联邦迁移学习

AI所面临的困境与机遇

杨强

中国人工智能学会副理事长

国际人工智能联合会 （IJCAI） 理事会主席

大数据驱动的AI

理想与现实

AI的起伏

$$效率=\frac{收益}{费用}$$

自动化

数字化

人工智能

时间

1955 • 达特茅斯会议标志着AI的诞生

1957 • 罗森布拉特发明第一款神经网络Perceptron，将人工智能推向第一个高峰

1970 • 计算能力突破没能使机器完成大规模数据训练和复杂任务，AI进入第一个低谷

1982 • 霍普菲尔德神经网络被提出

1986 • BP算法出现使得大规模神经网络的训练成为可能，将AI推向第二个黄金期

1990 • 人工智能计算机DARPA没能实现，政府投入缩减，AI进入第二次低谷

2006 • Hinton提出“深度学习”神经网络使得人工智能性能获得突破性进展

2013 • 深度学习算法在语音和视觉识别上取得成功，识别率分别超过99%和95%，进入感知智能时代

算法

算法

算法

算法

算力

Intel i386

Intel i486

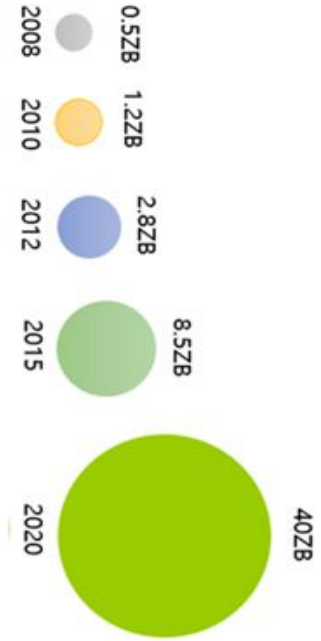
Intel Pentium
Intel Core

nVidia GPU

Google TPU

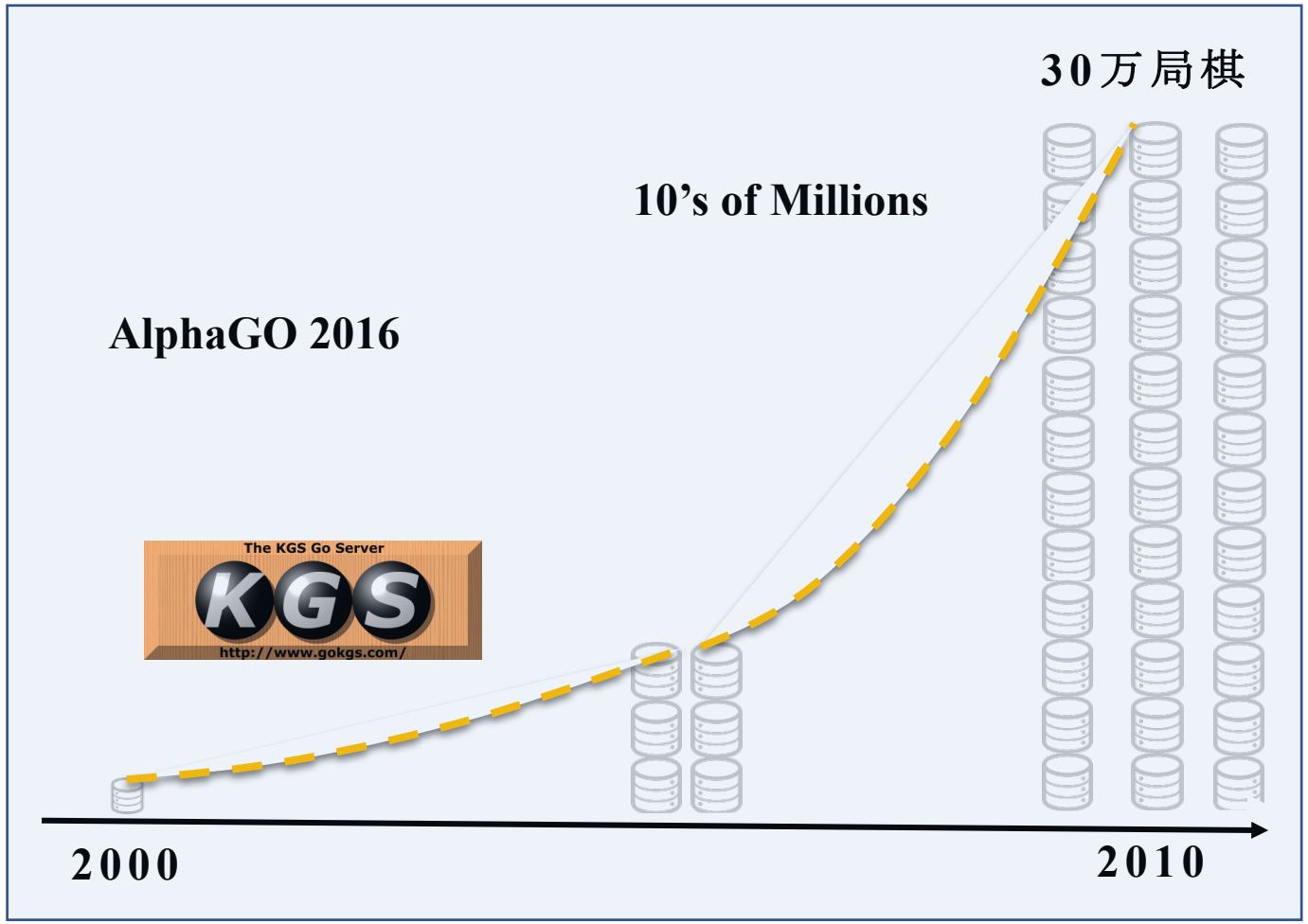
大数据
(40ZB)

1 ZB= 10^{21}Byte



来自互联网数据中心（IDC）

AlphaGo和大数据



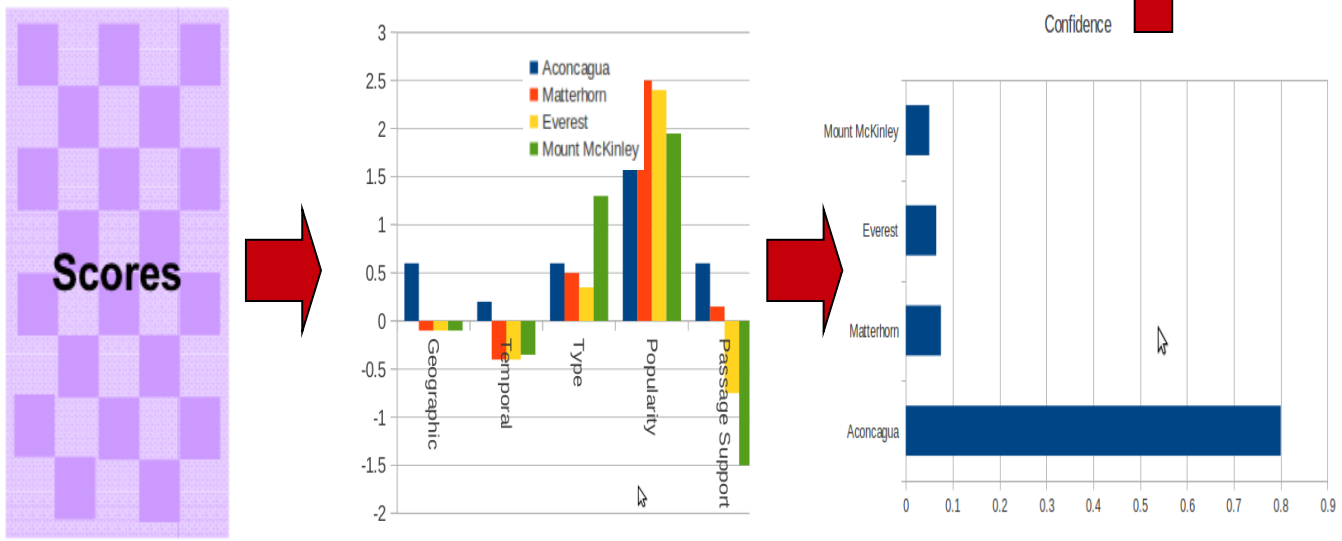
IJCAI 2018

Minsky Award to AlphaGo Team

IBM WATSON

Clue: In 1897 Swiss climber Matthias Zurbriggen became the first to scale this Argentinean peak.

What is Aconcagua?



