DOI: 10.3969/j.issn.2096-8299.2020.04.015

基于差分隐私的敏感数据挖掘技术研究

谢 荣, 温 蜜

(上海电力大学 计算机科学与技术学院, 上海 200090)

摘 要: 基于加密的数据挖掘技术往往计算复杂度太高,而差分隐私作为一种数据扰动技术,既能有效降低计算复杂度,又能让使用者分析数据的整体价值。简要分析了差分隐私在具有敏感信息的智能数据挖掘系统中的相关技术。首先,介绍了差分隐私的基本概念;其次,针对频繁项挖掘、回归与分类以及深度学习,分别介绍了差分隐私在敏感数据挖掘中的应用;最后,对比了最新研究方法的性能和优缺点,为进一步研究隐私保护数据挖掘技术提供相关参考。

关键词: 差分隐私; 数据挖掘; 机器学习; 深度学习

中图分类号: TP309.2 **文献标志码:** A **文章编号:** 2096-8299(2020)04-0401-07

Research on Sensitive Data Mining Technology Based on Differential Privacy

XIE Rong, WEN Mi

(*School of Computer Science and Technology, Shanghai University of Electric Power, Shanghai* 200090, *China*)

Abstract: Data mining technology based on encryption often has too high computational complexity. However, as a data perturbation technology, differential privacy can effectively reduce the computational complexity and allow users to analyze the overall value of data. This article briefly analyzes the related technologies of differential privacy in intelligent data mining systems with sensitive information. First, the basic concepts of differential privacy are introduced. Second, differential privacy is introduced for the three major categories of frequent item mining, regression and classification in the application of sensitive data mining, in deep learning. Finally, the performance, advantages and disadvantages of the latest research methods are compared, which provides a reference direction for further research on privacy-protected data mining technology.

Key words: differential privacy; data mining; machine learning; deep learning

数据挖掘是一种从大量含有潜在知识的数据中发现有用信息的技术。但大量的数据包含隐私敏感信息,数据挖掘可能导致隐私信息的泄露。在不影响数据挖掘准确性的前提下,保护数据隐私是一个关键的挑战。近年来,敏感数据的保护引起了社会的广泛关注[1],其主要研究方向为隐私保护数据挖掘(Privacy-preserving Data Mining, PPDM)。PPDM既能提供数据挖掘技术,又能保

收稿日期: 2020-03-18

通信作者简介: 谢荣(1997—),男,在读硕士。主要研究方向为差分隐私与机器学习。E-mail: rongxie@mail.shiep.edu.cn。

基金项目: 国家自然科学基金(61872230)。

护数据库中用户的隐私。然而,PPDM 的主要挑战是抵抗熟练敌手的攻击[2-3]。为了克服这一挑战,PPDM 使用数据扰动[4]和加密技术[5]进行敏感数据的保护。基于加密的隐私保护数据挖掘技术提供了良好的安全性和准确性,但因其具有较高的计算复杂度,使得加密技术不适合大规模的数据挖掘[6]。与加密技术相比,数据扰动拥有较低的计算复杂度,使得它对大数据挖掘更有效[7]。噪声添加、几何变换、随机化、数据压缩、混合扰动是数据扰动的相关技术[8]。一个隐私模型定义了特定扰动机制的隐私信息保护和泄漏的限制[9],其中早期的隐私模型包括 k - 匿名,l - 多样性,t - closeness[10-11]等。研究表明,这些模型容易受到不同的攻击,如最小攻击[12]、基于合成的攻击[13]和背景知识攻击[14],而这些攻击能利用扰动后的数据来重建隐私信息。差分隐私(Differential Privacy,DP)是一种强大的隐私模型,与以前的隐私模型相比,可以为 PPDM 提供更好的隐私保护[15-16]。

