中国计算机科学评论
Chinese Computer Sciences Review
2023 年第 01 卷第 01 期
Vol. 01, No. 01, 2023

隐私计算:技术方法和行业应用的综述

王　伟[1]，邵　瑜[1]，段　佳[2,*]，张泽华[2]

（1. 北京理工大学医学技术学院，北京 102676；2. 京东零售平台运营与营销中心，北京 102676）

摘要：人工智能与大数据的迅猛发展，使得数据成为了重要的生产资料和流通要素。如何能在安全合规，确保数据隐私安全的前提下，充分发挥数据价值，成为了公众关心的热点问题。隐私计算，作为新兴的技术体系，它可以通过密码学、可信硬件、多方安全计算、差分隐私等交叉融合技术，实现数据的可用不可见，达到数据安全流通，发挥数据价值的目的。随着学术界以及工业领域的日益关注，隐私计算已成为新的技术热点，也成为商业和资本竞争的热门赛道。文章综述了隐私计算的技术原理，对隐私计算中的关键技术进行了分类详述，包括可信计算、多方安全计算、联邦学习、差分隐私、匿踪查询等。同时，文章也从安全性，技术优势，存在的风险点等多维度，对隐私计算技术进行了对比分析。另外，文章也总结分析了隐私计算在国内各个行业的发展和应用，侧面验证了隐私计算在数据流通和数据价值实现等方面的显著贡献。最后，文章对隐私计算的发展现状和面临挑战进行了总结，并展望了隐私计算未来的发展趋势。

关键词：隐私计算；数据安全；联邦学习；差分隐私；多方安全计算

DOI：10.48014/ccsr.20230517001

引用格式：王伟，邵瑜，段佳，等. 隐私计算：技术方法和行业应用的综述[J]. 中国计算机科学评论，2023，1(1)：1-12.

0　引言

人工智能与大数据的迅猛发展，使得数据成为了重要的生产资料和流通要素。企业机构也迫切需要数据的流通来打破数据孤岛，实现数据的价值。但是，“复制”数据的流通方式并不能保障数据的安全性，并且无序的数据收集和没有约束的数据交易也扰乱了数据要素的正常流通。尤其近两年频发的隐私安全泄露事件，也让公众对数据安全和隐私保护的问题产生了担忧。如何能在安全合规，确保数据隐私安全的前提下，充分发挥数据价值，成为了公众关心的热点问题。

隐私保护计算（Privacy-Preserving Computation），又称“隐私计算”，是指运用密码学、可信硬件、多方安全计算、差分隐私等交叉融合技术，在确保数据隐私安全的前提下，对数据进行分析计算。隐私计算技术不指代某一项技术，而是泛指一个技术体系。通过利用众多交叉融合的技术，隐私计算可以实现数据的可用不可见，达到数据安全流通，实现数据价值的目的。

随着学术界以及工业领域的日益关注，隐私计算已成为新的技术热点，也成为商业和资本竞争的热门赛道。不同于之前的隐私计算综述文章[1,2]，本文将从技术原理以及分类、行业典型应用、产业发展现状、挑战以及未来发展趋势等方面对隐私计算进行系统全面的梳理和阐述。总体上，本文的贡献可以概括为以下三点：

(1)综合性技术总结：本文从技术原理的角度对隐私计算技术做出新的分类，并深入阐述了隐私计算中的关键技术，同时也总结了目前隐私计算的

* 通讯作者　Corresponding author：段佳，duanjia1@jd.com

收稿日期：2023-05-18；　录用日期：2023-08-25；　发表日期：2023-09-28

关键落地场景和应用。

(2)多维度技术对比:本文从技术优势、局限性、安全性以及风险点等多个维度对比了所有的隐私计算关键技术。

(3)未来挑战机遇:本文分析了隐私计算技术以及行业的发展现状,总结了隐私计算持续发展面临的挑战,并对未来的发展机遇进行了展望。

1 隐私计算技术分类和对比

隐私计算,作为数据安全流通的关键保障,其中运用到的关键技术也种类繁多。与其相似的一个概念则是隐私增强技术(Privacy-Enhancing Technologies PET),它的概念更加广泛,涵盖了隐私计算以及其他的隐私保护技术手段。经合组织的报告中将场景的 PET 技术分为了四大类:数据混淆技术,加密数据处理技术,联邦和分布式分析技术,数据问责工具。相比于 PET,隐私计算更多关注于安全技术本身,严格意义上来说,对问责工具系统并部涉及。因此,本文基于安全机制原理,将所有的关键技术进行分类,总体上可以划分为三类:基于密码学的技术,基于扰动的技术和基于软硬件的技术。具体的技术分类如图 1 所示。

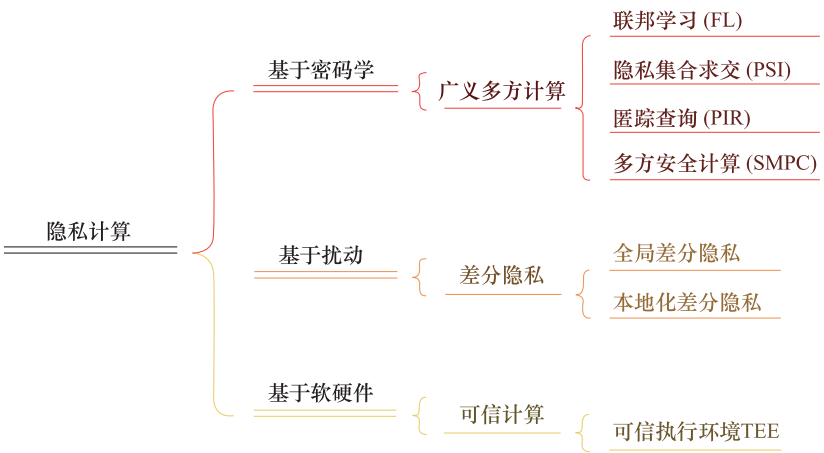

图 1 隐私计算技术分类

Fig. 1 The categories of privacy-preserving computation

在表 1 和表 2 中,通过分析对比可以看出,可信计算在支持运算、安全性、计算开销、损失精度方面都优于其他方法,但是它的信任机制是依赖硬件厂商,并且也会需要额外的硬件成本开销。多方安全计算,提供较高的安全性,但是却会带来较高的算力和耗时开销。联邦学习和差分隐私在安全性上有所妥协,但是算力开销小和容易实施都是它们的优势。隐私集合求交和匿踪查询都是具备一定安全性的技术方法,但是它们支持的运算操作有所局限。在第 2 节中,本文会对上述技术进行详细的阐述。

