連合学習システムに関する調査：ビジョン、誇大広告、データのプライバシーと保護の現実

Qinbin Li1、Zeyi Wen2、趙民呉1、Sixu Hu1、Naibo Wang1、元Li1、Xu Liu1、Bingsheng He1

1シンガポール国立大学2西オーストラリア大学1{qinbin、zhaomin、sixuhu、naibowang、liyuan、liuxu、hebs} @ comp.nus.edu.sg zeyi.wen@uwa.edu.au2

概要

連合学習は、プライバシーの制限の下でさまざまな組織間で機械学習モデルの共同トレーニングを可能にするためのホットな研究トピックです。研究者がさまざまなプライバシー保護アプローチでより多くの機械学習モデルをサポートしようとするにつれて、さまざまな連合学習アルゴリズムの開発を容易にするためのシステムとインフラストラクチャの開発が必要になります。ディープラーニングの開発を後押しするPyTorchやTensorFlowなどのディープラーニングシステムと同様に、連合学習システム（FLS)も同様に重要であり、有効性、効率、プライバシーなどのさまざまな側面からの課題に直面しています。この調査では、連合学習システムに関する包括的なレビューを実施します。スムーズな流れを実現し、将来の研究を導くために、連合学習システムの定義を紹介し、システムコンポーネントを分析します。さらに、データ配信、機械学習モデル、プライバシーメカニズム、通信アーキテクチャ、連合の規模、連合の動機など、6つの異なる側面に従って、連合学習システムを完全に分類します。分類は、ケーススタディに示されているように、連合学習システムの設計に役立ちます。既存の連合学習システムを体系的に要約することにより、設計要素、ケーススタディ、および将来の研究機会を提示します。

1はじめに

多くの機械学習アルゴリズムはデータを大量に消費し、実際には、プライバシー制限の保護の下でデータがさまざまな組織に分散しています。これらの要因により、連合学習（FL） [129、207、85]は機械学習のホットな研究トピックになっています。たとえば、さまざまな病院のデータが分離され、「データアイランド」になります。各データアイランドにはサイズと実際の分布の近似に制限があるため、単一の病院では、特定のタスクに対して優れた予測精度を持つ高品質のモデルをトレーニングできない場合があります。理想的には、病院は、データの結合について機械学習モデルを共同でトレーニングできれば、より多くの利益を得ることができます。ただし、さまざまな政策や規制により、病院間でデータを単純に共有することはできません。 「データアイランド」でのこのような現象は、金融、政府、サプライチェーンなどの多くの分野で一般的に見られます。一般データ保護規則（GDPR） [10]などのポリシーでは、さまざまな組織間でのデータ共有に関するルールが規定されています。

したがって、プライバシーを保護するためのポリシーや規制を遵守しながら、優れた予測精度を備えた連合学習システムを開発することは困難です。

最近、効果的な機械学習モデルをサポートするための連合学習アルゴリズムの実装に多くの努力が注がれています。具体的には、研究者は、ディープニューラルネットワーク（NN） [119、213、24、158、129]、勾配ブースティング決定木（GBDT） [217、38、104]など、さまざまなプライバシー保護アプローチを使用して、より多くの機械学習モデルをサポートしようとしています。 、ロジスティック回帰[141、36]およびサポートベクターマシン（SVM） [169]。たとえば、Nikolaenkoetal。 [141]およびChenetal。 [36]提案

線形回帰に基づいてFLを実行するためのアプローチ。 GBDTは近年非常に成功しているため[34、200]、対応する連合学習システム（FLS)もZhaoetalによって提案されています。 [217]、 Chengetal。 [38]、 Lietal。 [104]。さらに、NNのトレーニングをサポートする多くのFLSがあります。 Googleは、数千万のデバイスがディープニューラルネットワークをトレーニングできるようにするスケーラブルな本番システムを提案しています[24]。

FLアルゴリズムを構築するための一般的な方法と構成要素（たとえば、差分プライバシーなどのプライバシーメカニズム)があるため、さまざまなFLアルゴリズムの開発を容易にするシステムとインフラストラクチャを開発することは理にかなっています。システムとインフラストラクチャにより、アルゴリズム開発者は一般的なビルディングブロックを再利用でき、毎回ゼロからアルゴリズムを構築する必要がなくなります。深層学習アルゴリズムの開発を後押しするPyTorch [148、149]やTensorFlow [7]などの深層学習システムと同様に、FLSはFLの成功にとって同等に重要です。ただし、成功するFLSを構築することは困難であり、有効性、効率、プライバシー、自律性などの複数の側面を考慮する必要があります。

この論文では、システムの観点から既存のFLSについて調査します。まず、 FLSの定義を示し、従来のフェデレーションシステムと比較します。次に、当事者、管理者、計算通信フレームワークなど、FLSのシステムコンポーネントを分析します。第3に、データ配信、機械学習モデル、プライバシーメカニズム、通信アーキテクチャ、フェデレーションの規模、フェデレーションの動機という6つの異なる側面に基づいてFLSを分類します。これらの側面は、FLSの設計を一般的なビルディングブロックおよびシステム抽象化として指示することができます。第4に、これらの側面に基づいて、FLSの設計を指示するために使用できる既存の研究を体系的に要約します。最後に、FLをより実用的かつ強力にするために、今後の研究の方向性を示します。 FLの成功には、システムとインフラストラクチャが不可欠であると考えています。有効性、効率性、プライバシー、および自律性におけるシステム研究の問題に対処するには、さらに多くの作業を実行する必要があります。

1.1関連調査

FLに関するいくつかの調査がありました。ヤンらによって書かれた独創的な調査。 [207]は、FLの基本と概念を紹介し、さらに包括的な安全なFLフレームワークを提案しています。このホワイトペーパーは主に、通常はエンタープライズデータの所有者である比較的少数の関係者を対象としています。 Lietal。 [109]モバイルおよびエッジデバイスの大規模ネットワークにおけるFLの課題と将来の方向性を要約します。最近、Kairouz等。 [85]は、さまざまな研究トピックからのFLの特性と課題に関する包括的な説明を持っています。ただし、参加者が非常に多くのモバイルデバイスまたはIoTデバイスであるクロスデバイスFLに主に焦点を当てています。最近では、別の調査[11]で、連合学習のプラットフォーム、プロトコル、およびアプリケーションが要約されています。一部の調査は、連合学習の側面にのみ焦点を当てています。たとえば、Limetal。 [113]はモバイルエッジコンピューティングに固有のFLの調査を実施し、 [125]は連合学習への脅威に焦点を当てています。

1.2私たちの貢献

私たちの知る限り、FLSの既存のシステムとインフラストラクチャを確認し、FL用のシステムを作成することへの注目を高めるための調査はありません（ディープラーニングでのシステム研究の繁栄と同様）。前回の調査と比較して、本稿の主な貢献は以下のとおりである。 （1)私たちの調査は、システムコンポーネント、分類法、要約、設計、ビジョンなど、システムの観点からFLに関する包括的な分析を提供する最初の調査です。 （2)データ配信、機械学習モデル、プライバシーメカニズム、通信アーキテクチャ、フェデレーションの規模、フェデレーションの動機など、6つの異なる側面でFLSに対する包括的な分類を提供します。これらは、共通の構成要素およびシステムの抽象化として使用できます。 FLS。 （3)研究者や開発者が参照しやすい、既存の典型的かつ最先端の研究をドメイン別に要約します。 （4)FLSを成功させるための設計要素を提示し、各シナリオのソリューションを包括的にレビューします。 （5)次世代のFLSに向けた興味深い研究の方向性と課題を提案します。

残りの論文は次のように構成されています。セクション2では、 FLSの概念とシステムコンポーネントを紹介します。セクション3では、FLSを分類するための6つの側面を提案します。セクション4では、 FLに関する既存の研究とシステムを要約します。次に、セクション5でFLSの設計要素とソリューションを示します。最後に、セクション7でFLに関する将来の方向性を提案し、セクション8で論文を締めくくります。

2連合学習システムの概要

2.1背景

データ侵害が大きな懸念事項になるにつれて、欧州連合のGDPR [185]、シンガポールのPDPA [39]、米国のCCPA [1]など、ユーザーのデータを保護するための規制を確立する政府がますます増えています。
これらのポリシーに違反するコストは、企業にとってかなり高いものです。 2016年に60万人のドライバーの個人情報が侵害されたため、Uberは調査を解決するために1億4800万ドルを支払わなければなりませんでした[3]。 SingHealthは、PDPA違反でシンガポール政府から750,000ドルの罰金を科されました[5]。 Googleは、GDPRの違反に対して5,700万ドルの罰金を科されました[4]。これは、欧州連合のプライバシー法に基づく2020年3月18日現在の最大の罰則です。

このような状況の中で、ユーザーの元のデータを交換せずに共同学習する連合学習が、最近ますます注目を集めています。機械学習、特にディープラーニングは最近再び多くの注目を集めていますが、フェデレーションと機械学習の組み合わせは、新しくホットな研究トピックとして浮上しています。

2.2定義

FLを使用すると、ローカルデータを交換することなく、複数の関係者が共同で機械学習モデルをトレーニングできます。分散システム、機械学習、プライバシーなど、複数の研究分野の技術を網羅しています。他の研究[85、207]によって与えられたFLの定義に触発されて、ここでFLSの定義を示します。

連合学習システムでは、複数の関係者が生データを交換せずに機械学習モデルを共同でトレーニングします。システムの出力は、各パーティの機械学習モデルです（同じでも異なっていてもかまいません）。実用的な連合学習システムには、次の制約があります。テストの精度などの評価指標を考えると、連合学習によって学習されたモデルのパフォーマンスは、同じモデルアーキテクチャを使用したローカルトレーニングによって学習されたモデルよりも優れている必要があります。

2.3従来のフェデレーションシステムとの比較

フェデレーションの概念は、ビジネスやスポーツなどの現実の世界に対応するものと一緒に見つけることができます。
フェデレーションの主な特徴は協力です。フェデレーションは一般的に社会に登場するだけでなく、コンピューティングにおいても重要な役割を果たします。コンピュータサイエンスでは、フェデレーションコンピューティングシステムはさまざまな状況下で魅力的な研究分野となっています。

1990年頃、連合データベースシステム（FDBS)に関する多くの研究がありました[166]。 FDBSは、相互利益のために協力する自律型データベースのコレクションです。以前の研究[166]で指摘されているように、FDBSの3つの重要な要素は、自律性、不均一性、および分布です。

- 自律性。 FDBSに参加するデータベースシステム（DBS)は自律的です。つまり、独立した独立した制御下にあります。当事者は、FDBSがなくてもデータを管理できます。

- 不均一性。データベース管理システムは、FDBS内で異なる場合があります。たとえば、違いは、データ構造、クエリ言語、システムソフトウェア要件、および通信機能にある可能性があります。

- 配布。 FDBSが構築される前に複数のDBSが存在するため、データ分散はDBSごとに異なる場合があります。データレコードは、水平方向または垂直方向に異なるDBSに分割できます。また、信頼性を高めるために複数のDBSに複製することもできます。

最近では、クラウドコンピューティングの開発に伴い、フェデレーションクラウドコンピューティングについて多くの研究が行われています[97]。フェデレーションクラウド（FC)は、複数の外部および内部クラウドコンピューティングサービスの展開と管理です。クラウドフェデレーションの概念により、よりコスト効率の高い地域への部分的なアウトソーシングにより、コストをさらに削減できます。リソースの移行とリソースの冗長性は、フェデレーションクラウドの2つの基本機能です[97]。まず、リソースをあるクラウドプロバイダーから別のクラウドプロバイダーに転送できます。移行により、リソースの再配置が可能になります。第二に、冗長性により、異なるドメインで同様のサービス機能を同時に使用できます。たとえば、データは、同じ計算ロジックに従って、異なるプロバイダーでパーティション化および処理できます。全体として、さまざまなリソースのスケジューリングは、フェデレーションクラウドシステムの設計における重要な要素です。

FLSと従来のフェデレーションシステムにはいくつかの類似点と相違点があります。まず、フェデレーションの概念は引き続き適用されます。一般的で基本的な考え方は、複数の独立した当事者の協力についてです。したがって、当事者間の異質性と自律性を考慮するという観点は、FLSにも適用できます。第二に、分散システムの設計におけるいくつかの要因は、 FLSにとって依然として重要です。たとえば、当事者間でデータを共有する方法は、システムの効率に影響を与える可能性があります。違いについては、これらのフェデレーションシステムは、コラボレーションと制約に異なる重点を置いています。 FDBSは分散データの管理に重点を置き、FCはリソースのスケジューリングに重点を置いていますが、FLSは複数の関係者間の安全な計算に重点を置いています。 FLSは、分散トレーニングのアルゴリズム設計やプライバシー制限の下でのデータ保護などの新しい課題を引き起こします。

図1は、これら3つの研究分野の各年の論文数を示しています。ここでは、 Google Scholar1で「連合データベース」、「連合クラウド」、「連合学習」というキーワードを検索して論文を数えます。連合データベースは30年前に提案されましたが、近年、それについて言及している論文はまだ約400あります。フェデレーションクラウドの人気は、当初はフェデレーションデータベースよりも急速に成長しましたが、クラウドコンピューティングが成熟し、フェデレーションのインセンティブが低下したためか、近年は減少しているようです。 FLについては、関連論文の数が急増しており、昨年は約4,400件に達しました。今日、「データアイランド」現象は一般的であり、機械学習においてますます重要な問題になっています。また、一般の人々からのプライバシーへの懸念と社会的認識が高まっています。したがって、FLの人気は、成熟したFLSが存在するようになるまで、少なくとも5年間は増加し続けると予想されます。

2.4システムコンポーネント

FLSには、パーティ（クライアントなど）、マネージャー（サーバーなど）、機械学習モデルをトレーニングするための通信計算フレームワークの3つの主要コンポーネントがあります。

2.4.1当事者

FLSでは、当事者はFLのデータ所有者と受益者です。それらは、それぞれクロスサイロまたはクロスデバイス設定[85]という名前の組織またはモバイルデバイスにすることができます。 FLSの設計に影響を与える当事者の以下の特性を考慮します。

まず、当事者のハードウェア容量はどれくらいですか？ハードウェア容量には、計算能力とストレージが含まれます。当事者が携帯電話である場合、容量は弱く、当事者は多くの計算を実行して大きなモデルをトレーニングすることができません。たとえば、Wangetal。 [192] FLのリソースに制約のある設定を検討してください。彼らは、リソース予算を含める目的を設計し、ローカル更新のラウンドを決定するためのアルゴリズムを提案しました。

第二に、当事者の規模と安定性はどのくらいですか？組織の場合、規模はモバイルデバイスに比べて比較的小さいです。また、クロスサイロ設定の安定性は、クロスデバイス設定よりも優れています。したがって、クロスサイロ設定では、多くの研究で一般的な設定である、すべての関係者がフェデレーションプロセス全体で計算および通信タスクを継続的に実行できることが期待できます[104、38、169]。当事者がモバイルデバイスである場合、システムは次のような考えられる問題を処理する必要があります

[1] https://scholar.google.com/

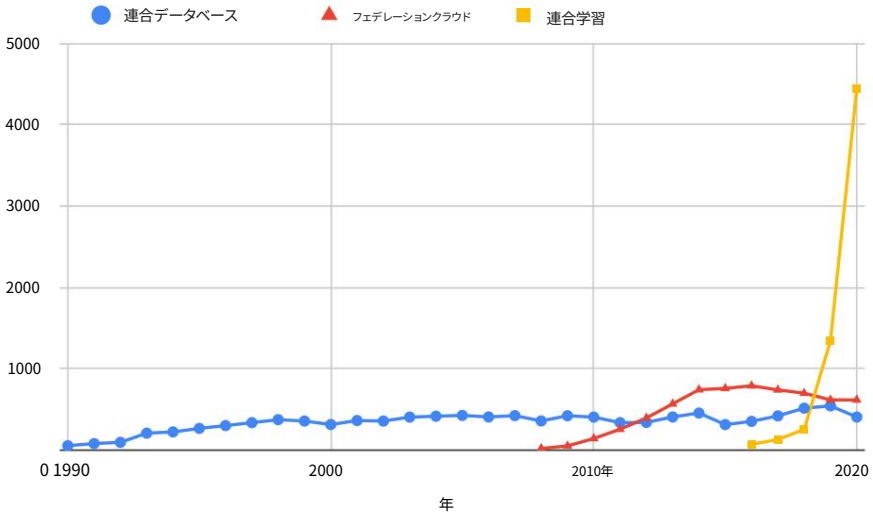


図1：「連合データベース」、「連合クラウド」、「連合学習」に関する関連論文の数

接続が失われたため[24]。さらに、デバイスの数は非常に多くなる可能性があるため（たとえば、数百万）、すべてのデバイスがFLのすべてのラウンドに参加すると想定するのは現実的ではありません。広く使用されている設定は、各ラウンドで計算を実行するデバイスの一部を選択することです[129、24]。

最後に、当事者間のデータ分布はどのようなものですか ?通常、クロスデバイスまたはクロスサイロの設定に関係なく、非IID（同一かつ独立して分散された)データ分散は、最近の研究[104、 213、111、189] 。このような非IIDデータの配布は、組織間でより明白になる可能性があります。

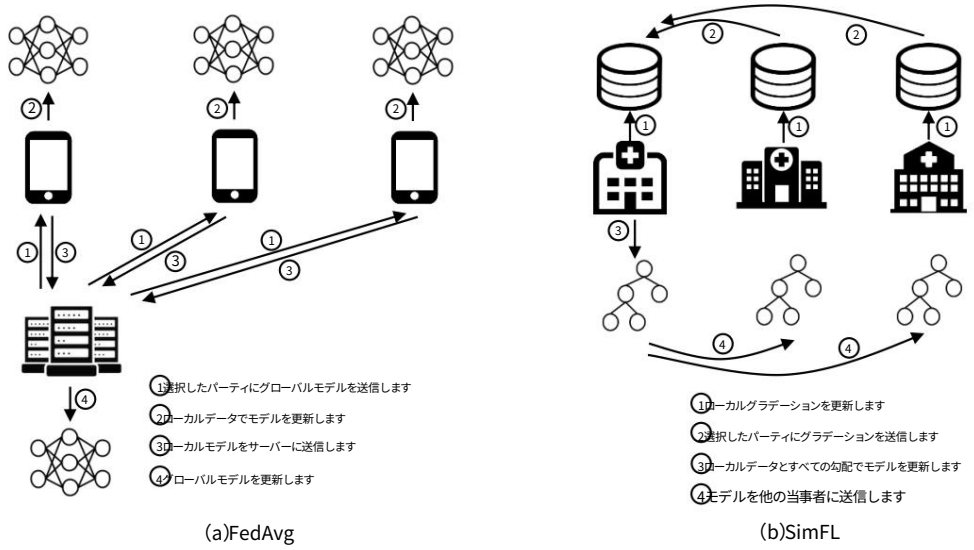
たとえば、銀行と保険会社はFLを実行して予測を改善できます（たとえば、人がローンを返済できるかどうか、人が保険商品を購入するかどうか)が、これらの組織では機能さえ大きく異なる可能性があります。転移学習[147]、メタ学習[55]、およびマルチタスク学習[157]の手法は、さまざまな種類の関係者の知識を組み合わせるのに役立つ場合があります。

2.4.2マネージャー

クロスデバイス設定では、マネージャーは通常、強力な中央サーバーです。グローバルな機械学習モデルのトレーニングを実施し、当事者とサーバー間の通信を管理します。サーバーの安定性と信頼性は非常に重要です。サーバーが正確な計算結果を提供できない場合、FLSは不良モデルを生成する可能性があります。これらの潜在的な問題に対処するために、ブロックチェーン[176]は、システムの信頼性を高めるために分散型ソリューションを提供するための可能な手法である可能性があります。たとえば、Kimetal。 [93]システム内の中央サーバーの代わりにブロックチェーンを活用します。ブロックチェーンにより、デバイスの更新を交換し、デバイスに報酬を提供できます。

クロスサイロ設定では、組織は強力なマシンを持っていることが期待されるため、マネージャーはFLプロセスを支配する組織の1つになることもできます。これは特に垂直FL [207]で使用されます。これについては、セクション3.1で詳しく説明します。 Liuらによる垂直FL設定で。 [119]、データの機能はパーティ間で垂直に分割され、1つのパーティのみがラベルを持っています。ラベルを所有する当事者は、当然、FLマネージャーと見なされます。

1つの課題は、特にクロスサイロ設定では、マネージャーとして信頼できるサーバーまたはパーティを見つけるのが難しいことです。次に、完全に分散化された設定が適切な選択となる可能性があります。この場合、当事者は互いに直接通信し、ほぼ均等にグローバルな機械学習モデルのトレーニングに貢献します。
これらの当事者は共同でFLタスクを設定し、FLSを展開します。 Lietal。 [104]連合勾配を提案する



(a)FedAvg (b)SimFL

図2 :連合学習フレームワーク

各パーティが決定木を順番にトレーニングし、最終的なモデルがすべてのツリーの組み合わせである、決定木のフレームワークを強化します。妥当な通信オーバーヘッドを備えた完全分散型FLSを設計することは困難です。

2.4.3通信-計算フレームワーク

FLSでは、計算は当事者とマネージャーで行われ、通信は当事者とマネージャーの間で行われます。通常、計算の目的はモデルのトレーニングであり、通信の目的はモデルのパラメーターを交換することです。

