隐私计算三剑客在营销中的应用

陈治宇 百度 资深安全工程师

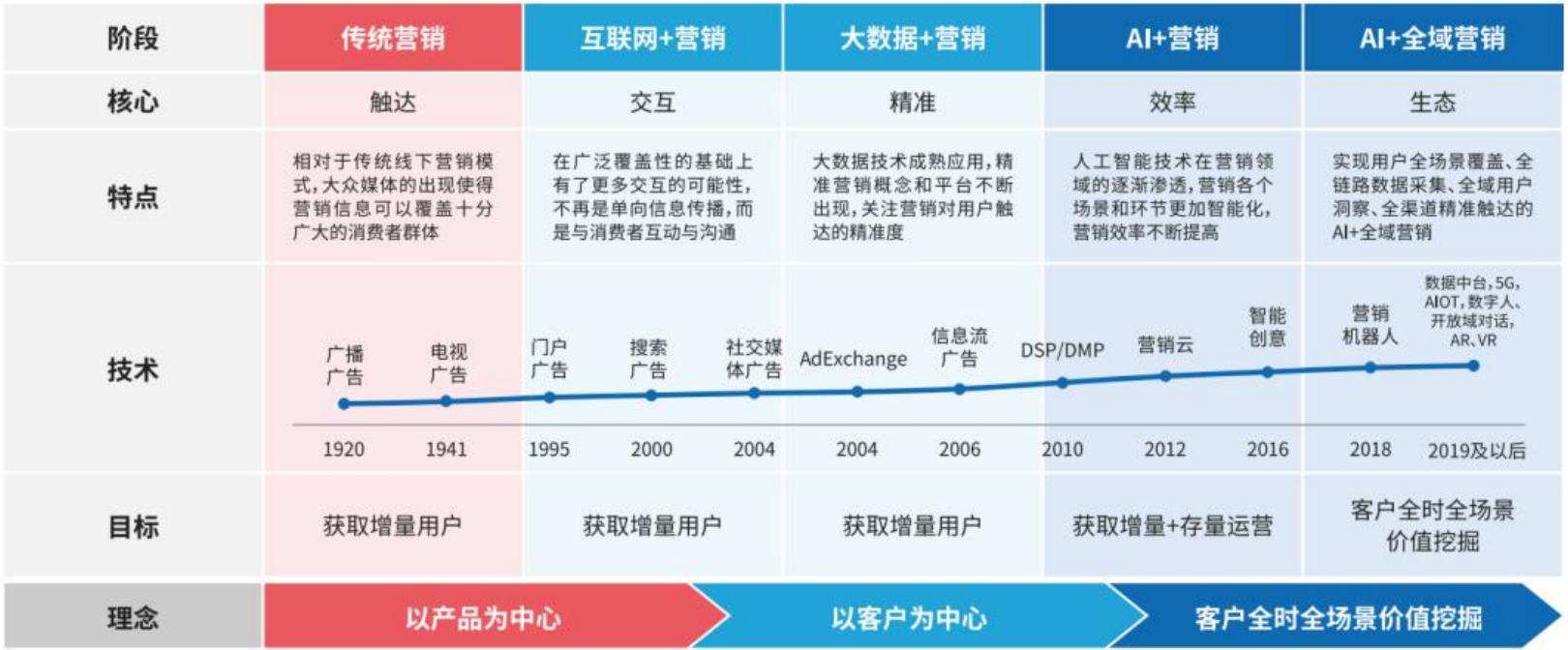
目录 CONTENT

01

数字营销与隐私

替换文字内容，点击添加相关标题文字

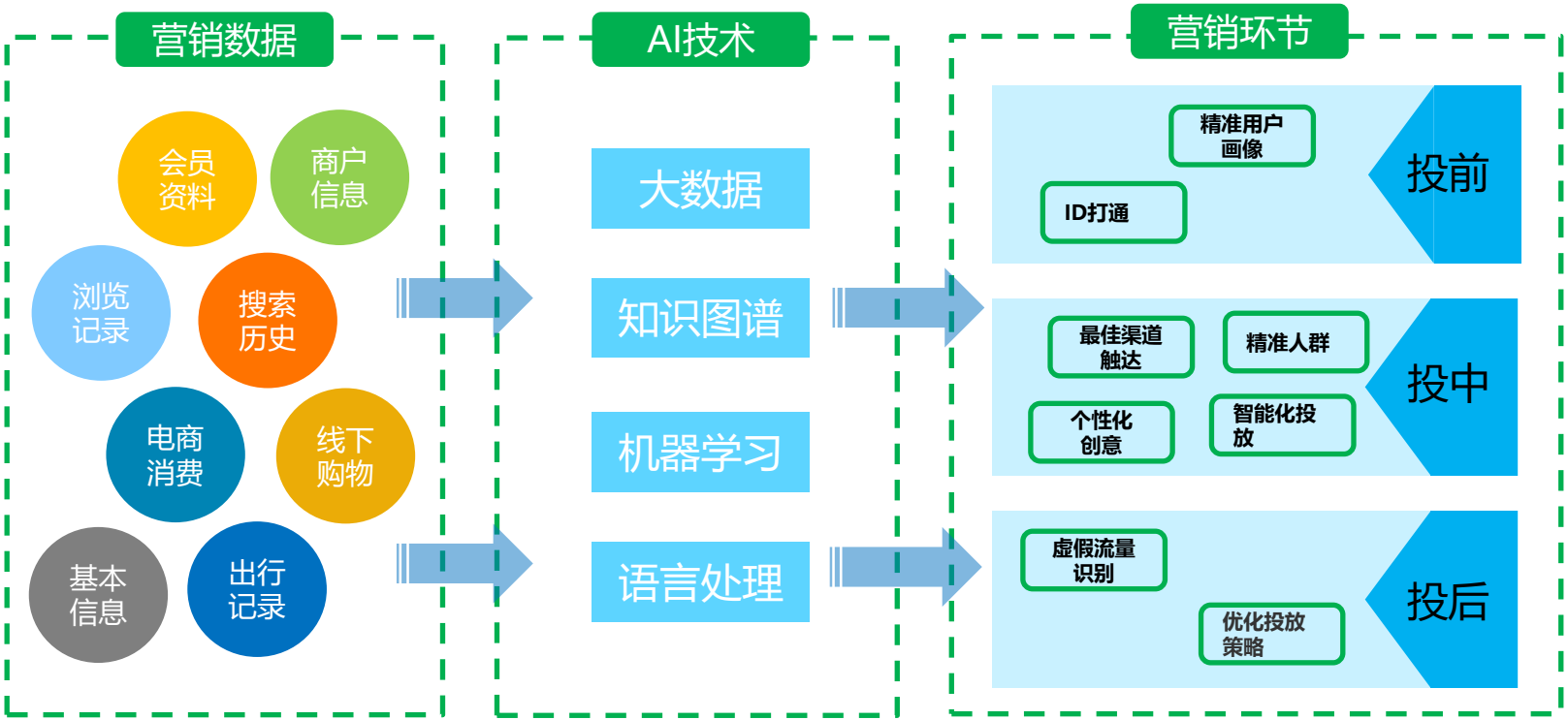
营销技术的发展



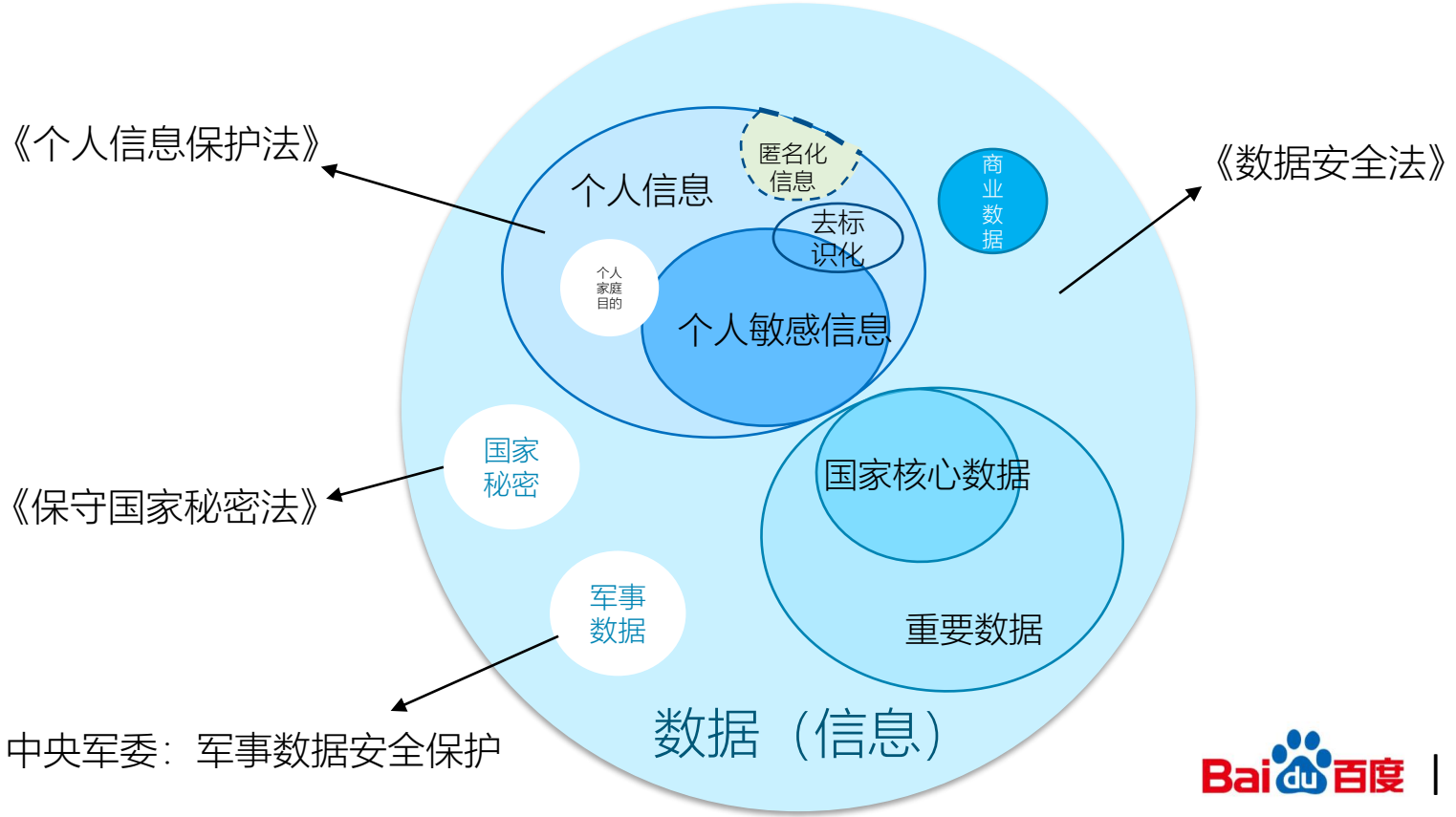
资料来源：知萌咨询公共资料整理。

图表引自：中国广告协会《2022AI营销白皮书》

