RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **ACB-T10**

Protecting Privacy in a Data-Driven World: Privacy-Preserving Machine Learning

Casimir Wierzynski

Senior Director, AI Products
Intel
@casimirw

Machine learning enables new services using sensitive data

- Thanks to ML/AI we enjoy innovative products and services
- But the data that feed them are very sensitive and personal
- **We must find ways to unlock the power of AI *while protecting data privacy***

Current approaches to privacy and ML

User control

Prescribe user's rights

Know what's collected, by whom, why, opt out..

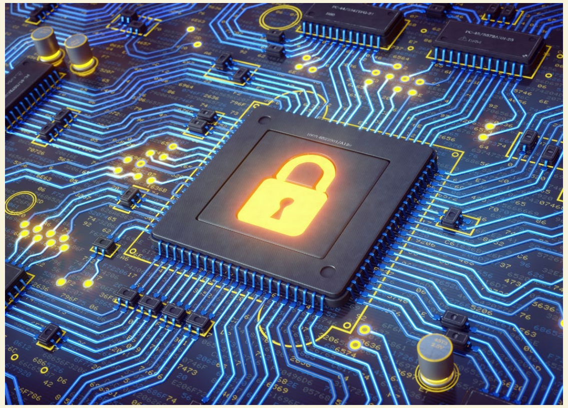
Data protection

Anonymize

Remove "identifiable information"

But identity can be inferred in many ways

Encrypt



Encrypt at rest, in transit

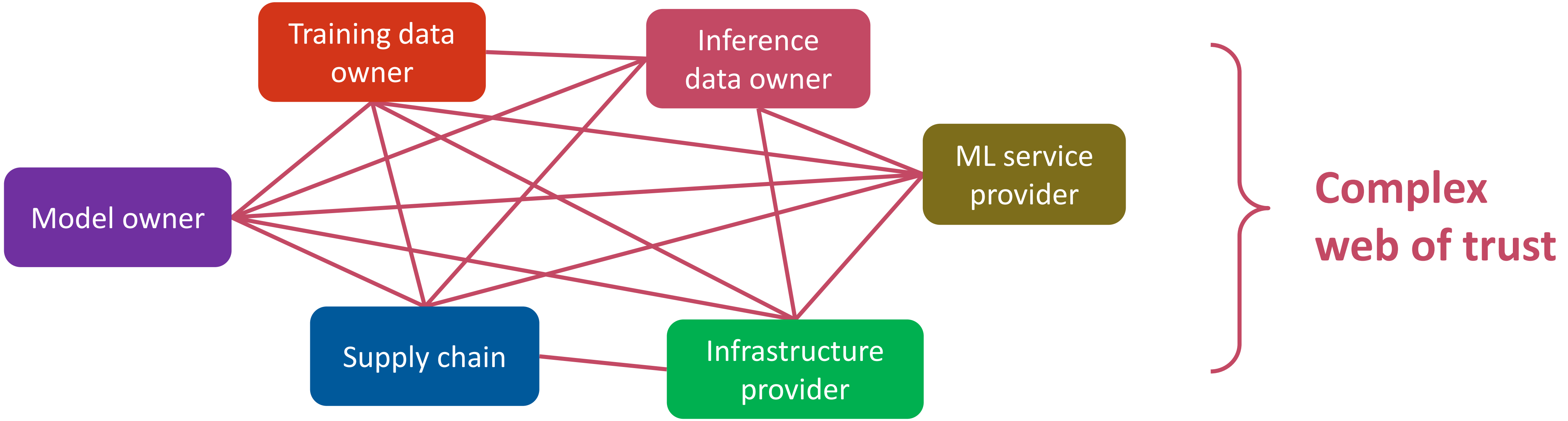
But it's decrypted during use

➔ **Need more protections on both fronts**

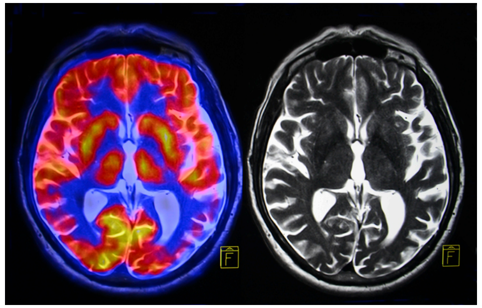
Current approaches to AI require complex webs of trust

- With digital assets: **"sharing" = "giving" + "<u>trust</u>"**

- Machine learning is fundamentally a multi-stakeholder computation:



What if untrusted parties could do machine learning together?

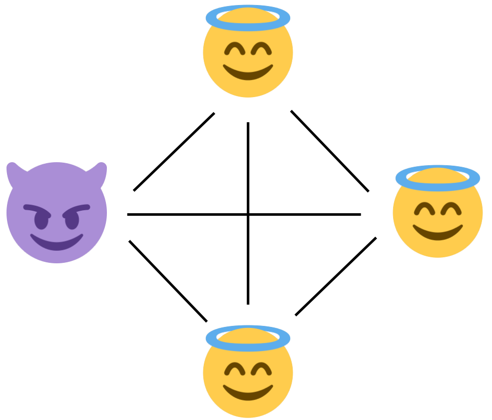
Finance / Insurance	8%		Rival banks could build joint anti-money laundering models
Healthcare	8%		Hospitals could use remote, 3rd party analytics on patient data
Retail	6%		Retailers could monetize their purchase data while protecting user privacy
TOTAL	**22%** of US GDP		

Source: https://www.bea.gov/system/files/2019-04/gdpind418_0.pdf

Introducing privacy-preserving machine learning (PPML)

- Using cryptography and statistics, you can do “magic”:

