前　言

随着大数据、云计算和物联网技术的蓬勃发展，人工智能已广泛渗透到科学研究、数字经济、健康与医疗卫生等各大领域，给人类生产生活带来了极大的便利. 机器学习的模型训练和推理预测都依赖于大规模数据集，而这些数据中可能包含着用户的敏感或隐私信息. 针对人工智能中日益加剧的数据安全与隐私保护需求，国内外学者获得了一系列重要研究成果. 然而，如何在保护用户数据安全的同时，实现人工智能技术的高可用性和高效性仍然是学术界和工业界广泛关注的具有挑战性的研究课题.

为进一步推动我国学者在数据安全与智能隐私保护领域的研究，及时报道我国学者在数据安全与智能隐私保护方面的最新研究成果，我们组织策划了“数据安全与智能隐私保护研究”专题. 本专题通过公开征文共收到 2 篇特邀投稿和 78 篇普通投稿，论文分别从多个方面阐述了数据安全理论基础与应用及智能隐私保护关键支撑技术研究领域具有重要意义的研究成果. 本专题的审稿严格按照《计算机研究与发展》期刊的审稿要求进行，特邀编委先后邀请了近百位相关领域的专家参与评审，每篇论文邀请至少 3～4 位专家进行评审，历经初审、复审、终审等阶段，整个流程历经一个半月，最终共录用文章 20 篇（含 2 篇特邀稿件）. 这 20 篇文章分别涵盖数据安全、智能隐私保护等研究内容，在一定程度上反映了当前国内各单位在数据安全与智能隐私保护领域的主要研究方向. 由于刊物单期容量所限，本专题将刊登在 2022 年第 10 期（16 篇）和第 11 期（4 篇）.

1　综　　述

本部分共收录了 4 篇综述.

在万物互联的智能时代下，以深度学习为代表的人工智能技术正全方位改变人类的生产和生活方式. 与此同时，云边端计算架构的成熟和发展使得边缘计算正在日益走向智能时代的舞台中央，轻量化模型在计算资源受限的嵌入式和物联网设备大规模部署和运行. 虽然人工智能技术日益流行，但算法的鲁棒脆弱性及易受对抗攻击等特点也给人工智能系统的广泛应用带来了极大的安全隐患. 针对此问题，国内外学术界和工业界已经开展了人工智能安全的相关研究，其中针对深度学习的对抗攻御研究已成为了当前的热点研究. 李前等人的综述文章“云边端全场景下深度学习模型对抗攻击和防御”一文聚焦于云边端全场景下的人工智能技术安全问题，分别整理归纳了针对大型网络和轻量化网络的对抗攻防御技术，对相关理论与研究方法进行了系统性的综述研究. 首先，论文介绍了几类主流的对抗攻击生成方法. 其次，论文从鲁棒先验视角出发，将现有对抗防御工作分为基于对抗训练的防御、基于正则化的防御、基于对抗样本检测和去噪的防御以及基于模型结构的防御四大类. 论文对现有的研究工作进行了系统总结和科学归纳，分析了当前研究的优势和不足. 最后，论文探讨了在云边端全场景下深度学习模型对抗

攻击和防御研究当前所面临的挑战以及未来潜在的研究方向.论文旨在为后续深度学习模型对抗鲁棒性领域的研究者提供帮助,并进一步推动该领域的研究和发展.

随着全球数字化进程逐渐加快,数据已经成为当今社会重要的生产要素.数据的流动为社会创造了无穷的价值,但也潜藏着巨大的隐私风险.随着欧盟通用数据保护条例(GDPR)的出台,个人数据安全成为了大数据时代下的敏感话题,也越来越受到研究人员的重视.赵景欣等人的综述文章“基于通用数据保护条例的数据隐私安全综述”一文对数据隐私安全发展历程进行了回顾,介绍了欧盟数据保护条例GDPR及其应用领域和影响.归纳分析了近几年国内外相关研究文献,将GDPR合规问题划分为3个方面:GDPR违规行为分析、隐私政策分析、GDPR模型框架,并分析了这3个方面的研究现状.总结分析了基于GDPR的数据技术,包括数据保护影响评估、数据分类分级和数据跨境流动3个方面,并分别探讨了GDPR在区块链、物联网等具体领域的应用.最后,根据对现有研究工作存在的不足与问题,指出了基于GDPR的数据隐私安全研究面临的主要挑战和机遇,并针对中国数据隐私保护提出了5点启示.

