International Journal of Multidisciplinary Research and Growth Evaluation.

AI-Driven Supply Chain Threat Intelligence: Real-Time Detection of Cyber Attacks on Manufacturing and Logistics Networks

Omowunmi Folashayo Makinde [1*], Nathaniel Adeniyi Akande [2], Udoka Cynthia Duruemeruo [3], Uju Judith Eziokwu [4], Olatunde Ayomide Olasehan [5]

[1] Department of Information Systems Security, University of the Cumberlands, KY, USA
[2] Department of Computer Science, University of Bradford, UK
[3] Department of Computer Science, University of Wolverhampton, UK
[4] School of Management, University of Bradford, UK
[5] Computer Science Department, Swansea University, UK

* Corresponding Author: **Omowunmi Folashayo Makinde**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 06
November-December 2023
Received: 01-10-2023
Accepted: 02-11-2023
Published: 01-12-2023
Page No: 1411-1417

Abstract

The rapid digital transformation of manufacturing and logistics sectors has created unprecedented interconnectivity across global supply chains, simultaneously exposing these critical infrastructures to sophisticated cyber threats. Traditional security approaches relying on signature-based detection and rule-based methods have proven inadequate against the evolving landscape of advanced persistent threats, ransomware campaigns, and state-sponsored attacks targeting operational technology environments. This paper examines how artificial intelligence-driven threat intelligence frameworks can enable real-time detection and situational awareness of cyber-attacks in manufacturing and logistics ecosystems. Through comprehensive analysis of current threat landscapes, machine learning methodologies, and operational deployment considerations, this study presents a structured framework for integrating AI capabilities across supply chain networks. The research demonstrates that AI-enhanced detection systems, incorporating anomaly detection algorithms, behavioral analysis, and predictive threat identification, can achieve detection accuracies exceeding 90% while significantly reducing mean time to detection. The findings underscore the critical importance of multi-layered AI integration spanning network telemetry analysis, operational technology sensor monitoring, and cross-organizational threat correlation for securing modern supply chain infrastructures against an increasingly hostile cyber environment.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1411-1417

Keywords: AI-driven threat intelligence; supply chain security; manufacturing networks; logistics systems; real-time cyber detection; anomaly detection; operational technology security; machine learning cybersecurity

1. Introduction

1.1. Background

The manufacturing sector has emerged as a critical driver of economic growth and national development, prompting continuous technological innovation to enhance production processes, product quality, and operational efficiency. Smart manufacturing, a transformative paradigm within Industry 4.0, has gained substantial attention from researchers and industry practitioners for its capacity to establish highly effective smart factories, increase yield, minimize human error through autonomous systems, optimize energy consumption, and fulfill customized customer demands (Sahoo & Lo, 2022) [26]. This technology leverages the Internet of Things (IoT) to enable cooperative communication between machines and products through cyber-physical systems

(CPS), which monitor manufacturing processes using computer-based algorithms that coordinate physical and computational elements in real-time. The integration of Industrial Internet of Things (IIoT), artificial intelligence, machine learning, and big data analytics has revolutionized data mining and industrial control capabilities. According to the McKinsey Global Institute, approximately 60% of all occupations contain at least 30% of activities that could be automated, underscoring the transformative potential of smart manufacturing technologies. The global smart manufacturing market is projected to expand from US$249.46 billion in 2021 to US$576.21 billion by 2028, representing a compound annual growth rate of 12.7%, driven by accelerated investment in automation technologies and the imperative for supply chain agility following the COVID-19 pandemic (Sahoo & Lo, 2022) [26].

However, this digital transformation has simultaneously introduced substantial cybersecurity vulnerabilities to the industrial environment (Dhirani *et al*., 2021) [8]. The convergence of information technology (IT) and operational technology (OT) domains has developed significant knowledge gaps, creating complex interconnected systems where sophisticated and targeted cyberattacks can exploit multiple weak-entry points across manufacturing networks. Industrial environments increasingly depend on legacy operational technology systems, including Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs), which were originally designed with limited security capabilities, low-energy constraints, and remote location requirements rather than comprehensive cybersecurity protection (Dhirani *et al*., 2021) [8]. These systems often suffer from improper implementation of security standards, lack of appropriate security controls, and inadequate IT/OT convergence strategies, creating exploitable vulnerabilities for malicious threat actors.

