Privacy Preserving ML

Federated Learning

Differential Privacy

Homomorphic Encryption

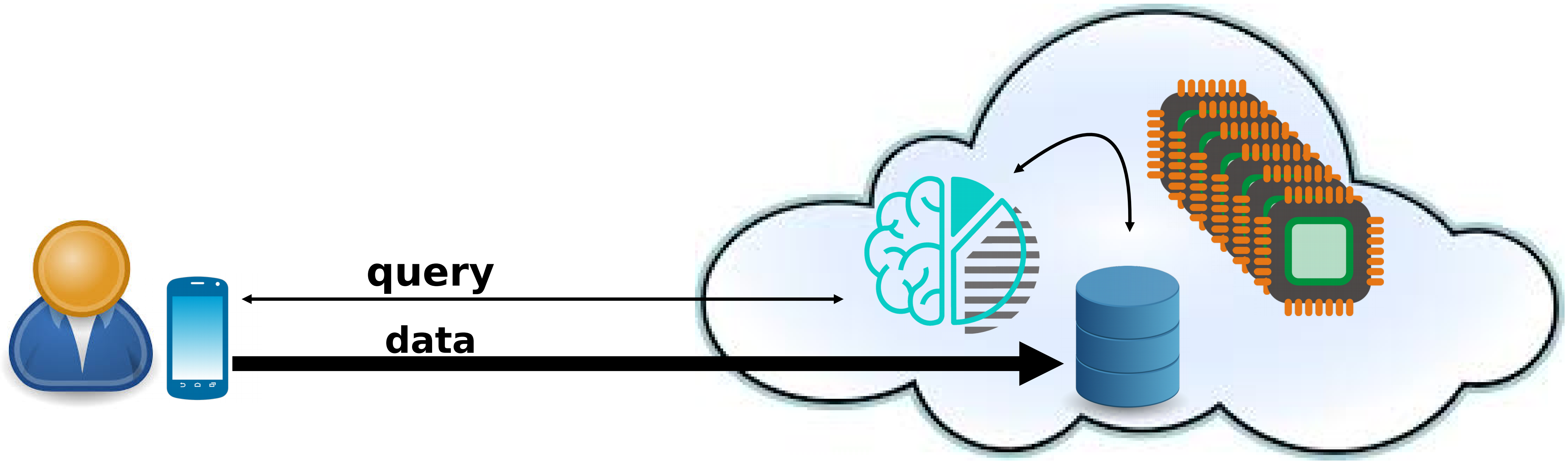
Trusted Execution Environments

Romeo Kienzler

IBM CODAIT

IBM Center for Open Source Data and AI Technologies

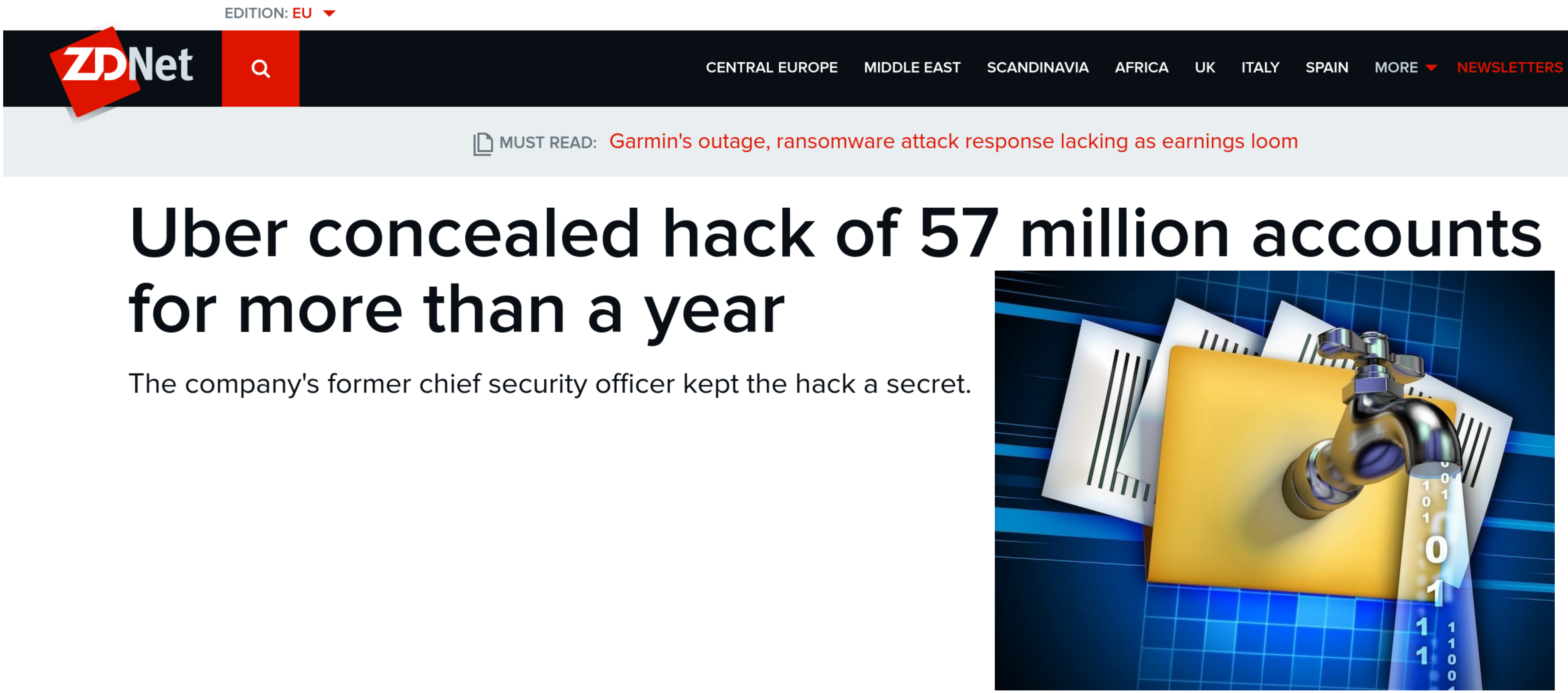
state of the art



Problem #1

data privacy

Unencrypted data laying around on servers is always a problem



EDITION: EU

MUST READ: Garmin's outage, ransomware attack response lacking as earnings loom

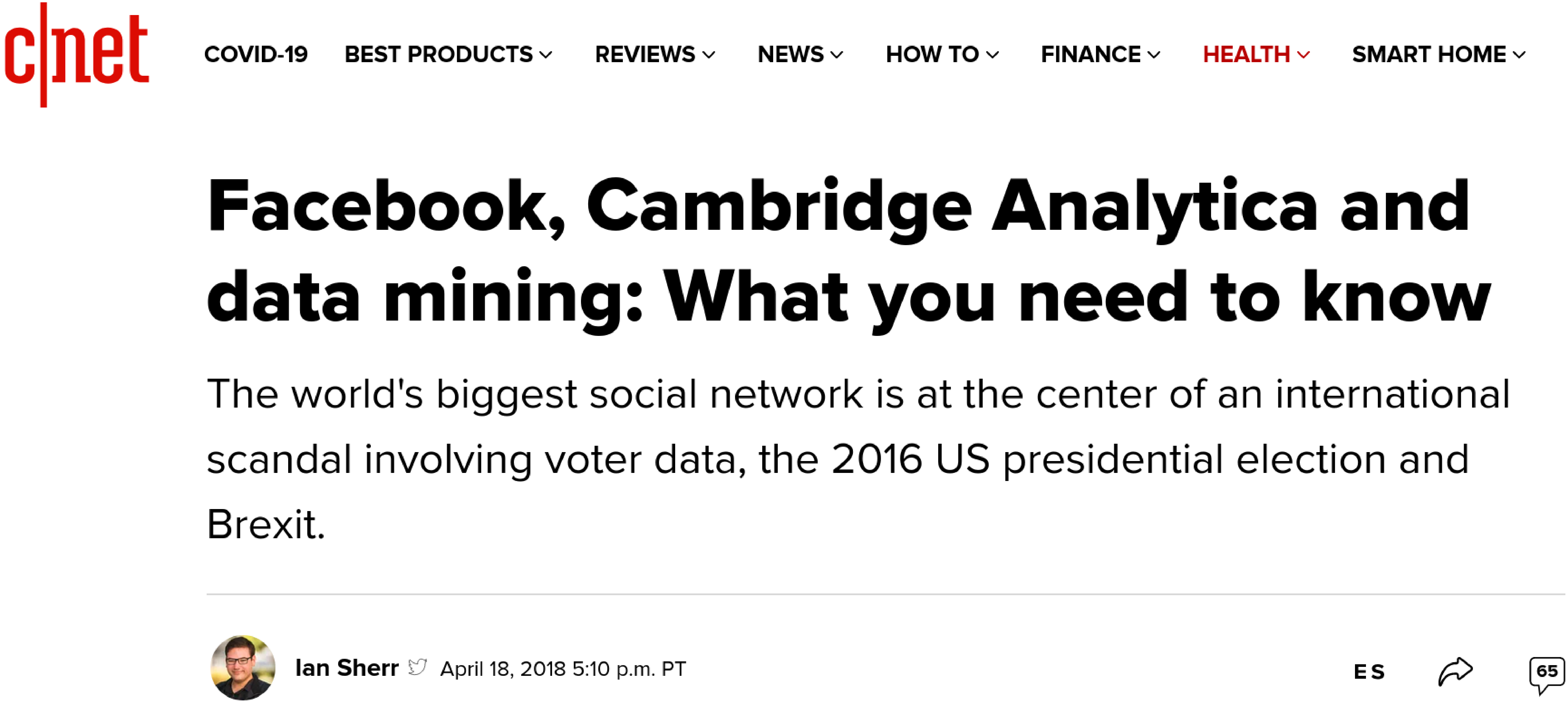
Uber concealed hack of 57 million accounts for more than a year

The company's former chief security officer kept the hack a secret.

https://www.zdnet.com/article/uber-concealed-hack-of-57-million-accounts-for-more-than-a-year/

Problem #2

competitive advantage / information cartels / data broker economy "one of the largest data leaks in the social network's history."



