蚂蚁集团 ANT GROUP | DataFun.

隐私计算在医疗行业的方案与实践

曹剑　　智能平台产品总监

目录

- 隐私计算认知
- 隐私计算产品
- 医疗行业实践

隐私计算的定义

问题

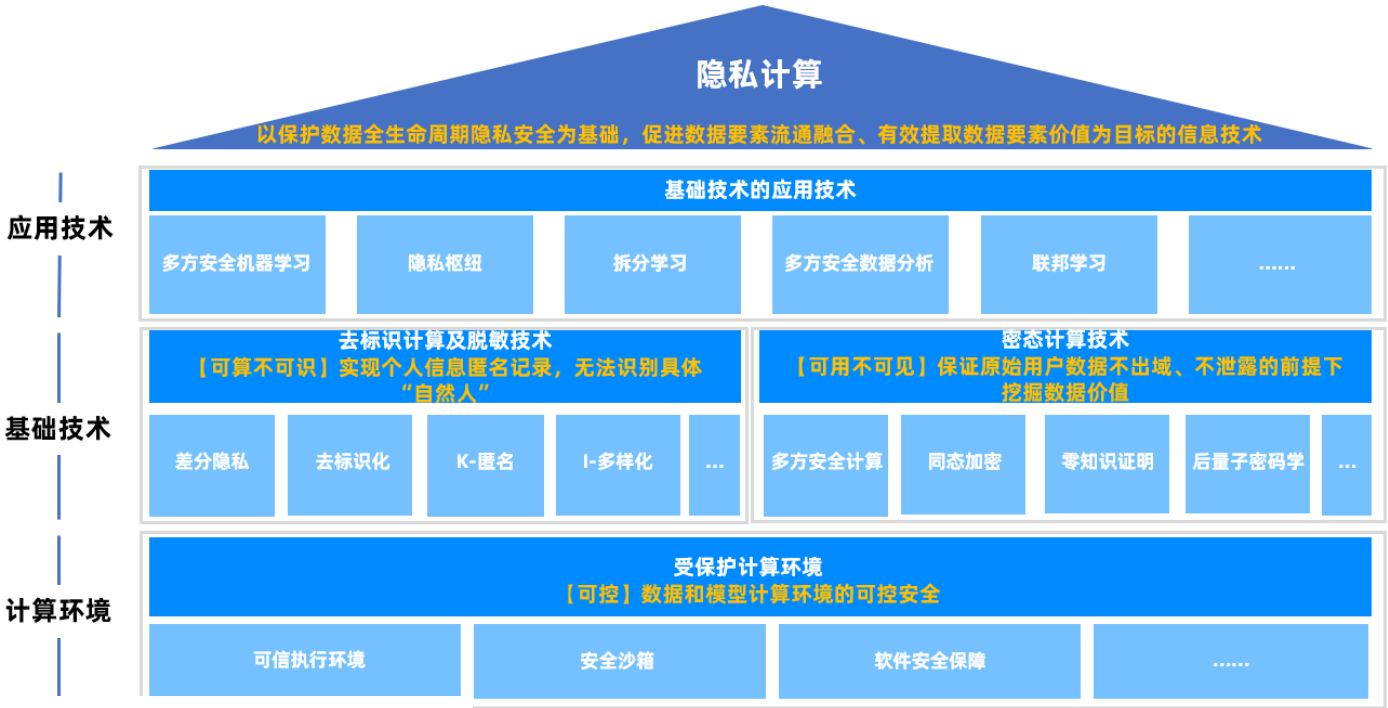
有多方参与
且各方互不信任的场景下，
能够聚合多方信息
并保护数据隐私的智能计算范式

目标

Privacy-Preserving Computation

An intelligent computing paradigm that can aggregate information from multiple parties and protect data privacy in scenarios where multiple parties are involved and the parties do not trust each other.

