



Enclave-NN

Alexander Schlögl

Introduction

Neural Nets are universal approximators.

Technical Details

- Forward pass is a series of algebraic operations
- Fully defined by their architecture and weights (parameters)

We focus solely on inference phase, so NNs for us are static functions.

Problem Statement

Monetization requires keeping parameters private.

Problem Statement

Monetization requires keeping parameters private.

Current Method

Online Oracles

- parameters never public
- require sharing of data for inference
- require provider's infrastructure

Problem Statement

Monetization requires keeping parameters private.

Current Method

Online Oracles

- parameters never public
- require sharing of data for inference
- require provider's infrastructure

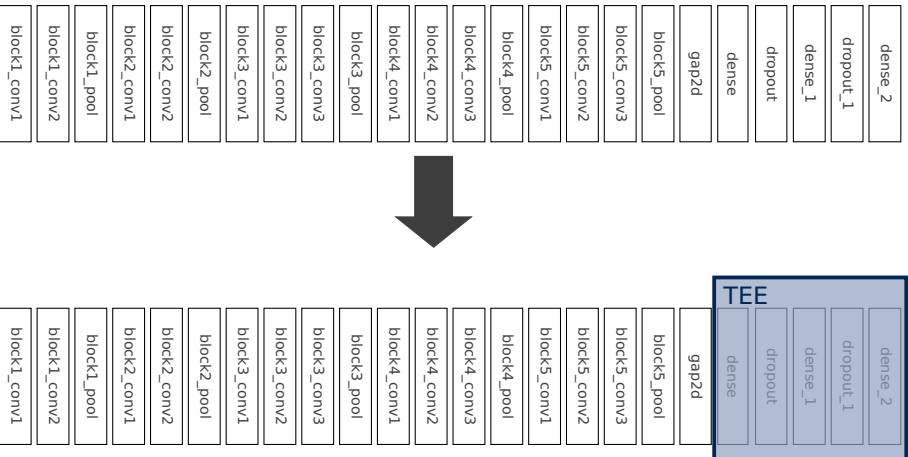
Idea

Use Trusted Execution Environments (TEEs) to hide parameters during inference

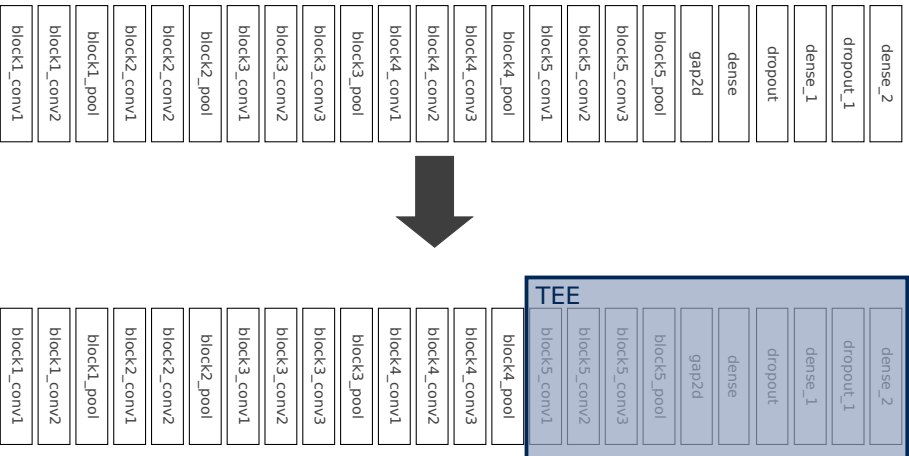


Approach

