International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 1124-1146
https://doi.org/10.70917/ijcisim-2026-4820
Article

An Intelligent Cyber-Physical Security Framework for Integrated Railway and Smart Port Operations

Anshad A.S[1], Kunal G Srinivas[2], Sahana S Kumar[3], B Raghunathreddy[4], Minal khobragade[5], Vijay Mohan Shrimal[6]

[1]Principal, MES Institute of Technology & Management, Chathannoor, Kollam, 691572, Kerala, https://orcid.org/my-orcid?orcid=0009-0009-2012-5787, India
(Corresponding Author)
vaagaipaper@gmail.com
[2]Department of computer application, Associate Professor, Malnad College of Engineering, Hassan, Karnataka-573202.
[3]Department of Information Science and Engineering, Assistant Professor, Malnad Collage of Engineering, Hassan, Karnataka-573202.
[4]Department of Civil engineering, Associate professor, Sai Rajeswari institute of technology, Lingapuram, proddatur, kadapa, ap 516362
[5]Department of CSE, Assistant Professor, Ramdeobaba University, Nagpur, Maharashtra, 440013, 0009-0002-0087-1845
[6]Department of AIT-CSE, Associate Professor, Chandigarh University, Gharuan, Mohali, Punjab-140413, 0009-0001-5296-4878

Abstract: With the fast pace of digitalization of transport infrastructure, smart elements and technologies have been integrated into railway networks and smart port operations, improving the degree of automation, real-time monitoring, predictive maintenance, and efficient logistics management. While all these developments enhance the efficiency and reliability of operations, they create new cybersecurity challenges with the increasing interconnections between cyber and physical elements. Such cyber threats as malware, distributed denial-of-service (DDoS) attacks, GPS spoofing, insider attacks, false data injection, and sensor tampering can impact transportation operations, tamper with operational data, and pose a threat to public safety for critical infrastructures. This research introduces an intelligent cyber-physical security framework for integrated railway and smart port operations, which integrates artificial intelligence (AI), Internet of Things (IoT) technologies, edge computing, blockchain-based secure communication, modeling and simulation with a digital twin, and decision support functions to create an all-encompassing cybersecurity architecture for the integrated transportation systems. The proposed framework was able to continuously retrieve diverse operational data from the railway signaling systems, smart port automation equipment, industrial control systems, IoT sensors, surveillance systems, communication networks, and logistics databases for real-time security analysis. Intelligent threat detection and classification are achieved with the help of advanced AI algorithms, and blockchain technology offers secure authentication and trusted information sharing and tamper-resistant data management. Edge computing can minimize communication delays by analyzing security data near operational assets, while digital twin technology can be used for predictive security risk evaluation, cyberattack simulation, infrastructure monitoring, and assessing infrastructure resilience. The experimental evaluation of the performance shows the ability to detect intrusions with better accuracy, false alarm rate, throughput, response time, and AUC values than the traditional machine learning and deep learning models.

Keywords: Cyber-Physical Security, Intelligent Transportation Systems, Railway and Smart Port Operations, Artificial Intelligence, Blockchain-Based Security, Intrusion Detection System (IDS)

Copyright: © 2026 by the authors

1. Introduction

The transportation sector has been experiencing a radical change, where digital technologies, intelligent automation, and cyber-physical systems (CPS) come together. Railways and maritime ports are among the most important parts of national and international logistics networks, enabling the efficient transport of people, goods, and commercial goods on regional and international supply chains. These infrastructures have been transformed into highly connected smart transportation systems with the rapid adoption of Internet of Things (IoT) devices, artificial intelligence (AI), cloud computing, edge computing, autonomous control systems, and advanced communication technologies [1]. Intelligent signaling, predictive maintenance, automated train control, and real-time monitoring on the modern railway enable improved efficiency and safety for passengers,

while smart ports use automated container terminals, intelligent cargo tracking, autonomous cranes, and digital logistics platforms to optimize cargo handling and vessel use. These smart infrastructures have the potential to form a connected transportation ecosystem that boosts the use of resources, minimizes delays in operations, and optimizes decision-making based on real-time data and information sharing [2]. The reliance on increasingly interconnected digital technologies, also increases the cyber-attack surface, putting critical transportation assets at risk from advanced forms of cybersecurity threats.

While digital transformation has significantly enhanced operational capabilities in railway and smart port settings, it has also created intricate cybersecurity issues that pose a risk to the reliability of critical transportation infrastructure. In contrast to traditional information technology systems, cyber-physical transportation systems seamlessly connect computation and physical operational processes, with cyber incidents affecting physical components, human life, safety, and logistics [3]. Railway signaling networks, train control systems, communication gateways, industrial control systems, supervisory control and data acquisition (SCADA) systems, cargo management applications, autonomous cranes, and wireless communication networks provide a technological landscape that was diverse and heterogeneous and offers numerous potential attack vectors. Examples of cyberattacks and threats against transportation systems have included but are not limited to ransomware and distributed denial-of-service (DDoS) attacks, GPS spoofing, malware infiltration, false data injection, insider attacks, communication hijacking, and sensor manipulation, which have shown their potential to disrupt transportation operations, compromise sensitive logistics information, and interrupt supply chain continuity [4]. As operational technologies become more and more deployed autonomously, the complexity of systems grows, and manual security monitoring was no longer enough to identify complex multi-stage attacks.

In recent years, advancements in AI have greatly improved the ability of cybersecurity solutions to identify, categories, and counteract constantly changing cyber threats affecting critical infrastructure. The machine learning and deep learning techniques allow security platforms to review massive amounts of complex operational data, find patterns that exist in the data but aren't captured by humans, and spot unusual activities that could be a sign of malicious attacks [5]. Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Graph Neural Networks (GNN), autoencoders, transformer architectures, and ensemble learning models have achieved outstanding results in intrusion detection, anomaly recognition, malware classification, and predictive cyber defense. At the same time, edge computing has proved to be a viable solution for processing security data close to the assets on-site, mitigating communication latency, and allowing for timely action without the need to rely heavily on centralized cloud-based security platforms [6]. Blockchain technology adds extra security by enabling decentralized authentication, immutability, secure information sharing, and trust management between geographically distributed entities in the transportation sector.

Although significant advances have been made in the area of intelligent transportation security research, most of the existing research focuses on railway cybersecurity, smart port protection, ICS security, or maritime cyber resilience as individual research fields. The vast majority of existing security frameworks focus on single transportation infrastructures and do not take into account their operational interdependencies as found in an integrated railway–port logistics ecosystem [7]. With the growing interdependency of multimodal transportation systems,

vulnerabilities can quickly spread in the system and from one mode to another via shared communication networks, cloud-based logistics platforms, intelligent scheduling systems, and autonomous cargo management apps. Current IDSs are often centralized, rely on signature-based detection, or are based on narrow machine learning models that are unable to detect new attack patterns and coordinated cyber-physical attacks [8]. A lot of the traditional cybersecurity solutions are not effective in the real-time response, cross-domain information sharing, digital asset integrity or predictive threat simulation in dynamic transportation environments. There was a research gap in the absence of a unified security architecture that can integrate artificial intelligence, blockchain, edge computing, IoT security, and digital twin solutions.

In response to these challenges, this study presents an Intelligent Cyber-Physical Security Framework (ICPSF) for Integrated Railway and Smart Port Operations. The framework integrates artificial intelligence, Internet of Things technologies, edge computing, blockchain-based secure communication, digital twin modelling and intelligent decision support to formulate a framework for cybersecurity in multimodal transportation systems. The proposed framework was designed to dynamically collect operational data from various sensors and devices located around the railway, the port, surveillance systems, logistics databases, communication gateways, and industrial control systems and present this information on a single platform so that operators can gain operational awareness [9]. Advanced DE heterogeneous algorithms enable real-time detection of anomalies and classification of cyber threats, and blockchain technologies enable secure authentication, tamper-proof data sharing, and trusted collaboration among stakeholders in the transportation sector. By processing security analytics near the critical operational assets, edge computing can help to improve the speed of threat detection and response, which was crucial for reducing latency. Edge computing can help to reduce latency by processing security analytics near the critical operational assets, which can speed up the detection and response process. Digital twin technology dynamically creates a representation of the physical transportation infrastructure to support predictive risk assessment, cyber threat simulation, transportation resilience modelling and recovery planning. The proposed framework was expected to enhance the accuracy of intrusion detection, minimize security response time, enhance cyber resilience and maintain the uninterrupted operation of smart ports and the railway [10].

2. Research Gap

Research on cybersecurity in railway networks, smart ports, industrial control systems and maritime infrastructure mainly focuses on cybersecurity in these isolated areas with little consideration given to security needs of integrated railway–smart port operations. Current solutions are based on centralized intrusion detection, traditional machine learning-based systems, and monolithic security solutions with limited capabilities to detect a coordinated cyber-physical attack in interdependent transportation systems. The integration of AI, edge computing, blockchain, Internet of Things (IoT), security, and digital twin technology in a single security framework was not well-explored [11]. The constraint underscores the necessity of an intelligent, scalable and real-time cyber-physical security system that can secure the interconnectedness of transportation infrastructures while guaranteeing operational resilience, information security and continuous logistics operations.