図2aに示すように、基本的で広く使用されているフレームワークは、2016年に提案されたFederated Averaging（FedAvg）[129]です。各反復で、サーバーは最初に現在のグローバルモデルを選択されたパーティに送信します。
次に、選択したパーティがローカルデータでグローバルモデルを更新します。次に、更新されたモデルがサーバーに返送されます。
最後に、サーバーは受信したすべてのローカルモデルを平均して、新しいグローバルモデルを取得します。
FedAvgは、指定された反復回数に達するまで上記のプロセスを繰り返します。サーバーのグローバルモデルが最終出力です。

FedAvgは集中型FLフレームワークですが、Liらによって提案されたSimFLです。 [109]は、分散型FLフレームワークを表します。 SimFLでは、信頼できるサーバーは必要ありません。各反復で、当事者は最初にローカルデータの勾配を更新します。次に、グラデーションが選択したパーティに送信されます。次に、選択したパーティは、ローカルデータとグラデーションを使用してモデルを更新します。最後に、モデルは他のすべての関係者に送信されます。
公平性を確保し、さまざまな関係者からのデータを利用するために、ほぼ同じラウンド数でモデルを更新するためにすべての関係者が選択されます。 SimFLは指定された回数の反復を繰り返し、最終モデルを出力します。

3分類法

さまざまなFLSに共通のシステム抽象化と構成要素を考慮して、FLSを、データパーティショニング、機械学習モデル、プライバシーメカニズム、通信アーキテクチャ、フェデレーションの規模、およびフェデレーションの動機の6つの側面で分類します。これらの側面には、以前のFLS [166、97]の一般的な要因（データの分割、通信アーキテクチャなど）と、FLSの独自の考慮事項（機械学習モデルやプライバシーメカニズムなど）が含まれます。さらに、これらの側面を使用して、FLSの設計をガイドできます。図3は、FLSの分類法の要約を示しています。

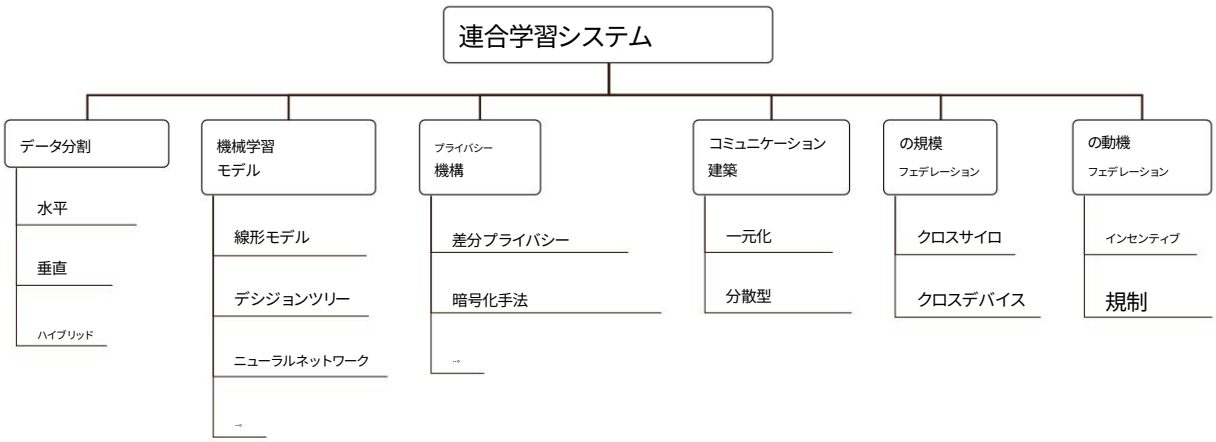


図3 :連合学習システムの分類法

[85]の表1では、分散学習、クロスデバイス連合学習、および設定、データ分散、通信などを含むクロスサイロ連合学習を区別するためにさまざまな特性を考慮しています。私たちの分類法は、さまざまな連合学習システムを区別するために使用されます展開の観点から、機械学習モデルや連合の動機などの側面は[85]では考慮されていません。

3.1データの分割

データがサンプルスペースとフィーチャスペースにどのように分散されるかに基づいて、FLSは通常、水平、垂直、およびハイブリッドFLSに分類できます[207]。

水平FLでは、異なるパーティのデータセットは同じ特徴空間を持ちますが、サンプル空間上の交差はほとんどありません。これは、特にクロスデバイス設定の場合の自然なデータ分割であり、さまざまなユーザーがFLを使用して同じタスクでモデルのパフォーマンスを向上させようとします。また、 FL研究の大部分は水平分割を採用しています。ローカルデータは同じフィーチャスペースにあるため、パーティは同じモデルアーキテクチャのローカルデータを使用してローカルモデルをトレーニングできます。グローバルモデルは、すべてのローカルモデルを平均化することで簡単に更新できます。図2に示すように、水平連合学習の基本的で一般的なフレームワークはFedAvgです。「HeySiri 」や「OKGoogle」などのウェイクワード認識[98]は、各ユーザーが話すため、水平パーティションの典型的なアプリケーションです。異なる声で同じ文。

垂直FLでは、異なるパーティのデータセットは同じまたは類似のサンプルスペースを持ちますが、特徴スペースが異なります。垂直FLSの場合、通常、エンティティの位置合わせ手法[206、41]を採用して、当事者の重複するサンプルを収集します。次に、重複したデータを使用して、暗号化方式を使用して機械学習モデルをトレーニングします。チェンら。 [38]は、損失のない垂直FLSを提案して、パーティが勾配ブースティング決定木を共同でトレーニングできるようにします。彼らはプライバシー保護エンティティの調整を使用して、2つのパーティ間で共通のユーザーを見つけます。その勾配は、意思決定ツリーを共同でトレーニングするために使用されます。異なる企業間の協力は、通常、垂直分割の状況として扱うことができます。

他の多くのアプリケーションでは、既存のFLSは主に1種類のパーティションに焦点を当てていますが、パーティ間のデータのパーティションは、水平パーティションと垂直パーティションのハイブリッドである可能性があります。例として癌診断システムを取り上げましょう。病院のグループは、がん診断用のFLSを構築したいと考えていますが、各病院には、さまざまな患者とさまざまな種類の健康診断結果があります。転移学習[147]は、そのようなシナリオの可能な解決策です。 Liuetal。 [119]共通のインスタンスを使用して、パーティの機能間の表現を学習できる安全なフェデレーション転送学習システムを提案します。

3.2機械学習モデル

FLは機械学習の問題を解決するために使用されるため、当事者は通常、特定のタスクについて最先端の機械学習モデルをトレーニングしたいと考えています。新しいモデルを開発したり、現在のモデルを連合の設定に再発明したりするために多くの努力が払われてきました。ここでは、現在広く使用されているモデルについて考察します。
現在最も人気のある機械学習モデルはニューラルネットワーク（NN)であり、画像分類や単語予測などの多くのタスクで最先端の結果を実現します[96、175]。確率的勾配降下法[129、189、24]に基づく多くの連合学習研究があり、NNのトレーニングに使用できます。

もう1つの広く使用されているモデルは、NNと比較してトレーニングが非常に効率的で、解釈が容易な決定木です。ツリーベースのFLSは、単一または複数の決定木（たとえば、勾配ブースティング決定木（GBDT)およびランダムフォレスト)のフェデレーショントレーニング用に設計されています。 GBDTは最近特に人気があり、多くの分類および回帰タスクで非常に優れたパフォーマンスを発揮します。 Lietal。 [104]およびChengetal。 [38]は、水平方向と垂直方向にそれぞれ分割されたデータのGBDT用のFLSを提案します。

NNとツリーに加えて、線形モデル（線形回帰、ロジスティック回帰、SVMなど)は、古典的で使いやすいモデルです。線形回帰とロジスティック回帰のためによく開発されたシステムがいくつかあります[141、72]。これらの線形モデルは、他の複雑なモデル（ NNなど)と比較して簡単に習得できます。

単一の機械学習モデルは弱いかもしれませんが、スタッキングや投票などのアンサンブル手法[150]をフェデレーション設定で適用できます。各パーティはローカルモデルをトレーニングしてサーバーに送信し、サーバーはすべてのモデルをアンサンブルとして集約します。アンサンブルは、最大投票による予測に直接使用することも、スタッキングによるメタモデルのトレーニングに使用することもできます。フェデレーションアンサンブル学習の利点は、モデルパラメーターの平均化がないため、各パーティが異種モデルをトレーニングできることです。以前の研究[213、103]に示されているように、フェデレーションアンサンブル学習も1回の通信ラウンドで優れた精度を達成できます。

現在、多くのFLフレームワーク[129、94、192、108]が確率的勾配降下法に基づいて提案されています。これは、ニューラルネットワークやロジスティック回帰を含む多くのモデルの典型的な最適化アルゴリズムです。ただし、FLの有効性を高めるには、モデルアーキテクチャを活用する必要がある場合があります[189]。 FLの研究はまだ初期段階であるため、FLSが最先端のモデルをより適切にサポートするためのギャップがまだあります。

3.3プライバシーメカニズム

ローカルデータはFLで公開されていませんが、交換されたモデルパラメータは、データに関する機密情報を漏洩する可能性があります。モデル反転攻撃[56]やメンバーシップ推論攻撃[167]など、機械学習モデルに対する多くの攻撃がありました[56、167、137、131] 。これらはモデルにアクセスすることで生データを推測できる可能性があります。さらに、差分プライバシー[48]やk-匿名性[50]など、さまざまなプライバシー保証を提供する多くのプライバシーメカニズムがあります。既存のプライバシーメカニズムの特徴は、調査[186]に要約されています。ここでは、データ保護のために現在のFLSで採用されている2つの主要なアプローチ、暗号化方式と差分プライバシーを紹介します。

準同型暗号化[15、72、28、156、116]や安全なマルチパーティ計算（SMC)[165、32、22、23]などの暗号化手法は、プライバシーを保護する機械学習アルゴリズムで広く使用されています。基本的に、当事者は、送信する前にメッセージを暗号化し、暗号化されたメッセージを操作し、暗号化された出力を復号化して最終結果を取得する必要があります。上記の方法を適用すると、FLSのユーザープライバシーは通常十分に保護できます[89、211、91、144] 。たとえば、SMC [63]は、転送された勾配を安全に集約するために使用できる出力以外は、すべての関係者が学習できないことを保証します。ただし、SMCは最終モデルのプライバシー保証を提供していません。最終モデルは依然として推論攻撃およびモデル反転攻撃に対して脆弱です[167、56]。また、追加の暗号化および復号化操作のために、そのようなシステムは非常に高い計算オーバーヘッドに悩まされます。

差分プライバシー[48、49]は、1つのレコードが関数の出力にあまり影響を与えないことを保証します。多くの研究では、データのプライバシー保護に差分プライバシー[31、8、105、180、220、112]を採用しており、個々のレコードが学習に参加しているかどうかを当事者が知ることができないようにしています。に

データまたはモデルパラメータにランダムノイズを注入することで[8、105、170、202]、差分プライバシーは、個々のレコードの統計的プライバシー保証とモデルへの推論攻撃に対する保護を提供します。学習プロセスのノイズのため、このようなシステムは精度の低いモデルを生成する傾向があります。

上記の方法は互いに独立しており、FLSはプライバシー保証を強化するために複数の方法を採用できることに注意してください[64、205、86]。ユーザーのプライバシーを保護するための他のアプローチもあります。
興味深いハードウェアベースのアプローチは、Intel SGXプロセッサ[159、145]などの信頼できる実行環境（TEE)を使用することです。これにより、内部にロードされたコードとデータが保護されます。このような環境は、中央サーバー内で使用して、その信頼性を高めることができます。

プライバシーレベルに関連して、脅威モデルはFLSでも異なります[125]。攻撃はどこからでも発生する可能性があります
入力、学習プロセス、および学習されたモデルを含む、FLのプロセスの段階。

- 入力悪意のある当事者は、FLに対してデータポイズニング攻撃[35、99、12]を実行する可能性があります。たとえば、当事者は特定のクラスのトレーニングサンプルのラベルを変更して、最終的なモデルがこのクラスでうまく機能しないようにすることができます。

- 学習プロセス学習プロセス中に、当事者はモデル中毒攻撃[16、203]を実行して、設計されたモデルパラメータをアップロードできます。データポイズニング攻撃と同様に、グローバルモデルは、ポイズニングされたローカル更新のために精度が非常に低くなる可能性があります。モデル中毒攻撃に加えて、ビザンチン将軍問題[27、21、173]も分散学習の一般的な問題であり、当事者が恣意的に悪い行動をとり、ランダムな更新をアップロードする可能性があります。

- 学習したモデル。学習したモデルが公開されている場合は、推論攻撃[56、167、131、137]を実行できます。サーバーは、交換されたモデルパラメーターからトレーニングデータに関する機密情報を推測できます。たとえば、メンバーシップ推論攻撃[167、137]は、特定のデータレコードがトレーニングで使用されているかどうかを推測できます。推論攻撃は、当事者のローカル更新にアクセスできるFLマネージャーによって学習プロセスで実行される場合もあることに注意してください。

3.4通信アーキテクチャ

FLSの通信には、集中型設計と分散型設計の2つの主要な方法があります。一元化された設計では、データフローは非対称であることがよくあります。つまり、マネージャーはパーティからの情報（ローカルモデルなど)を集約し、トレーニング結果を送り返します[24]。グローバルモデルのパラメーターの更新は、常にこのマネージャーで行われます。マネージャとローカルパーティ間の通信は、同期[129]または非同期[204、171]にすることができます。分散型設計では、通信はパーティ間で実行され[217、104]、すべてのパーティはグローバルパラメータを直接更新できます。

Googleキーボード[71]は、集中型アーキテクチャのケースです。サーバーは、ユーザーのデバイスからローカルモデルの更新を収集し、グローバルモデルをトレーニングします。これは、図2aに示すように、推論のためにユーザーに返送されます。スケーラビリティと安定性は、集中型FLのシステム設計における2つの重要な要素です。

集中型設計は既存の研究で広く使用されていますが、1台のサーバーに情報を集中させると潜在的なリスクや不公平が生じる可能性があるため、一部の側面では分散型設計が推奨されます。
ただし、分散型通信アーキテクチャの設計は困難であり、公平性と通信オーバーヘッドを考慮に入れる必要があります。現在、P2P [104、217]、グラフ[128]、またはブロックチェーン[191、219]の3つの異なる分散型設計があります。 P2P設計では、連合学習中に当事者に同等の特権と扱いが与えられます。例として、SimFL [104]があります。この場合、各パーティはツリーを順番にトレーニングし、他のすべてのパーティにツリーを送信します。通信アーキテクチャは、遅延や計算時間などの追加の制約を伴うグラフとしてモデル化することもできます。 Marfoqetal。 [128]スループットが最適なトポロジー設計を見つけるためのアルゴリズムを提案します。最近、ブロックチェーン[223]は、検討対象として人気のある分散型プラットフォームです。連合学習の当事者の情報を保存し、連合学習の透明性を確保するために使用できます[191]。

3.5フェデレーションの規模

FLSは、フェデレーションの規模によって2つの典型的なタイプに分類できます。クロスサイロFLSとクロスデバイスFLSです[85]。それらの違いは、パーティの数と各パーティに保存されているデータの量にあります。

クロスサイロFLSでは、当事者は組織またはデータセンターです。通常、パーティの数は比較的少なく、各パーティには比較的大量のデータと計算能力があります。
たとえば、Amazonは、世界中の何百ものデータセンターから収集されたショッピングデータをトレーニングすることで、ユーザーに商品を推奨したいと考えています。各データセンターには、膨大な量のデータと十分な計算リソースがあります。もう1つの例は、連合学習を医療機関間で使用できることです。さまざまな病院が連合学習を使用して、胸部X線画像をローカルに保持しながら胸部X線写真分類用のCNNをトレーニングできます[86]。連合学習を使用すると、モデルの精度を大幅に向上させることができます。このようなFLSが直面する課題の1つは、プライバシーモデルの制約の下でデータセンターに計算を効率的に分散する方法です[224]。

逆に、クロスデバイスFLSでは、パーティの数が比較的多く、各パーティのデータ量と計算能力は比較的少なくなっています。当事者は通常、モバイルデバイスです。
Googleキーボード[208]は、クロスデバイスFLSの例です。 Googleキーボードのクエリ提案は、FLを使用して改善できます。エネルギー消費の懸念があるため、デバイスに複雑なトレーニングタスクを実行するように依頼することはできません。この場合、システムは、多数の関係者を管理し、デバイスとサーバー間の不安定な接続などの考えられる問題に対処するのに十分強力である必要があります。

3.6連盟の動機

FLの実際のアプリケーションでは、個々の関係者がFLSに参加する動機を必要とします。動機は規制またはインセンティブである可能性があります。会社または組織内のFLは通常、規制によって動機付けられます（たとえば、会社のさまざまな部門にわたるFL）。たとえば、ユーザーのトランザクションレコードがある部門は、連合学習によって別の部門がユーザーのクレジットを予測するのに役立ちます。多くの場合、規制によって当事者にデータの提供を強制することはできません。ただし、連合学習への参加を選択した当事者は、モデルの精度が高くなるなど、その恩恵を受けることができます。たとえば、病院は連合学習を実施して、胸部X線写真分類[86]またはCOVID-19検出[152]用の機械学習モデルをトレーニングできます。そうすれば、病院は、人間の専門家よりも精度の高い優れたモデルと、フェデレーションなしでローカルでトレーニングされたモデルを取得できます。別の例はGoogleキーボード[208]です。ユーザーはGoogleキーボードが自分のデータを利用しないようにすることを選択できますが、入力データのアップロードに同意するユーザーは、より高い精度の単語予測を楽しむことができます。ユーザーは、利便性のために連合学習に積極的に参加することができます。

挑戦的な問題は、より多くの貢献をする当事者が連合学習からより多くの利益を得ることができるように、公正なインセンティブメカニズムをどのように設計するかです。ブロックチェーンでのインセンティブデザインの成功例がいくつかあります[228、51]。システム内の関係者は、競合他社だけでなく共同作業者になることもできます。
[88、87]のような他のインセンティブ設計は、FLの高品質データで参加者を引き付けるために提案されています。ゲーム理論モデル[163、84、136]とその平衡設計は、FLSの下で再検討する必要があります。 Googleキーボードの場合でも、ユーザーはこの共学習プロセスに参加するように動機付けられる必要があります。

4既存の研究の要約

このセクションでは2 、セクション3で検討した側面に従って、FLSに関する既存の研究を要約して比較します。

2最終更新日は2021年12月7日です。このセクションは定期的に更新され、最先端の貴重なFL研究が含まれます。次のURLで最新バージョンを確認してください：https：//arxiv.org/abs/1907.09693。また、この調査に追加したい参考資料がある場合は、Bingsheng He博士に電子メール（hebs@comp.nus.edu.sg)を送ってください。

4.1方法論

FLに関する既存の研究を見つけるために、GoogleScholarでキーワード「FederatedLearning」を検索します。ここでは、コンピュータサイエンスコミュニティで公開されている研究のみを検討します。

フェデレーションの規模とフェデレーションの動機は問題に依存するため、既存の研究をこれら2つの側面で比較しません。わかりやすくするために、「NN」、「DT」、「LM」を使用して、それぞれニューラルネットワーク、決定木、線形モデルを示します。さらに、「CM」と「DP」を使用して、それぞれ暗号化方式と差分プライバシーを示します。一部の研究のアルゴリズム（たとえば、連合確率的勾配降下法)は、多くの機械学習モデル（たとえば、ロジスティック回帰やニューラルネットワーク)を学習するために使用できることに注意してください。したがって、「モデルの実装」の列では、対応する論文の実験で実装されたモデルを示します。また、「メインエリア」欄には、論文が研究している主要エリアを示しています。

4.2個別研究

表1に示すように、既存の人気のある最先端の研究成果を要約します。表1から、次の4つの重要な調査結果が得られます。

まず、既存の研究のほとんどは、水平方向のデータ分割を考慮しています。その理由の一部は、水平方向のデータ分割における実験的研究とベンチマークが、垂直方向のデータ分割よりも比較的準備が整っていることであると推測します。ただし、垂直FLは、特に異なる組織間では、現実の世界でも一般的です。垂直FLは、多様な関係者間のより多くのコラボレーションを可能にします。したがって、ギャップを埋めるために、垂直FLにより多くの努力を払う必要があります。

第二に、ほとんどの研究では、プライバシーを保証せずに生のモデルパラメータを交換することを検討しています。将来、機械学習モデルに対するより強力な攻撃が発見された場合、これは正しくない可能性があります。現在、プライバシー保証を提供する主流の方法は、差分プライバシーと暗号化の方法です（たとえば、安全なマルチパーティ計算と準同型暗号化）。差分プライバシーは、最終的なモデルの品質に大きな影響を与える可能性があります。さらに、暗号化方式は多くの計算と通信のオーバーヘッドをもたらし、FLSのボトルネックになる可能性があります。私たちは、規制を満たすための合理的なプライバシー保証を備えた安価な方法を楽しみにしています。

第三に、一元化された設計が現在の実装の主流です。設定には信頼できるサーバーが必要です。ただし、特にクロスサイロ設定では、信頼できるサーバーを見つけるのが難しい場合があります。中央サーバーを削除するための単純なアプローチの1つは、パーティがモデルパラメータを他のすべてのパーティと共有し、各パーティも同じグローバルモデルをローカルで維持することです。この方法は、集中化された設定と比較して、より多くの通信と計算のコストをもたらします。分散型アーキテクチャを使用した実用的なFLについては、さらに調査を行う必要があります。

最後に、FLの主な研究の方向性（また主な課題)は、有効性、効率、プライバシーを改善することです。これらは、FLSを評価するための3つの重要な指標でもあります。一方、公平性やインセンティブメカニズムなど、FLに関する他の多くの研究トピックがあります。 FLは多くの研究分野に関連しているため、FLはより多くの研究者を引き付け、近い将来、より興味深い研究を見ることができると信じています。

