大数据时代下的工业互联网信息安全研究

邹　刚
（四川）产业互联网有限公司　四川　南充　637000

摘　要：大数据时代下，工业互联网作为新一代信息技术与制造业深度融合的产物，其信息安全问题日益凸显。本文深入探讨工业互联网在大数据环境中的信息安全挑战，包括数据泄露、网络攻击、隐私侵犯等风险。通过分析当前防护机制的不足，提出基于数据加密、访问控制、异常检测及云边协同防护策略的综合安全体系，旨在构建更加坚固的工业互联网安全防线，保障工业生产稳定与数据安全。

关键词：大数据时代；工业互联网；信息安全

1 工业互联网在推动制造业转型升级中的重要性

工业互联网作为新一代信息技术与制造业深度融合的产物，在推动制造业转型升级中扮演着至关重要的角色。第一，工业互联网通过集成大数据、云计算、物联网、人工智能等先进技术，实现了生产设备的互联互通和智能控制，使生产过程更加精准、高效。这不仅能够大幅提升生产效率，降低能耗和成本，还能实现定制化、柔性化生产，满足市场多元化、个性化的需求。第二，工业互联网平台能够实时收集和分析供应链各环节的数据，包括库存、物流、销售等信息，为企业提供全面的供应链可视化视图。这有助于企业精准预测市场需求，优化库存结构，减少库存积压，同时提高供应链的响应速度和灵活性，降低运营成本。第三，工业互联网促进了数据在产品设计、研发、制造、服务等全生命周期的流动与共享，为企业提供了丰富的数据源和创新灵感。基于这些数据，企业可以快速迭代产品，开发新产品和服务，提升产品竞争力，实现价值创造的新模式。第四，在工业互联网的支持下，制造业企业可以更加精准地控制生产过程中的能源消耗和污染排放，实现节能减排和资源高效利用。通过智能分析和预测，企业可以提前采取措施预防环境污染，推动制造业向绿色、低碳、可持续的方向发展[1]。第五，工业互联网打破了传统制造业的边界，促进了产业链上下游企业的紧密合作与协同创新。通过工业互联网平台，企业可以与其他企业、科研机构、高校等建立紧密的合作关系，共同推动技术创新和产业升级，构建开放、协同、共赢的产业生态。

2 大数据时代工业互联网信息安全现状分析

在大数据时代，工业互联网信息安全现状呈现出日益复杂和严峻的趋势。随着工业互联网的广泛应用和深入发展，其连接的设备数量、传输的数据量以及应用场景的多样性均大幅增加，这给信息安全带来了前所未有的挑战。工业互联网中涉及的海量数据，包括生产流程、产品设计、客户信息等敏感信息，一旦泄露或被非法利用，将对企业造成巨大的经济损失，甚至可能威胁到国家安全。数据泄露和隐私保护问题成为工业互联网信息安全的首要关注点。工业互联网系统通过互联网连接，使得其面临的网络攻击风险显著增加，恶意软件、网络钓鱼、DDoS攻击等手段层出不穷，攻击者可能利用工业互联网系统的漏洞，对生产系统进行破坏或控制，导致生产中断、设备损坏等严重后果。工业互联网的生态系统复杂多样，涉及多个供应商和合作伙伴，供应链的任何环节存在安全漏洞都可能被利用，从而对整个系统造成威胁。物联网设备的广泛应用也增加了安全管理的难度，这些设备可能存在安全漏洞，成为攻击者入侵系统的入口。

3 工业互联网信息安全问题分析

3.1 工业互联网信息安全面临的威胁与风险

工业互联网信息安全面临的威胁与风险日益严峻，这类威胁往往由专业黑客组织或国家背景的攻击者发起，他们利用复杂的攻击技术和策略，长期潜伏在工业互联网系统中，逐步渗透并窃取关键信息或破坏生产系统。APT攻击隐蔽性强、持续时间长，对工业互联网的安全构成重大威胁。业互联网中大量使用的物联网设备，如传感器、控制器等，往往存在安全漏洞。这些设备的安全防护能力相对较弱，容易成为攻击者入侵的跳板。一旦攻击者控制这些设备，就能对整个工业互联网系统造成严重影响。工业互联网的生态系统复杂，涉及多个供应商和合作伙伴。供应链中的任何一环出现安全漏洞，都可能被攻击者利用，对整个系统造成威胁。供应链攻击往往难以察觉和防范，给工业互联网安全带来巨大挑战。工业互联网系统中存储和传输的数据量巨大，包括生产数据、客户信息等敏感信息。一旦这些数据被