3. Research Methodology

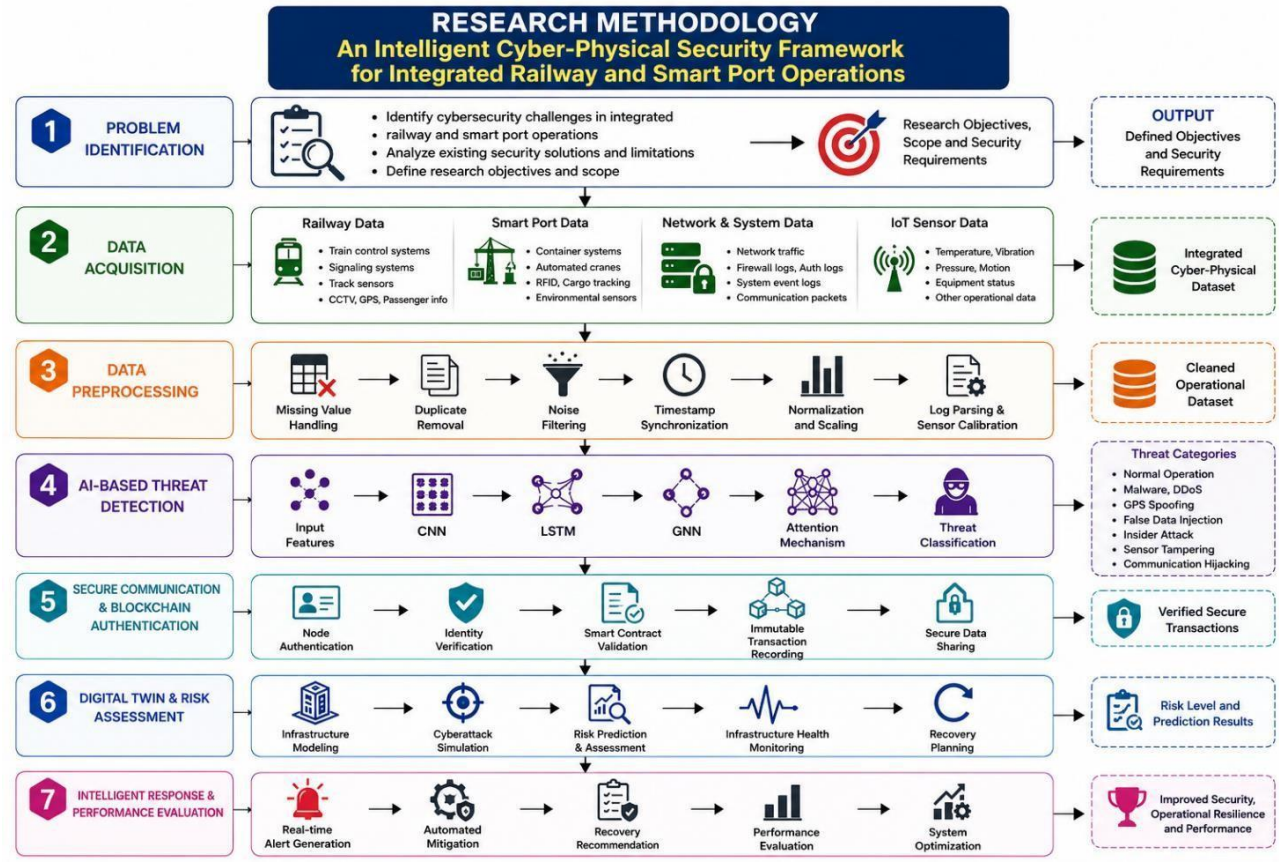

Figure 1: Research Methodology Data Acquisition and Cyber-Physical Integration

The data acquisition during the data acquisition phase, the proposed framework for intelligent cyber-physical security was set as the cornerstone; the operational information was continually gathered from both the railway and smart port environments. A wide range of cyber and physical elements are interwoven together to deliver a holistic view of transportation use and activity. Information was taken from the train control units, track monitoring equipment, surveillance cameras, communication gateways and Internet of Things (IoT) sensors. Likewise, the operational information from smart ports was integrated, such as container handling equipment, automated cranes, RFID readers, cargo tracking systems, environmental sensors and vessel monitoring systems. These different data sources are combined to continuously monitor infrastructure status and events of operation [12].

Data are gathered from physical infrastructure as well as digital communication networks to provide full system awareness. 'Physical data' refers to equipment conditions, train movements, cargo locations, weather data, and infrastructure conditions, while 'cyber data' are network traffic, authentication data, communication logs, firewall events, and access logs. These data sets are heterogeneous and synced using common timestamps to ensure consistency between the various operational platforms. Cyber and physical information integration creates a single, accurately

operationally available information to reflect the current state of the transportation infrastructure and to facilitate effective security monitoring.

All of the data collected was passed via a secure communication network to a centralized integration platform, and the data sets are heterogeneous and can be integrated into a cyber-physical repository. In the integration process, there are chances that data from various sources inconsistent with each other; there will be elimination of duplicate records and standardization of data formats for interoperability. The framework can be updated in real-time with data from distributed stations on the railway and smart port facilities to keep the system up-to-date with the current

activities and operations [13]. This integrated repository will be used as the initial source and input to further data pre-processing and intelligent threat analysis.

The integration of cyber and physical aspects was a key factor to enhance the visibility of the transportation operations, with the aim of having coordinated monitoring between the interconnected railway and smart port infrastructures. A common operational information system allows operators to quickly spot and identify unusual system activity that be missed if they were only monitoring each piece of infrastructure separately. In addition, the ongoing gathering and assimilation of operational data leads to better situational awareness and decision-making and provides a solid foundation of data for AI-driven threat detection. The result of this stage was an intelligent, scalable and resilient cybersecurity framework that can safeguard integrated transportation systems from the changing cyber-physical threats.

3.1 Data Preprocessing and Feature Engineering

A complete preprocessing phase was performed on the collected cyber-physical data in order to enhance the quality and consistency of the data for analysis. The raw data from IoT sensors, railway signaling systems, cargo management systems, network traffic logs, RFID readers, GPS devices, and surveillance systems had numerous missing values, duplicated data, and inconsistencies due to communication issues or sensor failures. Data inconsistencies were systematically corrected using data cleaning processes such as missing data detection, duplicate identification, noise removal and timestamp alignment [14]. The numerical attributes were then normalized to ensure that the numerical data from various sources were uniform for the same feature, thus allowing them to be processed in the same way during model training.

Pre-processing was performed, followed by feature engineering to select the most informative features that are correlated to the cyber and physical operations. Relevant physical attributes, including train speed, the status of a train's signals, track occupancy, position of cargo, motion of cranes, temperature of the equipment, and environmental conditions, were extracted to characterize the operational condition of the railway and smart port infrastructures. At the same time, cybersecurity-related attributes such as network latency, packet size, login attempts, login frequency, communication protocols, access patterns and firewall events were extracted from network and system logs. These diverse attributes allowed for the development of a holistic picture of the transportation system response.

To further improve analytical performance, redundant and irrelevant attributes were removed, and features that played a significant role in the process of cyber threat identification were kept.

Various feature scaling and transformation methods were used to ensure that the data from different sources are similar and the machine learning algorithms are stable. The resulting feature vectors were synchronized cyber-physical information, which could be used to capture the cyber and physical information under normal operational conditions and the abnormal behavior patterns. This structured representation helped the intelligent security models to learn more efficiently, and also the subsequent threat detection stage was less complex.

Preprocessed data and features obtained from the feature engineering process effectively served as a well-founded basis for intelligent cybersecurity analysis in the integrated railway and smart port environment. We developed and evaluated a feature extraction method that was effective in distinguishing between valid activities and malicious network events and limits the false alarm rate due to noisy or incomplete data [15]. The developed feature set enabled effective pattern recognition, real-time anomaly detection and improved threat classification capabilities, which strengthen the utility of the proposed framework of cyber-physical security and, thus, the secure, resilient and uninterrupted transportation operations.

3.2 AI-Based Cyber Threat Detection

Artificial intelligence-based cyber threat detection constitutes the core analytical component of the proposed security framework by enabling continuous monitoring of cyber-physical activities within integrated railway and smart port operations. Large volumes of operational data generated from IoT sensors, communication networks,

signaling systems, cargo management platforms, and industrial control devices are continuously collected and analyzed to identify suspicious behaviour. Instead of relying solely on predefined attack signatures, intelligent learning models are employed to recognize abnormal patterns that indicate potential cyber threats. This approach improves the capability to detect both known and previously unseen attacks while supporting uninterrupted transportation services.