4.2.1有効性の改善

一部のアルゴリズムはSGDに基づいていますが、他のアルゴリズムは1つまたは複数の種類のモデルアーキテクチャ用に特別に設計されています。したがって、それらをSGDベースのアルゴリズムに分類し、それに応じて特殊なアルゴリズムをモデル化します。

SGDベース

パーティのローカルデータを単一のバッチと見なす場合、SGDは、ラウンドごとに単一のバッチ勾配計算を実行することにより、フェデレーション設定で簡単に実装できます（つまり、FedSGD [129]）。ただし、このような方法では、収束するために多数の通信ラウンドが必要になる場合があります。通信ラウンドの数を減らすために、FedAvg [129]は、メインペーパーのセクション2.3.3および図1aで紹介されています。

表1 :既存の公開された研究間の比較。 LMは線形モデルを示します。 DMは決定を示します
木。 NNはニューラルネットワークを示します。 CMは暗号化メソッドを示します。 DPはディファレンシャルを示します
プライバシー。

FL 研究	主要 範囲	データ パーティショニング	モデル 実装	プライバシー 機構	コミュニケーション 建築	述べる
FedAvg [129]	効果的 アルゴリズム	水平	NN	＼	一元化	SGDベース
FedSVRG [94]			LM			
FedProx [108]			LM、NN			
足場[90]			LM、NN			
FedNova [190]			NN			
Per-FedAvg [52]			NN			
pFedMe [46]			LM、NN			
IAPGD、AL2SGD + [69]			LM			
IFCA [61]			LM、NN			
不可知論者FL[134]			LM、NN			
FedRobust [155]			NN			
FedDF [114]			NN			
FedBCD [120]		垂直	NN			NN-専門
PNFM [213]		水平				
FedMA [189]						
SplitNN [189]		垂直				
ツリーベースのFL[217]	実用性 強化	水平	DT	DP	分散型	DT-スペシャライズド
SimFL [104]				ハッシュ		
FedXGB [122]						
FedForest [121]						
SecureBoost [38]		垂直				
リッジ回帰FL[141]		水平	LM	CM		LM専門
PPRR [36]						
線形回帰FL[162]		垂直				
ロジスティック回帰FL[72]						
フェデレーションMTL[169]					一元化	マルチタスク学習
連合メタ学習[33]			NN			メタ学習
パーソナライズされたFedAvg[81]						
LFRL [115]						強化学習
FBO [44]			LM	＼		ベイズ最適化
構造の更新[95]			NN			効率 改善
多目的FL[226]						
オンデバイスML[79]						
スパース三項圧縮[164]						
DPASGD [128]					分散型	
クライアントレベルのDPFL[60]				DP		プライバシー 保証
LSTMで[130]						
ローカルDPFL[20]			LM、NN			
セキュアアグリゲーションFL[23]			NN	CM		
ハイブリッドFL[181]			LM、DT、NN CM、DP			
バックドアFL[16、174、188]			NN			堅牢性と攻撃
敵対レンズ[19]						
分散型バックドア[203]						
画像再構成[58]						
RSA [100]			LM			
モデル毒[53]q-			LM、NN			
FedAvg[110]			LM、NN	＼	一元化	公平性
BlockFL [93]			LM			インセンティブ
評判FL[87]						
FedCS [143]	アプリケーション		NN			エッジコンピューティング
DRL-MEC [194]						
リソースに制約のあるMEC[192]			LM、NN			
FedGKT [73]			NN			
FedCF [14]			LM			協調フィルター
FedMF [29]						行列の因数分解
FedRecSys [177]			LM、NN	CM		レコメンダーシステム
FLキーボード[71]			NN			自然言語処理
不正検出[222]			NN			クレジットカード取引
FedML [74]	ベンチマーク	水平 &垂直	LM、NN	＼	一元化 &分散型	汎用ベンチマーク
FedEval [30]		水平	NN		一元化	
OARF [77]			NN	CM、DP	一元化	
エッジAIベンチ[70]			＼		＼	
PerfEval [142]			NN	＼	一元化	ターゲットベンチマーク
FedReID [227]						
半教師ありベンチマーク[216]						
非IIDベンチマーク[117]					＼	
リーフ[25]			＼		一元化	データセット
ストリートデータセット[124]					＼	

現在、SGDに基づく典型的で実用的なFLフレームワークです。 FedAvgでは、各パーティがローカルモデルでSGDを使用して複数のトレーニングラウンドを実施します。次に、グローバルモデルの重みが、ローカルモデルの重みの平均として更新されます。グローバルモデルは、グローバル反復を完了するためにパーティに送り返されます。重みを平均化することにより、ローカルパーティは、ローカルモデルで最急降下法の複数のステップを実行できるため、FedSGDと比較して通信ラウンドの数を減らすことができます。 、

Konecn ˇ yetal 。 [94]連合SVRG（FSVRG)を提案する。フェデレーションSVRGとフェデレーション平均の主な違いは、ローカルモデルとグローバルモデルのパラメーターを更新する方法です（つまり、ステップ2とステップ4）。モデルの重みを更新する式は、確率的分散減少勾配（SVRG） [82]と、フェデレーションSVRGの分散近似ニュートンアルゴリズム（DANE)に基づいています。彼らは、アルゴリズムをCoCoA+ [126]や単純な最急降下法などの他のベースラインと比較します。彼らの方法は、ロジスティック回帰モデルと同じ通信ラウンドでより高い精度を達成できます。フェデレーション平均とフェデレーションSVRGの比較はありません。

連合学習における重要な課題は、ローカルデータ（つまり、非IIDデータ)の異質性であり[106]、連合学習のパフォーマンスを大幅に低下させる可能性があります[108、90、111]。ローカルモデルは、非IIDデータのために互いに遠く離れているローカル最適に向かって更新されるため、平均化されたグローバルモデルもグローバル最適から遠くなる可能性があります。挑戦に取り組むために、Li等。 [108] FedProxを提案します。

ローカル更新が多すぎると、平均化されたモデルがグローバル最適値から遠く離れる可能性があるため、FedProxは、ローカル目標に追加の近位項を導入して、ローカル変更の量を制限します。 SCAFFOLD [90]は、ローカル更新のサイズを直接制限する代わりに、分散削減手法を適用してローカル更新を修正します。 FedProxとSCAFFOLDはFedAvgのローカルトレーニング段階を改善しますが、FedNova [190]はFedAvgの集約段階を改善します。各パーティの異種のローカル更新を考慮に入れ、平均化する前にローカル更新に従ってローカルモデルを正規化します。

上記の研究の目的は、非IIDデータ設定の下でトレーニングデータセット全体の損失を最小限に抑えることです。もう1つの解決策は、パーソナライズされた連合学習アルゴリズムを設計することです。このアルゴリズムの目的は、各パーティがローカルデータで適切に実行できるパーソナライズされたモデルを学習することです。 Per-FedAvg [52]は、FedAvgのモデルにとらわれないメタ学習[55]フレームワークの概念を適用します。 pFedMe [46]は、モローエンベロープを使用して、パーソナライズされたモデルの最適化を分解します。 Hanzelyetal。 [69]パーソナライズされた連合学習最適化の通信の複雑さとローカルオラクルの複雑さの下限を確立します。さらに、それらは加速された近接勾配降下（APGD)と加速されたL2SGD + [68]を適用し、最適な複雑さの限界を達成することができます。 IFCA [61]は、パーティがローカルの目的によってクラスターに分割されていることを前提としています。代わりに、クラスターIDを推定しながら、損失関数を最小化するという考え方です。

非IIDデータ設定に関連する別の研究の方向性は、ローカル分布の可能な組み合わせに対して堅牢な連合学習を設計することです。 Mohrietal。 [134]不可知論者FLという名前の新しいフレームワークを提案します。ローカルクライアントからのデータ分布間の平均分布に関する損失を最小限に抑える代わりに、クライアント分布の混合によって形成される可能性のあるターゲット分布に最適化された集中型モデルをトレーニングしようとします。 FedRobust [155]は、構造化されたアフィン分布シフトを考慮しています。分散ミニマックス最適化問題を解くために最急降下法を提案します。

上記の研究はデータの不均一性を考慮していますが、ローカルモデルの不均一性は連合学習にも存在する可能性があります。パーティは、さまざまなアーキテクチャのモデルをトレーニングできます。 FedDF [114]は、知識蒸留[75]を利用してローカルモデルを集約します。サーバー側にパブリックデータセットが存在することを前提としています。これを使用して、ローカルモデルの知識を抽出し、グローバルモデルを更新できます。

SGDベースの垂直連合学習に関する研究はほとんどありません。 [120]垂直FL用のフェデレーションストア派ブロック座標降下（FedBCD)を提案します。座標降下法を適用することにより、各パーティは、中間結果を伝達する前に、複数のラウンドのローカルパラメータを更新します。また、FedBCDの収束分析も提供します。 Huetal。 [78]すべての関係者がラベルを持っていると仮定して、垂直FLのFDMLを提案します。中間結果を交換する代わりに、各参加者からのローカル予測を集約します。

ニューラルネットワーク

ニューラルネットワークはSGDオプティマイザーを使用してトレーニングできますが、モデルアーキテクチャも活用できる場合は、モデルの有用性を高めることができる可能性があります。 Yurochkinetal。 [213]ベイズのノンパラメトリック機構を適用することにより、多層パーセプトロンの確率的連合ニューラルマッチング（PFNM)を開発します[59]。
彼らは、ベータベルヌーイ過程の情報に基づくマッチング手順を使用して、ローカルモデルをフェデレーショングローバルモデルに結合します。実験は、彼らのアプローチがIIDと非IIDの両方のデータ分割でFedAvgを上回ることができることを示しています。

王ら。 [189]は、PFNMをCNN（畳み込みニューラルネットワーク)およびLSTM （長短期記憶ネットワーク)に適用する方法を示しています。さらに、彼らは、モデルアーキテクチャを調査することにより、レイヤーごとのマッチングスキームを備えたFederated Matched Averaging（FedMA)を提案しています。具体的には、一致した平均化を使用して、グローバルモデルのレイヤーを毎回更新します。これにより、通信サイズも削減されます。
実験は、FedMAがCNNおよびLSTMでFedAvgおよびFedProx [108]よりも優れたパフォーマンスを発揮することを示しています。

ニューラルネットワークでの垂直連合学習のもう1つの研究は、分割学習です[184]。 Vepakommaetal 。 [184]は、ニューラルネットワークが2つの部分に分割されているSplitNNという名前の新しいパラダイムを提案しています。
参加する各パーティは、ネットワークのいくつかのレイヤーをトレーニングする必要があります。その後、カットレイヤーでの出力は、ラベルを持っているパーティに送信され、残りのトレーニングを完了します。

木

ニューラルネットワークに加えて、決定木は学術および業界でも広く使用されています[34、92、54、105] 。
NNと比較して、ツリーのトレーニングと推論は非常に効率的です。ただし、ツリーパラメータをSGDで直接最適化することはできません。つまり、SGDベースのFLフレームワークは学習ツリーには適用できません。樹木に特化したフレームワークが必要です。ツリーモデルの中で、勾配ブースティング決定木（GBDT)モデル[34]は非常に人気があります。フェデレーションGBDTに関するいくつかの研究があります。

水平フェデレーションGBDTに関するいくつかの研究があります。趙ら[217] GBDT用の最初のFLSを提案します。それらのフレームワークでは、各決定木は、当事者間のコミュニケーションなしにローカルでトレーニングされます。パーティーで訓練された木は、次のパーティーに送られ、多数の木を継続的に訓練します。
差分プライバシーは、決定木を保護するために使用されます。 Lietal。 [104]局所性鋭敏型ハッシュを使用して、フェデレーションGBDTの構築に類似性情報を活用します[45]。それらは、類似したインスタンスの勾配を集約することにより、ローカルパーティのデータ分散を利用します。安全なマルチパーティ計算と比較して弱いプライバシーモデル内では、それらのアプローチは効果的かつ効率的です。
Liuetal。 [122]モバイルクラウドセンシングのための連合された極端なブースティング学習フレームワークを提案します。彼らは、GBDTのプライバシー保護学習を達成するために秘密共有を採用しました。

Liuetal。 [121]は、垂直FL設定でランダムフォレストをトレーニングできるようにするフェデレーションフォレストを提案します。各ノードの構築では、対応する分割機能を持つ当事者がサンプルを分割し、結果を共有する責任があります。プライバシーを保護するために、通信されたデータを暗号化します。
彼らのアプローチは、非連合バージョンと同じくらい正確です。

チェンら。 [38]垂直FL設定のGBDTのフレームワークであるSecureBoostを提案します。彼らの仮定では、一方の当事者だけがラベル情報を持っています。彼らは、エンティティアラインメント手法を使用して共通データを取得し、決定木を構築しました。勾配を保護するために、さらに準同型暗号化が使用されます。

線形/ロジスティック回帰

線形/ロジスティック回帰は、SGDを使用して実現できます。ここでは、SGDベースではなく、線形/ロジスティック回帰用に特別に設計された研究を示します。

水平FL設定では、Nikolaenkoetal。 [141]プライバシーを保護するリッジ回帰のシステムを提案します。彼らのアプローチは、準同型暗号化と八尾の文字化けした回路の両方を組み合わせて、プライバシー要件を達成します。アルゴリズムを実行するには、追加の評価者が必要です。 Chenetal。 [36]プライバシーを保護するリッジ回帰のシステムを提案します。彼らのアプローチは、安全な合計と準同型暗号化の両方を組み合わせて、プライバシー要件を達成します。彼らは、彼らのアプローチと以前の最先端のアプローチとの間の完全な通信と計算のオーバーヘッドの比較を提供しました。

垂直FL設定では、Saniletal。 [162]安全な回帰モデルを提示します。彼らは線形回帰モデルに焦点を合わせており、ソリューションのプライバシーを確保するために秘密分散が適用されています。ハーディ等。 [72]は、2者間の垂直フェデレーションロジスティック回帰のソリューションを提示します。それらは、エンティティ解決と追加的に準同型暗号化を適用します。

その他

FLを、マルチタスク学習[157]、メタ学習[55]、強化学習[133]、転移学習[147]などの他の機械学習手法と組み合わせた多くの研究があります。

スミス等。 [169] FLとマルチタスク学習を組み合わせる[26、215]。彼らの方法は、フェデレーション環境でのMTLの高い通信コスト、ストラグラー、およびフォールトトレランスの問題を考慮しています。 CorinziaとBuhmann [43]は、非凸モデルを使用したフェデレーションMTLメソッドを提案しています。彼らは中央サーバーとローカルパーティをベイジアンネットワークとして扱い、推論は変分法を使用して実行されます。

Chenetal。 [33] FedAvgの学習プロセスでメタ学習を採用します。ローカルNNをトレーニングしてモデルパラメータを交換する代わりに、当事者はローカルトレーニングでモデルにとらわれないメタ学習（MAML） [55]アルゴリズムを採用し、MAMLの勾配を交換します。江ら。 [81]既存のMAMLアルゴリズムに照らしてFedAvgを解釈します。さらに、彼らは爬虫類アルゴリズム[139]を適用して、FedAvgによってトレーニングされたグローバルモデルを微調整します。彼らの実験は、メタ学習アルゴリズムがグローバルモデルの有効性を向上させることができることを示しています。

Liuetal。 [115]生涯にわたる連合強化学習フレームワークを提案します。伝達学習手法を採用し、強化学習でロボットが学習したことを効果的に記憶するようにグローバルモデルをトレーニングします。

ダイら[44]はFLでのベイズ最適化を考慮しています。彼らは、クライアントの通信効率と異質性に対処するために、フェデレーショントンプソンサンプリングを提案しています。それらのアプローチは、連合学習のパラメーター検索で使用できる可能性があります。

FLのもう1つの問題は、FLプロセス中のパッケージの損失またはパーティの切断です。これは通常、モバイルデバイスで発生します。失敗したメッセージの数が少ない場合、グローバルモデルの更新に小さな重みがあるため、サーバーはそれらを単に無視できます。パーティの障害が重大な場合、サーバーは前のラウンドの結果から再起動できます[24]。有効性を向上させるために、切断の問題に対処するためのより新しいソリューションを楽しみにしています。

概要

上記の研究を以下のように要約します。

- SGDベースのフレームワークが広く研究され、使用されているため、最近、モデルに特化したFLに焦点を当てた研究が増えています。モデルに特化した方法を使用することで、モデルの精度が向上することを期待しています。さらに、研究者がフェデレーションデシジョンツリーモデルについて研究することをお勧めします。ツリーモデルはモデルサイズが小さく、ニューラルネットワークと比較してトレーニングが容易であるため、FLでの通信と計算のオーバーヘッドが低くなる可能性があります。

- FLに関する研究はまだ初期段階です。 ResNeXt [127]やEfficientNet [178]などの最先端のニューラルネットワークをトレーニングするためにFLを適用することについてはほとんど研究が行われていません。複雑な機械学習モデルをトレーニングするための効果的で実用的なアルゴリズムを設計する方法は、依然として挑戦的で進行中の研究の方向性です。

- ほとんどの研究は水平FLに焦点を当てていますが、垂直FL用の十分に開発されたアルゴリズムはまだありません。ただし、垂直フェデレーション設定は、複数の組織が関与する実際のアプリケーションでは一般的です。この有望な分野でのさらなる研究を楽しみにしています。

4.2.2通信効率

FLの計算は、ハイパフォーマンスコンピューティングコミュニティ[197、199]で最新のハードウェアと技術[123、101、102]を使用して高速化できますが、FLの研究は、主にFLプロセス中の通信サイズの削減に取り組んでいます。 [95] Konecn ˇ y et al。を減らすために、構造化された更新とスケッチされた更新の2つの方法を提案します。フェデレーション平均化における通信サイズ。構造化された更新の場合、ユーザーは、制限されたパラメーターを使用して更新の構造を制限します。スケッチされた更新の場合、ユーザーは、更新を送信する前に、ランダムな回転、量子化、および可変長コーディングを使用して更新を圧縮します。学習プロセスの各ラウンドにおける通信コストを削減します。

彼らの方法は、収束速度をわずかに低下させながら、通信コストを2桁削減することができます。 ZhuとJin [226]は、通信コストとグローバルモデルテストエラーを同時に最小化するための多目的進化的アルゴリズムを設計しています。通信コストの最小化とグローバル学習精度の最大化を2つの目的として、FLを二目的最適化問題として定式化し、多目的進化的アルゴリズムで解きました。チョン他[79]非IIDローカルデータを持つデバイスのためのFLフレームワークを提案します。彼らは、通信サイズが出力寸法に依存するがモデルサイズには依存しない連合蒸留を設計します。また、彼らは、生成的敵対的ネットワーク（GAN)を使用して、トレーニングデータセットをIIDにするデータ拡張スキームを提案しています。他の多くの研究も、非IIDデータの特殊なアプローチを設計しています[221、111、118、210]。 Sattleretal。 [164]は、スパース三項圧縮（STC)という名前の新しい圧縮フレームワークを提案します。具体的には、STCは、スパース化、3値化、エラー累積、および最適なゴロム符号化を使用して通信を圧縮します。彼らの方法は、非IIDデータと多数の関係者に対してロバストです。

通信サイズに加えて、通信アーキテクチャを改善してトレーニング効率を高めることもできます。 Marfoqetal。 [128]クロスサイロ連合学習のトポロジー設計を検討してください。
彼らは、トレーニング時間を大幅に短縮できるスループット最適トポロジを見つけるためのアプローチを提案しています。

4.2.3プライバシー、堅牢性、攻撃

元のデータはFLで交換されませんが、モデルパラメータはトレーニングデータに関する機密情報を漏らす可能性もあります[167、137、196]。したがって、交換されたローカル更新に対してプライバシー保証を提供することが重要です。

差分プライバシーは、プライバシーを保証するための一般的な方法です。 Geyeretal。 [60]クライアントレベルの観点から、フェデレーション平均化に異なるプライバシーを適用します。ガウスメカニズムを使用して勾配の更新の合計を歪め、単一のデータポイントではなくクライアントのデータセット全体を保護します。
マクマハン等。 [130] LSTMのトレーニングでフェデレーション平均を展開します。また、クライアントレベルの差分プライバシーを使用してパラメータを保護します。 Bhowmicketal。 [20] FLのパラメータを保護するために、ローカル差分プライバシーを適用します。モデルの品質を向上させるために、彼らは、個人のデータをデコードしたいが、それらに関する事前情報がほとんどない実用的な脅威モデルを検討します。この仮定の範囲内で、彼らはプライバシー予算をより有効に活用することができます。

Bonawitzetal。 [23]安全なマルチパーティ計算を適用して、フェデレーション平均に基づいてローカルパラメータを保護します。具体的には、秘密分散に基づいてベクトルの合計を安全に計算するための安全な集約プロトコルを提示します[165]。また、差分プライバシーと安全な集約を組み合わせる方法についても説明します。

Truexetal。 [181]プライバシーを保護するFLのために、安全なマルチパーティ計算と差分プライバシーの両方を組み合わせます。差分プライバシーを使用して、ローカルアップデートにノイズを注入します。次に、ノイズの多い更新は、中央サーバーに送信される前にPaillier暗号システム[146]を使用して暗号化されます。

FLへの攻撃の場合、一般的な攻撃の1つにバックドア攻撃があります。これは、悪意のあるローカル更新を交換することにより、不正なグローバルモデルを実現することを目的としています。

Bagdasaryanetal。 [16] FLに対してモデル中毒攻撃を行います。悪意のある当事者は、攻撃モデルをサーバーにコミットして、グローバルモデルがポイズニングされたデータに過剰適合する可能性があります。安全なマルチパーティ計算は、その機密性を保護することを目的としているため、このような攻撃を防ぐことはできません。

