

EPI RQ4 Research Update: Privacy Preserving Distributed Machine Learning

Saba Amiri
s.amiri@uva.nl



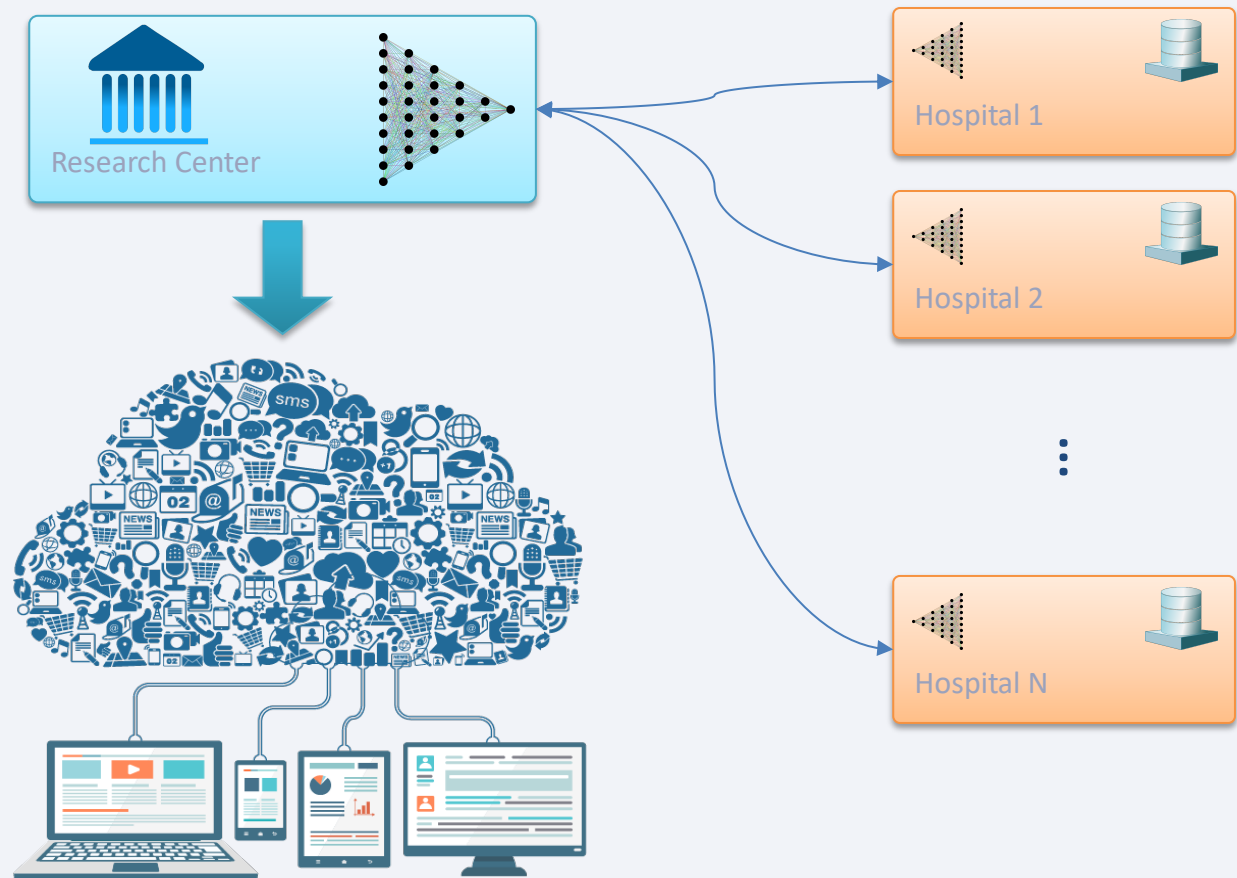
Supervisor: Adam Belloum

Promoters: Sander Klous, Leon Gommans

Multiscale Networked Systems Group

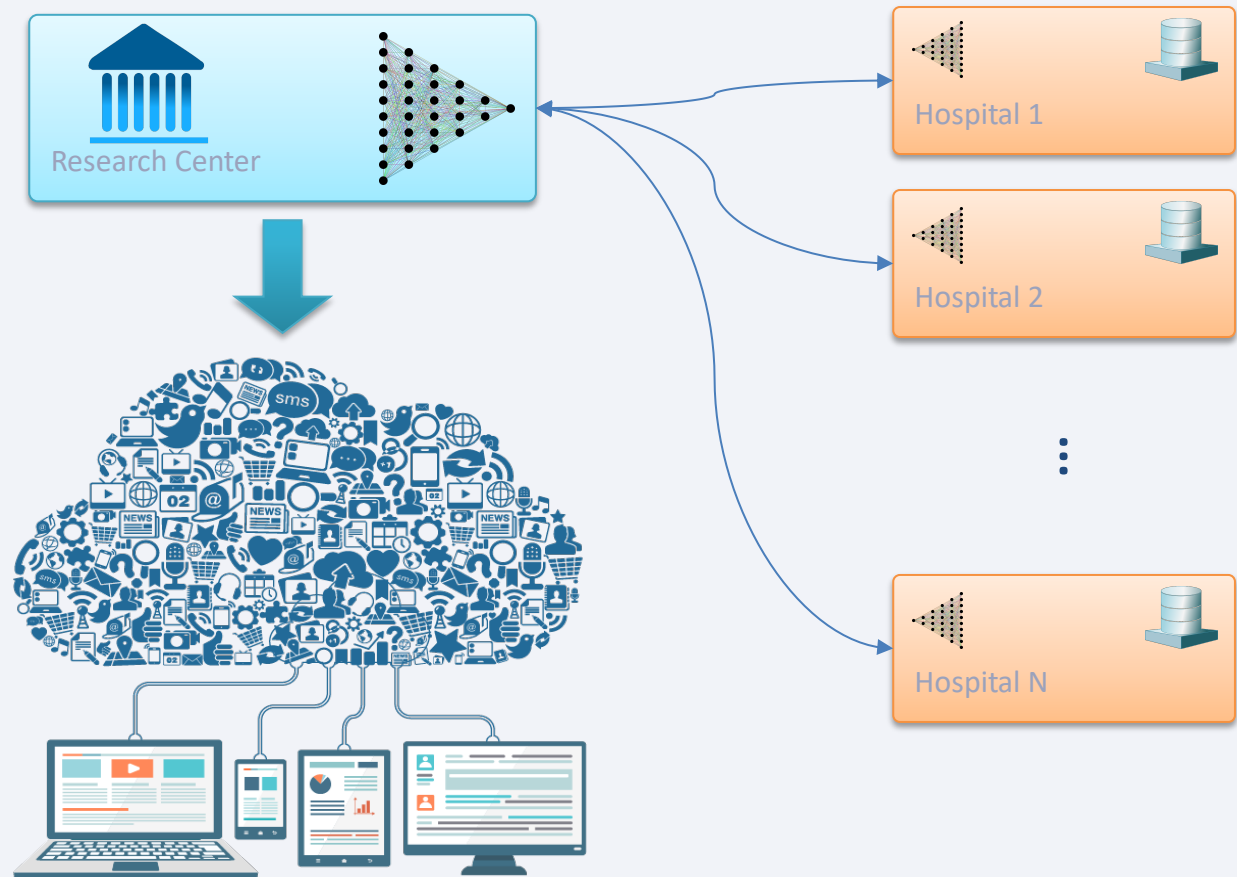