近年来,以深度学习为代表的人工智能技术在金融安防、自动驾驶、医疗诊断等领域取得了较为成功地应用.然而,图像分类作为上述应用中的一项基础视觉任务,正接受着对抗攻击等技术手段带来的巨大安全隐患.提高深度学习模型抵御对抗攻击的能力(即对抗鲁棒性)成为有效缓解该问题的可行技术途径.为了科学、全面地提升深度学习模型的对抗鲁棒性,众多学者从基准评估和指标评估2个角度围绕对抗鲁棒性评估开展了大量研究.李自拓等人的综述文章“面向图像分类的对抗鲁棒性评估综述”一文着重对上述指标评估相关研究进行综述.首先,介绍对抗样本相关概念以及存在的原因,总结提出进行对抗鲁棒性评估时需要遵循的评估准则;其次,从被攻击模型和测试数据2个维度,重点梳理和对比分析现有的主要对抗鲁棒性评估指标;而后,分析总结现阶段主流的图像分类数据集和对抗攻防集成工具,为后续开展对抗鲁棒性评估奠定基础;最后,探讨当前研究的优势和不足,以及未来潜在的研究方向.

近年来物联网安全事件频发,物联网安全得到了广泛的关注,物联网访问控制作为物联网生态系统中重要的安全机制发挥着举足轻重的作用.但物联网架构复杂、设备多样且存储与计算性能较低,难以建立统一的访问控制体系,现有的互联网访问控制策略无法直接应用在物联网中.目前已经有研究人员提出了诸多物联网访问控制方案,但并未重视其中的安全性问题,由于物联网与人类生产生活息息相关,其访问控制一旦被打破,将造成隐私数据泄露、权限滥用等严重后果,亟需对物联网访问控制的安全性问题与解决方案进行综合研究.刘奇旭等人的综述文章“物联网访问控制安全性综述”一文根据物联网的特性,梳理了物联网访问控制中的信任关系,论述了信任链中的风险传递规律.并围绕信任链,从感知层、网络层、应用层分别综述了现有的访问控制攻击面,分析了存在的安全风险.针对这些安全风险,提出了应有的访问控制安全性要求,并总结了现有的安全性解决方案.论文在最后讨论了物联网访问控制设计中所面临的挑战,指出了未来的研究方向.

2 数据安全

本部分共收录了8篇论文，主要围绕区块链隐私保护、云安全审计、隐私集合求交、可搜索加密、差分隐私等研究方向展开.

在基于区块链的群智感知系统中构建数据真值估计机制和用户激励机制受到了越来越多的关注. 与传统的群智感知系统依赖一个集中平台来承载数据感知任务不同，该系统利用区块链分布式结构和操作透明不可抵赖的特性，使其具有更好的安全性和交互性. 但是目前的研究总是独立分离设计数据真值估计机制和参与者激励机制，这导致2类机制在实际应用时往往具有局限性. 应臣浩等人的文章“区块链群智感知中基于隐私数据真值估计的激励机制”一文在综合考虑了数据真值估计精确度与用户激励后，提出了一类基于隐私保护数据真值估计的用户激励机制. 该机制由2个模块组成，即具有隐私保护的数据真值估计模块PATD和具有隐私保护的用户激励模块PFPI，这2个模块都是通过利用同态加密机制CKKS来构建的. 论文进行了大量实验来验证所提的基于隐私保护数据真值估计的用户激励机制的各种特性. 实验结果表明，该机制与最新方法相比具有更好的性能.

