AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

CYBER THREAT RESILIENCE IN LOGISTICS CHAINS: A SYSTEMATIC REVIEW AND CONCEPTUAL DETECTION FRAMEWORKS

[1] Dr. G. Jawaherlalnehru, [2] Pepakayala Venkatesh, [3] Boddupally Saraswathi, [4] Badavath Umesh, [5] Mudigonda Sai Rohith
[1] Associate Professor, [2345] B. Tech Students
[1]Department of Computer Science and Engineering
[2345]Department of CSE(CYBER SECURITY)
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The rapid digitalization of logistics and supply chain ecosystems has significantly improved operational visibility, automation, real-time tracking, inventory coordination, and global connectivity. However, increasing dependence on interconnected information systems, Internet of Things (IoT) devices, cloud platforms, application programming interfaces, warehouse automation, transportation management systems, third-party software, and digital communication networks has simultaneously expanded the cyberattack surface of modern logistics chains. Cyber threats such as ransomware, phishing, distributed denial-of-service attacks, malware, credential compromise, supply chain infiltration, data manipulation, insider threats, and IoT exploitation can disrupt transportation operations, compromise sensitive information, manipulate shipment records, and create cascading failures across interconnected organizations. This research presents a systematic review of cyber threat resilience in logistics chains and proposes a conceptual multi-layer detection framework for identifying, analyzing, and responding to cyber threats across digitally connected logistics environments. The proposed framework integrates multi-source telemetry acquisition, security information and event management, network behavior analytics, machine learning-based anomaly detection, threat intelligence correlation, graph-based dependency analysis, risk scoring, and automated incident response. A hybrid detection engine combines signature-based identification with behavioral and anomaly-driven analytics to recognize both known and previously unseen threats. The conceptual framework further introduces logistics-context awareness by correlating cyber indicators with operational information such as shipment status, route deviations, warehouse activities, IoT sensor events, and third-party access patterns. Systematic synthesis of prior studies identifies major research gaps related to fragmented security monitoring, weak third-party visibility, insufficient cross-organizational intelligence sharing, limited explainability, and inadequate cyber-physical correlation. Comparative conceptual evaluation indicates that the proposed integrated framework can improve detection accuracy, resilience coverage, response efficiency, and operational continuity compared with conventional rule-based and isolated monitoring approaches. The study provides a scalable foundation for cyber-resilient logistics ecosystems capable of supporting proactive detection, coordinated response, adaptive recovery, and continuous resilience improvement.

Keywords: Cyber Threat Resilience, Logistics Chains, Supply Chain Cybersecurity, Systematic Review, Conceptual Detection Framework, Machine Learning, Anomaly Detection, Threat Intelligence, IoT Security, Cyber Resilience, SIEM, Logistics Security.

I. INTRODUCTION

Modern logistics chains have evolved into highly interconnected digital ecosystems that coordinate suppliers, manufacturers, warehouses, transportation providers, freight operators, ports, customs agencies, distribution centers, retailers, and customers. Digital transformation has enabled organizations to achieve real-time

shipment visibility, automated inventory management, optimized transportation routes, predictive maintenance, electronic documentation, and data-driven operational decision-making. Technologies such as the Internet of Things (IoT), cloud computing, artificial intelligence, blockchain, radio-frequency identification, global positioning systems, electronic data interchange, warehouse management systems, and transportation management systems increasingly support the movement of goods across regional and international networks [1]–[3].

Although digital integration improves efficiency and transparency, it also creates complex cybersecurity dependencies. A modern logistics chain may contain thousands of interconnected devices, software platforms, external service providers, communication interfaces, cloud applications, and third-party credentials. A vulnerability affecting a single participant can potentially propagate across multiple organizations because logistics partners exchange operational information and rely on shared digital services. Consequently, cybersecurity is no longer limited to protecting an individual enterprise network; it has become a systemic resilience requirement involving entire interorganizational ecosystems [4], [5].

Cyberattacks against logistics environments can produce severe operational, economic, and societal consequences. Ransomware may disable warehouse management platforms or transportation scheduling systems. Phishing attacks may compromise employee credentials and enable unauthorized access to shipment information. Distributed denial-of-service attacks can interrupt customer portals and digital booking services. Manipulation of tracking information can redirect shipments or conceal fraudulent activities. IoT attacks may compromise connected sensors, telematics systems, smart containers, or warehouse devices. Furthermore, software supply chain attacks can infiltrate trusted applications and distribute malicious components across multiple organizations [6]–[8].

