基于人工智能的数据泄露预测与防御机制探索

徐世权[1]，方明星[2]，陈敏时[1]，宋刚[3]，高桐[3]
1. 中国移动通信集团有限公司，北京 100033
2. 中国移动通信集团设计院有限公司，北京 100080
3. 中国移动通信集团黑龙江有限公司，黑龙江 哈尔滨 150000
DOI: 10.61369/TACS.2025070042

摘　　要： 当前，已经步入数字时代，在数字化浪潮的席卷下，数据已经成为重要资产，在推动社会经济发展方面发挥着重要的作用。然而数据泄露、滥用等事件频发，给企业以及社会稳定发展带来了巨大损失。人工智能技术具备强大的数据收集和分析功能，能够为数据泄露预测与防御提供新的思路和方向。对此，本文围绕基于人工智能的数据泄露预测与预防机制进行深入分析，提出行之有效的建议和策略，旨在为构建更为科学、安全的数据保护体系提供一些有价值的借鉴和参考。
关 键 词： 人工智能；数据泄露预测；防御机制

Exploration of AI-Based Data Leakage Prediction and Defense Mechanisms

Xu Shiquan[1], Fang Mingxing[2], Chen Minshi[1], Song Gang[3], Gao Tong[3]
1. China Mobile Communications Group Co., Ltd., Beijing 100033
2. China Mobile Communications Group Design Institute Co., Ltd., Beijing 100080
3. China Mobile Communications Group Heilongjiang Co., Ltd., Harbin, Heilongjiang 150000

Abstract: At present, we have entered the digital age. Under the sweep of the digital wave, data has become an important asset and plays a crucial role in promoting social and economic development. However, incidents such as data leakage and abuse occur frequently, causing huge losses to enterprises and the stable development of society. Artificial intelligence (AI) technology possesses powerful data collection and analysis capabilities, which can provide new ideas and directions for data leakage prediction and defense.In this regard, this paper conducts an in-depth analysis around AI-based data leakage prediction and prevention mechanisms, and puts forward effective suggestions and strategies. The aim is to provide valuable references for building a more scientific and secure data protection system.
Keywords: artificial intelligence (AI); data leakage prediction; defense mechanisms

引言

在数字时代背景下，数据已经成为企业实现持续发展的核心资产[1]。然而，数据泄露事件呈现高发态势。造成数据泄露的原因有多种，比如说企业员工操作失误或恶意窃取、外部黑客攻击、恶意软件入侵等。数据泄露不仅会导致企业面临巨额的经济赔偿和监管处罚，同时还会大大削减其核心竞争力，损害其信誉，甚至可能会对国家的未来发展造成一定阻碍。因此，应重视数据安全防护体系的构建。

然而，传统的数据安全防护手段较为被动，主要以防火墙、入侵检测系统为主，主要以固定的规则和方式开展防御，这种防护手段难以应对新型的威胁。人工智能技术的出现，为数据泄露预测和防御提供了新的方向和思路。可以利用人工智能强大的数据分析和处理功能，自动识别异常行为，精准预测潜在的数据泄漏风险，并采取行之有效的防御举措，实现从被动防御向主动防御的转变。

一、人工智能在数据泄露预测中的应用

（一）用户行为分析预测

利用人工智能算法收集用户的行为数据，并以此为基础进行建模，是预测数据泄露的有效手段之一[3]。通过收集和分析员工在访问企业数据时行为数据，包括访问时间、访问频率、访问的数据类型等，构建每个用户或用户组的正常行为模式。例如，某企业通过分析员工的行为数据，发现该员工经常在上午的10点到11点间大量访问重要的财务数据，并且系统记录的访问数据较为稳定。然而，当某一员工突然在非工作时间大量下载重要的财务数据，系统会根据其行为偏离正常基线，从而自动发出预警提示，发现该员工存在恶意调取重要数据的嫌疑。除此之外，机器学习中的神经网络和聚类算法等技术也能够对用户的行为数据进行分析。神经网络能够处理较为复杂的行为模式，通过大量的数

据训练，能够不断提升预测的准确性。而聚类算法能够将具有相似行为特征的用户划分为一类，从而更为准确、有效地识别异常行为。

（二）网络流量深度分析预测

人工智能还能够对网络流量进行深度分析，异常的流量模式能够被精准识别，从而有效预测数据泄露的风险[4]。网络数据包具有丰富的特征信息，如目的地址、协议类型、流量大小等，深度学习算法能够对这些特殊信息进行全面分析，精准识别出隐藏在正常流量中的恶意数据传输，从而提升数据安全防护实效。除此之外，还能够根据威胁情报数据，运用人工智能技术对网络流量进行深入分析。通过收集来自全球的威胁情报数据，如最新的黑客攻击手段、恶意软件特征等，并将其与企业自身网络流量数据进行关联分析，从而及时发现潜藏的数据隐患。