Federated learning,
Multi-party Computation

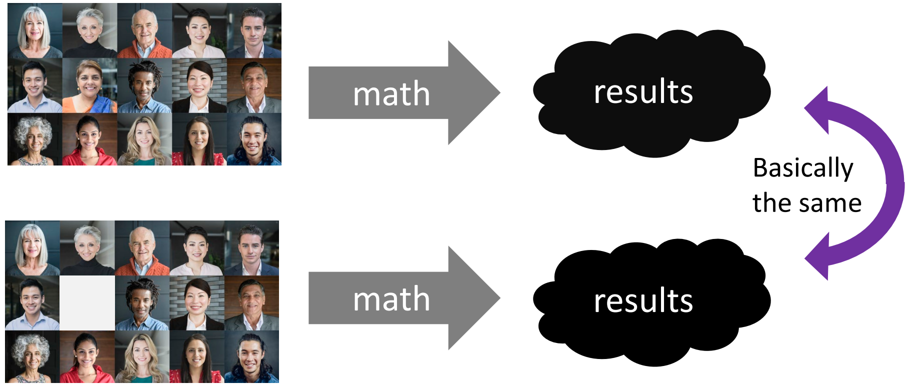


You can pool your data without sharing it

Homomorphic Encryption

You can do machine learning while data stays encrypted

Differential privacy



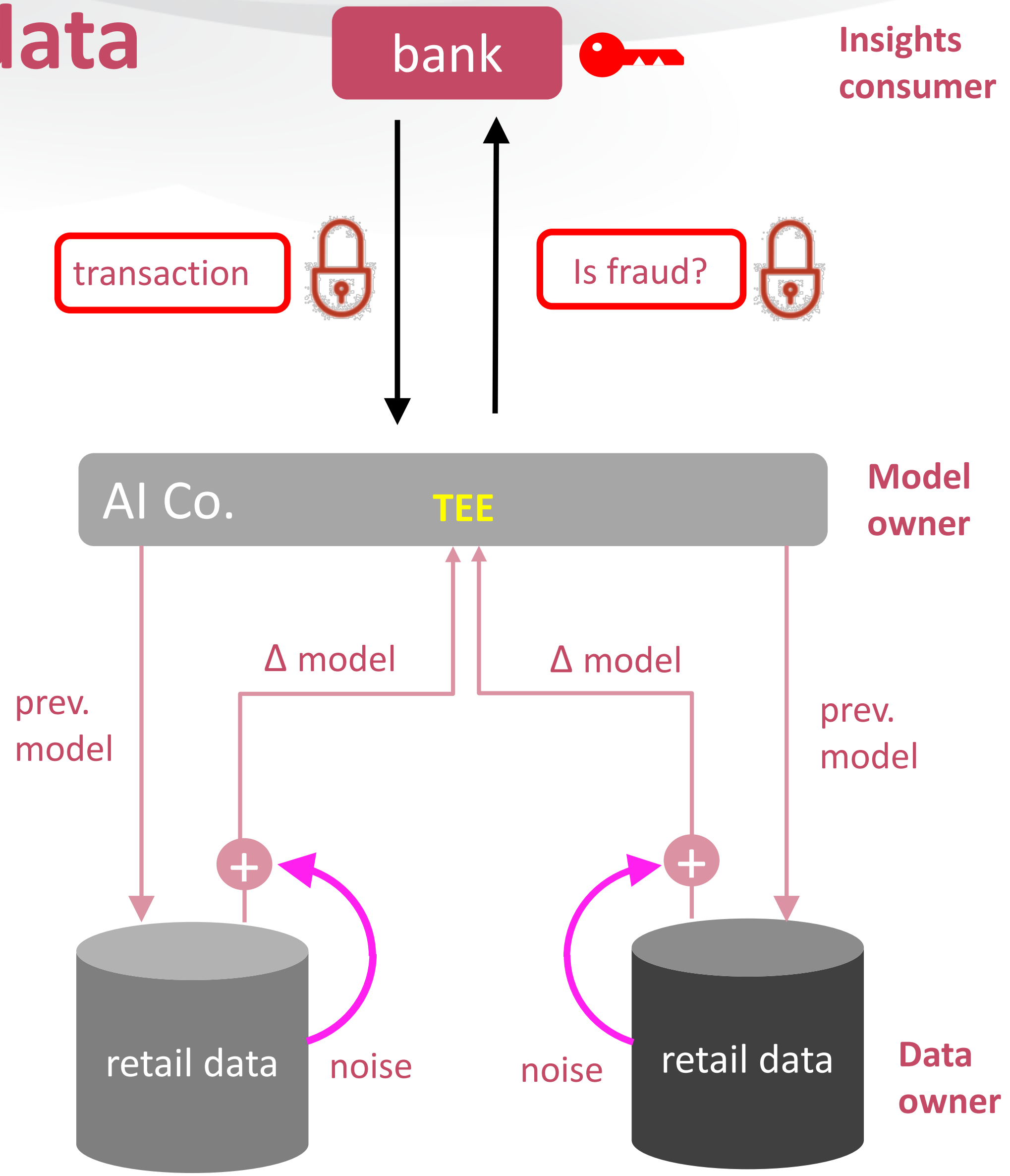
You can collect personal data with quantifiable privacy protections

We can amplify these building blocks using Trusted Execution Environments (TEEs), eg Intel SGX

https://commons.wikimedia.org/wiki/File:Twemoji_1f607.svg https://commons.wikimedia.org/wiki/File:Twemoji2_1f608.svg