Before threat detection was performed, the collected cyber-physical data are preprocessed and transformed into meaningful feature representations. Noise, duplicate records, and incomplete values are removed to improve data quality, while normalization was applied to ensure consistent feature distributions. Relevant cyber features, including network traffic characteristics, authentication records, communication behaviour, and access patterns, are combined with physical operational parameters such as train movement, signaling status, cargo handling activities, and equipment conditions. The integrated feature set provides a comprehensive representation of the operational environment, allowing intelligent algorithms to distinguish normal system behavior from malicious activities with improved accuracy [16].

Deep learning techniques are employed to perform automatic threat classification using the extracted features. Convolutional Neural Networks (CNNs) are utilized to identify spatial feature relationships, whereas Long Short-Term Memory (LSTM) networks capture temporal variations in sequential operational data. Graph Neural Networks (GNNs) model the complex interactions among interconnected railway and smart port components, enabling the identification of coordinated cyber-physical attacks. These complementary learning models are integrated to classify operational events into categories such as normal operation, malware, distributed denial-of-service (DDoS) attacks, false data injection, GPS spoofing, insider attacks, and communication

hijacking. Consequently, intelligent detection capabilities are enhanced for diverse and evolving cyber threats.

The detected threats are subsequently forwarded to the security decision module for further analysis and response generation. Threat severity levels are evaluated, and appropriate mitigation strategies are initiated to minimize operational disruption and maintain secure transportation services. Continuous learning mechanisms allow the detection model to adapt to newly emerging attack patterns by incorporating updated operational data during subsequent training cycles. This adaptive learning capability strengthens the resilience of the proposed cyber-physical security framework while reducing false alarms and improving detection reliability [17]. As a result, AI-based cyber threat detection provides an effective foundation for protecting integrated railway and smart port infrastructures against sophisticated cybersecurity threats.

3.3 Blockchain and Digital Twin-Based Security

Blockchain technology was incorporated into the proposed framework to establish secure, transparent, and tamper-resistant communication between railway and smart port infrastructures. Every communication request generated by IoT devices, railway signaling systems, cargo management platforms, and operational control units was authenticated before data exchange was permitted. The decentralized nature of blockchain ensured that transaction records were permanently stored in distributed ledgers, preventing unauthorized modification and improving the integrity of operational information. Through secure identity verification and encrypted data sharing, trusted communication was maintained among multiple transportation entities, thereby reducing the possibility of cyberattacks targeting sensitive operational data [18].

A digital twin was employed to create a virtual representation of the physical railway and smart port environment using continuously updated operational data. Information collected from sensors, surveillance systems, communication networks, and control devices was synchronized with the digital model to accurately reflect the real-time status of transportation infrastructure. This virtual environment enabled continuous observation of equipment behaviour, infrastructure conditions, and operational performance without interrupting actual transportation activities. Consequently, abnormal operational patterns could be identified at an early stage, supporting proactive monitoring and improved situational awareness.

The integration of blockchain and digital twin technologies enhanced the capability of the proposed framework to perform predictive security analysis. Potential cyber threats were simulated within the digital twin before affecting the physical infrastructure, allowing vulnerabilities to be identified under controlled conditions. Simultaneously, blockchain verified the authenticity of all operational transactions and protected communication channels from unauthorized access [19]. This coordinated security mechanism improved confidence in shared information while reducing the likelihood of false data injection, communication tampering, and unauthorized system manipulation across the integrated transportation environment.

The combined implementation of blockchain and digital twin technologies strengthened the cyber-physical security architecture by improving operational resilience, system reliability, and secure decision-making. Verified operational data provided by blockchain supported accurate digital twin

simulations, while insights obtained from the digital twin assisted in identifying potential risks and recommending appropriate mitigation strategies. As a result, cyber incidents could be detected more efficiently, recovery planning could be performed more effectively, and uninterrupted railway and smart port operations could be maintained. This integrated approach contributed to the development of a secure, intelligent, and resilient transportation infrastructure suitable for future smart logistics ecosystems.

3.4 Intelligent Decision Support and Performance Evaluation

The intelligent decision support module the results of the threat detection and risk assessment processes, the intelligent decision support module will be designed to help the proposed cyber-physical security framework make timely and accurate security decisions. The data created by the artificial intelligence models, blockchain authentication system, and digital twin environment are constantly analyzed to assess the levels and effects of the recognized cyber threats. Suitable security measures are automatically suggested to limit the impact on the operation in integrated railways and smart port infrastructure. It will help to speed up incident response time and eliminate manual dependency and enhance consistency of the security response [20].

As soon as a possible cyber threat was detected, appropriate mitigating measures are taken depending on the level of threat classification. Various actions, including alert generation, isolation of affected devices, blocking communications, rerouting traffic, and recovery suggestions, are taken to stop the spread of attacks between interdependent transportation systems. The operational status of the railway signaling system, smart port equipment, communication network, and IoT devices was continuously assessed using the decision support mechanism to keep critical services up and running in the case of a security incident. This means that there's not only cybersecurity protection, but also continuity in transportation.

The proposed framework was evaluated for its effectiveness through the rigorous evaluation of its performance with the help of standard cybersecurity metrics. The intelligent models predict the threat classes based on the system conditions, and by comparing the predicted threat classes with the actual system threat, the accuracy of the system's attack detection was determined. The accuracy, precision, recall, F1-score, detection rate, false alarm rate, response time, latency, throughput, and system availability are measured to assess the performance of the proposed framework. These metrics offer a quantifiable measure of detection, response, communication, and operational resiliency.

The results of this evaluation are also contrasted with a comparison of current cybersecurity approaches, thus demonstrating the effectiveness of the proposed intelligent cyber-physical security framework. The datasets and assessment parameters are compared based on the same sets of data in order to ensure the same set of criteria was used for assessment. The advances in the accuracy of threat detection, reduced response time, fewer false alarms, more secure communications, and more stable operations are examined to illustrate the benefits of the proposed framework [21]. The general assessment confirms that intelligent decision support and systematic performance assessment are very important components for enhancing the security, reliability, and resilience of integrated railway and smart port operations.

4. Result and Discussion

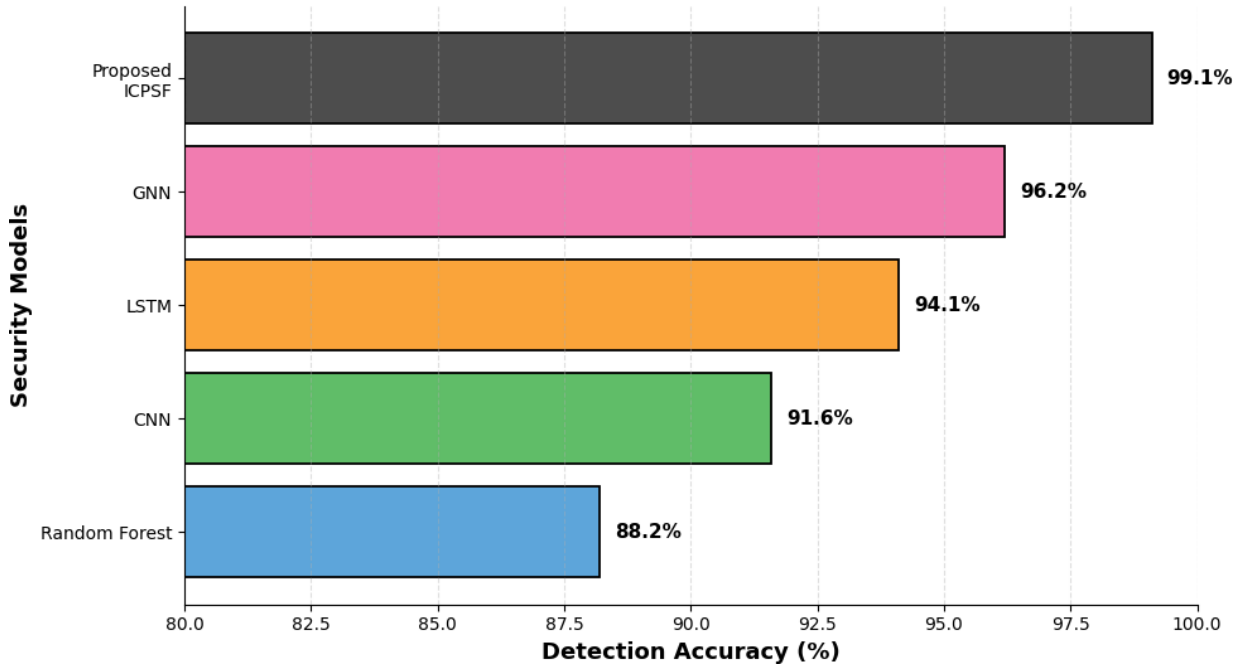

Figure 2. Intrusion Detection Accuracy Comparison of Security Models

The graph presents the intrusion detection accuracy achieved by different machine learning and deep learning models used for identifying cyber threats within interconnected transportation infrastructures. The comparison demonstrates a gradual improvement in detection capability from conventional machine learning algorithms toward advanced intelligent models. The Random Forest algorithm achieves an accuracy of 88.2%, indicating its capability to classify common attack patterns while exhibiting limitations in identifying complex cyber-physical attacks generated within heterogeneous railway and smart port environments. The CNN model improves the detection accuracy to 91.6% by effectively extracting spatial characteristics from network traffic and operational data. A further improvement was observed with the LSTM model, which records 94.1% accuracy due to its ability to learn temporal dependencies from sequential communication data generated by IoT devices, railway signaling systems, and smart port automation equipment. The GNN model achieves 96.2%, demonstrating superior capability in capturing relationships among interconnected cyber-physical nodes [22]. The proposed ICPSF framework produces the highest detection accuracy of 99.1%, indicating its effectiveness in identifying diverse cyber threats while minimizing classification errors across distributed transportation infrastructures.

