

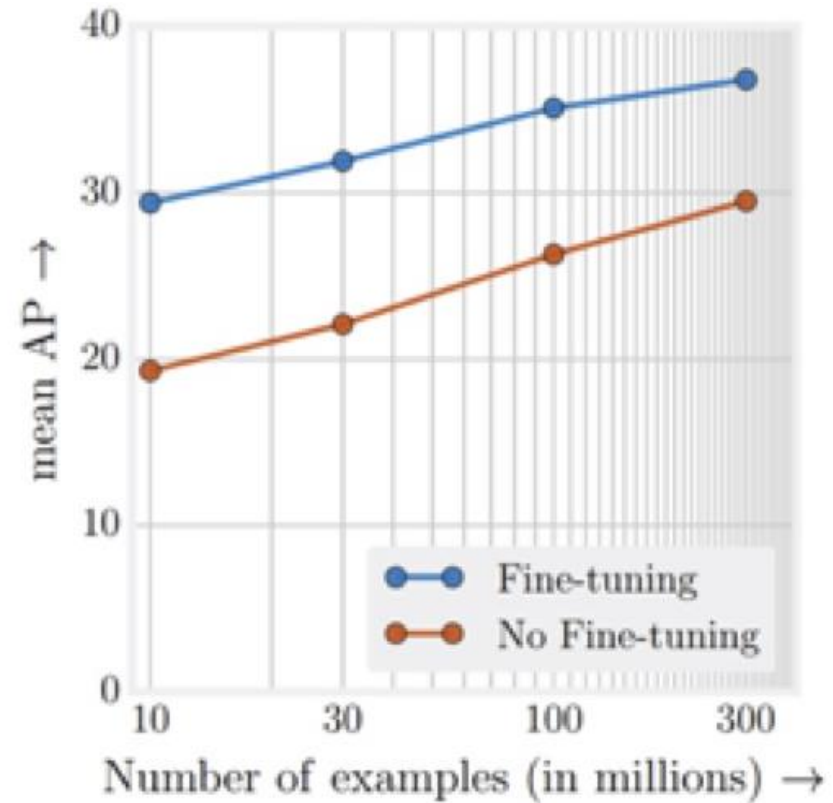
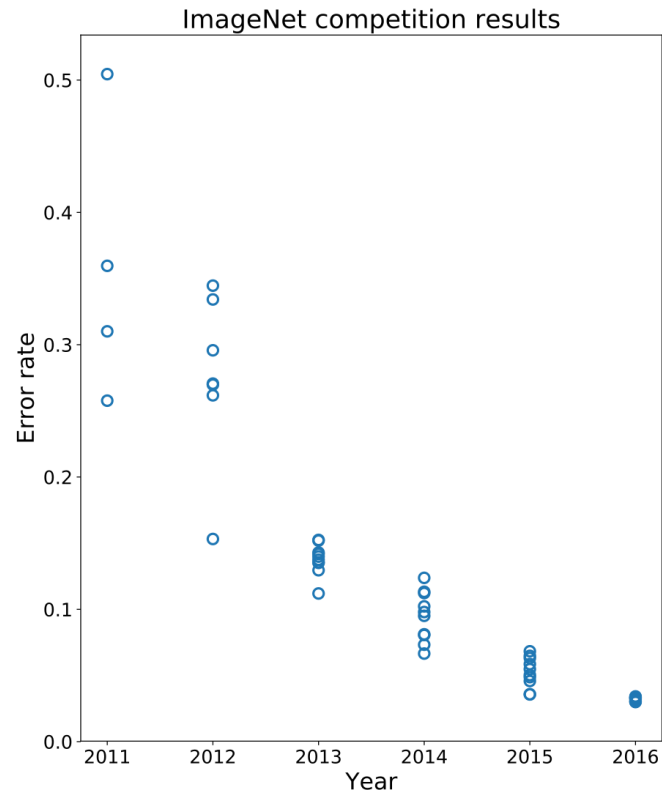
GDPR , Data Shortage and AI

Qiang Yang

Hong Kong University of Science and Technology

WeBank

AI and Big Data



**ImageNet performance over the years
From Wikipedia**

**“Revisiting Unreasonable Effectiveness of Data
in Deep Learning Era.” Google Research, 2017**

1. Most Applications Have Only Small Data

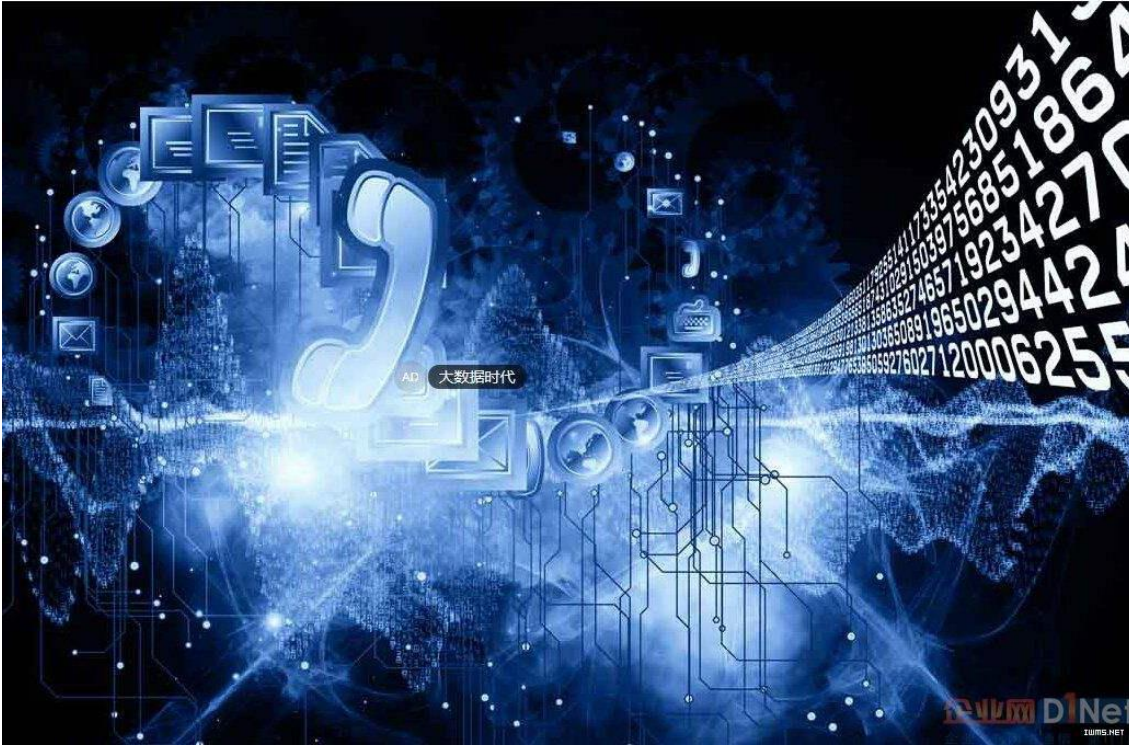
- Contract review law firms typically have annotated 10K - 20K of labeled contracts as samples (Bradley Arsenault, Electric Brain 2018)
- In finance industry, large loans are few, with only ~ 100 examples as typical samples (4paradigm.com, 2017)
- In medical image recognition, high-quality labeled data are few (A Survey on Deep Learning in Medical Image Analysis, Geert Litjens, et al. 2017 Arxiv.)

2. Data Sharing Among Parties: Difficult, Impossible or Immoral

- **Medical clinical trial data cannot be shared (by R. Stegeman 2018 on Genemetics)**
- **Our society demands more control on data privacy and security**
 - GDPR, Government Regulations
 - Corporate Security and Confidentiality Concerns
 - Data privacy concerns



Reality: Data often in form of Isolated Islands



What we expect: Big Data



What we see: Fragmented Data

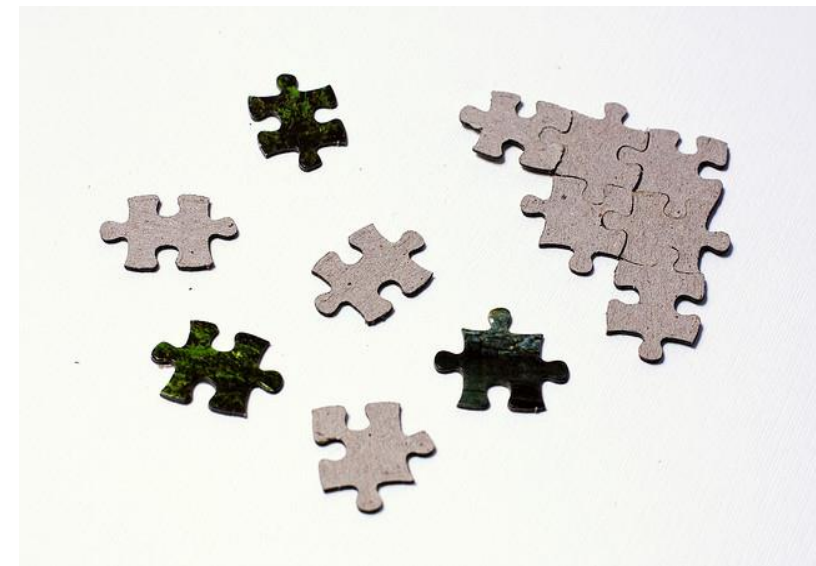
Two Challenges and Two Solutions

- Small Data

Transfer Learning from source task/domains to target tasks/domains

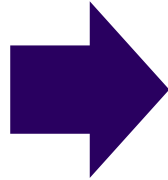
- Fragmented Data

Federated learning involving many parties collaboratively build models

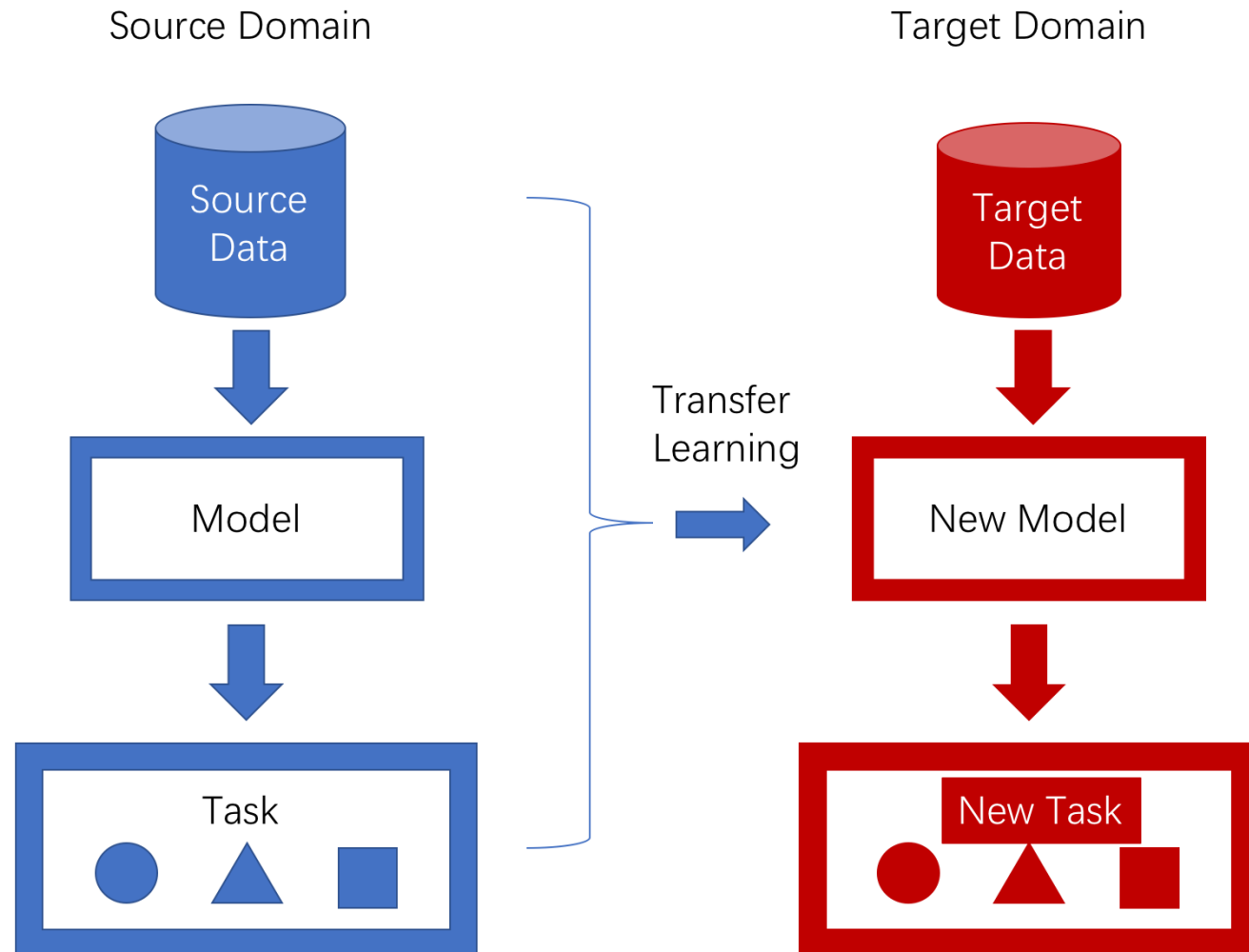


Often, these two problems occur together

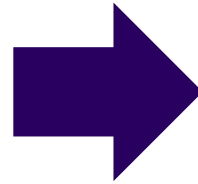
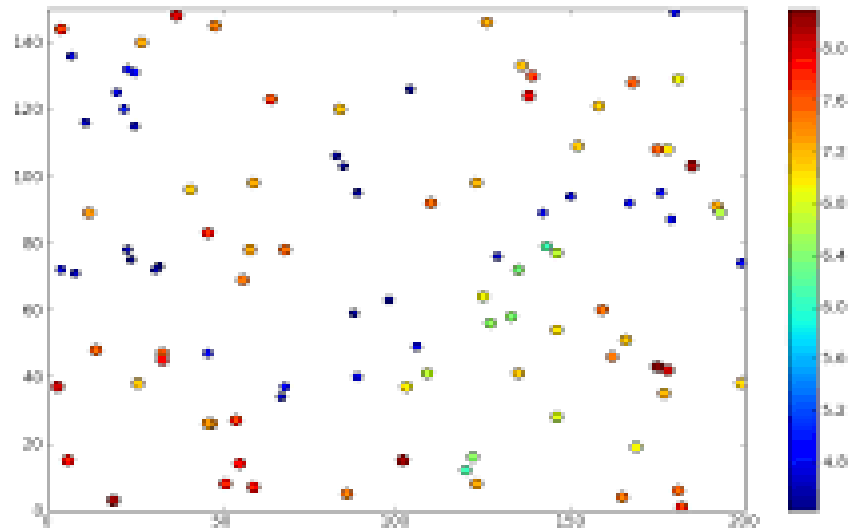
Transfer Learning