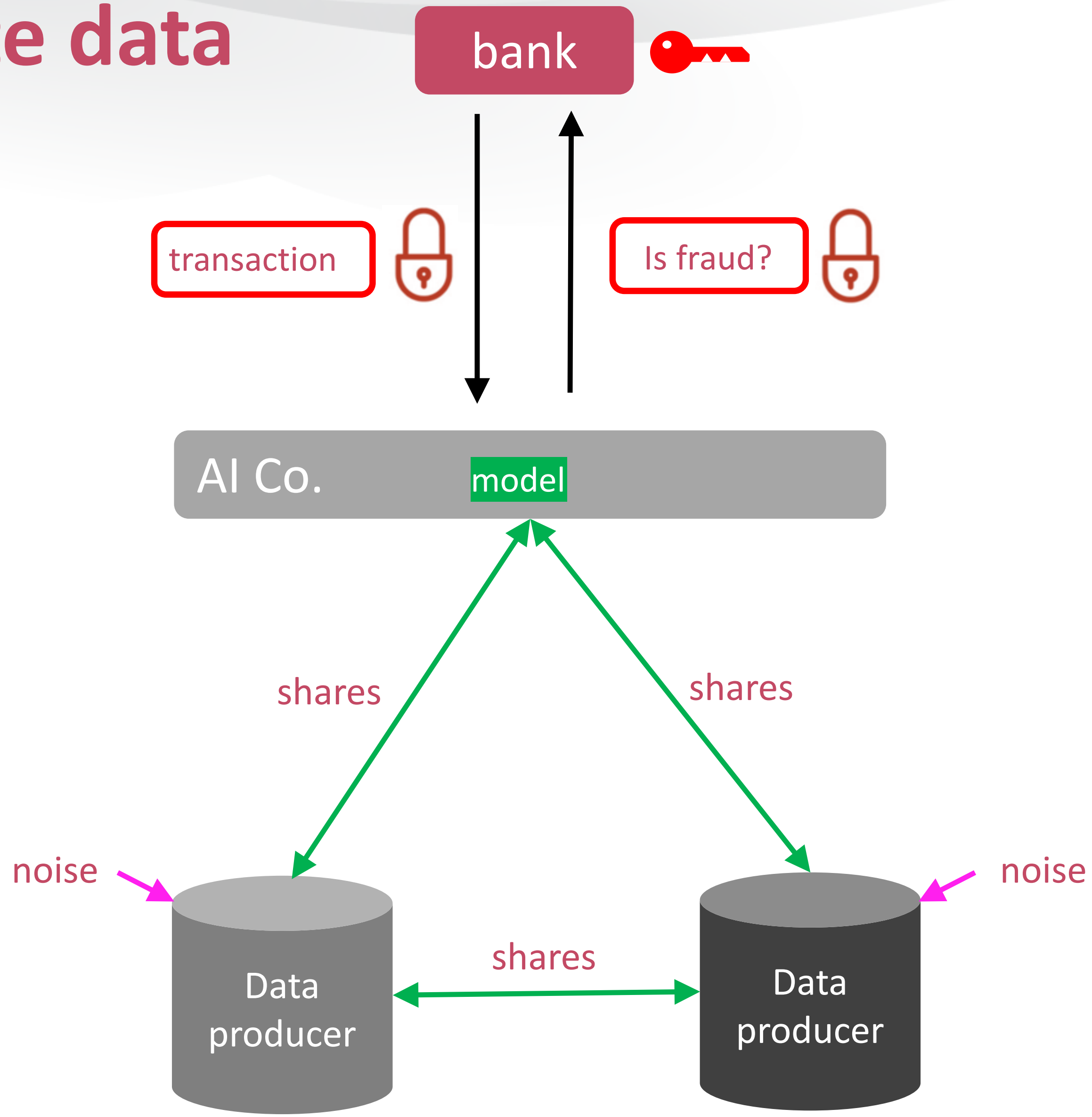
PPML use case: monetizing private data and insights

- Bank hires “AI company” for fraud model
- Retailers have private data
  - They update the model using private data



PPML use case: monetizing private data and insights

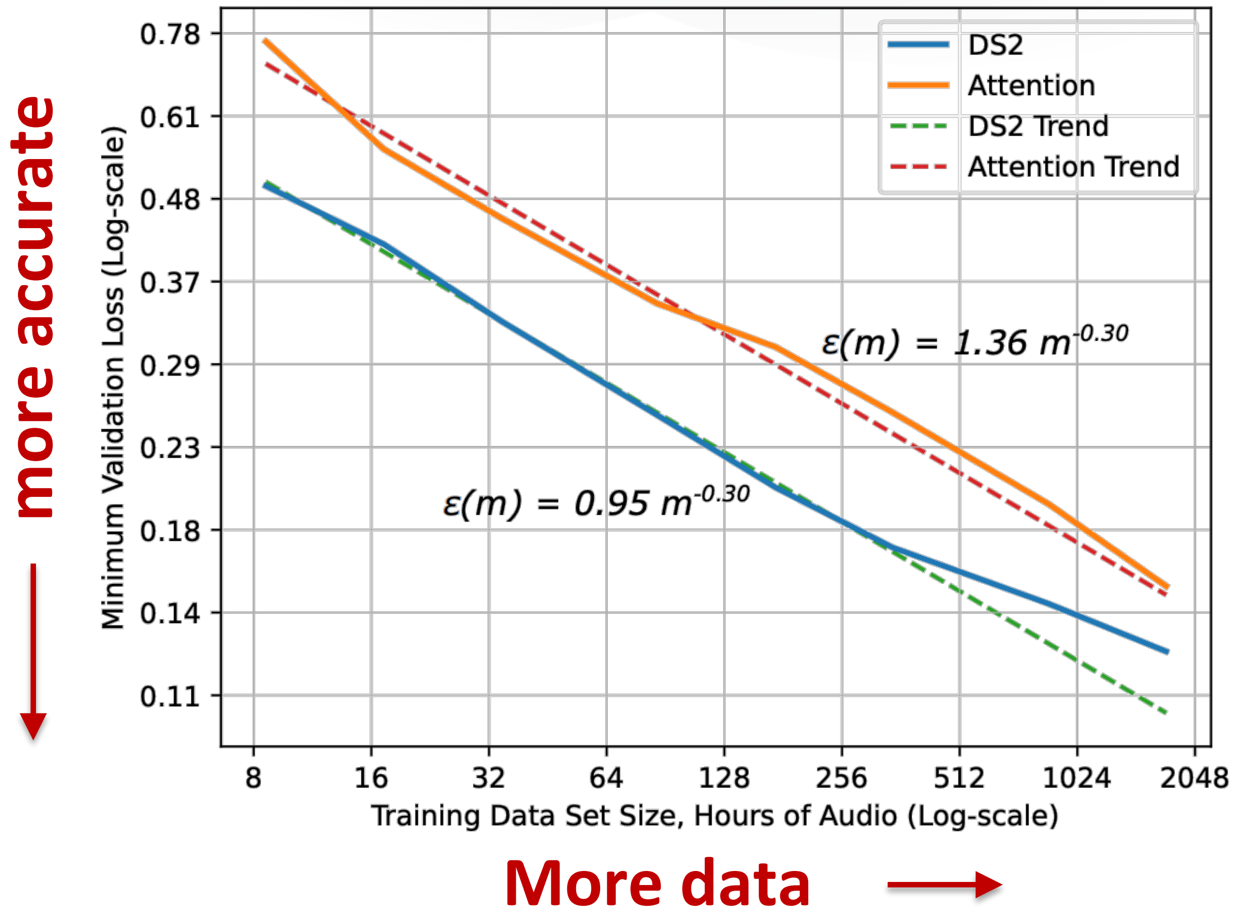
- Bank hires "AI company" for fraud model
- Retailers have private data
  - They update the model using private data
  - With MPC, model stays private



