BỘ GIÁO DỤC
VÀ ĐÀO TẠO

VIỆN HÀN LÂM KHOA HỌC
VÀ CÔNG NGHỆ VIỆT NAM

HỌC VIỆN KHOA HỌC VÀ CÔNG NGHỆ

Trần Anh Tú

NGHIÊN CỨU XÂY DỰNG GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN CHO QUÁ TRÌNH HỌC LIÊN KẾT DỰA TRÊN MẬT MÃ

TÓM TẮT LUẬN ÁN TIẾN SĨ KHOA HỌC MÁY TÍNH
Mã số: 9 48 01 01

Hà Nội - 2024

Công trình được hoàn thành tại: Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Người hướng dẫn khoa học:
Người hướng dẫn 1: PGS. TS. Lương Thế Dũng, Học viện Kỹ thuật mật mã
Người hướng dẫn 2: GS. TS. Huỳnh Văn Nam, Viện Khoa học và Công nghệ tiên tiến Nhật Bản (JAIST)

Phản biện 1:
Phản biện 2:
Phản biện 3:

Luận án được bảo vệ trước Hội đồng đánh giá luận án tiến sĩ cấp Học viện họp tại Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam vào hồi giờ , ngày tháng năm .

Có thể tìm hiểu luận án tại:
1. Thư viện Học viện Khoa học và Công nghệ
2. Thư viện Quốc gia Việt Nam

MỤC LỤC

GIỚI THIỆU

Tính cấp thiết của đề tài

Học sâu đã trở thành công cụ hiệu quả cho rất nhiều tác vụ học máy hiện nay. Tuy nhiên, việc phụ thuộc vào các bộ dữ liệu với kích thước lớn lại đặt ra những lo ngại về quyền riêng tư. Học cộng tác phân tán (federated learning) ra đời như một giải pháp đột phá, cho phép các bên hợp tác huấn luyện mô hình mà vẫn giữ dữ liệu an toàn trên thiết bị cá nhân. Mặc dù mang đến nhiều lợi ích, học cộng tác phân tán vẫn đối mặt với những thách thức, điển hình là rò rỉ dữ liệu gián tiếp. Các kỹ thuật nhiễu ngẫu nhiên và mã hóa đã được nghiên cứu và áp dụng như những kỹ thuật hứa hẹn, góp phần nâng cao tính riêng tư hiệu quả hơn cho phương pháp này. Tuy nhiên, đi kèm với sự tương cường tính an toàn cho mô hình thì những ảnh hưởng tiềm tàng đến độ chính xác của mô hình và sự phức tạp về mặt tính toán lại trở thành những vấn đề làm cho nó khó ứng dụng được trong thực tiễn.

Mục tiêu của luận án

Mục tiêu của luận án này là phát triển các giao thức học cộng tác phân tán hiệu quả và an toàn trên cơ sở sử dụng các giao thức tính toán bảo mật nhiều thành viên (SMC). Cụ thể:

- Phát triển các giao thức SMC hiệu quả cho tính tổng các vector số thực trong môi trường bán tin cậy, trong đó tồn tại giả thiết thông đồng giữa các bên tham gia.
- Đề xuất giao thức huấn luyện mạng học sâu phân tán mới đảm bảo tính chính xác, hiệu quả và an toàn bằng cách kết hợp cơ chế học cộng tác phân tán và các giao thức SMC được đề xuất.

Đóng góp chính của luận án

Luận án có các đóng góp chính sau đây:

- Đóng góp 1. Đề xuất ba giao thức SMC cho bài toán tính tổng các vector số thực trong trường hợp các bên tham gia bán tin cậy. Các giao thức này cho phép đảm bảo an toàn trong trường hợp tối đa có $n-2$ trong n bên tham gia thông đồng.

- Đóng góp 2. Phát triển các giao thức học cộng tác phân tán đảm bảo tính an toàn và hiệu quả sử dụng các giao thức SMC đã đề xuất.

Cấu trúc luận án

Ngoài phần Mở đầu và Kết luận, nội dung của đồ án chia làm ba chương:

- Chương 1 trình bày tổng quan về vấn đề đảm bảo tính riêng tư cho deep learning, khảo sát các nghiên cứu có liên quan và phát biểu bài toán nghiên cứu.
- Chương 2 đề xuất ba giao thức tính tổng bảo mật các vector số thực hiệu quả. Các giao thức bao gồm: giao thức kết hợp lượng tử hóa với biến thể hệ mật Elgamal, giao thức sử dụng ma trận mặt nạ kết hợp biến thể của hệ mật ECC, giao thức sử dụng ma trận mặt nạ có xác thực. Đối với mỗi giao thức thực hiện phân tích, chứng minh tính an toàn và hiệu quả của nó.
- Chương 3 trình bày hai giao thức học cộng tác phân tán trên cơ sở sử dụng các giao thức SMC đã được đề xuất trong cả hai trường hợp mạng tập trung có máy chủ bán tin cậy và mạng phi tập trung. Phân tích, đánh giá hiệu quả của các giao thức này trên khía cạnh lý thuyết, và thực nghiệm đánh giá trên một số bộ dữ liệu khác nhau như: MNIST, SMS Spam, và CSIC2010 trên các kiến trúc mạng học sâu khác nhau như: CNN, LSTM, và CLCNN.

CHƯƠNG 1. BẢO ĐẢM TÍNH RIÊNG TƯ CHO HỌC SÂU

Chương này trình bày vấn đề đảm bảo tính riêng tư trong học sâu. Học liên kết kết hợp mật mã cho thấy tiềm năng trong việc bảo vệ tính riêng tư khi huấn luyện mạng nơ-ron. Tuy nhiên, các phương pháp mã hóa gặp phải hai hạn chế lớn: nguy cơ thông đồng do chia sẻ khóa và khó khăn trong việc xử lý số thực, dẫn đến khả năng mất độ chính xác. Các nội dung trong Chương 1 đã được công bố trong **Công bố 1**.

1.1. Học sâu

Học sâu là một lĩnh vực học máy đòi hỏi nhiều lớp trừu tượng phi tuyến được thiết kế nhằm phát hiện và mô hình hóa các mẫu phức tạp. Học sâu gặp phải những thách thức lớn, bao gồm nhu cầu về lượng dữ liệu khổng lồ và yêu cầu sức mạnh tính toán đáng kể để tiến hành quá trình huấn luyện hiệu quả.

1.2. Đảm bảo tính riêng tư trong học sâu

Hiệu quả của các mạng nơ-ron sâu phụ thuộc đáng kể vào kích thước của tập dữ liệu huấn luyện. Việc huấn luyện mô hình toàn cục trong môi trường cộng tác gặp phải một thách thức lớn: chia sẻ dữ liệu riêng tư cục bộ giữa các bên tham gia. Để giải quyết vấn đề này, khái niệm đảm bảo tính riêng tư trong học sâu đã ra đời [1].

1.3. Một số phương pháp đảm bảo tính riêng tư

1.3.1. Nặc danh hóa

Để bảo vệ tính riêng tư trong quá trình huấn luyện mô hình, dữ liệu được tách biệt khỏi danh tính của chủ sở hữu. Tuy nhiên, việc ẩn danh đơn giản (ví dụ như loại bỏ tên) thường không đủ, như đã được minh chứng qua trường hợp cuộc thi Netflix Prize.

1.3.2. Các kỹ thuật mật mã và tính toán bảo mật nhiều thành viên

1.3.2.1. Khái niệm

Định nghĩa 1.3.1. *Giả sử K ($K \geq 2$) là số lượng phần tử của tập các thành viên tham gia vào mạng tính toán phân tán. Mỗi thành viên $i \in \{1, 2, \ldots, K\}$*

có một đầu vào $x_i \in X_i$. Hàm f được định nghĩa là một hàm tính toán đa bên như sau:

$$\begin{aligned} f &: X \to Y \\ \bar{x} = (x_1, x_2, \ldots, x_K) &\mapsto f(\bar{x}) = (f_1(\bar{x}), f_2(\bar{x}), \ldots, f_K(\bar{x})) \end{aligned} \tag{1.3.1}$$

Trong đó, $X = \{\bar{x} : \bar{x} = (x_1, \ldots, x_K)\}$ và $Y = \{y : y = (f_1(\bar{x}), \ldots, f_K(\bar{x}))\}$, và X_i là không gian giá trị của mỗi x_i.

