基于大数据的网络安全的重要性及防范策略

郅逍遥　刘贵坤
（郑州商贸旅游职业学院 郑州 450000）

摘　要　随着大数据时代网络安全问题的日益凸显，保护个人隐私和数据安全变得尤为重要。大数据的广泛应用，使个人数据和敏感信息容易受到黑客或病毒的恶意攻击，为应对这些挑战，加强网络安全意识和防范教育至关重要。文中深入探讨了基于大数据的网络安全的重要性，浅析了防范策略的创新与发展趋势，通过分析网络安全问题的现状与未来发展，以更好地准备和应对新型网络威胁，确保网络在大数据时代下的可信性，实现信息社会的可持续发展。

关键词：大数据；网络安全；数据安全；防范策略
中图法分类号　TP393.08

Importance and Prevention Strategies of Network Security Based on Big Data

ZHI Xiaoyao and LIU Guikun
（Zhengzhou Vocational College of Commerce and Tourism，Zhengzhou 450000，China）

Abstract　With the increasingly prominent cyber security issues in the era of big data，the protection of personal privacy and data security has become particularly important. The wide application of big data makes personal data and sensitive information vulnerable to malicious attacks by hackers or viruses. In order to cope with these challenges，it is essential to strengthen cyber security awareness and prevention education. This paper deeply discusses the importance of cyber security based on the big data，analyzes the innovation and development trend of prevention strategies，and analyzes the current situation and future development of cyber security issues to better prepare for and respond to new cyber threats，ensure the credibility of the network in the era of big data，and realize the sustainable development of the information society.

Keywords　Big data，Network security，Data security，Preventive strategies

0　引言

大数据的崛起改变了人们工作和生活模式，大数据的快速发展和广泛应用，为企业、组织和个人带来了巨大的机遇和便利，但也带来了网络安全挑战，如网络恐怖主义、数据窃取、勒索软件攻击等，使网络安全防护工作愈发复杂和困难。社会、企业和个人需要采取有效的网络安全防范策略，深入了解网络安全的现状和未来发展趋势，以更好地抵御网络威胁，更有效地应对网络安全挑战。

1　基于大数据的网络安全的重要性

1.1　保护个人隐私和数据安全

由于互联网的蓬勃发展和智能设备的普及，个人信息被大量地收集、存储和分析，构成了庞大的大数据生态系统，然而这些数据也带来了潜在的风险和威胁。(1)大数据的收集和共享使个人隐私面临巨大的泄露风险。个人隐私包括身份信息、地理位置、健康状况等敏感数据，这些数据的泄露可能会导致身份盗用、针对性攻击、敲诈勒索等，如黑客入侵数据库或公司内部泄露信息，都可能使大规模的个人隐私曝光，造成不可估量的损失。(2)大数据的快速传播和分析能力催生了精密的定向广告和个性化服务，但其也存在弊端，即对用户行为的密切监视，若这些数据落入不法分子手中，则可能会被滥用，如用于追踪、诈骗或侵犯用户权益[1]。另外，数据泄露和隐私侵犯会对个人心理健康造成影响，一旦个人的隐私受到侵害，就会导致其受到经济损失，甚至会引发心理上的恐惧与不安全感，对个人的社交和生活产生负面影响，导致心理疾病。

1.2　维护国家安全与经济稳定

大数据应用已经成为国家经济的重要支撑，其中涵盖金融、医疗、能源、交通等行业，但网络安全问题也可能导致金融欺诈、工业间谍行为、网络敲诈勒索等，这些现象会直接威胁到国家的经济稳定和可持续发展。其中，还涉及重要的基础设施，这是因为许多基础设施逐渐数字化、智能化，如电网、交通系统、水利设施等，它们的正常运行关乎生

收稿时间：2023-09-11
作者简介：郅逍遥(1987－)，硕士，助教，从事高职教育工作。

产和民生，一旦这些基础设施受到网络攻击，就可能会导致严重的事故和损失[2]。随着国家之间信息交流的日益频繁，网络攻击已经成为现代国家之间的主要竞争手段之一，政府、企业和组织都面临着网络攻击，如网络窃密、网络渗透、拒绝服务攻击等，严重影响着国家安全和社会稳定。

1.3 保障企业竞争力和商业利益

网络安全是企业竞争力的关键因素。在信息时代，企业的竞争力不仅取决于产品和服务的质量，更取决于数据的价值和应用。大数据分析为企业提供了深入了解市场和客户需求的能力，以优化产品设计、市场推广和客户服务，然而这些敏感数据如果被窃取或泄露，则会导致企业失去独特的竞争优势，丧失市场份额。为保护商业利益，需要预防网络攻击和数据泄露，勒索软件、雇员欺诈、供应链攻击等，都可能使企业的商业利益受损。例如，勒索软件攻击会导致企业系统瘫痪，无法正常运行，从而造成巨大的经济损失[3]。同时，数据泄露会揭示企业商业计划、破坏客户信任，甚至增加诉讼风险，严重影响企业的商业利益和声誉。另外，在大数据时代，企业面临着更多的合规要求，随着个人数据保护法规的不断加强，企业需要更加严格地管理和保护用户的个人信息，一旦违反法规，企业就可能面临巨额罚款和声誉损害，从而直接影响商业利益和市场声誉。