表 1 隐私计算技术的原理机制对比

Table 1 The comparison of privacy-preserving computation principle

	可信计算	多方安全计算	联邦学习 FL	差分隐私	匿踪查询	隐私集合求交
安全机制	可信硬件隔离 & 密码学	密码学 & 电路	数据不动,模型动 & 密码学	加入噪声扰动 & 随机响应	密码学	密码学
保护阶段	存储 & 使用	使用	使用	使用	使用	使用
信任基石	可信硬件不可攻破 & 密码学安全	多个参与方不存在完全串通 & 密码学安全	交互信息不包含原始数据	加入噪声扰动后,多次统计查询不可区分	密码学安全	密码学安全

续表

	可信计算	多方安全计算	联邦学习 FL	差分隐私	匿踪查询	隐私集合求交
支持运算	可信硬件内明文编程计算,理论上任意运算	底层支持常用算子,具体运算需要设计组合子协议	机器学习,深度学习	统计学查询,机器学习,深度学习	查询操作	求交集操作
额外计算开销	低	高	中	低	中～高	低～中
安全性	高	高	低～中	低	中～高	中～高
损失精度	无	低	低～中	中～高	低	低
特定硬件支持	需要	不需要	不需要	不需要	不需要	不需要

表 2 隐私计算关键技术优劣风险对比

Table 2 The advantage and disadvantage of different privacy-preserving computation

	优势特点	技术局限	风险点
可信计算	数据信息无损耗[3,4]; 域内无算法限制	需要硬件成本以及研发部署成本	硬件层面攻击; 可能面临侧信道攻击; 可信硬件黑盒未开源,需要完全信任芯片厂商
多方安全计算	理论上无须第三方参与[5,6]; 可直接得到结果和模型[7]	算力消耗大,耗时长	存在多个参与方串通风险; 存在密钥泄露的可能; 存在恶意参与方的可能
联邦学习	原始数据不出库[8]; 分布式架构降低总算力成本[9]	数据模型质量参差不齐; 通信复杂度较高	训练中间信息(梯度)可以部分逆推数据; 存在恶意参与方的可能
差分隐私	轻量化,易部署实施[10]; 噪声量级可变[11]	模型精准度存在损失; 安全性随着噪声变小而降低	噪声参数的选择需要在可用性和安全性之间平衡
匿踪查询	适用于数据交易流通[12,13]	仅限查询操作	存在数据方留存数据库的查询日志作为后门的可能
隐私集合求交	易实施[14,15]	仅限数据求交操作	简单方案中的 hash 容易被彩虹表攻击

2 隐私计算关键技术

2.1 可信计算

可信计算,也称作“机密计算”,是指在基于硬件的可信执行环境(Trusted Execution Environment,TEE)中对数据进行计算,同时保护数据的安全。它的主要目标是通过可信硬件构建程序运行态时的数据安全区。配合远程可信性验证,被加密保护的数据可以在 TEE 内直接完成隐私计算,实现“数据可用不可见”,确保隐私数据生命周期中使用隐私数据时的安全性。在可信计算的场景下,所有的信任根由安全可信硬件来保障,并以此为基础,结合密码学,向上构建透穿系统层直达应用层的可信执行环境信任链,并确保构建的信任链可以被远程度量验证。

TEE 的本质属性是隔离,即通过芯片等硬件技术与上层软件协同对数据进行保护,且同时保留与系统运行环境之间的算力共享。目前主要的 TEE 技术方案有 X86 指令集架构的 Intel SGX(Intel Software Guard Extensions)[3,4],AMD SEV(Secure Encrypted Virtualization)[16] 以及 RISC 指令集架构的 TrustZone 技术[17-19]。同时,国内芯片厂商也相继推出了支持 TEE 的技术方案,包括兆芯 ZX-TCT(Trusted Computing Technology),海光 CSV(China Security Virtualization),以及飞腾、鲲鹏也已经推出了自主实现的 TrustZone 功能。

具体地,Intel SGX 主要是将程序分成了可信和不可信两个部分。它通过构建一个受保护的安全容器 Enclave,来存放应用程序的敏感数据和代

码，而 Enclave 的安全边界只包含 CPU 和它本身。所有的敏感信息的安全操作都是在安全容器 Enclave 内部进行，Enclave 内部的代码和数据只能通过给定的接口访问。ARM TrustZone 则是在处理器层面引入了两个不同权限的保护区域：正常世界和安全世界，并通过一套鲁棒性的切换机制来保障任何时刻处理器仅在其中一个环境内运行。同时这两个世界完全是硬件隔离的，并具有不同的权限，正常世界中运行的应用程序或操作系统访问安全世界的资源受到严格的限制，反过来安全世界中运行的程序可以正常访问正常世界中的资源。AMD SEV 是 AMD 在安全虚拟化和安全内存加密基础上对虚拟机进行保护提供的安全虚拟化技术。加密虚拟机不仅可以让虚拟机免受物理威胁，还可以免受其他虚拟机甚至是 Hypervisor 本身。

2.2 安全多方计算(SMPC)

多方安全计算(Secure Multi-Party Computation，SMPC)是保障在无可信第三方的前提下，多方可以在不泄露信息的情况下参与计算并得到自己相应的输出。在安全多方计算中，框架协议都会首先假定安全挑战模型，主要包括半诚实敌手和恶意敌手模型。二者的主要区别在于是否诚实执行框架协议。针对不同的安全挑战模型，研究者已经提出了众多的开源多方安全计算框架：ABY/ABY3[5]，MP-SPDZ[6]，EzPC[7]等。

