Privacy Preserving Machine Learning with Analytics-Zoo & Intel SGX

August 2020

Analytics-Zoo Team

Shi Dongjie & Gong Qiyuan

Outlines

Part 1 (背景 & 现状)

- Data Privacy & GDPR
- PPML (Privacy Preserving Machine Learning)

Part 2 (技术干货)

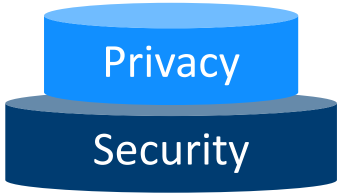
- Intel SGX & Graphene-SGX
- Analytics-Zoo
- PPML with Analytics-Zoo & Intel SGX

What is Data Privacy?

- Data Privacy

  Information privacy is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.

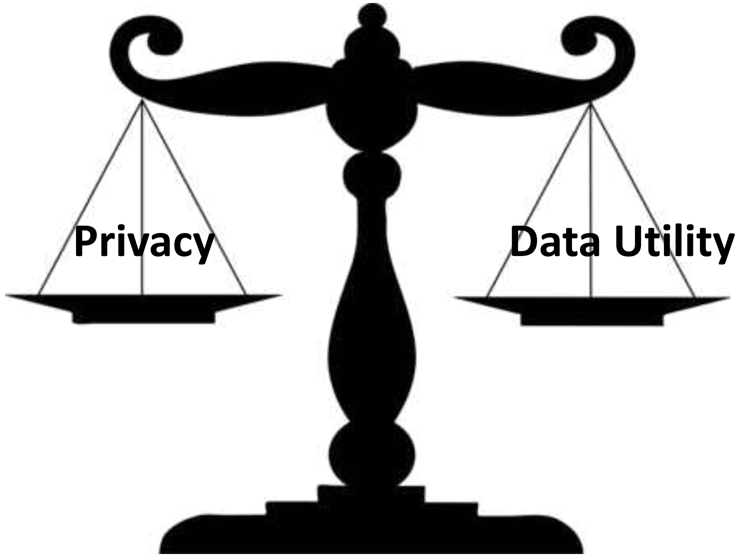
- Privacy & Security
  - No Security, then there is no privacy
  - Secured doesn't always means private
  - Win-Win: Secured & Privacy



https://en.wikipedia.org/wiki/Information_privacy

Data Privacy & Data Utility

- It's a tradeoff



Max Data Utiity (no privacy)

- All data is accessable
- Better analytics & machine learning with these data

Max Privacy (no utility)

- Not data sharing any more
- Analytics & machine learning maybe in trouble

A balanced status (Win-Win)

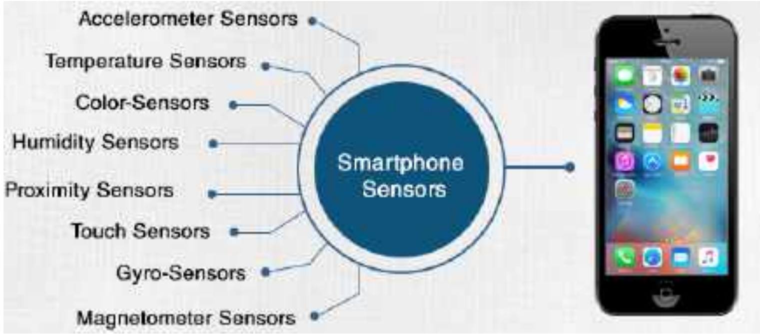
- Share some insenstive data
- Analytics & machine learning is good enough

Data privacy is challenging since it attempts to **use data while protecting an individual's privacy preferences and personally identifiable information**.[3] The fields of computer security, data security, and information security all design and use software, hardware, and human resources to address this issue.

https://www.clipartmax.com/middle/m2H7G6Z5N4G6H7H7_plourde-jean-b-silhouette-libra-drawing-measuring-scales-balance-clip-art/
https://en.wikipedia.org/wiki/Information_privacy

Data Privacy in Big Data era

- Lots of personal data are collected
  - Personal data: id, phone number etc
  - Photo & Video
  - Health data: movement, heart rate
- **Indirectly personal information is everywhere**
  - Input pattern, search log, click streaming etc
  - Music/Movie your liked/rated



How Target Figured Ou
Was Pregnant Before Her Father Did

Kashmir Hill

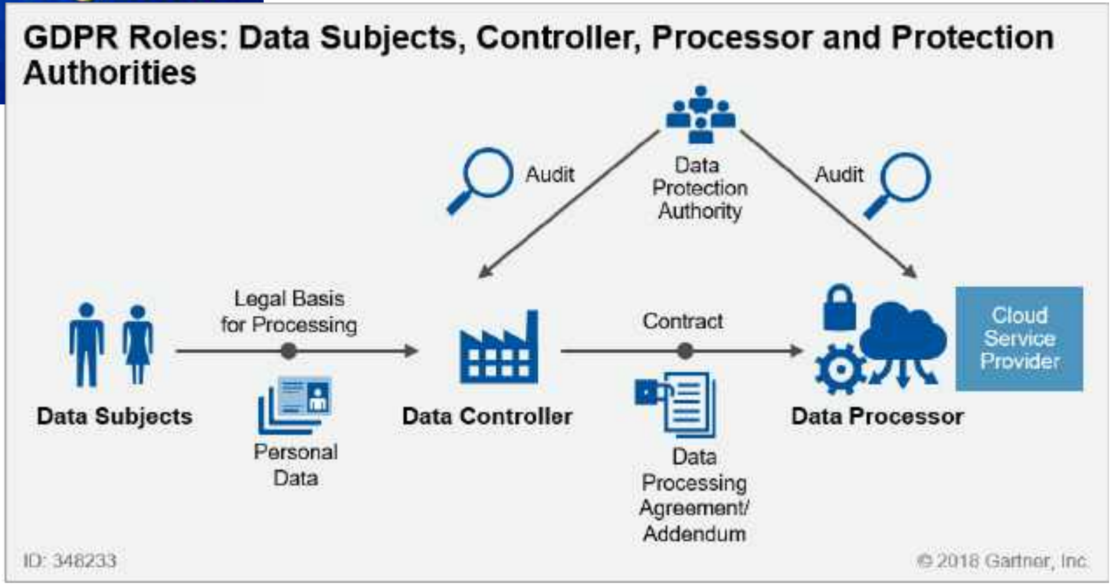
Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target , for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that

TARGET

https://en.wikipedia.org/wiki/Information_privacy
https://myphonefactor.in/2012/04/sensors-used-in-a-smartphone/
https://getsafeandsound.com/2018/09/cctv/

What is GDPR?



Increase penalty

- Up to €20 million or 2~4% turnover

Extend coverage

- Directly personal inform, e.g., location
- Indirectly personal inform, e.g., IP

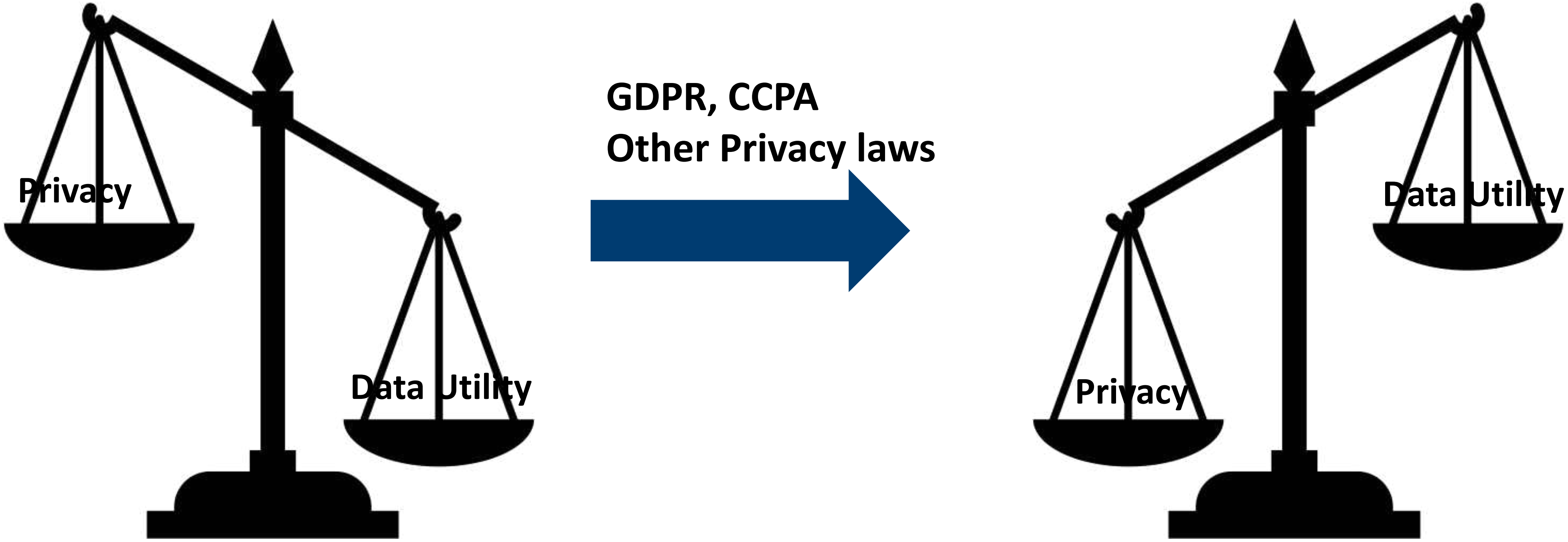
Give users more control/rights

- Be informed
- Erasure
- Access
- Rectification
- Automated decision making & profiling
- …

https://www.sentinelone.com/blog/gdpr-coming-sentinelone-can-help/
https://blogs.gartner.com/richard-watson/stop-agonising-gdrp-opt-emails-start-thinking-cloud-providers/
https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Why GDPR matters?