IBM WATSON 总结所有证据，计算出可信度

可信度分数加权平均，用图表展现

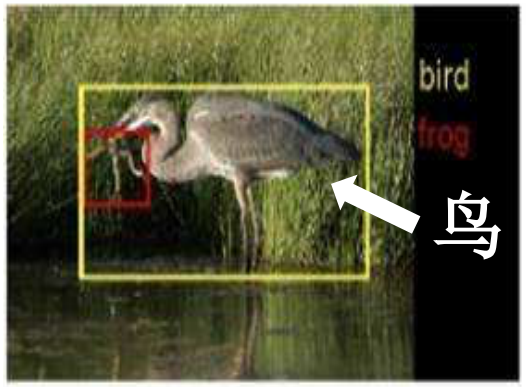
现状

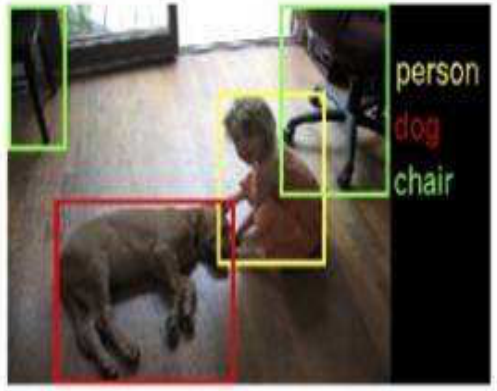
- MD Anderson Cancer Center : specialized data is seriously missing
- 输入Data：病症，基因序列，病理报告，内科医生报告，期刊论文
- 输出：病源，恢复时间表，等

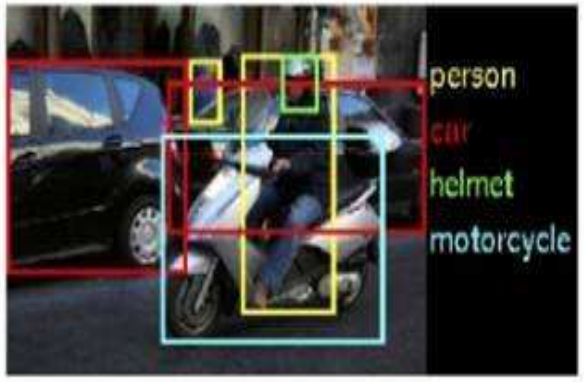
问题

- 无法了解基因与疾病的关系 （只有医生可以给数据打标签，不像无人汽车，人人都可以打标签）
- 买数据？ Verily Life Sciences 有一万名志愿者，但需要10年！

现实： 数据的X和Y





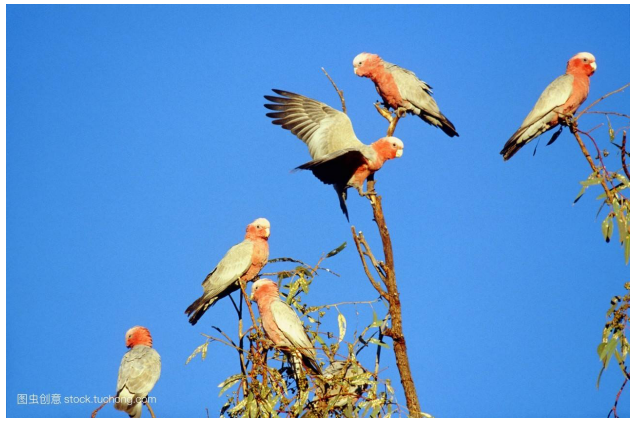


训练数据

User	X1	X2	X3		Y
				+	

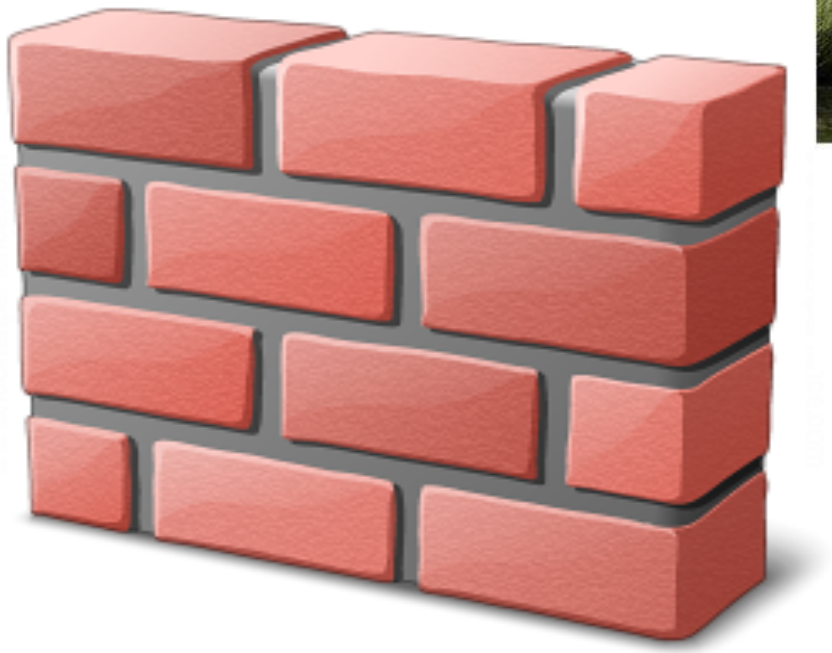
$$X + Y$$

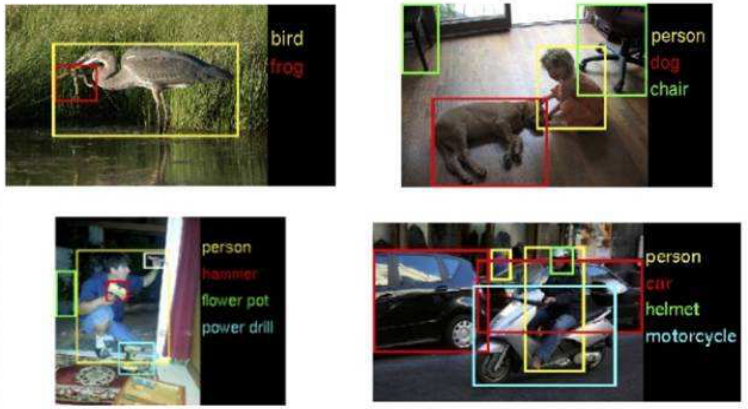
现实： 数据的X和Y



企业 A

X1





企业 B

(X2, Y)

现实： 数据的X和Y

举例： 微众银行+新零售

WeBank
微众银行
科技 · 普惠 · 连接

智慧零售门店的困扰

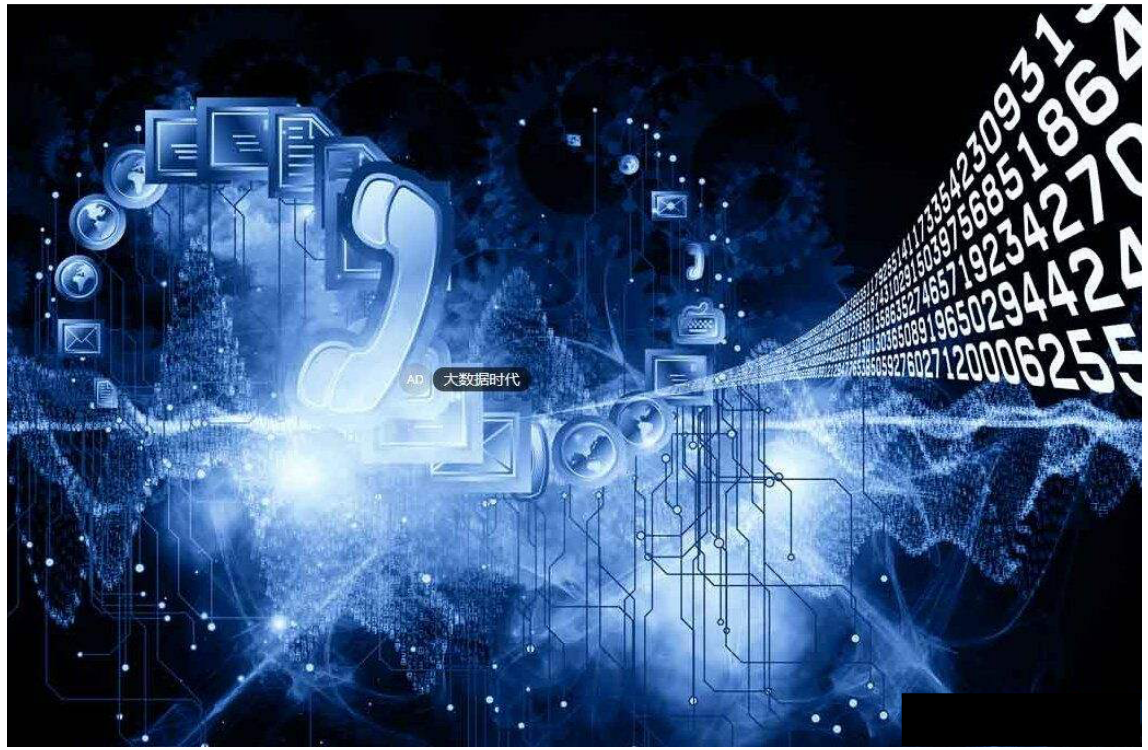
数据隔离，共享安全性低

数据库样本不足，标签缺失

数字化系统改造成本高

盲式联合，精准营销效率低

大数据时代？ 理想 vs 现实



两大困境及两个解法

①隐私，安全和监管

联邦学习生态 Federated Learning Network

②小数据，弱监督

迁移学习

两大困境及两个解法

①隐私，安全和监管

联邦学习生态 Federated Learning Network

②小数据，弱监督

迁移学习

大数据的困境： 欧盟的隐私保护法 - GDPR

大数据： 欧盟的 GDPR

- 《通用数据保护条例》（General Data Protection Regulation, 简称GDPR）为欧盟于2018年5月25日出台的条例
- 对违法企业的罚金最高可达2000万欧元（约合1.5亿元人民币）或者其全球营业额的4%，以高者为准
- 网站经营者必须事先向客户说明会自动记录客户的搜索和购物记录,企业不能再使用模糊、难以理解的语言，或冗长的隐私政策来从用户处获取数据使用许可。
- 明文规定了用户的“被遗忘权”（right to be forgotten），即用户个人可以要求责任方删除关于自己的数据记录。

