基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出　　2022 年度年次報告書

2021 年度採択研究代表者

田浦 健次朗

東京大学 大学院情報理工学系研究科
教授

実応用に即したプライバシー保護解析とセキュアデータ基盤

主たる共同研究者:

曹 洋（北海道大学 大学院情報科学研究院 准教授）
花岡 昇平（東京大学 医学部附属病院 専任講師）
塙 敏博（東京大学 情報基盤センター 教授）
吉川 正俊（京都大学 大学院情報学研究科 教授）

研究成果の概要

[1] プライバシー保護を強制可能なシステム(プライバシーサンドボックス)の実装方式検討を行い, WebAssembly 上にプロトタイプを作成した. また, プライバシー保護データ解析の実践例としてコロナ禍に東京大学で行われた Zoom 会議の通信品質調査を行った（情報処理学会 IOT 研究会藤村記念ベストプラクティス賞）.
[2] 機械学習タスクのための信頼できるデータ取得を促進するために, 信頼できないブローカーからプライバシーを保護する局所的プライベートモデル市場機構を提案した. この市場機構では, データ所有者が局所的な差分プライバシーにより局所的に勾配を変化させることを可能にし, プライバシー漏洩リスクを低減させることができる.
[3] 差分プライバシー(DP)が両側のエラー(two-sided errors, 即ち, Type I Error と Type II Error)を生む問題に対し, 非対称差分プライバシー(Asymmetric DP, ADP)を提案した. ADP は, 現実の一部のデータだけ機微である状況に対して, 適切なプライバシー保護を提供できる. また, 実世界のデータセットを用いた実験で, ADP の有用性と実現可能性が示された.
[4] 差分プライバシーを用いた連合学習の基礎的な実験に資するため, 2 つの発表を行った. すなわち架空肺癌症例の胸部単純写真の多数自動生成についてと, 3D U-Net を用いた頭部 MRI 画像の脳動脈瘤自動検出についての発表である. さらに差分プライバシーによる医用画像の匿名化手法を開発し, その AI による肺炎検出性能へ与える影響について検討, 発表し, 論文執筆中である.
[5] 公開鍵に基づく暗号化を行うユーザレベルファイルシステムを, encfs (共有鍵に基づく暗号化ファイルシステム)を元に基本方針を検討した.プロセスメモリの覗き見に対する耐性のある共有取り消しのための機構として SGX の適用範囲を検討した. 暗号化による方法と並行して, ユーザ/ファイルの権限管理で共有/非共有を Linux Security Module により実現する方法についても検討した.

【代表的な原著論文情報】

1) Takagi, Shun, Fumiyuki Kato, Yang Cao, and Masatoshi Yoshikawa. "Asymmetric differential privacy." In 2022 IEEE International Conference on Big Data (Big Data), pp. 1576-1581. IEEE, 2022.
2) 2) Shuyuan Zheng, Yang Cao, Masatoshi Yoshikawa, Huizhong Li, Qiang Yan: “FL-Market: Trading Private Models in Federated Learning”, Proc. of the IEEE International Conference on Big Data, pp. 1525-1534, Dec. 2022.3)
3) Hiraishi, Ryota, Masatoshi Yoshikawa, Shun Takagi, Yang Cao, Sumio Fujita, and Hidehito Gomi. "Mitigating Privacy Vulnerability Caused by Map Asymmetry." In Data and Applications Security and Privacy, pp 68-86, DBSec 2022.
4) 空閑 洋平, 中村 遼.「遠隔会議システムの計測データを用いた広域ネットワーク品質計測」インターネットと運用技術シンポジウム論文集, pp.31-38. 情報処理学会(2022).