Học máy liên kết: Khái niệm và ứng dụng

QIANG YANG, Đại học Khoa học và Công nghệ Hồng Kông, Hồng Kông
YANG LIU, Webank, Trung Quốc
TIANJIAN CHEN, Webank, Trung Quốc
YONGXIN TONG, Đại học Beihang, Trung Quốc

Trí tuệ nhân tạo ngày nay vẫn phải đối mặt với hai thách thức lớn. Một là trong hầu hết các ngành, dữ liệu tồn tại dưới dạng các hòn đảo bị cô lập. Hai là tăng cường quyền riêng tư và bảo mật dữ liệu. Chúng tôi đề xuất một giải pháp khả thi cho những thách thức này: học liên kết an toàn. Ngoài khuôn khổ học tập liên kết do Google đề xuất lần đầu tiên vào năm 2016, chúng tôi giới thiệu một khuôn khổ học tập liên kết an toàn toàn diện, bao gồm học tập liên kết theo chiều ngang, học tập liên kết theo chiều dọc và học tập liên kết chuyển đổi. Chúng tôi cung cấp các định nghĩa, kiến trúc và ứng dụng cho khung học tập liên kết và cung cấp một cuộc khảo sát toàn diện về các công trình hiện có về chủ đề này. Ngoài ra, chúng tôi đề xuất xây dựng dữ liệu giữa các tổ chức mạng dựa trên cơ chế liên kết như một giải pháp hiệu quả để cho phép chia sẻ kiến thức mà không ảnh hưởng đến quyền riêng tư của người dùng.

Các khái niệm về CCS: • Bảo mật và quyền riêng tư • Phương pháp điện toán Trí tuệ nhân tạo; học máy; học có giám sát;

Các từ và cụm từ khóa bổ sung: học tập liên kết, GDPR, học tập chuyển tiếp

Định dạng tham chiếu ACM:
Qiang Yang, Yang Liu, Tianjian Chen và Yongxin Tong. 2019. Học máy liên kết: Khái niệm và ứng dụng. ACM Trans. thông minh. hệ thống. công nghệ. 10, 2, Điều 12 (02/2019), 19 trang. https://doi.org/0000001.0000001

1. GIỚI THIỆU

2016 là năm trí tuệ nhân tạo (AI) lên ngôi. Với việc AlphaGo[59] đánh bại những kỳ thủ cờ vây hàng đầu của con người, chúng ta đã thực sự chứng kiến tiềm năng to lớn của trí tuệ nhân tạo (AI) và đã bắt đầu kỳ vọng vào công nghệ AI tiên tiến, phức tạp hơn trong nhiều ứng dụng, bao gồm ô tô không người lái, chăm sóc y tế, tài chính, v.v. Ngày nay, công nghệ AI đang thể hiện thế mạnh của mình trong hầu hết mọi ngành nghề và mọi tầng lớp xã hội. Tuy nhiên, khi nhìn lại quá trình phát triển của AI, không thể tránh khỏi sự phát triển của AI đã trải qua nhiều thăng trầm. Sẽ có một đợt suy thoái tiếp theo đối với AI? Khi nào nó sẽ xuất hiện và do những yếu tố nào? Mối quan tâm hiện tại của công chúng đối với AI một phần được thúc đẩy bởi tính sẵn có của Dữ liệu lớn: AlphaGo năm 2016 đã sử dụng tổng cộng 300.000 trò chơi làm dữ liệu huấn luyện để đạt được kết quả xuất sắc.

Với thành công của AlphaGo, mọi người đương nhiên hy vọng rằng AI dựa trên dữ liệu lớn như AlphaGo sẽ sớm được hiện thực hóa trong mọi khía cạnh của cuộc sống chúng ta. Tuy nhiên, các tình huống trong thế giới thực có phần đáng thất vọng: ngoại trừ một số ngành, hầu hết các lĩnh vực chỉ có dữ liệu hạn chế hoặc kém

Địa chỉ của tác giả: Qiang Yang, Đại học Khoa học và Công nghệ Hồng Kông, Hồng Kông, Trung Quốc; email: qyang@cse.ust.hk; Yang Liu, Webank, Thâm Quyến, Trung Quốc; email: yangliu@webank.com; Tianjian Chen, Webank, Thâm Quyến , Trung Quốc; email: tobychen@webank.com; Yongxin Tong (tác giả tương ứng), Trung tâm Đổi mới Tiên tiến về Dữ liệu Lớn và Điện toán Trí não, Đại học Beihang, Bắc Kinh, Trung Quốc; email: yxtong@buaa.edu.cn.

2157-6904/2019/2-ART12 $15,00
https://doi.org/0000001.0000001

dữ liệu chất lượng cao, khiến việc hiện thực hóa công nghệ AI trở nên khó khăn hơn chúng ta tưởng. Có thể kết hợp dữ liệu lại với nhau trong một trang web chung bằng cách vận chuyển dữ liệu giữa các tổ chức không? Trên thực tế, rất khó, nếu không muốn nói là không thể, trong nhiều tình huống để phá vỡ các rào cản giữa các nguồn dữ liệu. Nói chung, dữ liệu cần thiết trong bất kỳ dự án AI nào bao gồm nhiều loại. Ví dụ, trong dịch vụ giới thiệu sản phẩm dựa trên AI, người bán sản phẩm có thông tin về sản phẩm, dữ liệu mua hàng của người dùng, nhưng không có dữ liệu mô tả khả năng mua hàng và thói quen thanh toán của người dùng. Trong hầu hết các ngành, dữ liệu tồn tại dưới dạng các hòn đảo bị cô lập. Do sự cạnh tranh trong ngành, bảo mật quyền riêng tư và thủ tục hành chính phức tạp, ngay cả việc tích hợp dữ liệu giữa các bộ phận khác nhau của cùng một công ty cũng gặp phải sự phản đối nặng nề. Hầu như không thể tích hợp dữ liệu nằm rải rác khắp quốc gia và các tổ chức, hoặc chi phí bị cấm.

Đồng thời, với nhận thức ngày càng tăng của các công ty lớn ảnh hưởng đến bảo mật dữ liệu và quyền riêng tư của người dùng, việc nhấn mạnh vào quyền riêng tư và bảo mật dữ liệu đã trở thành một vấn đề lớn trên toàn thế giới. Tin tức về rò rỉ dữ liệu công cộng đang gây lo ngại lớn trên các phương tiện truyền thông đại chúng và chính phủ. Ví dụ, vụ vi phạm dữ liệu gần đây của Facebook đã gây ra một loạt các cuộc phản đối [70]. Đáp lại, các quốc gia trên khắp thế giới đang tăng cường luật pháp để bảo vệ quyền riêng tư và bảo mật dữ liệu. Một ví dụ là Quy định chung về bảo vệ dữ liệu (GDPR)[19] do Liên minh Châu Âu thực thi vào ngày 25 tháng 5 năm 2018. GDPR (Hình 1) nhằm mục đích bảo vệ quyền riêng tư cá nhân và bảo mật dữ liệu của người dùng. Nó yêu cầu các doanh nghiệp sử dụng các ngôn ngữ rõ ràng và dễ hiểu cho thỏa thuận người dùng của họ và cấp cho người dùng "quyền được lãng quên", nghĩa là người dùng có thể xóa hoặc thu hồi dữ liệu cá nhân của họ. Các công ty vi phạm dự luật sẽ bị phạt nặng. Các hành vi tương tự về quyền riêng tư và bảo mật đang được ban hành ở Hoa Kỳ và Trung Quốc. Ví dụ: Luật An ninh mạng của Trung Quốc và các Nguyên tắc chung của Luật Dân sự, được ban hành vào năm 2017, yêu cầu các doanh nghiệp Internet không được rò rỉ hoặc giả mạo thông tin cá nhân mà họ thu thập và khi thực hiện các giao dịch dữ liệu với bên thứ ba, họ cần đảm bảo rằng hợp đồng được đề xuất tuân theo các nghĩa vụ bảo vệ dữ liệu hợp pháp. Việc thiết lập các quy định này rõ ràng sẽ giúp xây dựng một xã hội dân sự hơn, nhưng cũng sẽ đặt ra những thách thức mới đối với các thủ tục giao dịch dữ liệu thường được sử dụng ngày nay trong AI.

Cụ thể hơn, các mô hình xử lý dữ liệu truyền thống trong AI thường liên quan đến các mô hình giao dịch dữ liệu đơn giản, trong đó một bên thu thập và chuyển dữ liệu cho bên khác và bên kia sẽ chịu trách nhiệm làm sạch và hợp nhất dữ liệu. Cuối cùng, một bên thứ ba sẽ lấy dữ liệu tích hợp và xây dựng các mô hình cho các bên khác sử dụng. Các mô hình thường là sản phẩm cuối cùng được bán dưới dạng dịch vụ. Thủ tục truyền thống này phải đối mặt với những thách thức với các quy định và luật dữ liệu mới ở trên. Đồng thời, vì người dùng có thể không rõ ràng về việc sử dụng các mô hình trong tương lai nên các giao dịch vi phạm các luật như GDPR. Do đó, chúng tôi phải đối mặt với một tình thế tiến thoái lưỡng nan là dữ liệu của chúng tôi ở dạng các hòn đảo bị cô lập, nhưng trong nhiều trường hợp, chúng tôi bị cấm thu thập, hợp nhất và sử dụng dữ liệu ở những nơi khác nhau để xử lý AI. Làm thế nào để giải quyết hợp pháp vấn đề phân mảnh và cô lập dữ liệu là một thách thức lớn đối với các nhà nghiên cứu và thực hành AI ngày nay.

Trong bài viết này, chúng tôi đưa ra cái nhìn tổng quan về một phương pháp mới được gọi là học liên kết, đây là một giải pháp khả thi cho những thách thức này. Chúng tôi khảo sát các công trình hiện có về học tập liên kết và đề xuất các định nghĩa, phân loại và ứng dụng cho một khung học tập liên kết an toàn toàn diện. Chúng tôi thảo luận về cách áp dụng thành công khuôn khổ học tập liên kết cho các doanh nghiệp khác nhau . Khi thúc đẩy học tập liên kết, chúng tôi hy vọng sẽ chuyển trọng tâm phát triển AI từ cải thiện hiệu suất mô hình, vốn là điều mà hầu hết lĩnh vực AI hiện đang làm, sang nghiên cứu các phương pháp tích hợp dữ liệu tuân thủ luật bảo mật và quyền riêng tư dữ liệu.

2 TỔNG QUAN VỀ LIÊN KẾT HỌC TẬP

Khái niệm học liên kết được Google đề xuất gần đây [36, 37, 41]. Ý tưởng chính của họ là xây dựng các mô hình học máy dựa trên các tập dữ liệu được phân phối trên nhiều thiết bị đồng thời ngăn chặn rò rỉ dữ liệu. Những cải tiến gần đây đã tập trung vào việc khắc phục

Quả sung. 1. GDPR: Quy định của EU về bảo vệ dữ liệu

thách thức thống kê [60, 77] và cải thiện bảo mật [9, 23] trong học tập liên kết. Ngoài ra còn có những nỗ lực nghiên cứu để làm cho việc học liên kết trở nên cá nhân hóa hơn [13, 60]. Tất cả các công việc trên đều tập trung vào học tập được liên kết trên thiết bị, nơi có liên quan đến tương tác của người dùng di động phân tán và chi phí liên lạc trong phân phối lớn, phân phối dữ liệu không cân bằng và độ tin cậy của thiết bị là một số yếu tố chính để tối ưu hóa. Ngoài ra, dữ liệu được phân vùng theo Id người dùng hoặc Id thiết bị, do đó, theo chiều ngang trong không gian dữ liệu. Dòng công việc này rất liên quan đến học máy bảo vệ quyền riêng tư, chẳng hạn như [58] vì nó cũng xem xét quyền riêng tư của dữ liệu trong môi trường học tập hợp tác phi tập trung. Để mở rộng khái niệm học tập liên kết để bao gồm các kịch bản học tập cộng tác giữa các tổ chức, chúng tôi mở rộng "học tập liên kết" ban đầu thành một khái niệm chung cho tất cả các kỹ thuật học máy cộng tác phi tập trung bảo vệ quyền riêng tư. Trong [71], chúng tôi đã đưa ra một cái nhìn tổng quan sơ bộ về kỹ thuật học liên kết và học chuyển giao liên kết. Trong bài viết này, chúng tôi tiếp tục khảo sát các nền tảng bảo mật có liên quan và khám phá mối quan hệ với một số lĩnh vực liên quan khác, chẳng hạn như lý thuyết đa tác nhân và khai thác dữ liệu bảo vệ quyền riêng tư. Trong phần này, chúng tôi cung cấp một định nghĩa toàn diện hơn về học liên kết xem xét các phân vùng dữ liệu, bảo mật và ứng dụng. Chúng tôi cũng mô tả quy trình làm việc và kiến trúc hệ thống cho hệ thống học tập liên kết.

