Multiparty Computation and Application

Eleftheria Makri
Lecturer/Researcher
Imec-COSIC, KU Leuven, BE &
Saxion University of Applied Sciences, NL
@MakriEleftheria
EPIC: Efficient Private Image Classification (or: Learning from the Masters)

E. Makri, D. Rotaru, N. P. Smart, F. Vercauteren
EPIC: Efficient Private Image Classification
Feature Extraction
Transfer Learning Feature Extraction (or: Learning from the Masters)

Plaintext (non-sensitive) images
EPIC Security

Active Security vs. Passive Security

All other protocols in the related work
Step 1: Create the ML model

Inception–v3
CNN

Linear SVM
Step 2: Alice secret shares the ML model
Step 2: Alice secret shares the ML model

\[ SVM_A + SVM_B + SVM_C = \]
Step 3: Bob extracts features

Inception–v3 CNN

Features

$X$
Step 4: Bob secret shares features
Step 4: Bob secret shares features

\[ X_A + X_B + X_C = \text{CNN-Feat}(\cdot) \]

Alice

Bob

Charlie
Step 5: Parties use MPC to help Charlie compute label of SVM-Alice(Bob-Image)
Step 5: Parties use MPC to help Charlie compute label of SVM-Alice(Bob-Image)
EPIC Performance – Simple Variant

**Computation Cost**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Offline (s)</th>
<th>Online (s)</th>
<th>Total (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFAR-10</td>
<td>0.5</td>
<td>0.1</td>
<td>0.6</td>
</tr>
<tr>
<td>MIT-67</td>
<td>1.5</td>
<td>0.3</td>
<td>1.8</td>
</tr>
<tr>
<td>Caltech-101</td>
<td>3.5</td>
<td>0.5</td>
<td>4.0</td>
</tr>
</tbody>
</table>

**Communication Cost**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Offline (MB)</th>
<th>Online (MB)</th>
<th>Total (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFAR-10</td>
<td>0.5</td>
<td>0.1</td>
<td>0.6</td>
</tr>
<tr>
<td>MIT-67</td>
<td>1.5</td>
<td>0.3</td>
<td>1.8</td>
</tr>
<tr>
<td>Caltech-101</td>
<td>3.5</td>
<td>0.5</td>
<td>4.0</td>
</tr>
</tbody>
</table>
Performance of the state-of-the-art private image classification

### Computation Cost

<table>
<thead>
<tr>
<th></th>
<th>Offline (s)</th>
<th>Online (s)</th>
<th>Total (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiniONN*</td>
<td>0.001</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>Gazelle**</td>
<td>0.1</td>
<td>10</td>
<td>10.1</td>
</tr>
<tr>
<td>EPIC</td>
<td>1000</td>
<td>10000</td>
<td>10010</td>
</tr>
</tbody>
</table>


### Communication Cost

<table>
<thead>
<tr>
<th></th>
<th>Offline (MB)</th>
<th>Online (MB)</th>
<th>Total (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiniONN*</td>
<td>0.001</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>Gazelle**</td>
<td>1000</td>
<td>10000</td>
<td>10010</td>
</tr>
<tr>
<td>EPIC</td>
<td>10000</td>
<td>1000000</td>
<td>1000100000</td>
</tr>
</tbody>
</table>

EPIC Efficiency Gain over the state-of-the-art

- EPIC vs. Gazelle\(^1\) on CIFAR-10:
  - 34 times faster runtime;
  - 50 times improvement of communication cost;
  - 7% higher classification accuracy.

- EPIC vs. Gazelle\(^1\) with the same accuracy:
  - 700 times faster runtime;
  - 500 times improvement of communication cost.

---

Now what?

• What would transform EPIC to a LEGENDARY solution?
  – Maintain security
  – Maintain or increase efficiency
  – **Increase accuracy!**

• Any ideas on how to do this (using MPC)?
  – Talk to me during the break, or
  – Contact me offline at: eleftheria.makri@esat.kuleuven.be
THAT WAS EPIC!