Federated Learning

Model accuracy fuels demand for bigger datasets

- To improve performance of ML system ➔ **get more data!**

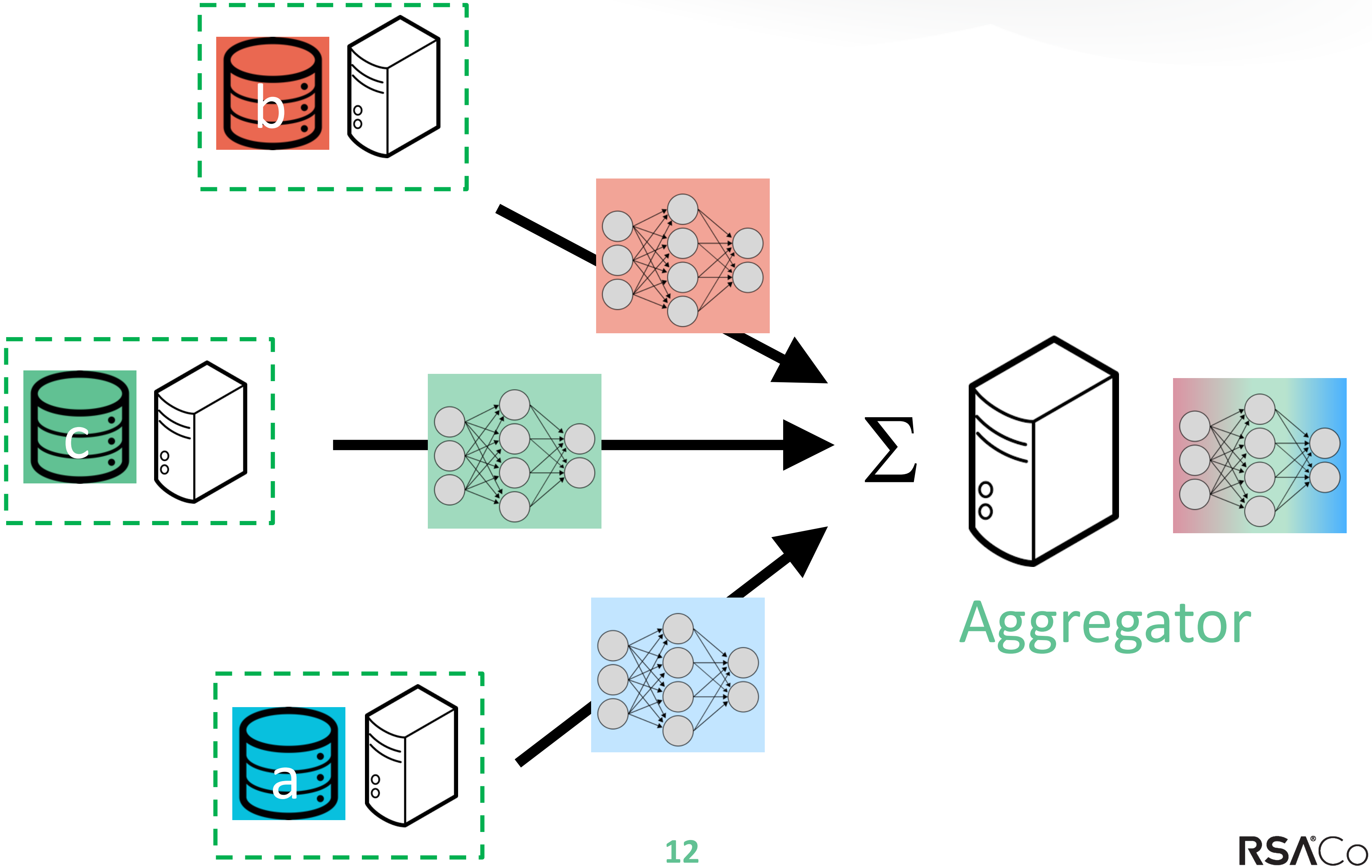


Hestness, Joel, et al. "Deep learning scaling is predictable, empirically." *arXiv preprint arXiv:1712.00409* (2017).

