The Future Begins Here

intel labs

Labs Day 2020 | December 3
Securing Data in Use
Advances in Federated Learning and Fully Homomorphic Encryption
Rosario Cammarota  Jason Martin
Principal Engineer  Principal Engineer
The world creates **2.5 quintillion** bytes of data every single day — yet only a fraction of it is utilized.

*Source: DOMO (2018)*
The Data Silo Problem

- Privacy / Legality
- Data too valuable
- Data too large to transmit
Value Extraction from Data

Training

Human

Bicycle

Strawberry

Lots of labeled data!

Inference

Model weights

Forward “Strawberry”

Error

“Bicycle”

Forward “Bicycle”?

Did you know?

Training with a large data set AND deep (many layered) neural network often leads to the highest accuracy inference

Data set size

Accuracy

Large NN

Medium NN

Small NN

Traditional Model
Federated Learning – Move Compute to Data

Centralized Learning

- Hospital A
  - Data A
- Hospital B
  - Data B
- Hospital C
  - Data C

Training Infrastructure

Model

Federated Learning

- Hospital A
  - Model Update A
- Hospital B
  - Model Update B
- Hospital C
  - Model Update C

Aggregation Server

Updated model
Intel-UPenn collaboration – What We’ve Done

- Introduced Federated Learning to the medical imaging domain for the first time
- Developed a proof-of-concept segmentation of brain tumors in MRI scans
- Showed Federated Learning approach achieved 99.42% of centralized learning accuracy and superior to alternative collaborative learning approaches

```
<table>
<thead>
<tr>
<th>Method</th>
<th>Global Validation DC*</th>
<th>Percent of Data-Sharing DC*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Learning</td>
<td>0.863</td>
<td>100%</td>
</tr>
<tr>
<td>Federated Learning</td>
<td>0.858</td>
<td>99.42%</td>
</tr>
<tr>
<td>Single Institution (average)</td>
<td>0.732</td>
<td>84.82%</td>
</tr>
</tbody>
</table>
```

See cited sources for workloads and configurations. Results may vary.


Brain tumor segmentation finds tumors from MRIs

How much better does each institution do when training on the full data vs. just their own data?
- 17% better on the hold-out BraTS data
- 2.6% better on their own validation data
Machine Learning Security & Privacy Risks

Model Extraction
Model extraction attacks recover IP from participants

Model Poisoning
Poisoning attacks maliciously alter models

Model Inversion
Model inversion attacks recover training data from model weights

Unprotected, Attackers Can *Compute Attacks* Directly and *Adapt Attacks* as the Model Trains
Machine Learning Security & Privacy Solutions

- **Learning**: Robust Optimization and Aggregation to help prevent poisoning and extraction attacks.
- **APIs**: Limited to prevent model extraction attacks.
- **Algorithms**: Run in a hardware trusted execution environment to help protect confidentiality and prevent integrity attacks.
- **Data**: Can stay always encrypted with privacy-enhancing technologies.
Federated Learning based on Intel® SGX
Dataflow with Adopted Cryptography

Data Processing Requires Decryption
Dataflow with Fully Homomorphic Encryption

Data Stays Encrypted at All Times
Things You Can Do with Homomorphic Encryption

- Enhance Security of Data
- Monetization
- Enhance security of Data Sharing and Collaboration
Technical Challenges with Homomorphic Cryptography

Data explosion:
HE Ciphertext 100x – 1000x larger than plaintext

Compute explosion:
HE Computation needs 10,000x – 1,000,000x more CPU ops than plaintext

\[
\begin{align*}
Enc(c) &= HE.mul(Enc(a), Enc(b)) \\
Enc(d) &= HE.add(Enc(d), Enc(c)) \\
Enc(d) &= HE.refresh(Enc(d)) \\
\end{align*}
\]
Technical Challenges with Homomorphic Cryptography

Standardization of Privacy-Enhancing technologies just started - in 2020 - at international bodies

Federal Information Processing Standards Publication 197
November 26, 2001

Announcing the ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).
Explorations to Make FHE Inexpensive

- Ecosystem
  - Standards, Community

- Research
  - Innovation in cryptography
  - Innovation in compilation to FHE

- FHE targeted innovation in hardware
  - Increased parallelism
  - Compute in memory

See cited sources for workloads and configurations. Results may vary:
Jung et al. [HEANN Demystified], arXiv:2003.04510, March 2020
Riazi et al. [HEAX], ASPLOS 2020
The Future Begins HERE

- Data Insights
- Scalability
- Security and Privacy
- Data Protection
Legal Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex. Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure. Your costs and results may vary. Intel technologies may require enabled hardware, software or service activation.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.
The Future Begins Here