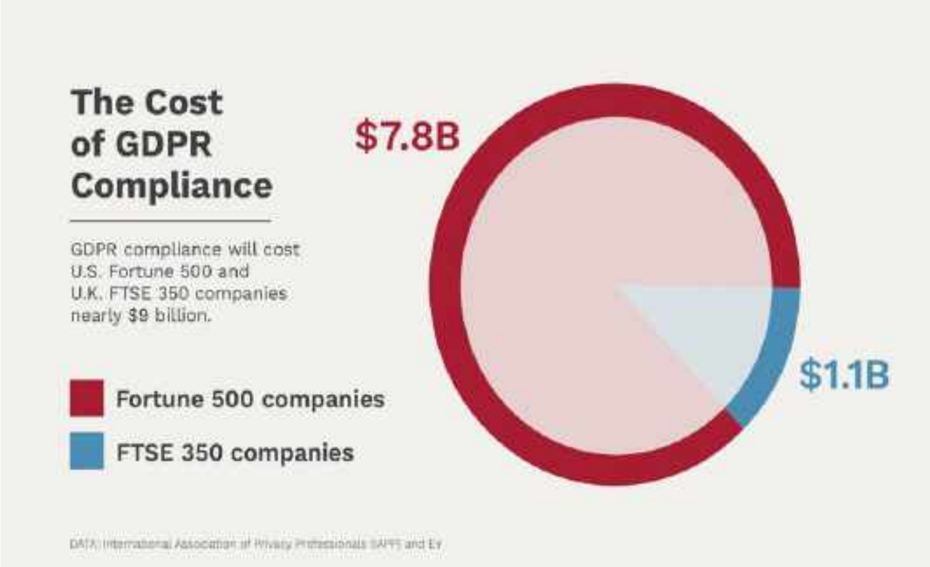
- Privacy laws & Regulations Trends



https://www.clipartmax.com/middle/m2H7G6Z5N4G6H7H7_plourde-jean-b-silhouette-libra-drawing-measuring-scales-balance-clip-art/
https://en.wikipedia.org/wiki/Information_privacy

What is happening after GDPR took effect?

Cost a lot of memory for adoption



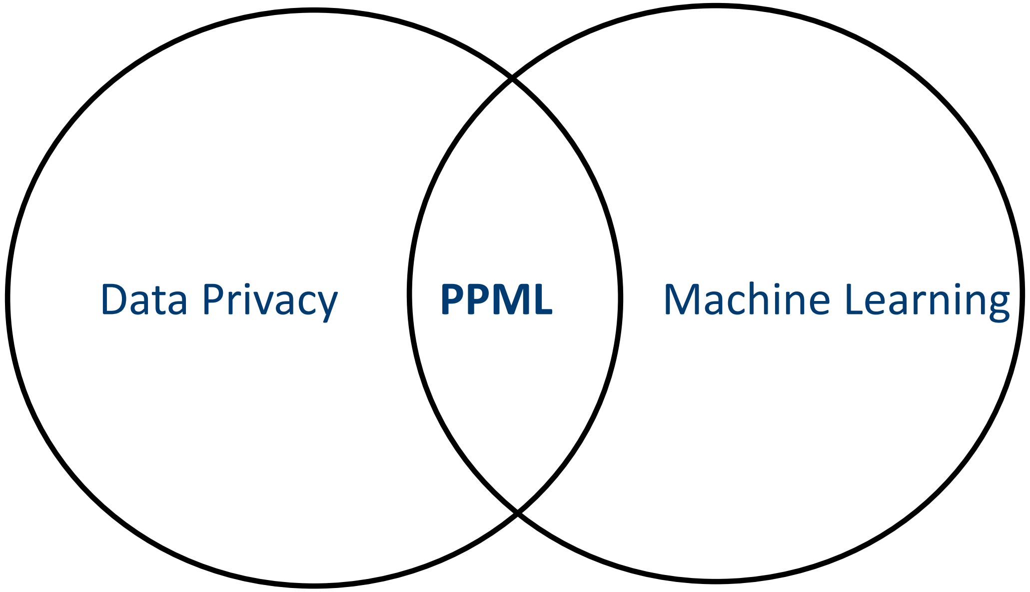
https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#696bf80a34a2

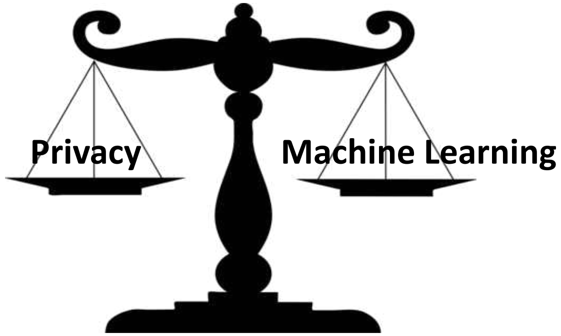
Huge Penalty: GDPR Top 3/381 cases

Country	Date	Fine [€]	Controller/Processor	Quoted Art.	Type
UNITED KINGDOM	2019-07-08	204,600,000	British Airways	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
UNITED KINGDOM	2019-07-09	110,390,200	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
FRANCE	2019-01-21	50,000,000	Google Inc.	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing

https://www.enforcementtracker.com/

PPML (Privacy Preserving Machine Learning)





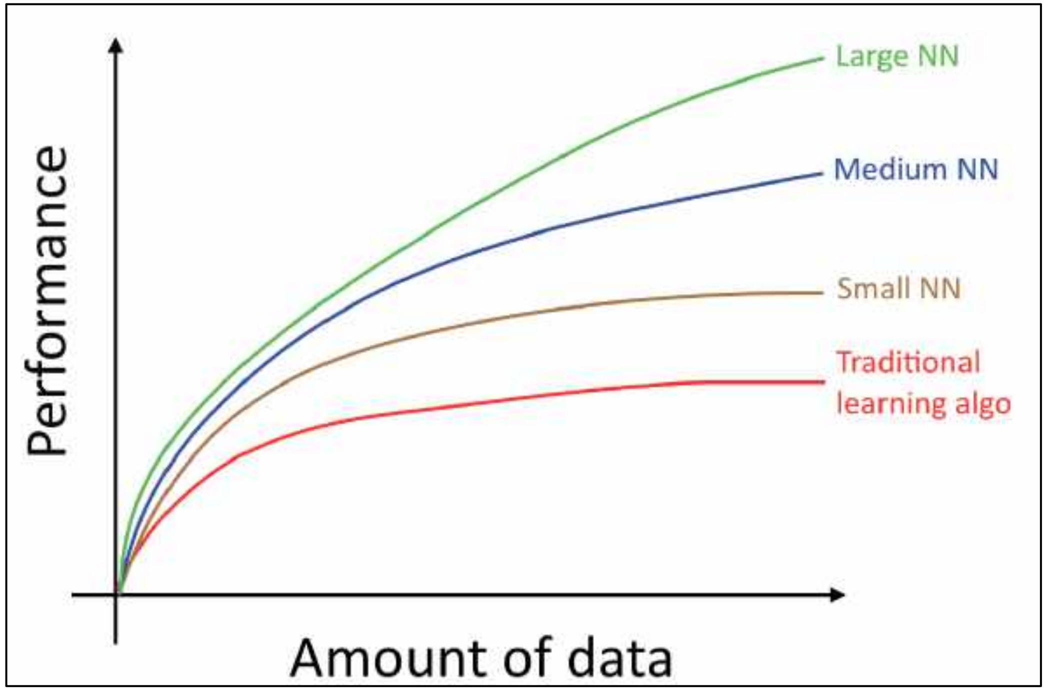
Using data to XXX without compromising privacy!

A brief hisory (from 1998 to ~):

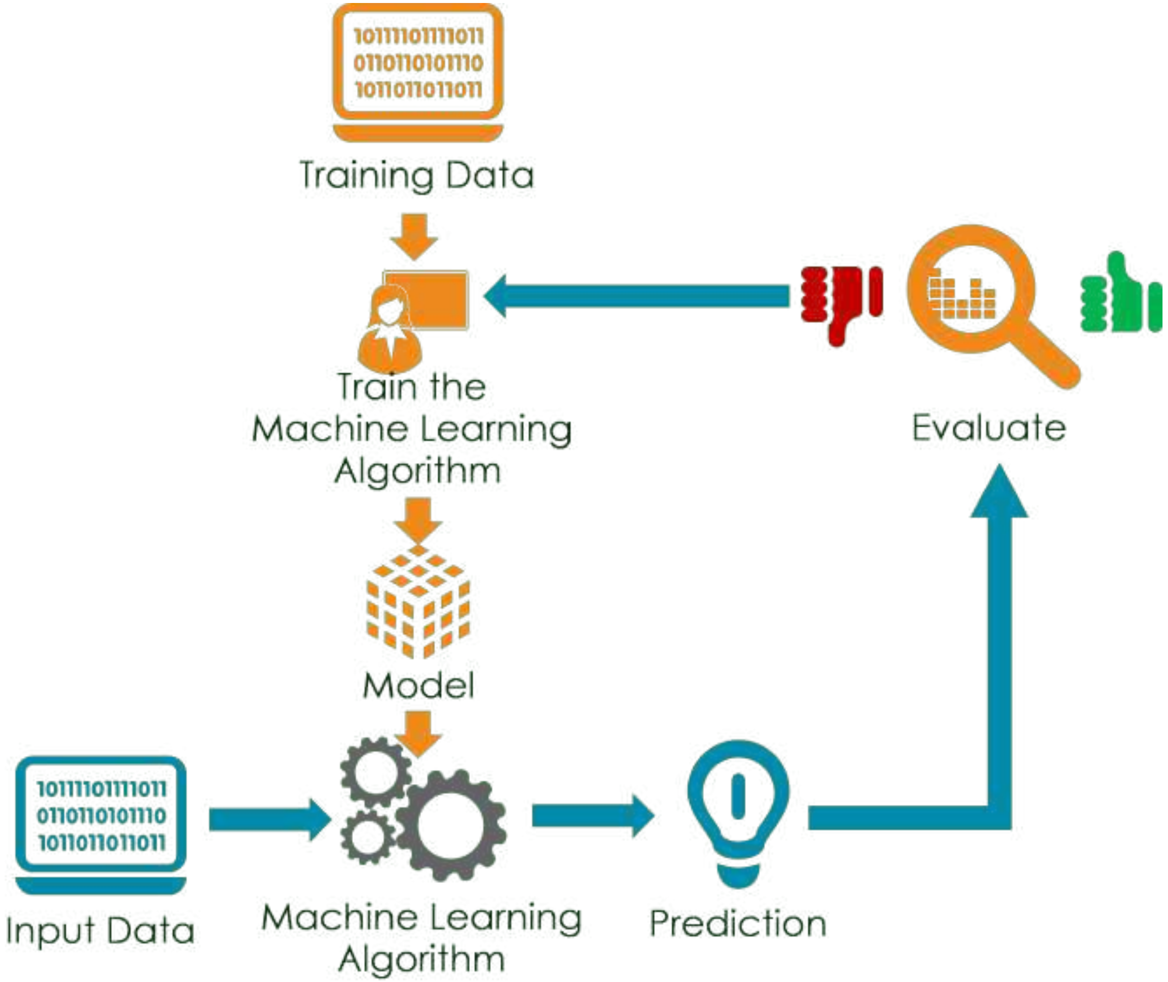
PPDS (Privacy Preserving Data Sharing)
PPDP (Privacy Preserving Data Publish)
PPDM (Privacy Preserving Data Mining)
…

