大数据与网络信息安全管理分析

杨宇涛

国家电投集团贵州金元绥阳产业有限公司，贵州 遵义 563305

摘　　要： 随着我国信息技术的飞速发展，大数据已崭露头角，成为当今时代的鲜明印记。然而，大数据的蓬勃发展在极大便利了社会生活的同时，也给网络信息安全管理带来了前所未有的严峻挑战。本文深入解析了大数据的基本概念及其核心特征，旨在为读者提供全面而清晰的认识。我们详细剖析了大数据在网络信息安全领域所遭遇的威胁与挑战，包括数据泄露、隐私侵犯、恶意攻击等诸多方面，以揭示大数据安全管理的紧迫性和重要性。面对这些挑战，本文进一步提出了切实可行的安全管理策略和建议。

关 键 词： 大数据；网络信息；安全管理

Big Data and Network Information Security Management and Analysis

Yang Yutao

State Power Investment Group Guizhou Jinyuan Suiyang Industry Co., LTD. Guizhou, Zunyi 563305

Abstract: With the rapid development of information technology in China, big data has emerged and become a distinct mark of the current era. However, the vigorous development of big data has not only greatly facilitated the social life, but also also brought unprecedented and severe challenges to the network information security management. This paper deeply analyzes the basic concepts and the core characteristics of big data, and aims to provide readers with a comprehensive and clear understanding. We analyze in detail the threats and challenges encountered by big data in the field of network information security, including data leakage, privacy invasion, malicious attacks and many other aspects, in order to reveal the urgency and importance of big data security management. Facing these challenges, this paper further proposes feasible safety management strategies and suggestions.

Keywords: big data; network information; security management

引言

数据，作为当代信息技术领域的重要概念，特指那些庞大而复杂的数据集，其规模之庞大、结构之复杂，以至于传统的软件工具在有限的时间内难以对其进行有效的捕捉、系统化的管理和高效的处理。这种数据的特点显著，包括数据量巨大、数据类型繁多、处理速度惊人以及价值密度相对较低等。随着大数据技术的迅猛发展和广泛应用，它已深入到我们生活的各个角落，极大地推动了社会的进步和变革。然而，与此同时，网络信息安全问题也日益凸显，成为阻碍大数据健康、可持续发展的关键因素之一。网络攻击、数据泄露、隐私侵犯等安全威胁层出不穷，给个人、企业乃至整个社会带来了严重的损失。加强大数据与网络信息安全管理的研究，不仅具有重要的理论价值，更具有迫切的现实意义。这不仅需要我们从技术层面出发，不断提升数据保护和安全防护的技术水平，还需要从管理层面着手，制定和完善相关法律法规和标准，加强行业自律，共同构建一个安全、可信的大数据环境。只有这样，我们才能充分发挥大数据的潜力，为经济社会发展注入新的动力。

一、大数据的概念

大数据，指的是一种庞大且复杂的数据集合，其规模之庞大以至于在合理的时间范围内，无法通过传统的软件工具进行高效捕捉、有效管理和精确处理。这类数据集合不仅拥有海量的数据量，还涵盖了多种多样的数据类型，包括结构化数据、非结构化数据以及半结构化数据等。[1]在处理上，大数据展现出惊人的速度，能够实时或近实时地进行数据分析和挖掘，为决策提供及时的数据支持。然而，由于数据量的庞大和类型的多样，大数据中的价值密度往往较低，需要借助先进的算法和技术手段来提炼和挖掘其中的价值。

作者简介：杨宇涛，1978年6月，男，汉族，助理工程师 从事工作研究方向：信息管理

二、网络信息安全的重要性

在当今的大数据时代，网络信息安全的重要性愈发凸显。它不仅直接关系到每个人的个人隐私和财产安全，更成为维护国家安全和社会稳定的关键因素。随着网络技术的飞速发展，数据的流动性和共享性日益增强，但同时也带来了信息安全方面的严峻挑战。一旦网络信息安全受到威胁，个人隐私泄露、财产损失，甚至国家安全受损等严重后果都可能发生。[2]我们必须高度重视并切实保障网络信息安全。这不仅需要政府部门的严格监管和立法保障，还需要社会各界的共同参与和努力。同时，广大网民也应增强信息安全意识，加强自我保护能力，共同构建一个安全、可靠、和谐的网络环境。

