人工智能辅助下的大数据政务信息安全风险识别与防范机制

王海伟　国　鹏　蔡明丽
政和科技股份有限公司　山东　济南　250000

摘　要：人工智能辅助下的大数据政务信息安全风险识别与防范机制，旨在通过先进的人工智能技术，实现对政务大数据的全面监控与智能分析。该机制利用深度学习、自然语言处理等算法，精准识别数据泄露、非法访问等潜在风险，并通过智能预警系统及时提醒管理人员。结合智能安全防护措施，有效阻断安全风险，确保政务信息的保密性、完整性和可用性。此机制的建立，不仅提升政务信息安全防护水平，也为智慧政府建设提供有力支撑。

关键词：人工智能；大数据政务信息；安全风险识别；防范机制

1 大数据政务信息安全简述

1.1 大数据政务的发展现状与趋势

随着互联网、大数据、人工智能等新一代信息技术的快速发展，以及信息化建设的不断深化，政府开始探索如何利用信息技术优化政务服务，提高公共服务的质量和效率。目前，我国大数据政务行业已经取得了显著的发展成果。各级政府纷纷推进政务服务平台建设，实现了政务服务事项的在线办理，提高了办事效率。政务数据共享和开放程度不断提高，为政府决策和社会治理提供了有力支持。人工智能、大数据等新技术在政务服务中的应用日益广泛，为公众提供了更加智能、便捷的服务体验。大数据政务在发展过程中也面临一些挑战，政务数据共享和开放程度仍有待提高，数据孤岛现象依然存在，影响了政务服务的整体效能。技术标准不统一和系统集成困难也是大数据政务面临的挑战之一。由于缺乏统一的政务技术标准，不同地区、不同部门之间在系统建设和数据接口上存在差异，导致系统集成困难，信息孤岛现象普遍，大数据政务人才短缺，制约了行业的发展。未来，随着政策支持力度加大和区域协调发展战略的实施，大数据政务有望取得进一步发展。云计算、大数据、人工智能等新技术将进一步融入政务服务，推动政务服务的创新和升级。

1.2 大数据政务信息安全的内涵与重要性

大数据政务信息安全的内涵主要包括几个方面：（1）从信息的层次看，大数据政务信息安全包括信息的完整性（保证信息的来源、去向、内容真实无误）、保密性（保证信息不会被非法泄露扩散）、不可否认性（保证信息的发送和接收者无法否认自己所做过的操作行为）等。这些特性确保了政务信息的真实性和可靠性，防止了信息的篡改和滥用[1]。（2）从网络层次看，大数据政务信息安全涉及网络的可靠性（保证网络和信息系统随时可用，运行过程中不出现故障，遇意外事故能够尽量减少损失并尽早恢复正常）、可控性（保证营运者对网络和信息系统有足够的控制和管理能力）等。这些特性确保了政务网络的稳定运行和有效管理，防止了网络攻击和破坏。大数据政务信息安全的重要性不言而喻。首先，政府信息涉及国家安全、商业机密和公民隐私，一旦泄露可能会对社会稳定和公民权益造成严重影响。其次，信息安全保障是提升公众对电子政务服务信任度的基础。只有确保政务信息的安全，才能赢得公众的信任和支持。最后，强化信息安全可以有效防范网络攻击和犯罪活动，确保政府信息系统的稳定运行。这对于维护国家安全和社会稳定、推动经济社会发展具有重要意义。

2 大数据政务信息安全风险类型

2.1 技术风险

在大数据政务环境中，技术风险是信息安全面临的首要挑战。信息技术的快速发展使得政务系统需要不断升级和更新，以适应新的安全威胁和业务需求。这种频繁的更新可能引入新的漏洞和错误，给系统带来不稳定性和安全隐患。政务系统的设计和实施过程中可能存在缺陷，如代码编写不规范、安全配置不当等，这些缺陷可能导致系统容易受到攻击。政务系统通常涉及多个部门和机构的协同工作，系统之间的接口和数据交换也可能成为安全漏洞的源头。技术风险还包括外部攻击和内部威胁，外部攻击可能来自黑客组织、恶意软件或网络钓鱼等，这些攻击可能利用系统漏洞或用户疏忽来窃取、篡改或破坏政务信息。内部威胁则可能来自内部员