2.1 Định nghĩa về học liên kết Xác định N chủ sở

hữu dữ liệu {F1, ...FN }, tất cả đều muốn đào tạo một mô hình học máy bằng cách consoli xác định niên đại cho dữ liệu tương ứng của họ {D1, ...DN }. Một phương pháp thông thường là tập hợp tất cả dữ liệu lại với nhau và sử dụng D = D1 ĐN để huấn luyện một mô hình MSU M . Hệ thống học liên kết là một quá trình học trong đó trong đó các chủ sở hữu dữ liệu hợp tác đào tạo một mô hình MF ED , Fi không để lộ dữ liệu Di của mình xử lý bất kỳ chủ sở hữu dữ liệu nào cho người khác nên rất gần với hiệu suất của MSU M , VSU M. Chính .Ngoài ra, độ chính xác của MF ED , được ký hiệu là VF ED thức, đặt δ là một số thực không âm , nếu

$$| VF ED \quad VSU M |< \delta \tag{Một}$$

chúng tôi nói thuật toán học liên kết bị mất độ chính xác δ.

2.2 Quyền riêng tư của việc học liên kết

Quyền riêng tư là một trong những thuộc tính cơ bản của việc học liên kết. Điều này đòi hỏi các mô hình bảo mật và phân tích để cung cấp các đảm bảo quyền riêng tư có ý nghĩa. Trong phần này, chúng tôi xem xét và so sánh ngắn gọn các kỹ thuật bảo mật khác nhau để học liên kết, đồng thời xác định các phương pháp và thách thức tiềm ẩn để ngăn chặn rò rỉ gián tiếp.

1Định nghĩa về bảo mật dữ liệu có thể khác nhau trong các tình huống khác nhau, nhưng cần phải cung cấp ý nghĩa đảm bảo quyền riêng tư. Chúng tôi trình bày các ví dụ về định nghĩa bảo mật trong phần 2.3

Tính toán đa bên an toàn (SMC). Các mô hình bảo mật SMC đương nhiên liên quan đến nhiều bên và cung cấp bằng chứng bảo mật trong khung mô phỏng được xác định rõ ràng để đảm bảo kiến thức hoàn toàn bằng không, nghĩa là mỗi bên không biết gì ngoại trừ đầu vào và đầu ra của mình. Không có tri thức là điều rất được mong muốn, nhưng đặc tính mong muốn này thường yêu cầu các giao thức tính toán phức tạp và có thể không đạt được hiệu quả. Trong một số trường hợp nhất định, tiết lộ một phần kiến thức có thể được coi là chấp nhận được nếu đảm bảo an ninh được cung cấp. Có thể xây dựng một mô hình bảo mật với SMC theo yêu cầu bảo mật thấp hơn để đổi lấy hiệu quả [16]. Gần đây, các nghiên cứu [46] đã sử dụng khung SMC để đào tạo các mô hình học máy với hai máy chủ và các giả định bán trung th Tham chiếu [33] sử dụng các giao thức MPC để đào tạo và xác minh mô hình mà người dùng không tiết lộ dữ liệu nhạy cảm. Một trong những khuôn khổ SMC tiên tiến nhất là Sharemind [8]. Tham khảo [44] đã đề xuất mô hình 3PC [5, 21, 45] với đa số trung thực và xem xét bảo mật trong cả hai giả định bán trung thực và độc hại. Những công việc này yêu cầu dữ liệu của người tham gia được chia sẻ bí mật giữa những người không thông đồng may chu .

Quyền riêng tư khác biệt. Một dòng công việc khác sử dụng các kỹ thuật Bảo mật khác biệt [18] hoặc k-Anonymity [63] để bảo vệ quyền riêng tư của dữ liệu [1, 12, 42, 61]. Các phương pháp riêng tư khác biệt, ẩn danh k và đa dạng hóa [3] liên quan đến việc thêm nhiễu vào dữ liệu hoặc sử dụng các phương pháp tổng quát hóa để che khuất một số thuộc tính nhạy cảm cho đến khi bên thứ ba không thể phân biệt được cá nhân, do đó khiến dữ liệu không thể được khôi phục bảo vệ quyền riêng tư của người dùng. Tuy nhiên, cốt lõi của các phương pháp này vẫn yêu cầu dữ liệu được truyền đi nơi khác và những công việc này thường liên quan đến sự đánh đổi giữa độ chính xác và quyền riêng tư. Trong [23], các tác giả đã giới thiệu một cách tiếp cận quyền riêng tư khác biệt đối với học tập liên kết để tăng cường bảo vệ dữ liệu phía khách hàng bằng cách ẩn các đóng góp của khách hàng trong quá trình đào tạo.

Mã hóa đồng hình. Mã hóa đồng hình [53] cũng được áp dụng để bảo vệ quyền riêng tư của dữ liệu người dùng thông qua trao đổi tham số theo cơ chế mã hóa trong quá trình học máy [24, 26, 48]. Không giống như bảo vệ quyền riêng tư khác biệt, bản thân dữ liệu và mô hình không được truyền đi và dữ liệu của bên kia cũng không thể đoán được chúng. Do đó, có rất ít khả năng rò rỉ ở cấp độ dữ liệu thô. Các công trình gần đây đã áp dụng mã hóa đồng cấu để tập trung hóa và đào tạo dữ liệu trên đám mây [75, 76]. Trên thực tế, Mã hóa đồng hình bổ sung [2] được sử dụng rộng rãi và cần thực hiện các phép tính gần đúng đa thức để đánh giá các hàm phi tuyến tính trong thuật toán học máy, dẫn đến sự đánh đổi giữa độ chính xác và quyền riêng tư [4, 35].

2.2.1 Rò rỉ thông tin gián tiếp. Các công trình tiên phong về học liên kết cho thấy các kết quả trung gian như cập nhật tham số từ thuật toán tối ưu hóa như Stochastic Gradient Descent (SGD) [41, 58], tuy nhiên không có đảm bảo bảo mật nào được cung cấp và việc rò rỉ các gradient này thực sự có thể làm rò rỉ thông tin dữ liệu quan trọng [51] khi được hiển thị cùng với cấu trúc dữ liệu, chẳng hạn như trong trường hợp pixel hình ảnh. Các nhà nghiên cứu đã xem xét tình huống khi một trong các thành viên của hệ thống học tập liên kết tấn công ác ý những người khác bằng cách cho phép chèn một cửa sau để tìm hiểu dữ liệu của người khác. Trong [6], các tác giả chứng minh rằng có thể chèn các cửa hậu ẩn vào một mô hình chung toàn cầu và đề xuất một phương pháp đầu độc mô hình "ràng buộc và quy mô" mới để giảm đầu độc dữ liệu. Trong [43], các nhà nghiên cứu đã xác định các lỗ hổng tiềm ẩn trong các hệ thống học máy cộng tác, trong đó dữ liệu đào tạo được sử dụng bởi các bên khác nhau trong học tập cộng tác dễ bị tấn công suy luận. Họ đã chỉ ra rằng một người tham gia đối nghịch có thể suy ra tư cách thành viên cũng như các thuộc tính được liên kết với một tập hợp con của dữ liệu đào tạo. Họ cũng thảo luận về các biện pháp bảo vệ có thể chống lại các cuộc tấn công này . công nhân.

Các nhà nghiên cứu cũng đã bắt đầu coi blockchain như một nền tảng để tạo điều kiện cho việc học tập liên kết. Trong [34], các nhà nghiên cứu đã xem xét kiến trúc học tập liên kết chuỗi khối (BlockFL), trong đó các bản cập nhật mô hình học tập cục bộ của thiết bị di động được trao đổi và xác minh bằng cách tận dụng chuỗi khối. Họ đã xem xét các vấn đề về tạo khối tối ưu, khả năng mở rộng mạng và độ bền .

2.3 Phân loại học liên kết Trong phần này, chúng ta thảo luận cách phân loại học liên kết dựa trên đặc tính phân phối của dữ liệu.

Đặt ma trận Di biểu thị dữ liệu được nắm giữ bởi mỗi chủ sở hữu dữ liệu i. Mỗi hàng của ma trận đại diện cho một mẫu và mỗi cột đại diện cho một tính năng. Đồng thời, một số bộ dữ liệu cũng có thể chứa dữ liệu nhãn. Chúng tôi biểu thị không gian tính năng là X, không gian nhãn là Y và chúng tôi sử dụng I để biểu thị không gian ID mẫu. Ví dụ: trong lĩnh vực tài chính, nhãn có thể là tín dụng của người dùng; trong lĩnh vực tiếp thị, nhãn có thể là mong muốn mua hàng của người dùng; trong lĩnh vực giáo dục, Y có thể là bằng cấp của sinh viên. Tính năng X, nhãn Y và Id mẫu I tạo thành tập dữ liệu huấn luyện hoàn chỉnh (I, X, Y). Tính năng và không gian mẫu của các bên dữ liệu có thể không giống nhau và chúng tôi phân loại học tập liên kết thành học tập liên kết theo chiều ngang, học tập liên kết theo chiều dọc và học tập chuyển giao có liên kết dựa trên cách dữ liệu được phân phối giữa các bên khác nhau trong không gian ID mẫu và đối tượng địa lý. Hình 2 cho thấy các khung học tập liên kết khác nhau cho kịch bản hai bên.

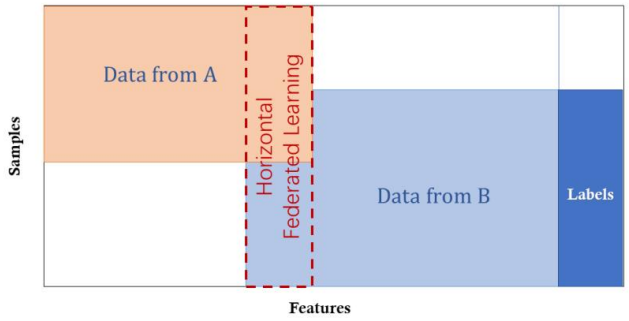
2.3.1 Học liên kết ngang. Học liên kết theo chiều ngang hoặc học liên kết dựa trên mẫu, được giới thiệu trong các tình huống mà các bộ dữ liệu chia sẻ cùng một không gian đặc trưng nhưng khác nhau về mẫu (Hình 2a). Ví dụ: hai ngân hàng khu vực có thể có các nhóm người dùng rất khác nhau từ các khu vực tương ứng của họ và tập giao nhau của những người dùng của họ là rất nhỏ. Tuy nhiên, hoạt động kinh doanh của họ rất giống nhau nên các không gian đặc trưng cũng giống nhau. Tham khảo [58] đã đề xuất một sơ đồ học sâu cộng tác trong đó những người tham gia đào tạo độc lập và chỉ chia sẻ các tập hợp con cập nhật tham số. Vào năm 2017, Google đã đề xuất một giải pháp học liên kết theo chiều ngang cho các bản cập nhật kiểu điện thoại Android [41]. Trong khuôn khổ đó, một người dùng duy nhất sử dụng điện thoại Android cập nhật cục bộ các tham số mô hình và tải các tham số lên đám mây Android, do đó cùng với các chủ sở hữu dữ liệu khác đào tạo mô hình tập trung. Một sơ đồ tổng hợp an toàn để bảo vệ quyền riêng tư của các cập nhật người dùng tổng hợp trong khuôn khổ học tập liên kết của họ cũng được giới thiệu [9]. Tham chiếu [51] sử dụng mã hóa đồng hình bổ sung cho tập hợp tham số mô hình để cung cấp bảo mật đối với máy chủ trung tâm.