モデルパラメータ。 Bhagojietal。 [19] FLに対するモデル中毒攻撃も研究しています。平均化ステップは悪意のあるモデルの影響を減らすため、コミットされた重みの更新を増やすために明示的なブースト方法を採用します。 Sunetal。 [174]実験を実施して、連合EMNISTデータセットで連合学習のバックドア攻撃と防御を評価し、敵のパフォーマンスに影響を与える可能性のある要因を確認します。彼らは、防御がない場合、攻撃のパフォーマンスは、提示された敵の割合と対象となるタスクの「複雑さ」に大きく依存することを発見しました。バックドアタスクが多ければ多いほど、メインタスクのパフォーマンスを維持しながら固定容量モデルをバックドアするのは難しくなります。王ら。 [188]理論的な観点からバックドア攻撃について議論し、 FLで実行可能であることを証明します。彼らはまた、現在の防御方法に耐性のあるエッジケースバックドアと呼ばれる新しいクラスのバックドア攻撃を提案しています。 Xieetal。 [203] FLに対する分散型バックドア攻撃を提案します。これらは、グローバルトリガーパターンをローカルパターンに分解します。各敵対者は、1つのローカルパターンのみを採用しています。実験は、分散型バックドア攻撃が中央バックドア攻撃よりも優れていることを示しています。

別の種類の攻撃はビザンチン攻撃です。この攻撃では、攻撃者が認証されたデバイスを完全に制御し、ネットワークを妨害するために任意に動作します。 Krum [21]やBulyan [132]など、分散学習にはいくつかの既存の堅牢な集計ルールがあります。これらのルールは、連合学習に直接適用できます。ただし、各当事者が連合学習で複数のローカル更新手順を実行するため、連合学習でのビザンチンの攻撃と防御を調査することは興味深いことです。 Lietal。 [100]非IIDデータ設定での連合学習のためのビザンチンロバストな確率的集約方法であるRSAを提案します。 Fangetal。 [53]ビザンチンに強い連合学習アプローチのためのモデル毒攻撃を提案する。

彼らのアプローチの目標は、グローバルモデルが正しい更新方向の逆に最も大きく逸脱するようにローカルモデルを変更することです。

FL攻撃に関するもう1つの研究は、推論攻撃です。一元化された設定でトレーニングされた機械学習モデルに対する推論攻撃[56、167、137]に関する既存の研究があります。フェデレーション設定については、Geipingetal。 [58]は、交換された勾配の知識からトレーニング画像を再構成することが可能であることを示しています。

4.2.4公平性とインセンティブメカニズム

FedAvgに基づいて公平性を考慮に入れることによって、Li等。 [110] q-FedAvgを提案します。具体的には、当事者のモデルのパフォーマンスの分散に従って公平性を定義します。そのような分散が小さければ、モデルはより公平になります。したがって、彼らはα-公平性に触発された新しい目的を設計します[13]。フェデレーション平均に基づいて、彼らは新しい目的を解決するためにq-FedAvgを提案します。 q-FedAvgとFedAvgの主な違いは、モデルパラメーターを更新する式にあります。

キムら[93]ブロックチェーンアーキテクチャとFLを組み合わせます。フェデレーション平均に基づいて、ブロックチェーンネットワークを使用して、デバイスのローカルモデルの更新を交換します。これは、中央サーバーよりも安定しており、デバイスに報酬を提供できます。カンら。 [87]は、マルチウェイト主観的論理モデルを使用して、信頼できるFLのための評判ベースの労働者選択スキームを設計しました。また、ブロックチェーンを活用して、否認防止性と改ざん防止性を備えたワーカーの安全な評判管理を分散化して実現します。

概要

上記のレビューによると、セクション4.2.2からセクション4.2.4の調査を次のように要約します。

- 有効性に加えて、効率とプライバシーはFLSの他の2つの重要な要素です。これらの3つの分野と比較すると、公平性とインセンティブのメカニズムに関する研究はほとんどありません。現実の世界でFLの使用を促進できる公平性とインセンティブメカニズムに関するさらなる研究を楽しみにしています。

- FLSの効率を向上させるために、通信のオーバーヘッドは依然として主要な課題です。
  ほとんどの研究[95、79、164]は、各反復の通信サイズを縮小しようとしています。合理的にする方法

通信ラウンド数の設定も有望です[226]。計算と通信の間のトレードオフは、さらに調査する必要があります。

- プライバシーを保証するために、差分プライバシーと安全なマルチパーティ計算は2つの一般的な手法です。ただし、差分プライバシーはモデルの品質に大きな影響を与える可能性があり、安全なマルチパーティ計算には非常に時間がかかる可能性があります。強力なプライバシー保証を備えた実用的なFLSを設計することは依然として困難です。また、中毒攻撃に対する効果的な堅牢なアルゴリズムはまだ広く採用されていません。

4.2.5アプリケーション

FLに関連する領域の1つは、エッジコンピューティング[140、212、153、47、218]であり、パーティはエッジデバイスです。
多くの研究は、FLをモバイルエッジシステムと統合しようとしています。 FLはまた、レコメンダーシステム[14、29、225]、自然言語処理[71] 、およびトランザクション不正検出[222]で有望な結果を示しています。

エッジコンピューティング

西尾と米谷[143]は、実用的なモバイルエッジコンピューティング（MEC)フレームワークにフェデレーション平均を実装しています。彼らは、MEC framworksのオペレーターを使用して、異種クライアントのリソースを管理します。
王ら。 [194]モバイルエッジコンピューティングシステムで分散深層強化学習（DRL)と連邦学習の両方を採用します。 DRLとFLを使用すると、モバイルエッジのコンピューティング、キャッシング、および通信を効果的に最適化できます。王ら。 [192]リソースに制約のあるMECシステムでFLを実行します。それらは、エッジで限られた計算および通信リソースを効率的に利用する方法の問題に対処します。フェデレーション平均を使用して、線形回帰、SVM、CNNなどの多くの機械学習アルゴリズムを実装します。彼等。 [73]は、エッジデバイスの限られたコンピューティングリソースも考慮します。彼らはFedGKTを提案します。この場合、各デバイスはResNet全体のごく一部のみをトレーニングして、計算のオーバーヘッドを削減します。

レコメンダーシステム

Ammad-ud dinetal。 [14]最初の統合協調フィルター法を策定します。確率的勾配アプローチに基づいて、アイテムファクターマトリックスは、ローカル更新を集約することにより、グローバルサーバーでトレーニングされます。
彼らは経験的に、フェデレーション方式は集中方式と比較して精度の低下がほとんどないことを示しています。チャイ他[29]フェデレーション行列因数分解フレームワークを設計します。彼らは、フェデレーションSGDを使用して行列を学習します。さらに、通信された勾配を保護するために準同型暗号化を採用しています。
タンら。 [177] FATEに基づいてフェデレーションレコメンダーシステム（FedRecSys)を構築します。 FedRecSysは、SMCプロトコルを使用して一般的なレコメンデーションアルゴリズムを実装しています。アルゴリズムには、行列因数分解、特異値分解、因数分解マシン、および深層学習が含まれます。

自然言語処理

Hardetal。 [71]モバイルキーボードの次の単語の予測にFLを適用します。彼らは連合平均法を採用して、結合入力と忘れゲート（CIFG）と呼ばれるLSTMの変形を学習します[65]。 FL法は、ログデータを使用したサーバーベースのトレーニングよりも高い適合率の再現率を実現できます。

トランザクション不正の検出

Zhengetal。 [222]クレジットカード取引の不正検出の分野にFLを導入します。彼らは、データのプライバシーを保証するだけでなく、既存のアプローチと比較して大幅に高いパフォーマンスを実現する、ディープKタプレットネットワークと呼ばれる新しいメタ学習ベースの連合学習フレームワークを設計します。

概要

上記の研究によると、以下の要約があります。

- エッジコンピューティングは、当然、クロスデバイスフェデレーション設定に適合します。 FLをエッジコンピューティングに適用する際の重要な問題は、エッジリソースを効果的に利用および管理する方法です。 FLを使用すると、特にモバイルデバイスサービスを改善するために、ユーザーにメリットをもたらすことができます。
- FLは、画像分類や作業予測など、多くの従来の機械学習タスクを解決できます。規制と「データアイランド」により、今後数年間はフェデレーション設定が一般的な設定になる可能性があります。 FLの急速な発展に伴い、コンピュータービジョン、自然言語処理、およびヘルスケアでのアプリケーションが増えると考えています。

4.2.6ベンチマーク

ベンチマークは、FLSの開発を指示するために重要です。最近、複数のベンチマーク関連の作業が実施されており、いくつかのベンチマークフレームワークがオンラインで利用できます。それらを3つのタイプに分類します。1)汎用ベンチマークシステムは、FLSを包括的に評価し、FLSのさまざまな側面の詳細な特性を提供することを目的としています。 2)ターゲットベンチマークは、小さなドメインに集中し、そのドメインのシステムのパフォーマンスを最適化しようとする1つ以上の側面を対象としています。 3）
データセットベンチマークは、連合学習専用のデータセットを提供することを目的としています。

汎用ベンチマークシステム

FedML [74]は、連合学習とベンチマーク機能の両方のフレームワークを提供する研究図書館です。ベンチマークとして、FedAvg、FedNAS、Vertical FL、分割学習など、複数のMLモデルとFLアルゴリズムの包括的なベースライン実装を提供します。さらに、分散トレーニング、モバイルオンデバイストレーニング、スタンドアロンシミュレーションの3つのコンピューティングパラダイムをサポートします。その実験結果のいくつかは現在まだ準備段階にありますが、それはその機能性に関する最も包括的なベンチマークフレームワークの1つです。

FedEval [30]は、連合学習のもう1つの評価モデルです。これは、「ACTPR」モデルを特徴としています。つまり、評価対象として、精度、通信、時間の消費、プライバシー、および堅牢性を使用します。 Dockerコンテナーを利用して、ハードウェアリソース制限の問題を回避するための分離された評価環境を提供し、実装で最大100のクライアントをシミュレートします。現在、FedSGDとFedAvgの2つの水平アルゴリズムがサポートされており、MLPとLeNetを含むモデルがテストされています。

OARF [77]は、FLベンチマーク用の一連のユーティリティとリファレンス実装を提供します。これは、FLアルゴリズム、暗号化メカニズム、プライバシーメカニズム、通信方法など、FLSのさまざまなコンポーネントの測定を特徴としています。さらに、さまざまなソースから収集された公開データセットを利用して実際のデータ分布を反映する、データセットの現実的なパーティション化も特徴としています。両方の水平垂直アルゴリズムがテストされます。

Edge AIBench [70]は、連合学習アプリケーションのテストベッドを提供し、リファレンス実装として4つのアプリケーションシナリオをモデル化します。ICU患者モニター、監視カメラ、スマートホーム、自動運転車です。実装はオープンソースですが、現在実験結果は報告されていません。

ターゲットベンチマーク

Nilssonetal。 [142]は、相関t検定を利用して、データ分布の影響を回避しながら、さまざまなタイプの連合学習アルゴリズムを比較する方法を提案しています。 3つのFLアルゴリズム、 FedAvg、FedSVRG [95] 、およびCO-OP [195]は、作業中のIIDと非IIDの両方のセットアップで比較され、その結果は、FedAvgが、データの方法に関係なく、3つのアルゴリズムの中で最高の精度を達成することを示しています。パーティション化されています。

Zhuangetal。 [227]ベンチマーク分析を利用して、連合者の再識別のパフォーマンスを改善します。ベンチマーク部分では、9つの異なるデータセットを使用して実際の状況をシミュレートし、参照実装として、部分的に異なるモデルの集約を可能にするアルゴリズムであるフェデレーション部分平均を使用します。

張ら。 [216]半教師あり連合学習設定を対象としたベンチマークを提示します。この場合、ユーザーにはラベルのないデータしかなく、サーバーにはラベルの付いたデータが少量しかありません。また、最終的なモデルの精度と複数の指標との関係を調査します。データ、アルゴリズムと通信設定、およびクライアントの数。実験結果を利用して、彼らの半教師あり学習の改善された方法は、より良い一般化パフォーマンスを達成します。

Liuetal。 [117]データセットが参加者間で不均一に分布している非IID問題に焦点を当てます。彼らの研究は、データ分布の歪度を定量的に説明する方法を探求し、いくつかの非IIDデータセット生成アプローチを提案しています。

データセット

LEAF [25]は、連合学習のための最も初期のデータセット提案の1つです。これには、画像分類、感情分析、次のキャラクターの予測など、さまざまなドメインをカバーする6つのデータセットが含まれています。データセットをIIDまたは非IIDの方法で異なるパーティに分割するための一連のユーティリティが提供されています。データセットごとに、トレーニングプロセスでのそのデータセットの使用法を示すためのリファレンス実装も提供されます。

羅ら[124] 26の異なる道路監視カメラから収集された実世界の画像データセットを提示します。
そのデータセット内の画像には、7つの異なるカテゴリのオブジェクトが含まれており、オブジェクト検出タスクに適しています。参照として、YOLOv3モデルとFasterR-CNNモデルを実行するフェデレーション平均を使用した実装が提供されています。

概要

上記の研究を要約すると、次の発見があります

- ベンチマークは、連合学習の開発において重要な役割を果たします。さまざまな種類のベンチマークを通じて、連合学習のさまざまなコンポーネントと側面を定量的に特徴付けることができます。連合学習におけるセキュリティとプライバシーの問題に関するベンチマークはまだ初期段階であり、さらなる開発が必要です。

- 現在、FLSのすべてのアルゴリズムまたはアプリケーションタイプをカバーするのに十分な包括的なベンチマークシステムは実装されていません。最も包括的なベンチマークシステムでさえ、システムの各レベルの特定のアルゴリズムと評価メトリックのサポートが不足しています。包括的なベンチマークシステムをさらに開発するには、広範なFLフレームワークのサポートが必要です。

- ほとんどのベンチマーク調査では、単一のデータセットから分割されたデータセットを使用しており、どのタイプの分割方法を使用するかについてのコンセンサスはありません。同様に、非IID問題に関しては、非IID性のメトリックに関するコンセンサスはありません。 FedML [74]およびOARF [77]で提案されているように、現実的な分割方法を使用すると、この問題を軽減できる可能性がありますが、大規模な連合学習では、異なるデータを収集することが難しいため、現実的な分割は適していません。
  ソース。

4.3オープンソースシステム

このセクションでは、5つのオープンソースFLSを紹介します：Federated AI Technology Enabler（FATE)3、Google TensorFlow Federated（TFF)4、OpenMined PySyft5、 BaiduPaddleFL6およびFedML7 。

[3] https://github.com/FederatedAI/FATE
[4] https://github.com/tensorflow/federated
[5] https://github.com/OpenMined/PySyft
[6] https://github.com/PaddlePaddle/PaddleFL
[7] https://github.com/FedML-AI/FedML

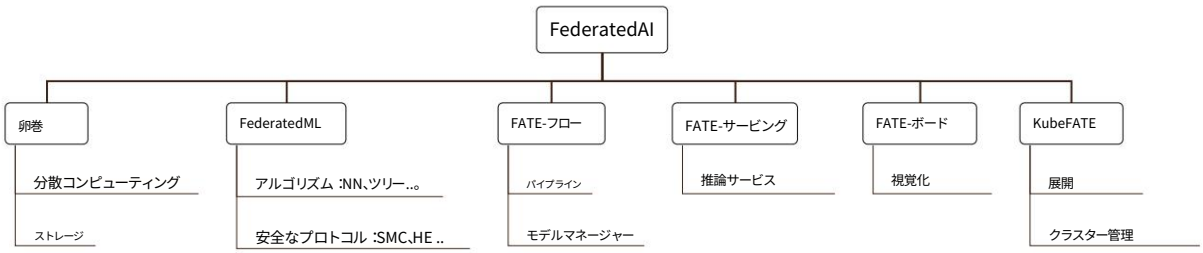


図4 :FATEシステム構造

4.3.1運命

FATEは、WeBankによって開発された産業レベルのFLフレームワークであり、さまざまな組織間でFLサービスを提供することを目的としています。 FATEはPythonに基づいており、LinuxまたはMacにインストールできます。 GitHubには約3.2kの星と900のフォークが集まっています。 FATEの全体的な構造を図4に示します。これには、EggRoll、FederatedML、FATE-Flow、FATE-Serving、FATE-Board、およびKubeFATEの6つの主要なモジュールがあります。 EggRollは、分散コンピューティングとストレージを管理します。他のモジュールにコンピューティングおよびストレージAIPを提供します。 FederatedMLには、フェデレーションアルゴリズムと安全なプロトコルが含まれています。
現在、 NN、GBDT、ロジスティック回帰など、水平および垂直の両方のフェデレーション設定でさまざまな種類の機械学習モデルのトレーニングをサポートしています。 FATEは、当事者が正直であるが好奇心が強いことを前提としています。したがって、安全なマルチパーティ計算と準同型暗号化を使用して、通信されるメッセージを保護します。ただし、最終モデルを保護するための差分プライバシーはサポートされていません。
FATE-Flowは、ユーザーがFLプロセスのパイプラインを定義するためのプラットフォームです。パイプラインには、データの前処理、フェデレーショントレーニング、フェデレーション評価、モデル管理、およびモデル公開を含めることができます。 FATE-Servingは、ユーザーに推論サービスを提供します。 FLモデルのロードとオンライン推論の実行をサポートします。 FATE-BoardはFATEの視覚化ツールです。これは、ジョブの実行とモデルのパフォーマンスを視覚的に追跡する方法を提供します。最後に、KubeFATEは、DockerまたはKubernetesを使用してクラスターにFATEをデプロイするのに役立ちます。カスタマイズされた展開およびクラスター管理サービスを提供します。一般的に、FATEは強力で使いやすいFLSです。ユーザーは、パラメーターを設定するだけでFLアルゴリズムを実行できます。さらに、FATEは、その展開と使用法に関する詳細なドキュメントを提供します。ただし、 FATEはアルゴリズムレベルのインターフェイスを提供するため、実践者はFATEのソースコードを変更して独自のフェデレーションアルゴリズムを実装する必要があります。これは、専門家でないユーザーにとっては簡単ではありません。

4.3.2 TFF

Googleによって開発されたTFFは、TensorFlowに基づくFLのビルディングブロックを提供します。 GitHubには約1.5kの星と380のフォークが集まっています。 TFFは、簡単にインストールおよびインポートできるPythonパッケージを提供します。図5に示すように、FLAPIとFederatedCore （FC)APIという異なるレイヤーの2つのAPIを提供します。 FL APIは、高レベルのインターフェースを提供します。これには、モデル、フェデレーション計算ビルダー、およびデータセットの3つの主要部分が含まれます。 FL APIを使用すると、ユーザーはモデルを定義したり、Keras [66]モデルをロードしたりできます。フェデレーション計算ビルダーには、一般的なフェデレーション平均化アルゴリズムが含まれています。また、FL APIは、FLのローカルデータセットにアクセスして列挙するためのシミュレートされたフェデレーションデータセットと関数を提供します。 FC APIには、高レベルのインターフェイスに加えて、 FLプロセスの基盤として低レベルのインターフェイスも含まれています。開発者は、フェデレーションコア内に機能とインターフェイスを実装できます。最後に、 FCはFLの構成要素を提供します。これは、フェデレーションサム、フェデレーションリデュース、フェデレーションブロードキャストなどの複数のフェデレーション演算子をサポートします。開発者は、 FLアルゴリズムを実装するための独自の演算子を定義できます。全体として、TFFは、開発者が新しいFLアルゴリズムを設計および実装するための軽量システムです。現在、TFFはFLトレーニング中に敵を考慮することを考慮していません。プライバシーメカニズムは提供しません。 TFFは現在、単一のマシンにのみ展開でき、フェデレーション設定はシミュレーションによって実装されています。

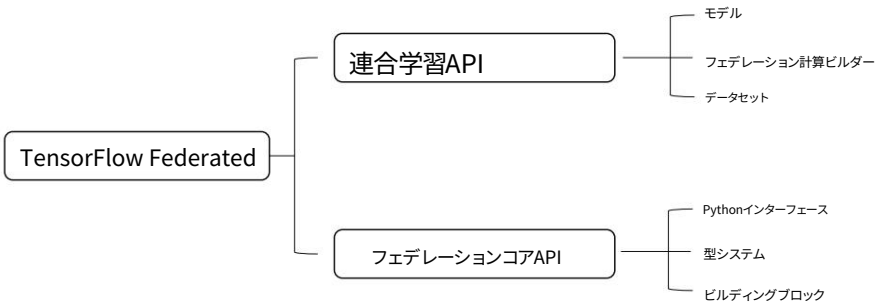


図5 :TFFシステム構造

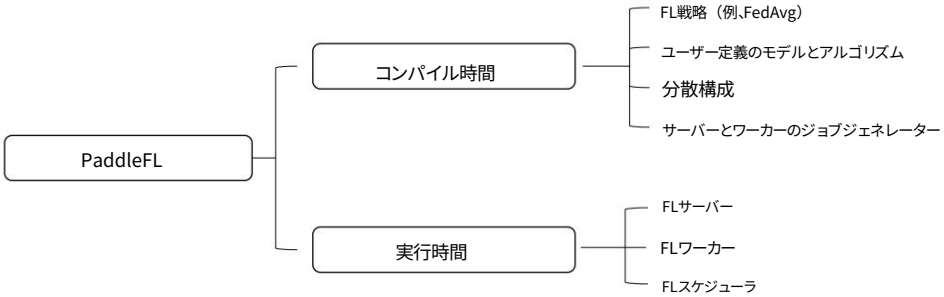


図6 :PaddleFLシステム構造

4.3.3 PySyft

PySyft、Ryffelらによって最初に提案されました。 [158]そしてOpenMinedによって開発された、開発者がトレーニングアルゴリズムを実装するためのインターフェースを提供するPythonライブラリです。 GitHubには約7.3kのスターと1.7kのフォークが集まっています。 TFFはTensorFlowに基づいていますが、PySyftはPyTorchとTensorFlowの両方でうまく機能します。 PySyftは、安全なマルチパーティ計算や差分プライバシーなど、複数のオプションのプライバシーメカニズムを提供します。したがって、正直だが好奇心旺盛なパーティーでの実行をサポートできます。さらに、単一のマシンまたは複数のマシンにデプロイでき、異なるクライアント間の通信はWebSocketAPIを介して行われます[168]。ただし、PySyftは一連のチュートリアルを提供していますが、そのインターフェイスとシステムアーキテクチャに関する詳細なドキュメントはありません。