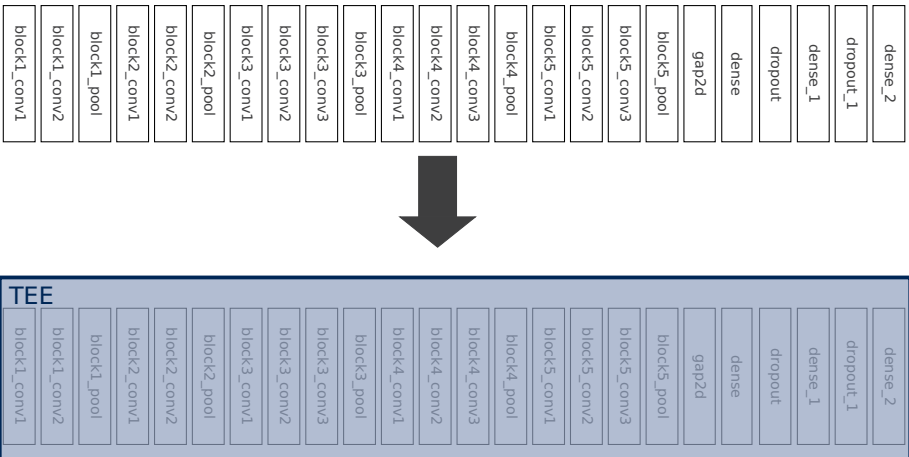
Approach



Approach



Approach



Approach

Move last n layers into TEE, send protected model to user

Advantages

- Less infrastructure required
- Semi offline usage possible
- Inference data can stay private

Disadvantages

- Performance impact
- Requires trust in manufacturer
- Potentially larger attack surface

Evaluation Method

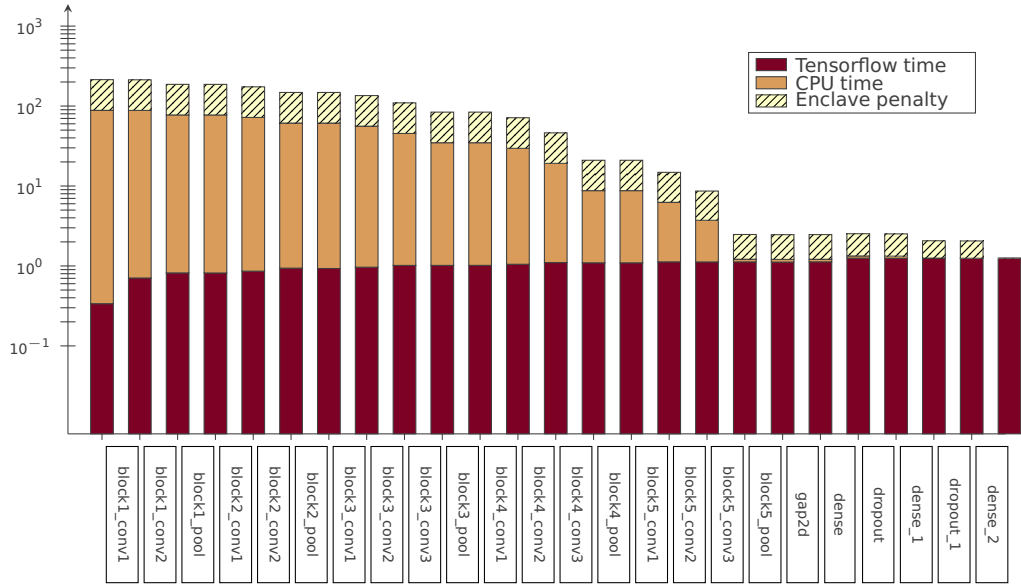
How large is the performance impact?

Procedure

- ① Split NN
- ② Compile TEE and native code
- ③ Measure inference time on single input
- ④ Separate CPU impact from TEE impact

Repeat for every possible split in NN

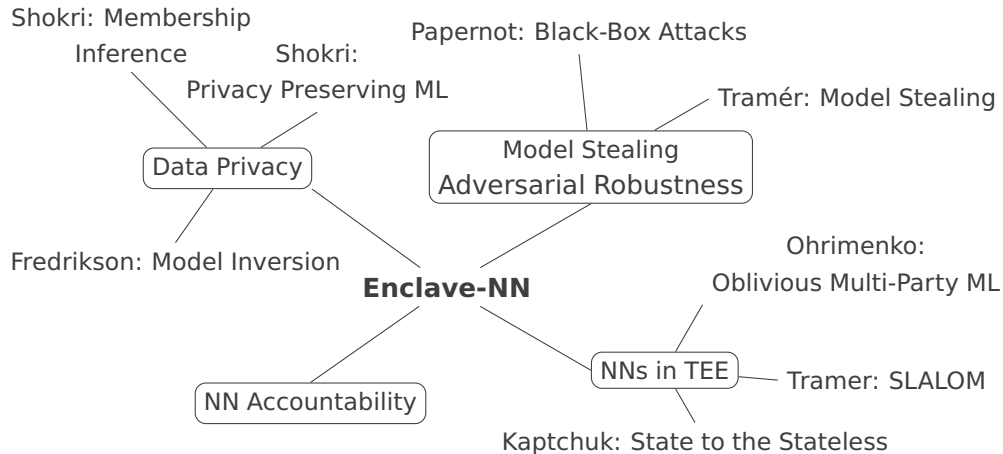
Results



Open Problem: Where to stop

- ✓ Generate weights
- ✓ Generate code for forward pass
- ✓ Interoperability with TF
- ✓ Run forward pass in TEE
- ✓ Hide weights
- ? Hide architecture
- ? Monetization prototype
- ? Different TEE technologies
- ✗ Automate for more code (TEE compiler target)