23 April 2021

➤ Digital Health Twin



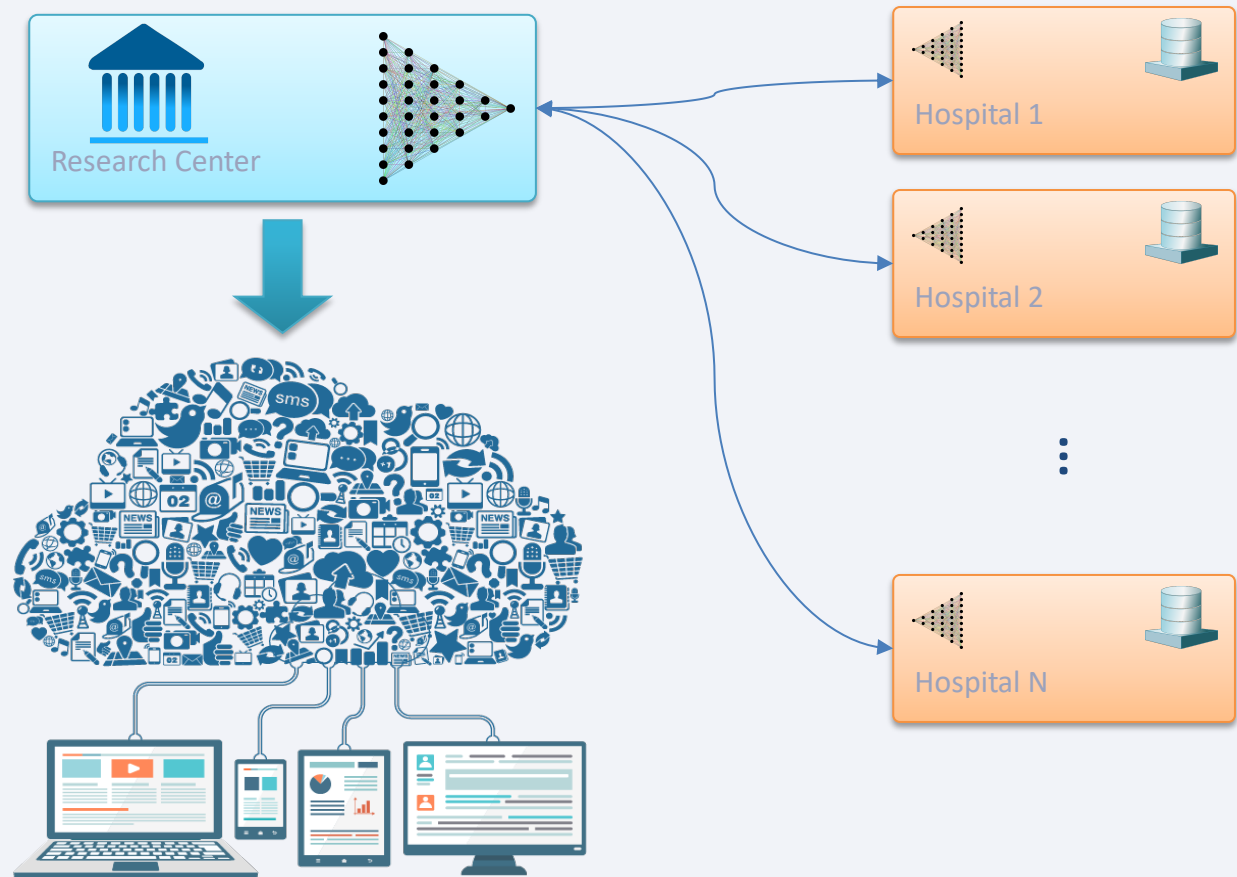
Research Domain

- Digital Health Twin
- Distributed Learning



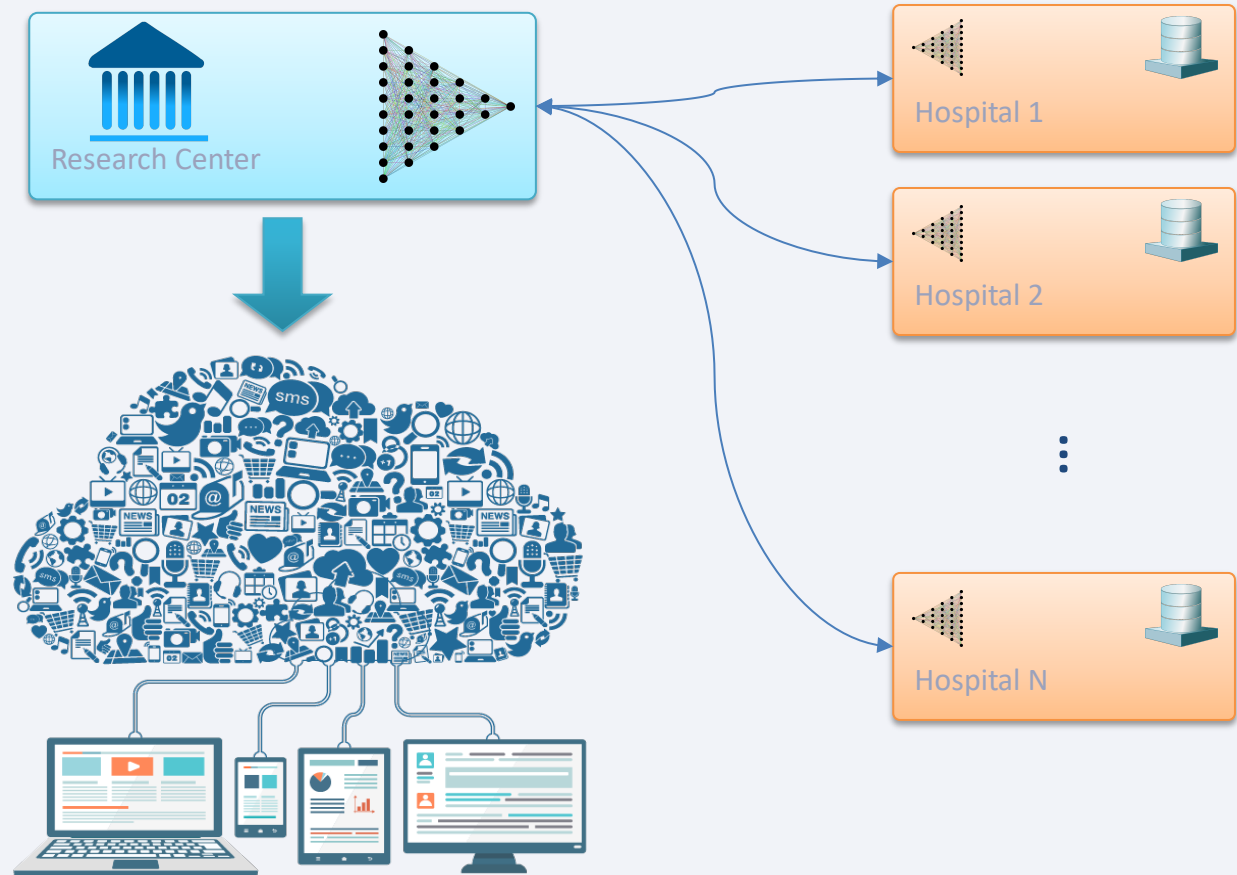
Research Domain

- Digital Health Twin
- Distributed Learning