AI+营销：涉及隐私数据



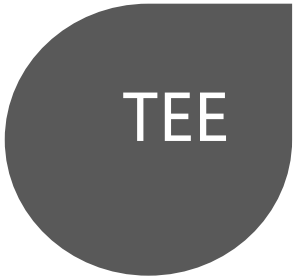
隐私数据



什么是：隐私计算?

- 解决的问题：“数据可用不可见”
- 什么效果：仅获取到”结果”，但得不到以外的信息
- 价值：“使用权”和“所有权”分离
- 怎么实现：软件，硬件，不软不硬

隐私计算：三剑客



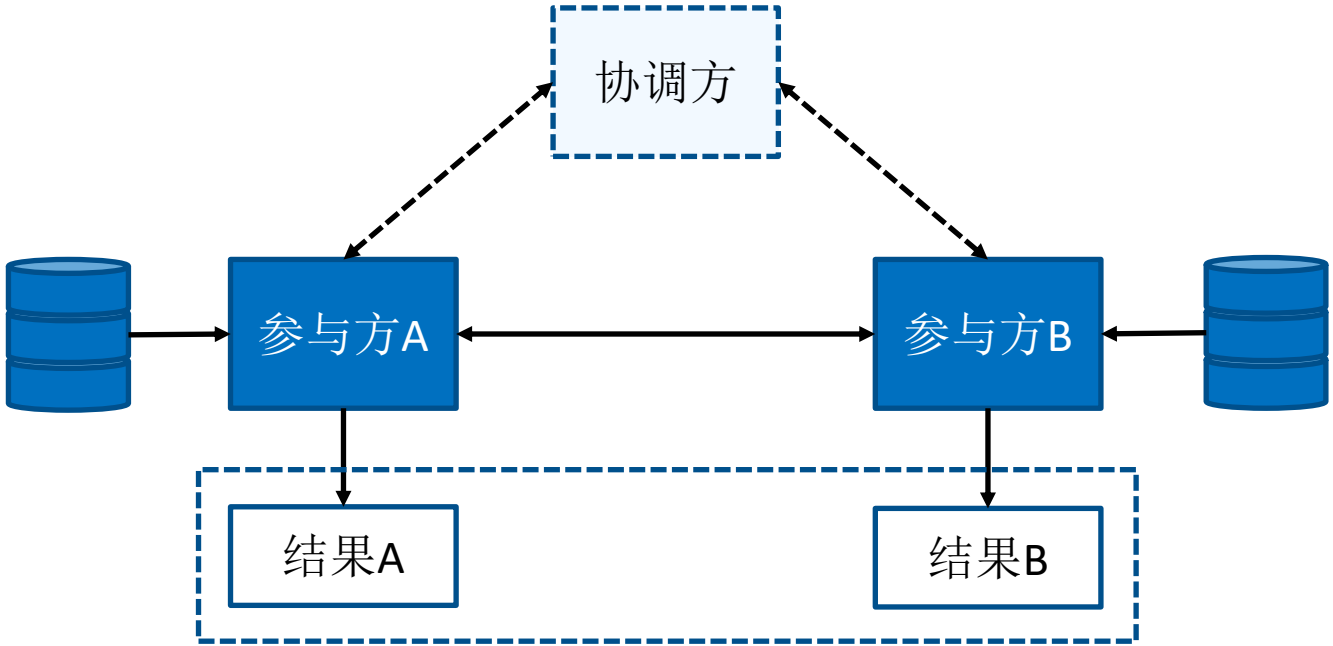
Baidu 百度 | DataFun.

