1ZA-02

プライバシ保護が必要な個人データに対応した分散機械学習モデルの検討

高野 紗輝† 中尾 彰宏†† 山口 実靖††† 小口 正人†
† お茶の水女子大学 †† 東京大学 ††† 工学院大学

1 はじめに

近年，スマートフォンや IoT デバイスのの普及および性能向上により，エッジデバイス上に膨大なデータが蓄積されるようになった．さらに，おすすめ表示や画像認識などと様々な場面で機械学習が活用されるようになり，エッジデバイスで収集した個人情報を含む大量のデータに対して，プライバシを守りながら機械学習を行うことが期待されている．

そこで，federated learning [1] などデバイス上にある個人情報を保護しながらそれらのデータをサーバ上での機械学習に用いることが盛んに研究されている．しかし，個人情報の一部をエッジデバイスの外へと持ち出すため，プライバシ保護が十分であるとはいえず [2]，機密性が高くデバイスの外へ情報を一切持ち出したくない個人データを学習に用いることができない．本研究ではリッチクライアントの登場により機械学習等の複雑な処理もエッジデバイス上で行うことが可能になったことと合わせ，エッジサーバと連携しつつエッジデバイス上でも機械学習を動かすプライバシ保護に優れた分散機械学習モデルの検討を行う．

2 提案モデル

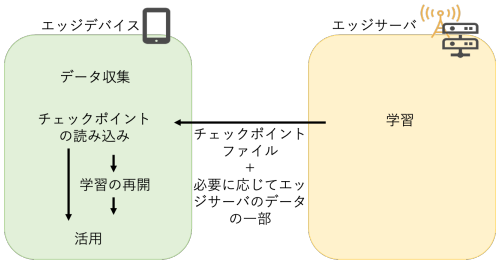

図 1: 提案モデル

図 1 に示す通り，エッジコンピューティングモデルにおいて従来エッジサーバ上で行っていたタスクの一部をエッジデバイスにオフロードすることでエッジデバイス上でも機械学習処理を行う．このモデルでは，エッジデバイスで収集した個人情報はエッジデバイス内のみで処理を行い，エッジサーバへ情報を一切渡さないという特徴を持つため，安全に個人情報を活用することができる．

3 実験

3.1 実験環境

使用したエッジサーバの性能は，OS Ubuntu 18.04 LTS，CPU Intel Core i7-8700，GPU GeForce RTX 2080Ti, Memory 32 Gbyte であり，エッジデバイスとして使用した Jetson Nano の性能は，OS Ubuntu 18.04 LTS, CPU Quad-core ARM A57 @ 1.43 GHz，GPU 128-core Maxwell，Memory 4 GB 64-bit LPDDR4 25.6 GB/s である．Jetson Nano は GPU を搭載した小型 AI コンピュータボードであり，近い将来スマートフォンや様々な IoT デバイスがこのような性能を持つことが期待される．

実験データとしては実際のアプリケーションなどで使用されることが想定される機密性が高く，容量の大きな顔画像を用いる．インターネット上より集められた jpg 画像を人物ごとにフォルダ分けしてある Labeled Faces in the Wild (以下 lfw) [3] から，それぞれの人物の写真約 30 枚のうち 2 割をテストデータ，残りを訓練データとしてぼかし等により 9 倍にして使用する．

32 名のデータを用い，エッジサーバとエッジデバイスにおいて同等の精度を得るための実行時間を比較すると，エッジデバイスはおよそ 20 倍の時間がかかり，65%の精度を得るために 2 時間以上の学習が必要となる．低速ではあるものの，エッジデバイス内のみでも十分学習できるが，エッジデバイスのみでの学習には限界があり，エッジサーバとの連携が重要になる．

3.2 実験概要

初めにエッジサーバにおいて個人情報を含まない一般的なデータを用いて十分学習させ，学習の重みを保存したチェックポイントファイルと必要に応じてエッジサーバのデータの一部をエッジデバイスへと送信する．そして，エッジデバイス側で個人の顔画像も含むデータを使って学習を再開させる．ここでは lfw に含まれている Tony をエッジデバイス上の個人情報とし

A Distributed Machine Learning Model for Privacy-Protective Personal Data
†Saki Takano ††Akihiro Nakao †††Saneyasu Yamaguchi †Masato Oguchi
†Ochanomizu University
††the University of Tokyo
†††Kogakuin University