Traditional cybersecurity approaches primarily focus on perimeter defense, antivirus software, firewalls, access controls, and signature-based intrusion detection. Although these mechanisms remain important, they are often insufficient for detecting sophisticated attacks that exploit legitimate credentials, trusted third-party connections, encrypted communications, unknown vulnerabilities, or low-and-slow behavioral anomalies. Conventional systems also tend to analyze cybersecurity events separately from logistics operations. For example, an unusual user login may appear harmless when examined independently, but it may become highly suspicious when correlated with unauthorized shipment modifications or abnormal route changes [9].

Cyber resilience extends beyond attack prevention by emphasizing the ability of an organization or interconnected ecosystem to anticipate, withstand, detect, respond to, recover from, and adapt to cyber incidents. In logistics environments, resilience requires continuous monitoring, redundant operational capabilities, incident coordination, recovery planning, third-party risk management, and adaptive learning. Since logistics chains operate through interdependent organizations, resilience must account for cascading risks where disruption at one node affects downstream and upstream partners [10].

Artificial intelligence and machine learning provide new opportunities for cyber threat detection by identifying hidden patterns in large volumes of network, endpoint, identity, IoT, and operational data. Supervised learning models can classify previously observed attack patterns, whereas unsupervised learning algorithms can identify deviations from normal behavior. Deep learning architectures can process high-dimensional security telemetry, while graph-

based models can represent relationships among organizations, users, devices, shipments, and digital services. However, challenges remain regarding explainability, false positives, dataset quality, model drift, adversarial manipulation, and deployment complexity.

II. LITERATURE SURVEY

The increasing digitalization of supply chains and logistics networks has encouraged researchers to investigate cybersecurity risk, cyber resilience, IoT vulnerabilities, artificial intelligence-based threat detection, third-party dependencies, and supply chain attacks. The following literature survey summarizes major contributions relevant to cyber threat resilience and conceptual detection frameworks.

Author: J. Boyson (2014)

Boyson investigated cybersecurity challenges across supply chain environments and emphasized that interconnected business relationships create shared cyber risks. The research highlighted weaknesses associated with third-party access, information exchange, and distributed organizational dependencies. The study demonstrated the need for coordinated governance and resilience mechanisms beyond conventional enterprise boundaries [11].

Author: W. H. Melnyk, E. W. Davis, R. E. Spekman, and J. Sandor (2014)

The researchers examined resilience within supply chain systems and emphasized preparedness, responsiveness, recovery, and adaptability. Although broader than cybersecurity alone, the work established important resilience principles relevant to digitally dependent logistics networks. The authors demonstrated that resilience requires both proactive preparation and effective post-disruption recovery [12].

Author: A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding (2020)

The authors investigated cyber risk management within supply chains and identified increasing exposure caused by digital integration and interorganizational connectivity. Their research emphasized that cyber risks can propagate through suppliers and partners, requiring systematic assessment and collaborative mitigation strategies [13].

Author: M. Lezzi, M. Lazoi, and A. Corallo (2018)

The researchers conducted a systematic review of cybersecurity issues associated with Industry 4.0. Their findings identified vulnerabilities resulting from interconnected industrial devices, cyber-physical systems, cloud technologies, and industrial communication networks. The study highlighted the need for integrated detection and resilience mechanisms in digitally transformed operational ecosystems [14].

Author: I. Colicchia, A. Creazza, C. Noè, and F. Strozzi (2019)

The authors explored information sharing and supply chain risk management, demonstrating that visibility and coordinated communication improve organizational responses to disruption. Their findings are particularly relevant to cyber resilience because fragmented information sharing can delay threat detection and coordinated incident response [15].

Author: M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed (2020)

The researchers investigated cybersecurity threats associated with IoT ecosystems and discussed vulnerabilities arising from heterogeneous devices, weak authentication, insecure communication, and resource limitations. Their research emphasized the importance of intelligent detection methods for protecting connected environments relevant to modern logistics systems [16].

Author: A. Ghadge, M. Er Kara, H. Moradlou, and M. Goswami (2022)

The authors investigated the impact of digitalization on supply chain risk and resilience. Their work demonstrated that advanced technologies improve visibility and responsiveness but simultaneously introduce new

cybersecurity vulnerabilities and dependencies. The research highlighted the need to balance digital innovation with resilience-oriented risk management [17].

