科学技术与教育 2026年第8期
ISSN: 3079-4455

基于深度学习的数据安全协同防御系统研究

桑金旭，张艳玲*，孙玉冰，周培祥，刘晓彤，刘伟伟
山东建筑大学信息与电气工程学院，山东济南，中国
*通讯作者

【摘要】针对工业控制系统在 IT/OT 深度融合背景下暴露出的未知威胁识别滞后、单点防护能力分散和跨节点响应效率不足等问题，本文提出一种基于深度学习的数据安全协同防御系统。系统由数据安全网关、多协议数据安全学习模块和网络安全防火墙模块组成，通过多源数据采集、特征预处理、CNN-LSTM/Transformer 异常检测、可信计算认证和分布式联动响应，形成从数据感知、威胁识别、策略生成到执行反馈的闭环防护机制。研究表明，该体系能够将网络流量、用户行为、文件操作审计和外部威胁情报进行统一分析，提升工业网络中异常行为识别和动态处置能力。在原方案指标基础上，系统检测 F1-score 可达到 95%以上，误报率低于 5%，并能将联动响应时间压缩至秒级，为关键基础设施和工业现场的数据安全防护提供了可扩展的技术路径。

【关键词】深度学习；协同防御；可信计算；CNN-LSTM；工业控制安全；纵深防御
【基金项目】大学生创新创业训练计划项目（编号：S202510430009）

1.引言

随着工业 4.0、智能制造和大数据技术在生产现场持续落地，工业控制系统逐步突破传统封闭专用的网络边界，向开放互联、多网融合的综合信息系统演进。IT 与 OT 深度融合打通了数据采集、生产调度和远程运维链路，也使工控协议、PLC 控制器、工程师站、企业数据中心和远程运维平台等核心资产暴露于更复杂的攻击面之中。相关研究表明，工业控制系统网络安全风险具有资产分布广、协议异构、实时性要求高和攻击后果外溢性强等特点，跨域攻击、勒索软件、零日漏洞利用、越权访问或 APT 渗透一旦突破防线，风险便可能从单一信息系统扩散至生产连续性、工艺数据完整性乃至公共安全层面[1-3]。

在关键基础设施数字化程度不断提升的背景下，工业现场设备和控制网络的安全问题不再只是局部技术缺陷。PLC、工程师站、APC 节点以及跨域数据交换通道广泛嵌入能源、水利、制造、交通等重要行业，细微漏洞经由网络联通和业务耦合放大后，可能引发跨系统连锁故障。相关研究指出，单纯依赖边界隔离或静态规则难以应对多阶段、隐蔽化和智能化攻击，必须结合数据安全治理、隐私保护和纵深防御体系[4]，从数据流、控制流和行为流三个维度持续监测关键资产安全状态[5-6]。

现有工控安全产品多以防火墙、VPN、入侵检测和日志审计为核心，能够对已知攻击形成一定拦截能力，但在高速工业网络和多协议混合环境下仍存在检测粒度不足、跨设备协同弱、策略更新滞后和误报率较高等问题。为提升未知威胁识别能力，近年来研究者开始将人工智能引入工业控制系统网络安全防护，利用深度学习模型从流量序列、协议字段、用户行为和设备日志中学习异常模式；其中，面向数据安全的深度学习关键技术、AI 驱动工控安全架构、CNN-LSTM 及其注意力改进模型已被用于工业控制网络入侵检测和立体化防御，在时序特征提取和复杂攻击识别方面表现出较好的适用性[7-11]。

然而，仅依靠单点检测模型仍难以满足工业场景对可信执行、跨域联动和可追溯审计的要求。一方面，网络间敏感数据交换需要可信计算、身份认证和安全等级评定机制支撑，保证通信主体可信、数据传输可控、访问过程可审计[12,13]；另一方面，分布式工业网络中的安全事件需要在网关、检测节点、管理平台和防火墙策略之间快速联动，通过协同防御机制完成威胁情报共享、策略下发和响应反馈[14]。同时，控制系统安全稳定与事件触发控制等研究，也为工业场景中低时延、可验证的响应策略设计提供了理论参考[15]。因此，构建融合深度学习、可信计算和协同防御的数据安全体系，是提升工业控制系统主动防护能力的重要方向。