SMPC 底层是由多种密码学技术或协议共同构建而成。通过这些协议和技术实现基础的运算单元，被称作子模块。目前多方安全计算的研究领域可以大致划分为三个方向：子模块设计，通用 SMPC 框架以及 SMPC 的应用。子模块设计中涉及的密码学技术，主要包括秘密分享[20]、混淆电路[21]、同态加密[22]、不经意传输[23]等。秘密分享策略是指多个参与方分享一个秘密，只有大于阈值 t 数量的参与方才可以恢复秘密。同态加密是一种特殊的加密方法，它允许操作者对密文进行特定的代数运算，得到的密文结果，与明文进行处理运算后再加密的结果保持一致。换言之，同态加密提供了数据在密文域进行处理运算的能力。混淆电路是将计算任务转换为布尔电路，然后进行加密打乱等操作，以达到保护输入数据的目的。不经意传输是一种经典的密码学协议，本质上是允许一个参与方从其他参与方的 n 个秘密中选择 k 个，但是不会泄露选择的秘密信息。

另外，通用的 SMPC 框架并不针对某一特定问题，而是针对任意计算函数，都允许多方参与并以安全的方式共同计算。它主要是在特定的安全挑战模型的前提下，将目标计算函数转换为算术或者布尔电路，并且将电路分解为一系列的算术门或逻辑门的组合，并为对应电路设计相应的计算协议。目前通用的 SMPC 框架方法有 LEGO[24]等。另外也有研究者提出将 SMPC 分解为预处理和实时计算两个过程[25]来提升实时计算效率。与此同时，随着人工智能的兴起，SMPC 也被应用到机器学习当中[26,27]，用以解决多方参与多数据源共同训练或推理的问题。

2.3 联邦学习(FL)

作为分布式机器学习的一个变种，联邦学习(Federated Learning，FL)[8]通过多方联合训练，以达到数据本地化持有的同时，能够以较高的性能达到全局聚合训练的结果。如图 2 所示，客户端负责基于本地数据进行训练，得到本地化模型。服务器负责聚合本地模型，得到全局模型。

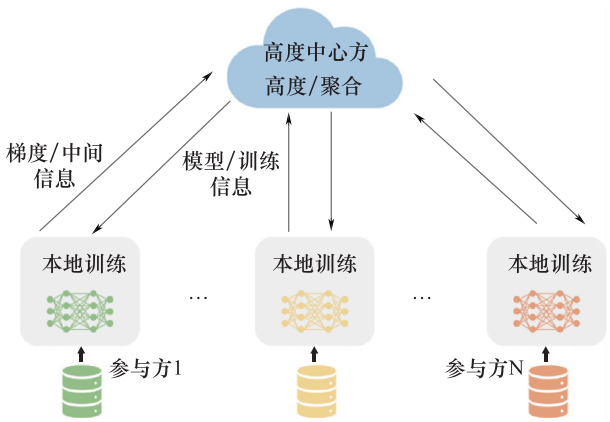

图 2 联邦学习结构流程图

Fig. 2 The flowchart of federated learning

在标准的联邦学习算法中，假设第 k 个客户端的数据集服从数据分布 D_k，并且客户端聚合权重定义为 p_k，其中 $\sum_{k=1}^{K} p_k = 1$。那么，K 个客户端参与的联邦学习优化算法可以定义为：

$$\min_{w\in\mathbb{R}^d} J(w)=\min_{w\in\mathbb{R}^d}\sum_{k=1}^{K} p_k \cdot J_k(w)$$
$$J_k(w)=\mathop{\mathbb{E}}_{z\sim D_k}[L_k(w;z)]$$

式中,$L_k(w;z)$ 表示在模型参数为 w 的情况下,第 k 个客户端对本地样本 $z=\{x,y\}$ 的损失函数。

根据联网络拓扑结构可以将联邦学习分为中心化联邦学习和去中心化联邦学习两种类型。二者的本质区别在于拓扑结构中是否有中心化的参与方。另外,根据参与方数据集的特征空间和样本空间的分布,联邦学习可被分为:横向联邦学习、纵向联邦学习学习,以及联邦迁移学习[9]。

在联邦学习中,由于分布式架构的特性,数据的质量,参与方的诚实度,网络的稳定性,聚合机制以及数据的分布等都极大地影响了最终的模型性能。针对联邦学习中的问题和挑战,众多研究者也开拓了多种多样的研究分支,主要涵盖优化算法,安全攻防以及产业应用等方面。针对加速联邦学习的优化问题,大量研究者提出了 FedAvg[8]、FedProx[28]、FedDYN[29]等优化算法用于加速联邦学习的收敛速率,或者解决数据分布不一致的问题。

另外,对于联邦学习中的安全性分析讨论,文章[30,31]提出了攻击算法,能够从梯度信息中较好地恢复出原始的数据集样本。鉴于梯度信息的不安全性,也有研究者提出了基于同态的横向联邦学习[32]和纵向联邦学习方案[33],用于保护梯度信息不泄露[32]。虽然学术界对联邦学习的安全性仍有讨论,但是由于其高效易实施的特性,联邦学习已经在医疗[34]、物联网[35]等多个领域有了实际应用。与此同时,国内的互联网企业也开发了安全的联邦学习框架,并应用于实际业务以解决数据孤岛问题,例如,微众银行的 FATE 框架应用于金融保险业务,京东和腾讯的京腾联邦应用于广告投放业务,百度的 PaddleFL 应用于信贷风控场景等。

2.4 差分隐私(DP)

差分隐私(Differential Privacy,DP)的目的是在描述数据集整体统计特征的同时,对数据集中个体的隐私提供保护[10]。它的数学定义[11]为,一个随机函数 $\mathcal{K}$,其值域集合为 S,即 $S\subseteq \mathrm{Range}(\mathcal{K})$。如果对所有的数据集 D_1 和 D_2,其中 D_1 和 D_2 仅仅存在一个元素不相同,都存在如下关系:

$$\Pr[\mathcal{K}(D_1)\in S]\leqslant \exp(\varepsilon)\times \Pr[\mathcal{K}(D_2)\in S]$$