Facebook, Cambridge Analytica and data mining: What you need to know

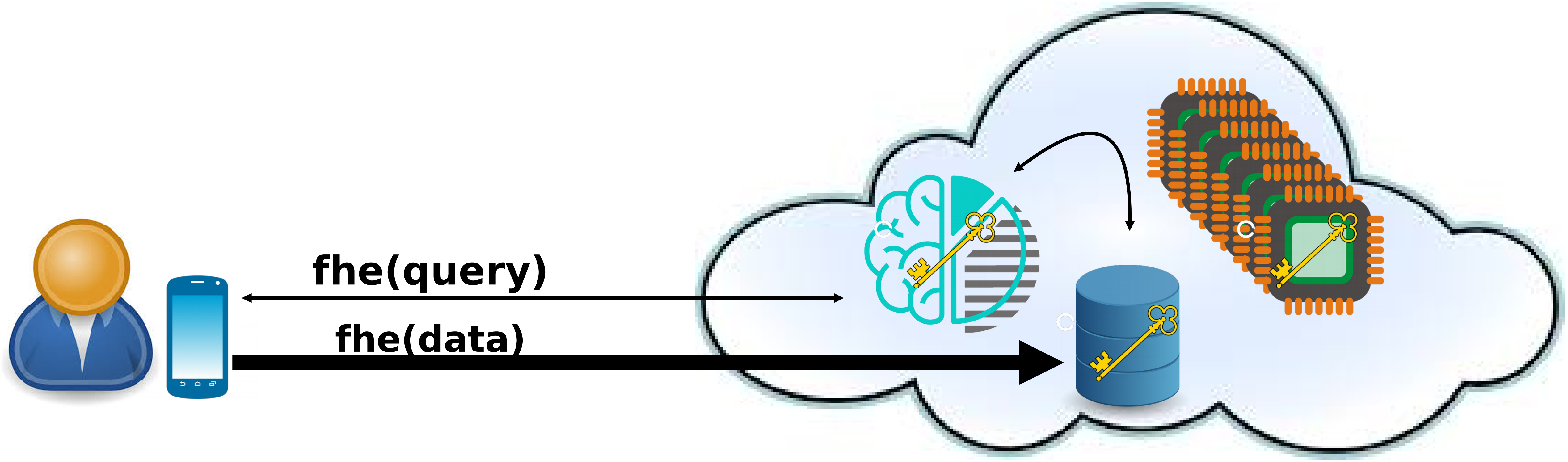
The world's biggest social network is at the center of an international scandal involving voter data, the 2016 US presidential election and Brexit.

Ian Sherr April 18, 2018 5:10 p.m. PT

https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/

homomorphic encryption

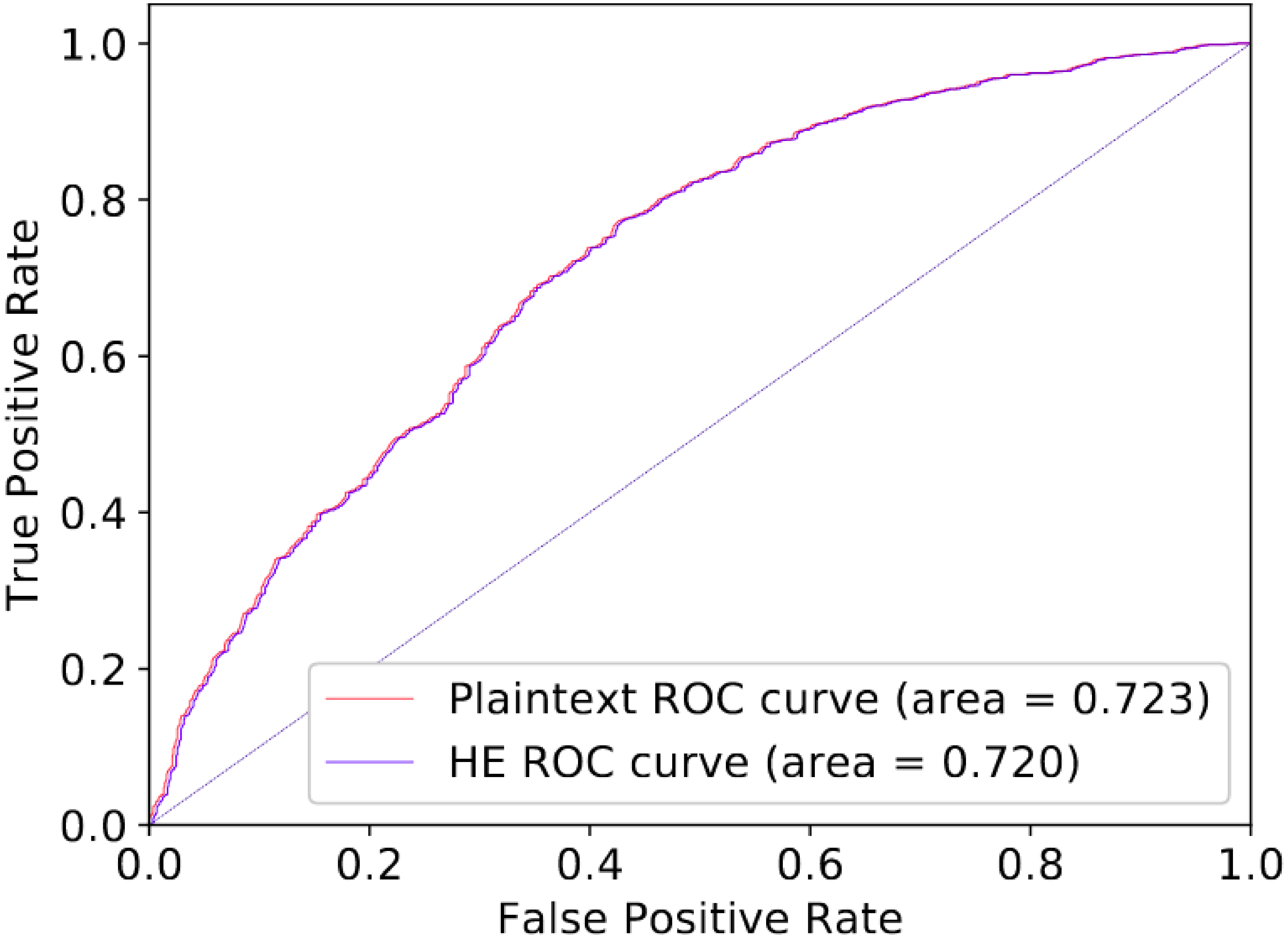
homomorphic encryption



Towards a Homomorphic Machine Learning Big Data Pipeline for the Financial Services Sector

Oliver Masters[1], Hamish Hunt[1], Enrico Steffinlongo[1], Jack Crawford[1], Flavio Bergamaschi[1], Maria Eugenia Dela Rosa[2], Caio Cesar Quini[2], Camila T. Alves[2], Fernanda de Souza[2], and Deise Goncalves Ferreira[2]

[1] IBM Research, Hursley, UK
{oliver.masters,enrico.steffinlongo,jack.crawford}@ibm.com
{hamishhun,flavio}@uk.ibm.com
[2] Banco Bradesco SA, Osasco, SP, Brasil
{maria.e.delarosa,caio.quini,camila.t.alves,fernanda.souza,deise.g.ferreira}@bradesco.com.br


1.0
0.8
0.6
0.4
0.2
0.0
True Positive Rate
0.0
0.2
0.4
0.6
0.8
1.0
False Positive Rate
Plaintext ROC curve (area = 0.723)
HE ROC curve (area = 0.720)