基于上述分析，本文提出一种面向工业场

景的深度学习数据安全协同防御系统，围绕异常检测、联动响应和可信执行三个环节展开研究。本文首先分析工业控制系统的数据安全风险与系统需求，随后设计由数据安全网关、多协议数据安全学习模块和协同防御决策中心构成的总体架构，并进一步给出多源数据融合、CNN-LSTM 异常检测、可信认证、访问控制和分布式联动响应等关键技术。本文的主要贡献在于：一是构建面向网络流量、文件审计和用户/设备行为日志的多源异常检测流程；二是设计安全网关、学习引擎与协同决策中心之间的闭环联动机制；三是结合可信计算、CA 认证和细粒度访问控制提升工业数据交换过程的完整性、可追溯性和动态防护能力。

2.相关技术与需求分析

2.1 工业控制系统数据安全风险

工业控制系统通常包含现场设备、控制器、工程师站、数据采集服务器、生产管理系统和远程运维接口等多个层级。这些层级之间的数据交互既包括实时控制指令，也包括设备状态、生产日志和用户操作审计信息。一旦攻击者通过弱口令、移动存储介质、远程维护通道或供应链漏洞进入系统，便可能进一步篡改控制指令、窃取敏感数据，甚至诱发生产中断。因此，工业数据安全不仅要求边界防护，还要求对数据流、行为流和控制流进行持续监测。

2.2 现有防护方案的局限

现有商用安全设备通常集成防火墙、VPN、入侵检测和日志审计等功能，能够满足常规网络边界防护需求。但在高速工业网络和多协议混合环境下，传统方案仍存在三个方面的不足：第一，依赖固定规则与人工配置，对未知攻击和变形攻击的识别能力有限；第二，安全设备之间缺乏统一的威胁上下文共享机制，难以形成跨区域联动；第三，防护策略与生产业务之间耦合不足，容易出现误拦截或告警疲劳。由此可见，数据安全防护需要从被动拦截转向主动感知、智能分析和协同响应。

2.3 系统设计需求

结合自主可控数据安全体系建设要求，系统需要满足以下需求：其一，能够统一采集网络流量、文件操作审计、用户与设备行为日志等多源数据；其二，能够利用深度学习模型识别未知威胁和异常模式；其三，能够将本地检测结果、外部威胁情报和跨节点安全事件进行融合决策；其四，能够通过安全网关、访问控制、IPSec 加密传输和 CA 认证等机制完成策略执行；其五，能够对告警、日志和响应过程进行存证与审计，保证安全事件可分析、可追踪和可复盘。

3.数据安全协同防御系统架构

本文设计的系统以“感知—分析—决策—执行—反馈”为主线，面向工业网络中的数据交换和访问控制过程建立闭环防护机制。系统前端通过数据安全网关和网络安全防火墙完成边界隔离、协议解析、内容检测和访问控制；中间层通过多协议数据安全学习模块完成特征提取、模型推理和异常判别；后端通过协同防御决策中心完成威胁情报融合、策略生成、联动处置和模型参数更新。深度学习协同防御系统总体流程如图 1 所示。