（三）数据关联与趋势预测

通过关联分析不同数据源的数据，人工智能还能够精准预测数据泄露的未来趋势[5]。例如，收集和分析企业的相关数据，如内部数据访问记录、员工行为数据、外部网络威胁情报数据等，能够发现某些员工在访问相关数据后，企业外部出现了与该数据相关的异常网络活动，这很可能在一定程度上预示着数据泄漏风险的上升。除此之外，还可以利用时间序列分析等技术，预测数据泄露事件的发生趋势。通过深入分析历史数据泄露事件的时间分布规律，结合当前数据安全态势以及威胁情报，从而精准预测未来一段时间内可能会发生数据泄露的时间和概率，为企业提前采取有效措施，避免发生数据泄露提供重要参考。

二、人工智能在数据泄露防御中的应用

（一）动态访问控制防御

动态访问控制防御是一种基于人工智能技术的主动防御手段，可以对用户的身份、行为、环境等多种数据进行分析，并根据实时的风险评估结果，动态调整用户的访问权限，从而降低发生数据泄露的风险[6]。在以往，访问控制主要基于用户的身份和角色进行授权，缺乏对用户行为、环境等数据的分析。而人工智能技术能够对用户的行为数据、环境数据等进行实时监测，一旦发现用户的登录地点、登录设备、访问时间等发生改变，并试图访问重要、敏感的数据时，系统会主动要求额外核实用户的身份信息，比如说短信验证码、面部识别等，一旦检测存在异常或存在潜在威胁，动态访问控制系统将会自动触发权限调整机制。除此之外，动态访问控制系统还能够与企业的身份管理系统深入融合，从而实现对企业员工的精细化管理[7]。

（二）智能加密与脱敏防御

智能加密与脱敏防御也是一种基于人工智能技术的重要数据防护手段。智能加密技术主要是通过对敏感、重要的数据进行加密处理，能够有效防止数据在传输、存储过程中被非法窃取或篡改。此外，该技术还能够根据数据的类型、用途以及访问者的身份，动态选择加密手段和密钥长度，这样做不仅能够显著提升数据的安全性，同时还能够提升数据安全防护工作效率。除此之外，脱敏防御技术能够确保在数据共享或测试环境中，敏感数据不会被泄露。

（三）实时监测与响应防御

实时监测与响应防御也是一种基于人工智能技术的主动数据防护手段，能够对数据安全威胁进行快速识别和处理[8]。通过部署智能化监测系统，能够对企业的内部往来、员工行为数据以及其他流动数据进行全面、多维、实时监控，及时发现潜在的数据安全隐患。例如，当系统检测到企业某台设备突然出现异常的高频率数据外发行为时，会立即触发预警机制，并自动采取相关措施进行阻断。通过这样的方式，防止数据泄露事件的发生。除此之外，该防御机制还能够利用机器学习算法，通过对历史数据的不断学习，从而不断提升自身的威胁识别能力和检测能力。在响应环节，人工智能技术可以根据提前设定的安全策略，快速生成解决方案，从而最大限度地减少安全事件造成的损失和影响。这种高效的检测和响应能力，不仅能够提升企业应对复杂网络安全的能力，同时也为推动数据安全防护体系建设奠基。

三、人工智能应用于数据泄露预测与防御面临的挑战及应对策略

（一）技术挑战及应对

1. 模型的准确性与可靠性

人工智能模型的准确性将会对数据泄露预测与防御的效果产生直接的影响[9]。然而，由于数据往往存在一定的复杂性和不确定性，这可能会对模型的准确性和可靠性造成一定影响，可能会使其产生错判或误判。因此，为了提升模型的准确性和可靠性，应不断优化算法模型，提高训练数据质量，并进行大量的测试和验证。

2. 对抗样本攻击

对抗样本攻击是一种针对人工智能模型的新型威胁，它通过精心设计的输入数据，从而诱导模型产生不正确的输出结果。对抗样本攻击能够使系统无法准确识别异常行为或潜藏数据风险，从而有效降低数据安全防护体系的防护效率。对此，为了应对这一威胁，可以从两方面着手。一方面，提升模型的鲁棒性。通过大量的对抗训练，增强模型对恶意样本的识别能力。另一方面，优化监测机制。可以引入多模型融合的检测方法，从而有效降低单一模型被攻击的风险。

（二）管理挑战及应对

1. 加强人员培训

人工智能技术的应用需要工作人员具备一定的专业素养和综合能力。然而，经过笔者实践调查发现，部分企业员工对人工智能技术缺乏深入了解，自身应用能力较为薄弱，安全意识不强，从而影响数据安全防护体系的构建。对此，企业应制定和完善关于员工人工智能技术的专项培训计划，全面革新他们的认知，培养其人工智能技术应用能力，使其成为符合企业发展需要的高质量人才。在培训内容方面，应构建系统化的课程体系，包括但不限于人工智能的基础理论讲解、核心技术原理剖析、典型应用场