Transfer Learning Models



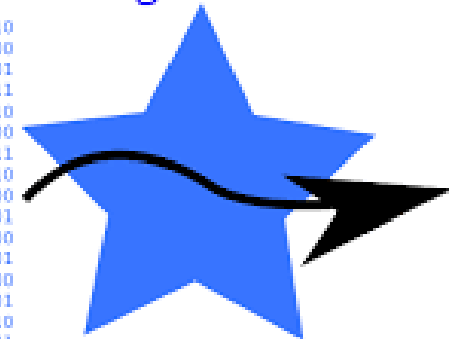
Why Transfer Learning? Small Data



Data

```
100100011101000000101000110111010110  
100100111101110000001111100110100100  
100001101101111101010011100001101001  
11111010000110111001010111100001011  
1100111110111111100100001110110110  
010000110100110110000110000100010000  
010101110011001111011001110100010111  
001000010101100101000001000010011110  
01110100111111001011101010101011100  
100010000101100010101101010111000101  
010010000100101011110011100001010000  
010110000010011101010010101110110001  
01101111010111100010100010100010000  
011010011011011010001000101111001101  
0001010000011001100011001000100010110  
100101010100010011100101010101111101
```

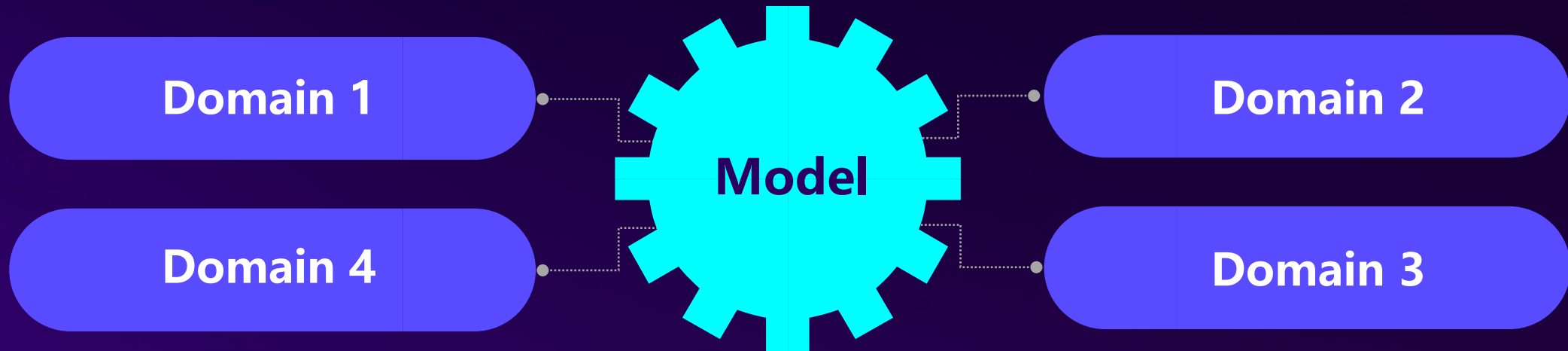
Algorithm



Model

$$f(\mathbf{x})$$

Why Transfer Learning : Reliability



Why Transfer Learning? Personalization



Learning to Transfer

Research issues

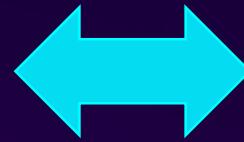
- When to transfer
- How to transfer
- What to transfer
- Learning how to learn by transfer learning



Key to Transfer Learning : Finding the Invariance



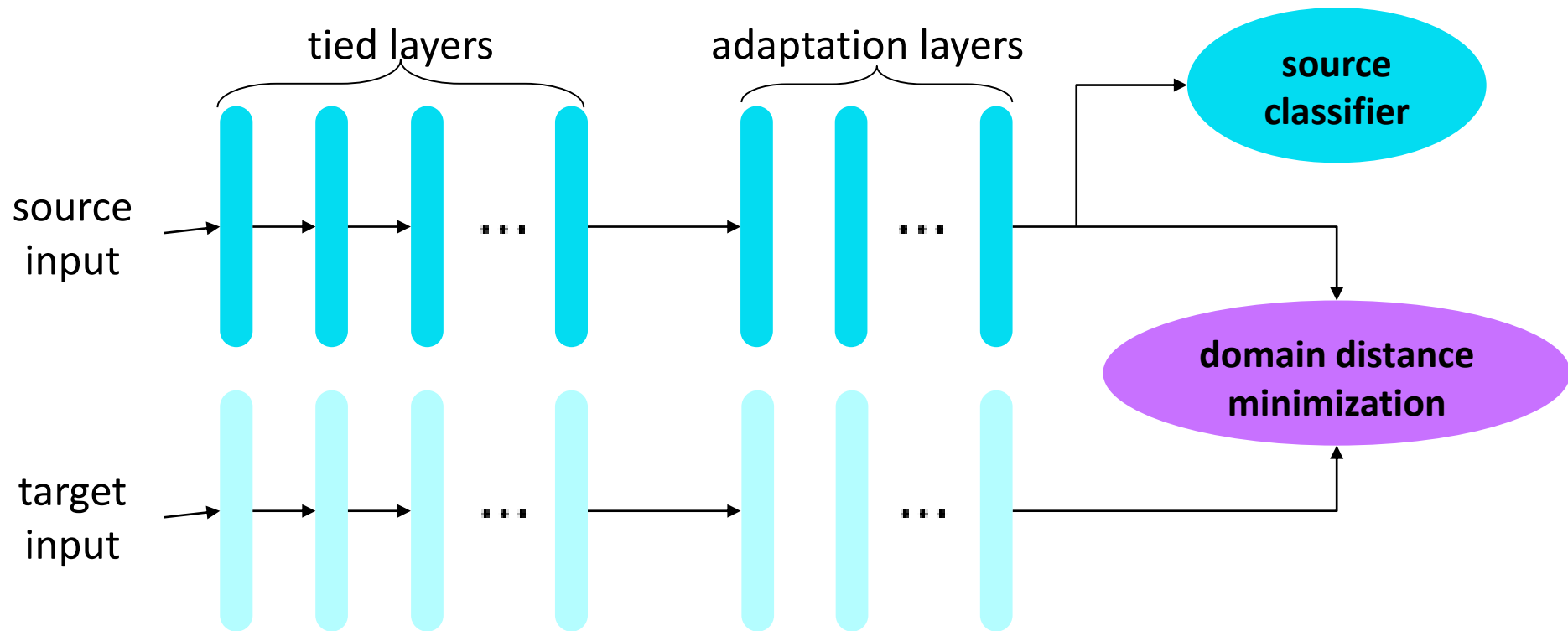
Driving in Mainland China



Driving in Hong Kong SAR, China

Transfer Learning in a Deep Model

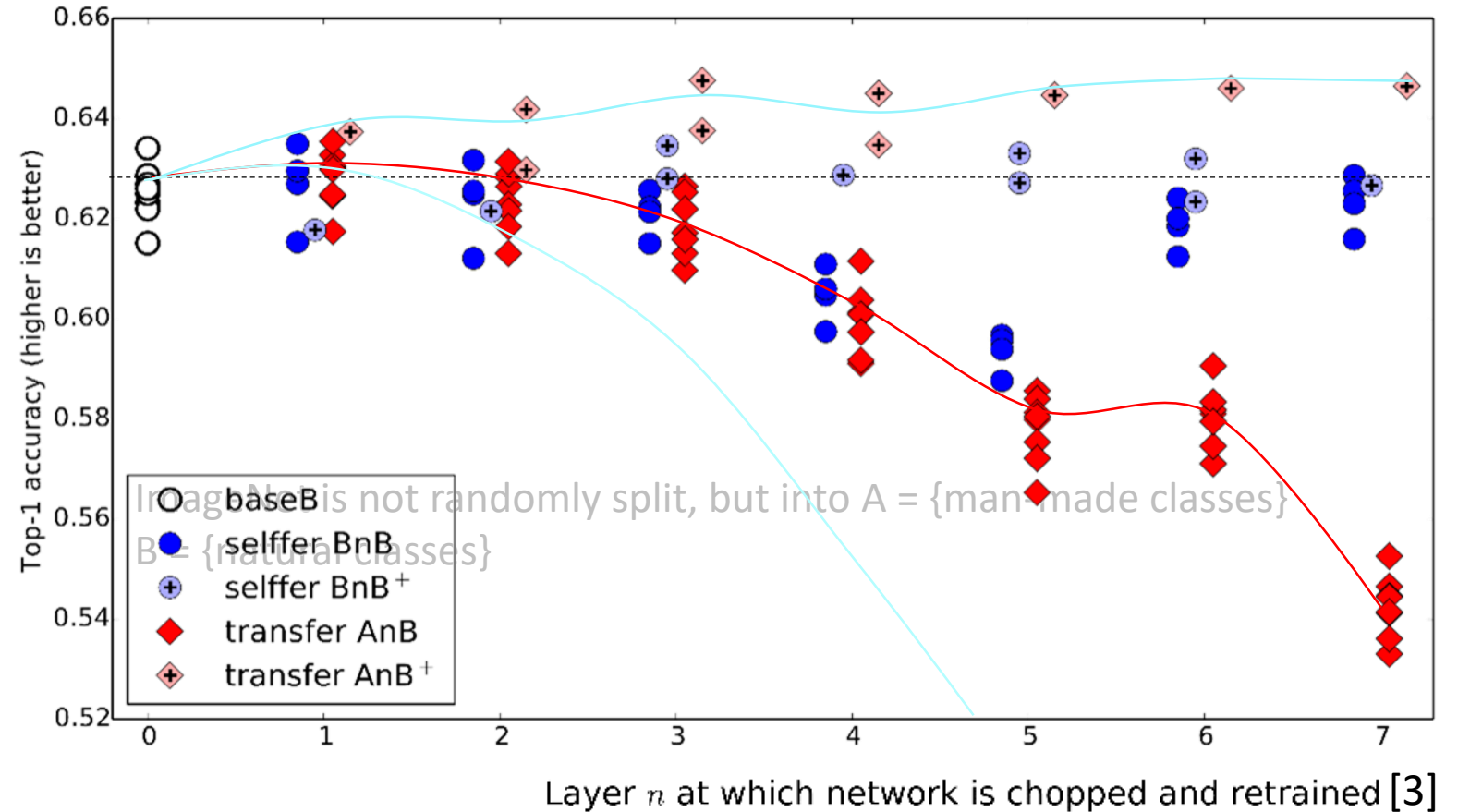
- **Objective** $\mathcal{L} = \mathcal{L}_{\text{source}} + \mathcal{L}_{\text{distance}}$



Learning transferable features with deep adaptation networks. M Long, Y Cao, J Wang, MI Jordan. International Conference on Machine Learning (ICML) 2015

Transfer Learning in a Deep Model

A Quantitative Study



Conclusion: lower layer features are more general and transferrable, and higher layer features are more specific and non-transferrable.