三、大数据的特点与网络信息安全挑战

（一）大数据的特点

大数据的显著特性可细化为以下四个方面：首先，大数据的“大”体现在其庞大的数据量上。这种数据量远超出了传统数据处理技术和系统的承载能力。它不仅涵盖了海量的历史数据，还包括了持续增长的实时数据流，从而为我们提供了丰富的信息来源。其次，大数据的数据类型极为多样。它不再局限于传统的结构化数据，如数据库中的表格数据，而是扩展到了非结构化数据，如社交媒体上的文本、图片、视频等，以及介于两者之间的半结构化数据，如 XML 文档、JSON 数据等。这种多样性要求我们必须采用更为灵活和高效的数据处理手段。再者，大数据的处理速度极快。在当今这个信息爆炸的时代，数据的产生和更新速度都极为迅速。因此，大数据处理要求能够实时或近实时地对数据进行分析和处理，以便我们能够迅速做出决策和响应。[3]大数据的价值密度相对较低。尽管我们拥有海量的数据，但其中真正有价值的信息却可能只占一小部分。这就要求我们采用先进的数据挖掘和分析技术，从大量的数据中提炼出有价值的信息，以支持我们的决策和行动。

（二）网络信息安全挑战

在当今的大数据时代，网络信息安全所遭遇的挑战变得愈发复杂和严峻。首先，数据泄露的风险显著上升。由于数据量庞大且结构复杂，其管理和保护难度相应增大，这直接导致了数据泄露事件频发，并可能引发严重的后果。其次，数据滥用问题日益凸显。不法分子往往利用大数据技术的先进性和便捷性，进行各种非法活动，如窃取商业机密、进行身份欺诈等，给社会和个人安全带来极大威胁。再者，网络安全威胁呈现多样化趋势。除了传统的网络攻击手段外，还出现了各种新型的网络攻击方式，如勒索软件、钓鱼攻击等。[4]病毒、木马等恶意软件的入侵也愈发频繁，给网络安全带来了极大的挑战。最后，隐私保护在大数据环境下变得更加困难。如何在充分利用大数据的同时，有效保护个人隐私成了一个亟待解决的问题。这需要我们不断探索和创新，建立更加完善的数据保护和隐私安全机制，确保个人信息安全和隐私权益得到有效保障。

四、大数据与网络信息安全管理策略

（一）加强法律法规建设

为了确保大数据技术的稳健发展和网络信息安全，政府应当迅速且全面地制定和完善相关法律法规体系。首先，要明确界定数据所有权，确保数据的原始创造者和拥有者享有合法权益，避免数据被非法获取或滥用。其次，规范数据使用权，制定明确的数据使用条件和限制，以保障数据在合法、公正、透明的环境下流通和使用。同时，隐私权保护是重中之重，政府应制定严格的隐私保护法规，确保个人和企业的隐私信息不被泄露或滥用。这些法律法规的完善，将为大数据的健康发展提供坚实的法律保障，促进数据资源的合理利用，推动社会经济的持续繁荣。为了保障大数据处理过程的安全性，建立一个全面的安全审计和监控机制显得尤为重要。我们需要明确安全审计与监控的目标，这包括但不限于保护敏感数据、防范内部和外部威胁、确保大数据处理的准确性和合规性等。在大数据环境中，监控范围应覆盖数据的全生命周期，从数据采集、传输、存储到使用和分析。同时，制定详细的监控策略，包括实时监控、日志收集与分析、访问控制等。通过安全信息与事件管理系统（SIEM），对大数据处理过程进行实时监控，包括监测入侵和攻击行为、系统性能等关键指标。[5]一旦检测到异常行为或性能下降，立即触发警报并采取相应措施。配置日志收集和分析系统，监控和记录大数据处理过程中的操作日志、事件日志等关键信息。通过分析日志数据，可以发现系统漏洞和异常行为，从而提前预警和处理。实施定期或不定期的审计活动，对大数据处理过程进行全面审查。采用专业的安全审计工具和技术，确保审计的准确性和效率。同时，对识别到的安全风险进行详细分析，制定相应的防范措施。

