ISSN:2705-0408(P)；2705-0416(O)

基于生成式人工智能的工业互联网安全技术应用

韦　滨
广东行政职业学院　广东广州　510000

摘　要：工业互联网作为目前新型工业化核心基础设施，当前面临着各类新型的网络威胁，如传统防护手段勒索软件和零日漏洞等风险。生成式人工智能凭借数据驱动 + 智能决策优势，可以重构安全防护体系，实现互联网威胁检测、漏洞预警和应急响应的效能提升。本文围绕生成式人工智能对工业互联网安全技术的重要性以及相关策略，为工业互联网安全防护提供可落实的解决方案。

关键词：生成式人工智能；工业互联网；安全技术应用

如今，工业互联网已深入融入国民经济的关键领域，但网络安全风险问题，传统的防护体系仍存在检测滞后、漏洞管理被动、以及数据协同不足等相关问题，让其难以适配复杂的安全需求。而生成式人工智能能通过智能化检测、前瞻化预警和自主化响应，突破传统防护局限，有效提升工业互联网安全防护的主动性和效率。基于此，本文从技术落地角度，提出几大应用策略，为解决工业互联网安全痛点提供新思路。

1 生成式人工智能的工业互联网安全技术的重要性

工业互联网已经深入到制造业、能源和交通等国民经济重要行业，其安全性事关企业的持续发展和社会公众的福祉。目前，网络攻击已呈现智能化和隐蔽化的特点，如一些攻击者冒充普通的工业命令侵入或通过供应链漏洞进行连锁攻击，而基于静态规则和人工巡检的传统保护方法，不但很难对其进行实时监测，而且由于工业场景中 IT 与 OT 之间的网络数据割裂，攻击路径很难被完全追溯，最终造成生产线停工和设备损毁等重大事故，因此，防护技术的革新显得尤为紧迫。

而基于生成式的人工智能技术为工业互联网的安全性研究带来了新的突破：突破了事后响应的局限性，生成式人工智能可以通过整合多维度工业大数据，实现构建安全威胁建模和异常行为特性，比如预先发现装置参数微小的异常变化以预警隐患，或者当受到攻击时迅速形成符合工业安全要求的防护措施，从而达到“事前预警，事前拦截”的目的。以智能工厂为例，利用生成式人工智能技术，实现对防护策略的实时优化，防止人为调节滞后造成的安全漏洞，从而有效提高工业系统对复杂环境的应对能力，为确保工业互联网的平稳运行提供重要的支持 [1]。

2 生成式人工智能的工业互联网安全技术应用策略

2.1 基于生成式人工智能的工业控制系统异常行为动态检测模型

工业控制系统（ICS）的安全关键是辨别设备正常操作和恶意行为，传统检测依靠预先设定的规则，很难适用于多个工业场景环境下的协议特征，对隐藏的异常如参数微幅篡改、协议字段隐藏等缺乏辨识能力。在此基础上，以生成式人工智能为基础的动态监测模型，从设备操作指令、传感器参数、网络通信特征等多维信息中提取出符合实际生产环境的常规行为基准。该模型提出一种不需要人工确定威胁规则，能够与基线进行实时比较，准确地捕获偏离特性，并通过持续学习生产过程的动态演变：如换产、设备维修等来进行基线的更新，从而有效地克服了以往的“虚警率高、漏报率高”的问题，从而为工业控制系统领域构筑起一道实时保护的防线。

例如，在实际应用中，某家汽车公司焊接车间的真实案例颇具代表性。该车间之前使用的是传统的防火墙和人工巡检方式，曾经因为不能辨识出隐藏在焊缝中的恶意参数而造成了多个焊接机器人的非正常停机。在引入生成式人工智能动态检测模型后，系统先学习了不同车型焊接作业的正常参数范围与指令交互规律，在一次生产制造过程中，该模型发现某台机器人当前的工作电流参数虽然没有超过安全临界值，但是其改变的参数频率却超过了指令的发射间隔偏离基线，从而引发了警报。经过技术人员调查，

发现这种异常是攻击者为了干扰焊接精确度而修改了上位机的指令，并将其进行了有效的风险拦截，从而防止了产品报废和生产线的停工，从而证明了这种方法的可行性和可靠性 [2]。

2.2 生成式人工智能驱动的工业互联网安全漏洞预测与响应机制

目前，工业互联网上的漏洞管理大多停留在检测到漏洞再进行修补的落后局面，主要依靠现有的漏洞数据库进行更新，很难应对设备异构和特殊协议的工业场景，并且需要人工调整到不同的工业系统，导致维修时间过长。生成式人工智能可以通过对漏洞数据、设备运行日志和协议特性学习分析，建立漏洞 – 攻击路径之间的关联模型，实现对可能存在的漏洞如设备固件缺陷、协议逻辑漏洞的预测，突破只能知道漏洞而不能防守的局限性。在漏洞响应过程，它可以针对工业装备的工作状况和安全性要求，自适应地生成相应的维修计划，如配置调整、补丁适配建议等，并协同保护设备迅速实施，从而大大减少了漏洞处理的时间，减少了被利用的危险 [3]。