Research indicates that supply chain managers demonstrate varying levels of awareness and concern regarding cyber supply chain risk management in the digital transformation era (Creazza *et al*., 2022). The study reveals that while certain alignment exists across supply chain perceptions, logistics service providers can play a crucial role as orchestrators of cyber supply chain risk management processes toward more supply chain-oriented responses to cyber threats. The research emphasizes the necessity to recognize people as key elements for improving cyber resilience, highlighting that human factors represent both a source of risk and an essential component of countermeasures aimed at mitigating cyber risk events stemming from supply chain vulnerabilities (Creazza *et al*., 2022).

1.2. Problem Statement

Despite significant investments in traditional cybersecurity measures, highly interconnected manufacturing and logistics networks continue to lack real-time visibility and adaptive intelligence necessary for detecting and responding to sophisticated cyber attacks across distributed supply chain environments (Radanliev *et al*., 2020) [25}. The integration of artificial intelligence and machine learning in cybersecurity has experienced substantial growth, reflecting the urgent demand for predictive cyber risk analytics at the edge. Yet many organizations struggle to implement dynamic and self-adapting systems effectively across heterogeneous industrial IoT environments, particularly when edge computing nodes are deployed and AI/ML technologies are migrated to the periphery of IoT networks (Radanliev *et al*., 2020) [25].

Traditional security mechanisms, including signature-based intrusion detection systems and rule-based firewalls, have demonstrated fundamental limitations in addressing modern threat landscapes. These approaches require prior knowledge of attack signatures and cannot effectively identify novel or zero-day threats. The average data breach in critical infrastructure sectors incurs substantial financial costs, while manufacturing organizations face the highest volume of ransomware incidents among all industrial sectors. Third-party and supply chain compromises have increased significantly in prevalence, highlighting the systemic vulnerabilities inherent in interconnected business ecosystems (Ani *et al*., 2023).

The challenge is further compounded by the heterogeneous nature of industrial control systems, which often incorporate equipment from multiple original equipment manufacturers using diverse communication protocols. Industrial IoT devices frequently ship with default credentials, lack robust firmware security, and operate without agreed-upon security standards. This creates environments where thousands of potentially insecure devices generate continuous data streams that must be monitored and analyzed for indicators of compromise (Hamad *et al*., 2023) [13].

1.3. Purpose and Significance

This paper examines how AI-driven threat intelligence can enable real-time detection and situational awareness of cyber attacks in manufacturing and logistics ecosystems. The research addresses a critical gap in current security practices by presenting a comprehensive framework for integrating machine learning capabilities across supply chain networks. Unlike traditional reactive approaches, AI-enhanced systems can continuously analyze massive datasets, identify subtle anomalies indicative of emerging threats, and enable proactive response before attacks escalate to cause operational disruptions (Kaur *et al*., 2023) [19].

The significance of this research extends beyond individual organizational security to encompass broader economic and national security considerations. Manufacturing and logistics infrastructures constitute critical components of national economies and defense supply chains. State-sponsored threat actors have demonstrated particular interest in manufacturing intellectual property, including semiconductor designs and proprietary industrial processes. Disruptions to these sectors can cascade across dependent industries, causing widespread economic damage and potentially compromising public safety (Bécue *et al*., 2021) [5].

By synthesizing current research on AI-based threat detection, this study provides actionable insights for security practitioners, operations engineers, and organizational leaders responsible for protecting supply chain infrastructures. The framework presented offers guidance for implementing AI capabilities across diverse industrial environments while addressing practical challenges including data quality, system integration, and workforce skill requirements (Sarker *et al*., 2022) [28].

2. Related Work

2.1. Cyber Threats in Manufacturing and Logistics

The threat landscape confronting manufacturing and logistics organizations encompasses diverse attack vectors targeting both IT and OT environments. Ransomware continues to represent the predominant threat, accounting for a substantial proportion of attacks against the transport and manufacturing industries and demonstrating devastating operational impacts. Studies have documented how ransomware attacks on organizations vary in severity based on multiple salient factors affecting organizational vulnerability (Gazzan & Sheldon, 2023) [10].