1.3.2.2. Mô hình tấn công

Trong tính toán bảo mật nhiều thành viên (SMC), các cuộc tấn công của đối thủ được phân loại theo hành vi, sức mạnh và loại hình tấn công. Về hành vi, đối thủ có thể là bán trung thực hoặc độc hại. Về năng lực tấn công, họ có thể bị giới hạn hoặc không giới hạn về mặt tính toán. Ngoài ra, đối thủ còn được phân thành tĩnh hoặc thích ứng, tùy thuộc vào cách họ lựa chọn mục tiêu để tấn công.

1.3.2.3. Định nghĩa an toàn

Luận án áp dụng định nghĩa an toàn cho các giao thức tính toán đa bên trong mô hình bán trung thực, sử dụng các kênh truyền thông công khai của O. Goldreich. [2].

Các kỹ thuật chính trong SMC bao gồm chuyển giao mù, mã hóa đồng cấu và chia sẻ bí mật.

1.3.3. Các kỹ thuật làm nhiễu dữ liệu

Các kỹ thuật làm nhiễu dữ liệu bao gồm việc thay đổi hoặc tạo dữ liệu từ tập dữ liệu gốc để huấn luyện mô hình. Những kỹ thuật này bao gồm nhiễu cộng, nhiễu nhân, tạo sinh nhiễu và tổng hợp dữ liệu.

1.4. Các phương pháp đảm bảo tính riêng tư cho học sâu

Các nghiên cứu về PPDL có thể được chia làm 3 nhóm phương pháp chính. Nhóm phương pháp đầu tiên liên quan đến việc chia sẻ tập dữ liệu cục bộ dưới dạng nhiễu hoặc mã hóa, sau đó sử dụng các thuật toán học máy chuyên biệt [3–7]. Phương pháp này, được gọi là "phương pháp chia sẻ dữ

liệu," sử dụng các kỹ thuật như mã hóa đồng cấu (HE), SMC, chia sẻ bí mật, hoặc thêm nhiễu.

PATE [8] là một phương pháp khác trong PPDL. Ở phương pháp thứ hai này, thay vì chia sẻ các tập dữ liệu huấn luyện cục bộ, các bên tham gia hoặc "giáo viên" chia sẻ kiến thức về đầu ra dự đoán cho một mô hình máy chủ "học sinh". Sau đó, máy chủ "học sinh" huấn luyện mô hình công khai bằng cách sử dụng một tập dữ liệu công khai chưa được gán nhãn trên kết quả của các mô hình giáo viên.

Học phân tán, đặc biệt là học liên kết, là phương pháp chủ đạo để huấn luyện các mô hình học sâu phân tán ngày nay. Phương pháp này giải quyết vấn đề rò rỉ dữ liệu trực tiếp bằng cách trao đổi các mô hình huấn luyện trung gian thay vì chia sẻ dữ liệu cục bộ. Tuy nhiên, việc chia sẻ trực tiếp các tham số mô hình có thể gây ra lỗ hổng do rò rỉ dữ liệu gián tiếp thông qua các cuộc tấn công như đảo ngược mô hình hoặc suy luận thành viên. Kết quả là, nhiều nghiên cứu đã tích hợp các kỹ thuật như DP và SMC để tăng cường bảo mật khi chia sẻ các vector tham số mô hình. Các phương pháp DP thường yêu cầu sự đánh đổi giữa độ chính xác của mô hình và tính riêng tư. Giảm nhiễu cải thiện độ chính xác của mô hình nhưng lại làm tăng nguy cơ bị tấn công dẫn đến rò rỉ dữ liệu gián tiếp. Do đó, việc sử dụng SMC trong Học liên kết được đánh giá cao. Tuy nhiên, các giao thức SMC hiện nay gặp phải hai hạn chế đáng chú ý.

- Hạn chế đầu tiên liên quan đến việc các bên tham gia phải chia sẻ cùng một khóa, khiến SMC dễ bị tổn thương trong các kịch bản thông đồng.
- Hạn chế thứ hai liên quan đến hiệu quả trong việc xử lý số thực dấu chấm động. Các vector tham số cần phải chuyển đổi thành số nguyên lớn, gây hạn chế đáng kể đến khả năng tính toán của các giao thức.

Do đó, cần phát triển các giao thức SMC có khả năng xử lý thông đồng và duy trì độ chính xác với các vector số thực trong Học liên kết. Luận án này đề xuất các giao thức SMC hiệu quả để bảo vệ tham số trong quá trình huấn luyện phân tán mô hình học sâu, đảm bảo hoạt động tốt với vector số thực trong môi trường đa bên, ngay cả khi có thông đồng.

1.5. Hạn chế của các phương pháp PPDL hiện nay

Phương pháp chia sẻ đầu vào thường bao gồm việc thêm nhiễu hoặc sử dụng mật mã. Tuy nhiên, việc thêm nhiễu làm suy yếu tính bảo mật khi dữ liệu trở nên dễ bị tấn công suy luận và làm giảm độ chính xác của mô hình

do sự biến dạng dữ liệu. Trong khi đó, SMC cải thiện an toàn nhưng lại làm tăng độ phức tạp tính toán và truyền thông. Nó cũng phụ thuộc vào việc chia sẻ khóa, giới hạn an toàn trong các tính toán hai bên, khiến nó phù hợp hơn cho dự đoán hơn là huấn luyện.

Chia sẻ đầu ra ảnh hưởng đến độ chính xác của mô hình do lỗi từ các mô hình giáo viên và yêu cầu dữ liệu công khai cùng các mô hình cục bộ chất lượng cao, điều này không thực tế trong các môi trường huấn luyện phân tán với dữ liệu hạn chế.

Chia sẻ mô hình, được chia thành học phân tách (split learning) và học liên kết (federated learning), mang lại các đánh đổi khác nhau. Học phân tách chia sẻ các tham số của một số lớp trong mạng và làm giảm độ chính xác và giới hạn số lượng người tham gia. Học liên kết là giải pháp thực tế nhất cho học sâu phân tán, cân bằng giữa độ chính xác và chi phí thực hiện trong khi ngăn ngừa rò rỉ dữ liệu trực tiếp. Dù vậy, nó vẫn dễ bị rò rỉ gián tiếp thông qua các tham số mô hình bị lộ. Để giảm thiểu điều này, các kỹ thuật như Bảo mật vi sai (DP) và SMC được đề xuất. Do DP phải hy sinh độ chính xác, vì vậy học liên kết kết hợp với SMC nổi lên như một hướng nghiên cứu đầy hứa hẹn, mang lại sự cân bằng giữa bảo mật và hiệu suất.

Tuy nhiên, việc tích hợp học liên kết với SMC đối mặt với các thách thức chính:

- Các bên tham gia phải chia sẻ khóa mật mã trực tiếp hoặc thông qua một trung gian đáng tin cậy, điều này dễ dẫn đến rủi ro thông đồng.
- Việc chuyển đổi số thực thành số nguyên lớn làm tăng tải tính toán và làm chậm cả quá trình tính toán lẫn truyền tải dữ liệu.

1.6. Kết luận chương

Chương này đã thảo luận về vấn đề đảm bảo tính riêng tư cho học sâu, các phương pháp khác nhau, và những ưu nhược điểm của từng phương pháp. Từ đó, luận án xác định trọng tâm nghiên cứu là đảm bảo tính riêng tư cho quá trình huấn luyện của các mạng học sâu phân tán, cụ thể hơn là các mô hình học liên kết. Thông qua phân tích, luận án cũng kết luận rằng quá trình huấn luyện này chủ yếu đòi hỏi việc tính tổng các vector số thực. Do đó, luận án sẽ đề xuất các giao thức hiệu quả để tính tổng các vector số thực nhằm phục vụ mục đích này.

