新技术背景下计算机网络信息安全防范机制研究

万永强　李敏　张德栋　陈小樟　郑小娜
厦门特勤疗养中心　福建厦门　361000

【摘　要】随着大数据时代的到来，各项信息技术得以普及和应用，尤其是互联网、物联网等信息技术的应用极大的给人们的工作和生活带来了极大的便利。在此背景下，计算机网络信息变的更为透明，网络信息安全迎来了新的挑战。基于此，本文从新技术背景下计算机网络信息安全的重要性入手，分析了目前影响信息安全的因素并由此提出了针对性的措施以期实现计算机网络的绿色发展。

【关键词】新技术 计算机网络信息 安全防范机制

Research on computer network information security prevention mechanism under the background of new technology

Wan Yongqiang　Li Min　Zhang Dedong　Chen Xiaozhang　Zheng Xiaona
Xiamen Special Service Sanatorium　Xiamen，Fujian　361000

【Abstract】With the advent of the big data era，various information technologies have become widespread and widely applied，particularly the internet and the Internet of Things，which have greatly facilitated people's work and life.In this context，computer network information has become more transparent，presenting new challenges to network information security.Based on this，this paper starts with the importance of computer network information security in the new technological landscape，analyzes the factors currently affecting information security，and proposes targeted measures to achieve green development in computer networks.

【Key words】new technology，computer network information security mechanism

引言

随着社会的发展以及科技的进步，计算机网络技术显然已成为人们生活和工作必不可少的工具，但随着新技术的应用给计算机网络技术提出了新的发展机遇的同时也提出了更高的要求，尤其是信息安全方面。具体来讲，随着人工智能技术的应用，一方面加强了对各项信息数据的挖掘和处理能力，另一方面也极易被不法分子恶意使用成为攻击网络的新技术；大数据海量存储功能在保证决策高效性的同时也增加了数据泄露的风险；云计算的应用虽然提升了传统计算效率和质量，但也致使数据主权以及安全管理难度系数增加；物联网的应用在让万物得以互联的同时也让安全变得更为模糊等等，在此机遇和挑战并存的背景下，加强新技术在计算机网络信息安全防范的研究一方面是保证用户个人隐私的必然要求，另一方面也是推动科技进步，社会稳定发展的重要措施。

1 新技术背景下计算机网络信息安全的重要性

1.1 强化计算机网络信息的安全防护等级

作为一个庞大且复杂的系统，计算机网络信息系统不仅仅涉及到个人敏感隐私，而且还包括了科研成果、医疗机构所需的病患记录、药品信息、电子商务等国家、社会发展所需的数据等。这些数据的安全对于维护国家的稳定、经济的长久发展、文化传承以及国家主权等非常重要。如果这些数据遭到恶意的泄露或者破坏势必会应发连锁反应，对于国家、社会以及经济的发展带来极大的危害。所以，为了保证网络系统的稳定就必须要加强计算机网络信息安全的防护，建立健全网络防御体系，即利用先进的安全技术以及完善的安全策略，可以切实提升网络恶意攻击效率，防止国家利益或者社会公益受到不法侵害。

1.2 维护计算机网络的稳定运行

随着科技的进步，计算机网络所涉及的功能也越来越强大，其不仅担负着信息管理和存储的责任，而且还包括了用户的实名认证个人信息、药品信息等信息的保护。用户在网上从事相关工作或者娱乐时，难以避免会提供姓名、地址、电话等个人信息，一旦这些信息数据被恶意破坏，不仅会危害到用户隐私以及药品信息安全，甚至还能出现盗窃、金融诈骗等网络安全事故，这些事故将直接影响到网络服务的正常供应，而且还会给用户带来巨大的经济损失。为此，为了确保网络稳定的运行，保障广大用户合法利益以及社会秩序的稳定就必须要加强计算机网络信息的安全管理。换而言之，通过采用有效科学的信息安全措施，将保证网络信息正常传播应用的同时还能发挥计算机网络在经济发展中的潜在价值。