那么称函数 $\mathcal{K}$ 满足 ε-差分隐私。从定义中可以看出,当参数 ε 越小时,两个相邻数据集经过函数 $\mathcal{K}$ 变换后的概率分布越相似,即对于攻击者而言,越难以区分这两个相邻数据集,对数据的保护程度也就越高。在实际应用中,根据特定的场景和函数,加入噪声扰动实现差分隐私的方法有很多种,例如,加入拉普拉斯或指数噪声,随机响应请求等等。基于噪声加入的位置不同,差分隐私可以分为两种类型:全局差分隐私和本地化差分隐私,具体参照图 3 所示。

全局差分隐私,它首先收集所有用户的原始数据,并假设存在一个数据管理者,由数据管理者来对特定查询加入扰动噪声,并对数据请求方的查询分析请求进行响应。在数据库发布方面,Dwork 首先提出了通过加入拉普拉斯噪声实现直方图数据发布的方法[36]。随后,Gupta 等[37]提出一种通用的迭代数据生成框架,理论涵盖了中位数机制和 PMW 机制。但是,上述的方案都是基于存在可信数据管理者的前提下,在现实中难以满足,并且集中式的数据管理,也存在容易被攻击和数据泄露的风险。

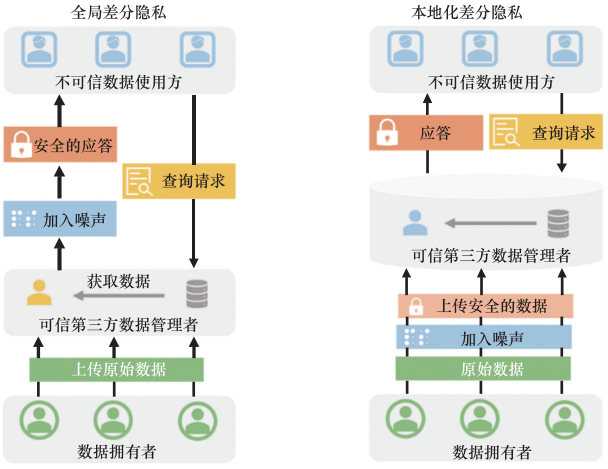

图 3 全局差分隐私和本地化差分隐私架构

Fig. 3 The architectures of global DP and local DP

本地化差分隐私则是在数据收集的源头加入噪声,然后再上传到数据中心。目前 Apple 和 Google 已经将本地化差分隐私[38]应用到了系统和浏览器当中。在统计查询方面,Kairouz 等[39]提出采用随机反馈机制,解决频率统计问题。随后,针

对频率统计问题，研究者利用 hash 映射[40]，随机矩阵[41]和 Hadamard 矩阵[42]变换等方法对频率统计中的通信效率进行了优化。而在机器学习场景方面，Zheng 等[43]采用对输入扰动，并构造目标函数的无偏估计来优化解决稀疏线性回归中的数据保护问题。同样地，在文章[44,45]中，Abadi 和 Wang 等人提出对梯度和目标函数进行扰动的策略，都可以很好地实现本地化差分隐私。

2.5 隐私集合求交(PSI)

隐私集合求交(Private Set Intersection，PSI)，它允许参与者秘密地计算各自数据源的交集，而不泄露除了交集以外的任何其他信息。虽然这种技术仅仅适用于数据求交集的操作，但是由于使用场景广泛，因此也是研究机构和企业追捧的一个研究热点。从技术原理的角度看，可以将目前的 PSI 方案分为 3 种：基于非对称密码的方案，基于混淆电路的方案和基于不经意传输的方案。

运用哈希可以快速实现 PSI，即将双方集合的所有元素以哈希函数映射，然后进行匹配求交。但是当参与双方存在半诚实或者恶意参与者时，恶意参与方可以通过彩虹表攻击等暴力碰撞方法，反推甚至恢复出非交集元素。基于非对称密码的方案，本质上是在哈希方案的基础上进行的安全性提升，其主要思想仍然是基于转换空间匹配，运用公钥技术，将原始集合的元素映射到不同的空间，可以得到基于不同公钥体制的 PSI 方案。例如，Meadows 首先在文章[46]中提出了基于 Diffie-Hellman 的 PSI 协议。整体方案的安全性保障是来源于 Diffie-Hellman 离散对数的 NP-hard 问题，因此安全性相比简单哈希，得到了极大的提升。后续，也有文章[14,15]致力于优化通信和计算开销，提升协议抵抗恶意攻击的能力。

除了采用非对称密钥协议的 PSI，也有研究者尝试采用基于电路的方案[47,48]。其主要是利用了基于电路的安全多方计算框架，这些框架不仅能进行 PSI 计算，也可以用于计算其他函数。这些方案虽然确保了安全性，但是计算代价和通信代价也有较大的提升。

不经意传输(Oblivious Transfer，OT)作为参与方交换秘密而不泄露额外信息的密码协议，由于其计算和通信效率高，被大量应用于两方或者多方 PSI 当中。基于 OT 协议构造不经意伪随机函数(Oblivious Pseudorandom Function，OPRF)的 PSI 方案是 Kolesnikov 等[49]提出的，主要是使用发送方的输入来对 OPRF 的密钥进行编程，相当于密钥与对方的集合元素相关。在直接使用 OT 协议完成 PSI 的方案中，Inbar 等[50]和 Dong 等[51]分别针对半诚实敌手提出了两方和多方 PSI 协议。

2.6 匿踪查询(PIR)

匿踪查询(Private Information Retrieval，PIR)，也被称为隐私信息检索[52]，用于保护用户查询信息，防止数据方得到用户的检索条件。具体地，PIR 场景描述为，客户端发送查询请求到服务端，服务端拥有一个数据库为客户端提供查询。在这种场景下，PIR 的目标是保护用户查询请求的隐私，以及同时保护服务端非请求数据的隐私安全。目前主流的 PIR 方案按照检索条件可以分为基于索引查询的方案(Index PIR)和基于匹配查询的方案(Keyword PIR)。

