安全科学与工程学报
Journal of Safety Science and Engineering
第 3 卷◆第 4 期◆版本 1.0◆2025 年
文章类型：论文丨刊号（ISSN）：2972-4716(P) / 2972-4724(O)

大数据背景下的信息安全问题与对策

姜智宇　孟繁君
中国联通哈尔滨软件研究院
DOI:10.32629/jsse.v3i4.17862

[摘　要] 随着大数据技术的迅猛发展,其在推动社会进步和经济发展的同时,也带来了一系列信息安全问题。本文在阐述大数据背景下信息安全重要性的基础上,分析了当前面临的信息泄露、网络攻击、数据滥用、隐私保护缺失等安全问题,探讨了问题产生的技术、管理、法律等层面的原因,并从技术防护、管理机制、法律法规、人才培养等方面提出了相应的对策,旨在为保障大数据环境下的信息安全提供参考,促进大数据技术的健康发展。
[关键词] 大数据；信息安全；安全问题；对策
中图分类号：P413　文献标识码：A

Information Security Issues and Countermeasures in the Context of Big Data

Zhiyu Jiang　Fanjun Meng
China Unicom Harbin Software Research Institute

[Abstract] With the rapid development of big data technology, it has brought a series of information security issues while promoting social progress and economic development. On the basis of elaborating the importance of information security in the context of big data, this article analyzes the current security issues such as information leakage, network attacks, data abuse, and lack of privacy protection. It explores the technical, management, and legal reasons for the problems and proposes corresponding countermeasures from the aspects of technical protection, management mechanisms, laws and regulations, and talent cultivation. The aim is to provide reference for ensuring information security in the big data environment and promote the healthy development of big data technology.
[Key words] big data; Information security; Security issues; Countermeasures

引言

大数据技术的出现和发展,为各行各业带来了前所未有的机遇。它能够对海量的数据进行挖掘、分析和处理,从中提取有价值的信息,为企业决策、政府治理、科学研究等提供有力支持。然而,大数据的开放性、多样性和复杂性也使得信息安全面临着严峻的挑战。在大数据时代,数据成为重要的战略资源,一旦发生信息安全事件,不仅会给个人带来隐私泄露、财产损失等危害,还可能对企业的生存发展、国家的安全稳定造成严重影响。因此,深入研究大数据背景下的信息安全问题,并提出有效的对策,具有重要的现实意义。

1 大数据背景下信息安全的重要性

1.1保护个人隐私

在大数据时代,个人的各种信息,如身份信息、消费记录、位置信息、社交数据等都被广泛收集和存储。这些信息一旦泄露,可能会被不法分子利用,进行诈骗、盗窃等违法犯罪活动,严重侵犯个人的隐私权和财产安全。例如,个人的身份证号、银行卡号等信息泄露后,可能会导致银行卡被盗刷;个人的位置信息被泄露,可能会遭受跟踪、骚扰等。

1.2保障企业发展

企业在生产经营过程中积累了大量的商业数据,包括客户信息、技术资料、经营策略等。这些数据是企业的核心竞争力,一旦发生泄露或被篡改,可能会给企业带来巨大的经济损失,甚至导致企业破产。例如,企业的客户信息泄露,可能会导致客户流失;企业的技术机密被窃取,可能会使企业在市场竞争中处于劣势。