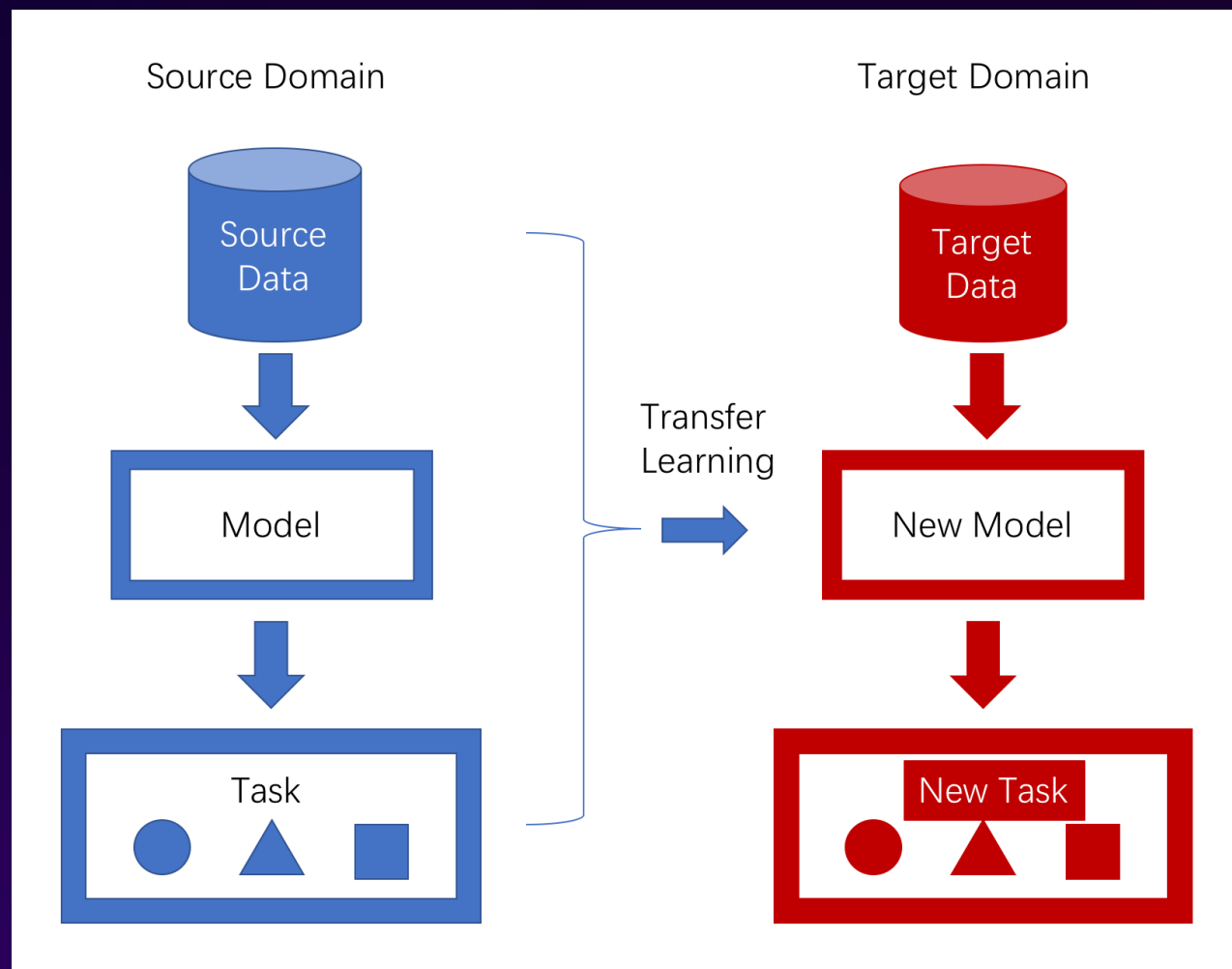
Transfer Learning Setting I :

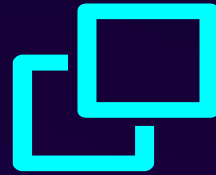
- Source domain: sufficient labeled data
- Target domain: no labeled data
- Domain Adaptation



Transfer Learning Setting II :

- Source domain: sufficient labeled data
- Target domain: little labeled data
- Supervised Transfer Learning





Transfer Learning Setting I

Source domain: sufficient labeled data

Target domain: no labeled data

Sentiment Analysis

rating

★ 10/10



This movie will **blow your mind** and break your heart - and make you desperate to go back for more. **Brave, brilliant and better** than it has any right to be.

shawneofthedead 25 April 2018

Over the past decade, Marvel has earned itself the benefit of the doubt. The studio has consistently delivered **smart, funny, brave films** that both embrace and transcend their comic-book origins. The 18 blockbuster movies produced since Iron Man first blasted off into the stratosphere in 2008 have not only reinvented superhero films as a genre - they've helped to legitimise it. Indeed, Marvel's two most recent films - Thor: Ragnarok and Black Panther - have received the kind of accolades usually reserved for edgy arthouse flicks.

rating

★ 1/10



I actually **laughed out loud** at the end

tenaciouspeas 23 May 2018

What a trash heap of a movie. I thought about giving it 2 stars because there were a couple of things that made me chuckle but I left the theater **so irritated** that I talked myself out of it. I kept singing the "I don't care" song for the last 2 hours of this movie, which seemed to last at least 5 hours long. I'm sure they could have fit at least 2 more bad CGI action fight scenes in there, to make it 6 hours long. I loved the first Avengers. I loved Thor Ragnarok. I **hated this movie** which can easily be summed up: A really long movie about a boring CGI character titled: Here's Thanos!

44 out of 80 found this helpful. Was this review helpful? | [Report this](#)

➤ Single-Domain Solution

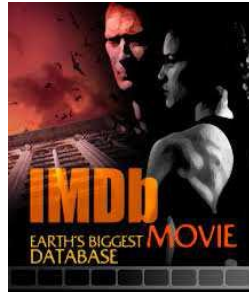
depends on sufficient labeled data

➤ Cross-domain solution: Transfer Learning

Transferring sentiment classification knowledge from one domain to another

Cross-Domain Features: Pivots

Source domain (**Movie**)



Target domain (**Electronics**)






	Great movie. His characters are engaging and thoughtful .	This great touchpad feels glossy and is responsive .
	It's a excellent , sobering drama.	It is very lightweight , excellent transition from PC.
	An terrible movie. It is very plotless and insipid .	It is blurry and fuzzy in very dark setting. So terrible HP.



Domain adaptation with structural correspondence learning, Blitzer et al. EMNLP 2006

Movie

	engaging thoughtful responsive glossy	Sobering lightweight	Plotless insipid Blurry fuzzy
	1	0	0
	0	1	0
	0	0	1






Training

$$y=f(\mathbf{x}) = \text{sgn}(\mathbf{w}\mathbf{x}^T), \mathbf{w} = [1, 1, -1]$$



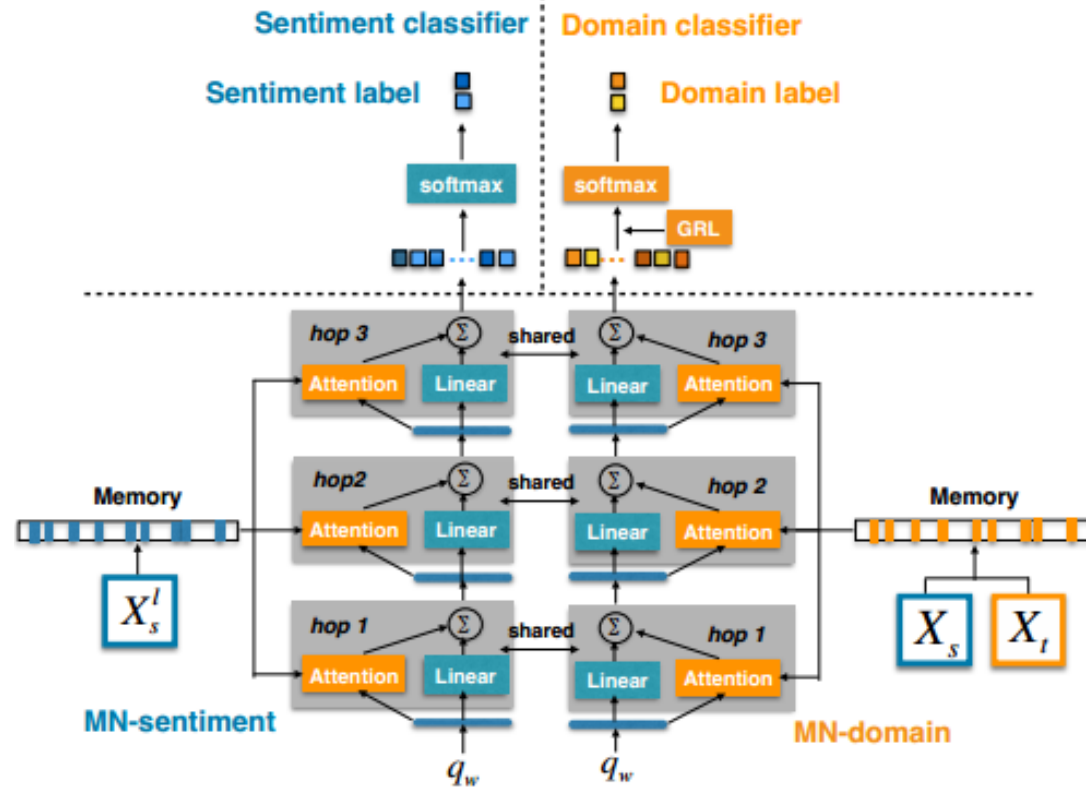
Prediction

Electronics

	engaging thoughtful responsive glossy	Sobering lightweight	Plotless insipid Blurry fuzzy
	1	0	0
	0	1	0
	0	0	1

An Adversarial Approach

Sentiment Classification Domain Classification



Domain Classification Objective:
Maximize domain classification error

Source data X_s
Target data X_t

S

Movie

Great movie. His characters are
engaging and thoughtful.

T

Electronics

This great touchpad feels glossy
and is responsive.

Li, Zheng, Qiang Yang, et al. "End-to-end adversarial memory network for cross-domain sentiment classification." IJCAI 2017.

Comparison with baseline methods

✓ Traditional methods:

SCL: Structural Correspondence Learning [Blitzer et al., 2006]

SFA: Spectral Feature Alignment [Pan et al., 2010]

✓ AMN model significantly outperforms the traditional methods SFA and SCL on Amazon Reviews Dataset

GT:1 Prediction:1
great dvd media i have burned over 100 of these in the past 6 months i have only had 1 burn badly havent found a dvd player yet that they wont play in

GT:1 Prediction:1
good for canon a95 **fantastic** take all the videos and pictures you want with the best quality

GT:1 Prediction:1
 you cannot beat a belkin cable **great** quality **excellent** construction and strong rj45 plugs i have worked with a decent share of cat5 and i have never had to cut and terminate a belkin cable due to regular wear and tear

GT:0 Prediction:0
 i **cant** hear you sound output is **terrible** you cant hear it in a car or airplane with high quality noise cancelling earphones when i called customer service they told me it was not intended for use in a car or airplane picture is very good but i have heard better sound from much cheaper players dont waste your money

GT:0 Prediction:0
 great technology **terrible** customer experience i had the same exact experience with the **poor** fit of these headphones and the rude customer service their surround sound he592 phones dont fit well either

GT:0 Prediction:0
uncomfortable i had these headphones for a few years then they got crushed in half in my bag they hurt your ears after about ten minutes they are durable though i would recommend the kind that clip behind your ear

(a) Electronics domain

GT:1 Prediction:1
great gifts i love the rapid ice wine coolers i give them for token gifts and use them frequently myself they are **great** for a spure of the moment glass of wine that needs chilling

GT:1 Prediction:1
 an **elegant** way of serving its a traditional serve ware for serving the soup course the color of the tureen set allows it to be used with many of the dinnerwares amp the size is adequate to serve at least 810 people the under plate is something not found with usual tureen sets which gives it an **elegant** look but it appears a little overpriced

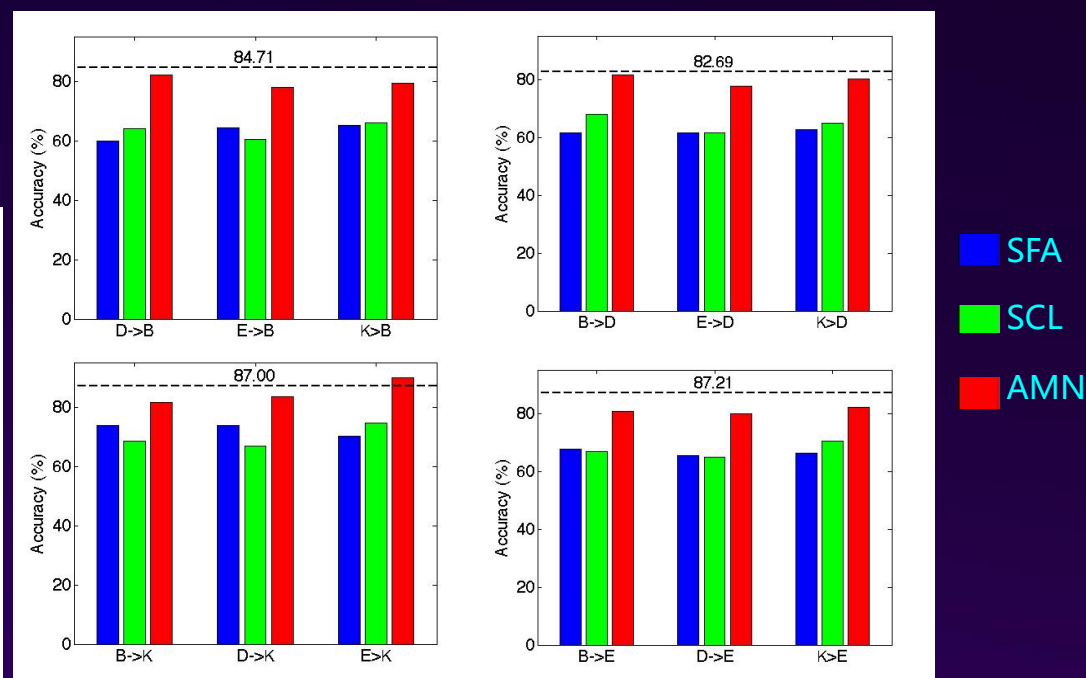
GT:1 Prediction:1
gorgeous i just received this as a wedding gift and it is beautiful a great gift

GT:0 Prediction:0
disappointed whisker i am usually very pleased with oxo products but this one is a big disappointment i have not found it to be good for or at anything wished id saved the five bucks

GT:0 Prediction:0
 too **poorly** made for everyday use we have a full line of fiesta dishware and thought having the matching flatware would be nice after a year of standard use and dishwashing about 13 of the flatware is **unusable** the upside is that it is cheap and replaceable but count me among those who would rather pay more for something that lasts we are in the process of ditching the fiesta flatware line and moving to something more robust

GT:0 Prediction:0
 totally **useless** we bought this to use at events for a chocolate themed group at college and used it several times before giving up

(b) Kitchen domain



Recommendation System

Supervised learning based RecSys

Single Domain RecSys

- Easy to get stuck in local optimal and keeps recommending the similar articles.
- Performs poor for new user, new article, and new domain.

- Insensitive to fast evolving user interests.
- Purely explores leading to worse short-term CTR.