4.3.4 PaddleFL

PaddleFLは、PaddlePaddle[8]に基づくFLSです。 、これは、Baiduによって開発された深層学習プラットフォームです。これはC++とPythonで実装されています。 GitHubには約260個の星と60個のフォークが集まっています。 PySyftと同様に、PaddleFLは差分プライバシーと安全なマルチパーティ計算の両方をサポートし、正直だが好奇心旺盛なパーティで機能します。 PaddleFLのシステム構造を図6に示します。コンパイル時には、FL戦略、ユーザー定義のモデルとアルゴリズム、分散トレーニング構成、およびFLジョブジェネレーターを含む4つのコンポーネントがあります。 FL戦略には、 FedAvgなどの水平FLアルゴリズムが含まれます。垂直FLアルゴリズムは将来統合される予定です。提供されているFL戦略に加えて、ユーザーは独自のモデルとトレーニングアルゴリズムを定義することもできます。分散トレーニング構成は、分散設定でトレーニングノード情報を定義します。 FLジョブジェネレーターは、フェデレーションサーバーとワーカーのジョブを生成します。実行時には、FLサーバー、FLワーカー、およびFLスケジューラーを含む3つのコンポーネントがあります。サーバーとワーカーは、それぞれFLのマネージャーとパーティです。スケジューラーは、各ラウンドのトレーニングに参加するワーカーを選択します。現在、PaddleFLの開発はまだ初期段階であり、ドキュメントと例は十分に明確ではありません。

[8] https://github.com/PaddlePaddle/Paddle

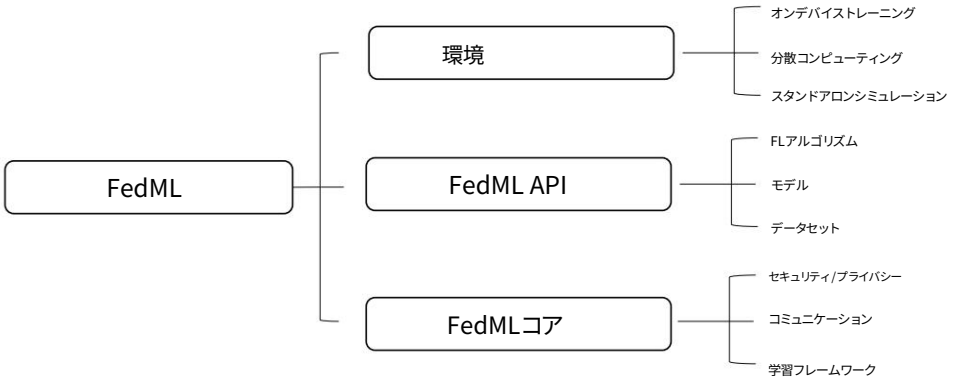


図7 :FedMLシステム構造

4.3.5 FedML

FedMLは、連合学習のフレームワークとFLベンチマークのプラットフォームの両方を提供します。これは、PyTorchに基づいて南カリフォルニア大学[74]のチームによって開発されました。 FedMLは、GitHubで約660個のスターと180個のフォークを集めています。 FLフレームワークとして、そのコア構造は、図7に示すように、2つのレベルに分割されます。低レベルのFedMLコアには、トレーニングエンジンと分散通信インフラストラクチャが実装されています。高レベルのFedML-APIはそれらの上に構築され、トレーニングモデル、データセット、およびFLアルゴリズムを提供します。参照アプリケーション/ベンチマークの実装は、FedML-APIの上にさらに構築されています。 FedMLに実装されているほとんどのアルゴリズムは敵対者を考慮していませんが、当事者からのメッセージを集約するときに差分プライバシーの適用をサポートしています。 FedMLは、スタンドアロンシミュレーション、分散コンピューティング、オンデバイストレーニングの3つのコンピューティングパラダイムをサポートしており、幅広いハードウェア要件に対応するシミュレーション環境を提供します。サポートされているすべてのFLアルゴリズムのリファレンス実装が提供されています。いくつかの実験結果と最適な結果の間にはまだギャップがありますが、それらはさらなる開発のための有用な情報を提供します。

4.3.6その他

他にもクローズドソースの連合学習システムがあります。 NVIDIAClaraの集中型アーキテ[9] FLを有効にしました。それは採用しますクチャと暗号化された通信チャネル。 Clara FLの対象ユーザーは、病院と医療機関です。 Ping An Technologyは、金融業界を対象としたHive [2]という名前の連合学習システムの構築を目指しています。 Clara FLはAPIとドキュメントを提供していますが、Hiveの公式ドキュメントは見つかりません。

4.3.7まとめ

全体として、FATE、PaddleFL、およびFedMLは、ユーザーが直接使用できるアルゴリズムレベルのAPIを提供しようとしますが、 TFFおよびPySyftは、開発者がFLプロセスを簡単に実装できるように、より詳細なビルディングブロックを提供しようとします。表2に、オープンソースシステム間の比較を示します。アルゴリズムレベルでは、FATEは、水平設定と垂直設定の両方で多くの機械学習モデルをサポートする最も包括的なシステムです。 TFFとPySyftは、セクション4.2に示すように、FLの基本的なフレームワークであるFedAvgのみを実装します。 PaddleFLは、現在NNおよびロジスティック回帰で使用されているいくつかの水平FLアルゴリズムをサポートしています。 FedMLは、FedOpt [154]やFedNova [190]などのいくつかの最先端のFLアルゴリズムを統合しています。 FATE、TFF、およびFedMLと比較して、PySyftおよびPaddleFLはより多くのプライバシーメカニズムを提供します。 PySyftは、TFFがサポートするリストされたすべての機能をカバーしますが、TFFはTensorFlowに基づいており、PySyftはPyTorchでより適切に機能します。 GitHubでの人気に基づくと、PySyftは現在、機械学習コミュニティで最も影響力のある連合学習システムです。

[9] https://developer.nvidia.com/clara

表2 :いくつかの既存のFLS間の比較。この表で使用されている表記は、
表1.システムが対応する機能をサポートしていない場合、セルは空のままになります。ありません
FedMLのリリースバージョン。

サポートされている機能		FATE 1.5.0	TFF 0.1	7.0 PySyft 0.3.0	PaddleFL 1.1.0	FedML	
オペレーティングシステム		✓✓		✓✓	✓✓✓✓✓✓		✓✓
							✓✓
	MacLinuxWindows						✓✓
	iOS						✓✓
	アンドロイド						✓✓
データ分割	水平	✓✓		✓✓	✓✓	✓✓	✓✓
	垂直	✓✓				✓✓	✓✓
モデル	NN	✓✓		✓✓	✓✓	✓✓	✓✓
	DT	✓✓					
	LM	✓✓		✓✓	✓✓	✓✓	✓✓
プライバシーメカニズム	DP			✓✓	✓✓	✓✓	✓✓
	CM	✓✓			✓✓	✓✓	
コミュニケーション	シミュレート	✓✓		✓✓	✓✓	✓✓	✓✓
	配布	✓✓			✓✓	✓✓	✓✓
ハードウェア	CPU	✓✓		✓✓	✓✓	✓✓	✓✓
	GPU			✓✓	✓✓		✓✓

5システム設計

図8は、FLSの設計で考慮する必要のある要素を示しています。ここで有効性、効率、
とプライバシーはFLSの3つの重要な指標であり、これらは連合の主要な研究の方向性でもあります。
学ぶ。連合データベース[166]に触発されて、私たちは自律性も考慮します。
FLSは実用的です。次に、これらの要因について詳しく説明します。

5.1有効性

FLSのコアは、（複数の）効果的なアルゴリズム（アルゴリズム）です。アルゴリズムを決定するには
表1に示すように、多くの既存の調査から実装され、最初にデータの分割を確認する必要があります
パーティーの。当事者が同じ機能を持っているがサンプルが異なる場合は、FedAvg [129]を使用して
樹木用のNNとSimFL [104] 。当事者が同じサンプルスペースを持っているが機能が異なる場合、
NNにはFedBCD[120]を使用し、ツリーにはSecureBoost[38]を使用します。

5.2プライバシー

FLSの重要な要件は、ユーザーのプライバシーを保護することです。ここでは、の信頼性を分析します
マネジャー。マネージャーが正直で好奇心がない場合は、追加の手法を採用する必要はありません。
FLフレームワークは、生データが交換されないことを保証するためです。マネージャーが正直だが好奇心が強い場合は、
次に、考えられる推論攻撃を考慮に入れる必要があります。モデルパラメータも公開する可能性があります
トレーニングデータに関する機密情報。差分プライバシー[60、40、130]を採用して注入することができます
パラメータにランダムノイズを入れるか、SMC [22、72、23]を使用して暗号化されたパラメータを交換します。の場合
マネージャはまったく信頼できないため、信頼できる実行環境[37]を使用してコードを実行できます。
マネージャーで。ブロックチェーンは、マネージャーとしての役割を果たすためのオプションでもあります[93]。

5.3効率

効率は、XGBoost [34]や
ThunderSVM [198]。連合学習には複数ラウンドのトレーニングとコミュニケーションが含まれるため、
計算と通信のコストが高くなる可能性があり、FLSの使用のしきい値が高くなります。に

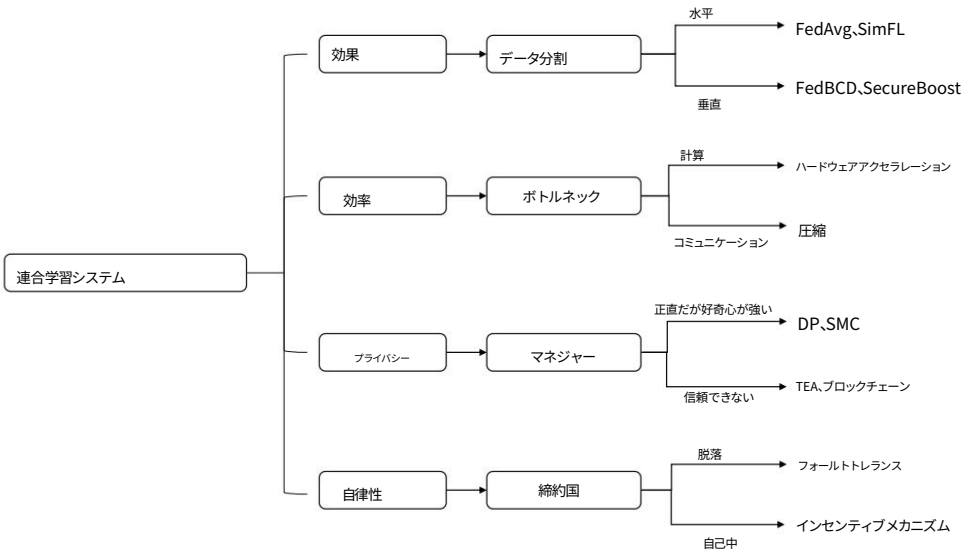


図8 :FLSの設計要素

効率を上げるには、最も効果的な方法はボトルネックに対処することです。ボトルネックが計算にある場合は、GPU [42]やTPU [83]などの強力なハードウェアを使用できます。ボトルネックが通信にある場合は、圧縮技術[18、95、164]を適用して通信サイズを縮小できます。

5.4自律性

連合データベース[166]のように、実際のFLSは当事者の自律性を考慮しなければなりません。特に規模が大きく、当事者の信頼性が低いクロスデバイス設定では、FLプロセス中に当事者が脱落する可能性があります（ネットワーク障害など） [85]。したがって、FLSは堅牢で安定している必要があります。これにより、当事者の障害を許容したり、障害の数を減らしたりすることができます。 Googleは実用的なFLSを開発しました[24]。彼らのシステムでは、デバイスのバッテリーや帯域幅を浪費しないように、デバイスのヘルス統計を監視しています。
また、障害が発生した場合、システムは現在のラウンドを完了するか、以前にコミットされたラウンドの結果から再起動します。張ら。 [214]は、デバイスの切断を検出するためのブロックチェーンベースのアプローチを提案しています。ロバストで安全な集約[17]は、パーティが脱落した場合に通信メッセージを保護するために適用できます。切断の問題に加えて、当事者は利己的であり、モデルを高品質で共有することをいとわない可能性があります。インセンティブメカニズム[87、88]は、当事者の参加を促し、最終的なモデルの品質を向上させることができます。

5.5デザインリファレンス

セクション3に示した分類法と図8に示した設計要素に基づいて、FLSを開発するための簡単な設計リファレンスを導き出します。

最初のステップは、システム設計に大きな影響を与える参加エンティティとタスクを特定することです。参加するエンティティは、通信アーキテクチャ、データパーティショニング、およびフェデレーションの規模を決定します。タスクは、トレーニングするのに適した機械学習モデルを決定します。次に、上記の属性と表1に従って、適切なFLアルゴリズムを選択または設計できます。FLアルゴリズムを修正した後、プライバシー要件を満たすために、通信されるメッセージを保護するためのプライバシーメカニズムを決定する場合があります。 SMCと比較してモデルのパフォーマンスよりも効率が重要な場合は、DPが推奨されます。最後に、システムを強化するためのインセンティブメカニズムを検討することができます。既存のシステム[74、24]は通常、インセンティブメカニズムをサポートしていません。ただし、インセンティブメカニズムは、当事者がシステムに参加して貢献することを奨励し、システムをより魅力的にすることができます。

シャープレイ値[193、187]は、考慮できる公正なアプローチです。

表3 :実際のフェデレーションシステムの要件

システムの側面	モバイルサービス	健康管理	金融
データ分割	水平分割ハイブリッド分割垂直分割		
機械学習モデル	特定のモデルなし特定のモデルなし特定のモデルなし		
連盟の規模	クロスデバイス	クロスサイロ	クロスサイロ
通信アーキテクチャ	一元化	分散	分散
プライバシーメカニズム	DP	DP / SMC	DP / SMC
連盟の動機	インセンティブ動機	ポリシーに動機付け	興味の動機

連合学習システムの実際のアプリケーションについては、補足資料のセクション4を参照してください。

5.6評価

FLSの評価は非常に困難です。調査したシステム要因によると、
次の側面：（1)モデルのパフォーマンス、（2)システムのセキュリティ、（3)システムの効率、および（4)システム
堅牢性。

モデルの評価には、2つの異なる設定があります。 1つはパフォーマンスを評価することです
（たとえば、予測精度)グローバルデータセットの最終的なグローバルモデル。もう1つは、
対応する非IIDローカルデータセットでの最終ローカルモデルのパフォーマンス。評価設定
FLの目的、つまり、グローバルモデルを学習するか、パーソナライズされたローカルモデルを学習するかによって異なります。

理論上のセキュリティ/プライバシー保証はシステムセキュリティの優れた評価指標ですが、別の
方法は、メンバーシップ推論攻撃[167]またはモデル反転攻撃[56]を実行して、システムをテストすることです。
安全。これらの攻撃は、次の2つの方法で実行できます。（1)ホワイトボックス攻撃 :攻撃者はすべてにアクセスできます
FLプロセス中に交換されたモデル。 （2)ブラックボックス攻撃 :攻撃者は
最終出力モデル。攻撃の成功率は、システムセキュリティの評価指標になります。

システムの効率には、計算効率と通信効率の2つの部分があります。
直感的な指標は、計算時間と通信時間を含むトレーニング時間です。 FLに注意してください
通常、マルチラウンドプロセスです。したがって、公正な比較のために、1つのアプローチはラウンドあたりの時間を次のように使用することです。
メトリック。別のアプローチは、同じ目標パフォーマンスを達成するために時間またはラウンドを記録することです[90、107]。

FLSの堅牢性を定量化することは困難です。考えられる解決策は、同様のメトリックを使用することです
堅牢で安全なアグリゲーション、つまり、
FLプロセス。

6ケーススタディ

このセクションでは、要約したように、分類法に従ってFLの実際のアプリケーションをいくつか紹介します。
表3。

6.1モバイルサービス

Googleキーボード[208]、 Appleの絵文字提案、QuickType [179]など、モバイルユーザーに予測サービスを提供している
企業はたくさんあります。これらのサービスは、
ユーザー。ただし、トレーニングデータは、スマートフォンなどのユーザーのエッジデバイスから取得されます。会社の場合
すべてのユーザーからデータを収集し、グローバルモデルをトレーニングすると、プライバシーが漏洩する可能性があります。に
一方、各シングルユーザーのデータは、正確な予測モデルをトレーニングするには不十分です。 FLは有効にします
これらの企業は、ユーザーの元のデータにアクセスせずに精度予測モデルをトレーニングします。
ユーザーのプライバシーを保護することを意味します。 FLSのフレームワークでは、ユーザーはローカルモデルを計算して送信します
元のデータの代わりに。つまり、Googleキーボードユーザーは、次の正確な予測を楽しむことができます。
入力履歴を共有せずに次の単語。 FLSがそのような予測に広く適用できるかどうか
サービスでは、データは常にエッジに保存されるため、データ漏洩がはるかに少なくなります。

このようなシナリオでは、データは通常、水平方向に数百万のデバイスに分割されます。したがって、単一デバイスの計算リソースと帯域幅の制限は、2つの主要な問題です。さらに、ユーザーはいつでもシステムに参加またはシステムから離れることができるため、システムの堅牢性も考慮する必要があります。言い換えれば、水平データ上の集中型のクロスデバイスFLSは、そのような予測サービス用に設計する必要があります。

FLSの基本的なフレームワークは、何らかの形で個人のプライバシーを保護することができますが、推論攻撃に対して安全ではない可能性があります[167]。個人の区別がつかないようにするために、差分プライバシーなどのいくつかの追加のプライバシーメカニズムを活用する必要があります。ここでは、各デバイスの計算能力が弱く、高価な暗号化操作を行う余裕がないため、安全なマルチパーティ計算は適切でない場合があります。ユーザーのプライバシーを保証することとは別に、ユーザーがデータを提供することを奨励するために、いくつかのインセンティブメカニズムを開発する必要があります。実際には、これらのインセンティブはバウチャーまたは追加サービスである可能性があります。

6.2ヘルスケア

現代の医療制度は、国の医療を改善するために、研究機関、病院、および連邦機関の間の協力を必要とします[57]。さらに、COVID-19 [6]のような世界的な健康緊急事態に直面する場合、各国間の共同研究は不可欠です。これらの医療システムは、主に病気の診断のためのモデルを訓練することを目的としています。これらの診断モデルは、可能な限り正確である必要があります。ただし、 GDPRなどの一部の規制では患者の情報を転送することは許可されていません[10]。データのプライバシーは、国際協力においてさらに懸念されています。プライバシーの問題を解決しないと、共同研究が停滞し、公衆衛生を脅かす可能性があります。このようなコラボレーションにおけるデータのプライバシーは、主に機密保持契約に基づいています。ただし、このソリューションは「信頼」に基づいているため、信頼性は高くありません。 FLは、理論的にプライバシーを確保できるため、協力が可能になります。これは、証明可能で信頼性があります。このように、すべての病院または研究所は、診断のための正確なモデルを取得するためにローカルモデルを共有するだけで済みます。

このようなシナリオでは、ヘルスケアデータは水平方向と垂直方向の両方に分割されます。各パーティには特定の目的（患者の治療など）の居住者のヘルスデータが含まれますが、各パーティで使用される機能は多様です。パーティの数は限られており、各パーティには通常、十分な計算リソースがあります。つまり、ハイブリッドパーティションデータのプライベートFLSが必要です。最も困難な問題の1つは、ハイブリッドパーティションデータをトレーニングする方法です。 FLSの設計は、単純な水平システムよりも複雑になる可能性があります。ヘルスケア連盟には、おそらく中央サーバーはありません。したがって、もう1つの難しい部分は、分散型FLSの設計です。これは、一部の不正または悪意のあるパーティに対しても堅牢である必要があります。さらに、プライバシーの懸念は、安全なマルチパーティ計算や差分プライバシーなどの追加のメカニズムによって解決できます。コラボレーションは主に規制によって動機付けられています。

6.3財務

金融連盟は銀行や保険会社などで構成されています。彼らはしばしば日常の金融業務に協力することを望んでいます。たとえば、一部の「悪い」ユーザーは、別の銀行から借りたお金でローンを1つにまとめる場合があります。すべての銀行は、他の顧客の情報を明らかにすることなく、そのような悪意のある行動を避けたいと考えています。また、保険会社も銀行から顧客の評判について学びたいと考えています。ただし、「良い」顧客の情報が漏洩すると、興味を失ったり、法的な問題が発生したりする可能性があります。