02

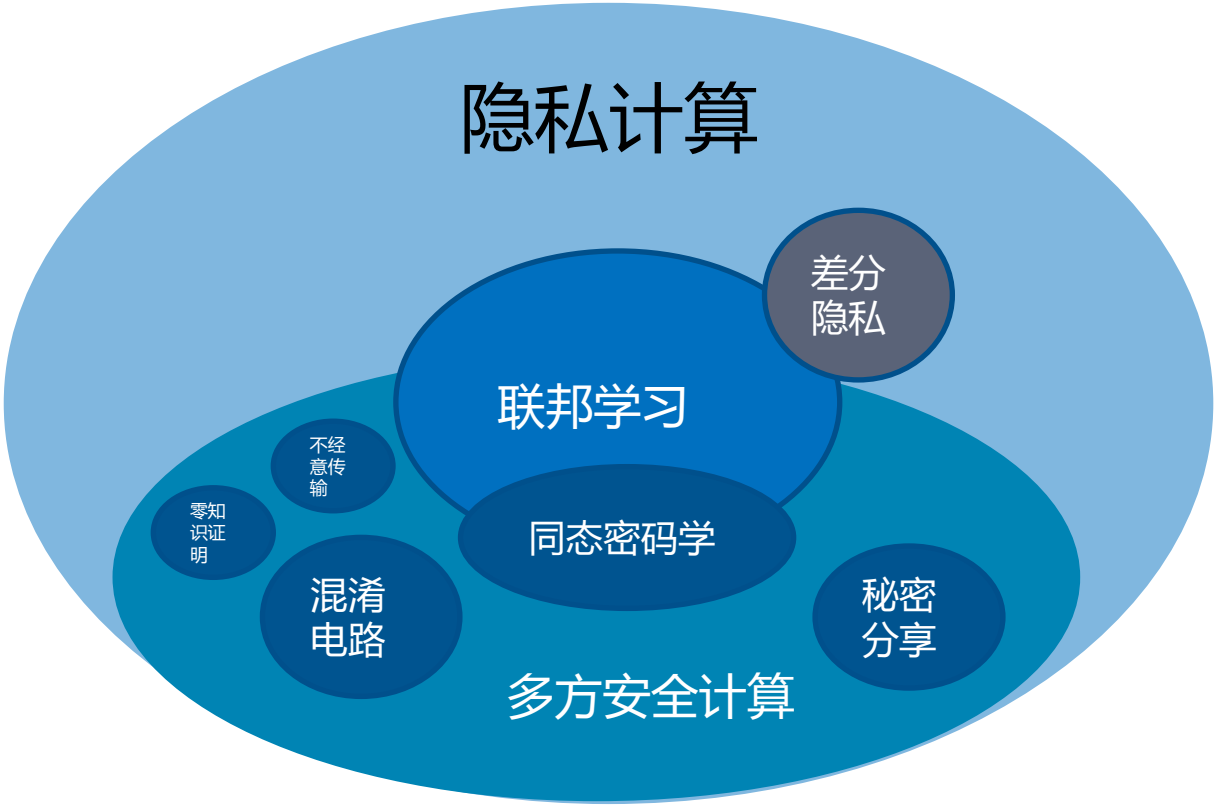
联邦学习/多方安全计算

替换文字内容，点击添加相关标题文字

联邦学习（FL）



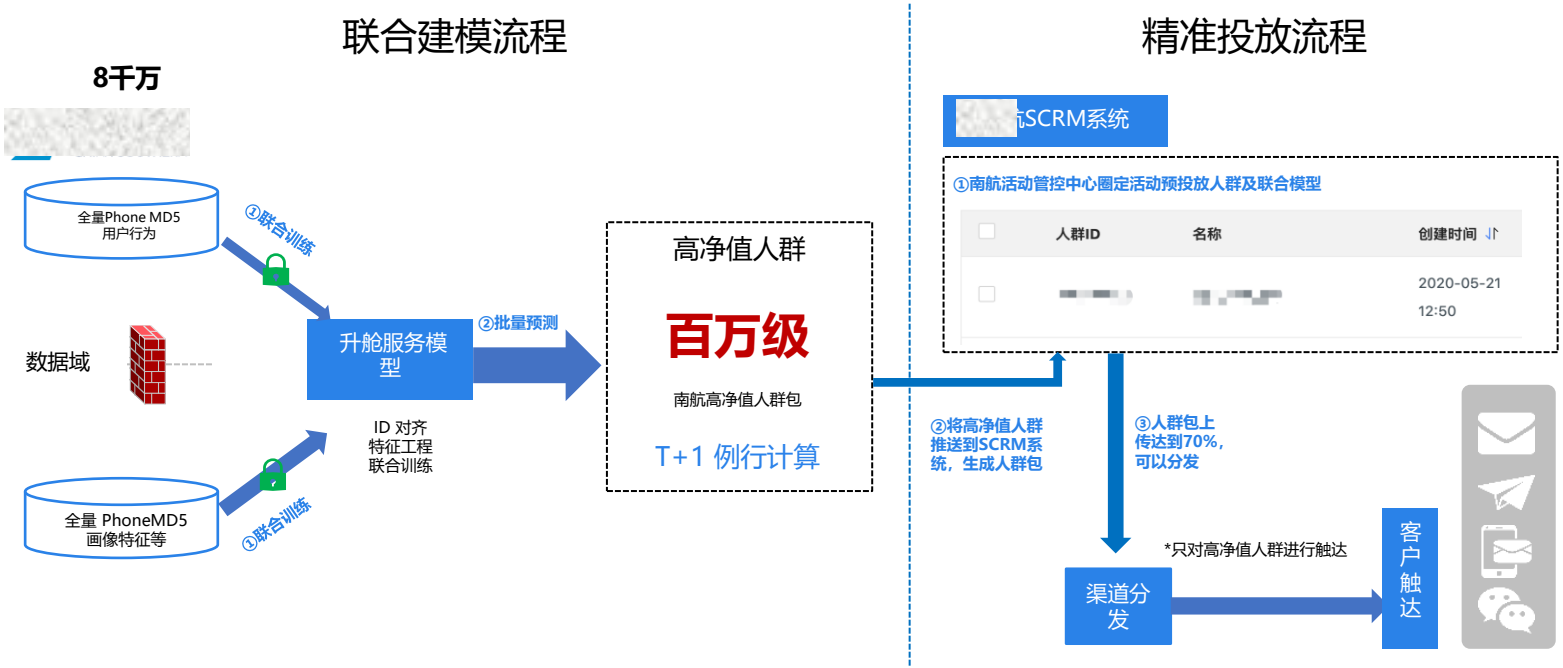
联邦学习和安全多方计算



优势

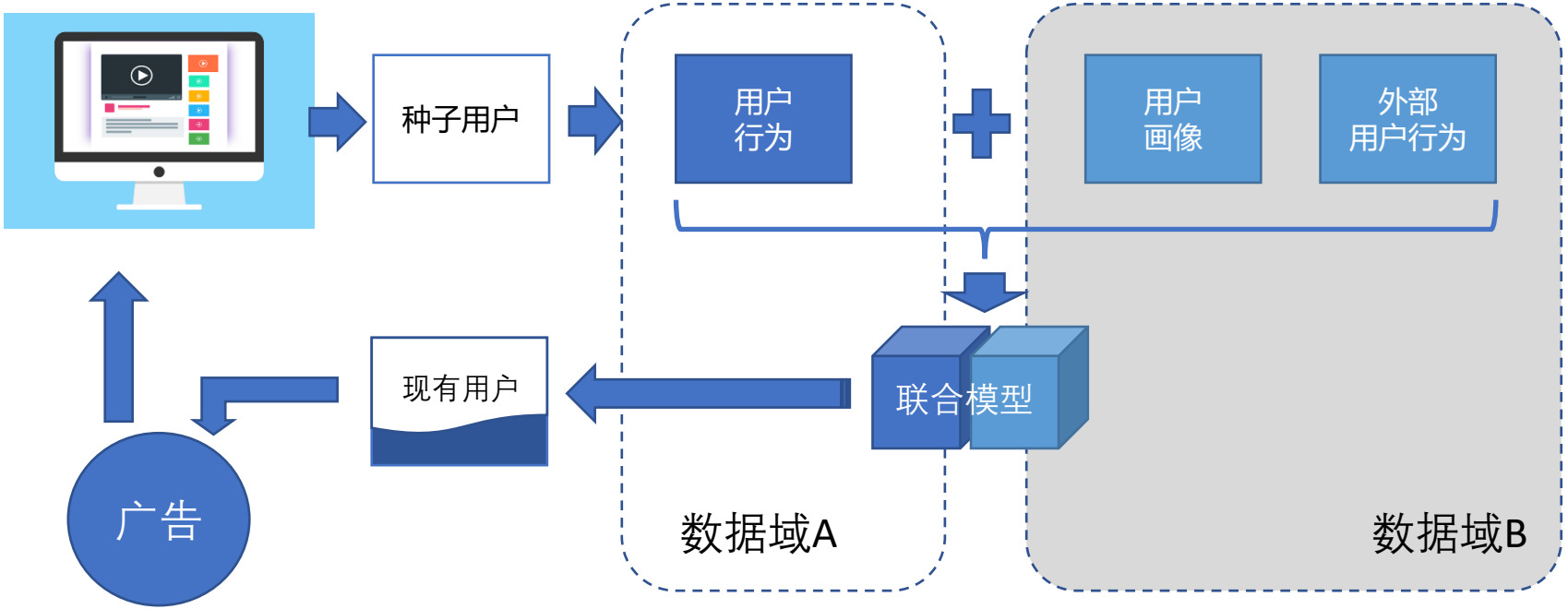
- 不依赖硬件
- 原始数据不出区域
- 点对点链接
- 知名度高

航空领域营销

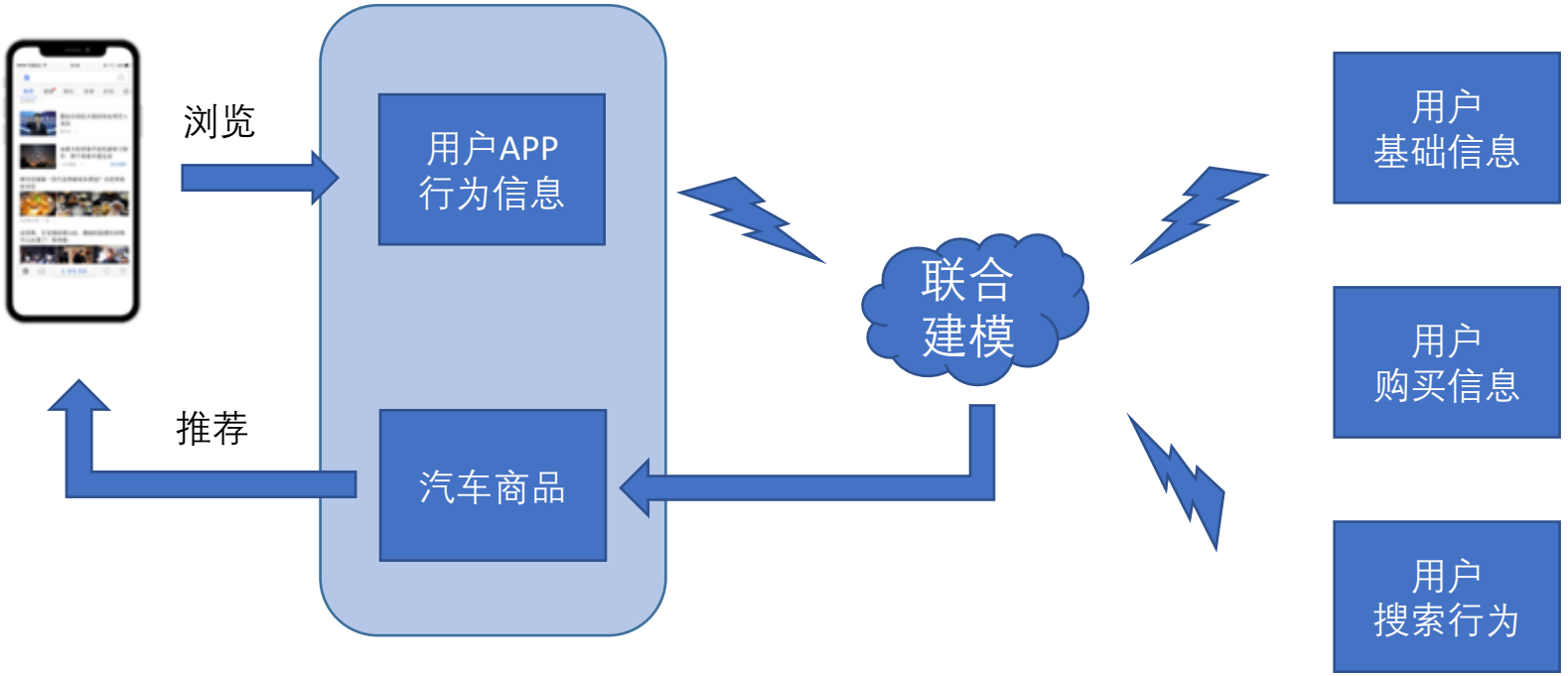


*针对高净值人群精准投放，提高了转化率，降低了成本，同时降低对低消费人群打扰，提升用户体验。

教育领域营销



汽车营销领域（推荐）



实现多样性

同态类型：
部分同态（Partially Homomorphic）
有点同态（Somewhat Homomorphic）
全同态（Fully Homomorphic）

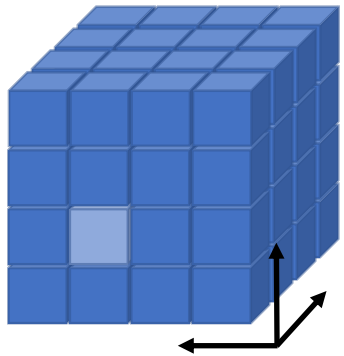
安全模型：
无攻击模型
半诚实模型（Semi-Honest Adversary ）
恶意模型模型（Malicious Adversary ）