泄露或非法利用，将对企业造成重大损失，甚至可能引发法律纠纷，个人隐私的侵犯也是工业互联网安全不可忽视的问题。除了外部攻击者，企业内部员工或合作伙伴也可能对工业互联网系统构成威胁。内部人员的恶意行为或误操作都可能导致系统受损或数据泄露。

3.2 大数据环境下的信息安全漏洞与攻击方式

在大数据环境下，信息安全漏洞与攻击方式呈现出多样化、复杂化的特点。大数据平台中存储着海量数据，包括敏感的个人信息、商业机密等。一旦平台的安全防护措施存在漏洞，如未加密存储、访问控制不严等，攻击者就能通过非法手段获取这些数据，进而进行出售、勒索或用于不正当竞争。攻击者可能利用SQL注入、命令注入等技术，向大数据处理系统注入恶意代码或命令，从而控制或破坏系统。这种攻击方式能够绕过系统的正常安全检测，直接对后台数据库或服务器进行操作，危害极大。在大数据环境下，Web应用是数据展示和交互的重要渠道。攻击者可能通过XSS攻击，在用户浏览器中注入恶意脚本，窃取用户信息、篡改网页内容或进行钓鱼攻击等。大数据平台往往需要处理来自海量用户的请求，这使得其成为DDoS攻击的理想目标。攻击者通过控制大量僵尸网络或利用物联网设备的漏洞，向大数据平台发送大量无效请求，导致平台资源耗尽，无法正常提供服务。除了外部攻击者，大数据环境下的信息安全还面临来自内部的威胁。企业内部员工或合作伙伴可能出于个人利益或恶意目的，滥用或泄露敏感数据。这种威胁往往难以防范，需要企业加强内部管理和监控。在大数据分析中，数据的真实性和准确性至关重要。攻击者可能通过篡改或伪造数据的方式，干扰分析结果，误导企业决策。这种攻击方式隐蔽性强，难以察觉，需要企业建立严格的数据验证和审计机制[2]。

3.3 工业互联网信息安全对生产运营的影响

工业互联网信息安全对生产运营的影响深远且重大，直接关系到企业的稳定运行、经济效益乃至市场竞争力。一旦工业互联网系统遭受安全威胁或攻击，可能会引发一系列连锁反应，对企业生产运营造成严重影响。信息安全漏洞和攻击可能导致生产系统中断或失控，工业互联网系统集成了众多生产设备和控制系统，这些系统的稳定运行是保障生产连续性的关键。一旦系统遭受攻击，如恶意软件感染、控制指令篡改等，就可能导致生产线停机、设备故障甚至安全事故，给企业带来巨大经济损失和声誉损害。数据泄露和非法获取会危及企业的商业机密和客户隐私，工业互联网系统中存储着大量敏感数据，包括生产计划、产品配方、客户信息等。这些数据一旦泄露，不仅可能导致企业失去竞争优势，还可能面临法律诉讼和巨额赔偿，客户隐私的泄露也会损害企业的品牌形象和市场信任度。信息安全问题还可能影响企业的决策效率和准确性，在大数据时代，数据分析是企业决策的重要依据，如果数据被篡改或伪造，就会导致分析结果失真，误导企业决策。

4 工业互联网信息安全解决方案

4.1 工业互联网信息安全架构设计

工业互联网信息安全架构设计是确保生产运营安全稳定的基础。一个全面且高效的安全架构应涵盖多个层次，以实现多层次、多维度、多重防护的目标。作为工业互联网安全架构的底层，感知层部署了各类传感器、设备和系统，实时采集网络流量、系统日志、安全事件等数据。这些数据为后续的安全分析和决策提供了基础。通过部署工业防火墙、入侵防御系统等设备，感知层能有效识别并阻止潜在的网络攻击。分析层利用大数据分析、机器学习、人工智能等先进技术，对感知层收集的数据进行深入分析。通过智能算法，分析层能够发现网络攻击、安全漏洞、异常行为等安全威胁，并及时发出预警，态势感知系统的引入，使得企业能够实时掌握工业互联网系统的安全态势，为决策提供有力支持。在发现安全威胁后，响应层迅速采取相应措施，包括隔离受感染设备、阻断网络攻击、修复安全漏洞等。自动化响应机制的建立，大大提高了响应速度和效率，减少了人工干预的延迟和错误。管理层负责工业互联网安全架构的统一管理和控制。通过制定安全策略、处理安全事件、进行安全审计等工作，管理层确保整个安全架构的有效运行，管理层还负责与其他安全系统（如企业IT系统）的集成和协同，形成整体安全防护网。