2 大数据网络安全防范策略

2.1 数据加密与隐私保护

数据加密可以有效防止未经授权的访问者读取或篡改数据，而隐私保护则着重于减少个人隐私的曝光和敏感信息的泄露。以某医疗保健机构的数据保护为例，在医疗保健机构中，对患者数据的保护尤为重要，因为其中包含着大量的个人信息，为确保数据加密和隐私保护的有效性，可以引入差分隐私技术，在保证数据统计准确性的前提下，加入噪音或扰动，使患者数据无法被关联到具体个人。而通过在大量匿名数据中的分析，医疗保健机构可以得出有关患者健康状况的结论，无需暴露个人敏感信息。还可以采用多层级的数据加密方案，确保数据在传输和存储过程中受到保护，并使用对称加密和非对称加密技术，对患者数据进行加密，确保数据在传输过程中不易被截获和解密。在数据存储中，还可对不同层级的数据设置不同的密钥和权限，以限制访问权限。此外，可以建立细粒度的数据访问控制策略，将数据访问权限控制为最低，使医疗保健机构内部员工和外部合作伙伴仅能访问其权限内的数据，而不是整个数据库，最大程度地减少数据泄露的风险。

2.2 威胁检测与风险评估

威胁检测与风险评估是网络安全防范的关键方法，通过及时发现潜在的威胁和评估安全风险，企业和组织可以采取预防措施，避免或最小化网络安全事件的发生。以金融机构的安全防范为例，在金融机构中，包含着大量敏感的财务和个人信息，使用机器学习算法，可以对用户的行为模式进行建模和分析，建立客户登录的典型行为模式，包括登录时间、地点、设备等，一旦发现异常行为，如来自陌生地点的登录尝试或异常的账户访问，系统就会自动触发警报并进行威胁检测。还可以与其他金融机构和安全组织建立情报共享合作机制，通过分享网络攻击事件和威胁情报，使金融机构更早地了解到新兴的网络威胁，并通过融合多方情报，对威胁进行更准确的评估和预测。同时，需定期对系统和应用程序进行全面的漏洞扫描和渗透测试，以发现并及时修补潜在的安全漏洞，减少攻击者的入侵路径，降低系统遭受攻击的概率。另外，还应建立实时的监控系统，对关键系统和数据进行持续监测，一旦发现异常行为或威胁事件，就应立即采取响应措施，如封锁恶意 IP 地址或停用被感染的账户，以防止进一步的安全威胁。

2.3 访问控制与身份认证

应用访问控制与身份认证，可以保证只有经过授权的用户才可以访问敏感数据和系统资源。传统的用户名和密码认证存在被猜测或被盗取的风险，通过引入多因素身份认证，如指纹识别、面部识别、硬件令牌等，可以大幅提高身份认证的安全性。多因素身份认证要求用户提供两个或以上不同类型的凭证，使攻击者难以突破多重安全屏障。传统访问控制通常基于静态的角色和权限，无法灵活适应不同场景的需求，而动态访问控制则通过实时监测用户行为，以进行风险评估，并根据用户当前的身份和行为来动态调整权限，确保用户在需要时才能获得相应的访问权限，以降低风险[4]。另外，应用零信任模型可以加强访问控制与身份认证，其认为不论用户是内部员工还是外部用户，都不能完全信任其身份，所有用户都需要进行身份认证，且在访问资源时持续验证，这种方法能及时发现异常访问行为，防止未经授权的访问和数据泄露。

2.4 网络安全意识与教育

人为因素是网络安全漏洞的主要来源，因此加强员工和用户的网络安全意识，提高其对网络安全威胁的认识，是防范网络安全风险的重要手段。为加强网络安全意识与教育，可以应用以下方法。(1)实施定期的网络安全培训和演练，通过组织网络安全培训，向员工和用户介绍网络安全知识，培训内容可以包括密码管理、社会工程学攻击识别、网络钓鱼识别等。(2)进行网络安全演练，模拟真实的网络安全事件，让员工和用户在实践中学习如何应对网络威胁，提高应对网络安全事件的能力。(3)借助游戏化的网络安全教育，设计有趣的网络安全游戏或挑战，让员工和用户在参与游戏的过程中学习网络安全知识。游戏化的教育方式能吸引人们的注意力，提高人们学习网络安全知识的积极性，增强其对网络安全知识的记忆和理解。(4)鼓励员工和用户积极参与网络安全讨论和知识分享，提高大家对网络安

全问题的关注和认知。内部网络安全社区可以提供一个开放的交流平台，让大家互相学习和帮助，共同提高网络安全意识。(5)组织网络安全宣传活动、发布网络安全警示通知，以提醒员工和用户了解网络安全的重要性，并利用企业内部媒体和社交平台，不断传播网络安全知识和最新威胁信息，增强网络安全意识的普及度和影响力。