Transferrable Contextual Bandit

王者荣耀里五个单体伤害最高的英雄，他曾经一个技能秒掉后羿！

天云解说



刚刚，苹果扔出重磅炸弹，华为或要哭了！

老板思维首府



终于看懂了，《天龙八部》原来就是一场杀人游戏

好友都在读 六神器磊谈金庸



王者荣耀里五个单体伤害最高的英雄，他曾经一个技能秒掉后羿！

天云解说



王者荣耀里五个单体伤害最高的英雄，他曾经一个技能秒掉后羿！

天云解说



王者荣耀里五个单体伤害最高的英雄，他曾经一个技能秒掉后羿！

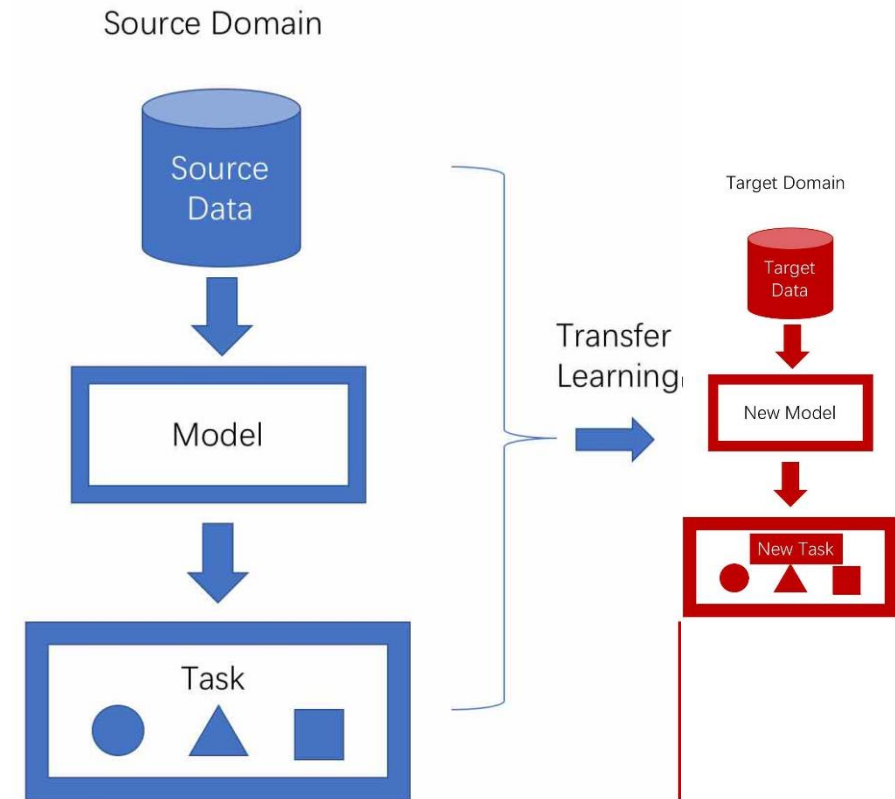
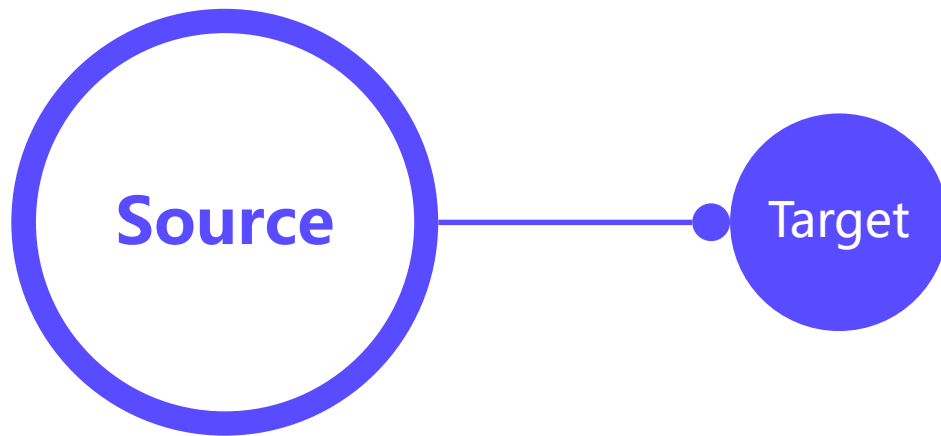
天云解说



Transferable Contextual Bandit for Cross-Domain Recommendation, Bo Liu, Yu Zhang, Qiang Yang et al. AAAI18

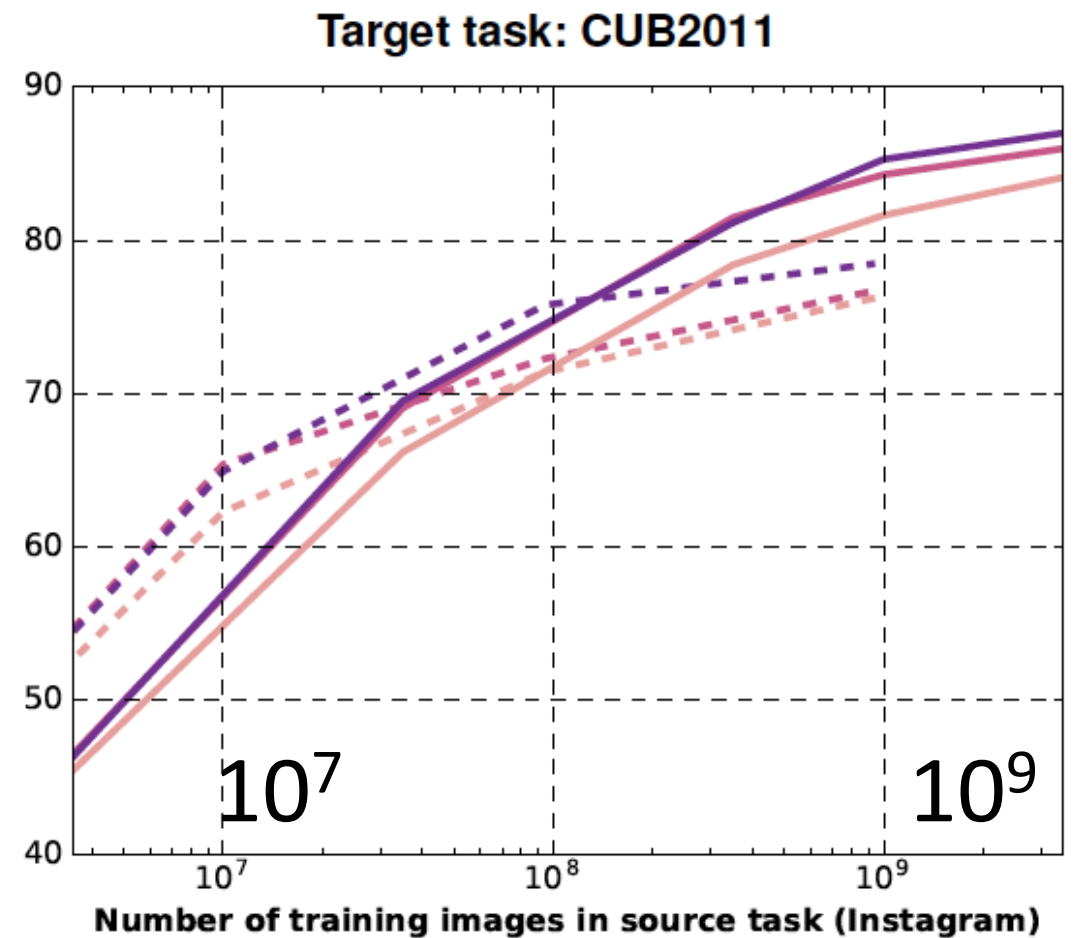
Trend in Transfer Learning : Using Huge Pretrained Model

- Source domain: **huge** labeled or unlabeled data
- Target domain: few labeled data
- Objective: transfer model from source domain to target domain **for same or different tasks**



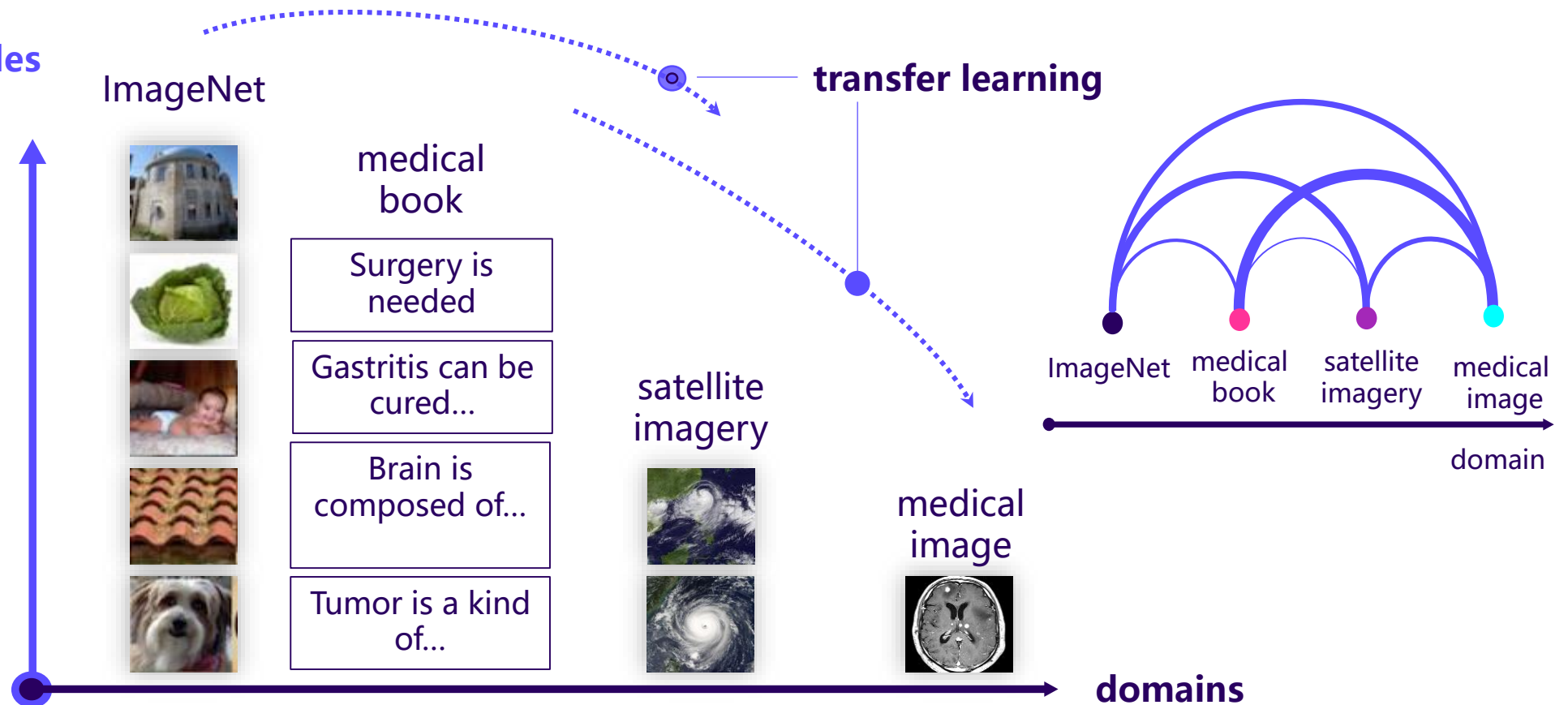
Source-Data Scale Matters in Transfer Learning (image)

- Dhruv Mahajan, et al.: **Exploring the Limits of Weakly Supervised Pretraining**. ECCV (2) 2018
- "Without manual dataset curation or sophisticated data cleaning, models trained on billions of Instagram images using thousands of distinct hashtags as labels exhibit excellent transfer learning performance"



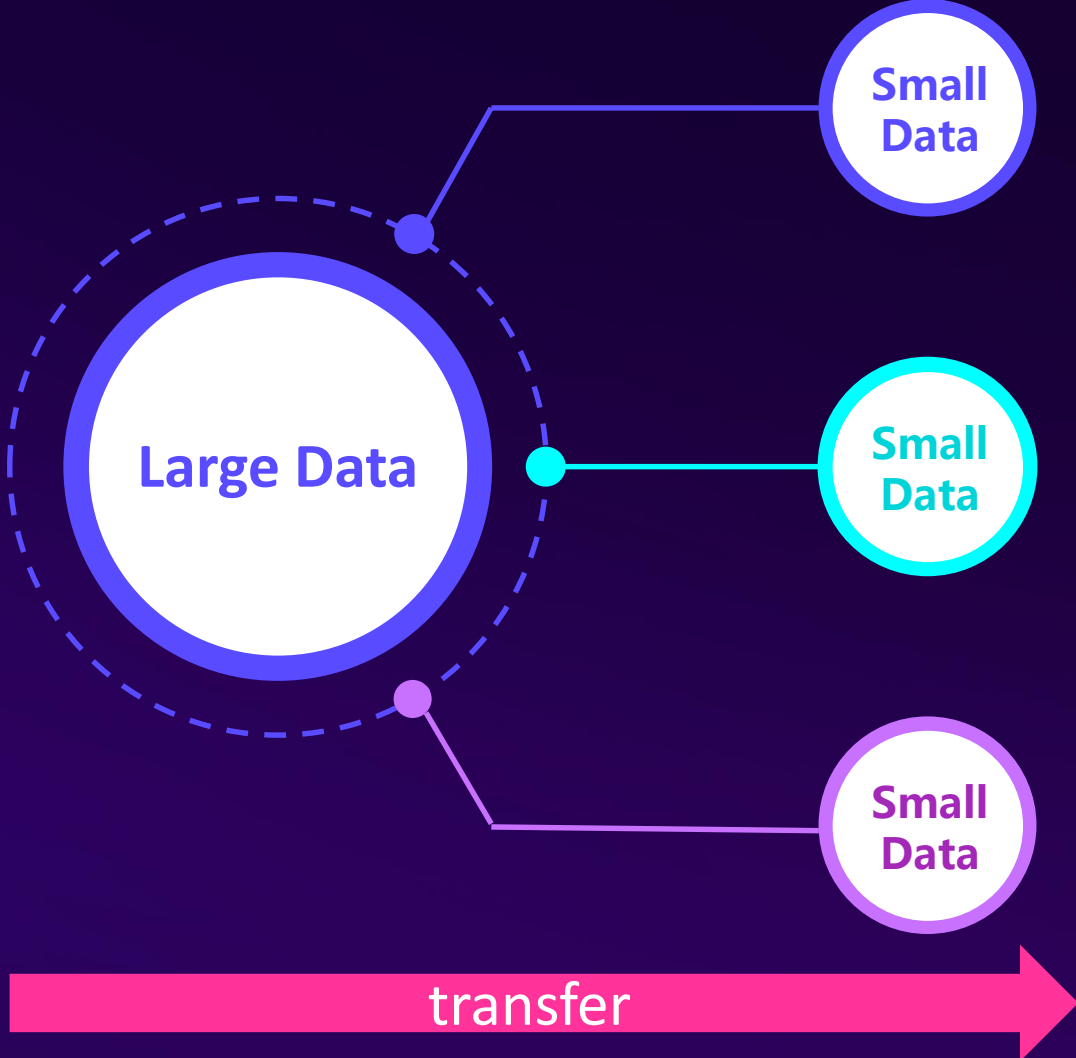
Transfer Learning via Learning to Transfer