Trong [60], một hệ thống học tập liên kết kiểu đa tác vụ được đề xuất để cho phép nhiều trang web hoàn thành các tác vụ riêng biệt, đồng thời chia sẻ kiến thức và bảo vệ tính bảo mật. Ngoài ra, mô hình học tập đa tác vụ được đề xuất của họ có thể giải quyết các vấn đề về chi phí liên lạc cao, sự chậm trễ và khả năng chịu lỗi. Trong [41], các tác giả đã đề xuất xây dựng cấu trúc máy khách-máy chủ an toàn trong đó hệ thống học liên kết phân chia dữ liệu theo người dùng và cho phép các mô hình được xây dựng tại thiết bị khách cộng tác tại trang máy chủ để xây dựng mô hình liên kết toàn cầu. Quá trình xây dựng mô hình đảm bảo không rò rỉ dữ liệu. Tương tự như vậy, trong [36], các tác giả đã đề xuất các phương pháp cải thiện chi phí truyền thông để tạo điều kiện thuận lợi cho việc đào tạo các mô hình tập trung dựa trên dữ liệu được phân phối trên các máy khách di động. Gần đây, một phương pháp nén được gọi là Nén Gradient Sâu [39] được đề xuất để giảm đáng kể băng thông truyền thông trong đào tạo phân tán quy mô lớn.

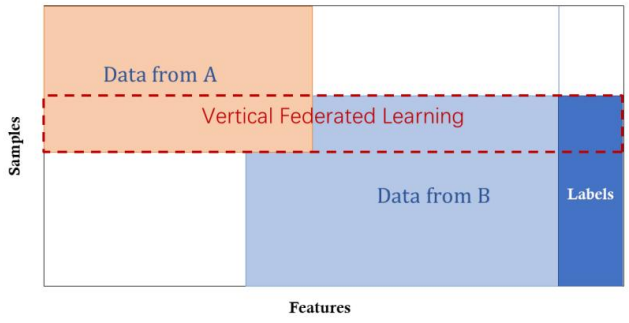
Chúng tôi tóm tắt học tập liên kết theo chiều ngang như sau:

$$Xi = Xj \ , \ Yi = Yj \ , \ Ii \quad Ij \ , \quad Di \ , \ Dj \ , ij \tag{2}$$

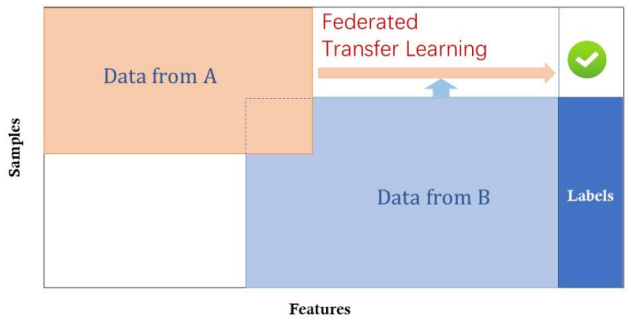
Định nghĩa bảo mật. Một hệ thống học tập liên kết theo chiều ngang thường giả định rằng những người tham gia trung thực và bảo mật đối với một máy chủ trung thực nhưng tò mò [9, 51]. Nghĩa là, chỉ máy chủ mới có thể thỏa hiệp



(a) Học liên kết ngang



(b) Học liên kết dọc



(c) Học chuyển tiếp liên kết

Quả sung. 2. Phân loại học tập liên kết

quyền riêng tư của những người tham gia dữ liệu. Bằng chứng bảo mật đã được cung cấp trong các tác phẩm này. Gần đây, một mô hình bảo mật khác xem xét người dùng độc hại [29] cũng được đề xuất, đặt ra những thách thức bổ sung về quyền riêng tư. Khi kết thúc khóa đào tạo, mô hình phổ quát và toàn bộ tham số mô hình được hiển thị cho tất cả những người tham gia.

2.3.2 Học liên kết dọc. Các thuật toán học máy bảo vệ quyền riêng tư đã được đề xuất cho dữ liệu được phân vùng theo chiều dọc, bao gồm Phân tích thống kê hợp tác [15], khai thác quy tắc kết hợp [65], hồi quy tuyến tính an toàn [22, 32, 55], phân loại [16] và giảm độ dốc [68] .
Gần đây, Ref [27, 49] đã đề xuất một sơ đồ học liên kết dọc để huấn luyện mô hình hồi quy logistic bảo vệ quyền riêng tư. Các tác giả đã nghiên cứu ảnh hưởng của độ phân giải thực thể đối với hiệu quả học tập và áp dụng xấp xỉ Taylor cho các hàm mất mát và độ dốc để mã hóa đồng hình có thể được áp dụng cho các tính toán bảo vệ quyền riêng tư.

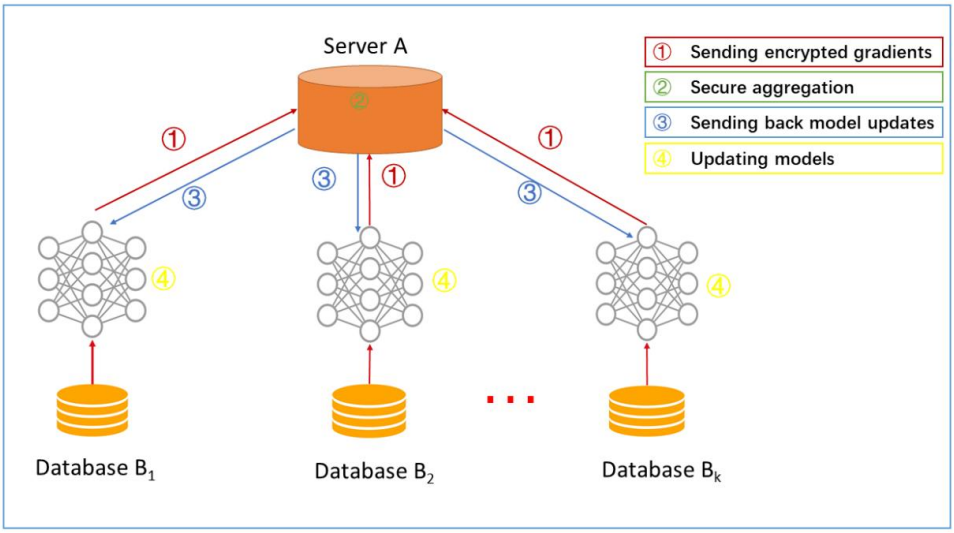
Học liên kết dọc hoặc học liên kết dựa trên tính năng (Hình 2b) được áp dụng cho các trường hợp hai tập dữ liệu chia sẻ cùng một không gian ID mẫu nhưng khác nhau về không gian đặc trưng. Ví dụ: hãy xem xét hai công ty khác nhau trong cùng một thành phố, một công ty là ngân hàng và công ty kia là công ty thương mại điện tử. Nhóm người dùng của họ có khả năng bao gồm hầu hết cư dân trong khu vực, do đó giao điểm của không gian người dùng của họ là lớn. Tuy nhiên, vì ngân hàng ghi lại hành vi thu chi và xếp hạng tín dụng của người dùng và thương mại điện tử lưu giữ lịch sử duyệt và mua hàng của người dùng, nên không gian tính năng của họ rất khác nhau. Giả sử rằng chúng tôi muốn cả hai bên có một mô hình dự đoán mua sản phẩm dựa trên thông tin sản phẩm và người dùng.

Học tập được liên kết theo chiều dọc là quá trình tổng hợp các tính năng khác nhau này và tính toán tổn thất đào tạo và độ dốc theo cách bảo vệ quyền riêng tư để xây dựng một mô hình với dữ liệu từ cả hai bên một cách cộng tác. Theo cơ chế liên bang như vậy, danh tính và địa vị của mỗi bên tham gia là như nhau và hệ thống liên bang giúp mọi người thiết lập chiến lược "của cải chung", đó là lý do tại sao hệ thống này được gọi là "học tập liên kết". Do đó, trong một hệ thống như vậy, chúng tôi có:

$$Xi\ Xj\ ,\ Yi\ Yj\ ,\ Ii = Ij \quad Di\ ,\ Dj\ ,ij \tag{3}$$

Định nghĩa bảo mật. Một hệ thống học tập liên kết theo chiều dọc thường giả định những người tham gia trung thực nhưng tò mò . Ví dụ, trong trường hợp hai bên, hai bên không thông đồng với nhau và nhiều nhất một trong số họ bị đối phương xâm phạm. Định nghĩa bảo mật là kẻ thù chỉ có thể tìm hiểu dữ liệu từ máy khách mà nó bị hỏng chứ không phải dữ liệu từ máy khách khác ngoài những gì được tiết lộ bởi đầu vào và đầu ra. Để tạo điều kiện thuận lợi cho việc tính toán an toàn giữa hai bên, đôi khi một bên thứ ba bán trung thực (STP) được giới thiệu, trong trường hợp đó, người ta cho rằng STP không thông đồng với bên nào. SMC cung cấp bằng chứng về quyền riêng tư chính thức cho các giao thức này [25]. Khi kết thúc quá trình học, mỗi bên chỉ nắm giữ các tham số mô hình liên quan đến các tính năng của riêng mình, do đó tại thời điểm suy luận, hai bên cũng cần cộng tác để tạo ra đầu ra.

2.3.3 Học chuyển giao liên kết (FTL). Học chuyển giao liên kết áp dụng cho các tình huống mà hai tập dữ liệu khác nhau không chỉ về mẫu mà còn về không gian đặc trưng. Hãy xem xét hai tổ chức, một là ngân hàng ở Trung Quốc và tổ chức kia là một công ty thương mại điện tử ở Hoa Kỳ.
Do hạn chế về địa lý, các nhóm người dùng của hai tổ chức có một điểm giao nhau nhỏ.
Mặt khác, do các doanh nghiệp khác nhau, chỉ một phần nhỏ không gian tính năng của cả hai bên trùng nhau. Trong trường hợp này, các kỹ thuật học chuyển giao [50] có thể được áp dụng để cung cấp giải pháp cho toàn bộ mẫu và không gian đặc trưng trong một liên kết (Hình 2c). Đặc biệt, một biểu diễn chung giữa hai không gian đặc trưng được học bằng cách sử dụng các tập mẫu chung giới hạn và sau đó được áp dụng để thu được dự đoán cho các mẫu chỉ có các đặc trưng một phía. FTL là một phần mở rộng quan trọng đối với các hệ thống học tập liên kết hiện có vì nó xử lý các vấn đề vượt quá giới hạn cho phép.



Quả sung. 3. Kiến trúc cho hệ thống học liên kết ngang

phạm vi của các thuật toán học liên kết hiện có:

$$\text{Xi Xj , Yi Yj , Ii} \quad \text{Ij} \quad \text{Di , Dj ,ij} \tag{4}$$

Định nghĩa bảo mật. Một hệ thống học tập chuyển giao liên kết thường bao gồm hai bên. Như sẽ được trình bày trong phần tiếp theo, các giao thức của nó tương tự như các giao thức trong học liên kết dọc, trong trường hợp đó, định nghĩa bảo mật cho học liên kết dọc có thể được mở rộng ở đây.

