秘密保護学習技術における通信量比較および産業利用性の検討

藤井　智也† 　坂元　哲平† 　渡部　耕大†† 　安部　裕之† 　西村　拓哉†
今倉　暁††† 　櫻井　鉄也†††

† 株式会社 NTT データ 技術革新統括本部　〒 135–6011 東京都江東区豊洲 3-3-9
†† 株式会社 NTT データ 金融事業推進部　〒 135–6011 東京都江東区豊洲 3-3-9
††† 筑波大学 システム情報系　〒 305–8573 茨城県つくば市天王台 1-1-1
E-mail: †{tomoya.fujii,teppei.sakamoto,hiroyuki.abe,takuya.nishimura}@nttdata.com,
††kodai.watanabe@nttdata.com , †††{imakura,sakurai}@cs.tsukuba.ac.jp

あらまし　機械学習では一般的に学習データ量が多いほど高い精度を達成できるが，単独組織で大量のデータサンプルを用意するのは困難である．そこで，複数組織が協調してデータサンプルを集約させることが理想であるが，それは情報保護の観点から許容できないケースが多い．このような場合に，情報の秘匿性を保ちつつ複数の組織が持つ学習データをモデルに反映させる秘密保護学習手法がいくつか提案されている．しかし，秘密保護学習は手法毎の比較と考察が十分に進んでいないのが現状である．本研究では，秘密保護学習の代表手法である Federated Learning と Data Collaboration の要する通信量を実測して比較検証を行うとともに，両手法の産業利用について検討する．

キーワード　情報保護，プライバシ，機械学習，Federated Learning，Data Collaboration

1 はじめに

近年では，ビッグデータの効率的な流通・利活用を推進するために，それに関連した技術が盛んに提案されている．データの秘匿性を担保しつつモデリングが行える秘密保護学習技術もその一つである．機械学習では，一般的に学習データ量が多いほど高い精度を達成できる．しかし，現実的には単独の組織で十分な学習データを用意するのは困難であるケースが多い [1]．そこで，複数の組織が持つ学習データを活用してモデリングすることが望ましいが，情報秘匿性を担保することが課題となる．現在，情報秘匿性を保ちつつモデリングを実施するための方針は大きく分けて以下の 2 つがある．

(a)　各クライアントでモデル学習を行い，そのモデルのパラメータ情報を集約させる．
(b)　各クライアントでデータをサンプル毎に秘匿化し，その秘匿化データを集約させる．

(a) は勾配モデルを対象としている手法であり，まず，各クライアントが自組織の学習データを使って，モデルの反復学習を行う．その際に，パラメータの更新情報を外部に共有することで，各組織の学習データの性質を反映させたモデリングが可能となる．代表的な手法として，Google 社が提案している Federated Learning [2] [3] [4] 等がある．

(b) の手法はモデルを学習する前にデータ自体をサンプル毎に秘匿化したのちに，データを集約させモデリングを行う．そのため，モデルの形式は問わない．代表的な手法として Data Collaboration [5] [6] [7] や暗号化手法を用いた秘密計算モデリング [8] [9] [10] がある．

これらの手法は性質は大きく異なるものの，組織横断でのモデリングを目的とする点で共通しており，実用上はこれらの性質を考慮して，ユースケースごとに適否を判断して使い分けることでより効率的なモデリングが可能になると考えられるが，性質の比較や使い分けの整理は現状では十分に進んでいない．

本論文では，(a)，(b) の代表手法としてそれぞれ Federated Learning, Data Collaboration を採用し，比較を行う．具体的には，現実的なデータセットを想定し PySyft [13] を用いたシミュレータを作成する．これは仮想マシンを複数台立てて仮想マシン間で通信を行い，複数機関による秘匿保護学習フローを再現するものである．仮想マシン間の通信から通信量の計測をして比較を行う．また，両手法の産業利用を想定し，導入コストの観点からスキーム構築案について検討を行う．本論文の主な貢献は下記の二点である．

