星绽密态计算助力农业农村普惠金融

苏贤明

2024/10/22

CONTENT

目录

Part 1

农村普惠金融的痛点与挑战

农村普惠金融的痛点

贷款依赖
数据支撑

农户资产

生产经营情况

抵质押物少

无信用记录

数字化程度低

- 土地承包关系
- 农资/农机推导
- ……

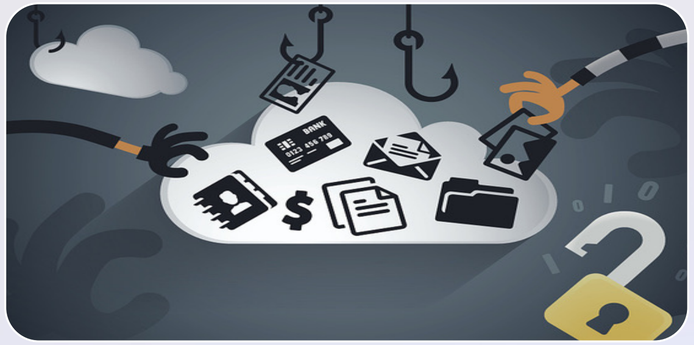
有多少地

种什么东西

- 卫星遥感识别
- 农资/农机推导
- ……

多源数据融合建模

多源数据融合建模的挑战



数据共享存在风险

- 数据孤岛问题突出，数据共享日益重要，但存在买卖、泄露和滥用等问题
- 买卖用户数据等

公众和政府日益重视隐私保护

- 欧盟GDPR法律正式实施，多国在效仿
- 我国的《数据安全法》、《个人信息保护法》等

金融科技行业新的难题

- 在满足安全、隐私和监管等要求下，如何设计相应框架，实现数据的多方协同和授权共享，得到更准确高效的模型和决策，进一步释放数据价值

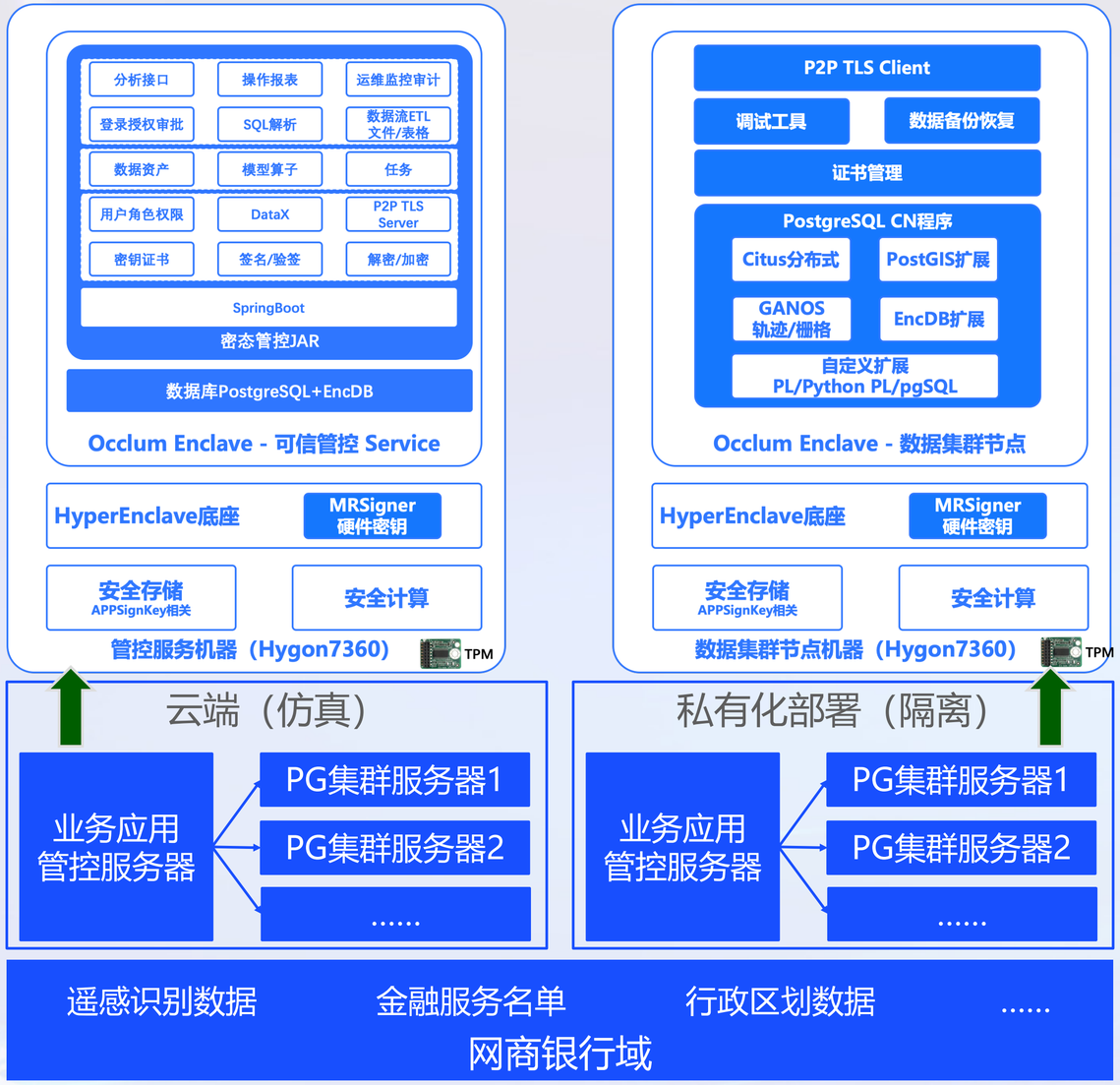
Part 2

隐私融合计算方案的选择

数据要素流转与融合计算方案选型

方案	基本原理	适用场景
多方安全计算MPC	密码学协议：保证每个参与方的数据对其他参与方保密，计算过程保持加密状态	适用于不能直接共享原始数据的场景
联邦学习	分布式机器学习技术：允许多个设备或机构在不交换本地数据的情况下训练模型，即局部模型→全局模型	移动设备的个性化推荐、智能助手训练、跨机构的数据合作等
密态计算TEE	安全区域：通过硬件手段创建一个与主操作系统隔离的安全区域，区域内的代码和数据受到保护	高性能数据处理、数据隔离等场景
差分隐私	一种数学框架：通过添加噪声到查询结果来保护个人记录	需要发布统计数据或者分析结果的场景
同态加密	一种加密技术：允许在不解密数据的情况下直接对密文进行计算	云端计算、外包计算
私有集合求交PSI	密码学协议：允许多个参与方计算各自持有集合的交集而不泄露交集以外的任何信息	撞库