支付通道网络作为区块链的扩容手段受到广泛关注. 然而，目前对支付通道网络的路由研究主要集中在路径连通性、通道利用率等方面，缺乏对节点信誉引起的路由安全风险及可能支付的高昂跨链服务中间手续费用影响小额支付发起者择路偏好的具体考量. 张谦等人的文章“多因素反向拍卖的跨链支付路由方案”一文定义了节点质量评价函数，包括节点手续费报价、网络距离和历史信誉，设计了多因素反向Vickrey拍卖(multi-factor reverse auction，MFRA)的路由方案，以实现跨链支付路由过程中基于候选中间节点质量的综合选择. 建立了候选节点的等价投标函数，用于将节点质量中的非价格属性因素转化为价格属性，并引入了以2为基数的指数机制实现对于等效投标价格的差分隐私，保障了参与节点的报价不被泄露. 安全性分析和性能评估表明，MFRA路由方案在降低节点手续费开销的同时，可以有效保障交易参与节点的报价隐私，实现快速高效的多跳跨链支付.

云存储提供数据托管服务，解决了本地端数据管理与分享受限问题. 但现有用于确保云存储数据完整性的审计方案面临一个重要的安全问题：签名密钥一旦泄露，依赖于该密钥产生签名的审计方案将无法提供完整性保护. 此外，现有审计方案均默认在整个审计期间仅有一个审计者，然而审计者可能由于被攻陷、被贿赂或资源不足不能再提供审计代理服务. 周磊等人的文章“支持密钥更新与审计者更换的云安全审计方案”一文提出一个支持密钥更新与审计者更换的审计方案AKUAR. 针对密钥暴露导致签名无效的问题，AKUAR结合双线性对与代理重签名思想设计了高效安全的密钥与标签更新机制，并且由云端承担计算复杂的标签更新操作，仅在本地端引入了少量的开销. 此外，当充当审计者的雾节点退出审计时，新的雾节点可以代替其继续进行完整性审计工作，在保证新签名密钥不被泄露给旧雾节点的同时实现了审计服务的可持续性. 安全分析

证明了AKUAR是安全的,性能评估也证实了AKUAR在标签生成与密钥更新阶段仅引入了少量可接受的计算开销与通信开销.

本地差分隐私具有不需要可信第三方、交互少、运行效率高等优点,近年来受到了广泛关注.然而,现有本地差分隐私集合数据频率估计机制未能考虑数据的隐私敏感度差异,将所有数据同等对待,这会对非敏感数据保护过强,导致估计结果准确度低.曹依然等人的文章“效用优化的本地差分隐私集合数据频率估计机制”一文定义了集合数据效用优化本地差分隐私(set-valued data utility-optimized local differential privacy,SULDP)模型,考虑了原始数据域同时包含敏感值和非敏感值的情况,在不减弱对敏感值保护的前提下,允许降低对非敏感值的保护.进一步,提出了符合SULDP模型5种频率估计机制suGRR,suGRR-Sample,suRAP,suRAP-Sample和suWheel,理论分析证实,相对于现有的本地差分隐私机制,所提方案能够对敏感数据实现完全相同的保护效果,并通过降低非敏感数据的保护效果,实现了频率估计结果的准确度提升.

整体结构是分组密码的重要特征,也是首要的研究对象,对于分组密码的轮数选取、软硬件实现性能都有非常大的影响.对于类AES算法的设计,当选用非最优分支数的矩阵作为列混淆操作时,向量置换(即字换位操作)的选择可有效提高整体结构的安全性.李晓丹等人的文章“uBlock类结构最优向量置换的高效搜索”一文通过研究uBlock类结构的特点及其扩散性,给出了其全扩散轮数的下界及等价类划分准则,提出了一种uBlock类结构最优向量置换的搜索策略.依据全扩散轮数最优、超级扩散层的分支数最优及uBlock类结构扩散层的特殊性质,证明了左右向量置换都不能是恒等变换,给出了uBlock类结构的一系列最优向量置换.该搜索策略大幅度减少了需要测试的置换对,为后续uBlock类算法的设计提供技术支持.