- シミュレータを用いた比較により，Data Collaboration と Federated Learning に対して，要求される通信量の理論値と，オーバーヘッドを含む実測値が大きく乖離しないことを示した．
- 両手法の導入コストの差を踏まえて，産業利用を想定したスキーム案を示した．

2 背　　景

本章では，検証対象の手法について述べる．

2.1 Federated Learning

Federated Learning はモデルのパラメータ情報を共有することにより，組織横断でのモデリングを可能とする．Federated Learning では，モデルのパラメータ情報を集約させる中央サー

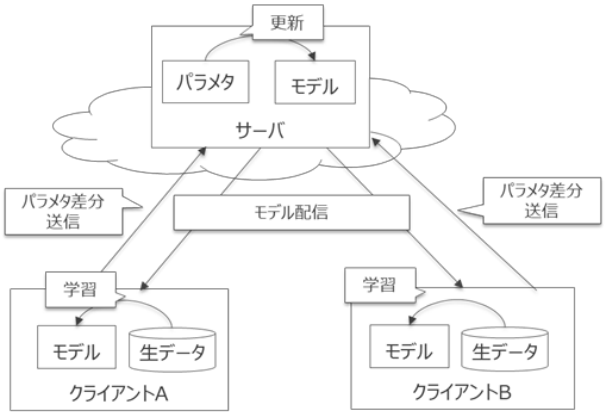

図 1　Federated Learning 概略図

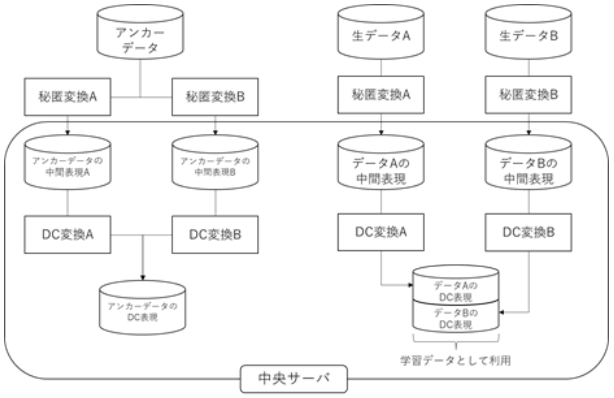

図 2　Data Collaboration 概略図

Algorithm 1 Federated Learning プロセス

1: 中央サーバがモデルを初期化し，そのモデル情報を全クライアントへブロードキャストする．
2: 各組織は受け取ったモデル情報を元に学習を進め，パラメータ更新差分を計算する．
3: 各組織はパラメータ更新差分情報を中央サーバに送信する．
4: 中央サーバは更新差分情報をモデルに反映させた後，モデル情報を全クライアントへ配信する．
5: 2-4 を学習が収束するまで反復的に実行する．

バを用意する．各データ提供組織は自組織が持つ学習データを用いてモデリングを行い，モデルのパラメータを更新する度に，パラメータの更新差分情報を中央サーバに送信する．中央サーバは受け取った更新情報をモデルに反映させた後，モデル情報を全クライアントへ配信することを繰り返す．以下に概略図として図 1，大まかなプロセスを Algorithm1 に示す．

2.2　Data Collaboration

Data Collaboration は各組織の生の学習データを秘匿化して，中間表現データを集約させてモデリングを行う手法である．こうすることで，生データを外部に流通させることなく安全にモデリングが実施できる．

X_i を組織 i が持つ生の学習データセットとする．写像 f_i を通した中間表現データセット $\tilde{X}_i$ を外部組織に流通させることを考える．d は参画組織の数，n_i は組織 i の学習データのサンプル数，l_i は写像 f_i の写像先の次元数を表す．

$$\tilde{X}_i = [\tilde{x_{i,1}}, \tilde{x_{i,2}}, ..., \tilde{x_{i1}}]^\top = f_i(X_i) \in \mathbb{R}^{n_i \times l_i}$$

