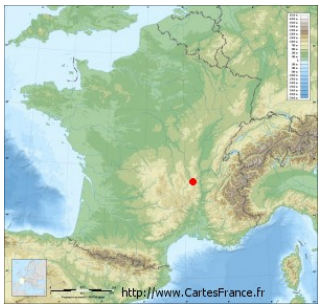
AI for IoT and Smart Cities

ISC2 Tutorial

Guillaume MULLER and
Kamal SINGH

{fname.lname}@univ-st-etienne.fr
Saint-Etienne, France

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE



September 7, 2021

Outline

Outline

Inputs: Sensors

- Means to *collect* Data

From (Big) Data to Rich Services

Inputs: Sensors

- Means to *collect* Data

Output: Actuators

- Means to *act* on the world

From (Big) Data to Rich Services

Inputs: Sensors

- Means to *collect* Data

Output: Actuators

- Means to *act* on the world

Our Goal: Rich (Smart) Applications (IoT Examples)

Health Care plan operations, detect/predict diseases...

Smart Cities transport, energy saving...

From (Big) Data to Rich Services

Inputs: Sensors

- Means to *collect* Data
- Big Data
  - **V**olume, **V**elocity
  - **V**ariety, **V**eracity
  - **V**alue ...

Output: Actuators

- Means to *act* on the world

Our Goal: Rich (Smart) Applications (IoT Examples)

Health Care plan operations, detect/predict diseases...

Smart Cities transport, energy saving...

Smartness: Machine Learning (ML) / Data Science / AI

"Machine" $\Rightarrow$ Automatic

- 5 Vs
- Less human prior knowledge 

From (Big) Data to Rich Services

Smartness: Machine Learning (ML) / Data Science / AI

"Machine" $\Rightarrow$ Automatic

- 5 Vs
- Less human prior knowledge 

"Learning" $\Rightarrow$ Adapt

- Distribution drift

From (Big) Data to Rich Services

Smartness: Machine Learning (ML) / Data Science / AI

"Machine" $\Rightarrow$ Automatic

- 5 Vs
- Less human prior knowledge 

"Learning" $\Rightarrow$ Adapt

- Distribution drift

ML Goals

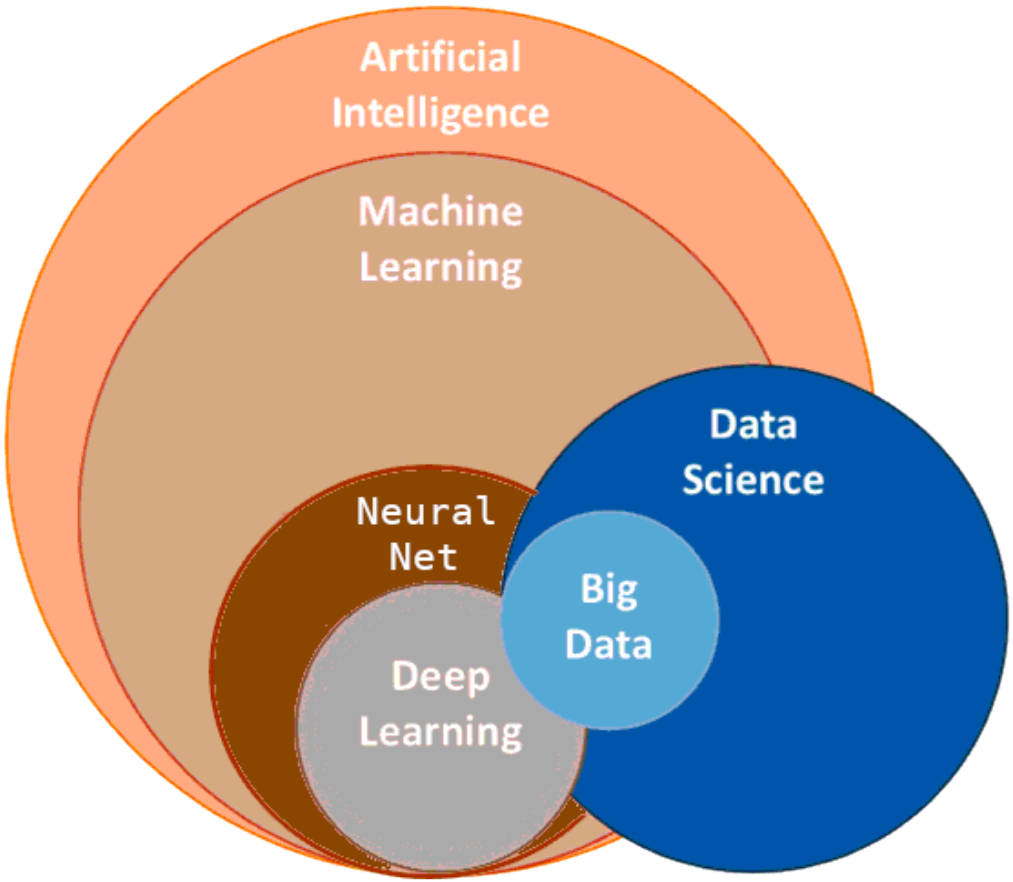
- Extract relevant information from raw data
  - Group/Rank elements, Predict values...
- Make relevant decisions based on this information
  - Take "optimal" decision

Big Data Market

"Data Scientist = Sexiest Job of 21st Century", HBR, 2012

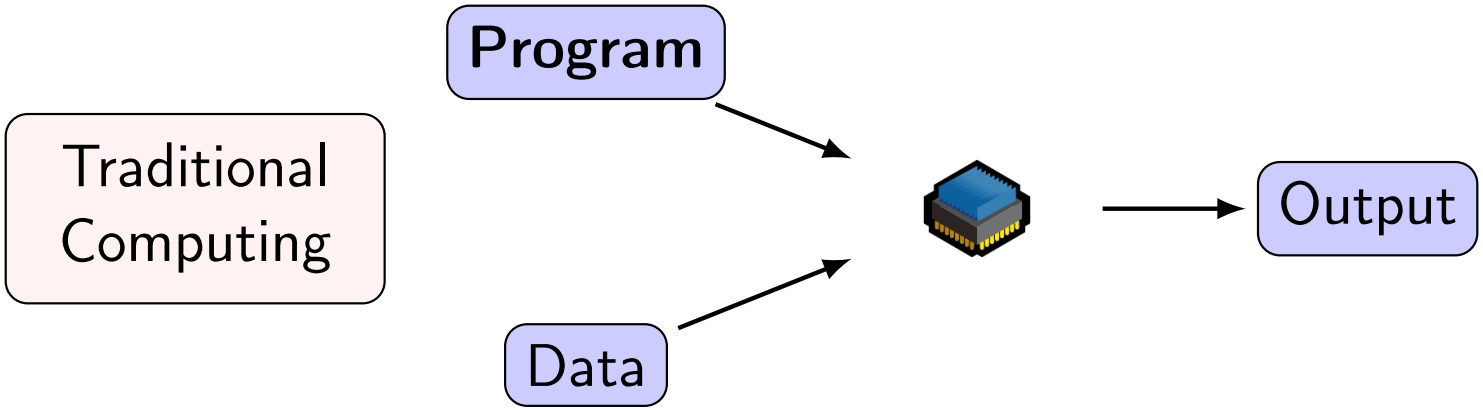
Outline

Big Data "Technologies"

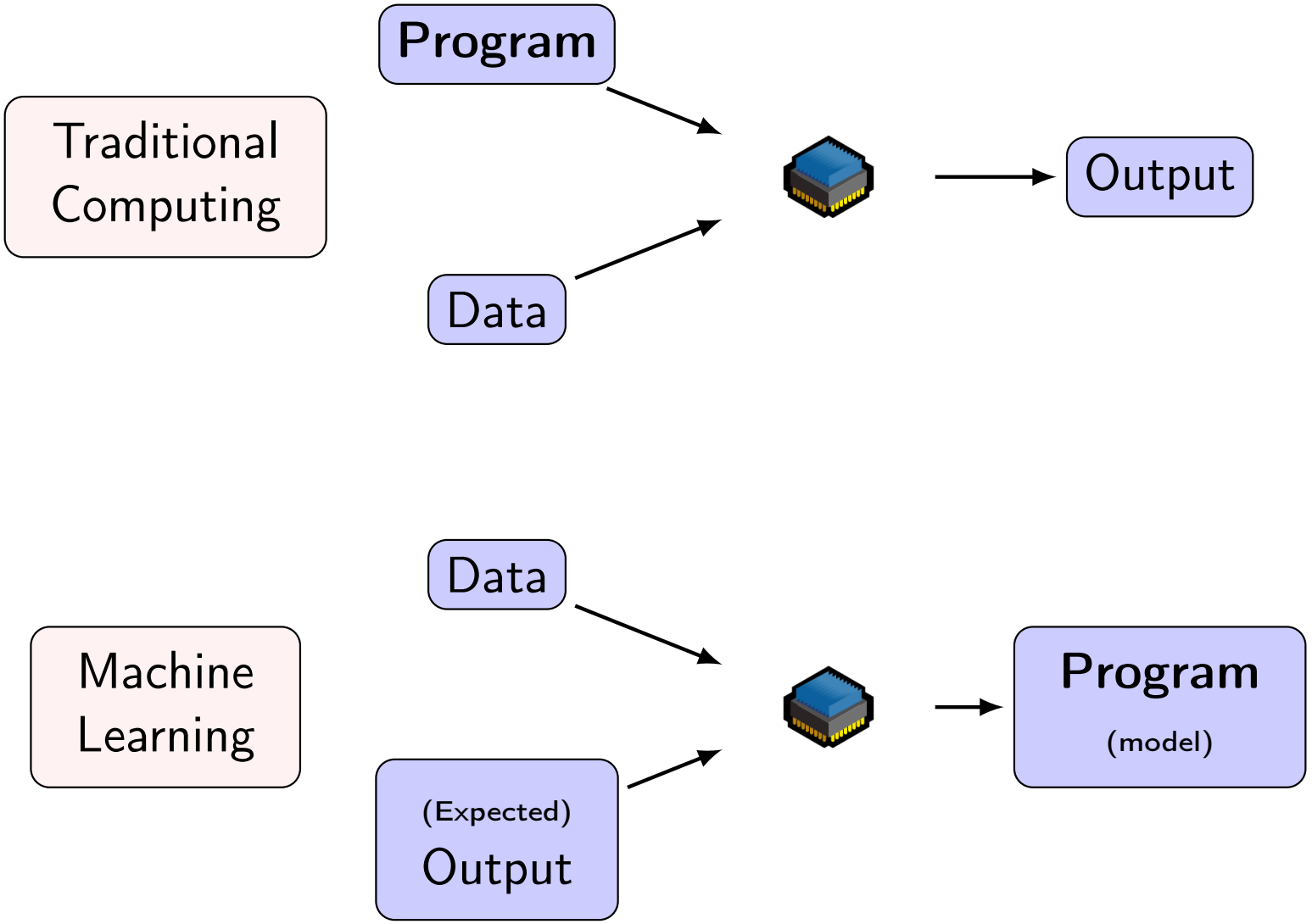


Based on: GMG Group

Machine Learning (vs. Traditional computing)

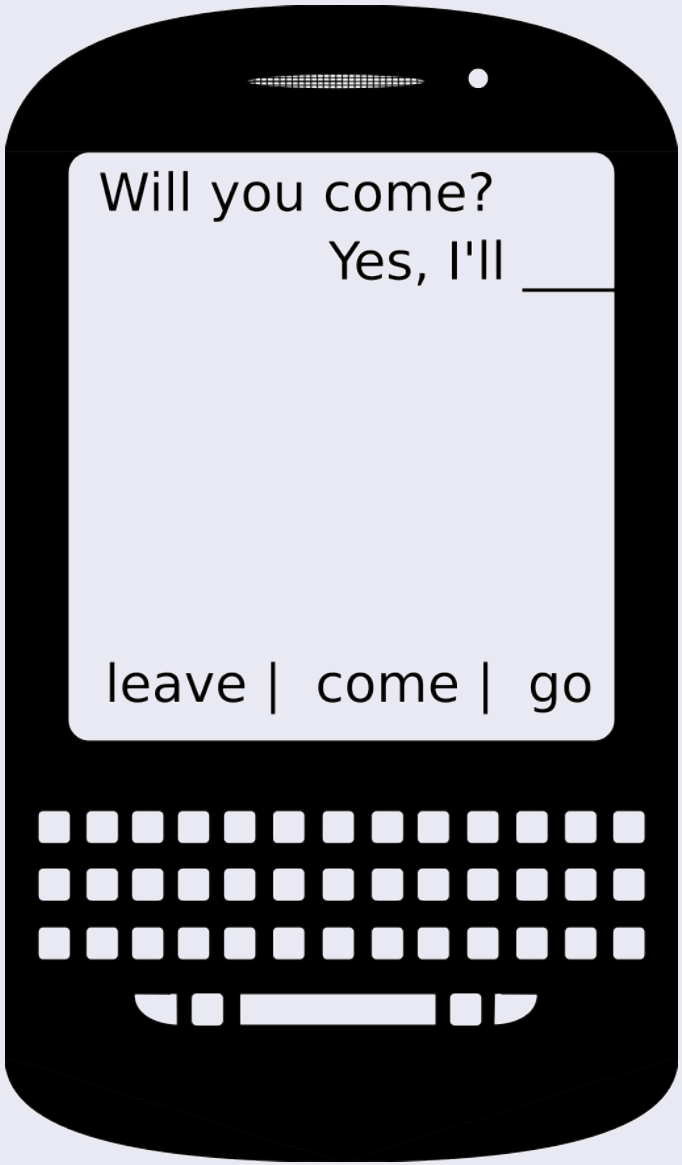


Machine Learning (vs. Traditional computing)



Machine Learning Example – Next Word Prediction

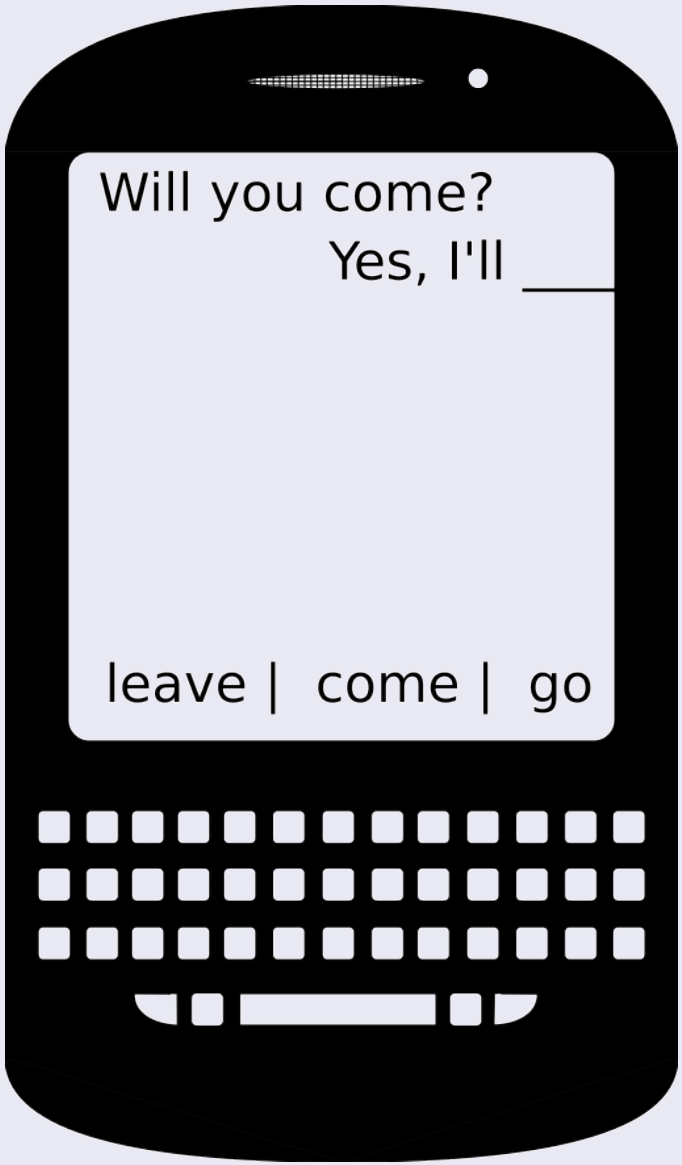
Machine Learning Example – Next Word Prediction



Machine Learning Process

- **Phase 1:** Train *@server*
  - Collect sentences
  - Compute "statistics"

Machine Learning Example – Next Word Prediction

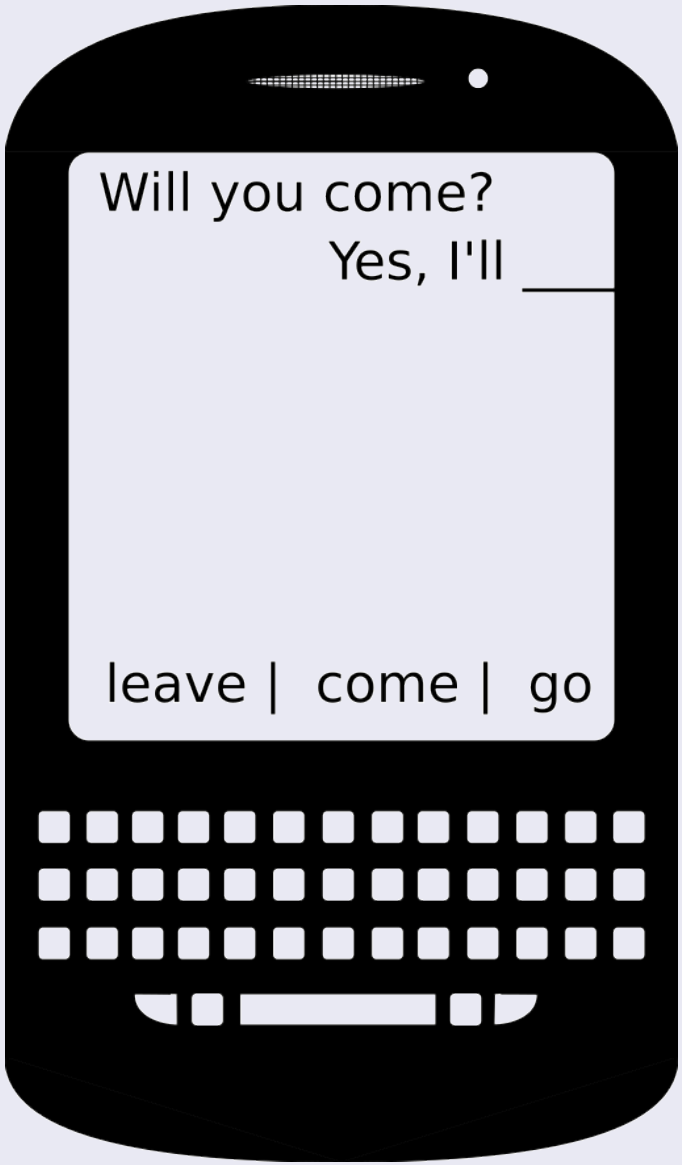


Machine Learning Process

- **Phase 1:** Train *@server*
  - Collect sentences
  - Compute "statistics"

Trained Model

Machine Learning Example – Next Word Prediction

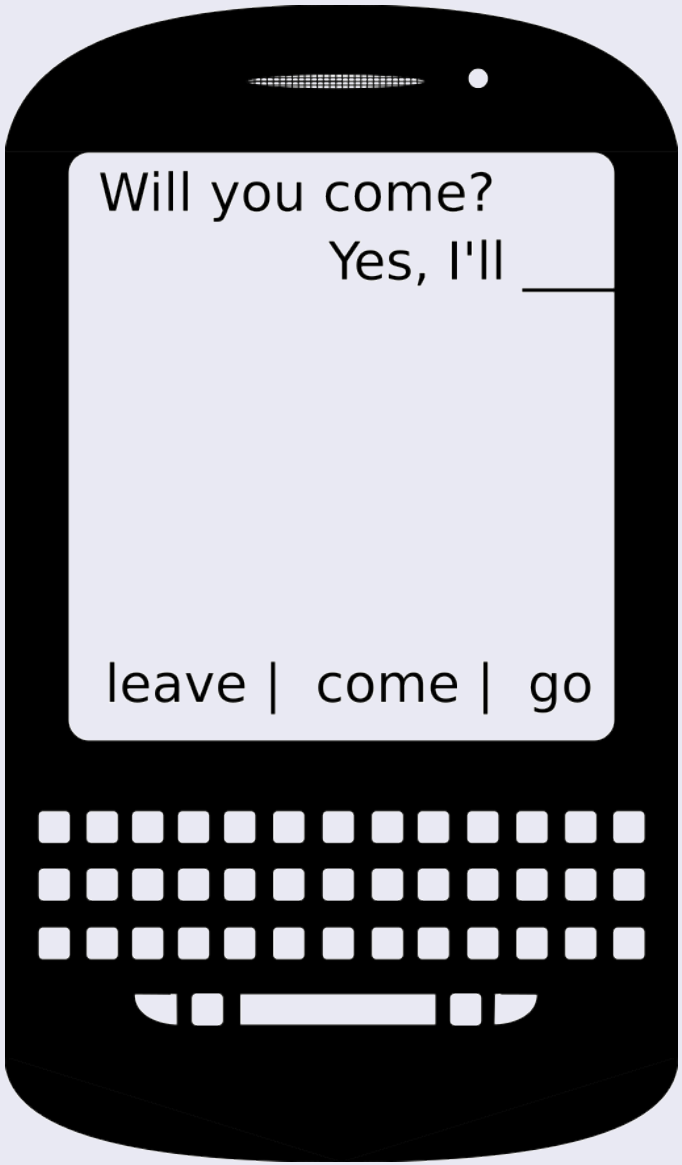


Machine Learning Process

- **Phase 1:** Train *@server*
  - Collect sentences
  - Compute "statistics"
  - Evaluate performance (`loss`)

Trained Model

Machine Learning Example – Next Word Prediction



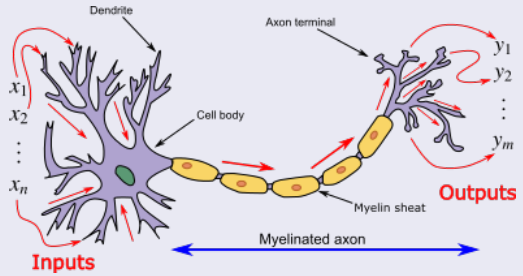
Machine Learning Process

- **Phase 1:** Train *@server*
  - Collect sentences
  - Compute "statistics"
  - Evaluate performance (`loss`)

Trained Model

- **Phase 2:** Use *@phone*
  - Get start of a sentence
  - Show most probable words