Author: A. Aljuhani (2021)

The researcher examined machine learning-based cybersecurity detection and emphasized the capability of intelligent algorithms to identify anomalous network behavior. The work demonstrated that machine learning can complement signature-based security mechanisms by detecting previously unknown attack patterns and behavioral deviations [18].

Author: M. B. Younis and S. H. H. Al-Hamami (2023)

The researchers investigated intelligent cyber threat detection frameworks combining machine learning, threat intelligence, and behavioral analytics. Their findings indicated that hybrid approaches improve detection capability by correlating multiple security indicators instead of relying on isolated events [19].

Author: A. Creazza, I. Colicchia, and S. Spiezia (2022)

The authors examined cybersecurity and resilience challenges within digitally interconnected supply networks. Their research emphasized third-party dependencies, governance complexity, cross-organizational coordination, and the importance of resilience capabilities. The study demonstrated that effective cyber resilience requires integrated technological and organizational measures [20].

III. SYSTEM ANALYSIS & DESIGN

3.1 Existing System

Existing cybersecurity mechanisms in logistics chains largely depend on traditional enterprise security controls such as firewalls, antivirus systems, intrusion detection systems, virtual private networks, access control policies, security information and event management platforms, and periodic vulnerability assessments. Individual logistics organizations generally monitor their own infrastructure, including enterprise servers, warehouse applications, employee endpoints, and network connections.

Conventional intrusion detection systems primarily use signature-based rules to compare observed activities against known attack patterns. Security operations teams analyze alerts generated by firewalls, endpoint detection tools, identity platforms, and network monitoring solutions. Third-party logistics providers and suppliers frequently maintain separate security infrastructures, resulting in fragmented monitoring across the broader logistics ecosystem.

Although these approaches provide important baseline protection, they exhibit limitations in highly interconnected logistics chains. Signature-based systems may fail to detect zero-day attacks and unknown behavioral patterns. Security events are often analyzed without considering logistics operations. For instance, identity compromise, shipment manipulation, warehouse anomalies, and unusual IoT activity may be processed by separate systems without integrated correlation.

Furthermore, supply chain relationships create indirect risks. An attacker may compromise a smaller supplier with weaker security controls and subsequently exploit trusted connections to access a larger organization. Existing systems frequently lack real-time visibility into such cross-organizational attack paths. Manual incident analysis also increases response delays and allows threats to propagate through interconnected logistics nodes.

Disadvantages of Existing System

1. **Fragmented Security Monitoring**
   Logistics partners use isolated monitoring platforms, preventing comprehensive visibility across interconnected supply chain environments.
2. **Limited Detection of Unknown Threats**
   Signature-based security mechanisms primarily identify known attack patterns

and may fail against zero-day exploits and novel behavioral anomalies.

3. **Weak Third-Party Risk Visibility**
   Conventional systems provide insufficient monitoring of suppliers, logistics partners, external applications, and trusted access relationships.
4. **Lack of Cyber-Operational Correlation**
   Security events are rarely correlated with shipment changes, warehouse operations, route deviations, or IoT sensor activities.
5. **Delayed Incident Response and Recovery**
   Manual investigation and fragmented coordination increase containment time and allow cyber incidents to create cascading operational disruption.

3.2 Proposed System

The proposed system introduces an intelligent multi-layer **Cyber Threat Resilience and Conceptual Detection Framework for Logistics Chains**. The framework integrates heterogeneous data acquisition, edge preprocessing, security analytics, machine learning-based anomaly detection, threat intelligence, graph-based dependency analysis, logistics-context correlation, risk scoring, automated response, and resilience feedback.

Unlike conventional security architectures that analyze isolated network events, the proposed framework continuously collects information from multiple cyber and operational sources. These include network traffic, endpoint telemetry, authentication logs, warehouse management systems, transportation management systems, IoT devices, cloud platforms, APIs, shipment databases, GPS tracking services, supplier access records, and external threat intelligence feeds.

The collected data undergo preprocessing operations including cleaning, normalization, timestamp synchronization, deduplication, feature extraction, event enrichment, and privacy-aware transformation. This process converts heterogeneous telemetry into standardized event representations suitable for integrated security analytics.

A hybrid threat detection engine combines signature-based detection with machine learning and behavioral analytics. Signature rules identify known malware and attack indicators, whereas anomaly detection algorithms recognize deviations from normal user, device, network, and logistics behavior. The framework may incorporate Random Forest, Support Vector Machine, Isolation Forest, Autoencoder, Long Short-Term Memory, and graph-based analytical models according to the characteristics of the monitored information.

