated Learning:
    - Số vòng huấn luyện: 100
    - Tổng số người tham gia: 10
    - Số người tham gia trong mỗi vòng: 2
    - Dữ liệu của mỗi người tham gia: 7661 mẫu (do chia đều 76612 mẫu cho 10 người tham gia)
    - Dữ liệu kiểm tra: 32834 mẫu

```
model = models.Sequential()

model.add(layers.InputLayer(input_shape=(187,)))
model.add(layers.Dense(128, activation="relu"))
model.add(layers.Dense(32,  activation="relu"))
model.add(layers.Dense(num_classes, activation="softmax"))
model.compile(loss='categorical_crossentropy', optimizer='adam', metrics=['accuracy'])
```

Hình 4.3.1: Model ANN được sử dụng trong thực nghiệm

```
# Define client
class Client(fl.client.NumPyClient):
    def get_parameters(self):  # type: ignore
        return model.get_weights()

    def fit(self, parameters, config):
        model.set_weights(parameters)
        history = model.fit(X_train,y_train, epochs =1)
        predY = model.predict(X_test)
        y_pred = np.argmax(predY,axis=1)
        y_actual = np.argmax(y_test,axis=1)
        matrix = confusion_matrix(y_actual, y_pred)
        print(matrix)
        print(classification_report(y_actual, y_pred, target_names=labels))
        return model.get_weights(), len(X_train), {}

    def evaluate(self, parameters, config):
        model.set_weights(parameters)
        loss, accuracy = model.evaluate(X_test, y_test)
        return loss, {"accuracy": accuracy}

# Start Flower client
fl.client.start_numpy_client("0.0.0.0:8080", client=Client())
```

Hình 4.3.2: Hàm huấn luyện của người tham gia

```
    def evaluate(weights: fl.common.Weights):
        model.set_weights(weights)
        models.save_model(model, './fl.hdf5')
        loss, accuracy = model.evaluate(X_test, y_test)
        history_loss.append(loss)
        history_acc.append(accuracy)
        print(history_loss)
        print(history_acc)
        os.system('./kill.sh')
        os.system('./run_client.sh')
        return loss, {"accuracy": accuracy}

    return evaluate


strategy = fl.server.strategy.FedAvg(
    fraction_fit=0.2,
    min_available_clients=10,
    eval_fn=get_eval_fn(model)
)
fl.server.start_server("0.0.0.0:8080", config={"num_rounds": 40},strategy=strategy)
```

Hình 4.3.3: Hàm tổng hợp và đánh giá của máy chủ trung tâm

**Thực nghiệm 2:** So sánh giữa mô hình Centralize Learning và Federated Learning trên tập dữ liệu Brain Tumor Classification (MRI).

Để so sánh sự khác nhau khi huấn luyện trên Centralize Learning và Federated Learning. Trong thực nghiệm này, nhóm tác giả sử dụng cùng một model CNN để huấn luyện. Model CNN chúng tôi chọn là model VGG16 bao gồm 16 layer trong đó gồm 13 lớp convolution có kernel ($\mathbf{3 \times 3}$), sau mỗi lớp convolution, kết quả sẽ được maxpooling downsize xuống 0.5, và 3 lớp fully connection. Đầu vào model là một Vector với kích thước ($\mathbf{150 \times 150 \times 3}$) tương ứng với kích thước của hình ảnh trong tập dữ liệu, đầu ra là Vector có độ dài 4 tương ứng với 4 nhãn trong tập dữ liệu Brain Tumor Classification (MRI). Các thông số cài đặt riêng cho từng mô hình huấn luyện như sau:

- Centralize Learning: huấn luyện qua 20 vòng, dữ liệu huấn luyện gồm 2284 mẫu (70%), tập kiểm tra gồm 980 mẫu (30%)
- Federated Learning:
  - Số vòng huấn luyện: 40
  - Tổng số người tham gia: 10
  - Số người tham gia trong mỗi vòng: 2
  - Dữ liệu của mỗi người tham gia: 228 mẫu (do chia đều 2284 mẫu cho 10 người tham gia)
  - Dữ liệu kiểm tra: 980 mẫu

```
base_model = VGG16(input_shape = (150, 150, 3),include_top = False, weights = 'imagenet')
for layer in base_model.layers:
    layer.trainable = False
x = layers.Flatten()(base_model.output)
x = layers.Dense(512, activation='relu')(x)
x = layers.Dropout(0.5)(x)
x = layers.Dense(4, activation='softmax')(x)
model = tf.keras.models.Model(base_model.input, x)
model.compile(optimizer = tf.keras.optimizers.RMSprop(learning_rate=0.0001), loss = 'categorical_crossentropy',metrics =
```

Hình 4.3.4: Model CNN được sử dụng trong thực nghiệm

```
    def evaluate(weights: fl.common.Weights):
        model.set_weights(weights)
        loss, accuracy = model.evaluate(X_test, y_test)
        models.save_model(model, './fl.hdf5')
        os.system('./kill.sh')
        os.system('./run_client.sh')
        return loss, {"accuracy": accuracy}

    return evaluate

strategy = fl.server.strategy.FedAvg(
    fraction_fit=0.2,
    min_available_clients=10,
    eval_fn=get_eval_fn(model)
)

fl.server.start_server("0.0.0.0:8080", config={"num_rounds": 100},strategy=strategy)
```

