大数据背景下计算机网络安全风险与防范研究

唐颖
成都工业学院，四川 成都 610031
DOI: 10.61369/TACS.2025100042

摘　　要： 在大数据蓬勃发展的当下，计算机网络安全面临诸多严峻挑战，数据泄露事件频发，敏感信息被非法获取与利用；恶意软件借助大数据传播渠道迅速扩散，严重威胁系统稳定运行；网络攻击手段日益复杂多样，传统防护体系难以有效抵御。基于此，本文深入探究了大数据与计算机网络安全基础认知、大数据背景下计算机网络安全风险类型、大数据背景下计算机网络安全风险成因、大数据背景下计算机网络安全防范策略，旨在通过不同的策略提升网络安全防护能力，保障大数据环境下的信息安全。
关 键 词： 大数据；计算机网络安全；风险与防范

Research on Computer Network Security Risks and Prevention in the Big Data Era

Tang Ying
Chengdu Technological University, Chengdu, Sichuan 610031

Abstract: With the vigorous development of big data, computer network security is facing numerous severe challenges. Data leakage incidents occur frequently, with sensitive information being illegally obtained and exploited; malware spreads rapidly through big data transmission channels, seriously threatening the stable operation of systems; network attack methods are becoming increasingly complex and diverse, making traditional protection systems difficult to resist effectively. Based on this, this paper deeply explores the basic cognition of big data and computer network security, the types of computer network security risks in the big data era, the causes of these risks, and the corresponding prevention strategies. It aims to improve network security protection capabilities through various strategies and ensure information security in the big data environment.
Keywords: big data; computer network security; risks and prevention; risk causes; protection strategies

引言

人工智能安全治理框架当中明确指出秉持共同、综合、合作、可持续的安全观，坚持发展和安全并重，以促进人工智能创新发展为第一要务，以有效防范化解人工智能安全　险为出发点和落脚点，构建技术与管理相结合、监管与治理相衔接、国内与国际相协同、社会各方积极参与且有效互动的治理机制，压实相关主体安全责任，打造全过程全要素治理链条，培育安全、可靠、公平、透明的人工智能技术研发和应用生态，积极研究应对人工智能灾难性　险的共识性准则，推动人工智能健康发展和规范应用，切实维护国家主权、安全和发展利益，保障公、法人和其他组织的合法权益，确保人工智能技术造福于人类[1]。高校在进行网络安全授课的过程当中，应该根据国家的政策进行展开，这样才能够更好地培养出更多优秀合法的人才[2]。