- Privacy Preservation



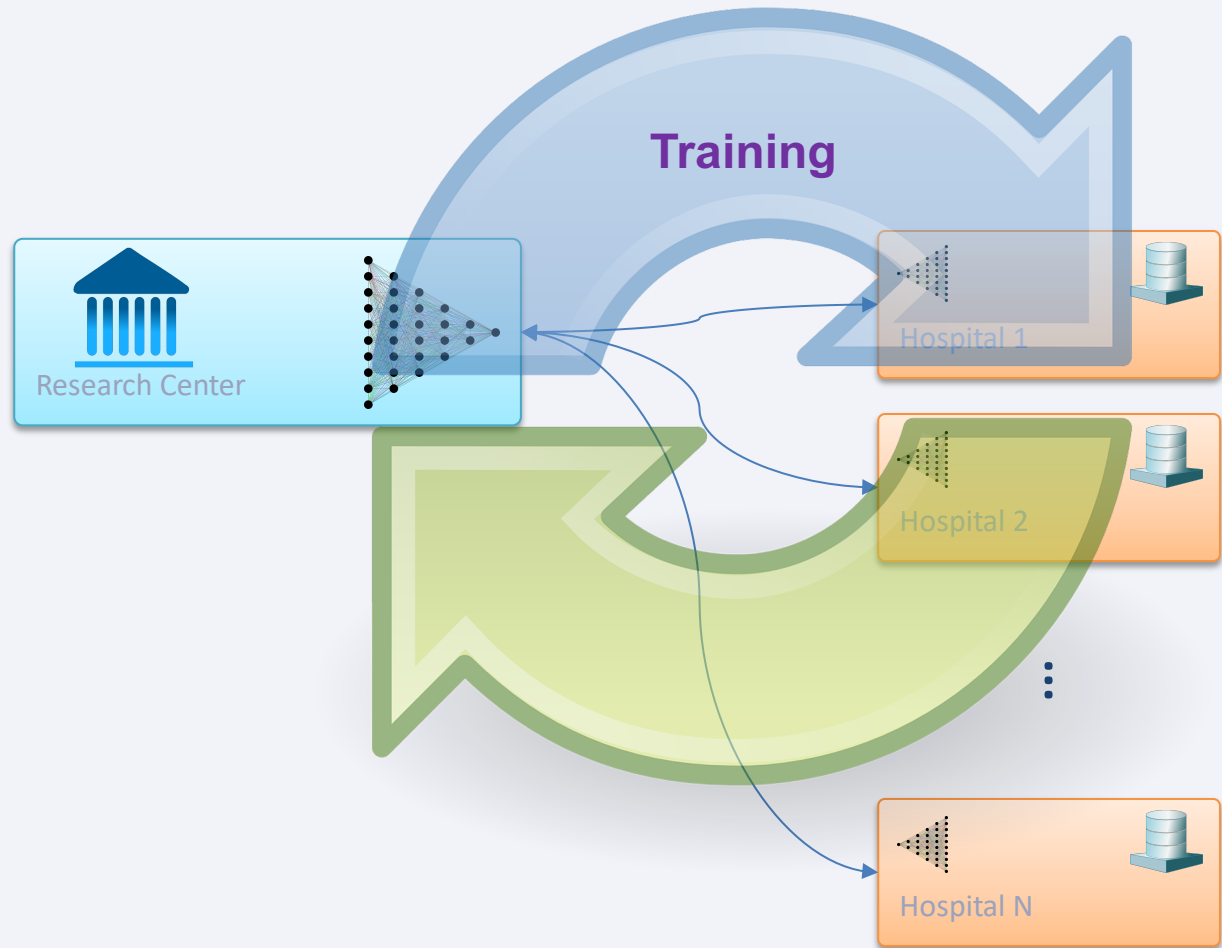
Definition of Privacy

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole



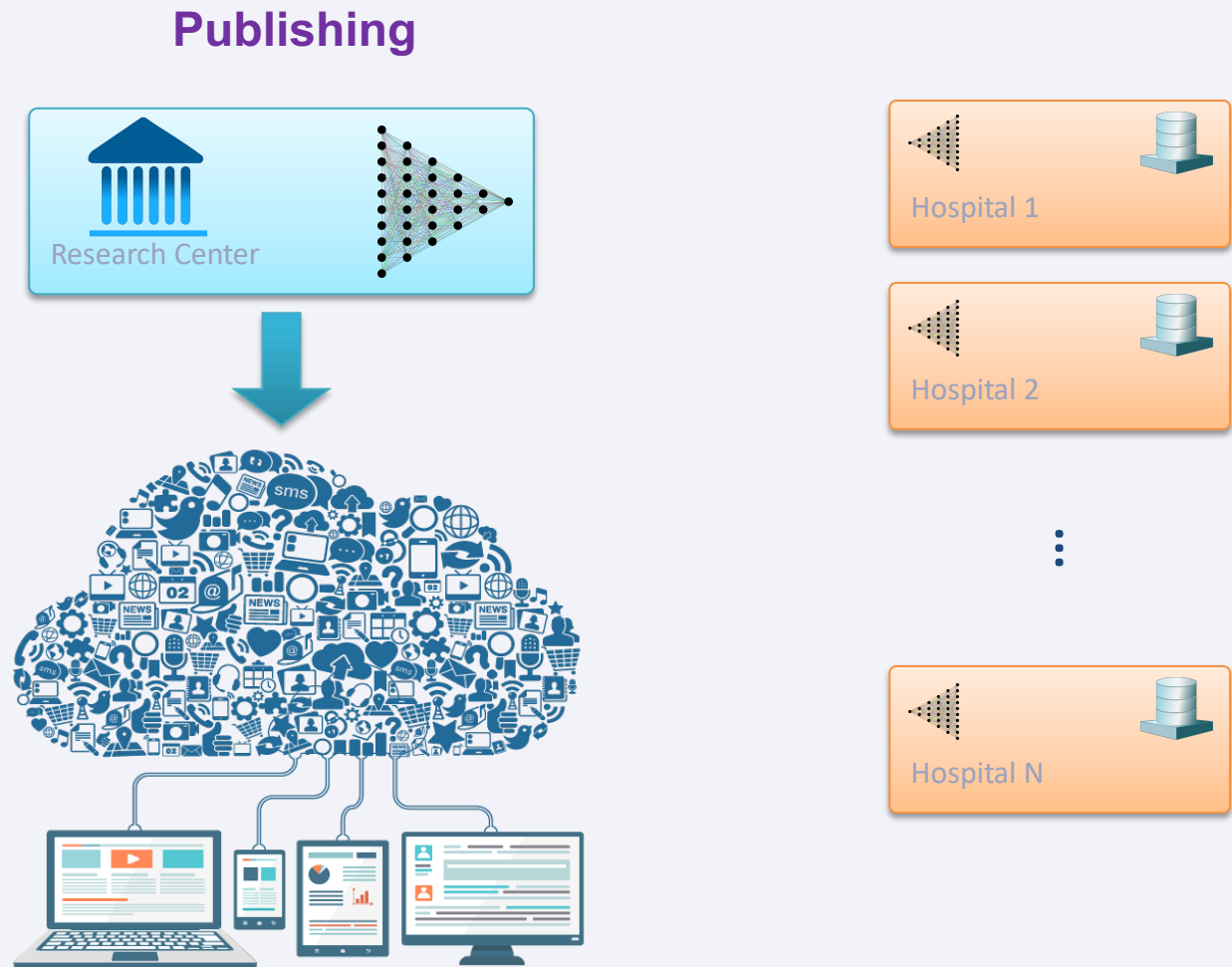
Typical Federated Learning Scenario

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole



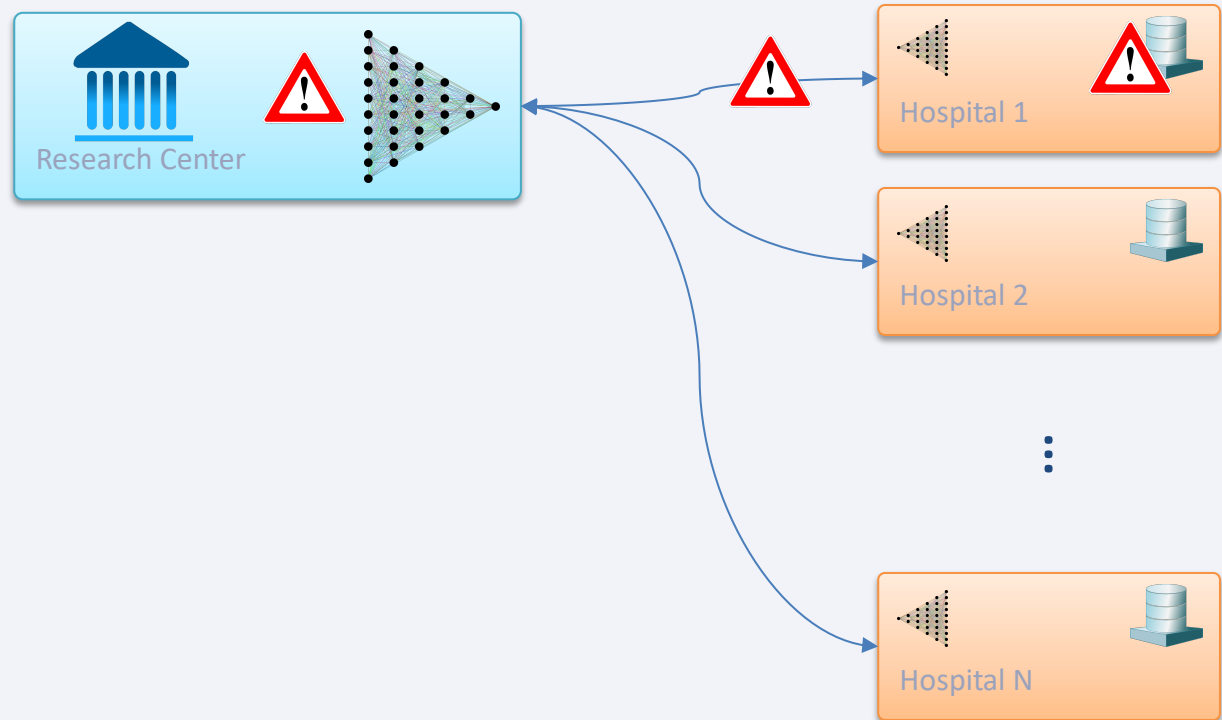
Typical Federated Learning Scenario - Publishing

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole



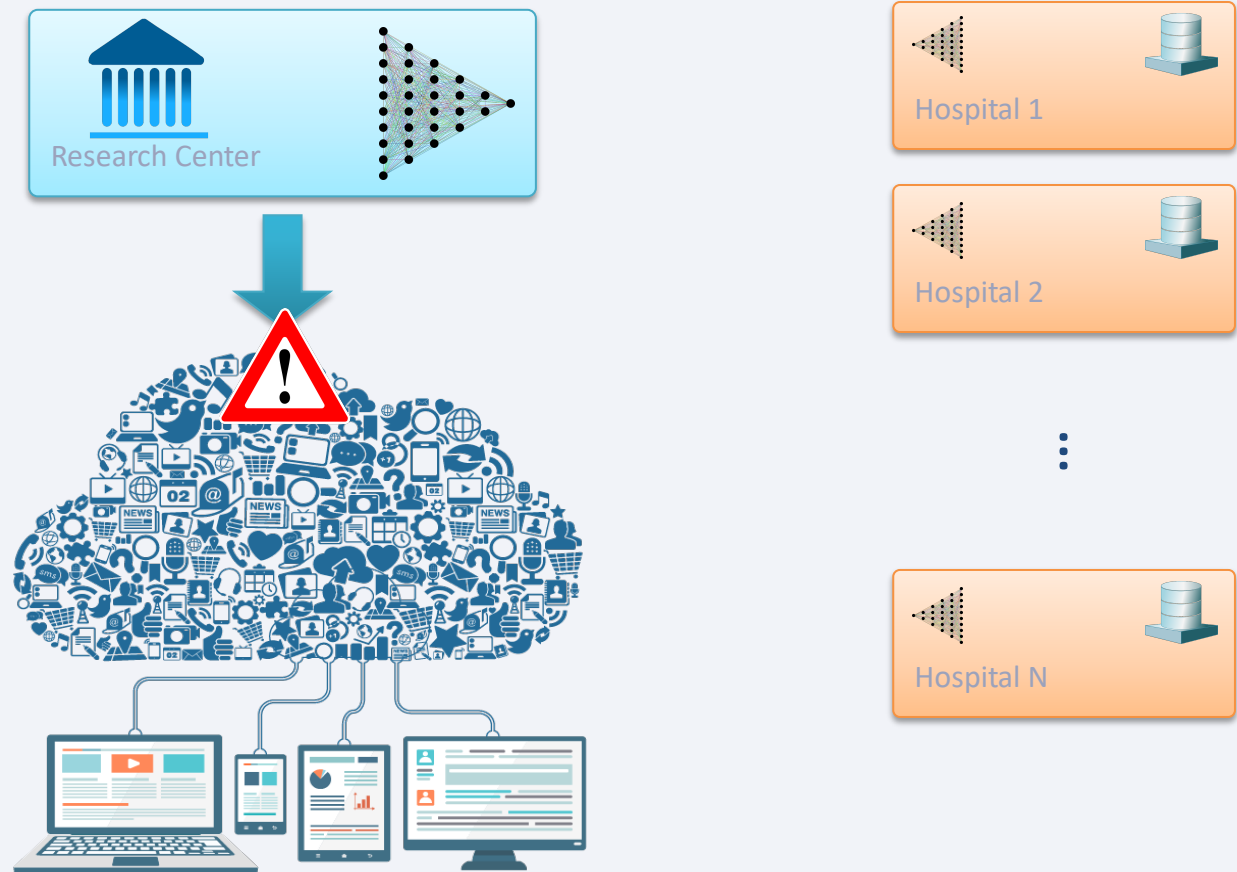
Typical Federated Learning Scenario – Training Risks