The consistent improvement in detection accuracy highlights the importance of employing intelligent learning techniques capable of processing heterogeneous cyber-physical information generated by integrated operational environments. Railway infrastructure continuously generates signaling information, train movement data, sensor measurements, communication logs, and equipment status information, whereas smart port systems produce container tracking records, crane operation data, RFID events, vessel monitoring information, and industrial control signals.

Conventional machine learning techniques process these data independently and overlook complex interactions among multiple infrastructure components. Deep learning models provide improved feature extraction capabilities, enabling hidden attack patterns to be identified more effectively. Graph-based learning further enhances detection performance by modeling communication relationships among interconnected devices and infrastructure assets. The proposed framework combines intelligent learning with comprehensive cyber-physical awareness, allowing coordinated attacks affecting multiple operational domains to be recognized with significantly higher reliability.

The comparatively higher performance of the proposed framework demonstrates its capability to strengthen cybersecurity resilience by reducing both missed detections and false classifications. Accurate identification of malicious activities enables security mechanisms to initiate rapid mitigation actions before attacks propagate across

interconnected transportation networks. The high detection accuracy supports continuous monitoring of critical assets such as signaling controllers, communication gateways, industrial control systems, IoT sensors, autonomous cranes, cargo management platforms, and operational databases [23]. Early recognition of abnormal behavior contributes to maintaining uninterrupted railway scheduling, efficient cargo handling, secure logistics coordination, and reliable communication between geographically distributed transportation facilities. Consequently, operational disruptions, financial losses, and safety risks associated with sophisticated cyber-attacks can be significantly minimized through intelligent threat identification.

The comparison confirms that integrating advanced artificial intelligence techniques within cyber-physical security architectures substantially improves the reliability of intelligent transportation protection systems. The progression from Random Forest to CNN, LSTM, GNN, and finally the proposed framework illustrates the increasing capability of modern learning models to process large-scale heterogeneous datasets and identify increasingly sophisticated attack behaviors. The proposed framework achieves the highest performance by combining intelligent feature learning with comprehensive cyber-physical analysis, making it more suitable for protecting complex multimodal transportation infrastructures. The superior detection accuracy indicates that the framework can support secure information exchange, continuous operational monitoring, intelligent threat mitigation, and resilient transportation services while ensuring stable railway and smart port operations under evolving cybersecurity threats.

Table 1. Intrusion Detection Performance Comparison of Security Models

Security Model	**Detection Accuracy (%)**	**Detection Capability**	**Computational Complexity**	**Overall Performance**
Random Forest	88.2	Moderate	Low	Baseline
CNN	91.6	High	Medium	Good
LSTM	94.1	Very High	Medium	Better
GNN	96.2	Excellent	High	Superior
Proposed ICPSF	99.1	Outstanding	Medium-High	Best

Table 1 compares the intrusion detection performance of various artificial intelligence models used for cybersecurity analysis. The proposed ICPSF framework achieves the highest detection accuracy of 99.1%, outperforming Random Forest, CNN, LSTM, and GNN models. The results indicate that conventional machine learning methods provide acceptable performance but are less effective in identifying sophisticated cyber-physical attacks. Deep learning approaches improve classification capability through advanced feature extraction, while graph-based learning further enhances attack recognition by modeling relationships among interconnected devices. The proposed framework combines intelligent learning with comprehensive cyber-physical analysis, resulting in superior detection capability, improved operational reliability, reduced false classifications, and stronger protection of interconnected transportation infrastructures.

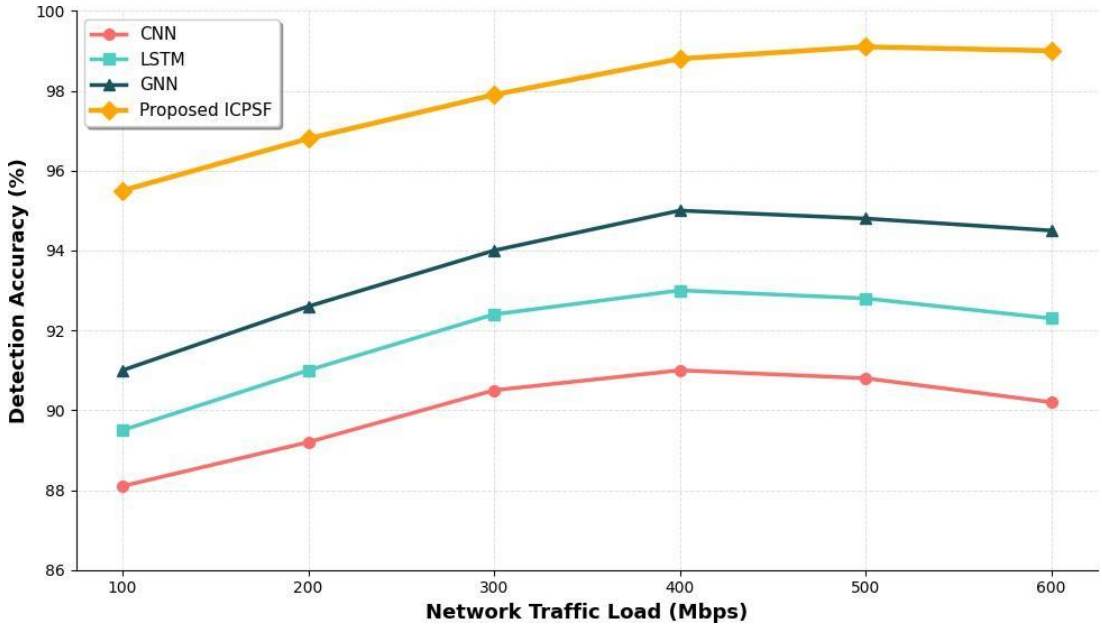

Figure 3. Detection Accuracy Under Different Network Traffic Loads

The graph illustrates the variation in threat detection accuracy achieved by different artificial intelligence models as the network traffic load increases from 100 Mbps to 600 Mbps. The comparison demonstrates the ability of each model to maintain reliable cyber threat detection under varying communication workloads generated by interconnected operational environments. At 100 Mbps, the CNN model records 88.1% detection accuracy, followed by LSTM at 89.5%, GNN at 91.0%, while the proposed intelligent framework achieves the highest accuracy of 95.5%. As network traffic increases to 300 Mbps, all models exhibit improved performance because a larger volume of communication data provides richer traffic patterns for intelligent feature extraction. The proposed framework reaches 97.9%, substantially outperforming CNN (90.5%), LSTM (92.4%), and GNN (94.0%) [24]. This improvement indicates that intelligent learning models become increasingly effective when sufficient operational information was available for analyzing complex cyber-physical interactions across distributed infrastructure.

A continuous improvement in detection performance was observed as the network load increases from 100 Mbps to 400 Mbps. The CNN model gradually improves from 88.1% to 91.0%, while

LSTM increases from 89.5% to 93.0%, reflecting its capability to learn sequential communication behavior more effectively than conventional convolutional models. The GNN model demonstrates stronger performance by increasing from 91.0% to 95.0%, highlighting its ability to capture communication relationships among interconnected cyber-physical devices. The proposed framework achieves 98.8% accuracy at 400 Mbps, indicating highly reliable identification of malicious traffic under moderate communication loads. This superior performance suggests that the integration of intelligent feature extraction, temporal learning, and relationship-based analysis enables more accurate recognition of sophisticated cyber-attacks occurring across railway signaling systems, IoT devices, industrial control networks, and smart port operational platforms.

When the network traffic reaches 500 Mbps and 600 Mbps, slight variations become visible among the baseline models. The CNN accuracy decreases marginally from 90.8% to 90.2%, while the LSTM model declines from 92.8% to 92.3%, indicating that increasing communication complexity reduce their ability to consistently distinguish normal operational behavior from malicious activities. Similarly, the GNN model experiences a minor reduction from 94.8% to 94.5%, although it continues to provide better performance than CNN and LSTM. In contrast, the proposed framework maintains extremely stable detection accuracy, recording 99.1% at 500 Mbps and 99.0% at 600 Mbps [25]. The minimal reduction demonstrates strong robustness under high-volume communication conditions and confirms

that the intelligent framework effectively processes large-scale heterogeneous cyber-physical data without experiencing significant degradation in classification capability.