1.3维护国家安全

大数据涉及到国家的政治、经济、军事、文化等各个领域的信息。国家的重要数据,如国防数据、能源数据、金融数据等,一旦被泄露或遭受攻击,可能会威胁到国家的安全稳定。

2 大数据背景下信息安全存在的问题

2.1信息泄露问题突出

内部泄露：企业或机构内部员工因疏忽、故意或被利诱,

将敏感信息泄露给外部。如员工误发含敏感信息文件,或为私利出售商业机密。

外部攻击:不法分子通过网络攻击,如黑客攻击、病毒感染,非法获取信息系统数据。[1]大数据下,网络攻击手段更多样智能,威胁更大,如黑客利用漏洞窃取客户信息。

数据交易黑市猖獗:因数据有商业价值,不法分子获取数据后在黑市交易,形成黑色产业链,加剧信息泄露。

2.2网络攻击手段多样化

分布式拒绝服务攻击(DDoS):攻击者控制大量僵尸主机向目标服务器发大量请求,使服务器无法处理合法请求致服务瘫痪。大数据环境下,数据中心服务器更易成为目标。

勒索软件攻击:攻击者植入勒索软件加密文件,向受害者索要赎金,否则删除或公开。该攻击隐蔽性强、危害大,大数据下呈爆发式增长。

人工智能攻击:不法分子利用人工智能技术攻击,如生成逼真钓鱼邮件提高成功率,优化升级攻击使其更具针对性和有效性。

2.3数据滥用现象严重

过度收集数据:一些企业或机构为获利超范围收集用户数据,如APP安装时索要无关权限,数据可能被滥用[2]。

非法使用数据:企业或机构将用户数据用于未经授权的用途,如出售消费数据用于营销、用个人信息进行非法调查。

数据歧视:企业或机构根据用户数据分类评估,采取歧视性对待,如金融机构对低信用评分用户提高贷款利率或拒贷,企业根据消费能力提供不同产品和服务。

2.4隐私保护机制不完善

法律法规不健全:虽然我国已经出台了一些关于信息安全和隐私保护的法律法规,如《网络安全法》《数据安全法》《个人信息保护法》等,但在大数据环境下,这些法律法规还存在一些不足之处,如对数据跨境流动、数据匿名化处理等方面的规定还不够完善,导致隐私保护缺乏有效的法律保障。

技术手段落后:在大数据环境下,数据的数量庞大、类型多样,传统的隐私保护技术已经难以满足需求[3]。用户隐私保护意识薄弱:很多用户对个人隐私保护的重要性认识不足,在使用网络服务时,随意泄露个人信息,如在社交网络上公开自己的个人信息、点击不明链接等,给信息安全带来了隐患。

2.5数据存储和管理存在风险

数据存储安全隐患:大数据的数据量巨大,需要存储在大型的数据中心。数据中心的存储设备可能会因为硬件故障、自然灾害等原因导致数据丢失或损坏。此外,数据中心的物理安全也存在隐患,如未经授权的人员进入数据中心,窃取或破坏数据存储设备。

数据管理不规范:一些企业或机构在数据管理方面存在漏洞,如数据备份不及时、数据访问控制不严格等。数据备份不及时,一旦发生数据丢失,无法及时恢复;数据访问控制不严格,可能会导致未经授权的人员访问敏感数据。

3 大数据背景下信息安全问题产生的原因

3.1技术层面

大数据技术本身的漏洞:大数据技术是一种新兴的技术,在发展过程中还存在一些技术漏洞[4],如分布式计算框架的安全漏洞、数据存储技术的安全漏洞等,这些漏洞为信息安全问题的产生提供了可乘之机。

安全技术发展滞后:与大数据技术的快速发展相比,信息安全技术的发展相对滞后。现有的安全技术难以应对大数据环境下的各种安全威胁,如对大规模网络攻击的检测和防御能力不足,对数据隐私的保护技术不够成熟等。

3.2管理层面

安全管理意识淡薄:一些企业或机构对信息安全的重要性认识不足,没有建立健全的信息安全管理体系,对信息安全工作不够重视[5]。例如,一些企业没有设立专门的信息安全管理部门,没有制定完善的信息安全管理制度,导致信息安全工作缺乏有效的组织和管理。

安全管理制度不健全:即使一些企业或机构建立了信息安全管理制度,但制度不够完善,缺乏可操作性和执行力。

人员管理不到位:企业或机构的员工是信息安全的第一道防线,但一些企业或机构对员工的管理不到位,缺乏对员工的信息安全培训和教育,导致员工的信息安全意识淡薄,容易出现信息泄露等问题。

3.3法律层面

法律法规不完善:如前所述,我国关于信息安全和隐私保护的法律法规还存在一些不足之处,对一些新型的信息安全问题缺乏明确的法律规定,导致不法分子有机可乘。

执法力度不够:即使有相关的法律法规,但在实际执行过程中,执法力度不够,对违法犯罪行为的打击力度不足,导致违法成本较低,无法有效遏制信息安全问题的发生。

3.4社会层面

信息安全意识淡薄:整个社会的信息安全意识还比较淡薄,很多人对信息安全的重要性认识不足,缺乏自我保护意识。例如,一些用户在使用网络时不注意保护个人信息,随意点击不明链接,下载不明软件等。

数据黑市的存在:数据黑市的存在为信息安全问题的产生提供了利益驱动。一些不法分子为了获取巨额利润,不惜铤而走险,从事数据窃取、交易等违法犯罪活动。

4 大数据背景下应对信息安全问题的对策

4.1加强技术防护

数据加密技术:采用先进的数据加密技术,对敏感数据进行加密处理,确保数据在存储和传输过程中的安全性。例如,采用对称加密算法和非对称加密算法相结合的方式,对数据进行加密;对数据库中的敏感字段进行加密存储,防止数据被非法窃取。

访问控制技术:建立严格的访问控制机制,对用户访问数据的权限进行严格管理。根据用户的角色和职责,授予不同的访问

权限，确保只有授权人员才能访问敏感数据。同时，采用多因素认证技术，如密码、指纹、短信验证码等，提高访问控制的安全性。

入侵检测和防御技术：部署入侵检测和防御系统，实时监测网络中的异常行为和攻击活动，及时发现和阻止网络攻击。利用大数据分析技术，对网络流量、系统日志等数据进行分析，提高入侵检测的准确性和效率。