工或合作伙伴，他们可能出于各种原因泄露敏感信息或破坏系统。

2.2 数据风险

大数据政务的核心是数据的收集、存储、分析和利用。然而，数据风险也是信息安全领域的重要问题。政务数据通常包含敏感信息，如个人隐私、商业秘密和国家机密等。这些信息的泄露可能对个人、企业和国家造成重大损失。政务数据具有海量性，这意味着数据管理和存储的难度大大增加。海量数据需要高效的存储和处理技术，否则可能导致数据丢失、损坏或无法及时访问。海量数据还增加了数据泄露的风险，因为攻击者可能更容易在大量数据中找到敏感信息。数据风险还包括数据的流动性和共享性，政务数据通常需要在不同部门、机构和地区之间共享和交换，以实现信息的互联互通和协同工作。这种流动性和共享性也可能导致数据泄露或被滥用。

2.3 伦理风险

随着大数据技术的广泛应用，政务部门能够收集和分析大量个人数据，以优化公共服务和政策制定。这种数据的收集和使用也可能引发伦理争议和道德风险。首先，个人隐私权是每个人的基本权利之一，政务部门在收集和使用个人数据时，必须确保数据的合法性和正当性，避免侵犯个人隐私[2]。在实际操作中，政务部门可能因缺乏明确的法律规范和监管机制而滥用个人数据，导致个人隐私泄露或被滥用。其次，政务部门在数据分析和利用过程中可能涉及对个人行为的预测和干预。这种预测和干预可能引发道德争议和伦理风险。然而这种预测和干预可能侵犯个人自由和尊严，引发社会不满和争议。

2.4 法律风险

大数据政务的法律风险主要源于相关法律法规的缺失或不完善，以及政务部门在数据收集、使用和处理过程中可能违反法律规定的问题。政务部门在收集和使用个人数据时可能面临法律风险，由于相关法律法规的缺失或不明确，政务部门可能无法确定数据的合法性和正当性，导致数据泄露或被滥用。政务部门在数据共享和交换过程中也可能面临法律风险，因为不同国家和地区之间的法律法规存在差异和冲突。政务部门在数据分析和利用过程中可能违反法律规定。例如，政务部门可能利用个人数据进行歧视性决策或侵犯个人权益的行为；或者在没有明确法律依据的情况下对个人数据进行预测和干预。这些行为都可能引发法律纠纷和诉讼风险。

3 人工智能辅助下的大数据政务信息安全风险防范机制

3.1 健全数据安全制度规范

在大数据政务信息安全风险防范体系中，健全数据安全制度规范是基石。应明确数据分类分级标准，根据数据的敏感性、重要性等因素，将数据划分为不同等级，实施差异化的保护措施。针对不同等级的数据，制定相应的访问权限、存储要求及传输规范，确保数据的保密性、完整性和可用性。建立健全数据安全管理制度，包括但不限于数据生命周期管理、数据备份与恢复策略、数据脱敏与匿名化处理规则等。这些制度应详细规定数据的采集、存储、使用、共享和销毁等各个环节的安全要求，确保数据在全生命周期内得到妥善保护。随着大数据技术的快速发展，相关法律法规也在不断完善中。政务部门应密切关注相关法律法规的变化，及时调整和完善内部管理制度，确保政务信息安全管理工作的合法合规性。在人工智能的辅助下，可以更加智能地识别数据风险点，自动匹配相应的制度规范，提高制度执行的准确性和效率。

3.2 提升平台技术防护能力

大数据政务平台作为政务信息存储、处理和传输的核心载体，其技术防护能力的提升至关重要。一方面，应加强平台的基础安全设施建设，如部署防火墙、入侵检测系统、安全审计系统等，有效抵御外部攻击和内部威胁。采用加密技术对敏感数据进行保护，确保数据在传输和存储过程中的安全性。另一方面，应利用人工智能技术提升平台的智能安全防护能力。例如，通过深度学习算法对海量数据进行实时监测和分析，及时发现并处置异常行为；利用自然语言处理技术对日志信息进行智能解析，提高安全事件的识别效率和准确性；运用知识图谱技术对安全事件进行关联分析，挖掘潜在的安全威胁和攻击模式。还应加强平台的应急响应和灾难恢复能力建设，制定详细的应急预案，定期组织应急演练，确保在发生安全事件时能够迅速响应、有效处置。建立完善的灾难恢复机制，确保在遭受重大灾难时能够迅速恢复系统正常运行，保障政务服务的连续性[3]。

3.3 强化数据安全运行管理

数据安全运行管理是确保大数据政务信息安全的关键环节。建立全面的数据安全监控体系，通过实时监控数据访问、操作行为等关键指标，及时发现异常情况和潜在威胁。利用人工智能技术对数据访问模式进行智能分析，识别出异常访问行为，及时采取阻断、报警等措施。加强数据安全审计工作，定期对数据操作行为、系统运行状态等进行全面审计，确保各项安全制度得到有效执行。通过人工智能技术自动收集和分析审计数据，