$$\tilde{x}_{i,k} = f_i(X_i) \qquad (1 \leqq i \leqq d, 1 \leqq k \leqq n)$$

f_i は組織に依存する写像関数であるため，同一のデータサンプルについて，同一の写像先とはならない．そこで，さらに近似特徴空間に写像するために，各組織で定めた写像 G_i による変換を考える．なお，G_i は線形写像とする [5]．

$$G_i f_i(x) \approx G_j f_j(x)$$

このような写像 G_i による変換で，生データセットにおける各サンプルの関係性を保持したようなデータセットが得られる．この写像 G_i を構築するために，アンカーデータセット x_{anc} という共有してもよいダミーデータセットを用意する．このアンカーデータセット x_{anc} を使って，以下を満たすように写像 G_i を構成する．

$$G_i f_i(x_{anc}) \approx G_j f_j(x_{anc})$$

このアンカーデータセット x_{anc} は各クライアントの統計値から生成する．そのため，各クライアントは自身が保持するデータセットの統計値を外部に共有する必要があり，本技術は統計値がセンシティブデータにあたらないという前提のもと適用される．

Data Collaboration による統合学習データ作成までの概略図を図 2 に，プロセスを Algorithm2 に示す．データ提供組織であるクライアント以外のサーバとし統計値からアンカーデータセット x_{anc} を作成する中央サーバ A，写像 G_i を構成し統合学習データを作成する中央サーバ B を想定する．

Algorithm 2 Data Collaboration プロセス

1: 各データ提供組織は自組織データセットの統計情報を中央サーバ A に共有する．
2: 中央サーバ A は集約された統計データ情報を用いてアンカーデータセット x_{anc} を作成．
3: 中央サーバ A はアンカーデータセット x_{anc} を全組織に送信する．
4: 各データ提供組織は自前の秘匿化写像 f_i を用いて，アンカーデータ x_{anc} を中間アンカーデータセット $f_i(x_{anc})$ に変換．中央サーバ B に送信する．
5: それぞれの組織から集約した中間アンカーデータセット $f_i(x_{anc})$ を使って，中央サーバ B が写像 G_i を作成する．
6: 各組織は学習データを秘匿化写像で中間学習データ $f_i(x_i)$ を作成し，中央サーバ B に送信．このとき一緒に教師ラベルも送信される．
7: 中央サーバ B は中間学習データを，写像 G_i を使って，学習に使う統合学習データ $Gif_i(x_i)$ に変換する．

3　比 較 観 点

秘密保護学習技術においての産業利用性を議論するうえで，

考慮すべき比較観点を述べる．

精度

秘密保護学習技術では，精度評価の汎用的ベンチマークを設定することは難しく，精度評価方法はユースケースの目的によって設計する必要がある．例えば，テストデータをどのように作成するか，Federated Learning のようなモデルが複数生成される手法では評価対象とするモデルとして何を選定するかなどをユースケースに応じて適切に決めなければならない．

セキュリティ強度

メンバーシップ推定攻撃 [11] やモデル反転攻撃 [12] などのプライバシ攻撃手法に対して，理論的にどの程度の秘匿性を担保できるかといった観点での評価が求められる．ユースケースによって許容できるセキュリティリスクの範囲と程度が異なるため，ユースケースに応じた技術手法選定を円滑にするためにも事前にセキュリティ強度を整理する意義は高い．

要求計算資源

Federated Learning ではデータを拠出するクライアントの全てが，モデリングを実行可能な計算機環境を用意する必要がある一方で，Data Collaboration ではモデリング用の計算機環境は 1 ノードに抑えられる．

学習時間

秘密保護学習技術においては，学習処理において通信プロセスがボトルネックとなりうる．Federated Learning では，学習のイテレーション毎に，外部にモデルのパラメータ情報を共有するために，通信頻度が高い．そのため，通信時間がボトルネックとなり，モデリングに要する時間が著しく増大してしまう．それに対して，Data Collaboration 手法では，通信が発生するタイミングは学習前の秘匿化データを集約するまでのプロセスに限られており，Federated Learning の手法と比較して，通信量・通信回数が抑えられることが見込める．

