差分隐私在数据保护中的应用

Application of Differential Privacy in Data Protection

王宇/Wang Yu[1]，由永桥/You Yongqiao[1]，袁琦/Yuan Qi[2]，田琛/Tian Chen[2]，安媛媛/An Yuanyuan[2]，孙良友/Sun Liangyou[3]
（1. 烟台市大数据中心，中国 烟台264600；
2. 中国信息通信研究院，中国 北京100191；
3. 烟台海颐软件股份有限公司，中国 烟台264001）
(1. Yantai Big Data Center, Yantai 264600, China;
2. China Academy of Information and Communications Technology (CAICT), Beijing 100191, China;
3. Yantai Haiyi Software Co. , Ltd. , Yantai 264001, China)

DOI：10.12142/ZTETJ.202605013
网络出版地址：https://link.cnki.net/urlid/34.1228.TN.20241012.1529.002
网络出版日期：2024-10-12
收稿日期：2024-09-15

摘要：针对匿名化、脱敏等传统技术难以抵御重新识别与差分攻击的局限，提出一种融合中心化与本地化差分隐私的通用数据保护架构，可灵活配置两种模式：本地化模式下由终端完成数据扰动，保障原始数据不出域；中心化模式下由数据管理器统一加噪，实现隐私泄露的量化管控。同时明确3类组件的功能要求，并结合具体实践验证其可行性。差分隐私可有效解决传统方案对攻击者背景知识的依赖，为数据“可用不可见”提供可落地的技术路径。

关键词：差分隐私；数据安全；隐私保护

Abstract: To address the limitations of traditional techniques such as anonymization and desensitization in resisting re-identification and differential attacks, a general data protection architecture that integrates centralized and local differential privacy is proposed, supporting flexible configuration of two modes: in the local mode, data perturbation is performed at the terminal to ensure that raw data does not leave its domain; in the centralized mode, noise is added uniformly by the data manager to achieve quantitative control over privacy leakage. The functional requirements of the three types of components are also specified, and the feasibility of the proposed architecture is validated through practical implementations. Differential privacy can effectively eliminate the dependence of traditional schemes on attackers´ background knowledge and provide a practical technical pathway for making data "usable but invisible."

Keywords: differential privacy; data security; privacy protection

引用格式：王宇, 由永桥, 袁琦, 等. 差分隐私在数据保护中的应用 [J]. 中兴通讯技术, 2026, 32(5): 97-102. DOI: 10.12142/ZTETJ.202605013
Citation：Wang Y, You Y Q, Yuan Q, et al. Application of differential privacy in data protection [J]. ZTE technology journal, 2026, 32(5): 97-102. DOI: 10.12142/ZTETJ.202605013

在中国数字经济不断探索发展的过程中，数字应用广泛融入人们的生产、生活之中。数字应用的过程中，会涉及个人隐私数据，如身份信息、生物识别信息、医疗信息、财产信息等。数据一旦发生严重安全事件，带来的危害是巨大的。

当前较常使用匿名化技术、脱敏技术、同态加密和多方安全计算来保护个人隐私数据。上述技术能够提供一定的安全保护，但无法保护个人信息主体免受恶意攻击者的重新识别攻击，也无法抵抗差分攻击。因此，差分隐私作为一种应对差分攻击的新型隐私保护方法，被广泛研究和应用[1]。美国已于2020年人口普查过程中使用差分隐私技术，在保护公民个人隐私的前提下，公开尽可能多的人口信息，进而服务于人口政策研究。

目前，差分隐私技术作为一种数据保护方案，在某些领域的数据采集、发布和分析方面具有一定优势，可以充分发挥差分隐私技术的潜力，满足日益增长的数据隐私保护需求。本文将对差分隐私的分类、基于差分隐私的数据保护技术以及差分隐私技术应用现状进行研究和分析。

1 差分隐私的概念和分类

1.1 差分隐私概念

Cynthia Dwork 于2006年最早提出了差分隐私保护模型[2-3]，其核心概念来自密码学语义安全，即攻击者无法区分不同明文的加密结果。该模型通过对原始数据加入随机噪声，确保在某一数据集中插入或删除一条记录的操作不会影