隐私计算的组成



密态计算技术可保证原始数据不出域情况下即可实现数据价值共享

通过多方安全计算，同态加密等技术，用户的原始数据可以在不出域、不泄漏的前提下共享提取数据价值，实现信息的“可用不可见”

去标识化技术可确保数据共享过程中不会向第三方泄露消费者身份

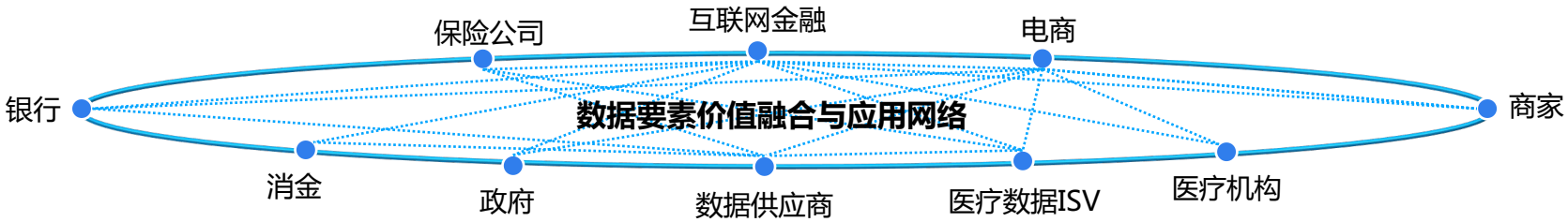
通过使用可信去标识化和可证无身份关联技术，可确保合作第三方不能通过数据反向逆推出数据主体，做到共享信息的“可算不可识”

可信执行环境等技术可有效增强数据计算环境安全性

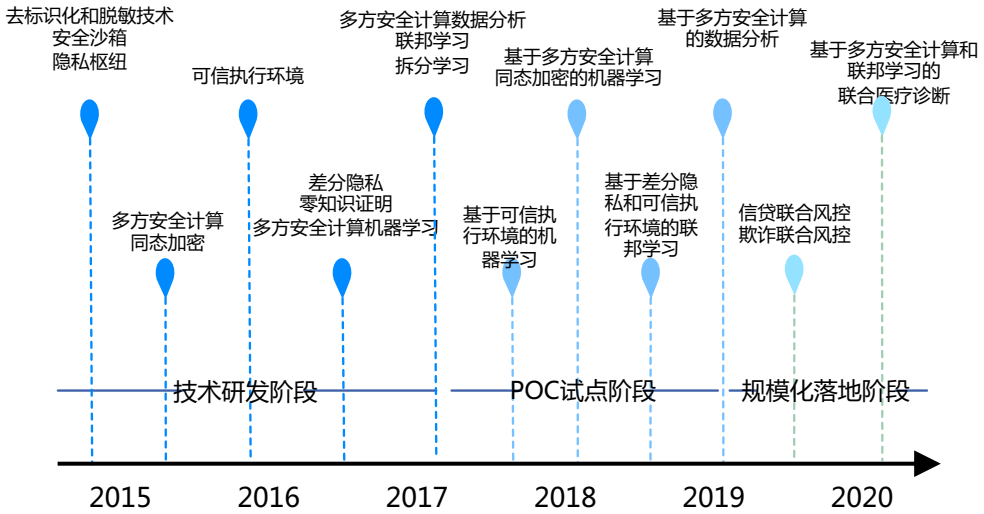
在隐私计算的过程中，通过安全沙箱、可信执行环境等受保护计算环境技术，可以提升数据和模型计算环境的安全性，确保全程安全可控

隐私计算的网络效应

从社会角度，隐私计算可链接数据孤岛、打破数据垄断、填补信任鸿沟



蚂蚁隐私计算领域专利与实践



排名	企业简称	国家/组织/地区	全球隐私计算技术发明专利申请数量/件（截至2022年3月8日）
1	蚂蚁集团	中国	1152
2	中国平安	中国	423
3	Microsoft	美国	374
4	阿里巴巴	中国	313
5	IBM	美国	252
6	华为	中国	206
7	国家电网	中国	206
8	微众银行	中国	204
9	Intel	美国	180
10	Samsung	韩国	154