4.2 大数据安全处理与隐私保护

在工业互联网环境中，大数据的安全处理和隐私保护是至关重要的。采用先进的加密技术，如AES、RSA等，对敏感数据进行加密存储和传输，这些技术能够有效防止数据在存储和传输过程中被窃取或篡改，企业还应对加密密钥进行严格管理，确保密钥的安全性和可用性。对于需要共享或外发的数据，企业应进行脱敏处理。通过替换、掩码等方式，将敏感信息转换为非敏感信息，以保护个人隐私和商业机密[3]。引入差分隐私、联邦学习等隐私保护技术，在保障数据分析效果的同时，保护个人隐私不被泄露。这些技术允许企业在不直接访问原始数据的情况下，对数据进行统计和分析。企业应遵循相关法律法规和行业标准，如GDPR、HIPAA等，建立完善的数据保护政策和流程。通过定期进行合规性审

查和审计，确保企业在数据处理和隐私保护方面符合法律要求。

4.3 安全审计与监控技术在工业互联网中的应用

安全审计与监控技术是提高工业互联网系统安全性和稳定性的重要手段。通过实时监控和定期审计，企业能够及时发现并处理潜在的安全威胁。部署入侵检测与防御系统（IDS/IPS），对工业互联网系统的网络流量进行实时监测和分析。通过识别异常流量和攻击行为，系统能够及时发出预警并采取防御措施。建立完善的日志审计系统，对系统操作、用户行为、安全事件等进行全面记录和分析。通过定期审计和查询日志，企业能够追溯安全事件的原因和过程，为后续的安全改进提供依据。在关键网络节点部署流量监测探针，采集网络流量并进行预处理和预检测。将预处理后的数据传输到态势感知平台进行分析，以洞察全网安全态势。通过整合各类安全设备和系统的日志和事件信息，安全态势感知平台能够实时展示工业互联网系统的安全态势。利用可视化技术，平台能够直观展示安全威胁的分布和趋势，帮助安全管理人员快速做出决策。

5 大数据时代下信息安全技术发展趋势

大数据时代下，信息安全技术正经历着快速而深刻的发展趋势，这些趋势不仅反映了技术进步的必然方向，也体现了对日益复杂安全挑战的积极应对。随着人工智能、机器学习等技术的不断成熟，信息安全系统将具备更强的自我学习和自适应能力。它们能够自动识别和响应安全威胁，从而大大提高安全防护的效率和准确性。在大数据时代，个人隐私保护成为社会各界关注的焦点。为了平衡数据利用与隐私保护之间的矛盾，新的隐私保护技术不断涌现，如差分隐私、联邦学习等。这些技术能够在保护个人隐私的同时，实现数据的共享和计算，为数据安全和隐私保护提供了新的解决方案。随着云计算和边缘计算的广泛应用，云安全和边缘计算安全成为信息安全领域的新挑战。云安全将更加注重数据的加密存储、访问控制、安全审计等方面；而边缘计算安全则需要解决设备安全、网络通信安全、数据隐私保护等问题[4]。未来，云安全与边缘计算安全将形成互补，共同构建更加完善的安全防护体系。零信任安全架构强调“永不信任，始终验证”的原则，要求对所有访问都进行身份验证和授权。这种架构能够有效防止内部威胁和外部攻击，提高整体安全防护水平。随着企业对安全性的要求不断提高，零信任安全架构将得到更广泛的应用。信息安全问题涉及多个领域和方面，需要跨学科、跨领域的合作与创新。未来，信息安全技术将与其他领域的技术（如物联网、区块链、5G等）深度融合，共同推动信息安全技术的创新与发展，企业、政府、科研机构等各方也将加强合作与交流，共同应对信息安全挑战。

结束语

随着大数据技术的持续革新，工业互联网的信息安全防御需不断创新与进化。本文虽就当前主要问题提出了若干解决思路，但面对未来更加复杂多变的网络环境，仍需深化技术研究，加强行业协作，共同推动安全标准的制定与实施。通过持续优化安全防护体系，有信心筑牢工业互联网安全基石，促进数字经济与实体经济深度融合，推动制造业高质量发展。

参考文献

[1]周天成.大数据时代下的工业互联网信息安全研究[J].上海管理科学,2021,43(6):110-112,119.DOI:10.3969/j.issn.1005-9679.2021.06.019.

[2]陈雪鸿,杨帅锋,张雪莹.浅谈工业互联网数据安全防护[J].自动化博览.2021,(1).15-17.

[3]孙念,傅为政.基于大数据的工业互联网安全分析[J].数字通信世界.2020,(5).DOI:10.3969/J.ISSN.1672-7274.2020.05.083.

[4]王冲华,李俊,陈雪鸿.工业互联网平台安全防护体系研究[J].信息网络安全.2019,(9).6-10.DOI:10.3969/j.issn.1671-1122.2019.09.002.