隐私集合交集(private set intersection,PSI)允许持有私有集合的参与方安全地获得集合的交集,而不会泄露除交集之外任何元素的信息.现有的两方/多方PSI协议大多基于不经意传输(oblivious transfer,OT)协议,具有很高计算效率的同时,也带来了巨大通信开销.在很多场景中,扩展网络带宽是非常昂贵甚至不可行的,而目前不依赖于OT设计且计算高效的多方PSI协议仍然较少.张蕾等人的文章“高效且恶意安全的三方小集合隐私交集计算协议”一文基于一轮密钥协商构造了三方参与的PSI计算协议,分别在半诚实模型和恶意安全性模型下,证明了协议的安全性且允许任意两方的合谋攻击.通过实验仿真,在大集合场景,相比现有基于OT的多方PSI协议,本协议具有最优的通信轮数且通信量降低了89%~98%;在小集合场景(500个元素或更少),相比适用弱通信网络的同类PSI协议,具有最优运行时间和通信负载,比依赖于同态加密的PSI协议快10~25倍.

基于混合整数线性规划(MILP)的自动化搜索方法被广泛用于搜索密码算法的差分特征,已形成一套完整的框架.该框架采用的基本原理是用线性不等式来刻画密码算法的各个操作,该框架适用于搜索采用4-bit S盒的密码算法的差分特征.对于采用8-bit S盒的密码算法,基于该框架的搜索模型计算量很大,以致无法高效地找到差分特征.

SM4 算法是 2006 年由中国政府发布，于 2012 年成为国家密码行业标准，于 2016 年成为国家标准的迭代分组密码算法，其分组状态为 128 比特，每轮包含 4 个 8-bit 的 S 盒. 为了高效地搜索 SM4 算法的差分特征，潘印雪等人的文章“基于 MILP 寻找 SM4 算法的差分特征”一文研究了对 8-bit S 盒进行 MILP 建模的问题，对于采用 8-bit S 盒的密码算法，改进了搜索高概率差分特征的方法. 对于 19 轮 SM4 算法，不仅找到了概率为 2^{-124} 的差分特征，而且找到了概率为 2^{-123} 的差分特征，这是目前基于 MILP 建模找到的 SM4 算法轮数最多、概率最高的差分特征.

近年来，满足前后向安全的动态对称可搜索加密（dynamic symmetric searchable encryption，DSSE）一直备受关注，它可以抵抗文件注入攻击，同时限制服务器学习已删除文档的相关信息. 不过大多数满足前后向安全的 DSSE 方案仅支持单关键词搜索，Patranabis 等人在 NDSS 2021 会议上提出了一种支持联合搜索且满足前后向安全的动态可搜索加密方案，但该方案在某些情况下不能得到准确的查询结果，同时不能支持多用户查询. 针对以上问题，张蓝蓝等人的文章“一种支持联合搜索的多用户动态对称可搜索加密方案”一文改进了不经意交叉索引（oblivious cross tags，OXT）协议，提出了一种支持联合搜索的多用户动态对称可搜索加密方案. 该方案利用有限域中元素具有乘法逆元的性质，引入了一次性盲因子，并结合数字信封技术实现了多客户端查询的功能. 方案分析与实验表明，论文所提方案满足了前向安全与后向安全，不仅可以提供准确的联合查询功能，而且支持多客户端查询，同时计算效率仅与更新次数最低的关键词更新次数有关.

3 智能隐私保护

本部分共收录了 8 篇论文，主要围绕隐私保护机器学习、智能网络入侵检测、联邦学习、深度学习等研究方向展开.

