电子科技大学 信息与软件工程 学院

文献研究报告

课程名称 信息安全导论

教师 赵洋

学号 2020090916007

姓名 贾怀宇

电子科技大学教务处制表

隐私保护技术应用现状调研与发展趋势分析

2020090916007 贾怀宇

摘要

随着智能化设备的普及和信息的高度关联，人们越来越注意自己的隐私。如何保护好数据隐私是当下大热的一个话题。隐私保护涉及到许多方向，如隐私计算，密码学，联邦学习，网络安全。本文重点介绍隐私保护中的隐私计算，联邦学习和多方安全计算。差分隐私和同态机密是隐私计算中的组成之一，联邦学习也是近些年来受欢迎的数据隐私保护方式。联邦学习不仅依靠本身的机器学习思路，还会结合差分隐私和同态加密，来抵抗更高强度的隐私工具。多方安全计算也是隐私保护常用的技术。此外，我们为未来的研究和可能的应用提出了几个可能的方向。

关键词：Differential privacy, Federated learning, homomorphic encryption, MPC

一、隐私保护技术应用现状调研

1.1 隐私保护技术的应用价值与意义

什么是隐私？

隐私是指个人或实体不愿被外界知晓的信息。早在 19 世纪发表在《哈佛法律评论》上的《论隐私权》 [1]中就将隐私定义为“不受打扰的权利”。随后，各国不断修整完善涉及隐私权的法律法规，直到 2018 年 5 月欧盟实施了最严格的隐私保护法——《通用数据保护条例》[2]，要求企业赋予用户“被遗忘的权利”。同年，数据隐私被纳入计算机专有名词，指数据中直接或间接蕴含的，涉及个人或组织的，不宜公开的，需要在数据收集、数据存储、数据查询和分析、数据发布等过程中加以保护的信息。敏感信息是指不当使用或未经授权被人接触或修改会不利于国家利益、联邦政府计划的实行、不利于个人依法享有的个人隐私权的所有信息。隐私保护技术通过对原始数据的变换达到保护个人敏感信息不泄露的目的，同时保证能在变换后的数据上获取信息、模型或服务。[13]

什么是隐私保护？

隐私保护是指使个人或集体等实体不愿意被外人知道的信息得到应有的保护。[5]隐私包含的范围很广，对于个人来说，一类重要的隐私是个人的身份信息，即利用该信息可以直接或者间接地通过连接查询追溯到某个人;对于集体来说，隐私一般是指代表一个团体各种行为的敏感信息。隐私保护关注的是是否提供了隐私信息的匿名性。通常来讲，隐私保护是信息安全问题的一种，可以把隐私保护看成是数据机密性问题的具体体现。例如，如果数据中包含了隐私信息，则数据机密性的破坏将造成隐私信息的泄露.[3]

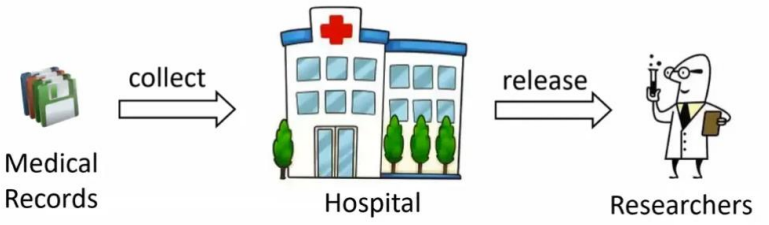
为什么要隐私保护？

在大数据的时代我们越来越离不开数据，利用数据可以给我们提供更好更方便迅捷的服务，比如依据位置自动为你推送附近的餐厅或者咖啡，依据你的浏览偏好为你展示你感兴趣的内容，依据你的就诊记录医生可以对你的身体情况有了一个初步的判断。但是这些数据一定程度上也正在给你带来严重的隐私问题，一些木马可以依据你的浏览偏好有意地推送那些你更容易点击的链接从而给你造成严

重的损失。
因此我们需要对数据进行一定的加工处理，保证它可用的同时又不会造成严重的隐私泄露问题。也就是说，我们需要保证我们的数据能够提供合适的信息为生活服务带来便利，但又不会泄露个人的敏感信息招致自身利益受损。