隐蔽敌手模型（Covert Adversary）

调度方式：
算子层面：Operator Layer
算法层面：Algorithm Layer
组件层面： Component Layer
引擎层面：Engine Layer

计算平台:
Local
Docker/Kubernetes
Spark
MPI

通信方式：
Socket通信
RPC通信
MQ通信
P2P通信

存储方式:
File
DataFrame(vTable)
DataBase



劣势

- 速度慢 (计算复杂度，网络波动)
- 原理复杂，安全性难以度量(多样性)
- 可用算法有限

期待，有没有：

1. 速度快
2. 简单易懂
3. 有充足的算法?

是否可以通过“硬件”解决?

Baidu 百度 | DataFun.

03

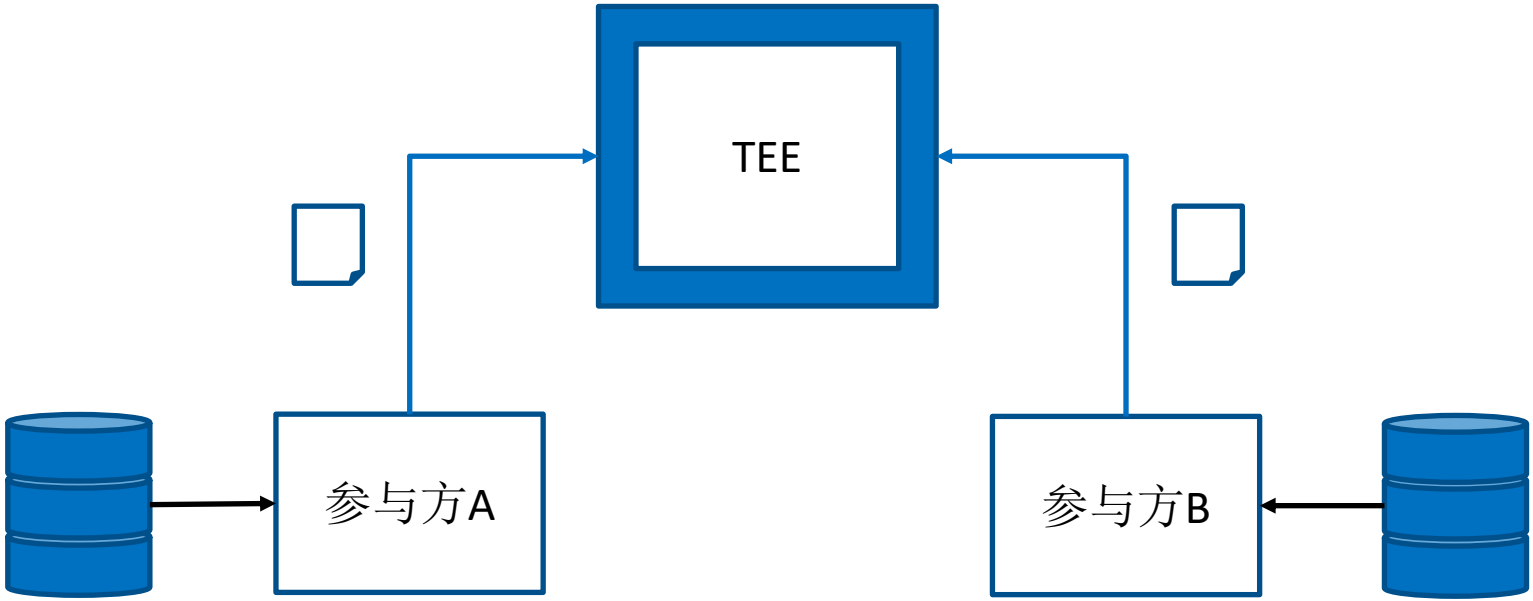
可信执行环境

替换文字内容，点击添加相关标题文字

优势

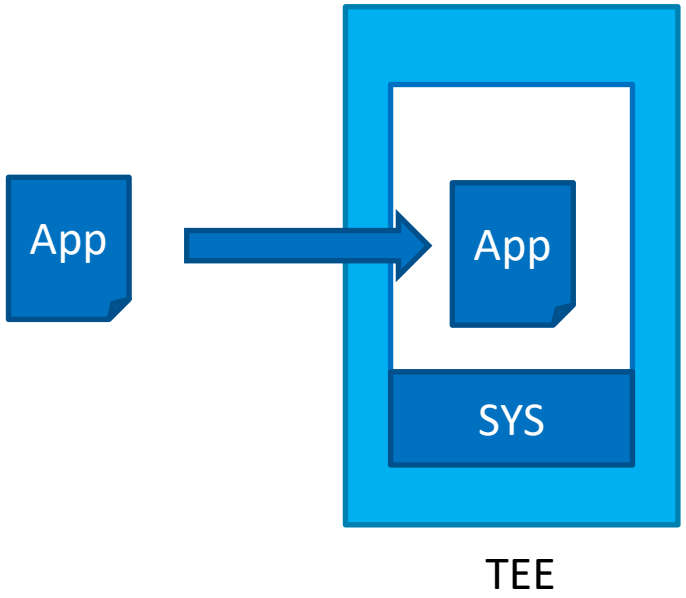
- 计算速度快：大数据，低延迟
- 执行逻辑较清晰，容易度量其安全
- 移植算法成本较低，可以用的算法很多