て 86 枚の顔画像をぼかし等で 9 倍に加工したものを使用する．

3.3 実験結果

エッジサーバから全てのデータをエッジデバイスへと送信した際の結果を図 2 に示す．ここでは全体の 10%を個人情報が占める test データを用い，エッジデバイスでチェックポイントファイルを読み込む直前からの時間を横軸として学習精度との関係を比較する．

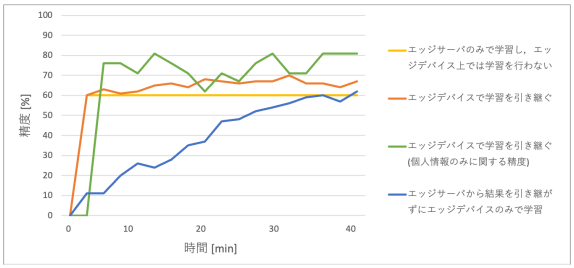

図 2: エッジデバイスがエッジサーバの全てのデータを保持している際の精度

エッジデバイス上における個人データを含む学習によって全体の精度および個人情報に対する精度が上がる．さらにエッジサーバから学習を引き継がずにエッジデバイスのみで学習を行うと，エッジデバイスの性能はエッジサーバに比べ低いため，精度が上がるまでにかなりの時間がかかり，エッジサーバの助けを借りることが有効だと言える．

しかし，エッジサーバの全てのデータを送受信することは非現実的であるため，一部のみを受け取ることを考える．エッジサーバからエッジデバイスへと送信するデータ量をエッジサーバのデータの 0〜10 割と変化させた際の結果を図 3〜5 に示す．

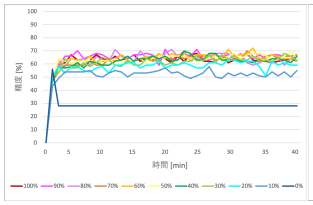

図 3: 一般的なデータを 10 人とした際の精度

図 4: 一般的なデータを 20 人とした際の精度

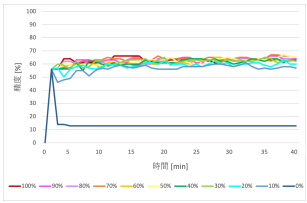

図 5: 一般的なデータを 30 人とした際の精度

一般的なデータを一切含めずに個人情報のみで学習した 0 割の際は，一般的なデータに対応できずに低い精度となり，エッジデバイス上での学習にも一般的なデータを含める必要がある．一般的なデータを 1 割，2 割と多少含めることで精度がかなり上がり，3 割，4 割と一般的なデータを増やしていくとこのデータセットでの学習の上限近くまで精度が上がる．一方，9 割，10 割とデータを増やした場合であっても，精度は 3，4 割の場合とほぼ同じ結果となり，エッジデバイスの性能や画像を転送する通信コストを考慮すると全てのデータをエッジサーバからエッジデバイスへと送信することは好ましくないと考えられる．

4 結論

以上の実験より，エッジサーバにおいて一般的なデータで学習を行い，エッジデバイスで学習を引き継ぐことで早い段階において精度の高い学習結果を得ることができ，本提案モデルを用いることで機密性の高いデータも含めた学習が可能となる．さらに，エッジデバイス上での学習には一般的なデータを含める必要があり，このデータ構成においては，エッジサーバのデータのうち 1 割与えるだけでかなり良い精度となり，3 割与えると上限近くまで学習可能となる．

5 まとめと今後の課題

エッジデバイスの外へと持ち出したくない個人データを含めた学習を可能とすることを目的として，リッチクライアントを用いた分散機械学習モデルの検討を行った．Jetson Nano を用いて実装した結果，プライバシ保護が可能であり，今回のデータ構成においてはサーバのデータのうち 3 割程度を受け取るだけで良い精度を得ることが可能であることが示された．

今後はデータを変化させて実験を行い，様々な個人情報に対応したより良いモデルの検討を予定している．

謝辞

本研究は一部，JST CREST JPMJCR1503 の支援を受けたものである．

参考文献

[1] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, Vol. 10, No. 2, pp. 1–19, 2019.

[2] Mengkai Song, Zhibo Wang, Zhifei Zhang, Yang Song, Qian Wang, Ju Ren, and Hairong Qi. Analyzing user-level privacy attack against federated learning. *IEEE Journal on Selected Areas in Communications*, Vol. 38, No. 10, pp. 2430–2444, 2020.

[3] Labeled Faces in the Wild. `http://vis-www.cs.umass.edu/lfw/`. (2021/04 閲覧).