2018年5月28日报道：

Facebook和谷歌等美国企业成为GDPR法案下第一批被告。

GDPR是否禁止使用机器学习模型？

- 对使用自动化模型决策全面禁止
  - 指在没有人直接参与决策的情况下做出决定的模型
  - 例如，在营销中，将用户分类为“潜在客户”或“40-50岁的男性”等
  - 用户可以对模型决定提出质疑，还有权对自动决策做出解释
  - 用户有权知道模型的使用目的
  - 用户有权撤回数据

UW Prof. Pedro Domingos, a leading AI researcher, started a firestorm with his tweet

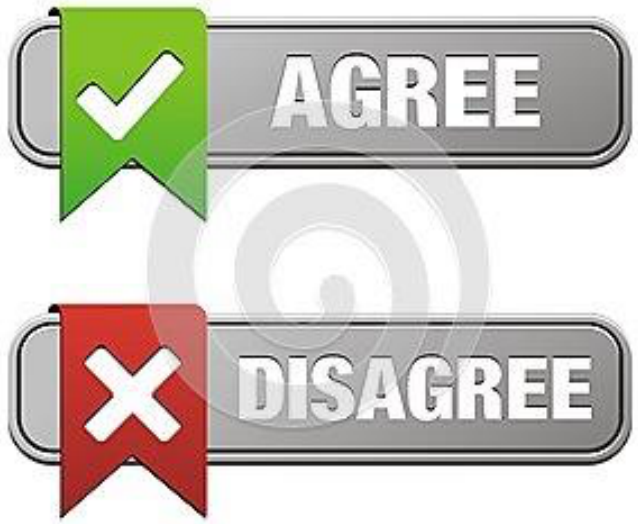
Starting May 25, the European Union will require algorithms to explain their output, making deep learning illegal

— Pedro Domingos (@pmddomingos) January 29, 2018

GDPR对机器学习的重大影响

① 让用户同意并不容易

- 用户可以同意许多不同类型的数据处理，并且他们也可以在任何时候撤销同意
- 这意味着用户同意需要细化和进一步的规范



② 使用自主决策合法的三个领域

- 合同处理的必要性
- 其他法律另行授权
- 数据主体明确同意

差分隐私理论(Differential Privacy): 不再能使用？

联邦迁移学习(Federated Transfer Learning)

- 联邦迁移学习思路

建立机器学习的企业生态

- 各个企业自有数据不出本地，模型效果不变（LOSSLESS）

(X)

(U, Z)

WeBank 微众银行 科技 · 普惠 · 连接

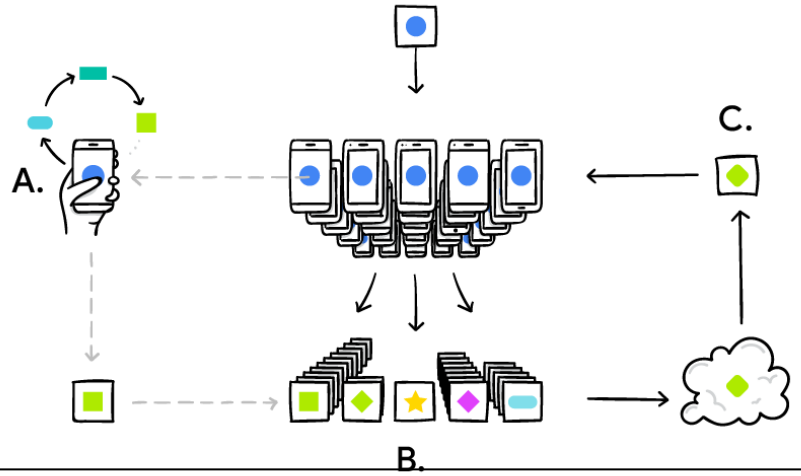
(V, Y)

- 利用联邦迁移学习加密技术，协同建模

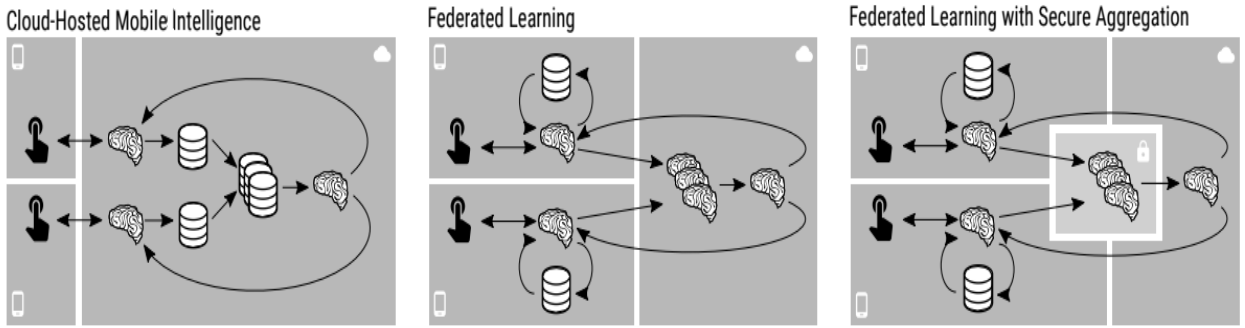
学习模型过程不交换用户数据

不侵犯和泄露隐私

联邦学习 Federated Learning： GOOGLE



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



Keith Bonawitz , Vladimir Ivanov et al, ***Practical Secure Aggregation for Privacy-Preserving Machine Learning***, Google, 2017

① 特点

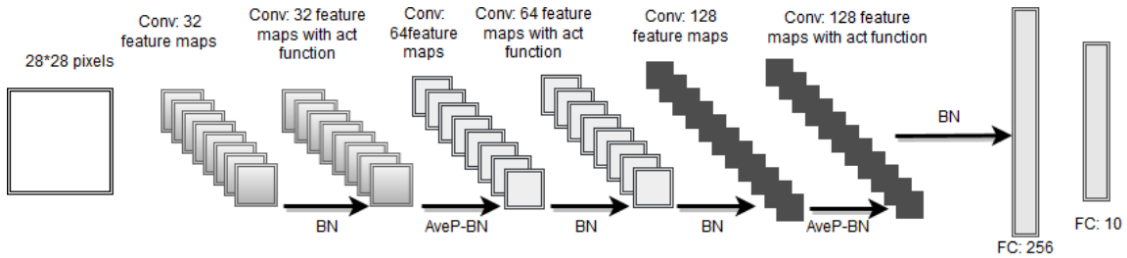
参与者特征相同，样本不同

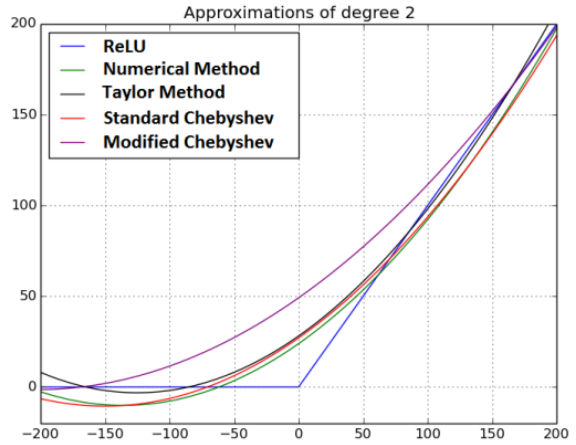
② 应用举例

手机终端的新闻推荐模型更新

隐私保护的Deep Learning举例 - CryptoDL

3.5 CNN Model 2 with Polynomial Activation Function





(a) Approximation of ReLU using different methods

E Hesamifard et al, “CryptoDL: Deep Neural Networks over Encrypted Data”,2017

① 特点 用于Inference Time

参与者特征相同，样本不同

② 同态加密技术可用于多项式

③ 应用(Inference)时使用

客户端流数据应用server模型做分析和标注

隐私保护的Deep Learning举例 - DeepSecure

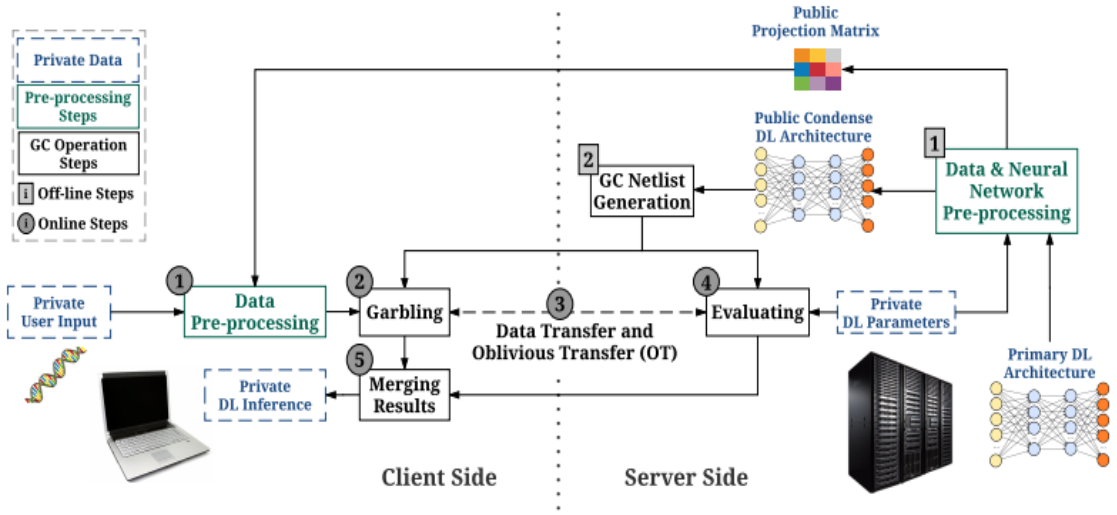


Figure 2: Global flow of DeepSecure framework including both off-line (indexed by rectangular icons) and online (indexed by oval icons) steps. The operations shown in the left hand side of the figure are executed by the client (Alice) while the operations on the right hand side are performed by the server (Bob).