CHƯƠNG 2. NGHIÊN CỨU ĐỀ XUẤT CÁC GIAO THỨC TÍNH TỔNG BẢO MẬT VECTOR SỐ THỰC

Chương này giới thiệu ba giao thức mới được đề xuất để tính tổng bảo mật các vector số thực, được thiết kế để chống lại sự thông đồng. Nội dung của chương này liên quan đến các **Công bố 3, 5, 6**, và **7**.

2.1. Một số kiến thức cơ sở về mật mã

Nghiên cứu này dựa trên hai nền tảng quan trọng trong lĩnh vực mật mã, đó là bài toán logarit rời rạc trên các đường cong elliptic và trên các trường hữu hạn.

2.2. Giao thức tính tổng bảo mật vector số thực với kỹ thuật lượng tử hóa

2.2.1. Giao thức đề xuất

Giao thức đề xuất đầu tiên sử dụng kỹ thuật lượng tử hóa được mô tả trong Hình. 2.1.

2.2.2. Ước lượng sai số tính toán

Mệnh đề 2.2.1. *Giao thức đề xuất có thể xấp xỉ tổng của n vector với sai số của mỗi thành phần thứ j được tính theo công thức:*

$$\Delta S^{(j)} = \sqrt{(\delta_1^{(j)})^2 + (\delta_2^{(j)})^2 + \ldots + (\delta_n^{(j)})^2} \leq d(n+1).$$

Ở đây, d là số chữ số thập phân dùng để làm tròn.

2.2.3. Phân tích an toàn

Mệnh đề 2.2.2. *Giao thức tính tổng bảo mật cho n thành viên được trình bày trong Hình có khả năng bảo vệ tính riêng tư của mỗi bên tham gia trung thực trước máy chủ và lên đến $(n-2)$ bên bị tấn công.*

2.2.4. Đánh giá hiệu năng của giao thức

2.2.4.1. Chi phí tính toán

Chi phí tính toán cho việc tạo ra các giá trị chia sẻ và thời gian thực hiện tổng hợp bảo mật (dựa trên thuật toán Shank) được thể hiện trong Hình

Input:

- Mỗi bên U_i có vector riêng tư $W_i = \{W_i^{(j)}, 1 \leq j \leq model\_size\}$.
- Mỗi bên U_i có hai vector khóa riêng tư: $x_i = \{x_i^{(j)}\}, y_i = \{y_i^{(j)}\}$.
- Các tham số hệ thống: hệ số nhân (γ), $\mathbb{Z}_\mathbf{p}$ và phần tử sinh g.

Output: Tổng gần đúng của vector: $\tilde{W} = \sum_{i=1}^{n} W_i$.

Giai đoạn 1: Khởi tạo

- Mỗi bên U_i gửi các vector khóa công khai của mình $\{X_i^{(j)}\} = \{\mathbf{g}^{\mathbf{x}_i^{(j)}}\}, \{Y_i^{(j)}\} = \{\mathbf{g}^{\mathbf{y}_i^{(j)}}\}$, cùng với hệ số chuẩn hóa $(minW_i + \sigma_i, maxW_i + \sigma_i')$ tới máy chủ.
- Máy chủ tính toán: $X = \left\{ \prod_{i=1}^{n} X_i^{(j)} \right\}$; $Y = \left\{ \prod_{i=1}^{n} Y_i^{(j)} \right\}$ cho $1 \leq j \leq model\_size$ và $W_{max} = \max_{i=1}^{n}(maxW_i + \sigma_i')$ và $W_{min} = \min_{i=1}^{n}(minW_i + \sigma_i)$, sau đó gửi lại cho tất cả các bên tham gia.

Giai đoạn 2: Giai đoạn chính

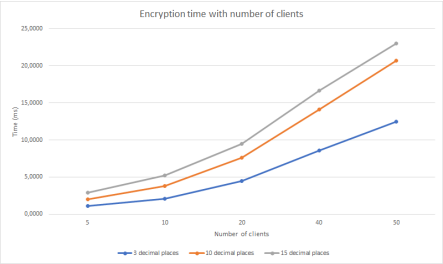
- Mỗi bên thực hiện lượng tử hóa các vector tham số: $\tilde{W}_i^{(j)} \leftarrow \frac{W_i^{(j)} - W_{min}}{W_{max} - W_{min}} \cdot 10^{\gamma}$, cho $1 \leq j \leq model\_size$.
- Mỗi bên U_i mã hóa các vector tham số bí mật: $\left\{ V_i^{(j)} = \frac{X^{(j)\mathbf{y}_i^{(j)}}}{Y^{(j)\mathbf{x}_i^{(j)}}} \cdot \mathbf{g}^{\tilde{W}_i^{(j)}} \right\}$ cho $1 \leq j \leq model\_size$ và gửi đến máy chủ.
- Máy chủ tính toán $\{V^{(j)}\} = \left\{ \prod_{i=1}^{n} V_i^{(j)} \right\}$ cho $1 \leq j \leq model\_size$.
- Máy chủ thực hiện thuật toán Shank để tìm $S^{(j)}$ với: $g^{S^{(j)}} = V^{(j)}$ cho $1 \leq j \leq model\_size$.
- Máy chủ tính tổng vector: $\frac{S^{(j)}}{10^{\gamma}}(W_{max} - W_{min}) + W_{min}$.

Hình 2.1: Giao thức Tính tổng Bảo mật của Vector dựa trên lượng tử hóa số nguyên và hệ mật Elgamal

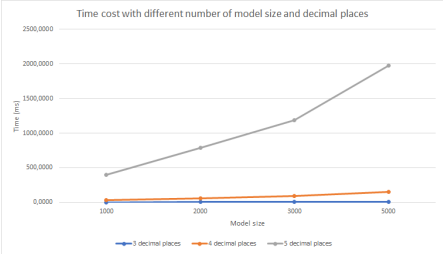
2.2. Kết quả cho thấy giao thức có chi phí thực thi thấp, khiến nó phù hợp cho các tình huống ứng dụng thực tế.

2.2.4.2. Chi phí truyền thông

Mức tiêu thụ băng thông tại phía các máy khách và Máy chủ cho mỗi vòng của giao thức được trình bày trong Bảng 2.1. Kết quả cho thấy giao thức yêu cầu băng thông gấp bốn lần so với mô hình không có bảo vệ quyền riêng tư. Tuy nhiên, sự đánh đổi này có thể chấp nhận được trong các ứng dụng thực tế, nhờ vào việc tăng cường đảm bảo quyền riêng tư.



(a) Thời gian trung bình để tính các giá trị chia sẻ



(b) Thời gian để tính giá trị tổng khi tổng hợp

Hình 2.2: Chi phí tính toán của quá trình tính các giá trị chia sẻ và tổng hợp tổng trong giao thức 1

	Máy khách i	**Máy chủ**
Vòng 1	$2 \times$ model size $\times$ key size	$2 \times$ model size $\times$ key size $\times\, n$
Vòng 2	model size $\times$ key size	model size $\times$ real number size $\times\, n$

Bảng 2.1: Chi phí truyền thông của giao thức 1

2.3. Giao thức tính tổng các vector số thực sử dụng ma trận mặt nạ

2.3.1. Giao thức đề xuất

Sử dụng hệ mật trên đường cong Elliptic, giao thức thứ hai cho phép nhiều bên cùng hợp tác tính toán tổng các thông điệp riêng tư mà không làm lộ giá trị thực. Giao thức này được tóm lược trong Hình 2.3.

2.3.2. Chứng minh tính đúng đắn

Mệnh đề 2.3.1. *Giao thức được đề xuất trong Hình 2.3 có thể tính chính xác tổng của n vectơ.*

Có thể chứng minh rằng $\sum_{i=1}^{n} T_i$ bằng $\sum_{i=1}^{n} W_i$, hay $T = \sum_{i=1}^{n} W_i$.