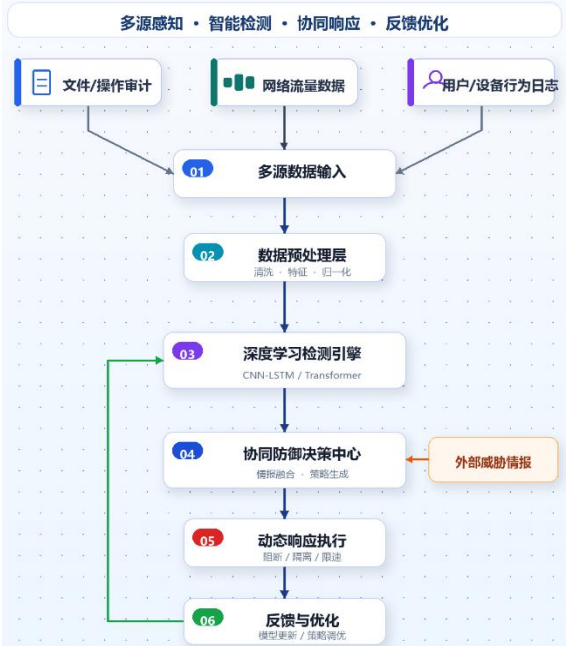

图 1.深度学习协同防御系统总体流程

3.1 数据安全网关模块

数据安全网关部署在工业网络关键边界，负责对送往设备节点和服务器的数据包进行源地址、服务端口、协议类型和内容特征过滤。过滤进程采用阻塞等待方式处理报文，接收到数据后完成解析、规则匹配和异常标记。为保证实时性，过滤进程不直接承担复杂日志分发任务，而是将安全事件交由通信进程和审计模块分级处理：重要日志本地存储，普通日志和告警日志通过加密通道上传至网管系统。

3.2 多协议数据安全学习模块

多协议数据安全学习模块面向工业控制协议、通用 TCP/IP 协议、Web 访问行为和文件操作审计记录进行统一建模。模块首先对原始数据进行清洗、归一化和字段标准化，再将流量统计特征、时序行为特征和内容语义特征

组合为多模态特征向量，随后输入深度学习检测引擎完成协议识别、异常评分和攻击类型判别。

3.3 协同防御决策中心

协同防御决策中心接收本地检测结果、外部威胁情报和其他节点共享的安全事件，综合生成阻断、隔离、限速、告警、策略更新等处置动作。该中心同时负责模型参数管理和策略回传，使边缘节点能够在不暴露敏感原始数据的情况下参与协同训练与防御优化。

4.关键技术设计

4.1 多源数据预处理与特征融合

系统将文件操作审计、网络流量数据以及用户/设备行为日志作为主要输入源。预处理层对缺失字段、异常字符、重复记录和不同协议格式进行统一处理，并根据业务场景提取会话持续时间、包长分布、访问频率、指令序列、文件敏感级别和用户角色等特征。经过归一化和标准化后，多源特征被融合为可供检测引擎使用的统一输入。多源数据预处理流程如图 2 所示。

图 2.多源数据预处理流程

4.2 深度学习异常检测模型

检测引擎采用 CNN-LSTM 与 Transformer 相结合的建模思路。CNN 结构用于提取局部流量模式和协议字段组合特征，LSTM 结构用于学习控制指令、登录行为和通信会话中的时序依赖，Transformer 结构则用于增强模型对长距离关联和多源上下文的表达能力。模型输出包括异常概率、攻击类型标签和置信度评分，协同防御中心据此触发不同等级的处置策略。

为降低传统安全设备中常见的告警疲劳问题，系统在模型输出层设置分级阈值与业务白名单机制。对低置信度事件，系统优先进入观察和复核流程；对高危事件，则直接触发阻断、隔离或策略下发。这种分级方式能够在保障生产连续性的同时提升未知威胁识别效率。

4.3 可信计算与身份认证机制

系统以可信平台模块（Trusted Platform Module，TPM）作为硬件信任根，通过密钥产生、随机数生成、HMAC 校验和完整性度量等机制，为安全网关、检测节点和管理平台之间的身份认证提供基础。结合 CA 证书链和 IPSec 加密通道，系统能够在互联网、现场层和工业控制层之间建立可信通信关系，缓解动态端口、跨网访问和远程运维带来的安全风险。

