	<b>VIETTEL AI RACE</b>	TD073
	Phương pháp Học Liên Kết (Federated Learning) trong Bảo Mật Dữ Liệu Y Tế	Lần ban hành: 1

## 1. Bối cảnh và động lực

Trong ngành y tế, việc ứng dụng trí tuệ nhân tạo (AI) vào chẩn đoán, dự đoán và phân tích dữ liệu bệnh nhân ngày càng phổ biến. Tuy nhiên, dữ liệu y tế thường chứa thông tin cá nhân cực kỳ nhạy cảm (hồ sơ bệnh án, hình ảnh y khoa, kết quả xét nghiệm), chịu ràng buộc bởi các quy định nghiêm ngặt như HIPAA (Mỹ), GDPR (châu Âu) và các tiêu chuẩn bảo mật dữ liệu quốc gia.

Vấn đề: Các bệnh viện, phòng khám và tổ chức nghiên cứu muốn hợp tác để xây dựng mô hình AI có độ chính xác cao, nhưng không thể chia sẻ dữ liệu thô do rào cản pháp lý và đạo đức.

Giải pháp: Học Liên Kết (Federated Learning – FL) cho phép huấn luyện mô hình chung trên nhiều nguồn dữ liệu phân tán mà không cần chuyển dữ liệu ra khỏi cơ sở lưu trữ cục bộ.


## 2. Federated learning là gì?

Federated Learning là một phương pháp nhằm đào tạo các mô hình AI mà không cần bất kỳ ai nhìn thấy hoặc tác động vào dữ liệu của bạn. Điều này giúp bạn có thể sử dụng thông tin mà không cần chia sẻ dữ liệu thật sự, để phục vụ cho các ứng dụng AI mới.

## 3. Nguyên lý hoạt động của Federated Learning

Federated Learning được triển khai theo mô hình “huấn luyện phân tán – tổng hợp tập trung”:

1. Khởi tạo mô hình toàn cục (Global Model):  
Máy chủ trung tâm (server) gửi mô hình khởi tạo đến từng máy khách (client).
2. Huấn luyện cục bộ (Local Training):  
Mỗi cơ sở y tế huấn luyện mô hình trên dữ liệu của riêng mình.

	<b>VIETTEL AI RACE</b>	TD073
	Phương pháp Học Liên Kết (Federated Learning) trong Bảo Mật Dữ Liệu Y Tế	Lần ban hành: 1


3. Gửi trọng số (Model Updates):  
Chỉ các thông số/gradient đã cập nhật được gửi về máy chủ, không truyền dữ liệu thô.
4. Tổng hợp (Aggregation):  
Máy chủ dùng thuật toán như *Federated Averaging* để hợp nhất các trọng số, tạo ra mô hình toàn cục mới.
5. Lặp lại:  
Quá trình này tiếp tục cho đến khi mô hình hội tụ.

#### 4. Lợi ích trong y tế

- Bảo mật và quyền riêng tư:  
Dữ liệu bệnh nhân không bao giờ rời khỏi bệnh viện, giảm nguy cơ rò rỉ.
- Đa dạng dữ liệu:  
Mô hình được huấn luyện trên dữ liệu phong phú từ nhiều vùng miền, nâng cao khả năng tổng quát hóa.
- Tuân thủ pháp lý:  
Đáp ứng các quy định bảo mật nghiêm ngặt mà vẫn hợp tác được giữa nhiều tổ chức.

#### 5. Kiến trúc và thành phần chính

- Central Server (Máy chủ trung tâm): Quản lý mô hình toàn cục, điều phối việc tổng hợp trọng số.
- Clients (Máy khách): Bệnh viện, phòng thí nghiệm hoặc thiết bị y tế thông minh.
- Secure Communication Layer: Giao thức truyền thông bảo mật (SSL/TLS) để gửi thông số mô hình.
- Aggregation Algorithm: Thuật toán như *FedAvg*, *FedProx* để cân bằng chênh lệch dữ liệu giữa các khách.