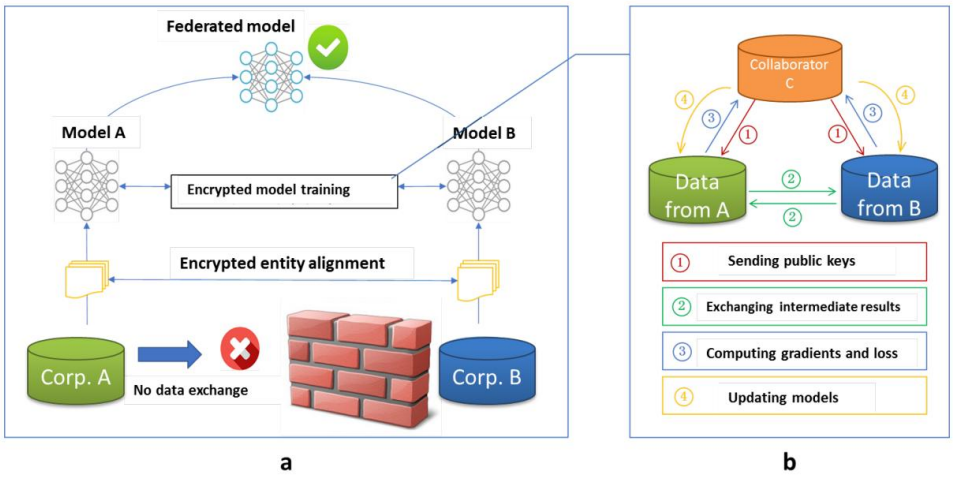
2.4 Kiến trúc cho một hệ thống học tập liên kết Trong phần

này, chúng tôi minh họa các ví dụ về kiến trúc chung cho một hệ thống học tập liên kết. Lưu ý rằng kiến trúc của các hệ thống học tập liên kết ngang và dọc khá khác nhau theo thiết kế và chúng tôi sẽ giới thiệu chúng một cách riêng biệt.

2.4.1 Học liên kết ngang. Một kiến trúc điển hình cho hệ thống học tập liên kết theo chiều ngang được hiển thị trong Hình 3. Trong hệ thống này, k người tham gia có cùng cấu trúc dữ liệu cùng nhau học một mô hình máy học với sự trợ giúp của một tham số hoặc máy chủ đám mây. Một giả định điển hình là những người tham gia trung thực trong khi máy chủ trung thực nhưng tò mò, do đó không được phép rò rỉ thông tin từ bất kỳ người tham gia nào vào máy chủ [51]. Quá trình đào tạo của một hệ thống như vậy thường bao gồm bốn bước sau:

- Bước 1: người tham gia tính toán cục bộ độ dốc đào tạo, che giấu lựa chọn độ dốc bằng kỹ thuật mã hóa [51], quyền riêng tư khác biệt [58] hoặc chia sẻ bí mật [9] và gửi kết quả được che giấu đến máy chủ;
- Bước 2: Server thực hiện tổng hợp an toàn mà không cần tìm hiểu thông tin về bất kỳ người tham gia nào quần dài;
- Bước 3: Máy chủ gửi lại kết quả tổng hợp cho người tham gia; • Bước 4:

Người tham gia cập nhật mô hình tương ứng của họ với các gradient được giải mã.



Quả sung. 4. Kiến trúc cho hệ thống học liên kết dọc

Lặp lại các bước trên tiếp tục cho đến khi hàm mất mát hội tụ, do đó hoàn thành toàn bộ quá trình đào tạo. Kiến trúc này độc lập với các thuật toán học máy cụ thể (hồi quy logistic, DNN, v.v.) và tất cả những người tham gia sẽ chia sẻ các tham số mô hình cuối cùng.

Phân tích bảo mật. Kiến trúc trên được chứng minh là bảo vệ chống rò rỉ dữ liệu đối với máy chủ bán trung thực, nếu việc tổng hợp độ dốc được thực hiện với SMC [9] hoặc Mã hóa đồng hình [51]. Nhưng nó có thể bị tấn công trong một mô hình bảo mật khác bởi một người tham gia độc hại đào tạo Mạng đối thủ chung (GAN) trong quá trình học tập hợp tác [29].

2.4.2 Học liên kết dọc. Giả sử rằng các công ty A và B muốn cùng đào tạo một mô hình học máy và mỗi hệ thống kinh doanh của họ đều có dữ liệu riêng. Ngoài ra, công ty B cũng có dữ liệu nhãn mà mô hình cần dự đoán. Vì lý do riêng tư và bảo mật dữ liệu, A và B không thể trao đổi dữ liệu trực tiếp. Để đảm bảo tính bảo mật của dữ liệu trong quá trình đào tạo, cộng tác viên bên thứ ba C đã tham gia. Ở đây chúng ta giả sử cộng tác viên C trung thực và không thông đồng với A hoặc B, nhưng bên A và B là trung thực nhưng tò mò với nhau. Bên thứ ba đáng tin cậy C một giả định hợp lý vì bên C có thể được chơi bởi các cơ quan có thẩm quyền như chính phủ hoặc được thay thế bằng nút điện toán an toàn như Tiện ích mở rộng bảo vệ phần mềm Intel (SGX) [7]. Hệ thống học tập liên kết bao gồm hai phần, như trong Hình 4.

Phần 1. Căn chỉnh thực thể mã hóa. Do nhóm người dùng của hai công ty không giống nhau nên hệ thống sử dụng các kỹ thuật căn chỉnh ID người dùng dựa trên mã hóa như [38, 56] để xác nhận người dùng chung của cả hai bên mà không để A và B tiết lộ dữ liệu tương ứng của họ. Trong quá trình căn chỉnh thực thể , hệ thống không hiển thị những người dùng không trùng lặp với nhau.

Phần 2. Đào tạo mô hình mã hóa. Sau khi xác định các thực thể chung, chúng ta có thể sử dụng dữ liệu của các thực thể chung này để huấn luyện mô hình máy học. Quá trình đào tạo có thể được chia thành bốn bước sau (như trong Hình 4):

- Bước 1: cộng tác viên C tạo cặp mã hóa, gửi public key cho A và B; • Bước 2: A và B mã hóa và trao đổi kết quả trung gian để tính toán độ dốc và tổn thất tions;

- Bước 3: A và B tính toán độ dốc được mã hóa và thêm mặt nạ bổ sung tương ứng, và B cũng tính toán tổn thất được mã hóa; A và B gửi giá trị mã hóa cho C;
- Bước 4: C giải mã và gửi lại gradient và loss đã giải mã cho A và B; A và B vạch mặt các gradient, cập nhật các tham số mô hình cho phù hợp.

Ở đây chúng tôi minh họa quá trình đào tạo bằng cách sử dụng hồi quy tuyến tính và mã hóa đồng cấu làm ví dụ. Để đào tạo một mô hình hồi quy tuyến tính với các phương pháp giảm dần độ dốc, chúng ta cần tính toán an toàn về độ mất mát và độ dốc của nó. Giả sử tỷ lệ học tập η, tham số chuẩn hóa λ, tập dữ liệu $D_A = \{x_i^A, y_i\}_i$ và các tham số mô hình θ_A, θ_B tương ứng với không gian đặc trưng của x_i^A, x_i^B DB , tương ứng, mục tiêu đào tạo là:

$$\min_{\theta_A, \theta_B} \|\theta R i u_i^A + \theta B x_i^B - y_i\|_2 + \frac{\lambda}{2}(\|\theta A\|_2 + \|\theta B\|_2) \quad (5)$$

một cho bạn $= \theta A x_{i,u}^A = \theta B x_{i,}^B$ tổn thất được mã hóa là:

$$[[L]] = [[((bạn^A + u_i^B) - y_i))2 + \frac{\lambda}{2}(\|\theta A\|_2 + \|\theta B\|_2)]] \quad (6)$$

trong đó mã hóa đồng cấu phụ gia được ký hiệu là [[ ]]. Đặt $[[LA]] = [[[LB]] = [[y_i) ((bạn^A)^2) + \frac{\lambda}{2}\theta_A^2]]$, $((bạn^B)^2) + \frac{\lambda}{2}\theta_B^2]]$ và $[[LAB]] = 2 ([[u^A]](bạn^B) - y_i))$, sau đó

$$[[L]] = [[LA]] + [[LB]] + [[LAB]] \quad (7)$$

Tương tự, đặt $[[di]] = [[u^A]] + [[u^B - y_i]]$, thì độ dốc là:

$$[[\frac{\partial L}{\partial \theta A}]] = [[di]]x^A + [[\lambda \theta A]] \quad (số 8)$$

$$[[\frac{\partial L}{\partial \theta B}]] = [[di]]x^B + [[\lambda \theta B]] \quad (9)$$

Bảng 1. Các bước đào tạo để học liên kết dọc: Hồi quy tuyến tính

	bên A	bên B	bên C tạo
bước 1	khởi tạo θA	khởi tạo θB	cặp khóa mã hóa , gửi khóa công khai cho A và B;
bước 2	tính $[[u^A]]$,[[LA]] và gửi cho B;	tính toán $[[u^B]]$,$[[d^B]]$,[[L]], gửi $[[d^B]]$ đến A, gửi [[L]] đến C;	
bước 3	khởi tạo RA, tính toán $[[\frac{\partial L}{\partial \theta A}]]$+[[RA]] và gửi đến C;	khởi tạo RB, tính toán $[[\frac{\partial L}{\partial \theta B}]]$+[[RB]] và gửi đến C;	C giải mã L, gửi $L + RA$ đến A, $\theta B \frac{\partial L}{\partial} + RB$ đến B;
bước 4	cập nhật θA θA	cập nhật θB θB	
thu được gì	là		

Bảng 2. Các bước đánh giá để học liên kết dọc: Hồi quy tuyến tính

	bên A	bên B	người điều tra
bước 0			C gửi ID người dùng i cho A và B;
bước 1	tính toán $\text{bạn}_{\text{MỘT}}$ và gửi đến C	tính toán bạn_{b} và gửi đến C;	nhận được kết quả $\text{bạn}_{\text{MỘT}}$ B + $u_{\text{tôi}}$;

Xem Bảng 1 và 2 để biết các bước chi tiết. Trong quá trình căn chỉnh thực thể và đào tạo mô hình, dữ liệu của A và B được lưu giữ cục bộ và tương tác dữ liệu trong quá trình đào tạo không dẫn đến rò rỉ quyền riêng tư dữ liệu. Lưu ý khả năng rò rỉ thông tin đến C có thể hoặc không thể được coi là vi phạm quyền riêng tư. Để tiếp tục ngăn C tìm hiểu thông tin từ A hoặc B trong trường hợp này, A và B có thể ẩn thêm độ dốc của chúng khỏi C bằng cách thêm các mặt nạ ngẫu nhiên được mã hóa. Do đó, hai bên đạt được một mô hình đào tạo chung một cách hợp tác với sự trợ giúp của học tập liên kết. Bởi vì trong quá trình đào tạo, tổn thất và độ dốc mà mỗi bên nhận được hoàn toàn giống với tổn thất và độ dốc mà họ sẽ nhận được nếu cùng nhau xây dựng một mô hình với dữ liệu được thu thập tại một nơi mà không có ràng buộc về quyền riêng tư, tức là mô hình này không mất dữ liệu. Hiệu quả của mô hình phụ thuộc vào chi phí truyền thông và chi phí tính toán của dữ liệu được mã hóa. Trong mỗi lần lặp, thông tin được gửi giữa tỷ lệ A và B với số lượng mẫu chồng chéo. Do đó, hiệu quả của thuật toán này có thể được cải thiện hơn nữa bằng cách áp dụng các kỹ thuật tính toán song song phân tán.

Phân tích bảo mật. Giao thức đào tạo được hiển thị trong Bảng 1 không tiết lộ bất kỳ thông tin nào cho C, bởi vì tất cả các lần học của C đều là các gradient được che dấu và tính ngẫu nhiên cũng như bí mật của ma trận được che giấu được đảm bảo [16]. Trong giao thức trên, bên A học gradient của nó ở mỗi bước, nhưng điều này là không đủ để A học bất kỳ thông tin nào từ B theo phương trình 8, vì tính bảo mật của giao thức tích vô hướng được thiết lập tốt dựa trên việc không thể giải n phương trình trong hơn n ẩn số [16, 65]. Ở đây, chúng tôi giả sử số lượng mẫu NA lớn hơn nhiều so với nA, trong đó nA là số lượng tính năng. Tương tự, bên B không thể tìm hiểu bất kỳ thông tin nào từ A. Do đó, tính bảo mật của giao thức đã được chứng minh. Lưu ý rằng chúng tôi đã giả định rằng cả hai bên đều trung thực. Ví dụ: nếu một bên có ác ý và lừa hệ thống bằng cách giả mạo thông tin đầu vào của mình, bên A chỉ gửi một đầu vào khác 0 với duy nhất một tính năng khác 0, thì $\text{bên đó có thể cho biết giá trị của u cho tính năng đó}_{b}$ của mẫu đó. Mặc dù vậy, nó vẫn không thể cho biết x hoặc 0B và độ lệch sẽ làm sai lệch kết quả cho lần lặp tiếp theo, báo động cho bên kia biết rằng họ sẽ chấm dứt quá trình học. Khi kết thúc quá trình đào tạo, mỗi bên (A hoặc B) vẫn không biết cấu trúc dữ liệu của bên kia và nó chỉ nhận được các tham số mô hình được liên kết với các tính năng của chính nó. Tại thời điểm suy luận, hai bên cần cộng tác tính toán kết quả dự đoán, với các bước như trong Bảng 2 mà vẫn không dẫn đến rò rỉ thông tin.