B. D. Rouhani, M. S. Riazi, F. Koushanfar, DeepSecure: Scalable Provably-Secure Deep Learning, CoRR, abs/1705.08963, 2017.

① **特点： 应用Time使用**

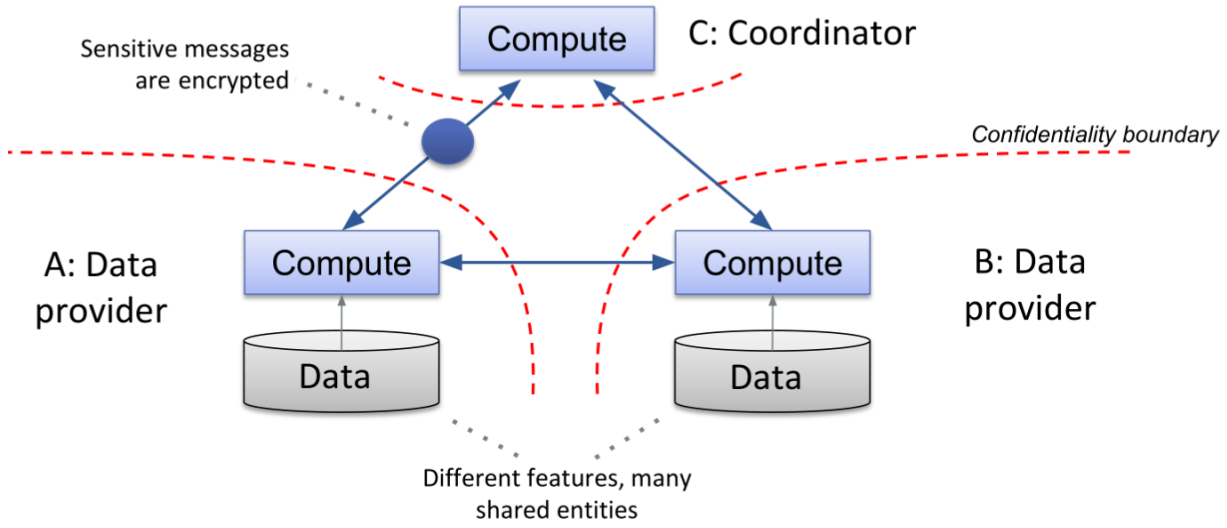
参与者特征相同，样本不同

② **Rao Data 加密技术：使用 YAO's Garbled Circuit Protocol**

③ **应用 （Inference）**

客户端流数据应用server模型做分析和标注

联邦学习(Federated Learning) - 样本纵向分割



G. Patrini et al, "Privacy-preserving entity resolution and logistic regression on encrypted data", PSML workshop, ICML 2017

① 特点:

参与者特征不同，样本ID相同; 模型在各自端更新，并在第三方聚合

② 应用举例

企业对共同用户联合建模（如银行和保险公司建立联合营销模型）

- **优点**

  LR模型可用

- **缺点**

我们下面来解决这个问题

联邦学习框架：微众银行的决策树和森林模型

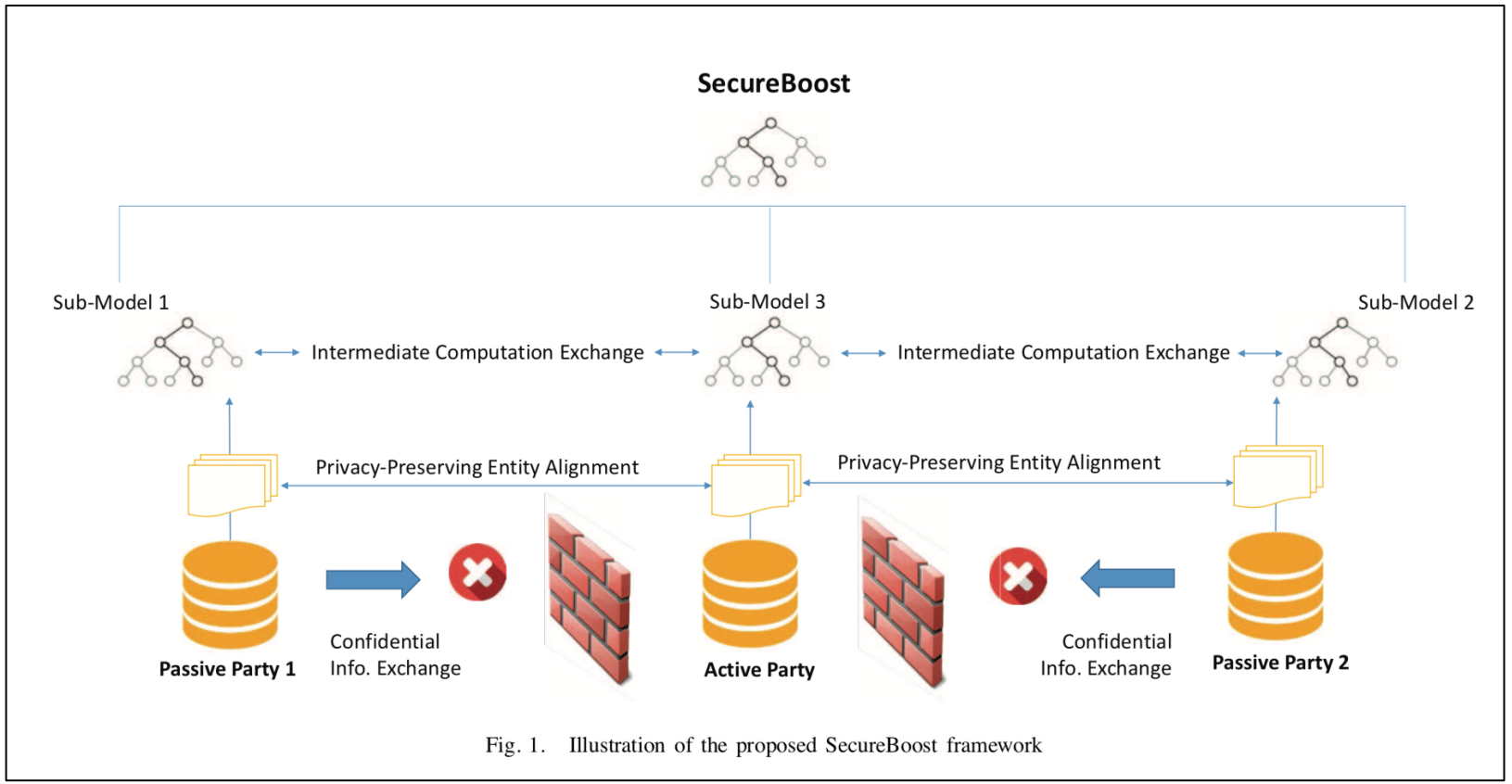


Fig. 1. Illustration of the proposed SecureBoost framework

(X)

WeBank 微众银行 科技·普惠·连接

(V, Y)

(U, Z)