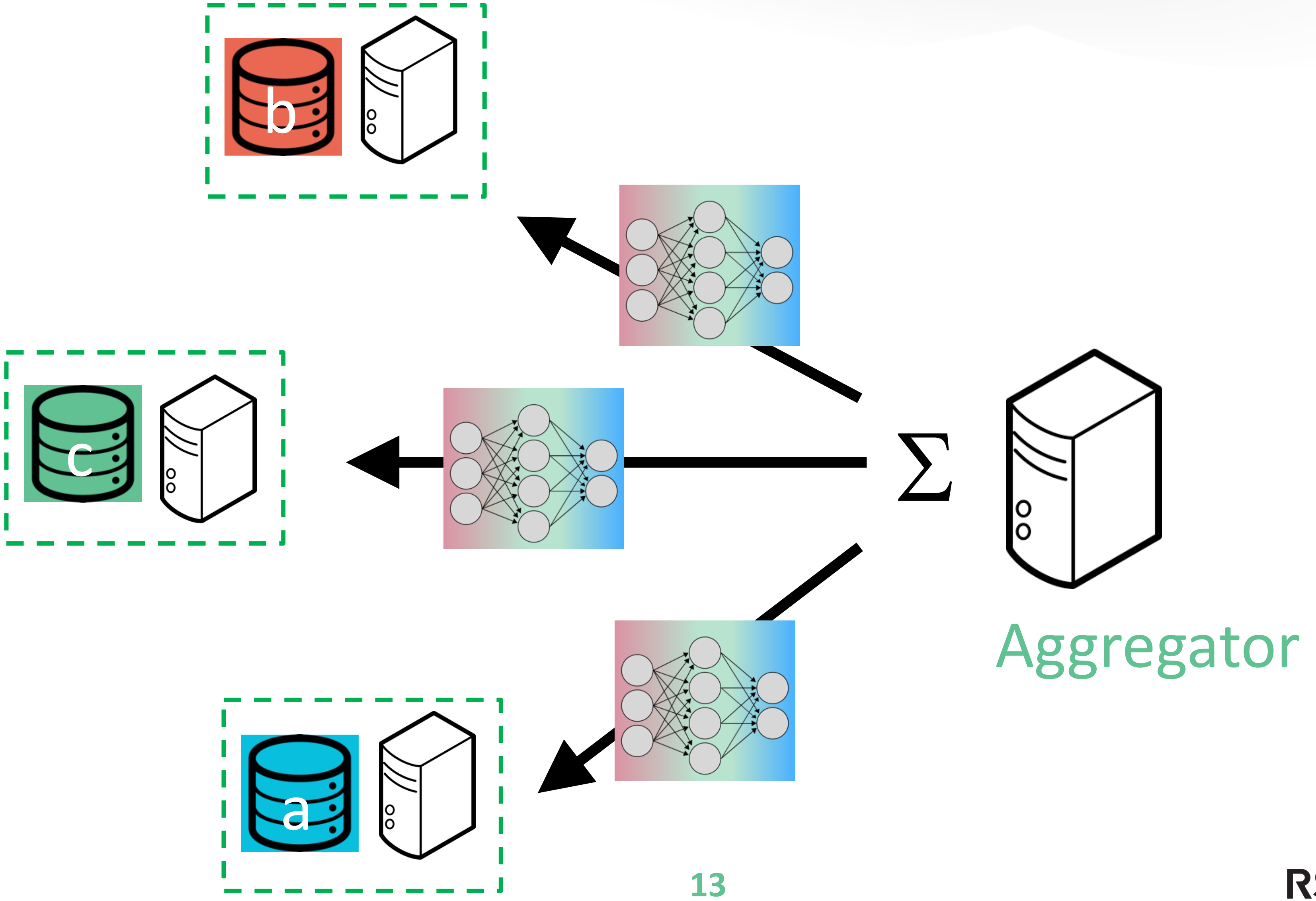
The data silo problem

- Privacy / Legality (HIPAA / GDPR)
- Data too valuable (or value unknown)
- Data too large to transmit