隐私保护的意义
大数据时代，隐私保护更加受到人们的关注。[6]事实层面上，大数据时代发展至今，个人隐私泄漏问题已然成为社会发展的隐患。人民网的调查显示，89%的被调查者不堪个人隐私泄露之忧。价值层面上，认为保护个人隐私相较发展大数据更有意义是一种更人性化的价值观。我们提倡保护个人隐私相较发展大数据科技更有意义，不是劝导人封闭自我、拒绝大数据时代，而是号召公众提高对于个人隐私的保护意识，APP 商家自觉承担起保护消费者隐私的责任，社会各界以一种冷静和审慎的态度对待科技的发展。

1.2　隐私保护技术的应用现状与案例
从隐私保护的角度来说，隐私的主体是单个用户，只有牵涉到某个特定用户的才叫隐私泄露，发布群体用户的信息（一般叫聚集信息）不算泄露隐私。 记得高德地图发过一张图，大意是开凯迪拉克的群体喜欢去洗浴中心…很多人说暴露隐私, 其实从学术定义上来说，这个不算隐私泄露，因为没有牵涉到任何个体。那么我们是不是可以任意发布聚集信息呢？倒是未必。
举例来说：医院发布了一系列信息，说我们医院这个月有 100 个病人，其中有 10 个感染 HIV。假如攻击者知道另外 99 个人是否有 HIV 的信息，那么他只需要把他知道的 99 个人的信息和医院发布的信息比对，就可以知道第 100 个人是否感染 HIV。



图一：HIV 举例

HIV 是相对敏感的信息，用户肯定不愿意泄露这一隐私，但在医院看病又会提到自己患有 HIV，那么如何保护好患者的个人信息不被非法者所利用就很重要。这也是隐私保护的重点。
二、隐私保护技术研究现状分析
2.1　隐私保护技术需解决的关键问题
隐私保护技术经过多年的发展，逐渐形成了几类较为成熟的方法：差分隐私的数据保护技术，联邦学习的机器学习安全，以安全多方计算为代表的隐私计算技术等。[3,4,5,6]隐私保护的应用场景从最初的关系型数据发布、基于位置的服务等简单场景，逐渐发展到较为复杂的社交网络、电子商务、图像识别等领域。在上述隐私保护应用场景中，数据可用性与隐私保护度是一对矛盾，隐私保护技术的关键问题就在于如何在保护隐私的前提下提高数据可用性。而在机器学习联邦学习场景下，隐私保护度和模型精确度是一对矛盾，隐私保护度的提升意味着模型预测精确度的下降、模型的收敛速度变慢等问题。尤其是深度学习模型结构异常