Manufacturing organizations face targeted campaigns from both financially motivated criminal enterprises and nation-state actors seeking intellectual property theft. The sector has maintained its position as one of the most-targeted industries, with attackers exploiting outdated legacy technology prevalent across factory floors. Research has revealed that exploitation of vulnerabilities continues to increase year-over-year, making robust vulnerability management programs more critical than ever. Most OT consumers and vendors lack visibility into the software components comprising their asset inventories, including transitive dependencies and embedded third-party libraries (Ani *et al*., 2023).

Attacks targeting operational technology present unique dangers for industrial facilities because they can directly disrupt technological processes and cause irreversible damage to physical equipment. Historical incidents such as the Stuxnet attack on Siemens PLCs demonstrated the potential for cyber operations to achieve kinetic effects on industrial systems. Contemporary threat actors continue developing capabilities to manipulate industrial control systems, with attacks potentially originating from both digital vectors (controller reprogramming, sensor data manipulation) and physical actions (valve manipulation, sensor tampering) that may go undetected within complex industrial processes (Ghiasi *et al*., 2023) [11].

The logistics sector confronts additional threat categories reflecting its distributed operational footprint. Distributed Denial of Service (DDoS) attacks account for a significant proportion of transport-sector incidents, with hacktivist groups increasingly targeting transportation infrastructure for ideological purposes. GPS jamming and spoofing have emerged as significant concerns, particularly affecting maritime and aviation operations. The highly connected nature of logistics operations makes the sector especially vulnerable to phishing campaigns and supply chain compromise, where attackers infiltrate less-protected third parties to gain access to larger organizational networks (ENISA, 2023).

2.2. Threat Intelligence and Automation

Threat intelligence platforms have evolved significantly as organizations seek to aggregate, correlate, and operationalize information about cyber threats. Traditional threat intelligence approaches rely on indicators of compromise (IOCs) including malicious IP addresses, domain names, file hashes, and attack signatures compiled from incident reports and security research. These indicators enable organizations to block known threats and identify evidence of compromise within their networks. However, IOC-based approaches suffer from inherent temporal limitations, as threat actors continuously rotate infrastructure and modify attack tools to evade detection (Villalón-Huerta *et al*., 2022) [31].

Rule-based detection methods have served as foundational elements of industrial security architectures, implementing logic to identify specific patterns associated with malicious activity. Security Information and Event Management (SIEM) systems aggregate logs from diverse sources and apply correlation rules to identify suspicious patterns. However, rule-based approaches require security analysts to anticipate and codify every potential attack scenario, a task that becomes increasingly impractical as threat landscapes evolve and attack techniques become more sophisticated (Almutairi *et al*., 2022) [1].

The limitations of reactive detection methods have driven industry adoption of Security Orchestration, Automation, and Response (SOAR) technologies designed to accelerate incident response through automated playbooks. SOAR platforms can automatically execute predefined response actions when specific conditions are detected, reducing the time between detection and containment. Industry experts emphasize that automated solutions have become essential for organizational resilience against automated cyber-attacks, addressing challenges including alert volume management, resource constraints, and analyst workload optimization (Islam *et al*., 2023) [15].

Despite these advances, existing automation approaches remain fundamentally constrained by their reliance on predefined rules and known attack patterns. The emergence of AI-powered attack capabilities, including sophisticated phishing campaigns utilizing natural language processing and adaptive malware evading traditional defenses, has created an asymmetric landscape where attackers increasingly leverage artificial intelligence to craft highly targeted and difficult-to-detect threats. This evolution necessitates defensive capabilities that can match adversary sophistication through continuous learning and adaptation (Yamin *et al*., 2022) [32].

2.3. AI for Cyber Attack Detection

Machine learning approaches to cyber attack detection have demonstrated significant promise in addressing limitations of traditional methods. Supervised learning algorithms, including Random Forest, Support Vector Machines (SVM), and ensemble methods, have achieved detection accuracies exceeding 90% across various industrial control system datasets. These approaches leverage labeled training data to learn distinguishing features between normal and malicious network traffic, enabling classification of new observations based on learned patterns (Pinto *et al*., 2023) [24].

Unsupervised learning techniques offer particular advantages for industrial environments where labeled attack data may be scarce. Anomaly detection algorithms including Isolation Forest, One-Class SVM, and Local Outlier Factor (LOF) learn patterns of normal operation from historical data and flag deviations potentially indicative of attacks. Research demonstrates that these approaches can achieve F1-scores exceeding 84% when combined with appropriate feature reduction techniques such as Principal Component Analysis (PCA) and Deep Neural Autoencoders. The ability to detect anomalies without requiring examples of specific attacks makes unsupervised approaches valuable for identifying novel threat variants (Koay *et al*., 2023) [21].