	<b>VIETTEL AI RACE</b>	<b>TD073</b>
	Phương pháp Học Liên Kết (Federated Learning) trong Bảo Mật Dữ Liệu Y Tế	Lần ban hành: 1

## 6. Các phương pháp bảo mật nâng cao


1. Differential Privacy (DP):  
Thêm nhiễu vào gradient hoặc trọng số trước khi gửi về server, che giấu thông tin cá nhân.
2. Secure Multi-Party Computation (SMPC):  
Cho phép nhiều bên tính toán chung mà không tiết lộ dữ liệu riêng.
3. Homomorphic Encryption:  
Mã hóa dữ liệu sao cho vẫn có thể tính toán trực tiếp trên dữ liệu mã hóa.
4. Trusted Execution Environment (TEE):  
Sử dụng phần cứng bảo mật để đảm bảo chỉ các quá trình được phép mới có thể truy cập thông tin.

## 7. Ứng dụng thực tiễn

- Chẩn đoán hình ảnh y khoa:  
Huấn luyện mô hình phân tích MRI, CT từ nhiều bệnh viện để phát hiện ung thư sớm.
- Dự đoán nguy cơ bệnh mãn tính:  
Kết hợp dữ liệu hồ sơ bệnh án điện tử từ nhiều cơ sở để dự đoán tiểu đường, tim mạch.
- Theo dõi thiết bị đeo y tế:  
Đồng bộ dữ liệu cảm biến từ hàng nghìn thiết bị đeo để phát hiện sớm rối loạn tim.

## 8. Thách thức kỹ thuật


- Dữ liệu không đồng nhất (Non-IID):  
Mỗi bệnh viện có đặc điểm dân số, thiết bị và quy trình thu thập dữ liệu khác nhau.

	<b>VIETTEL AI RACE</b>	<b>TD073</b>
	Phương pháp Học Liên Kết (Federated Learning) trong Bảo Mật Dữ Liệu Y Tế	Lần ban hành: 1

- Kết nối mạng:  
Cần đường truyền ổn định và bảo mật.
- Chi phí tính toán cục bộ:  
Một số cơ sở y tế có hạ tầng hạn chế, khó chạy mô hình lớn.
- Cân bằng quyền lực giữa các bên:  
Đảm bảo công bằng giữa các bệnh viện lớn nhỏ khi đóng góp dữ liệu.
- Kết nối mạng:  
Cần đường truyền ổn định và bảo mật.
- Chi phí tính toán cục bộ:  
Một số cơ sở y tế có hạ tầng hạn chế, khó chạy mô hình lớn.
- Cân bằng quyền lực giữa các bên:  
Đảm bảo công bằng giữa các bệnh viện lớn nhỏ khi đóng góp dữ liệu.
- Kết nối mạng:  
Cần đường truyền ổn định và bảo mật.
- Chi phí tính toán cục bộ:  
Một số cơ sở y tế có hạ tầng hạn chế, khó chạy mô hình lớn.
- Cân bằng quyền lực giữa các bên:  
Đảm bảo công bằng giữa các bệnh viện lớn nhỏ khi đóng góp dữ liệu.

## 9. Hướng phát triển tương lai

- Federated Learning kết hợp Edge Computing:  
Đưa FL xuống thiết bị di động, thiết bị đeo y tế để huấn luyện trực tiếp trên biên mạng.
- Hybrid Federated + Transfer Learning:  
Dùng transfer learning để giảm số vòng huấn luyện liên kết.

	<b>VIETTEL AI RACE</b>	TD073
	Phương pháp Học Liên Kết (Federated Learning) trong Bảo Mật Dữ Liệu Y Tế	Lần ban hành: 1

- Tích hợp Blockchain: Đảm bảo tính minh bạch, bất biến trong ghi nhận quá trình huấn luyện và cập nhật mô hình.
- Mô hình lượng tử hóa: Giảm kích thước trọng số để tiết kiệm băng thông và thời gian truyền.