精度，セキュリティ強度，要求計算資源を観点に議論された先行研究は多いものの [3] [4] [21]，秘匿保護学習技術の比較という枠組みで学習時間について議論されたものはほとんどない．そのため，本研究では学習時間の比較のため，Federated Learning と Data Collaboration で，使用する通信量を計測し，通信コストの比較を行う．

4 実　　験

本章では Federated Learning と Data Collaboration の通信量の比較を行う．まず二手法の理論上の通信量について計算した後，複数の仮想マシンを用いた実験によって通信のオーバーヘッドによって理論値と実際の値にどれほどの乖離が生じるかについて評価する．その後，他のデータセットで同様の実験を行った際の結果について，理論上の通信量の計算を通して考察する．

	ユニット数
入力層	109
中間層 1	100
中間層 2	100
出力層	2

表 1　ニューラルネットワーク構成

4.1 実 験 条 件

仮想ノード間でシミュレータを作成し単一マシン内で通信量の計測を行った．シミュレータの作成には PySyft[11] を使用した．学習モデルとしてニューラルネットワークを採用し，3 層の全結合層で構成した（1）．本実験では，Federated Learning のイテレーション数と通信量の関係，および，参画組織の数と通信量の関係を示す．クライアント数を 2，バッチサイズを 100 として，エポック数が 1, 10, 100 の場合についてそれぞれ総通信量と総通信回数を測定した．

4.2 データセット

データセットは Census Income Data [14] を使用した．これは 14 カラムからなるデータ数 48,842（今回は学習データ数 32,560，テストデータ数 16,240 に分割して検証）の 2 値分類タスク向けデータセットである．モデリングにあたって，カテゴリ変数についてはワンホット表現に変換するという前処理を挟み，最終的なカラム数は 109 となった．Data Collaboration では中間表現のカラム数を 13 とした．

4.3 理論上の通信量

まず，比較対象の二手法それぞれにおける理論上の通信量の計算式について述べる．Federated Learning の通信量 C_f は，モデルサイズ m，イテレーション数 r，クライアント数 n で表現でき，以下のようになる．

$$C_f = 2mrn$$

一方で，Data Collaboration の通信量 C_d は，アンカーデータセット容量 A，中間アンカーデータセット容量 A'，各クライアントの中間表現データセット容量 d_i の総和を合わせたものである．

$$C_d = An + A'n + \sum_{i=1}^{n} d_i$$

次に，本章での実験条件において期待される通信量について述べる．なお，モデル，およびデータのパラメータは単精度型 (4 byte) とした．

Federated Learning の計算量について述べる．表 5.1 よりモデルのパラメータ数は約 21,100 と見積もられる．1 パラメータあたり 4byte(32bit) であるから，モデル容量 m は

$$m = 4 \times 21,100 = 84,400 \quad (byte)$$

イテレーション数 r, クライアント数 n はそれぞれ 163, 2 であ

エポック数（イテレーション回数）	Federated Learning	Data Collaboration
1 (163)	69	10
10 (1,630)	681	10
100 (16,300)	6,852	10

表 2　Federated Learning と Data Collaboration 総通信量比較 (MB)

エポック数（イテレーション回数）	Federated Learning	Data Collaboration
1 (163)	752	6
10 (1,630)	7,520	6
100 (16,300)	75,200	6

表 3　Federated Learning と Data Collaboration 総通信回数比較

るから

$$\begin{aligned} C_f &= 2mrn \\ &= 2 \times 84,400 \times 2 \times 163 \\ &= 55,028,800 \quad (byte) \\ &\fallingdotseq 55 \quad (MB) \end{aligned}$$

よって，1 epoch あたりに発生する通信量はおおよそ 55MB であると推測される．10 epoch なら 550MB，100 epoch なら 5.5GB というように線形にスケールすることが期待される．

