大数据和人工智能时代数据安全风险及应对策略

蒋宗昊　陆　芸*
杭州云鹭科技有限公司　浙江杭州　310000

摘　要：随着大数据和人工智能技术的快速发展，数据安全问题日益突出，成为全球信息技术领域关注的焦点。大数据和人工智能技术不仅推动了各行业的创新发展，也使得数据安全面临前所未有的挑战。本文首先探讨了人工智能时代数据安全风险的内涵与特点，分析了数据泄露、篡改与破坏、以及数据决策风险等多种形式的安全威胁。通过对现有数据安全问题的深入分析，文章进一步探讨了针对这些风险的应对策略。具体来说，本文提出了加强数据加密技术、建立严格的数据访问控制机制、完善人工智能算法的透明度与可解释性等多项解决方案。此外，文章还探讨了政府和企业在应对数据安全风险方面的责任与义务，提出了合作与规范化的建议。最后，本文展望了在大数据与人工智能技术不断发展变化的背景下，如何通过持续创新与完善安全措施，确保数据的安全性与隐私保护，通过对这些问题的研究，本文希望为数据安全领域的学术研究与实际操作提供理论支持和实践指导。

关键词：大数据；人工智能时代；数据安全；风险

序言

随着这些技术的广泛应用，数据安全问题逐渐成为人们日益关注的焦点。无论是在企业内部的数据管理，还是在国家层面的信息治理中，数据安全的保障成为了不可忽视的课题。尤其是在人工智能的快速发展推动下，数据作为驱动AI技术的核心元素，面临着极大的安全风险。从大规模的数据泄露事件到复杂的数据篡改与破坏，再到AI系统决策中的潜在风险，数据安全威胁无处不在。本文通过分析人工智能时代数据安全风险的内涵、特点及表现形式，深入探讨了当前数据安全面临的主要威胁，并提出了一系列切实可行的应对策略，旨在为学术界、企业界以及政府部门提供有价值的参考与建议。

一、人工智能时代数据安全风险的内涵与特点

随着人工智能技术的快速发展，数据的生成、存储、处理和传输变得更加复杂和多样化[1]。在这一背景下，数据安全风险的内涵与特点也呈现出新的变化。首先，人工智能时代的数据安全风险具有高隐蔽性和复杂性。数据通过多种方式采集，并经过人工智能算法的处理，可能在未经授权的情况下被泄露或滥用[2]。随着AI技术的深入应用，黑客和攻击者可以利用同样的技术手段发起更加精准和隐蔽的攻击，人工智能时代的数据安全风险具有动态性、复合性、与技术高度融合的特点，这使得现有的数据安全管理方法面临严峻挑战[3]。

二、人工智能时代数据安全风险的表现形式

（一）数据泄露风险威胁

数据泄露是人工智能时代最为常见和危险的数据安全风险之一。随着大量敏感数据的生成和储存，尤其是在云计算和物联网等技术的推动下，数据泄露事件的发生频率显著上升[4]。黑客攻击、内部人员泄密、恶意软件等多种因素都可能导致数据的泄露。而在人工智能技术的应用中，数据泄露不仅仅局限于简单的个人信息泄露，还可能涉及到大量的商业机密、政府敏感数据、AI训练数据等[5]。近年来数据泄露事件的数量和规模持续攀升，数据泄露的形式也日益复杂，例如，通过高级持续性威胁（APT）攻击，攻击者可以潜伏在系统内部，长时间获取并传输数据，给企业和政府带来巨大的安全风险和经济损失。因此，防范数据泄露成为当前数据安全防护的首要任务，尤其是在涉及AI模型训练和数据分析时，如何确保数据的隐私性与安全性显得尤为重要。图1为数据泄露风险威胁类型。

作者简介：
蒋宗昊（1993.2-），男，汉族，浙江杭州人，本科，研究方向为大数据安全、人工智能。
陆芸（1979.12-），女，汉族，浙江杭州人，硕士研究生，研究方向为大数据和人工智能。