2.4.3 Học chuyển giao liên kết. Giả sử trong ví dụ học tập liên kết theo chiều dọc ở trên, bên A và B chỉ có một tập hợp mẫu chồng chéo rất nhỏ và chúng tôi quan tâm đến việc tìm hiểu các nhãn cho tất cả tập dữ liệu trong bên A. Kiến trúc được mô tả trong phần trên cho đến nay chỉ hoạt động cho tập dữ liệu chồng chéo. Để mở rộng phạm vi phủ sóng của nó ra toàn bộ không gian mẫu, chúng tôi giới thiệu phương pháp học chuyển giao. Điều này không làm thay đổi kiến trúc tổng thể được hiển thị trong Hình 4 nhưng các chi tiết của kết quả trung gian được trao đổi giữa bên A và bên B. Cụ thể, học chuyển giao thường liên quan đến việc học một biểu diễn chung giữa các tính năng của bên A và B và giảm thiểu các lỗi trong việc dự đoán nhãn cho bên miền đích bằng cách tận dụng các nhãn trong bên miền nguồn (B trong trường hợp này). Do đó, các tính toán gradie

bên A và bên B khác với kịch bản học liên kết theo chiều dọc. Tại thời điểm suy luận, nó vẫn yêu cầu cả hai bên tính toán kết quả dự đoán.

2.4.4 Cơ chế ưu đãi. Để thương mại hóa hoàn toàn học tập liên kết giữa các tổ chức khác nhau, cần phải phát triển một nền tảng công bằng và các cơ chế khuyến khích [20]. Sau khi mô hình được xây dựng, hiệu suất của mô hình sẽ được thể hiện trong các ứng dụng thực tế và hiệu suất này có thể được ghi lại trong một cơ chế ghi dữ liệu vĩnh viễn (chẳng hạn như Blockchain). Các tổ chức cung cấp nhiều dữ liệu hơn sẽ hoạt động tốt hơn và hiệu quả của mô hình phụ thuộc vào sự đóng góp của nhà cung cấp dữ liệu vào hệ thống. Hiệu quả của các mô hình này được phân phối cho các bên dựa trên cơ chế liên kết và tiếp tục thúc đẩy nhiều tổ chức tham gia liên kết dữ liệu hơn.

Việc triển khai kiến trúc trên không chỉ xem xét việc bảo vệ quyền riêng tư và hiệu quả của mô hình cộng tác giữa nhiều tổ chức, mà còn xem xét cách thưởng cho các tổ chức đóng góp nhiều dữ liệu hơn và cách thực hiện các biện pháp khuyến khích bằng cơ chế đồng thuận. Do đó, học tập liên kết là một cơ chế học tập "vòng kín".

3 CÔNG TRÌ NH LIÊ N QUAN

Học liên kết cho phép nhiều bên cùng nhau xây dựng một mô hình máy học trong khi vẫn giữ dữ liệu đào tạo riêng tư của họ ở chế độ riêng tư. Là một công nghệ mới, học tập liên kết có một số chủ đề độc đáo, một số chủ đề bắt nguồn từ các lĩnh vực hiện có. Dưới đây chúng tôi giải thích mối quan hệ giữa học liên kết và các khái niệm liên quan khác từ nhiều góc độ.

3.1 Học máy bảo vệ quyền riêng tư Học liên kết có

thể được coi là học máy cộng tác phi tập trung bảo vệ quyền riêng tư , do đó, nó có liên quan chặt chẽ với học máy bảo vệ quyền riêng tư của nhiều bên. Nhiều nỗ lực nghiên cứu đã được dành cho lĩnh vực này trong quá khứ. Ví dụ, Ref [17, 67] đã đề xuất các thuật toán cho cây quyết định đa bên an toàn cho dữ liệu được phân vùng theo chiều dọc. Vaidya và Clifton đã đề xuất các quy tắc khai thác liên kết an toàn [65], phương tiện k an toàn [66], bộ phân loại Naive Bayes [64] cho dữ liệu được phân vùng theo chiều dọc. Tham khảo [31] đã đề xuất một thuật toán cho các quy tắc kết hợp trên dữ liệu được phân vùng theo chiều ngang. Thuật toán Máy vectơ hỗ trợ an toàn được phát triển cho dữ liệu được phân vùng theo chiều dọc [73] và dữ liệu được phân vùng theo chiều ngang [74]. Tham khảo [16] đề xuất các giao thức an toàn cho phân loại và hồi quy tuyến tính đa bên . Tham khảo [68] đã đề xuất các phương pháp giảm độ dốc đa bên an toàn. Tất cả các công trình trên đều sử dụng tính toán đa bên an toàn (SMC) [25, 72] để đảm bảo quyền riêng tư.

Nikolaenko và cộng sự[48] đã triển khai một giao thức bảo vệ quyền riêng tư cho hồi quy tuyến tính trên dữ liệu được phân vùng theo chiều ngang bằng cách sử dụng mã hóa đồng cấu và các mạch bị cắt xén của Yao và Ref [22, 24] đã đề xuất phương pháp hồi quy tuyến tính cho dữ liệu được phân vùng theo chiều dọc. Các hệ thống này đã giải quyết vấn đề hồi quy tuyến tính một cách trực tiếp. Tham khảo [47] đã tiếp cận vấn đề với Stochastic Gradient Descent (SGD) và họ cũng đề xuất các giao thức bảo vệ quyền riêng tư cho hồi quy logistic và mạng thần kinh. Gần đây, một công việc tiếp theo với mô hình ba máy chủ được đề xuất [44]. Aono và cộng sự.[4] đề xuất một giao thức hồi quy logistic an toàn sử dụng mã hóa đồng hình. Shokri và Shmatikov [58] đã đề xuất đào tạo mạng lưới thần kinh cho dữ liệu được phân vùng theo chiều ngang với việc trao đổi các tham số được cập nhật. Tham khảo [51] đã sử dụng mã hóa đồng hình bổ sung để phục vụ trước tính riêng tư của độ dốc và tăng cường tính bảo mật của hệ thống. Với những tiến bộ gần đây trong học sâu, suy luận mạng thần kinh bảo vệ quyền riêng tư cũng đang nhận được rất nhiều mối quan tâm nghiên cứu [10, 11, 14, 28, 40, 52, 54].

3.2 Học liên kết so với Học máy phân tán Thoạt nhìn học liên kết ngang có phần giống với Học máy phân tán.

Học máy phân tán bao gồm nhiều khía cạnh, bao gồm lưu trữ phân tán dữ liệu đào tạo, vận hành phân tán các tác vụ tính toán, phân phối kết quả mô hình phân tán, v.v. Máy chủ tham số [30] là một yếu tố điển hình trong học máy phân tán. Là một công cụ để tăng tốc quá trình đào tạo, máy chủ tham số lưu trữ dữ liệu trên các nút làm việc phân tán, phân bổ dữ liệu và đặt tài nguyên thông qua một nút lập lịch trình trung tâm, để đào tạo mô hình hiệu quả hơn. Đối với học liên kết theo chiều ngang, nút làm việc đại diện cho chủ sở hữu dữ liệu. Nó có toàn quyền tự chủ đối với dữ liệu cục bộ và có thể quyết định thời điểm và cách thức tham gia học liên kết. Trong máy chủ tham số, nút trung tâm luôn nắm quyền kiểm soát, do đó, việc học liên kết phải đối mặt với một môi trường học phức tạp hơn. Thứ hai, học tập liên kết nhấn mạnh đến việc bảo vệ quyền riêng tư dữ liệu của chủ sở hữu dữ liệu trong quá trình đào tạo mô hình. Các biện pháp hiệu quả để bảo vệ quyền riêng tư của dữ liệu có thể đối phó tốt hơn với môi trường pháp lý về quyền riêng tư và bảo mật dữ liệu ngày càng nghiêm ngặt trong tương lai.

Giống như trong cài đặt học máy phân tán, học liên kết cũng sẽ cần xử lý dữ liệu Non-IID. Trong [77] đã chỉ ra rằng với dữ liệu cục bộ không phải iid, hiệu suất có thể giảm đáng kể đối với việc học liên kết. Đáp lại, các tác giả đã cung cấp một phương pháp mới để giải quyết vấn đề tương tự như học chuyển đổi.

3.3 Học liên kết so với điện toán biên Học tập liên kết có thể được coi là một hệ điều hành cho điện toán biên, vì nó cung cấp giao thức học để phối hợp và bảo mật.

Trong [69], các tác giả đã xem xét lớp chung của các mô hình học máy được đào tạo bằng cách sử dụng các phương pháp tiếp cận dựa trên độ dốc. Họ phân tích giới hạn hội tụ của giảm dần độ dốc phân tán từ quan điểm lý thuyết, dựa trên đó họ đề xuất thuật toán điều khiển xác định sự đánh đổi tốt nhất giữa cập nhật cục bộ và tổng hợp tham số toàn cầu để giảm thiểu chức năng mất mát theo ngân sách tài nguyên nhất định.

3.4 Hệ thống học tập liên kết vs Hệ thống cơ sở dữ liệu liên kết

Hệ thống cơ sở dữ liệu liên kết [57] là những hệ thống tích hợp nhiều đơn vị cơ sở dữ liệu và quản lý toàn bộ hệ thống tích hợp. Khái niệm cơ sở dữ liệu liên kết được đề xuất để đạt được khả năng tương tác với nhiều cơ sở dữ liệu độc lập. Một hệ thống cơ sở dữ liệu được liên kết thường sử dụng lưu trữ phân tán cho các đơn vị cơ sở dữ liệu và trong thực tế, dữ liệu trong mỗi đơn vị cơ sở dữ liệu là không đồng nhất. Do đó, nó có nhiều điểm tương đồng với học liên kết về kiểu và cách lưu trữ dữ liệu. Tuy nhiên, hệ thống cơ sở dữ liệu được liên kết không liên quan đến bất kỳ cơ chế bảo vệ quyền riêng tư nào trong quá trình tương tác với nhau và tất cả các đơn vị cơ sở dữ liệu hoàn toàn hiển thị đối với hệ thống quản lý. Ngoài ra, trọng tâm của hệ thống cơ sở dữ liệu liên kết là các hoạt động cơ bản của dữ liệu bao gồm chèn, xóa, tìm kiếm và hợp nhất, v.v., trong khi mục đích của việc học liên kết là thiết lập một mô hình chung cho mỗi chủ sở hữu dữ liệu dưới tiền đề của bảo vệ quyền riêng tư của dữ liệu, để các giá trị và luật khác nhau mà dữ liệu chứa phục vụ chúng ta tốt hơn.

4 ỨNG DỤNG

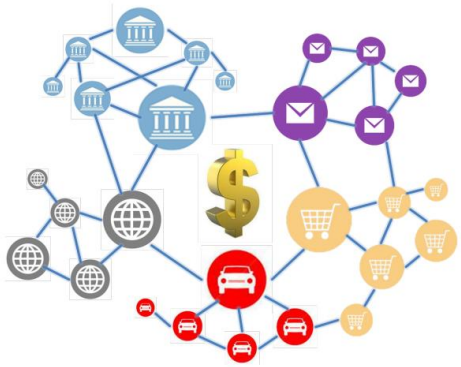
Là một cơ chế lập mô hình đổi mới có thể đào tạo một mô hình thống nhất trên dữ liệu từ nhiều bên mà không ảnh hưởng đến quyền riêng tư và bảo mật của những dữ liệu đó, học tập liên kết có một ứng dụng đầy hứa hẹn trong bán hàng, tài chính và nhiều ngành khác, trong đó dữ liệu không thể được tổng hợp trực tiếp để đào tạo các mô hình học máy do các yếu tố như quyền sở hữu trí tuệ, bảo vệ quyền riêng tư và bảo mật dữ liệu.