labeled examples

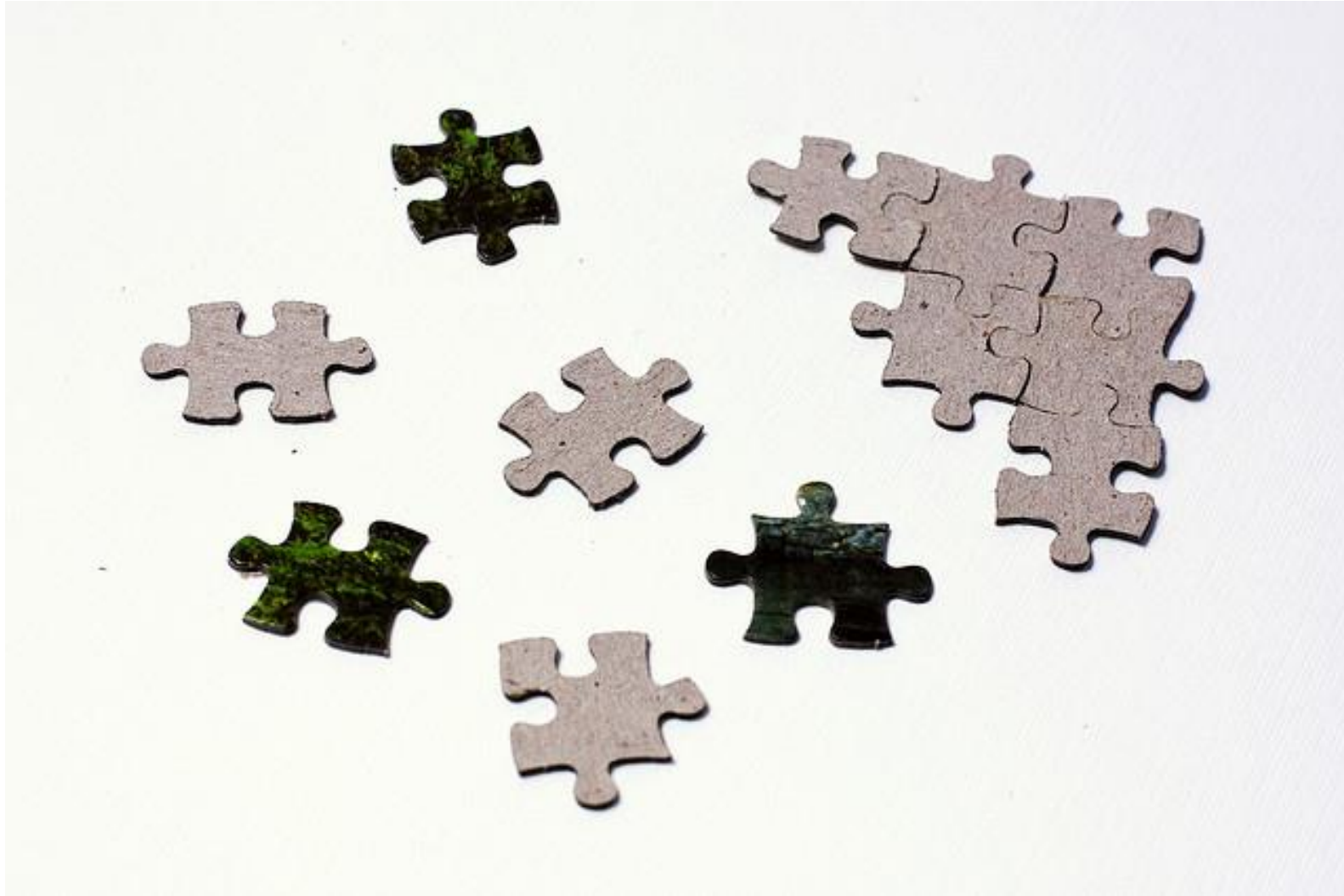


Transfer Learning via Learning to Transfer, Ying Wei, Qiang Yang et al. ICML 2018

Transfer Learning from Large Data to Small Data



Next Problem: Data Are Fragmented



Challenges to AI: Data Privacy and Confidentiality

Facebook's data privacy scandal

Market summary > Facebook, Inc. Common Stock
NASDAQ: FB - Mar 19, 2:21 PM EDT

172.32 USD ↓12.77 (6.90%)



Open	177.01	Mkt cap	500.59B
High	177.17	P/E ratio	27.97
Low	170.06	Div yield	-

Brian Acton
@brianacton [Follow](#)

It is time. [#deletefacebook](#)

4:00 PM - 20 Mar 2018

10,390 Retweets 20,530 Likes

2019/1/19

FTC reportedly planning 'record-setting' fine against Facebook for mishandling user data

Chance Miller - Jan. 20th 2019 7:31 am PT [@ChanceHMiller](#)

- In 2012, the FTC fined Google \$22.5 million over failing to improve privacy practices – a record for such a punishment.
- The Washington Post says that the fine against Facebook is expected to be “much larger.”

- More than 50 million people affected
- UK assessed a £500,000 fine to Facebook
- the worst single-day market value decrease for a public company in the US, dropping \$120 billion, or 19%

The General Data Protection Regulation (GDPR)



- No Autonomous Modeling and Decision
- Interpretability of Model Decisions
- Users' Right for Data to be Forgotten
- Data Privacy By Design
- Explicit Consent for Data Usage

California Consumer Privacy Act (CCPA)

- Takes effect in 2020
- grants consumers the right to know what information is collected and **whom it is shared with**
- Consumers will have the option of barring tech companies from selling their data
- Provides some of the strongest **regulations in the USA.**



China's Data Cyber Security Law

- Enacted in 2017
- Requires that Internet businesses must not leak or tamper with the personal information
- When conducting data transactions with third parties, they need to ensure that the proposed contract follow legal data protection obligations.
- More to come...

From Report by KPMG 2017

Highlights and interpretation of the Cybersecurity Law



Highlights of the Cybersecurity Law

Comprising 79 articles in seven chapters, the Cybersecurity Law contains a number of cybersecurity requirements, including safeguards for national cyberspace sovereignty, protection of critical information infrastructure and data and protection of individual privacy. The Law also specifies the cybersecurity obligations for all parties. Enterprises and related organisations should prioritise the following highlights of the Cybersecurity Law:



Personal information protection

The Cybersecurity Law clearly states requirements for the collection, use and protection of personal information.



Critical information infrastructure

The Cybersecurity Law frequently mentions the protection of "critical information infrastructure".



Network operators

"Network operators" are the owners and administrators of networks and network service providers. The Cybersecurity Law clarifies operators' security responsibilities.



Preservation of sensitive information

The Cybersecurity Law requires personal information/important data collected or generated in China to be stored domestically.



Certification of security products

Critical cyber equipment and special cybersecurity products can only be sold or provided after receiving security certifications.



Legal liabilities

Enterprises and organisations that violate the Cybersecurity Law may be fined up to RMB1,000,000.

Challenges to AI : small data and fragmented data



Low Security in Data Sharing
Lack of Labeled Data
Segregated Datasets

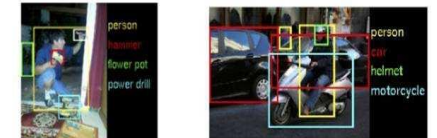
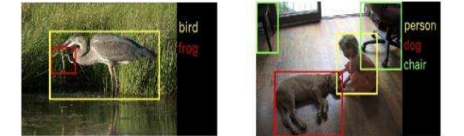


Enterprise A

X1



Data silos



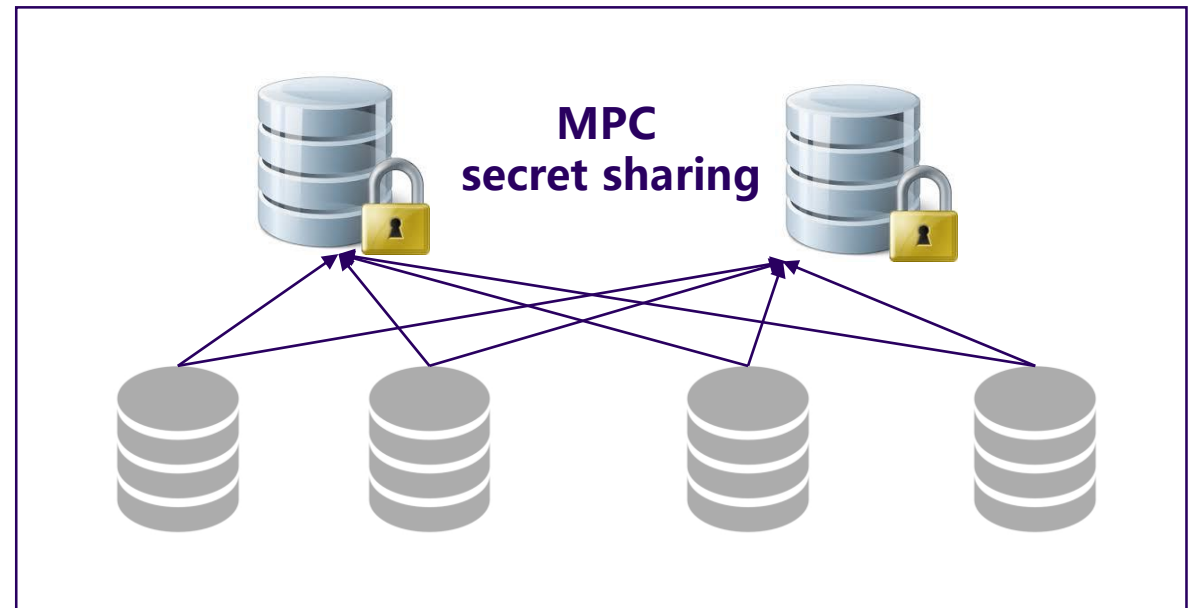
Enterprise B

(X2, Y)

Over 80% of enterprises' information in data silos!

SecureML : Privacy-preserving machine learning for linear regression, logistic regression and neural network training

- Combines secret sharing, garbled circuits and oblivious transfer
- Learns via two un-trusted, but non-colluding servers
- Computationally expensive



Mohassel, P., & Zhang, Y. (2017, May). SecureML: A system for scalable privacy-preserving machine learning. In *2017 38th IEEE Symposium on Security and Privacy (SP)* (pp. 19-38). IEEE.

Homomorphic Encryption

- Full Homomorphic Encryption and Partial Homomorphic Encryption.
- **Paillier** partially homomorphic encryption

$$\begin{aligned} \textit{Addition:} \quad & [[u]] + [[v]] = [[u+v]] \\ \textit{Scalar multiplication:} \quad & n[[u]] = [[nu]] \end{aligned}$$

- For public key $pk = n$, the encoded form of $m \in \{0, \dots, n - 1\}$ is

$$\text{Encode}(m) = r^n (1 + n)^m \bmod n^2$$

r is randomly selected from $\{0, \dots, n - 1\}$.

- For float $q = (s, e)$, encrypt $[[q]] = ([[s]], e)$, here $q = s\beta^e$ is base- β exponential representation.

Rivest, R. L.; Adleman, L.; and Dertouzos, M. L. 1978. On data banks and privacy homomorphisms. Foundations of Secure Computation, Academia Press 169–179.