一、大数据与计算机网络安全基础认知

（一）大数据特性剖析

数据规模庞大：大数据涵盖海量信息，其存储与处理需要强大计算资源，规模增长使管理难度呈指数级上升，为安全防护带来巨大挑战[3]。

数据类型多样：包含结构化、半结构化和非结构化数据，不同类型数据的安全需求和处理方式各异，增加了安全策略制定的复杂性。

数据处理快速：实时数据处理需求促使系统高速运转，快速处理过程中可能因安全检查不充分，给攻击者可乘之机。

（二）计算机网络安全内涵

系统完整性维护：确保计算机系统硬件、软件和数据不受未经授权的破坏、更改，保持系统正常运行和数据的准确可靠。

数据保密性保障：防止敏感信息泄露给非授权个人或实体，通过加密、访问控制等手段保护数据隐私[4]。

系统可用性确保：保证计算机系统在需要时能够正常运行，不被恶意攻击或故障导致服务中断，满足用户业务需求。

（三）大数据与网络安全关联

数据价值提升风险：大数据蕴含巨大商业和战略价值，吸引更多攻击者，使其成为网络攻击的重点目标，安全威胁加剧。

技术融合带来新隐患：大数据与云计算、物联网等技术融合，新架构和模式产生新的安全漏洞，如虚拟化安全、设备接入安全等[5]。

数据处理环节增多：大数据从采集、存储、传输到分析应用，环节增多，每个环节都可能存在安全隐患，扩大安全风险面。

二、大数据背景下计算机网络安全风险类型

（一）数据泄漏风险

内部人员违规操作：员工因疏忽、利益诱惑或恶意目的，违规访问、复制或传播敏感数据，导致数据泄露。

外部攻击窃取数据：黑客通过网络攻击手段，如入侵系统、破解密码、利用漏洞等，获取企业或个人的数据[6]。

供应链安全漏洞：供应链中的第三方服务商可能存在安全薄弱环节，数据在传输或存储过程中被窃取或篡改。

（二）网络攻击风险

拒绝服务攻击：攻击者通过发送大量请求，耗尽目标系统资源，使其无法正常提供服务，影响业务连续性[7]。

恶意软件感染：病毒、木马、蠕虫等恶意软件感染计算机系统，窃取数据、破坏系统功能或控制设备，造成严重危害。

高级持续性威胁：攻击者长期潜伏在目标系统中，持续收集敏感信息，对国家安全和企业核心利益构成重大威胁。

（三）数据篡改风险

数据完整性破坏：攻击者篡改数据内容，使数据失去真实性和准确性，影响基于数据的决策和业务运营。

业务逻辑被干扰：篡改关键业务数据，导致业务流程混乱，引发经济损失和声誉损害，如金融交易数据篡改。

信任体系受损：数据篡改会破坏用户对系统和数据的信任，降低用户粘性，影响企业的市场竞争力。

（四）隐私侵犯风险

个人信息过度收集：企业和机构未经用户同意，收集大量个人信息，超出合理使用范围，侵犯用户隐私权[8]。

数据二次利用风险：收集的个人信息被用于未经授权的其他目的，如精准营销、数据贩卖等，给用户带来困扰。

隐私政策不透明：部分企业和机构的隐私政策表述模糊，用户难以了解个人信息的使用方式和保护措施，增加隐私泄漏风险。

三、大数据背景下计算机网络安全风险成因

（一）技术层面因素

安全技术滞后：大数据技术发展迅速，但安全技术相对落后，难以满足大数据环境下的安全防护需求，如加密技术、访问控制技术等。

系统漏洞存在：计算机系统和软件存在各种漏洞，攻击者可以利用这些漏洞进行入侵和攻击，而漏洞修复不及时或不彻底，增加了安全风险。

安全架构不完善：大数据系统的安全架构设计不合理，缺乏有效的安全防护层次和机制，难以抵御复杂的网络攻击。

（二）管理层面因素

安全意识淡薄：企业和个人对网络安全重视不够，缺乏安全意识和防范意识，容易忽视安全风险，导致安全事件发生。

安全管理制度不健全：缺乏完善的安全管理制度和流程，安全管理工作不规范，责任不明确，难以有效落实安全措施[9]。

人员管理不到位：对内部人员的管理和监督不足，员工安全培训不足，存在违规操作和恶意行为的风险，如内部人员泄露数据。

（三）法律层面因素

法律法规不完善：大数据安全相关法律法规不健全，对网络犯罪的定义、处罚标准和责任界定不够明确，难以有效打击网络违法犯罪行为。

法律执行难度大：大数据的跨地域、跨行业特性使得法律执行难度加大，不同地区和行业的法律适用和协调存在问题，影响法律的实施效果。

国际合作不足：大数据安全问题具有全球性，但国际在网络安全领域的合作不够紧密，缺乏统一的国际标准和规范，难以形成有效的全球治理机制。

（四）社会层面因素

网络环境复杂：互联网的开放性和匿名性使得网络环境复杂多变，不法分子利用网络进行各种违法犯罪活动，如网络诈骗、网络攻击等。

信息传播迅速：大数据时代信息传播速度快、范围广，安全事件一旦发生，容易引发社会恐慌和不良影响，加大安全事件的危害。

公众安全素养不高：公众对网络安全知识和技能掌握不足，缺乏自我保护能力，容易成为网络攻击的受害者，如点击恶意链接、泄露个人信息等[10]。

四、大数据背景下计算机网络安全防范策略

（一）技术防范策略