基于索引查询的方案(Index PIR)[12,13,53]需要客户端在查询数据库之前，已经预先得知想要查询的数据索引信息，并利用不经意传输(OT)或者同态加密的策略完成信息查询，并保障查询索引不被泄露给服务端的同时，非查询结果无法额外泄露给客户端。

如果服务端数据库的索引信息是需要保密不能泄露的，那么上述的 Index PIR 就会泄露数据库的分布情况。这时，另外一种基于匹配查询的方案(Keyword PIR)应运而生。Keyword PIR 的要求是，服务端不知道客户端请求的 key，也无法分辨客户端得到的 value。Keyword PIR 方案[54,55]可以利用同态加密和拉格朗日多项式插值的方式实现。相较于 Index PIR，Keyword PIR 在通信量上与同态方案的 Index PIR 相当，但是计算开销，却随着数据集数目的增长，呈线性增长。

3 行业应用

随着隐私计算技术的深入研究，隐私计算赛道在近几年迎来了投资融资的高潮，大量的技术研发

公司如雨后春笋般崛起,国内外涌现了大量隐私计算的实践应用。总体来看,目前的隐私计算应用场景主要覆盖在政务、金融、医疗、营销、运营商、零售、制造、交通等行业。在众多行业中,都存在大量的成功案例,例如,金融行业的信贷风控,医疗行业的识别病灶辅助诊断,交通的智慧交通车路协同隐私计算等。根据行业调研报告[56],本文接下来会针对应用占比最多的政务、金融、医疗以及广告营销行业的隐私计算发展和应用进行阐述。

3.1 金融行业

对信息安全要求较高的金融行业,隐私计算的落地实践众多。目前,在信贷风控中,金融机构可以通过 PSI 和 PIR,依托内部已有的企业信息,横向打通包括税务、交通、公安、征信以及其他关联经营交易数据,纵向打通垂直领域的行业数据,从而实现企业风控的基础信息补足,丰富企业主体风险评估的信息维度。其次,在场景金融中,为了给小微商户带来更加快速便捷、精准的客户体验,利用联邦学习技术,通过引入场景方和其他三方数据,为小微商户提供精准画像,从而提供高效且风险可控的信贷服务。第三,在预防、监控洗钱活动方面,银行等金融机构,通过引入横向联邦学习和多方安全计算技术,建立特殊客群信息安全融合与共享,可以极大地提高反洗钱监管的能力。特别是针对跨机构的资金追踪,还原资金链路等场景,隐私计算技术都提供了安全可行的解决方案。最后,在保险业务中,隐私计算技术也得到了大量的应用,用于安全高效地精算定价,存量挖掘以及保险理赔等场景。

3.2 医疗行业

利用隐私计算技术,促进医疗数据安全有序的流通共享,是一个促进医疗信息化转型,提升医疗信息价值的重要举措。目前医疗行业中,隐私计算主要落地应用的场景从临床研究到医保结算,涉及的整个医疗体系的各个环节。首先,医疗影像识别诊断中,可以利用横向联邦学习方法,将多家医院的医疗图像数据进行联合建模,多方共同参与训练一个通用的模型来识别病灶辅助诊断。其次,在电子病例结构化场景中,也可以通过横向联邦学习框架来完成信息抽取模型的训练。第三,在临床医学研究中,术后并发症预防以及罕见病的诊断问题都可以抽象为多个小样本在分布式架构下的分类学习任务,可以利用联邦学习等方法来解决。第四,针对医疗诊断相关分组(DRGs)问题,利用多方安全计算以及联邦学习技术,将多家医疗机构的数据进行联合训练,依据国家医保局公布的 CHS-DRGs 分组规范,将患者分入若干诊断组进行管理,从而基于诊疗数据进行更为精准的 DRGs 预测,帮助医保局实现精准控费。

3.3 政务行业

尽管政务大数据包含有巨大的社会与经济价值,但是在缺乏有效的安全保障的情况下,政务数据的开放受到了许多因素的制约。隐私计算技术的蓬勃发展,让政务数据共享开放看到了新的曙光。目前政务场景中,利用多方安全计算以及联邦学习技术,可以建设统一的政务数据共享开放计算平台,为数据跨境/域,民生服务提供坚实的保障基座。其次,审计机构跨域查询,可以在保障安全隐私的前提下,大大地提高跨域审计的工作效率,节省政府工作的各项开支。第三,由于政府部门的数据汇集了交通、教育、税务等多个维度的高价值数据,构建大规模的数据交易所,也成为了数据开放化、有序流通的有效举措。最后,智慧城市涉及安防、交通、环保、文旅等各个行业,通过对政务大数据(交通出行数据、公安数据、水电燃气数据等)融合利用,智慧城市可以有效提高整个城市的公共管理、公共服务、公共安全水平。其中涉及的数据融合利用,就离不开隐私计算技术的保驾护航。

3.4 广告营销

由于链路复杂,参与方众多,广告营销行业的数据孤岛问题愈发凸显。目前,已经有不少企业利用隐私计算的技术优势,合法合规地发挥全链路数据价值,赋能提效广告营销业务。具体地,流量平台利用隐私计算技术助力其高效合规地识别流量的质量,提升后续链路投放的效果。其次,部分媒体平台与广告主共同构建纵向联邦学习框架,利用“数据不动,模型动”的方式将双方数据源的特征联合建模,以达到更加精准的广告投放的目标。第

三,广告或者电商平台也利用 PSI/PIR 技术,安全引入三方价值数据,丰富用户数据维度,优化推荐效果,以达到促活拉新的目的。最后,基于 PSI/PIR,SMPC 以及联邦学习等技术,媒体/广告平台等也引入丰富的数据,可以使得广告做到多触点归因,准确识别每个用户触点的增益收益,在完备的经济学归因模型指导下,将广告贡献进行公平分配,实现广告资源的合理配比,最大化提升整体营销收益。