Applying HE to Machine Learning

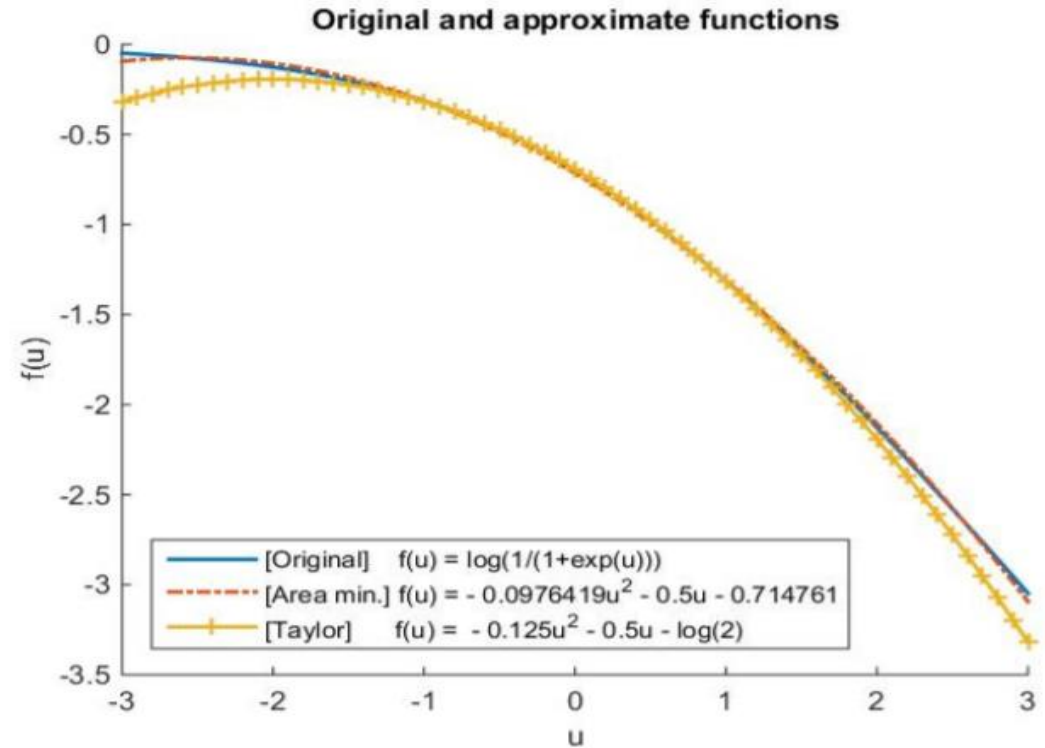
Polynomial approximation for logarithm function

$$\log\left(\frac{1}{1+\exp(u)}\right) \approx \sum_{j=0}^k a_j u^j$$

Encrypted computation for each term in the polynomial function

$$\text{loss} = \log 2 - \frac{1}{2} y w^T x + \frac{1}{8} (w^T x)^2$$

$$[[\text{loss}]] = [[\log 2]] + \left(-\frac{1}{2}\right) * [[y w^T x]] + \frac{1}{8} [[(w^T x)^2]]$$



- Kim, M.; Song, Y.; Wang, S.; Xia, Y.; and Jiang, X. 2018. Secure logistic regression based on homomorphic encryption: Design and evaluation. JMIR Med Inform 6(2)
- Y. Aono, T. Hayashi, T. P. Le, L. Wang, Scalable and secure logistic regression via homomorphic encryption, CODASPY16

Is the Gradient Info Safe to Share?

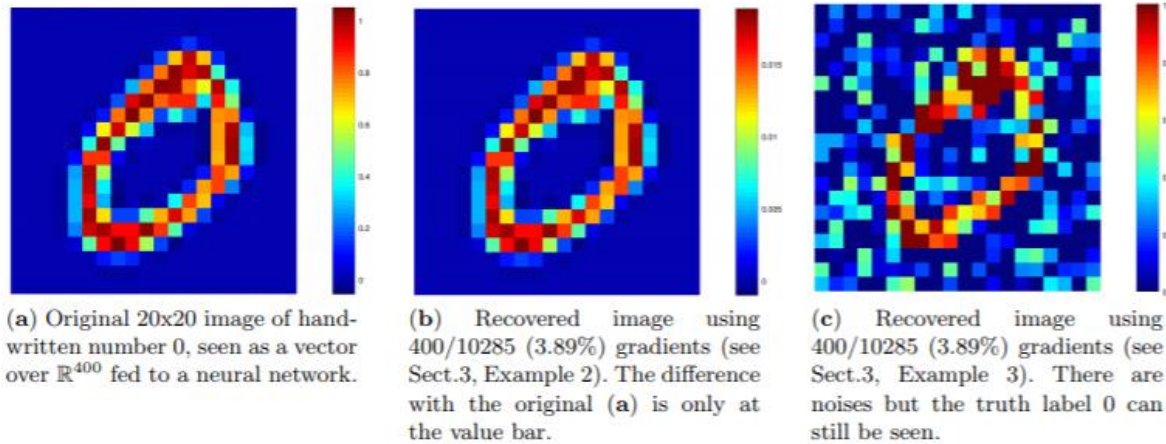
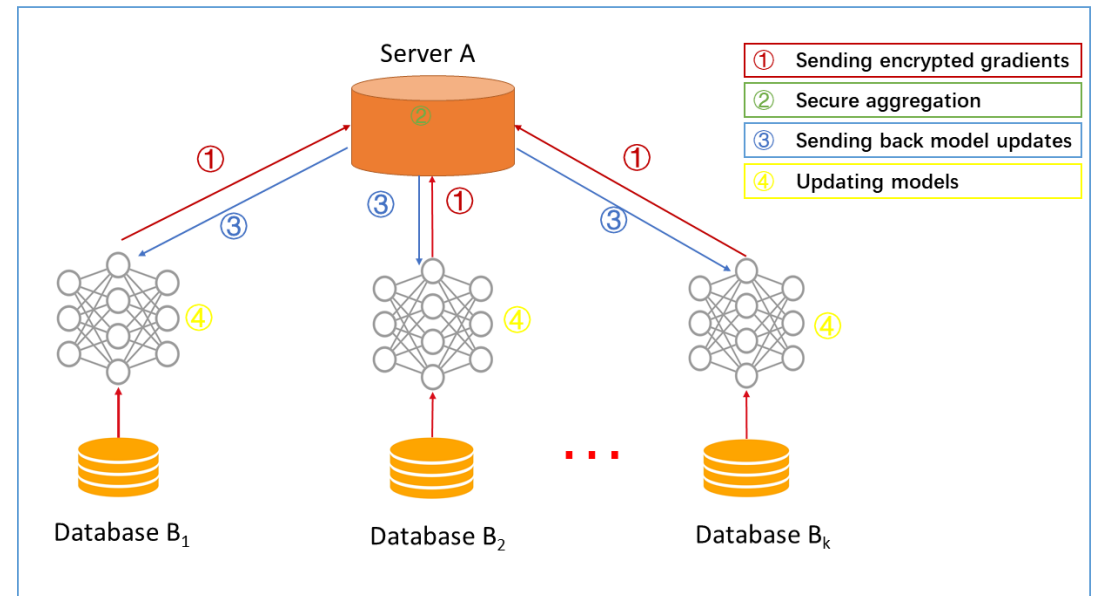


Fig. 3. Original data (a) vs. leakage information (b), (c) from a small part of gradients in a neural network.

Protect gradients with Homomorphic Encryption



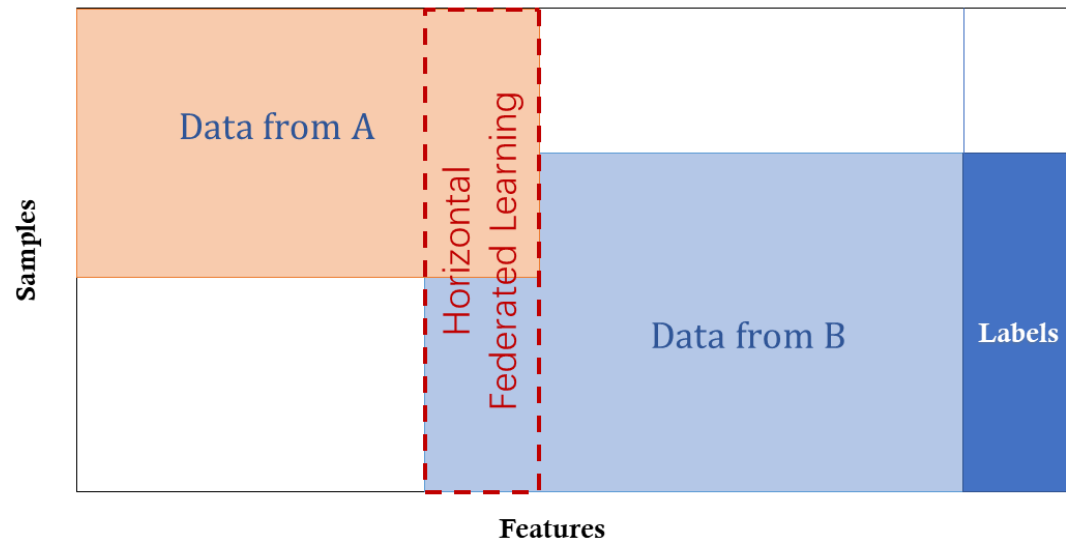
- Le Trieu Phong, et al. 2018. Privacy-Preserving Deep Learning via Additively Homomorphic Encryption. IEEE Trans. Information Forensics and Security , 13, 5 (2018),1333–1345

- **Algorithm ensures that no information is leaked to the semi-honest server, provided that the underlying additively homomorphic encryption scheme is secure*.**

* Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: concepts and applications, ACM TIST, ,2018

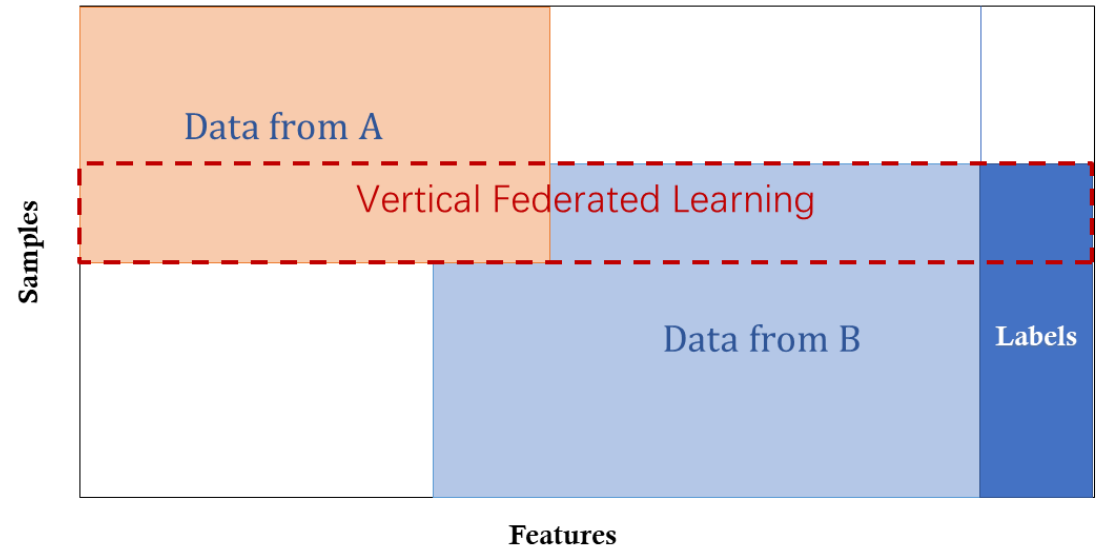
Categorization of Federated Machine Learning

Horizontal FML



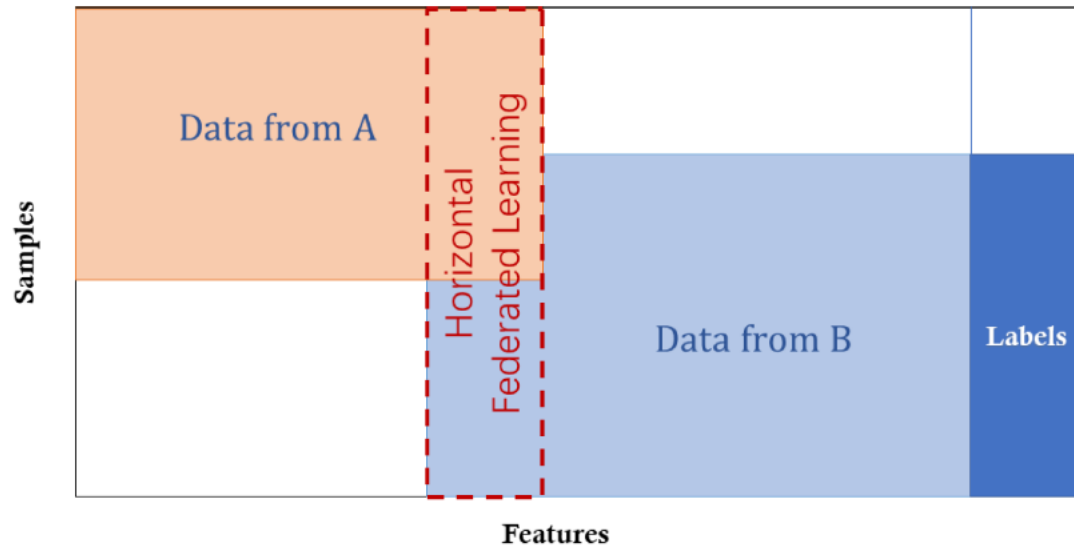
Large overlap of **features** of the two data sets

Vertical FML



Large overlap of **sample IDs (users)** of the two data sets

Horizontal Federated Learning: Divide by Users/Samples



(a) Horizontal Federated Learning

FEDERATED LEARNING FOR MOBILE KEYBOARD PREDICTION, Andrew Hard, et al., Google, 2018

Step 1: Participants compute training gradients locally

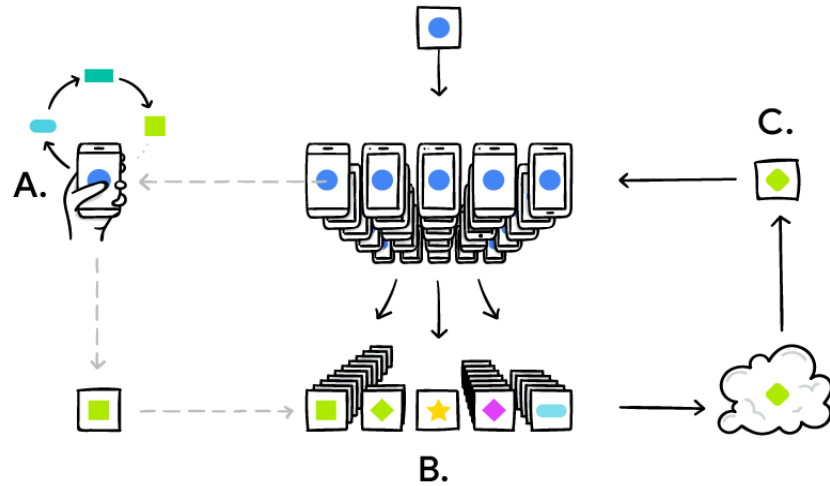
- mask gradients with encryption, differential privacy, or secret sharing techniques
- all participants send their masked results to server