生成审计报告，为管理决策提供科学依据。还应建立完善的应急处理机制，针对可能发生的安全事件制定详细的应急预案和处置流程。在发生安全事件时，能够迅速启动应急预案，组织力量进行处置，最大限度地减少损失和影响。同时对安全事件进行事后分析和总结，不断完善应急预案和处置流程，提高应对能力。

3.4 人工智能在风险防范中的辅助作用

人工智能在大数据政务信息安全风险防范中发挥着越来越重要的作用。人工智能可以实现对数据风险的智能识别，利用深度学习、自然语言处理等算法对海量数据进行实时监测和分析，自动发现数据泄露、篡改等异常行为，为风险防范提供科学依据。人工智能可以实现数据风险的智能预警，通过对历史数据的学习和分析，建立风险预警模型，对潜在的安全风险进行预测和预警。当风险指标达到预警阈值时，自动触发预警机制，提醒管理人员及时采取措施进行处置。人工智能还可以实现数据风险的智能处置，在发生安全事件时，人工智能可以自动分析事件类型、影响范围等信息，快速生成处置方案，并自动执行或辅助管理人员进行处置。通过人工智能技术的引入，可以大大提高风险防范的智能化水平和应对能力。

4 人工智能辅助下的大数据政务信息安全实践案例分析

在当今数字化时代，大数据政务已成为提升政府服务效率和管理水平的重要手段。随着数据的海量增长和应用的不断深化，政务信息安全问题也日益凸显。为了有效应对这一挑战，我国某市政府积极引入人工智能技术，构建了一套高效的大数据政务信息安全防范体系，取得了显著成效。该市政府首先意识到，传统的人工安全监控方式已难以满足大数据环境下的安全需求。因此他们决定引入人工智能技术，实现对数据风险的智能识别、预警和处置。在具体实践中，该市政府利用深度学习算法，对政务系统中的海量数据进行实时监测和分析。通过训练模型，系统能够自动识别出数据泄露、非法访问等异常行为[4]。为了进一步提高风险防范的及时性，该市政府建立基于人工智能的风险预警系统。该系统通过对历史数据的学习和分析，建立风险预警模型。当风险指标达到预警阈值时，系统会自动触发预警机制，通过短信、邮件等方式向管理人员发送预警信息。系统还会根据风险类型和影响范围，自动生成处置建议，辅助管理人员进行快速响应。为了确保各项安全制度得到有效执行，该市政府还引入了智能安全审计系统，该系统利用自然语言处理等技术，对政务系统中的日志信息进行智能解析和审计。通过对比实际操作行为与预设的安全规范，系统能够自动发现违规行为，并生成审计报告。这不仅大大提高了审计效率，还有效降低人为因素导致的安全风险。在安全防护方面，该市政府采用了基于人工智能的防火墙和入侵检测系统，这些系统能够自动识别并拦截恶意攻击和非法访问行为，有效保障了政务系统的安全稳定运行。他们还利用人工智能技术对数据进行了脱敏和匿名化处理，确保在数据共享和交换过程中不会泄露个人隐私和敏感信息。通过引入人工智能技术，该市政府成功构建一套高效的大数据政务信息安全防范体系。这一体系不仅提高了风险防范的智能化水平和应对能力，还有效降低安全风险对政务服务的影响。在实践中，该市政府成功避免了多起数据泄露和非法访问事件，确保政务信息的保密性、完整性和可用性。这一成功案例不仅为该市政府赢得良好的社会声誉，也为其他地方政府提供了可借鉴的经验和做法。展望未来，随着人工智能技术的不断发展和应用深化，大数据政务信息安全防范体系将进一步完善和优化。

结束语

综上所述，人工智能辅助下的大数据政务信息安全风险识别与防范机制，是应对大数据环境下政务信息安全挑战的有效途径。通过智能技术的引入，实现了对政务大数据风险的精准识别与高效防范，为政府服务的连续性和稳定性提供了坚实保障。未来，将继续深化人工智能技术的应用，不断优化和完善风险防范机制，为智慧政府建设贡献力量。

参考文献

[1]蔡文选.大数据环境下电子政务信息安全体系的构建[J].城建档案,2022(11):61-64.

[2]朱莉.计算机网络安全技术及防火墙技术的分析[J].电子技术与软件工程,2021（012）：251-252.

[3]何力.大数据云计算和人工智能等新技术应用带来的网络安全风险[J].中国新通信,2020（22）：155-156.

[4]周晓晶.大数据环境下计算机网络安全研究[J].中国科技信息,2021（19）：46-47.