复杂，且不具备可解释性，使得隐私保护与模型可用性之间的矛盾关系无法量化。针对联邦学习中的隐私泄露问题，需要设计新的隐私保护方案。

2.2　隐私保护技术的研究思路与成果

联邦学习

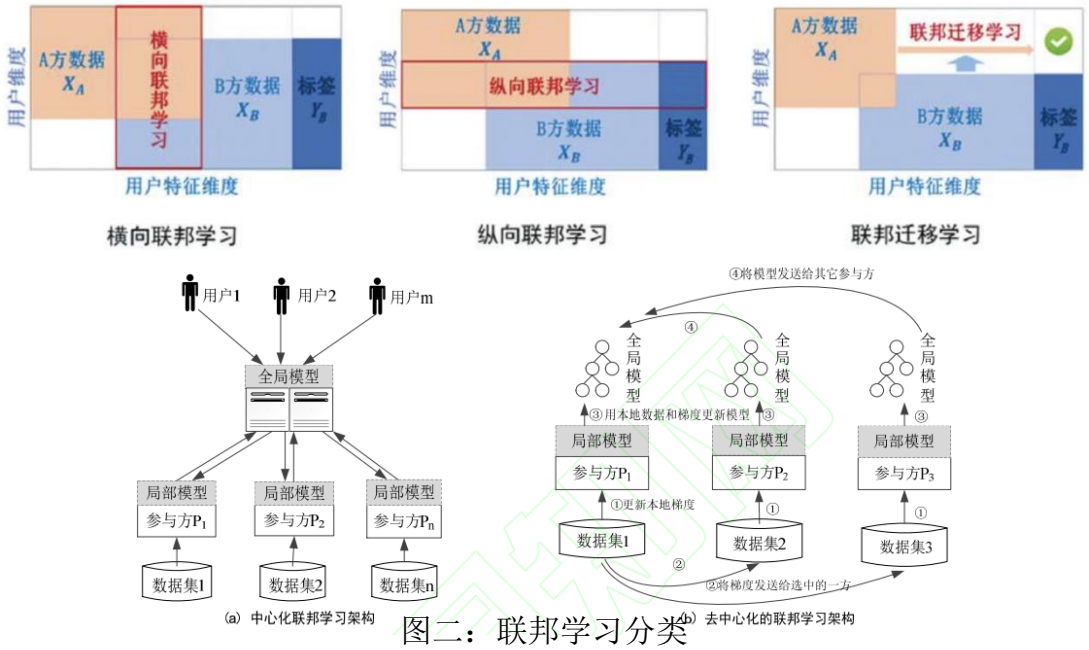
联邦学习是一种分布式机器学习架构，由中心服务器、参与方 Pi (1≤i≤ n)及用户构成。[3]其中，参与方各自持有本地数据集 Di，无需进行数据共享，通过协作的方式训练在全局数据上的模型 [3]。与传统的分布式系统不同，联邦学习的各参与方可以是“异质”的，即参与方软硬件配置、持有的数据格式、数据分布、模型结构等都可不同，

依据不同角度可对联邦学习进行如下分类：

(1) 根据参与方数量的多寡与算力的强弱，联邦学习可分为 cross-device 和 cross-silo 两类[5，6]。Cross-silo 中参与方往往为大型组织（如医疗、金融等相关机构），数量较少但算力较强；cross-device 中参与方为个人设备，数量庞大且算力较弱，在该场景下，不是每个参与方都有机会参与每一轮训练，通常利用采样的方式确定哪些用户可以参与训练过程。

(2) 根据联邦学习架构中是否存在中心服务器，联邦学习架构可以分为中心化架构与去中心化架构，如图所示。去中心化架构不需要可信服务器，在每次迭代中，参与方在本地数据上更新梯度，将梯度发送到选定的一方，选定方使用其本地数据和梯度值再度更新模型，直到所有参与方都更新了模型，最后将模型广播给所有参与方。为了保证模型的公平性，充分利用各方数据，参与方事先约定迭代相同的轮数。

(3) 根据不同参与方之间的数据特征分割方式，联邦学习又可分为横向联邦学习(Horizontal federated learning)、纵向联邦学习 (Vertical federated learning) 和联邦迁移学习(Transfer Federated Learning, TFL)[5]。数据水平分割指数据持有方存储了不同用户的具有相同属性的数据；数据垂直分割指数据持有方存储了相同用户的不同属性的数据；联邦迁移学习指数据持有方持有的数据中用户和属性重叠都较少的情况，如图所示。

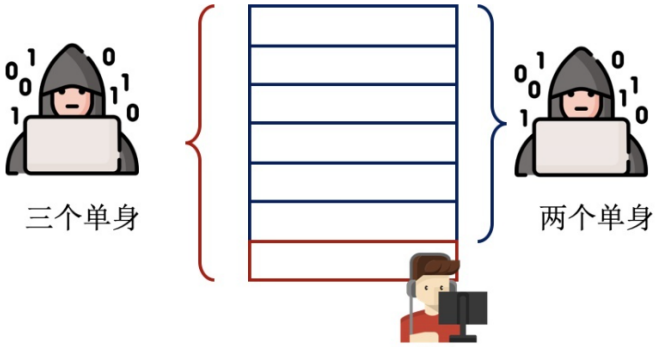


图二：联邦学习分类

差分隐私

差分隐私是建立在严格的数学理论基础之上的强隐私保护模型，能保证攻击者即便在具有最大背景知识的前提下，即已知数据库中除目标记录以外其他所有记录的信息，也无法推测出目标记录的敏感信息。