2.3.3. Phân tích an toàn

Mệnh đề 2.3.2. *Giao thức được đề xuất trong Hình 2.3 có thể bảo vệ tính riêng tư cho các thành viên trung thực trước máy chủ và tối đa* $(n-2)$ *thành*

Đầu vào:

- Mỗi bên U_i có ma trận riêng $\overline{W}_i = [W_i^{(kj)}]; 1 \leq j,k \leq d$.
- Mỗi bên U_i có bốn ma trận khóa bí mật: $p_i = [p_i^{(kj)}], q_i = [q_i^{(kj)}], c_i = [c_i^{(kj)}], d_i = [d_i^{(kj)}]$.
- Mỗi bên U_i có bốn ma trận ngẫu nhiên bí mật: M_i, N_i, r_i, s_i.
- Tham số hệ thống: Đường cong Elliptic $E(\mathbb{Z}_\mathbf{q})$ với bậc $\mathbf{q}$ và điểm sinh G.

Đầu ra: Vectơ tổng: $W = \sum_{i=1}^{n} W_i$.

Giai đoạn 1: Khởi tạo

- Thiết lập tham số hệ thống $E(\mathbb{Z}_\mathbf{q})$ và điểm sinh G.
- Mỗi bên U_i gửi khóa công khai của mình $P_i = \{p_i^{(kj)}G\}, Q_i = \{q_i^{(kj)}G\}$, và $C_i = \{c_i^{(kj)}G\}, D_i = \{d_i^{(kj)}G\}$ tới máy chủ.
- Máy chủ tính toán và gửi lại: $P = \sum_{i=1}^{n} P_i, Q = \sum_{i=1}^{n} Q_i, C = \sum_{i=1}^{n} C_i, D = \sum_{i=1}^{n} D_i$.

Giai đoạn 2: Giai đoạn chính

- Mỗi bên U_i tính toán và gửi các vectơ tham số công khai của mô hình đến máy chủ: $A_i = M_i + r_i, B_i = N_i + s_i$, $R_i = \{r_i^{(kj)}G + q_i^{(kj)}P^{(kj)} - p_i^{(kj)}Q^{(kj)}\}, S_i = \{s_i^{(kj)}G + c_i^{(kj)}D^{(kj)} - d_i^{(kj)}C^{(kj)}\}$
- Máy chủ sau đó tính $R = \sum_{i=1}^{n} R_i, S = \sum_{i=1}^{n} S_i$ và tìm r và s sao cho mỗi phần tử thỏa mãn $r^{(kj)}G = R^{(kj)}$ và $s^{(kj)}G = S^{(kj)}$, sau đó gửi $M = \sum_{i=1}^{n} A_i - r, N = \sum_{i=1}^{n} B_i - s$ cho tất cả các bên
- Mỗi bên tính $T_i = W_i + M_i N - M N_i$ và gửi T_i cho máy chủ
- Máy chủ nhận được tổng tất cả các thông điệp của các bên dưới dạng $T = \sum_{i=1}^{n} T_i = \sum_{i=1}^{n} W_i = W$.

Hình 2.3: Giao thức tính tổng vectơ bảo mật dựa trên ma trận mặt nạ

viên bị xâm phạm khác (cùng thông đồng với máy chủ) trong mô hình bán trung thực.

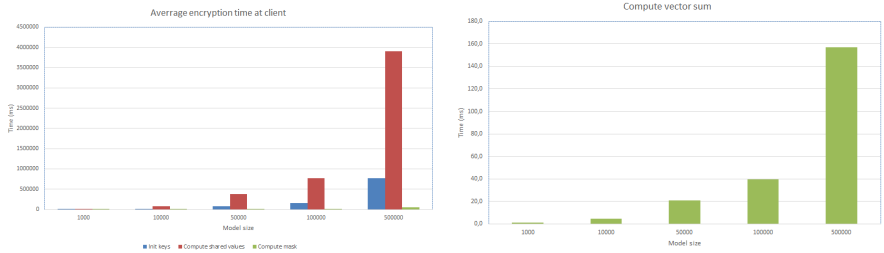
2.3.4. Đánh giá hiệu năng của giao thức

2.3.4.1. Chi phí tính toán

Chi phí tính toán cho việc tạo các giá trị chia sẻ và thời gian thực hiện tổng hợp kết quả (dựa trên thuật toán Shank) được minh họa trong Hình 2.4. Kết quả cho thấy giao thức chỉ phát sinh chi phí thực thi thấp, điều này giúp nó phù hợp cho các kịch bản ứng dụng thực tế.

2.3.4.2. Chi phí truyền thông

Chi phí băng thông trong mỗi vòng của giao thức được thể hiện trong Bảng 2.2. Kết quả chỉ ra rằng giao thức này yêu cầu băng thông cao hơn đáng kể so với giao thức đề xuất đầu tiên. Tuy nhiên, đối với các kịch bản yêu cầu độ chính xác cao, giao thức này lại có chi phí tính toán thấp hơn. Do đó, nó



(a) Trung bình tính giá trị chia sẻ (b) Thời gian thực hiện tính giá trị tổng

Hình 2.4: Chi phí tính toán giá trị chia sẻ và giá trị tổng trong giao thức SVS2

vẫn là một lựa chọn khả thi cho các ứng dụng thực tiễn.

	Thành viên i	**Máy chủ**
Vòng 1	$4 \times$ model size $\times$ key size	$4 \times$ model size $\times$ key size $\times\, n$
Vòng 2	$4 \times$ model size $\times$ real number size $+ 2 \times$ model size $\times$ key size	$2 \times$ model size $\times$ real number size $\times\, n$
Vòng 3	model size $\times$ real number size	model size $\times$ real number size $\times\, n$

Bảng 2.2: Chi phí truyền thông tại các vòng của giao thức SVS2

2.4. Giao thức tính tổng bảo mật vector sử dụng ma trận mặt nạ có xác thực

2.4.1. Giao thức đề xuất

Giao thức được đề xuất thứ ba được mô tả như trong Hình. 2.5.

2.4.2. Chứng minh tính đúng đắn

Mệnh đề 2.4.1. *Giao thức được đề xuất trong Hình 2.5 có thể tính chính xác tổng của n vectơ.*

Ta có: $V = (T - Q)H^{-1} = \left(\sum_{i=1}^{N} v_i\right) HH^{-1} = \sum_{i=1}^{N} v_i.$

2.4.3. Phân tích an toàn

Phần này của luận án chứng minh rằng (i) mỗi người dùng U_i, với các tham số P_i, r_i, s_i, đều được xác thực thành công, (ii) giao thức được chứng

Đầu vào:

- Mỗi bên U_i có ma trận riêng $\overline{W}_i = [W_i^{(kj)}]; 1 \leq j,k \leq d$.
- Mỗi bên U_i có hai ma trận khóa bí mật: $x_i = [x_i^{(kj)}], y_i = [y_i^{(kj)}]$.
- Tham số hệ thống: Trường hữu hạn $\mathbb{Z}_{\mathbf{p}}$, phần tử sinh g và ma trận khả nghịch H kích thước $d \times d$.

Đầu ra: Vectơ tổng: $W = \sum_{i=1}^{n} W_i$.

Giai đoạn 1: Giai đoạn khởi tạo

- Mỗi bên U_i gửi khóa công khai $\{X_i^{(jk)}\} = \{\mathbf{g}^{\mathbf{x}_i^{(jk)}}\}, \{Y_i^{(jk)}\} = \{\mathbf{g}^{\mathbf{y}_i^{(jk)}}\}$ đến máy chủ.
- Máy chủ tính toán: $\{X^{(jk)}\} = \left\{\prod_{i=1}^{n} X_i^{(jk)}\right\}$; $\{Y^{(jk)}\} = \left\{\prod_{i=1}^{n} Y_i^{(jk)}\right\}$ và gửi chúng lại cho tất cả các bên.

