工业互联网网络数据安全分析与研究

文◆中国石油大庆油田有限责任公司数智技术公司　张　宇

引言

近年来，国内外研究人员非常重视工业互联网的研发工作，在工业互联网中充分运用物联网、SDN 以及 5G 技术，从而打造出可靠性高、延迟问题小、覆盖范围大的工业互联网，其中网络数据安全问题成为工业互联网研究中的主要内容。随着数据泄露和网络攻击的增加，安全和隐私变得更加重要。企业需要在 IT 生命周期的各个阶段考虑安全措施，包括数据加密、身份验证和访问控制。

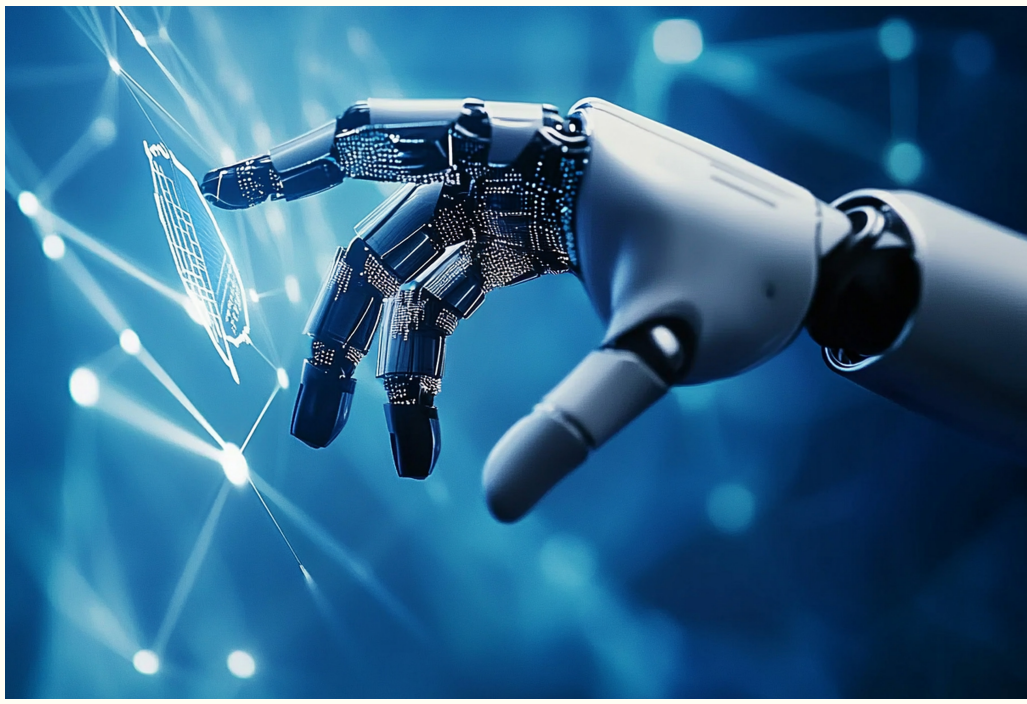
1 工业互联网的研究背景

在工业互联网应用过程中，利用设备、传感器组态网实时传输企业信息，安全问题显得尤为重要。企业应研发满足工业互联网发展需求的安全保护技术，加大工业互联网的安全防护力度，确保工业互联网能够抵御网络攻击，并安全运行。因此，企业技术人员参照我国推出的《信息安全技术网络安全等级保护要求》和《中华人民共和国数据安全法》，将企业安全防护工业互联网的方式划分为 5 个方面，即设备安全方面、控制安全方面、网络安全方面、应用安全方面和数据安全方面 [1]。

有专家学者提出，使用计算复杂度取代工业互联网以往使用的状态复杂度，借助智能数据协助技术人员开展数据选择和数据关联分析工作，及时解决工业互联网当前面临的网络问题，提高工业互联网的网络服务质量。通过工业互联网加强访问控制、检查网络入侵情况、设置病毒防治方案等，针对工业互联网异构系统流量分析情况，设置具有针对性的安全防护措施，在工业互联网出现异常行为时进行问题追溯，及时检查存在的网络异常问题，并发出预警，以便于工作人员维护工业互联网安全。

2 工业互联网的网络数据分析方式

工业互联网主要由信息物理系统、物联网、云计算构成，新技术和架构的引入也带来了新的威胁和攻击表面。例如，物联网和边缘计算的兴起增加了设备和数据的暴露风险，而区块链的普及可能引发分布式系



