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
2021 年度採択研究代表者

2021 年度
年次報告書

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

§1. 研究成果の概要

[1] 管理者への信頼に依拠しないセキュアファイルシステム

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)を元にプロトタイプを作成した。 その過程で、 共有取り消しのための機構は、プロセスメモリの覗き見に対する体制はないことが明らかになった。 これ以降、 TEE (Trusted Execution Environment)、 具体的には Intel Software Guard eXtension (SGX)を用いてこの問題を解決する方向性が定まった。

[2] プライバシー保護を強制・追跡可能なシステム機構

プライバシー保護を強制するための基本的な枠組みの設計を行った。 その中のひとつである、サンドボックスの実装方法について有望な方向性が明らかになった。

[3] 柔軟なプライバシー保護データ解析・機械学習

1. 連合学習における参加インセンティブ付与とプライバシー保護に関する研究を行った。 局所差分プライバシーに基づく連合学習用データ市場を設計し、雑音が少ないプライベートモデルを取引するインセンティブを与える学習機能付きオークション機構と、最適なモデル更新のために局所的な勾配を正確な大域的勾配に集約するための集約機構を開発した。

2. パーソナルデータ市場における価格設定:

市場からのデータ購買者による裁定行動を防ぐために従来研究されてきた無裁定価格設定の概念を拡張し部分的無裁定価格設定を導入しその性質を明らかにした。

3. 非対称差分プライバシー:

データによってプライバシー保護程度が異なるような非対称型の差分プライバシーの概念を定式化しそれを実現するための具体的なプライバシー保護機構を与えた。

[4] 医療・軌跡データ実応用での実証

「汎用の医用画像-付帯情報データベース」については、「プライバシー保護を強制・追跡可能なシステム機構」に画像を処理する機能を付加することを考えている。 flow-based generative model の一種である Glow アルゴリズムを用いて画像をベクトル化し、 それを global differential privacy を用いて処理するものについて、 実装可能性を検討中である。 なお、local differential privacy を画像に適用する手法については既報はあるが、 我々でも Glow をベースにした実装を行い、 只今論文執筆中である。

§2. 研究実施体制

(1)田浦グループ

① 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)

② 研究項目

・セキュア分散ファイルシステムの方式設計

・セキュア分散ファイルシステムの実装

・セキュアストレージとプライバシー保護システム機構の連携・統合

・プライバシー保護システム機構の方式設計・API 設計

・プライバシー保護システム機構の実装

・プライバシー保護システム機構へのフィードバック

・セキュアファイルシステム・プライバシー保護機構へのフィードバック

(2)吉川グループ

① 主たる共同研究者:吉川 正俊 (京都大学 大学院情報学研究科 教授)

② 研究項目

・データ保護型処理検証機能の開発

・データの意味を考慮した差分プライバシーに基づくデータ解析

・医療データ実応用システムにおけるプライバシー保護システム・データ解析の検証

(3)花岡グループ

① 主たる共同研究者: 花岡 昇平(東京大学 医学部附属病院 専任講師)

② 研究項目

・federated learning の細粒化

・同意撤回可能な個人情報保護システム上での医用 AI ソフトウェア作成実証

(4)塙グループ

① 主たる共同研究者: 塙 敏博(東京大学 情報基盤センター 教授)

② 研究項目

・セキュア分散ファイルシステムの方式設計

・データ処理オフローディング, TEE によるセキュリティ機構の設計

・セキュア分散ファイルシステムの実装

・セキュア分散ファイルシステムによる実応用プラットフォーム提供と実証実験サポート