第三方权威机构IPRdaily与incoPat创新指数研究中心联合发布了《2022年全球隐私计算技术发明专利排行榜》。榜单显示，截至2022年3月8日蚂蚁集团以1152件专利数排名第一，这也是蚂蚁集团连续两年位列排行榜第一。

蚂蚁隐私计算牵头标准制定

牵头和参与多项标准制定

金标委行业标准：

- 参与制定金标委已发布标准《多方安全计算技术金融应用规范》
- 与工行等联合牵头《联邦学习技术金融应用规范》的行标立项申报

国家标准：

- 牵头信安标委国家标准《隐私计算技术应用指南》，立项流程中

国际标准：

- 牵头IEEE P2830《基于可信执行环境的共享学习技术框架和要求标准》，已发布
- 牵头IEEE P2952《基于可信执行环境的安全计算标准》，征求意见稿
- 牵头ITU-T 《隐私保护机器学习技术框架》，已发布，ITU首部隐私计算标准

团体标准：

- 牵头浙江省互金协会、 AIIA联盟等《共享学习系统技术要求》，已发布
- 牵头互联网广告协会《互联网广告隐私保护计算平台技术规范》，已立项
- 深度参与信通院十余项团标的制定……

地方标准：

- 参与上海地标《金融场景下的隐私计算通用框架》《跨平台互联互通》，立项中

蚂蚁整体牵头十余项，参与数十项隐私计算的国际/国家/行业/团体标准

通过多项标准测评

已测评通过：

- 国家金融科技检测中心（BCTC）基于人行《安全多方计算技术金融应用规范》测评
- 中国金融认证中心（CFCA）的代码安全审查
- 中国人工智能学会组织的科技成果鉴定
- 国家信息技术安全研究中心组织的信息安全技术检测
- 信通院《多方安全计算安全专项》测评
- 信通院《联邦学习安全专项》测评
- 信通院团体标准《基于TEE的数据流通产品》
- 信通院团体标准《基于MPC的数据流通产品》
- 信通院《数据安全治理能力评估》

蚂蚁隐私计算智能服务平台产品结构

隐私计算智能服务平台是以联邦学习FL、安全多方计算MPC、可信硬件执行环境TEE等隐私数据保护技术工具为基础服务的平台。

核心价值：保证原始数据不出本地即可完成多方数据联合建模和联合计算能力，同时支持安全隐私保护集合求交、安全隐私查询、安全统计分析。实现各合作机构数据在流通、计算过程中，端到端的安全保护和可审计， 推动跨行业的可信数据价值的融合和协同，很好地解决了业界数据孤岛的难题。

产品能力大图

行业应用解决方案

保险应用	信用风控应用	安全风控应用	营销应用	医疗应用	政务
核保 核赔	授信 提额	反欺诈 反洗钱	圈人 画像	诊断分类 诊断分析	信用 风控
联合风控	联合风控	联合风控	联合营销	联合诊断	一网通办

中心平台

隐私计算服务平台

模型服务、分析服务、规则服务、隐私求交（撞库）服务

工作台（联合项目）

多方安全计算（MPC） | 联邦学习（FL） | 多方安全统计分析（SCQL） | 多方安全规则 | 隐私求交

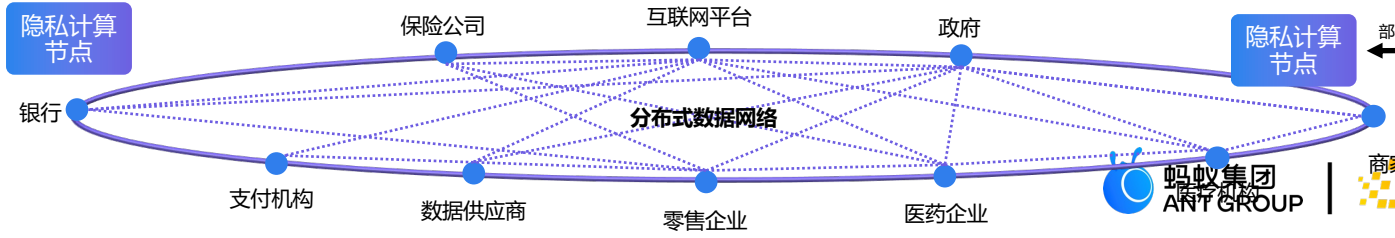
管理台---机构（分租户）管理台
（管理节点、节点网络授权、数据注册/授权，联合项目）