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - ❑ Data
 - ❑ Communication
 - ❑ Infrastructure



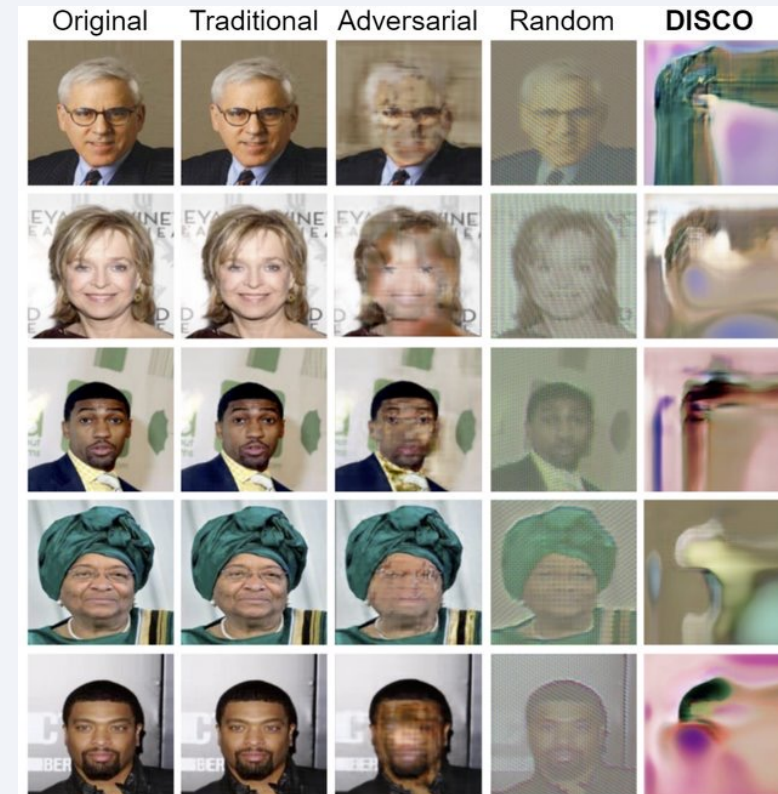
Typical Federated Learning Scenario – Publication Risks

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - ❑ Data
 - ❑ Communication
 - ❑ Infrastructure
 - ❑ **Machine learning model output**



The Need for Privacy Preserving Machine Learning

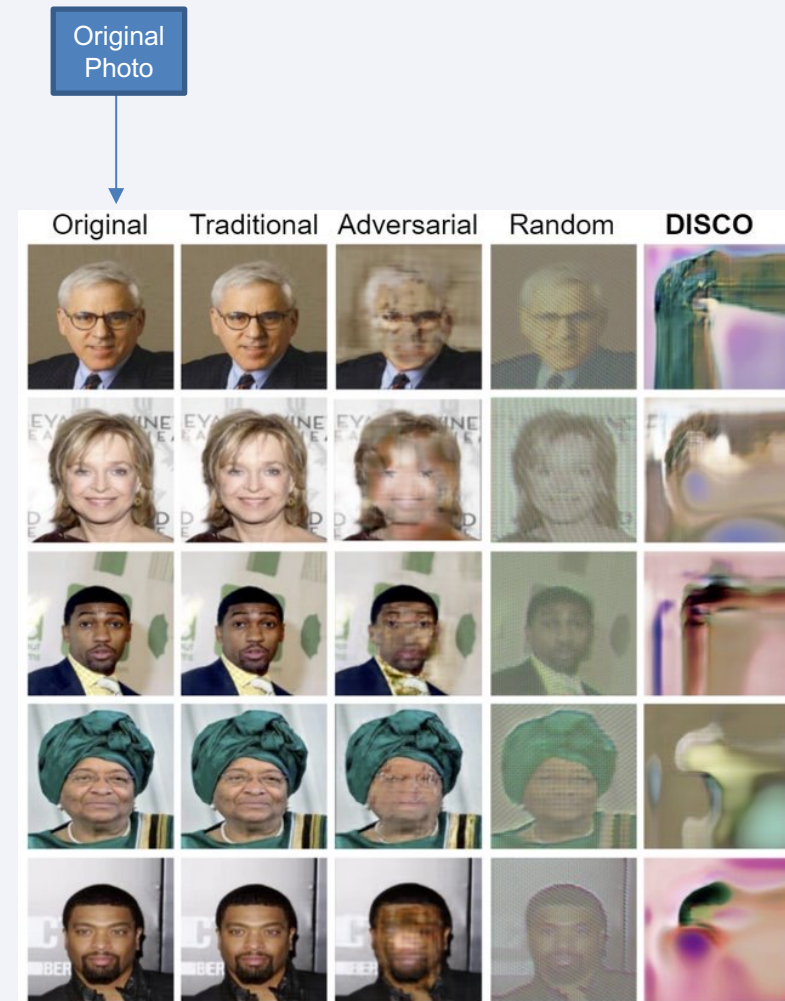
- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - ❑ Data
 - ❑ Communication
 - ❑ Infrastructure
 - ❑ Machine learning model output



Singh, Abhishek, et al. "DISCO: Dynamic and Invariant Sensitive Channel Obfuscation for deep neural networks." *arXiv preprint arXiv:2012.11025* (2020)

The Need for Privacy Preserving Machine Learning

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - ❑ Data
 - ❑ Communication
 - ❑ Infrastructure
 - ❑ **Machine learning model output**