响任何计算的输出结果。当满足差分隐私保护要求时，任何一个个体的变化不会对查询结果产生明显影响。与传统隐私保护方案不同，差分隐私模型假设攻击者拥有最大背景知识（即攻击者能够获得除目标记录外所有其他记录的信息），且建立在严谨的数学公式推导之上，可以有效解决传统隐私保护技术对攻击者背景知识的依赖以及缺乏量化分析评估能力的问题。

差分隐私的基本原理是：数据处理者使用特别设计的随机算法在准确结果中注入适量噪声，得到一个不影响统计分析的带噪查询结果并返回给第三方，确保输出的查询结果受单个记录的影响始终低于某个阈值，从而使得第三方无法从带噪结果中推理出单个记录的更改或者增删，即无法获得单个记录的准确数据，实现数据可用不可见，从而防止隐私数据泄露。

下面通过数据定义更形式化地理解差分隐私。假设有随机算法 M，S 是 M 所有可能输出结果组成的集合，Pr[·]表示概率。对于两个相邻数据集 D 和 D'（两个有且仅有一条记录不同的数据集合可称为相邻数据集），满足公式（1）：

$$\exp(-\varepsilon) \leqslant \frac{\Pr[M(D') \in S]}{\Pr[M(D) \in S]} \leqslant \exp(\varepsilon) \quad (1),$$

则该算法满足 ε–差分隐私。从差分隐私的数学定义中可以看出，差分隐私要求算法 M 在相邻数据集上的输出分布具有相似性。相似性越大，ε 越小，所对应模型的隐私性越高。

1.2 差分隐私分类

差分隐私可以从 3 个方面进行分类：一是根据噪声数据扰动使用的方式和使用阶段的不同，差分隐私可分为基于输入扰动的差分隐私、基于输出扰动的差分隐私、基于目标扰动的差分隐私和基于梯度扰动的差分隐私；二是根据算法实现方式，差分隐私可分为拉普拉斯机制、指数机制、高斯机制和随机应答机制等差分隐私；三是根据噪声添加的位置及统计计算的先后执行位置，差分隐私可分为中心化差分隐私（CDP）和本地化差分隐私（LDP）[4–5]。下面重点介绍第 3 种差分隐私技术的分类。

Cynthia Dwork 最早提出的差分隐私是一种中心化差分隐私，是指在对用户数据进行采集后，通过一个可信任的第三方数据处理器对查询结果统一进行加噪处理，从而保护数据隐私。具体来说，可信任的第三方数据处理器会在采集到所有数据后，对整个数据集进行加噪处理后发布加噪后的数据集，如图 1 所示。

中心化差分隐私技术的实现依赖于可信第三方数据处理器，而实际情况中可信第三方数据处理器非常少，因为它们需要具备高度的诚信和保密能力，以确保差分隐私技术的正确实现和使用，并确保不会滥用或泄露用户的个人隐私信息。因此，中心化差分隐私技术的应用仍然面临一定的挑战和限制。

由于在实际应用中寻找一个真正可信的第三方数据处理器十分困难，本地化差分隐私技术应运而生。该技术消除了对可信第三方处理器的假设，在数据采集阶段由用户终端对每个用户数据添加噪声，使用户原始数据不离开终端，从而保护个人隐私。具体来说，分布于 N 个终端的用户数据在本地进行加噪处理后，再提交至不可信的第三方数据处理器进行聚合统计，并发布统计结果，如图 2 所示。