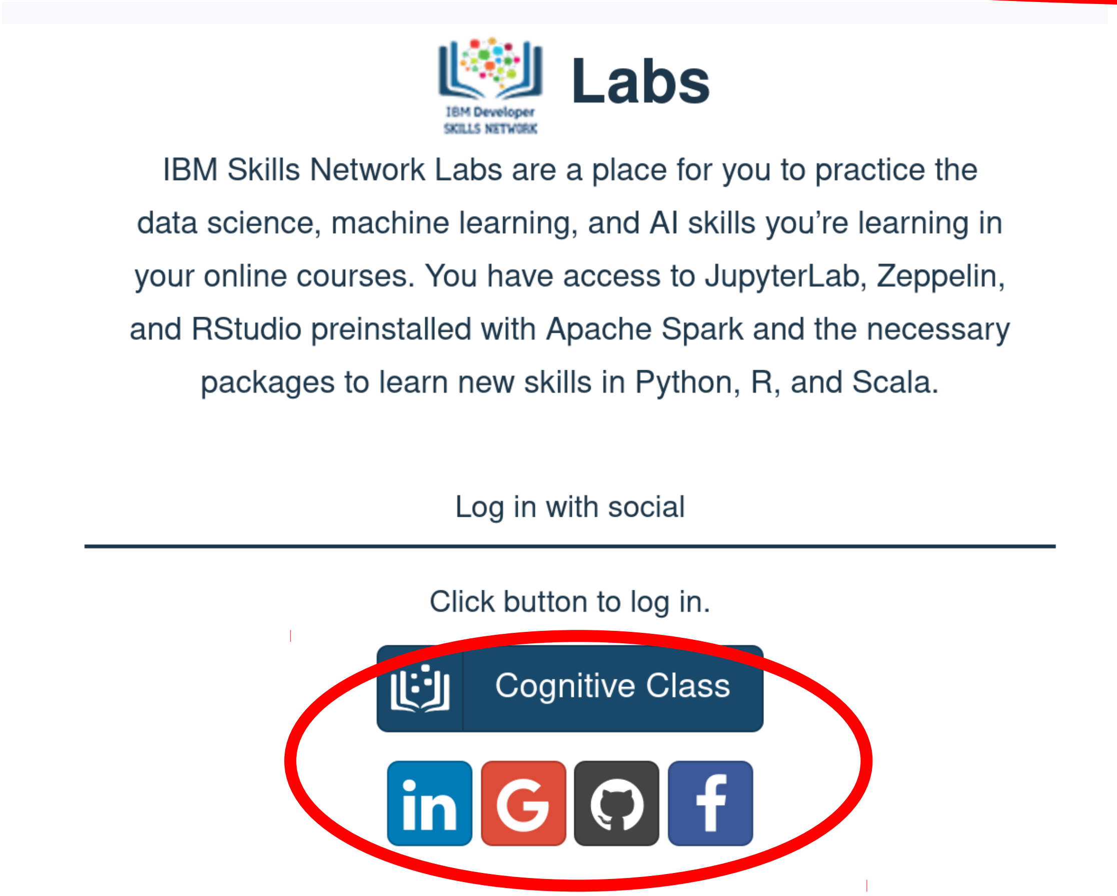
https://github.com/homenc/HElib

Lab 1: Homomorphic Encrytion

https://github.com/romeokienzler/ppml

he_1.ipynb

labs.cognitiveclass.ai

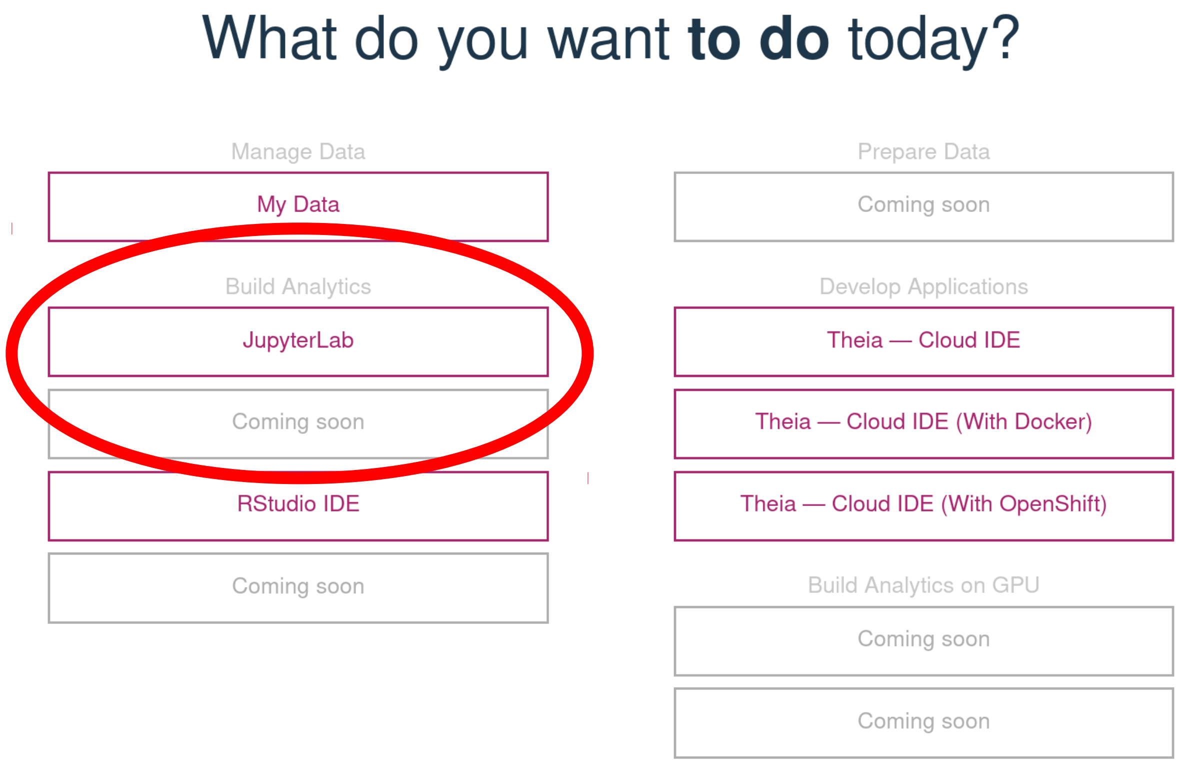


Labs

IBM Skills Network Labs are a place for you to practice the data science, machine learning, and AI skills you're learning in your online courses. You have access to JupyterLab, Zeppelin, and RStudio preinstalled with Apache Spark and the necessary packages to learn new skills in Python, R, and Scala.

Log in with social

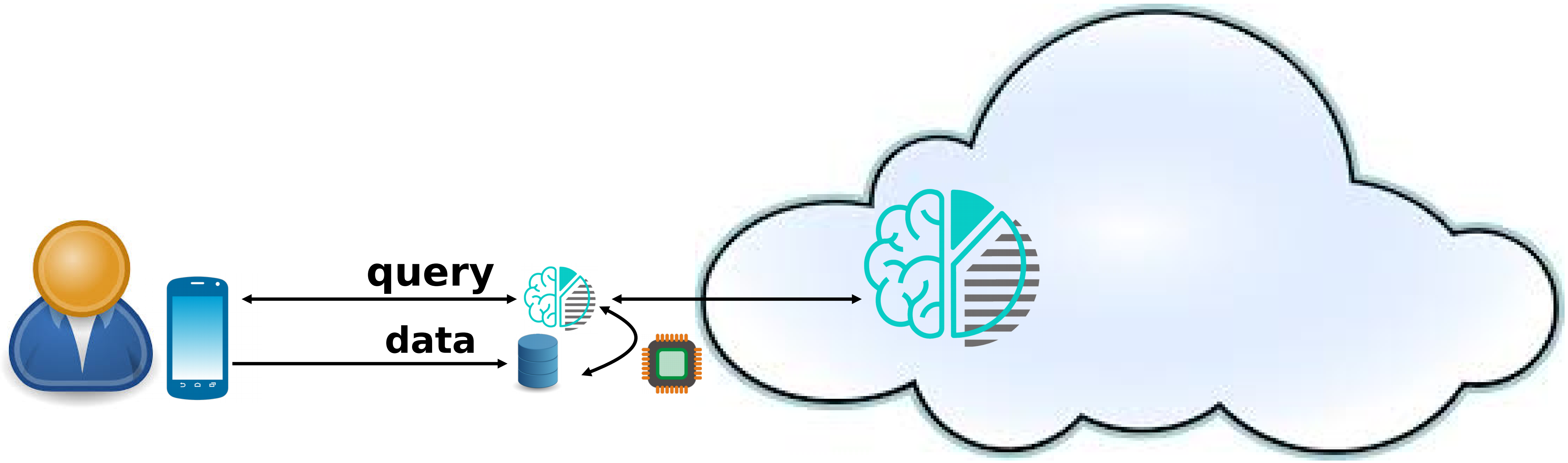
Click button to log in.