4 发展现状及挑战

4.1 发展现状

根据目前的隐私计算技术和产品的发展,整体市场尚处于前中期发展,稳定增长的阶段,环境已经日趋完备,市场空间巨大,整体处于高速发展的前中期。

近年来,国内外数据安全及隐私保护的立法进程不断加快,隐私保护和数据安全的环境日渐完善,主要体现有:

(1)隐私数据安全法规的颁布。各个国家分别颁布了数据安全及隐私保护法规。特别地,中国颁布实施的《网络安全法》《民法典》《数据安全法》以及《个人信息保护法》,都是从立法角度明确地规范和约束了数据生产流通过程中的数据安全。

(2)用户隐私保护意识及认知的提升。据调查显示,用户对于侵犯个人信息的关注度高达 80.94%。同时,随着各种数据泄露事件频发,用户也越来越关注自身的数据安全和个人信息的隐私保护。

(3)各项标准规范指引的制定。国际组织 ISO/IEC 和 IEEE-SA 都已经制定了对于安全多方计算、联邦学习、可信执行环境的国际标准。另外,仍有大量的隐私计算相关标准在立项制定中。

隐私计算在技术和产品层面都取得了飞速的发展,国内外技术产品出现以下情形:

(1)国外技术研究持续创新,商业化有所局限。国外的技术发展早于国内,并在不同技术层面取得了相应的成果。但是,这些企业对隐私计算的商业实践较为局限,目前主要发力于平台化建设和技术迭代探索。在具体的应用场景拓展方面,国外的大部分企业还处于发展起步阶段。

(2)国内技术产品迅猛发展,产品落地实践众多。国内的技术起步较晚,直到 2016 年,才逐渐出现在隐私计算垂直领域的厂商企业。但是也是从此时开始,国内隐私计算相关的文章数量以及技术企业的融资事件,都呈现逐年增长趋势。与此同时,金融、政务、医疗等几大热门行业纷纷入场隐私计算技术的探索和场景实践。这也极大促进了国内的隐私计算技术和应用实践的飞速发展。

4.2 面临挑战

虽然国内的隐私计算发展已经进入到快速上升期,但是也存在着一些发展瓶颈挑战。目前不少头部企业都具备隐私计算的技术实力,而视隐私保护程度的不同,相应方案的计算效率也不尽相同。但是,实际上,计算效率和安全性是互相制衡的两个因素。完美的技术方案往往是在计算代价,通信代价,安全性之间寻求平衡。因此,真正合理的隐私计算方案,应该在提供可证明安全的前提下,提供可衡量的计算效率。这里的可证明安全,是指明确定义安全假设,明确方案可以保护的维度,即在什么样的情形下,能够防御什么样的攻击,不能防御什么样的攻击。只有提供了技术方案的可证明安全,用户才可以在不同的场景中,依据自身的安全性需求,在安全性,计算代价,通信代价之间寻求一个适合的技术方案。

当前的隐私计算技术,都普遍存在多种隐私计算框架平台并存的现象。大部分企业,为了扩大技术影响力,闭源自研隐私计算平台或者框架,加上技术路线的多样化,系统架构不同以及功能实现等差异,导致了不同平台之间无法实现数据的可信流通。这就导致了,如果用户需要转换方案或者接入其他平台,代价往往是从零开始重新部署应用,以及重复建设和运营成本的提升。以上的情况,不仅会降低用户的业务效率,又会导致新的“计算孤岛”问题的出现。

因此,当前隐私计算发展亟须解决的挑战是,通过规范化接口,制定标准化协议,让不同隐私计算平台实现管理系统,算法协议等各层面的交互,进而能够让不同隐私计算平台共同完成同一项计

算任务,打破计算孤岛的限制。总而言之,互联互通的有效实现是数据要素全面流通的基础,也是产业全域数据可信流通的关键。

5 未来发展趋势

5.1 数据计算平台建设,产品服务化转型

目前隐私计算市场处于高期望高投资阶段,参与者众多且可以概括为生态型、技术型、应用型三种。不同类型的企业发展战略和能力优势也各有不同。但随着整个垂直领域的持续发展,市场和资本投入都会趋于稳定。未来几年,隐私数据计算平台建设将会成为一个稳定且持续的发展方向。无论是生态型还是技术型企业,打造综合性的隐私数据计算平台,整合多种数据源,构建完善的隐私计算技术壁垒,聚焦于特定的垂直领域,并持续实践应用,将成为企业的主导战略规划。因为,只有具备数据源,隐私计算技术,成功案例的成熟计算平台,才能在大浪淘沙的市场中吸引更多的行业用户,在资本热度退却的同时,完成自身的持续稳定发展。另外,在打造成熟平台建设的同时,隐私计算技术从方案化到产品化的转型也是市场发展的必然规律。随着行业的持续发展,只有打造精益敏捷的产品服务,才能更多地赢得市场。另外,已经初见雏形的数据交易所,在未来几年,将手握数据要素和安全技术实力,将在整个数据流通使用链路上拥有强有力的竞争实力。

5.2 核心竞争力:强大的技术优势,差异化的数据源,精益的产品能力

隐私计算未来的成熟发展是以完善的隐私计算基础设施建设为基石的。未来的商业应用将逐步迈入应用差异化场景实践的时期。行业应用的聚焦点由以前的“基础技术产品”转向“完善的数据计算服务”。在整体数据计算服务方面,面对日益增多的业务需求,都需要快速敏捷的产品调整来达成。这时,强大的技术优势将成为市场竞争中的基础门槛,差异化的数据源将成为市场竞争中的产品特色,精益化的产品能力将成为赢得用户的有力手段。

6 结束语

随着数据流通需求的日益提升,隐私计算作为保障数据流通安全,实现数据价值的有效手段,已经成为了科研和业界的热点技术方向。本文对其中的关键技术以及行业应用进行了详细阐述,并进行了分类和多维度的对比。同时,本文也总结了隐私计算的发展现状以及面临的挑战,并对未来的发展机遇进行了展望。

利益冲突:作者声明无利益冲突。

参考文献(References)

[1] 符芳诚,侯忱,程勇,等. 隐私计算关键技术与创新[J]. 信息通信技术与政策,2021,47(6):27.