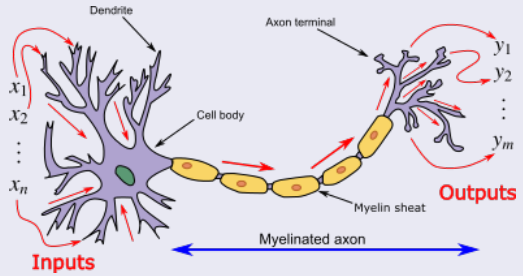
Biological Neuron



From: Prof. Loc Vu-Quoc

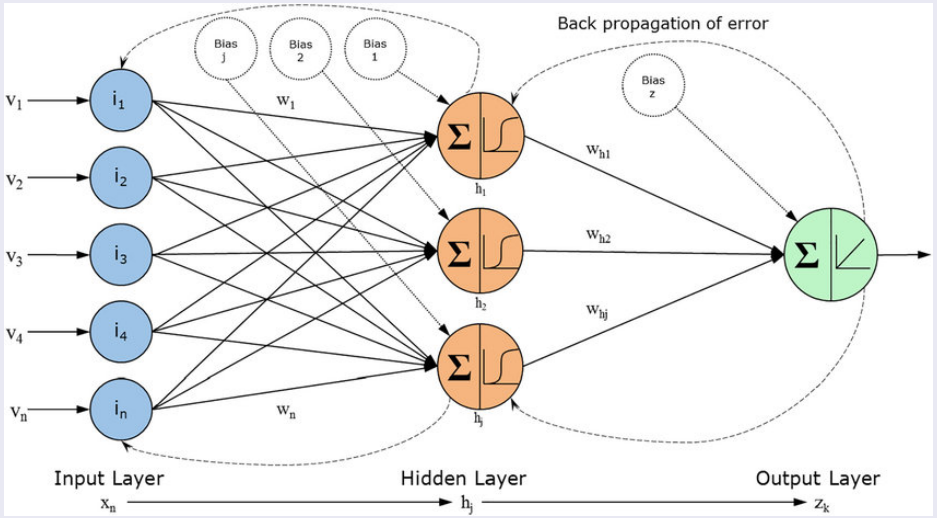
Neural Network (1 type of Machine Learning)

Biological Neuron



From: Prof. Loc Vu-Quoc

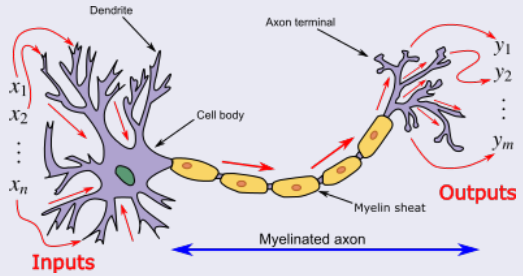
Artifical Neuron (Perceptron, Rosenblatt 1957)



From: D. Zafeiris, S. Rutella, G. R. Ball

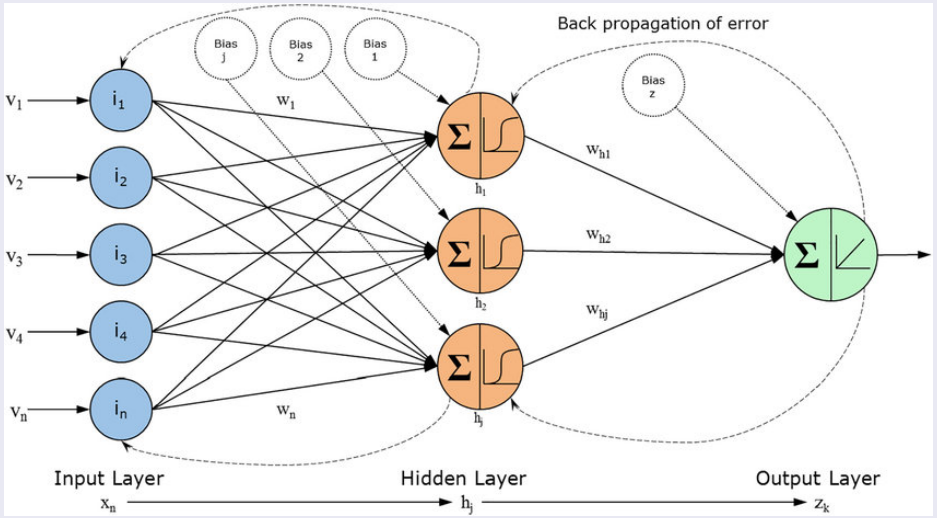
Neural Network (1 type of Machine Learning)

Biological Neuron



From: Prof. Loc Vu-Quoc

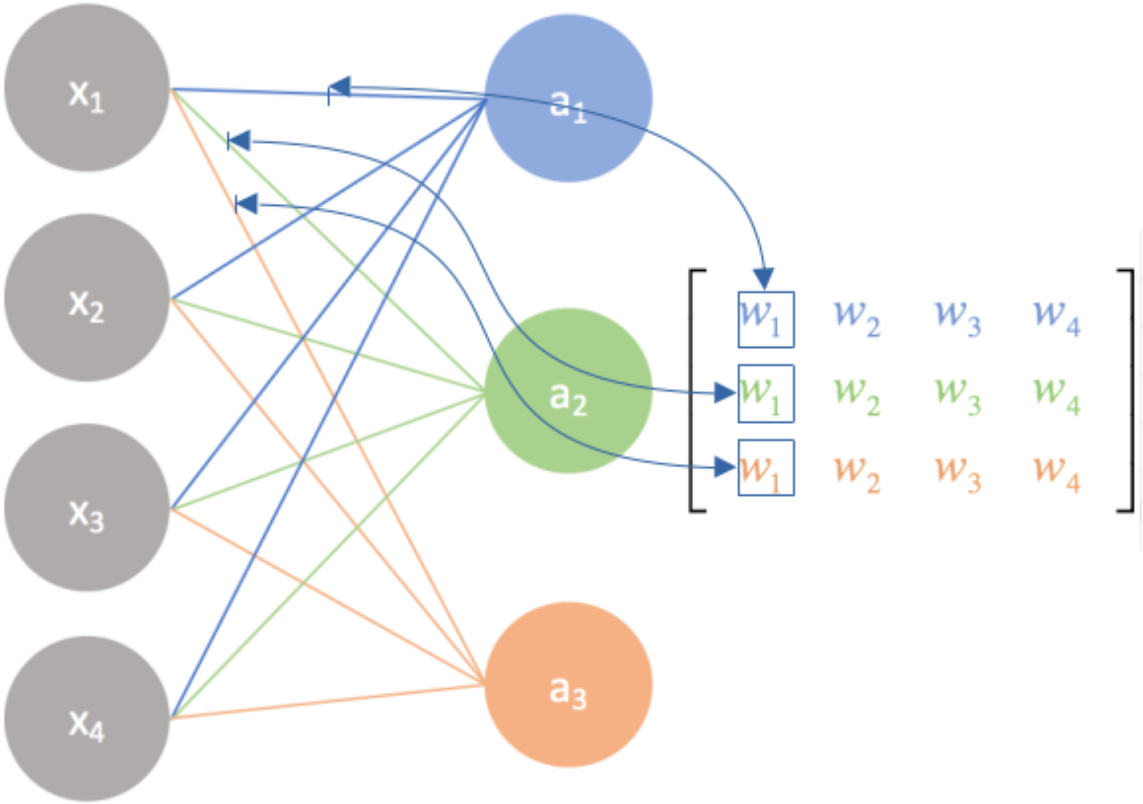
Artifical Neuron (Perceptron, Rosenblatt 1957)



From: D. Zafeiris, S. Rutella, G. R. Ball

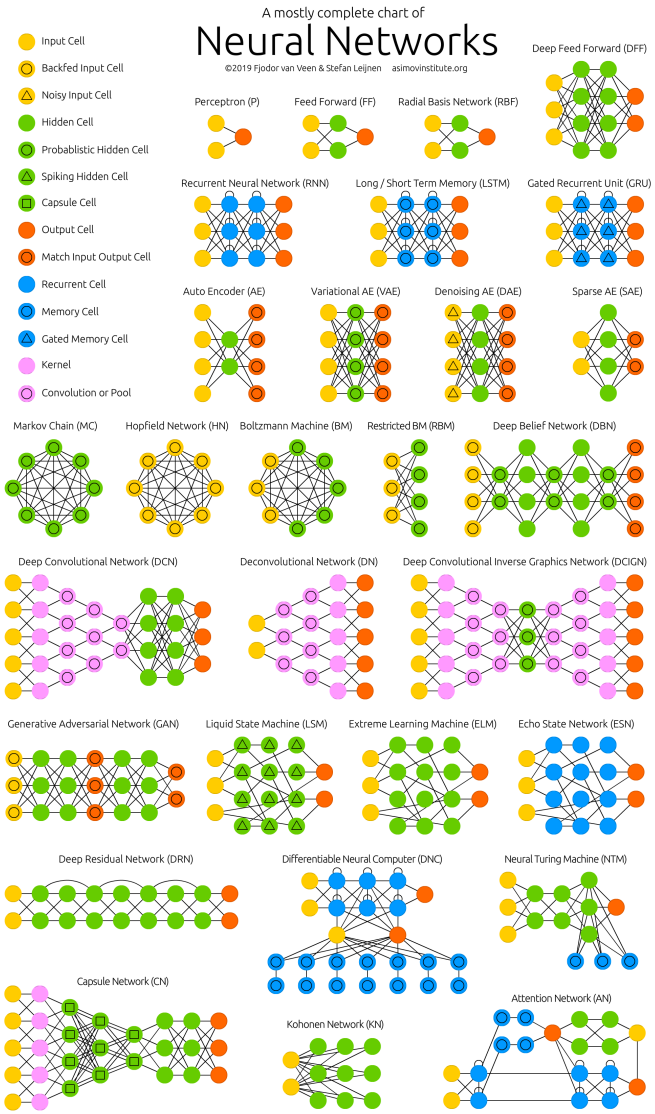
All numbers!

(Artificial) Neural Network as Matrices



From: jeremyjordan.me

(Artificial) Neural Network Zoo



From: Asimov Institute

Section Outline

Basics

- Feed Forward NN
- Recurrent NN
- Convolutional NN
- Auto-Encoder

State-of-the-art

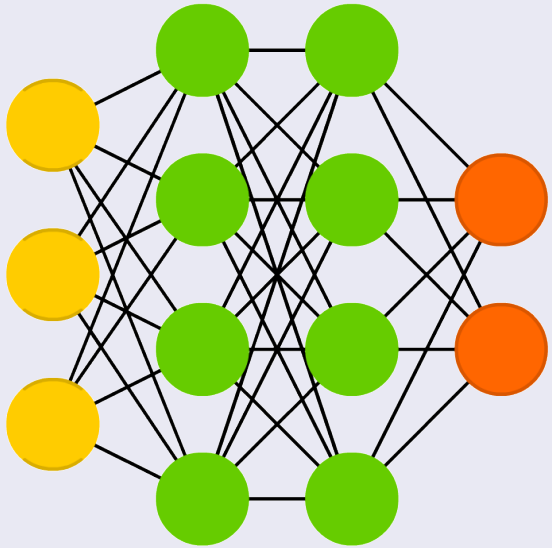
- Variational Auto-Encoder
- Generative Adversarial Network
- Attention Network

One/Few-shot training

- Siamese Networks

Feed Forward NN (MLP/FCN, Rosenblatt 1961)

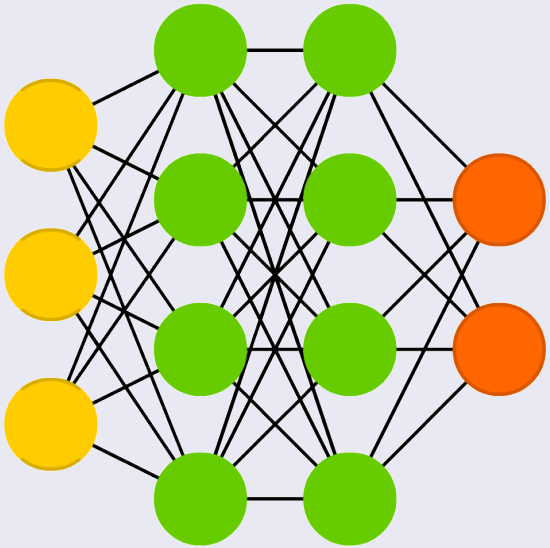
Deep Feed Forward (DFF)



From: Asimov Institute

Feed Forward NN (MLP/FCN, Rosenblatt 1961)

Deep Feed Forward (DFF)

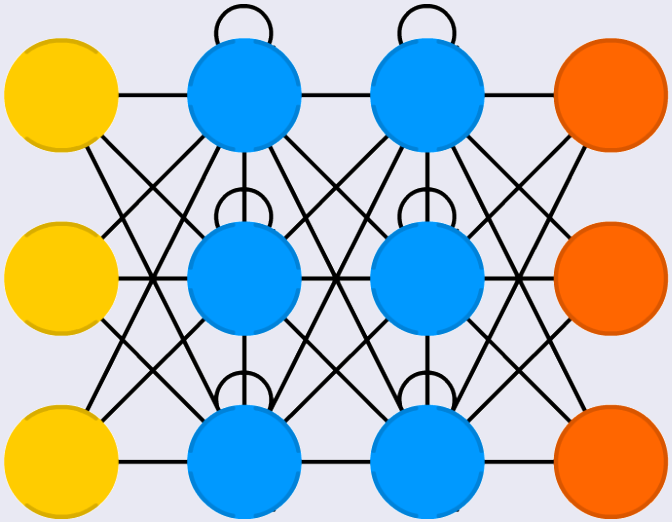


From: Asimov Institute

- Feed: Forward
- Train: Backward
  - Backpropagation
  - Gradient Descent

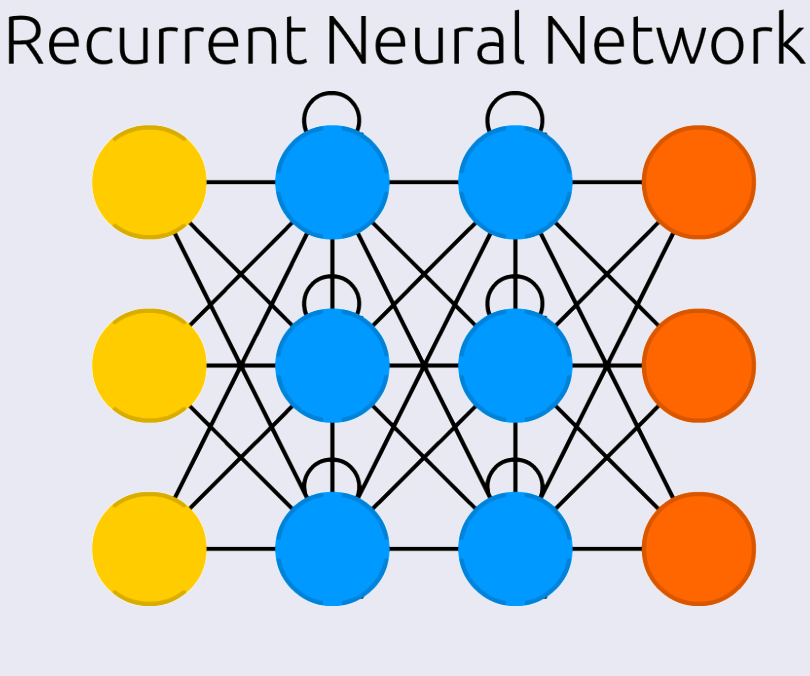
Recurrent Neural Network (RNN, Rumelhart 1986)

Recurrent Neural Network



From: Asimov Institute

Recurrent Neural Network (RNN, Rumelhart 1986)

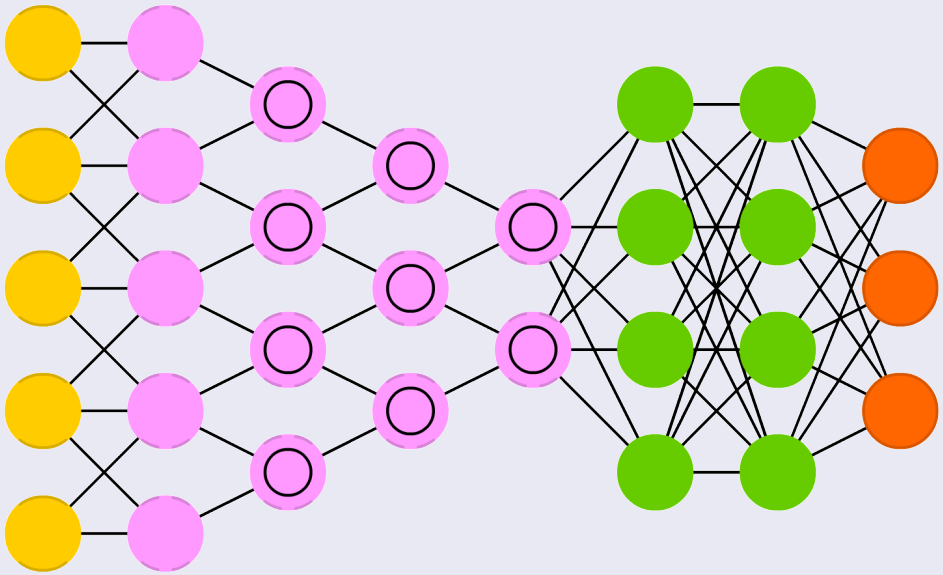


From: Asimov Institute

- For Sequences, Time Series (Memory)
- Harder to train: Vanishing/Exploding Gradient
- Improvements: LSTM / GRU

Convolutional Neural Network (CNN, Lecun 1989)

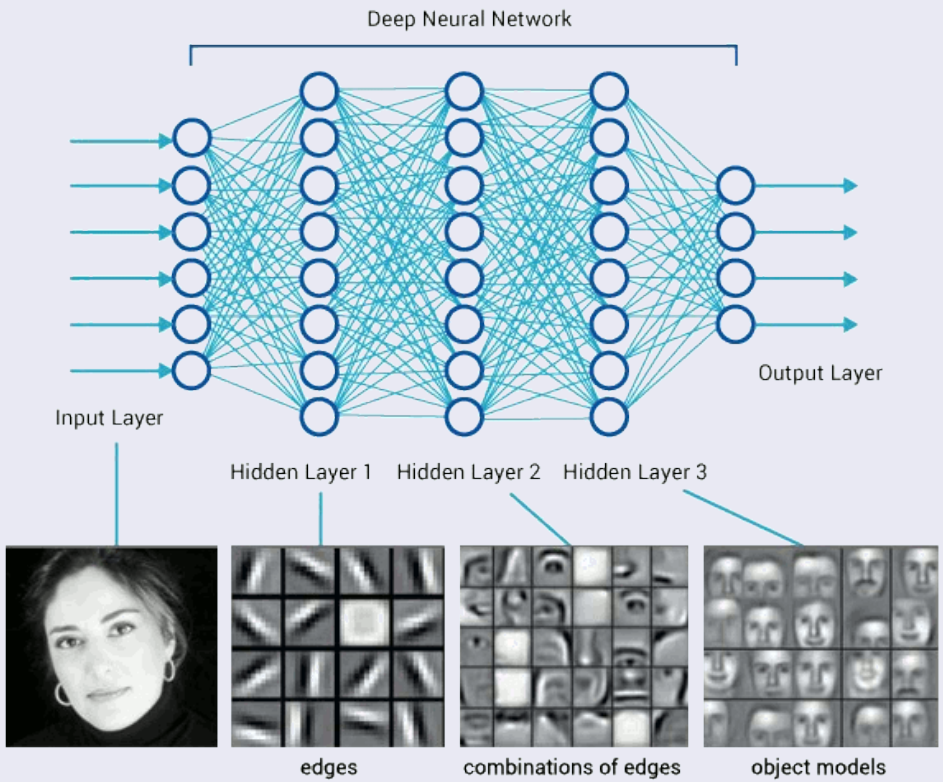
Deep Convolutional Network (DCN)



From: Asimov Institute

- Convolutions = filters (e.g. edge detector)

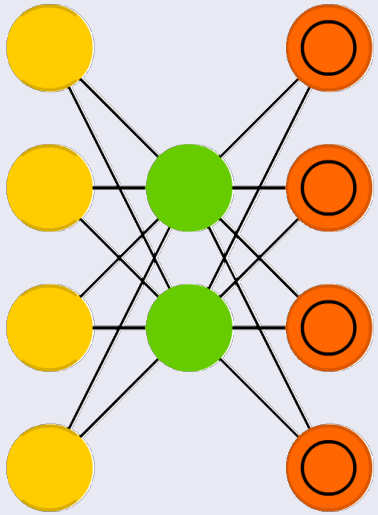
Convolutional Neural Network (CNN, Lecun 1989)



From: diary of a wannapreneur

Auto-Encoder (AE, Lecun 1987, Kramer 1991, Hinton 1994)

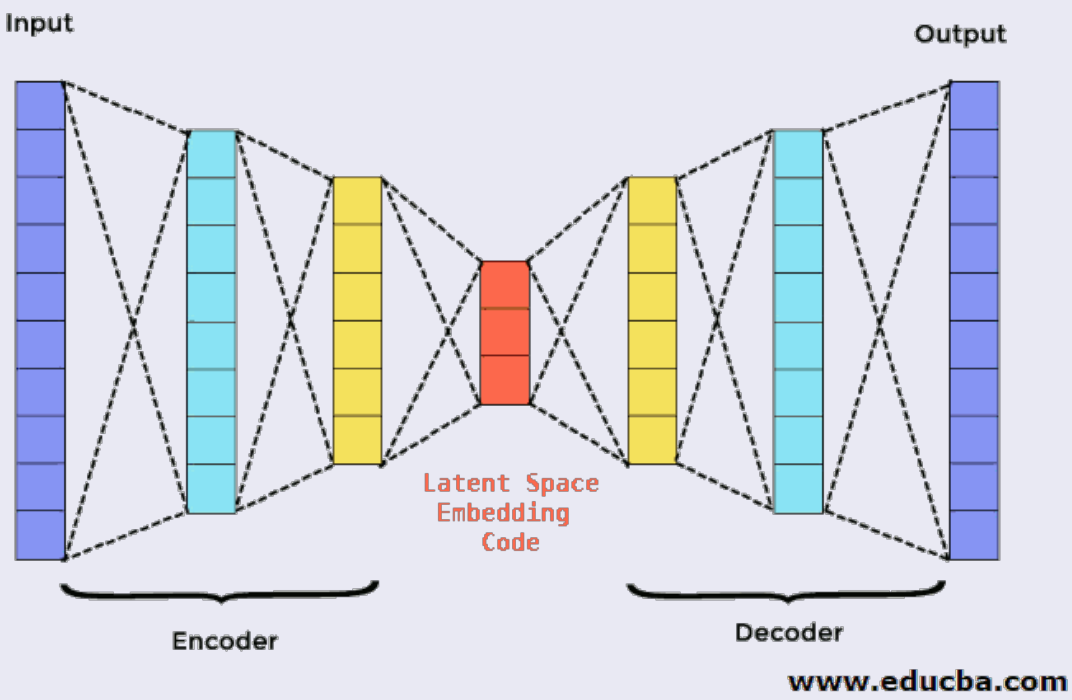
Auto Encoder (AE)