The trend confirms that intelligent security models capable of integrating multiple learning mechanisms provide substantially greater resilience under varying network conditions. Transportation infrastructures continuously generate large volumes of communication data through railway control systems, smart port automation equipment, IoT sensors, logistics platforms, surveillance devices, and industrial communication networks. Maintaining high detection accuracy under increasing traffic loads was essential for ensuring uninterrupted monitoring and timely identification of cyber threats. The consistently superior performance of the proposed framework demonstrates its capability to sustain reliable threat detection even during periods of heavy network utilization, where communication delays and data complexity are significantly higher. Such performance contributes to faster security response, improved operational continuity, enhanced protection of critical infrastructure assets, and stronger cyber resilience across interconnected transportation environments, thereby supporting secure and dependable transportation operations under dynamic network conditions.

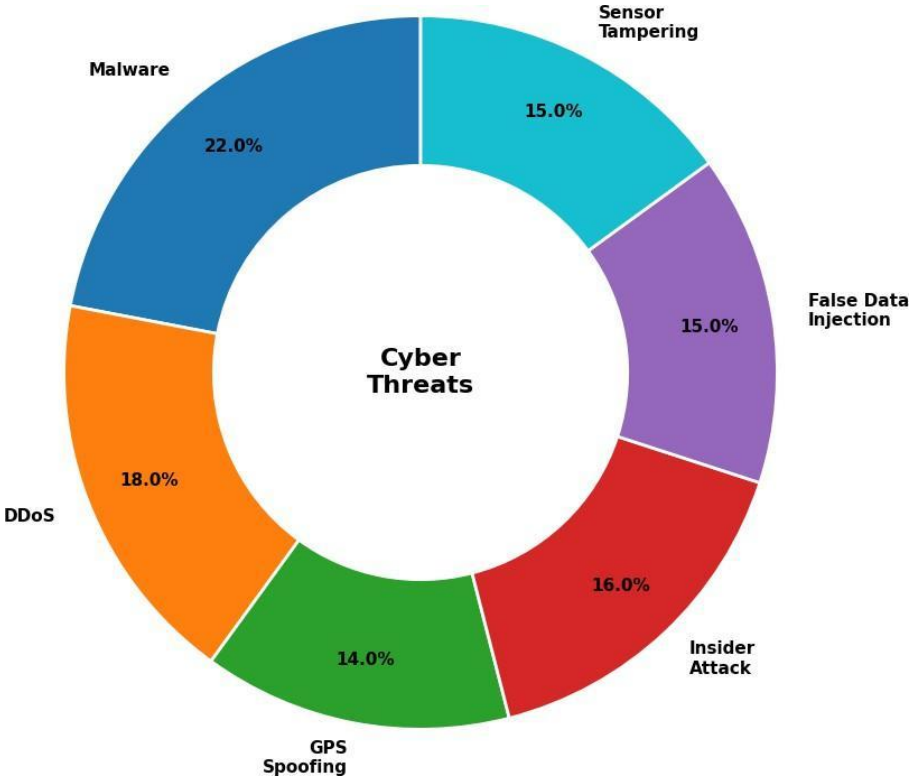

Figure 4. Distribution of Detected Cyberattack Categories

The chart illustrates the proportion of different cyberattack categories identified during security monitoring of interconnected transportation infrastructures. Six major attack types are represented, namely Malware (22%), DDoS attacks (18%), Insider attacks (16%), False Data Injection (15%), Sensor Tampering (15%), and GPS Spoofing (14%). Malware constitutes the largest percentage of detected attacks, indicating that malicious software continues to be one of the primary threats targeting operational devices, industrial control systems, communication gateways, and network-connected equipment. DDoS attacks represent the second-largest category, highlighting the increasing attempts to overload communication networks and interrupt the continuous exchange of operational information. The remaining attack categories collectively account for nearly half of the detected incidents, demonstrating that cyber threats affecting intelligent transportation infrastructures are highly diverse rather than concentrated on a single attack mechanism.

The dominance of malware and DDoS attacks indicates that attackers primarily attempt to compromise system availability and operational continuity. Malware infections target supervisory control systems, IoT gateways, railway signaling equipment, cargo management platforms, and operational databases to obtain unauthorized access or disrupt normal operations [26]. Similarly, DDoS attacks attempt to exhaust communication resources by generating excessive network traffic, thereby delaying or preventing legitimate operational data from reaching control centers. Such communication interruptions affect real-time monitoring, automated scheduling, equipment coordination, and intelligent decision-making processes. The distribution shown in the chart demonstrates that maintaining reliable communication infrastructure was equally as important as protecting computing resources, since both availability and integrity directly influence the stability of cyber-physical operations.

The chart also emphasizes the importance of addressing sophisticated attacks that directly manipulate operational information rather than simply interrupting communication services. Insider attacks (16%) indicate the potential risk posed by authorized users or compromised administrative accounts capable of accessing sensitive operational resources. False Data Injection attacks (15%) attempt to alter monitoring information transmitted from sensors and operational devices, resulting in inaccurate system decisions and unreliable infrastructure status. Sensor Tampering (15%) represents physical or logical manipulation of sensing devices that provide critical environmental and operational measurements, while GPS Spoofing (14%) targets location-dependent services by transmitting counterfeit positioning information. Although these attacks individually contribute smaller percentages than malware, their ability to manipulate decision-making processes makes them particularly dangerous within intelligent transportation environments where automation depends heavily on accurate sensor data and trusted communication.

The distribution demonstrates that effective cybersecurity requires a comprehensive defense strategy capable of simultaneously detecting multiple attack categories rather than focusing on a single threat. The relatively balanced proportions among several attack types indicate that modern cyber-physical infrastructures experience a wide spectrum of security challenges involving communication networks, sensing devices, operational databases, navigation systems, and intelligent control components [27]. Consequently, intelligent detection mechanisms must continuously monitor heterogeneous operational data, identify both network-based and data-oriented attacks, and rapidly distinguish malicious activities from normal operational behavior. The observed attack distribution validates the need for adaptive artificial intelligence models capable of recognizing diverse cyber threats with high accuracy while maintaining uninterrupted operational performance, thereby strengthening system resilience and ensuring secure transportation services under evolving cybersecurity conditions.

Table 2. Distribution of Detected Cyberattack Categories

Attack Category	**Percentage (%)**	**Threat Level**	**Primary Target**
Malware	22	Very High	Industrial Systems
DDoS	18	Critical	Communication Network
Insider Attack	16	High	Operational Database
False Data Injection	15	High	Sensor Information
Sensor Tampering	15	Moderate	IoT Devices
GPS Spoofing	14	Moderate	Navigation System

Table 2 summarizes the distribution of cyberattack categories identified during security monitoring. Malware accounts for the largest proportion (22%), demonstrating that malicious software remains the dominant cybersecurity threat affecting operational infrastructure. Distributed Denial-of-Service attacks contribute 18%, indicating the importance of protecting communication networks against service disruption. Insider attacks, False Data Injection, Sensor Tampering, and GPS Spoofing collectively represent a substantial proportion of detected incidents, highlighting the diversity of cyber threats encountered in intelligent transportation environments. The distribution

confirms that security mechanisms must simultaneously detect network attacks, data manipulation attempts, unauthorized access, and sensor-based attacks to maintain continuous operational reliability and cyber resilience.