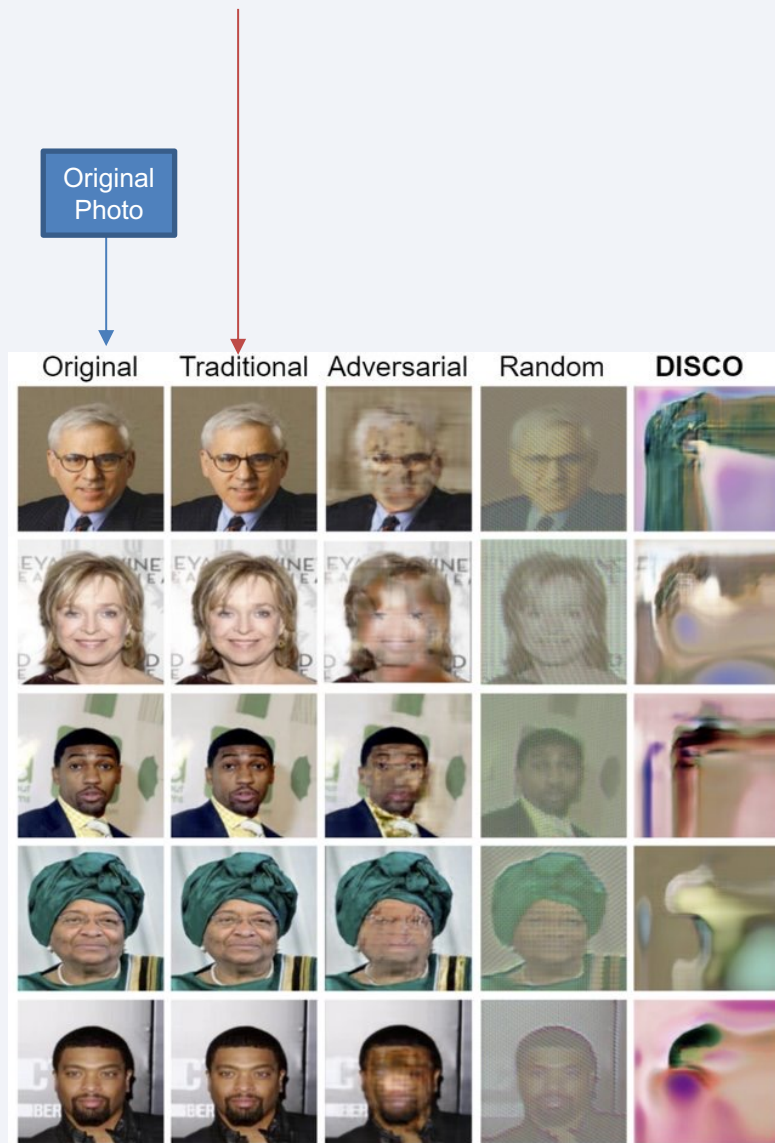


Singh, Abhishek, et al. "DISCO: Dynamic and Invariant Sensitive Channel Obfuscation for deep neural networks." *arXiv preprint arXiv:2012.11025* (2020)

The Need for Privacy Preserving Machine Learning

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - ❑ Data
 - ❑ Communication
 - ❑ Infrastructure
 - ❑ Machine learning model output

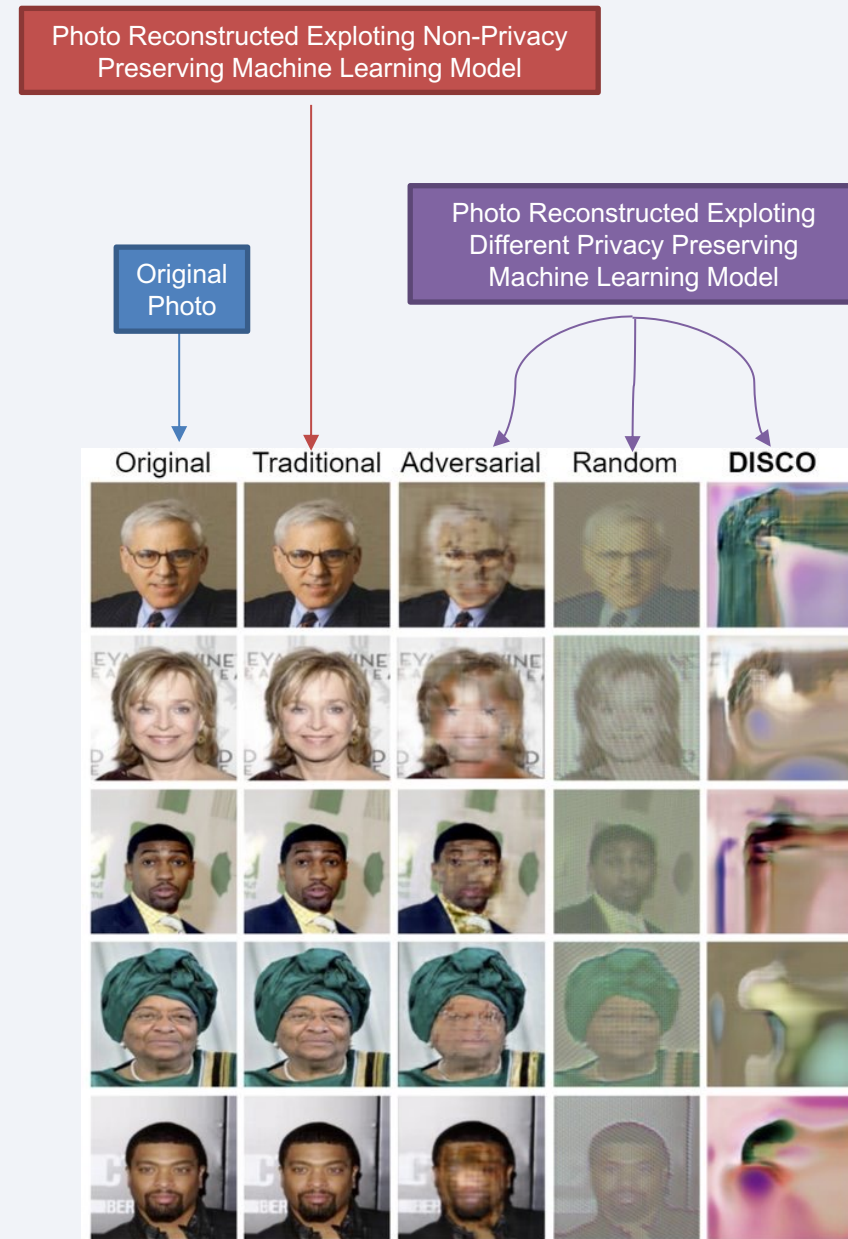
Photo Reconstructed Exploiting Non-Privacy Preserving Machine Learning Model



Singh, Abhishek, et al. "DISCO: Dynamic and Invariant Sensitive Channel Obfuscation for deep neural networks." *arXiv preprint arXiv:2012.11025* (2020)

The Need for Privacy Preserving Machine Learning

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - ❑ Data
 - ❑ Communication
 - ❑ Infrastructure
 - ❑ Machine learning model output

