 DOI: https://doi.org/10.12349/iser.v6i6.6047

Research on anomaly behavior recognition and security control technology of industrial sensitive data driven by artificial intelligence

Huiming Wu Huasong Jin

Fujian Zhongxin Network Security Information Technology Co., Ltd., Fuzhou, Fujian, 350011, China

Abstract

With the rapid development of the industrial internet, industrial data is experiencing explosive growth. Industrial sensitive data, a core asset for enterprises, includes critical information such as product design blueprints, production process parameters, and customer information, which are essential for the survival and development of enterprises. However, the increasing complexity of the industrial environment and the evolving methods of cyber attacks pose unprecedented security challenges to industrial sensitive data. Artificial intelligence (AI) technology, with its robust capabilities in data analysis, pattern recognition, and intelligent decision-making, offers new solutions for protecting industrial sensitive data. By learning from large volumes of behavioral data within industrial systems, AI can establish normal behavior models, accurately identify abnormal behaviors, and provide real-time protection for sensitive data. Therefore, it is crucial to conduct in-depth research on AI-driven technologies for identifying abnormal behaviors and managing security risks associated with industrial sensitive data.

Keywords

artificial intelligence; industrial sensitive data; abnormal behavior identification; security management technology

人工智能驱动的工业敏感数据异常行为识别与安全管控技术研究

吴慧明 金华松

福建中信网安信息科技有限公司，中国 · 福建 福州 350011

摘 要

随着工业互联网的快速发展，工业数据呈爆发式增长。其中，工业敏感数据作为企业的核心资产，涵盖产品设计蓝图、生产工艺参数、客户信息等关键内容，对企业的生存与发展至关重要。然而，工业环境的日益复杂和网络攻击手段的不断演进，使工业敏感数据面临前所未有的安全挑战，人工智能技术，以其强大的数据分析、模式识别和智能决策能力，为工业敏感数据的安全防护提供了新的途径。通过对工业系统中大量行为数据的学习，人工智能能够建立正常行为模型，精准识别异常行为，实现对敏感数据的实时保护。因此，深入研究人工智能驱动的工业敏感数据异常行为识别与安全管控技术具有重要的现实意义。

关键词

人工智能；工业敏感数据；异常行为识别；安全管控技术

1 引言

随着工业互联网的迅猛发展，工业系统与外部网络间的互联程度越来越高，受到的攻击范围也越来越广，行业内的敏感数据受到了空前的威胁。传统的防火墙和 IDS 等安全防御手段在面对新型复杂的网络攻击时越来越显示出其局限性。随着人工智能的快速发展，对工业领域内敏感信息的保护提出了新的要求。人工智能在大数据处理与模式识别方面具有极强的优势，可从大量工业大数据中自动学习常态行为，并精确辨识异常行为，对提高整个工业系统的安全稳定运行具有重要意义。

2 工业敏感数据概述

2.1 工业敏感数据定义与范畴

在工业生产运营过程中会产生并使用大量的工业敏感数据，这些数据如果被泄露、篡改或被滥用，将会给企业、行业甚至国家带来巨大的不利影响，其包含了一些重要的信息，如设计图、技术专利等、生产工艺数据（工艺配方、设备参数）、供应链数据（供应商信息、物流订单）、客户数据（交易记录、需求偏好）、经营管理数据（财务报表、战略规划）等。

2.2 工业敏感数据安全现状与挑战

当前，工业敏感数据面临着诸多安全威胁，主要体现

在以下几个方面：

网络攻击手段多样化：工控系统安全漏洞、网络协议漏洞等是黑客的主要攻击手段，比如高级持续威胁（APT），具有隐蔽性强、持续性强、不易被及时检测与预防的特点，难以被及时发现和防范，可窃取大量敏感数据。例如，震网病毒可以瞄准工控系统，通过 USB 传播，从而摧毁了一些重要的工业设施，并盗取关键的生产数据。

内部人员违规操作：一些员工由于缺乏安全意识和利润的驱动，会无意或有意地泄漏机密数据。例如，员工将包含机密数据的档案透过外部电邮传送给他人，或是在网路上使用非安全性的工作数据。

数据共享与第三方风险：当工业企业与其他企业进行数据共享时，如果不能对其进行有效的安全管理，那么在传递和保存过程中，数据很容易被泄漏。比如，一些企业会把重要的生产数据外包没有足够的安全保护的数据分析企业来处理，若该企业安全防护不足，数据可能面临风险。

新兴技术应用带来新风险：随着 5 G、云计算、边缘计算等新兴技术的广泛使用，工业数据的传输与存储环境变得更加复杂，传统的工业数据处理方法难以满足日益增长的需求。例如，5 G 的高速、广连接性等特点，会引发更多的黑客攻击，云计算中的多租户环境又会带来数据隔离等问题[1]。