中心化差分隐私和本地化差分隐私需要噪声实现机制来保证算法满足 ε–差分隐私。中心化差分隐私的典型机制是拉普拉斯机制和指数机制：拉普拉斯机制旨在向数值型数据

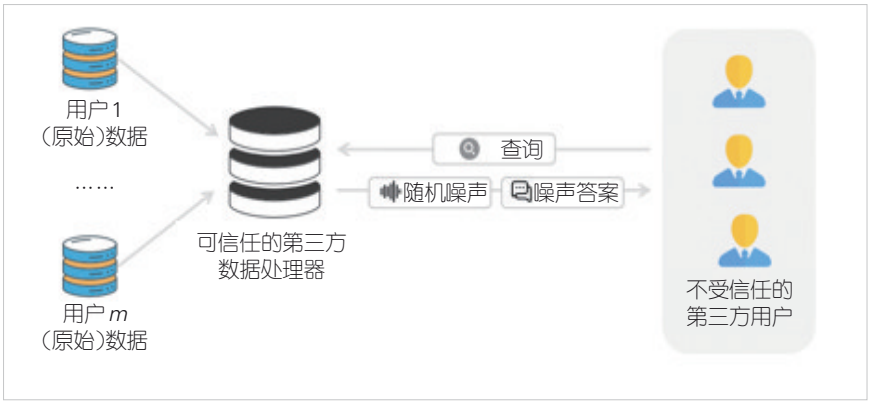


图1　中心化差分隐私技术

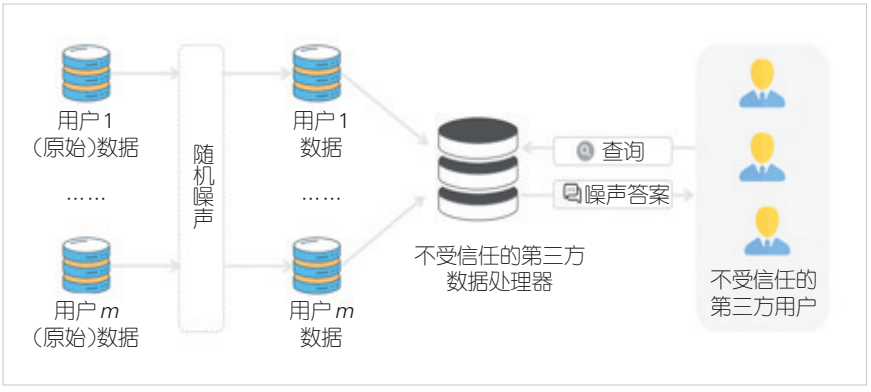


图2　本地化差分隐私技术

的查询结果中添加拉普拉斯噪声；指数机制旨在对离散型数据的查询结果进行随机化处理。以上两种机制均与定义在相邻数据集 D 和 D' 之上的敏感度有关。本地化差分隐私是在用户终端对每个用户的原始数据添加噪声，数据集中只有一个用户的数据，因此不存在敏感度的概念。本地化差分隐私技术的典型实现采用随机响应机制。

2 基于差分隐私的数据保护技术

2.1 技术架构

基于差分隐私的数据保护技术架构如图3所示。该技术架构包括用户端、数据管理器和接收端3部分，能够根据噪声添加位置的不同，灵活配置本地化模式和中心化模式，为实际系统应用提供差分隐私功能。具体而言，整体技术流程如下：

1）当配置为本地化差分隐私模式时，用户端对各种类型的数据进行采集，然后根据业务需求进行必要的数据预处理、添加噪声，并判断是否满足本地化差分隐私需求。随后，数据通过加密网络汇聚到数据管理器，进行存储、数据变换等操作。最终，数据被传输给接收端进行数据分析。

2）当配置为中心化差分隐私模式时，用户端采集并预处理数据后，将数据直接汇聚给数据管理器，并由数据管理器统一完成噪声添加操作。然后，数据被传输给接收端进行数据分析。从框架图中可以看出，两种模式的差别在于噪声添加机制的实施阶段不同，具体噪声添加算法也存在差异。