この種の協力は、政府のような信頼できる第三者機関があれば起こり得ます。しかし、多くの場合、政府は連邦に関与していないか、政府が常に信頼されているわけではありません。
そのため、プライバシーメカニズムを備えたFLSを導入できます。 FLSでは、理論的に証明されたプライバシーメカニズムによって各銀行のプライバシーを保証できます。

このようなシナリオでは、財務データは多くの場合、ユーザーIDによってリンクされ、垂直に分割されます。垂直に分割されたデータで分類器をトレーニングすることは非常に困難です。一般に、トレーニングプロセスは、プライバシー保護レコードリンケージ[183]と垂直フェデレーショントレーニングの2つの部分に分けることができます。最初の部分は、垂直に分割されたデータ間のリンクを見つけることを目的としており、十分に研究されています。第二部は訓練することを目的としています

各当事者の元のデータを共有せずにリンクされたデータ。これは依然として課題です。このフェデレーションでは、クロスサイロと分散型の設定が適用されます。また、このシナリオではいくつかのプライバシーメカニズムを採用する必要があり、参加者は興味を持って動機付けられます。

7ビジョン

このセクションでは、今後取り組むべき興味深い方向性を示します。セクション4で紹介した既存の調査では、いくつかの方向性がすでに取り上げられていますが、それらは重要であり、より多くの洞察を提供すると考えています。

7.1不均一性

当事者の異質性はFLSの重要な特徴です。基本的に、当事者は、アクセシビリティ、プライバシー要件、フェデレーションへの貢献、および信頼性が異なる可能性があります。したがって、 FLSでこのような実際的な問題を検討することが重要です。
動的スケジューリングパーティの不安定性のため、学習プロセス中にパーティの数が固定されない場合があります。しかし、多くの既存の研究では政党の数は固定されており、彼らは新しい政党の参入や現在の政党の離脱がある状況を考慮していません。システムは動的スケジューリングをサポートし、パーティの数に変更があったときに戦略を調整する機能を備えている必要があります。この問題に取り組むいくつかの研究があります。たとえば、Googleのシステム[24]は、デバイスのドロップアウトを許容できます。また、ブロックチェーン[223]の出現は、マルチパーティ学習にとって理想的で透過的なプラットフォームになる可能性があります。しかし、私たちの知る限り、 FL中にますます多くの関係者を研究する研究はありません。このような場合、現在のグローバルモデルは既存の関係者に対して十分に訓練されている可能性があるため、後の関係者により多くの注意が払われる可能性があります。

多様なプライバシー制限ほとんどの作業では、当事者が異なるプライバシー要件を持っているFLSのプライバシーの異質性については考慮されていません。既存のシステムは、同じレベルのすべての関係者のモデルパラメータまたは勾配を保護するための手法を採用しています。ただし、実際には、当事者のプライバシー制限は通常異なります。プライバシーの制限に応じて当事者を異なる方法で扱うFLSを設計することは興味深いでしょう。学習したモデルは、プライバシー制限に違反せずに各当事者のデータを最大限に活用できれば、パフォーマンスが向上するはずです。異種差分プライバシー[9]は、ユーザーが異なるプライバシー態度と期待を持っているような設定で役立つ場合があります。

インテリジェントなメリ
ット直感的には、一方の当事者がより多くの情報を提供する場合、FLSからより多くの利益を得る必要があります。既存のインセンティブメカニズムは主にシャープレイ値に基づいており[193、187]、計算のオーバーヘッドが大きな懸念事項です。計算効率が高く公正なインセンティブメカニズムを開発する必要があります。

7.2システム開発

FLSの開発を後押しするには、詳細なアルゴリズム設計に加えて、高レベルの観点から研究する必要があります。

システムアーキテクチャパラメータ同期を制御する深層学習のパラメータサーバー[76]と同様に、FLについてはいくつかの一般的なシステムアーキテクチャを調査する必要があります。 FedAvgは広く使用されているフレームワークですが、適用できるシナリオはまだ限られています。たとえば、教師なし学習[129、107、108]は、モデル集約方法としてモデル平均化を採用していますが、これは、当事者が異種モデルをトレーニングしたい場合には機能しません。さまざまな設定に対して多くの集計方法と学習アルゴリズムを提供する一般的なシステムアーキテクチャが必要です。

モデル市場モデル市場[182]は、モデルの保存、共有、販売のための有望なプラットフォームです。興味深いアイデアは、連合学習にモデル市場を使用することです。パーティはモデルを購入して、モデルの集約をローカルで実行できます。さらに、ターゲットタスクなどの追加情報を使用して、モデルを市場に提供できます。このような設計は、フェデレーションにより多くの柔軟性をもたらします。

FLはいくつかのトランザクションと同じように、組織にとってより受け入れやすくなります。このようなシステムでは、モデルを十分に評価することが重要です。インセンティブメカニズムが役立つかもしれません[201、87、88]。
ベンチマークより多くのFLSが開発されているため、既存のシステムを評価し、将来の開発を指示するには、代表的なデータセットとワークロードを備えたベンチマークが非常に重要です。かなりの数のベンチマークがありますが[25、77、74]、連合学習研究の実験で広く使用されているベンチマークはありません。代表的なデータセットと厳格なプライバシー評価を備えた堅牢なベンチマークが必要です。また、モデルのパフォーマンス、システムの効率、システムのセキュリティ、システムの堅牢性などの包括的な評価指標は、既存のベンチマークでは無視されることがよくあります。非IIDデータセットのモデルパフォーマンスとデータ汚染下のシステムセキュリティの評価には、さらに調査が必要です。

データのライフサイクル学習は、連合システムの1つの側面にすぎません。データライフサイクル[151]は、データの作成、保存、使用、共有、アーカイブ、破棄を含む複数の段階で構成されています。アプリケーション全体のデータセキュリティとプライバシーのために、FLコンテキストで新しいデータライフサイクルを発明する必要があります。データ共有は明らかに焦点を絞った段階の1つですが、FLSの設計は他の段階にも影響を及ぼします。たとえば、データの作成は、FLに適したデータと機能の準備に役立つ場合があります。

7.3ドメインのFL

モノのインターネットセキュリティとプライバシーの問題は、モノのインターネットアプリケーションの展開が増加しているため、フォグコンピューティングとエッジコンピューティングのホットな研究分野となっています。詳細については、最近の調査[172、209、135]を参照してください。 FLは、データプライバシーの問題に対処するための1つの潜在的なアプローチでありながら、適度に優れた機械学習モデルを提供します[113、138]。追加の重要な課題は、計算とエネルギーの制約から生じます。プライバシーとセキュリティのメカニズムにより、実行時のオーバーヘッドが発生します。たとえば、Jiangetal。 [80]独立したガウスランダム射影を適用してデータのプライバシーを改善すると、ディープネットワークのトレーニングにコストがかかりすぎる可能性があります。

著者は、より多くの計算能力を備えたノードにワークロードを移動するために、新しいリソーススケジューリングアルゴリズムを開発する必要があります。同様の問題は、車車間ネットワークなどの他の環境でも発生します[160]。

規制FLは生データを公開せずに共学習を可能にしますが、FLが既存の規制にどのように準拠しているかはまだ明らかではありません。たとえば、GDPRはデータ転送の制限を提案しています。
モデルとグラデーションは実際には十分に安全ではないので、そのような制限はモデルまたはグラデーションに適用されますか？また、グローバルモデルはローカルモデルの平均であるため、「説明可能性の権利」を実行するのは困難です。 FLモデルの説明可能性は未解決の問題です[67、161]。さらに、ユーザーがデータを削除したい場合、データなしでグローバルモデルを再トレーニングする必要がありますか[62]。 FL技術と実際の規制の間にはまだギャップがあります。コンピュータサイエンスコミュニティと法コミュニティの間の協力が期待されるかもしれません。

8結論

連合学習システム（FLS)の開発に多くの努力が注がれてきました。既存のFLSの完全な概要と要約は、重要で意味のあるものです。以前のフェデレーションシステムに触発されて、不均一性と自律性が実用的なFLSの設計における2つの重要な要素であることを示しました。
さらに、6つの異なる側面で、FLSの包括的な分類を提供します。これらの側面に基づいて、既存のFLS間の機能と設計の比較も示します。さらに重要なことに、ベンチマークの増加からブロックチェーンなどの新しいプラットフォームの統合に至るまで、多くの機会を指摘してきました。 FLSは、機械学習、システム、データプライバシーコミュニティの努力を必要とする刺激的な研究の方向性となるでしょう。

了承

この作品は、シンガポールのMoE AcRF Tier 1助成金（T1 251RES1824）、SenseTime Young Scholars Research Fund、およびMOE Tier 2助成金（MOE2017-T2-1-122)によってサポートされています。

参考文献

[1]カリフォルニア州消費者プライバシー法のホームページ。 https://www.caprivacy.org/。

[2] URL https://www.intel.com/content/www/us/en/customer-spotlight/stories/ ping-an-sgx-customer-story.html。

[3] Uberは、2018年に1億4800万ドルでデータ侵害の調査を解決しました。URLhttps ：//www.nytimes.com/2018/ 09/26 / technology/ uber-data-breach.html。

[4] Googleは、2019年のヨーロッパのデータプライバシー法に基づいて5,700万ドルの罰金を科されています。URLhttps ：//www.nytimes.com/ 2019/01/21 / technology/google-europe-gdpr-fine.html。

[5] 2019年は「素晴らしい」年です ：Pdpcは、2019年のデータ侵害で記録的な129万ドルの罰金をスポア企業に課しました。URL https://vulcanpost.com/676006/pdpc-data-breach-singapore-2019/。

[6]コロナウイルス病に関する最新情報（covid-19）、2020年。URLhttps: //www.who.int/emergencies/ 病気/新規コロナウイルス-2019/events-as-they-happen。

[7]マルティン•アバディ、ポール•バーハム、ジャンミン•チェン、ジフェン•チェン、アンディ•デイビス、ジェフリー•ディーン、マシュー•デヴィン、サンジャイ•ゲマワット、ジェフリー•アーヴィング、マイケル•アイザード他Tensorflow ：大規模な機械学習のためのシステム。第12回{USENIX}オペレーティングシステムの設計と実装に関するシンポジウム（{OSDI} 16）、265〜283ページ、2016年。

[8]マルティン•アバディ、アンディ•チュー、イアン•グッドフェロー、Hブレンダン•マクマハン、イリヤ•ミロノフ、クナル•タルワール、リー•チャン。差分プライバシーによるディープラーニング。コンピュータと通信のセキュリティに関する2016ACMSIGSAC会議の議事録、 308〜318ページ。 ACM、2016年。

[9] Mohammad Alaggan、Sebaśtien Gambs、およびAnne-MarieKermarrec。不均一差プライバシー。 arXiv preprint arXiv ：1504.06998、2015。

[10]ヤン•フィリップ•アルブレヒト。 GDPRが世界をどのように変えるか。ユーロ。データ保護L. Rev.、2 ：287、2016年。

[11] Mohammed Aledhari、Rehma Razzak、Reza M Parizi、およびFahadSaeed。連合学習 ：テクノロジー、プロトコル、およびアプリケーションを実現するための調査。 IEEE Access、8 ：140699–140725、2020 。

[12]スコット•アルフェルド、シャオジン•チュー、ポール•バーフォード。自己回帰モデルに対するデータポイズニング攻撃。人工知能に関する第30回AAAI会議、2016年。

[13]エイタン•オルトマン、コンスタンティン•アヴラチェンコフ、アンドレイ•ガルナエフ。ワイヤレスネットワークにおける一般化されたα-公正なリソース割り当て。 2008年の第47回IEEEConferenceon Decision and Control、2414〜2419ページ。 IEEE、2008年。

[14] Muhammad Ammad-ud din、Elena Ivannikova、Suleiman A Khan、Were Oyomno、Qiang Fu、Kuan Eeik Tan、および AdrianFlanagan。プライバシーを保護するパーソナライズされたレコメンデーションシステムのための統合協調フィルタリング。 arXiv preprint arXiv ：1901.09888、2019。

[15]青野義典、林拓也、王李華、森内志保ほか。相加的準同型暗号化によるプライバシー保護ディープラーニング。 IEEE Transactions on Information Forensics and Security、13（5） ：1333–1345、2018。

[16] Eugene Bagdasaryan、Andreas Veit、Yiqing Hua、Deborah Estrin、およびVitalyShmatikov。連合学習をバックドアする方法。人工知能と統計に関する国際会議、 2938〜2948ページ。 PMLR、2020。

[17] James Henry Bell、Kallista A Bonawitz、Adria Gasc on、Tancr ede Lepoint、およびMarianaRaykova。（ポリ）対数オーバーヘッドを使用して、単一サーバーの集約を保護します。 CCSでは、2020年。

[18] Jeremy Bernstein、Yu-Xiang Wang、Kamyar Azizzadenesheli、およびAnimaAnandkumar。 signgd：非凸問題の圧縮最適化。 arXiv preprint arXiv：1802.04434、2018。

[19] Arjun Nitin Bhagoji、Supriyo Chakraborty、Prateek Mittal、およびSeraphinCalo。敵対的なレンズを通して連合学習を分析する、2018年。

[20]アビシェーク•ボウミック、ジョン•ダッチ、ジュリアン•フロイディガー、ガウラヴ•カプール、ライアン•ロジャース。再構築に対する保護とその民間連合学習への応用。 arXiv preprint arXiv：1812.00984、2018。

[21] Peva Blanchard、Rachid Guerraoui、Julien Stainer、他。敵対者との機械学習：ビザンチン耐性の勾配降下。ニューラル情報処理システムの進歩、 119〜129ページ、2017年。

[22]キース•ボナウィッツ、ウラジミール•イワノフ、ベン•クルーター、アントニオ•マルセドン、Hブレンダン•マクマハン、サーバル•パテル、ダニエル•ラマージュ、アーロン•シーガル、カーン•セス。ユーザーが保持するデータの連合学習のための実用的な安全な集約。 arXiv preprint arXiv：1611.04482、2016。

[23]キース•ボナウィッツ、ウラジミール•イワノフ、ベン•クルーター、アントニオ•マルセドン、Hブレンダン•マクマハン、サーバル•パテル、ダニエル•ラマージュ、アーロン•シーガル、カーン•セス。プライバシーを保護する機械学習のための実用的な安全な集約。コンピュータと通信のセキュリティに関する2017ACMSIGSAC会議の議事録、 1175〜1191ページ。 ACM、2017年。

[24]キース•ボナウィッツ、ヒューバート•アイヒナー、ヴォルフガング•グリスカンプ、ズミトリー•フバ、アレックス•インガーマン、ウラジミール•イワノフ、クロエ•キドン、ヤクブ•コネニー、ステファノ•マゾッキ、Hブレンダン•マクマハン他大規模な連合学習に向けて：システム設計。 arXiv preprint arXiv：1902.01046、2019。

[25] Sebastian Caldas、Peter Wu、Tian Li、Jakub Konecnˇ y、H Brendan McMahan、Virginia Smith、および AmeetTalwalkar。リーフ：フェデレーション設定のベンチマーク。 arXiv preprint arXiv：1812.01097、2018 。

[26]リッチカルアナ。マルチタスク学習。機械学習、28（1）：41–75、1997。

[27]ミゲル•カストロ、バーバラ•リスコフ他。実用的なビザンチンフォールトトレランス。 OSDI、第99巻、 173〜186ページ、1999年。

[28] Herve Chabanne、Amaury de Wargny、Jonathan Milgram、Constance Morel、およびEmmanuelProuff。 ディープニューラルネットワークでのプライバシー保護分類。 IACR Cryptology ePrint Archive、2017年：35、2017年。

[29] Di Chai、Leye Wang、Kai Chen、QiangYang。安全なフェデレーション行列の因数分解。arXiv プレプリントarXiv：1906.05108、2019。

[30] Di Chai、Leye Wang、Kai Chen、およびQiangYang。 Fedeval：連合学習のための包括的な評価モデルを備えたベンチマークシステム。 arXivプレプリントarXiv：2011.09655、2020。

[31]カマリカ•チョウドリ、クレア•モンテレオーニ、アナンド•D•サルワテ。差分プライベート経験 リスクの最小化。 Journal of Machine Learning Research、12（3月）：1069–1109、2011年。

[32]デビッド•チャウム。食事する暗号学者の問題：無条件の送信者と受信者のトレースなし 能力。 Journal of cryptology、1（1）：65–75、1988。

[33] Fei Chen、Zhenhua Dong、Zhenguo Li、およびXiuqiangHe。推奨者のためのフェデレーションメタ学習 日付。 arXiv preprint arXiv：1802.07876、2018。

[34] TianqiChenとCarlosGuestrin。 Xgboost：スケーラブルなツリーブースティングシステム。 KDDでは、ページ 785〜794。 ACM、2016年。

[35] Xinyun Chen、Chang Liu、Bo Li、Kimberly Lu、およびDawnSong。データポイズニングを使用したディープラーニングシステムへの標的型バックドア攻撃。 arXiv preprint arXiv :1712.05526、2017。

[36] Yi-Ruei Chen、Amir Rezapour、およびWen-GueyTzeng。プライバシー保護リッジ回帰分散データ。情報科学、451 :34–49、2018。

[37] Yu Chen、Fang Luo、Tong Li、Tao Xiang、Zheli Liu、およびJinLi。信頼できる実行環境を備えたトレーニング整合性プライバシー保護連合学習スキーム。情報科学、 522 :69–79、2020。

[38] Kewei Cheng、Tao Fan、Yilun Jin、Yang Liu、Tianjian Chen、Qiang Yang。Secureboost :ロスレスフェデレーション学習フレームワーク。arXivpreprintarXiv :1901.08755、2019。

[39]ウォーレン•B•チク。シンガポールの個人データ保護法とデータプライバシー改革の将来の傾向の評価。 Computer Law &Security Review、29（5） :554–575、2013。

[40] Olivia Choudhury、Aris Gkoulalas-Divanis、Theodoros Salonidis、Issa Sylla、Yoonyoung Park、 Grace Hsu、およびAmarDas。機密性の高い健康データのための差分プライバシー対応の連合学習。 arXiv preprint arXiv :1910.02578、2019。

[41]ピーター•クリステン。データマッチング :レコードリンケージ、エンティティ解決、および重複検出。 Springer Science &Business Media、2012年。

[42]シェーンクック。 CUDAプログラミング :GPUを使用した並列コンピューティングの開発者向けガイド。ニューンズ、2012年。

[43] LucaCorinziaとJoachimMBuhmann。変分フェデレーションマルチタスク学習。 arXivプレプリント arXiv :1906.06268、2019。

[44] Zhongxiang Dai、Kian Hsiang Low、およびPatrickJaillet。を介したフェデレーションベイズ最適化トンプソンサンプリング。 NeurIPS、2020年。

[45]マユール•ダタール、ニコール•インモルリカ、ピョートル•インディク、ヴァハブ•ミロクニ。 p-stable分布に基づく局所性鋭敏型ハッシュスキーム。計算幾何学に関する第20回年次シンポジウムの議事録、 253～262ページ。 ACM、2004年。

[46] Canh T Dinh、Nguyen H Tran、およびTuanDungNguyen。モローエンベロープを使用したパーソナライズされた連合学習。 arXiv preprint arXiv :2006.08848、2020。

[47] MomingDuan。 Astraea :モバイルディープラーニングアプリケーションの分類精度を向上させるための自己バランス型連合学習。arXiv preprint arXiv :1907.01132、2019。

[48]シンシア•ドワーク、フランク•マクシェリー、コビ•ニッシム、アダム•スミス。プライベートデータ分析における感度に対するノイズの較正。暗号化会議の理論、265～284ページ。 Springer、2006年。

[49]シンシア•ドワーク、アーロン•ロス他。差分プライバシーのアルゴリズムの基礎。 FoundationsandTrends®inTheoreticalComputerScience 、9（3–4） :211–407、2014。

[50]カリド•エル•エマムとフィダ•カマル•ダンカー。 k-匿名性を使用してプライバシーを保護します。ジャーナル American Medical Informatics Association、15（5） :627–637、2008年。

[51] Ittay Eyal、Adem Efe Gencer、Emin Gun Sirer、およびRobbertVanRenesse。 Bitcoin-ng :スケーラブルなブロックチェーンプロトコル。ネットワークシステムの設計と実装に関する第13回USENIXシンポジウム（NSDI 16）、45～59ページ、カリフォルニア州サンタクララ、2016年3月。USENIX協会。 ISBN978-1-931971-29-4 。 URLhttps ://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal。

[52] Alireza Fallah、Aryan Mokhtari、およびAsumanOzdaglar。理論的保証を備えたパーソナライズされた連合学習：モデルにとらわれないメタ学習アプローチ。ニューラル情報処理システムの進歩、33、2020。

[53] Minghong Fang、Xiaoyu Cao、Jinyuan Jia、NeilGong。ローカルモデル中毒攻撃ビザンチン-堅牢な連合学習。 USENIXでは、2020年。

[54] Ji Feng、Yang Yu、およびZhi-HuaZhou。多層勾配ブースティング決定木。ニューラル情報処理システム、3551〜3561ページ、2018年。

[55]チェルシー•フィン、ピーター•アビール、セルゲイ•レヴィン。ディープネットワークの高速適応のためのモデルにとらわれないメタ学習。機械学習に関する第34回国際会議の議事録第70巻、1126〜1135ページ。 JMLR。組織、2017年。

[56]マット•フレデリクソン、ソメシュ•ジャー、トーマス•リステンパート。信頼情報と基本的な対策を悪用するモデル反転攻撃。コンピュータと通信のセキュリティに関する第22回ACMSIGSAC会議の議事録、 1322〜1333ページ。 ACM、2015年。

[57]チャールズ•P•フリードマン、アダム•K•ウォン、デビッド•ブルーメンソール。全国的な学習保健システムの実現。科学翻訳医学、2（57）：57cm29–57cm29、2010年。