近年来,差分隐私技术大致可分为两种:中心化差分隐私(Centralized Differential Privacy,CDP)和本地化差分隐私(Local Differential Privacy,LDP)[17-18],主要区别在于是否具有可信的第三方。中心化差分隐私应用的前提是聚合器是可信的,即第三方不会泄露用户隐私。本地化差分隐私不需要可信的第三方,仍然能保护用户的隐私数据,因而更加实用。虽然本地化差分隐私是最近才流行的,但已在工业界得到了应用,例如微软公司将其用于个人地理位置保护;苹果公司在用户的设备上也采用了本地化差分隐私来保护用户隐私;谷歌也在浏览器中加入了该技术来保护用户的浏览行为[19]。

1 差分隐私技术

1.1 中心化差分隐私

1.1.1 中心化差分隐私模型

定义 1(ε - DP) 扰动机制 K,其中 D 为机制 K 输出的集合。对于任意的一对相邻数据集 A 和 A',如果机制 K 满足:

$$\Pr[K(A) \in D] \leqslant e^{\varepsilon}\Pr[K(A') \in D] \quad (1)$$

则称 K 满足 ε - DP,其中参数 ε 为隐私预算。

当参数 ε 越小时,K 对数据的保护程度就越高,即扰动后和扰动前的数据概率分布情况接近,这样攻击者就很难分辨了。相反,隐私预算越高,保护程度就越低。中心化差分隐私保护模型如图 1 所示。

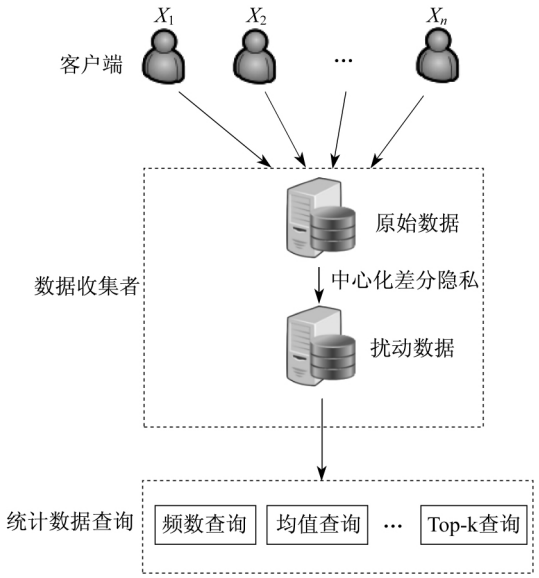

图 1 中心化差分隐私模型

1.1.2 中心化差分隐私框架

中心化差分隐私有交互式和非交互式两种数据保护框架[20]。在交互式保护模型下,数据管理者会根据数据应用需求设计出相应的差分隐私算法 K,当用户对数据服务器发出查询时,返回的结果将经过中心化差分隐私的处理才返回给用户。这一框架下存在的最大问题是隐私预算耗尽,然而解决这个问题的现有方法是限制查询数目,这也使得其在应用中具有一定的局限性。交互式保护模型如图 2 所示。

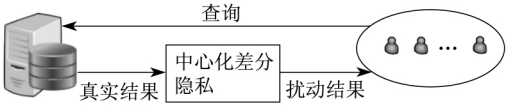

图 2 交互式保护模型

在非交互式保护模型下,数据的管理者会根据数据信息的特点来设计要发布哪些统计信息,并设计出隐私算法来进行处理发布。此时,用户只能对发布后的合成数据库进行查询或者挖掘任务来获得近似的结果。如何合理分配隐私预算,并尽可能地提高发布数据的可用性,是此框架下的研究重点。非交互式保护模型如图 3 所示。

图 3　非交互式保护模型

1.2　本地化差分隐私

1.2.1　本地化差分隐私模型

近年来,许多研究都投入到本地化差分隐私中。本地化差分隐私与中心化差分隐私的功能一样,最大的区别在于其在用户端对数据进行随机扰动,而非在数据库中。本地化保护模型如图 4 所示。