Lấy bán lẻ thông minh làm ví dụ. Mục đích của nó là sử dụng các kỹ thuật máy học để cung cấp cho khách hàng các dịch vụ được cá nhân hóa, chủ yếu bao gồm các dịch vụ bán hàng và giới thiệu sản phẩm. Các tính năng dữ liệu liên quan đến kinh doanh bán lẻ thông minh chủ yếu bao gồm sức mua của người dùng, sở thích cá nhân của người dùng và đặc điểm sản phẩm. Trong các ứng dụng thực tế, ba tính năng dữ liệu này có thể nằm rải rác giữa ba phòng ban hoặc doanh nghiệp khác nhau. Ví dụ: sức mua của người dùng có thể được suy ra từ khoản tiết kiệm ngân hàng của cô ấy và sở thích cá nhân của cô ấy có thể được phân tích từ mạng xã hội của cô ấy, trong khi các đặc điểm của sản phẩm được ghi lại bởi một cửa hàng điện tử. Trong kịch bản này, chúng tôi đang phải đối mặt với hai vấn đề. Đầu tiên, để bảo vệ quyền riêng tư và bảo mật dữ liệu, các rào cản dữ liệu giữa các ngân hàng, trang mạng xã hội và trang mua sắm điện tử rất khó bị phá vỡ. Do đó, dữ liệu không thể được tổng hợp trực tiếp để đào tạo một mô hình. Thứ hai, dữ liệu được lưu trữ trong ba bên thường không đồng nhất và các mô hình học máy truyền thống không thể hoạt động trực tiếp trên dữ liệu không đồng nhất. Hiện tại, những vấn đề này vẫn chưa được giải quyết hiệu quả bằng các phương pháp học máy truyền thống, điều này cản trở việc phổ biến và ứng dụng trí tuệ nhân tạo trong nhiều lĩnh vực hơn.

Học liên kết và học chuyển là chìa khóa để giải quyết những vấn đề này. Đầu tiên, bằng cách khai thác các đặc điểm của học tập liên kết, chúng tôi có thể xây dựng mô hình học máy cho ba bên mà không cần xuất dữ liệu doanh nghiệp, mô hình này không chỉ bảo vệ hoàn toàn quyền riêng tư và bảo mật dữ liệu mà còn cung cấp cho khách hàng các dịch vụ được cá nhân hóa và nhắm mục tiêu, từ đó đạt được mục tiêu nhưng lơ i ich chung. Trong khi đó, chúng ta có thể tận dụng học chuyển đổi để giải quyết vấn đề về tính không đồng nhất của dữ liệu và vượt qua những hạn chế của các kỹ thuật trí tuệ nhân tạo truyền thống. Do đó, học tập liên kết cung cấp hỗ trợ kỹ thuật tốt để chúng tôi xây dựng một hệ sinh thái liên doanh nghiệp, dữ liệu chéo và miền chéo cho dữ liệu lớn và trí tuệ nhân tạo.

Người ta có thể sử dụng khung học liên kết để truy vấn cơ sở dữ liệu nhiều bên mà không làm lộ dữ liệu. Ví dụ: giả sử trong một ứng dụng tài chính, chúng tôi quan tâm đến việc phát hiện khoản vay của nhiều bên, vốn là một yếu tố rủi ro chính trong ngành ngân hàng. Điều này xảy ra khi một số người dùng nhất định vay một cách ác ý từ một ngân hàng để trả khoản vay tại một ngân hàng khác. Vay mượn nhiều bên là mối đe dọa đối với sự ổn định tài chính vì một số lượng lớn các hành động bất hợp pháp như vậy có thể khiến toàn bộ hệ thống tài chính sụp đổ. Để tìm những người dùng như vậy mà không để lộ danh sách người dùng giữa các ngân hàng A và B với nhau , chúng ta có thể khai thác khung học liên kết. Đặc biệt, chúng ta có thể sử dụng cơ chế mã hóa của học liên kết và mã hóa danh sách người dùng ở mỗi bên, sau đó lấy giao điểm của danh sách được mã hóa trong liên kết. Việc giải mã kết quả cuối cùng đưa ra danh sách những người vay nhiều bên, mà không để lộ những người dùng "tốt" khác cho bên kia. Như chúng ta sẽ thấy bên dưới, thao tác này tương ứng với khung học liên kết theo chiều c

Chăm sóc sức khỏe thông minh là một lĩnh vực khác mà chúng tôi mong đợi sẽ được hưởng lợi rất nhiều từ sự gia tăng của các kỹ thuật học tập liên kết. Dữ liệu y tế như triệu chứng bệnh, trình tự gen, báo cáo y tế rất nhạy cảm và riêng tư, tuy nhiên dữ liệu y tế rất khó thu thập và chúng tồn tại ở các trung tâm y tế và bệnh viện biệt lập. Việc thiếu nguồn dữ liệu và thiếu nhãn đã dẫn đến hiệu suất không đạt yêu cầu của các mô hình học máy, trở thành nút cổ chai của chăm sóc sức khỏe thông minh hiện nay. Chúng tôi dự tính rằng nếu tất cả các tổ chức y tế hợp nhất và chia sẻ dữ liệu của họ để tạo thành một tập dữ liệu y tế lớn, thì hiệu suất của các mô hình máy học được đào tạo trên tập dữ liệu y tế lớn đó sẽ được cải thiện đáng kể. Học tập liên kết kết hợp với học tập chuyển đổi là cách chính để đạt được tầm nhìn này. Học chuyển giao có thể được áp dụng để lấp đầy các nhãn còn thiếu, do đó mở rộng quy mô của dữ liệu có sẵn và cải thiện hơn nữa hiệu suất của một mô hình được đào tạo. Do đó, học chuyển giao liên kết sẽ đóng một vai trò then chốt trong sự phát triển của chăm sóc sức khỏe thông minh và nó có thể đưa việc chăm sóc sức khỏe con người lên một tầm cao mới.



Quả sung. 5. Liên minh dữ liệu phân bổ lợi ích trên chuỗi khối

5 LIÊ N MINH HỌC TẬP VÀ DỮ LIỆU LIÊ N KẾT CỦA CÁ C DOANH NGHIỆP

Học tập liên kết không chỉ là một tiêu chuẩn công nghệ mà còn là một mô hình kinh doanh. Khi mọi người nhận ra tác động của dữ liệu lớn, suy nghĩ đầu tiên xuất hiện trong họ là tổng hợp dữ liệu lại với nhau, tính toán các mô hình thông qua bộ xử lý từ xa và sau đó tải xuống kết quả để sử dụng tiếp. Điện toán đám mây ra đời xuất phát từ nhu cầu như vậy. Tuy nhiên, với tầm quan trọng ngày càng tăng của quyền riêng tư dữ liệu và bảo mật dữ liệu cũng như mối quan hệ chặt chẽ hơn giữa lợi nhuận của công ty và dữ liệu của công ty, mô hình điện toán đám mây đã bị thách thức. Tuy nhiên, mô hình kinh doanh của học tập liên kết đã cung cấp một mô hình mới cho các ứng dụng của dữ liệu lớn. Khi dữ liệu bị cô lập của mỗi tổ chức không thể tạo ra một mô hình lý tưởng, cơ chế học tập liên kết giúp các tổ chức và doanh nghiệp có thể chia sẻ một mô hình thống nhất mà không cần trao đổi dữ liệu. Hơn nữa, học tập liên kết có thể tạo ra các quy tắc công bằng để phân bổ lợi nhuận với sự trợ giúp của cơ chế đồng thuận từ các kỹ thuật chuỗi khối. Những người sở hữu dữ liệu, bất kể quy mô dữ liệu họ có, sẽ có động lực tham gia vào liên minh dữ liệu và kiếm lợi nhuận cho riêng họ. Chúng tôi tin rằng việc thiết lập mô hình kinh doanh cho liên minh dữ liệu và cơ chế kỹ thuật cho học tập liên kết nên được thực hiện cùng nhau. Chúng tôi cũng sẽ đưa ra các tiêu chuẩn cho học tập liên kết trong các lĩnh vực khác nhau để đưa vào sử dụng càng sớm càng tốt.

6 KẾT LUẬN VÀ TRIỂN VỌNG

Trong những năm gần đây, việc cô lập dữ liệu và nhấn mạnh vào quyền riêng tư của dữ liệu đang trở thành những thách thức tiếp theo đối với trí tuệ nhân tạo, nhưng học tập liên kết đã mang lại cho chúng ta hy vọng mới. Nó có thể thiết lập một mô hình thống nhất cho nhiều doanh nghiệp trong khi dữ liệu cục bộ được bảo vệ, để các doanh nghiệp có thể cùng nhau giành chiến thắng khi lấy bảo mật dữ liệu làm tiền đề. Bài viết này giới thiệu chung về khái niệm cơ bản, kiến trúc và kỹ thuật của học liên kết và thảo luận về tiềm năng của nó trong các ứng dụng khác nhau. Dự kiến trong tương lai gần, học tập liên kết sẽ phá vỡ rào cản giữa các ngành và thiết lập một cộng đồng nơi dữ liệu và kiến thức có thể được chia sẻ cùng nhau một cách an toàn và lợi ích sẽ được phân bổ công bằng tùy theo đóng góp của mỗi người tham gia. Phần thưởng của trí tuệ nhân tạo cuối cùng sẽ được đưa đến mọi ngóc ngách trong cuộc sống của chúng ta.

NGƯỜI GIỚI THIỆU

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, và Li Zhang. 2016. Học sâu với quyền riêng tư khác biệt. Trong Kỷ yếu của Hội nghị ACM SIGSAC 2016 về Bảo mật Máy tính và Truyền thông (CCS '16). ACM, New York, NY, Hoa Kỳ, 308–318. https://doi.org/10.1145/2976749.2978318

[2] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, và Mauro Conti. 2018. Khảo sát về các lược đồ mã hóa đồng hình: Lý thuyết và triển khai. Máy tính ACM. sống sót 51, Khoản 4, Điều 79 (07/2018), 35 tr. https://doi.org/10.1145/3214303 [3] Rakesh Agrawal và Ramakrishnan Srikant. 2000. Khai thác dữ liệu bảo vệ quyền riêng tư. Trong Kỷ yếu của Hội nghị Quốc tế ACM SIGMOD năm 2000 về Quản lý Dữ liệu (SIGMOD '00). ACM, New York, NY, Hoa Kỳ, 439–450. https://doi.org/10.1145/342009.335438 [4] Yoshinori Aono, Takuya Hayashi, Lê Triệu Phong, và Lệ Hoa Vương. 2016.
Hồi quy logistic có thể mở rộng và an toàn thông qua mã hóa đồng hình. Trong Kỷ yếu của Hội nghị ACM lần thứ sáu về Bảo mật và Quyền riêng tư của Dữ liệu và Ứng dụng (CODASPY '16). ACM, New York, NY, Hoa Kỳ, 142–144. https://doi.org/10.1145/2857705.2857731

[5] Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof, và Kazuma Ohara. 2016. Điện toán ba bên bảo mật bán trung thực thông lượng cao với đa số trung thực. Trong Kỷ yếu của Hội nghị ACM SIGSAC 2016 về Bảo mật Máy tính và Truyền thông (CCS '16). ACM, New York, NY, Hoa Kỳ, 805–817. https://doi.org/10.1145/2976749.2978331

[6] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, và Vitaly Shmatikov. 2018. Làm thế nào để Backdoor Học liên kết. arXiv:cs.CR/1807.00459

[7] Raad Bahmani, Manuel Barbosa, Ferdinand Brasser, Bernardo Portela, Ahmad-Reza Sadeghi, Guillaume Scerri và Bogdan Warinschi. 2017. Tính toán nhiều bên an toàn từ SGX. Trong Mật mã tài chính và Bảo mật dữ liệu - Hội nghị quốc tế lần thứ 21, FC 2017, Sliema, Malta, ngày 3-7 tháng 4 năm 2017, Các bài báo được chọn đã sửa đổi. 477–497. https: //doi.org/10.1007/978-3-319-70972-7_27

[8] Dan Bogdanov, Sven Laur và Jan Willemson. 2008. Sharemind: Khung tính toán bảo vệ quyền riêng tư nhanh chóng . Trong Kỷ yếu của Hội nghị chuyên đề Châu Â u lần thứ 13 về Nghiên cứu Bảo mật Máy tính: Bảo mật Máy tính (ESORICS '08). Springer-Verlag, Berlin, Heidelberg, 192–206. https://doi.org/10.1007/978-3-540-88313-5_13

[9] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal và Karn Seth. 2017. Tập hợp an toàn thực tế cho học máy bảo vệ quyền riêng tư. Trong Kỷ yếu của Hội nghị ACM SIGSAC 2017 về Bảo mật Máy tính và Truyền thông (CCS '17). ACM, New York, NY, Hoa Kỳ, 1175–1191. https://doi.org/10.1145/3133956.3133982

[10] Florian Bourse, Michele Minelli, Matthias Minihold, và Pascal Paillier. 2017. Đánh giá đồng hình nhanh của sâu Mạng thần kinh rời rạc. IACR Cryptology ePrint Archive 2017 (2017), 1114.