可信执行环境（TEE）

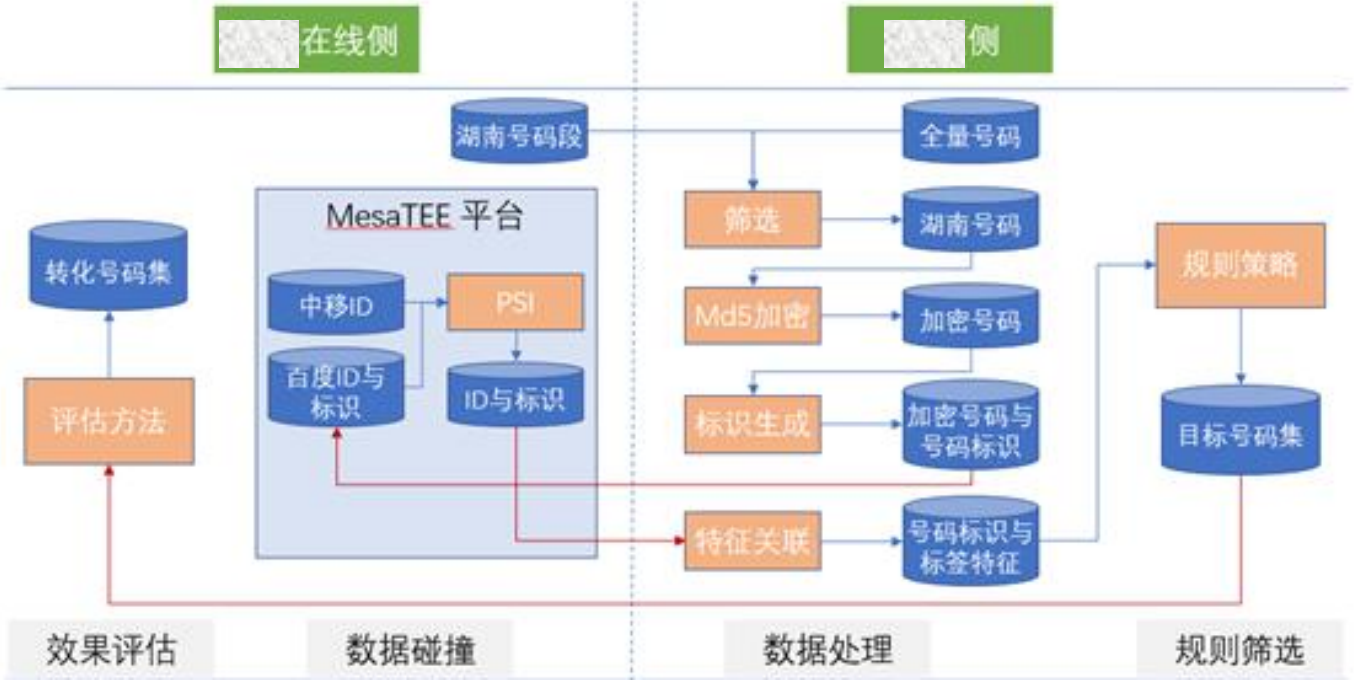


更加简单化的TEE

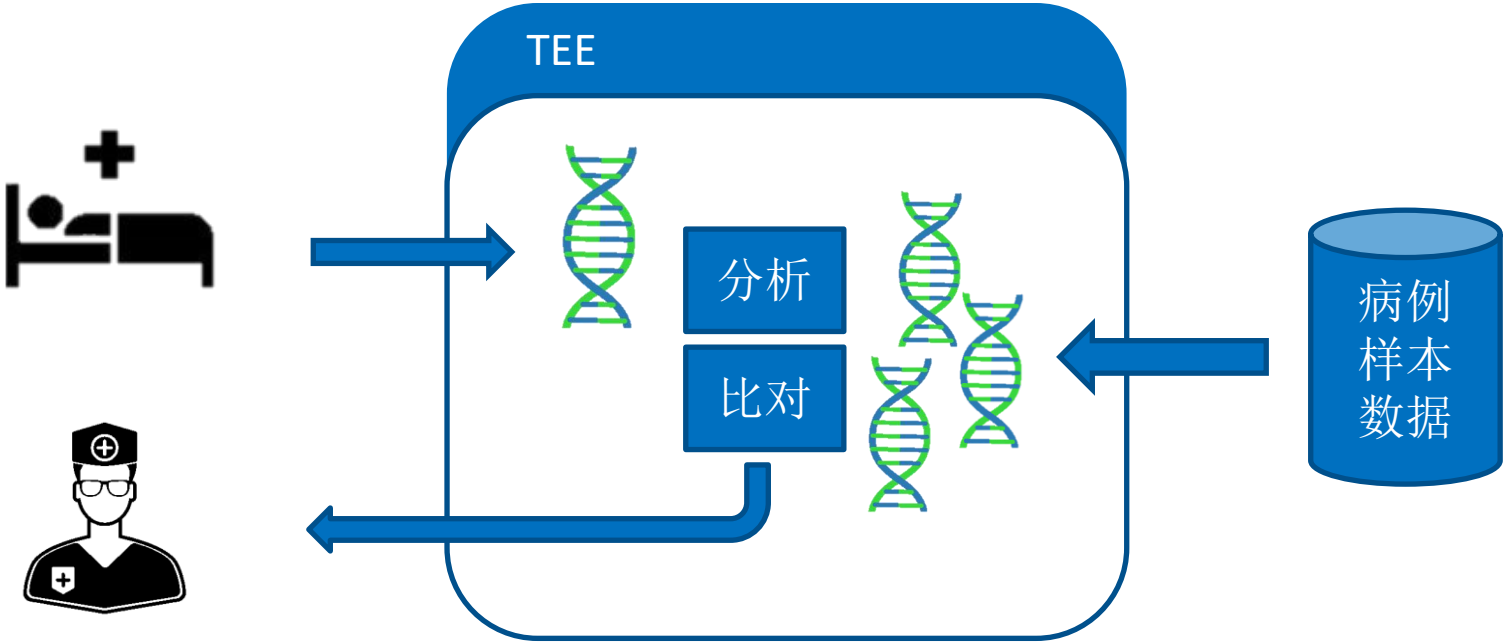
- 基于LibOS的可信执行环境
  - Occlum
  - Gramine(GrapheneSGX)
- 基于可信虚拟化技术
  - AMD: SEV,SEV-ES
  - INTEL: TDX
  - ARM: CCA