联邦学习框架

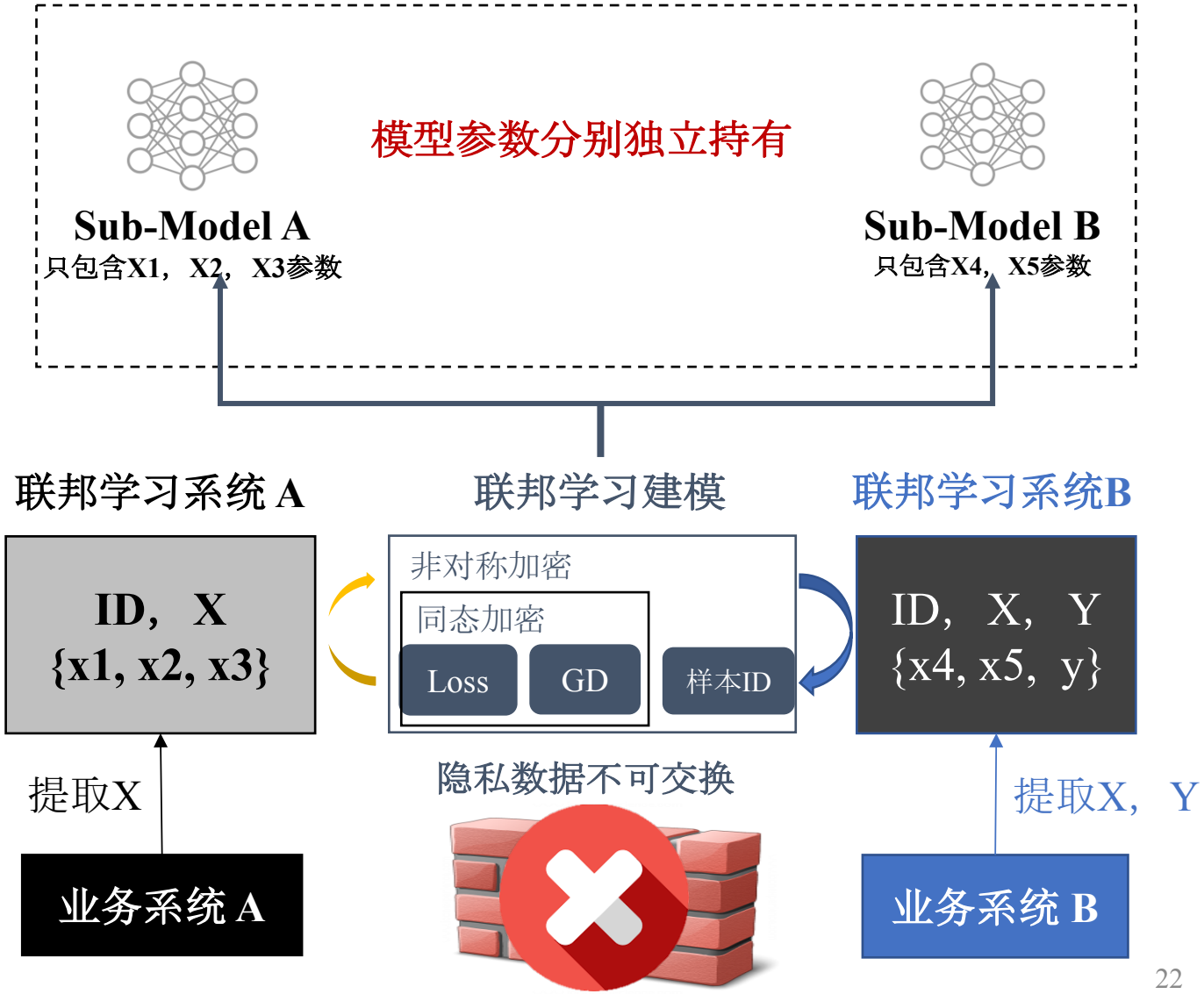
- **数据隐私保护**

  建模样本ID差集不泄露

  任何底层X，Y数据不泄露

- **模型参数保护**

  分别持有，联合使用



两大困境及两个解法

①隐私，安全和监管

联邦学习生态 Federated Learning Network

②小数据，弱监督

迁移学习

“第四范式”公司：利用迁移学习解决大额消费金融的困境

4Paradigm.com

在千万量级微信公众号客户中，挖掘近期有购车意向的客户，通过微信营销购车分期业务。客户可点击其中链接提交申请。

难点：新渠道，成功办理客户<100

方法：基于全渠道营销数据（成功次数>1亿），帮助汽车分期贷款模型学习

效果：与SAS模型相比，营销响应率提升**200%+**

迁移学习本质

迁移学习本质：找出不变量

跨领域舆情分析

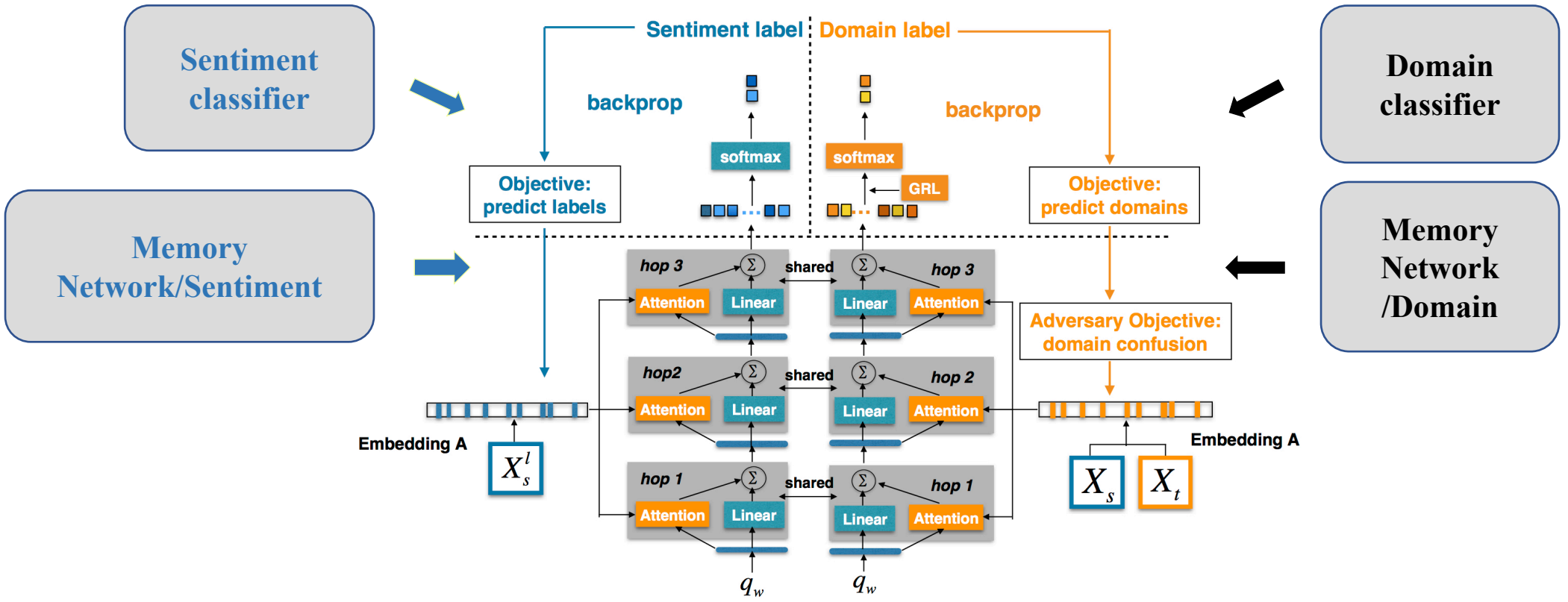
- **End-to-End Adversarial Memory Network for Cross-domain Sentiment Classification, IJCAI 2017, Zheng Li, et al.**
- **问题：如何自动找出 领域间“桥接”Pivot 关键词？**

舆情	Books (源领域)	Restaurant (目标领域)	舆情
	Great books. His characters are engaging.	The food is great, and the drinks are tasty and delicious.	?
	It is a very nice and sobering novel.	The food is very nice and tasty, and we’ll go back again.	?
	A awful book and it is a little boring.	Shame on this place for the rude staff and awful food.	?

跨领域舆情分析

- **End-to-End Adversarial Memory Network for Cross-domain Sentiment Classification, IJCAI 2017, Zheng Li, et al.**
- **问题：如何自动找出 领域间“桥接”Pivot 关键词？**

同时使用Memory Network 和 GAN



跨领域舆情分析

跨领域舆情分析结果

Domain	#Train	#Test	#Unlab.	% Neg.
Books	1600	400	6000	13.45%
DVD	1600	400	34741	21.47%
Electronics	1600	400	13153	11.92%
Kitchen	1600	400	16785	17.82%

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

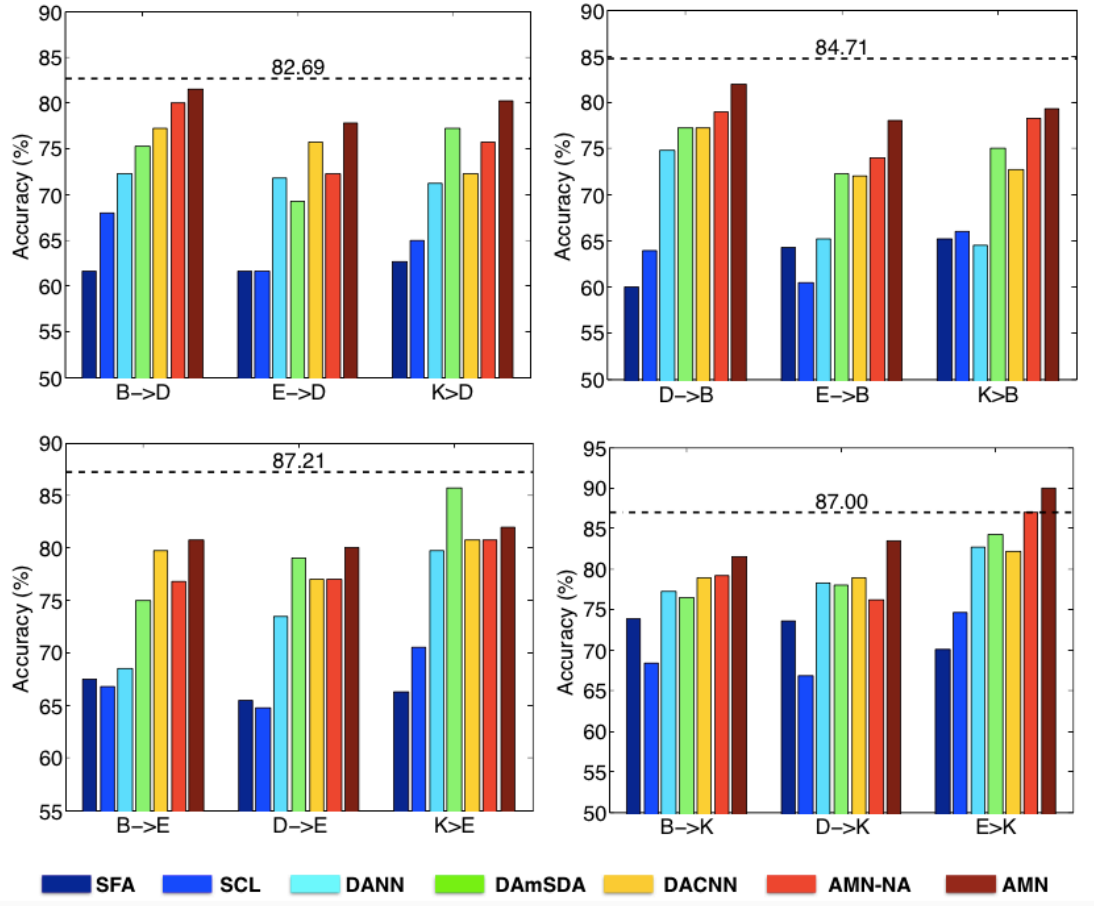
GT:1 Prediction:1
gorgeous i just received this as a wedding gift and it is beautiful a great gift