Giai đoạn 2: Giai đoạn chính

- Mỗi bên U_i tính toán mặt nạ công khai: $R_i^{(jk)} = g^{r_i^{(jk)}} \frac{X^{(jk)y_i^{(jk)}}}{Y^{(jk)x_i^{(jk)}}}$ và thông điệp $T_i = v_i H + r_i$ sau đó gửi đến máy chủ.
- Máy chủ sau đó tính $\{M_s^{(jk)}\} = \{\prod_{i=1}^{n} R_i^{(jk)}\}$ và tìm Q sao cho $g^{Q^{(jk)}} = M_s^{(jk)}$.
- Máy chủ thu được vectơ tổng bằng cách tính: $V = \sum_{i=1}^{n} v_i = (T - Q)H^{-1}$.

Hình 2.5: Giao thức SVS dựa trên ma trận mặt nạ có xác thực

minh là an toàn trước các cuộc tấn công tiềm ẩn trong mô hình tiên tri ngẫu nhiên, và (iii) giao thức thể hiện khả năng chống lại sự thông đồng của tối đa $n-2$ thành viên, bao gồm cả máy chủ tổng hợp.

Mệnh đề 2.4.2. *Giao thức được đề xuất trong Hình 2.5 đảm bảo an toàn trong mô hình bán trung thực.*

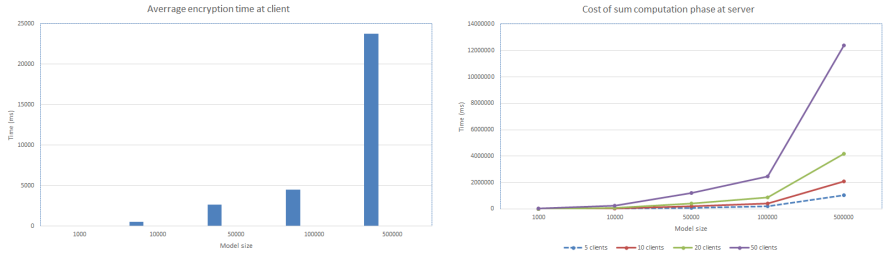
Mệnh đề 2.4.3. *Giao thức được đề xuất trong Hình 2.5 đảm tính riêng tư của các thành viên trung thực ngay cả trong trường hợp có tối đa n-2 thành viên thông đồng (và thông đồng với máy chủ).*

Các chứng minh cho hai mệnh đề này dựa trên các biến đổi tính toán và giả thiết an toàn của hệ mật sử dụng.

2.4.4. Đánh giá hiệu năng của giao thức

2.4.4.1. Chi phí tính toán

Hình 2.6 thể hiện chi phí tính toán cho việc tạo các giá trị chia sẻ và thời gian cần thiết để thực hiện tổng hợp bảo mật sử dụng thuật toán Shank. Kết quả cho thấy giao thức duy trì chi phí thực thi thấp, khiến nó trở thành một lựa chọn hiệu quả và thực tế cho các ứng dụng.



(a) Thời gian tính giá trị chia sẻ (b) Thời gian tính tổng an toàn

Hình 2.6: Chi phí tính toán cho việc tính giá trị chia sẻ và tính tổng bảo mật của giao thức SVS3

2.4.4.2. Chi phí truyền thông

Chi phí truyền thông trong mỗi vòng của giao thức được trình bày chi tiết trong Bảng 2.3. Kết quả cho thấy giao thức yêu cầu băng thông gấp bốn lần so với mô hình không có biện pháp bảo vệ quyền riêng tư. Tuy nhiên, sự gia tăng băng thông này là một sự đánh đổi hợp lý trong các ứng dụng thực tiễn, vì nó đảm bảo mức độ bảo vệ tính riêng tư cao hơn.

	Thành viên i	**Máy chủ**
Vòng 1	$2 \times$ model size $\times$ key size	$2 \times$ model size $\times$ key size $\times\, n$
Vòng 2	model size $\times\, (2 \times$ key size $+$ real number size$)$	model size $\times$ real number size $\times\, n$

Bảng 2.3: Chi phí truyền thông tại mỗi vòng

2.5. Tổng kết chương

Chương này đã phân tích và đề xuất ba giao thức mới cho phép tính tổng các vec tơ số thực một cách an toàn. Các giao thức được đề xuất đã được chứng minh là an toàn trong mô hình bán trung thực. Các đánh giá cũng đã chỉ ra tính hiệu quả của chúng. Do đó, các giao thức này có khả năng được áp dụng vào các bài toán thực tiễn yêu cầu tính toán an toàn giá trị tổng hoặc tần suất.

CHƯƠNG 3. XÂY DỰNG CÁC GIAO THỨC HUẤN LUYỆN MẠNG HỌC SÂU CỘNG TÁC PHÂN TÁN DỰA TRÊN SMC

3.1. Giao thức huấn luyện mạng học sâu phân tán với máy chủ tổng hợp bán tin cậy

3.1.1. Giao thức đề xuất

Giao thức 1 dưới đây thể hiện giao thức huấn luyện mạng học sâu phân tán với chủ tổng hợp bán tin cậy:

Giao thức 1: Khung học liên kết an toàn với máy chủ tổng hợp bán tin cậy

Đầu vào: Một máy chủ tổng hợp bán tin cậy và tập hợp n thành viên tham gia $\mathscr{U} = U_1, U_2, \ldots, U_n$, mỗi thành viên có một tập dữ liệu riêng tư tương ứng D_i với kích thước m_i, F: Tỷ lệ thành viên tham gia trong mỗi vòng giao tiếp, W^0 (mô hình toàn cục ban đầu).
Đầu ra: Mô hình toàn cục đã được huấn luyện W.
Quy trình huấn luyện:
Giai đoạn huấn luyện gồm T vòng giao tiếp. Mỗi vòng, ký hiệu là t, bao gồm các thao tác sau:

- Máy chủ chọn $n_t = F \times n$ thành viên cho vòng huấn luyện hiện tại.
- **Giai đoạn (1) - Tính toán các giá trị chia sẻ công khai:**
  - *Phía máy khách (thực hiện bởi n_t khách hàng đồng thời)*: Gửi các giá trị công khai tương ứng với các giá trị riêng tư của mình đến máy chủ.
  - *Máy chủ tổng hợp bán tin cậy:* Tính toán các giá trị chia sẻ công khai và phân phối chúng, cùng với mô hình toàn cục W^t, cho tất cả các bên tham gia vòng này.
- **Giai đoạn (2) - Tính toán tổng bảo mật:**
  - *Phía thành viên (thực hiện bởi n_t thành viên đồng thời):*
    - Huấn luyện mô hình W^t trên dữ liệu D_i của họ trong E vòng lặp, thu được W_i^{t+1}.
    - Truyền mô hình W_i^{t+1} đã được che giấu: $Mask(W_i^{t+1})$, sau khi áp dụng các biến đổi dựa trên các giá trị bí mật, đến máy chủ.
  - *Máy chủ tổng hợp bán tin cậy:*
    - Thực hiện giai đoạn tính toán tổng bảo mật với $Mask(W_i^{t+1}), 1 \leq i \leq n_t$ để thu được mô hình toàn cục:

$$W^{t+1} \leftarrow \sum_{i=1}^{n} \frac{m_i}{M} W_i^{t+1}.$$

    - Gửi mô hình toàn cục đã được cập nhật W^{t+1} cho tất cả các bên tham gia.

Hoạt động của khung được minh họa trong Khung 1 bao gồm: **Giai đoạn (1) - Tính toán các giá trị chia sẻ công khai** và **Giai đoạn (2) - Tính toán tổng bảo mật** thể hiện các giai đoạn thực thi của các giao thức tính toán bảo mật SMC trong Chương 2.