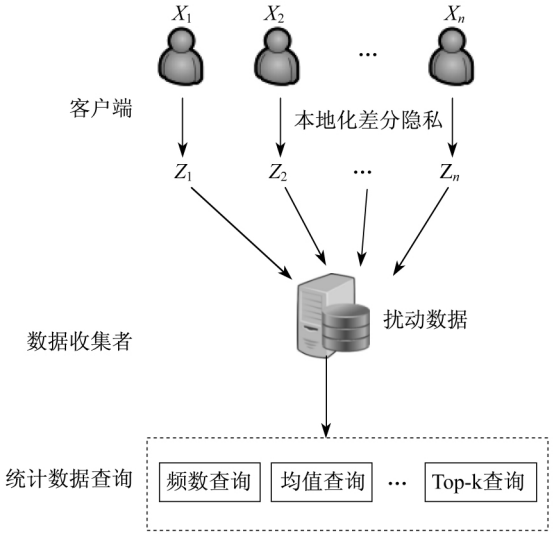

图 4　本地化差分隐私保护模型

定义 2(ε – LDP)　对于一组用户,每个用户拥有一条数据,若随机机制 K 在任意两条数据 x 和 x'上得到结果 z 满足式(2) ,则称机制 K 满足 ε – LDP。

$$\Pr[K(x) = z] \leqslant e^{\varepsilon}\Pr[K(x') = z] \quad (2)$$

1.2.2　本地化差分隐私框架

本地化差分隐私保护数据的框架[17]也有交互式和非交互式两种,如图 5 和图 6 所示。

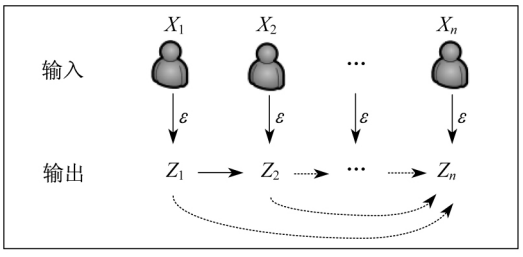

图 5　交互式框架

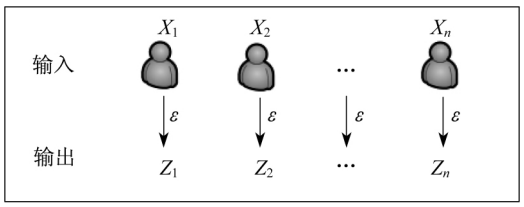

图 6　非交互式框架

其最大特点是针对单个用户而言,充分考虑了数据间的关联关系。图 5 和图 6 中,当 X_1,X_2,X_3,…,X_n为输入序列,Z_1,Z_2,Z_3,…,Z_n为输出序列,箭头表示依赖关系,则整个框架表示为: $Q(Z_j \mid X_j)$,Q 表示查询。

在交互式框架中,第 j 个输出Z_j依赖于第 j 个输入X_j以及前 $j-1$ 个输出Z_1,Z_2,Z_3,…,Z_{j-1},但与前 $j-1$ 个输入无依赖关系。因此,本地化差分隐私的形式定义为: 对任意的 x 和x',给定隐私预算 ε,若查询 Q 满足式(3) ,则认为Z_j是X_j的一个满足 ε – LDP 保护的表示,即

$$\sup_s \frac{Q(Z_j \mid X_j = x, Z_1, \cdots, Z_{j-1})}{Q(Z_j \mid X_j = x', Z_1, \cdots, Z_{j-1})} \leqslant e^{\varepsilon} \quad (3)$$

在非交互式框架中,第 j 个输出Z_j仅依赖于第 j 个输入X_j。因此,非交互式框架下的本地化差分隐私可以表示为: 对任意的 x 和 x',给定隐私预算 ε,若查询 Q 满足式(4) ,则认为Z_j是X_j的一个满足 ε – LDP 保护的表示,即

$$\sup_s \frac{Q(Z_j \mid x)}{Q(Z_j \mid x')} \leqslant e^{\varepsilon} \quad (4)$$