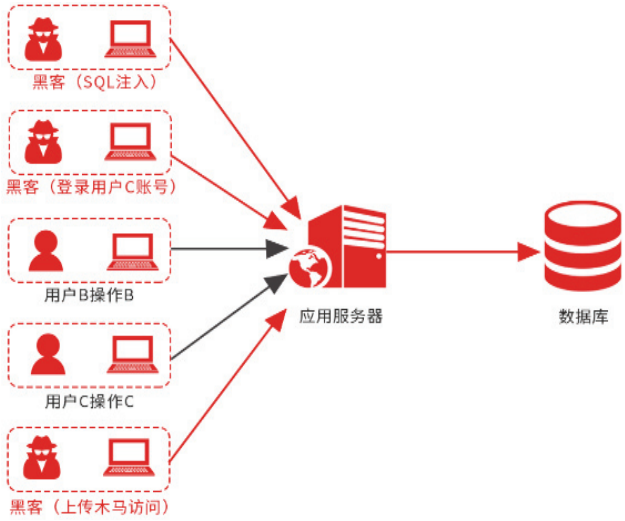

图1　数据泄露风险威胁

（二）数据投毒攻击

数据投毒是一种通过污染训练数据或利用反馈机制向人工智能模型注入错误信息的攻击方式，严重影响模型的有效性和可靠性，具体过程见图1。攻击者通常采用两种策略，一是模型偏斜，即在训练阶段向数据集中添加带有特殊标签的污染数据（如错误样本或伪装数据），导致模型学习到错误的分类边界，从而在推理时做出错误判断；二是反馈误导，即利用模型的反馈机制，在运行过程中注入伪造的数据或错误信息，干扰模型的持续学习过程，使模型逐渐偏离正确方向。这些攻击方式尤其对自动驾驶系统构成极大的安全隐患。例如，攻击者可以通过向训练数据集中添加伪造的交通标志或异常行为数据，使自动驾驶算法在实际路况下识别错误，从而违反交通规则或引发交通事故。此外，由于模型偏斜会改变模型的分类边界，导致其对正常数据的判断产生错误，进而影响系统的稳定性。面对数据投毒带来的威胁，加强对训练数据的安全检测和反馈机制的安全审查是保障人工智能系统安全的关键。

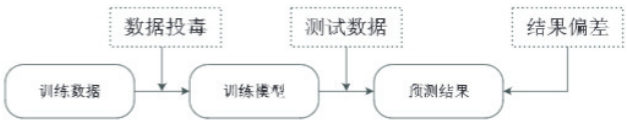

图2　数据投毒

（三）数据决策风险

数据决策风险是指由于人工智能系统在处理和分析数据时，可能因为算法的偏差、数据的质量问题或外部干扰因素，导致错误的决策或不公正的结果。例如，人工智能在招聘领域的应用可能因历史数据的偏差而导致性别、种族等方面的歧视；在金融领域，AI算法可能因数据不完整或处理不当而做出错误的投资建议。数据决策风险的产生与人工智能算法本身的设计密切相关，若算法缺乏透明性、可解释性，或者数据来源存在问题，都会影响决策的公正性和准确性。因此，在应用人工智能进行数据决策时，必须确保数据质量的可靠性和算法的公平性，以减少潜在的决策风险。

三、数据安全风险产生的原因

（一）人工智能算法的局限性

人工智能算法在数据处理和自动化决策方面发挥着重要作用，但其固有的局限性使数据安全风险难以避免。首先，AI算法依赖于大规模数据集进行训练，但数据集的质量、完整性和多样性直接影响模型的性能。数据偏差和数据污染会导致训练结果失真，导致模型输出具有偏见或错误判断。其次，深度学习模型的“黑箱”特性使其决策过程难以解释，导致出现错误时难以追溯原因和纠正。此外，人工智能模型易受对抗性攻击的威胁，攻击者可以通过微小的扰动来欺骗模型，使其作出错误判断。最后，模型更新和版本迭代可能引入新的漏洞，若未及时发现并修补，将会加剧数据安全风险。因此，在技术层面，人工智能算法的局限性成为数据安全风险的核心诱因，需要采取措施增强模型的鲁棒性和安全性。

（二）数据安全治理体系不完善

数据安全治理体系的不完善是人工智能时代数据安全风险的重要诱因。首先，数据安全管理制度滞后于技术发展，数据采集、存储、传输、使用等环节缺乏全流程风险管控机制，导致数据泄露和滥用现象频发。其次，企业和机构对数据安全责任认识不足，数据安全意识薄弱，未能形成完善的数据安全管理文化。再者，跨部门数据协作和共享过程中缺乏数据访问控制与权限管理，增加了数据泄露的风险。此外，数据安全审计机制不健全，对数据使用过程中的违规行为难以及时发现和追责。最后，缺乏应急响应机制，一旦发生数据安全事件，往往难以及时处置并有效控制损失。因此，建立完善的数据安全治理体系，强化数据安全管理能力，是应对数据安全风险的关键。