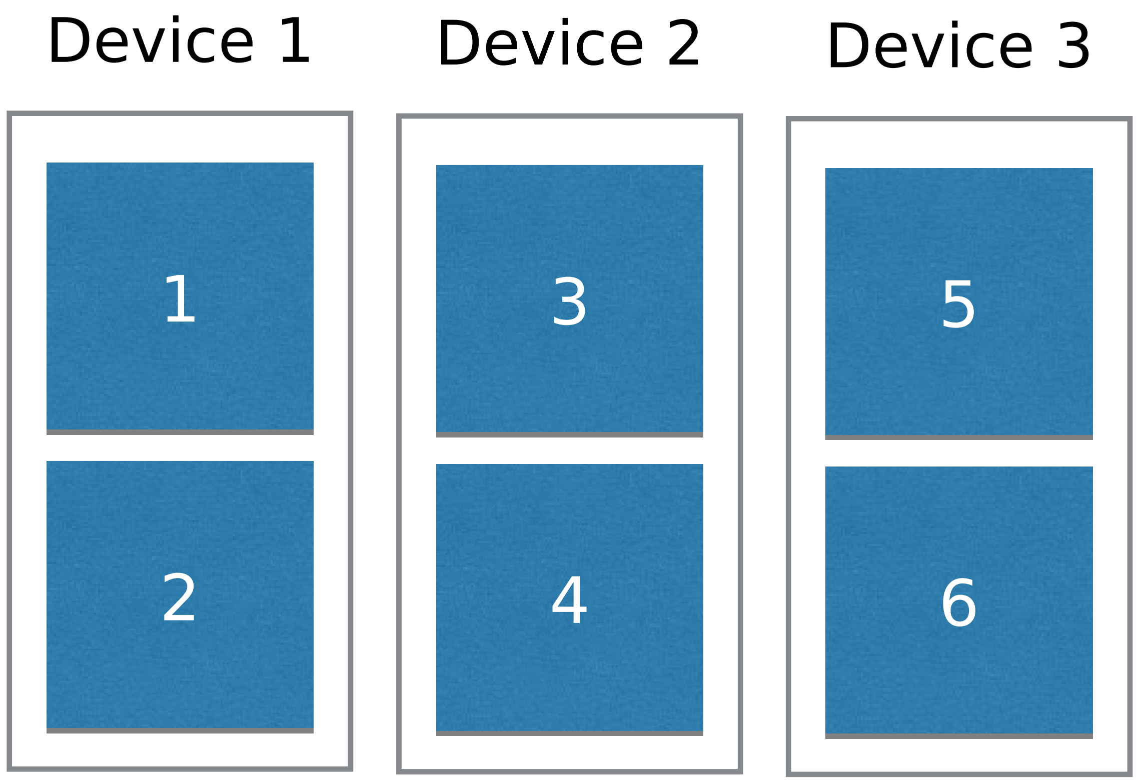


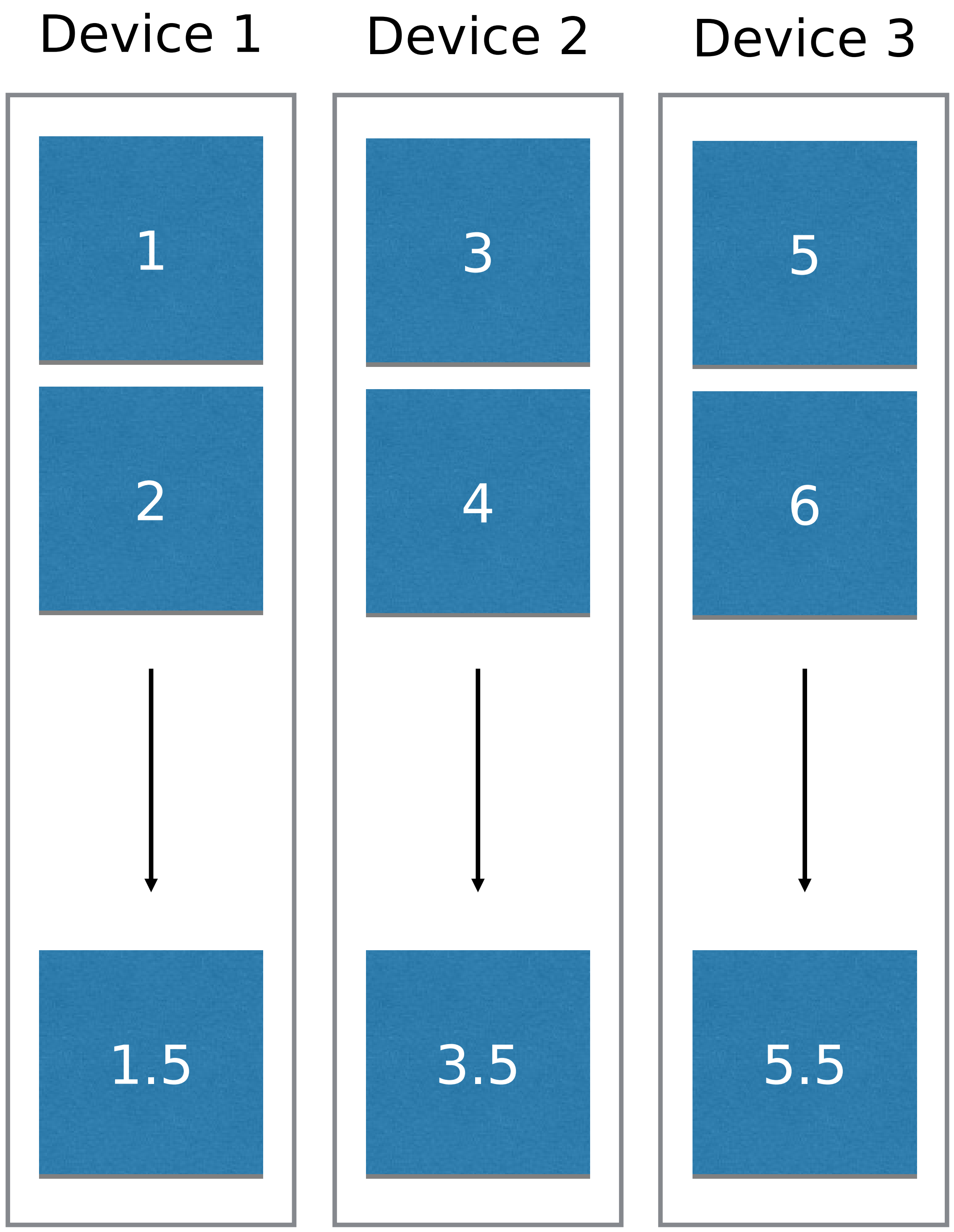
What do you want **to do** today?