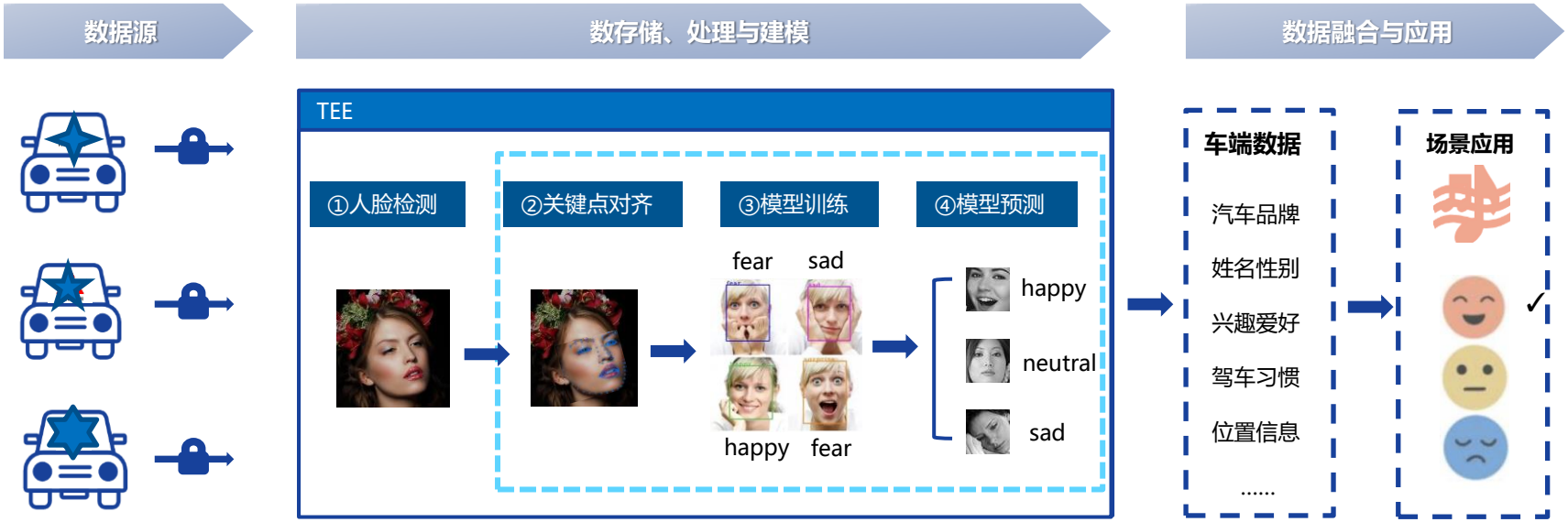
通信领域营销



生物基因领域



汽车音乐推荐



- 人脸检测：有效识别图片中的人脸，精确定位人脸位置，返回高精度人脸；
- 关键点对齐：对图片中的人脸进行关键点定位，并返回人脸关键点坐标位置，包括人脸轮廓、眼睛、眉毛、嘴唇以及鼻子轮廓等；
- 模型训练：通过读取训练集海量图片，进行情绪识别模型多轮迭代，输出模型参数；
- 模型预测：输入测试集人脸图片，调用情绪识别模型，输出情绪识别结果（happy/sad/neutral）
- 数据融合与应用：结合用户情绪识别结果与车端其他数据，可以用于车载音频切换，随着客户的情绪，切换相关主题音乐

劣势

- 数据需要加密后传到TEE
- 依赖硬件
  - INTEL：SGX1/2，TDX
  - AMD：SME，SEV，SEV-ES
  - ARM：TRUSTZONE，CCA
- 算法需要移植适配
- 需要权衡安全性和高可用：数据重放