3 人工智能驱动的异常行为识别技术

3.1 用户行为建模与异常检测

3.1.1 正常行为模型构建

采用机器学习的分簇方法与深度学习神经网络相结合的方法，从企业员工、合作伙伴等多个角度，对工业生产过程中用户（员工、合作伙伴等）的操作行为数据进行学习。其中包含了多个方面的数据，如登录时间、系统模块、操作频率、下载数据等。比如，利用 K-Means 聚类算法，将员工对产品信息的存取行为进行聚类，把行为模式相近的员工分组，并针对不同群体建立常态行为模型。另一种方法是利用 LSTM 神经网络对用户行为序列进行模型化，并从中学习出常规作业流的时序特性。

3.1.2 异常行为识别

针对新用户行为数据，会计算出与一般模式之间的偏差。如果偏差超出了设置的阈值，就被确定为异常行为。比如，当员工在非工作日频繁地下载大量的敏感生产数据，并且这些数据与所在的群组的常规行为有明显的不同时，就会得到警告。可以通过欧氏距离和马氏距离等测量手段，研究基于深度网络的数据融合算法，并利用训练样本的可信度来判定系统的异常行为。

3.1.3 模型动态更新

为了确保模型的精度与效率，在实际生产过程中，经常需要利用新的行为数据对其进行更新。比如，每月将过去一个月内的用户行为数据加入到训练集中，然后对这个模型进行再培训，使其能够在新的工作方式、业务流程的变动以及员工的变动等方面得到更好的应用。

3.2 网络流量分析与异常识别

3.2.1 流量特征提取

运用深度学习技术对工业网络流量数据进行分析。首先，对网络数据包进行分析，包括源 IP 地址、目的 IP 地址、端口号、协议类型、数据包大小、流量速率等。比如，利用卷积神经网络来处理网络流量数据，可以从网络数据中自动提取出这些特性的高级表示，并捕捉其中的复杂模式。

3.2.2 异常流量模式识别

通过训练深度学习模型，学习正常网络流量的模式。在新的流量数据出现时，该模型将判定它是否与已学习的正常模式相一致。比如，利用自编码器（AE）模型，对正常流量数据进行编、解码训练，使之可以重建正常流量数据。当遇到异常流量时，自编码器的重建误差将明显增加，并能有效地识别出异常流量。此外，还可利用生成对抗网络，生成器生成正常流量数据，并将其与已产生真实正常流量、异常流量进行区别，并通过判别器对新流量数据进行判定，从而实现对异常流量的识别。

3.2.3 实时监测与预警

建立实时网络流量监测系统，对网络业务进行持续的采集与分析。当发现异常流量时，系统会即时警报，并给出相应的流量来源、流向、流量特性等信息，使安全人员能够及时采取相应的对策。比如，可以通过与防火墙和入侵检测系统等安全设备的连接来阻断网络中的异常数据流。

3.3 设备行为分析与故障预测

利用传感器等设备对工业设备进行温度、压力、振动、转速等工作参数的采集。对采集到的数据进行清洗、预处理，剔除噪声、异常值，使数据格式统一。比如，利用移动平均滤波算法消除数据中的噪声波动，并利用归一化的方法把多个传感器采集到相同的数值区间，方便以后的分析。

同时，采用机器学习、深度学习等方法，对采集到的

【基金项目】福州市科技创新创业人才培育计划项目－工业领域敏感数据资产安全管控关键技术研究及应用（项目编号：2023-R-006）；福州市科技计划项目－对外合作项目“基于零信任的数据安全管控系统关键技术研发及应用”（项目编号：2024-Y-013）；福州市科技计划项目—高校科研机构联合创新创新项目“AI 驱动的 APT 攻击检测与防御关键技术应用研究”（项目编号：2024-SG-005）；福建省科技计划项目—高校产学研合作项目“基于智能可信区块链的数据安全监测防护装置关键技术研发及产业化”（项目编号“2024H6008”）；福州市科技计划项目—科技重大项目“基于数字孪生的网络空间测绘与数据动态溯流关键技术研发及产业化”（项目编号：2023-ZD-003）。

【作者简介】吴慧明（1981－），男，中国福建政和人，本科，工程师，从事数据安全、网络安全研究。

设备运行数据进行模型化，以获取其在正常工作条件下的行为规律。比如，采用高斯混叠模型（GMM）对装备的振动数据进行建模，将其按正态分布分解成多个高斯分布格式，每一种正态分布表示一种常态工况。利用深度置信网络（DBN）对多源传感数据进行联合建模，获取多种工作状态下的综合运行特性。

最后，基于所建立的设备正常行为模型，对设备的运行状态进行实时监控，并对其进行异常行为识别。如果该设备行为与正常模式不一致，则被确定为异常。同时，通过对设备运行过程中出现的异常现象进行分析，并对其发展趋势进行预测，从而对可能出现的故障进行预警。比如，采用 ARIMA 模型等时间序列分析方法，对设备操作参数的时序进行预测，如果预测值与实测值之间存在较大的偏离，且持续超过一定时间，就表示有可能出现设备失效问题。