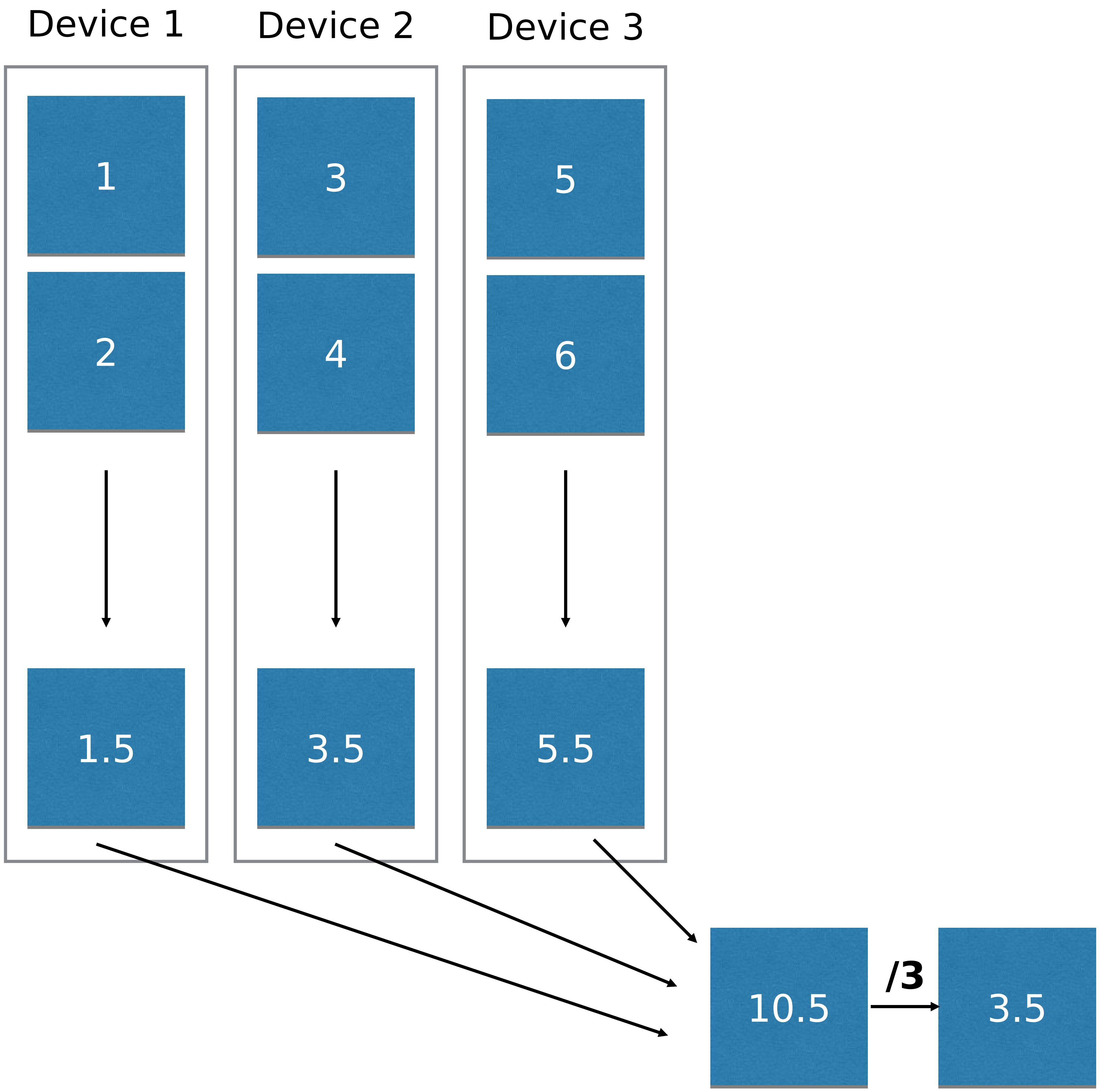
federated learning

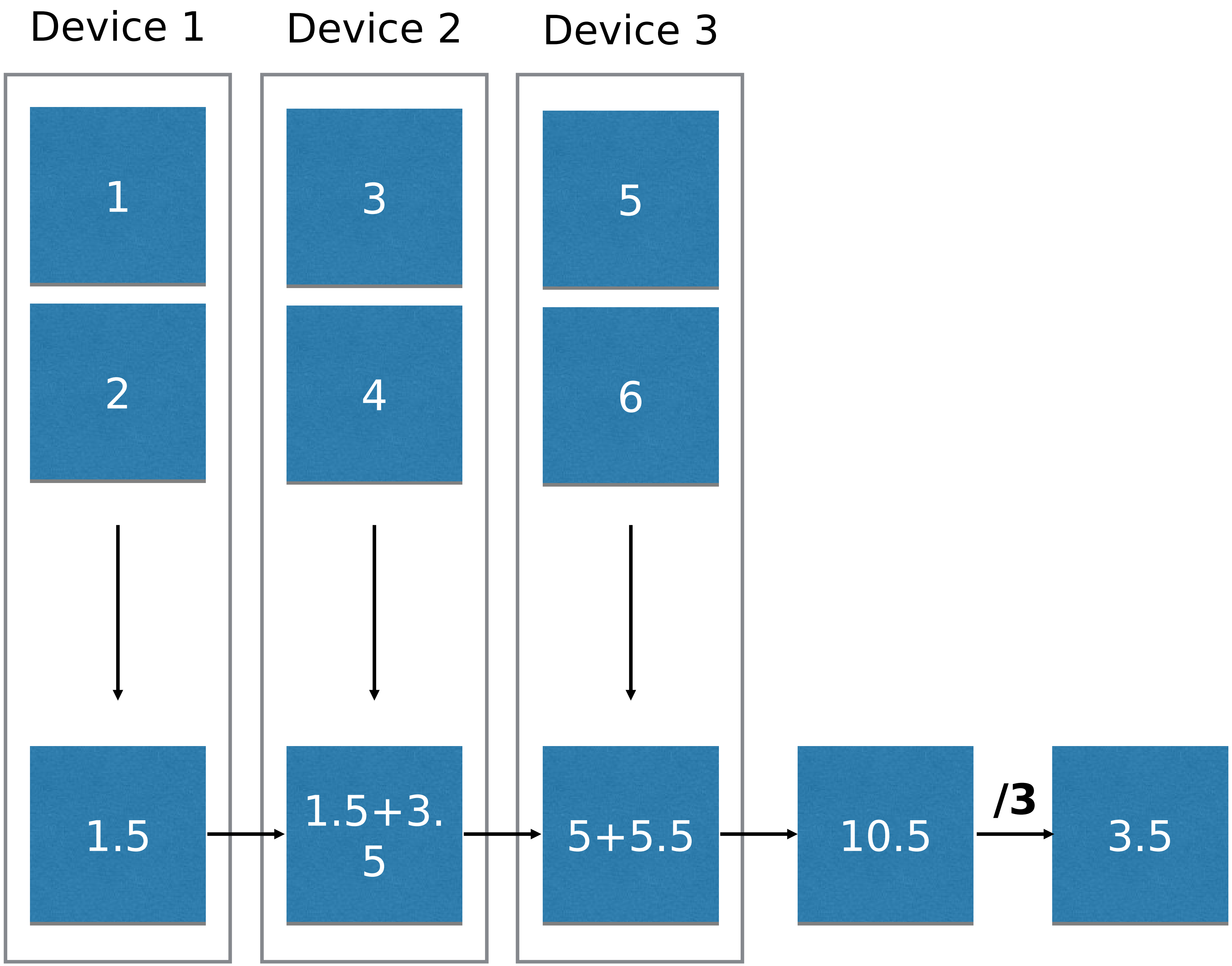
federated learning




Device 1
Device 2
Device 3
1
3
5
2
4
6


Device 1
Device 2
Device 3
1
3
5
2
4
6
1.5
3.5
5.5


Device 1
Device 2
Device 3
1
3
5
2
4
6
1.5
3.5
5.5
10.5
/3
3.5



Device 1

Device 2

Device 3

1

2

3

4

5

6

1.5

1.5+3.5

5+5.5

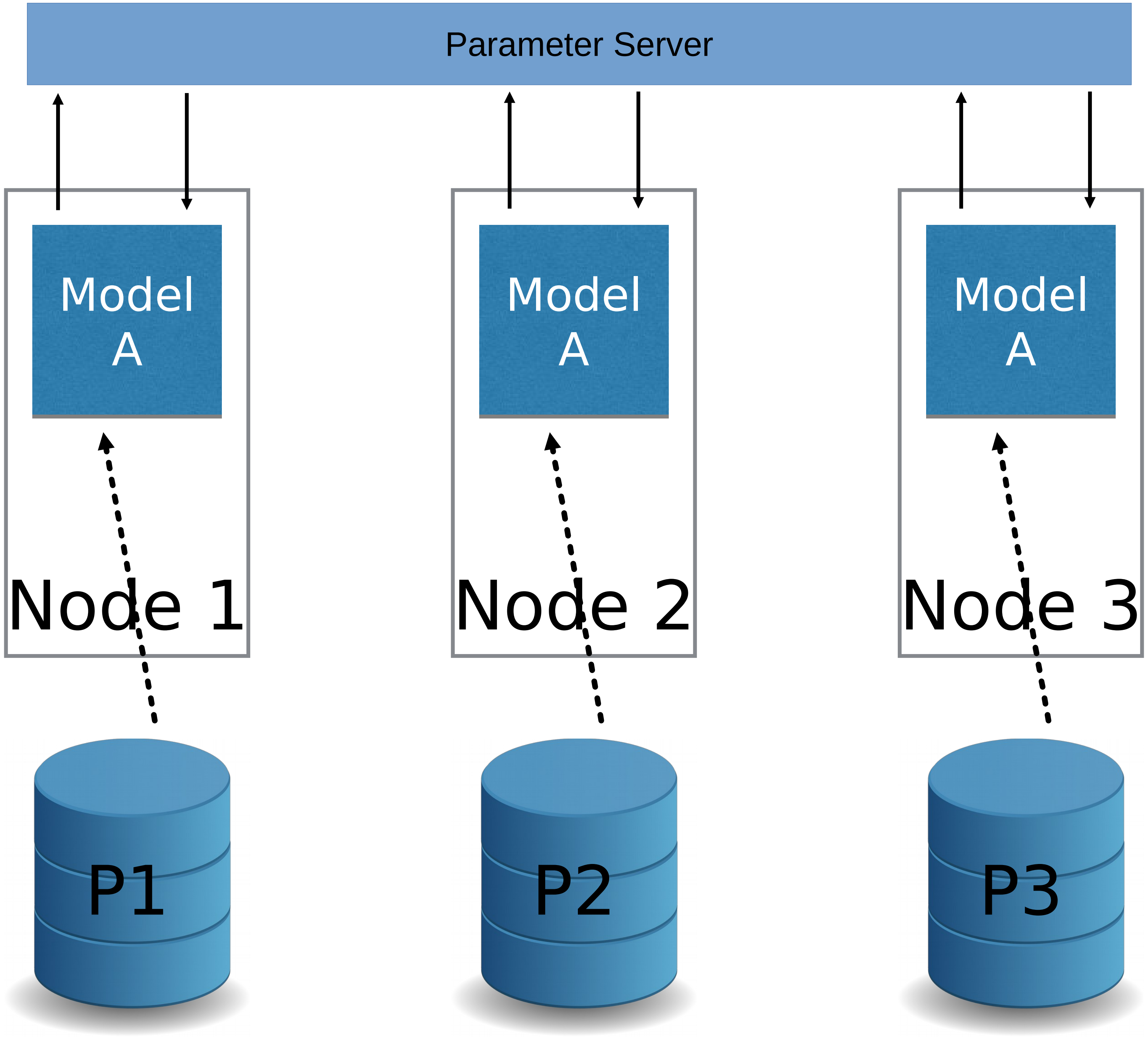
10.5

/3

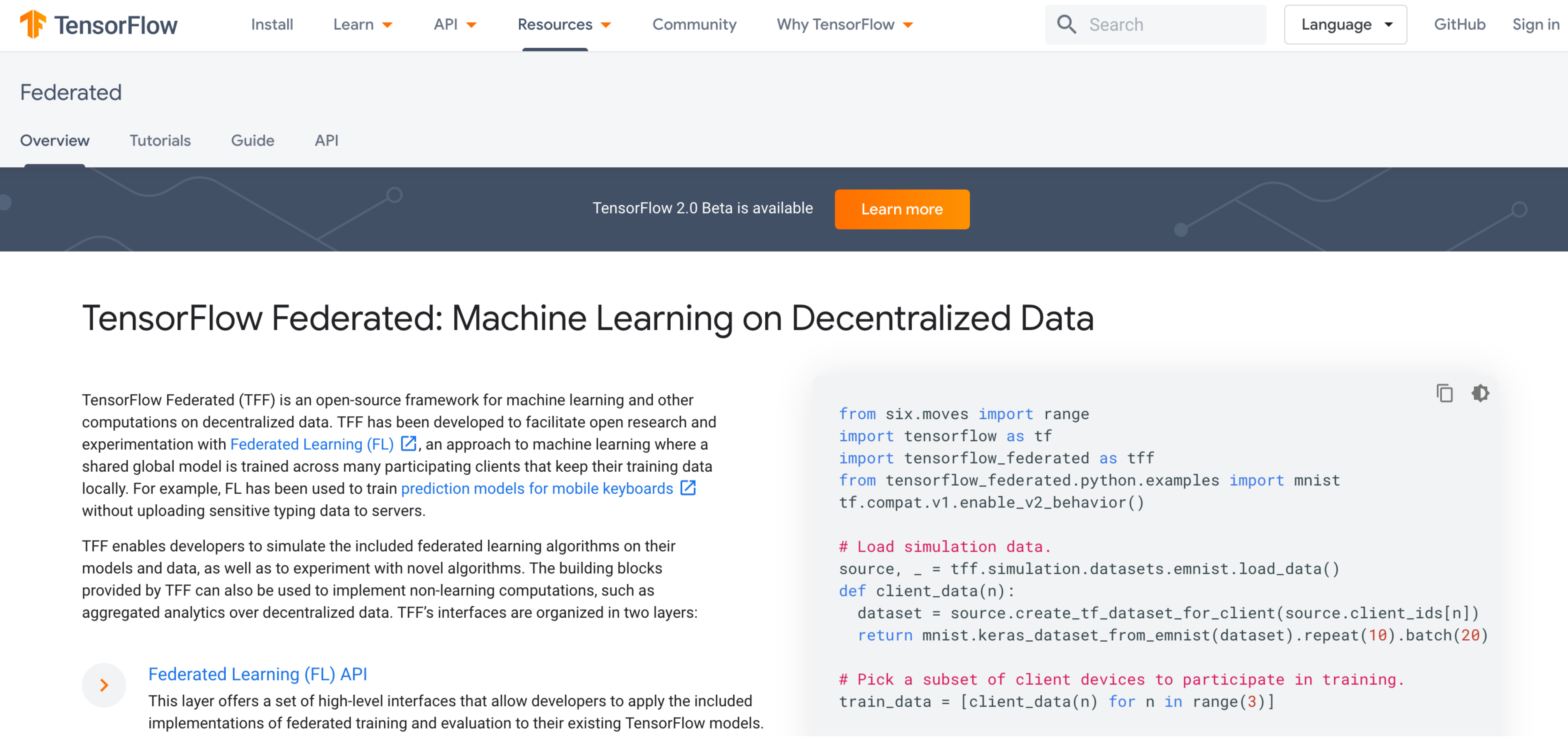
3.5

data parallelism

aka. “Jeff Dean style” parameter averaging



Romeo Kienzler



TensorFlow Federated: Machine Learning on Decentralized Data

TensorFlow Federated (TFF) is an open-source framework for machine learning and other computations on decentralized data. TFF has been developed to facilitate open research and experimentation with Federated Learning (FL), an approach to machine learning where a shared global model is trained across many participating clients that keep their training data locally. For example, FL has been used to train prediction models for mobile keyboards without uploading sensitive typing data to servers.