[11] Hervé Chabanne, Amaury de Wargny, Jonathan Milgram, Constance Morel, và Emmanuel Prouff. 2017. Phân loại bảo vệ quyền riêng tư trên các mạng lưới thần kinh sâu. IACR Cryptology ePrint Archive 2017 (2017), 35.

[12] Kamalika Chaudhuri và Claire Monteleoni. 2009. Hồi quy logistic bảo vệ quyền riêng tư. Trong Những tiến bộ trong Hệ thống xử lý thông tin thần kinh 21, D. Koller, D. Schuurmans, Y. Bengio và L. Bottou (Biên tập). Curran Associates, Inc., 289–296. http://papers.nips.cc/paper/3486-privacy-preserving-logistic-regression.pdf [13] Fei Chen, Zhenhua Dong,
Zhenguo Li, và Xiuqiang He. 2018. Siêu học liên kết cho các đề xuất. CoRR abs/1802.07876 (2018). arXiv:1802.07876 http://arxiv.org/abs/1802.07876 [14] Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter,
Michael Naehrig và John CryptoNets: Á p dụng Mạng nơ-ron vào Dữ liệu được mã hóa với mức cao thông qua Wernsing. 2016. đặt và Độ chính xác.
Tường trình kỹ thuật. https://www.microsoft.com/en-us/research/publication/ cryptonets-áp dụng-mạng nơ-ron-vào-dữ-liệu-được-mã-hóa-với-thông-lượng-và-độ-chính-xác-cao/ [15] W. Du và M. Atallah. 2001. Phân
tích thống kê hợp tác bảo vệ quyền riêng tư. Trong Kỷ yếu của Hội nghị Ứng dụng Bảo mật Máy tính Thường niên lần thứ 17 (ACSAC '01). IEEE Computer Society, Washington, DC, USA, 102–. http: //dl.acm.org/cite.cfm?id=872016.872181

[16] Wenliang Du, Yunghsiang Sam Han, and Shigang Chen. 2004. Phân tích thống kê đa biến bảo vệ quyền riêng tư: Hồi quy tuyến tính và phân loại. Trong SDDM.

[17] Wenliang Du và Zhijun Zhan. 2002. Xây dựng bộ phân loại cây quyết định trên dữ liệu cá nhân. Trong Kỷ yếu của Hội nghị Quốc tế IEEE về Quyền riêng tư, Bảo mật và Khai thác Dữ liệu - Tập 14 (CRPIT '14). Hiệp hội Máy tính Úc, Inc., Darlinghurst, Úc, Úc, 1–8. http://dl.acm.org/citation.cfm?id=850782.850784

[18] Cynthia Dwork. 2008. Quyền riêng tư khác biệt: Khảo sát kết quả. Trong Kỷ yếu của Hội nghị Quốc tế lần thứ 5 về Lý thuyết và Ứng dụng của các Mô hình Tính toán (TAMC'08). Springer-Verlag, Berlin, Heidelberg, 1–19. http: //dl.acm.org/cite.cfm?id=1791834.1791836

[19] EU. 2016. QUY ĐỊNH (EU) 2016/679 CỦA NGHỊ VIỆN CHÂ U Â U VÀ CỦA HỘI ĐỒNG về bảo vệ thể nhân liên quan đến việc xử lý dữ liệu cá nhân và về việc di chuyển tự do dữ liệu đó, đồng thời bãi bỏ Chỉ thị 95/46/EC (Quy định chung Quy định bảo vệ dữ liệu). Có tại: https://eur-lex. châu Â u. eu/legal-content/EN/TXT (2016).

[20] Boi Faltings, Goran Radanovic, và Ronald Brachman. 2017. Lý thuyết trò chơi cho khoa học dữ liệu: Khai thác thông tin trung thực. Nhà xuất bản Morgan & Claypool.

[21] Jun Furukawa, Yehuda Lindell, Ariel Nof, và Or Weinstein. 2016. Điện toán ba bên an toàn thông lượng cao dành cho đối thủ nguy hiểm và đa số trung thực. Cryptology ePrint Lưu trữ, Báo cáo 2016/944. https://eprint.iacr.

tổ chức/2016/944.

[22] Adrià Gascón, Phillipp Schoppmann, Borja Balle, Mariana Raykova, Jack Doerner, Samee Zahur, và David Evans. 2016. Hồi quy tuyến tính an toàn trên bộ dữ liệu được phân vùng theo chiều dọc. IACR Cryptology ePrint Archive 2016 (2016), 892.

[23] Robin C. Geyer, Tassilo Klein, và Moin Nabi. 2017. Học tập liên kết riêng tư khác nhau: Quan điểm cấp độ khách hàng. CoRR abs/1712.07557 (2017). arXiv:1712.07557 http://arxiv.org/abs/1712.07557

[24] Irene Giacomelli, Somesh Jha, Marc Joye, C. David Page, và Kyonghwan Yoon. 2017. Hồi quy độ dốc bảo vệ quyền riêng tư chỉ với Mã hóa đồng hình tuyến tính. Cryptology ePrint Lưu trữ, Báo cáo 2017/979. https: http://eprint.iacr.org/2017/979.

[25] O. Goldreich, S. Micali, và A. Wigderson. 1987. Cách chơi BẤT KỲ Trò chơi tinh thần nào. Trong Kỷ yếu của Hội nghị chuyên đề ACM thường niên lần thứ 19 về Lý thuyết máy tính (STOC '87). ACM, New York, NY, Hoa Kỳ, 218–229. https://doi.org/10.1145/28395.28420

[26] Rob Hall, Stephen E. Fienberg, và Yuval Nardi. 2011. Bảo mật hồi quy tuyến tính bội dựa trên homomorphic mã hóa. Tạp chí Thống kê Chính thức 27, 4 (2011), 669–691.

[27] Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Richard Nock, Giorgio Patrini, Guillaume Smith và Brian Thorne. 2017. Học liên kết riêng trên dữ liệu được phân vùng theo chiều dọc thông qua độ phân giải thực thể và mã hóa đồng hình bổ sung. CoRR abs/1711.10677 (2017).

[28] Ehsan Hesamifard, Hassan Takabi, và Mehdi Ghasemi. 2017. CryptoDL: Mạng thần kinh sâu trên dữ liệu được mã hóa. CoRR abs/1711.05189 (2017). arXiv:1711.05189 http://arxiv.org/abs/1711.05189

[29] Briland Hitaj, Giuseppe Ateniese, và Fernando Pérez-Cruz. 2017. Mô hình sâu dưới GAN: Rò rỉ thông tin từ Học tập sâu hợp tác. CoRR abs/1702.07464 (2017).

[30] Qirong Ho, James Cipar, Henggang Cui, Jin Kyu Kim, Seunghak Lee, Phillip B. Gibbons, Garth A. Gibson, Gregory R. Ganger và Eric P. Xing. 2013. ML phân tán hiệu quả hơn thông qua máy chủ tham số song song đồng bộ cũ. Trong Kỷ yếu Hội nghị Quốc tế lần thứ 26 về Hệ thống Xử lý Thông tin Thần kinh - Tập 1 (NIPS'13). Curran Associates Inc., Hoa Kỳ, 1223–1231. http://dl.acm.org/cite.cfm?id=2999611.2999748

[31] Murat Kantarcioglu và Chris Clifton. 2004. Khai thác phân tán bảo vệ quyền riêng tư của các quy tắc kết hợp trên dữ liệu được phân vùng theo chiều ngang. IEEE Trans. trên Kiến thức. và Data Eng. 16, 9 (tháng 9 năm 2004), 1026–1037. https://doi.org/10.1109/TKDE. 2004.45

[32] Alan F. Karr, X. Sheldon Lin, Ashish P. Sanil, và Jerome P. Reiter. 2004. Phân tích bảo vệ quyền riêng tư theo chiều dọc Dữ liệu được phân vùng bằng các sản phẩm ma trận an toàn.

[33] Niki Kilbertus, Adria Gascon, Matt Kusner, Michael Veale, Krishna Gummadi, và Adrian Weller. 2018. Công lý mù quáng: Công bằng với các thuộc tính nhạy cảm được mã hóa. Trong Kỷ yếu Hội nghị Quốc tế lần thứ 35 về Học máy (Proceedings of Machine Learning Research), Jennifer Dy và Andreas Krause (Eds.), Vol. 80. PMLR, Stockholmsmässan, Stockholm Thụy Điển, 2630–2639. http://proceedings.mlr.press/v80/kilbertus18a.html

[34] Hyesung Kim, Jihong Park, Mehdi Bennis, và Seong-Lyun Kim. 2018. Học liên kết trên thiết bị thông qua chuỗi khối và Phân tích độ trễ của nó. arXiv:cs.IT/1808.03949 [35] Miran Kim, Yongsoo Song, Shuang Wang, Yuhou Xia, và Xiaoqian Jiang. 2018. Hồi quy logistic an toàn dựa trên mã hóa đồng hình: Thiết kế và đánh giá. JMIR Med Thông báo 6, 2 (17 tháng 4 năm 2018), e19. https://doi.org/10.2196/ medinform.8805

[36] Jakub Konecný, H. Brendan McMahan, Daniel Ramage, và Peter Richtárik. 2016. Tối ưu hóa liên kết: Học máy phân tán cho trí thông minh trên thiết bị. CoRR abs/1610.02527 (2016). arXiv:1610.02527 http://arxiv.org/abs/1610.02527

[37] Jakub Konecný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, và Dave Bacon. 2016. Học tập liên kết: Các chiến lược để cải thiện hiệu quả giao tiếp. CoRR abs/1610.05492 (2016). arXiv:1610.05492 http://arxiv.org/abs/1610.05492

[38] Gang Liang và Sudarshan S Chawathe. 2004. Hoạt động liên cơ sở dữ liệu bảo vệ quyền riêng tư. Trong Hội nghị Quốc tế về Tình báo và An ninh Tin học. Springer, 66–82.

[39] Yujun Lin, Song Han, Huizi Mao, Yu Wang, và William J. Dally. 2017. Nén Gradient sâu: Giảm băng thông truyền thông cho đào tạo phân tán. CoRR abs/1712.01887 (2017). arXiv:1712.01887 http: //arxiv.org/abs/1712.01887 [40] Jian Liu, Mika Juuti, Yao Lu, và N. Asokan. 2017. Dự đoán mạng lưới thần kinh không rõ ràng thông qua chuyển đổi MiniONN. Trong Kỷ yếu của Hội nghị ACM SIGSAC 2017 về Bảo mật Máy tính và Truyền thông (CCS '17). ACM, New York, NY, Hoa Kỳ, 619–631. https://doi.org/10.1145/3133956.3134056

[41] H. Brendan McMahan, Eider Moore, Daniel Ramage, và Blaise Agüera y Arcas. 2016. Học liên kết các mạng sâu bằng cách sử dụng tính trung bình của mô hình. CoRR abs/1602.05629 (2016). arXiv:1602.05629 http://arxiv.org/abs/1602.05629 [42] H. Brendan McMahan, Daniel Ramage, Kunal Talwar, và Li Zhang. 2017. Học ngôn ngữ riêng khác biệt Mô hình mà không làm mất độ chính xác. CoRR abs/1710.06963 (2017).