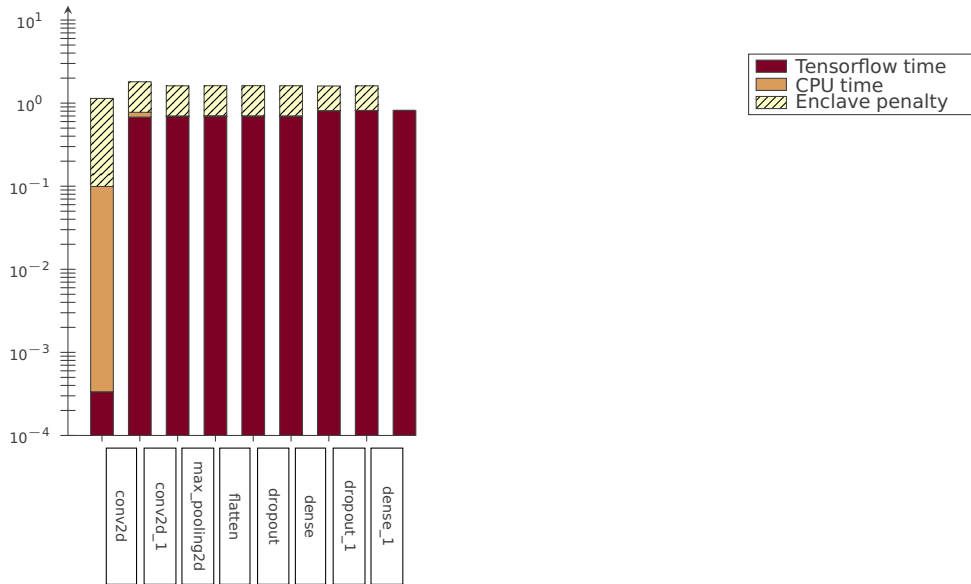
Open Problem: Where to send it



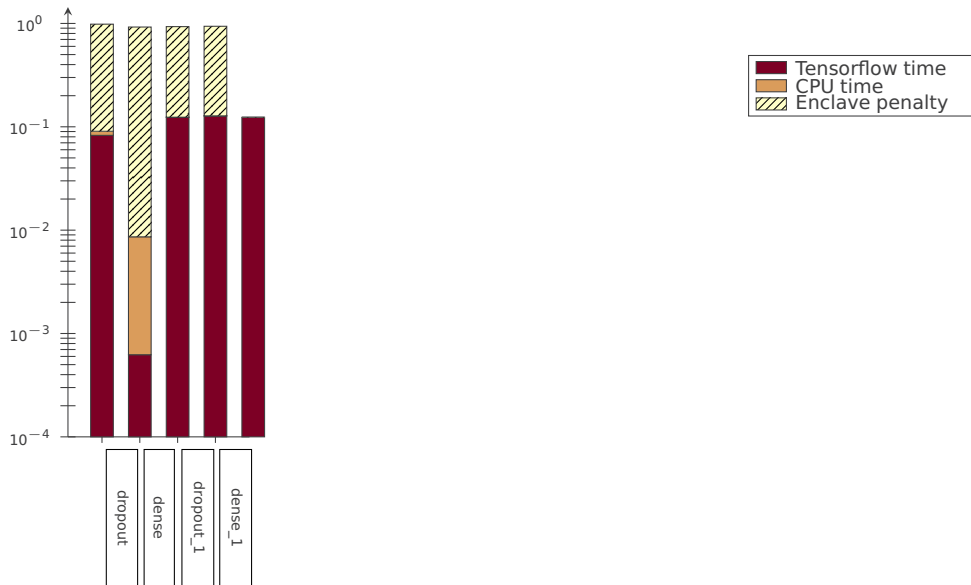
Open Problems

- How to split total work in submissions
- Which community to submit work to

MNIST Results



IMDB Results



Rotten Tomatoes Results