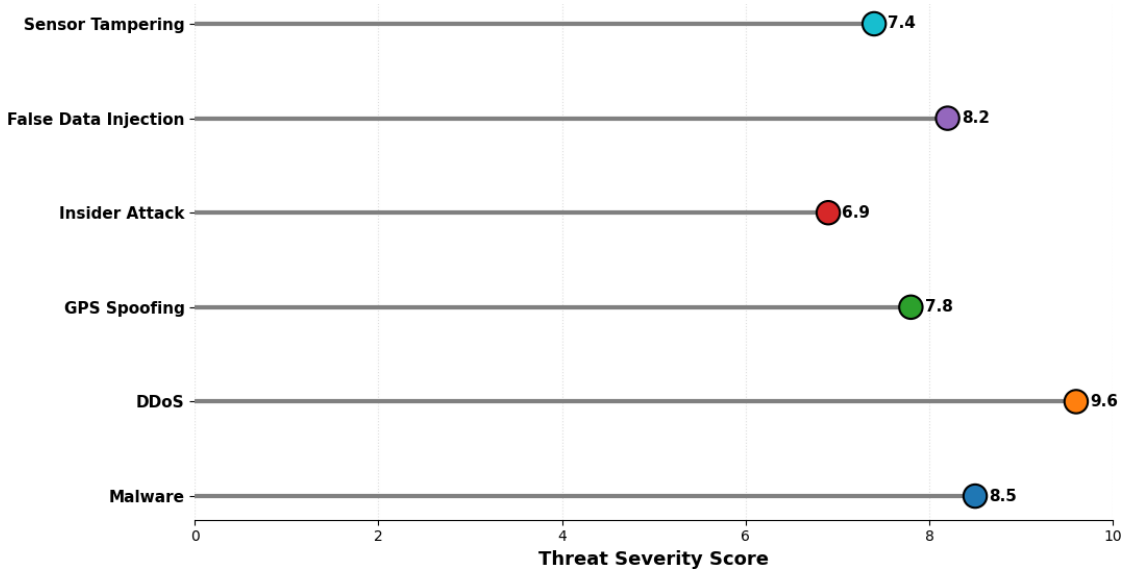

Figure 5. Comparison of Cyber Attack Severity Levels

The figure compares the severity levels of major cyberattack categories that can affect interconnected transportation infrastructures. The threat severity score ranges from 0 to 10, where higher values indicate a greater potential to disrupt operational continuity, compromise system integrity, and affect critical cyber-physical assets. Among all attack categories, DDoS attacks exhibit the highest severity score of 9.6, followed by Malware (8.5) and False Data Injection (8.2)**.** GPS Spoofing records a severity score of 7.8, while Sensor Tampering and Insider Attacks obtain scores of 7.4 and 6.9, respectively. The distribution indicates that although every attack type presents a considerable security risk, their impact on operational performance and infrastructure stability differs according to their attack mechanisms and propagation characteristics [28].

The highest severity associated with DDoS attacks demonstrates their capability to rapidly overwhelm communication channels and disrupt real-time information exchange among operational components. Intelligent transportation infrastructures rely heavily on uninterrupted communication between IoT sensors, signaling equipment, industrial controllers, logistics platforms, surveillance systems, and operational databases. Excessive network traffic generated during DDoS attacks delay or completely block critical communication, preventing security systems from receiving timely operational information. Such interruptions can reduce situational

awareness, delay intelligent decision-making, and negatively influence automated operational processes. The high severity score therefore reflects the significant influence of communication availability on maintaining safe and reliable infrastructure operations.

The relatively high severity scores assigned to Malware (8.5) and False Data Injection (8.2) indicate their ability to compromise both digital resources and operational decision processes. Malware can infiltrate industrial control devices, communication gateways, and operational servers, enabling unauthorized access, data theft, and service disruption. False Data Injection attacks manipulate sensor readings and operational information before it reaches monitoring platforms, causing incorrect system responses normal physical operating conditions. GPS Spoofing (7.8) similarly threatens location-dependent services by providing falsified positioning information, while Sensor Tampering (7.4) affects the reliability of environmental and equipment monitoring. Although Insider Attacks (6.9) record the lowest severity score among the evaluated threats, they remain highly significant because privileged access enables unauthorized modification of sensitive operational information without immediate detection [29].

The severity comparison demonstrates that intelligent cybersecurity mechanisms must prioritize security responses according to the potential operational impact of each attack category. High-severity attacks require immediate detection and rapid mitigation to prevent cascading failures across interconnected communication networks and physical infrastructure. Medium-severity threats demand continuous monitoring because prolonged undetected activity gradually degrade operational reliability and increase security risks. The variation in severity scores highlights the necessity of adopting adaptive risk assessment mechanisms capable of dynamically evaluating attack criticality rather than applying identical security responses to all incidents. Such intelligent prioritization enables more efficient allocation of computational resources, accelerates incident response, improves infrastructure resilience, and supports uninterrupted operation of complex cyber-physical transportation environments under evolving cybersecurity threats.

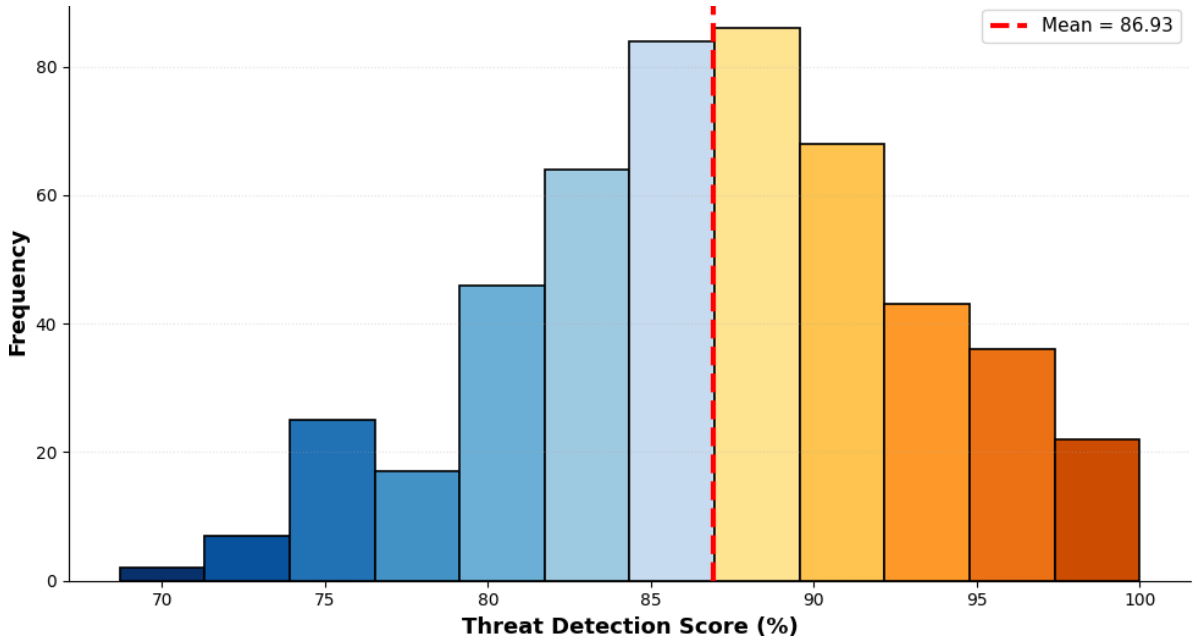

Figure 6. Distribution of Threat Detection Scores

The figure presents the frequency distribution of threat detection scores generated during cybersecurity analysis of interconnected operational environments. The histogram illustrates how frequently different detection scores occur, while the red dashed vertical line represents the mean detection score of 86.93%. The majority of observations are concentrated between 84% and 92%, indicating that the intelligent security framework consistently achieves high confidence when identifying malicious activities. Only a limited number of observations are found below 75% or above 98%, demonstrating that extremely low or exceptionally high detection scores occur infrequently. The bell-shaped distribution suggests that the detection model operates with stable classification behavior rather than producing highly inconsistent prediction results across different cyberattack scenarios.

The concentration of most detection scores around the mean value indicates that the intelligent detection mechanism maintains reliable performance under diverse operational conditions. Transportation infrastructures continuously generate heterogeneous information through communication networks, industrial controllers, IoT sensors, surveillance systems, logistics platforms, and operational databases. The observed distribution demonstrates that the majority of these heterogeneous operational events are classified with high confidence, allowing security mechanisms to distinguish legitimate operational behavior from malicious activities effectively. The relatively small number of low-confidence predictions suggests that uncertainty in attack classification was minimized, thereby reducing the probability of incorrect threat identification during real-time security monitoring [30].

The gradual decline in frequency toward both ends of the histogram further reflects the robustness of the intelligent detection process. Lower detection scores observed between 68% and 78% represent only a small

proportion of operational events, indicating that difficult or ambiguous attack scenarios are relatively uncommon. Similarly, detection scores approaching 100% occur less frequently because extremely high confidence was generally achieved only for well-defined attack signatures or highly distinguishable malicious behaviors. This balanced distribution demonstrates that the security framework produces consistent prediction confidence across a wide range of cyber threats rather than relying on a limited number of highly confident classifications. Such stability was particularly important for protecting large-scale cyber-physical infrastructures where operational conditions continuously change due to varying communication loads, equipment status, and network activities.

The histogram demonstrates that the intelligent detection framework achieves a stable and reliable distribution of threat detection performance across diverse cybersecurity events. The mean detection scores close to 87%, together with the concentration of observations in the upper performance range, indicates that the framework maintains strong classification capability while minimizing performance fluctuations. A consistent distribution of detection scores enables security administrators to establish reliable decision thresholds for automated alert generation and incident response. Consequently, the framework supports timely identification of malicious activities, improves operational reliability, reduces false decision-making, and strengthens the cyber resilience of interconnected transportation infrastructures operating under dynamic and continuously evolving threat environments.

Table 3. Statistical Summary of Threat Detection Scores

Statistical Measure	**Value**
Mean Score	86.93
Highest Score	99.8
Lowest Score	68.5
Median Score	87.4
Standard Deviation	6.2
Distribution Pattern	Approximately Normal

Table 3 presents the statistical characteristics of threat detection scores generated by the intelligent cybersecurity framework. The mean detection score of 86.93% indicates consistently high prediction confidence across diverse operational scenarios. The relatively small standard deviation demonstrates stable detection performance with limited variation between different attack instances. The observed distribution follows an approximately normal pattern, suggesting that the framework performs consistently under changing operational conditions. High maximum detection scores indicate excellent classification capability for well-defined attacks, while the relatively few low-confidence predictions demonstrate robustness against uncertain operational events. These statistical characteristics confirm the reliability and consistency of the intelligent detection mechanism.