From: Asimov Institute

- Symmetrical
- Feature Engineering / Unsupervised

Auto-Encoder (AE, Lecun 1987, Kramer 1991, Hinton 1994)



From: EducBA

Section Outline

Basics

- Feed Forward NN
- Recurrent NN
- Convolutional NN
- Auto-Encoder

State-of-the-art

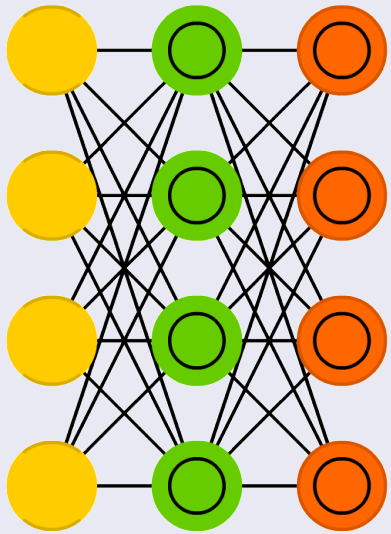
- Variational Auto-Encoder
- Generative Adversarial Network
- Attention Network

One/Few-shot training

- Siamese Networks

Variational Auto-Encoder (VAE, Kingma 2014)

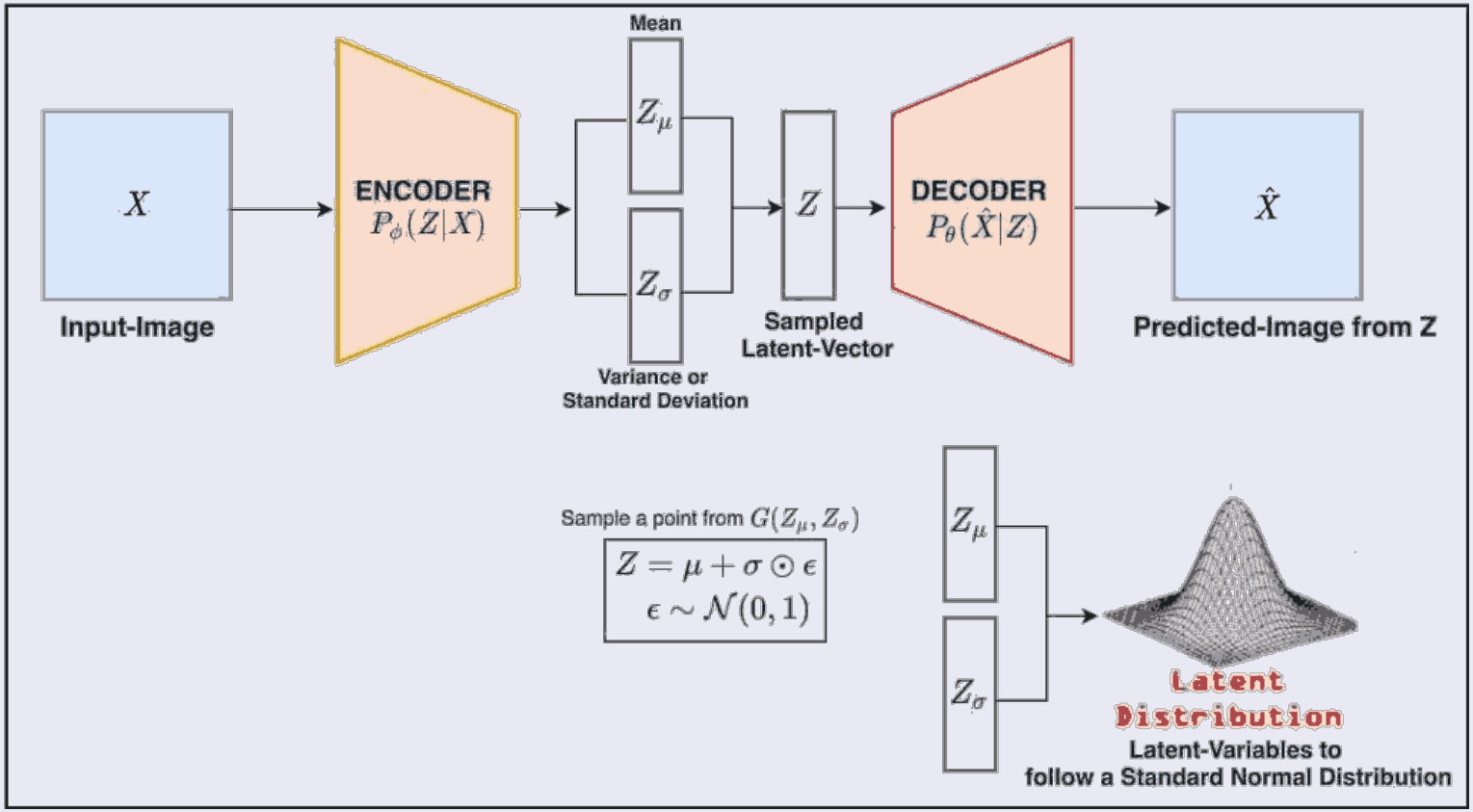
Variational AE (VAE)



From: Asimov Institute

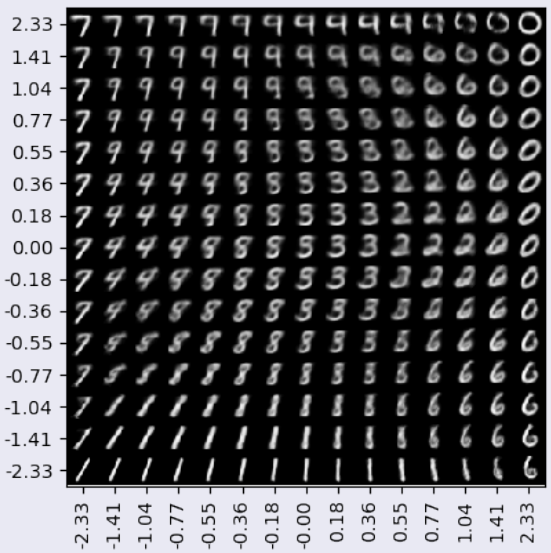
- Latent Space = Normal Distribution
- Can be used to generate data

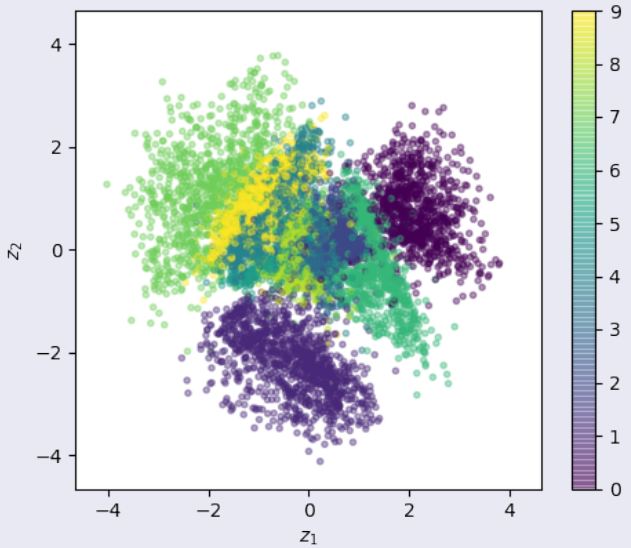
Variational Auto-Encoder (VAE, Kingma 2014)



From: Learn OpenCV

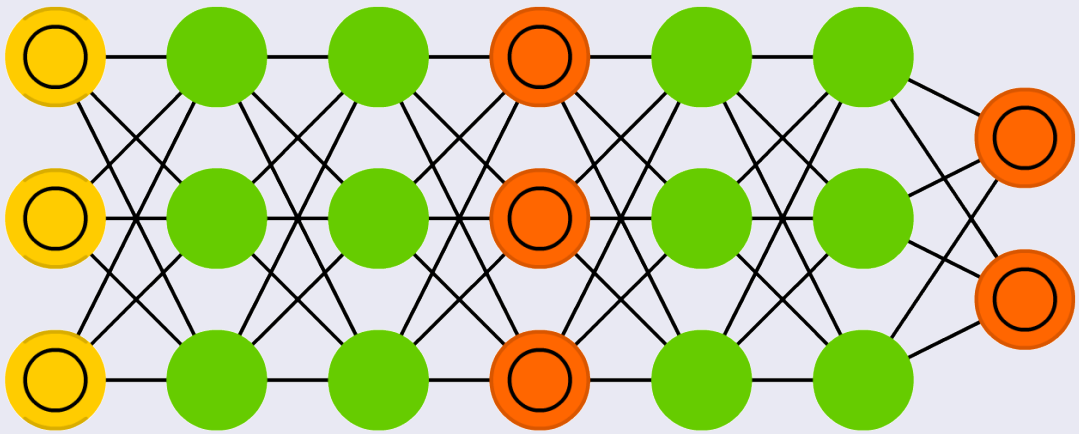
Variational Auto-Encoder (VAE, Kingma 2014)





From: tioao.io

Generative Adversarial Network (GAN)



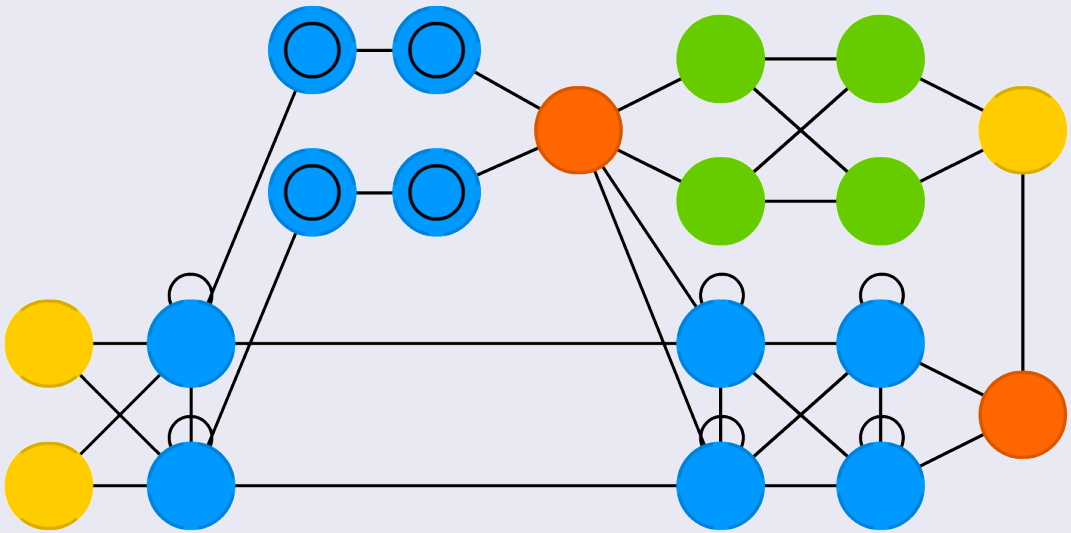
From: Asimov Institute

Generative Adversarial Network (GAN, Goodfellow 2014)

From: Towards Datascience

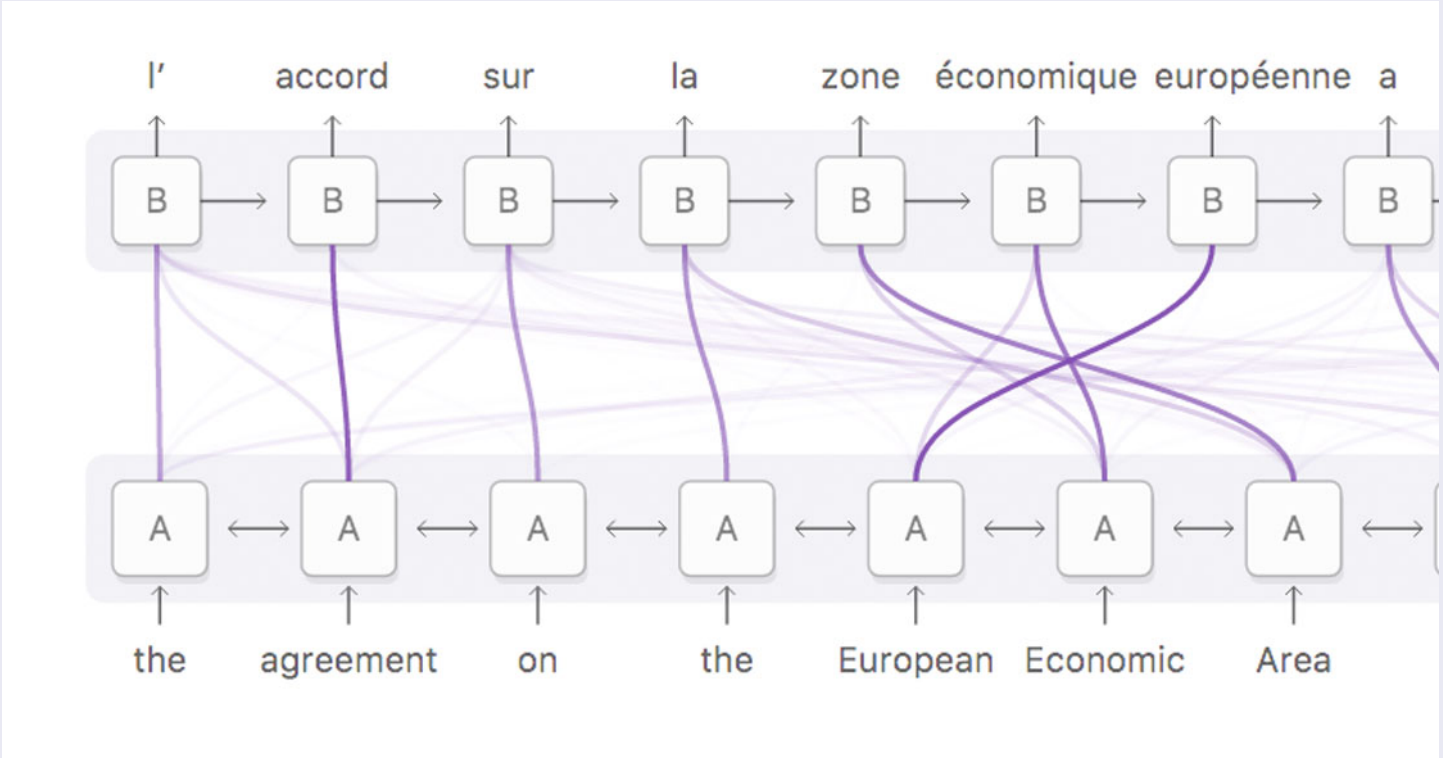
- "Old" AI Principle of Co-evolution
- Can be used to generate data

Attention Network (Vaswani 2017)



From: Asimov Institute

Attention Network (Vaswani 2017)



From: C. Olah, S. Carter (Google Brain) @Distill

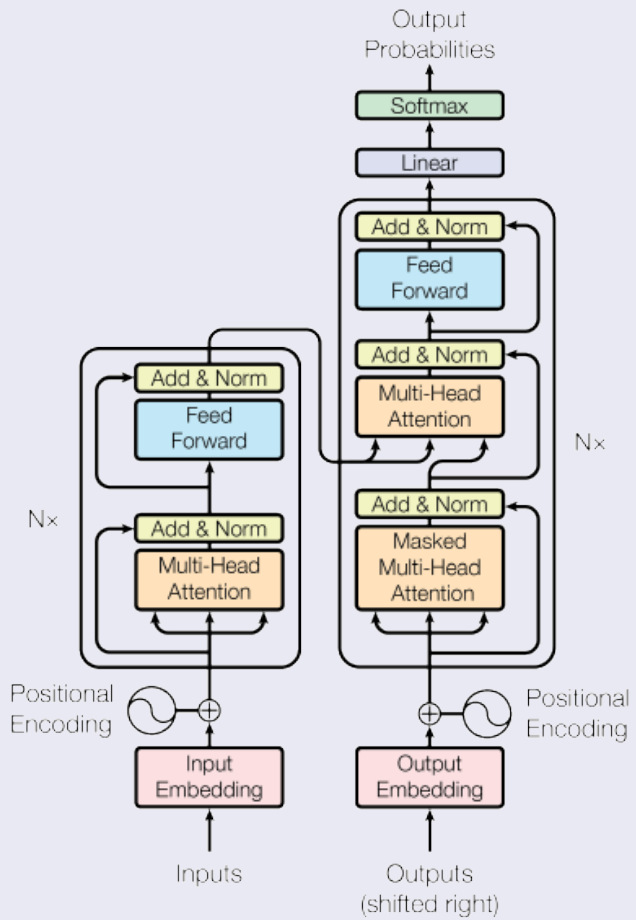
Attention Network (Vaswani 2017)

A woman is throwing a frisbee in a park.

A dog is standing on a hardwood floor.

From: "Show, attend and tell...", K. Xu *et al* 2015.

Attention Network (Vaswani 2017)



- From: "Attention is all you need", A. Vaswani *et al*, 2017.

- Transformers
  - BERT, GPT-3...
- "Replaces" RNN, CNN

Section Outline

Basics

- Feed Forward NN
- Recurrent NN
- Convolutional NN
- Auto-Encoder

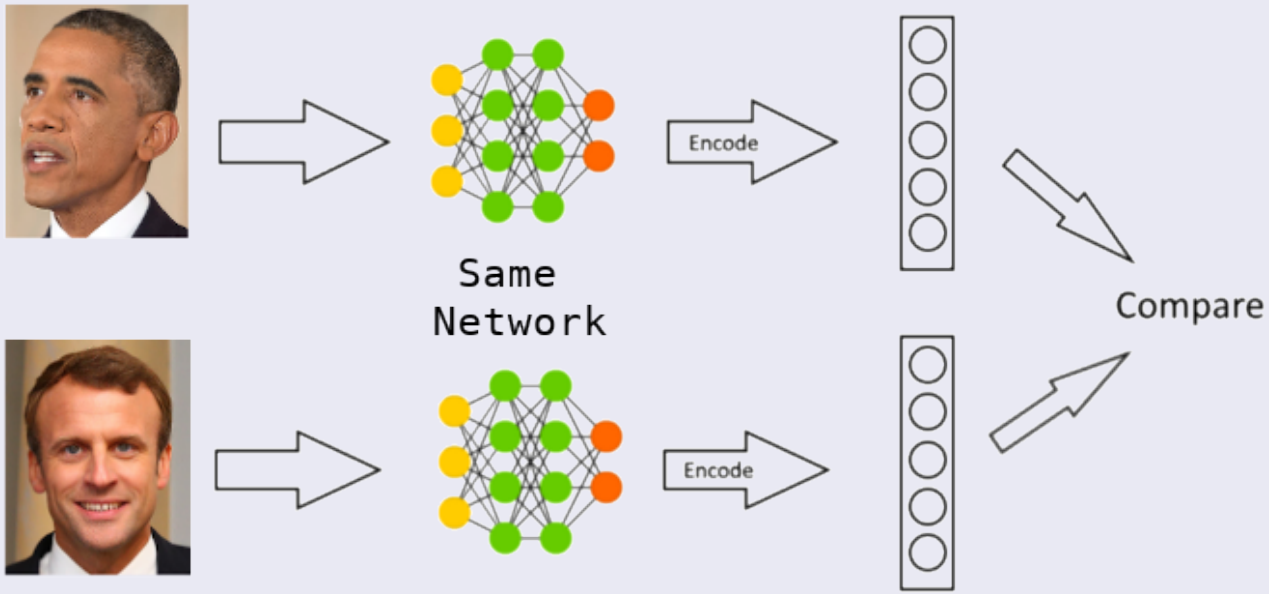
State-of-the-art

- Variational Auto-Encoder
- Generative Adversarial Network
- Attention Network

One/Few-shot training

- Siamese Networks

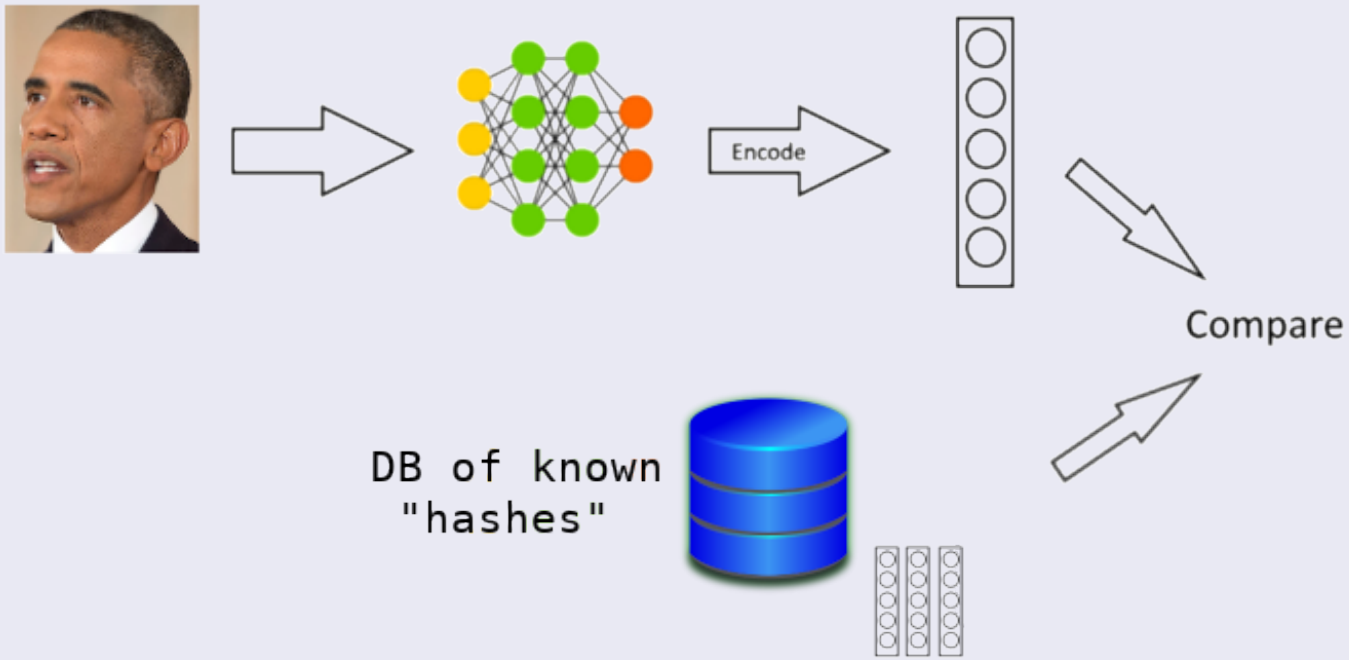
One/Few-Shot Learning (Bromley 1994, Chopra 2005)