Federated learning part 1: train locally and aggregate



Federated learning part 2: share aggregate; goto step 1



Federated learning (FL): some care required

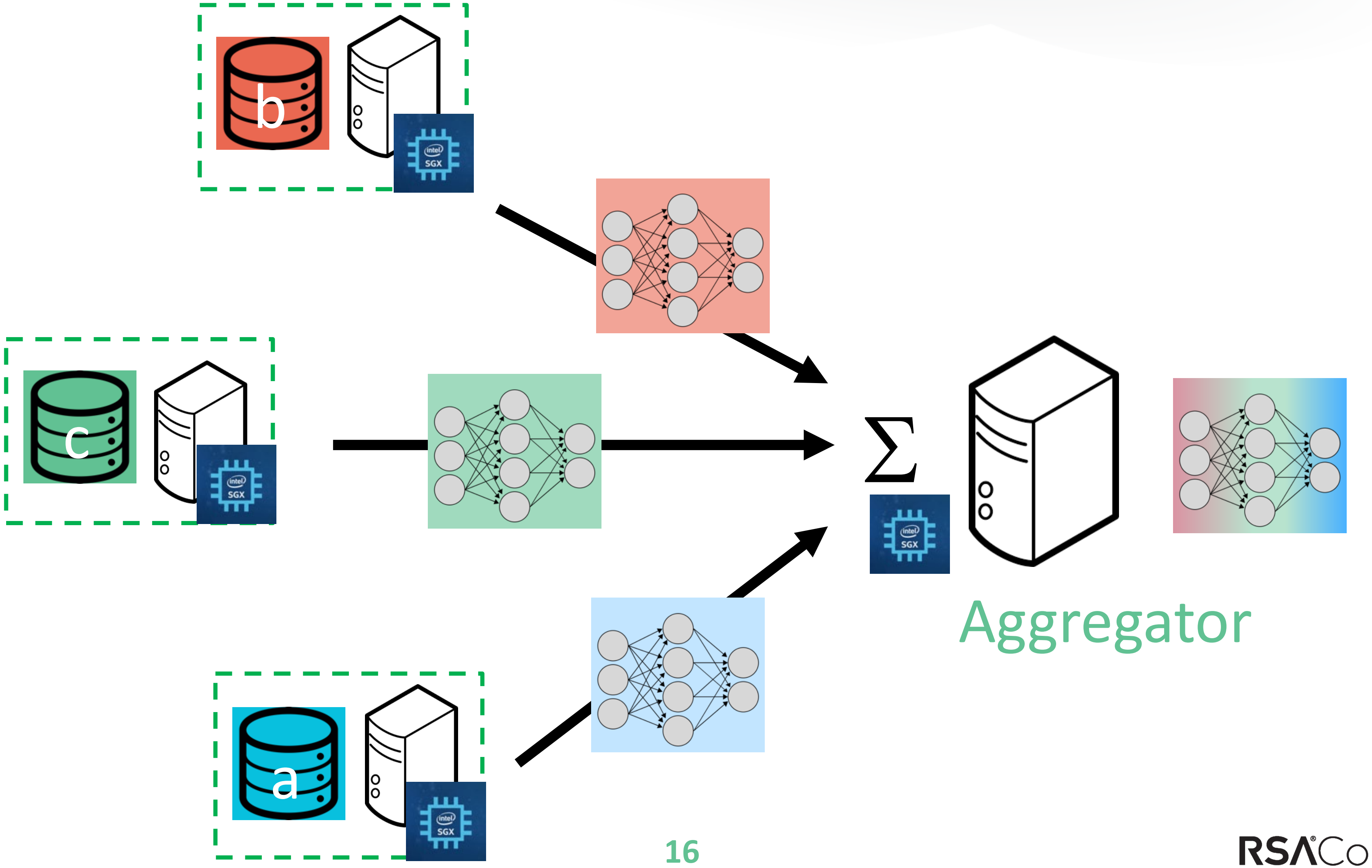
Security / privacy

- FL solves a lot of data access problems.

- Data holders can see the model
- Data holders can tamper with the protocol
- Model updates leak information

https://software.intel.com/en-us/sgx

Federated learning with Intel SGX



A vision for protecting FL with Intel® SGX

Confidentiality

- Model IP won't be stolen.
- Attacks can't be computed.

Integrity & attestation

- Only approved models/training procedures.
- All participants know rules are enforced.
- Algorithmic defenses can't be bypassed.

Stops attackers from using the model.

Stops attackers from being adaptive.

No product or component can be absolutely secure.

Federated Learning (FL): some more care required

Data science

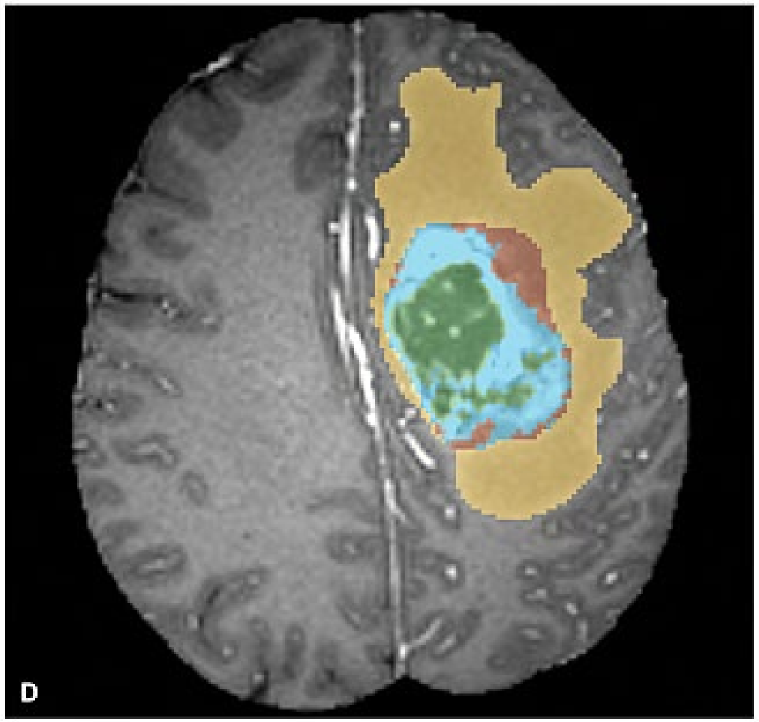
- Data owners only need local data.
- Will FL converge to model from pooled data?

Distributed vs Pooled data: A medical case study

BraTS Multimodal Brain Tumor Segmentation Challenge

Perelman School of Medicine UNIVERSITY of PENNSYLVANIA

- BraTS = Brain Tumor Segmentation Challenge
- Intel / UPenn collaboration
- Compare Federated Learning to training on pooled data
    - What are the benefits of pooling the data?
    - How much of this benefit can FL achieve?