基于星绽的密态时空计算方案

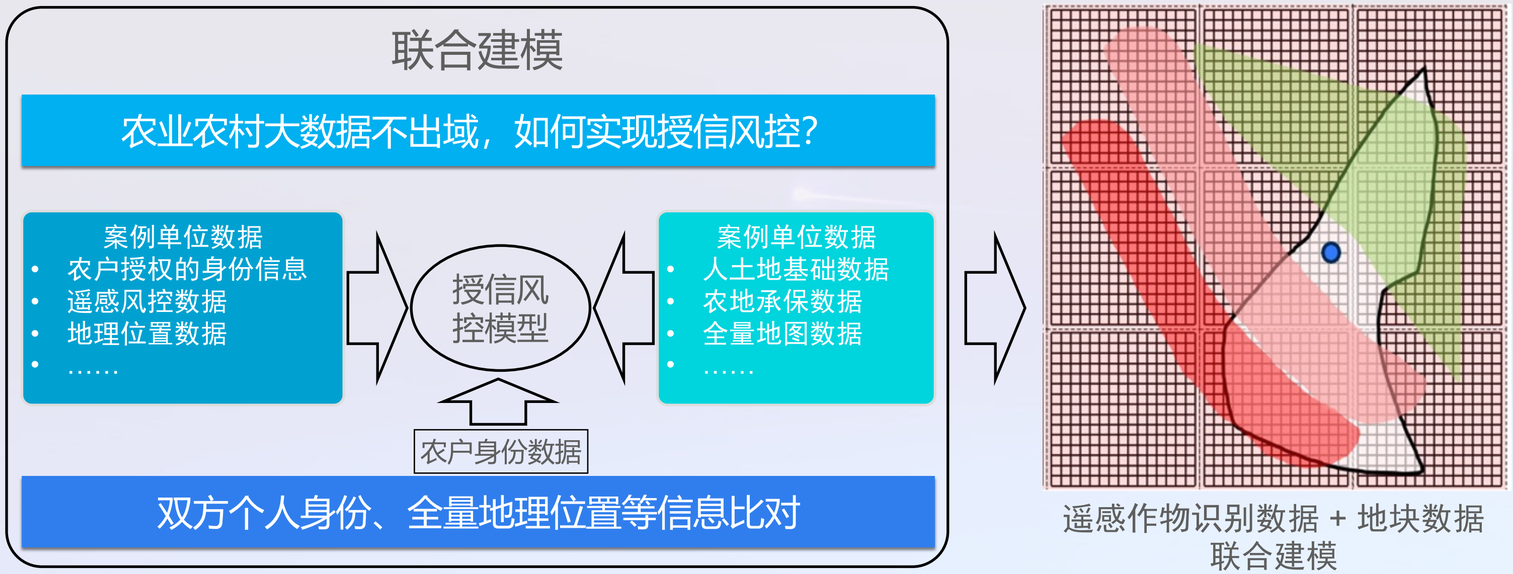


- 自主可控
  - 默认支持海光国产CPU等信创硬件平台
  - 信任根筑基于国家金融信息安全基础设施
- 安全可证
  - 代码经过权威机构审查认证
  - 具备金融科技产品认证
  - 安全性经过形式化证明
- TEE能力完整实现
  - 隔离执行、远程证明、内存加密、数据封印
- 软件生态完备
  - 主流数据库，大数据框架开箱即用，兼容SGX SDK，Rust SGX SDK等已有TEE 生态。
- 容器化设计理念