隐私计算服务---中心节点/安全计算节点（异构分布式系统）

进入联合项目操作 → 算法或数据开发者（面向服务开发者）

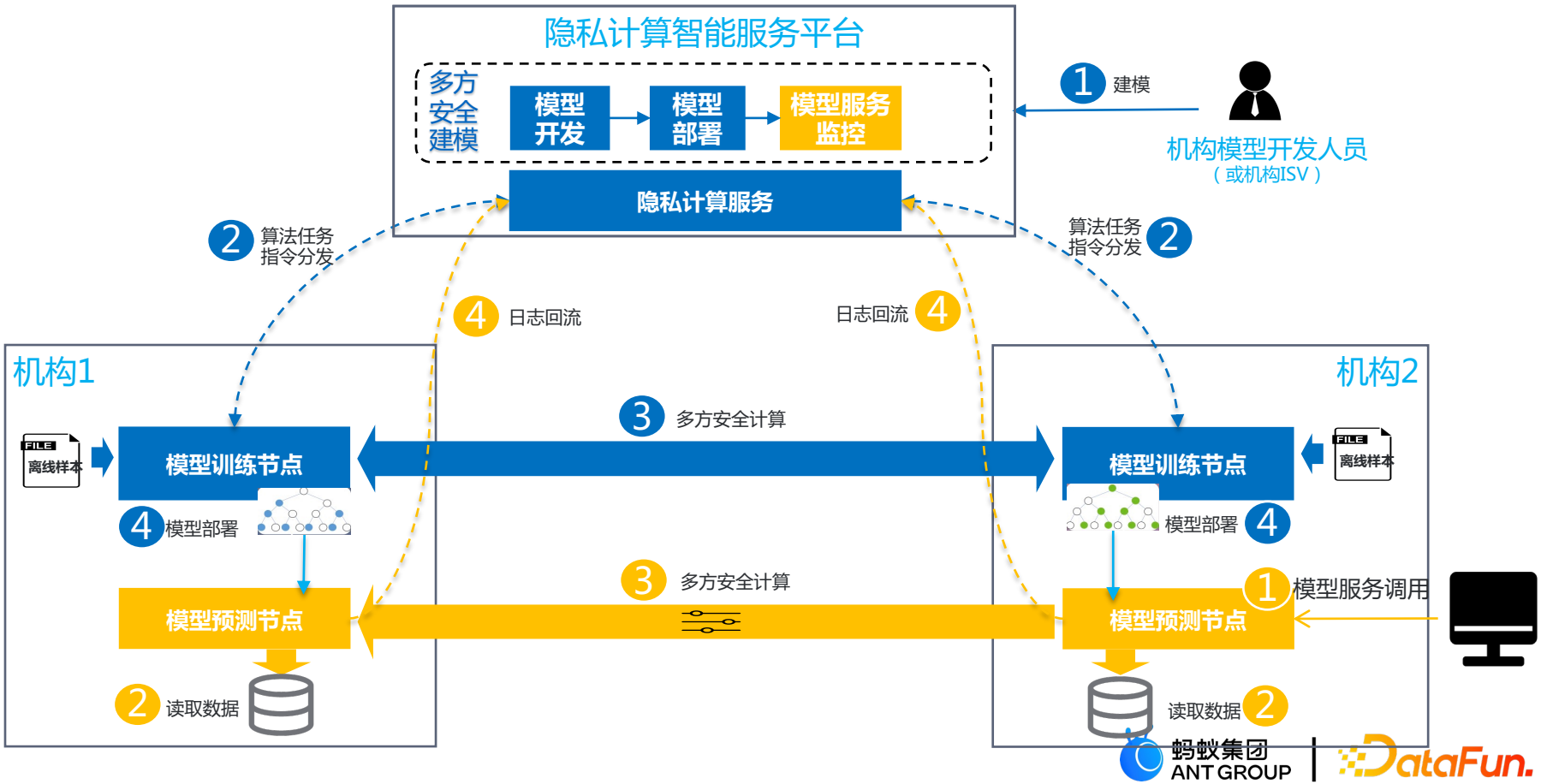