例如，某家汽配工厂的智能化生产线曾经出现过一次故障，就是因为没有对机械臂的操作软件漏洞及时修补，造成了多台设备暂时失去了控制，从而影响了整个生产线的正常运转。在引进了生成式人工智能漏洞机制上，系统将对生产线上的装备漏洞历史和运营数据进行持续分析，并对某型号的机械臂存在的固件漏洞风险进行预警，并在此基础上形成不需要停机的补丁适配方案，并将其发送到控制终端和后台。在此基础上，保证产线正常运转，降低人工排查和维修费用，具有较高的实际应用价值。

2.3 工业互联网安全数据增强与隐私保护的生成式人工智能应用策略

工业互联网的安全防护主要依靠海量有标注数据训练模型，然而在实际生活中，异常攻击样本、设备漏洞日志等安全数据存在着标记数量小、标记困难等问题，如果直接共享容易引发用户的隐私泄漏风险，从而限制了跨场景和企业间的安全数据协作。基于此，生成式人工智能提出一种基于对抗产生网络技术（GAN）的仿真工业场景的安全数据，以弥补现实中的实际数据缺失，提高其推广能力。同时，结合联邦学习和差分隐私等技术，使生成式人工智能在数据不远离本地的情况下，自动进行建模，达到数据可用不可见的目的，从而在保护隐私的同时，能整合多方的安全数据优势 [4]。

例如，某区域新能源动力电池产业集群过去由于害怕制造工艺中的数据泄漏，很多企业都不愿意将其存储在电池车间中的设备安全日志进行共享，从而使得现有的安全模型只能对本地常见威胁进行辨识，无法有效应对来自跨企业之间的新的网络攻击。在此基础上，采用基于生成式人工智能的方法，利用 GAN 产生模拟的电池充电和放电的异常数据，对其进行自适应训练学习。在此基础上，企业利用实际和产生的数据共同进行局部建模，只对模型的参数进行共享。最终在无信息泄露的情况下，对集群中的企业进行安全隐患辨识，使其在保证用户信息使用和用户隐私保护两个方面取得较好的效果。

2.4 生成式人工智能在工业互联网安全合规性与风险管理中的实践路径

工业互联网的安全合规涉及到数据分类、跨境传输、设备安全等多个方面的法律规范，例如数据安全法等。同时，由于生产过程中存在着大量的不确定性，使得设备和数据中潜在的风险进行实时评估是非常困难的。生成式 AI 可以通过对合规文本的解读和企业业务流程的映射，实现合规清单和治理意见的自动化产生，并对工业的运营数据进行动态追踪，并对其进行更新风险登记，以应对人工合规和风险管理响应速度慢、覆盖范围窄等问题 [5]。

例如，某汽车整车厂在过去需要人工完成对供应链数据的符合性需求，需要两个星期的时间才能完成，并且很难与新修订的汽车数据安全管理规范相适应。在引进了生成式人工智能之后，该系统会对相关的法律条款自动分解，并对零部件采购和数据传输进行匹配，一日之内就能完成符合条件的核对；在此基础上，通过对供应商的数据交换进行实时监测，一旦发现境外的供应商数据在没有备案的情况下，及时发出警告和推送备案流程建议，从而大大减少合规工作时间，规避了违法风险，从而有效地提高了合规和风险管理的效率 [6]。

3 结束语

生成式人工智能对于企业来说，工业互联网安全技术可以稳定根基，有效突破传统防护的痛点，助力构建主动防护体系，为其安全高效的发展奠定基础。

参考文献：

[1] 王和龙 , 宋静鹏 , 李聪 . 人工智能技术在工业互联网信息服务安全评估中的应用 [J]. 电声技术 , 2022, 46 (11): 70–73.

[2] 郭刚 , 林紫微 , 杨超 , 等 . 工业互联网网络体系安全防护研究 [J]. 信息安全与通信保密 , 2022, (09): 9–17.

[3] 白彦茹 . 工业互联网企业网络安全分类分级防护探索 [J]. 工业信息安全 , 2023, (06): 80–87.

[4] 曹天杰 , 鲍宇 . 基于生成式人工智能技术的网络安全教学实践 [J]. 科教文汇 , 2024(15):77–81.

[5] 董耀聪 , 张倩 , 李宝强 , 等 . 基于生成式人工智能的工业互联网安全技术与应用研究 [J]. 信息通信技术与政策 , 2024, 50(8):32–37.

[6] 陶彧 , 唐珂 , 陈玉峰 , 等 . 生成式人工智能服务技术特点与应用研究 [J]. 通信与信息技术 , 2024(2):108–110.