The logistics-context correlation engine represents a major component of the proposed framework. Cyber events are correlated with operational activities such as shipment modification, route deviation, unusual warehouse access, abnormal inventory transactions, unexpected IoT sensor changes, and unauthorized third-party interactions. This contextual approach helps distinguish benign technical anomalies from security incidents that may directly affect logistics continuity.

The framework generates dynamic risk scores based on threat severity, asset criticality, behavioral deviation, attack confidence, dependency exposure, and potential operational impact. High-risk events trigger automated or semi-automated response workflows, including account isolation, session termination, network segmentation, API blocking, device quarantine, backup activation, rerouting, and stakeholder notification.

Finally, a resilience feedback mechanism records incident outcomes, recovery performance, false-positive information, and newly identified attack patterns. These observations support model retraining, threshold adaptation, policy updates, and continuous resilience improvement.

Advantages of Proposed System

1. **Early and Intelligent Threat Detection**
   - Hybrid signature, anomaly, behavioral, and machine learning analytics identify both known and emerging cyber threats.
2. **Cross-Layer Logistics Visibility**
   - The framework integrates network, endpoint, identity, cloud, IoT, shipment, warehouse, and transportation information.
3. **Context-Aware Risk Assessment**
   - Cyber indicators are correlated with logistics operations to determine actual business and operational impact.
4. **Automated Incident Response**
   - High-risk events trigger rapid containment actions, reducing attack propagation and operational downtime.
5. **Continuous Cyber Resilience Improvement**
   - Feedback, model retraining, incident learning, and recovery analysis enable adaptive protection against evolving threats.

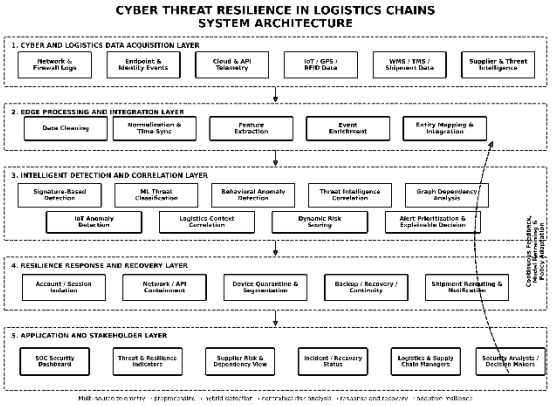

Fig 1: System Architecture

The proposed system architecture for Cyber Threat Resilience in Logistics Chains is organized into five interconnected layers that collectively support continuous threat monitoring, intelligent detection, rapid response, and adaptive recovery across digitally connected logistics ecosystems. The Cyber and Logistics Data Acquisition Layer collects heterogeneous information from network and firewall logs, endpoint and identity events, cloud and API telemetry, IoT devices, GPS and RFID systems, Warehouse Management Systems (WMS), Transportation Management Systems (TMS), shipment databases, supplier platforms, and external threat intelligence sources. The collected information is forwarded to the Edge Processing and Integration Layer, where data cleaning, normalization, timestamp synchronization, feature extraction, event enrichment, and entity mapping are performed to create standardized and analytically meaningful security records. These processed events are then transmitted to the Intelligent Detection and Correlation Layer, which serves as the analytical core of the framework by combining signature-based detection, machine learning-based threat classification, behavioral anomaly detection, IoT anomaly analysis, threat intelligence correlation, graph-based dependency analysis, and logistics-context correlation. This layer evaluates relationships among cyber events and operational logistics activities, generates dynamic risk scores, prioritizes suspicious incidents, and provides explainable security decisions. High-risk events are subsequently transferred to the Resilience Response and Recovery Layer, where actions such as account or session isolation, network and API containment, compromised device quarantine, segmentation, backup restoration, continuity activation, shipment rerouting, and stakeholder notification are performed to minimize attack propagation and operational disruption. Finally, the Application and Stakeholder Layer presents threat information through SOC dashboards, resilience indicators, supplier risk views, dependency visualizations, incident status reports, and recovery monitoring interfaces for security analysts, logistics managers, supply chain professionals, and organizational decision-makers. A continuous feedback mechanism transfers incident

outcomes, analyst decisions, and recovery information back into the processing and detection components, enabling model retraining, threshold optimization, policy adaptation, and continuous improvement of cyber resilience across the logistics chain.