简单来说就是防范差分攻击的，举个简单的例子来说，假设现在有一个婚恋数据库，2 个单身 8 个已婚，只能查有多少人单身。刚开始的时候查询发现，2 个人单身；现在张三跑去登记了自己婚姻状况，再一查，发现 3 个人单身。所以张三单身。



图三：差分隐私示例

从数学的角度来说：查询函数：f(x):x->R，随机噪声可以用 r 表示，最终得到的查询结果就是 M(x)=f(x)+r，对于两个汉明距离为 1 的数据集 x,x`，对于任意的输出集合 S，应该有：

$$\Pr[\mathcal{M}(x) \in S] \leq e^{\varepsilon} Pr[\mathcal{M}(x') \in S]$$

这是差分隐私的核心算法，许多差分隐私手段都是基于这一算法扩展的。

安全多方计算

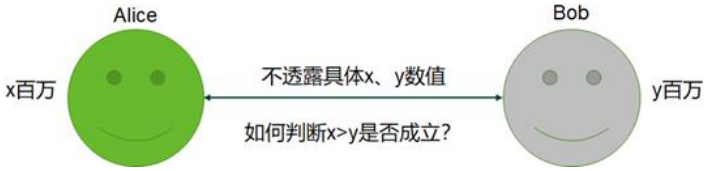
MPC：Secure Muti-Party Computation

安全多方计算的研究主要是针对无可信第三方的情况下，如何安全地计算一个约定函数的问题。安全多方计算是电子选举、门限签名以及电子拍卖等诸多应用得以实施的密码学基础。

MPC 的核心关键点在于加密本身的安全性和协议效率。其中协议效率的关键在加密算法的速度和通讯成本。

MPC 中最著名的就是百万富翁问题：[15]

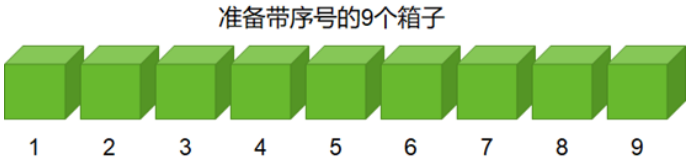
如图所示，姚氏百万富翁问题可解释为：两个争强好胜的富翁 Alice 和 Bob 在街头相遇（假定 Alice 财富为 x 百万，Bob 财富为 y 百万），如何在不暴露各自财富的前提下比较出谁更富有？



图四：百万富翁问题

对于图中的姚氏百万富翁问题，我们将以非密码学的、通俗易懂的语言讲解如何解决该问题。假定 x=3，y=7，即 Alice 拥有 3 百万，Bob 拥有 7 百万，他们只关心自己的财富在百万这个量级上，谁更富有。假定他们的财富都不会超过 1 千万，则可以默认为 Alice 和 Bob 的财富

值 x、y 取值范围为 1~9。
第一步：如图 2 所示，Alice 首先准备带序号 1-9 的 9 个箱子。



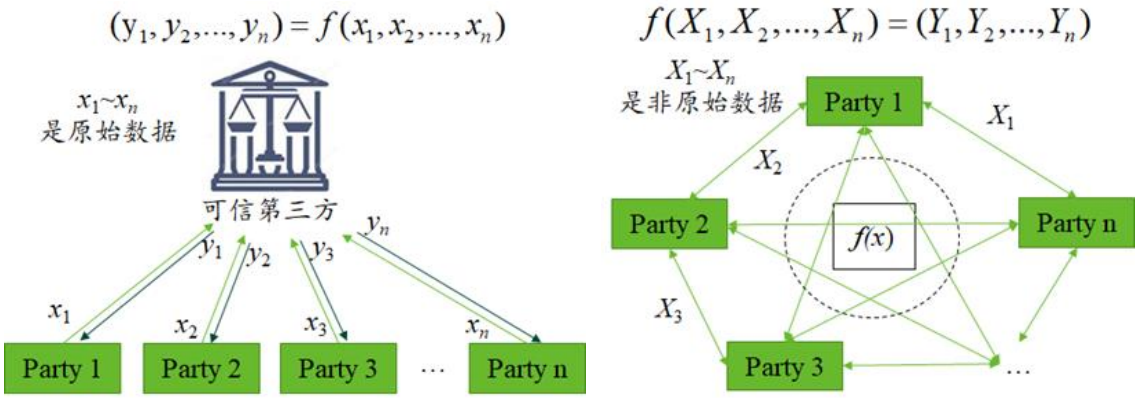
图五：百万富翁问题
第二步：Alice 在箱子内分别放入苹果和香蕉，规则为，如果箱子序号小于自己的财富值 x，则放入苹果，否则放入香蕉。由于 x=3，因此前 2 个箱子为苹果，后 7 个箱子为香蕉。
将带序号的 9 个箱子封装后，交给 Bob。