1. 加强数据加密技术

采用先进的加密算法和技术，对数据进行加密处理，确保数据在传输和存储过程中的保密性和完整性，如对称加密、非对称加密等。

2. 完善访问控制机制

建立严格的访问控制体系，根据用户角色和权限，限制用户对数据的访问，采用身份认证、授权管理等技术手段，防止非法访问。

3. 部署安全防护设备

安装防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、

防病毒软件等安全防护设备，实时监测和防范网络攻击，及时发现和处理安全威胁。

4. 采用大数据安全分析技术

利用大数据分析技术，对网络流量、用户行为、系统日志等进行实时监测和分析，发现异常行为和潜在安全威胁，及时采取应对措施。

（二）管理防范策略

1. 增强安全意识

加强企业和个人的网络安全意识教育，开展安全培训和宣传活动，增强安全防范意识和能力，使员工和用户自觉遵守安全规定。

2. 健全安全管理制度

建立完善的安全管理制度和流程，明确安全责任和义务，规范安全管理工作，如数据备份与恢复制度、安全审计制度等，确保安全措施的有效执行。

3. 加强人员管理

加强对内部人员的管理和监督，建立人员背景审查和离职审计制度，对员工进行定期的安全培训和考核，防止内部人员泄露数据和进行恶意攻击。

4. 定期进行安全评估和演练

定期对计算机系统和网络进行安全评估，发现安全隐患并及时整改；开展安全演练，提高应对安全事件的能力和应急响应速度。

（三）法律防范策略

1. 完善法律法规

加快大数据安全相关法律法规的制定和完善，明确网络犯罪的定义、处罚标准和责任界定，加大对网络违法犯罪行为的打击力度。

2. 加强法律执行

加强执法部门的技术装备和人员培训，提高法律执行能力，确保法律法规的有效实施，对网络犯罪行为进行及时、严厉地惩处。

3. 加强国际合作

积极参与国际网络安全合作，加强与国际组织和各国在网络安全领域的交流与合作，共同制定国际标准和规范，打击跨国网络犯罪活动。

（四）社会防范策略

1. 营造良好网络环境

加强网络文化建设，倡导文明上网、安全上网，营造健康、和谐的网络环境，减少网络不良信息的传播和影响。

2. 加强信息传播管理

加强对网络信息的传播管理，规范信息发布行为，建立信息审核机制，防止虚假信息和有害信息的传播，维护网络信息秩序。

3. 提高公众安全素养

通过多种渠道和方式，向公众普及网络安全知识和技能，如开展网络安全宣传周活动、发布网络安全指南等，提高公众的自我保护能力和安全素养。

4. 建立社会监督机制

建立社会监督机制，鼓励公众参与网络安全监督，设立举报渠道，对发现的网络安全问题及时进行举报和处理，形成全社会共同维护网络安全的良好氛围。

五、结束语

在大数据浪潮席卷的当下，计算机网络安全风险愈发复杂多元，数据隐私泄露、恶意攻击肆虐等问题亟待解决。本文虽对大数据背景下计算机网络安全风险与防范进行了研究，但网络安全领域不断演变。未来，需持续跟进技术发展，强化安全意识，完善防护体系，多方协同共筑安全防线，以保障大数据环境稳定有序，推动其健康可持续发展。

参考文献

[1] 刘萍 . 人工智能和大数据技术在计算机网络安全防御系统中的应用研究 [J]. 造纸装备及材料 ,2024,53(12):96-98.

[2] 黄浩 . 一种基于大数据的计算机网络信息安全分析方法及系统 [J]. 软件 ,2024,45(12):71-73.

[3] 戚晓伟 . 新质生产力下高职创新型拔尖人才培养模式的探讨——以 " 计算机网络技术 " 专业为例 [J]. 中国多媒体与网络教学学报 (中旬刊),2024,(12):185-188.

[4] 郭文龙 , 姜惠娟 , 李勇 . 词云技术与 CIPP 评价模式相结合的计算机网络课程思政实施及评价方法探索 [J]. 计算机教育 ,2024,(12):78-83.

[5] 谢吉伦 . 基于人工智能技术的计算机网络安全风险评估系统设计 [J]. 信息记录材料 ,2024,25(12):40-42.

[6] 谷廷秀 . 基于职业技能大赛的计算机网络技术课程教学改革策略研究 [J]. 教师 ,2024,(33):99-101.

[7] 廖芳芳 , 曹子坤 . 计算机网络在高职学生综合素质评价数据采集中的应用研究 [J]. 信息系统工程 ,2024,(11):135-138.

[8] 赵玉梅 . 计算机网络安全技术的影响因素与防范策略分析 [J]. 集成电路应用 ,2024,41(11):412-414.

[9] 张娴 . 探究将网络安全教育融入高职新工科专业基础课程教学实施路径——以《信息安全技术》教学为例 [J]. 网络安全技术与应用 ,2024,(11):88-90.

[10] 陈洁 . 网络安全软件开发项目全过程质量影响因素及对策研究 [D]. 南京林业大学 ,2024.