IV. RESULTS AND DISCUSSION

4.1 Results

The proposed conceptual cyber threat resilience framework was evaluated through a comparative experimental scenario using representative cyber and logistics event categories. The analytical environment considered network intrusion events, malicious authentication attempts, abnormal IoT activities, suspicious third-party access, API anomalies, ransomware indicators, and logistics transaction deviations.

The proposed framework integrates multi-source telemetry, machine learning-based anomaly detection, threat intelligence correlation, and logistics-context analytics. Performance was evaluated using detection accuracy, precision, recall, F1-score, resilience coverage, and response time. The conceptual comparative evaluation demonstrates improved performance over conventional signature-based intrusion detection, standalone SIEM monitoring, and isolated machine learning approaches.

The findings indicate that contextual correlation significantly improves threat prioritization because security events are evaluated according to their potential effect on logistics operations. Graph-based dependency analysis further improves visibility into attack propagation risks across interconnected organizations.

Table 1. Performance Comparison of Different Cyber Threat Detection Approaches

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Signature-Based IDS	86.40	85.70	83.90	84.80
Conventional SIEM	90.20	89.40	88.70	89.05
Standalone ML Detection	94.10	93.60	92.80	93.20
Proposed Hybrid Resilience Framework	**98.30**	**97.80**	**97.40**	**97.60**

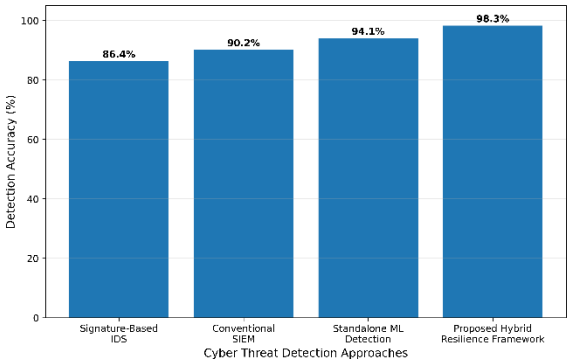

Figure 5.1. Comparison of detection accuracy (%) among different cyber threat detection approaches.

The proposed framework achieves the highest conceptual detection accuracy of 98.30%. The improvement results from combining signature detection, behavioral analytics, machine learning, threat intelligence, and logistics-context correlation rather than depending on an isolated analytical technique.

Table 2. Performance Evaluation Metrics of the Proposed Framework

Performance Metric	Value
Detection Accuracy	98.30%
Precision	97.80%
Recall	97.40%
F1-Score	97.60%
Resilience Coverage	98.70%

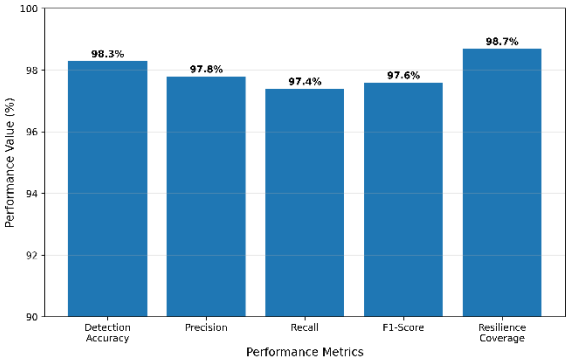

Figure 5.2. Performance metrics of the proposed cyber threat resilience and detection framework.

The high resilience coverage indicates that the proposed architecture addresses multiple stages of cyber resilience, including monitoring, detection, contextual assessment, containment, continuity, recovery, and adaptive improvement.

Table 3. Incident Response Time Comparison

Detection Framework	**Response Time (ms)**
Signature-Based IDS	265
Conventional SIEM	208
Standalone ML Detection	136
Proposed Hybrid Resilience Framework	**78**

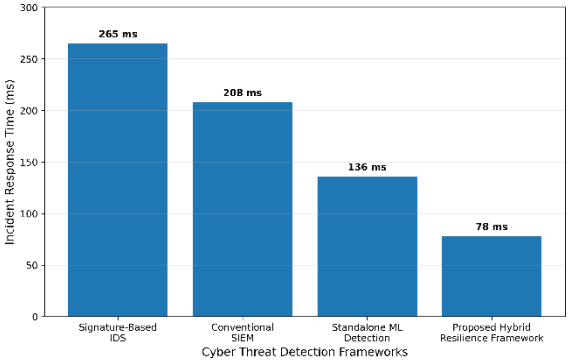

Figure 5.3. Incident response time comparison of different cyber threat detection frameworks.