图六：百万富翁问题
第三步：如图所示，Bob 收到带序号的箱子后，避开 Alice 的视线，挑选序号与自己财富值 y 相等的箱子，然后撕掉序号，扔掉其他箱子。注意，Bob 只能诚实的挑选 1 次箱子。

图四：百万富翁问题
第四步：Bob 当着 Alice 的面打开选中的箱子，如果是香蕉，则 y≥x；是苹果则 x>y。本例中 Alice 最后看到的是一个如图 5 所示，没有序号的、带香蕉的箱子，表示 x>y 不成立，知道自己的财富不比 Bob 多。

通过以上步骤可知，在最后阶段，虽然 Alice 和 Bob 都看到了箱子里放的是香蕉（MPC 算法的计算结果），但由于箱子序号被撕掉，所以 Alice 并不知道 Bob 选的是第几个箱子（实现了 Bob 财富 y 对 Alice 的隐藏）；对于 Bob 来说，并不能确定序号 1-6 的 6 个箱子里，从第几个箱子开始，由苹果变成了香蕉（实现了 Alice 财富 x 对 Bob 的隐藏）。

安全多方计算可形式化描述为，n 个计算参与方分别持有数据 x1,x2,⋯,xn，协议的目的是利用各方的秘密数据计算一个预先达成的共识函数 y1,y2,⋯yn=f(x1,x2,⋯,xn)，此时任意一方可以得到对应的结果 yi，但无法获得其他任何信息。



图九：安全多方计算

在传统分布式计算模型下，传统的分布式计算由中心节点协调各用户的计算进程，收集各参与方的明文输入信息，各参与方的原始数据对第三方来说毫无秘密可言，很容易造成数据泄露。

在 MPC 计算模式下，不需要可信第三方收集所有参与节点的原始明文数据，只需要各参与节点之间相互交换数据即可，而且交换的是处理后（如同态加密、秘密共享等处理方法）的数据，保证其他参与节点拿到数据后，也无法反推原始明文数据，确保了各参与方数据的私密性。

三、总结与展望

3.1 现有技术存在的问题与不足

隐私保护技术从提出到现在只有短短二十年的发展时间，虽然现在隐私保护手段已经层出不穷，基于模型的改进方法和新的隐私保护模型不断被提出，与此同时，隐私保护技术的问题也不断显现。

应用实践十分困难：一项技术的提出终究是要落地，面向社会的。隐私保护技术虽然在不断完善，但真正应用到现实生活中还十分困难。一是人们对这一类技术的接受性普遍不高，二是技术尚未成熟，许多模型还存在于理论模型阶段，针对现实中复杂的情况鲁棒性未知。

假设过多：许多模型技术都是基于一定的假设。[13]尤其是对于联邦学习和差分隐私来说，它们更多是依靠对数据集来源做假设，在一定条件下实现自己的方法。也就是说，传统隐私保护模型的缺陷在于对攻击者的背景知识和攻击模型都给出了过多的假设。但这些假设在现实中往往并不完全成立，因此攻击总是能够找到各种各样的攻击方法来进行攻击。

