“Hariram, Veeramani”
Review for Paper Titled:

“Cerebro: A Platform for Multi-Party Cryptographic Collaborative Learning”

1- Summary

This work presents an end-to-end collaborative platform that enables parties to Compute learning without sharing PlainText Data which is also an order of magnitude faster compared to equivalent State of the art Platforms.
The Two obstacles that this work intends to ease are “Generality and Performance”- where the hand-tuning MPC for specific learning tasks & choice of generic and sub-generic protocols only make the task of choosing the right combination of tools as well as optimizations in an efficient secure execution more difficult and daunting. The second obstacle is the inherent conflict between the Transparency and Privacy interests of the participating parties. This work accomplishes these tasks by introducing multiple Compute & Auditing policies, optimizations and by extending support to Multiple Backends that support both Semi-honest and malicious security by adding Domain Specific Language (DSI) and API support for all these functionalities.

2- Novelty/Contribution

Specifically, Cerebro which is built on top of SCALE-MAMBA introduces many supports and functionalities related to the notions of Secure computing and Privacy. In order to support both Arithmetic and Boolean MPC, this work contributes to design of Boolean Circuit Generator based on EMP-toolkit. This in addition to the Arithmetic Circuit Generator permits the users to write programs that could be compiled into different secure computation representations. Cerebro also implements different cryptographic backends that support both semi-honest and malicious security using State of the art Malicious Frameworks SPDZ and AG-MPC.

3- Evaluation

This work carries out both Microbenchmark based evaluations based on Fitting cost models, Vectorization and Layout planning and evaluations based on Machine learning applications such as Decision tree prediction, Logistic regression via SGD and Linear regression via ADMM, various Compute policies such as Threshold-based validation, Accuracy comparison and cross validation and Differential privacy, Model Memorization policies. When evaluation against Hand-tuned protocols, Cerebro is found to have 25x times speed improvement during evaluation.

4- Unique Strength/Weakness

Until reading this paper, I never thought of the idea of having an integrated platform which can not only support multiple backends needed for Efficient Secure computation but also offer rigorous Evaluation policies across different aspects along with DSL based automatic optimizations being offered- such an end-to-end approach is the strength of this work.