开放网络下分布式深度学习的兴起带来潜在数据泄露风险. 作为分布式模型构建中的重要信息载体，训练梯度是模型和端侧数据共同计算的产物，包含参与计算的私密用户数据信息. 因此，近年的研究工作针对训练梯度提出一系列新型攻击方法，尤以数据重建攻击（data reconstruction attack）所造成的攻击效果为最. 然而，已有数据重建攻击大多仅停留在攻击方法设计和实验验证层面，对重要实验现象缺乏深层机理分析. 尽管有研究发现，满足特定神经元激活独占性（exclusivity）条件的任意大小训练数据批次能被攻击者从训练梯度中像素级重建，然而，潘旭东等人的文章“基于神经元激活模式控制的深度学习训练数据泄露诱导”一文实证研究表明在实际训练数据中满足该条件的训练数据批次比例较少，难以造成实际泄露威胁，并提出基于线性规划的神经元激活模式控制算法，为给定训练批次生成微小扰动，从而满足神经元激活独占性，以增强后续数据重建攻击效能. 在实际中，通过在端侧节点部署该算法，半诚实（honest-but-curious）分布式训练服务能诱导本地训练批次的训练梯度具有理论保证的可重建性. 在 5 个涵盖人脸识别、智能诊断的数据集上的实验结果表明，提出方法在与原始攻击算法

重建效果持平的情况下，将可重建训练批次大小从 8 张提升至实际应用大小，并提升攻击效率 10 倍以上.

近几年数据安全和隐私泄露事件不断增加，使得目前的机器学习面临着严重的隐私泄露问题，结合密码学工具设计高效的隐私保护机器学习方案成为广受关注的研究领域. 目前相关的 Trident 和 Swift 方案中，前者为了提高方案的在线阶段的效率，需要额外引入一个诚实参与方，但当参与方中存在恶意行为时协议就会中止，用户就会得不到任何的输出，不适用于外包环境. 后者提出的方案可以选出一个诚实方作为可信第三方继续进行计算，保证协议一定有输出结果，但是所有的参与方都会将自己的信息发送给该参与方，这样该参与方将会拥有所有用户的敏感数据. 阎允雪等人的文章“基于秘密分享的高效隐私保护四方机器学习方案”一文设计了基于秘密分享的隐私保护四方机器学习的高效协议，方案中的 4 个参与方基于诚实大多数的原则，不需要额外引入一个诚实方. 在协议的执行过程中会选择出 2 个参与方作为可信的参与方，并将计算任务委托给它们来实现，不仅能够更好地保护用户隐私，而且保证协议有正确的输出. 通过实验分析本文提出的方案具备一定的实用性和可行性.

人工智能已被广泛应用于网络入侵检测系统，由于流量样本存在概念漂移现象，系统模型必须频繁更新以适应新的特征分布，更新后模型的有效性依赖新增训练样本的质量. 然而目前流量样本的污染过滤工作仍依赖专家经验，这导致在模型更新过程中存在样本筛选工作量大、模型准确率不稳定、系统易受投毒攻击等问题. 现有工作无法在保证模型性能的同时实现污染过滤或模型修复，为解决上述问题，刘广睿等人的文章“基于边缘样本的智能网络入侵检测系统数据污染防御方法”一文为智能网络入侵检测系统设计了一套支持污染数据过滤的通用模型更新方法. 其中，所设计的 EdgeGAN 算法利用模糊测试使生成对抗网络快速拟合模型边缘样本分布，并通过检查新增训练样本与原模型的 MSE 值，识别出误差样本子集，保证模型平稳更新；通过检查新模型对旧边缘样本的 F_β 分数，识别出中毒样本子集，保证分类边界不因投毒偏斜；通过让模型学习恶意边缘样本，抑制投毒样本对模型的影响，保证模型在中毒后快速复原. 在 5 种典型智能网络入侵检测系统上进行实验测试，对比现有最先进的算法，该方法对投毒样本的检测率平均提升 12.50%，对中毒模型的修复效果平均提升 6.38%.