PPML (Privacy Preserving Machine Learning)
PPDL (Privacy Preserving Deep Learning)
Privacy AI

Machine Learning



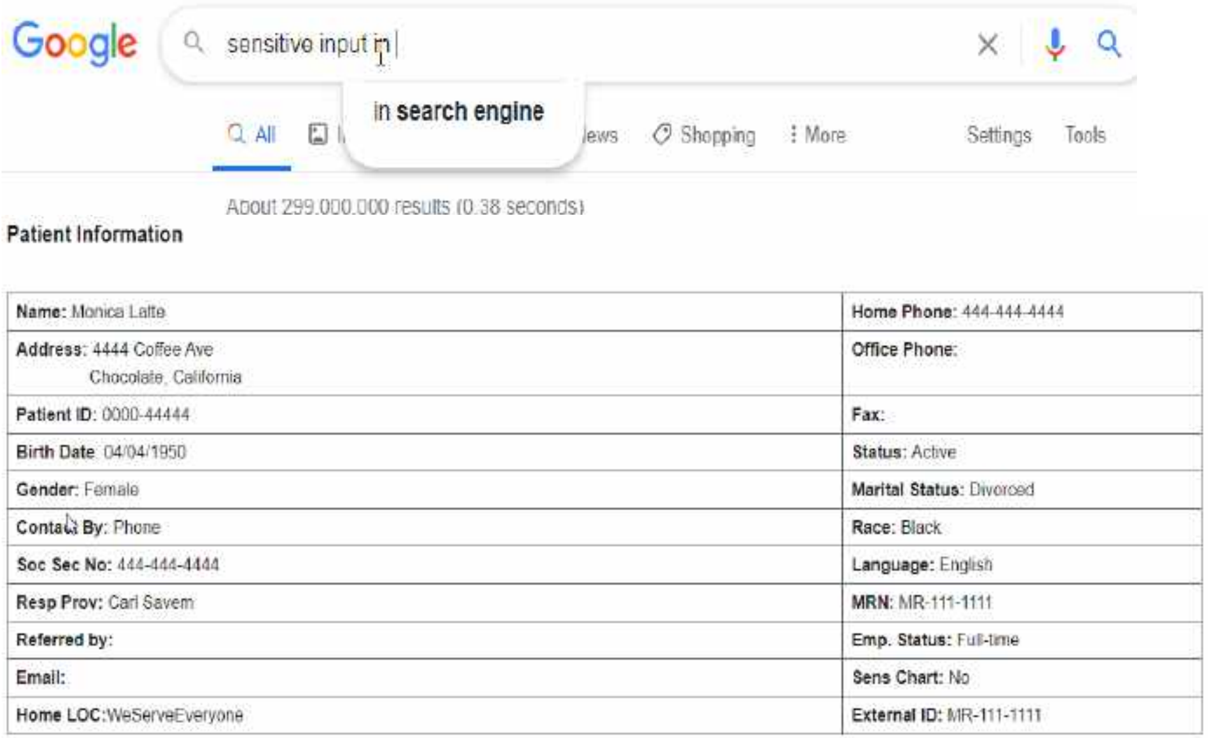
Machine Learning Yearning, Andrew Ng, 2016



https://intellipaat.com/blog/tutorial/data-science-tutorial/modeling-the-data/

PPML Attack Surface

Training Data & input data



Patient Information

Name: Monica Latte	**Home Phone:** 444-444-4444
Address: 4444 Coffee Ave Chocolate, California	**Office Phone:**
Patient ID: 0000-44444	**Fax:**
Birth Date 04/04/1950	**Status:** Active
Gender: Female	**Marital Status:** Divorced
Contact By: Phone	**Race:** Black
Soc Sec No: 444-444-4444	**Language:** English
Resp Prov: Carl Savem	**MRN:** MR-111-1111
Referred by:	**Emp. Status:** Full-time
Email:	**Sens Chart:** No
Home LOC: WeServeEveryone	**External ID:** MR-111-1111

https://www.ahrq.gov/ncepcr/tools/pf-handbook/mod8-app-b-monica-latte.html

Photos & Face

https://pythonawesome.com/vggface2-dataset-for-face-recognition/

PPML Attack Surface

Attack on models

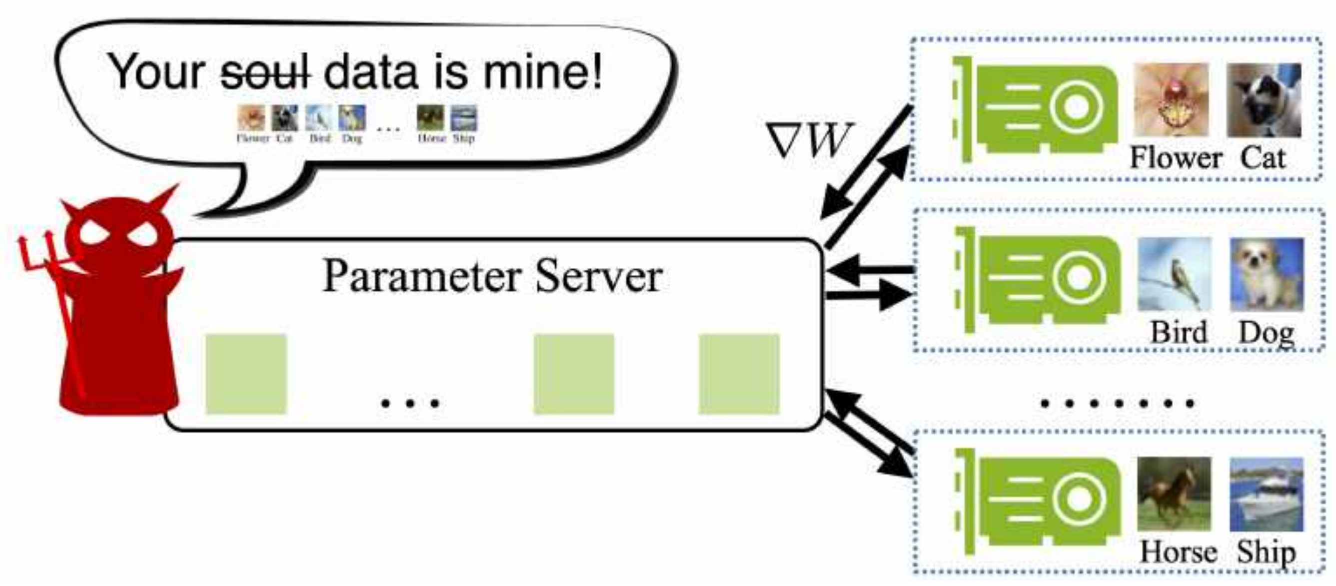
Figure 1: An image recovered using a new model inversion attack (left) and a training set image of the victim (right). The attacker is given only the person's name and access to a facial recognition system that returns a class confidence score.

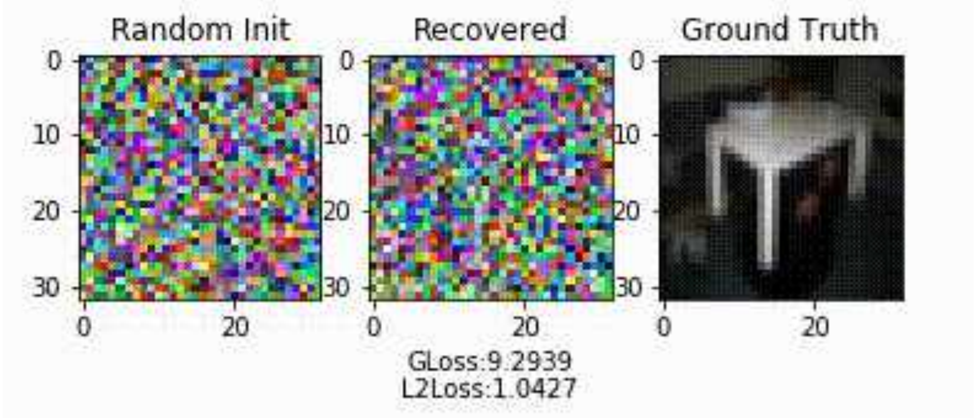
Figure 7: Reconstruction without using Process-DAE (Algorithm 2) (left), with it (center), and the training set image (right).

Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures, CCS 2015

PPML Attack Surface

Attack on Gradient

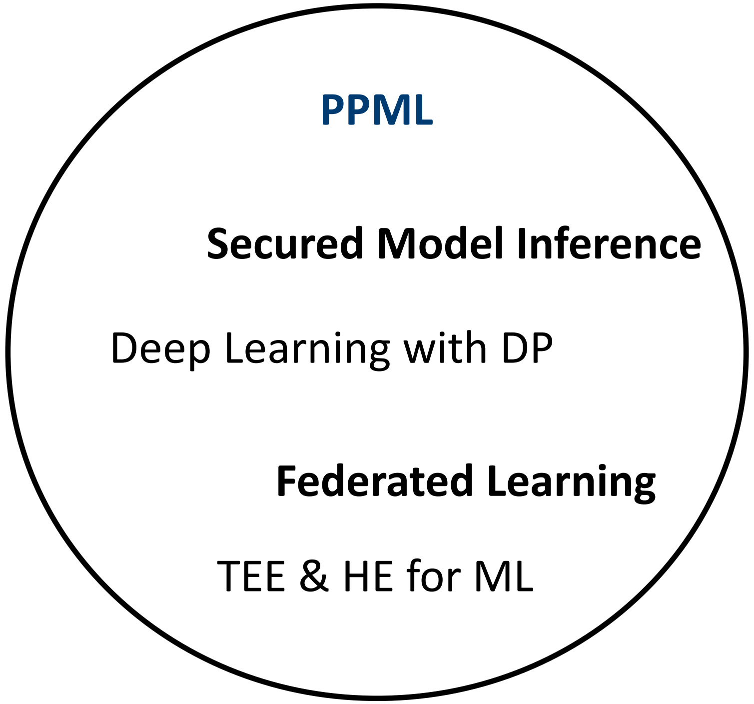




Deep Leakage from Gradients, 2019, NIPS

PPML related Techniques & Hot topic

- PPML Related Techniques
  - TEE (Trusted Execution Environment)
  - HE (Homomorphic Encryption)
  - DP (Differential Privacy)
  - ~~SMPC/MPC (Secure Multi-Party Computation)~~
- PPML Hot Topic
  - Secured Model Inference
  - FL (Federated Learning)

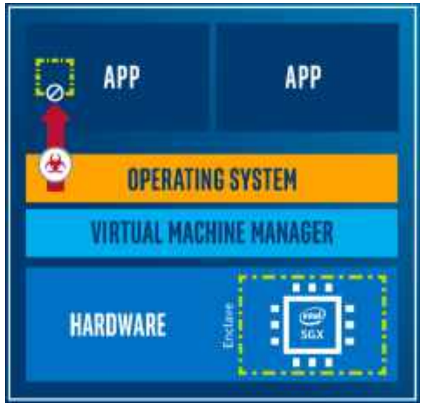


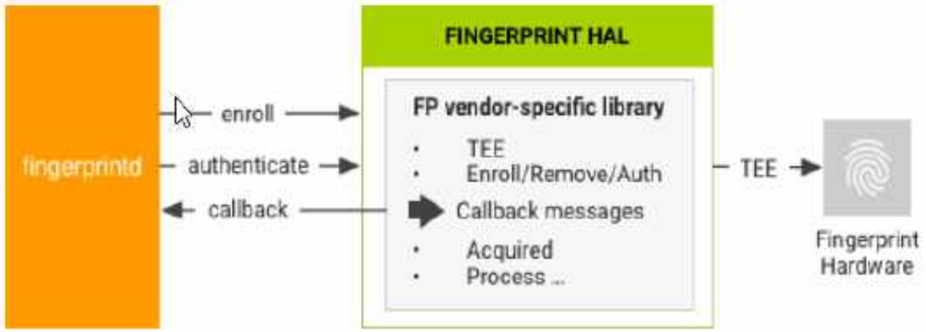
TEE (Trusted Execution Environment)

Hardware Security Implementation

Main solutions

- ARM TrustZone
- Intel SGX





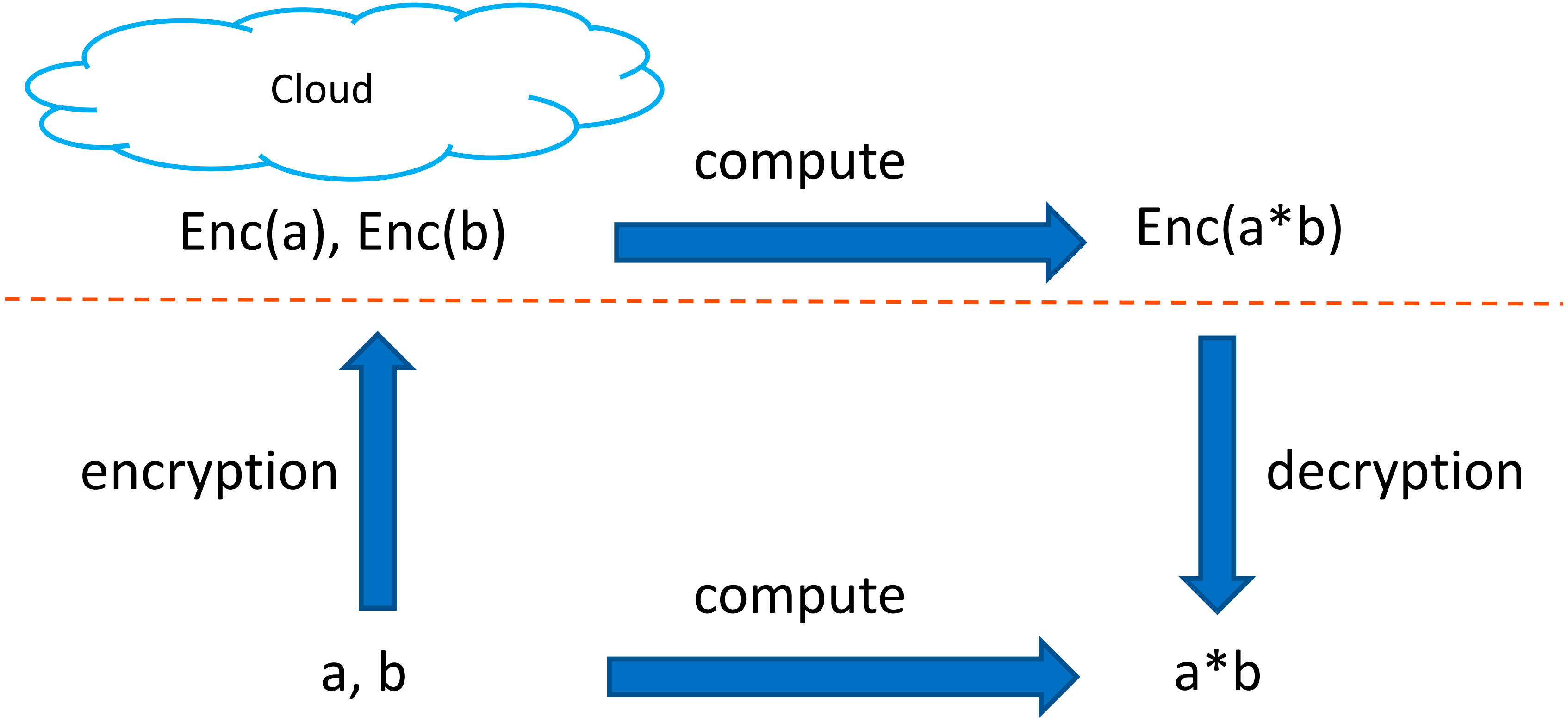
Using secured API, need to redesign your app

Now, we have a solution in Part 2

https://source.android.com/security/authentication/fingerprint-hal
https://en.wikipedia.org/wiki/Touch_ID