管理本机构资源 → 数据提供方管理员（面向数据资源管理方）

安全计算节点（数据不出域）



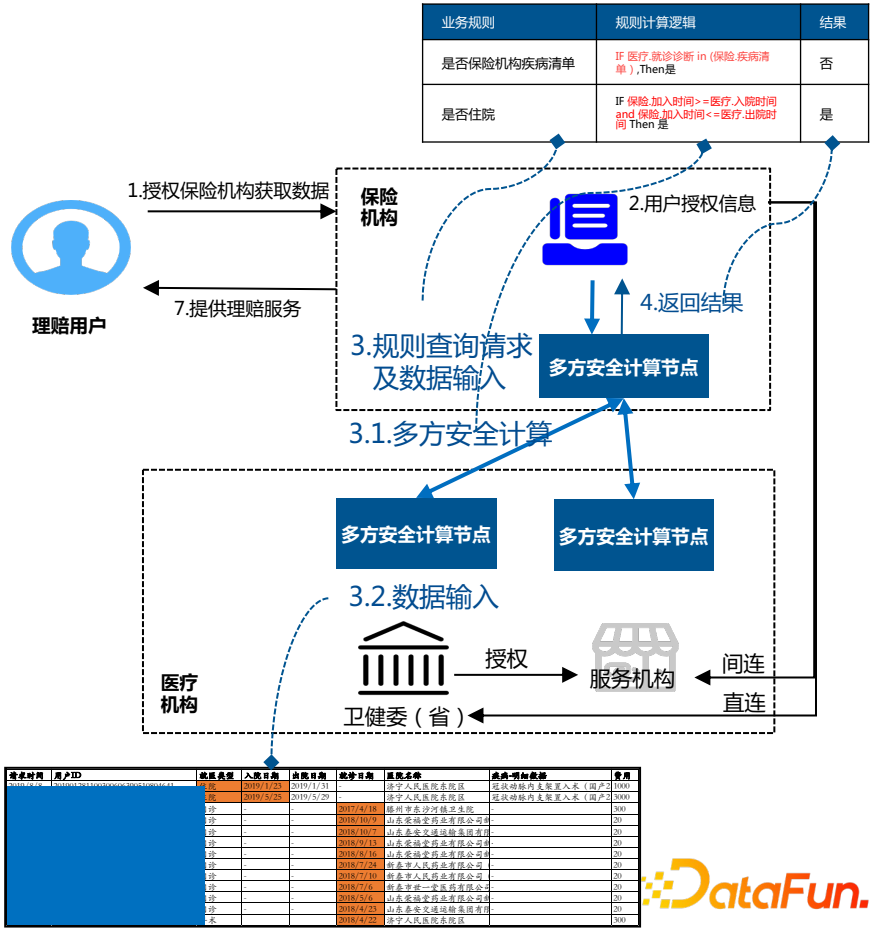
蚂蚁集团 ANT GROUP | DataFun.