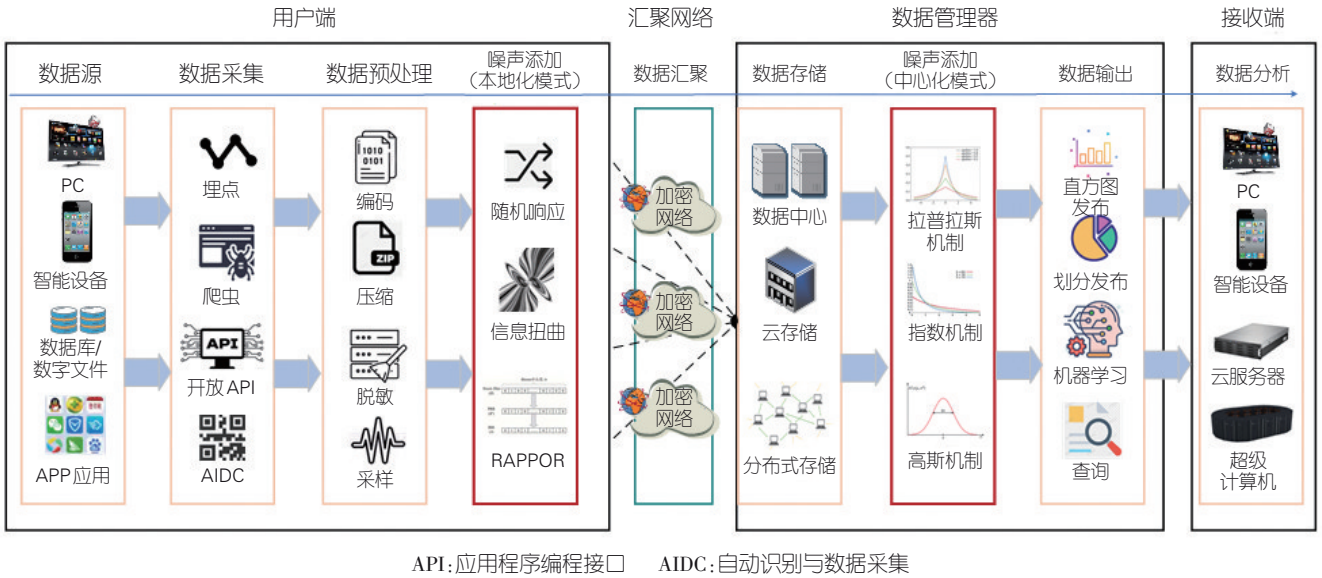
2.2 核心模块与关键技术

1） 用户端

用户在日常生活及使用互联网服务时会产生聊天记录、图片、视频、语音、电话号码、位置等各类隐私信息。本文中我们将能够直接产生用户数据的软硬件实体统称为用户端，例如PC台式机、智能手机手表以及各类APP应用及数据库软件等。在本地化差分隐私中，用户端扮演着重要角色，需要完成数据采集、预处理以及噪声添加等关键操作：

（1）数据采集

由于数据源往往高度多样化，数据采集技术也会根据不同场景采用不同方式。常见方式包括数据埋点技术、自动识别与数据采集（AIDC）、爬虫技术以及开放应用程序编程接口（API）调用等。埋点技术是指开发人员集成采集软件开发工具包（SDK），在触发事件的具体方法中植入多行代码，将需要上传的数据上报至服务端。AIDC是一种自动识别和收集数据对象并存储于计算机中的技术。例如，射频识别、条形码磁条扫描、全球定位系统（GPS）传感器等都属于用于识别与捕获物理数据的方法。爬虫技术是一种自动化、系统化收集Web端数据的技术。根据收集内容和策略不同，爬虫可以细分为基于链接、基于内容、基于图标的爬虫，以及广度优先、深度优先爬虫等。针对已有平台数据，往往可以采用开放API调用的方式，获取已有数据库中的数据。通过配置接口链接、请求参数、请求参数值确认接口访问信息，并配置访问次数、访问频次、分页设置等，完成接口的调度执行，最终将接口数据集成到数据表中。



API：应用程序编程接口　　AIDC：自动识别与数据采集

图3　基于差分隐私的数据保护技术架构

数据采集者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的方式和范围。数据采集者应制定标准的采集模板、数据采集方法、策略和规范，采集策略参数配置应包括采集周期、有效性、检测时间、入口地址和采集深度等。数据采集者采集数据的类型包括低维数据和高维数据。如果采集数据的特征数量大于采集数据量，这类数据属于典型的高维数据。例如，健康保健数据涉及的个体特征数量非常巨大，如血压、静息心率、免疫系统状态、手术史、身高、体重、现状等。

（2）数据预处理

将各个用户终端的原始数据汇聚到服务端之前，需要进行一些必要的数据预处理操作。例如，智能手机设备中能够唯一标识用户的信息需要从被采集数据集中剔除，这些信息包括IP地址、设备ID、设备类型及状态、国际移动设备识别码（IMEI）、时间戳等。此外，为了方便服务端处理，还经常会对原始数据进行编码与压缩操作，常用的编码格式包括美国信息交换标准代码（ASCII）、信息交换用汉字编码字符集（GB2312）、8位统一码转换格式（UTF-8）、16位统一码转换格式（UTF-16）、Base64编码等。