期待，有没有：

1. 速度更快
2. 简单易懂
3. **所有算法和工具可用**
4. **不依赖硬件**

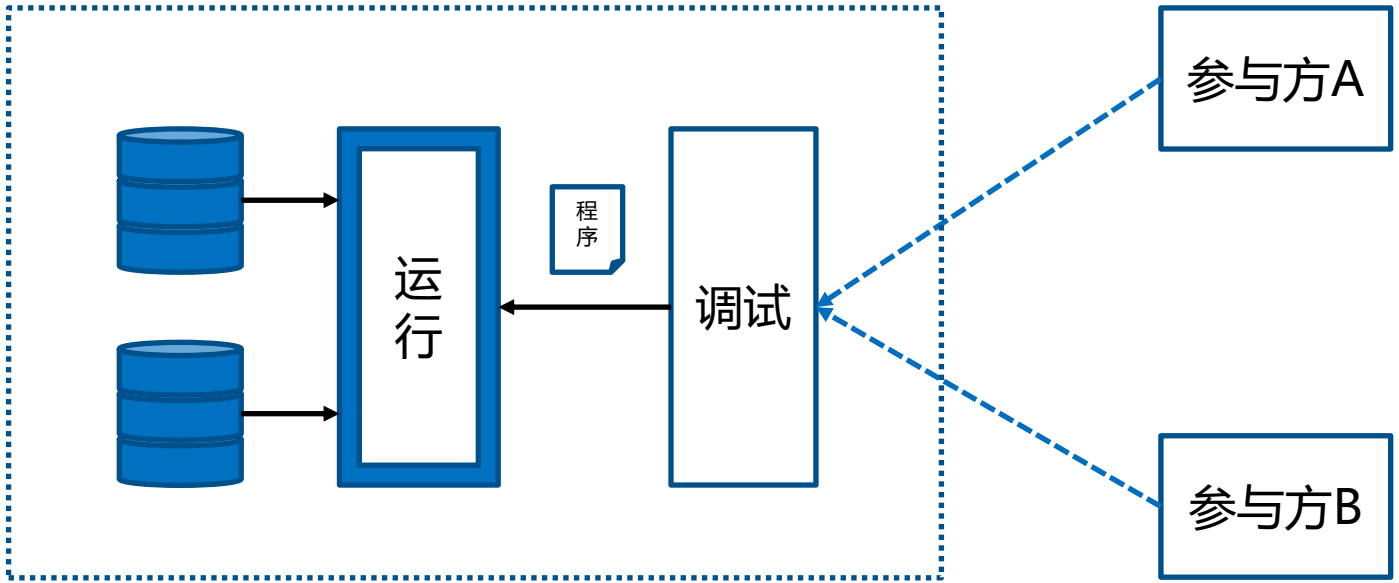
是否可以通过“隔离”解决？

04

安全数据沙箱

替换文字内容，点击添加相关标题文字

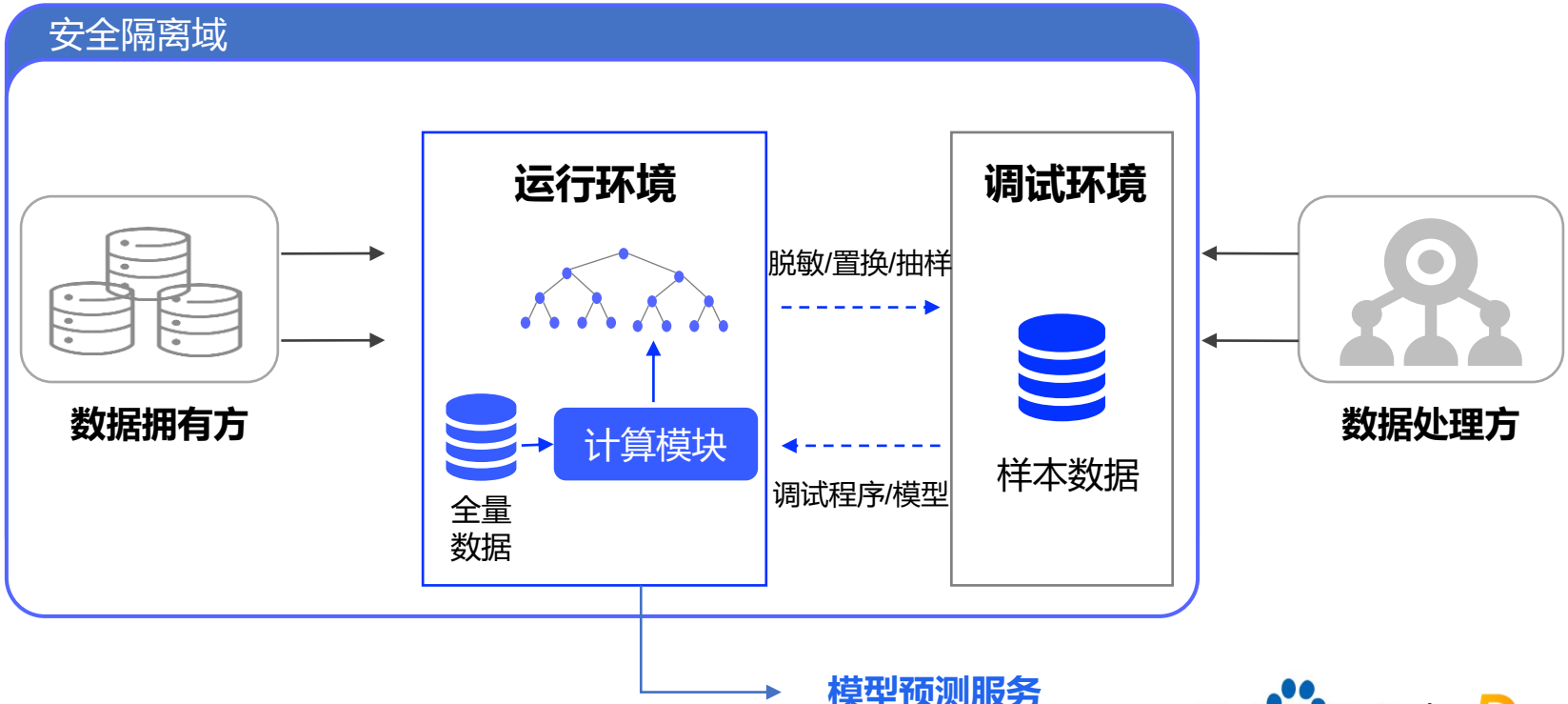
安全数据沙箱（SANDBOX）



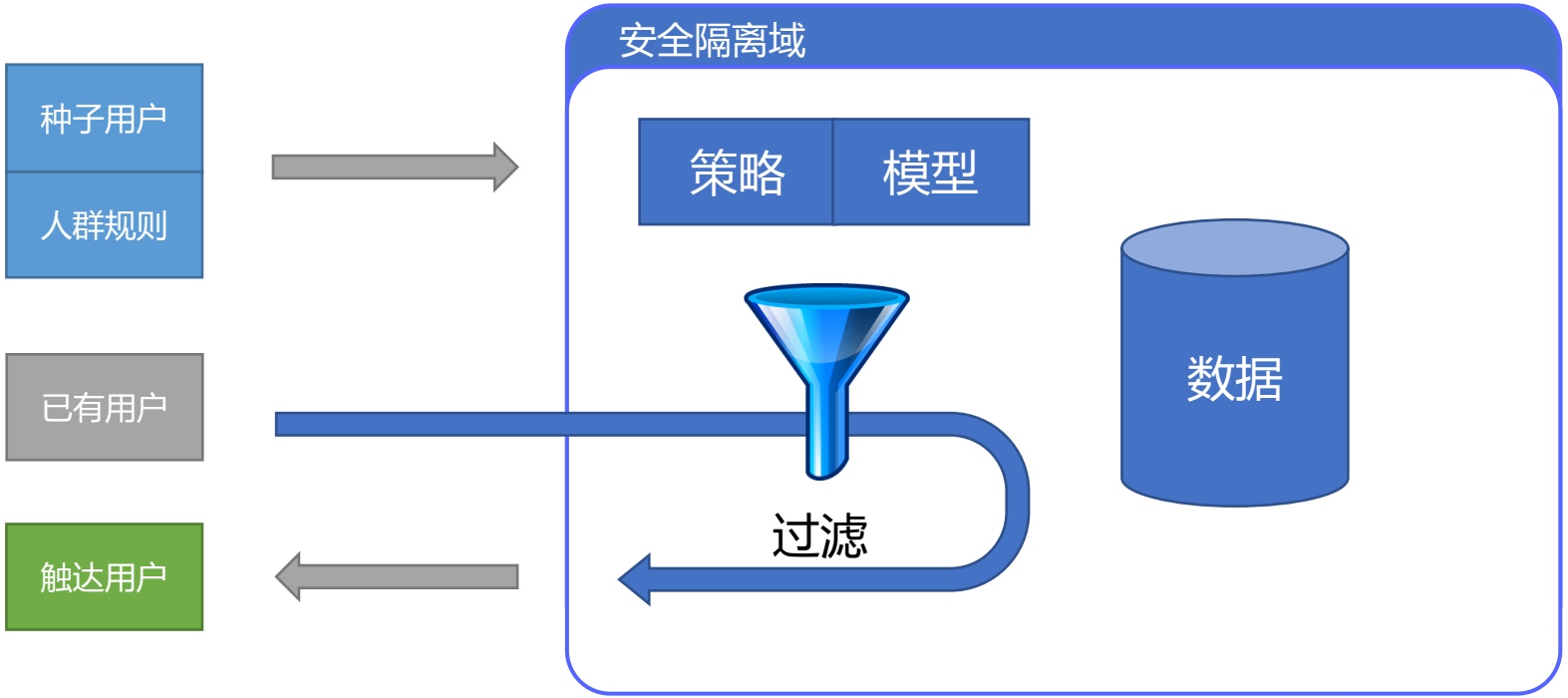
优势

- 简单，速度快，几乎无损耗
- 可大规模应用，适用特大的数据场景
- 不依赖物理硬件
- 所有算法都可以使用

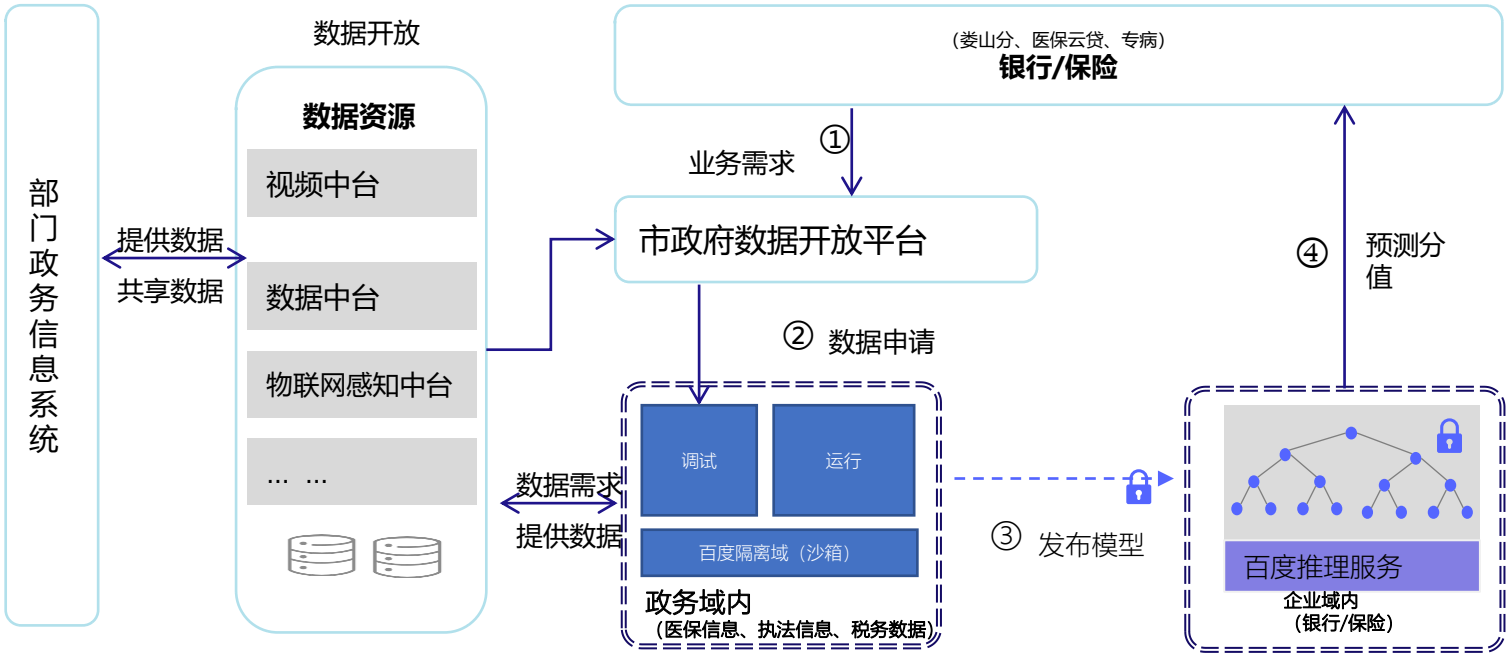
广告传媒领域



金融理财营销



政务数据在营销里的应用



劣势

- 仅保护平台方的数据安全

期待，有没有：

1. 不依赖硬件
2. 速度快
3. 简单易懂
4. 所有算法和工具可用
5. **两方的数据可进出**

是否有“全覆盖”的产品？

Baidu 百度 | DataFun.