HE (homomorphic encryption) 同态加密

Compute with encrypted Data



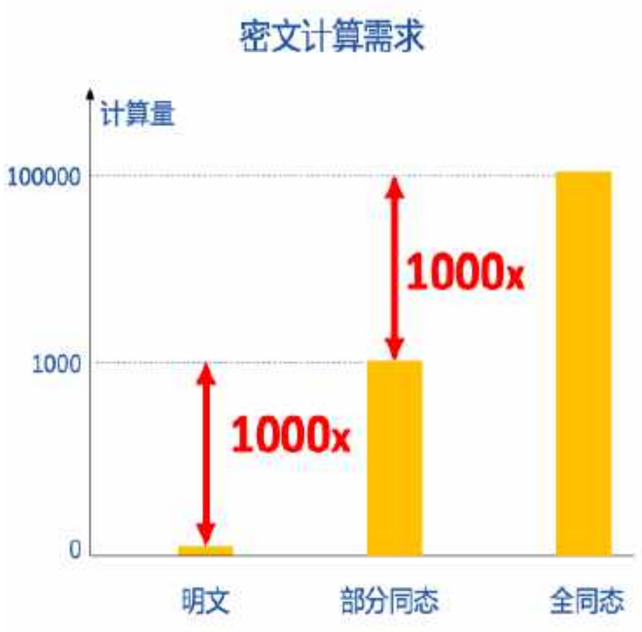
First proposed in 1978, first FHE 2009

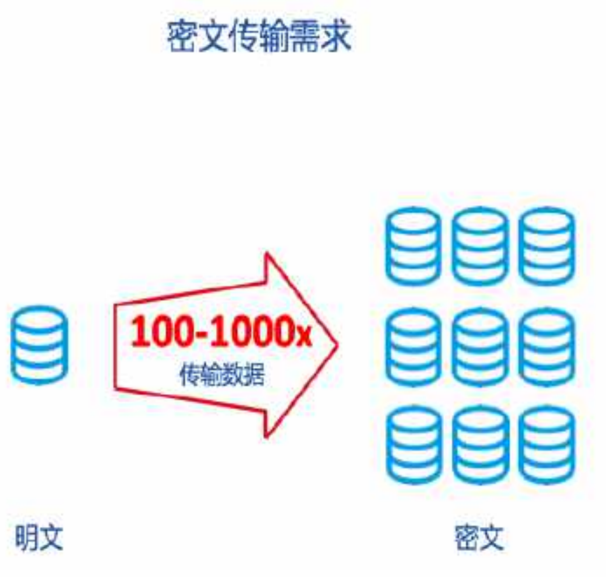
HE (homomorphic encryption) 同态加密

- Full Homomorphic Encryption (任意计算)
- **Partial Homomorphic Encryption (限定计算)**

Performance is not good enough

Some operations are not supported

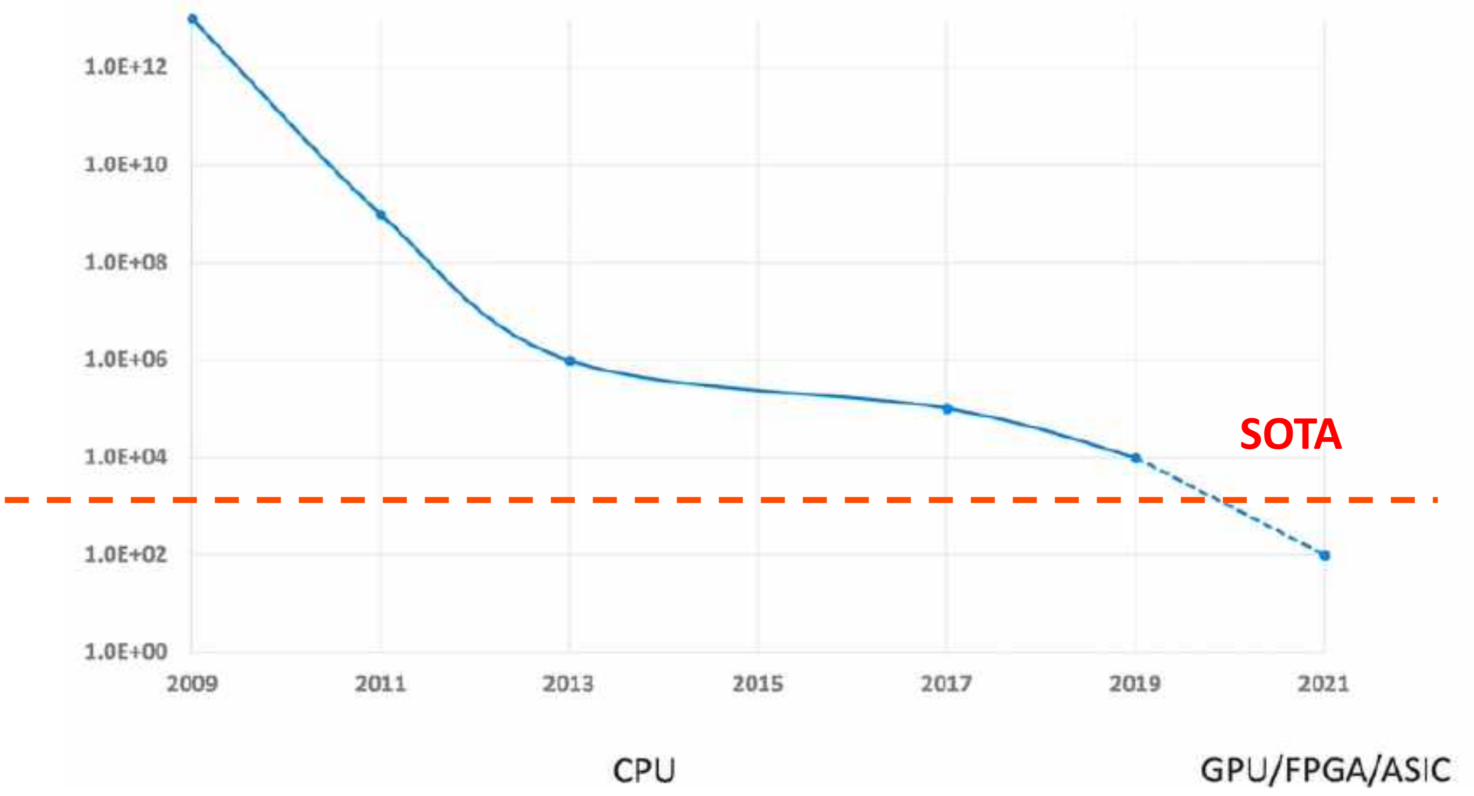




https://www.leiphone.com/news/202006/SbATMUxnVFkGtcSj.html

HE (homomorphic encryption) 同态加密

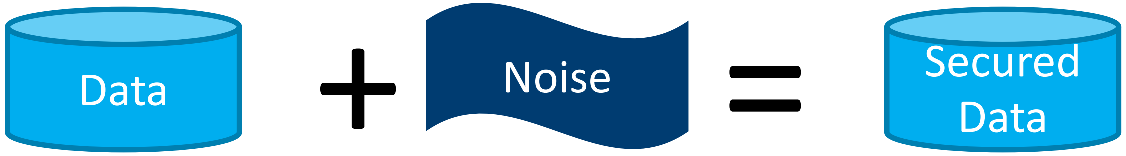
Bright future for HE

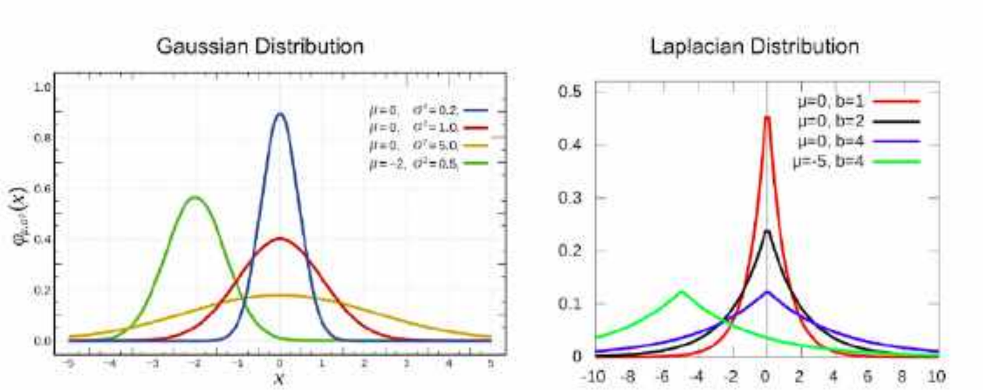


[Kristin Lauter's TED Talk on Private AI at Congreso Futuro during Panel 11 / SOLVE]
[https://www.microsoft.com/en-us/research/project/microsoft-seal/]

Differential Privacy (DP) 差分隐私

Noise based

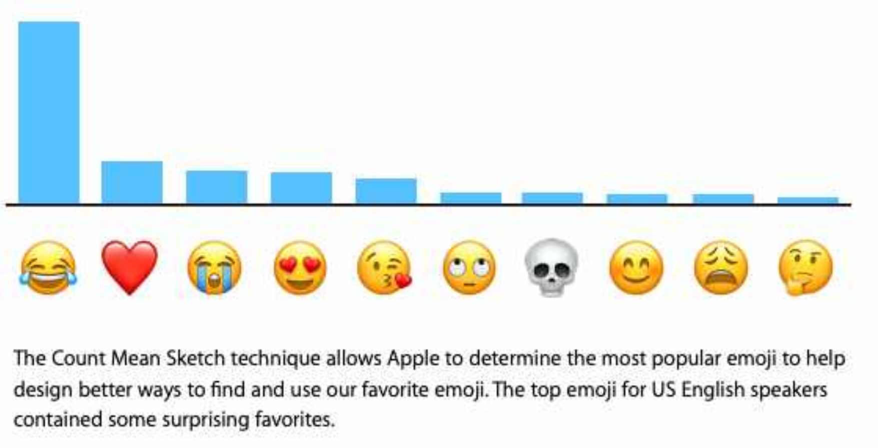




https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf
https://github.com/google/differential-privacy

Proposed in 2006-2008 by Dwork from MSR

Privacy/Noise budge is hard to define
Impact Accuracy

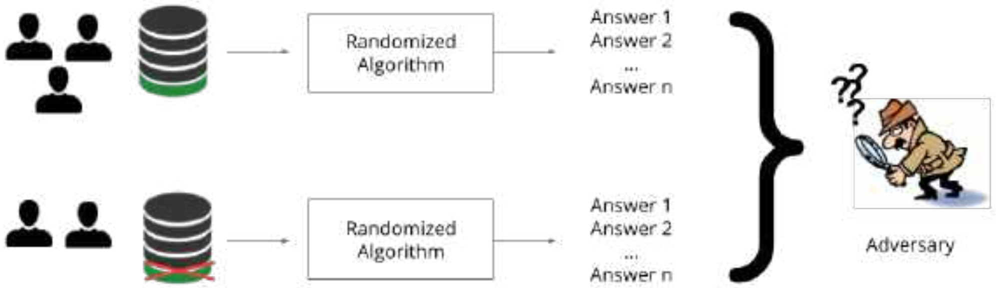


Already used in

Differential Privacy (DP) 差分隐私

With DP you can make your model learning common patterns in a dataset without memorizing individual examples

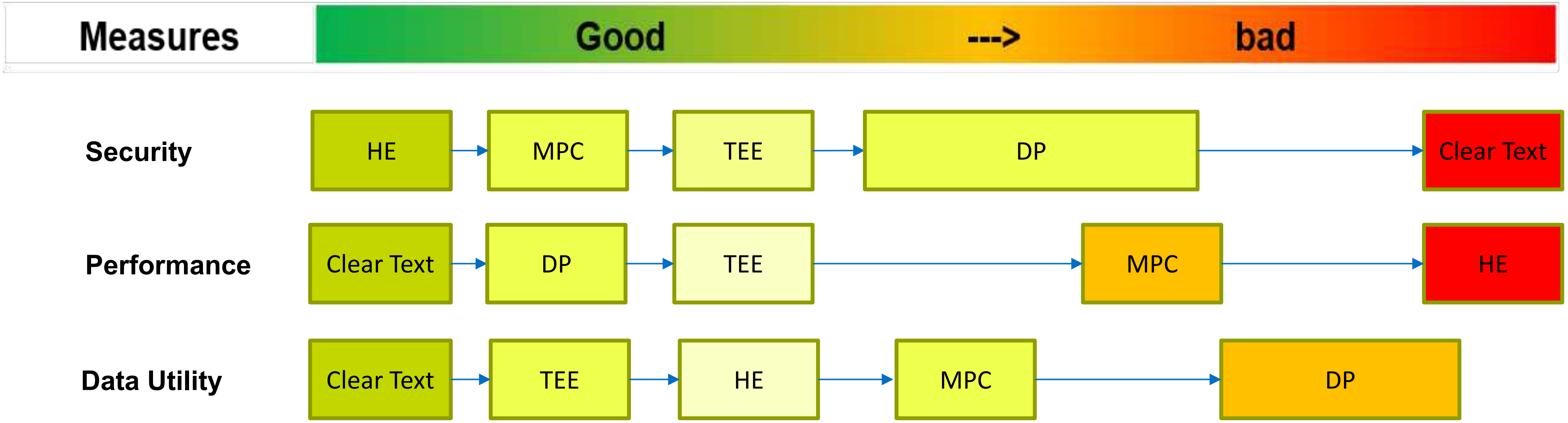
- **Add noise in train data**
- **Add Nosie in SGD**



http://www.cleverhans.io/privacy/2018/04/29/privacy-and-machine-learning.html

Learning Differentially Private Recurrent Language Models. *ICLR 2018*

Comparison of PPML Technologies



Note that DP is a little special because of budget

A Simple example with TEE, HE & DP

- 部门同事一起点外卖，但是要投票决定，让其中一个人取外卖
  - 被投最高票的人去取外卖
  - 大家都不想被他知道我投了他/她（因为他可能是你老板）

- 怎么做呢？

A Simple example with TEE, HE & DP

- TEE (加密数据送进TEE，解开后计算)
  - 大家把投票折叠（加密）起来，放到小黑屋里面，让一个可信的同事计票，例如HR或者产品经理
- HE (加密数据直接计算)
  - 大家把投票结果用HE加密，让任意同事（甚至老板）去计票，然后把计票结果解密
- DP (计算加了噪声的数据)
  - 给每一票增加噪声扰动，每一票都无法解读，但统计结果是基本正确