3 大数据与网络安全的未来发展趋势

3.1 大数据与人工智能的结合

大数据与人工智能的结合，可以使网络安全防护更加智能化和自适应化。大数据技术可以帮助收集、存储和分析海量的安全数据，包括网络流量、日志、事件等。应用机器学习和深度学习算法，人工智能可以从这些数据中发现隐藏的威胁模式和异常行为，实现实时检测和预警，使网络安全防护能更加智能化地识别和应对新型的安全威胁。

大数据与人工智能的结合，将推动网络安全防护的自动化发展。传统的网络安全防护通常需要人工干预，以处理大量的安全事件和警报，但随着大数据和人工智能的融合，安全防护将越来越自动化，并能自动发现和应对威胁，减少对人力资源的依赖。自动化的网络安全防护还能提高应对速度和准确性，缩短安全事件的响应时间，从而减少潜在的损失。此外，通过对大数据的综合分析，人工智能可以预测潜在的安全威胁和风险，提前采取预防措施，避免安全事件的发生。预测性和预防性的网络安全防护，将有效减少安全漏洞和风险，为组织提供更加稳定、全面的网络安全保障。

3.2 区块链技术在网络安全中的应用

区块链的去中心化、不可篡改、高度安全等特性，使其成为保护大数据和网络安全的理想工具，随着该技术的不断发展和成熟，其将在网络安全领域扮演越来越重要的角色。以“去中心化身份验证系统”为例，传统的身份验证系统通常集中在单个中心服务器上，如果这个服务器遭受攻击或被黑客入侵，则会导致大量的用户数据和身份信息被盗用，但应用区块链技术，就可以实现去中心化的身份验证系统。此时，用户的身份信息将被加密并存储在区块链网络上的多个节点中，每个节点都有完整的身份信息备份，且需要通过共识算法来验证身份信息的准确性，当用户需要进行身份验证时，系统将通过区块链网络进行验证，而不再依赖单个中心服务器。如此，即使某个节点受到攻击，其他节点依然可以提供有效的身份验证，确保用户信息的安全性。区块链还可以用于加密数据的存储和传输，通过将数据加密并存储在区块链上，可以使数据免受未经授权的访问和改动。区块链的分布式特性还能提高数据的可靠性和冗余性，防止数据丢失或损坏。

3.3 新型威胁与应对挑战

在大数据与网络安全领域，新型威胁与挑战的未来发展趋势将更加复杂、多样化，随着技术的不断进步和大数据的广泛应用，恶意黑客和网络攻击者也会继续寻找新的方式来攻击和窃取数据。以“AI 攻击”为例，随着人工智能技术的快速发展，黑客和攻击者将越来越倾向于利用人工智能进行攻击，利用人工智能强大的计算能力和智能分析能力，攻击者可以更准确地识别网络弱点，发动更精密的攻击，甚至自动进行网络攻击，如 AI 攻击可以更有效地进行网络钓鱼攻击，伪造更真实的欺骗性信息，使用户更容易受骗。面对这一威胁，应将人工智能技术用于网络安全防御，实现“AI 防御”，利用人工智能强大的分析能力和实时监测能力，来对抗 AI 攻击。例如，AI 防御可以利用智能分析算法，及时识别并拦截可疑的网络活动和异常行为，它还可以实时更新网络防御策略，快速应对新型的 AI 攻击手段，增强网络的弹性和适应能力。此外，加强跨界合作与信息共享也是未来应对新型威胁的重要策略。网络安全威胁往往不受国界限制，攻击者可以来自全球各地，而各国政府、企业和组织需要加强合作，共同分享威胁情报和安全经验，通过建立跨界的信息共享平台，更及时地了解和应对新型威胁，形成联防联控的网络安全防护体系。

4 结语

随着科技的进步，网络威胁越来越复杂、隐蔽，对个人、企业和国家产生了严重的威胁，但许多创新的防范策略和技术的出现，如大数据与人工智能的结合，则为网络安全防护带来了新的可能。为保护个人隐私和数据安全，维护国家安全和经济稳定，人们需要不断加强网络安全意识与学习，推动法律法规与监管的完善，并积极应用大数据技术来创新防御手段。只有共同努力，汇集多方力量，才能建立更加安全、稳固的网络环境，让数字世界成为一个更加安全、可信的空间。

参考文献

[1] 梁超强.大数据时代计算机网络信息安全与防护研究[J].大众科技，2022，24(12)：1-3.

[2] 徐彬.网络安全对大数据信息技术应用的影响研究[J].网络安全和信息化，2022(12)：25-27.

[3] 万丽平.基于大数据视域的网络安全研究[J].电声技术，2022，46(12)：76-78.

[4] 李祺.大数据与网络安全技术分析[J].集成电路应用，2022，39(11)：222-223.