4.4 分布式协同防御与动态响应

在多节点工业网络中，单一设备难以及时掌握全局威胁态势。系统通过分布式威胁情报共享和联邦学习聚合机制，将各节点本地检测结果转化为全局威胁图谱，再由策略生成模块向 SDN 控制器、防火墙 ACL 和边缘节点同步防御规则。必要时，系统可将异常终端隔离到受控区域，并将相关日志写入审计链路，为后续追踪与复盘提供依据。联邦学习聚合与协同响应流程如图 3 所示。

图 3.联邦学习聚合与协同响应流程

从执行流程看，数据源首先将原始流量和审计记录发送至预处理层，检测引擎完成特征推理后向协同中心上报威胁事件。协同中心根据事件等级和资产重要性下发防御策略，执行单元完成阻断、隔离或限流操作，并将处置结果反馈给检测引擎，用于更新模型参数和优化后续策略。系统协同防御交互时序如图 4 所示。

图 4.系统协同防御交互时序

5.系统部署与功能实现

5.1 网络部署模式

在数据中心场景中，系统部署于服务器集群和汇聚交换层之间，对访问数据中心服务器的南北向与东西向流量进行统一控制。防火墙、安全网关和检测引擎共同承担访问控制、状态检测、网络地址转换、隧道加密和异常流量识别任务。该模式适用于生产管理系统、数据采集平台和关键业务服务器集中部署的企业网络。数据中心防火墙部署模式如图 5 所示。

在 Internet 边界场景中，系统主要承担外部攻击防范、公众服务器安全防护和内部用户访问管理等任务。对于 Web、邮件、DNS 等对外服务，系统在保证正常访问的同时进行攻击流量识别、会话状态检测和内容过滤；对于内部用户访问互联网行为，系统结合身份认证和应用识别策略，避免网络资源滥用和外部风

险引入。Internet 边界防火墙部署模式如图 6 所示。

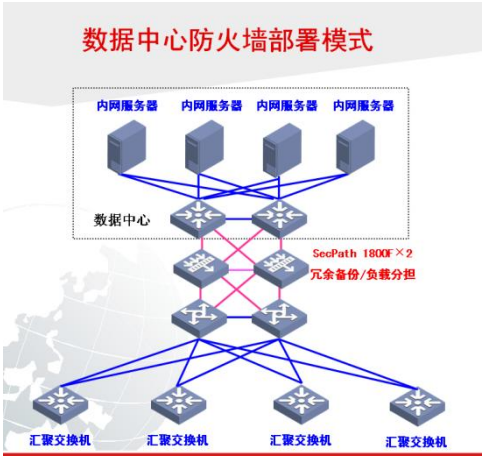

图 5.数据中心防火墙部署模式

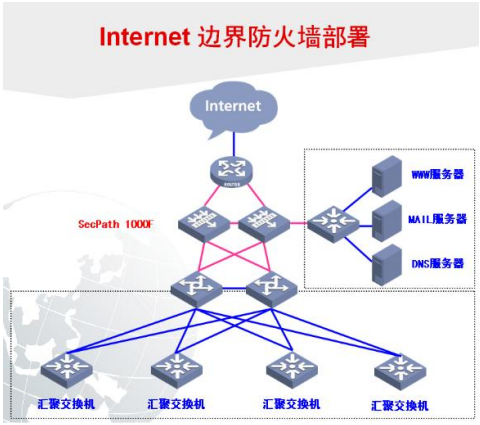

图 6. Internet 边界防火墙部署模式

5.2 访问控制、日志审计与远程配置

系统支持基于用户身份、角色、应用类型、域名、TLS 特征和服务端口的细粒度访问控制。管理员可通过浏览器远程登录管理平台，查看控制节点过滤信息、设备故障、通信故障和安全告警。远程配置系统由 Web 服务端、配置数据库和网关后台进程组成，配置项经身份认证后写入数据库，网关进程在初始化和策略变更时读取并生效。

在用户管理方面，系统区分用户管理员、配置管理员和审计管理员三类角色。用户管理员负责账号和权限维护，配置管理员负责安全策略调整，审计管理员负责日志和报警信息管理。通过角色分离，系统降低单一账号误操作或越权操作带来的风险。