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

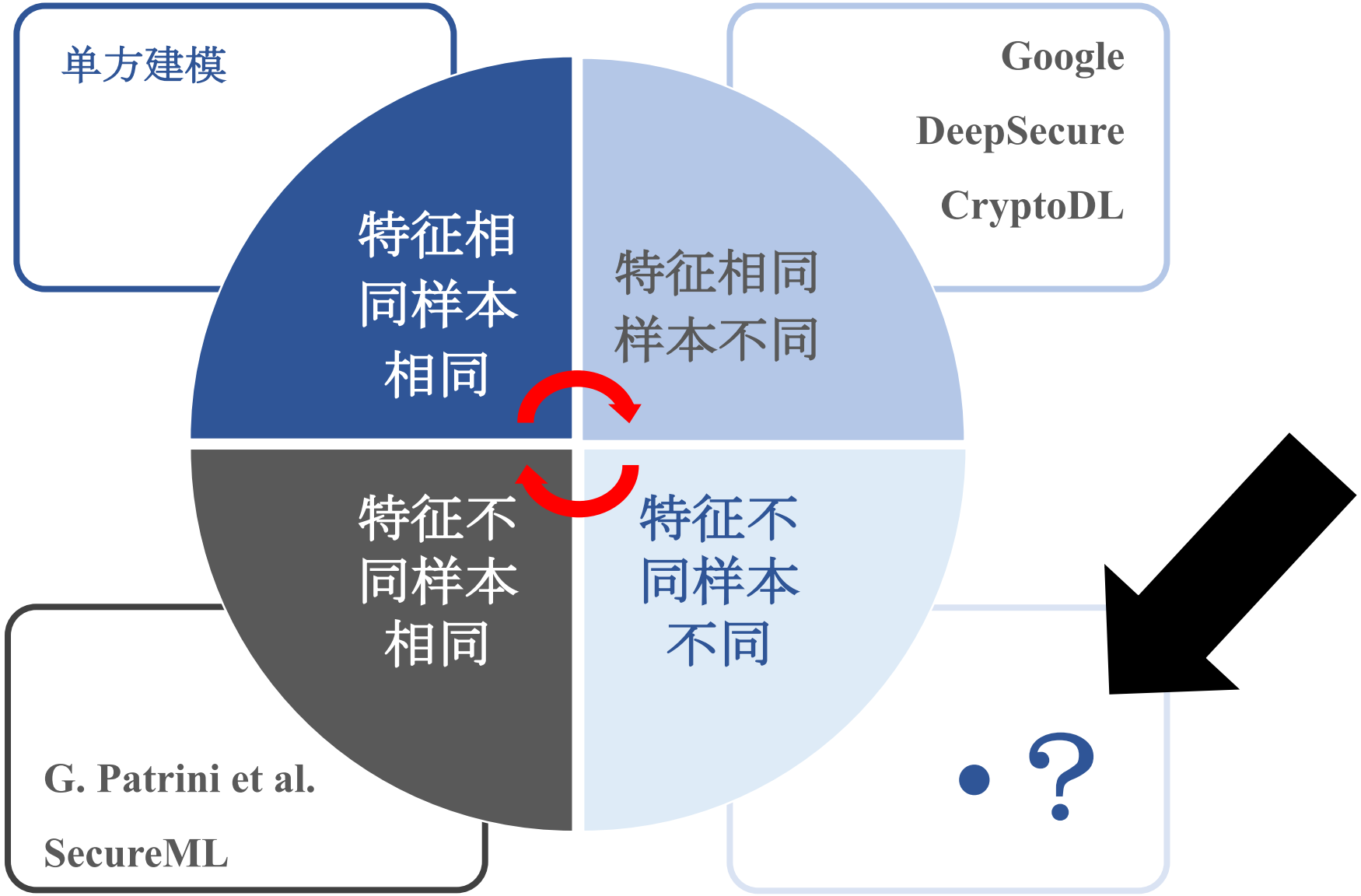
GT:0 Prediction:0
too poorly made for everyday use we have a full line of fiesta dishware and thought having the matching flatware would be nice after a year of standard use and dishwashing about 13 of the flatware is unusable the upside is that it is cheap and replaceable but count me among those who 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



联邦学习+迁移学习


单方建模
特征相同
同样本
相同
特征相同
样本不同
Google
DeepSecure
CryptoDL
特征不
同样本
相同
特征不
同样本
不同
G. Patrini et al.
SecureML
?