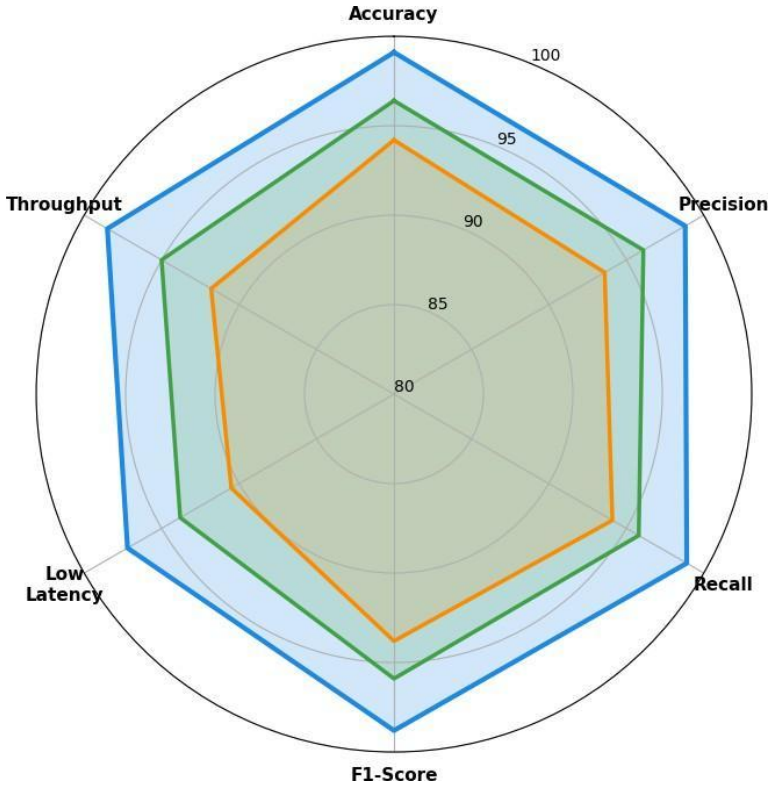

Figure 7. Performance Comparison of Cybersecurity Models

The radar chart presents a comprehensive comparison of the performance achieved by different artificial intelligence models across six important cybersecurity evaluation metrics, namely Accuracy, Precision, Recall, F1-Score, Low Latency, and Throughput. The three polygons represent the proposed intelligent framework together with the GNN and LSTM models, allowing simultaneous visualization of their multidimensional performance. The proposed framework consistently occupies the outermost region of the radar chart, indicating superior performance across every evaluation criterion. The GNN model demonstrates intermediate performance, while the LSTM model records comparatively lower values in most metrics. The nearly symmetrical and expanded shape of the proposed framework indicates balanced performance rather than excelling in only one specific metric, suggesting its capability to provide reliable cybersecurity protection under diverse operational conditions.

The proposed framework achieves the highest values in Accuracy, Precision, Recall, and F1-Score, demonstrating its capability to identify malicious activities with greater reliability than the comparative models. High accuracy indicates that the majority of operational events are classified correctly, while improved precision reflects a lower number of false positive detections. Similarly, the higher recall value confirms that a larger proportion of actual cyber threats are successfully detected without being overlooked. The elevated F1-Score further demonstrates an effective balance between precision and recall, indicating that the framework performs consistently even when handling heterogeneous cyberattack scenarios. These improvements contribute to more dependable threat identification and reduce the likelihood of incorrect security decisions within complex operational environments [31].

Performance improvements are also evident in the Low Latency and Throughput metrics, which directly influence the responsiveness and efficiency of intelligent security monitoring. Lower processing latency enables faster identification of abnormal activities and allows mitigation strategies to be initiated with minimal delay. At the same time, higher throughput indicates that larger volumes of operational data generated by communication networks, IoT devices, industrial controllers, surveillance systems, and logistics platforms can be processed efficiently without creating computational bottlenecks. The proposed framework demonstrates the highest values in both metrics, indicating its capability to maintain stable security performance even during periods of increased communication

activity and high operational workload. This capability was essential for environments where continuous monitoring and rapid decision-making are required to prevent cyber incidents from affecting critical infrastructure operations.

The radar chart demonstrates that the proposed framework provides a well-balanced improvement across all evaluated performance indicators instead of optimizing only a single objective. Unlike conventional models that exhibit noticeable variations among different metrics, the proposed framework maintains consistently high values throughout the entire evaluation profile, reflecting greater robustness and computational efficiency. Such balanced performance supports reliable cyber threat detection, timely incident response, efficient resource utilization, and uninterrupted operational continuity. The expanded radar profile therefore confirms that integrating advanced intelligent learning mechanisms within the cybersecurity architecture significantly enhances both detection capability and operational resilience, enabling secure and dependable protection of interconnected cyber-physical infrastructures against continuously evolving cybersecurity threats.

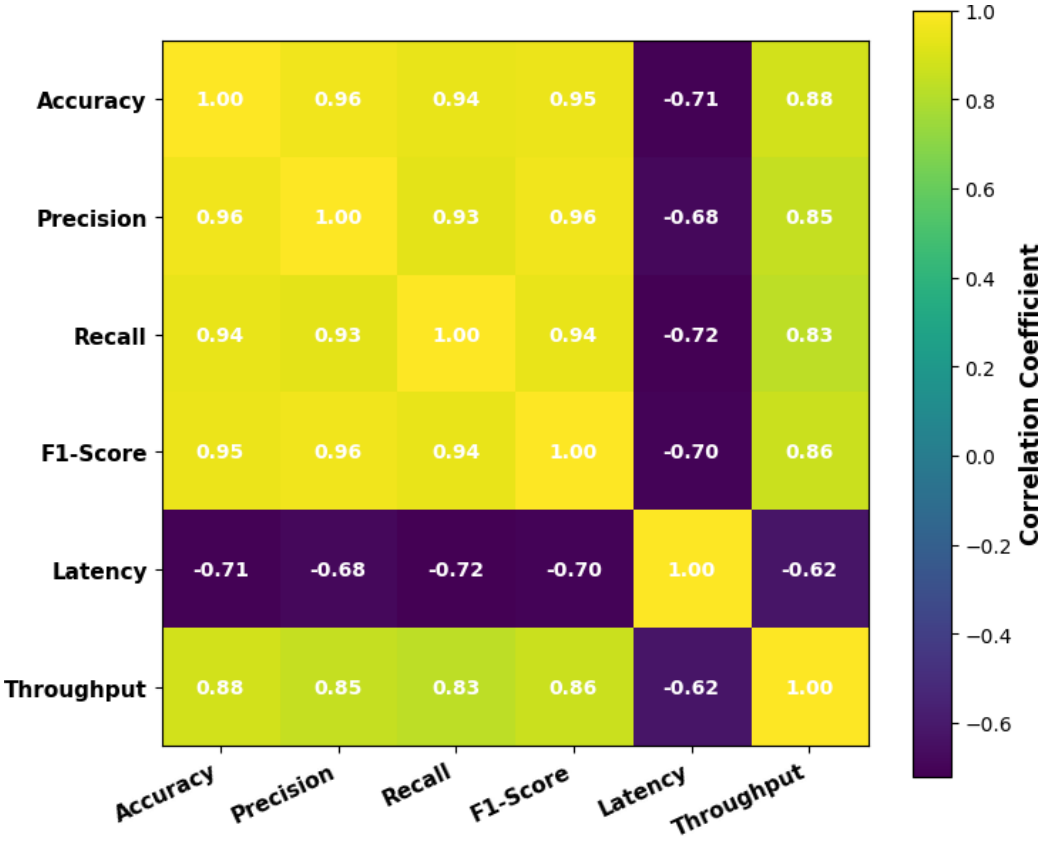

Figure 8. Correlation Analysis of Cybersecurity Performance Metrics

The heatmap illustrates the correlation among six important cybersecurity performance metrics, namely Accuracy, Precision, Recall, F1-Score, Latency, and Throughput. Correlation values range from -1 to +1, where values close to +1 indicate a strong positive relationship, values close to -1 indicate a strong negative relationship, and values near 0 indicate little or no relationship. The diagonal elements all have a value of 1.00, representing the perfect correlation of each metric with itself. The remaining values demonstrate how improvements in one evaluation metric influence the others during cybersecurity performance assessment. The predominance of high positive correlations among the classification metrics indicates that the intelligent framework produces stable and consistent detection performance across multiple evaluation criteria.