Step 2: The server performs secure aggregation without learning information about any participant

Step 3: The server sends back the aggregated results to participants

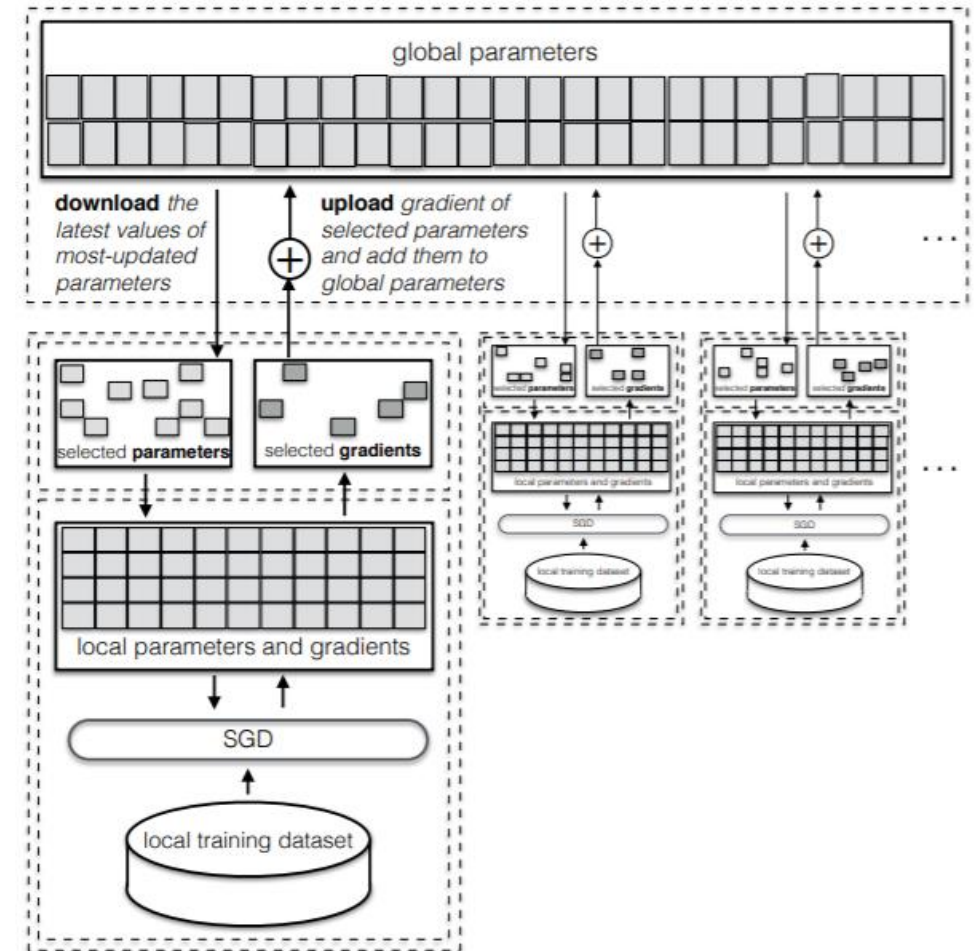
Step 4: Participants update their respective model with the decrypted gradients

Horizontal Federated Learning



H. Brendan McMahan et al, *Communication-Efficient Learning of Deep Networks from Decentralized Data*, Google, 2017

- **Multiple clients, one server**
- **Data is horizontally split across devices, homogeneous features**
- **Local training**
- **Selective clients**



Reza Shokri and Vitaly Shmatikov. 2015. *Privacy-Preserving Deep Learning*. In Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS ' 15). ACM, New York

Vertical Federated Learning

Objective:

- Party (A) and Party (B) co-build a FML model

Assumptions :

- Only one party has label Y
- Neither party wants to expose their X or Y

Challenges:

- Parties with only X cannot build models
- Parties cannot exchange raw data by law

Expectations :

- Data privacy for both parties
- model is LOSSLESS



ID	X1	X2	X3	ID	X4	X5	Y
U1	9	80	600	U1	6000	600	No
U2	4	50	550	U2	5500	500	Yes
U3	2	35	520	U3	7200	500	Yes
U4	10	100	600	U4	6000	600	No
U5	5	75	600	U8	6000	600	No
U6	5	75	520	U9	4520	500	Yes
U7	8	80	600	U10	6000	600	No

Retail A Data

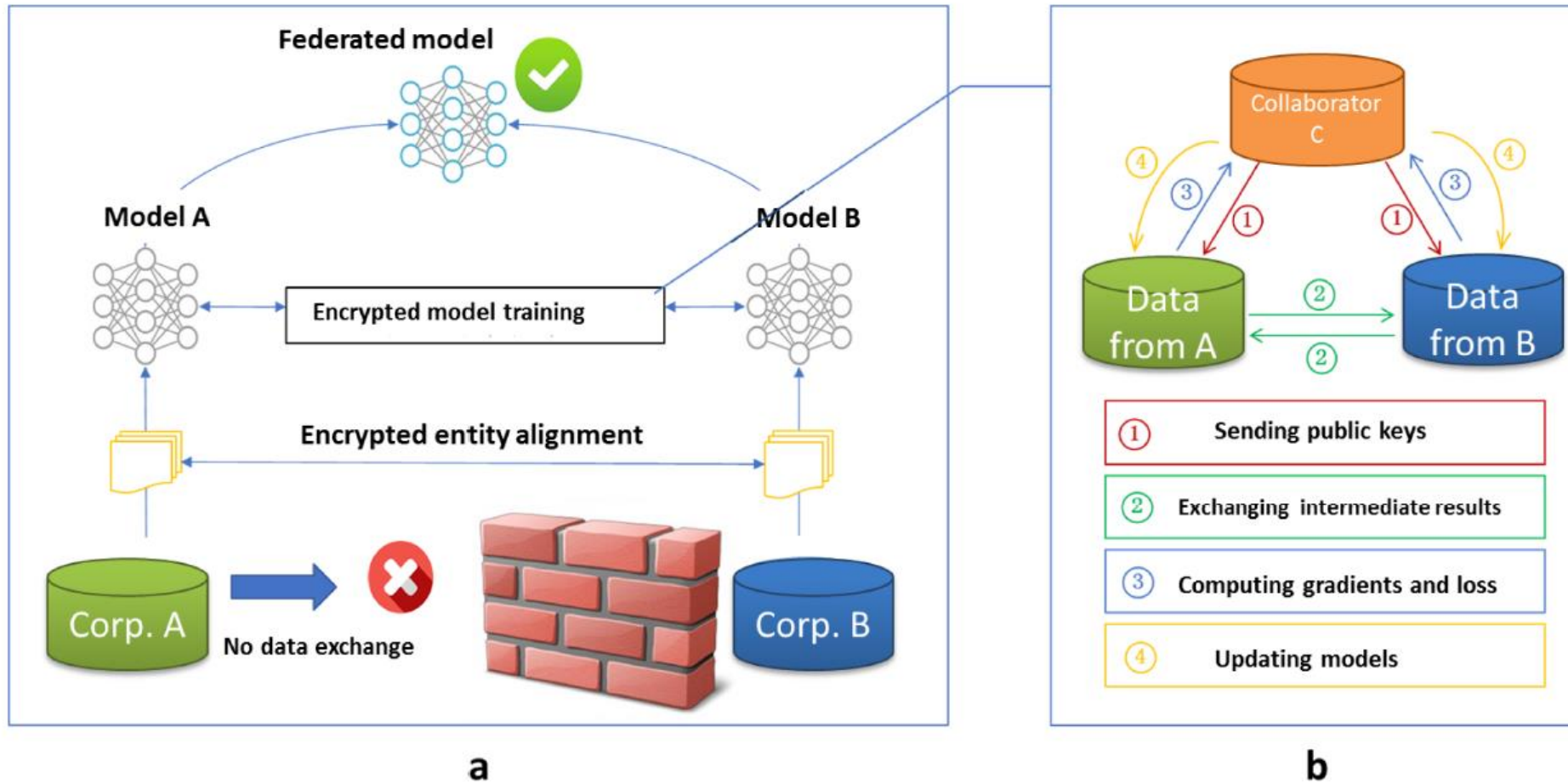
Bank B Data

Privacy-Preserving Entity Match

- Party A and B learns their overlapping IDs but nothing else

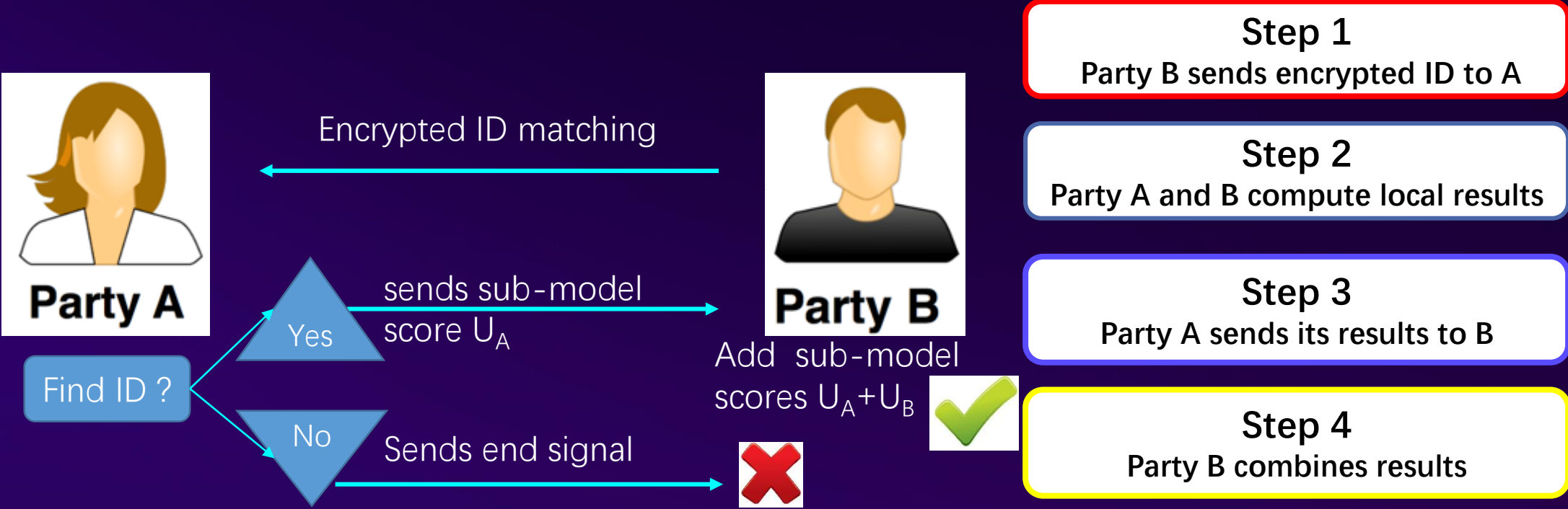


Vertical Federated Learning



Privacy-Preserving inference

- Suppose a new user ID arrives at Party B,



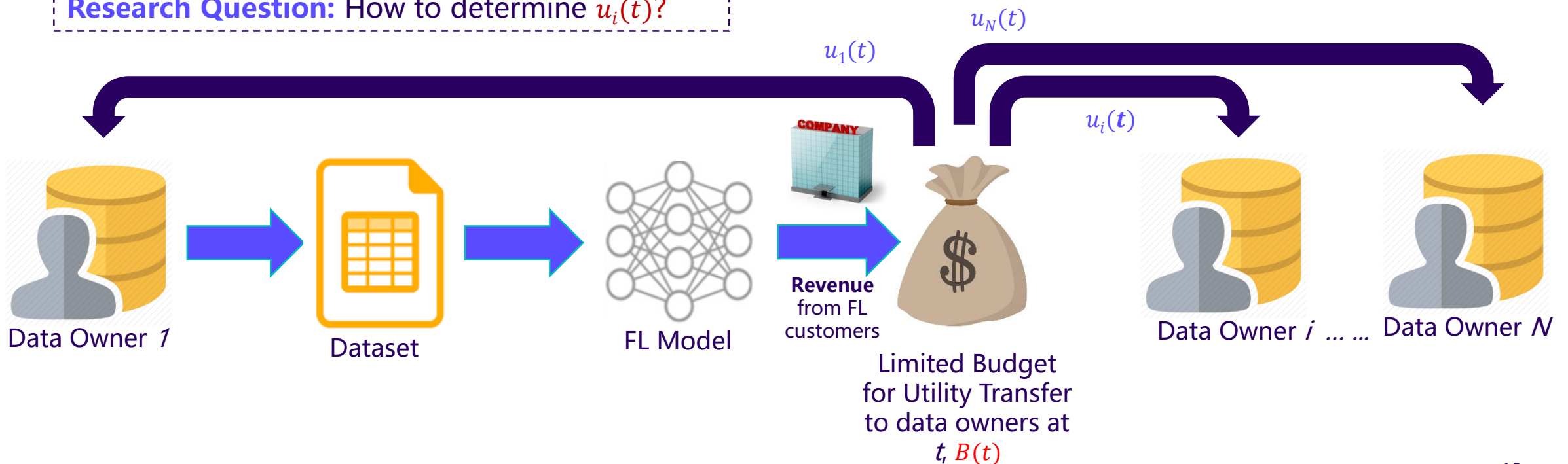
Security Analysis

- Security against third-party C
 - all C learns are the masked gradients and the randomness and secrecy of the masked matrix are guaranteed
- Security against each other
 - Party A learns its gradient at each step, but this is not enough for A to learn any information from B
 - inability of solving n equations in more than n unknowns
- Security in the semi-honest setting

Incentivize Parties to Join: Federated Learning Exchange

- **Observation:** The success of a federation depends on data owners to share data with the federation
- **Challenge:** How to motivate continued participation by data owners in a federation?