蚂蚁隐私计算智能服务平台产品部署架构



隐私计算服务医保理赔

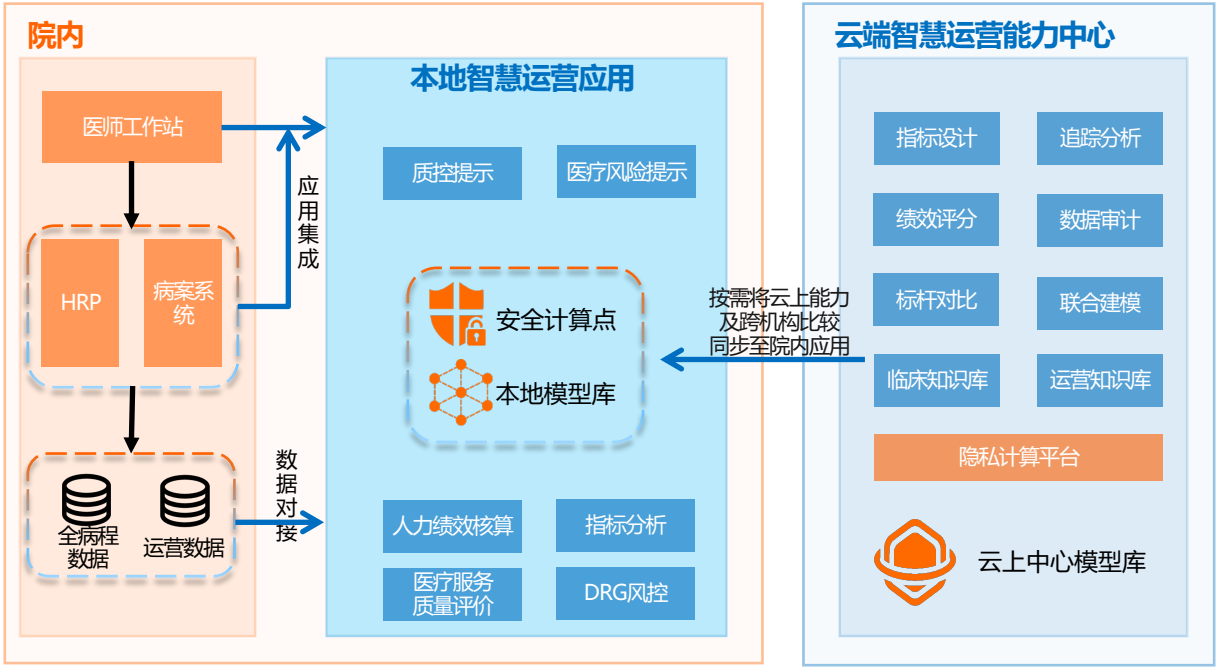
行业-场景	保险-医疗保险理赔
问题	保护用户隐私，数据可用不可见（不出域）实现数据价值赋能　　供方-医疗机构 安全合规的连接医疗诊断数据实现智能理赔，降低核赔成本且提升效率需方　　需方-保险机构
解决方案	多方安全联合规则
解决方案	1. 保护用户隐私　没有明细信息暴露风险 2. 计算过程/结果安全　密态计算保护计算过程可证安全，计算结果无法反推原始数据 3. 按需获取结果　满足合规数据最小可用输出原则 4. 保护需方业务策略　例如保险机构风控策略不泄漏



DataFun.

隐私计算服务医院数字化运营

在医保支付改革的背景下，用智能化工具减少医院经济风险和临床风险。通过为医院搭建面向医院运营管理的数据融合平台，利用智能算法（知识图谱、文本挖掘、DRG分组等），动态规范医护临床行为，为管理者提供数字化绩效管理分析，帮助医院建立精细化运营管理体系，并和部分科室KOL联合，进行科学实验室的合作。



Successful cases

- **病理质控**

甲级病案例由80%提升到97%，上线初期日均检验病历问题300+，高危病历20+；

- **DRG管理**

2021.1-3，浙江某三级医院累计减少40.7w结算损失；编码入组，医保反馈分析工作量降低72%

◆ DRG/DIP入组准确率高达97.%

◆ 人机协同，优化修正

◆ 接入隐私计算，数据安全可控，可用不可见

隐私计算服务卫建临床辅助决策

某卫健为了赋能三四级地市以及社区医院、乡镇卫生院的临床诊断能力，尤其是提升针对某些疑难重病的初筛排查能力，构建了基于隐私计算平台的临床辅助决策系统，通过主要三甲医院相关科室的大量病案数据在原始数据不出域的情况下，通过数据训练有效提升决策系统的准确率。

如果想要了解更多，可以关注微信公众号“隐语的小剧场”与我们联系。

非常感谢您的观看

蚂蚁集团 ANT GROUP | DataFun.