景演示等基础模块；同时也要重点加强数据安全防护专业技能方面的培训，比如说访问控制机制、数据加密技术、异常行为检测等技能。除此之外，还应引入真实案例，并引导员工进行分析和研究，从而帮助他们更好地掌握人工智能工具的操作方法。在人员培训过程中，企业应格外关注员工数据安全防护意识的培养。可以通过模拟风险场景、典型案例分析等方式，促使员工能够准确识别日常工作中的相关数据安全隐患，并熟练采取相应对策进行处置。为了确保员工培训效果，企业还应构建完善的评估机制，定期组织员工参与实战演练、技能考核以及知识测试等活动，并从多个维度和层面对员工的数据安全防护素养进行评价，及时发现并弥补培训中的不足和缺陷。同时，还应构建培训效果跟踪机制，持续关注员工在实际工作中的知识运用情况，确保培训成果能够转化为工作能力，从而为企业构建数据安全防护体系、实现持续发展奠定坚实的人才基础。

2. 安全策略制定与执行

企业还应制定科学、完善的安全策略，明确人工智能在数据泄露预测与防御中的应用范围和规则。然而，部分企业在实际执行过程中，往往存在政策难以落地、执行不严格等问题。对此，企业应构建科学合理的安全管理体系。一方面，制定完善、详细的安全管理制度和操作规程，明确各个部门的职责范围。另一方面，还应构建常态化的监督检查机制。定期安排专业人员对安全策略的执行情况进行全面检查和科学评估。通过组织安全演练、开展专项审计以及建立检查台账等方式，及时发现安全策略执行过程中存在的问题，并采取行之有效的方式进行处理和改善。同时，要建立考核评价体系，将安全策略执行情况纳入绩效考核，以此确保各项安全管理制度真正落到实处，持续提升企业整体安全管理水平。

3. 跨部门协作与沟通

数据泄露预测与防御往往会涉及企业的多个部门，比如说财务部、业务部、安全部等。因此各个部门之间的相互沟通和协作就显得尤为重要。对此，企业应构建跨部门协作机制，加强各个部门之间的沟通和交流，通过这样的方式，有效减少部门之间的信息不通畅、协作不顺畅等问题，共同有效应对数据泄漏风险。

四、结束语

总之，在新时期，人工智能技术的飞速发展和广泛应用，为数据泄露预测与防御提供了强大的支撑。通过运用用户行为分析、数据关联与趋势预测等先进技术，能够精准预测数据泄露的风险；通过运用动态访问、智能加密与脱敏、实时监测与响应等防御策略，能够有效降低企业数据泄露事件的发生概率，提升企业数据安全水平。

参考文献

[1] 徐伟，韦红梅 . 生成式人工智能训练数据风险治理：欧盟经验及其启示 [J]. 现代情报 ,2025,45(05):89-98.

[2] 王梅艺 . 人工智能时代数据安全风险及应对策略 [J]. 中阿科技论坛 (中英文),2024,(11):139-143.

[3] 孙清白 . 论人工智能大模型训练数据风险治理的规范构建 [J]. 电子政务 ,2024,(12):41-52.DOI:10.16582/j.cnki.dzzw.2024.12.004.

[4] 王译，李嘉飞 . 嵌入与转型：人工智能赋能国家监察的系统逻辑与治理之策 [J]. 中共天津市委党校学报 ,2024,26(05):43-52.DOI:10.16029/j.cnki.1008-410X.2024.05.005.

[5] 马丽娅·哈则孜别克 . 人工智能时代下数据安全法律规范的探讨 [J]. 法制博览 ,2024,(25):15-18.

[6] 辜凌云 . 人工智能大模型开源面临的问题及数据保护 [N]. 民主与法制时报 ,2024-09-04(003).DOI:10.28579/n.cnki.nmzfz.2024.001614.

[7] 关伟东 . 国外人工智能数据安全规制及对我国的启示 [J]. 信息通信技术与政策 ,2024,50(08):68-72.

[8] 邓智超 . 人工智能时代保险消费者的数据风险及其应对 [J]. 上海保险 ,2024,(08):19-23.

[9] 沈怡然 .IBM:2024 年企业数据泄露成本创下新高 [N]. 经济观察报 ,2024-08-05(020).DOI:10.28421/n.cnki.njjgc.2024.000850.

[10] 蔡智权 . 生成式人工智能助力新质生产力的价值证成、技术隐忧与战略因应 [J]. 西南金融 ,2024,(07):89-102.