次に，Data Collaboration の計算量について述べる．生データのカラム数は 14，中間表現のカラム数は 13，データのサンプル総数は 32,560 であるから

$$\begin{aligned} \sum_{i=1}^{n} d_i &= 13 \times 32,560 \times 4 = 1,693,120 \quad (byte) \\ A &= 14 \times 32,560 \times 4 = 1,823,360 \quad (byte) \\ A' &= 13 \times 32,560 \times 4 = 1,693,120 \quad (byte) \end{aligned}$$

よって，クライアント数 n が 2 のとき，

$$\begin{aligned} C_d &= An + A'n + \sum_{i=1}^{n} d_i \\ &= 1,823,360 \times 2 + 1,693,120 \times 2 + 1,693,120 \\ &= 8,726,080 \quad (byte) \qquad \fallingdotseq 9 \quad (MB) \end{aligned}$$

よって，Data Collaboration で発生する通信量は約 9MB と推測される．

4.4 結　　果

本実験では参画クライアント数を 2 として計測した．計測結果を表 2 と表 3 に示す．表 2 は両手法の実行中に発生した通信量について，表 3 は総通信回数について，エポック数ごとにまとめたものである．なお，Data Collaboration の通信量はエポック数に依らず一定である．

表 2 に二つの手法の総通信量を示す．4.3 節との比較から，理論上の通信量との乖離は大きくなく，本章の実験設定においては通信のオーバーヘッドは通信量に大きな影響を与えなかった

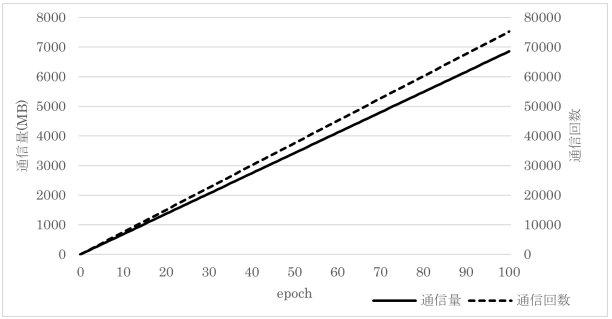

図 3　Federated Leanring における epoch 数と通信量・通信回数の関係

ことが分かる．

次に，本章の実験における二つの手法の通信量について分析する．表 2 の総通信量に加えて，表 3 に総通信回数を，図 3 に Federated Leanring における epoch 数と通信量・通信回数の関係を示す．Federated Learning は通信量，通信回数ともにイテレーション回数に比例して増大する傾向にあることがわかる．通信回数については，Data Collaboration は各ノードが 3 回ずつデータを送受信するのみであるため，イテレーション毎に各ノードが通信する Federated Learning よりも通信回数が極めて少ない．また，6 回という少なさから Data Collaboration はオンラインでの通信を前提とせずに適用可能な手法であるといえる．

次に，異なるデータセットを用いた場合の結果について述べる．本実験では，通信量に関して Federated Learning の方が大きくなっているが，Federated Learning の通信量はモデルサイズとイテレーション回数に依存し，Data Collaboration の通信量はデータセットサイズに依存するため，通信量の多寡を本実験の結果のみから結論付けることはできない．一方で，理論上の通信量と実際の通信量には大きな乖離が生じないことも確かめられている．そこで，代表的なデータセットとモデルに対し，その学習にかかるイテレーション数から Federated Learning と Data Collaboration の理論上の通信量の概算値を算出し比較する（表 4）. [15] [16] [17] [18] で言及されているモデルの収束に要したイテレーション数を参照し，4.3 節で示した式で両手法の通信量を算出した．推測した理論値としての通信量と先の実験から得られた実測値は大きく乖離しなかったことから，概ね実測値に近しい通信量が算出されたと期待できる．imageNet [19] のデータセットサイズは 1,200, CIFAR-10 [20] は 50,000 とし，データ型は単精度浮動小数点 (32bit) を使用するものとした．比較対象としたデータセットとモデルではいずれも Federated Learning の通信量は Data Collaboration の 1,000 倍以上大きくなった．学習対象とするデータセットサイズが大きくなるにしたがって，Data Collaboration の通信量は増えるが，それ以上に Federated Learning では適切なモデルのパラメータ数とその収束に必要なイテレーション数が大きくなり，通信量が増大することがわかる．したがって，多くの場合で Data Collaboration の方が低い通信コストで適用可能な手法であるといえる．

