2023 年度年次報告書
社会変革に向けた ICT 基盤強化
2022 年度採択研究代表者

三輪 忍

電気通信大学 大学院情報理工学研究科
准教授

HPC ユーザのための TEE 利用支援フレームワーク

研究成果の概要

HPC ユーザのための TEE 利用支援フレームワークの開発を目指して，本年度は主に TEE の基本性能評価を行った．

最新の SGX フレームワークである Gramine を用いて，SGX がノードのコア性能とメモリ性能に与える影響をそれぞれ評価した．コア性能の評価には GEMM を，メモリ性能の評価には STREAM と linked-list traversal を行うプログラムをそれぞれ使用した．また，HPC ベンチマークに関しては，先行研究で使用された複数のアプリケーションに加えて Pytorch アプリケーションの性能評価を行った．評価の結果，コア性能に関しては Gramine+SGX の影響がほとんどなかった一方で，メモリ性能に関してはバンド幅が最大 13%，レイテンシが最大 2.7 倍低下することを確認した．また，HPC ベンチマークに関しては，Gramine+SGX によるアプリケーション性能の低下は最大で 4.4 倍，平均 1.5 倍であった．以上の結果より， Gramine+SGX による性能低下は多くのアプリケーションにおいて許容範囲内であることが確認できた．以上の研究成果は，2023 年 11 月に開催された高性能計算分野のトップカンファレンスの 1 つである SC23 の併設ワークショップにて発表を行った[1]．現在は，Gramine+SGX がノード間の通信性能に与える影響を評価するための実験準備を進めているところである．

上記以外にも，本年度は，提案システムのターゲットアプリケーションとして，オープンデータ（例えばオープン医療画像）とコンフィデンシャルデータ（例えばある医療機関が所有する患者データ）を混合して分散深層学習を行うアプリケーションを選定した．また，脅威モデルに関して，特権ユーザによる攻撃を想定し，ノード間で共有の鍵管理システムを用いてプロジェクトごとの鍵ペアを管理するシステムを考案した．さらに，与えられたアプリケーションコードから TEE 実行を行う部分コードをプログラムスライシングによって抽出する LLVM パスの開発に着手した．具体的には，以前に別の研究で研究代表者が実装したプログラムスライシングを行う LLVM パスを最新の LLVM-19.0.0 に移植する作業を行った．

【代表的な原著論文情報】

1) S. Miwa, and S. Matsuo, Analyzing the Performance Impact of HPC Workloads with Gramine+SGX on 3rd Generation Xeon Scalable Processors, The SC'23 Workshops of the International Conference on High Performance Computing, Network, Storage, and Analysis (SC-W'23), pp. 1850-1858 (Nov 2023).