Research Question: How to determine $u_i(t)$?



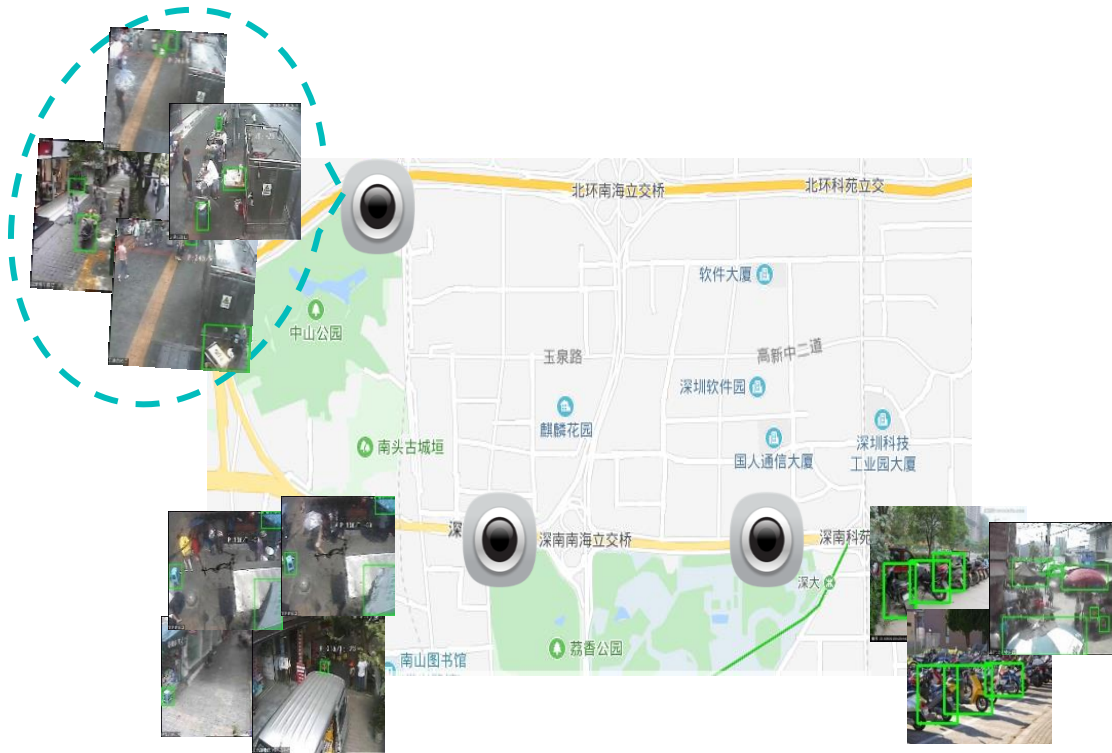
Federated Machine Learning: Advantages

	Coalition games with transferable utility [1]	Labour union games [2,3]	Fair-value games / Shapley games [2,3]	Federated Learning (this work)
Players do not need to engage in complex negotiations	X	√	√	√
Players can join multiple coalition at the same time, cost for joining a coalition, the value of a dataset does not depreciate after being shared, and players' time spent waiting for cost to be compensated	X	X	X	√
Players' marginal contribution is important	√	X	√	√

- 1) B. Faltings, G. Radanovic & R. Brachman. *Game theory for data science: Eliciting truthful information*. Morgan & Claypool Publishers, p. 152, 2017.
- 2) J. Augustine, N. Chen, E. Elkind, A. Fanelli, N. Gravin & D. Shiryayev. Dynamics of profit-sharing games. *Internet Mathematics*, 1:1–22, 2015.
- 3) S. Gollapudi, K. Kollias, D. Panigrahi & V. Pliatsika. Profit sharing and efficiency in utility games. In *ESA*, pp. 1–16, 2017.

Application: FML Network for Object Detection

- For parking and street vendor violation
- A partner project of WeBank AI and Extreme Vision in Shenzhen, China



Challenges

- Difficult detection task with few labels;
- Data are scattered; Expensive to centralize and manage data;
- Delayed feedback and delayed model updates.

A federated learning approach

- Online feedback loop and model updates;
- No need to upload and centralize data;
- No sharing data.

7 class : {table, chair, carton, sunshade, basket, gastank, electrombile} with 6 cameras, 1922 images

Federated AI Ecosystem



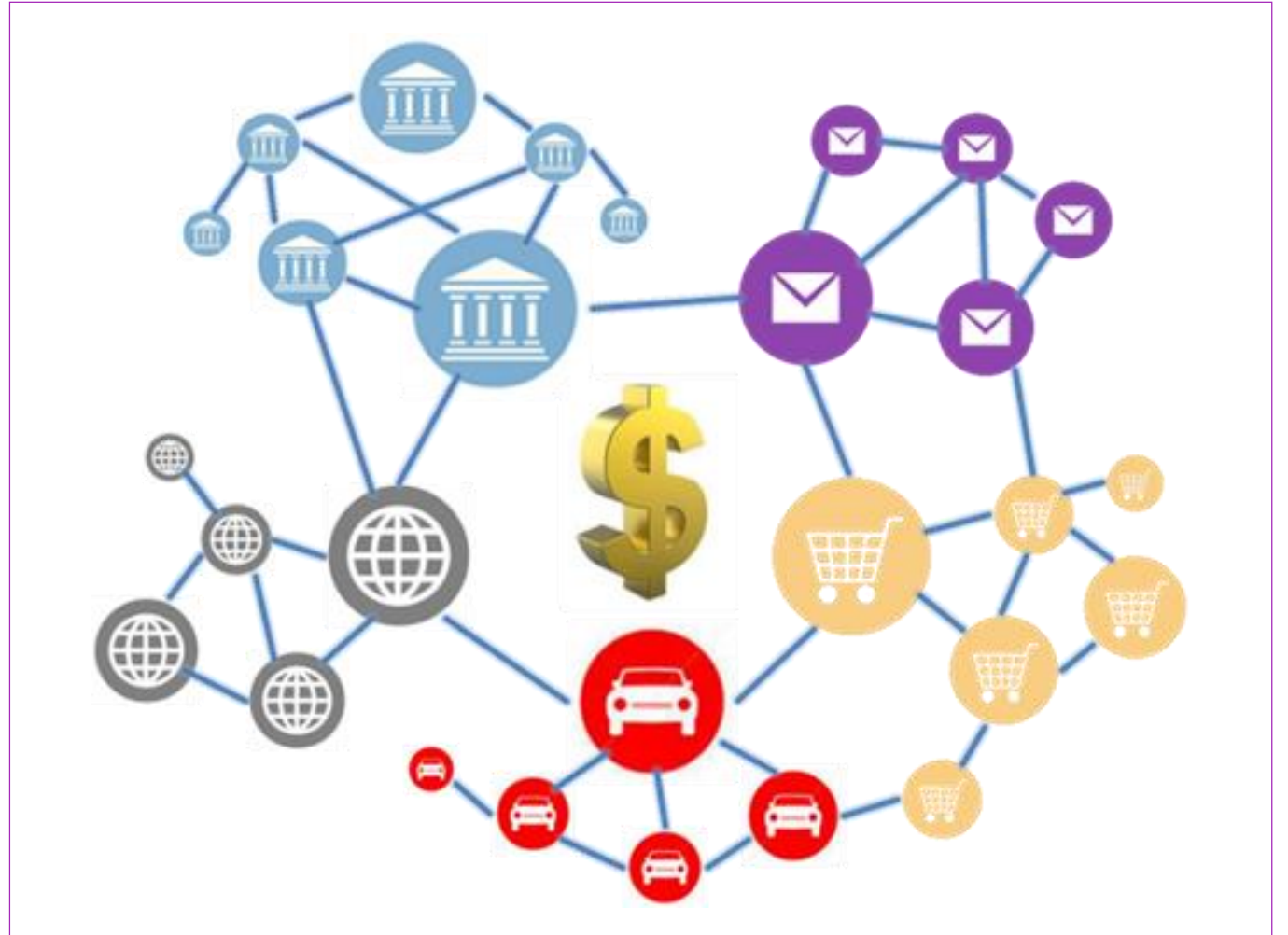
Security & Compliance



Lossless performance



Effective for small data and weak-supervision problem



IEEE Standard P3652.1 – Federated Machine Learning

➤ Title:

- Guide for Architectural Framework and Application of Federated Machine Learning
- Descriptions and definition of federated machine learning
- Categories of federated learning and their applications
- Performance evaluation of federated learning
- Associated regulatory requirements

➤ First working group meeting:

- First working group meeting
- Dates: February 21~22, 2019
- Location: Shenzhen, China
- <https://sagroups.ieee.org/3652-1/>

Open Source in Feb 2019 – Federated AI Technology Enabler (FATE)

➤ FATE is an open-source project initiated by Webank's AI Department

- Supports federated learning architectures including horizontal federated learning, vertical federated learning and federated transfer learning
- Implements secure computation protocols based on homomorphic encryption and multi-party computing (MPC)
- Supports the secure computation of various machine learning algorithms, including logistic regression, tree-based algorithms, and deep learning and transfer learning

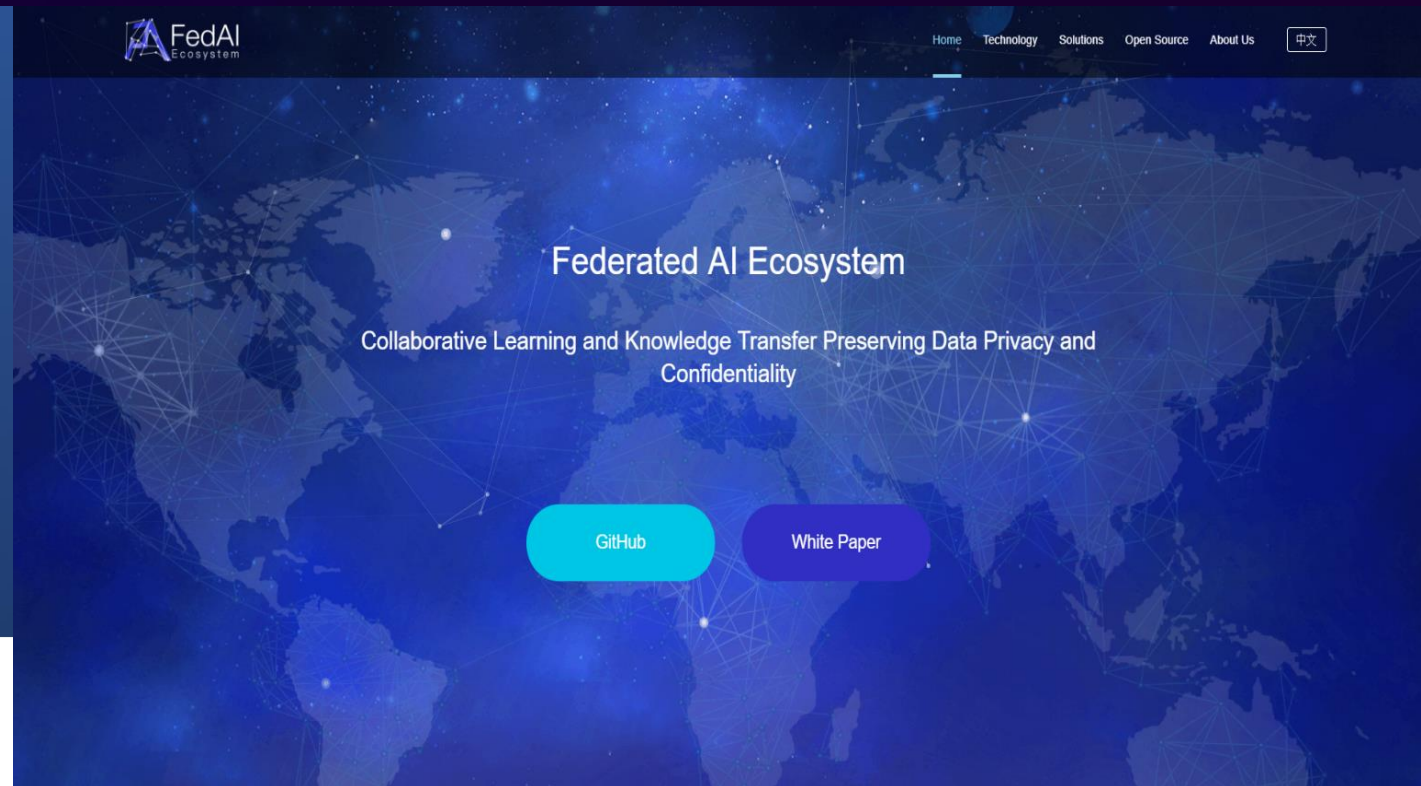


Federated Learning: User Privacy, Data Security and Confidentiality in Machine Learning

AAAI 2019 Tutorial

Go to www.fedai.org

Abstract



<https://www.fedai.org/>

Summary

- AI' s Data Challenge: data shortage, regulations, and fragmentation
- Transfer Learning: from pretrained large models to small data
- Federated Machine Learning: secure collaboration in model building
- Federated Transfer Learning, Incentive Mechanisms and Open Source Frameworks
- <https://sagroups.ieee.org/3652-1/>
- <https://www.fedai.org/>