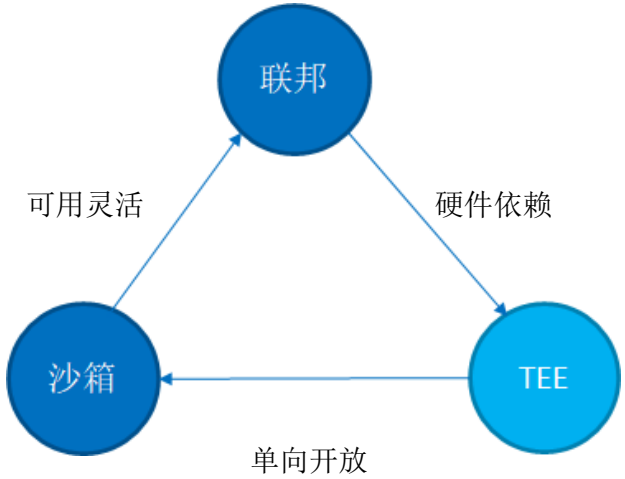
05

百度产品矩阵

替换文字内容，点击添加相关标题文字

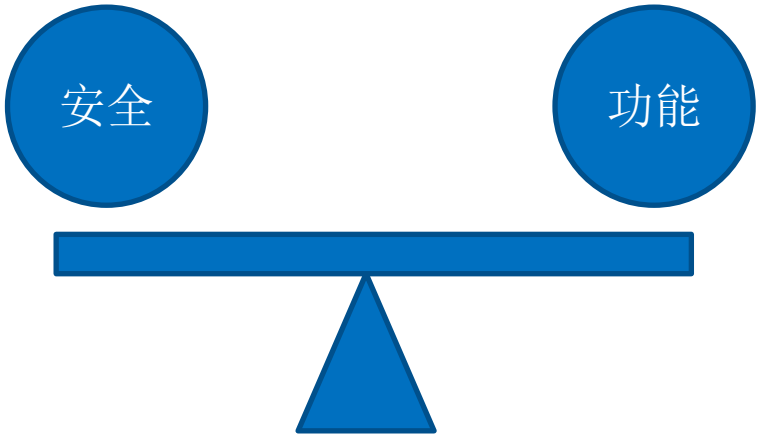
隐私计算中的舍得

- 联邦学习FL
  - 舍：计算效率，可用的算法
  - 得：无硬件要求，原始数据不出域
- 可信执行环境TEE
  - 舍：硬件的通用性，加密原始出域
  - 得：更快的计算效率，一定算法的可扩展
- 安全数据沙箱SBX
  - 舍：仅保护数据方的安全
  - 得：超大规模的数据计算，复用所有的算法和工具



恰当的应用隐私技术

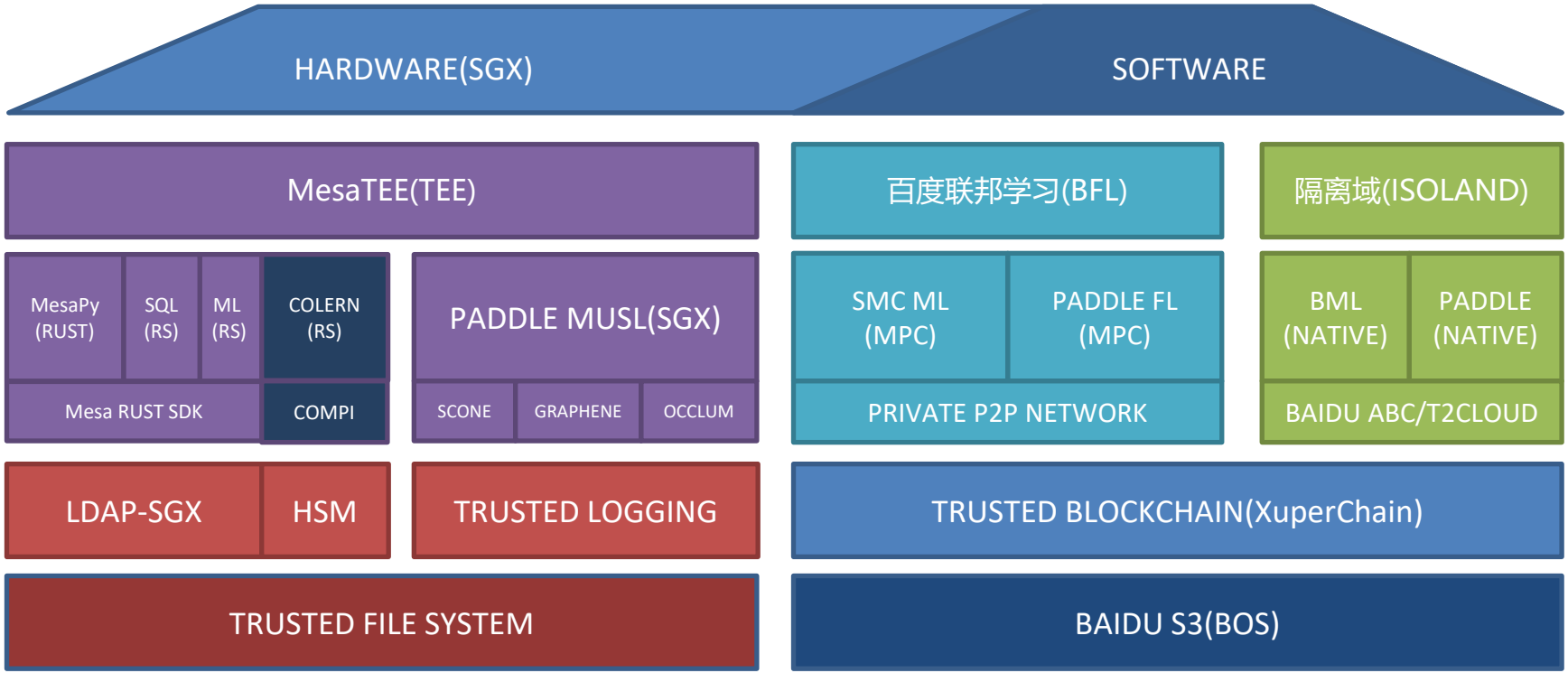
- 明确保护/防御对象
- 明确数据的规模
- 明确操作的范围
- 明确实施的运行环境



隐私计算一指禅

- 数据小，两方不出，常规算法：***联邦学习***
- 数据中，两方汇聚，专用算法：***可信执行环境***
- 数据大，一方不出，任意算法：***安全沙箱***

百度隐私计算：技术框架图



Baidu 百度 | DataFun.

06

未来趋势分析

替换文字内容，点击添加相关标题文字

趋势1：技术融合

- 联邦FL/MPC + TEE -> 降复杂，提效率
- SANDBOX + TEE -> 使用方数据安全问题
- SANDBOX + MPC -> 外部数据引入

趋势2：软硬结合

- FL/MPC + GPU/FPGA -> 深度学习提速

Paddle/PaddleFL, CryptGPU/CrypTen

MPC：CPU(200X) 降低到 GPU(35X)，提升10X以上

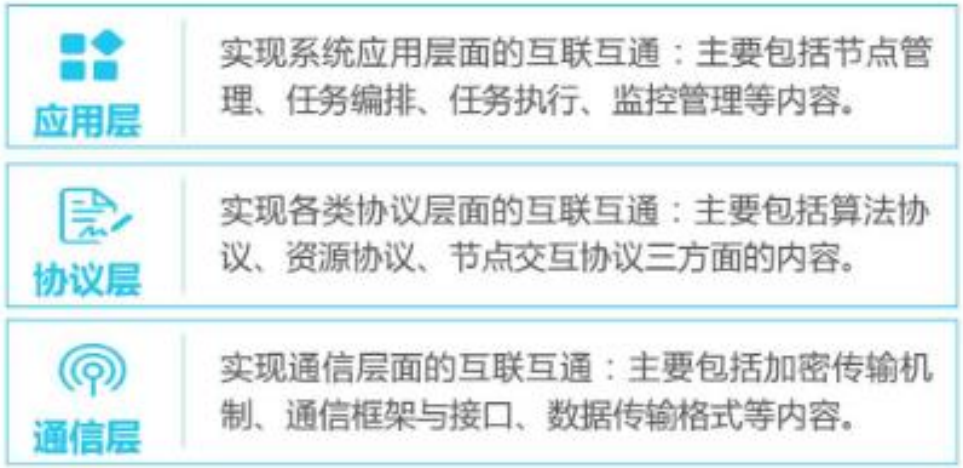
- SANDBOX + TrustedVM + Clear Container

启动加速，不同数据，不同等级

启动速度：100s 降低到 10s以内

趋势3：互联互通

- 隐私计算平台的互通
  - 中国信通院云大所《隐私计算 跨平台互联互通》系列标准
  - IEEE SA《P3117 - Standard for Interworking Framework for Privacy-Preserving Computation》



非常感谢您的观看

Baidu 百度 | DataFun.