特征不同，样本也不同怎么办？

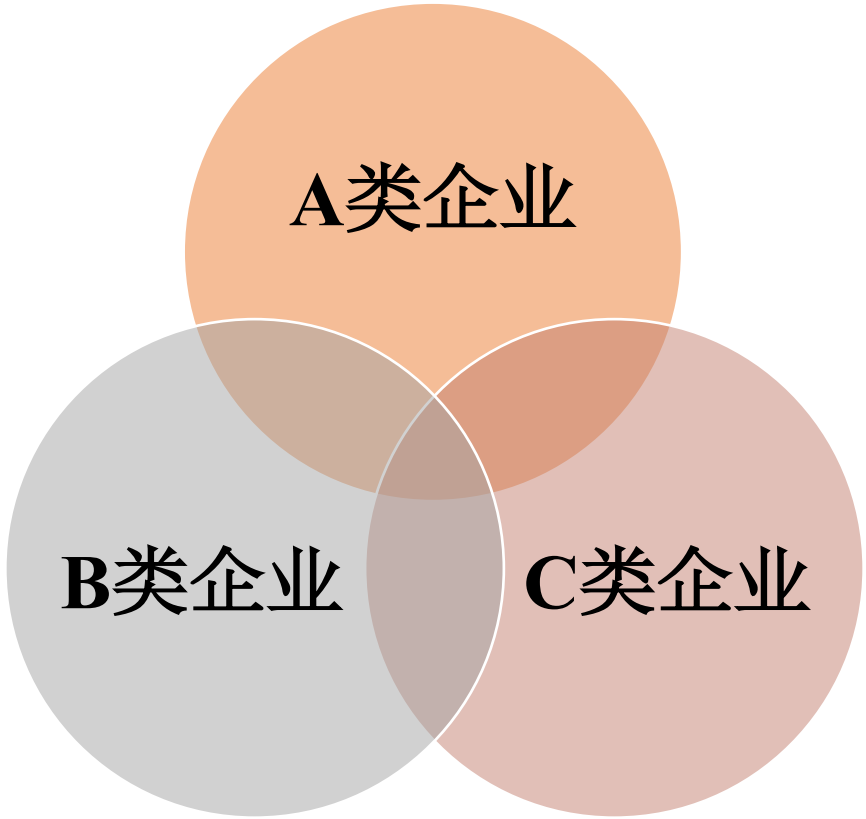
实际场景特点

各方非交集用户为多数，不可忽略

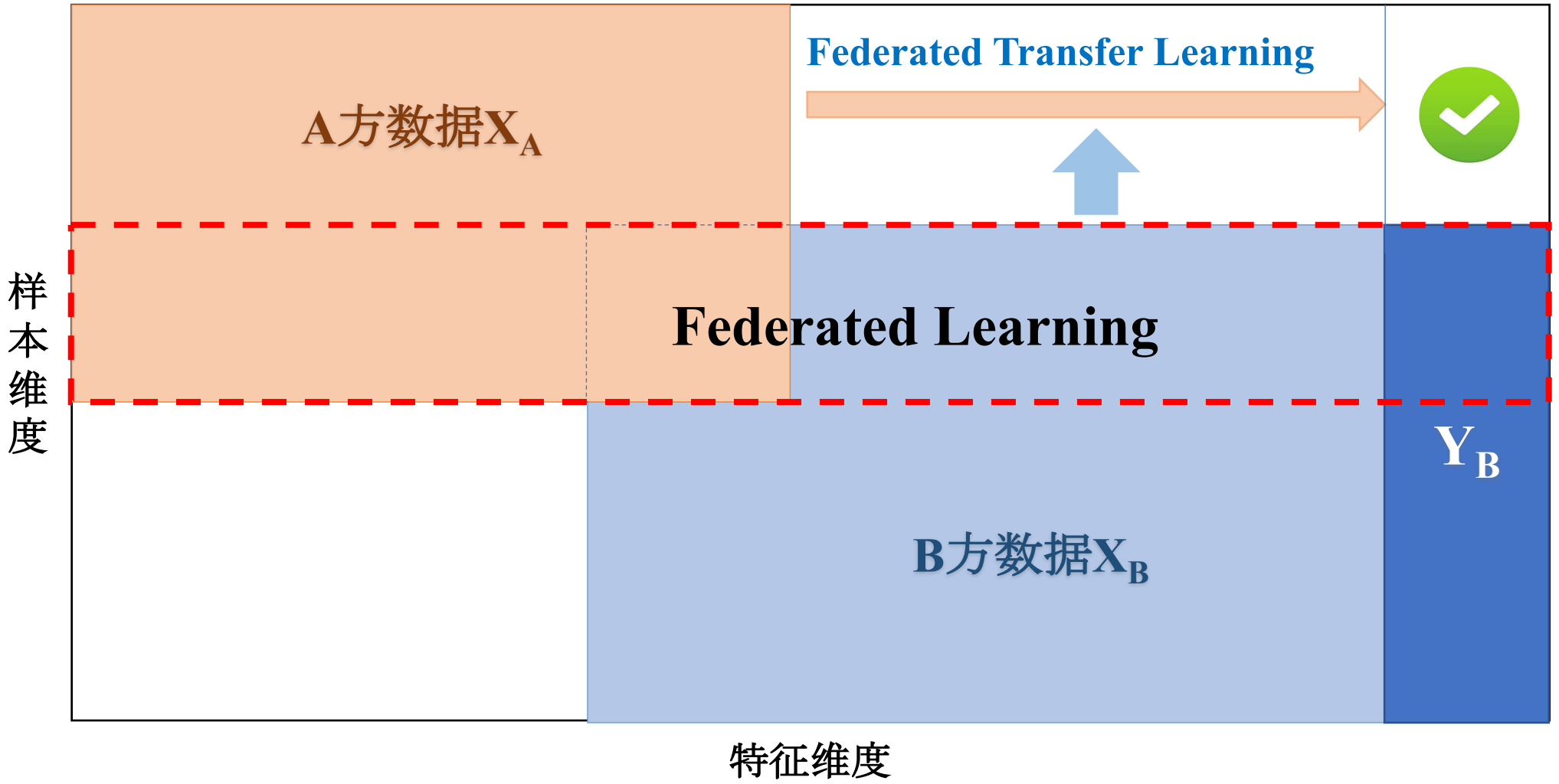
大量非交集用户数据有巨大挖掘价值

解决方案

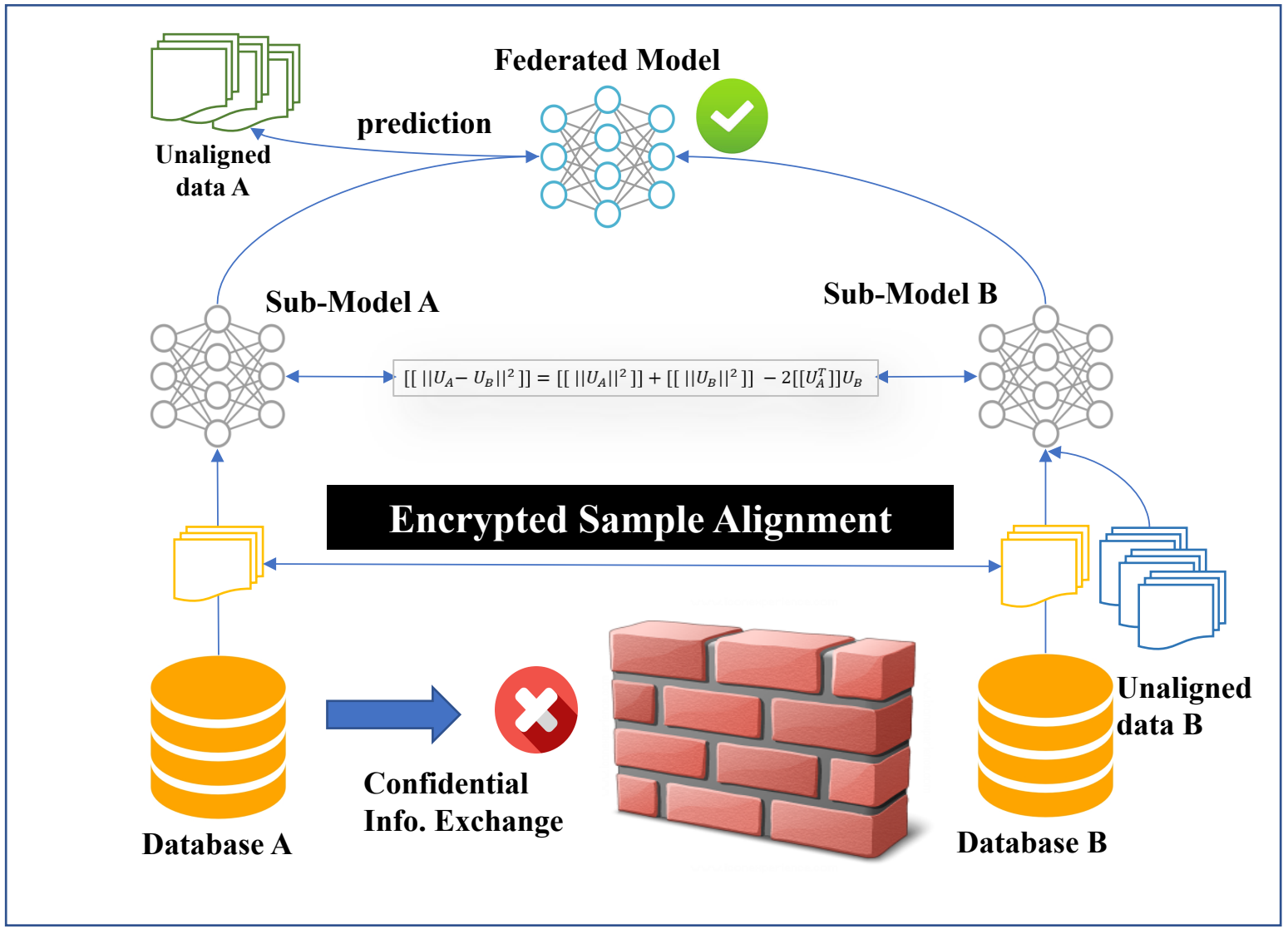
联邦学习+迁移学习



联邦迁移学习 Federated Transfer Learning：问题四大类



联邦迁移学习框架 Federated Transfer Learning



(X)

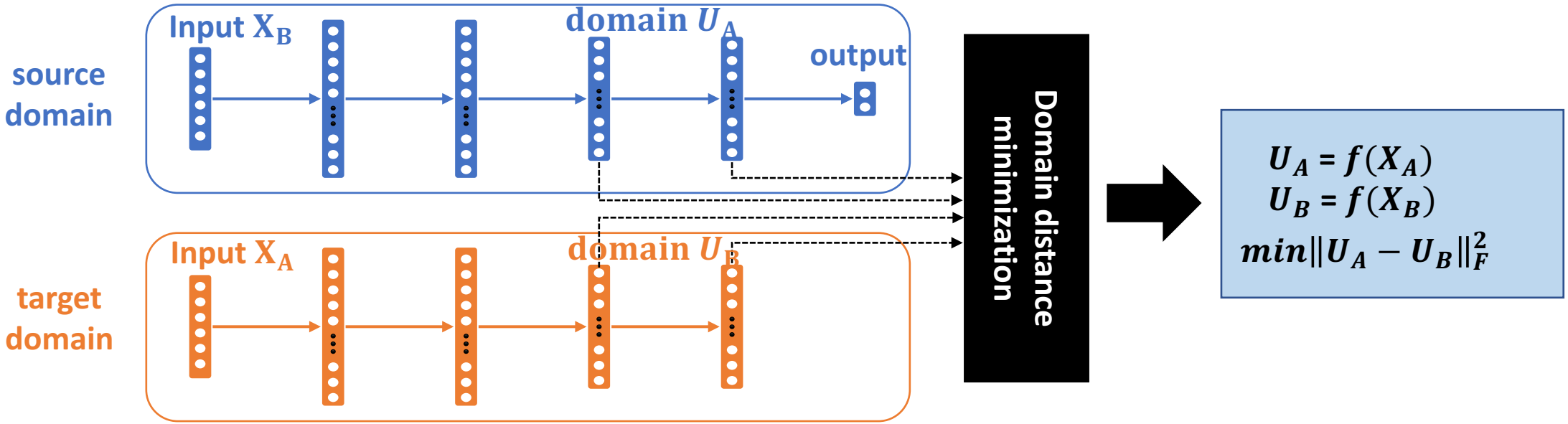
WeBank 微众银行 科技·普惠·连接

(V, Y)

(U, Z)

联邦迁移学习 FTL和深度学习

- 迁移学习找到共同特征表达 **Heterogenous Transfer Learning to find latent representations**
- 同态加密下的模型处理 **Homomorphism-aware loss function via Polynomial Approximation**
- 隐私保护下样本ID匹配 **Privacy-Preserving Entry-id Match**