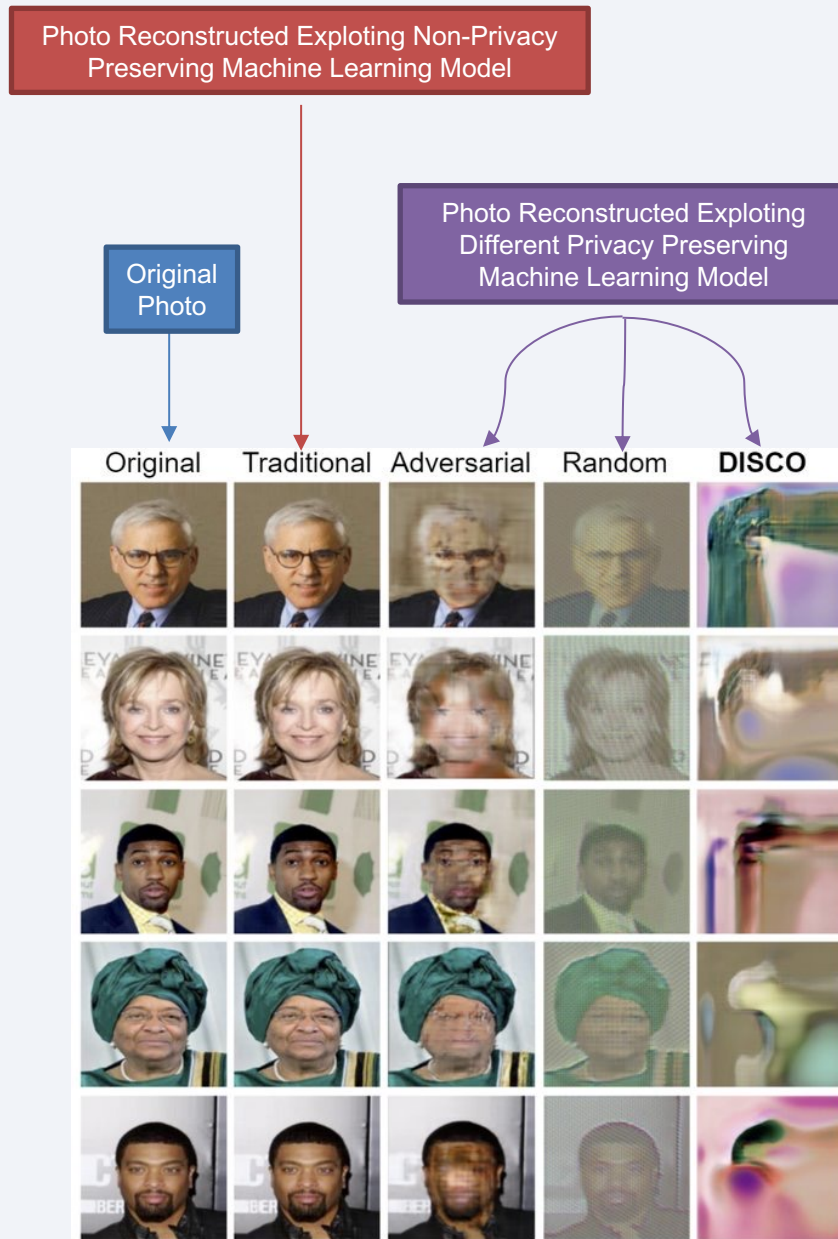


Singh, Abhishek, et al. "DISCO: Dynamic and Invariant Sensitive Channel Obfuscation for deep neural networks." *arXiv preprint arXiv:2012.11025* (2020)

The Need for Privacy Preserving Machine Learning

- Digital Health Twin
- Distributed Learning
- Privacy Preservation
 - Definition: Providing patient/record level protection to every member of the training set while gaining useful insights about the populations as a whole
 - What is not private?
 - Data
 - Communication Satisfies our privacy definition
 - Infrastructure
 - Machine learning model output
 - Solution
 - Privacy Preserving Machine Learning
 - Mechanism
 - Differential Privacy

Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." *Foundations and Trends in Theoretical Computer Science* 9.3-4 (2014): 211-407.



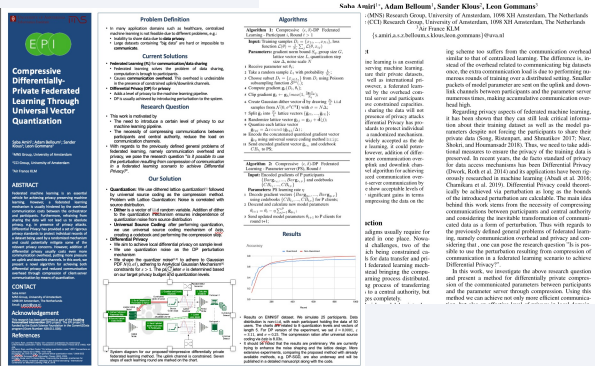
Singh, Abhishek, et al. "DISCO: Dynamic and Invariant Sensitive Channel Obfuscation for deep neural networks." *arXiv preprint arXiv:2012.11025* (2020)



Past and Present Activities

- Supervision of 3 B.Sc. AI Theses (concluded)^[1]
- Supervision of 3 M.Sc. computer science literature reviews (concluded) ^[1]
- Short paper on *local differentially private federated learning through compression* (PPAI@AAAI-21) ^[2]
- Research on *local and global differentially private federated learning through compression* (experiments underway, paper being prepared)
- Review paper on *differentially private synthetic data generation* submitted. (pending editorial decision) ^[1]
- Review paper on *privacy attacks against machine learning systems* (receiving internal feedback) ^[1]
- Review paper on *privacy preserving distributed machine learning w/ Corinne* (being prepared)
- General paper on *EPI project* (being prepared)
- Supervision of 4 M.Sc. computer science and data science theses (underway)
- Research on DP distributed synthetic data generation (underway)

Compressive Differentially-Private Federated Learning Through Universal Vector Quantization



Privacy Preserving Machine Learning-Based Methods for Synthetic Data Generation: A Survey and Review

Carlijn Nijhuis*, Saba Amir*, Adam Bellman*, Sander Kloos*, Loon Gommans*

*Madsisee Networked Systems (MNS) Research Group, University of Amsterdam, 1009 SB Amsterdam, The Netherlands
*Complex Cyber Adaptation (CCA) Research Group, University of Amsterdam, 1009 SB Amsterdam, The Netherlands

Abstract

In recent years, it has been given that machine learning systems need a large amount of data to be trained and tested. This is especially true for deep learning based methods and in some cases such as computer vision. Gathering such a large amount of data leads to several challenges, two of the most important ones being lack of availability and privacy concerns. Synthetic data generation is one of the solutions to overcome the lack of availability. Although numerous data generation methods have already been reported in the literature with high levels of utility, the question of privacy still remains. Viability of different machine learning models against attacks such as reconstruction and membership inference potentially puts the information used to train the data generation models at risk. Thus, methods of privacy preserving machine learning need to be utilized to ensure the privacy of the training data is preserved. This paper provides a survey of privacy preserving machine learning based synthetic data generation methods. We first review the synthetic data generation methods and introduce privacy preserving synthetic data generation methods and attempt to define the research space by pointing these methods into different categories in comparison and elaboration. We conclude by discussing open problems in the field and suggested research areas.