Based on: E. Craeymeersch

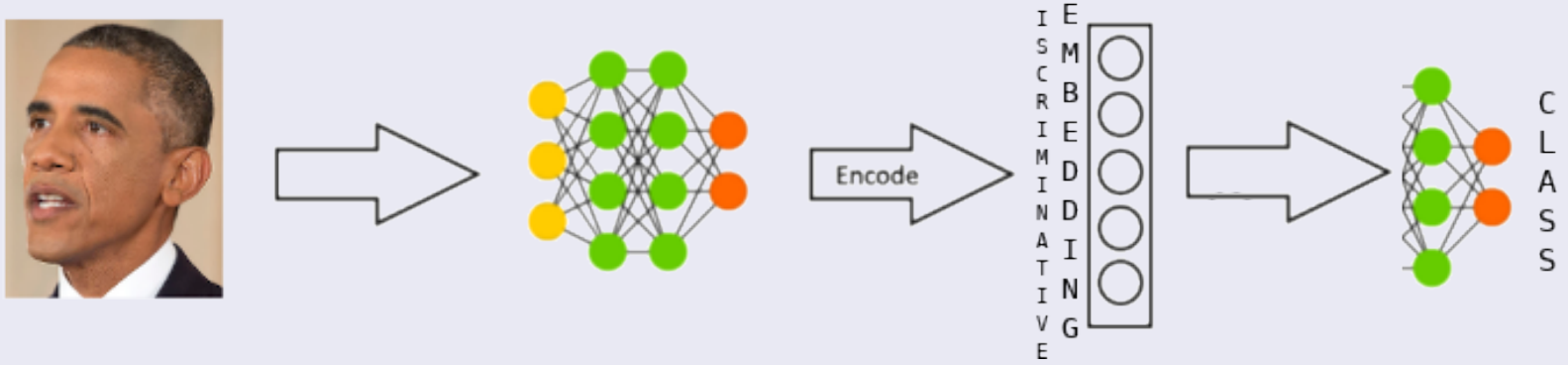
- "Siamese" Network
- When few data is available

One/Few-Shot Learning (Bromley 1994, Chopra 2005)



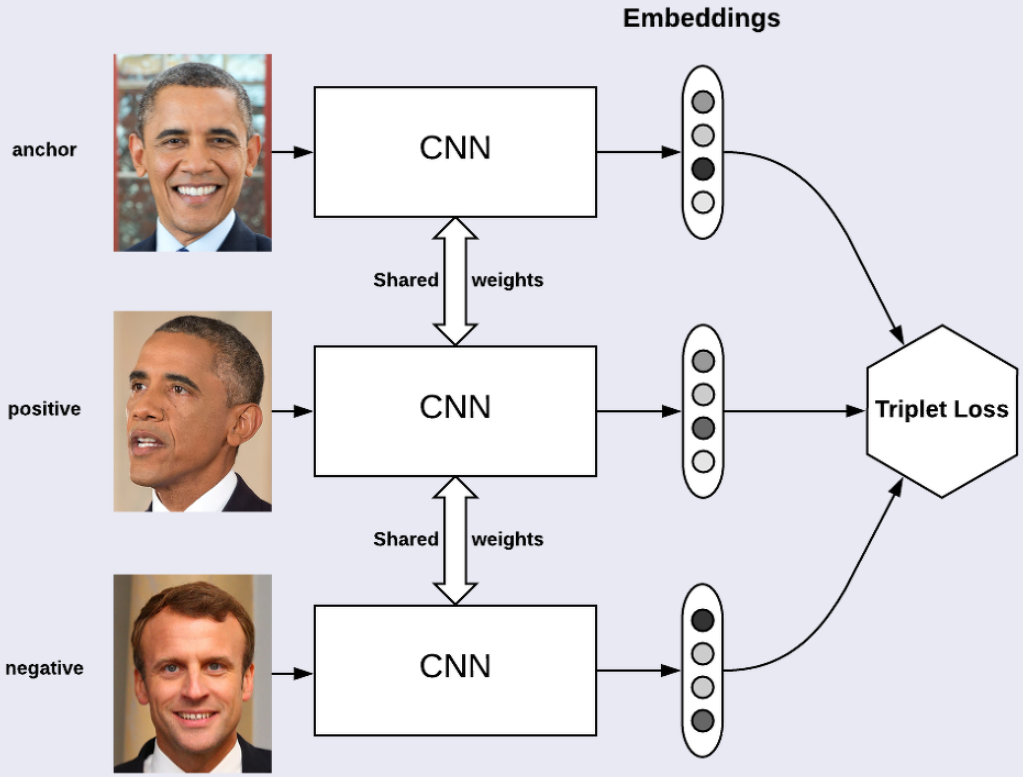
- Example: Mobile Phone facial recognition
- Same principle as Hashed passwords

One/Few-Shot Learning (Bromley 1994, Chopra 2005)



- For classification
- Concatenate a FCN at the end
- Siamese vs. FCN: discriminative latent space / few data

One/Few-Shot Learning (Bromley 1994, Chopra 2005)



From: Deep Play

- Finds most discriminative latent space (distance)
- Requires less input data (pairs, triplets)

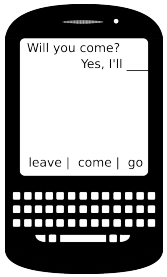
How to train these models?

Deep Neural Networks

- Billions of parameters to tune
- $\Rightarrow$ Billions of data!

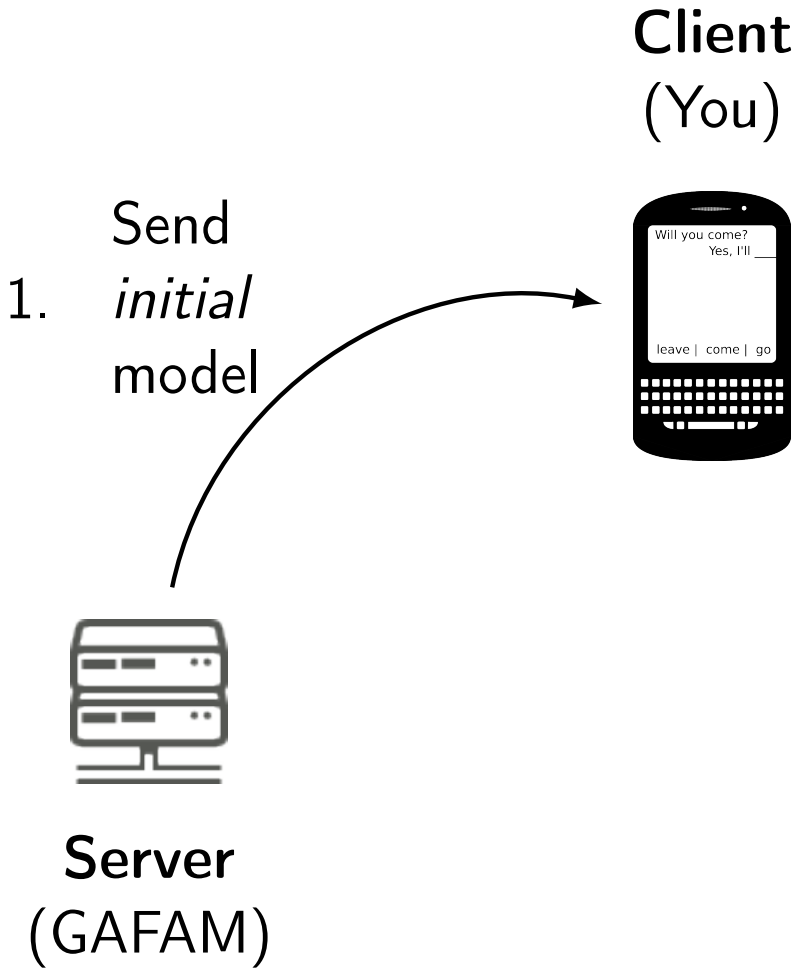
"Traditional" Machine Learning

Client
(You)



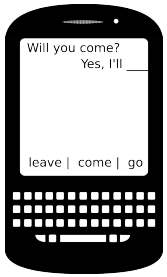
Server
(GAFAM)

"Traditional" Machine Learning



"Traditional" Machine Learning

Client
(You)

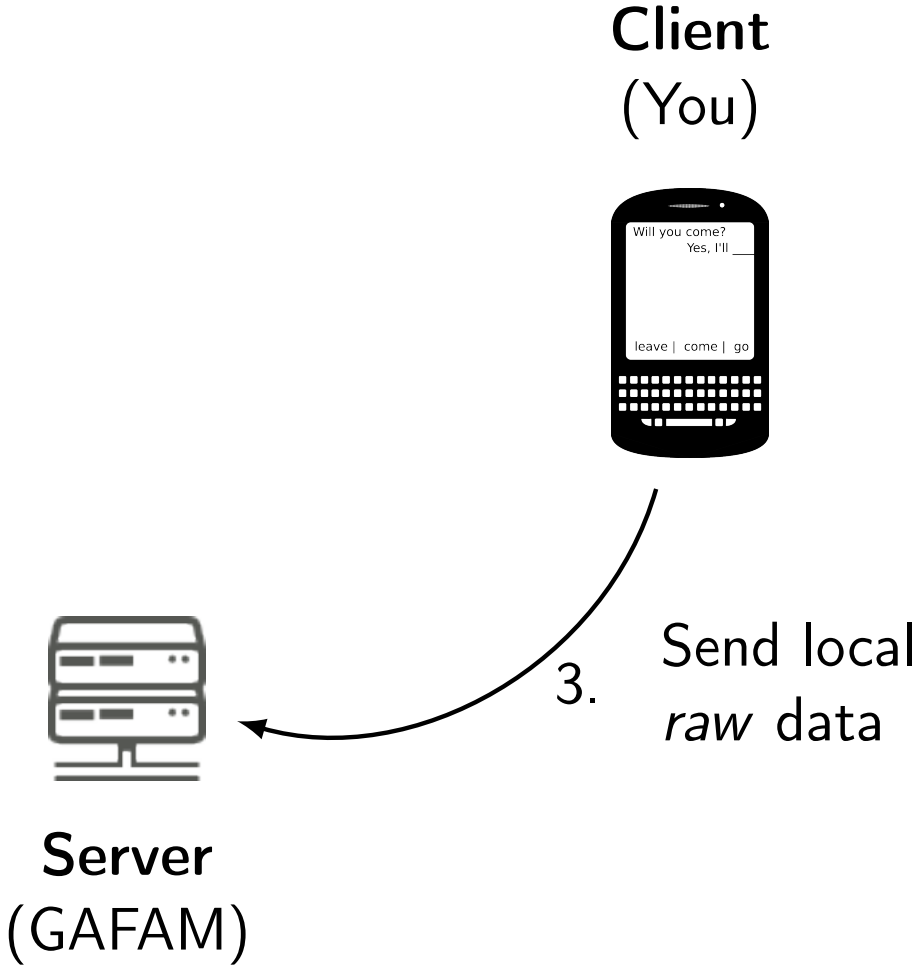


2.

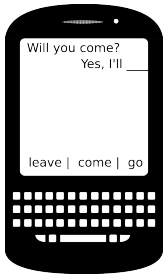
- *Use* model
- Collect data

Server
(GAFAM)

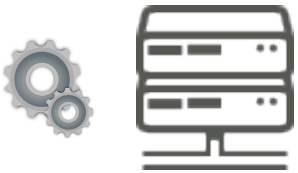
"Traditional" Machine Learning



Client
(You)

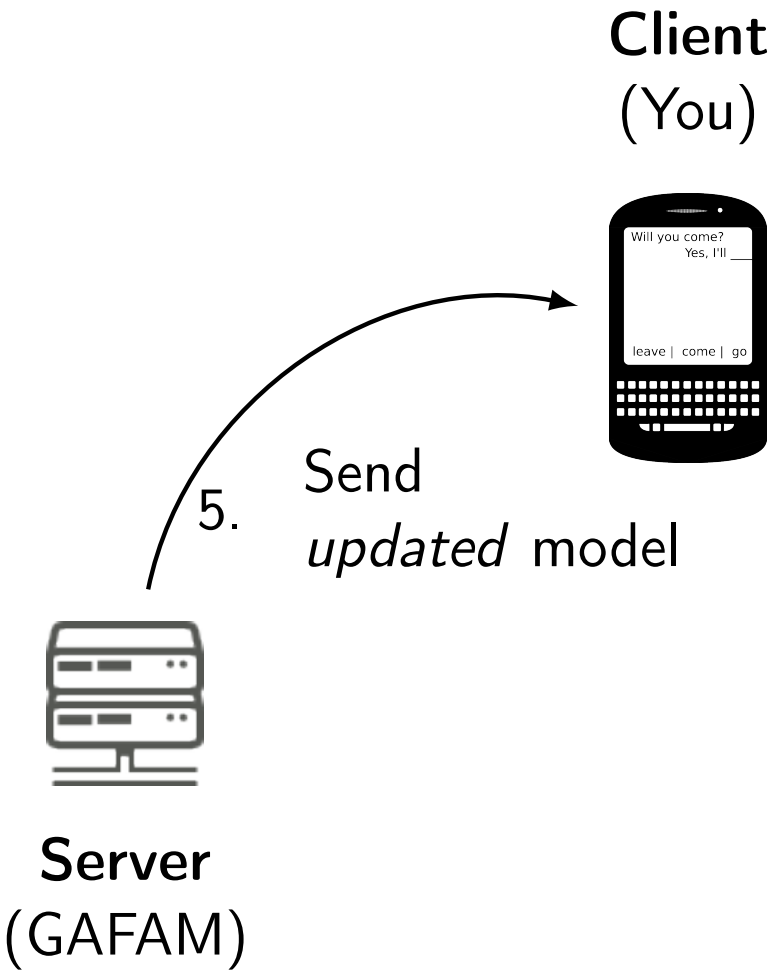


4. (re)Train model

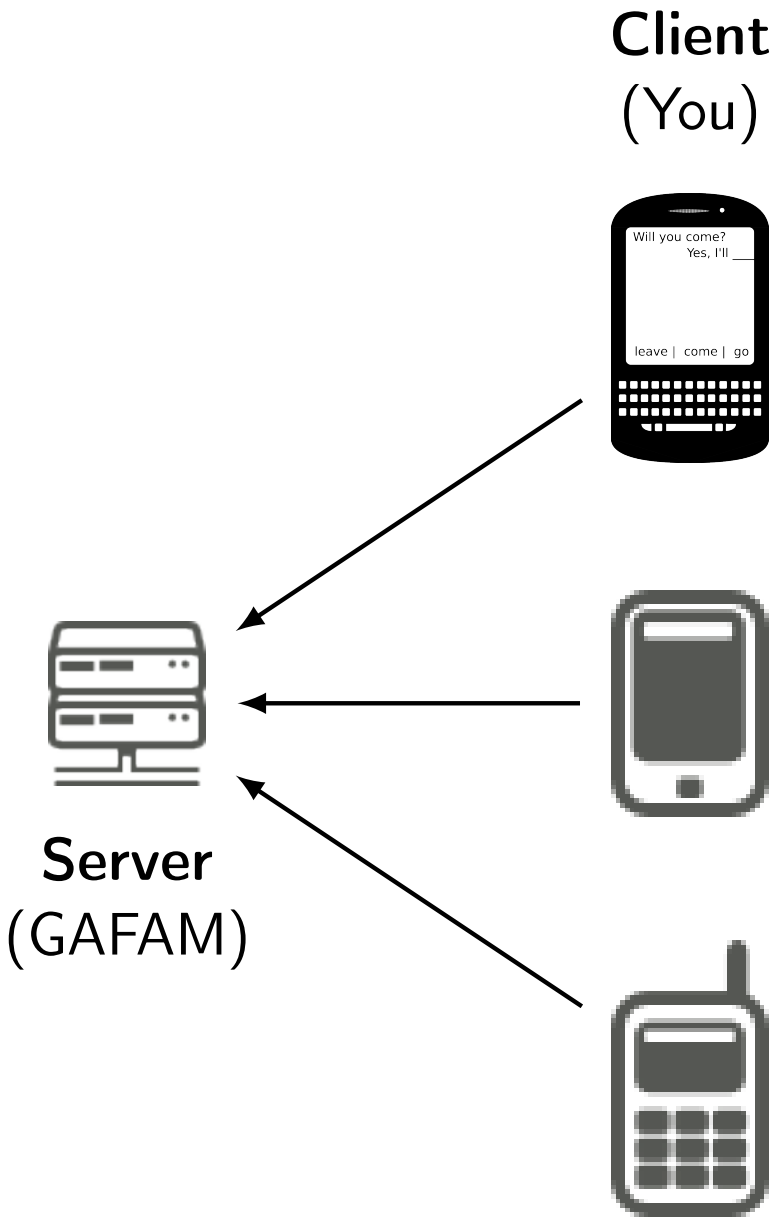


Server
(GAFAM)

"Traditional" Machine Learning



"Traditional" Machine Learning



Problem!

- Single device
  - sensitive data
- Multiple devices
  - crossed data

"Traditional" Machine Learning – Limits

Privacy Problem...

- Keyboard = everything
  - Passwords
  - Sensitive messages
  - Visited websites
  - ...

Efficiency Problem...

- Raw data = ⚖
  - Images
  - Videos
  - Sound
  - ...

"Traditional" Machine Learning – Limits

Privacy Problem...

- Keyboard = everything
  - Passwords
  - Sensitive messages
  - Visited websites
  - ...

...in general

- "Data is the new Oil"
- Health Care (ECG, EEG), Industry 4.0 (Machine logs)...
  - $\Rightarrow$ Diseases, IP...

Efficiency Problem...

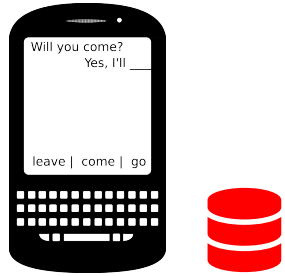
- Raw data = ⚖
  - Images
  - Videos
  - Sound
  - ...

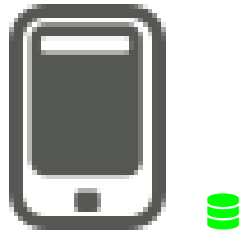
...in general

- Network Traffic
- Server Load

Outline

Federated Learning – Principle

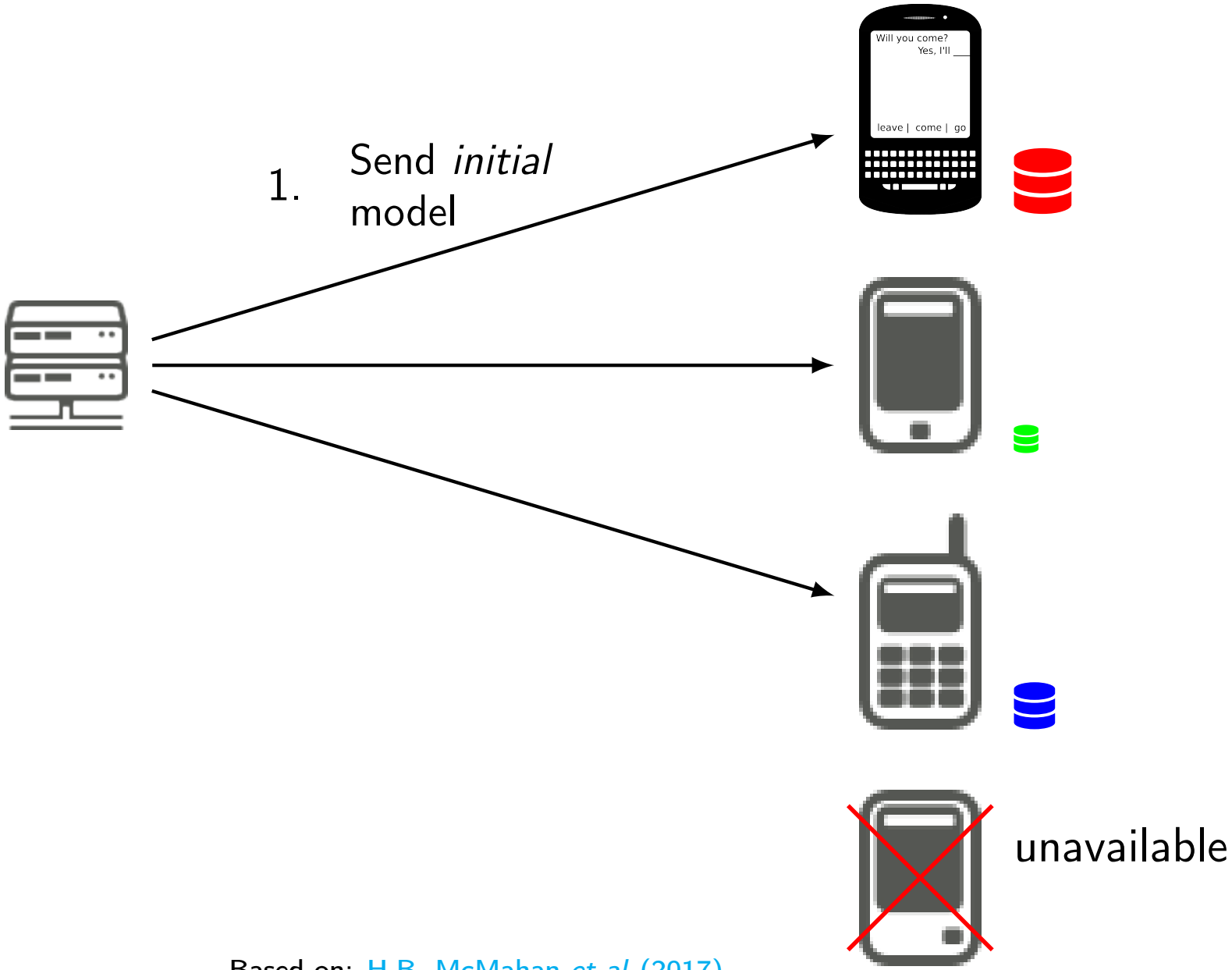




unavailable

Based on: H.B. McMahan *et al* (2017)

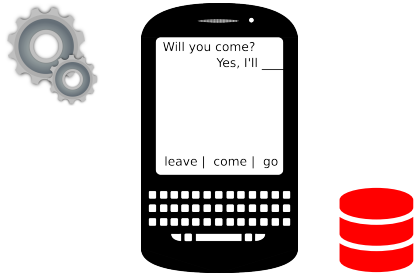
Federated Learning – Principle

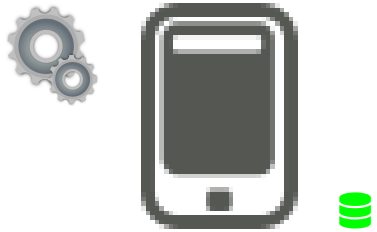


Based on: H.B. McMahan *et al* (2017)