4 人工智能驱动的安全管控技术

4.1 智能访问控制

4.1.1 动态权限管理

基于人工智能技术的访问控制系统，能够依据用户实时行为特征、身份信息、设备运行状态以及网络环境条件等多维度因素，动态调控用户对工业敏感数据的访问权限。例如，当系统侦测到使用者通过陌生设备登入，企图存取高度敏感的数据，便会利用机器学习模式进行风险评估。如果评估结果是危险程度较高，那么系统就会对使用者进行限制，例如只允许使用者浏览部分数据，而不能进行下载、修改等。另外，系统也会与使用者的历史行为数据相结合，如果发现使用者平常并不经常存取这类敏感数据，则此异常存取行为将会启动附加的认证过程，如短信验证码验证、指纹识别验证等 [2]。

4.1.2 风险评估与决策

采用深度学习方法，融合用户行为数据、设备安全状态数据和外部威胁情报数据，建立风险评估模型。该模型可以对用户的接入请求进行动态评价，从而为接入控制策略的制定提供参考。比如，把用户的登录位置、登录时间、登录次数和数据操作类型等信息作为输入变量，利用所建立的深层神经网络模型进行风险评估。如果该风险值超出一定的阈值，那么该系统就会拒绝该接入申请，并且会将有关的信息记录下来供后续的审核。此外，利用已有的风险事件数据，持续地对风险评估策略进行优化，以提升评估的精度与可信度。

4.2 数据加密与脱敏

4.2.1 智能加密策略制定

人工智能可以根据数据的敏感程度、应用场景和访问频率等因素，自动选择合适的密码算法和密钥管理机制。比如，对于敏感而又不常用的产品数据，选择 AES-256 这样的高安全性密码算法，并设计严格的密钥管理机制，比如定期更换密钥、使用多因素认证等。针对一般敏感和高存取率的数据，利用 ChaCha20 等轻量级但效率较高的加密算法，实现密码安全和系统性能的均衡。同时，利用机器学习算法，分析加密过程中的历史数据和应用情况进行动态调整，以适应新的安全威胁和业务需求。

4.2.2 数据脱敏处理

利用自然语言处理和机器学习等方法，在数据分享和测试中实现对敏感数据的自动识别和脱敏处理。比如，对于包含客户姓名、身份证号码、银行卡号等敏感信息的文本数据，首先利用自然语言处理模型对敏感域进行定位，然后通过泛化、替代和加密等手段对其进行脱敏。具体来说，就是用匿名编号代替客户的姓名，并在身份证号码中用星号代替部分数字。对于结构化数据，例如数据库中的客户信息表，根据数据字典和预设的脱敏规则，针对敏感字段进行适当的脱敏操作。同时，对脱敏后的数据进行质量评价，保证在满足用户隐私的前提下，仍能满足商业应用的需要。

4.3 安全策略优化

4.3.1 基于数据分析的策略调整

对工业系统中各种安全数据进行采集和分析，包括安全事件日志、网络流量、用户行为、设备工作状态等，利用机器学习和数据挖掘等方法，从海量的数据中挖掘出安全隐患和漏洞。例如，在对大量安全事件进行分析后，发现一种网络攻击往往会对某一特定的系统漏洞进行攻击，而现有的防御措施尚不完善。在分析结果的基础上，对安全策略进行实时的优化，并加强对这一漏洞的修补和保护。

4.3.2 智能策略推荐与生成

结合行业属性、业务需求、安全现状和威胁态势等因素，为企业推荐个性化的安全策略推荐方案。以汽车制造业为例，针对其生产过程中存在的多个工控系统和多个供应链之间的数据交互问题，应加强工控系统安全性保护、构建供应链数据安全共享机制等研究思路。同时，还可以通过深度学习等方法，在复杂的安保环境下，自主地产生新的安全策略。例如，针对新型网络攻击手段，研究其攻击特点和已有的保护机制，并生成针对性的保护策略，例如针对特定的数据流过滤和用户的行为控制等 [3]。

5 结语

综上所述，通过多源异构数据挖掘以及机器学习、深度学习等人工智能算法的运用，对网络中的异常行为进行精确识别，能够有效提高对网络环境中的安全威胁的早期预警能力。在安全管控层次上，将传统的安全技术与人工智能的动态调整相结合，形成一种智能化、自适应的管控机制，使其能够有效提升企业的抗安全风险能力，有效减少数据泄漏的可能。未来，还需要对其进行深入的研究，以扩展其在工业敏感数据安全保护方面的应用范围，从而保障工业行业的安全和稳健发展。

参考文献

[1] 张少杰.面向工业自动化的时间敏感网络动态调度算法研究[D].北京交通大学,2024.

[2] 杨茜娅.基于工业互联网标识的工业数据共享机制研究[D].北京邮电大学,2024.

[3] 王志通.面向时间敏感网络工控系统的两安一体化调度方法研究[D].华中科技大学,2024.