Keywords: synthetic data generation, privacy preserving machine learning, differential privacy, generative models

Privacy Attacks on Machine Learning Systems: A Review

SABA AMIR¹, Madsisee Networked Systems (MNS) Research Group, University of Amsterdam
 JELKE BEEKS², Madsisee Networked Systems (MNS) Research Group, University of Amsterdam
 WILLEMJAN BEEKS¹, Madsisee Networked Systems (MNS) Research Group, University of Amsterdam
 MIKE SCHRIJVER, Madsisee Networked Systems (MNS) Research Group, University of Amsterdam
 ADAM BELLMAN, Madsisee Networked Systems (MNS) Research Group, University of Amsterdam
 SANDER KLOOS, Complex Cyber Adaptation (CCA) Research Group, University of Amsterdam
 LOON GOMMANS, Ad Fontein XLN

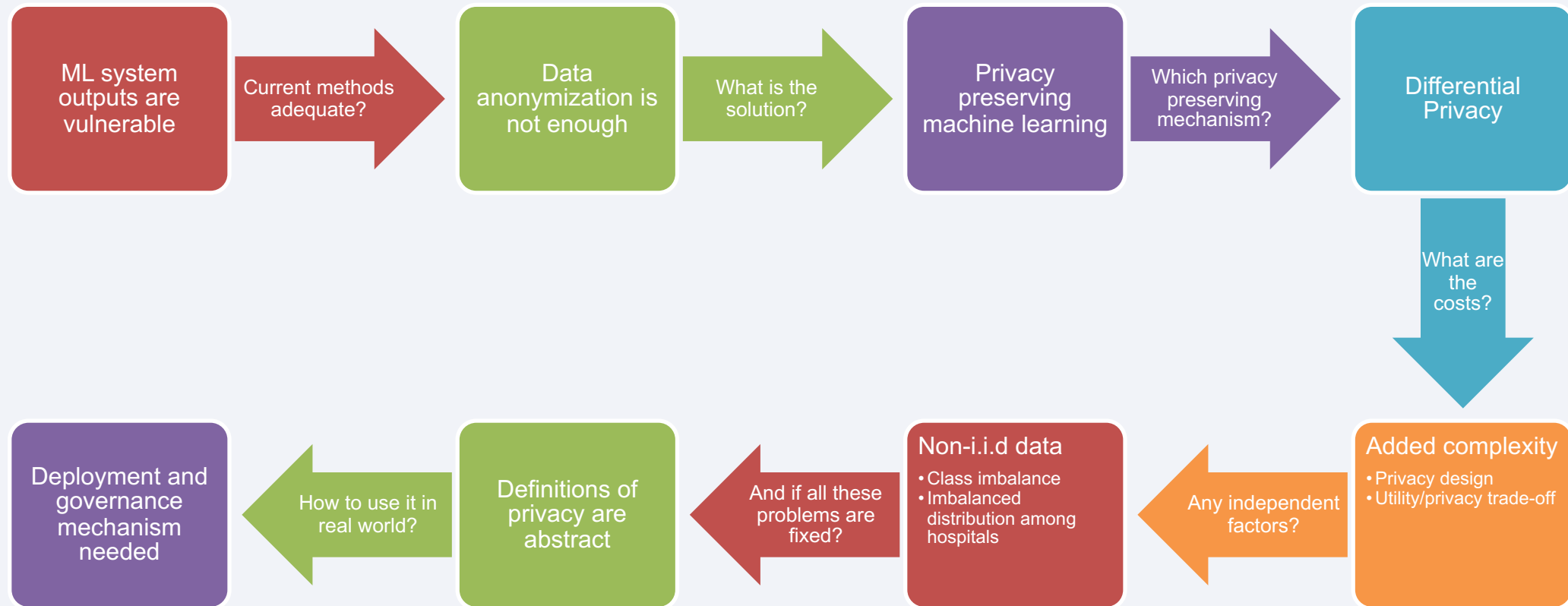
Machine learning models are often placed in cloud environments to make them publicly accessible. This comes with the price of not having full control over the data that has been learned against from models. This work surveys the privacy and security risks in an increasing amount of data that has been learned against from models. The work surveys the privacy and security risks in an increasing amount of data that has been learned against from models. The work surveys the privacy and security risks in an increasing amount of data that has been learned against from models. The work surveys the privacy and security risks in an increasing amount of data that has been learned against from models.

1. Introduction

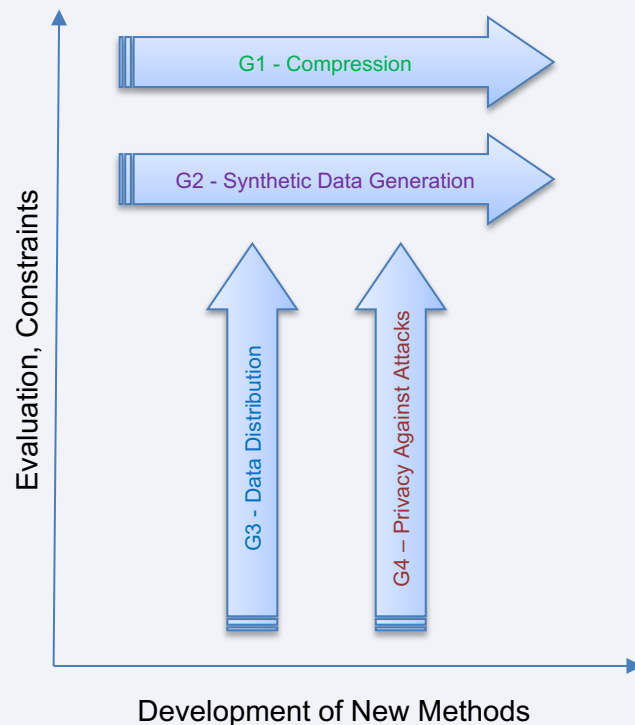
State-of-the-art machine learning systems have shown great potential and high degrees of success when applied to a wide range of tasks [1, 2]. This success is largely due to the availability of large amounts of training data. However, this success comes with a cost: access to the data used to train machine learning models is often restricted to a small number of individuals. This is especially true for deep learning based methods, which require large amounts of data to be trained. This is especially true for deep learning based methods, which require large amounts of data to be trained. This is especially true for deep learning based methods, which require large amounts of data to be trained.

[1] Reports and paper available upon request; Code will be published by August 2021 depending on permission from consortium

[2] <https://ppai21.github.io/files/29-paper.pdf>



- G1 - Achieve Differential Privacy Through Compression
- G2 - Generate differentially-private synthetic tabular data in a distributed setting
- G3 - Analyze the effect of non-i.i.d data on the performance of differentially private machine learning models
- G4 - Measure the privacy level of DP machine learning methods from the perspective of privacy attacks





- [1] July 2021
 - Research on local/global compressive differentially private federated learning
 - Research on comparison of JAX framework against Pytorch for privacy preserving federated learning ^[1]
 - Research on privacy preserving federated learning on Vantage6 framework ^[2]
 - Output: paper; Code + experiments
- [2] September 2021
 - Research on distributed DP synthetic data generation using VAEs
 - Research on distributed DP synthetic data generation using GANs
 - Output: paper; Code + experiments
- [3] October 2021
 - Research on effect of non-i.i.d data in privacy preserving and non-privacy preserving federated learning
 - Output: paper; Code + experiments (**repo ready**)
- [4] 2021 Q4, 2022 Q1
 - Research on extension of [2]
- [5] 2022 Q2
 - Utilization of the results of [3] in [2], [4]
- [6] 2022 Q2, Q3
 - Research on privacy analysis by measuring resiliency against privacy attacks

Thank you!