  - Enclave-as-a-Container简化应用接入成本， 提供new、build、run、stop、kill等命令

Part 3

网商银行星绽密态计算联合建模实践

网商银行密态时空联合建模方案

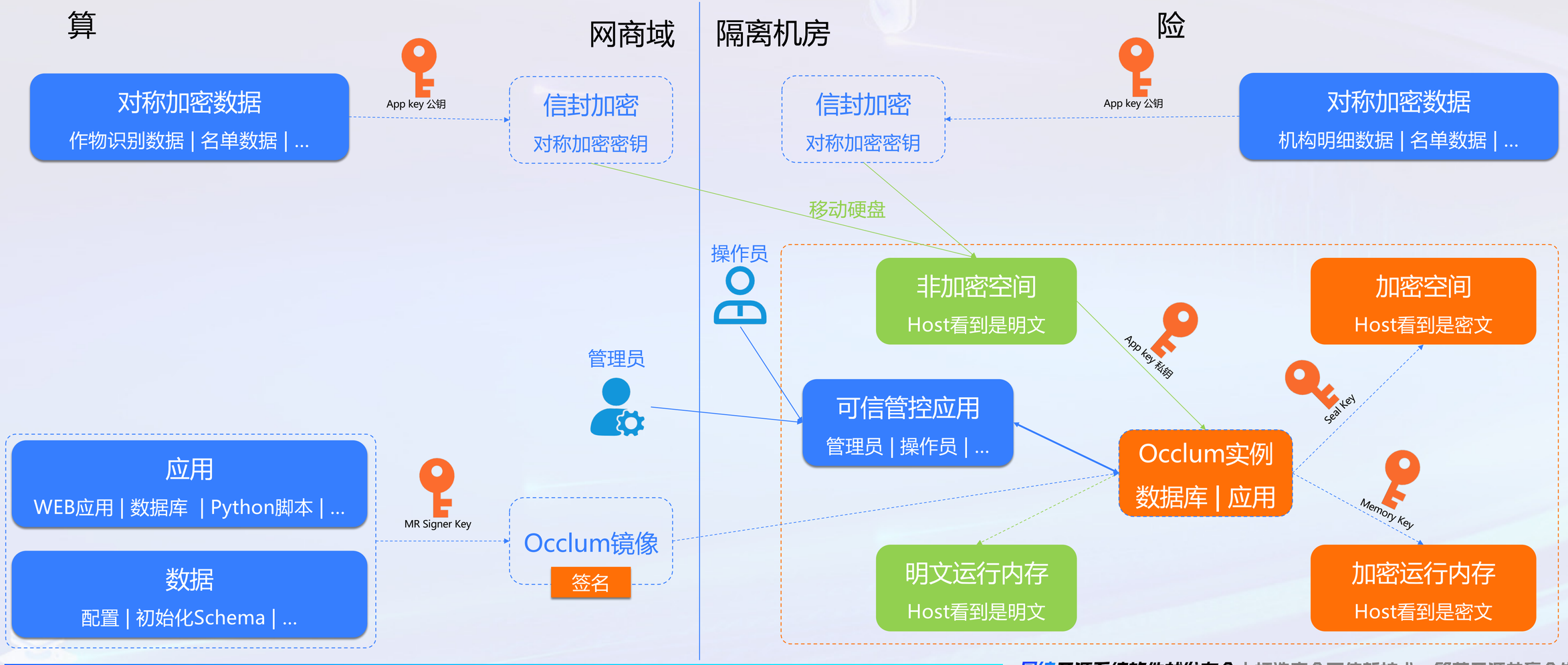


遥感作物识别数据 + 地块数据联合建模

- 国家数据局“数据要素X”唯一一个金融领域的全国典型案例
- 首个国家部委级TEE私有化部署的创新应用

星绽私有化部署端到端安全保障方案

- 数据全链路加密存储，内存机密计算
- 星绽4级密钥保障数据可信管控流通
- 应用用户权限管控保障操作风险



Thanks