[43] Luca Melis, Congzheng Song, Emiliano De Cristofaro, và Vitaly Shmatikov. 2018. Suy luận tấn công học tập hợp tác . CoRR abs/1805.04049 (2018). arXiv:1805.04049 http://arxiv.org/abs/1805.04049 [44] Payman Mohassel và Peter Rindal. 2018. ABY3: Khung giao thức hỗn hợp cho máy học. Trong Kỷ yếu của Hội nghị ACM SIGSAC 2018 về Bảo mật Máy tính và Truyền thông (CCS '18). ACM, New York, NY, Hoa Kỳ, 35–52. https://doi.org/10.1145/3243734.3243760 [45] Payman Mohassel, Mike Rosulek, và Ye Zhang. 2015. Tính toán ba bên nhanh chóng và an toàn: Phương pháp tiếp cận mạch bị cắt xén. Trong Kỷ yếu của Hội nghị ACM SIGSAC lần thứ 22 về Bảo mật Máy tính và Truyền thông (CCS '15). ACM, New York, NY, Hoa Kỳ, 591–602. https://doi.org/10.1145/2810103.2813705

[46] Payman Mohassel và Yupeng Zhang. 2017. SecureML: Hệ thống học máy bảo vệ quyền riêng tư có thể mở rộng. Trong Hội nghị chuyên đề về bảo mật và quyền riêng tư của IEEE. Hiệp hội máy tính IEEE, 19–38.

[47] Payman Mohassel và Yupeng Zhang. 2017. SecureML: Hệ thống học máy bảo vệ quyền riêng tư có thể mở rộng. IACR Cryptology ePrint Archive 2017 (2017), 396.

[48] Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh, và Nina Taft. 2013. Hồi quy sườn bảo vệ quyền riêng tư trên hàng trăm triệu bản ghi. Trong Kỷ yếu của Hội nghị chuyên đề IEEE 2013 về Bảo mật và Quyền riêng tư (SP '13). IEEE Computer Society, Washington, DC, USA, 334–348. https://doi.org/10.1109/SP.2013.30 [49] Richard Nock, Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Giorgio Patrini, Guillaume Smith, và Brian Thorne. 2018. Entity Resolution và Federated Learning nhận được một Nghị quyết liên kết. CoRR abs/1803.04035 (2018). arXiv:1803.04035 http://arxiv.org/abs/1803.04035 [50] Sinno Jialin Pan và Qiang Yang. 2010. Khảo sát về học tập chuyển giao. IEEE Trans. trên Kiến thức. và Data Eng. 22, 10 (Tháng 10 năm 2010), 1345–1359. https://doi.org/10.1109/TKDE.2009.191

[51] Lê Triệu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, và Shiho Moriai. 2018. Học sâu bảo vệ quyền riêng tư thông qua mã hóa đồng hình bổ sung. IEEE Trans. Pháp y và Bảo mật Thông tin 13, 5 (2018), 1333–1345.

[52] M. Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M. Songhori, Thomas Schneider, và Farinaz Koushanfar. 2018. Chameleon: Khung tính toán bảo mật lai cho các ứng dụng máy học. CoRR abs/1801.03239 (2018).

[53] R. L. Rivest, L. Adleman, và M. L. Dertouzos. 1978. Về ngân hàng dữ liệu và tính đồng nhất về quyền riêng tư. Nền tảng của Bảo mật Tính toán, Academia Press (1978), 169–179.

[54] Bita Darvish Rouhani, M. Sadegh Riazi, và Farinaz Koushanfar. 2017. DeepSecure: DeepSecure-Provable-Secure có thể mở rộng Học hỏi. CoRR abs/1705.08963 (2017). arXiv:1705.08963 http://arxiv.org/abs/1705.08963

[55] Ashish P. Sanil, Alan F. Karr, Xiaodong Lin, và Jerome P. Reiter. 2004. Mô hình hồi quy bảo toàn quyền riêng tư thông qua tính toán phân tán. Trong Kỷ yếu của Hội nghị quốc tế ACM SIGKDD lần thứ 10 về khám phá tri thức và khai thác dữ liệu (KDD '04). ACM, New York, NY, Hoa Kỳ, 677–682. https://doi.org/10.1145/1014052.1014139 [56] Monica Scannapieco, Ilya Figotin, Elisa Bertino, và Ahmed K. Elmagarmid. 2007. Lược đồ bảo vệ quyền riêng tư và đối sánh dữ liệu. Trong Kỷ yếu của Hội nghị Quốc tế ACM SIGMOD 2007 về Quản lý Dữ liệu (SIGMOD '07). ACM, New York, NY, Hoa Kỳ, 653–664. https://doi.org/10.1145/1247480.1247553

[57] Amit P. Sheth và James A. Larson. 1990. Hệ thống cơ sở dữ liệu liên kết để quản lý cơ sở dữ liệu phân tán, không đồng nhất và tự trị. Máy tính ACM. sống sót 22, 3 (tháng 9 năm 1990), 183–236. https://doi.org/10.1145/96602.96604 [58] Reza Shokri và Vitaly Shmatikov. 2015. Deep Learning bảo vệ quyền riêng tư. Trong Kỷ yếu của Hội nghị ACM SIGSAC lần thứ 22 về Bảo mật Máy tính và Truyền thông (CCS '15). ACM, New York, NY, Hoa Kỳ, 1310–1321. https: //doi.org/10.1145/2810103.2813687 [59] David Silver, Aja Huang, Christopher J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot, Sander Dieleman, Dominik Grewe, John Nham, Nal Kalchbrenner, Ilya Sutskever, Timothy Lillicrap, Madeleine Leach, Koray Kavukcuoglu, Thore Graepel và Demis Hassabis. 2016. Làm chủ trò chơi cờ vây với mạng lưới thần kinh sâu và tìm kiếm trên cây. Thiên nhiên 529 (2016), 484–503. http://www.nature.com/nature/journal/v529/n7587/full/nature16961.html

[60] Virginia Smith, Chao-Kai Chiang, Maziar Sanjabi, và Ameet S Talwalkar. 2017. Học đa nhiệm liên kết. Trong Những tiến bộ trong Hệ thống xử lý thông tin thần kinh 30, I. Guyon, UV Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan và R. Garnett (Biên tập). Curran Associates, Inc., 4424–4434. http://papers.nips.cc/paper/ 7029-federated-multi-task-learning.pdf

[61] Shuang Song, Kamalika Chaudhuri, và Anand D. Sarwate. 2013. Giảm dần độ dốc ngẫu nhiên với sự riêng tư khác biệt cập nhật. 2013 Hội nghị Toàn cầu của IEEE về Xử lý Tín hiệu và Thông tin (2013), 245–248.

[62] Lili Su và Jiaming Xu. 2018. Bảo mật máy học phân tán ở các chiều cao. CoRR abs/1804.10140 (2018). arXiv:1804.10140 http://arxiv.org/abs/1804.10140 [63] Latanya Sweeney. 2002. K-anonymity: Một mô hình bảo vệ sự riêng tư. quốc tế J. Không chắc chắn. Hệ thống dựa trên kiến thức mờ 10, 5 (tháng 10 năm 2002), 557–570. https://doi.org/10.1142/S0218488502001648

[64] Jaideep Vaidya và Chris Clifton. [nd]. Bảo vệ quyền riêng tư Trình phân loại Naive Bayes cho dữ liệu được phân vùng theo chiều dọc. Trong Kỷ yếu của Hội nghị SIAM lần thứ tư về Khai thác dữ liệu, 2004. 330–334.

[65] Jaideep Vaidya và Chris Clifton. 2002. Bảo vệ quyền riêng tư Khai thác quy tắc kết hợp trong dữ liệu được phân vùng theo chiều dọc. Trong Kỷ yếu của Hội nghị Quốc tế ACM SIGKDD lần thứ 8 về Khám phá Tri thức và Khai thác Dữ liệu (KDD '02). ACM, New York, NY, Hoa Kỳ, 639–644. https://doi.org/10.1145/775047.775142 [66] Jaideep Vaidya và Chris Clifton. 2003. Phân cụm K-mean bảo vệ quyền riêng tư trên dữ liệu được phân vùng theo chiều dọc. Trong Kỷ yếu của Hội nghị Quốc tế ACM SIGKDD lần thứ IX về Khám phá Tri thức và Khai thác Dữ liệu (KDD '03). ACM, New York, NY, Hoa Kỳ, 206–215. https://doi.org/10.1145/956750.956776 [67] Jaideep Vaidya và Chris Clifton. 2005. Cây quyết định bảo vệ quyền riêng tư đối với dữ liệu được phân vùng theo chiều dọc. Trong Bảo mật dữ liệu và ứng dụng XIX, Sushil Jajodia và Duminda Wijesekera (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 139–152.

[68] Li Wan, Wee Keong Ng, Shuguo Han, và Vincent CS Lee. 2007. Bảo vệ quyền riêng tư cho các Phương pháp giảm độ dốc. Trong Kỷ yếu của Hội nghị Quốc tế ACM SIGKDD lần thứ 13 về Khám phá Tri thức và Khai thác Dữ liệu (KDD '07). ACM, New York, NY, Hoa Kỳ, 775–783. https://doi.org/10.1145/1281192.1281275

[69] Shiqiang Wang, Tiffany Tuor, Theodoros Salonidis, Kin K. Leung, Christian Makaya, Ting He, và Kevin Chan. 2018. When Edge Meets Learning: Adaptive Control for Resource-Restricted Machine Learning. CoRR abs/1804.05271 (2018). arXiv:1804.05271 http://arxiv.org/abs/1804.05271

[70] Wikipedia. 2018. https://en.wikipedia.org/wiki/Facebook-Cambridge_Analytica_data_scandal.

[71] Qiang Yang, Yang Liu, Tianjian Chen, và Yongxin Tong. 2018. Học tập liên kết. Truyền thông của CCF 14, 11 (2018), 49–55.

[72] Andrew C. Yao. 1982. Các giao thức cho tính toán an toàn. Trong Kỷ yếu của Hội nghị chuyên đề thường niên lần thứ 23 về Nền tảng của Khoa học Máy tính (SFCS '82). IEEE Computer Society, Washington, DC, USA, 160–164. http://dl.acm.org/citement. cfm?id=1382436.1382751

[73] Hwanjo Yu, Xiaoqian Jiang, và Jaideep Vaidya. 2006. SVM bảo vệ quyền riêng tư bằng cách sử dụng hạt nhân phi tuyến trên dữ liệu được phân vùng theo chiều ngang. Trong Kỷ yếu của Hội nghị chuyên đề ACM 2006 về Điện toán ứng dụng (SAC '06). ACM, New York, NY, Hoa Kỳ, 603–610. https://doi.org/10.1145/1141277.1141415 [74] Hwanjo Yu, Jaideep Vaidya, và Xiaoqian Jiang. 2006. Phân loại SVM bảo vệ quyền riêng tư trên dữ liệu được phân vùng theo chiều dọc. Trong Kỷ yếu của Hội nghị châu Á -Thái Bình Dương lần thứ 10 về những tiến bộ trong khám phá tri thức và khai thác dữ liệu (PAKDD'06). Springer-Verlag, Berlin, Heidelberg, 647–656. https://doi.org/10.1007/11731139_74

[75] Jiawei Yuan và Shucheng Yu. 2014. Bảo vệ quyền riêng tư Học tập mạng nơ-ron lan truyền ngược trở nên thiết thực với điện toán đám mây. IEEE Trans. Phân phối song song. hệ thống. 25, 1 (tháng 1 năm 2014), 212–221. https://doi.org/10.1109/TPDS.2013.18 [76] Qingchen Zhang, Laurence T. Yang, và Zhikui Chen. 2016. Bảo vệ quyền riêng tư Mô hình tính toán sâu trên đám mây để học tính năng dữ liệu lớn. IEEE Trans. Điện toán. 65, 5 (tháng 5 năm 2016), 1351–1362. https://doi.org/10.1109/TC.2015.2470255 [77] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, và Vikas Chandra. 2018. Học liên kết với Dữ liệu không phải IID. arXiv:cs.LG/1806.00582