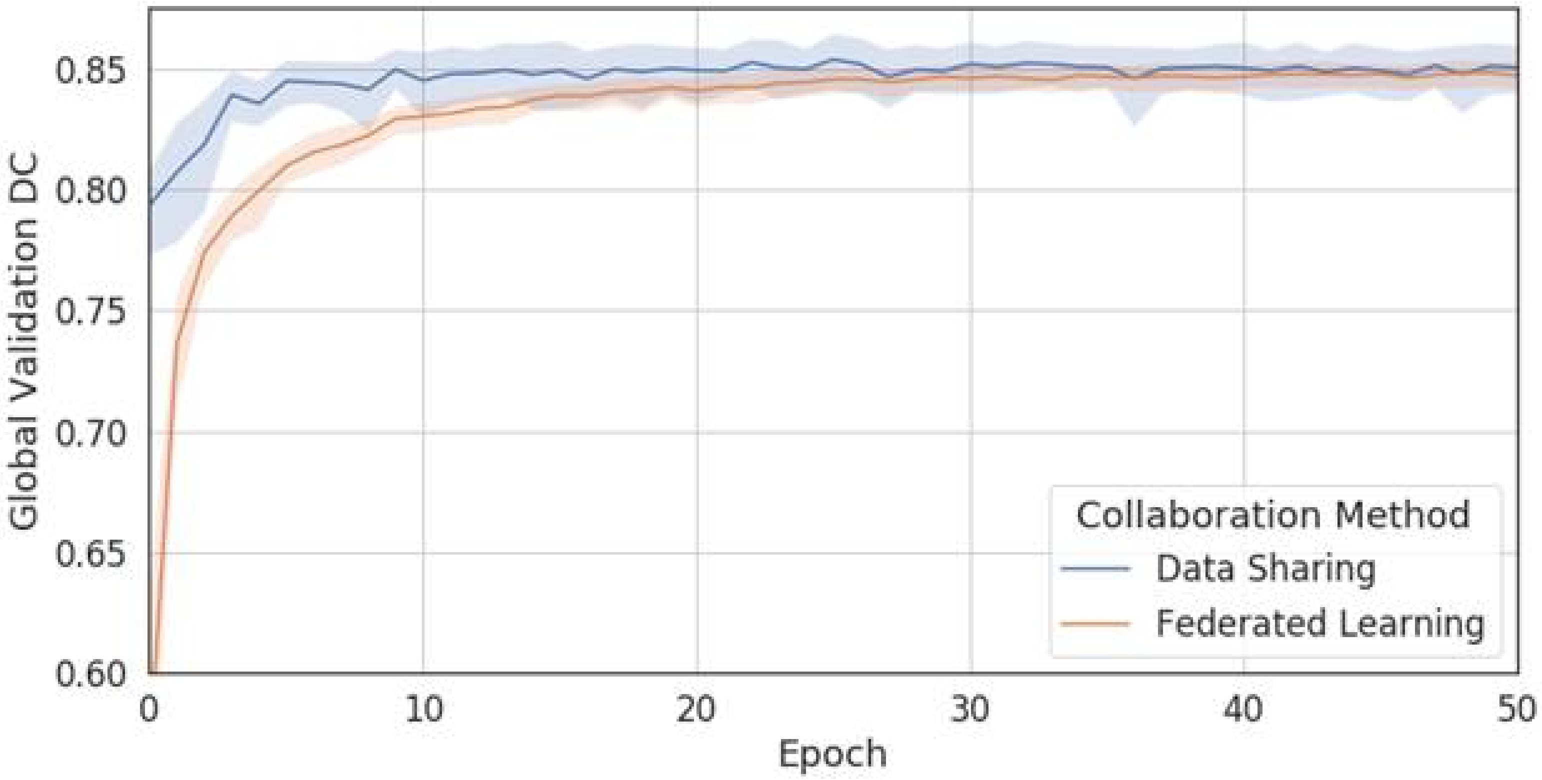


Brain tumor segmentation finds tumors from MRIs

https://www.med.upenn.edu/sbia/brats2017.html

Federated training on brain tumor data (BraTS)

Method	Accuracy (Dice coeff)	% of Data-Sharing accuracy
Data-sharing	0.862	100%
Federated Learning	0.855	99%
Single Institution	0.704	81%

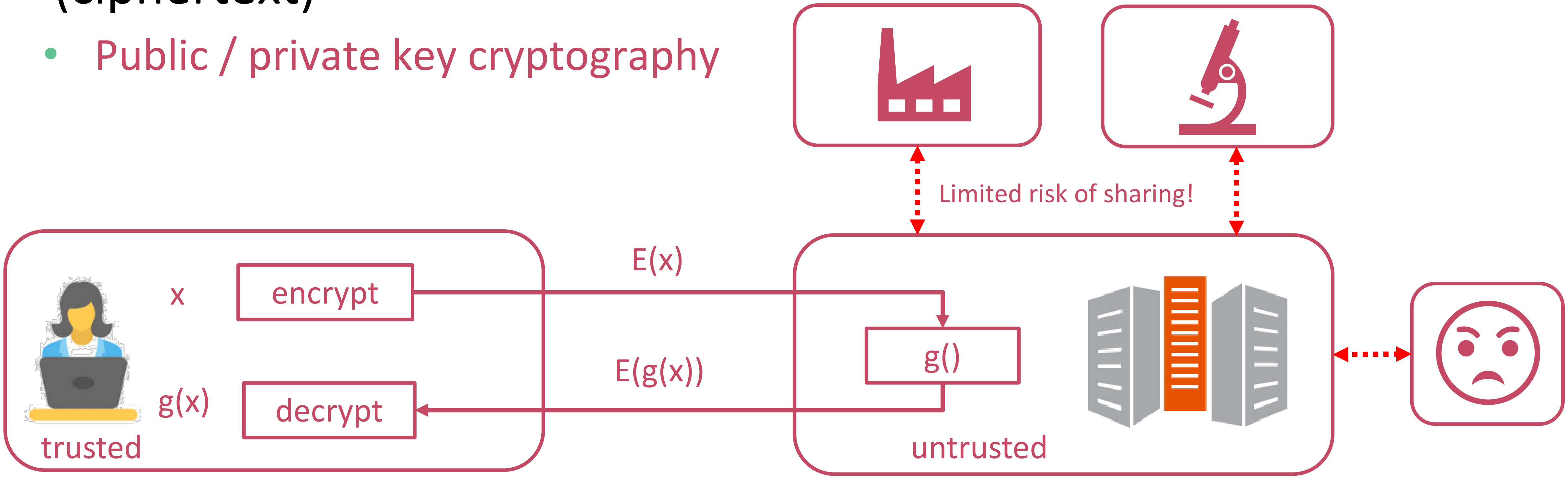


Sheller, Micah J., et al. "Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation." *International MICCAI Brainlesion Workshop*. Springer, Cham, 2018.