1.3 推动科技创新

任何一项新技术的发展均离不开安全可靠的网络信息环境，而信息安全保证工作将为科技创新发展提供了坚实的基础。药品科研机构以及企业可以在安全的网络环境中放心的开展相关研究，并不用担心核心数据被盗取或者破坏，而投资者也会更加愿意对具有安全网络信息环境的药品科技项目进行投资，从而为科技创新提供充足的资金支持。安全的网络环境还将有效地促进各个国家、不同领域间的交流合作，进而加快科技创新效率，并且信息安全技术自身也是科技创新的领域之一，其自身也将推动网络安全技术的革新升级。

2 新技术背景下计算机网络信息安全防范存在的问题

2.1 技术复杂性引发的安全漏洞

随着科技的发展和进步，计算机网络技术架构的复杂程度越来越高。具体来说，人工智能、大数据等先进的科学技术与计算机技术的融合发展虽然为人们日常生产生活提供了极大的便利，但由此也衍生出一系列的的安全漏洞。其中的人工智能算法很有可能出现被恶意篡改的情况，由此影响计算机系统的安全决策，从而危及整个计算机网络信息的安全。同时，技术的深度融合发展也会带来海量的数据存储和处理的需求，这会大大增加计算机数据管理系统的压力，稍有差池就会出现数据泄露的情况。新技术背景下，多租户资源共享模式会使得数据隔离和访问控制的难度进一步提升，导致若计算机网络信息安全防范系统出现异常，用户个人隐私数据和药品信息就会出现泄露的风险。而且物联网等新技术的应用会连接大量的智能设备和系统，由于数据计算和存储能力的限制，也会常常出现弱密码、软件漏洞等安全隐患，从而使得不法分子觅得良机，攻击计算机网络信息安全系统。

2.2 恶意攻击手段的不断升级

随着科技的发展和进步，计算机网络恶意攻击手段和形式的多样化程度越来越高。病毒、木马等传统的恶意攻击手段逐渐演变成为隐蔽性和破坏性更强的新型恶意攻击手段，而且还会出现更高阶的高级持续性威胁（APT）攻击、零日漏洞攻击、社交工程攻击等攻击手段。其中，高级持续性攻击的发起者一般都是有组织有预谋的黑客组织，会长期持续地针对同一计算机网络信息安全系统目标进行渗透和攻击，具有极强的隐蔽名和破坏性。而零日漏洞攻击主要是由于软件系统出现安全漏洞且未能及时修复而导致的，破坏性也比较强。社交工程攻击则是以钓鱼邮件、社交网络等欺骗的方式破坏计算机网络信息安全防范系统，以非法获取目标信息，随着恶意攻击手段的升级和创新，这无疑会加大对计算机网络信息安全的威胁。

2.3 人为因素导致的安全风险

新技术背景下，计算机网络信息会面临人为因素而导致的安全风险。主要体现在两个方面，其一，计算机网络信息技术人员的误操作、行为不当等情况会增加安全风险；或者是人员自身的专业水平较低、职业道德较差等情况也会为计算机网络信息安全防范带来隐患。其二，计算机网络用户的安全意识不强，安全密码设置过于简单，破解难度较低，且对于来源不明的链接或者软件未能保持高度警惕心理，随意下载和点击，由此引发一系列的计算机网络信息风险，威胁到药品信息的安全。

2.4 法律法规与监管的滞后

随着经济的发展和科技的进步，计算机网络技术取得了突飞猛进的发展，但关于其信息安全的相应法律法规和监管制度却表现出滞后的状态。虽然相关部门和单位已经逐渐完善相关法律法规，但关于新型网络攻击和违法行为的界定和监管仍然存在真空地带，或者惩治措施不够严厉。其中对于跨国网络犯罪的管辖问题也常常出现争议。同时，监管部门的专业技术水平面对日益复杂且多样的网络信息安全威胁稍显吃力，由此进一步增加了计算机网络信息的安全风险。

3 新技术背景下计算机网络信息安全防范机制研究

3.1 技术层面安全防范机制

第一，深度强化加密技术的应用。新技术背景下，加密技术也需要不断地强化和创新。作为保障计算机网络信息安全的有效举措之一，加密技术能够有效规避网络信息被非法访问或篡改的行为，从而显著提升计算机网络信息安全性，最大限度保证药品信息的安全。具体来说，数据加密技术主要包括对称和非对称两种。对于对称加密技术来说，需要通过相同的秘钥实现数据的加密和解密操作，具有较快的处理速度，但秘钥自身存在一定的安全隐患。而对于非对称加密技术来说，需要通过公钥和私钥分别处理数据的加密和解密操作，能够显著提升网络信息数据的安全性和高效性。与此同时，随着技术的发展，量子技术在网络信息数据加密中的应用，为计算机网络信息安全防范提供了新思路。通过量子力学特征能够大大增强数据信息传输的安全性。量子密钥也具有很强的不可破解性。此外，还需要进一步优化和完善传统的加密技术，在人工智能、云计算算法等先进技术的作用下，进一步强化秘钥的安全等级，实现计算机网络信息的高效防护，从而最大限度保证药品信息的安全。