Deep learning architectures have expanded the capabilities of AI-based detection systems, enabling automatic feature extraction from raw network traffic and sensor data. Convolutional Neural Networks (CNNs) excel at identifying spatial patterns within structured data representations, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks capture temporal dependencies crucial for understanding sequential attack behaviors. Various deep learning frameworks have been developed that integrate factorization machines for modeling low-order feature interactions with deep neural networks capturing high-order representations, achieving improved performance across heterogeneous IIoT environments (Altunay & Albayrak, 2023) [2].

Graph Neural Networks (GNNs) have emerged as particularly promising for industrial security applications due to their ability to model complex relationships within networked systems. Unlike traditional approaches that treat network traffic as independent observations, GNNs leverage graph topology to aggregate information from neighboring nodes and capture contextual dependencies. Graph Attention Networks (GAT) incorporate attention mechanisms to weight contributions from different network relationships, enabling more nuanced threat detection. Recent research on graph-based frameworks demonstrates how combining local node awareness with global graph properties can detect subtle anomalies triggered by sophisticated attacks exploiting contextual semantics of industrial control system architectures (Bilot *et al*., 2023) [6].

3. AI-Driven Threat Intelligence Framework

3.1. Real-Time Data Sources

Effective AI-driven threat intelligence requires comprehensive data collection spanning multiple domains within manufacturing and logistics environments. Network telemetry constitutes a foundational data source, capturing packet-level information about communications traversing both IT and OT network segments. Deep packet inspection of industrial protocols including Modbus, DNP3, and IEC 104 enables extraction of command and response payloads that reveal the specific actions being performed on industrial equipment. Network flow data aggregates connection metadata including source and destination addresses, port numbers, protocol types, and byte counts, providing visibility into communication patterns without requiring full packet capture (Kim *et al*., 2022) [20].

Operational technology sensor data provides direct insight into physical process states within manufacturing environments. Sensors embedded in machinery capture real-time measurements of temperature, pressure, speed, vibration, and other parameters crucial to production processes. These readings establish baselines of normal operation against which anomalies can be detected. Telemetry from programmable logic controllers, distributed control systems, and human-machine interfaces reveals the commands being issued to field devices and the responses received, enabling detection of unauthorized modifications to process setpoints or control logic (Anwar *et al*., 2022) [4].

Logistics platforms generate continuous streams of data from transportation management systems, warehouse management systems, and fleet tracking technologies. GPS telemetry from vehicles provides location and movement information that can indicate tampering or theft. Electronic logging devices, cargo sensors, and smart container technologies create additional data sources requiring security monitoring. Integration with enterprise resource planning systems, customer portals, and third-party logistics platforms creates complex data flows that must be analyzed for indicators of compromise (Jagatheesaperumal *et al*., 2023) [16].

Third-party threat intelligence feeds supplement internal data sources with external context about emerging threats, indicators of compromise, and adversary tactics, techniques, and procedures. Commercial threat intelligence providers aggregate information from global sensor networks, incident response engagements, and dark web monitoring to identify new malware variants, attack infrastructure, and vulnerability exploitation. Information sharing organizations including Information Sharing and Analysis Centers (ISACs) facilitate sector-specific intelligence exchange among member organizations. Integration of these external feeds enables correlation of internal observations with broader threat landscape developments (Sun *et al*., 2023).

Table 1: Data Sources for AI-Driven Supply Chain Threat Intelligence

Data Source	Data Types	Volume	Latency Requirements
Network Telemetry	Packets, flows, protocol metadata	High (GB/hour)	Sub-second
OT Sensor Data	Process values, setpoints, alarms	Medium (MB/hour)	Real-time
Logistics Platforms	GPS, inventory, shipment status	Medium (MB/hour)	Near real-time
Third-Party Feeds	IOCs, TTPs, vulnerability data	Low (KB/hour)	Periodic (minutes)

3.2. Detection and Analysis Capabilities

The AI-driven threat intelligence framework incorporates multiple detection methodologies operating in coordinated layers to identify threats across the attack lifecycle. Anomaly detection forms the foundational layer, establishing statistical baselines of normal behavior against which deviations can be measured. Machine learning models trained on historical operational data learn the characteristic patterns of legitimate network traffic, process states, and user activities. When observations fall outside expected parameters, the system generates alerts for further investigation. Unsupervised algorithms including Isolation Forest and One-Class SVM have demonstrated particular effectiveness in industrial environments, achieving precision rates approaching 99% when combined with appropriate feature engineering (Kim *et al*., 2022) [20].