Homomorphic encryption

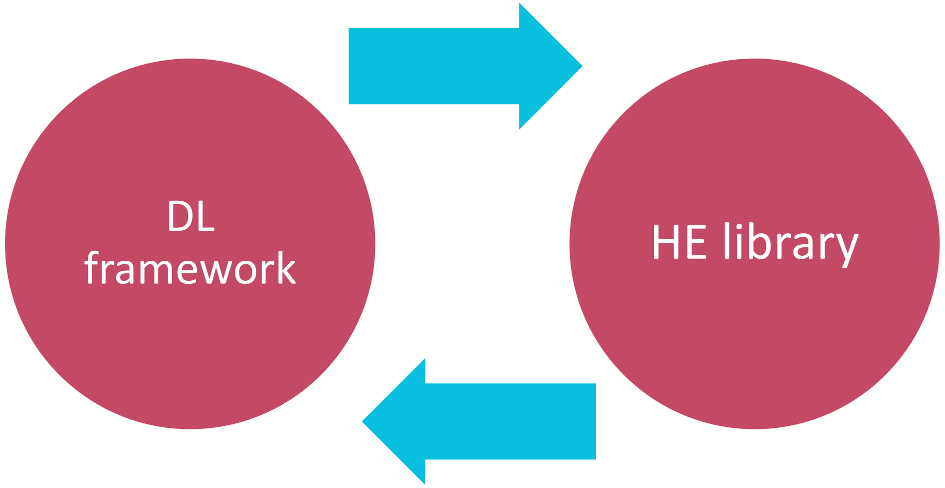
Homomorphic encryption (HE)

- Computation on encrypted data (ciphertext)
  - Public / private key cryptography



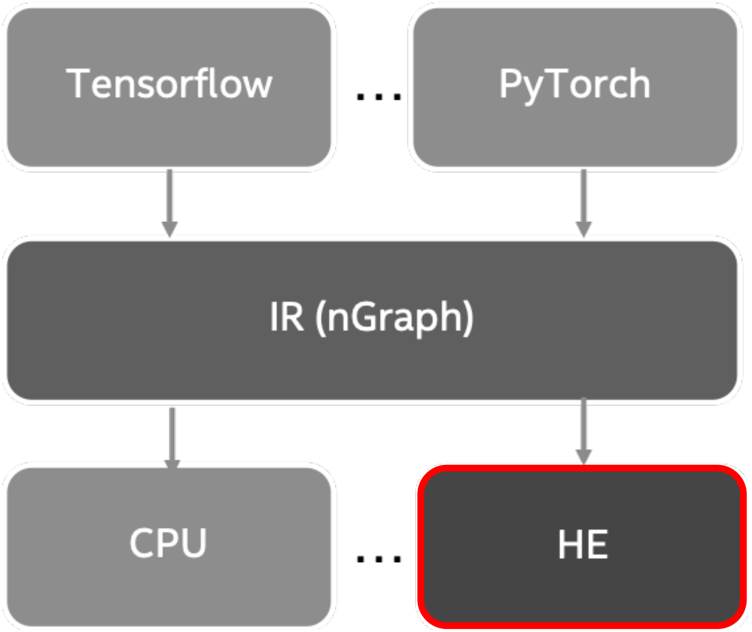
Deploying deep learning [DL] on HE?

- Difficulties
  - Redefining low-level operations (+, *)
  - New data types (ciphertext)
- Solution
  - Add HE library calls to DL framework?
  - Add DL library calls to an HE framework?
- Requires expertise in cryptography, DL, software engineering



HE-transformer for nGraph: nGraph-HE

- Simply treat HE as another nGraph hardware target
- Optimizations in HE and graph compilers are largely orthogonal
- SEAL encryption library
  - Supports BFV and CKKS encryption schemes
- Direct integration with TensorFlow
  - PyTorch, ONNX, etc. use nGraph serialization



HE performance trends

nGraph-HE2: A High-Throughput Framework for Neural Network Inference on Encrypted Data

https://arxiv.org/abs/1908.04172

Table 7: CryptoNets performance comparison. Results are sorted by throughput (Thput).

Method	Acc. (%)	Latency (s)	Thput. (im/s)
LoLa [8]	98.95	2.2	0.45
CryptoNets [22]	98.95	250	16.4
Gazelle [25]	98.95	0.03	33.3
Faster CryptoNets [14]	98.7	39.1	210
nGraph-HE [5]	98.95	16.7	245
CryptoNets 3.2 [8]	98.95	25.6	320
nGraph-HE2	98.95	2.05	1,998
nGraph-HE2-ReLU	98.62	0.69	2,959

HE performance trends

http://www.image-net.org/

MobileNetV2 Model	Unencrypted Accuracy (%)		Encrypted Accuracy (%)		Runtime			
					Localhost		LAN	
	Top-1	Top-5	Top-1	Top-5	Amortized (ms)	Total (s)	Amortized (ms)	Total (s)
0.35-96	42.370	67.106	42.356 (−0.014)	67.114 (+0.008)	27	112 ± 5	71	292 ± 5
0.35-128	50.032	74.382	49.982 (−0.050)	74.358 (−0.024)	46	187 ± 4	116	475 ± 10
0.35-160	56.202	79.730	56.184 (−0.018)	79.716 (−0.014)	71	290 ± 7	197	807 ± 19
0.35-192	58.582	81.252	58.586 (+0.004)	81.252 (−0.000)	103	422 ± 23	278	1,141 ± 22
0.35-224	60.384	82.750	60.394 (+0.010)	82.768 (+0.018)	129	529 ± 18	$\boxed{381}$	1,559 ± 27

Boemer, Fabian, et al. "nGraph-HE2: A High-Throughput Framework for Neural Network Inference on Encrypted Data." *Proceedings of the 7th ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography*. 2019.

Conclusions

- Advancing both AI and privacy is not a zero-sum game.
- No single technology “solves” privacy.
- **Privacy–preserving ML (PPML)** enables new ML use cases and business models

Applying what you've learned today

- **In 1 week**: Read our papers on PPML
- **1 month:** Download and try HE-Transformer; Build a ML model that operates on ciphertext.
- **6 months:** Identify ML tasks in your organization that operate on sensitive data and how PPML can help.