2　敏感数据挖掘方法介绍

差分隐私在敏感数据挖掘中的应用大致可分为频繁项挖掘、回归与分类以及深度学习 3 大类。在中心化差分隐私下的敏感数据挖掘任务已得到了广泛研究,但在本地化差分隐私环境下的应用还非常有限,并且模型也很简单。

2.1　敏感数据频繁项挖掘

频繁项挖掘是一项核心的数据挖掘任务,同时具有重要的经济和研究意义。然而,发布频繁项集会带来隐私方面的挑战。

文献[21]提出了两种有效的算法来挖掘敏感数据集中的 k 个最频繁模式: 第 1 个算法基于指数机制; 第 2 个算法基于拉普拉斯机制,通过返

回与数据中 k 个最常见模式的实际列表接近的噪声模式列表来解决敏感数据挖掘。文献 [22] 提出了 Privbasis 的方法——一个称为基集的概念，并用其来寻找最频繁的项集。文献 [23] 提出了一种在高隐私度下效果更好的方法，首先识别 Top – k 频繁项集，然后用它们构造一个差分隐私的 FP 树。文献 [24] 为 ROPPOR 机制提出了一种新疑的解码算法，该算法能够估算“未知数”，即我们不知道的字符串，并且该算法不是 ROPPOR 特有的，可以推广到其他本地化差分隐私机制中，以学习字符串中随机变量的分布。文献 [25] 从高维数据隐私出发，提出了一种基于本地化差分隐私的多维联合分布估计算法，实现了多属性间的相关性识别。文献 [26] 提出了一种实用、准确和高效的 Harmony 系统，用于在满足本地化差分隐私的前提下收集和分析来自智能设备的数据，其适用于包含数值和分类属性的多维数据，并支持基本的统计数据，尤其是均值估计。

2.2 敏感数据的回归与分类

隐私和安全问题通常会阻止用户数据的共享，甚至会阻止从中获得知识的共享，从而阻止有价值的信息被利用。隐私保护数据挖掘，如果正确使用，可以缓解这一问题。回归与分类是数据挖掘中最重要、应用最广泛的技术之一。

文献 [27] 提出了一种基于随机决策树方法的差分隐私决策树集成算法，用差分隐私的查询来构造保护隐私的 ID3 决策树，则能在数据集较小的情况下获得良好的预测精度。文献 [28] 提出了一种基于多类高斯混合模型分类器的学习算法，可利用带扰动正则项的大边缘损失函数来保持数据的差分隐私。文献 [29] 考虑到在分布式多方环境中开发保护隐私的机器学习算法问题，提出了一种新的针对多方设置的差分隐私算法，使用基于随机梯度下降的过程直接优化整个多方对象，而不是从优化局部目标中学到的分类器的组合。文献 [30] 在差分隐私模型的基础上开发了一个朴素贝叶斯分类器，可以允许一个提供者集中访问一个数据集。最近文献 [31] 在本地化差分隐私模型的基础上开发了朴素贝叶斯分类器，首先个人发送他们的扰动输入，以保持要素值与类标签之间的关系，然后数据聚合器估计朴素贝叶斯分类器所需的所有概率，最后基于估计的概率对新实例进行分类。文献 [32] 首次使非交互式本地化差分隐私模型下的学习任务成为可能，并从多个方面扩展了非交互式本地化差分隐私的学习领域。

2.3 敏感数据的深度学习

基于深度学习的技术在许多领域都取得了显著效果。通常，模型的训练需要大量具有代表性的数据集，这些数据集可能是由众包获得的，并且包含敏感信息，模型不应该在这些数据集中公开隐私信息，所以需要设计满足隐私保护的深度学习算法。