3.1.2. Triển khai thực nghiệm

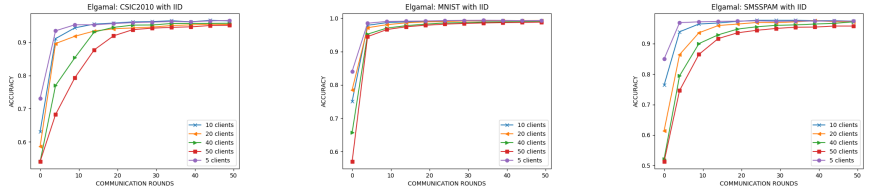
Các thực nghiệm đã được thực hiện trên ba bộ dữ liệu—CSIC2010, MNIST và SMS-Spam—để kiểm tra tác động của các yếu tố khác nhau lên hiệu suất của mô hình toàn cục, sử dụng các kiến trúc mạng tương ứng là CLCNN, CNN và LSTM.

3.1.3. Kết quả thực nghiệm và đánh giá

3.1.3.1. Hiệu suất của mô hình tổng quát

Khung học liên kết tập trung với giao thức tính tổng nhiều bên an toàn sử dụng ma trận mặt nạ

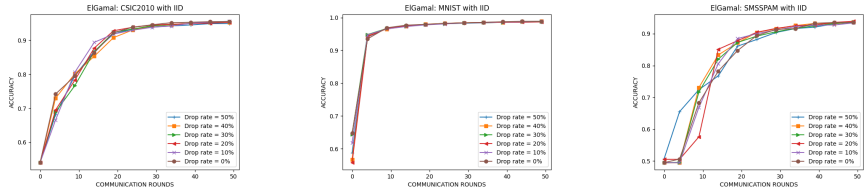
- *Tác động của số lượng thành viên.* Thực nghiệm đầu tiên liên quan đến việc đánh giá hiệu suất của mô hình toàn cục dưới sự thay đổi về số lượng thành viên. Các giao thức tính tổng bảo mật sử dụng ma trận mặt nạ được sử dụng để huấn luyện trong 50 vòng giao tiếp. Hình 3.1 trình bày kết quả với ba bộ dữ liệu: CSIC2010, MNIST và SMS-Spam.



Hình 3.1: Kết quả độ chính xác của mô hình theo số lượng thành viên.

- *Tác động của tỷ lệ thành viên rời bỏ trong mỗi vòng*. Hình 3.2 cho thấy tác động của các tỷ lệ dropout khác nhau lên hiệu suất của mô hình. Các đánh giá có hệ thống đã được thực hiện với các tỷ lệ dropout lần lượt là 0%, 10%, 20%, 30%, 40% và 50%.

Qua quá trình kiểm tra kỹ lưỡng, rõ ràng rằng kết quả thu được khi sử dụng giao thức tính tổng an toàn với mật mã ElGamal tương đồng chặt chẽ

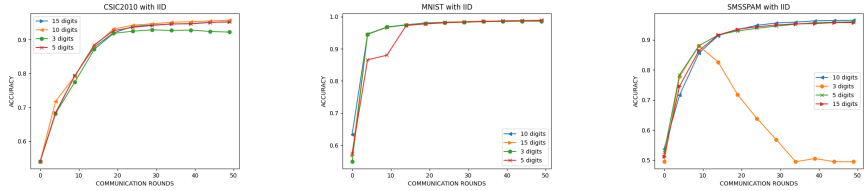


Hình 3.2: Độ chính xác của mô hình với các tỷ lệ số thành viên rời bỏ.

với kết quả từ việc thử nghiệm giao thức tính tổng an toàn sử dụng mật mã ECC. Sự tương đồng này có được là nhờ việc bảo toàn các tham số mô hình ở định dạng số thực ban đầu, đảm bảo tính toàn vẹn của tổng trong mô hình mong muốn.

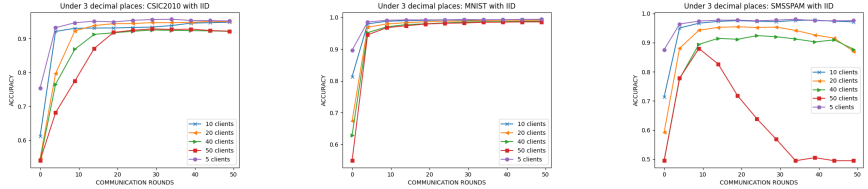
Kết quả độ chính xác của mô hình với giao thức sử dụng kỹ thuật lượng tử hóa

- *Ảnh hưởng của số số thập phân*. Như minh họa trong Hình 3.3, rõ ràng rằng việc làm tròn các tham số mô hình xuống chỉ còn 3 chữ số thập phân dẫn đến sự sụt giảm đáng kể về độ chính xác. Ngược lại, khi sử dụng các cài đặt độ chính xác mã hóa cao hơn (tức là 5 và 10 chữ số thập phân), chỉ có những biến đổi không đáng kể về hiệu suất. Đáng chú ý, việc giảm độ chính xác mã hóa không chỉ làm suy giảm độ chính xác của mô hình mà còn ảnh hưởng xấu đến tốc độ hội tụ, khiến mô hình cần thêm thời gian để hội tụ.



Hình 3.3: Độ chính xác của mô hình với số lượng số thập phân khác nhau.

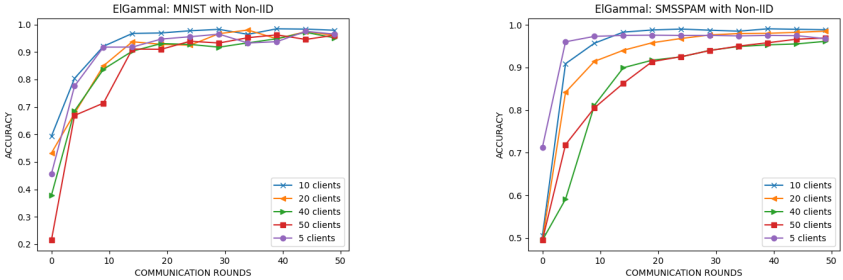
Khi số chữ số thập phân được cố định ở mức 3, Hình 3.4 minh họa độ chính xác của mô hình huấn luyện theo sự thay đổi về số lượng thành viên tham gia.



Hình 3.4: Độ chính xác của mô hình với 3 chữ số thập phân với số lượng thành viên khác nhau

3.1.3.2. Hiệu suất của mô hình với dữ liệu non-IID

- *Ảnh hưởng của số lượng thành viên tham gia.* Hình 3.5 cho thấy rằng việc tăng số lượng thành viên không nhất thiết dẫn đến hiệu suất tốt hơn. Khi số lượng thành viên tăng, sự đa dạng của dữ liệu có thể tăng theo. Tuy nhiên, các thách thức liên quan đến việc điều phối các thành viên và tổng hợp các cập nhật của họ cũng tăng lên. Điều này có thể thấy rõ trong trường hợp 50 thành viên, khi mô hình dường như gặp khó khăn trong việc tìm ra một mô hình hội tụ tốt.

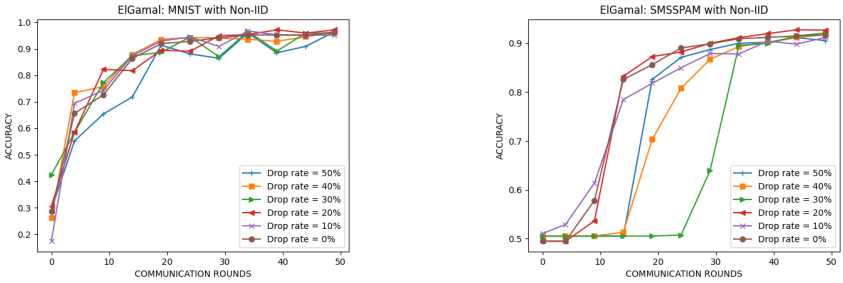


Hình 3.5: Độ chính xác của mô hình với sự thay đổi số lượng thành viên trong trường hợp non IID.