5.3 可视化管理与威胁分析

网管系统对各隔离安全网关的过滤信息进行集中汇总，并通过可视化界面展示工业网络安全状态。系统可从应用类型、威胁等级、实现技术和功能特点等维度对网络应用进行分类，帮助管理员快速定位异常应用、异常用户和异常设备。同时，系统结合外部威胁情报实现安全态势感知和风险预测，为策略优化提供依据。

6.验证结果与讨论

6.1 验证方案与评价指标

为增强验证部分的可读性，本文在原型验证环境中构造网络流量、用户/设备行为日志、文件操作审计和协同响应链路等多类数据输入，围绕检测准确性、误报控制、响应时延和工业现场适用性进行综合评价。评价指标包括 Precision、Recall、F1-score、误报率、平均响应时间和策略联动效果。其中，Precision 反映告警命中质量，Recall 反映异常事件发现能力，F1-score 用于综合衡量检测模型的稳定性。验证场景与评价指标设置如表 1 所示。

表 1.验证场景与评价指标设置

验证对象	数据来源/场景	主要指标	验证目的
异常检测模型	网络流量、文件审计、用户/设备行为日志	Precision、Recall、F1-score、误报率	评价多源融合检测能力
协同响应链路	检测引擎、协同中心、防火墙/ACL、边缘节点	平均响应时间、策略同步状态	评价联动处置效率
工业现场防护	PLC、工程师站、APC 节点、OPC/Modbus 通信	隔离效果、访问控制、日志可追溯性	评价现场适配能力

6.2 检测性能对比分析

在检测性能方面，本文将传统规则/签名检测、单点 CNN-LSTM 检测和本文提出的多源协同防御系统进行对比。结果如图 7 所示，传统规则方法对已知攻击具有一定识别能力，但对变形攻击和跨阶段攻击链的召回能力不足；单点 CNN-LSTM 能够学习流量时序特征，整体性能明显提升；本文系统进一步融合文件审计、行为日志和外部威胁情报，F1-score 达到 95%以上，误报率低于 5%，说明多源融合与协同决策能够有效降低单一数据源带来的判断偏差。

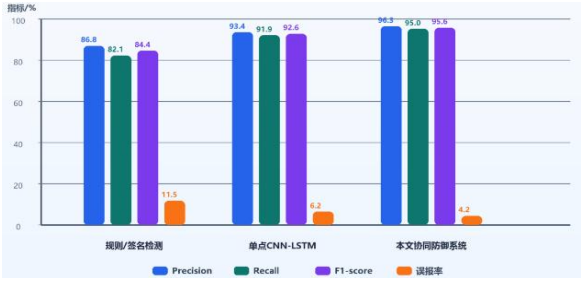

图 7.检测性能对比

6.3 协同响应效果分析

在响应效率方面，传统人工处置通常需要经历告警汇总、人工研判和手工下发策略等步骤，处置链路较长。本文系统通过检测引擎、协同防御决策中心、SDN 控制器、防火墙 ACL 和边缘节点同步形成闭环联动，可将攻击响应从分钟级压缩至秒级。由图 8 可见，协同响应机制不仅缩短平均响应时间，也通过分级阈值、白名单和反馈优化降低误报噪声，使安全策略更适合工业现场连续生产要求。

图 8.协同响应效果对比

6.4 工业现场适用性讨论

从工业现场应用角度看，系统的价值不仅体现在检测指标提升，还体现在可信认证、访问控制和审计追溯能力的增强。在主动防御方面，系统基于 CA 信任链、静态度量、动态度量和访问控制机制识别异常程序与异常数据，构建具备自免疫特征的安全防护链路。在工业现场与控制层之间，设备 CA 认证可缓解 OPC 等协议动态端口带来的安全防护瓶颈，降低非法访问和数据篡改风险。对于关键控制器，系统通过规则组态和专有协议识别限制非授权操作站访问；对于工程师站和 APC 节点，系统通过独立隔离降低移动介质、第三方设备和无线接入带来的入侵概率。