（3）噪声添加（本地化差分隐私模式）

在本地化差分隐私中，由于不存在全局敏感度的概念，每个用户将各自的数据进行扰动后，再上传至数据收集者（在本框架内由数据管理器承担该角色）并进行频数统计。主流的扰动机制采用随机响应技术，其中经典算法是RAPPOR算法。具体而言，该算法首先将每个用户的字符串数据编码为长度为h的二进制向量，同时记录字符串与布隆过滤器（Bloom Filter）的映射关系矩阵；然后利用随机响应技术对向量$\boldsymbol{B}$的每一位加入扰动，得到永久性随机响应（PRR）结果$\boldsymbol{B}$和$\boldsymbol{B}'$；再对$\boldsymbol{B}'$的每一位进行第2次扰动，得到瞬时性随机响应（IRR）结果S。每个用户得到扰动结果S后，将其发送至服务端，服务端统计每一位上1出现的次数并进行校正，然后结合映射矩阵，通过Lasso回归方法完成用户数据的频数统计。除此之外，一些新的机制被用于实现扰动功能，例如基于信息压缩和扭曲的扰动机制。该方法通过基于信息扭曲的扰动函数对每个用户数据进行噪声添加操作。信息扭曲度规定了原始用户数据与扰动数据偏差的数学期望上限，并根据确定的扭曲值设计实际的扰动函数，以满足ε-本地化差分隐私。

2） 数据管理器

从各种数据源采集的数据通过加密网络汇聚到数据管理器，由数据管理器统一进行存储、噪声添加以及数据变换等操作。下面我们进行详细介绍。

（1）数据存储

根据不同的数据规模与业务场景，数据管理器采用的技术形态会有所不同。对于规模不大的结构化数据（例如医院的病例数据、酒店入住人员信息等），通常可以采用传统的关系型数据库进行存储，并满足复杂联合查询的需求。对于半结构化数据（例如用户的简历、调查问卷等），可以使用非关系型数据库（NoSQL）进行处理，主流技术包括Apache HBase、MongoDB、Amazon Neptune、Redis等。针对大规模的非结构化数据（例如文本、图像、视频等），Hadoop集群则能够利用其自身的大规模并行处理能力，为收集来的数据提供存储和快速查询能力。

（2）噪声添加（中心化差分隐私模式）

在中心化差分隐私中，数据管理器充当可信第三方的角色。由于其能够看到所有收集数据的集合，因此可以根据全局敏感度为查询结果添加相应噪声，并通过统计方式限制隐私信息泄露的量化边界。拉普拉斯机制和指数机制是两种常见的中心化差分隐私噪声添加机制。以拉普拉斯机制为例，当需要发布的数据是n个等宽的直方图$H=\{H_1, H_2, \cdots, H_n\}$时，通过为每个直方图加入Lap$(1/\varepsilon)$的噪声量，最终的查询误差边界为$O(n/\varepsilon^3)$。

拉普拉斯机制往往适用于数值型数据查询与发布。对于非数值型查询（例如输出结果是一组离散数据$R=\{R_1, R_2, \cdots, R_n\}$），则可以采用指数机制添加噪声。在指数机制作用下，设计人员制定评价函数$q(D, R_i)$，并以$\exp(\varepsilon q(D, R_i)/2\Delta q)$的概率返回离散数据集合中的任意元素$R_i$，从而实现$\varepsilon$-差分隐私要求。

（3）数据输出

在完成数据的噪声添加后，需要以某种形式将数据输出，为接收终端提供服务。除了前面提到的直方图发布外，根据不同的业务场景，噪声添加机制往往还有一些特殊设计，数据输出形式还包括各类查询服务（如极值查询、均值查询等）、数据挖掘、机器学习等。

3） 接收端

最终接收数据并进行分析的软硬件实体统称为接收端。常见的接收端包括个人电脑、智能手机以及执行大数据分析的服务器或超级计算机等。

3 差分隐私技术应用现状

目前，差分隐私在移动互联网领域受到了广泛认可，基于本地化差分隐私模型的数据采集、数据共享与数据分析已得到广泛应用。包括谷歌、苹果和微软在内的大型互联网公

司已将本地化差分隐私技术部署在相关落地产品中；Uber和火山引擎则在数据平台中采用中心化差分隐私技术保障用户隐私数据安全。

1）在智能终端使用本地化差分隐私技术保障用户隐私数据安全

苹果、华为、小米等大型科技互联网公司已将本地化差分隐私技术应用于智能终端数据采集过程中，在用户隐私数据上传服务器前使用差分隐私算法进行加噪处理，确保用户的原始数据仅保存在智能终端中，从而保障用户隐私数据安全。