- *Ảnh hưởng của tỷ lệ rời bỏ trong mỗi vòng.* Hình 3.6 biểu diễn độ chính xác của mô hình với các tỷ lệ số thành viên rời bỏ khác nhau trong trường hợp non IID.

3.1.3.3. So sánh với các phương pháp khác

Kết quả so sánh được chỉ ra trong Bảng. 3.1.



Hình 3.6: Độ chính xác với tỷ lệ rời bỏ khác nhau.

Bảng 3.1: So sánh hiệu suất so với các phương pháp khác

Method	**Data**					
	IID			**Non-IID**		
	MNIST	**CSIC 2010**	**SMS Spam**	**MNIST**	**CSIC 2010**	**SMS Spam**
Standalone	.9658	.9448	.9203	.314	.6103	.8821
Centralized	.9943	.9676	.9806	.9943	.9676	.9806
Fed-Avg (small noise)	.9741	.9469	.9147	.9454	.9442	.8173
Fed-Avg (large noise)	.9659	.8745	.6397	.8954	.7214	.5634
Selective learning	.9629	.9575	.9619	.9724	.8534	.9662
FedAvg + SMC 1	.9942	.9685	.9728	.9882	.9433	.9762
FedAvg + SMC 2	.9913	.9654	.9692	.9869	.9621	.9793
FedAvg + SMC 3	.9913	.9654	.9692	.9869	.9621	.9793

3.2. Giao thức huấn luyện mạng học sâu phân tán trong môi trường phi tập trung

3.2.1. Giao thức đề xuất

Phần này trình bày giao thức huấn luyện mạng học sâu phân tán trong trường hợp các bên tham gia phi tập trung và không tồn tại bên thứ ba bán tin cậy.

Giao thức 2: Khung học liên bang phi tập trung với giao thức tính tổng nhiều bên an toàn

Đầu vào: Tập hợp n thành viên $\mathscr{U} = U_1, U_2, \ldots, U_n$ với các tập dữ liệu riêng tư D_i có kích thước m_i. F: Tỷ lệ thành viên tham gia trong mỗi vòng giao tiếp. Siêu tham số: T (số vòng giao tiếp), E (số vòng lặp cục bộ), B (kích thước mini-batch cục bộ), W^0 (mô hình toàn cục ban đầu). **Đầu ra:** Mô hình toàn cục đã được huấn luyện W.

Quy trình huấn luyện:
Giai đoạn huấn luyện bao gồm T vòng giao tiếp. Mỗi vòng, ký hiệu là t, bao gồm các thao tác sau:

- Các thành viên tham gia vào quá trình bỏ phiếu để chọn một nút chính, U_{master}. Nút chính chọn $n_t = F \times n$ thành viên cho vòng hiện tại.
- **Giai đoạn (1) - Tính toán các giá trị chia sẻ công khai:**
  - *Thao tác phía thành viên (thực hiện bởi n_t thành viên đồng thời)*: Gửi các giá trị công khai tương ứng với các giá trị riêng tư của thành viên tới nút chính.
  - *Thao tác phía nút chính*: Tính toán các giá trị chia sẻ công khai và phân phối chúng, cùng với mô hình toàn cục W^t, cho tất cả các thành viên tham gia trong vòng này.
- **Giai đoạn (2) - Tính toán tổng bảo mật:**
  - *Thao tác phía thành viên (thực hiện bởi n_t thành viên đồng thời)*:
    * Huấn luyện cục bộ mô hình W^t trên dữ liệu D_i của họ trong E vòng lặp, thu được W_i^{t+1}.
    * Tính toán các giá trị che giấu cho W_i^{t+1} bằng cách sử dụng các khóa bí mật tương ứng của thành viên i.
    * Truyền mô hình cục bộ đã được che giấu $Mask(W_i^{t+1})$ tới U_{master}.
  - *Thao tác phía nút chính*:
    * Huấn luyện cục bộ mô hình W^t trên dữ liệu D_{master} của nó trong E vòng lặp, tạo ra W_{master}^{t+1}.
    * Kết hợp các mô hình đã được che giấu nhận được và mô hình của chính nó, và thực hiện giai đoạn tính toán tổng bảo mật để thu được mô hình toàn cục:

$$W^{t+1} \leftarrow \sum_{i=1}^{n_t} \frac{m_i}{m} W_i^{t+1} + \frac{m_{\text{master}}}{m} W_{\text{master}}^{t+1}.$$

    * Truyền mô hình toàn cục W^{t+1} cho tất cả các thành viên.

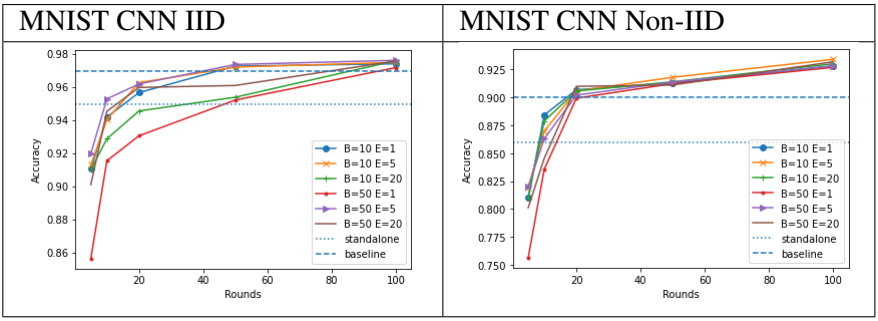
3.2.2. Triển khai thực nghiệm

Các thử nghiệm đã được tiến hành sử dụng bộ dữ liệu MNIST và UCI SMS Spam để đánh giá giao thức được đề xuất. Phần này trình bày hiệu quả của giao thức được đề xuất trong xử lý dữ liệu IID, Non-IID và không cân bằng với chi phí truyền thông thấp và độ chính xác cao.

3.2.3. Kết quả thực nghiệm và đánh giá

Hiệu suất tổng thể của mô hình. Hiệu suất của Khung công việc Huấn luyện Phân tán An toàn (SDTF) được minh họa trong Bảng 3.2. Sau 100 vòng truyền thông, giao thức được đề xuất đạt độ chính xác là 97.6% trên tập dữ liệu IID, trong khi con số đối với tập dữ liệu Non-IID là 93%. Mặc dù có sự thay đổi trong các tham số cục bộ, khung công việc có thể được coi là một mô hình có hiệu suất và độ chính xác cao.

Bảng 3.2: Độ chính xác với các tham số huấn luyện cục bộ khác nhau trên bộ dữ liệu MNIST với kiến trúc CNN



So sánh với một số mô hình khác. Thực nghiệm thứ hai so sánh độ chính xác của framework được đề xuất với sáu chiến lược huấn luyện khác khi sử dụng cùng một mô hình CNN trong 100 vòng truyền thông đầu tiên. Kết quả được trình bày trong Bảng 3.5. Framework được đề xuất thực hiện tốt hơn so với hầu hết các mô hình CNN được cung cấp trong kịch bản này với độ chính xác là 98.57% sau 100 vòng truyền thông.