（三）相关法规制度滞后

在法律层面，相关法规制度的滞后性使数据安全风险不断加剧。首先，现有的数据安全法律法规尚未充分覆盖大数据和人工智能应用带来的新风险，数据采集、使用、共享和跨境传输等环节存在法律空白。其次，针

对人工智能模型训练过程中数据合规性的监管措施尚不完善，对数据来源的合法性和用户隐私保护的监管不到位。再者，数据安全事故发生后的法律追责机制不健全，导致违法成本过低，难以形成有效的震慑作用。此外，跨国数据流动的法律协调机制缺失，数据跨境流动中的隐私保护和数据主权面临法律冲突的挑战。因此，当前的法律法规体系已难以应对大数据和人工智能技术引发的复杂数据安全问题，亟需完善法律框架，加强数据安全监管力度。

四、应对人工智能时代数据安全风险的对策建议

（一）加强关键技术研发，提升数据安全保障能力

面对人工智能时代的数据安全挑战，加强关键技术研发是提升数据安全保障能力的关键。首先，要加快发展隐私保护计算技术，如联邦学习、差分隐私和同态加密等，确保数据在使用过程中不泄露原始信息。其次，增强对抗性样本检测和防御技术，提升人工智能系统的鲁棒性，降低模型被攻击的风险。此外，要开发具备透明性和可解释性的AI模型，使人工智能决策过程透明可追溯，有助于及时发现和纠正潜在风险。同时，研究数据水印、溯源技术，实现数据来源可追踪，防止数据被篡改或滥用。最后，通过不断加强技术创新，提升大规模数据存储、传输、分析过程中安全防护能力，建立完善的数据安全技术防护体系。

（二）健全数据安全管理制度，完善治理体系

健全数据安全管理制度，完善数据安全治理体系是防范数据安全风险的基础。首先，要建立数据安全全生命周期管理机制，覆盖数据采集、存储、使用、传输和销毁等各个环节。其次，加强数据分级分类管理，根据数据的重要性和敏感性实施差异化的安全保护措施。再者，明确数据安全责任，建立数据安全问责机制，强化企业和机构的主体责任。此外，要完善数据访问控制和权限管理机制，防止数据滥用和未授权访问。还需加强数据安全风险评估和审计机制，及时发现和防范潜在风险。通过构建全面的数据安全治理体系，可有效提升数据安全管理水平，降低数据安全风险。

（三）制定专门法律法规，规范人工智能数据应用

为应对人工智能时代的数据安全风险，必须制定专门的法律法规，规范数据应用，通过完善数据安全法律体系，对大数据采集、存储、使用、共享和跨境流动等环节进行明确规定。通过建立数据合规审查机制，确保数据采集与使用符合法律法规要求，强化用户隐私保护。再者，要设立AI系统安全审核标准，明确算法透明性、数据安全性和伦理规范，防止算法滥用和数据歧视。此外，完善数据安全事故的法律追责机制，提高违法成本，形成有效的法律震慑。最后，强化跨国数据流动法律协同机制，平衡数据安全与数据自由流动的关系，为国际数据流动建立统一的法律标准。通过制定全面的数据安全法规体系，可为人工智能的安全发展提供法律保障。

结语

综上所述，随着大数据和人工智能技术的广泛应用，数据安全风险已成为不可忽视的挑战。技术层面的算法局限性、管理层面的数据安全治理缺失以及法律层面的法规滞后，共同导致了数据安全风险的日益加剧。为有效应对这些风险，必须采取多维度的应对措施。通过加强关键技术研发，提升数据安全保障能力，可以有效增强系统的防御能力；健全数据安全管理制度，完善治理体系，有助于提升全流程数据安全管控水平；制定专门法律法规，规范人工智能数据应用，为数据安全提供法律保障。只有从技术、管理、法律三方面协同发力，才能有效化解大数据和人工智能时代的数据安全风险，促进数据要素安全、高效、合规地流通，为人工智能技术的持续发展保驾护航。

参考文献

[1]方艳梅.深度伪造对人脸识别支付系统安全性的挑战与应对[J].金融科技时代，2020，28（3）：5.

[2]纪守领，杜天宇，李进锋，等.机器学习模型安全与隐私研究综述[J].软件学报，2021，32（1）：41-67.

[3]杨洗.数字媒体时代的数据滥用：成因、影响与对策[J].中国出版，2020（12）：3-8.

[4]刘金瑞.数据安全范式革新及其立法展开[J].环球法律评论，2021，43（1）：5-21.

[5]苗杰.人脸识别“易破解”面临的风险挑战及监管研究[J].信息安全研究，2021，7（10）：984-988.