Summary of SHE and GAZELLE For Providing Secure Neural Network Inference

Author: Sultan Aloufi
Mentor: Lei Jiang

Introduction

• Problem Space
  • Cloud servers providing machine learning as a service can access client’s raw data which produces privacy risks. So there is a strong incentive to protect the privacy of healthcare records, financial data, and other sensitive information of clients uploaded to cloud servers.

SHE: A Fast and Accurate Deep Neural Network for Encrypted Data

• Executive Summary
  • SHE: Accuracy-lossless CNN, performance ↑76.12%
  • It provides faster inference and higher accuracy compared to previous works by implementing RELU and Max pooling layers using TFHE
  • It also uses cheap Shift-Accumulation to support deeper neural networks

GAZELLE: A low Latency Framework for Secure Convolutional Neural Networks

• Executive Summary
  • Gazelle efficient secure computation protocols consist of combining two conventional encryption techniques. Homomorphic encryption and garbled circuits.
  • It enables the neural network to run efficiently and quickly compared to other methods while maintaining privacy of the user’s input and the parameters of the model
  • An encrypted image to the server running CNN on Gazelle is sent. The sender and server share encrypted messages forward and backward with the end goal of classifying the user’s image.

A secure Neural Networks by Homomorphic Encryption

• Servers learn on encrypted data and output encrypted prediction
• Only client can decrypt the encrypted prediction with the private key

The performance and accuracy comparisons

Yao’s Garbled Circuit Protocol

Alice (circuit generator) | Bob (circuit evaluator)
---|---
secret input a | secret input b
Agree on function f
Learns nothing else about b
Learns nothing else about a
Output Classes
airplane
automobile
truck

Convolution Neural Networks