文献 [33] 专注于深度学习中的自动编码器，并提出了具有隐私保护的深度自动编码器。其主要思想是通过干扰传统深度自动编码器的目标功能来实施数据的差分隐私，并将其用于社区网络中人类行为预测，具有良好的性能。文献 [34] 提出了一种用于语义丰富数据的通用隐私发布框架，其中数据管理员没有对数据进行清理后发布，而是发布了一个深度生成模型。该模型使用原始数据以差分隐私的方式进行训练，利用生成的模型，分析人员能够分析任务生成的合成数据。文献 [35] 提出了一种差分隐私生成对抗网络模型，其主要思想是在学习过程中为梯度添加经过精心设计的噪声来实现生成对抗网络中数据的差分隐私。文献 [36] 首次提出了一种在本地化差分隐私模型下的卷积神经网络。该算法分为 3 层，即卷积模块、随机化模块和全连接模块，与以往的模型相比，其将隐私保护的功能量化为隐私预算系数而非隐私预算，就导致即使在较低的隐私预算下也可以实现较高的准确性。该模型在 MNIST 和 CIFAR – 10 上的测试精度均优于以往算法。

3 性能分析

3.1 基于差分隐私的频繁项挖掘

本文选择了数据挖掘中几个经典的方案进行性能分析。具体分析结果如表 1 所示。

3.2 基于差分隐私的回归与分类

目前，中心化差分隐私发展比较成熟，在敏感数据挖掘中的应用也比较广泛。本文主要分析了本地化差分隐私在回归与分类中的应用。具体分析结果如表 2 所示。

表 1　差分隐私在敏感数据频繁项挖掘中方案比较

方案	优点	缺点
文献 [19]	发布误差较小,数据可用性高	需考虑 Bloom filter 参数的设置问题
文献 [25]	弱化高维度对精度的影响	高昂的通信代价和计算开销
文献 [26]	时间复杂度低,发布误差小,数据可用性高	个体数据偏离原始数据的程度大
文献 [27]	容易实现,分类准确率高	不易控制隐私预算系数分配
文献 [30]	模型简单,易于实现,能处理多分类任务	依赖于对数据分布的假设,而且数据集越小噪声越大
文献 [31]	模型更安全,通信代价低	降维技术可能会对精度产生影响

表 2　差分隐私在敏感数据的回归与分类中方案比较

方案	优点	缺点
文献 [36]	噪声误差小	仅适用于目标函数一阶和二阶导数的绝对值受常数约束的情况
文献 [37]	满足差分隐私,防止敏感信息泄露	回归分类精度低,噪声误差大
文献 [38]	满足差分隐私,防止敏感信息泄露	权向量的灵敏度计算开销大,仅适用于约束条件强的目标函数、凸函数和对偶可微函数
文献 [39]	分类精度高,噪声误差小	仅适用于线性表示的目标函数
文献 [40]	满足差分隐私,防止敏感信息泄露	权向量的灵敏度计算开销高,仅适用于约束条件强的目标函数
文献 [41]	高精度,低噪声	仅适用于特定数据集
文献 [42]	在本地差分隐私下用指数机制寻找局部最优解的一种优选方法	计算开销大

3.3　基于差分隐私的敏感数据的深度学习

文献 [43] 为不共享输入数据集的神经网络开发了一种分布式多方学习机制,称为 [SS15]。该方法基于随机梯度下降优化算法,其隐私损失根据模型的参数计算。由于存在许多模型参数,通常会有数千个这样的模型参数,因此,该方法可能会导致大量的隐私损失。文献 [44] 引入了一种基于中心差分隐私的高效差分隐私机制,称为 [ACG + 16]。该模型运行在用于机器学习的 TensorFlow 软件库上,能够在适度的隐私预算下实现较高的效率和性能。其算法是基于随机梯度下降的差分隐私保护。此外,他们还引入了一种跟踪隐私损失的机制,即隐私会计,允许对隐私损失进行严密的自动化分析。但当该方法用于更大的数据集时,其差分隐私机制的错误率可能会导致不稳定的隐私泄漏。文献 [36] 提出了一种基于本地差分隐私的一元编码机制,称为 LATENT。他们将优化的一元编码进行改进,引入上界定理,并提出了隐私预算系数的概念,将隐私保护程度转移到了隐私预算系数上。该模型在本地进行数据的扰动,并在云端进行模型的训练,可以既安全又高效地实现数据的处理任务。[SS15]、[ACG + 16]、LATENT 3 种方法的性能对比如图 7 所示。