联邦迁移学习 FTL： 微众银行的智慧零售落地场景案例

金融领域联邦学习联盟

Financial Federated Learning Network **- 在隐私保护下共建金融企业大数据生态**

案例：智慧零售营销解决方案

智慧零售门店的困扰

数据隔离，共享安全性低

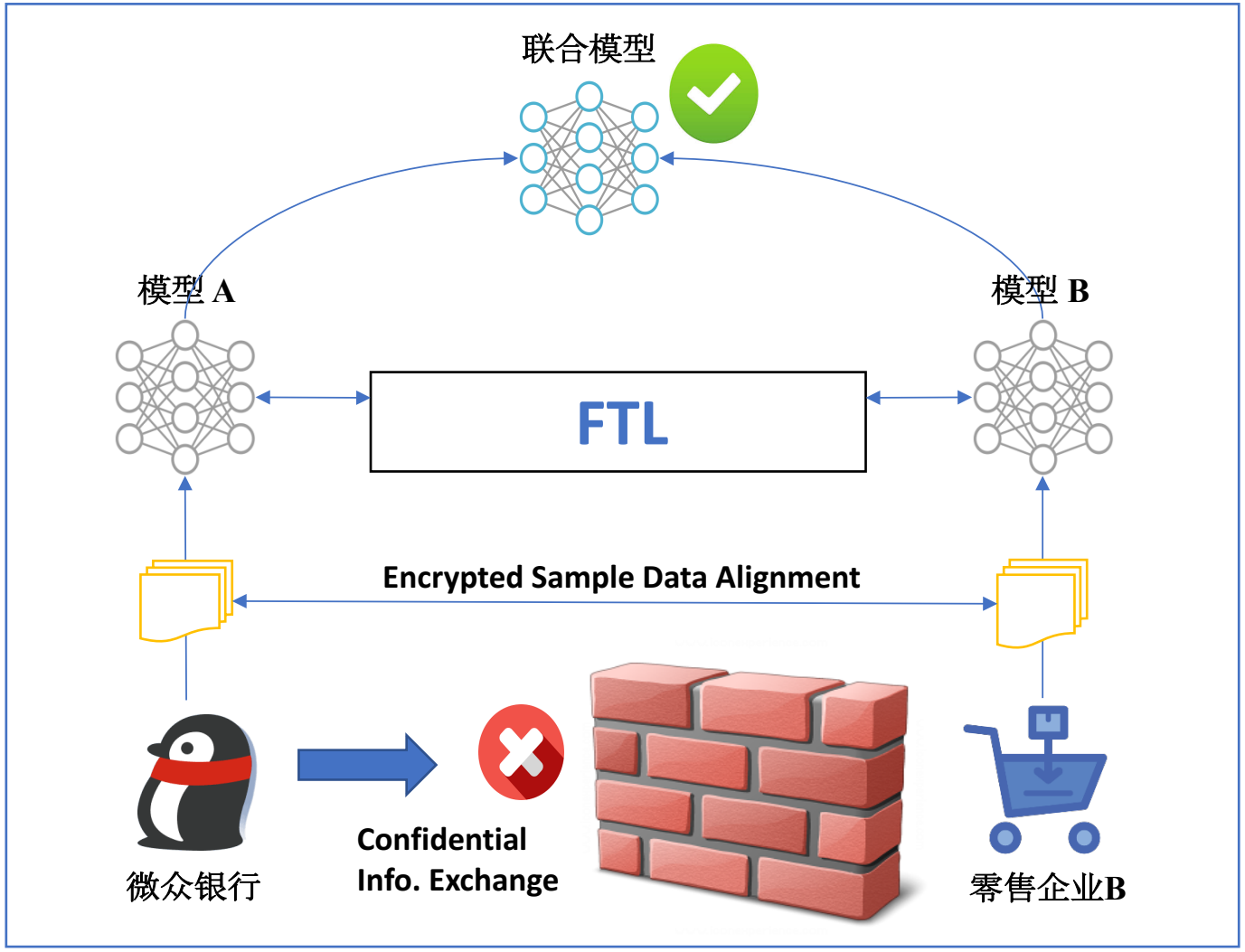
数据库样本不足，标签缺失

数字化系统改造成本高

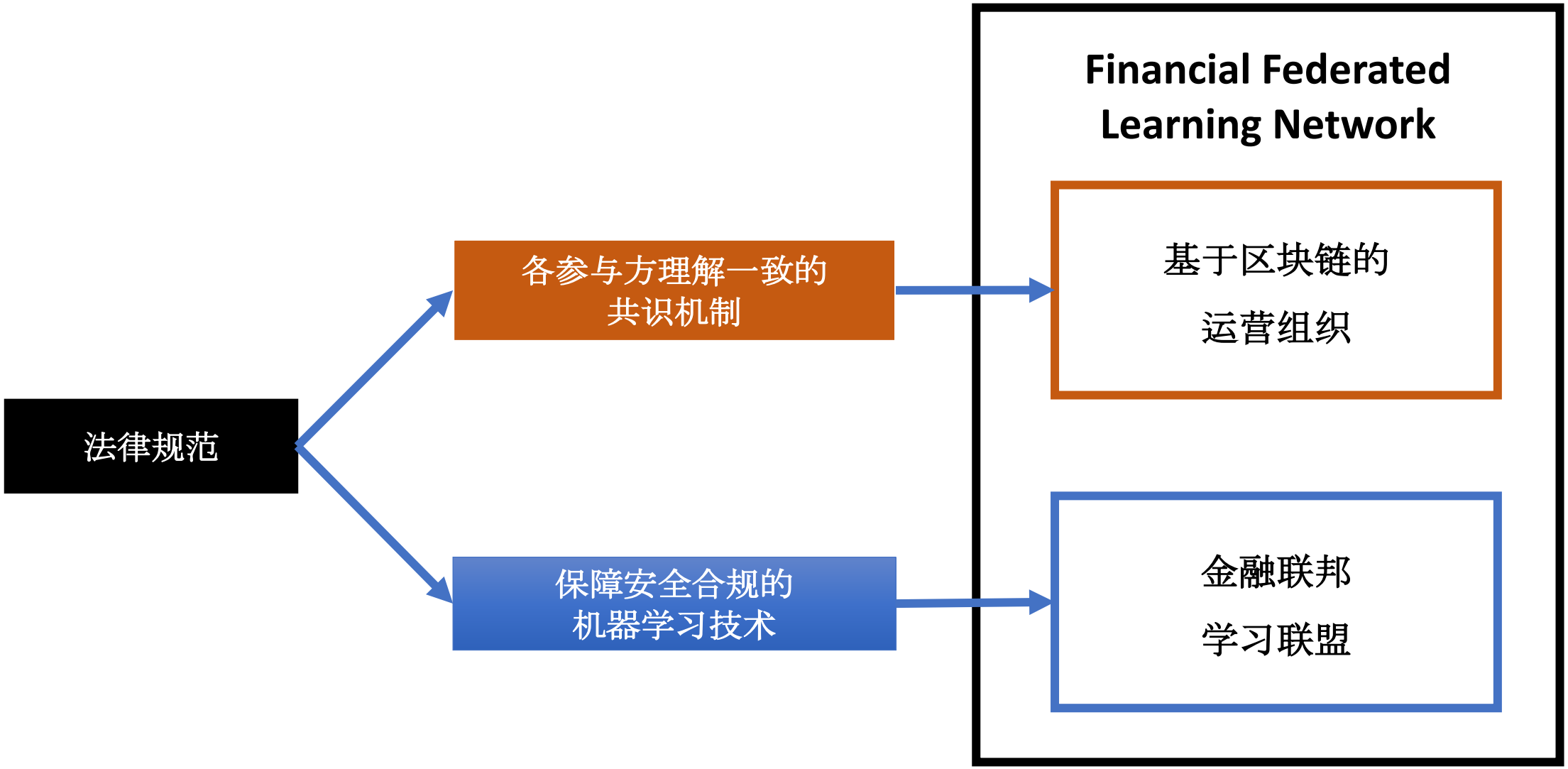
盲式联合，精准营销效率低

联合建模解决方案：克服数据屏障

- ✓ 数据本地化，数据库独立
- ✓ 与新零售企业合作对共有用户数据联合建立金融服务模型
- ✓ 对非共有用户数据采用联邦迁移模型提升预测覆盖能力



构建安全合规的大数据 + AI生态



结语：AI面临的困境与机遇

CCAI 2018

①社会对隐私安全的要求，GDPR 数据隐私法案， 小数据

②解决途径：联邦迁移学习框架

③企业生态：建立金融业联邦学习联盟

④感谢：微众银行AI团队

References

- H. Brendan McMahan Eider Moore et al, *Communication-Efficient Learning of Deep Networks from Decentralized Data*, Google, 2017
- Keith Bonawitz , Vladimir Ivanov et al, *Practical Secure Aggregation for Privacy-Preserving Machine Learning*, Google, 2017
- S. Hardy, W. Henecka, H. Ivey-Law, R. Nock, G. Patrini, G. Smith, and B. Thorne. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. arXiv:1711.10677, 2017
- G. Liang and S. S. Chawathe, “Privacy-preserving inter-database operations,” in International Conference on Intelligence and Security Informatics. Springer, 2004, pp. 66–82
- Wei, Y., Zhu, Y., Leung, C.W.k., Song, Y., Yang, Q.: Instilling social to physical: Coregularized heterogeneous transfer learning. In: Proceedings of the AAAI National Conference on Artificial Intelligence. pp. 1338–1344 (2016)
- P. Mohassel, Y, Zhang. SecureML: A System for Scalable Privacy-Preserving Machine Learning. IACR Cryptology ePrint Archive, 2017
- E Hesamifard et al, “CryptoDL: Deep Neural Networks over Encrypted Data”,2017
- G. Patrini et al, “Privacy-preserving entity resolution and logistic regression on encrypted data”, PSML workshop, ICML 2017
- B. D. Rouhani, M. S. Riazi, F. Koushanfar, DeepSecure: Scalable Provably-Secure Deep Learning, CoRR, abs/1705.08963, 2017
- Zheng Li, Yu Zhang, Ying Wei, Yuxiang Wu, and Qiang Yang. End-to-End Adversarial Memory Network for Cross-domain Sentiment Classification. In: *Proceedings of the 26th International Joint Conference on Artificial Intelligence* (IJCAI), pp. 2237-2243, Melbourne, Australia, 2017.