[2] 闫树,吕艾临. 隐私计算发展综述[J]. 信息通信技术与政策,2021,47(6):1-1.

[3] Costan V,Devadas S. Intel SGX Explained[J]. Cryptology ePrint Archive,2016.

[4] Zheng W,Wu Y,Wu X,et al. A Survey of Intel SGX and Its Applications[J]. Frontiers of Computer Science,2021,15(3):1-15. https://doi.org/10.1007/s11704-019-9096-y

[5] Mohassel P,Rindal P. ABY3:A Mixed Protocol Framework for Machine Learning[C]. Proc. ACM SIGSAC Conf. Computer Communications Security:35-52.

[6] Keller M. MP-SPDZ:A Versatile Framework for Multi-party Computation[C]. Proc. ACM SIGSAC Conf. Computer and Communications Security:1575-1590.

[7] Chandran N,Gupta D,Rastogi A,et al. EzPC:Programmable,Efficient,and Scalable Secure Two-Party Computation for Machine Learning[C]. 2019 IEEE European Symposium on Security and Privacy(EuroS&P),2017:496-511.

[8] Mcmahan B,Moore E,Ramage D,et al. Communication-Efficient Learning of Deep Networks from Decentralized Data[C]. Proc. Artificial Intelligence and Statistics:1273-1282.

[9] Yang Q,Liu Y,Chen T,Tong Y. Federated Machine Learning:Concept and Applications[J]. ACM Trans. Intelligent Systems and Technology,2019,10(2):1-19. https://doi.org/10.1145/3298981

[10] 丁丽萍,卢国庆. 面向频繁模式挖掘的差分隐私保护研

究综述[J]. 通信学报,2014,35(10):200-209.
https://doi.org/10.3969/j.issn.1000-436x.2014.10.023

[11] Dwork C. The Differential Privacy Frontier[C]. Proc. Theory of Cryptography Conf.:496-502.

[12] Angel S,Chen H,Laine K,Setty S. PIR with Compressed Queries and Amortized Query Processing[C]. Proc. IEEE Symposium on Security and Privacy:962-979.

[13] Ali A,Lepoint T,Patel S,et al. Communication-Computation Trade-offs in PIR[C]. Proc. USENIX Security Symposium:1811-1828.

[14] Bay A,Erkin Z,Alishahi M,Vos J. Multi-Party Private Set Intersection Protocols for Practical Applications[C]. Proc. Int. Conf. Security and Cryptography:515-522.

[15] Bay A,Erkin Z,Hoepman J-H,et al. Practical Multi-Party Private Set Intersection Protocols[J]. IEEE Trans. Information Forensics and Security,2021,17:1-15.
https://doi.org/10.1109/TIFS.2021.3118879

[16] Kaplan D,Powell J,Woller T. AMD Memory Encryption[R]. White Paper,2016.

[17] Pinto S,Santos N. Demystifying Arm Trustzone:A Comprehensive Survey[J]. ACM Computing Surveys,2019,51(6):1-36.
https://doi.org/10.1145/3291047

[18] Pinto S,Garlati C. Multi Zone Security for Arm Cortex-M Devices[C]. Proc. Embedded World Conference.

[19] Feng E,Lu X,Du D,et al. Scalable Memory Protection in the PENGLAI Enclave[C]. Proc. USENIX Symposium on Operating Systems Design and Implementation:275-294.

[20] Shamir A. How to Share A Secret[J]. Communications of the ACM,1979,22(11):612-613.
https://doi.org/10.1145/359168.359176

[21] Yao A C. Protocols for Secure Computations[C]. Proc. Annual Symposium on Foundations of Computer Science:160-164.

[22] Gentry C. Fully Homomorphic Encryption Using Ideal Lattices[C]. Proc. ACM Symposium on Theory of Computing,2009:169-178.

[23] Rabin M O. How to Exchange Secrets with Oblivious Transfer[R]. Cryptology ePrint Archive,2005:1-26.

[24] Nielsen J B,Orlandi C. LEGO for Two-Party Secure Computation[C]. Proc. Theory of Cryptography Conf.,2009:368-386.

[25] Damgård I,Zakarias S. Constant-Overhead Secure Computation of Boolean Circuits Using Preprocessing[C]. Proc. Theory of Cryptography Conf.,2013:621-641.

[26] Huang Z,Lu W J,Hong C,Ding J. Cheetah:Lean and Fast Secure Two-Party Deep Neural Network Inference[J]. IACR Cryptol. ePrint Arch.,2022:207.

[27] Rathee D,Rathee M,Kumar N,et al. CrypTFlow2:Practical 2-Party Secure Inference[C]. Proc. ACM SIGSAC Conf. Computer and Communications Security,2020:325-342.

[28] Li T,Sahu A K,Zaheer M,et al. Federated Optimization in Heterogeneous Networks[C]. Proc. Machine Learning and Systems,2020:429-450.

[29] Acar D a E,Zhao Y,Matas R,et al. Federated Learning Based on Dynamic Regularization[C]. Proc. Int. Conf. Learning Representations,2021:1-36.

[30] Zhu L,Liu Z,Han S. Deep leakage from gradients[C]. Proc. Int. Conf. Neural Info. Processing Systems,2019:14774-14784.

[31] Yin H,Mallya A,Vahdat A,et al. See Through Gradients:Image Batch Recovery via Gradinversion[C]. Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition,2021:16337-16346.

[32] Zhang C,Li S,Xia J,et al. Batchcrypt:Efficient Homomorphic Encryption for Cross-silo Federated Learning[C]. Proc. USENIX Annual Technical Conf,2020:493-506.