Federated Learning – Principle

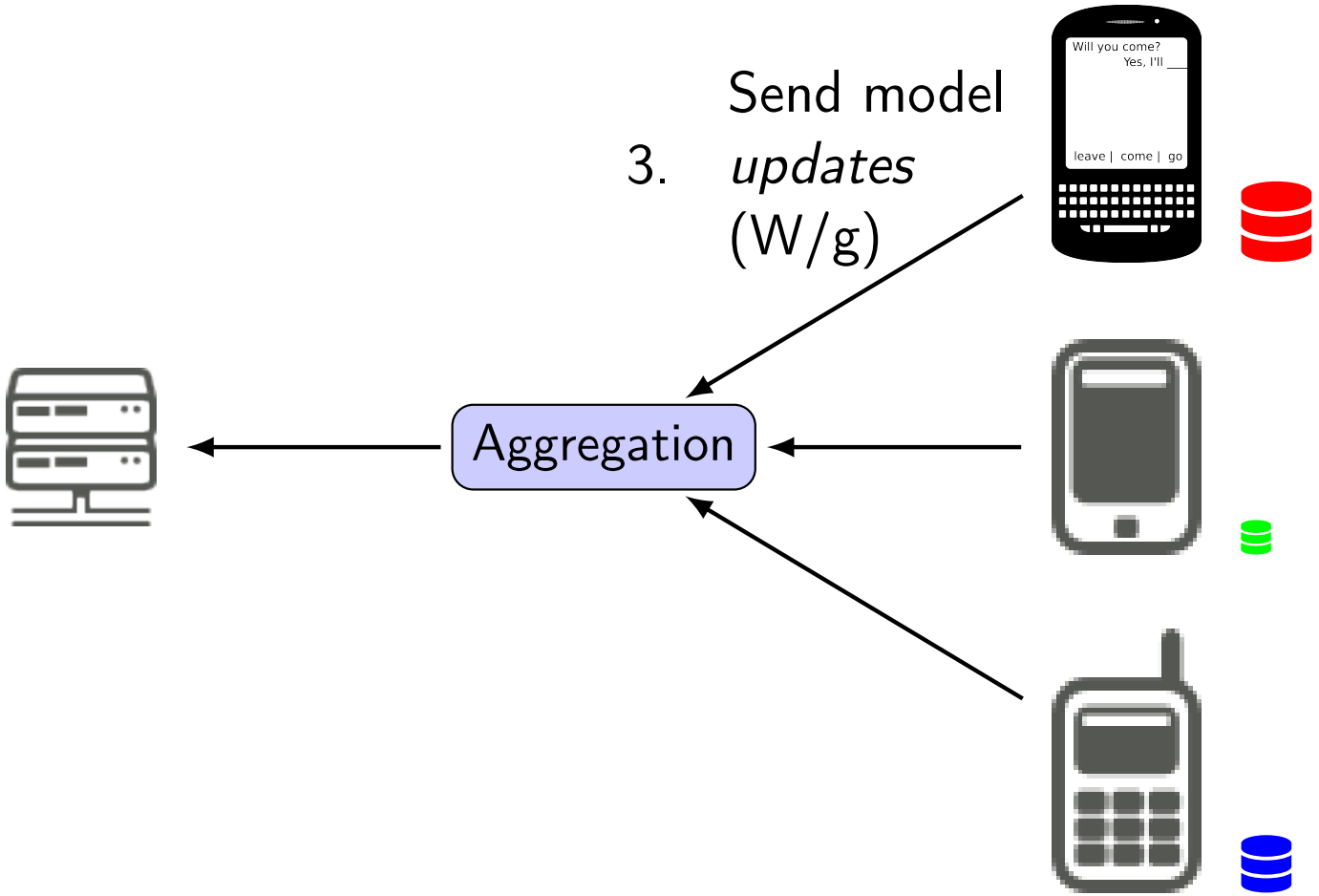
2. Train model on *local* data





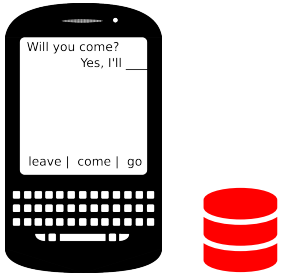
Based on: H.B. McMahan *et al* (2017)

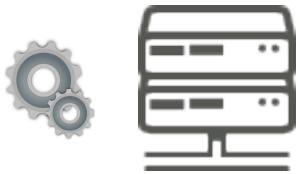
Federated Learning – Principle

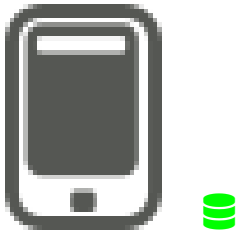


Based on: H.B. McMahan *et al* (2017)

Federated Learning – Principle



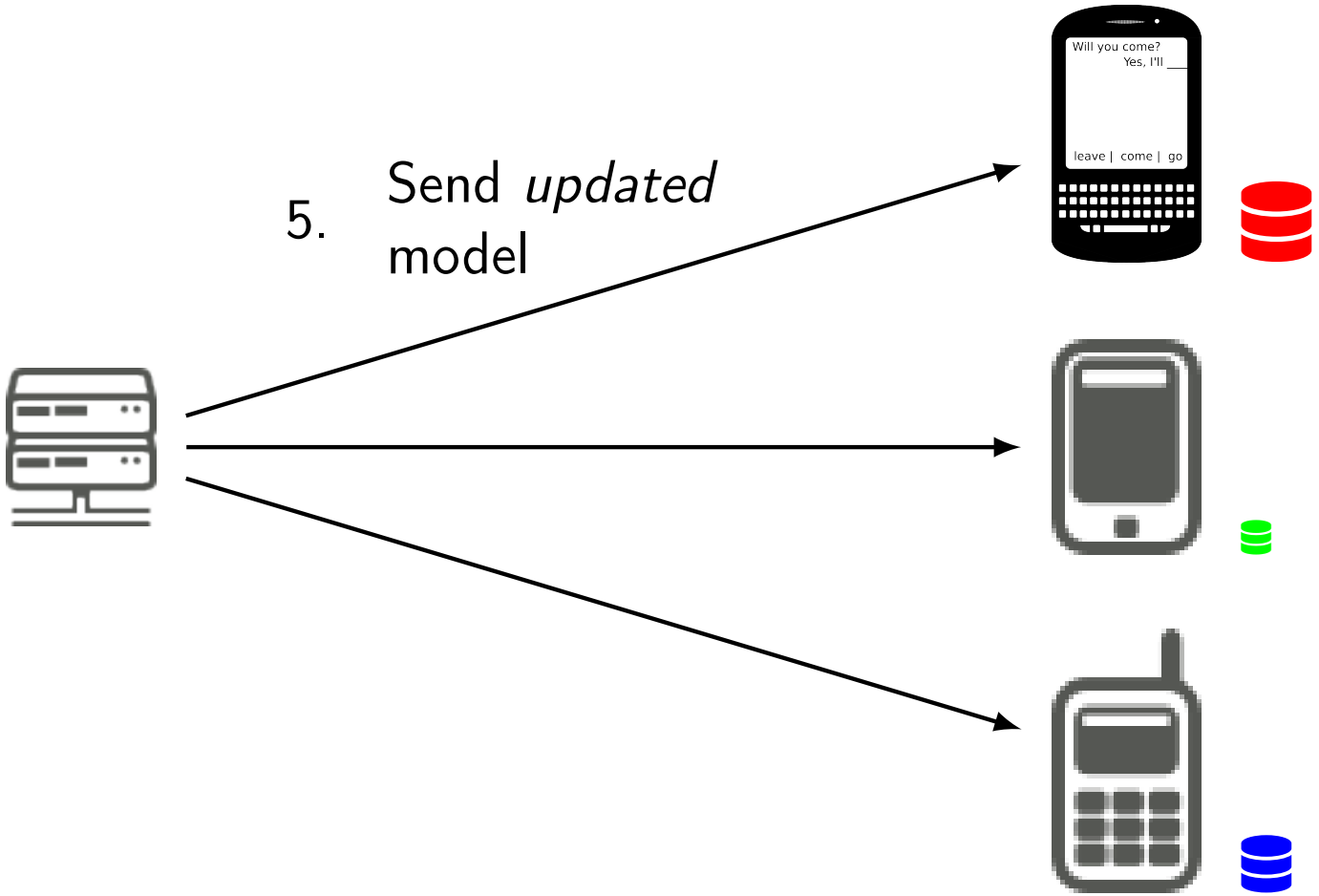




4. Update *global* model

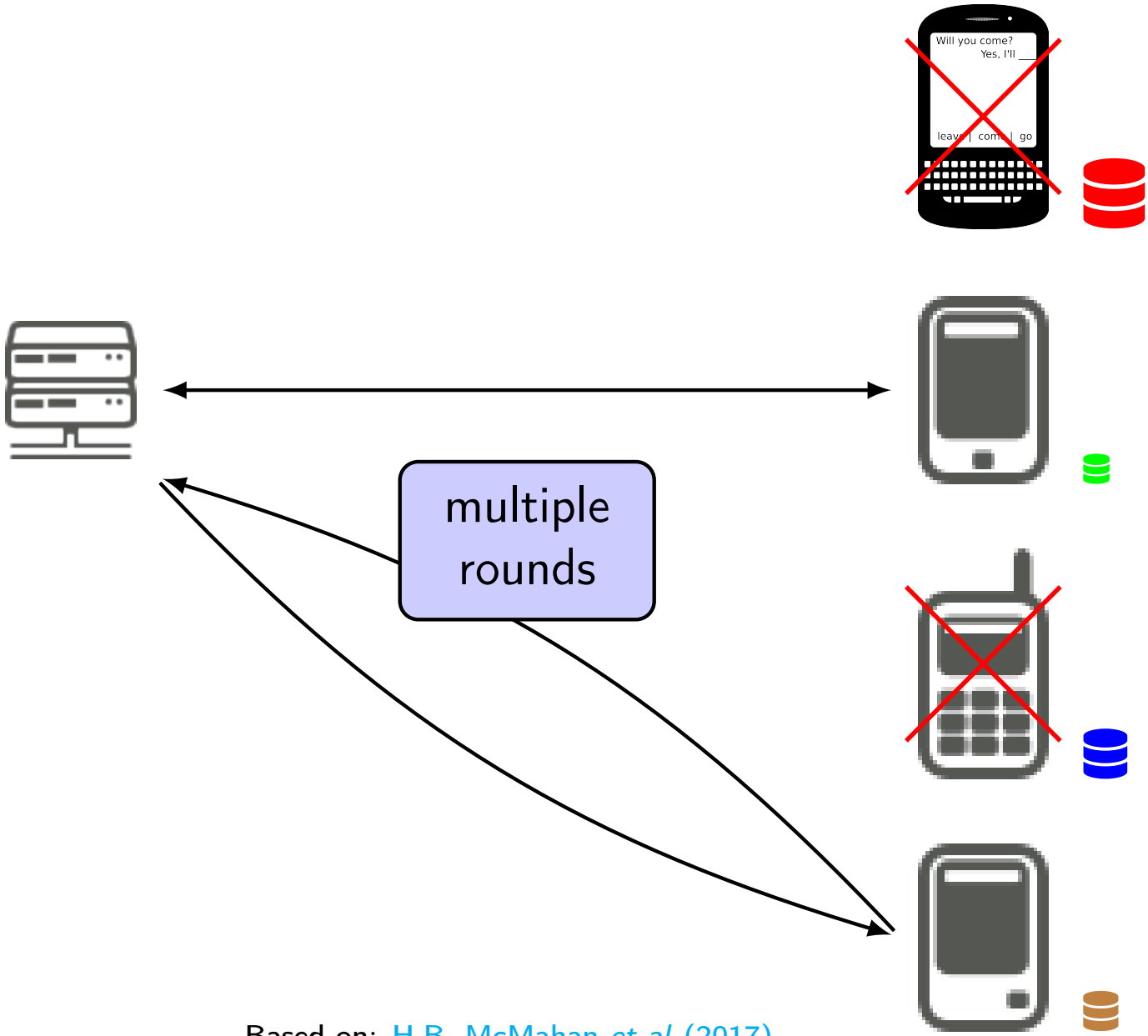
Based on: H.B. McMahan *et al* (2017)

Federated Learning – Principle



Based on: H.B. McMahan *et al* (2017)

Federated Learning – Principle



Based on: H.B. McMahan *et al* (2017)

Federated Learning – Pros & Cons

Pros

- **Privacy**
  - model updates = unreadable (Weights/Gradients)*
- **Efficiency**
  - **CPU**: distributed computing**
  - **Net**: `size(raw data)` $\ggg$ `size(model updates)`***

Cons

Practice works!****

Theory still research to do on *many* aspects!

Outline

Privacy Problem in Standard FL

Model Inversion (M. Fredrikson *et al*, 2015)

Privacy Problem in Standard FL

Model Inversion (M. Fredrikson *et al*, 2015)

Privacy Problem in Standard FL

Model Inversion (M. Fredrikson *et al*, 2015)

Model Inversion (B. Hitaj *et al*, 2017)

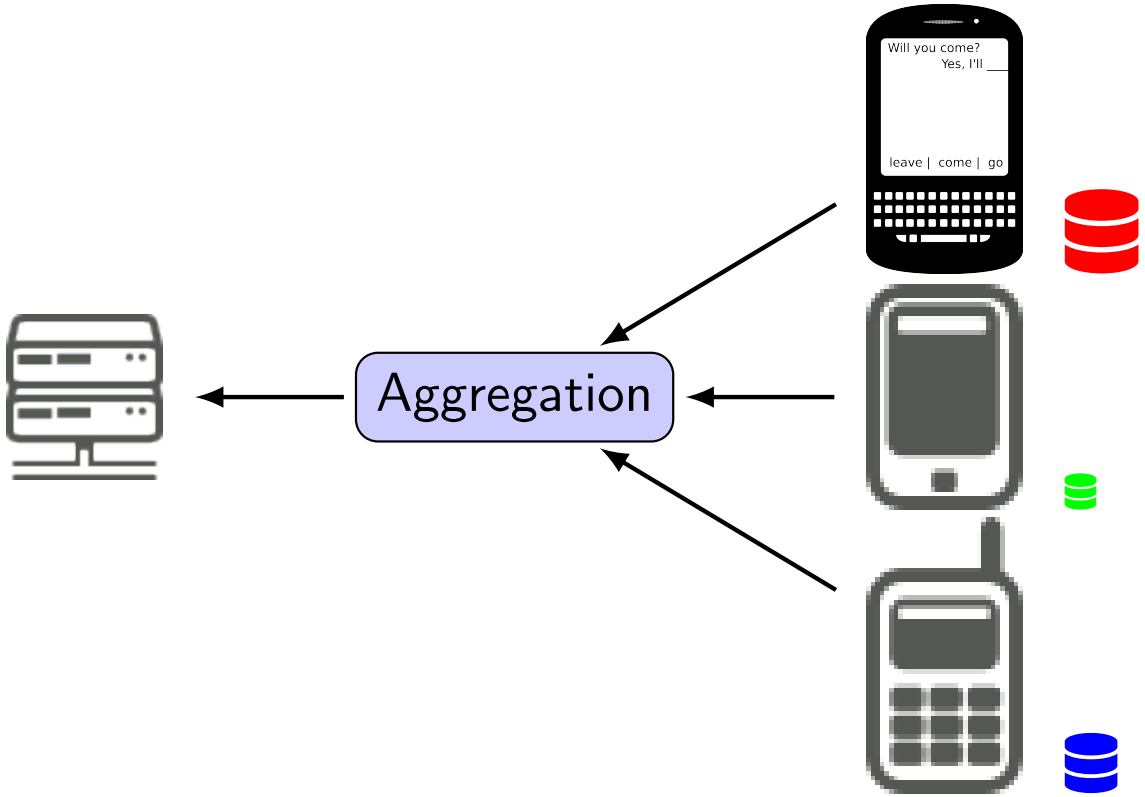
Original

$\theta_u = 1$
$\theta_d = 1$

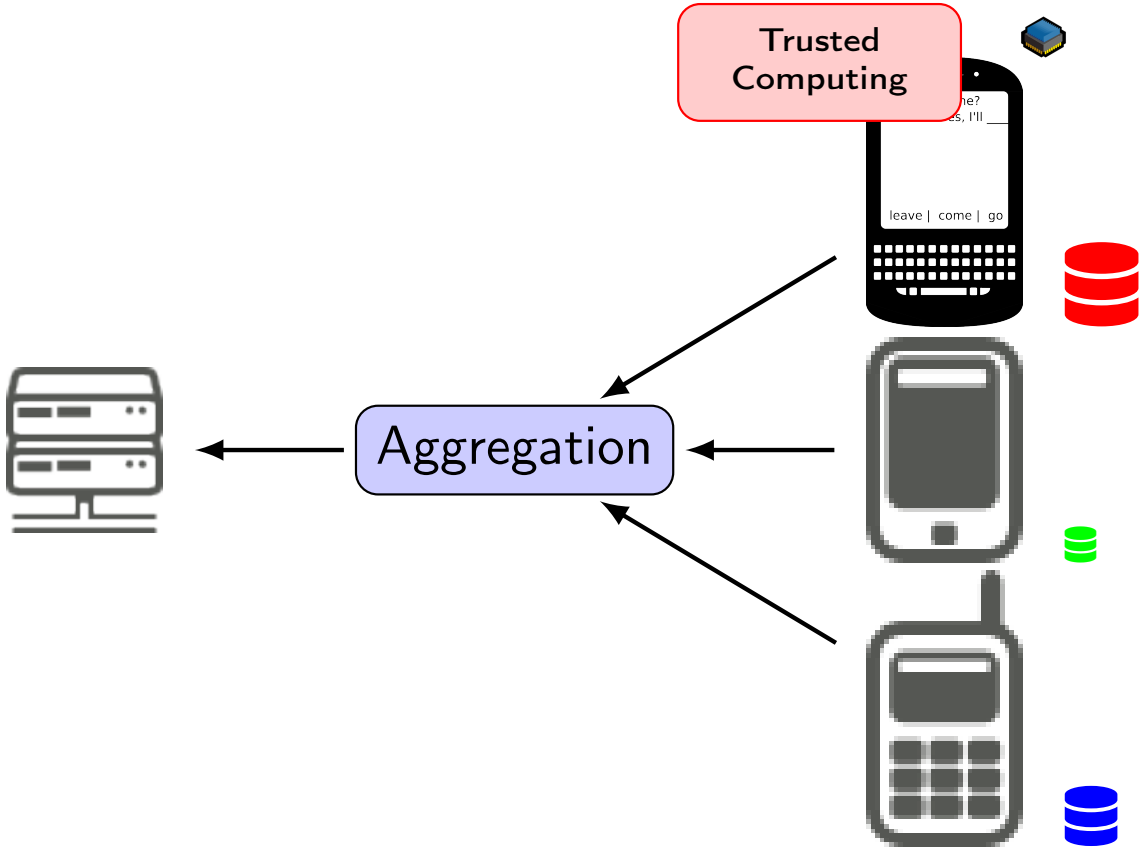
$\theta_u = 0.1$
$\theta_d = 1$

$\theta_u = 0.1$
$\theta_d = 0.1$

Protecting Privacy in FL (Based on: C. Wierzynski)



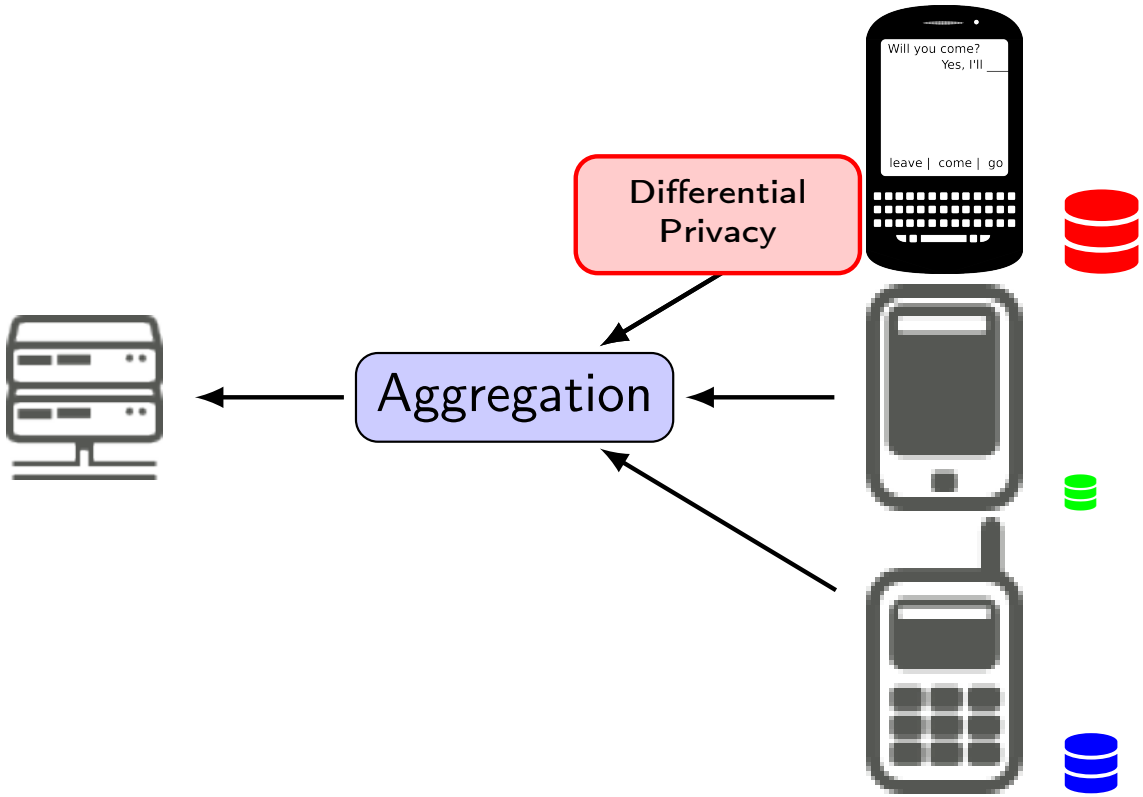
Protecting Privacy in FL (Based on: C. Wierzynski)



Trusted Execution Environment (TEE)

- Prevents external processes from reading RAM
  - Raw Data, Model, Gradients...
- Hardware protection (Intel, AMD, ARM, RISC-V...)