[58] Jonas Geiping、Hartmut Bauermeister、Hannah Droge、およびMichaelMoeller。勾配の反転–連合学習でプライバシーを破るのはどれほど簡単ですか？ arXiv preprint arXiv：2003.14053、2020。

[59]サミュエル•J•ガーシュマンとデビッド•M•ブレイ。ベイジアンノンパラメトリックモデルに関するチュートリアル。 Journal of Mathematical Psychology、56（1）：1–12、2012。

[60] Robin C Geyer、Tassilo Klein、およびMoinNabi。差分プライベート連合学習：クライアントレベルの視点。 arXiv preprint arXiv：1712.07557、2017。

[61] Avishek Ghosh、Jichan Chung、Dong Yin、およびKannanRamchandran。のための効率的なフレームワーククラスター化された連合学習。 arXiv preprint arXiv：2006.04088、2020。

[62]アントニオ•ジナート、メロディー•グアン、グレゴリー•ヴァリアント、ジェームス•Y•ゾウ。 aiにあなたを忘れさせる：機械学習におけるデータの削除。ニューラル情報処理システムの進歩、ページ3513–3526、2019。

[63]オデ•ゴールドライヒ。安全なマルチパーティ計算。原稿。暫定版、78、1998。

[64] SlawomirGoryczkaとLiXiong。マルチパーティの安全な追加と差分プライバシーの包括的な比較。信頼性が高く安全なコンピューティングに関するIEEEトランザクション、14（5）：463–477、 2015年。

[65] Klaus Greff、Rupesh K Srivastava、Jan Koutn´ k、 Bas R Steunebrink、およびJurgenSchmidhuber。Lstm：検索スペースのオデッセイ。ニューラルネットワークと学習システムでのIEEEトランザクション、28 （10）：2222–2232、2016年。

[66]アントニオ•ガリとスジット•パル。 Kerasによるディープラーニング。 Packt Publishing Ltd、2017年。

[67]デビッド•ガニング。説明可能な人工知能（xai）。防衛先端研究プロジェクトエージェンシー（DARPA）、nd Web、2017年2月。

[68]フィリップ•ハンゼリーとピーター•リクタリック。グローバルモデルとローカルモデルの混合の連合学習。 arXiv preprint arXiv：2002.05516、2020。

[69] Filip Hanzely、Slavom´ r Hanzely、Samuel Horvath、およびPeterRichtarik。パーソナライズされた連合学習のための下限と最適なアルゴリズム。 arXivプレプリントarXiv：2010.02372、2020。

[70] Tianshu Hao、Yunyou Huang、Xu Wen、Wanling Gao、Fan Zhang、Chen Zheng、Lei Wang、Hainan Ye、Kai Hwang、Zujie Ren、etal。 Edgeaibench：包括的なエンドツーエンドのエッジコンピューティングベンチマークに向けて。 arXiv preprint arXiv：1908.01924、2019。

[71] Andrew Hard、Kanishka Rao、Rajiv Mathews、 Franc¸oiseBeaufays、Sean Augenstein、Hubert Eichner、Chloe Kiddon、および DanielRamage。モバイルキーボード予測のための連合学習。 arXiv preprint arXiv：1811.03604、2018。

[72]スティーブン•ハーディ、ウィルコ•ヘネッカ、ハミッシュ•アイビー•ロー、リチャード•ノック、ジョルジオ•パトリーニ、ギヨーム•スミス、ブライアン•ソーン。エンティティの解決と追加的な準同型暗号化を介した、垂直に分割されたデータに関するプライベート連合学習。 arXiv preprint arXiv：1711.10677、2017。

[73] Chaoyang He、Murali Annavaram、およびSalmanAvestimehr。グループ知識の伝達：エッジでの大規模なcnnの連合学習。ニューラル情報処理システムの進歩、33、2020。

[74] Chaoyang He、Songze Li、Jinhyun So、Mi Zhang、Hongyi Wang、Xiaoyang Wang、Praneeth Vepakomma、Abhishek Singh、Hang Qiu、Li Shen、etal。 Fedml：連合機械学習のための研究図書館とベンチマーク。 arXivプレプリントarXiv：2007.13518、2020。

[75]ジェフリーヒントン、オリオールヴィニャルス、ジェフディーン。神経ネットワークで知識を抽出します。 arXiv プレプリントarXiv：1503.02531、2015。

[76] Qirong Ho、James Cipar、Henggang Cui、Seunghak Lee、Jin Kyu Kim、Phillip B Gibbons、Garth A Gibson、Greg Ganger、および EricPXing。古い同期並列パラメーターサーバーを介したより効果的な分散ml 。ニューラル情報処理システムの進歩、1223〜1231ページ、 2013年。

[77] Sixu Hu、Yuan Li、Xu Liu、Qinbin Li、Zhaomin Wu、およびBingshengHe。 oarfベンチマークスイート：連合学習システムの特性評価と影響。 arXiv preprint arXiv：2006.07856、2020 。

[78] Yaochen Hu、Di Niu、Jianming Yang、およびShengpingZhou。 Fdml：分散機能のための協調的な機械学習フレームワーク。知識発見とデータマイニングに関する第25回ACMSIGKDD国際会議の議事録、2232〜2240ページ、2019年。

[79] Eunjeong Jeong、Seungeun Oh、Hyesung Kim、Jihong Park、Mehdi Bennis、およびSeong-LyunKim。 通信効率の高いデバイス上の機械学習：非iidプライベートデータの下での統合された蒸留と拡張。 arXiv preprint arXiv：1811.11479、2018。

[80] Linshan Jiang、Rui Tan、Xin Lou、およびGuoshengLin。モノのインターネットオブジェクトの軽量プライバシー保護協調学習について。モノのインターネットの設計と実装に関する国際会議の議事録、IoTDI '19、70〜81ページ、ニューヨーク、ニューヨーク、米国、2019年。 ACM。 ISBN978-1-4503-6283-2。土井：10.1145/3302505.3310070。 URLhttp ://doi.acm.org/10.1145/3302505.3310070。

[81] Yihan Jiang、Jakub Konecnˇ y、Keith Rush、およびSreeramKannan。モデルにとらわれないメタ学習による連合学習のパーソナライズの改善。 arXiv preprint arXiv：1909.12488、2019。

[82] RieJohnsonとTongZhang。予測分散を使用した確率的勾配降下法の加速 割引。ニューラル情報処理システムの進歩、315〜323ページ、2013年。

[83] Norman P Jouppi、Cliff Young、Nishant Patil、David Patterson、Gaurav Agrawal、Raminder Bajwa、 Sarah Bates、Suresh Bhatia、Nan Boden、AlBorchersなど。テンソルプロセッシングユニットのデータセンター内パフォーマンス分析。コンピュータアーキテクチャに関する第44回年次国際シンポジウムの議事録、2017年1〜12ページ。

[84] R.JurcaとB.Faltings。インセンティブと互換性のあるレピュテーションメカニズム。 Eコマースに関するEEE国際会議、2003年。CEC2003.、285〜292ページ、2003年6月。doi：10.1109/COEC。 2003.1210263。

[85] Peter Kairouz、H Brendan McMahan、Brendan Avent、Aurelien Bellet、Mehdi Bennis、Arjun Nitin Bhagoji、Keith Bonawitz、Zachary Charles、Graham Cormode、RachelCummingsなど。連合学習における進歩と未解決の問題。 arXiv preprint arXiv：1912.04977、2019。

[86] Georgios Kaissis、Alexander, Ziller、Jonathan Passerat-Palmbach、Theo Ryffel、Dmitrii Usynin、Andrew Trask、Ionesio Lima、Jason Mancuso、Friederike Jungmann、Marc-MatthiasSteinbornなど。多施設医用画像に関するディープラーニングを維持するエンドツーエンドのプライバシー。 Nature Machine Intelligence、1〜12ページ、2021年。

[87] Jiawen Kang、Zehui Xiong、Dusit Niyato、Shengli Xie、およびJunshanZhang。信頼できる連合学習のためのインセンティブメカニズム：評判と契約理論を組み合わせるための共同最適化アプローチ。 IEEEモノのインターネットジャーナル、2019年。

[88] Jiawen Kang、Zehui Xiong、Dusit Niyato、Han Yu、Ying-Chang Liang、DongInKim。モバイルネットワークにおける効率的な連合学習のためのインセンティブ設計：契約理論アプローチ。 arXiv preprint arXiv：1905.07479、2019。

[89] MuratKantarcioglu とChrisClifton。水平に分割されたデータの相関ルールのプライバシー保護分散マイニング。 IEEE Transactions on Knowledge＆Data Engineering、（9）： 1026-1037、2004。

[90] Sai Praneeth Karimireddy、Satyen Kale、Mehryar Mohri、Sashank Reddi、Sebastian Stich、およびAnandaTheerthaSuresh。Scaffold：連合学習のための確率的制御平均。機械学習に関する国際会議の5132〜5143ページ。 PMLR、2020。

[91]アラン•F•カー、シャオドン•リン、アシッシュ•P•サニル、ジェローム•P•ライター。安全なマトリックス製品を使用した、垂直に分割されたデータのプライバシー保護分析。 Journal of Official Statistics、25（1）：125、 2009年。

[92] Guolin Ke、Qi Meng、Thomas Finley、Taifeng Wang、Wei Chen、Weidong Ma、Qiwei Ye、 Tie-Yan Liu。Lightgbm：非常に効率的な勾配ブースティング決定木。NIPS、2017年。

[93]キム•ヘソン、パク•ジホン、メフディ•ベニス、キム•ソンリョン。ブロックチェーンを介したデバイス上の連合学習とその遅延分析。 arXivプレプリントarXiv：1808.03949、2018。

[94] Jakub Konecnｖ`y、H Brendan McMahan、Daniel Ramage、およびPeterRichtari亿ェデレーション最適化：オンデバイスインテリジェンスのための分散型機械学習。 arXiv preprint arXiv：1610.02527、2016。

[95] Jakub Konecnｖ y、H Brendan McMahan、Felix X Yu、Peter Richt arik、Ananda TheerthaSuresh、およびDaveBacon。連合学習：コミュニケーション効率を改善するための戦略。 arXiv preprint arXiv：1610.05492、2016。

[96] Alex Krizhevsky、Ilya Sutskever、およびGeoffreyEHinton。深い畳み込みニューラルネットワークによるImagenet分類。神経情報処理システムの進歩、 1097〜1105ページ、2012年。

[97] Tobias Kurze、Markus Klems、David Bermbach、Alexander Lenk、Stefan Tai、およびMarcelKunze。クラウドフェデレーション。クラウドコンピューティング、2011：32–38、2011。

[98] David Leroy、Alice Coucke、Thibaut Lavril、Thibault Gisselbrecht、およびJosephDureau。キーワードスポッティングのための連合学習。 ICASSP 2019-2019 IEEE International Conference on Acoustics、 Speech and Signal Processing（ICASSP）、ページ6341–6345。 IEEE、2019年。

[99] Bo Li、Yining Wang、Aarti Singh、およびYevgeniyVorobeychik。因数分解ベースの協調フィルタリングに対するデータポイズニング攻撃。神経情報処理システムの進歩、 1885～1893ページ、2016年。

[100] Liping Li、Wei Xu、Tianyi Chen、Georgios B Giannakis、およびQingLing。 Rsa：異種データセットからの分散学習のためのビザンチンロバストな確率的集計方法。 AAAI、 2019年。

[101] Peilong Li、Yan Luo、Ning Zhang、およびYuCao。 Heterospark：機械学習アルゴリズム用の異種CPU/GPUスパークプラットフォーム。 2015年、IEEE International Conference on Networking、 Architecture and Storage（NAS）、347～348ページ。 IEEE、2015年。

[102] Qinbin Li、Zeyi Wen、およびBingshengHe。 svmトレーニング用の適応カーネル値キャッシング。ニューラルネットワークと学習システムでのIEEEトランザクション、2019年。

[103] Qinbin Li、Bingsheng He、およびDawnSong。モデルにとらわれないラウンド-知識移転による最適な連合学習。 arXivプレプリントarXiv：2010.01017、2020。

[104] Qinbin Li、Zeyi Wen、およびBingshengHe。実用的なフェデレーション勾配ブースティング決定木。人工知能に関するAAAI会議の議事録、第34巻、4642～4649ページ、2020年。

[105] Qinbin Li、Zhaomin Wu、Zeyi Wen、およびBingshengHe。プライバシーを維持する勾配ブースティング決定木。人工知能に関するAAAI会議の議事録、第34巻、 784～791ページ、2020年。

[106] Qinbin Li、Yiqun Diao、Quan Chen、およびBingshengHe。非iidデータサイロでの連合学習：実験的研究。 arXiv preprint arXiv：2102.02079、2021。

[107] Qinbin Li、Bingsheng He、およびDawnSong。モデル対照連合学習。 CVPRでは、2021年。

[108] Tian Li、Anit Kumar Sahu、Manzil Zaheer、Maziar Sanjabi、Ameet Talwalkar、VirginiaSmith。異種ネットワークでのフェデレーション最適化。 arXiv preprint arXiv：1812.06127、2018。

[109] Tian Li、Anit Kumar Sahu、Ameet Talwalkar、VirginiaSmith。連合学習：課題、方法、および将来の方向性、2019年。

[110] Tian Li、Maziar Sanjabi、VirginiaSmith。連合学習における公平なリソース割り当て。 arXivプレプリントarXiv：1905.10497、2019。

[111] Xiang Li、Kaixuan Huang、Wenhao Yang、Shusen Wang、ZhihuaZhang。収束について非iidデータに対するfedavgの影響。 arXiv preprint arXiv：1907.02189、2019。

[112]ハンス•アルバート•リアント、ヤン•ジャオ、ジュン•ジャオ。連合学習への攻撃：ユーザー勾配からトレーニングデータを回復するためのレスポンシブWebユーザーインターフェイス。コンピュータと通信のセキュリティに関するACMアジア会議（ASIACCS）、2020年。

[113] Wei Yang Bryan Lim、Nguyen Cong Luong、Dinh Thai Hoang、Yutao Jiao、Ying-Chang Liang、Qiang Yang、Dusit Niyato、Chunyan Miao。モバイルエッジネットワークでの統合学習：包括的な調査、2019年。

[114]タオ•リン、リンジン•コング、セバスチャン•U•スティッチ、マーティン•ジャギ。連合学習におけるロバストなモデル融合のためのアンサンブル蒸留。 arXiv preprint arXiv：2006.07242、2020。

[115] Boyi Liu、Lujia Wang、Ming Liu、およびChengzhongXu。生涯連合強化学習：クラウドロボットシステムでのナビゲーションのための学習アーキテクチャ。 arXiv preprint arXiv：1901.06455、2019 。

[116] Jian Liu、Mika Juuti、Yao Lu、およびNadarajahAsokan。ミニオン変換による忘却型ニューラルネットワークの予測。 2017 ACM SIGSAC Conference on Computer and Communications Securityの議事録、619〜631ページ。 ACM、2017年。

[117] Lifeng Liu、Fengda Zhang、Jun Xiao、ChaoWu。大規模な連合の評価フレームワーク 学ぶ。 arXiv preprint arXiv：2003.01575、2020。

[118] Lumin Liu、Jun Zhang、SH Song、およびKhaledBLetaief。エッジ支援階層フェデレーション 非iidデータを使用した学習。 arXiv preprint arXiv：1905.06641、2019。

[119]ヤン•リウ、ティアンジアン•チェン、チャン•ヤン。安全なフェデレーション転送学習。 arXiv preprint arXiv：1812.03337、2018。

[120] Yang Liu、Yan Kang、Xinwei Zhang、Liping Li、Yong Cheng、Tianjian Chen、Mingyi Hong、QiangYang 。コミュニケーション効率の高い垂直連合学習フレームワーク。arXivpreprintarXiv：1912.11187、2019。

[121] Yang Liu、Yingting Liu、Zhijie Liu、Junbo Zhang、Chuishi Meng、YuZheng。連合林。arXivpreprintarXiv：1905.10053、2019。

[122]ヤン•リウ、ジュオ•マ、シメン•リウ、シキ•マ、スーリヤ•ネパール、ロバート•デン。プライベートブースト：モバイルクラウドセンシングのためのプライバシー保護連合の極端なブースト。 arXiv preprint arXiv：1907.10218、2019。

[123]ノエル•ロープスとベルナルデテ•リベイロ。 Gpumlib：効率的なオープンソースのGPU機械学習ライブラリ。 International Journal of Computer Information Systems and Industrial Management Applications、3：355–362、2011。

[124] Jiahuan Luo、Xueyang Wu、Yun Luo、Anbu Huang、Yunfeng Huang、Yang Liu、およびQiangYang。 連合学習のための実世界の画像データセット。 arXiv preprint arXiv：1910.11089、2019。

[125] Lingjuan Lyu、Han Yu、およびQiangYang。連合学習への脅威：調査。 arXiv preprint arXiv：2003.02133、2020。

[126] Chenxin Ma、Jakub Konecn ˇ y、Martin Jaggi、Virginia Smith、Michael I Jordan、Peter Richt arik、 MartinTaka´c。任意のローカルソルバーによる分散最適化。最適化の方法とソフトウェア、32（4）：813–848、2017。

[127] Dhruv Mahajan、Ross Girshick、Vignesh Ramanathan、Kaiming He、Manohar Paluri、Yixuan Li、Ashwin Bharambe、およびLaurens vanderMaaten。弱教師あり事前トレーニングの限界を探る。コンピュータビジョンに関する欧州会議（ECCV)の議事録、 181〜196ページ、2018年。

[128] Othmane Marfoq、Chuan Xu、Giovanni Neglia、およびRichardVidal。クロスサイロ連合学習のためのスループット最適なトポロジー設計。 arXivプレプリントarXiv：2010.12229、2020。

[129] H Brendan McMahan、Eider Moore、Daniel Ramage、Seth Hampson、他。分散型データからのディープネットワークの通信効率の高い学習。 arXiv preprint arXiv：1602.05629、2016。

[130] Hブレンダン•マクマハン、ダニエル•ラマージュ、クナル•タルワール、リー•チャン。差分プライベート学習 反復言語モデル。 arXiv preprint arXiv：1710.06963、2017。

[131]ルカ•メリス、コンチェン•ソング、エミリアーノ•デ•クリストファロ、ヴィタリー•シュマティコフ。共学習における傾向のない機能の漏洩を利用する。 2019 IEEE Symposium on Security and Privacy （SP）、691〜706ページ。 IEEE、2019年。

[132] El Mahdi El Mhamdi、Rachid Guerraoui、およびSebastienRouault。ビザンチウムにおける分散学習の隠れた脆弱性。 arXiv preprint arXiv：1802.07927、2018。

[133] Volodymyr Mnih、Koray Kavukcuoglu、David Silver、Andrei A Rusu、Joel Veness、Marc G Bellemare 、Alex Graves、Martin Riedmiller、Andreas K Fidjeland、GeorgOstrovskiなど。深層強化学習による人間レベルの制御。 Nature、518（7540） :529–533、2015年。

[134] Mehryar Mohri、Gary Sivek、およびAnandaTheerthaSuresh。不可知論的な連合学習。 arXiv プレプリントarXiv :1902.00146、2019。

[135] M. Mukherjee、R。Matam、L。Shu、L。Maglaras、MA Ferrag、N。Choudhury、およびV.Kumar。 フォグコンピューティングにおけるセキュリティとプライバシー :課題。 IEEE Access、5 :19293–19304、2017年。doi： 10.1109/ACCESS.2017.2749422。

[136] Moni Naor、Benny Pinkas、およびReubanSumner。プライバシー保護オークションとメカニズムデザイン。 電子商取引に関する第1回ACM会議の議事録、EC '99、129〜139ページ、ニューヨーク、ニューヨーク、米国、1999年。ACM。 ISBN1-58113-176-3。土井 :10.1145/336992.337028。 URLhttp ://doi.acm.org/10.1145/336992.337028。

[137]ミラッド•ナスル、レザ•ショクリ、アミール•フマンサドル。ディープラーニングの包括的なプライバシー分析 :集中型および連合学習に対するパッシブおよびアクティブなホワイトボックス推論攻撃。ディープラーニングの包括的なプライバシー分析 :集中型および連合学習に対するパッシブおよびアクティブホワイトボックス推論攻撃、0ページ。IEEE、2019年。

[138] Thien Duc Nguyen、Samuel Marchal、Markus Miettinen、Hossein Fereidooni、N。Asokan、およびAhmad-RezaSadeghi。 D¨Iot： 2018年のIoT向けのフェデレーション自己学習異常検出システム。

[139]アレックス•ニコルとジョン•シュルマン。爬虫類 :スケーラブルなメタ学習アルゴリズム。 arXivプレプリント arXiv :1803.02999、2 :2、2018。

[140] Solmaz Niknam、Harpreet S Dhillon、およびJefferyHReed。無線通信のための連合学習 :動機、機会および課題。 arXiv preprint arXiv :1908.06847、2019。

[141] Valeria Nikolaenko、Udi Weinsberg、Stratis Ioannidis、Marc Joye、Dan Boneh、およびNinaTaft。 何億ものレコードでのプライバシー保護リッジ回帰。 2013年のセキュリティとプライバシーに関するIEEEシンポジウム、334〜348ページ。 IEEE、2013年。

[142]エイドリアン•ニルソン、サイモン•スミス、グレガー•ウルム、エミル•グスタフソン、マット•ジャーストランド。連合学習アルゴリズムのパフォーマンス評価。ディープラーニングのための分散インフラストラクチャに関する第2回ワークショップの議事録、 1〜8ページ。 ACM、2018年。