Hình 4.3.5: Hàm tổng hợp và đánh giá của máy chủ trung tâm

### 4.3.3. Các phương pháp đánh giá độ hiệu quả mô hình

#### a) Accuracy

Accuracy là một phương pháp đánh giá mô hình machine learning dựa trên sự chính xác. Sự chính xác này được xác định bằng tỉ lệ giữa số mẫu dữ liệu được dự đoán đúng và tổng số mẫu dữ liệu trong tập dữ liệu kiểm tra.

Công thức tính accuracy:

$$\boldsymbol{Accuracy} = \frac{\textbf{số mẫu dự đoán đúng}}{\textbf{tổng số mẫu}}$$

#### b) Ma trận Confusion

Accuracy chỉ cho ta cái nhìn tổng quan về kết quả trên toàn bộ các nhãn dữ liệu được phân loại đúng mà không chỉ ra được cụ thể mỗi nhãn được phân loại như thế nào, lớp nào được phân loại đúng nhiều nhất, và dữ liệu thuộc lớp nào thường bị phân loại nhầm vào lớp khác. Để có thể đánh giá được các giá trị này, sử dụng một ma trận được gọi là confusion matrix.

Ma trận Confusion thể hiện có bao nhiêu mẫu dữ liệu được phân loại đúng theo từng nhãn, và bao nhiêu mẫu bị nhầm với nhãn khác. Trong nghiên cứu này, nhóm tác giả sẽ kết hợp sử dụng ma trận confusion để đánh giá kết quả một cách chi tiết hơn.

```
[[17983    46    54    22    13]
 [  199   346    10     0     1]
 [  115     5  1295    31     2]
 [   26     0    15   121     0]
 [   69     2    12     0  1525]]
```

Hình 4.3.6. Ma trận confusion

**c) Precision và Recall**

Đối với một số tập dữ liệu có tỷ lệ các nhãn là chênh lệch nhau lớn, có một phép đó hiệu quả thường được sử dụng là Precision và Recall.

Precision được định nghĩa là tỉ lệ số điểm True Positive (TP) trong số những điểm được phân loại là Positive (TP + FP).

Recall được định nghĩa là tỉ lệ số điểm True Positive (TP) trong số những điểm thực sự là Positive (TP + FN).

Kết quả Precision cao đồng nghĩa với việc độ chính xác của các điểm Positive phân loại đúng là cao. Recall cao đồng nghĩa với việc True Positive Rate cao, tức tỉ lệ bỏ sót các điểm thực sự Positive là thấp.

## 5. Tên sản phẩm:

**FedHealth** - Mô hình Federated Learning ứng dụng trong chẩn đoán bệnh.

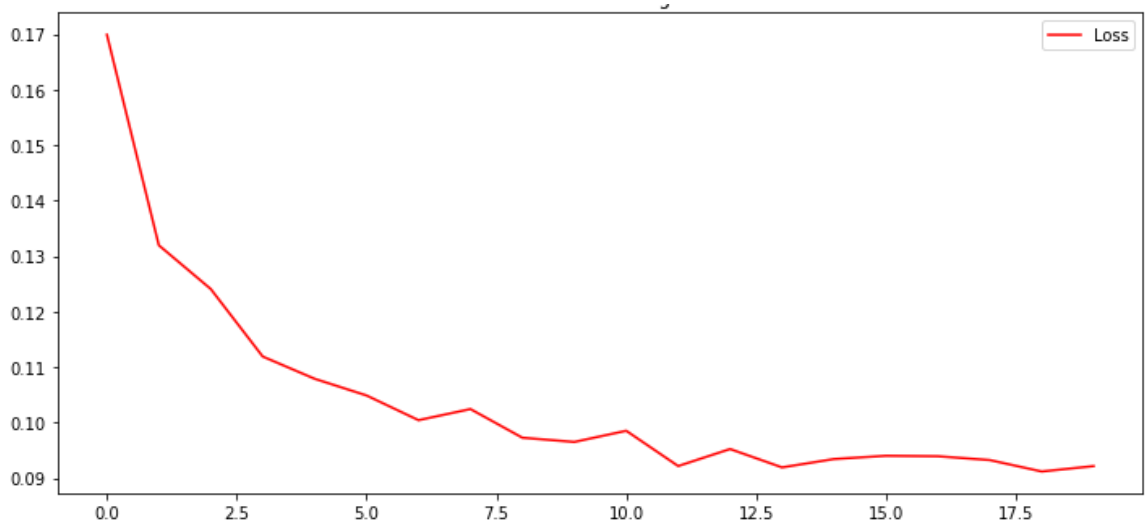
## 6. Hiệu quả, phương thức chuyển giao kết quả nghiên cứu và khả năng áp dụng:

### 6.1. Đánh giá kết quả thực nghiệm

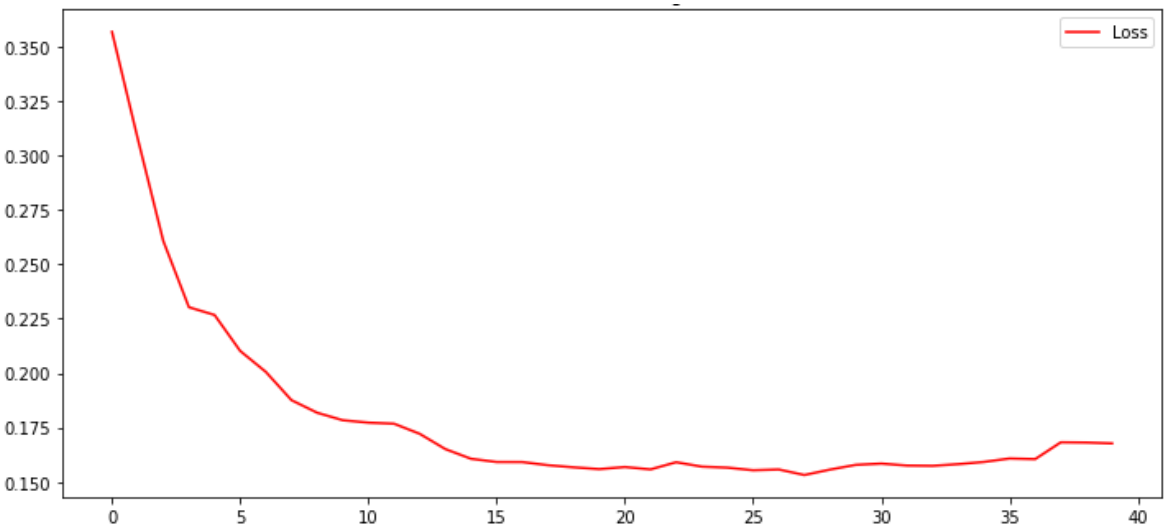
#### 6.1.1. Thực nghiệm 1

Thực nghiệm này được thực hiện trên tập dữ liệu ECG Heartbeat Categorization. Sử dụng mô hình học máy tập trung và mô hình Federated Learning để đánh giá độ hiệu quả của mô hình Federated Learning. Kết quả thực nghiệm thu được như sau:

**a) Đồ thị biểu hiện Training loss**



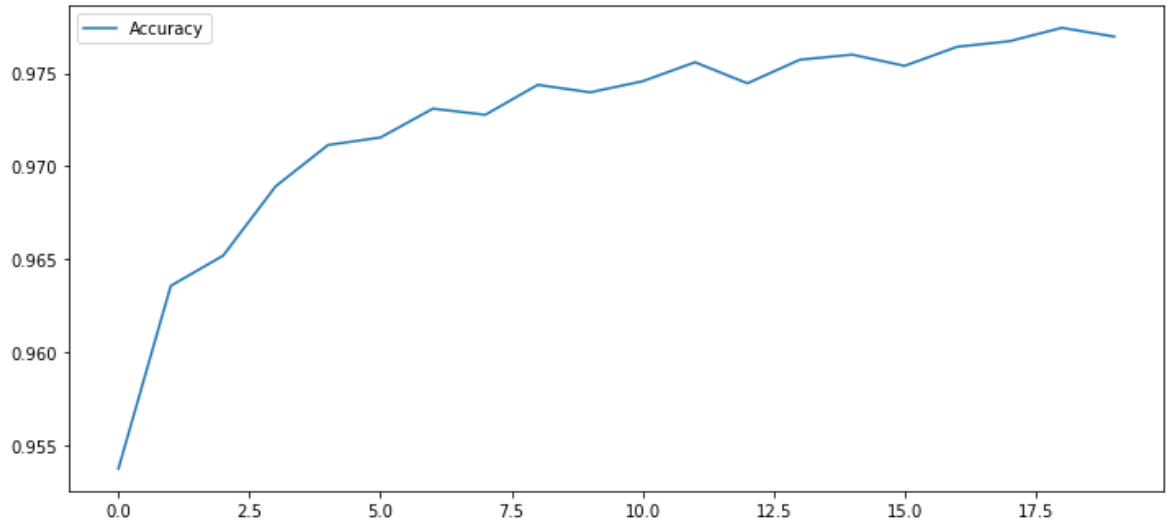

Hình 6.1.1. Kết quả trên mô hình Centralize Learning



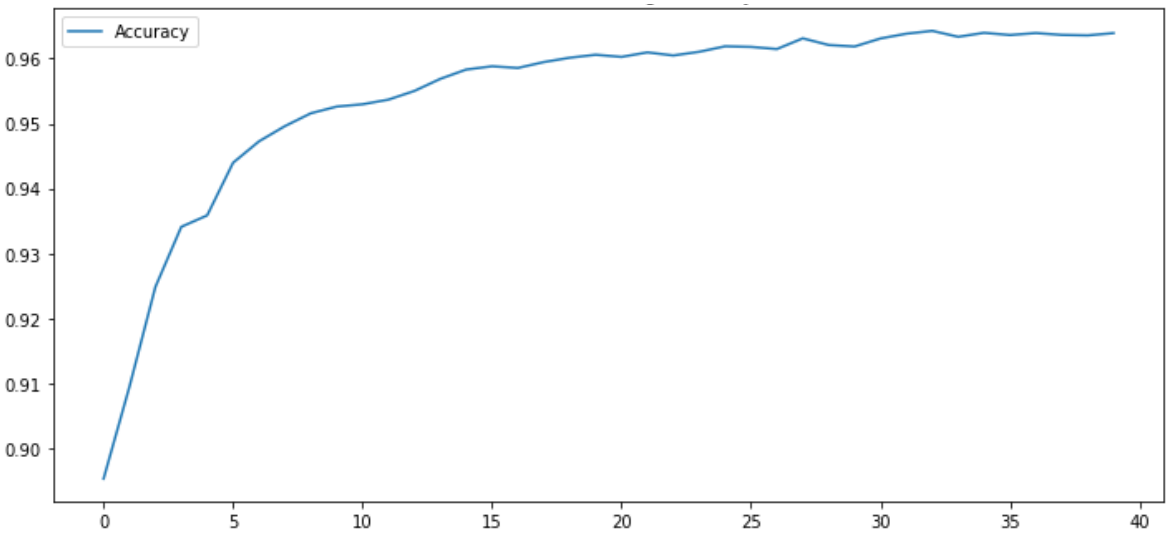

Hình 6.1.2. Kết quả trên mô hình Federated Learning

Dựa vào hai đồ thị trên cho thấy, qua các vòng huấn luyện giá trị training loss đã có chiều hướng giảm ở cả hai mô hình. Cụ thể trên Centralize Learning đã giảm xuống xấp xỉ khoảng 0.1 và khoảng 0.15 trên Federated Learning.

**b) Đồ thị biểu hiện Accuracy**




Hình 6.1.3. Kết quả trên mô hình Centralize Learning




Hình 6.1.4. Kết quả trên mô hình Federated Learning

Dựa vào hai đồ thị trên cho thấy, qua các vòng huấn luyện giá trị Accuracy đã tăng cao ở cả hai mô hình, và kết quả sau cùng gần như tương đồng nhau. Cụ thể trên Centralize Learning đã đạt khoảng 97% và khoảng 96% trên Federated Learning.

**c) Ma trận confusion**

```
[[17983    46    54    22    13]
 [  199   346    10     0     1]
 [  115     5  1295    31     2]
 [   26     0    15   121     0]
 [   69     2    12     0  1525]]
```

Hình 6.1.5. Kết quả trên mô hình Centralize Learning

```
[[17936    61    85    11    25]
 [  214   329    12     0     1]
 [  120     7  1289    23     9]
 [   35     1    16   110     0]
 [   86     4    20     0  1498]]
```

Hình 6.1.6. Kết quả trên mô hình Federated Learning

Dựa vào kết quả ma trận confusion cho thấy được tổng quan hơn về độ chính xác của từng nhãn trong tập dữ liệu. Ma trận trên đã cho thấy sự chênh lệnh kết quả của từng nhãn khi huấn luyện trên Federated Learning so với Centralize Learning là rất thấp.

**d) Kết quả đánh giá**

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Normal | 0.98 | 0.99 | 0.99 | 18118 |
| Artial Premature | 0.87 | 0.62 | 0.72 | 556 |
| Premature ventricular contraction | 0.93 | 0.89 | 0.91 | 1448 |
| Fusion of ventricular and normal | 0.70 | 0.75 | 0.72 | 162 |
| Fusion of paced and normal | 0.99 | 0.95 | 0.97 | 1608 |
| accuracy | | | 0.97 | 21892 |
| macro avg | 0.89 | 0.84 | 0.86 | 21892 |
| weighted avg | 0.97 | 0.97 | 0.97 | 21892 |

Hình 6.1.7. Kết quả trên mô hình Centralize Learning

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Normal | 0.98 | 0.99 | 0.98 | 18118 |
| Artial Premature | 0.82 | 0.59 | 0.69 | 556 |
| Premature ventricular contraction | 0.91 | 0.89 | 0.90 | 1448 |
| Fusion of ventricular and normal | 0.76 | 0.68 | 0.72 | 162 |
| Fusion of paced and normal | 0.98 | 0.93 | 0.95 | 1608 |
| accuracy | | | 0.97 | 21892 |
| macro avg | 0.89 | 0.82 | 0.85 | 21892 |
| weighted avg | 0.97 | 0.97 | 0.97 | 21892 |