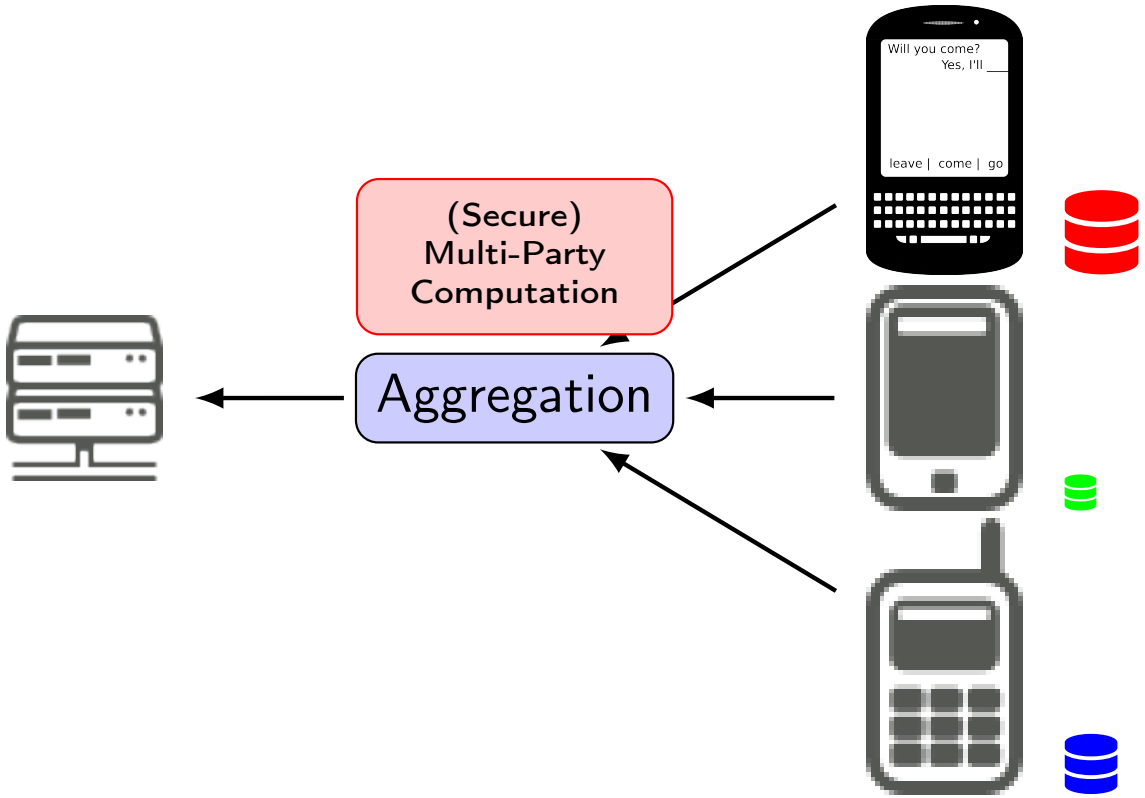
Protecting Privacy in FL (Based on: C. Wierzynski)



Differential Privacy (DP), (C. Dwork *et al*, 2014)

- Add noise to dataset so that stats remain same ⇒ ML possible
  - Limited Bugdet
- Limits "Model Inversion" attacks

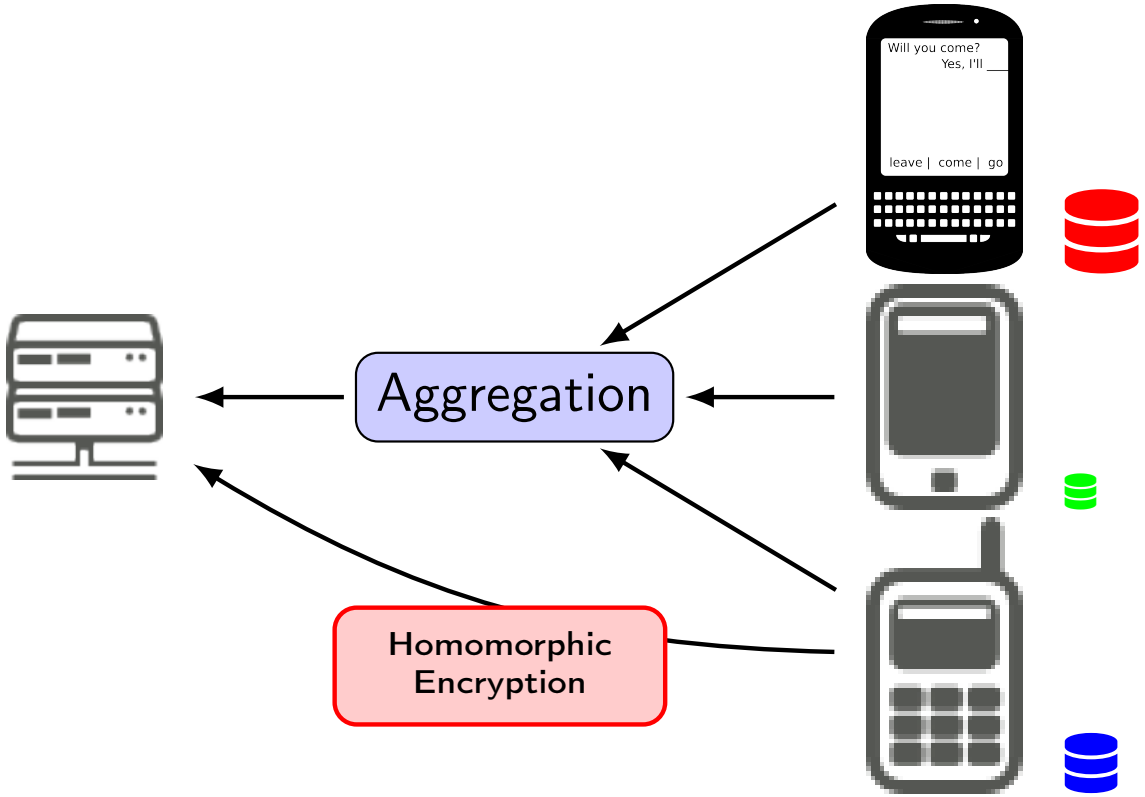
Protecting Privacy in FL (Based on: C. Wierzynski)



(Secure) Multi-Party Computation ([S]MPC)

- Jointly compute a function while keeping inputs private
  - $(\mathcal{A} + x) + (\mathcal{B} + y) + (\mathcal{C} + z) = (\mathcal{S} - s), s = x + y + z$
- Protects from network eavesdroppers (MitM)

Protecting Privacy in FL (Based on: C. Wierzynski)



Homomorphic Encryption (FEH) (C. Gentry, 2009)

- Compute directly on cyphered data
- Similar technology as SMPC
- 🏆, but order of magnitude less efficient

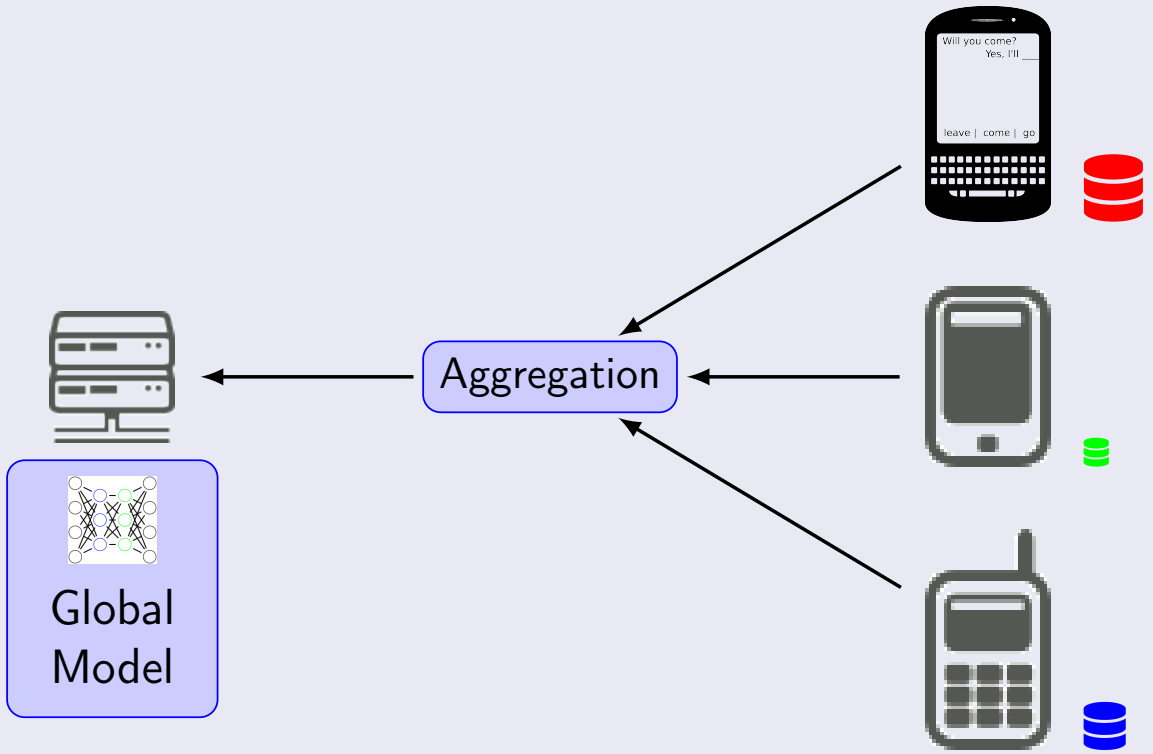
Outline

Federated Learning – Research areas

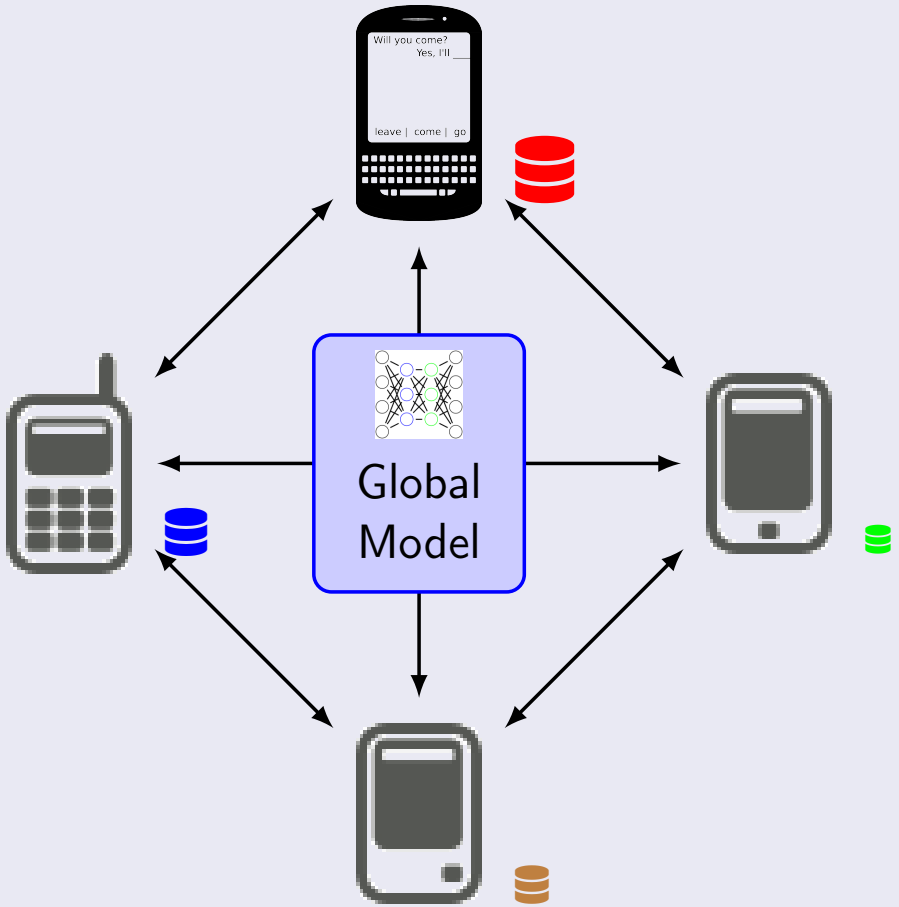
Sources

- Kairouz *et al* (2019) (105p)
- Beutel *et al* (2020) (platforms)
- Khan *et al* (2021) (IoT)