对敏感数据和系统操作实施严格的访问控制，限制特定人员的权限，防止未授权访问和操作。定期对大数据处理系统进行安全评估和渗透测试，发现潜在的安全漏洞并及时修复。加强员工关于信息安全的培训和意识教育，增强员工的安全意识和防范能力。对于识别到的安全风险和漏洞，建立问题跟踪机制，及时跟进问题的整改情况。对于未整改的问题，采取相应的措施进行进一步的处理和解决。同时，对整改后的系统进行重新评估，确保安全风险得到有效控制。通过定期审计评估，可以及时发现新的安全风险和漏洞，并对现有的防范措施进行评估和调整。同时，对安全审计工作的效果进行评估和反馈，为后续的工作提供参考和改进方向。[6]形成详细的审计结果报告，记录审计过程、识别到的安全风险和漏洞、防范措施的执行情况等内容，并提交给相关领导和部门。建立全面的安全审计和监控机制对于保障大数据处理过程的安全性至关重要。通过明确审计与监控目标、确定监控范围与策略、实施实时监控与审计、强化安全控制措施、问题跟踪与整改以及定期审计评估与报告等措施的有机结合，可以确保大数据处理过程的安全性和合规性。

（二）强化技术防范措施

企业应当高度重视并持续加强网络安全技术防范措施，以构建一个坚不可摧的数字防线。在数据传输和存储过程中，务必采

用先进的数据加密技术，确保信息的机密性和完整性。此外，防火墙的设置也是关键，它能有效监控和阻止潜在的网络威胁，为企业筑起一道坚实的防线。[7]企业还应引入先进的入侵检测系统，实时识别并应对各类网络攻击。除了上述的防御性措施，企业还应注重数据安全备份和恢复能力的建设。建立完善的数据备份机制，确保关键数据在面临丢失或损坏风险时能够迅速恢复，从而保障业务的连续性和稳定性。这不仅是对企业资产的保护，更是对客户信任的维护。因此，企业应全面提升网络安全防护水平，确保数据在各个环节的安全无忧。

（三）增强安全意识与培训

为了全面提升公司的网络信息安全水平，我们必须加强对员工在大数据与网络信息安全领域的认知与专业培训。我们需要通过系统性的培训课程，让员工深入理解大数据的重要性和网络信息安全的基本原理，从而增强他们的安全意识。这不仅包括对数据的敏感性认知，也包括对数据泄露和滥用的严重后果的认识。其次，我们还应注重提升员工的操作技能。通过实操演练和模拟攻击，使员工能够熟练掌握应对网络安全威胁的方法和技巧。[8]这将有助于他们在面对真实的安全威胁时，能够迅速、准确地作出反应，降低公司的安全风险。我们必须高度重视并持续推进这项工作，以确保公司的数据安全和业务的稳定运行。

（四）建立合作与共享机制

为了有效应对当前大数据与网络信息安全所面临的严峻挑战，政府、企业以及研究机构之间亟须建立一种紧密而富有成效的合作与共享机制。[9]这一机制的核心目标是通过三方共同努力，构建一个更为坚固的网络信息安全防护体系。具体而言，这一合作应包括但不限于安全信息的及时互通，包括最新威胁情报、安全漏洞信息等，以便各方能够迅速作出反应，降低潜在风险。同时，技术资源的共享也至关重要，各方可以共享先进的网络安全技术、解决方案和工具，共同提升网络安全防护的技术水平。此外，经验教训的分享同样不容忽视，通过分享成功与失败的经验，各方可以相互学习，避免重蹈覆辙，从而提升整个网络安全社区的防护能力和响应效率。