无论哪种方法，大家都无法获取投票的真实内容，投票人的隐私被保护

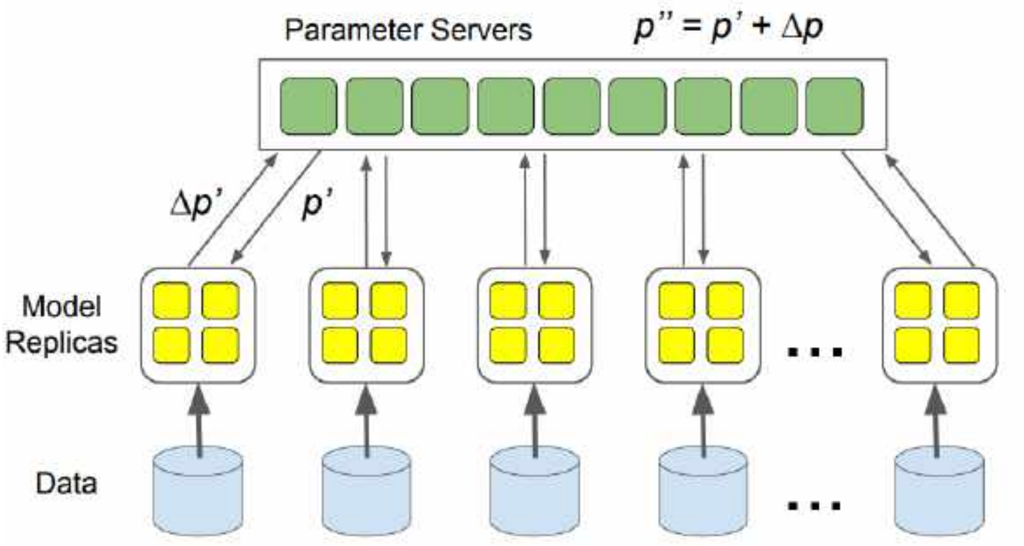
Federated (Machine) Learning 联邦(机器)学习

- Address Information silo

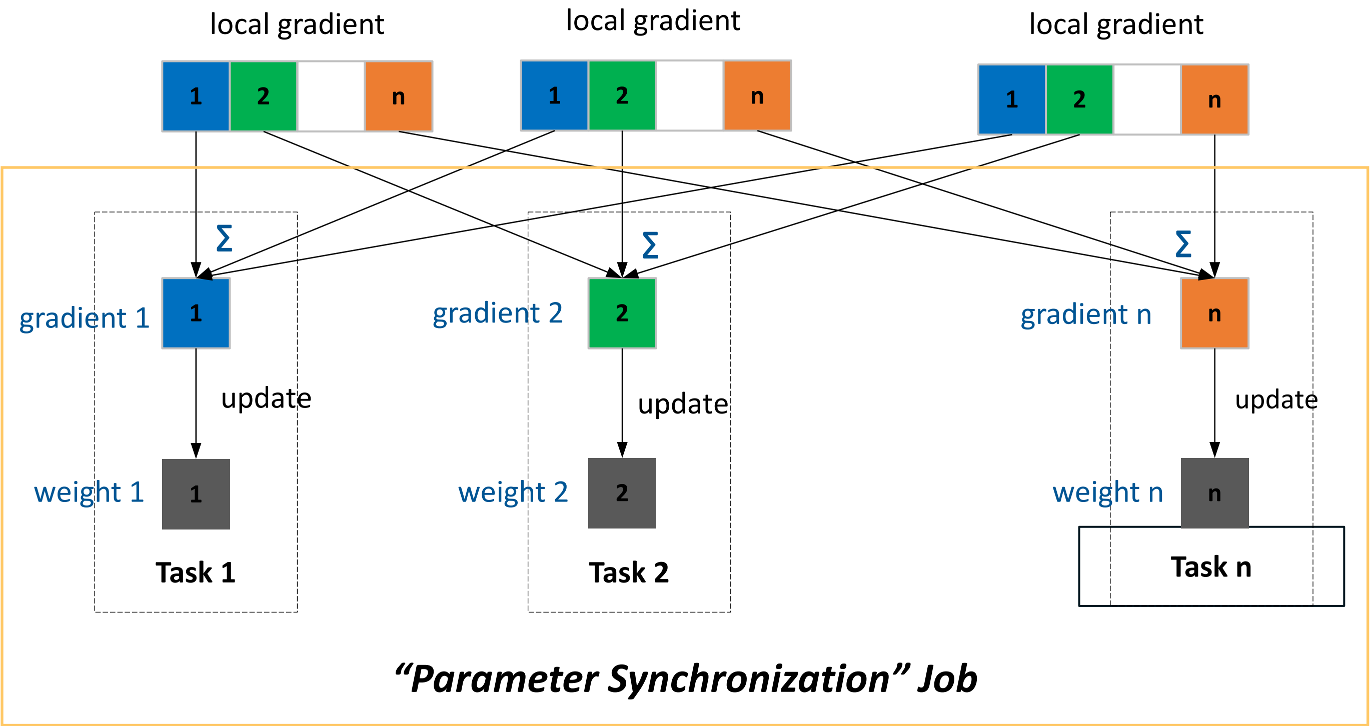
https://www.enterpriseirregulars.com/10802/information-silos-and-it-governance-failure/

Distributed Training in Deep Learning

Parameter Server



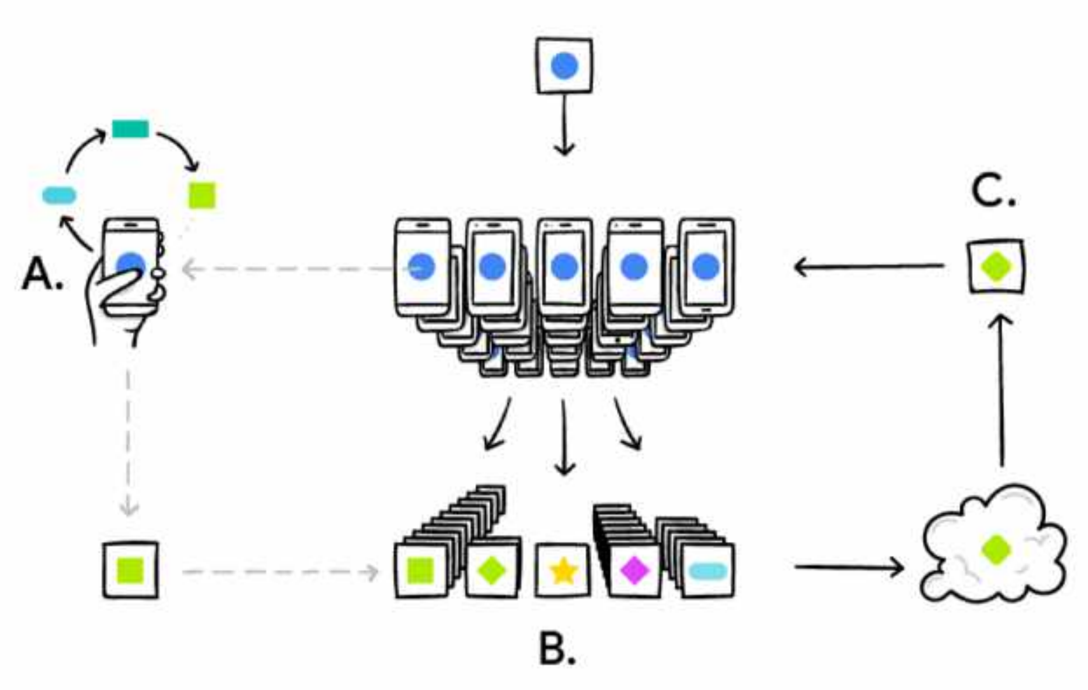
BigDL Allreduce



Accelerating Training with more resource/nodes

https://static.googleusercontent.com/media/research.google.com/en//people/jeff/BayLearn2015.pdf