需要说明的是，本文验证仍以原型系统和模拟工业网络场景为主，后续还需在真实生产网络中持续积累多类型攻击样本，进一步验证模型在罕见攻击、跨域攻击和高实时性控制场景下的泛化能力。同时，深度学习模型在边缘设备上的部署仍受计算资源、延迟和能耗约束，未来可从模型压缩、增量学习和隐私保护联邦训练等方向继续优化。

7.结论

本文围绕工业控制系统在数字化转型过程中面临的数据安全风险，提出了一种基于深度学习的数据安全协同防御系统。系统通过数据安全网关、多协议学习模块和网络安全防火墙的协同工作，实现了多源数据感知、异常行为识别、可信认证、策略联动和反馈优化。与传统规则驱动的单点防护方案相比，该体系能够更好地适应未知威胁、跨节点攻击和工业现场多协议并存的复杂环境。

参考文献

[1] 樊政晔.工业控制系统网络安全风险评估与防护[J].网络安全和信息化，2026，（5）：152-154.
[2] Ma Y W, Tu Y H, Tsou C W, Chiang Y N, Chen J L. A Survey of Cyber Security and Safety in Industrial Control Systems[J]. Journal of Internet Technology, 2024, 25(4): 541-550.
[3] Lin C W, Zhu C Y, Wan J J, Chen P. Research on Dataset Construction and Risk Analysis for Cross-Domain Attacks in Industrial Control Scenarios[C]//2024 Asia Conference on Advances in Electrical and Power Engineering (ACEPE). 2024: 1-8. DOI:10.1109/ACEPE63527.2024.10871790.
[4] 范渊，刘博.数据安全与隐私计算[M].电子工业出版社：2023.
[5] 王帆.基于数据安全治理与虚拟化技术的纵深防御体系研究[J].网络安全和信息化，2026，（2）：131-133.
[6] 早明华，柳晓静，官雄明，等.工业控制系统网络安全纵深防御体系构建[J].中国科技信息，2025，（17）：115-118.
[7] 郝猛，李洪伟，陈涵霄.深度学习环境下数据安全的关键技术研究[M].成都电子科技大学出版社：2025.
[8] 周玉锁.基于深度学习的工控网络安全立体化防御体系研究[J].计算机与网络，2025，51（1）：45-49. DOI: 10.20149/j.cnki.issn1008-1739.2025.01.007.
[9] 陈浩博，段右辰，杨成林.工业控制系统网络安全中的 AI 驱动架构设计与效能评估[J].标准生活，2025，（S1）：36-37.
[10] 赖坤宁，邓旎.基于 CNN-LSTM 的工业控制网络入侵检测方法研究[J].现代信息科技，2025，9（24）：180-185. DOI: 10.19850/j.cnki.2096-4706.2025.24.034.
[11] 李笛，杨东，王文庆，等.基于 CNN-LSTM-Attention 的工业控制系统网络入侵检测方法研究[J].热力发电，2024，53（5）：115-121. DOI:10.19666/j.rlfd.202401014.
[12]叶紫光.基于可信计算的网络间隐私数据安全交换方法[J].网络安全技术与应用，2026，（2）：49-51.
[13]朱晨鸣，魏珂悦，李富勇，等.工控系统中

基于可信计算的数据安全等级评定与分类技术研究[J].网络安全技术与应用，2025（3）：77-79.

[14]沈伍强，信息安全一体化协同防御技术研究.广东省，广东电网公司信息中心，2019-03-27.

[15]Zhang M J, Yang X S, Zheng W X, Huang T W. Secure Stabilization of Nonlinear Switched System via Practical Asynchronous Event- Triggered Control[J]. International Journal of Robust and Nonlinear Control, 2025, 35(16): 6945-6954. DOI:10.1002/rnc.70031.