TFF enables developers to simulate the included federated learning algorithms on their models and data, as well as to experiment with novel algorithms. The building blocks provided by TFF can also be used to implement non-learning computations, such as aggregated analytics over decentralized data. TFF's interfaces are organized in two layers:

Federated Learning (FL) API

This layer offers a set of high-level interfaces that allow developers to apply the included implementations of federated training and evaluation to their existing TensorFlow models.

```
from six.moves import range
import tensorflow as tf
import tensorflow_federated as tff
from tensorflow_federated.python.examples import mnist
tf.compat.v1.enable_v2_behavior()

# Load simulation data.
source, _ = tff.simulation.datasets.emnist.load_data()
def client_data(n):
  dataset = source.create_tf_dataset_for_client(source.client_ids[n])
  return mnist.keras_dataset_from_emnist(dataset).repeat(10).batch(20)

# Pick a subset of client devices to participate in training.
train_data = [client_data(n) for n in range(3)]
```

Lab 2: Federated Learning

https://github.com/romeokienzler/ppml
fl_1.ipynb

differential privacy

Federated Learning Idea:
Share aggregates only

differential privacy

Problem:
https://en.wikipedia.org/wiki/Reconstruction_attack

differential privacy

Example:
Sales by County + Sales by LOB + Total Sales
May reveal sales of entities which are alone in a LOB/county combination

differential privacy

Conclusion:
No privacy without noise

ε-differential privacy

Summary:
Calibrating noise to sensitivity in private data analysis.

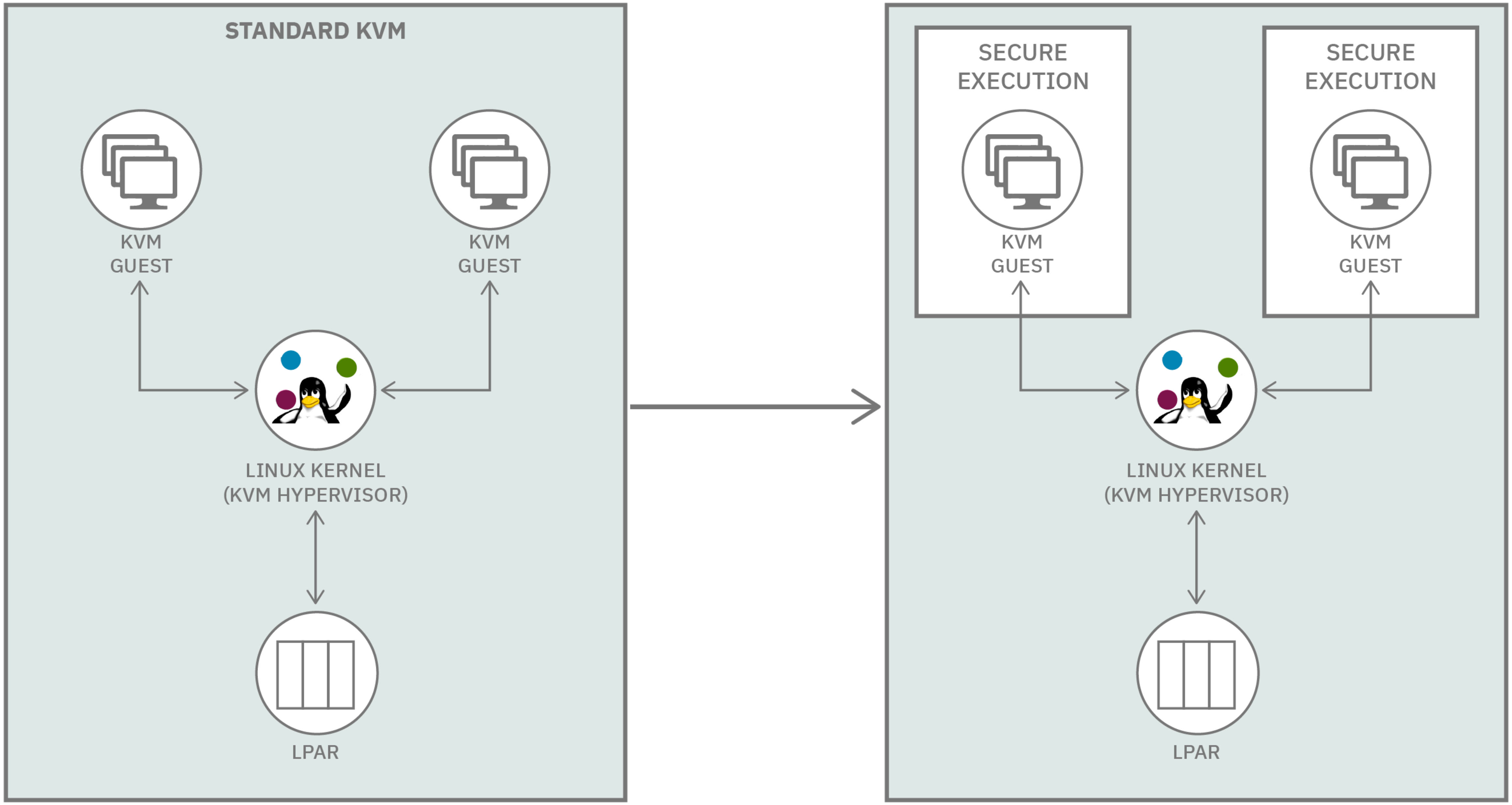
ε-differential privacy

In other words:

The more individuals are involved in an aggregate, the less noise needs to be added

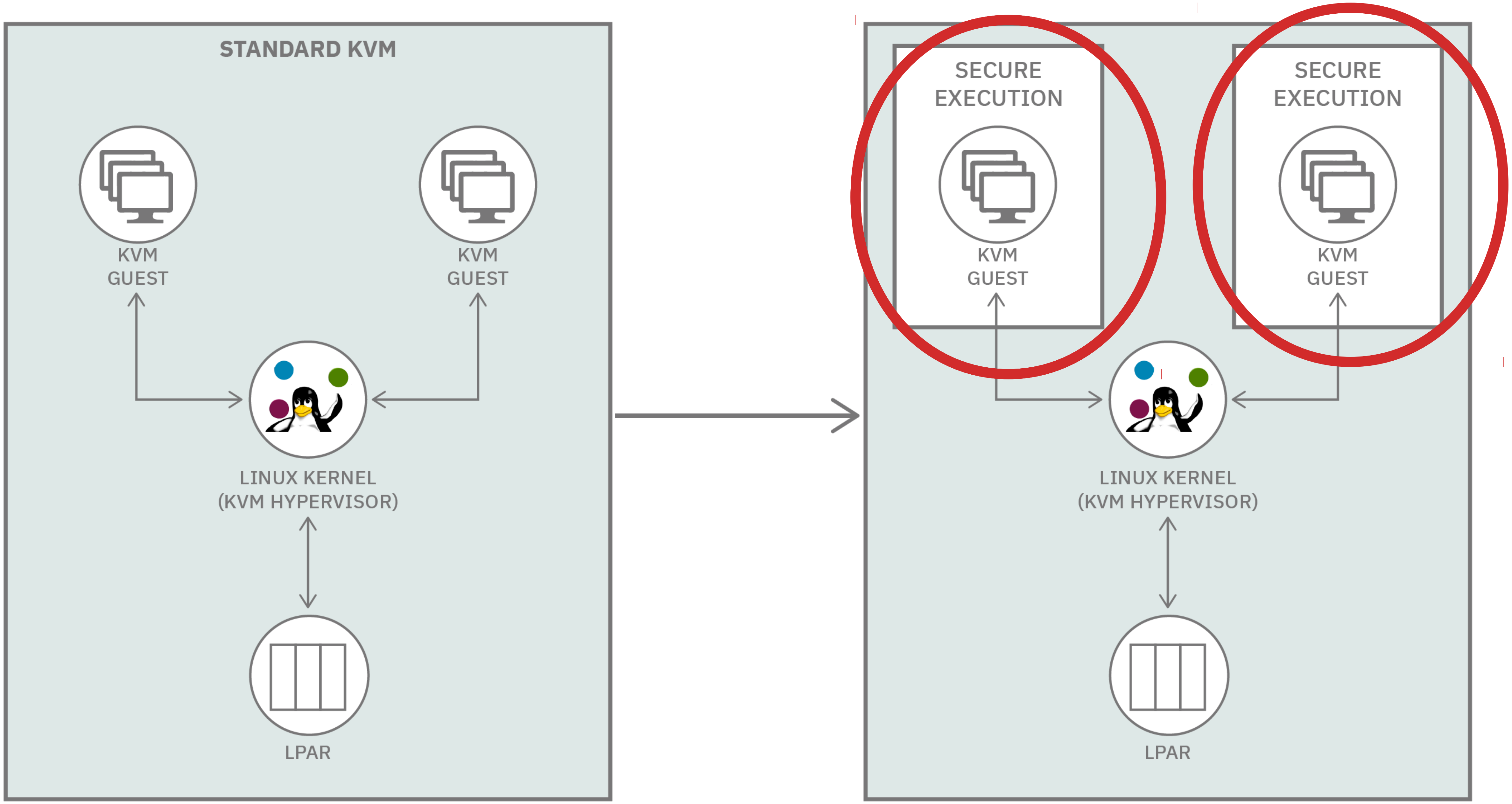
Trusted execution environments

Trusted Execution Environments



https://developer.ibm.com/components/ibmz/blogs/technical-overview-of-secure-execution-for-linux-on-ibm-z/