（五）加强国际合作与交流

在全球化的时代背景下，网络信息安全问题愈发凸显其跨国性和紧迫性。为了有效应对这一全球性挑战，各国应当摒弃孤立主义，深化合作与交流，携手共进。[10]具体而言，各国可以建立定期的信息安全对话机制，通过这一平台，分享最新的安全威胁情报、技术防范措施以及成功的安全管理经验。这种互信互助的合作模式将有助于及时发现和解决潜在的网络安全问题，进而提高全球网络信息安全水平，确保网络空间的和平、稳定与繁荣。[11]

结语

在当今日新月异的科技浪潮中，大数据与网络信息安全管理已成为一个既复杂又紧迫的议题。随着大数据技术的广泛应用，其蕴含的巨大价值不言而喻，但同时也带来了前所未有的挑战和机遇。为了确保大数据的健康发展，我们需从多个维度出发，采取一系列综合性的措施。法律法规建设是基石。我们需要不断完善与大数据和网络信息安全相关的法律法规，明确各方责任与义务，为数据的安全使用提供法律保障。这不仅能有效遏制违法行为，还能为大数据的合法利用提供清晰明确的指导。技术防范措施是保障。我们必须强化技术手段的应用，通过加密技术、防火墙、入侵检测等手段，提升网络信息安全防护能力。同时，不断研发新的安全技术，以应对日益复杂多变的网络攻击。增强安全意识与培训是关键。企业和个人都应增强对大数据安全的重视程度，加强安全意识和防范意识的培养。同时，通过定期的安全培训，提高相关人员的专业技能和应对能力，确保在面对网络攻击时能够迅速作出反应。建立合作与共享机制是必由之路。在大数据时代，信息安全的威胁往往跨越国界和地域，因此需要加强国际合作与交流，共同应对挑战。同时，建立信息共享机制，促进安全信息的快速传递和共享，提高整体防范能力。只有从法律法规建设、技术防范措施、安全意识与培训以及合作与共享机制等方面出发，我们才能确保大数据的健康发展，并为社会经济的繁荣稳定提供有力支撑。这是一项长期而艰巨的任务，需要我们共同努力和不懈追求。

参考文献

[1]李红杏，戚晗，赵亮，等. 基于量子神经网络的网络安全态势感知［J］沈阳航空航天大学学报，2023,40(1):78-85.
[2]胡向东，吕高飞，白银. 基于优化支持向量回归的网络信息安全态势预测方法［J］. 电子学报，2023,51(2):446-454.
[3]张瀚驰，黄河燕. 改进支持向量机的计算机网络安全态势预测方法［J］. 信息与电脑（理论版），2023,35(1):108-110.
[4]曹波，李成海，宋亚飞，等. 基于Stacking集成学习的网络安全态势预测方法［J］. 空军工程大学学报，2022,23(5):101-107.
[5]张亮，屈刚，李慧星，等. 智能电网电力监控系统网络安全态势感知平台关键技术研究及应用［J］. 上海交通大学学报，2021,55(增刊2):103-109.
[6]胡向东，田正国. 融合注意力机制和BSRU的网络信息安全态势预测方法［J］. 网络与信息安全学报，2022,8(1):41-51.
[7]唐延强，李成海，王坚，等. IGAPSO-ELM：一种网络安全态势预测模型［J］. 电光与控制，2022,29(2):30-35.
[8]苏小玉，董兆伟，孙立辉，等. 基于强化LSTM的网络安全态势预测方法［J］. 计算机技术与发展，2021,31(7):127-133.
[9]秦志红，樊里略，宋冰. 基于AIS的网络信息融合系统网络安全态势预测［J］. 舰船科学技术，2022,42(22):151-153.
[10]何春蓉，朱江. 基于注意力机制的GRU神经网络安全态势预测方法［J］. 系统工程与电子技术，2021,43(1):258-266.
[11]李雨泽，张中信. 基于排队模型的网络安全风险损失评估方法［J］. 计算机仿真，2021,38(4):258-262.