[143]西尾隆行と米谷亮。モバイルエッジで異種リソースを使用した連合学習のためのクライアントの選択。 ICC 2019-2019 IEEE International Conference on Communications （ICC)の1〜7ページ。 IEEE、2019年。

[144]リチャード•ノック、スティーブン•ハーディ、ウィルコ•ヘネッカ、ハミッシュ•アイビー•ロー、ジョルジオ•パトリーニ、ギヨーム•スミス、ブライアン•ソーン。エンティティの解決と連合学習は、連合の解決を取得します。 arXiv preprint arXiv :1803.04035、2018。

[145] Olga Ohrimenko、Felix Schuster、Cedric Fournet、Aastha Mehta、Sebastian Nowozin、Kapil Vaswani、およびManuelCosta。信頼できるプロセッサでの気付かないマルチパーティの機械学習。第25回{USENIX}セキュリティシンポジウム（{USENIX}セキュリティ16）、ページ619–636、2016年。

[146]パスカルパイリエ。複合次数剰余性クラスに基づく公開鍵暗号システム。暗号技術の理論と応用に関する国際会議、 223〜238ページ。 Springer、1999年。

[147]シンノ•ジャリン•パンとチャン•ヤン。転移学習に関する調査。知識に関するIEEEトランザクション およびデータエンジニアリング、22（10） :1345–1359、2010。

[148]アダム•パスケ、サム•グロス、スミス•チンタラ、グレゴリー•チャナン、エドワード•ヤン、ザカリー•デヴィート、ゼミング•リン、アルバン•デスメゾン、ルカ•アンティガ、アダム•レラー。 pytorchの自動微分。 2017年。

[149] Adam Paszke、Sam Gross、Francisco Massa、Adam Lerer、James Bradbury、Gregory Chanan、 Trevor Killeen、Zeming Lin、Natalia Gimelshein、LucaAntigaなど。 Pytorch：必須のスタイル、高性能のディープラーニングライブラリ。ニューラル情報処理システムの進歩、ページ8024–8035、2019。

[150]ロビ•ポリカール。アンサンブル学習。アンサンブル機械学習。 Springer、2012年。

[151] Neoklis Polyzotis、Sudip Roy、Steven Euijong Whang、およびMartinZinkevich。生産機械学習におけるデータライフサイクルの課題：調査。 ACM SIGMODレコード、47（2）：17–28、2018。

[152] Adnan Qayyum、Kashif Ahmad、Muhammad Ahtazaz Ahsan、Ala Al-Fuqaha、およびJunaidQadir。ヘルスケアのための協調的連合学習：エッジでのマルチモーダルcovid-19診断、2021年。

[153] Yongfeng Qian、Long Hu、Jing Chen、Xin Guan、Mohammad Mehedi Hassan、およびAbdulhameedAlelaiwi。連合学習によるモバイルエッジコンピューティングのためのプライバシーを意識したサービスの配置。情報科学、505：562–570、2019。

[154] Sashank Reddi、Zachary Charles、Manzil Zaheer、Zachary Garrett、Keith Rush、Jakub Konecn y、Sanjiv Kumar、およびHBrendanMcMahan。アダプティブフェデレーション最適化。 arXiv preprint arXiv：2003.00295、2020。

[155] Amirhossein Reisizadeh、Farzan Farnia、Ramtin Pedarsani、およびAliJadbabaie。堅牢な連合学習：アフィン分布シフトの場合。 arXiv preprint arXiv：2006.08907、2020。

[156] M Sadegh Riazi、Christian Weinert、Oleksandr Tkachenko、Ebrahim M Songhori、Thomas Schnei der、およびFarinazKoushanfar。カメレオン：機械学習アプリケーション向けのハイブリッドで安全な計算フレームワーク。コンピュータと通信のセキュリティに関するアジア会議の2018年の議事録、 707～721ページ。 ACM、2018年。

[157]セバスティアン•ルーダー。ディープニューラルネットワークでのマルチタスク学習の概要。 arXiv preprint arXiv：1706.05098、2017。

[158] Theo Ryffel、Andrew Trask、Morten Dahl、Bobby Wagner、Jason Mancuso、Daniel Rueckert、およびJonathanPasserat-Palmbach。ディープラーニングを維持するプライバシーのための一般的なフレームワーク。 arXiv preprint arXiv：1811.04017、2018。

[159] Mohamed Sabt、Mohammed Achemlal、およびAbdelmadjidBouabdallah。信頼できる実行環境：それが何であるか、そして何でないか。 2015年、IEEE Trustcom / BigDataSE / ISPA、第1巻、57～64ページ。 IEEE、2015年。

[160] Sumudu Samarakoon、Mehdi Bennis、Walid Saad、およびMerouaneDebbah。連合学習超信頼性の低遅延v2v通信、2018年。

[161] Wojciech Samek、Thomas Wiegand、およびKlaus-RobertMuller。説明可能な人工知能：深層学習モデルの理解、視覚化、解釈。 arXiv preprint arXiv：1708.08296、2017 。

[162] Ashish P Sanil、Alan F Karr、Xiaodong Lin、およびJeromePReiter。分散計算によるプライバシー保護回帰モデリング。知識発見とデータマイニングに関する第10回ACMSIGKDD国際会議の議事録、677～682ページ。 ACM、2004年。

[163]ユヌスサリカヤとオズグルエルセチン。連合学習における労働者の動機付け：シュタッケルベルグゲーム展望、2019。

[164] Felix Sattler、Simon Wiedemann、Klaus-Robert Muller、およびWojciechSamek。非iidデータからの堅牢で通信効率の高い連合学習。 arXiv preprint arXiv：1903.02891、2019 。

[165]アディ•シャミア。秘密を共有する方法。 ACMのコミュニケーション、22（11）：612–613、1979。

[166]アミット•シェスとジェームズ•ア•ラーソン。分散型、異種型、および自律型のデータベースを管理するための連合データベースシステム。 ACM Computing Surveys（CSUR）、22（3）：183–236、1990。

[167] Reza Shokri、Marco Stronati、Congzheng Song、およびVitalyShmatikov。機械学習モデルに対するメンバーシップ推論攻撃。 2017年のIEEESymposiumon Security and Privacy（SP）、 3〜18ページ。 IEEE、2017年。

[168] Dejan Skvorc、Matija Horvat、およびSinisaSrbljic。全二重Webストリームを実装するためのWebSocketプロトコルのパフォーマンス評価。 2014年、第37回情報通信技術、電子機器、マイクロ電子機器に関する国際条約（MIPRO）、1003〜1008ページ。
IEEE、2014年。

[169]バージニア•スミス、チャオカイ•チェン、マジアル•サンジャビ、アミート•タルヴァル。フェデレーションマルチタスク学習。ニューラル情報処理システムの進歩、4424〜4434ページ、2017年。

[170]シュアン•ソング、カマリカ•チョウドリ、アナンド•D•サルワテ。差分プライベート更新による確率的勾配降下法。 2013年のIEEEGlobalConference on Signal and Information Processing、245〜248ページ。 IEEE、2013年。

[171] Michael R Sprague、Amir Jalalirad、Marco Scavuzzo、Catalin Capota、Moritz Neun、Lyman Do、およびMichaelKopp。地理空間アプリケーションのための非同期連合学習。データベースにおける機械学習と知識発見に関する欧州合同会議、21〜28ページ。 Springer、 2018年。

[172] Ivan Stojmenovic、Sheng Wen、Xinyi Huang、およびHaoLuan。フォグコンピューティングとそのセキュリティ問題の概要。同意します。計算します。 ：練習。 Exper。、28（10）：2991–3005、2016年7月。ISSN1532-0626。土井：10.1002/cpe.3485。
URLhttps ://doi.org/10.1002/cpe.3485。

[173] LiliSuとJiamingXu。高次元での分散型機械学習の保護。 arXiv preprint arXiv：1804.10140、2018。

[174] Ziteng Sun、Peter Kairouz、Ananda Theertha Suresh、およびHBrendanMcMahan。あなたは本当に連合学習を裏口にすることができますか？ arXiv preprint arXiv：1911.07963、2019。

[175]マーティン•サンダーマイヤー、ラルフ•シュルター、ハーマン•ネイ。言語モデリングのためのLstmニューラルネットワーク。 2012年の国際音声コミュニケーション協会の第13回年次会議で。

[176]メラニースワン。ブロックチェーン：新しい経済の青写真。 ” O'Reilly Media、Inc。”、2015年。

[177]ベン•タン、ボー•リウ、ヴィンセント•チェン、チャン•ヤン。オンラインサービスのための連合レコメンダーシステム。レコメンダーシステムに関する第14回ACM会議、579〜581ページ、2020年。

[178] MingxingTanとQuocVLe。 Efficientnet：畳み込みニューラルのモデルスケーリングを再考するネットワーク。 arXiv preprint arXiv：1905.11946、2019。

[179]ADPチーム他。大規模なプライバシーで学ぶ。 Apple Machine Learning Journal、1（8）、2017年。

[180] Om Thakkar、Galen Andrew、およびHBrendanMcMahan。アダプティブクリッピングによる差分プライベート学習。 arXiv preprint arXiv：1905.03871、2019。

[181] Stacey Truex、Nathalie Baracaldo、Ali Anwar、Thomas Steinke、Heiko Ludwig、Rui Zhang、およびYiZhou。プライバシーを保護する連合学習へのハイブリッドアプローチ。人工知能とセキュリティに関する第12回ACMワークショップの議事録、1〜11ページ。 ACM、2019年。

[182] Manasi Vartak、Harihar Subramanyam、Wei-En Lee、Srinidhi Viswanathan、Saadiyah Husnoo、 Samuel Madden、およびMateiZaharia。 Modeldb：機械学習モデル管理のためのシステム。ヒューマンインザループデータ分析に関するワークショップの議事録、2016年1〜3ページ。

[183] Dinusha Vatsalan、Ziad Sehili、Peter Christen、およびErhardRahm。ビッグデータのプライバシー保護レコードリンケージ：現在のアプローチと研究課題。ビッグデータテクノロジーのハンドブック、 851〜895ページ。 Springer、2017年。

[184] Praneeth Vepakomma、Otkrist Gupta、Tristan Sweden、およびRameshRaskar。健康のための分割学習：生の患者データを共有せずに分散型ディープラーニング。 arXiv preprint arXiv：1812.00564、2018。

[185] PaulVoigtとAxelVondemBussche。 euの一般データ保護規則（gdpr）。実用ガイド、第1版、Cham：Springer International Publishing、2017年。

[186]イザベル•ワーグナーとデビッド•エックホフ。技術的なプライバシー指標：体系的な調査。 ACMコンピューティング調査（CSUR）、51（3）：57、2018。

[187] Guan Wang、Charlie Xiaoqian Dang、およびZiyeZhou。連合学習への参加者の貢献度を測定します。 2019 IEEE International Conference on Big Data（Big Data）、2597〜2604ページ。IEEE、2019年。

[188] Hongyi Wang、Kartik Sreenivasan、Shashank Rajput、Harit Vishwakarma、Saurabh Agarwal、Jy yong Sohn、Kangwook Lee、およびDimitrisPapailiopoulos。尻尾の攻撃：はい、あなたは本当に連合学習を裏口にすることができます。ニューラル情報処理システムの進歩、33、2020。

[189] Hongyi Wang、Mikhail Yurochkin、Yuekai Sun、Dimitris Papailiopoulos、およびYasamanKhazaeni。一致した平均化による連合学習。 arXiv preprint arXiv：2002.06440、2020。

[190] Jianyu Wang、Qinghua Liu、Hao Liang、Gauri Joshi、およびHVincentPoor。異種フェデレーション最適化における客観的な不整合の問題への取り組み。ニューラル情報処理システムの進歩、2020年。

[191] Rui Wang、Heju Li、およびErwuLiu。車両のインターネットでのアプリケーションを備えたモバイルエッジネットワークでのブロックチェーンベースの連合学習。 arXiv preprint arXiv：2103.01116、2021。

[192]王Shiqiang、Tiffany Tuor、Theodoros Salonidis、Kin K Leung、Christian Makaya、Ting He、およびKevinChan 。リソースに制約のあるエッジコンピューティングシステムにおける適応連合学習。 IEEE Journal on Selected Areas in Communications、37（6）：1205–1221、2019。

[193] Tianhao Wang、Johannes Rausch、Ce Zhang、Ruoxi Jia、およびDawnSong。への原則的なアプローチ連合学習のためのデータ評価。連合学習の153〜167ページ。スプリンガー、2020年。

[194] Xiaofei Wang、Yiwen Han、Chenyang Wang、Qiyang Zhao、Xu Chen、およびMinChen。 In-edge ai：連合学習によるモバイルエッジコンピューティング、キャッシング、通信のインテリジェント化。 IEEEネットワーク、2019年。

[195]王悠子。 Co-op：モバイルデバイスからの協調的な機械学習。 2017年。

[196] Zhibo Wang、Mengkai Song、Zhifei Zhang、Yang Song、Qian Wang、HairongQi。クラス代表者の推測を超えて：連合学習からのユーザーレベルのプライバシー漏洩。 IEEE INFOCOM 2019-IEEE Conference on Computer Communications、2512〜2520ページ。 IEEE、2019年。

[197] Zeyi Wen、Bingsheng He、Ramamohanarao Kotagiri、Shengliang Lu、およびJiashuaiShi。効率的な勾配により、GPUでのデシジョンツリートレーニングが強化されました。 2018年のIEEEInternationalParallel and Distributed Processing Symposium（IPDPS）、234～243ページ。 IEEE、2018年。

[198] Zeyi Wen、Jiashuai Shi、Qinbin Li、Bingsheng He、およびJian Chen。ThunderSVM：高速SVM GPUおよびCPU上のライブラリ。 Journal of Machine Learning Research、19：797–801、2018。

[199] Zeyi Wen、Jiashuai Shi、Bingsheng He、Jian Chen、Kotagiri Ramamohanarao、およびQinbinLi。効率的な勾配ブースティング決定木のトレーニングのためにGPUを活用します。並列および分散システムでのIEEEトランザクション、2019年。

[200] Zeyi Wen、Jiashuai Shi、Qinbin Li、Bingsheng He、およびJian Chen。Thundergbm：GPU上の高速GBDTとランダムフォレスト。https：//github.com/Xtra-Computing/thundergbm、2019年。

[201] Jiasi Weng、Jian Weng、Jilian Zhang、Ming Li、Yue Zhang、Weiqi Luo。ディープチェーン：ブロックチェーンベースのインセンティブによる監査可能でプライバシーを保護するディープラーニング。信頼できる安全なコンピューティングに関するIEEEトランザクション、2019年。

[202] Xiaokui Xiao、Guozhang Wang、およびJohannesGehrke。ウェーブレット変換による差分プライバシー。 IEEE Transactions on Knowledge and Data Engineering、23（8）：1200–1214、2010。

[203] Chulin Xie、Keli Huang、Pin-Yu Chen、Bo Li。Dba：分散型バックドア攻撃連合学習。表現学習国際学会、2019年。

[204] Cong Xie、Sanmi Koyejo、およびIndranilGupta。非同期フェデレーション最適化。 arXiv preprint arXiv：1903.03934、2019。

[205] Runhua Xu、Nathalie Baracaldo、Yi Zhou、Ali Anwar、HeikoLudwig。 Hybridalpha：プライバシーを保護する連合学習のための効率的なアプローチ。人工知能とセキュリティに関する第12回ACMワークショップの議事録、2019年13～23ページ。

[206] Zhuang Yan、Li Guoliang、およびFengJianhua。知識ベースのエンティティアラインメントに関する調査。 Journal of Computer Research and Development、1：165–192、2016年。

[207] Qiang Yang、Yang Liu、Tianjian Chen、およびYongxinTong。連合機械学習：概念とアプリケーション。インテリジェントシステムとテクノロジーに関するACMトランザクション（TIST）、10（2）：12、2019。

[208]ティモシー•ヤン、ガレン•アンドリュー、ヒューバート•アイヒナー、ハイチェン•サン、ウェイ•リー、ニコラス•コング、ダニエル•ラマージュ、フランソワーズ•ボーフェ。応用連合学習：Googleキーボードクエリの提案を改善します。 arXiv preprint arXiv：1812.02903、2018。

[209] Shanhe Yi、Zhengrui Qin、およびQunLi。フォグコンピューティングのセキュリティとプライバシーの問題：調査。のWASA、2015年。

[210] Naoya Yoshida, Takayuki Nishio, Masahiro Morikura, Koji Yamamoto, and Ryo Yonetani. Hybrid fl: Cooperative learning mechanism using non-iid data in wireless networks. arXiv preprint arXiv:1905.07210, 2019.

[211] Hwanjo Yu、Xiaoqian Jiang、およびJaideepVaidya。水平方向に分割されたデータで非線形カーネルを使用してプライバシーを保護するsvm 。応用コンピューティングに関する2006年ACMシンポジウムの議事録、 603～610ページ。 ACM、2006年。

[212] Zhengxin Yu、Jia Hu、Geyong Min、Haochuan Lu、Zhiwei Zhao、Haozhe Wang、Nektarios Georgalas 。エッジコンピューティングにおける連合学習ベースのプロアクティブコンテンツキャッシング。2018年のIEEEグローバルコミュニケーションカンファレンス（GLOBECOM）、1～6ページ。 IEEE、2018年。

[213] Mikhail Yurochkin、Mayank Agarwal、Soumya Ghosh、Kristjan Greenewald、Trong Nghia Hoang、およびYasamanKhazaeni。ニューラルネットワークのベイズノンパラメトリック連合学習。 arXiv preprint arXiv：1905.12022、2019。

[214] Weishan Zhang、Qinghua Lu、Qiuyu Yu、Zhaotong Li、Yue Liu、Sin Kit Lo、Shipping Chen、Xiwei Xu、LimingZhu。産業用IOTにおけるデバイス障害検出のためのブロックチェーンベースの連合学習。IEEEモノのインターネットジャーナル、2020。

[215] YuZhangとQiangYang。マルチタスク学習に関する調査。 arXivプレプリントarXiv：1707.08114、2017年。

[216] Zhengming Zhang、Zhewei Yao、Yaoqing Yang、Yujun Yan、Joseph E Gonzalez、Michael W Mahoney。半教師あり連合学習のベンチマーク。arXivpreprintarXiv：2008.11364、2020 。

[217] Lingchen Zhao、Lihao Ni、Shengshan Hu、Yaniiao Chen、Pan Zhou、Fu Xiao、およびLibingWu。プライベートディギング：差分プライバシーを使用したツリーベースの分散データマイニングを有効にします。 INFOCOMの2087～2095ページ。 IEEE、2018年。

[218]ヤン•ジャオ、ジュン•ジャオ、リンシャン•ジャン、ルイ•タン、デュシット•ニヤト。モバイルエッジコンピューティング、ブロックチェーン、レピュテーションベースのクラウドソーシング、連合学習：安全で分散型のプライバシー保護システム。 arXiv preprint arXiv：1906.10893、2019。

[219]ヤン•ジャオ、ジュン•ジャオ、リンシャン•ジャン、ルイ•タン、デュシット•ニヤト、ゼンシャン•リー、リンジュアン•リュウ、インボ•リウ。IoTデバイス向けのプライバシー保護ブロックチェーンベースの連合学習。 IEEEモノのインターネットジャーナル、2020年。

[220]ヤン•ジャオ、ジュン•ジャオ、メンメン•ヤン、テン•ワン、ニン•ワン、リンジュアン•リュウ、デュシット•ニヤト、クォック•ヤン•ラム。モノのインターネットのためのローカルディファレンシャルプライバシーベースの連合学習。 arXivプレプリントarXiv：2004.08856、2020。

[221] Yue Zhao、Meng Li、Liangzhen Lai、Naveen Suda、Damon Civin、VikasChandra。非iidデータを使用した学習。 arXiv preprint arXiv：1806.0582、2018。

[222] Wenbo Zheng、Lan Yan、Chao Gou、およびFei-YueWang。不正なクレジットカード検出のための統合メタ学習。 2020年の第29回人工知能国際合同会議（IJCAI-20)の議事録。

[223] Zibin Zheng、Shaoan Xie、Hong-Ning Dai、Xiangping Chen、Huaimin Wang。ブロックチェーンの課題と機会：調査。InternationalJournalof Web and Grid Services、14（4）： 352–375、2018。

[224] Amelie Chi Zhou、Yao Xiao、Bingsheng He、Jidong Zhai、Rui Mao、他。地理的に分散したクラウドデータセンターにおけるプライバシー規制を意識したプロセスマッピング。並列および分散システムでのIEEEトランザクション、2019年。

[225] Pan Zhou、Kehao Wang、Linke Guo、Shimin Gong、BolongZheng。ソーシャルリコメンダーシステムでビッグデータをサポートする、プライバシーを保護する分散型コンテキストフェデレーションオンライン学習フレームワーク。知識とデータエンジニアリングに関するIEEEトランザクション、2019年。

[226]HangyuZhuとYaochuJin。多目的進化的連合学習。 IEEEトランザクションニューラルネットワークと学習システム、2019年。

[227] Weiming Zhuang、Yonggang Wen、Xuesen Zhang、Xin Gan、Daiying Yin、Dongzhan Zhou、Shuai Zhang、ShuaiYi。ベンチマーク分析による連合者の再識別のパフォーマンスの最適化。第28回ACMマルチメディア国際会議の議事録、ページ955–963、2020 。

[228] G. Zyskind、O。Nathan、およびA.'。ペントランド。プライバシーの分散化：ブロックチェーンを使用して個人データを保護します。 2015 IEEE Security and Privacy Workshops、180〜184ページ、2015年5月。doi： 10.1109/SPW.2015.27。