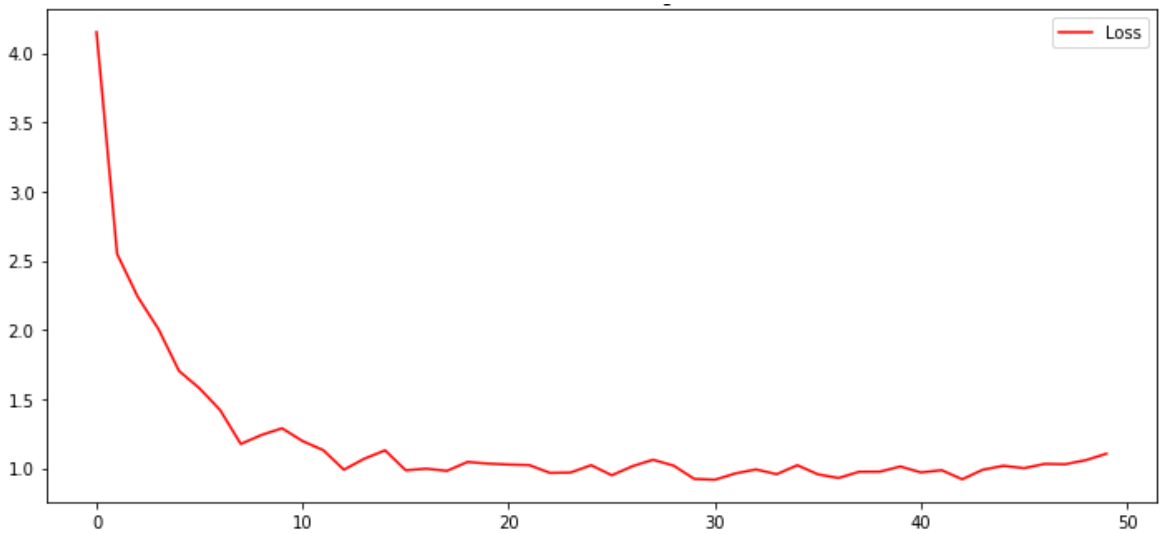
Hình 6.1.8. Kết quả trên mô hình Federated Learning

Dựa vào kết quả tổng quan của từng nhãn được đánh giá qua các giá trị Precision, Recall và F1-score của 2 mô hình. Cho thấy kết quả khi huấn luyện trên Centralize Learning và Federated Learning gần như tương đồng nhau trong mọi giá trị.

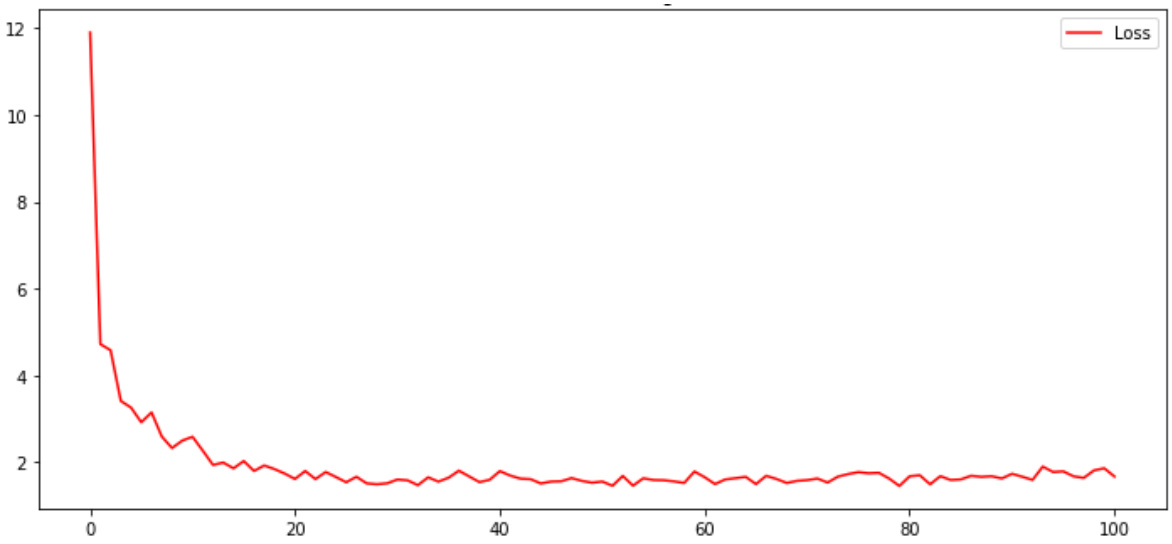
### 6.1.2. Thực nghiệm 2

Thực nghiệm này được thực hiện trên tập dữ liệu Brain Tumor Classification (MRI). Sử dụng mô hình học máy tập trung và mô hình Federated Learning để đánh giá độ hiệu quả của mô hình Federated Learning. Kết quả thực nghiệm thu được như sau:

**a) Đồ thị biểu hiện Training loss**



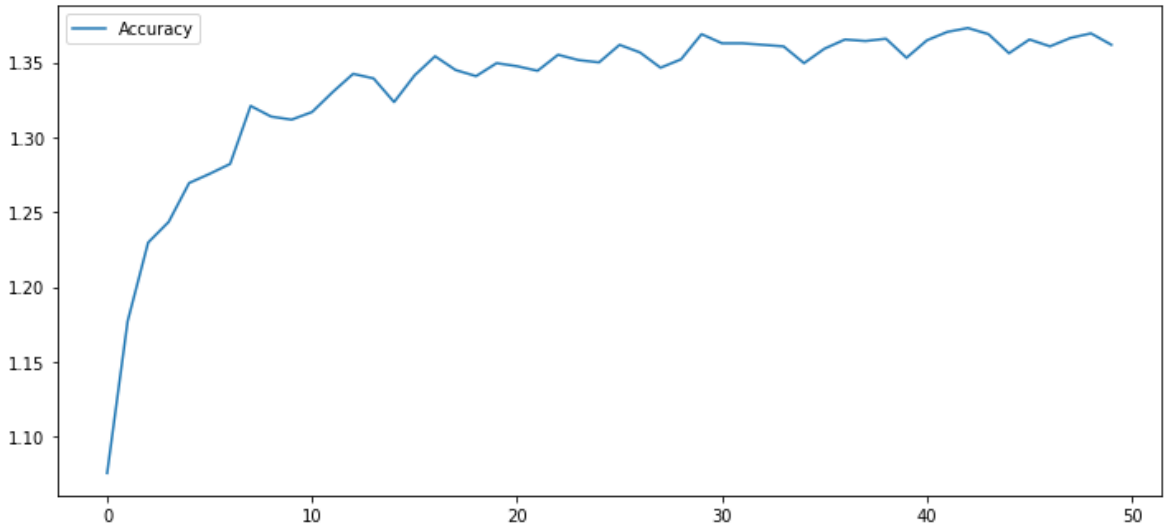

Hình 6.1.9. Kết quả trên mô hình Centralize Learning



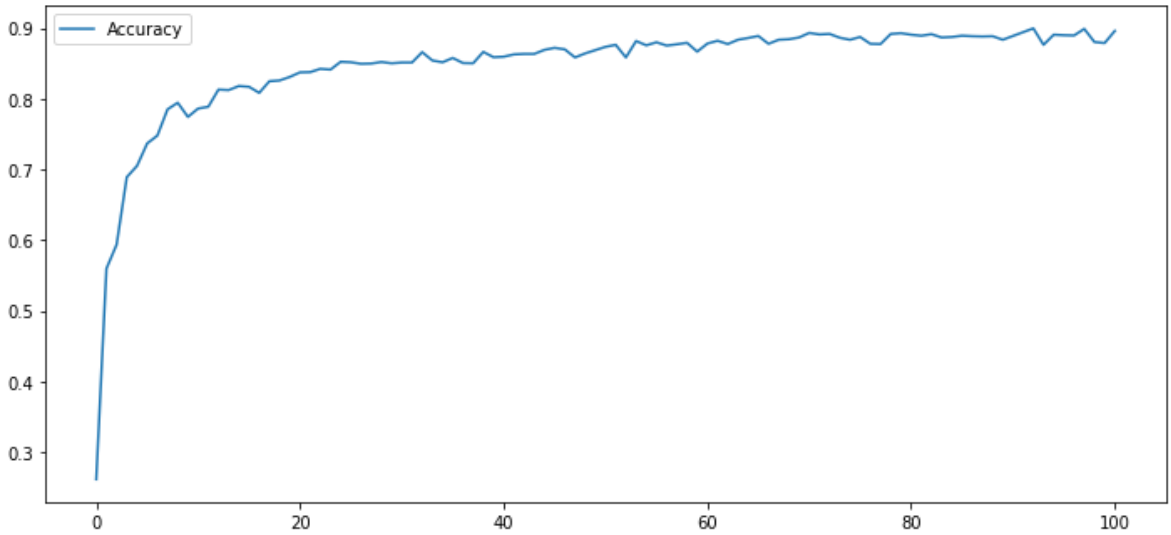

Hình 6.1.10. Kết quả trên mô hình Federated Learning

Dựa vào hai đồ thị trên cho thấy, qua các vòng huấn luyện giá trị training loss đã có chiều hướng giảm ở cả hai mô hình. Cụ thể trên Centralize Learning đã giảm xuống xấp xỉ khoảng 0.9 và khoảng 1.5 trên Federated Learning.

**b) Đồ thị biểu hiện Accuracy**




Hình 6.1.11. Kết quả trên mô hình Centralize Learning




Hình 6.1.12. Kết quả trên mô hình Federated Learning

Dựa vào hai đồ thị trên cho thấy, qua các vòng huấn luyện giá trị Accuracy đã tăng cao ở cả hai mô hình, và kết quả sau cùng gần như tương đồng nhau. Cụ thể trên Centralize Learning đã đạt khoảng 90% và khoảng 89% trên Federated Learning.