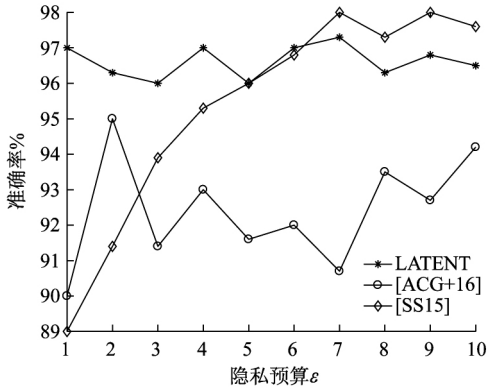

图 7　3 种方法在敏感数据深度学习中的性能比较

由图 7 可知,LATENT 即使是在扰动较大的情况下仍能保持较高的精度; 而 [SS15] 和 [ACG + 16] 只有在扰动较小的情况下才能体现出令人满意的精度。此外, [SS15] 和 [ACG + 16] 的另一个缺点是需要可信的第三方。因此,在对安全性要求较高的场景下,可使用 LATENT 方法; 在对安全性要求较低的场景,推荐使用 [SS15] 方法。

4　基于差分隐私的敏感数据挖掘技术面临的挑战

近年来,虽然 PPDM 得到了广泛研究,但面对各种分布数据如何设计出一种安全和实用的技术仍然面临很大的挑战。

(1) 在分布式环境下,敏感数据类型较多,面对离散与连续、低维与高维以及键值对数据,如何有效地并行处理难度较大。

(2) 在本地化差分隐私环境下比在差分隐私

环境下设计的算法安全性更高，但扰动误差更大，如何设计合理的扰动机制具有一定的难度。

(3) 在物联网环境中，大多的隐私保护需要轻量级方案，如何设计出通信代价低的算法也较为困难。

(4) 近年来，联邦学习作为一种新型的分布式机器学习被广泛研究。该模型虽然解决了用户数据的隐私问题，但其模型参数仍能受到攻击，而且该模型最大的阻碍就是通信代价。针对差分隐私保护技术，如何设计出既能保护模型参数和减小通信代价，又能保证模型精度的机制也存在困难。

5 结 语

在大数据时代，数据挖掘技术不断发展，个人隐私数据的保护显得尤其重要，数据挖掘技术的隐私问题是阻碍其发展的重要因素。差分隐私作为一种成熟的隐私保护技术，凭借其隐私性好、计算开销低等特点被广泛研究。近些年，国内外学者对隐私保护数据挖掘技术进行了广泛和深入的研究，然而在本地设置中的研究还非常有限，究其原因主要是本地化差分隐私的扰动在本地进行，算法设计不当会产生较大误差。因此，目前最大的挑战就是在本地设计出一种误差小、开销低的算法，从而使敏感数据挖掘技术更加可靠。

参考文献:

[1] 魏为民，孔志伟，杨朔，等. 基于大数据的安全威胁情报研究[J]. 上海电力学院学报，2018，34(1)：53-58.

[2] YANG K，HAN Q，LI H，et al. An efficient and fine-grained big data access control scheme with privacy-preserving policy [J]. IEEE Internet of Things Journal，2017，4(2)：563-571.

[3] ATSALAN D，SEHILI Z，CHRISTEN P，et al. Privacy-preserving record linkage for big data: current approaches and research challenges [M]//ZOMAYA A Y，SAKR S. Handbook of Big Data Technologies. Berlin: Springer，2017: 851-895.

[4] CHEN K K，LIU L. A random rotation perturbation approach to privacy preserving data classification [EB/OL]. (2015-01-01) [2020-03-18]. https://corescholar.libraries.wright.edu/knoesis/916/.