2016年6月，苹果公司将本地化差分隐私技术应用于用户最喜爱表情分析、QuickType输入建议、搜索提示等场景中，在智能终端对用户的输入表情数据、输入文字、搜索历史使用本地化差分隐私技术进行加密处理，并上传至苹果服务器，用于计算用户群体的行为模式。

2019年，华为公司将本地化差分隐私技术应用到华为音乐的“统计分析场景”。华为音乐APP利用差分隐私技术，在用户终端应用本地化差分隐私进行加噪处理，上传经差分隐私算法处理后的数据至云服务器进行统计分析。原始数据保存在用户终端，无须上传至云服务器，从而保护个人隐私。

2020年4月，小米公司在MIUI系统中使用本地化差分隐私技术，在用户的原始数据上传至服务器之前添加干扰噪声，确保不将用户真实数据上传服务器。2020年12月，小米再次将本地化差分隐私技术应用到“模糊定位”功能中，对用户的位置信息在本地进行差分隐私处理，确保手机应用无法获取用户的准确位置，从而保护用户隐私。

2023年，苹果公司在iOS 17及后续系统中，进一步将本地化差分隐私扩展至健康数据趋势分析、日记应用（Journal）推荐等场景，持续强化端侧隐私保护。

2024年，谷歌在安卓15中优化了差分隐私在广告归因和用户体验改进计划中的实现，确保用户交互数据在设备端完成扰动后再上传。

2）在数据平台采用中心化差分隐私技术保障用户隐私数据安全

2017年，Uber发布了差分隐私工具。该工具将中心化差分隐私机制嵌入数据平台的数据查询流程中，通过在原始查询结果中添加噪声，使返回的最终数据满足差分隐私要求。使用该平台查询结果的数据分析师无法获取用户的原始数据，从而确保在数据挖掘过程中不会泄露用户隐私数据。

2022年，火山引擎推出了基于中心化差分隐私技术的数据隐私查询服务（DPSQL）。DPSQL服务同样采用中心化差分隐私技术，以返回带有噪声的查询结果。目前，火山引擎的客户数据平台已接入DPSQL服务，为各行业客户提供具备差分隐私保护的用户群体洞察服务。

2023—2024年，微软在Azure Data Explorer中集成了差分隐私查询功能，为企业级数据分析提供内置的隐私保障；亚马逊云科技（AWS）也在其数据协作服务Clean Rooms中增强了差分隐私能力，支持多方数据在不泄露原始信息的前提下进行联合分析。

3）向开发者提供开源差分隐私计算框架

部分大型科技公司已推出基于差分隐私技术的开源隐私计算框架，有效降低了开发者应用的技术门槛，助力差分隐私技术应用于人工智能（AI）、数据分析等领域，解决用户隐私数据保护痛点。

2019年9月，谷歌推出了基于C++、Java和Go的差分隐私库开源版本，供开发者免费使用。2022年，谷歌与OpenMined合作，为开发者提供了基于Python的差分隐私库，帮助数以百万计的开发者快速将差分隐私技术应用于程序构建中，在保护用户隐私数据的基础上充分利用数据价值。

2022年，蚂蚁集团面向全球开发者正式开源可信隐私计算框架“隐语”，提供丰富的差分隐私机制，并将差分隐私与多方安全计算（MPC）、联邦学习技术相结合，实现全链路的计算隐私保护，已在医疗行业的联合诊断增强中进行探索性应用。

2023年，微软持续更新其开源差分隐私项目“Smart-Noise”，谷歌也迭代了DP库以适配PyTorch、TensorFlow等深度学习框架的最新版本，进一步降低了开发者在AI应用中集成差分隐私的门槛。

4）在生成式人工智能与大模型训练中的应用

2023年以来，随着大语言模型（LLM）的快速发展，训练数据泄露和模型记忆问题引发广泛关注。差分隐私随机梯度下降（DP-SGD）技术成为防止模型记忆敏感信息的关键路径。谷歌、Meta、微软等企业在模型预训练和对齐阶段引入差分隐私机制，有效防止了敏感个人信息被模型记忆和复现。

2024—2025年，OpenAI在定制化GPT模型中探索应用差分隐私以保护用户上传的专有数据；中国企业如百度、智谱AI等也在其大模型产品中集成差分隐私选项，为金融、政务等高敏感场景提供合规的AI服务。差分隐私与隐私计算技术的融合，正成为生成式AI时代数据安全与合规的重要基石。