完整性度量框架是可信计算平台的重要组成部分之一，之前研究工作所提出的完整性度量框架设计在实际应用于嵌入式设备场景时，往往体现出不同程度的局限性. 贾巧雯等人的文章“一种嵌入式 Linux 系统上的新型完整性度量架构”一文提出了 DIMAK，一种针对嵌入式 Linux 操作系统的实用化完整性度量架构，以期为基于 Linux 的嵌入式设备提供有效且高性能的运行时完整性验证能力. 该架构支持对映射至系统内核空间及用户进程的可执行文本、静态数据以及动态链接信息等关键内容实施即时（Just-In-Time）完整性校验. 利用 Linux 内核的进程/内存/页面管理机制，DIMAK 实现了对被度量内容所驻留物理页面的运行时校验，避免了基于文件的静态度量方法可能存在的检查与使用时差（time-of-check to time-of-use，TOCTTOU）漏洞. 通过首次引入对位置

无关代码的重定位/动态链接信息的完整性基线预测方法，DIMAK 在面对包括基于 hooking 的控制流劫持、恶意代码运行时载入等攻击威胁时具有较之现存同类技术更强的完备性. 另外，通过引入对软件热补丁功能的可信验证支持，DIMAK 在系统完整性度量问题中将该应用场景与恶意攻击行为正确地加以区分. 根据各种被度量实体的不同类型，DIMAK 在离线阶段、系统启动时、进程加载时和代码动态加载时等时机分别为生成其对应的完整性基线，确保其完整性验证行为的正确性. 真机测试显示，DIMAK 架构所产生的性能开销完全可以满足嵌入式设备场景下的实际应用要求.

随着企业、政府以及私人等图像数据资产的不断增加，机器学习领域对于图像等分类应用需求也随之不断增涨. 为了应对各种实际的需求，机器学习即服务（machine learning as a service，MLAAS）的云服务部署思想逐渐成为主流. 然而，基于云服务实现的应用往往会带来严重的数据隐私安全问题，金歌等人的文章“FPCBC：基于众包聚合的联邦学习隐私保护分类系统”一文将分类任务众包给多个边缘参与方并借助云计算来完成，不过我们不再使用联合训练理想模型的方式来得到可信度高的分类结果，而是让参与方先根据本地有限数据训练出的模型进行推理，然后我们再使用成熟的算法对推理结果聚合得到较高准确率的分类. 重要的是，我们保证了数据查询方不会泄露任何隐私数据，很好地解决了传统 MLAAS 的隐私安全问题. 在系统实现中，我们使用同态加密来对需要进行机器学习推理的图像数据进行加密；改善了一种众包的联邦学习分类算法，并通过引入双服务器机制来实现整个系统的隐私保护计算. 通过实验和性能分析表明了该系统的可行性，且隐私保护的安全程度得到了显著提升.

深度学习技术的快速发展给我们带来了极大的便利，但同时也导致大量隐私数据的泄露. 联邦学习允许客户端在只共享梯度的情况下联合训练模型，这看似解决了隐私泄露问题，但研究表明联邦学习框架中传输的梯度依然会导致隐私信息泄露. 并且，联邦学习的高通信代价的特点难以适用于资源受限的环境. 为此，陈律君等人的文章“基于秘密共享和压缩感知的通信高效联邦学习”一文提出了 2 个通信高效且安全的联邦学习算法，算法使用 Top-K 稀疏及压缩感知等技术以减少梯度传输造成的通信开销，另外利用安全多方计算中的加法秘密共享对重要的梯度测量值加密，以实现在减少通信开销的同时进一步增强其安全性. 2 个算法的主要区别是客户端与服务器通信时传递的分别为梯度测量值与梯度测量值的量化结果. 在 MNIST 及 Fashion-MNIST 数据集上的实验表明，与其他算法相比，论文所提的算法在保证通信代价较低的情况下进一步增加了安全性，同时在模型准确性上也有较好的性能.