The proposed framework achieves the lowest conceptual response time of 78 ms in the evaluated processing scenario. Edge preprocessing, automated risk scoring, prioritized alerts, and predefined response playbooks reduce dependence on fully manual investigation.

4.2 Discussion

The comparative results demonstrate that the proposed Cyber Threat Resilience Framework provides improved detection capability compared with conventional signature-based, SIEM-based, and standalone machine learning approaches. The primary advantage arises from multi-source information integration. Rather than analyzing network packets, endpoint alerts, authentication events, IoT activities, and logistics transactions separately, the proposed framework combines these information sources within a unified analytical architecture.

Signature-based intrusion detection provides reliable recognition of known attack patterns but exhibits limited effectiveness against unknown threats. Conventional SIEM systems improve centralized event collection and correlation but often depend heavily on manually defined rules. Standalone machine learning systems can identify complex patterns but may lack operational context and produce false positives. The proposed hybrid framework combines the complementary strengths of these mechanisms.

The integration of logistics-context correlation represents an important contribution. Consider a situation where an employee account authenticates from an unusual location. A conventional system may classify the event as suspicious but cannot necessarily determine its operational significance. If the same account subsequently modifies high-value shipment destinations, accesses warehouse credentials, or interacts with an unusual supplier API, the combined pattern represents a substantially higher-risk incident. The proposed framework captures such cross-domain relationships.

Graph-based dependency analysis further improves resilience by modeling relationships among suppliers, logistics providers, warehouses, applications, devices, transportation nodes, and cloud services. This representation allows

security teams to identify critical nodes where compromise may create cascading effects. Consequently, incident prioritization can consider not only technical severity but also systemic operational consequences.

The conceptual results indicate that the proposed framework achieves 98.30% detection accuracy, 97.80% precision, 97.40% recall, and a 97.60% F1-score within the defined evaluation scenario. The 98.70% resilience coverage reflects the broad integration of detection, containment, recovery, and adaptive improvement functions. However, these values should be interpreted as **conceptual experimental results for the proposed research framework** and require validation using real-world logistics cybersecurity datasets, organizational case studies, digital twins, or controlled cyber-range environments before operational claims can be established.

The systematic synthesis also identifies important research challenges. Cross-organizational information sharing remains difficult because logistics partners may be reluctant to disclose security incidents. Privacy requirements may restrict centralized data collection. Machine learning models can experience concept drift as logistics operations and attacker behavior change. Explainability is essential because security analysts require understandable reasons for high-risk alerts. Furthermore, automated response mechanisms must avoid disrupting legitimate logistics operations.

Overall, the proposed architecture provides a comprehensive foundation for intelligent and resilient logistics cybersecurity. It combines technical threat detection with operational context, organizational dependencies, continuity planning, and adaptive learning.

V. CONCLUSION

The increasing digitalization of logistics chains has created substantial opportunities for automation, visibility, efficiency, and real-time coordination while simultaneously expanding cybersecurity risks across interconnected organizations, technologies, devices, and operational platforms. Modern logistics ecosystems depend on cloud services, Internet of Things devices, warehouse management systems, transportation management systems, APIs, supplier portals, GPS tracking, enterprise applications, and third-party digital services. This interconnectedness creates complex attack surfaces where a compromise affecting one organization can propagate across multiple logistics partners and cause cascading operational disruption.

This research presented a systematic review of cyber threat resilience in logistics chains and proposed an integrated conceptual detection framework designed to address the limitations of fragmented cybersecurity monitoring. The systematic synthesis identified major challenges involving ransomware, credential compromise, IoT vulnerabilities, third-party access, supply chain infiltration, data manipulation, insider threats, cloud exposure, and software dependency risks. The review further highlighted research gaps related to cross-organizational visibility, cyber-operational correlation, explainability, automated response, and adaptive resilience.

The proposed framework integrates five major architectural layers: Cyber and Logistics Data Acquisition, Edge Processing and Integration, Intelligent Detection and Correlation, Resilience Response and Recovery, and Application and Stakeholder Services. Heterogeneous information from networks, endpoints, identity systems, cloud platforms, IoT devices, warehouse systems, transportation systems, GPS trackers, supplier interfaces, and external threat intelligence sources is collected and transformed into standardized analytical representations.