第二，强化入侵检测和防御系统的智能化程度。基于人工智能和机器学习等先进的科学技术，强化入侵检测和防御系统的智能化程度。具体来说，该系统能够基于网络数据的学习和分析，对非法入侵计算机系统的异常行为和攻击进行自动识别，并发出警报采取有效防御策略。通过机器学习算法能够对入侵检测模型进行优化和完善，以显著提升计算机网路系统应对攻击行为的能力。此外，还可以在大数据技术的作用下，提升计算机网络信息安全监测机制的高效性和灵敏性，以实现计算机网络信息数据流、数据内容的实时追踪以及安全预警。据此，大数据技术在计算机网络信息安全防范机制中的应用，能够全方位、多维度、深层次地分析和挖掘网络信息，以显著提升系统自动识别安全隐患和风险的能力。同时，还需要不断优化和完善计算机网络信息安全事件的快速反应机制，一旦发现系统遭受安全攻击，要第一时间启动应急预案，以有效控制危险时态发展，从而进一步提升计算机网络信息的安全性。

第三，建立健全兼具精细化和自动化的安全漏洞管理机制，以自动且精准识别、评估和修复系统安全漏洞。要定期通过安全漏洞扫描工具对计算机系统进行扫描检查，以确定其中是否存在安全隐患和风险。适时引入大数据技术，深度分析和挖掘信息安全漏洞，以对安全漏洞的等级和影响程度进行有效评估。之后通过自动修复系统及时更新补丁，修复漏洞，从而确保计算机网络信息的安全。同时，还需要创新网络数据信息安全漏洞的共享机制，以有效应对计算机网路信息的安全威胁。此外，还需要创新网络信息恢复机制。在处理完成计算机网络信息所遭受非法攻击后，要在大数据技术的帮助下，创建一个能够兼容高度复杂和关联性强的数据信息恢复机制，确保计算机网络信息遭受安全攻击后能够保持数据信息的完整性和可访问性，以及快速重修和复原网络系统，进一步强化计算机网络信息的安全防范水平，从而保证药品信息的安全。

3.2 管理层面安全防范机制

第一，建立健全计算机网络信息安全管理机制。要制定明确的网络信息安全管理制度，将安全职责明确至具体部门和个人。基于人员、设备、数据等计算机网络信息系安全要素强化管理工作，以提升计算机网络信息访问行为和数据处理的规范性。要视具体的工作需要分配相应的用户管理权限，避免出现滥用权限的情况。而且还需要不断优化和完善数据信息备份和恢复机制，定期自动备份重要数据，从而进一步提升计算机网络信息的安全管理水平。

第二，强化人员的专业技术能力和信息安全意识。要定期组织开展关于计算机网络信息安全的专业技术培训活动，以切实提升工作人员的专业技术能力。培训内容包括但不限于网络安全基础知识、安全操作规程、应急响应措施等等，而且还要强化人员的实践操作能力，促使人员能够熟练掌握网络信息安全事件的处理方法和手段。同时，要强化计算机用户的网络信息安全防范意识。1.加强计算机网络信息安全防范的宣传力度，充分发挥新技术的优势，创新兼具多样性和有效性的网络信息安全防范宣传形式和渠道，宣传计算机网络信息安全防范内容，旨在强化计算机用户的网络安全防范意识。2.还可以定期开展计算机网络信息安全走入社区的活动，结合具体的网络信息安全案例和数据，定期开展网络信息安全防范机制的宣传教育，尽可能选择更贴近计算机用户实际生活的人或事件案例，进一步强化用户的网络信息安全防范意识，加强计算机用户安全防范技术的掌握和应用能力，从而营造良好的计算机网络信息安全环境。