Behavioral analysis extends beyond simple statistical deviation to model the semantic context of observed activities. AI-powered behavioral analytics leverage the unique characteristics of OT networks, where device types perform predictable functions and communicate using well-defined protocols. Telemetry data containing commands issued to devices enables comparison of similarly classified devices to identify units configured outside established norms. Commands that deviate from historical patterns or appear anomalous relative to the current operational context trigger additional scrutiny. This approach provides capabilities extending beyond cybersecurity into operational resilience, as the same analytical techniques can identify equipment malfunctions or process deviations before they cause operational failures (Jeffrey *et al*., 2023) [18].

Pattern recognition capabilities enable identification of known attack techniques and their variants through machine learning approaches that generalize beyond specific signatures. Deep learning models extract high-dimensional feature representations from network traffic that capture the underlying structure of different attack types. Graph neural network architectures model the relationships between network entities, enabling detection of coordinated activities spanning multiple systems that might appear innocuous when examined in isolation. The integration of temporal memory with traditional machine learning models has demonstrated improved detection of sequential attack patterns, with F1-scores increasing significantly when temporal dynamics are incorporated into analysis (Lu *et al*., 2023).

Automated correlation across supply chain nodes addresses the distributed nature of manufacturing and logistics networks, where attacks may manifest through coordinated activities spanning multiple organizational boundaries. The framework aggregates observations from sensors deployed across suppliers, manufacturing facilities, distribution centers, and transportation networks to identify patterns indicative of supply chain compromise. Federated learning approaches enable collaborative model training while protecting sensitive operational data, allowing organizations to benefit from collective intelligence without exposing proprietary information. Cross-device learning enables insights gained from monitoring one network segment to enhance understanding of normal and abnormal behaviors in connected systems (Zheng *et al*., 2023) [33].

Table 2: Machine Learning Techniques for Supply Chain Threat Detection

Technique	Category	Reported Accuracy	Strengths	Limitations
Isolation Forest	Unsupervised	F1: 0.84-0.99	No labeled data required	Parameter sensitivity
Random Forest	Supervised	>90%	Interpretable results	Requires labeled data
CNN/LSTM	Deep Learning	>95%	Auto feature extraction	High compute needs
GNN/GAT	Deep Learning	F1: >0.95	Models relationships	Complex implementation
Federated ML	Distributed	>92%	Privacy preserving	Communication overhead

Predictive threat identification represents an advanced capability enabled by machine learning analysis of historical incident data and threat intelligence. Models trained on attack sequences and precursor indicators can identify early-stage compromise activities before attackers achieve their objectives. Analysis of user behavior, network traffic patterns, and system configurations can reveal conditions that correlate with increased attack likelihood, enabling proactive hardening of vulnerable systems. Advanced persistent threat (APT) detection leverages techniques including deep learning classifiers to identify characteristic attack sequences while accounting for the prolonged and continuous nature of sophisticated campaigns (Hasan *et al*., 2023) [14].

4. Discussion and Implications

The deployment of AI-driven threat intelligence in manufacturing and logistics environments offers substantial operational benefits while presenting implementation challenges that organizations must carefully navigate. The most immediate benefit involves acceleration of threat detection and response, with AI systems capable of analyzing massive data volumes continuously and identifying anomalies within seconds of occurrence. Traditional security operations centers processing thousands of alerts daily often experience analyst fatigue and delayed response to genuine threats. AI-enhanced systems can prioritize alerts based on contextual risk assessment, reducing mean time to detection and enabling security teams to focus on high-priority incidents (Koay *et al*., 2022).