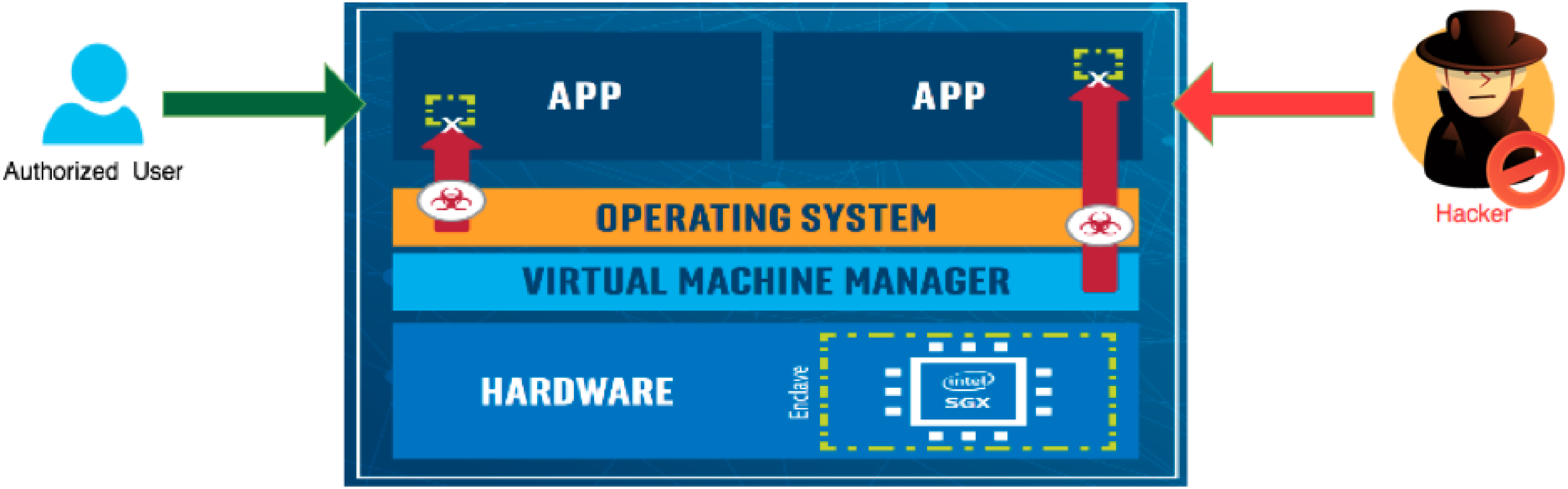
Trusted Execution Environments



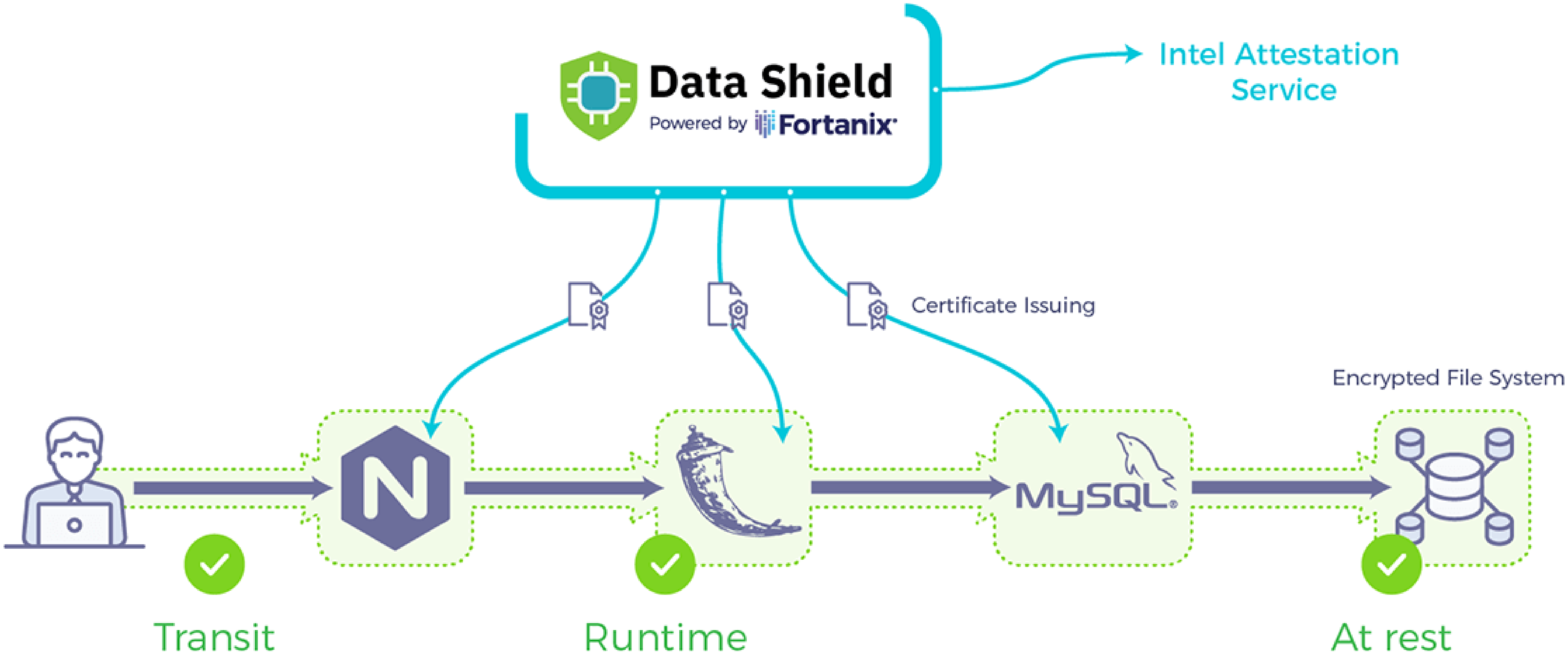
https://developer.ibm.com/components/ibmz/blogs/technical-overview-of-secure-execution-for-linux-on-ibm-z/

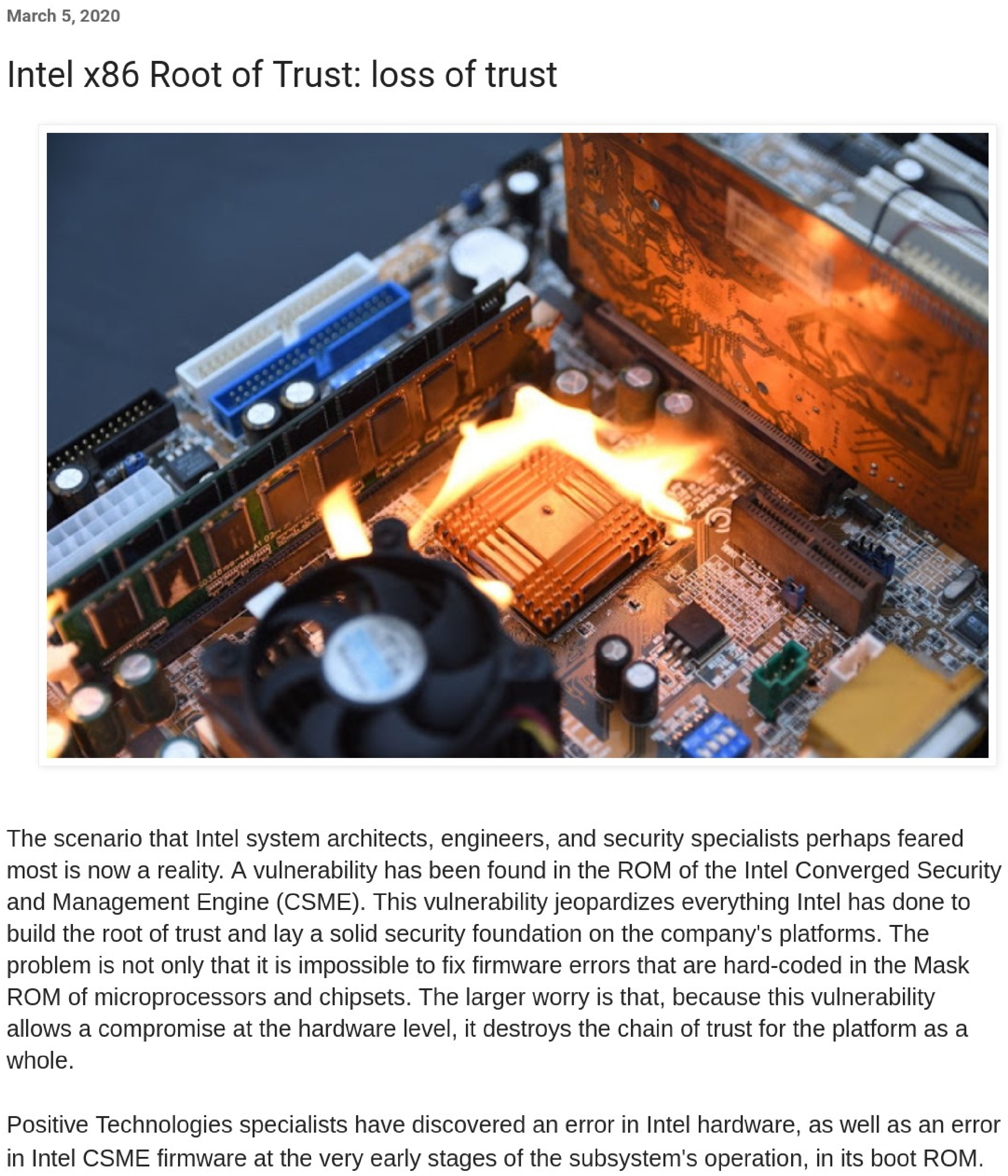
Intel SGX

(Software Guard Extensions)