第三，组建计算机网络信息安全审计和监管机制。要确保审计部门具有高度的独立性，以便于定期开展计算机网络信息安全状态的审计工作，其中所涉及到的内容主要是安全

策略的执行、用户安全行为规范和网络信息安全漏洞的检测和修复等等，及时发现其中存在的安全隐患和风险，并适时给予必要的指导和改进意见。而且为了鼓励人员监督网络信息安全违规行为，还需要建立健全举报机制，以营造良好的计算机网络信息安全监督环境，从而保证药品信息的安全。

3.3 法律法规层面安全防范机制

建立健全计算机网络信息安全防范法律法规，对网络违法行为进行明确界定，并加强惩治措施的力度。对于新技术背景下计算机网络信息面临的安全问题，需要不断优化和完善法律法规，弥补其中的真空地带，强化网络信息的安全防护水平，以为计算机网络信息安全提供有力的法律保障。而且还需要积极开展跨国合作，以应对日益严峻的跨国网络犯罪，从而提升计算机网络信息的安全水平。此外，还需要强化执法单位的人员的专业技术能力，强化网络信息犯罪的惩治力度，提升网络信息安全事件的响应速度，以保障网络信息的安全。要进一步强化网络服务运营商的监管力度，明令其必须要严格贯彻和落实网络信息安全保障义务。

3.4 加强合作，充分发挥社会多方作用

第一，为有效提升行业整体信息安全防护能力，需着力加强行业内各主体间的协作。具体而言，应推动成立行业信息安全联盟，搭建企业间信息共享与技术交流平台。通过联盟机制，企业可共同应对行业性安全威胁，分享安全防护策略与成功经验。此举有助于整合行业资源，形成安全防护合力，显著降低安全风险。例如，在遭遇大规模网络攻击时，联盟成员可迅速协同作战，实施联合防御，大幅提升抗攻击能力。

第二，为加速信息安全技术创新与应用，应大力促进高校、科研机构与企业之间的深度合作。高校与科研机构应充分发挥其科研优势，为企业提供前沿安全技术支撑与理论指导；企业则需积极开放实践平台，为高校与科研机构提供丰富的应用场景。通过产学研紧密结合，不仅能够加速信息安全技术的转化应用，还能有效培养一批高素质的信息安全专业人才，为计算机网络信息安全构筑坚实的人才后盾。

4 总结

随着科技的发展和进步，计算机网络信息面临日益复杂且严峻的安全威胁，这对于计算机网络信息安全防范机制提出了更高的要求。对此，需要客观认识到现阶段网络信息安全防范存在的问题和不足，优化和创新网络信息安全防范机制，从而最大限度保障药品信息安全。

参考文献

[1]刘博.大数据背景下计算机网络信息安全技术与防范机制[J].办公自动化，2024，29（11）：39-41.
[2]樊德慧.信息化背景下中职学校网络信息安全防范探究[J].网络安全技术与应用，2024，（02）：72-74.
[3]孙美玲.基于大数据分析的计算机网络信息安全监测[J].信息与电脑（理论版），2023，35（22）：239-241.
[4]李俊.计算机网络信息安全中的网络技术运用[J].信息记录材料，2023，24（11）：109-111，114.
[5]孙强等.人工智能技术与网络信息安全分析[J].集成电路应用，2023，40（06）：351-353.

作者简介：万永强，出生年月：1988.12，男，籍贯具体到省市：云南永平，民族：汉，职称：助理工程师，学历：本科，学位：工学学士，研究方向（与工作相关）：信息安全；
李敏，出生年月：1973.12，女，籍贯具体到省市：江苏省徐州市，民族：汉，职称：副主任护师，学历：本科，学位：法学学士，研究方向（与工作相关）：信息安全管理；
张德栋，出生年月：1980.11，男，籍贯具体到省市：福建厦门，民族：汉，职称：副主任药师，学历：研究生，学位：硕士，研究方向（与工作相关）：药事管理；
陈小樟，出生年月：1989.01，女，籍贯具体到省市：福建上杭，民族：汉，职称：主管药师，学历：本科，学位：学士，研究方向（与工作相关）：药事管理；
郑小娜，出生年月：1996.3，女，籍贯具体到省市：福建厦门，民族：汉，职称：药师，学历：本科，学位：学士，研究方向（与工作相关）：药事管理。