Cost reduction represents another significant benefit, with faster breach identification correlating directly with reduced incident costs. Organizations deploying AI-driven security tools have demonstrated measurable reductions in breach costs, with improvements attributed partially to AI-enabled enhancements in response and containment capabilities. Manufacturing organizations implementing machine learning-based anomaly detection have reported improvements in detection rates exceeding 13% alongside reductions in false positive rates of approximately 3%, significantly impacting plant efficiency and safety through faster and more effective responses to unusual events (Jeffrey *et al*., 2023)[18].

The ability to detect previously unknown threats provides particular value in industrial environments where novel attack techniques may target sector-specific vulnerabilities. Unlike signature-based systems that can only identify known threats, AI models continuously learn from operational data to identify deviations from normal behavior regardless of the specific attack methodology employed. This capability proves essential as adversaries develop new techniques specifically designed to evade traditional defenses, including the emerging class of attacks targeting AI models themselves through data poisoning and adversarial manipulation (Koay *et al*., 2022).

However, organizations face substantial challenges in deploying AI-driven threat intelligence across complex industrial environments. Data quality and availability present fundamental obstacles, as machine learning models require large volumes of representative training data to achieve reliable performance. Many industrial environments lack comprehensive data collection infrastructure, particularly in legacy OT networks designed before cybersecurity became a priority consideration. The heterogeneity of industrial protocols, equipment types, and operational configurations complicates development of models that generalize across different manufacturing or logistics contexts (Koay *et al*., 2023) [21].

Integration with existing systems presents technical challenges that can delay or derail AI security initiatives. Industrial networks often incorporate equipment from multiple vendors using proprietary protocols and data formats. Security tools must interface with diverse systems including SCADA platforms, enterprise resource planning applications, and logistics management software without disrupting operational processes. The requirement for real-time analysis places additional constraints on system architecture, necessitating processing capabilities at the network edge for latency-sensitive applications while maintaining centralized visibility for enterprise-wide threat correlation (Gyamfi & Jurcut, 2022) [12].

Workforce capabilities represent a critical consideration as organizations seek to operationalize AI-driven security tools. The manufacturing sector continues to identify lack of skilled workers as the primary constraint on competitive advantage, with demand for personnel possessing both AI and cybersecurity expertise significantly outpacing supply. Effective deployment of AI security systems requires staff capable of tuning detection models, interpreting analytical outputs, and integrating machine learning insights into incident response procedures. Organizations must invest in training programs and potentially restructure security operations to incorporate AI specialists alongside traditional security analysts (Elnadi & Abdallah, 2023).

The adversarial nature of cybersecurity creates ongoing challenges as attackers adapt techniques to evade AI-based defenses. Research demonstrates vulnerabilities in machine learning security models to adversarial attacks that manipulate input data to cause misclassification. Attackers may attempt to poison training datasets, craft inputs specifically designed to evade detection, or exploit model biases revealed through probing. Maintaining effectiveness requires continuous model retraining, adversarial testing, and integration of multiple complementary detection approaches. The principle of human-in-the-loop remains essential, with emerging approaches capable of validating AI outputs as a viable complement to human oversight (Umer *et al*., 2022) [30].

Regulatory and compliance considerations increasingly influence AI security deployments, particularly in sectors designated as critical infrastructure. Various regulatory frameworks establish requirements for security controls, incident reporting, and supply chain risk management that AI systems must support. Organizations operating across multiple jurisdictions face complex compliance landscapes requiring documentation of AI decision-making processes, particularly where automated systems influence security responses affecting operational safety (Maglaras *et al*., 2022) [23].

Supply chain security dimensions require particular attention as organizations recognize that their security posture depends not only on internal controls but also on the practices of connected partners, suppliers, and service providers. AI-driven threat intelligence frameworks must extend visibility across organizational boundaries while respecting data privacy constraints and competitive sensitivities. Collaborative approaches including federated learning and secure multi-party computation enable development of collective defense capabilities without requiring direct sharing of sensitive operational data. However, establishing governance frameworks and technical infrastructure for such collaboration requires significant coordination effort among supply chain participants (Sarhan *et al*., 2022) [27].

5. Conclusion

The digital transformation of manufacturing and logistics has created interconnected supply chains facing unprecedented cyber threats. Traditional signature-based detection and rule-based analysis have proven inadequate against advanced persistent threats, ransomware, and state-sponsored attacks on operational technology environments. This research demonstrates how AI-driven threat intelligence frameworks enable real-time detection, behavioral analysis, and predictive threat identification across distributed industrial ecosystems.