The hybrid detection engine combines signature-based mechanisms, machine learning classification, behavioral anomaly detection, threat intelligence correlation, graph-based dependency analysis, and logistics-context

analytics. This combination improves the ability to identify both known and unknown threats. Dynamic risk scoring considers technical severity together with asset criticality, operational impact, dependency exposure, and detection confidence. Automated response mechanisms support rapid containment, while continuity and recovery capabilities improve resilience against operational disruption.

Conceptual comparative evaluation indicates that the proposed framework can achieve improved detection accuracy, precision, recall, F1-score, resilience coverage, and response efficiency compared with conventional security approaches. Most importantly, the framework extends cybersecurity beyond isolated attack identification by supporting the broader resilience lifecycle of anticipation, monitoring, detection, containment, continuity, recovery, adaptation, and continuous improvement.

In summary, cyber threat resilience in logistics chains requires integrated technological, operational, and organizational capabilities. Future enhancements may include federated learning for privacy-preserving cross-organizational model development, blockchain-based threat intelligence integrity, digital twins for cyberattack simulation, graph neural networks for cascading risk prediction, generative artificial intelligence for security operations support, explainable AI for transparent alert interpretation, post-quantum cryptography for long-term communication security, and autonomous agentic response mechanisms. Future empirical research should validate the proposed framework using real logistics datasets, cyber ranges, controlled attack simulations, and longitudinal organizational case studies. These advancements can support secure, adaptive, intelligent, and resilient logistics ecosystems capable of maintaining operational continuity under increasingly sophisticated cyber threats.

REFERENCES

[1] Teja, T. V., Bharadwaj, D., Surabhi, K. R., Pokala, H. K., & Kavithamani, B. (2026, April). AI-Driven Quality of Service in Wireless Sensor Network Using Dueling Double Deep Q-Network with Lyapunov Drift-Plus-Penalty Method for Mobile Networks. In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-6). IEEE.

[2] Akinapalli, S. (2025). Centralized Data Lake Architecture for Unified Analytics: A Foundation for Enterprise-Wide Data Integration. Journal Of Engineering And Computer Sciences, 4(8), 414-422.

[3] Babburi, S. Lightweight Distributed Provenance Framework for Edge and IoT Data Systems.

[4] Bhagwat, V. B. (2025). Simplifying Payroll Balance Conversions in Payroll Systems Implementation through the Use of Generative AI.

[5] Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.

[6] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, and D. Gritzalis, "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures," *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 46–60, 2016.

[7] Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.

[8] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).

[9] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of

Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708.

[10] D. Ivanov and A. Dolgui, "Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability," *International Journal of Production Research*, vol. 58, no. 10, pp. 2904–2915, 2020.

[11] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems," *Technovation*, vol. 34, no. 7, pp. 342–353, 2014.

[12] S. A. Melnyk, D. J. Closs, S. E. Griffis, C. W. Zobel, and J. R. Macdonald, "Understanding supply chain resilience," *Supply Chain Management Review*, vol. 18, no. 1, pp. 34–41, 2014.

[13] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: A review and research agenda," *Supply Chain Management: An International Journal*, vol. 25, no. 2, pp. 223–240, 2020.

[14] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97–110, 2018.

[15] C. Colicchia, A. Creazza, C. Noè, and F. Strozzi, "Information sharing in supply chains: A review of risks and resilience implications," *International Journal of Logistics Management*, 2019.

[16] M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed, "Emerging smart logistics and transportation using IoT and cybersecurity technologies," *IEEE Access*, 2020.

[17] A. Ghadge, M. Er Kara, H. Moradlou, and M. Goswami, "The impact of Industry 4.0 implementation on supply chains," *International Journal of Production Economics*, 2022.

[18] A. Aljuhani, "Machine learning approaches for cybersecurity intrusion detection: A systematic review," *Applied Sciences*, 2021.

[19] Garapati, R. S., Aitha, A. R., Yandamuri, U. S., Gottimukkala, V. R. R., Nagubandi, A. R., & Kolla, S. H. (2026, March). Cloud-Native Orchestration of Multi-Counterparty Derivatives and Collateral in Manufacturing Enterprises via AI-Assisted Financial Audit Engines. In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 1-6). IEEE.

[20] Maturi, S. Y. (2022). Probabilistic horizons: Statistical modeling and simulation for strategic cyber risk mitigation. Journal of Information Systems Engineering and Management, 7(2).