**c) Ma trận confusion**

```
[[215   5  34   1]
 [  5 154   5   4]
 [ 20   1 260   9]
 [  3   1  12 251]]
```

Hình 6.1.13. Kết quả trên mô hình Centralize Learning

```
[[206   8  37   4]
 [  1 161   4   2]
 [ 14   3 253  20]
 [  2   2  11 252]]
```

Hình 6.1.14. Kết quả trên mô hình Federated Learning

Dựa vào kết quả ma trận confusion cho thấy được tổng quan hơn về độ chính xác của từng nhãn trong tập dữ liệu. Ma trận trên đã cho thấy sự chênh lệnh kết quả của từng nhãn khi huấn luyện trên Federated Learning so với Centralize Learning là rất thấp.

**d) Kết quả đánh giá**

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| glioma_tumor | 0.88 | 0.84 | 0.86 | 255 |
| no_tumor | 0.96 | 0.92 | 0.94 | 168 |
| meningioma_tumor | 0.84 | 0.90 | 0.87 | 290 |
| pituitary_tumor | 0.95 | 0.94 | 0.94 | 267 |
| accuracy | | | 0.90 | 980 |
| macro avg | 0.91 | 0.90 | 0.90 | 980 |
| weighted avg | 0.90 | 0.90 | 0.90 | 980 |

Hình 6.1.15. Kết quả trên mô hình Centralize Learning

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| glioma_tumor | 0.92 | 0.81 | 0.86 | 255 |
| no_tumor | 0.93 | 0.96 | 0.94 | 168 |
| meningioma_tumor | 0.83 | 0.87 | 0.85 | 290 |
| pituitary_tumor | 0.91 | 0.94 | 0.92 | 267 |
| accuracy | | | 0.89 | 980 |
| macro avg | 0.90 | 0.90 | 0.89 | 980 |
| weighted avg | 0.89 | 0.89 | 0.89 | 980 |

Hình 6.1.16. Kết quả trên mô hình Federated Learning

Dựa vào kết quả tổng quan của từng nhãn được đánh giá qua các giá trị Precision, Recall và F1-score của 2 mô hình. Cho thấy kết quả khi huấn luyện trên Centralize Learning và Federated Learning gần như tương đồng nhau trong mọi giá trị.

## 6.2. Phương thức chuyển giao kết quả nghiên cứu

Quá trình chuyển giao kết quả nghiên cứu như sau:

- Nghiên cứu và tìm hiểu về các công nghệ nền tảng trong thiết kế và xây dựng mô hình Federated Learning.
- Thiết kế và triển khai mô hình thực nghiệm Federated Learning trên framework Flower.
- Xây dựng model thực nghiệm ANN và CNN cho 2 tập dữ liệu ECG Heartbeat Categorization và Brain Tumor Classification (MRI).
- Thực nghiệm trên mô hình học máy tập trung và mô hình học máy Federated Learning.
- So sánh và đánh giá kết quả thực nghiệm.
- Cải tiến mô hình thực nghiệm và đưa ra hướng phát triển.

### 6.3. Khả năng áp dụng

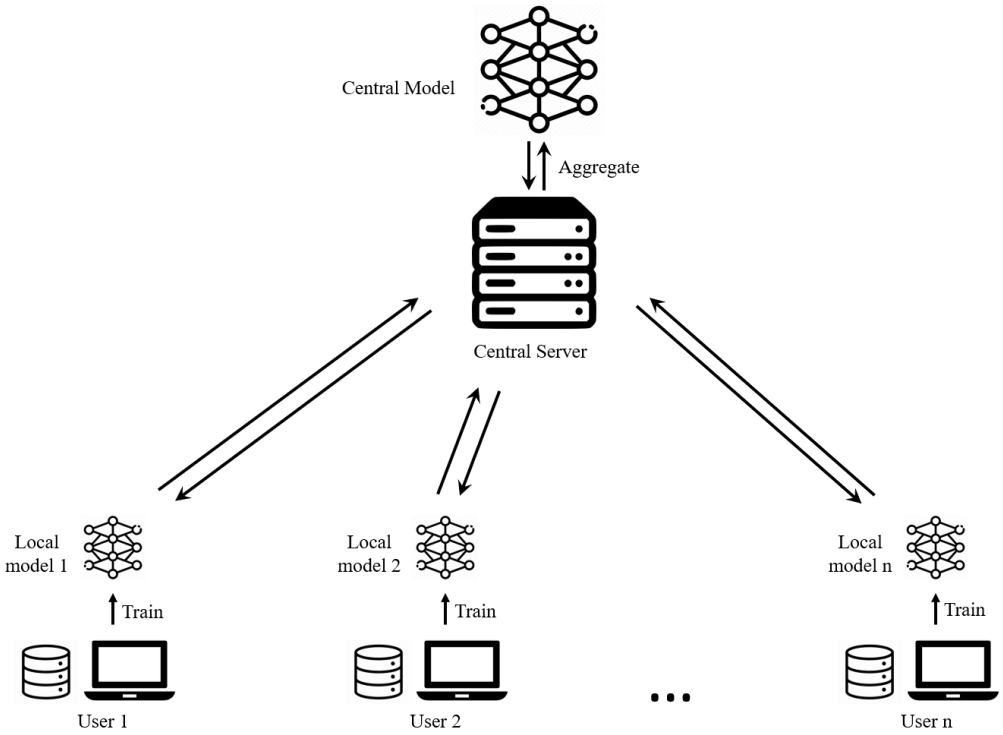
Dựa vào các kết quả nhóm tác giả đã thực nghiệm trên mô hình Centralize Learning và Federated Learning với 2 tập dữ liệu về chẩn đoán bệnh. Kết quả thu được đã cho thấy khi huấn luyện trên mô hình Federated Learning mang lại kết quả tương đồng với mô hình Centralize Learning trên cả 2 tập dữ liệu. Kết quả này đã chứng minh được độ hiệu quả khi áp dụng Federated Learning trong việc đào tạo các mô hình học máy để chẩn đoán bệnh trong y tế mà không cần phải tập trung dữ liệu về một nơi như trong mô hình Centralize Learning. Federated Learning sẽ đảm bảo được các vấn đề về tính riêng tư trong việc cộng tác dữ liệu của bệnh nhân.