[5] KERSCHBAUM F，HÄRTERICH M. Searchable encryption to reduce encryption degradation in adjustably encrypted databases [C]//IFIP Annual Conference on Data and Applications Security and Privacy. Springer，2017: 325-336.

[6] GAI K，QIU M，ZHAO H，et al. Privacy-aware adaptive data encryption strategy of big data in cloud computing [C]//2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). Beijing，China: IEEE，2016: 273-278.

[7] XU H，GUO S，CHEN K. Building confidential and efficient query services in the cloud with rasp data perturbation [J]. IEEE Transactions on Knowledge and Data Engineering，2014，26(2)：322-335.

[8] CHAMIKARA M A P，BERTOK P，LIU D，et al. Efficient data perturbation for privacy preserving and accurate data stream mining [J]. Pervasive and Mobile Computing，2018(5)：1-19.

[9] MACHANAVAJJHALA A，KIFER D. Designing statistical privacy for your data [J]. Communications of the ACM，2015，58(3)：58-67.

[10] CHAMIKARA M A P，BERTOK P，LIU D，et al. Efficient privacy preservation of big data for accurate data mining [J]. Information Sciences，2019(5)：420-443.

[11] LI N，LI T，VENKATASUBRAMANIAN S V. T-closeness: privacy beyond k-anonymity and l-diversity [C]//2007 IEEE 23rd International Conference on Data Engineering. Istanbul，Turkey: IEEE，2007: 106-115.

[12] ZHANG L，JAJODIA S，BRODSKY A. Information disclosure under realistic assumptions: privacy versus optimality [C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria，Virginia，USA: ACM. 2007: 573-583.

[13] GANTA S R，KASIVISWANATHAN S P，SMITH A. Composition attacks and auxiliary information in data privacy [C]//Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM，2008: 265-273.

[14] WONG R C W，FU A W C，WANG K，et al. Can the utility of anonymized data be used for privacy breaches? [J]. ACM Transactions on Knowledge Discovery from Data，2011，5(3)：16.

[15] DWORK C. The differential privacy frontier [C]//Proceedings of the 6th Theory of Cryptography Conference，2009: 496-502. https://doi.org/10.1007/978-3-642-00457-5_290

[16] MOHAMMED N，CHEN R，FUNG B，et al. Differentially private data release for data mining [C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Diego，CA，USA: ACM. 2011: 493-501.

[17] KASIVISWANATHAN S P，LEE H K，NISSIM K，et al. What can we learn privately? [J]. SIAM Journal on Computing，2011，40(3)：793-826.

[18] DUCHI J C，JORDAN M I，WAINWRIGHT M J. Local privacy and statistical minimax rates [C]//2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS). Berkeley，CA，USA: IEEE，2013: 429-438.

[19] ERLINGSSON Ú,PIHUR V,KOROLOVA A. Rappor: randomized aggregatable privacy-preserving ordinal response [C] //Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 1054-1067. DOI. 10.1145/2660267.2660348.

[20] ZHANG X,MENG X. Differential privacy in data publication and analysis [J]. Chinese Journal of Computers,2014(4): 927-949.

[21] BHASKAR R,LAXMAN S,SMITH A,et. al. Discovering frequent patterns in sensitive data [C] //Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Washington DC,USA: ACM. 2010: 503-512.

[22] LI N H,QARDAJI W,SU D,et al. Privbasis: frequent itemset mining with differential privacy [J]. Proceedings of the VLDB Endowment,2012,5(11): 1340-13510.

[23] LEE J,CLIFTON C W. Top-k frequent itemsets via differentially private FP-trees [C] //Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM,2014: 931-940.

[24] FANTI G,PIHUR V,ERLINGSSON U. Building a rappor with the unknown: privacy-preserving learning of associations and data dictionaries [EB/OL]. (2015-03-04) [2019-12-15]. https://arxiv.org/abs/1503.01214v1.

[25] REN X B,YU C M,YU W R,et al. LoPub: high-dimensional crowdsourced data publication with local differential privacy [J]. IEEE Transactions on Information Forensics and Security, 2018,13(9): 2151-2166.