IBM Data Shield





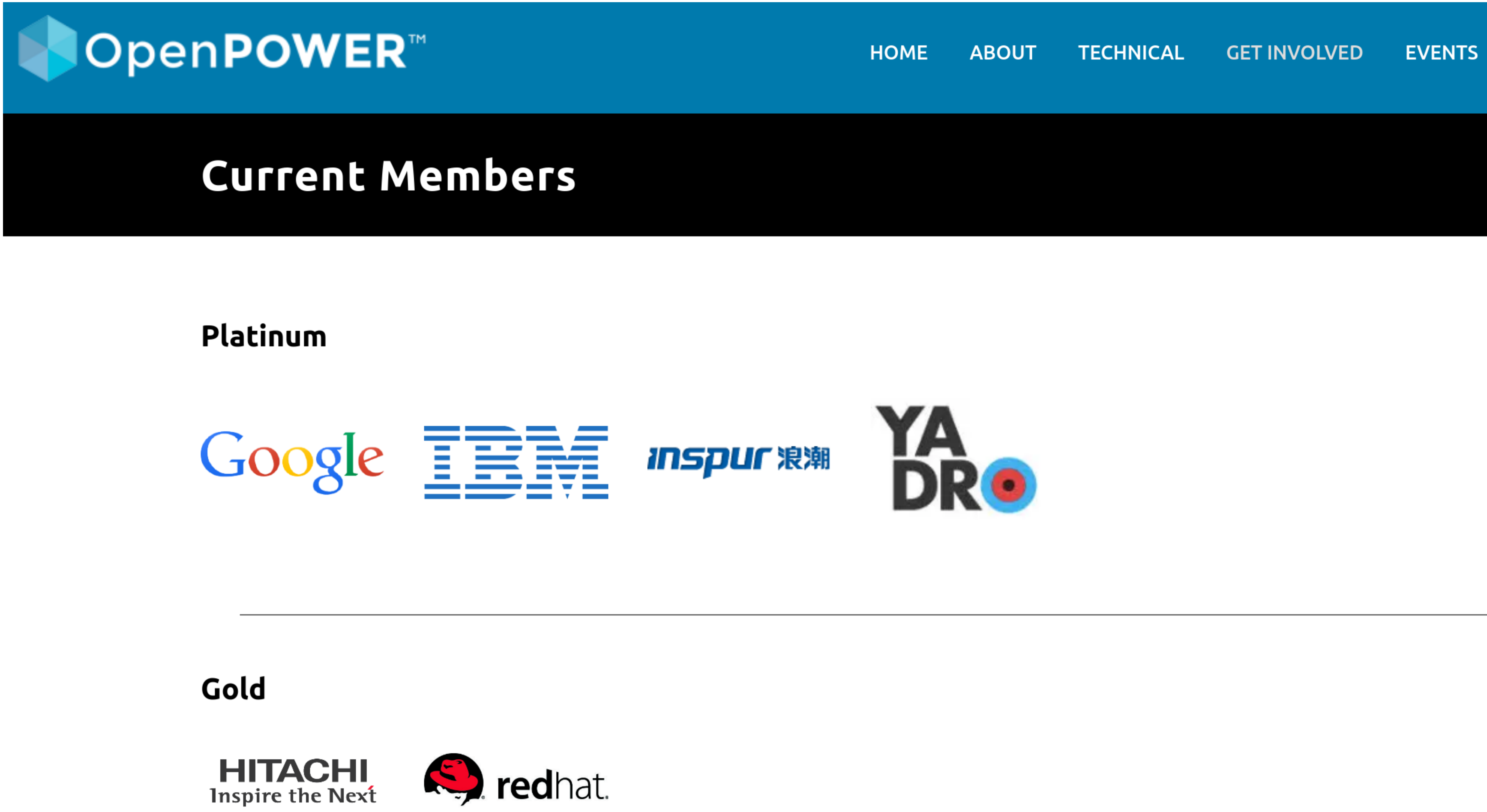
March 5, 2020

Intel x86 Root of Trust: loss of trust

The scenario that Intel system architects, engineers, and security specialists perhaps feared most is now a reality. A vulnerability has been found in the ROM of the Intel Converged Security and Management Engine (CSME). This vulnerability jeopardizes everything Intel has done to build the root of trust and lay a solid security foundation on the company's platforms. The problem is not only that it is impossible to fix firmware errors that are hard-coded in the Mask ROM of microprocessors and chipsets. The larger worry is that, because this vulnerability allows a compromise at the hardware level, it destroys the chain of trust for the platform as a whole.

Positive Technologies specialists have discovered an error in Intel hardware, as well as an error in Intel CSME firmware at the very early stages of the subsystem's operation, in its boot ROM.

http://blog.ptsecurity.com/2020/03/intelx86-root-of-trust-loss-of-trust.html

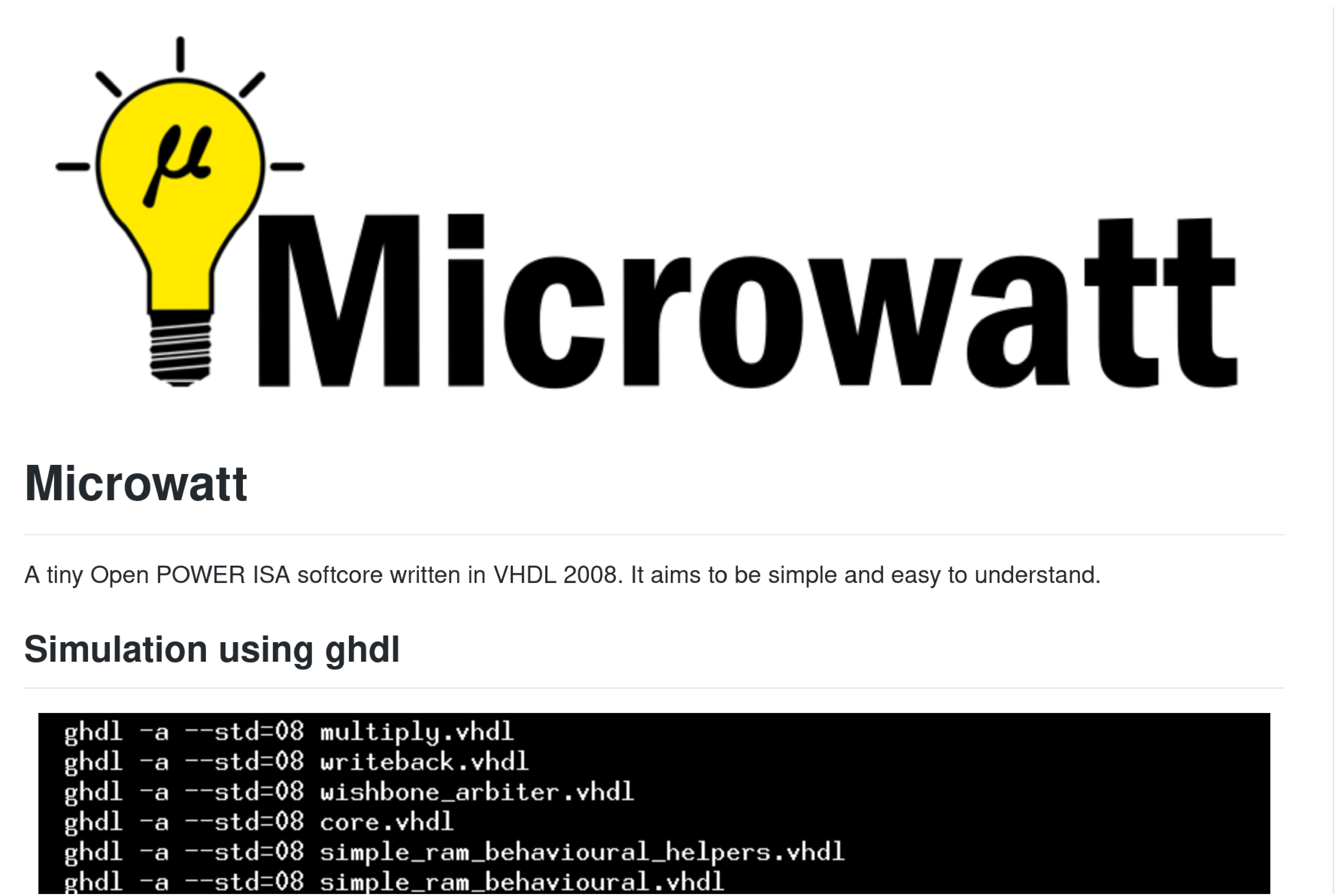


Current Members

Platinum

Gold

https://openpowerfoundation.org/membership/current-members/



Microwatt

A tiny Open POWER ISA softcore written in VHDL 2008. It aims to be simple and easy to understand.

Simulation using ghdl

```
ghdl -a --std=08 multiply.vhdl
ghdl -a --std=08 writeback.vhdl
ghdl -a --std=08 wishbone_arbiter.vhdl
ghdl -a --std=08 core.vhdl
ghdl -a --std=08 simple_ram_behavioural_helpers.vhdl
ghdl -a --std=08 simple_ram_behavioural.vhdl
```

https://github.com/antonblanchard/microwatt

…discussion…

(questions, comments, additions, complaints, suggestions, feedback, …)