データセット	モデル	入力画像サイズ	モデルパラメータ数	イテレーション数	FL 通信量	DC 総通信量
imageNet	AlexNet	224 × 224	60M	844K	405,000.0 GB	362.0 GB
imageNet	VGG-16	256 × 256	138M	370K	808,000.0 GB	472.0 GB
imageNet	Noisy Student	224 × 224	9.2M	205K	15,000.0 GB	362.0 GB
CIFAR-10	NesT-T	32 × 32	6M	59K	708.0 GB	1.3 GB

表 4　代表的データセットとモデルでの総通信量比較 [15] [16] [17] [18]
通信量は 1 クライアントあたりの量で算出.

5　産業利用における二手法の比較

本実験で得られた知見に基づき，Federated Learning と Data Collaboration の適用条件とその適するユースケースについて整理する．適するユースケースの整理においては，本研究で示された知見に加えて，Bodganova [21] の示した参画クライアント数が少ない場合に Data Collaboration の精度が優れる傾向があるという知見も考慮する．二手法それぞれについて，得意とする条件を整理したものを下記に示す.

- Federated Learning
  - 高い通信頻度，膨大な通信量をともに許容できる.
  - 参画クライアントごとに学習用の計算リソースを用意可能.
  - モデリング学習に費やせる時間的余裕がある.
  - 参画クライアントが多い [21].

- Data Collaboration
  - 許容できる通信頻度，通信量が限られている.
  - インターネット通信環境を構築するのが困難.
  - 学習用の計算リソースが限られている.
  - 参画クライアントが少ない [21].

まず，導入コストの点で比較を行うと，Federated Learning は大規模なデータセット，かつ，十分な通信・計算リソースを割くことができる場合に，Data Collaboration はリソースを節約したい場合に適するということから，Federated Learning の方が Data Collaboration よりも導入コストが高い傾向にあるといえる.

秘密保護学習技術の選定を行う際に考慮すべき要素として，秘密保護学習は組織横断でデータを活用する技術であり，かつその効果は適用前に見積もりづらいという点がある．秘密保護学習技術は組織横断でデータを活用することで，高精度なモデルを作成することを目的にしている．すなわち，活用可能なデータサンプル数が増えることで，データバリエーションの網羅性を上げることを期待しており，他組織に自組織に不足しているようなバリエーションのサンプルがあるのが望ましい．反対に，組織間でデータのバリエーションが似通っていれば，秘密保護学習技術の効能は得られにくい．また，Federated Learning と Data Collaboration の両手法とも，外部へデータの解像度を下げて共有することで，秘匿性を担保している点においては共通している．モデル精度への影響を考慮すると，解像度を落とすプロセスで，データがもつモデリングへの寄与度の高い特徴を欠落させないことが望ましいが，どちらの手法がそれに優れるかを一般に結論付けることは難しい．つまり，秘密保護学習技術の適用効果があるかはデータセットに強く依存する．以上のことから，モデル学習前から適用効果を見積もることが困難である.

しかしながら，産業利用において高精度なモデルを作成できるという確証が得られないままでは，組織横断でのモデリングを進めにくい．導入コストが高いならば尚更である．上記の議論から，まず，導入コストの低い Data Collaboration で組織横断でのデータ活用に有効性があるのかを検証し，適用効果が認められれば，Federated Learning でのモデリングを導入するといったユースケースが考えられる．また，データ活用することへの有益性を示すことができれば，場合によっては，組織間で直接データを流通させるようなスキーム構築に貢献できうる.