数据备份和恢复技术：建立完善的数据备份和恢复机制，定期对数据进行备份，确保在数据丢失或损坏时能够及时恢复。采用异地备份、多副本备份等方式，提高数据备份的可靠性。

4.2完善管理机制

建立健全信息安全管理体系：企业或机构应建立健全信息安全管理体系，制定完善的信息安全管理制度和操作规程，明确各部门和人员的信息安全职责。定期对信息安全管理体系进行审核和评估，及时发现和解决存在的问题。

加强人员管理：加强对员工的信息安全培训和教育，提高员工的信息安全意识和技能。定期组织员工参加信息安全培训课程，开展信息安全演练活动，使员工掌握信息安全的基本知识和技能，提高应对信息安全事件的能力。同时，建立员工保密制度，与员工签订保密协议，对违反保密规定的员工进行严肃处理。

强化数据生命周期管理：对数据的采集、存储、使用、传输、销毁等整个生命周期进行严格管理。在数据采集阶段，确保数据的合法性和安全性；在数据存储阶段，采用安全的存储方式，定期对数据进行备份和检查；在数据使用阶段，严格遵守数据使用规定，防止数据被滥用；在数据传输阶段，采用加密传输方式，确保数据的安全性；在数据销毁阶段，采用彻底的销毁方式，防止数据被恢复。

4.3健全法律法规

完善相关法律法规：进一步完善关于信息安全和隐私保护的法律法规，明确数据收集、使用、存储、传输等方面的规范和要求。加强对数据跨境流动的监管，制定数据跨境流动的安全评估机制和备案制度；完善数据匿名化处理的标准和规范，确保数据在匿名化处理后不会泄露个人隐私。

加大执法力度：加强对信息安全违法犯罪行为的打击力度，提高违法成本。建立健全信息安全执法协作机制，加强公安、网信、工商等部门之间的协作配合，形成执法合力。对涉嫌信息安全违法犯罪的行为，依法严肃查处，追究相关人员的法律责任。

4.4加强人才培养

培养专业的信息安全人才：高校和职业院校应加强信息安全专业建设，培养具有扎实的理论基础和实践能力的信息安全人才。根据市场需求，调整专业课程设置，增加大数据安全、网络安全等方面的课程内容，提高学生的专业素养。

引进高端信息安全人才：企业或机构应加大对高端信息安全人才的引进力度，吸引国内外优秀的信息安全专家加入。为高端人才提供良好的工作环境和发展空间，充分发挥他们的专业优势，提高企业或机构的信息安全防护能力。

加强在职人员培训：对于在职的信息安全人员，应加强培训和继续教育，不断更新知识结构，提高专业技能。通过参加行业研讨会、培训课程等方式，了解最新的信息安全技术和趋势，提升应对信息安全问题的能力。

4.5提高社会信息安全意识

开展信息安全宣传教育活动：通过各种媒体渠道，如电视、报纸、网络等，开展信息安全宣传教育活动，提高公众的信息安全意识。宣传信息安全的重要性、常见的信息安全威胁和防范措施等知识，引导公众树立正确的信息安全观念，增强自我保护意识。

加强行业自律：行业协会应发挥自律作用，制定行业信息安全标准和规范，引导企业或机构加强信息安全管理，自觉遵守相关法律法规和行业规范。组织行业内的信息安全交流活动，分享信息安全经验和技术，共同提高行业的信息安全水平。

5 结论

大数据技术的发展为社会带来了巨大的机遇，但也带来了严峻的信息安全挑战。信息安全问题不仅关系到个人的隐私和财产安全，也关系到企业的发展和国家的安全稳定。在大数据背景下，我们应充分认识到信息安全问题的严重性，采取有效的对策加以应对。通过加强技术防护、完善管理机制、健全法律法规、加强人才培养和提高社会信息安全意识等措施，构建一个安全、可靠的大数据环境，促进大数据技术的健康发展，为社会经济的发展提供有力支持。

[参考文献]

[1]宗庆.大数据背景下高等学历继续教育在线学习平台信息安全管理对策研究[J].信息与电脑,2025,37(07):233-235.

[2]闫金凤.大数据背景下统计信息安全面临的挑战与对策[J].中国会展(中国会议),2025,(04):170-172.

[3]罗奇.大数据背景下公民信息安全问题及治理对策研究[J].华东科技,2024,(12):116-118.

[4]石方夏,高屹.大数据背景下西藏网络信息安全对策[J].西藏发展论坛,2024,(06):82-88.

[5]刘娅琳.基于大数据背景下智慧交通规划中数据信息安全问题与对策研究[J].人民公交,2024,(20):20-22.

作者简介：

姜智宇(1987--),男,汉族,山东莱州市人,硕士研究生,职称：工程师,研究方向：数据分析、企业智能化。