4 差分隐私技术存在的问题与相关建议

差分隐私作为一种新兴的数据保护技术，在数据采集、发布和分析中具有一定的应用前景，同时也存在一些问题。

当使用差分隐私数据保护技术时，用户端容易遭受数据投毒攻击，例如伪造原始数据和伪造扰动数据等。该攻击通过设计原始采集数据或伪造针对性的扰动数据，并将其发送给数据采集者，从而影响接收端的数据统计分析结果。针对这一问题，可以在数据采集阶段使用虚假用户检测、聚类分析、异常值检测等技术手段防御投毒攻击；通过基于账号节点特征的方式，识别数据采集节点的异常行为并检测出潜在虚假用户；通过K-means算法生成正常数据与投毒数据的聚类集，并删除投毒数据聚类集，以确保采集数据正常使用。此外，还可以通过比较正常数据和采集数据的标准差来进行异常值检测。

当接收端对高维数据进行分析时，高维数据分析要达到低维数据分析的同等性能，所需数据量会呈几何级增长，因而会面临因统计分析而引起的维度灾难问题。差分隐私数据保护框架中各个组成部分（如汇聚网络、数据管理器）的通信代价随着数据维度的增加呈线性增长或指数增长。为了减少计算开销和通信代价，可以在数据预处理阶段采用PriV - iew机制，将高维数据分解为低维视图，对数据进行降维操作，以缓解该问题。

未来需要进一步完善差分隐私算法和技术，以适应数据隐私保护不断变化和升级的需求。

参考文献

[1] 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

[2] Dwork C. Diferentialprivacy [EB/OL]. [2026-08-05]. https://dl.acm.org/doi/10.1007/11787006_1

[3] Bugliesi M, Preneel B, Sassone V, et al. Automata，languages and programming [EB/OL]. [2026-08-03]. http://link. springer. com/book/10.1007/11786986

[4] Dwork C, Lei J. Differential privacy and robust statistics [EB/OL]. [2026-08-03]. http://dl.acm.org/doi/10.1145/1536414.1536466

[5] Kasiviswanathan S P, Lee H K, Nissim K, et al. What can we learn privately? [C]//Proceedings of 49th Annual IEEE Symposium on Foundations of Computer Science. IEEE, 2008: 531-540. DOI: 10.1109/focs.2008.27

[6] Duchi J C, Jordan M I, Wainwright M J. Local privacy and statistical minimax rates [C]//Proceedings of IEEE 54th Annual Symposium on Foundations of Computer Science. IEEE, 2013: 429-438. DOI: 10.1109/focs.2013.53

作 者 简 介



王宇，山东省烟台市大数据中心副主任，正高级工程师；主要从事政务信息化项目规划建设、大数据应用分析和人工智能创新应用等工作；参与和承担市级重点信息化项目7个，所主持项目先后荣获2022年度新型智慧城市扩面打榜优秀案例、2023年山东省地理空间数据十大应用创新案例和第三届（2022—2023）中国城市治理创新优秀案例等荣誉；发表论文2篇，拥有著作权1项。



由永桥，山东省烟台市大数据中心部长，正高级工程师；主要从事政务信息化项目规划、设计、实施，大数据应用分析和大模型创新应用等工作；参与和承担国家及省市信息化建设项目27个，主持或参与地方标准制订7项；发表论文6篇，出版专著3部，拥有著作权11项。



袁琦，中国信息通信研究院正高级工程师、主任；长期从事移动互联网、物联网及安全技术领域的科研专项、标准、软科学和测试研究工作；主持或参与国家级或省部级科研专项20余项，主持或参与制定国家或通信行业标准100余项；获得省部级奖励9项；发表论文40篇，参与编著书籍3部，拥有授权专利7项。



田琛，中国信息通信研究院高级工程师；主要研究方向为智能终端安全、AI安全、隐私保护、区块链等；主持及参与国家级及企业科研项目等20余项。



安媛媛，中国信息通信研究院工程师；长期从事移动终端安全与数据安全研究，主要研究方向包括终端系统安全、应用安全、数据合规与隐私保护、安全测评与标准研究。



孙良友，烟台海颐软件股份有限公司高级工程师；主要从事企业级应用开发平台、微服务与云原生等领域的技术研发与技术管理工作；参与和承担信息化建设项目10个、研发项目16个，主持或参与团体标准制订1项；所负责项目先后荣获市级奖项1项；发表论文3篇，获授权发明专利3项。