6　結論と今後の課題

本研究では，秘密保護学習手法である Federated Learning と Data Collaboration の通信量について，具体的なデータセットを想定し，シミュレータによる比較検証を行い，Data Collaboration が Federated Learning に対して，通信量を抑えられる傾向にあることを確認した．また，両手法の産業利用を想定した場合，導入コストの低い Data Collaboration で組織横断でのデータ活用に有効性があるのかを検証し，その結果を踏まえて，Federated Learning や組織間で直接データを流通させるなどのスキーム構築の可能性が示唆された．一方で，検証事例が少なく，期待効果の見積もりが困難だという課題があり，今後様々な事例で検証を進める必要がある.

文　献

[1] 総務省. 令和 2 年版 情報通信白書 第 1 部. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf

[2] Konečný, Jakub, et al. "Federated learning: Strategies for improving communication efficiency." arXiv preprint arXiv:1610.05492 (2016).

[3] Li, Qinbin, Zeyi Wen, and Bingsheng He. "Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection." (2019).

[4] Li, Tian, et al. "Federated learning: Challenges, methods, and future directions." IEEE Signal Processing Magazine 37.3 (2020): 50-60.

[5] Akira Imakura, Tetsuya Sakurai, Data Collaboration Analysis Framework Using Centralization of Individual Intermediate Representations for Distributed Data Sets, ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, Vol. 6, Issue 2, 04020018,

2020.

[6] Akira Imakura, Xiucai Ye, Tetsuya Sakurai, Collaborative Data Analysis: Non-Model Sharing-Type Machine Learning for Distributed Data, In: Uehara H., Yamaguchi T., Bai Q. (eds) Knowledge Management and Acquisition for Intelligent Systems. PKAW 2021. Lecture Notes in Computer Science, vol 12280. Springer, Cham, pp. 14-29, 2021.

[7] Akira Imakura, Hiroaki Inaba, Yukihiko Okada, Tetsuya Sakurai, Interpretable collaborative data analysis on distributed data, Expert Systems with Applications, Vol. 177, 114891, 2021.

[8] Mohassel, Payman, and Yupeng Zhang. "Secureml: A system for scalable privacy-preserving machine learning." 2017 IEEE symposium on security and privacy (SP). IEEE, 2017.

[9] Wagh, Sameer, Divya Gupta, and Nishanth Chandran. "SecureNN: 3-Party Secure Computation for Neural Network Training." Proc. Priv. Enhancing Technol. 2019.3 (2019): 26-49.

[10] 三品気吹, 濱田浩気, and 五十嵐大. "平文上の処理ロジックを再現した秘密計算ディープラーニング." IEICE Conferences Archives. The Institute of Electronics, Information and Communication Engineers, 2019.

[11] Shokri, Reza, et al. "Membership inference attacks against machine learning models." 2017 IEEE symposium on security and privacy (SP). IEEE, 2017.

[12] Fredrikson, Matt, Somesh Jha, and Thomas Ristenpart. "Model inversion attacks that exploit confidence information and basic countermeasures." Proceedings of the 22nd ACM SIGSAC conference on computer and communications security. 2015.

[13] `https://github.com/OpenMined/PySyft`

[14] `https://archive.ics.uci.edu/ml/datasets/Census+Income`

[15] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. "Imagenet classification with deep convolutional neural networks." Advances in neural information processing systems 25 (2012): 1097-1105.

[16] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." ICLR (2015).

[17] Xie, Qizhe, et al. "Self-training with noisy student improves imagenet classification." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020.

[18] Zhang, Zizhao, et al. "Aggregating nested transformers." arXiv preprint arXiv:2105.12723 (2021).

[19] Deng, Jia, et al. "Imagenet: A large-scale hierarchical image database." 2009 IEEE conference on computer vision and pattern recognition. Ieee, 2009.

[20] `https://www.cs.toronto.edu/~kriz/cifar.html`

[21] Anna Bogdanova, Akie Nakai, Yukihiko Okada, Akira Imakura, Tetsuya Sakurai, Federated Learning System without Model Sharing through Integration of Dimensional Reduced Data Representations, In: Proceedings of International Workshop on Federated Learning for User Privacy and Data Confidentiality in Conjunction with IJCAI 2020 (FL-IJCAI'20), 2021.