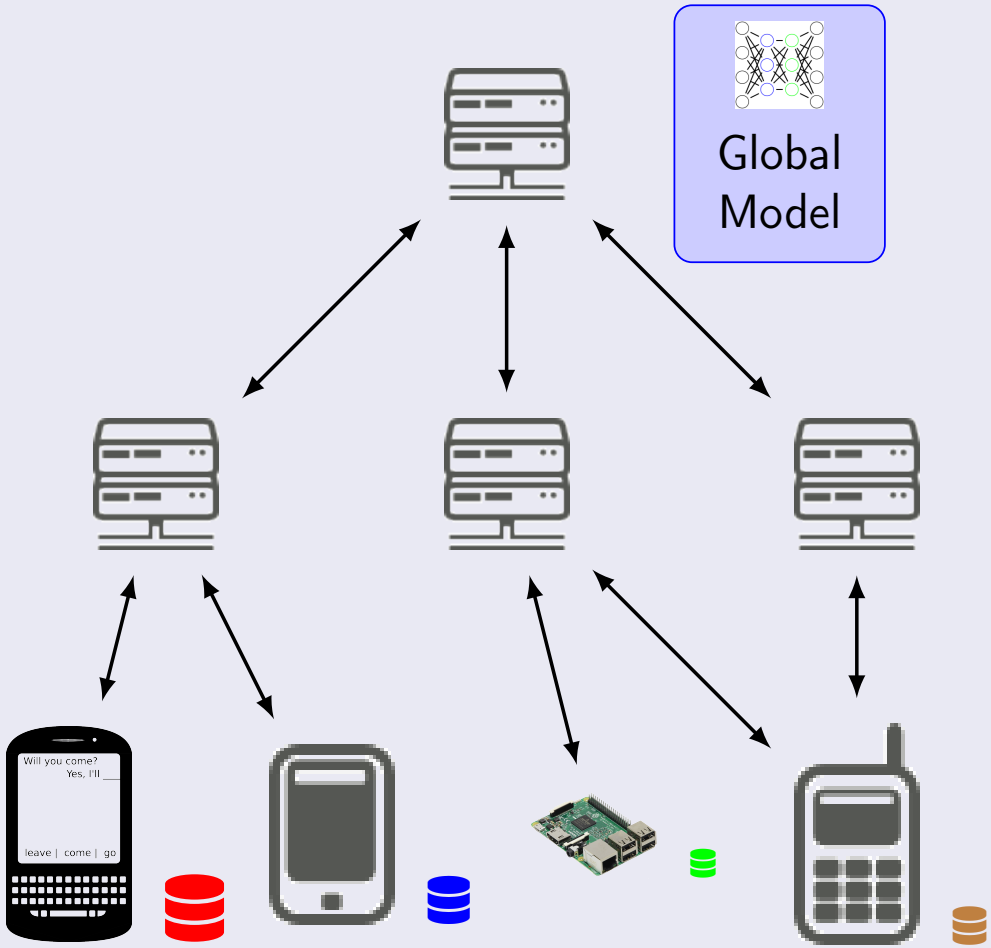
Centralized



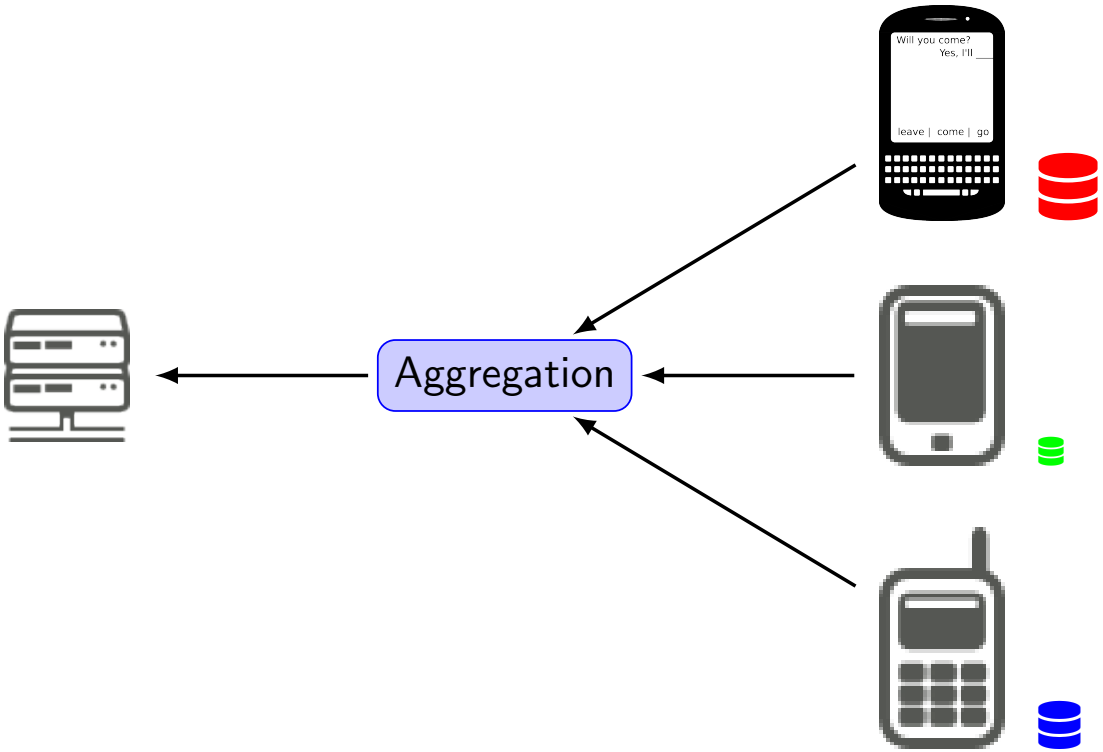
Decentralized



Hybrid

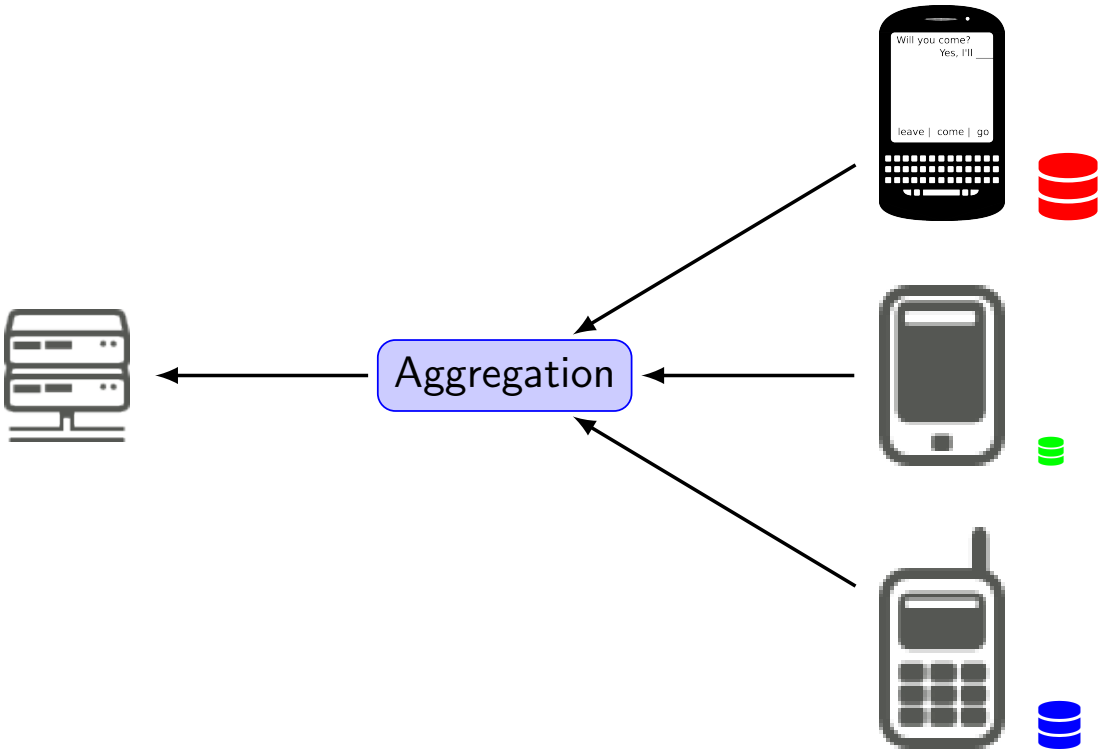


Federated Learning – Research areas

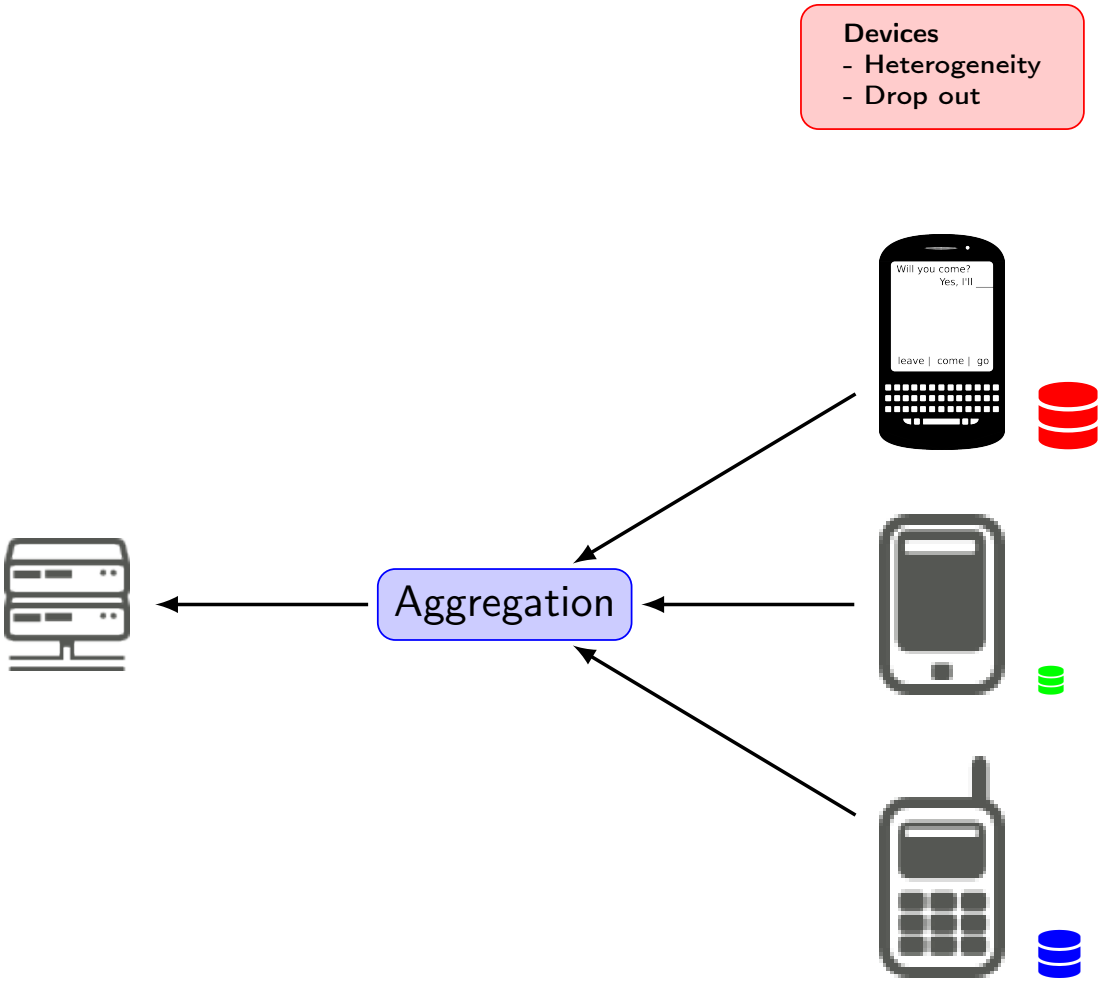


Federated Learning – Research areas

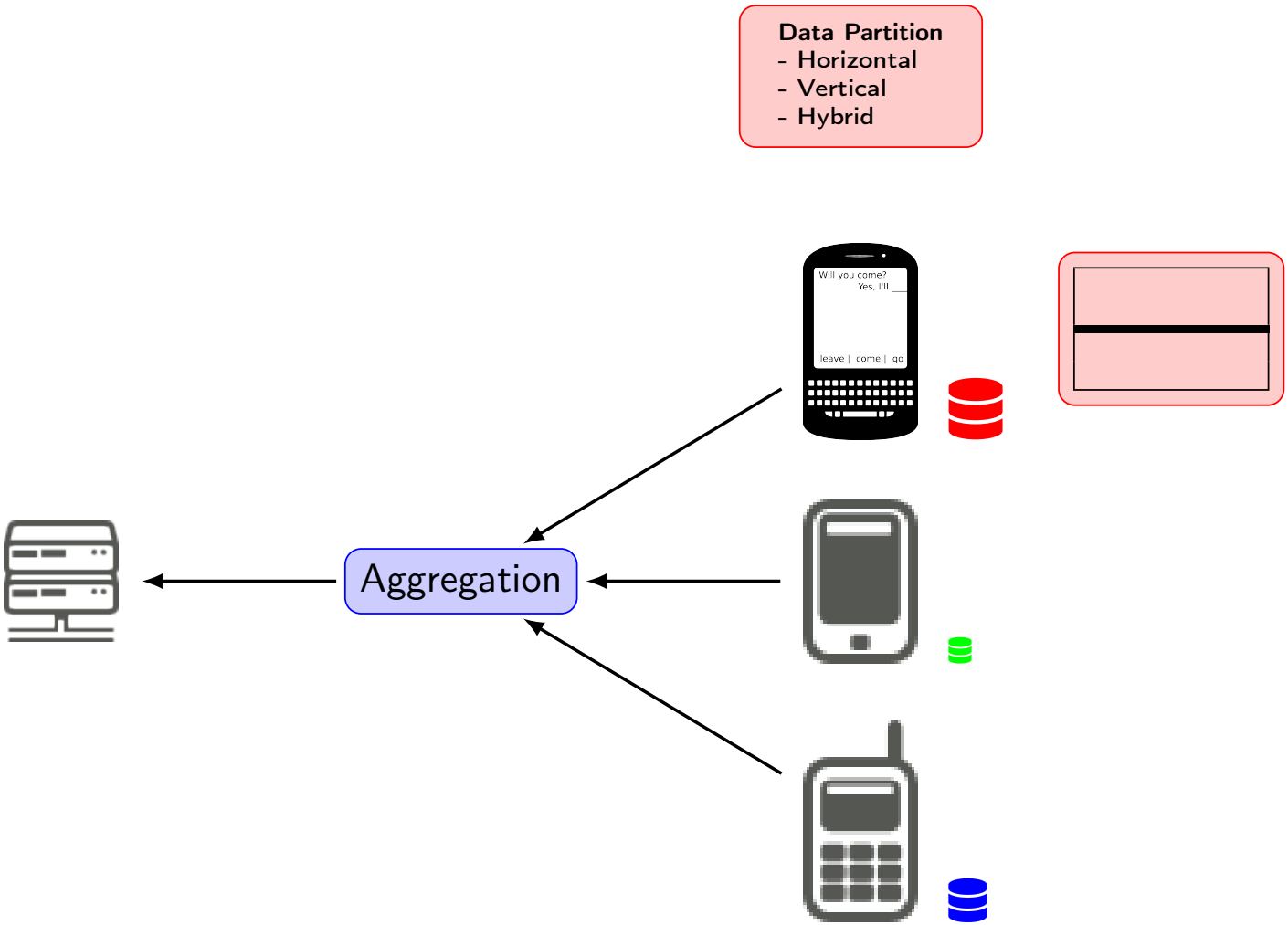
Players
- Cooperative
- Competitive
- Incentive to participate



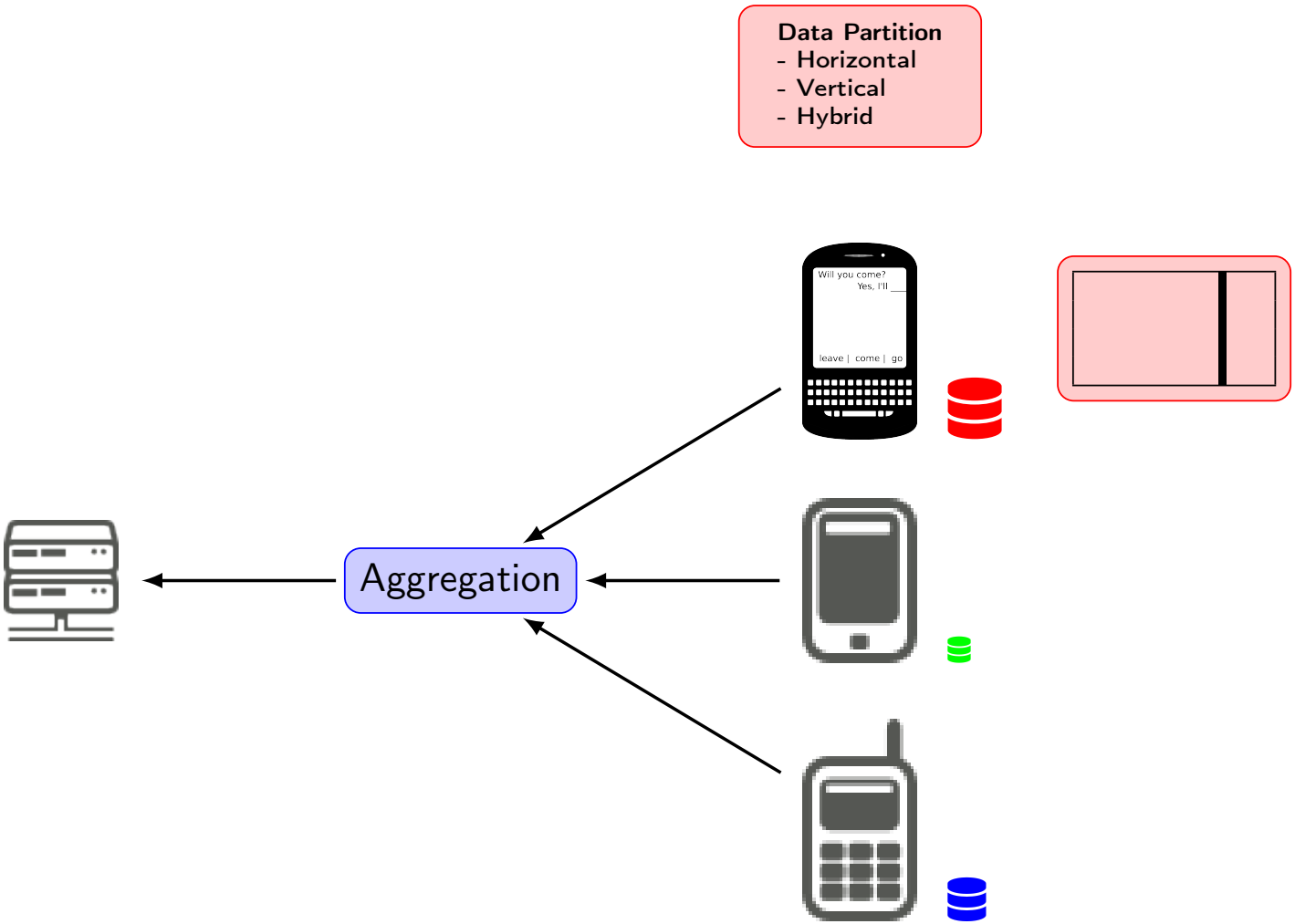
Federated Learning – Research areas



Federated Learning – Research areas

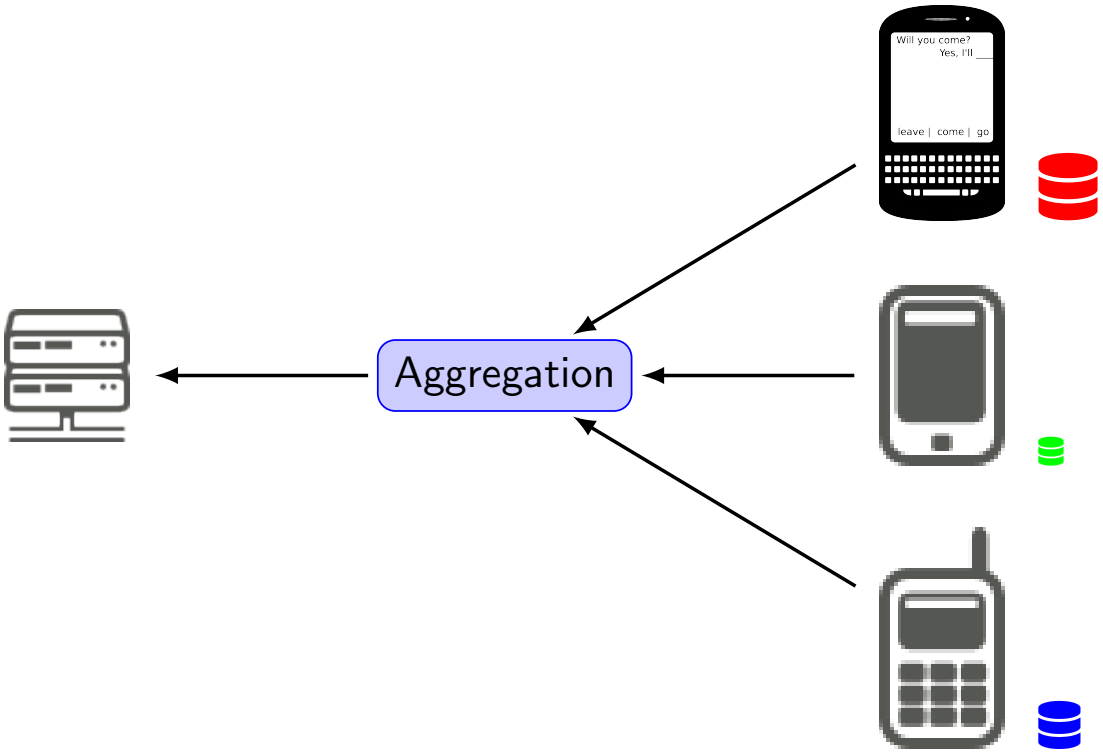


Federated Learning – Research areas

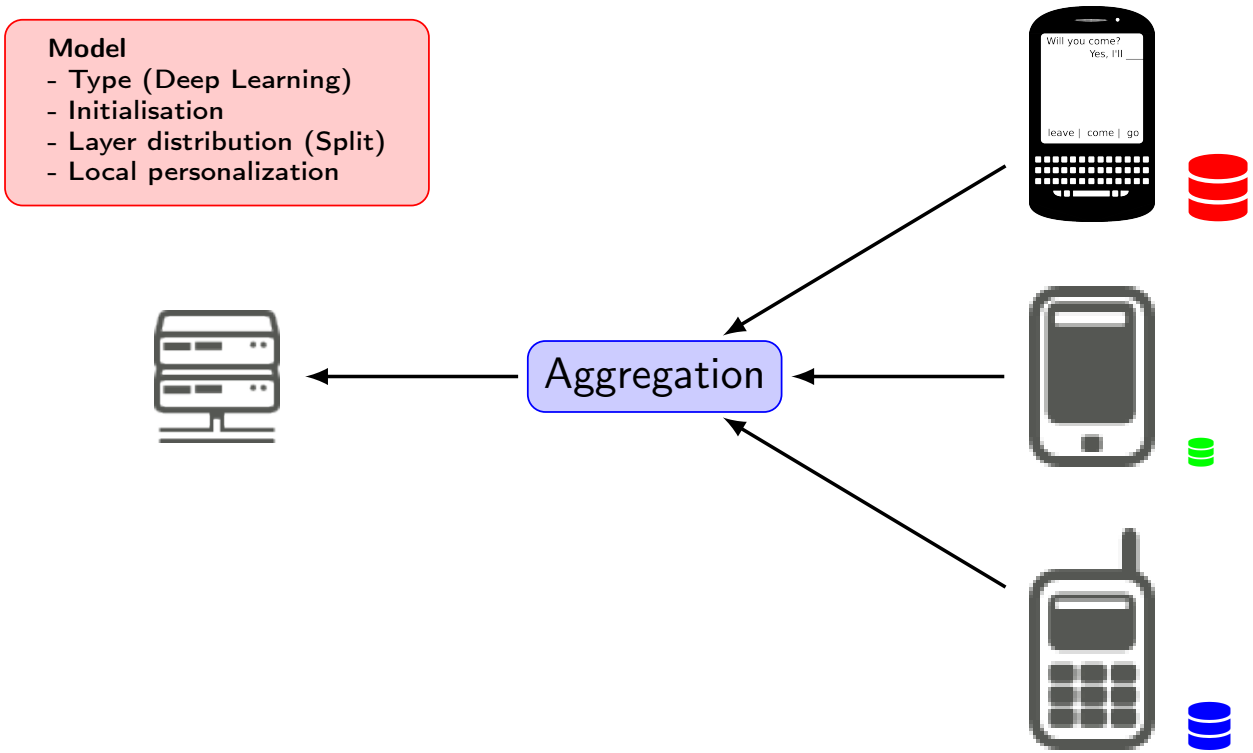


Federated Learning – Research areas

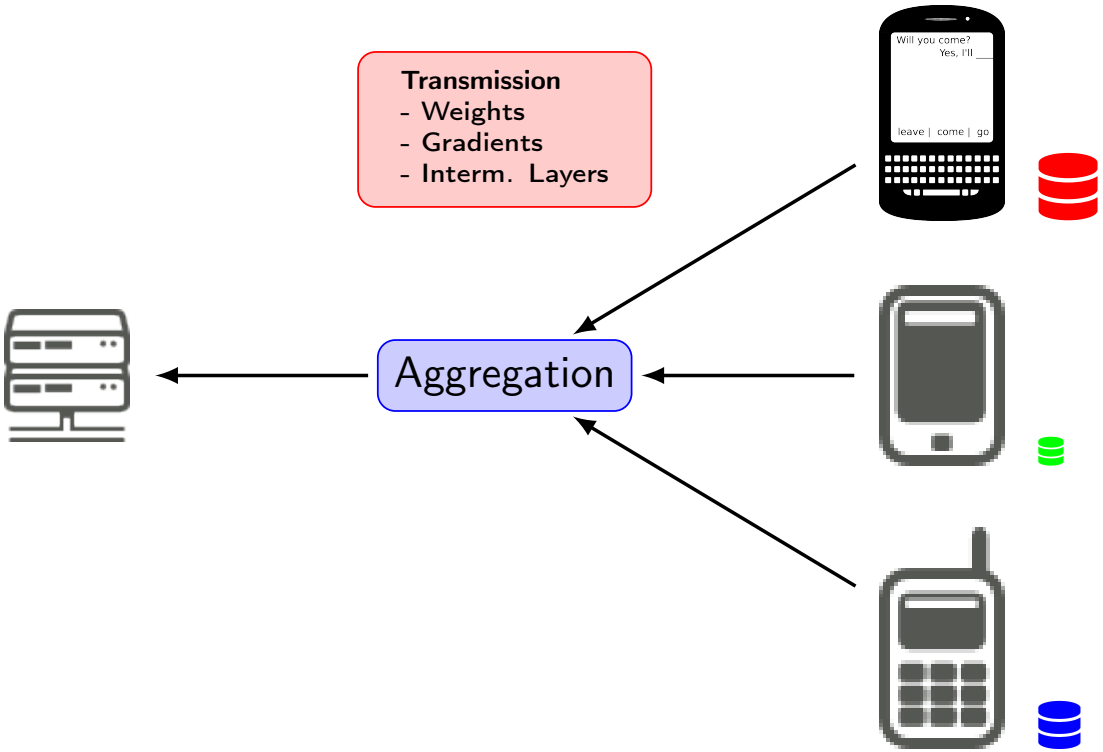
Data Distribution (non/IID)
- im/balance
- in/dependence
- label/feature shifts...