[26] NGUYÊN T T,XIAO X K,YANG Y,et al. Collecting and analyzing data from smart device users with local differential privacys [EB/OL]. (2016-06-16) [2019-12-15]. https://arxiv.org/abs/1606.05053.

[27] JAGANNATHAN G, PILLAIPAKKAMNATT K, WRIGHT R N. A practical differentially private random decision tree classifier [C] //2009 IEEE International Conference on Data Mining Workshops. Miami,FL,USA,2009: 114-121.

[28] PATHAK M A,RAJ B. Large margin gaussian mixture models with differential privacy [J]. IEEE Transactions on Dependable and Secure Computing,2012,9(4): 463-469.

[29] RAJKUMAR A,AGARWAL S. A differentially private stochastic gradient descent algorithm for multiparty classification [C] //Proceedings of the 15th International Conference on Artificial Intelligence and Statistics. PMLR,2012: 933-941.

[30] VAIDYA J,SHAFIQ B,BASU A,et al. Differentially private naive bayes classification [C] //2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT). Atlanta,GA,USA,2013: 571-576.

[31] YILMAZ F,AL-RUBAIE M,CHANG J M. Locally differentially private naive bayes classification [EB/OL]. (2019-03-03) [2019-12-28]. https://arxiv.org/abs/1905.01039v1.

[32] ZHENG K,MOU W L,WANG L W. Collect at once,use effectively: making non-interactive locally private learning possible [EB/OL]. (2017-01-11) [2019-12-18]. https://arxiv.org/abs/1706.03316.

[33] PHAN N,WANG Y,WU X,et al. Differential privacy preservation for deep auto-encoders: an application of human behavior prediction [C] //Proceedings of the 30th AAAI Conference on Artificial Intelligence. Phoenix, Arizona, USA, 2016: 1309-1316.

[34] ZHANG X,JI S,WANG T. Differentially private releasing via deep generative model [EB/OL]. (2018-03-25) [2019-12-15]. https://arxiv.org/abs/1801.01594.

[35] XIE L Y,LIN K X,WANG S,et al. Differentially private generative adversarial network [EB/OL]. (2018-02-19) [2019-12-15]. https://arxiv.org/abs/1802.06739.

[36] CHAMIKARA M A P,BERTOK P,KHALIL I,et al. Local differential privacy for deep learning [EB/OL]. (2019-08-08) [2019-12-28]. https://arxiv.org/abs/1908.02997? context=cs.CR.

[37] SMITH A. Privacy-preserving statistical estimation with optimal convergence rates [C] //Proceeding of ACM Symposium on Theory of Computing. San Jose,CA,USA: ACM. 2011.

[38] SAMET S. Privacy-preserving logistic regression [J]. Journal of Advances in Information Technology,2015,6(3): 88-95.

[39] ZHANG J,ZHANG Z J,XIAO X K,et al. Functional mechanism: regression analysis under differential privacy [J]. Proceeding of VLDB Endowment,2012,5(11): 1364-1375.

[40] CHAUDHURI K,MONTELEONI C,SARWATE A D. Differentially private empirical risk minimization [J]. J Mach Learn Res,2011,12: 1069-1109.

[41] LEI J. Differentially private m-estimators [C] //Proceedings of the 24th International Conference on Neural Information Processing Systems,2011: 361-369.

[42] ZHANG J,XIAO X,YANG Y,et al. Privgene: differentially private model fitting using genetic algorithms [C] //Proceeding of ACM SIGMOD International Conference on Management of Data. ACM,2013: 665-676.

[43] SHOKRI R,SHMATIKOV V. Privacy-preserving deep learning [C] //2015 53rd Annual Allerton Conference on Communication,Control,and Computing. Monticello,IL,USA,2015: 1310-1321.

[44] ABADI M,CHU A,GOODFELLOW I,et al. Deep learning with differential privacy [C] //Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM,2016: 308-318.

(责任编辑　胡小萍)