【作者简介】张宇（1989—），女，黑龙江大庆人，本科，工程师，研究方向：网络安全。

统的新安全问题。为了使异构网络能够顺利完成数据处理工作，应创建统一的交互操作模型，并利用新技术和架构使数据更加有价值，但同时也使数据变得更敏感，因此需要采取严格的保护措施来防止数据泄露和滥用。

2.1 使用大数据平台收集异构多源数据

企业应创建工业互联网监控系统，对工业互联网上传的异构数据、多源数据展开全面分析，依照预测结果动态优化企业的生产规划，保证工业网络能够满足动态制造需要。企业可以从提高设备自动化水平、建设智能工程的角度着手，建设科学的编码、规范的技术、统一的标准，以便能够与其他信息系统或将来建设的信息系统互联，实现系统的集成和数据的一致。在此基础上，借助已有数据接口创建更为高效的网络数据采集系统，全面采集行业数据，对企业生产情况展开实时监控管理，使得与工业互联网相连接的智能设备能够顺利完成数据互通传输[2]。

通过融合采用具备可落地性的解决方案及技术架构，选用符合企业信息化发展需求的软硬件产品，确保系统的建设应用，可以使企业自动化生产线和设备实现数字化发展目标。在工业互联网的支持下，大数据平台能够实时采集设备运行信息、机床运行状态、机床加工情况和程序信息等，并将这些数据信息统一汇总在数据库中，为后续信息利用提供便利性。

2.2 工业数据建模、大数据分析

近年来，大数据批处理框架、流处理框架已经大面积运用在处理海量数据中。各种机器检测系统已涵盖资产管理业务、数据出境安全评估业务、数据监测业务、特定场景的数据安全保护业务等。结合数据安全管理办法所提升的安全评估、监测、保护及管理能力，可以借助大数据算法进行数据内容技能型分析，实时分析共享数据的共享情况，并对数据进行深层次的挖掘研究，充分发挥工业发展数据资源的价值[3]。

3 加强工业互联网网络安全的方式

3.1 寻找攻击源

在工业互联网受到网络攻击的过程中，工作人员应重点分析网络数据包，重构工业互联网收集清洗、统计分析、数据建模、风险预测，实现对数据安全的管理集中化、监测可视化。在建设好 IT 攻击特征模型架构后，寻找合适的匹配算法，针对恶意网络攻击设置安全防范方式，不断提高工业互联网的网络安全。

3.2 工业互联网流量降维方式

工业互联网通过预处理网络数据能力在一定程度上降低网络数据安全分析的复杂程度。因此，企业应提高对特征选择方式的重视程度，对网络数据的流量特征进行排序，依照安全问题紧急程度确定处理顺序，借助流量降维方式进一步提升工业互联网的应用安全性。

3.3 创建工业互联网安全事件溯源模型

在工业互联网应用过程中，应将企业的商密数据、员工个人信息以及数据安全业务单位所认定的重要数据作为监管对象。在满足国家对数据安全评估、监管要求的基础上，提供数据资产梳理、数据安全检查等服务。通过对数据的监测及业务分析，实现对数据流动监测、内容合规性鉴别、数据流向定位。同时，通过数据监测管理模块进行综合数据分析，实现数据安全管理集中化和监测可视化。为了构建一个更完善、合理、合规且合法的工业互联网安全事件溯源模型，需要确保数据的可知性、可见性和可管性，从而实现数据的合规性、安全性、保密性和可用性目标。为此，将从数据安全的事前风险发现与评估、事中的安全风险监测及安全保护、以及事后的安全响应这 3 个层次、4 个方面来设计建设方案，以形成对工业互联网数据的全面安全管理。

结语

在应用工业互联网后，有利于进一步提升企业的生产效率，但同时也面临着网络攻击带来的数据安全风险，故企业应加大对工业互联网的安全防护力度，使用大数据平台收集异构多源数据。在开展工业数据建模、大数据分析工作的同时，寻找攻击源，并使用工业互联网流量降维方式，创建工业互联网安全事件溯源模型，及时处理工业互联网存在的网络安全问题，不断提高工业互联网在企业数据安全传输中的应用效果。

引用

[1] 肖风超.工业互联网网络数据安全分析与研究[J].数据通信,2022(3):19-21+49.

[2] 邓梦茹.大数据技术在网络安全分析中的应用研究[J].无线互联科技,2021,18(12):19-20.

[3] 杨承.互联网时代的网络数据安全分析[J].电子技术与软件工程,2020(9):258-260.