Federated (Machine) Learning 联邦(机器)学习



Google 2016-2018 on **mobile device (in production)**

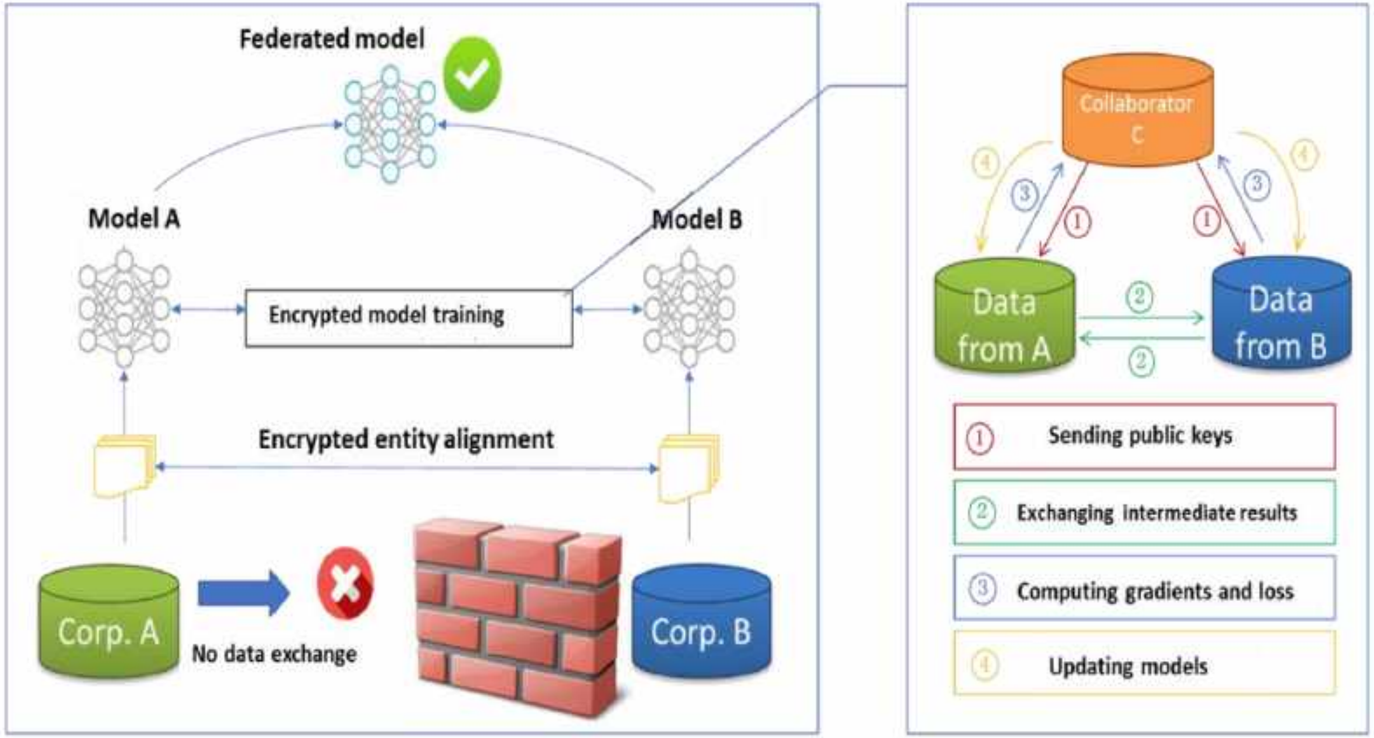
Motivation

- More/better data in user device
- Better model based on these data

[TensorFlow Federated]

[TensorFlow Privacy]

Federated (Machine) Learning 联邦(机器)学习



Webank (Yang Qiang etc)

Extend scope of Google's Federated Learning

(https://www.fedai.org/ & FATE)

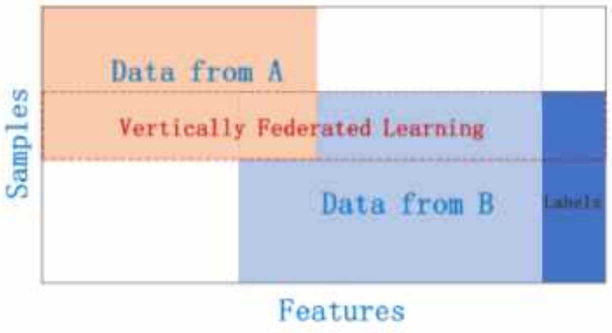
Federated Learning White Paper and RFC

Motivation

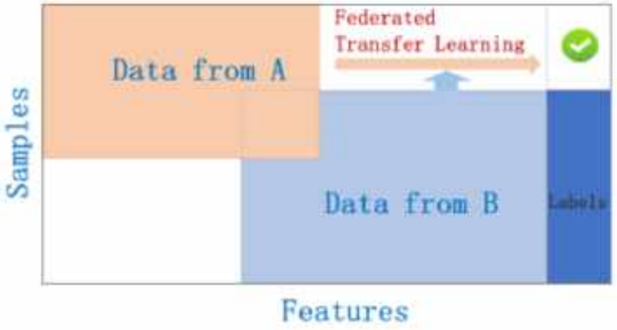
- **More/better data across different Crops**
- **Better model based on these data**
- **Federated Data Union (long term)**

Federated (Machine) Learning 联邦(机器)学习

Horizontally Federated Learning



Vertically Federated Learning



Federated Transfer Learning

Party A

Party B

Location	Time
Georgia	2018.5
Florida	2019.1
Hawaii	2017.3
Kansas	2018.5
Georgia	2018.10
Florida	2019.9

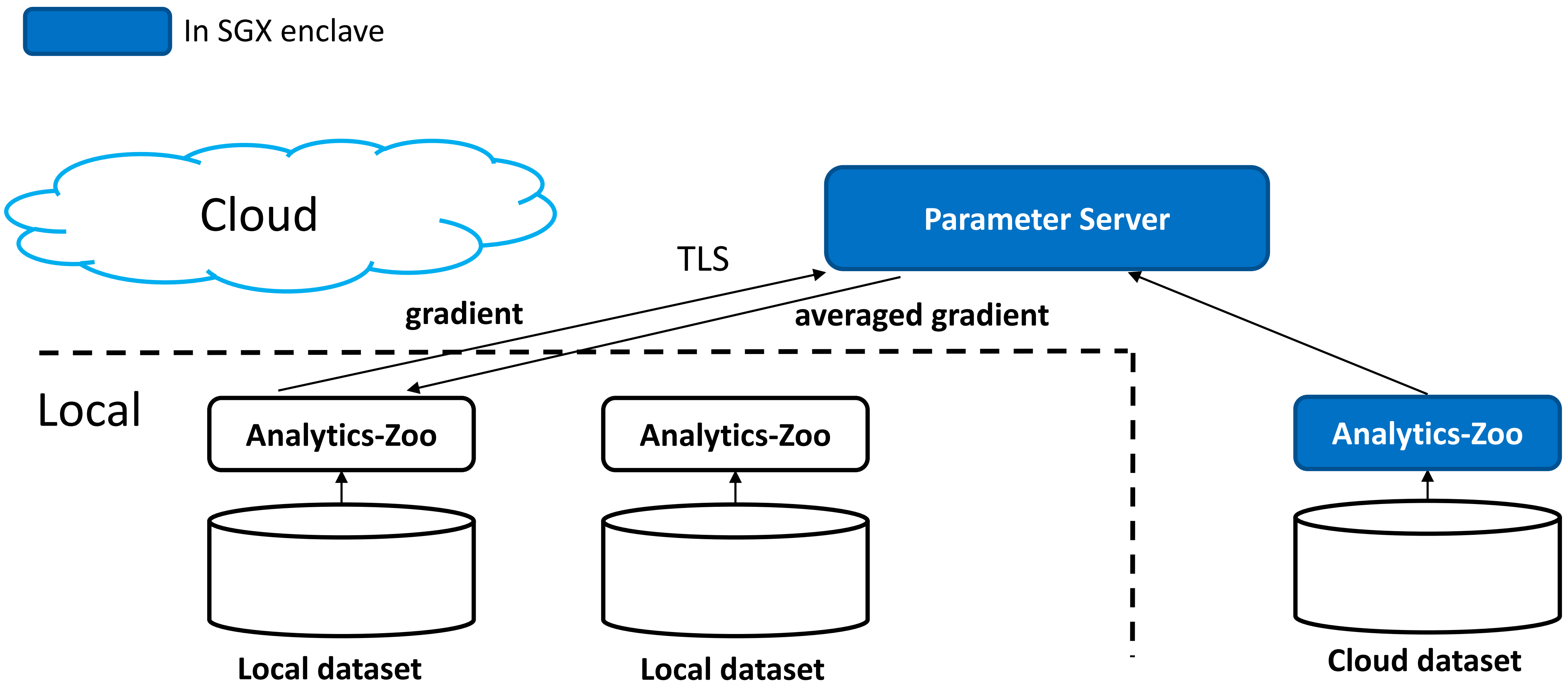
Party A

Sports	Photography	Movie	Food
Y	N	N	N
N	N	N	N
Y	N	N	Y
Y	Y	N	N
N	Y	Y	N
N	Y	Y	Y

Party B

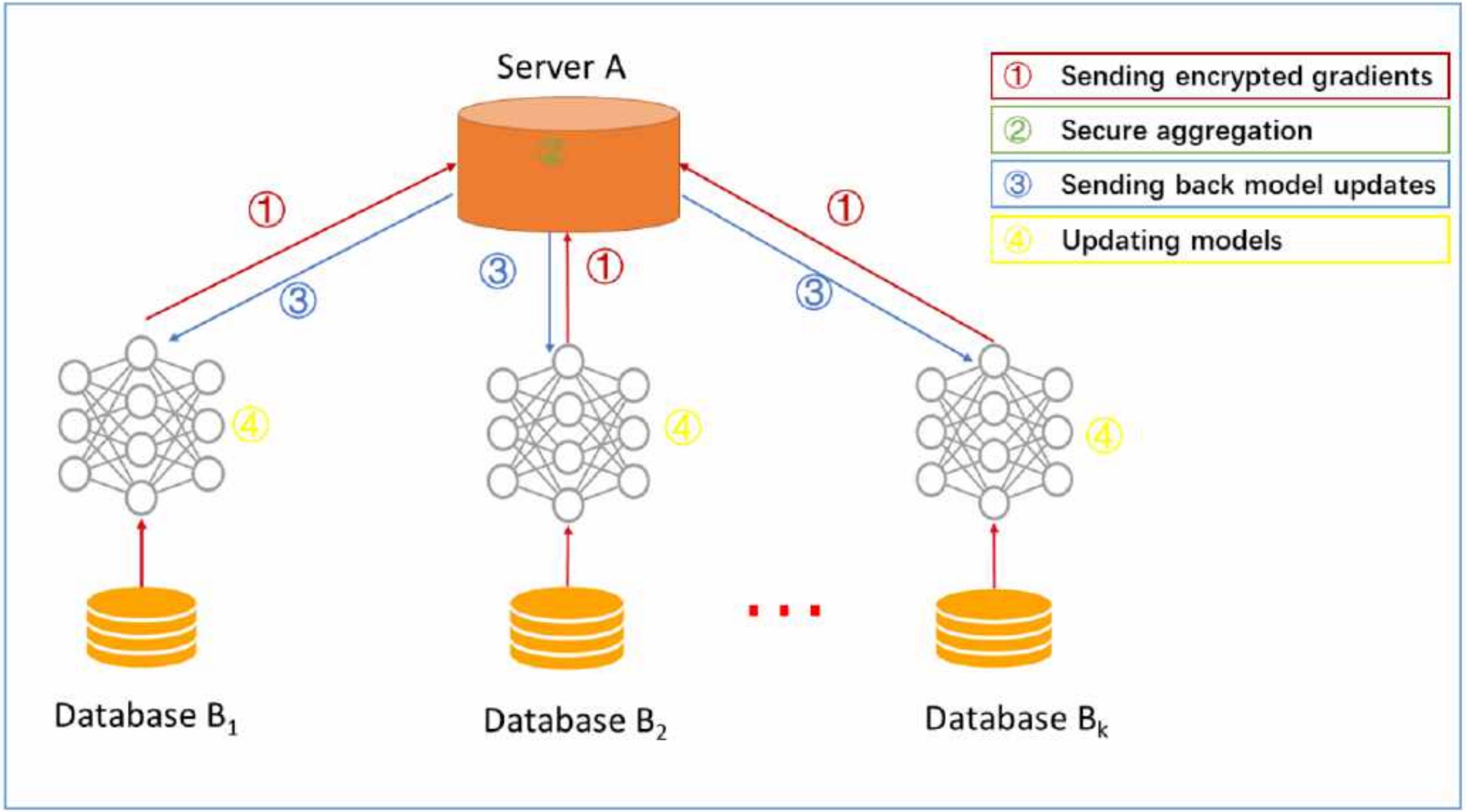
https://www.infoq.cn/article/gtvvYvcWecNKURxeYapD

