IoT デバイスセキュリティに向けた フォグコンピューティングと連合学習に関する研究

Study on Fog Computing and Federated Learning for IoT Devices Security

白石敬典・法制倫理分科会・情報セキュリティ大学院大学

***Abstract*—**In recent years, IoT devices have become increasingly popular. Many companies are sending huge amount of data generated by IoT devices to Cloud environment for analysis using AI, etc., and utilizing the data as valuable information for their business. On the other hand, IoT devices and data generated by IoT devices have security and privacy issues. In this paper, we discuss the research on Fog Computing and Federated Learning that have been proposed recently to address these issues.

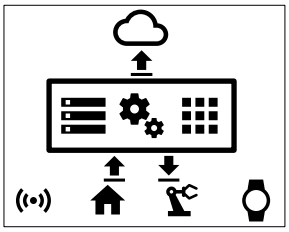
本研究の背景

近年 IoT デバイスの普及が進んでいる．多くの企業が IoT デバイスが生成する膨大なデータをクラウド環境へ送り AI 等を用いて分析し，価値のある情報としてビジネスに活用している．一方 IoT デバイスや IoT デバイスが生成するデータにはセキュリティやプライバシーの問題が存在する．本研究は，これら諸問題に対して近年提唱されたフォグコンピューティングと連合学習を応用し，対処する方法について検討するものである．

フォグコンピューティングとは

ネットワーク機器メーカー Cisco Systems, Inc. が提唱するネットワークアーキテクチャ．IoT デバイスの近くでデータ処理を行い，クラウド環境の負荷分散処理を目的とした階層型モデル．

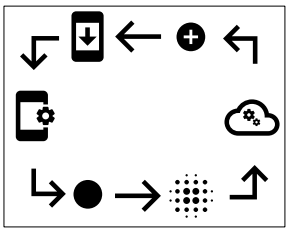
主な機能	
1	リアルタイムデータ受信
2	リアルタイム分析 App 実行
3	リアルタイム処理要求への応答
4	一時的なデータストレージ機能
5	データのクラウドへの送信



連合学習とは

Google LLC が提唱する機械学習手法．IoT デバイスがそれぞれ独立してローカルデータに基づき，現在のモデルの更新を計算．その更新を中央サーバに伝達し、IoT デバイスの更新を集約し新しいグローバルモデルを計算することが可能．

学習モデルの更新手順	
1	基本モデルのダウンロード
2	エッジデバイスでの学習処理
3	特徴量のみを抽出・共有
4	特徴量を使いモデルを更新
5	以降、同様の処理を繰り返す

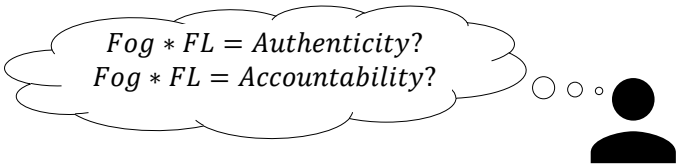


検討している方法

IoT デバイスセキュリティを守るため，フォグコンピューティングと連合学習を組み合わせた新たな方法を検討．

本研究が目指す方向性

フォグコンピューティングと連合学習は，通信にかかるオーバーヘッドの削減や，データプライバシーの保護に対して有益な手段．これら技術を用いて真正性 (Authenticity) や責任追跡性 (Accountability) を実現するため課題を明確にし，実社会における実現可能なモデルケースの確立を目指す．



本研究の進め方

スマートシティを具体的なユースケースと想定
- スマートシティで利用される IoT デバイスの特定
- やり取りされるデータの分類と課題の明確化
- 技術要素に関する学習，及び環境の構築・評価
- 実現可能なモデルケースの確立
- 対外的発表 (CSS2022，第84回全国大会)

参考文献

[1] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Goren, and C. Mahmoudi, "Fog Computing Conceptual Model", NIST special publ (SP) 500-325, 2018
[2] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, and A. Leon-Garcia, "Fog Computing: A Comprehensive Architectural Survey", IEEE Access (Volume: 8), 2020
[3] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtarik, A. T. Suresh, and D. Bacon "Federated Learning: Strategies for Improving Communication Efficiency", NIPS Workshop on Private Multi-Party Machine Learning (2016)
[4] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of Things intrusion Detection: Centralized, On-Device, or Federated Learning?", IEEE Network (Volume: 34, Issue: 6, November/December 2020)
[5] Google Developers, "フェデレーション ラーニング：集中トレーニング データを使用しない協調機械学習", https://developers-jp.googleblog.com/2017/05/federated-learning-collaborative.html, (参照 2021/0/2/12)