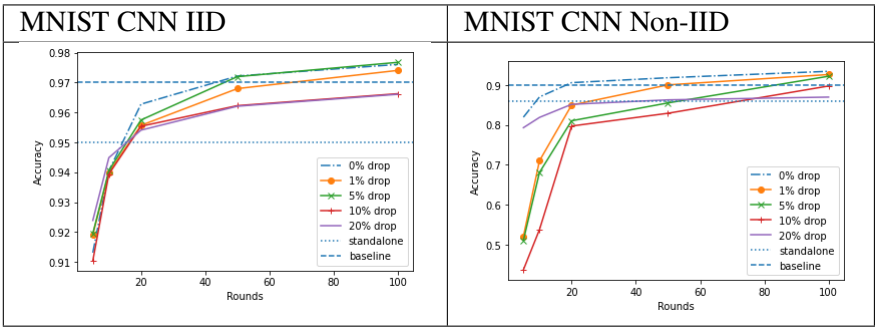
Bảng 3.3: So sánh độ chính xác của mô hình với trường hợp dữ liệu cân bằng phân bố đồng đều

	Selective 10%	Selective 50%	FedAVG		Downpour SGD	CNN Centralize	CNN Standalone	SDTF
			Large Noise	Small Noise				
5	0.7436	0.8141	0.75	0.899	0.8913	0.9756	0.9061	0.9616
10	0.7902	0.8417	0.802	0.901	0.9295	0.9824	0.9341	0.9798
20	0.8171	0.8686	0.866	0.934	0.9518	0.9889	0.9354	0.9803
50	0.8214	0.8991	0.871	0.945	0.9768	0.9901	0.9355	0.9843
100	0.8862	0.9105	0.88	0.96	0.9817	0.9912	0.9479	0.9857

Ảnh hưởng của tỷ lệ số nút rời bỏ trong mỗi vòng truyền thông.

Trong phần này, hiệu suất của framework được đề xuất được đánh giá trong bối cảnh có node dropout, xem xét các tỷ lệ dropout khác nhau. Kết quả được tóm tắt trong Bảng 3.4.

Bảng 3.4: Kết quả về hiệu suất của framework với các tỷ lệ nút rời bỏ mạng khác nhau trên tập dữ liệu MNIST.



Với dữ liệu không cân bằng. Thực nghiệm cuối cùng đánh giá cách mà framework được đề xuất xử lý dữ liệu mất cân bằng. Việc so sánh được thực hiện giữa SDTF và năm chiến lược huấn luyện khác nhau: học tập chọn lọc với 10%, học tập chọn lọc với 50%, DownpourSGD, FedAvg, và LSTM tập trung. Kết quả được trình bày trong Bảng 3.5.

Bảng 3.5: Độ chính xác của mô hình với dữ liệu không cân bằng

	Selective 10%	Selective 50%	Downpour SGD	FedAVG	LSTM Centralize	LSTM standalone	SDTF
5	0.9499	0.9507	0.9634	0.9568	0.9676	0.8645	0.9658
10	0.9551	0.9542	0.9641	0.9563	0.9689	0.867	0.9677
20	0.9559	0.9561	0.9684	0.9683	0.9782	0.9052	0.9686
50	0.9623	0.9678	0.9719	0.9696	0.9788	0.9134	0.9695
100	0.9688	0.9692	0.9726	0.9719	0.9813	0.9257	0.9721

3.3. Kết luận chương

Chương này đã giới thiệu hai giao thức huấn luyện học sâu phân tán dựa trên các phương pháp tính tổng vectơ số thực an toàn từ chương trước. Đánh giá trên các bộ dữ liệu MNIST, SMS Spam, và CSIC 2010 cho thấy các mô hình thu được đạt độ chính xác cao, vượt trội so với các phương pháp khác, chứng minh tính khả thi của các giao thức này trong thực tế. Những phát hiện này được trình bày chi tiết trong **Các công bố [2,3,4,5,6,7]**.

CHƯƠNG 4. KẾT LUẬN VÀ KIẾN NGHỊ

Luận án đã đề xuất ba giao thức tính tổng bảo mật nhiều thành viên cho vector số thực cũng như phát triển hai giao thức huấn luyện mạng học sâu phân tán dựa trên các giao thức này. Đối với mỗi đề xuất, luận án đã thực hiện phân tích các khía cạnh về tính an toàn, đánh giá hiệu năng và tính chính xác thu được của giao thức. Tóm lại, các kết quả chính của luận án như sau:

- Kết quả đầu tiên của luận án đó là ba giao thức tính tổng bảo mật cho các vector số thực trong đó đảm bảo tính tổng các vector số thực hiệu quả đảm bảo tính an toàn ngay cả trong trường hợp tối đa $n-2$ trong số n thành viên tham gia thông đồng trong môi trường bán trung thực. Các giao thức này bao gồm: giao thức sử dụng kỹ thuật lượng tử hóa, giao thức sử dụng ma trận mặt nạ và giao thức sử dụng ma trận mặt nạ có xác thực. Chúng đều được chứng minh là an toàn và hiệu quả để triển khai trong các ứng dụng thực tế.
- Kết quả thứ hai của luận án đó là phát triển các giao thức huấn luyện mạng học sâu phân tán sử dụng kết hợp kỹ thuật học cộng tác phân tán và các giao thức tính tổng bảo mật đã được đề xuất trong hai trường hợp có máy chủ bán tin cậy và phi tập trung. Các kết quả phân tích về khía cạnh an toàn và hiệu năng đã chứng minh rằng những giải pháp mới này đáp ứng được các yêu cầu thực tế để xây dựng những ứng dụng và hiệu quả.

Các kết quả của luận án đã góp phần trong việc phát triển các giao thức đảm bảo tính riêng tư cho học sâu nhằm đưa lĩnh vực này gần hơn với việc ứng dụng thực tế. Tuy nhiên, đây là lĩnh vực mới, đầy thử thách do đó cần có nhiều nghiên cứu hơn trong tương lai. Hướng phát triển tương lai của Luận án bao gồm:

- Phát triển các giao thức mới đảm bảo tính an toàn hậu lượng tử cùng với sự tiến bộ của các công nghệ mật mã.
- Phát triển, đánh giá các giao thức an toàn trong một số bài toán mới trong học máy như học máy giải thích được, học máy với dữ liệu bất định, học đa mục tiêu,...
- Ứng dụng các giao thức vào một số bài toán ứng dụng cụ thể như: y tế, tài chính.
- Xây dựng các giao thức mới để đáp ứng các tình huống tính toán phân tán mới hoặc các yêu cầu từ các bài toán thực tế.

DANH MỤC CÁC BÀI BÁO ĐÃ XUẤT BẢN
LIÊN QUAN ĐẾN LUẬN ÁN

1. Anh-Tu Tran, The-Dung Luong, Van-Nam Huynh. A Comprehensive Survey and Taxonomy on Privacy-Preserving Deep Learning. Neurocomputing Volume 576, 2024, Pages 127345 (SCI/ISI indexed, Scopus Q1).
2. Anh-Tu Tran, The-Dung Luong, Jessada Karnjana, Van-Nam Huynh. An efficient approach for privacy preserving decentralized deep learning models based on secure multi-party computation. Neurocomputing, Volume 422, 2021, Pages 245-262, ISSN 0925-2312. (SCI/ISI indexed, Scopus Q1).
3. Anh-Tu Tran, The Dung Luong, and Xuan Sang Pham. A Novel Privacy-preserving Federated Learning Model based on Secure Multi-party Computation. In: International Symposium on Integrated Uncertainty in Knowledge Modelling and Decision Making. Cham: Springer Nature Switzerland, 2023. (Scopus)
4. Anh-Tu Tran, and Xuan Sang Pham. A novel privacy-preserving deep learning scheme for the classification of Covid-19 in chest x-ray images. The 15th IEEE International Conference on KNOWLEDGE AND SYSTEMS ENGINEERING (KSE 2023), 2023.
5. Anh-Tu Tran, Van Vu Thi, Xuan Sang Pham. A Novel Federated Learning Model with Integer Encoding Method for Web Attack Detection. In Proceedings of the 15th National Conference on Fundamental and Applied Information Technology Research (FAIR'2022), 2022.
6. Anh-Tu Tran, The Dung Luong, and Xuan Sang Pham. Privacy-preserving Deep Learning Model with Integer Quantization and Secure Multi-party Computation. Annals of Operations Research, 2024 (SCI/ISI indexed, Scopus Q1).
7. Anh-Tu Tran, Van-Nam Huynh, Viet-Hung Dang. A Novel Privacy Preserving Framework for Training Dempster Shafer Theory-based Evidential Deep Neural Network. In International Conference on Belief Functions (pp. 98-107). Cham: Springer Nature Switzerland, 2024. (ISI indexed, Scopus).