### 6.4. Hướng phát triển

- Nhóm tác giả sẽ xây dựng một mô hình thực nghiệm phức tạp hơn sử dụng các thư viện tốt hơn. Từ các kết quả thực nghiệm thu được cho thấy kết quả vẫn chưa được tối ưu, quá trình trao đổi dữ liệu tiêu hao rất nhiều thời gian. Điều này cũng có thể giúp cho chúng tôi mở rộng quy mô của mô hình thực nghiệm.
- Nhóm sẽ nghiên cứu chạy thực nghiệm trên các tập dataset khác để đánh giá kĩ hơn về mô hình hệ thống, triển khai không chỉ trên lĩnh vực sức khỏe mà còn trên nhiều lĩnh vực khác cần bảo vệ quyền riêng tư của người dùng.

- Ngoài ra, một mục tiêu nữa mà nhóm tác giả nhắm tới đó chính là triển khai mô hình thực nghiệm lên thiết bị vật lý.

**7. Hình ảnh, sơ đồ minh họa chính:**




**8. Tài liệu tham khảo**

[1] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *Acm Transactions on Intelligent Systems and Technology,* vol. 10, no. 2, Feb 2019

[2] M. Grama, M. Musat, L. Muñoz-González, J. Passerat-Palmbach, D. Rueckert, and A. Alansary, "Robust aggregation for adaptive privacy preserving federated learning in healthcare," *arXiv preprint arXiv:2009.08294,* 2020

[3] L. Lyu, H. Yu, J. Zhao, and Q. Yang, "Threats to Federated Learning," in *Federated Learning*: Springer, 2020, pp. 3-16.

[4] G. H. Lee and S.-Y. Shin, "Federated Learning on Clinical Benchmark Data: Performance Assessment," *Journal of Medical Internet Research,* vol. 22, no. 10, Oct 26 2020

[5] P. Kairouz *et al.*, "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning,* vol. 14, no. 1-2, pp. 1-210, 2021 2021

[6] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare," *Ieee Intelligent Systems*, vol. 35, no. 4, pp. 83-93, Jul-Aug 2020

[7] W. Li *et al.*, "Privacy-Preserving Federated Brain Tumour Segmentation," in, Shenzhen, PEOPLES R CHINA, 2019 Oct 13-17 2019, vol. 11861, in Lecture Notes in Computer Science, 2019, pp. 133-141.

[8] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated Electronic Health Records," *International Journal of Medical Informatics*, vol. 112, pp. 59-67, Apr 2018

[9] A. Vaid *et al.*, "Federated Learning of Electronic Health Records to Improve Mortality Prediction in Hospitalized Patients With COVID-19: Machine Learning Approach," *Jmir Medical Informatics*, vol. 9, no. 1, Jan 2021

[10] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1-19, 2021

[11] L. O. Gostin, "National health information privacy: regulations under the Health Insurance Portability and Accountability Act," *Jama*, vol. 285, no. 23, pp. 3015-3021, 2001

[12] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," *Ieee Access*, vol. 8, pp. 140699-140725, 2020 2020

[13] T. Yang *et al.*, "Applied federated learning: Improving google keyboard query suggestions," *arXiv preprint arXiv:1812.02903*, 2018

[14] D. Leroy, A. Coucke, T. Lavril, T. Gisselbrecht, J. Dureau, and Ieee, "Federated Learning for Keyword Spotting," in *44th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, ENGLAND, 2019

May 12-17 2019, in International Conference on Acoustics Speech and Signal Processing ICASSP, 2019, pp. 6341-6345.

[15] F. Hartmann, S. Suh, A. Komarzewski, T. D. Smith, and I. Segall, "Federated learning for ranking browser history suggestions," *arXiv preprint arXiv:1911.11807*, 2019

[16] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *Ieee Signal Processing Magazine*, vol. 37, no. 3, pp. 50-60, May 2020

[17] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," *arXiv preprint arXiv:1710.06963*, 2017

| Cơ quan Chủ trì<br>*(ký, họ và tên, đóng dấu)* | Chủ nhiệm đề tài<br>*(ký, họ và tên)* |
|---|---|
| | **Đoàn Thanh Phương** |