联邦学习通过用上传模型参数的方式取代了数据传输，降低了隐私泄露的风险. 传统的联邦学习方法通常基于客户端模型统一的假设，且为单层联邦学习. 然而，在云边端框架下，存在边缘和终端 2 层分布式框架，且终端节点因资源异构问题难以达成训练模型的统一. 钟正仪等人的文章“一种面向云边端系统的分层异构联邦学习方法”一文从云边端系统的隐私安全问题出发，结合联邦学习技术，设计了分层部署模型的联邦学习方案，考虑到终端节点资源异构性，通过在终端模型插入分支的方式，将大模型拆分

为不同复杂度的小模型适配不同客户端资源状态，从而实现分层异构联邦学习. 同时，考虑到终端存在大量无标签数据，论文提出了针对联邦框架的半监督学习方法，实现对无标签数据的有效利用. 以 MNIST 和 FashionMNIST 数据集为例进行了验证，实验结果表明，在有效避免隐私泄露的前提下，相比于其他学习方法，其提出的方法最大可提升 22%的模型准确率；在计算、通信、存储等资源开销上均有明显降低.

联邦学习作为一种分布式机器学习框架，可以有效保护各参与方的数据隐私. 然而，传统的联邦学习依赖一个中央服务器，模型训练过程易受单点故障和节点恶意攻击的影响；明文传递的中间参数也可能被用来推断出数据中的隐私信息，其在加强用户数据安全和隐私保护上受到越来越多的挑战. 此外，联邦学习没有提供合适的激励机制吸引更多的训练数据和计算资源. 为解决上述挑战，周炜等人的文章“基于区块链的隐私保护去中心化联邦学习模型”一文提出了一种基于区块链的去中心化、安全、公平的联邦学习模型，利用同态加密技术保护协同训练方的中间参数隐私，通过选举的联邦学习委员会进行模型聚合和协同解密. 解密过程通过秘密共享方案实现安全的密钥管理，并利用双线性映射累加器为秘密份额提供正确性验证. 模型还引入信誉值作为评估参与方可靠性的指标，利用主观逻辑模型实现不信任增强的信誉计算作为联邦学习委员会的选举依据，信誉值作为激励机制的参考还可以保障参与公平性. 模型信息和信誉值通过区块链实现数据的防篡改和不可抵赖. 实验表明，模型在训练精度相比中心化学习模型略有损失的情况下，能够保障在多方协作的环境下以去中心化的方式训练模型，有效实现了各参与方的隐私保护.

承蒙各位作者、审稿专家和编辑部等方面的全力支持，本专题得以顺利出版. 目前数据安全与智能隐私保护研究涉及领域十分广泛，这给审稿人及特邀编委的审稿、选稿工作带来了巨大挑战. 由于投稿数量大、主题广泛、时间安排紧张、专题容量有限等原因，本专题仅选择了部分有代表性的研究工作予以发表，无法全面体现该领域所有的最新研究工作. 部分优秀稿件无法列入专题发表，敬请谅解. 我们要特别感谢《计算机研究与发展》编委会和编辑部，从专题的立项到征稿启事的发布，从审稿专家的邀请到评审意见的汇总，以及最后的定稿、修改和出版工作，都凝聚了他们辛勤的汗水. 本专题的出版期望能给广大相关领域研究人员带来启发和帮助. 在审稿过程中难免出现不尽人意之处，希望各位作者和读者包容谅解，同时也请各位同行不吝批评指正. 最后，再次衷心感谢各位作者、审稿专家、特邀编委和编辑部的辛勤工作.

曹珍富 华东师范大学
徐秋亮 山东大学
张玉清 中国科学院大学
董晓蕾 华东师范大学

2022 年 9 月