现实数据的制约：现实生活中的数据依托互联网的发展早已达到不可估量的数值，大数量的数据十分考验模型。另外，数据的种类也十分复杂，并不是简单的数字和字符的组合，它代表着一个人生活各方面的细微信息。这种脆弱性的数据如何保护，是一个技术难点。

3.2 未来技术的发展方向

隐私保护技术，尤其是隐私计算，未来必将成为社会的热点。[14]它的发展将会

有以下几点：

技术模型完善：虽然针对隐私保护计算的关键技术研究已有多年，但在规模化应用时仍然存在多项难点，如上述所说等问题。当前市场对于隐私计算产品及服务的选择是建立在对于以市场落地实际需求为牵引的前提下，不断夯实关于安全多方计算、联邦学习、差分隐私等理论研究基础，积极开展面向实际产业需求的工程探索，不断提升隐私保护计算的技术成熟度和产业化能力。

多方协同发展：一项出色的技术发展离不开良好的团队合作。隐私保护技术复杂度高，技术面广，也有着较低的容错率，并且市场潜力强大。但是迅猛发展的市场也极易出现解决方案隐私保护水平高低不均、落地效果良莠不齐的现象。如何提高隐私保护技术的公信力，提升技术的竞争力，这就要求多方协同发展。共同研究，共同探讨，客服难点，一起发展隐私保护技术。

3.4 结论

本文简单介绍了隐私保护技术的主流手段，并且对比分析，提出现有技术的缺点和未来发展。本文先行回顾隐私的定义和隐私保护的必要性，再者介绍三种隐私保护的常见类型：联邦学习，差分隐私和安全多方计算。它们都是在隐私保护方向具有良好的架构与可塑性。最后我们指出，隐私保护发展的短短几年，虽然发展迅速，但还存在着许多缺点，是未来隐私保护技术的发展的重点。

参考文献

[1] Warren S, Brandeis L. The right to privacy[M]//Killing the Messenger. Columbia University Press, 1989: 1-21.

[2] Regulation GDP. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46[Z]. Official Journal of the European Union (OJ), 2016, 59(1-88): 294.

[3]尹春勇,屈锐.基于个性化差分隐私的联邦学习算法[J/OL].计算机应用:1-9[2022-12-07].http://kns.cnki.net/kcms/detail/51.1307.TP.20220530.2032.012.html

[4]刘松逢. 差分隐私保护的个性化联邦学习方法研究[D].广西师范大学,2022.DOI:10.27036/d.cnki.ggxsu.2022.001097.

[5]汪林玉.基于区块链的社会网络用户属性差分隐私保护研究方案[J].软件,2022,43(04):60-62.

[6]王腾,霍峥,黄亚鑫,范艺琳.联邦学习中的隐私保护技术研究综述[J/OL].计算机应用:1-15[2022-12-07].http://kns.cnki.net/kcms/detail/51.1307.TP.20220425.1937.008.html

[7] Zhu T, Li G, Zhou W, et al. Differentially private data publishing and analysis: A survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2017, 29(8): 1619-1638.

[8] Mohammed N, Chen R, Fung B C M, et al. Differentially private data release for data mining[C]//Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining. 2011: 493-501.

[9]阎允雪,马铭,蒋瀚.基于秘密分享的高效隐私保护四方机器学习方案[J].计算机研究与发展,2022,59(10):2338-2347.

[10] Hardt M, Ligett K, McSherry F. A simple and practical algorithm for differentially private data release[J]. Advances in neural information processing systems, 2012, 25.

[11] Blocki J, Blum A, Datta A, et al. Differentially private data analysis of social networks via restricted sensitivity[C]//Proceedings of the 4th conference on Innovations in Theoretical Computer Science. 2013: 87-96.

[12] Bowen C M K, Liu F. Comparative study of differentially private data synthesis methods[J]. Statistical Science, 2020, 35(2): 280-307.

[13] http://www.cac.gov.cn/2015-06/01/c_1115473995.htm

[14] http://www.caict.ac.cn/kxyj/qwfb/ztbg/202011/P020201110408006418997.pdf

[15] http://blog.nsfocus.net/calcul-ns/