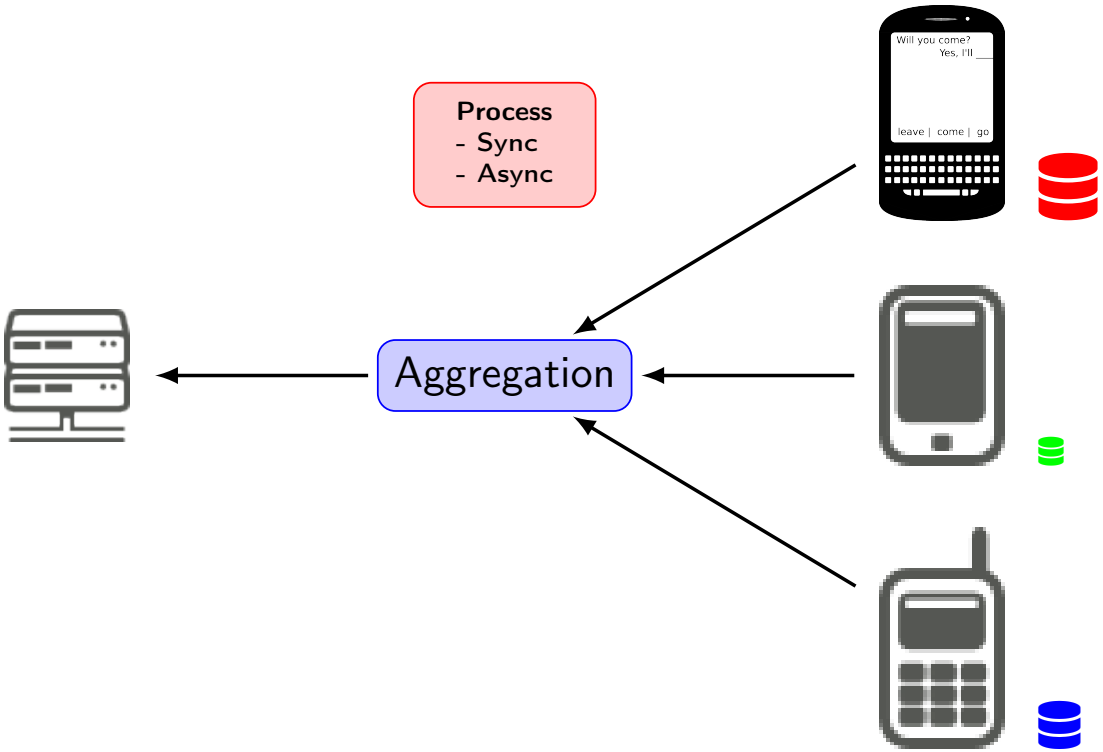
Federated Learning – Research areas



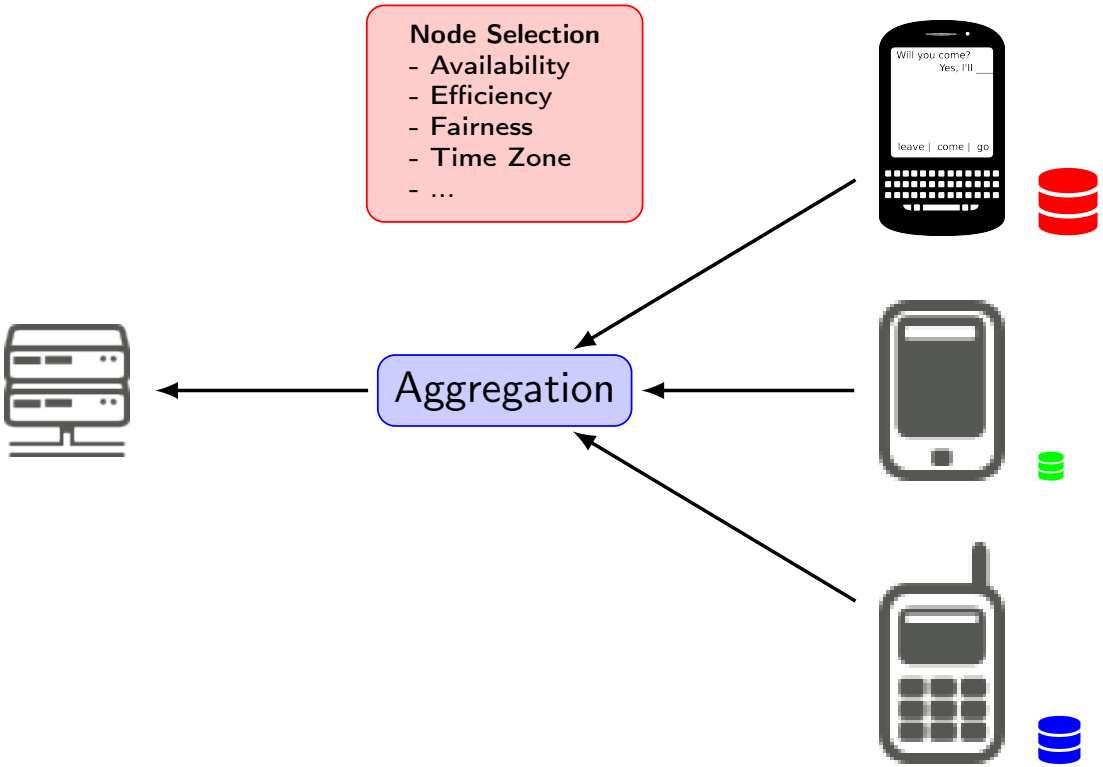
Federated Learning – Research areas



Federated Learning – Research areas

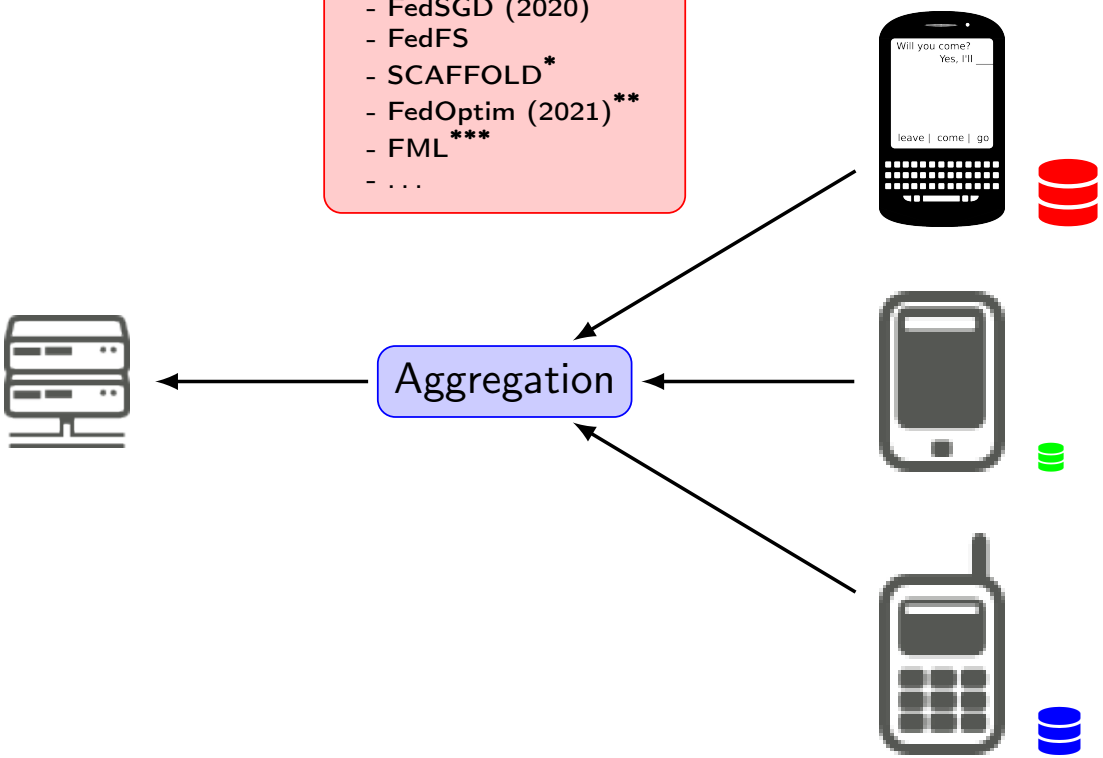


Federated Learning – Research areas

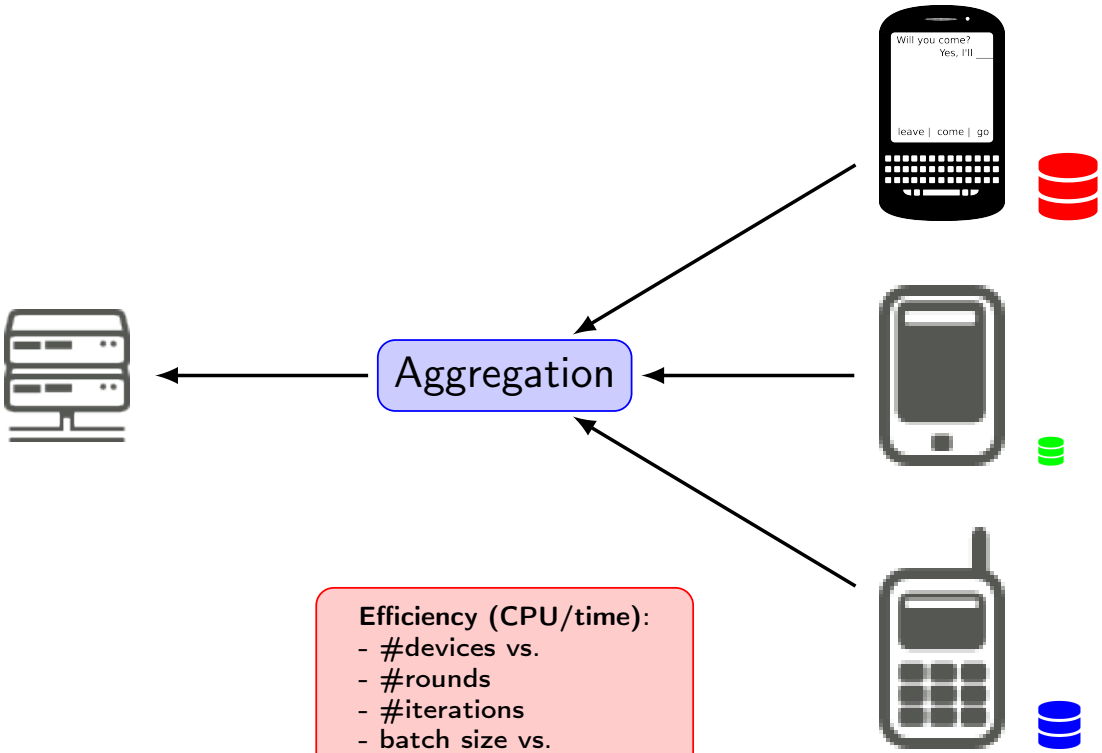


Federated Learning – Research areas

Averaging
- FedAVG (2017)
- SecAgg
- FedProx (2018)
- MATCHA (2019)
- FedSGD (2020)
- FedFS
- SCAFFOLD*
- FedOptim (2021)**
- FML***
- ...

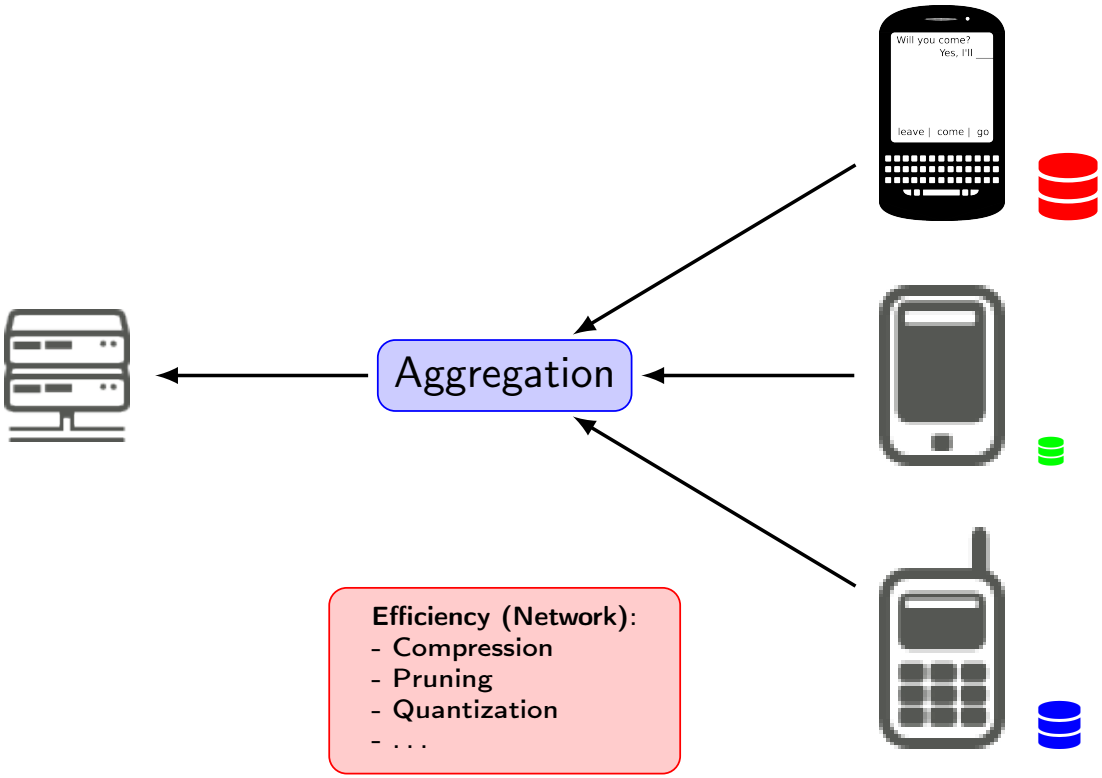


Federated Learning – Research areas

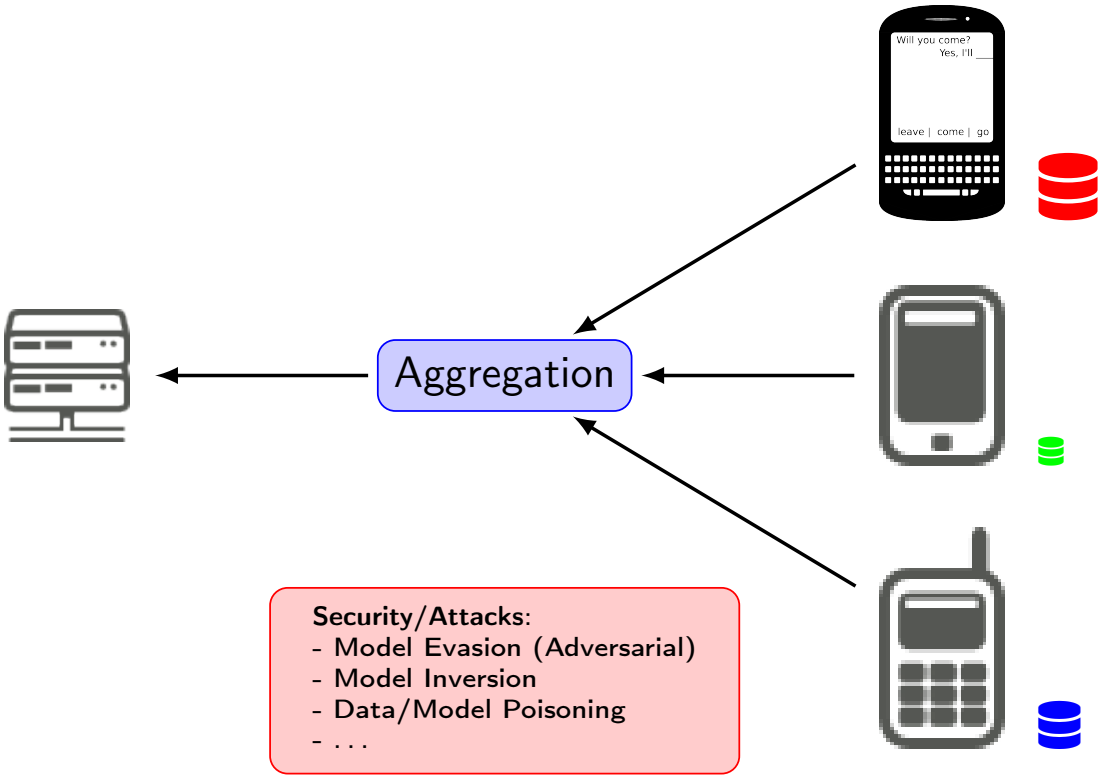


Efficiency (CPU/time):
- #devices vs.
- #rounds
- #iterations
- batch size vs.
- convergence time vs.
- accuracy vs.
- ...

Federated Learning – Research areas



Federated Learning – Research areas



Outline

A lot of platforms!!!

Big Players – "Red Hot"

- PySyft (OpenMined)
- Tensor Flow Federated (Google)

Big Players – "Industrial"

- FATE (WeBank)
- IBM-FL (IBM)
- CLARA (NVIDIA)
- Open Federated Learning (Intel)
- PaddleFL (Baidu)
- Owkin Connect (Owkin)

Big Players – "Academic"

- FedML (USC)
- LEAF (Carnegie Mellon)
- Flower (UK, DE, FR)

Others

- XayNet
- G(alaxy)FL
- Sherpa.ai
- DiscreetAI

A lot of platforms!!!

Big Players – "Red Hot"

- **PySyft (OpenMined)**
- **Tensor Flow Federated (Google)**

Big Players – "Industrial"

- FATE (WeBank)
- IBM-FL (IBM)
- CLARA (NVIDIA)
- Open Federated Learning (Intel)
- PaddleFL (Baidu)
- Owkin Connect (Owkin)

Big Players – "Academic"

- FedML (USC)
- LEAF (Carnegie Mellon)
- Flower (UK, DE, FR)

Others

- XayNet
- G(alaxy)FL
- Sherpa.ai
- DiscreetAI

A lot of platforms!!!

Big Players – "Red Hot"

- **PySyft (OpenMined)**
- **Tensor Flow Federated (Google)**

Big Players – "Industrial"

- FATE (WeBank)
- IBM-FL (IBM)
- CLARA (NVIDIA)
- Open Federated Learning (Intel)
- PaddleFL (Baidu)
- **Owkin Connect (Owkin)**

Big Players – "Academic"

- FedML (USC)
- LEAF (Carnegie Mellon)
- Flower (UK, DE, FR)

Others

- XayNet
- G(alaxy)FL
- Sherpa.ai
- DiscreetAI

A lot of platforms!!!

Big Players – "Red Hot"

- **PySyft (OpenMined)**
- **Tensor Flow Federated (Google)**

Big Players – "Industrial"

- FATE (WeBank)
- IBM-FL (IBM)
- CLARA (NVIDIA)
- Open Federated Learning (Intel)
- PaddleFL (Baidu)
- **Owkin Connect (Owkin)**

Big Players – "Academic"

- **FedML (USC)**
- LEAF (Carnegie Mellon)
- **Flower (UK, DE, FR)**

Others

- XayNet
- G(alaxy)FL
- Sherpa.ai
- DiscreetAI

PySyft

https://github.com/OpenMined/PySyft

Who

- OpenMined (Andrew Trask)

What

- Low level
- Central Controller
- PyTorch & TensorFlow

Focus

- Privacy

Pros

- Lots of docs

https://www.youtube.com/watch?v=NJBBE_SN90A (commercial)
https://www.youtube.com/watch?v=4zrU54VIK6k (technical)

Tensor Flow Federated (TFF)

https://www.tensorflow.org/federated

Who

- Google (Krzysztof Ostrowski, Emily Ganz)

What

- Low level
- TensorFlow only

Focus

- Privacy (GBoard)

Pros

- Lots of docs

https://www.youtube.com/watch?v=m17IgaHaoTI

Owkin

https://owkin.com/platform/software-stack/

Who

- Owkin (French startup, Thomas Clozel)

What

- Totally decentralized
- Uses & Ledger/BlockChain (↓ cheating & computation)

Focus

- Health Care Applications
- Vertical FL

Cons

- Only core is FLOSS ("Substra")

https://www.youtube.com/watch?v=mjqTpahgkGs

FedML

https://github.com/FedML-AI/FedML

Who

- Consortium
  - Academics: USC + Stanford + MIT + MSU...
  - Companies: Tencent + WeBank...
- Presented @NeurIPS in dec. 2020

What

- Simulation & On-device
- Device/Platform/Framework Agnostic

https://arxiv.org/abs/2007.13518

Flower

https://flower.dev/

Who

- Consortium (UK + Germany + France...)

What

- Simulation & On-device
- Device/Platform/Framework Agnostic
  - PyTorch, TensorFlow, MXNet...
  - IoT, Servers...

https://arxiv.org/abs/2007.14390

Machine Learning at Laboratoire Hubert Curien

ML ("Data Intelligence" Team)

- Transfer Learning/DA, PAC Bayesian, Graph NN, Fairness...

Machine Learning at Laboratoire Hubert Curien

ML ("Data Intelligence" Team)

- Transfer Learning/DA, PAC Bayesian, Graph NN, Fairness...

FL & Networking (GM + K. Singh)

- Intrusion detection (+ Univ. Nantes)

Machine Learning at Laboratoire Hubert Curien

ML ("Data Intelligence" Team)

- Transfer Learning/DA, PAC Bayesian, Graph NN, Fairness...

FL & Networking (GM + K. Singh)

- Intrusion detection (+ Univ. Nantes)
- Network Management (+ Univ. Poitiers + Huawei)
  - French National Project (ANR)
  - Interpretability
  - Safety

Machine Learning at Laboratoire Hubert Curien

ML ("Data Intelligence" Team)

- Transfer Learning/DA, PAC Bayesian, Graph NN, Fairness...

FL & Networking (GM + K. Singh)

- Intrusion detection (+ Univ. Nantes)
- Network Management (+ Univ. Poitiers + Huawei)
  - French National Project (ANR)
  - Interpretability
  - Safety
- ⚠ PhD/post-doc positions ⚠

Machine Learning at Laboratoire Hubert Curien

ML ("Data Intelligence" Team)

- Transfer Learning/DA, PAC Bayesian, Graph NN, Fairness...

FL & Networking (GM + K. Singh)

- Intrusion detection (+ Univ. Nantes)
- Network Management (+ Univ. Poitiers + Huawei)
  - French National Project (ANR)
  - Interpretability
  - Safety
- ⚠ PhD/post-doc positions ⚠

FL & Small Devices (GM + V. Fresse + Telecom Bretagne)

- FPGAs + Split Learning

FL & Privacy (T.N. Le, A. Habrard, M. Sebban)

- Random Projections

Take aways

IoT & AI for Smart Cities

- Smart Applications $\Rightarrow$ Machine Learning
  -  &
  

Take aways

IoT & AI for Smart Cities

- Smart Applications ⇒ Machine Learning
  -  & 

IoT = Decentralized setup / Constrained resources

- Ensure Privacy & Efficiency ⇒ Federated Learning

Take aways

IoT & AI for Smart Cities

- Smart Applications ⇒ Machine Learning
  -  & 

IoT = Decentralized setup / Constrained resources

- Ensure Privacy & Efficiency ⇒ Federated Learning

Federated Learning works!

- There are many platforms
- But there are still challenges in many specific points

Thematic Bibliography – Basics

Fundational Paper

[MMR+17] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera

y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017

Surveys

[KMA+19] Peter Kairouz, H. Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista A. Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, Rafael G. L. D'Oliveira, Salim El Rouayheb, David Evans, Josh Gardner, Zachary Garrett, Adrià Gascón, Badih Ghazi, Phillip B. Gibbons, Marco Gruteser, Zaïd Harchaoui, Chaoyang He, Lie He, Zhouyuan Huo, Ben Hutchinson, Justin Hsu, Martin Jaggi, Tara Javidi, Gauri Joshi, Mikhail Khodak, Jakub Konečný, Aleksandra Korolova, Farinaz Koushanfar, Sanmi Koyejo, Tancrède Lepoint, Yang Liu, Prateek Mittal, Mehryar Mohri, Richard Nock, Ayfer Özgür, Rasmus Pagh, Mariana Raykova, Hang Qi, Daniel Ramage, Ramesh Raskar, Dawn Song, Weikang Song, Sebastian U. Stich, Ziteng Sun, Ananda Theertha Suresh, Florian Tramèr, Praneeth Vepakomma, Jianyu Wang, Li Xiong, Zheng Xu, Qiang Yang, Felix X. Yu, Han

Yu, and Sen Zhao. Advances and open problems in federated learning. *CoRR*, abs/1912.04977, 2019

[KSH+20] Latif U. Khan, Walid Saad, Zhu Han, Ekram Hossain, and Choong Seon Hong. Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *CoRR*, abs/2009.13012, 2020

[BTM+20] Daniel J. Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Titouan Parcollet, and Nicholas D.

Lane. Flower: A friendly federated learning research framework. *CoRR*, abs/2007.14390, 2020

[YLC+19] Qiang Yang, Yang Liu, Yong Cheng, Yan Kang, Tianjian Chen, and Han Yu. Morgan & Claypool, 2019

Thematic Bibliography – Aggregation

- (FedAVG) [MMR+17] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017
- (SecAgg) [BIK+17] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1175–1191, 2017
- (FedProx) [SLS+18] Anit Kumar Sahu, Tian Li, Maziar Sanjabi, Manzil Zaheer, Ameet Talwalkar, and Virginia Smith. On the convergence of federated optimization in heterogeneous networks. *CoRR*, abs/1812.06127, 2018
- (MATCHA) [WSY+19] Jianyu Wang, Anit Kumar Sahu, Zhouyi Yang, Gauri Joshi, and Soummya Kar. MATCHA: speeding up decentralized SGD via matching decomposition sampling. *CoRR*, abs/1905.09435, 2019
- (FedSVG) [RCZ+20] Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečnỳ, Sanjiv Kumar, and H Brendan McMahan. Adaptive federated optimization. *arXiv preprint arXiv:2003.00295*, 2020
- (FedFS) [BTM+20] Daniel J. Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Titouan Parcollet, and Nicholas D. Lane. Flower: A friendly federated learning research framework. *CoRR*, abs/2007.14390, 2020
- (SCAFFOLD) [KKM+20] Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. SCAFFOLD: Stochastic controlled averaging for federated learning. In *International Conference on Machine Learning*, pages 5132–5143. PMLR, 2020
- (FedOptim) [RCZ+21] Sashank J. Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečný, Sanjiv Kumar, and Hugh Brendan McMahan. Adaptive federated optimization. In *International Conference on Learning Representations*, 2021

Thematic Bibliography – Attacks

Model Evasion

[SZS+13] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*, 2013

[GSS14] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*, 2014

Model Inversion

[HAPC17] Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz. Deep models under the gan: information leakage from collaborative deep learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 603–618, 2017

[FJR15] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, pages 1322–1333, 2015

Data/Model Poisoning

[LMA+17] Yingqi Liu, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, and Xiangyu Zhang. Trojaning attack on neural networks. Technical report, Purdue University. Department of Computer Science Technical Reports. Paper 1781, 2017. https://docs.lib.purdue.edu/cstech/1781

[BNL12] Battista Biggio, Blaine Nelson, and Pavel Laskov. Poisoning attacks against support vector machines. *arXiv preprint arXiv:1206.6389*, 2012

Thematic Bibliography – Platforms

Platforms

[ZTL+21] Alexander Ziller, Andrew Trask, Antonio Lopardo, Benjamin Szymkow, Bobby Wagner, Emma Bluemke, Jean-Mickael Nounahon, Jonathan Passerat-Palmbach, Kritika Prakash, Nick Rose, Théo

Ryffel, Zarreen Naowal Reza, and Georgios Kaissis. *PySyft: A Library for Easy Federated Learning*, pages 111–139. Springer International Publishing, Cham, 2021

[Goo] Google. TensorFlow Federated learning platform. https://www.tensorflow.org/federated

[WeB] WeBank. FATE federated learning platform. https://github.com/FederatedAI/FATE

[IBM] IBM. IBM-FL federated learning platform. https://github.com/IBM/federated-learning-lib

[NVI] NVIDIA. CLARA machine learning platform (includes federated learning)

[Int] Intel. Open federated learning platform. https://github.com/IntelLabs/OpenFederatedLearning

[Bai] Baidu. Paddlefl federated learning platform. https://github.com/PaddlePaddle/PaddleFL

[Owk] Owkin. Owkin connect federated learning platform. https://owkin.com/platform/software-stack/ , https://github.com/SubstraFoundation

[HLS+20] Chaoyang He, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang,

Praneeth Vepakomma, Abhishek Singh, Hang Qiu, et al. FedML: A research library and benchmark for federated machine learning. *arXiv preprint arXiv:2007.13518*, 2020

[Mel] Carnegie Mellon. Leaf federated learning platform. https://leaf.cmu.edu/

[BTM+20] Daniel J. Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Titouan Parcollet, and Nicholas D.

Lane. Flower: A friendly federated learning research framework. *CoRR*, abs/2007.14390, 2020

Thematic Bibliography – 4

Split Learning

[VGSR18] Praneeth Vepakomma, Otkrist Gupta, Tristan Swedish, and Ramesh Raskar. Split learning for health: Distributed deep learning without sharing raw patient data. *arXiv preprint arXiv:1812.00564*, 2018

Pricacy

(Differential Privacy) [DR14] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014

(Homorphic Encryption) [Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery

IoT/FL in practice

Preliminaries

- `apt install python3`

Virtual Env

- `apt install python3-venv`
- `python -m venv isc2lab && cd isc2lab && . ./bin/activate`

FL Platform: Flower + ML lib: TensorFlow

- `pip3 install flwr`
- `pip3 install tensorflow`

Code & Dataset

- https://github.com/GMTSE/isc2-IoT-AI-smart-tutorial