[33] Hardy S,Henecka W,Ivey-Law H,et al. Private Federated Learning on Vertically Partitioned Data via Entity Resolution and Additively Homomorphic Encryption[J]. arXiv preprint arXiv:1711.10677,2017.
https://doi.org/10.48550/arXiv.1711.10677

[34] Brisimi T S,Chen R,Mela T,et al. Federated Learning of Predictive Models from Federated Electronic Health Records[J]. Int. Journal of Medical Informatics,2018,112:59-67.
https://doi.org/10.1016/j.ijmedinf.2018.01.007

[35] Jiang L,Tan R,Lou X,et al. On Lightweight Privacy-Preserving Collaborative Learning for Internet-of-Things Objects[C]. Proc. Int. Conf. Internet of Things Design and Implementation,2019:70-81.

[36] Dwork C,Mcsherry F,Nissim K,et al. Calibrating Noise to Sensitivity in Private Data Analysis[C]. Proc. Theory of Cryptography Conf.,2006:265-284.

[37] Gupta A,Roth A,Ullman J. Iterative Constructions and Private Data Release[C]. Proc. Theory of Cryptography

Conf. ,2012:339-356.

[38] Cormode G,Jha S,Kulkarni T,et al. Privacy at Scale: Local Differential Privacy in Practice[C]. Proc. Int. Conf. Management of Data,2018:1655-1658.

[39] Kairouz P,Bonawitz K,Ramage D. Discrete Distribution Estimation under Local Privacy[C]. Proc. Int. Conf. Machine Learning,2016:2436-2444.

[40] Wang T,Blocki J,Li N,et al. Locally Differentially Private Protocols for Frequency Estimation[C]. Proc. USENIX Security Symposium,2017:729-745.

[41] Bassily R,Smith A. Local,Private,Efficient Protocols for Succinct Histograms[C]. Proc. ACM Symposium on Theory of Computing,2015:127-135.

[42] Acharya J,Sun Z,Zhang H. Hadamard Response:Estimating Distributions Privately, Efficiently, and with Little Communication[C]. Proc. Artificial Intelligence and Statistics,2019:1120-1129.

[43] Zheng K,Mou W,Wang L. Collect at Once,Use Effectively:Making Non-Interactive Locally Private Learning Possible[C]. Proc. Int. Conf. Machine Learning,2017:4130-4139.

[44] Abadi M,Chu A,Goodfellow I,et al. Deep Learning with Differential Privacy[C]. Proc. ACM SIGSAC Conf. Computer and Communications Security,2016:308-318.

[45] Wang D,Gaboardi M,Xu J. Empirical Risk Minimization in Non-Interactive Local Differential Privacy Revisited[C]. Proc. Int. Conf. Neural Info. Processing Systems,2018:973-982.

[46] Meadows C. A More Efficient Cryptographic Matchmaking Protocol for Use in The Absence of A Continuously Available Third Party[C]. Proc. IEEE Symposium on Security and Privacy,1986:134-144.

[47] Huang Y,Evans D,Katz J. Private Set Intersection:Are Aarbled Circuits Better than Custom Protocols? [C]. Proc. NDSS,2012:1-5.

[48] Huang Y,Evans D,Katz J,et al. Faster Secure {Two-Party} Computation Using Garbled Circuits[C]. Proc. USENIX Security Symposium,2011:35-45.

[49] Kolesnikov V,Kumaresan R,Rosulek M,et al. Efficient Batched Oblivious PRF with Applications to Private Set Intersection[C]. Proc. ACM SIGSAC Conf. Computer and Communications Security,2016:818-829.

[50] Inbar R,Omri E,Pinkas B. Efficient Scalable Multiparty Private Set-Intersection via Garbled Bloom Filters [C]. Proc. Int. Conf. Security and Cryptography for Networks,2018:235-252.

[51] Dong C,Chen L,Wen Z. When Private Set Intersection Mmeets Big Data:An Eefficient and Scalable Protocol [C]. Proc. ACM SIGSAC Conf. Computer and Communications Security,2013:789-800.

[52] Chor B,Kushilevitz E,Goldreich O,et al. Private Information Retrieval[J]. Journal of the ACM,1998,45(6):965-981.
https://doi.org/10.1145/1721654.1721674

[53] Mughees M H,Chen H,Ren L. OnionPIR:Response Efficient Single-Server PIR[C]. Proc. ACM SIGSAC Conf. Computer and Communications Security,2021:2292-2306.

[54] Chen H,Huang Z,Laine K,Rindal P. Labeled PSI from Fully Homomorphic Encryption with Malicious Security[C]. Proc. ACM SIGSAC Conf. Computer and Communications Security,2018:1223-1237.

[55] Chor B,Gilboay N,Naorz M. Private Information Retrieval by Keywords[J]. IACR Cryptol. ePrint Arch. ,1997:1-19.

[56] 艾瑞咨询. 2022 年中国隐私计算行业研究报告[R]. 2022:1-89.

Privacy-Preserving Computation: A Comprehensive Survey of Methods and Applications

WANG Wei[1], SHAO Yu[1], DUAN Jia[2,*], ZHANG Zehua[2]

(1. School of Medical Technology, Beijing Institute of Technology, Beijing 102676, China;
2. JD Retail Platform Operation and Marketing Center, JD. com, Beijing 102676, China)

Abstract: This paper presents a comprehensive review of privacy-preserving computation, including its various methods, such as Trusted Environment Execution(TEE)computation, Secure Multi-Party Computation (SMPC), Federated Learning(FL), Differential Privacy(DP), and Private Information Retrieval(PIR), et. It also analyzes and compares these methods from the aspects of security, advantages/disadvantages, and risks. Additionally, this paper investigates the applications and development of privacy-preserving computation, which finally demonstrates that privacy-preserving computation has a significant contribution on data circulation and data value realization. At last, the paper analyzes the current situation and challenges of privacy-preserving computation, while pointing out the future direction of it.

Keywords: Privacy-preserving computation; data security; federated learning; differential privacy; secure multi-party computation

DOI: 10. 48014/ccsr. 20230517001

Citation: WANG Wei, SHAO Yu, DUAN Jia, et al. Privacy-preserving computation: a comprehensive survey of methods and applications[J]. Chinese Computer Sciences Review, 2023, 1(1): 1-12.