Federated Learning with TEE



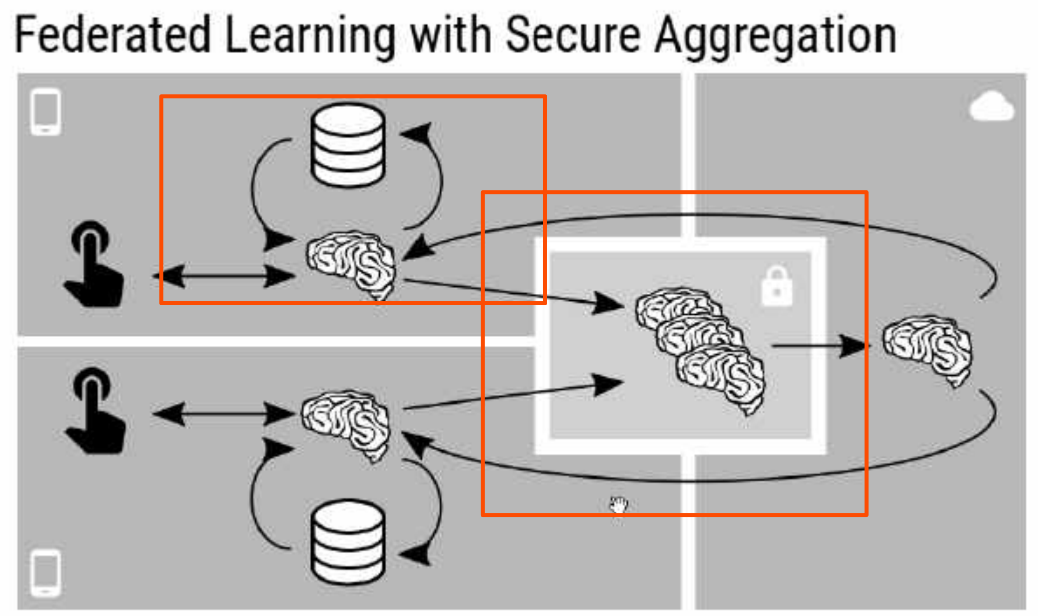
https://github.com/intel-analytics/analytics-zoo All Analytics-Zoo examples & models are supported

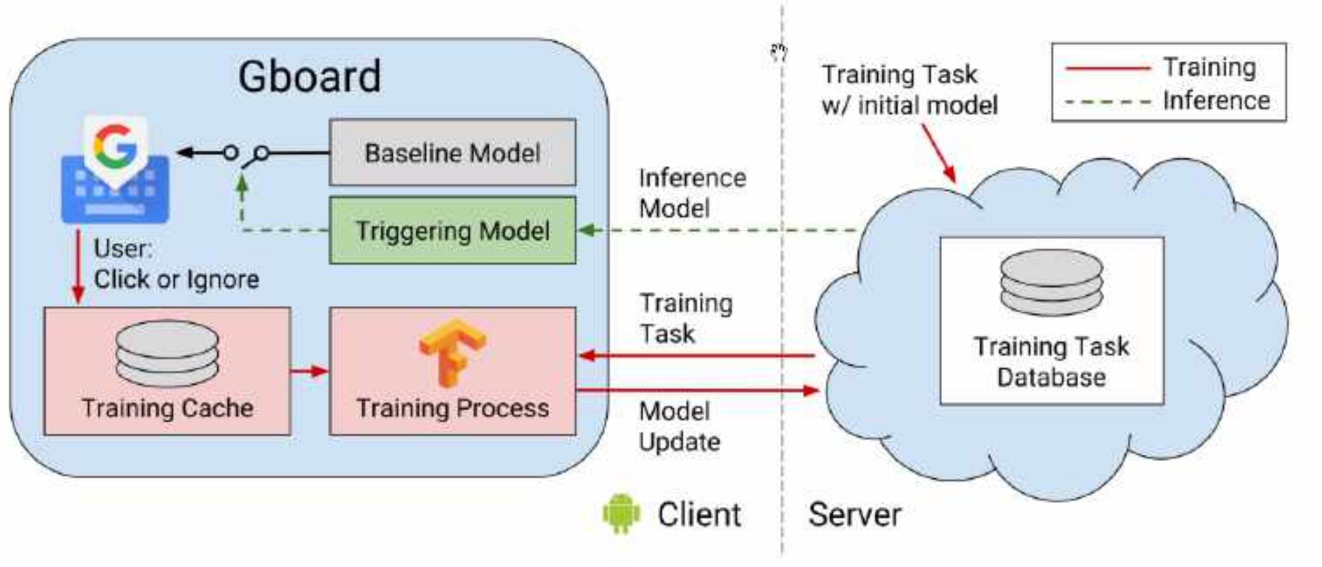
Federated Learning with HE



https://github.com/FederatedAI/FATE

Federated Learning with DP





Secured aggregate with DP

Applied Federated Learning: Improving Google Keyboard Query Suggestions

intel®

Artificial
intelligence

Legal Notices and Disclaimers

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

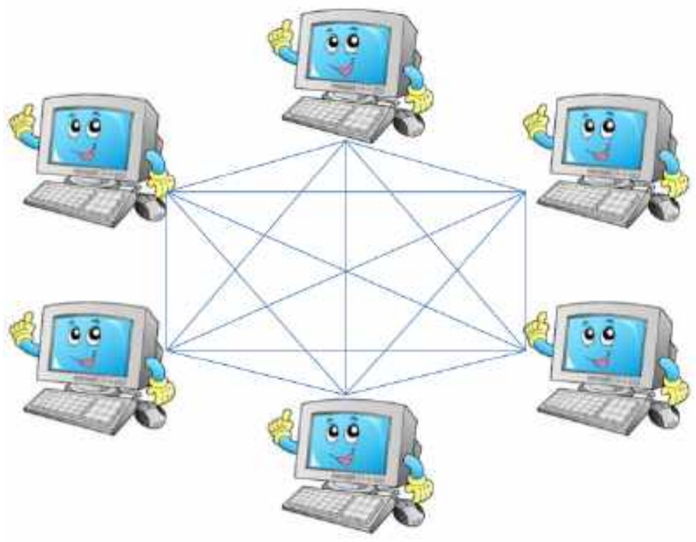
Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

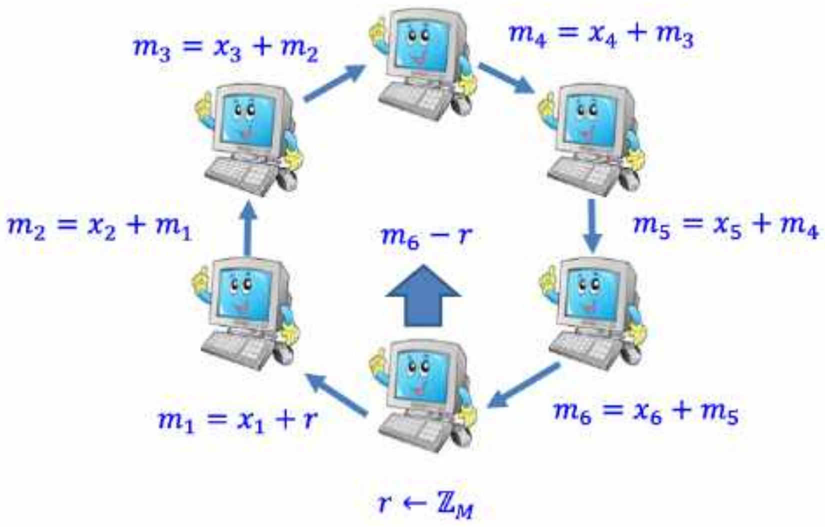
Intel, the Intel logo, Xeon, Xeon phi, Lake Crest, etc. are trademarks of Intel Corporation in the U.S. and/or other countries.

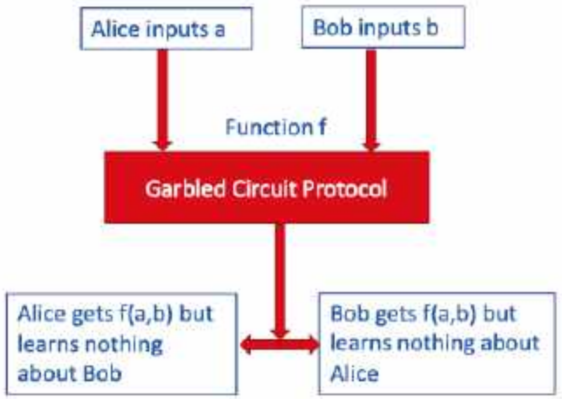
*Other names and brands may be claimed as the property of others.

© 2019 Intel Corporation

Secure Multi-party computations (SMPC) 安全多方计算







Yao's Garbled Circuit Protocol (Andrew Yao, 1980s)

Secure Multiparty Computation: Introduction