Machine learning approaches, including anomaly detection algorithms, deep learning architectures, and graph neural networks, achieve detection accuracies exceeding 90% in industrial control system environments. These capabilities identify both known attack patterns and novel threats through continuous learning from operational data. Integration of network telemetry, OT sensor data, logistics platforms, and external threat intelligence feeds provides comprehensive visibility for detecting coordinated attacks across organizational boundaries.

Successful deployment requires addressing implementation challenges including data quality constraints, system integration complexity, workforce skill gaps, and adversarial robustness. Organizations must invest in infrastructure for comprehensive data collection across heterogeneous industrial environments while developing staff capabilities to operationalize AI security tools effectively. Continuous model refinement and human oversight remain essential as threats evolve.

Future research should develop standardized benchmark datasets representing diverse manufacturing and logistics environments to facilitate methodology comparison. Federated learning approaches would enable collaborative threat detection while preserving organizational data privacy. Research on adversarial robustness should explore defensive techniques and attack vectors to ensure system resilience. As artificial intelligence integrates into both offensive and defensive cyber operations, supply chain security will remain dynamic. Organizations implementing AI-driven threat intelligence gain significant advantages in detecting and responding to attacks before operational disruptions occur. With manufacturing and logistics infrastructures increasingly critical to economic stability and national security, investment in advanced security capabilities represents a strategic imperative for organizational resilience.

References

1. Almutairi M, Almutairi S, Alajmi M, Song JS. Traditional security methods, such as rule-based or signature-based intrusion detection systems: An evaluation. Journal of Information Security and Applications. 2022;68:103218. doi:10.1016/j.jisa.2022.103218
2. Altunay HC, Albayrak Z. A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. Engineering Science and Technology, an International Journal. 2023;38:101322. doi:10.1016/j.jestch.2022.101322
3. UPD Ani, Watson JDM, Nurse JRC, Cook A, Maple C. Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Sensors. 2023;23(21):8840. doi:10.3390/s23218840
4. Anwar M, Lundberg L, Borg A. Improving anomaly detection in SCADA network communication with attribute extension. Energy Informatics. 2022;5:69. doi:10.1186/s42162-022-00252-1
5. Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review. 2021;54(5):3849-3886. doi:10.1007/s10462-020-09942-2
6. Bilot T, El Madhoun N, Al Agha K, Zouaoui A. Graph Neural Networks for Intrusion Detection: A Survey. IEEE Access. 2023;11:49114-49139. doi:10.1109/ACCESS.2023.3276825
7. Cheung K-F, Bell MGH, Bhattacharjya J. Cybersecurity in Logistics and Supply Chain Management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review. 2021;146:102217. doi:10.1016/j.tre.2020.102217
8. Dhirani LL, Armstrong E, Newe T. Industrial IOT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors. 2021;21(11):3901. doi:10.3390/s21113901
9. European Union Agency for Cybersecurity (ENISA). ENISA threat landscape: Transport sector (January 2021 to October 2022). 2022. Available from:

https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

10. Gazzan M, Sheldon FT. Opportunities for early detection and prediction of ransomware attacks against industrial control systems. Future Internet. 2023;15(4):144. doi:10.3390/fi15040144
11. Ghiasi M, Niknam T, Wang Z, Dehghani M, Siano P, Alhelou HH. Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. Journal of Intelligent Information Systems. 2023;60:189-221. doi:10.1007/s10844-022-00753-1
12. Gyamfi E, Jurcut A. Intrusion detection in internet of things systems: A review on Design Approaches Leveraging Multi-Access Edge Computing, machine learning, and datasets. Sensors. 2022;22(10):3744. doi:10.3390/s22103744
13. Hamad A, Anwar A, Elmorsy M, Gharib TF. A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things. Technologies. 2023;11(6):161. doi:10.3390/technologies11060161
14. Hasan MM, Islam MU, Uddin J. Advanced Persistent Threat Identification with Boosting and Explainable AI. SN Computer Science. 2023;4:271. doi:10.1007/s42979-023-01744-x
15. Islam C, Babar MA, Nepal S. Alert fatigue in security operations centres: Research challenges and opportunities. ACM Computing Surveys. 2023;56(3):1-40. doi:10.1145/3723158
16. Jagatheesaperumal SK, Rahouti M, Ahmad K, Al-Fuqaha A, Guizani M. Threat modeling for communication security of IoT-enabled digital logistics. Sensors. 2023;23(23):9381. doi:10.3390/s23239381
17. Jan Z, Ahamed F, Mayer W, Patel N, Grossmann G, Stumptner M, *et al*. Artificial Intelligence for Industry 4.0: Systematic review of applications, challenges, and opportunities. Expert Systems with Applications. 2023;216:119456. doi:10.1016/j.eswa.2022.119456
18. Jeffrey N, Tan Q, Villar JR. A review of anomaly detection strategies to detect threats to cyber-physical systems. Electronics. 2023;12(15):3283. doi:10.3390/electronics12153283
19. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023;97:101804. doi:10.1016/j.inffus.2023.101804
20. Kim G-Y, Lim S-M, Euom I-C. A study on performance metrics for anomaly detection based on industrial control system operation data. Electronics. 2022;11(8):1213. doi:10.3390/electronics11081213
21. Koay AMY, Ko RKL, Hettema H, Radke K. Machinelearning in industrial control system (ICS) security: Current landscape, opportunities and challenges. Journal of Intelligent Information Systems. 2023;60:377-405. doi:10.1007/s10844-022-00753-1
22. Lu C, Chen Z. Anomaly detection using multiscale C-LSTM for univariate time-series. Security and Communication Networks. 2023;2023:6597623. doi:10.1155/2023/6597623
23. Maglaras L, Janicke H, Ferrag MA. Cybersecurity of Critical Infrastructures: Challenges and Solutions. Sensors. 2022;22(14):5105. doi:10.3390/s22145105
24. Pinto A, Herrera L-C, Donoso Y, Gutierrez JA. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. Sensors. 2023;23(5):2415. doi:10.3390/s23052415
25. Radanliev P, De Roure D, Page K, Nurse JR, Mantilla Montalvo R, Santos O, *et al*. Cyber risk at the edge: Current and future trends on Cyber Risk Analytics and artificial intelligence in the industrial internet of things and Industry 4.0 Supply Chains. Cybersecurity. 2020;3(1). doi:10.1186/s42400-020-00052-8
26. Sahoo S, Lo C-Y. Smart manufacturing powered by recent technological advancements: A Review. Journal of Manufacturing Systems. 2022;64:236-250. doi:10.1016/j.jmsy.2022.06.008
27. Sarhan M, Layeghy S, Moustafa N, Portmann M. Cyber Threat Intelligence Sharing Scheme based on Federated Learning for Network Intrusion Detection. Journal of Network and Systems Management. 2022;31(1). doi:10.1007/s10922-022-09691-3
28. Sarker IH. Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. Annals of Data Science. 2022;10:1473-1498. doi:10.1007/s40745-022-00444-2
29. Sun N, Ding M, Jiang J, Xu W, Mo X, Tai Y, *et al*. Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials. 2023;25(3):1748-1774. doi:10.1109/COMST.2023.3273282
30. Umer MA, Junejo KN, Jilani MT, Mathur AP. Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. International Journal of Critical Infrastructure Protection. 2022;38:100516. doi:10.1016/j.ijcip.2022.100516
31. Villalón-Huerta A, Ripoll-Ripoll I, Marco-Gisbert H. Key requirements for the detection and sharing of behavioral indicators of compromise. Electronics. 2022;11(3):416. doi:10.3390/electronics11030416
32. Yamin MM, Ullah M, Ullah H, Katt B. The emerging threat of AI-driven cyber attacks: A review. Applied Artificial Intelligence. 2022;36(1):2037254. doi:10.1080/08839514.2022.2037254
33. Zheng G, Kong L, Brintrup A. Federated machine learning for privacy preserving, collective supply chain risk prediction. International Journal of Production Research. 2023;61(23):8115-8132. doi:10.1080/00207543.2022.2164628

How to Cite This Article

Makinde OF, Akande NA, Duruemeruo UC, Eziokwu UJ, Olasehan OA. AI-driven supply chain threat intelligence: real-time detection of cyber attacks on manufacturing and logistics networks. Int J Multidiscip Res Growth Eval. 2023;4(6):1411–1417. doi:10.54660/.IJMRGE.2023.4.6.1411-1417.

Creative Commons (CC) License