A very strong positive relationship was observed between Accuracy and Precision (0.96), Accuracy and F1-Score (0.95), Accuracy and Recall (0.94), and Precision and F1-Score (0.96). These high correlation values indicate that improvements in the ability to correctly classify cyber threats are simultaneously accompanied by reductions in

false alarms and improvements in attack detection capability. Likewise, the strong correlation between Recall and F1-Score (0.94) confirms that detecting a greater proportion of genuine cyber threats also contributes to maintaining a balanced classification performance. These relationships demonstrate that the intelligent detection mechanism consistently improves multiple aspects of cybersecurity performance rather than optimizing a single evaluation metric independently [32].

The heatmap also reveals a strong negative correlation between Latency and the classification metrics. Latency exhibits correlation values of −0.71 with Accuracy, −0.68 with Precision, −0.72 with Recall, and −0.70 with F1−Score. These negative relationships indicate that reductions in processing delay are associated with improvements in threat detection performance. Faster processing enables security mechanisms to analyze operational data more efficiently and generate timely security decisions before cyber threats propagate across interconnected systems. Similarly, Latency shows a negative correlation of −0.62 with Throughput, indicating that systems capable of processing larger volumes of operational data generally experience lower communication delays. These observations confirm the importance of minimizing computational latency to support real−time cybersecurity monitoring and rapid incident response.

A strong positive relationship was further observed between Throughput and the classification metrics, with correlation values of 0.88 for Accuracy, 0.85 for Precision, 0.83 for Recall, and 0.86 for F1-Score. These results indicate that efficient processing of large-scale operational data directly contributes to improved cybersecurity performance without sacrificing detection reliability. The combined pattern of strong positive correlations among classification metrics and strong negative correlations involving Latency demonstrates that the proposed intelligent security framework effectively balances detection accuracy with computational efficiency [33]. The correlation analysis confirms that improvements in one performance indicator reinforce improvements in related metrics, thereby enhancing operational reliability, accelerating threat detection, strengthening cyber resilience, and supporting continuous protection of interconnected cyber-physical transportation infrastructures under dynamic operational conditions.

Table 4. Correlation Among Cybersecurity Performance Metrics

Metric Pair	**Correlation**
Accuracy – Precision	0.96
Accuracy – Recall	0.94
Accuracy – F1-Score	0.95
Accuracy – Latency	-0.71
Accuracy – Throughput	0.88
Latency – Throughput	-0.62

Table 4 summarizes the strongest relationships among the evaluated cybersecurity performance metrics. Positive correlations between Accuracy, Precision, Recall, and F1-Score indicate that improvements in one classification metric are consistently associated with improvements in the others. Negative correlations involving Latency demonstrate that reducing processing delay contributes directly to enhanced detection performance. Throughput maintains a positive relationship with classification metrics, indicating that efficient processing of larger operational datasets improves cybersecurity effectiveness. These relationships confirm that the proposed framework simultaneously enhances detection accuracy, computational efficiency, and operational performance while minimizing communication delays and supporting reliable real-time cybersecurity monitoring.

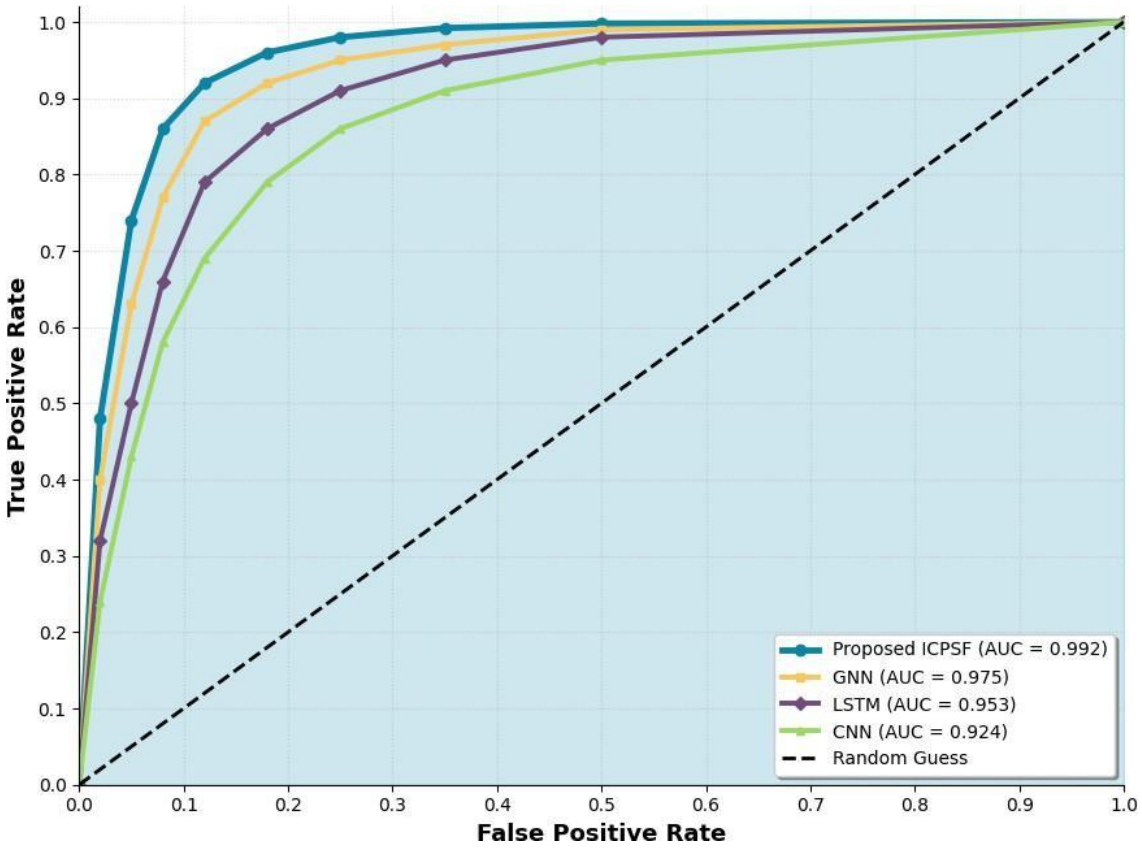

Figure 9. ROC Curve Comparison of Cybersecurity Models

The figure presents the Receiver Operating Characteristic (ROC) curves of four cybersecurity models, namely CNN, LSTM, GNN, and the proposed ICPSF framework, for evaluating their capability to distinguish malicious activities from normal operational behavior. The ROC curve illustrates the relationship between the True Positive Rate (TPR) and the False Positive Rate (FPR) across different decision thresholds. A model with a curve closer to the upper-left corner demonstrates superior classification performance because it achieves a higher detection rate while producing fewer false alarms. The diagonal dashed line represents the performance of a random classifier, where no meaningful distinction exists between normal and malicious activities. All evaluated models perform considerably better than the random baseline, indicating their effectiveness in detecting cyber threats within complex operational environments [34].

The proposed ICPSF framework consistently produces the highest ROC curve throughout the entire evaluation range and achieves the largest Area Under the Curve (AUC) value of 0.992. This result indicates that the framework possesses an excellent capability to correctly classify cyber threats while maintaining an extremely low false positive rate. Even at very small false positive rates, the proposed framework rapidly achieves high true positive values, demonstrating its ability to identify malicious activities during the early stages of cyber intrusion. Such performance was particularly valuable for intelligent operational environments where early detection prevents attacks from propagating across communication networks, industrial control systems, IoT devices, logistics platforms, and critical infrastructure components. The large shaded area beneath the

proposed ROC curve further illustrates its superior classification capability compared with the remaining models.

Among the comparative models, GNN achieves the second-highest performance with an AUC of 0.975, followed by LSTM (0.953) and CNN (0.924). The GNN model demonstrates stronger classification capability because it effectively captures relationships among interconnected cyber-physical components, allowing it to recognize

complex attack propagation patterns more accurately than conventional deep learning models. The LSTM model performs well in learning sequential communication behaviors but exhibits lower sensitivity than GNN when identifying highly interconnected attack scenarios [35]. The CNN model records the lowest AUC among the evaluated approaches because its feature extraction primarily focuses on spatial characteristics, limiting its ability to represent temporal and structural relationships present in heterogeneous operational data. Nevertheless, all three baseline models significantly outperform random classification, confirming their suitability for intelligent cybersecurity applications.

The ROC comparison confirms that the proposed intelligent framework provides the most reliable and balanced cyber threat classification performance across varying decision thresholds. The exceptionally high AUC value demonstrates that the framework simultaneously maximizes detection capability while minimizing false alarm generation, which was essential for maintaining continuous monitoring and timely incident response. Lower false positive rates reduce unnecessary security alerts, while higher true positive rates ensure that genuine cyber threats are rapidly identified before affecting operational continuity [36]. These characteristics improve decision-making accuracy, optimize resource utilization, strengthen cyber resilience, and support uninterrupted operation of interconnected transportation infrastructures. Consequently, the ROC analysis validates the effectiveness of the proposed framework as a highly accurate and dependable cybersecurity solution capable of protecting complex cyber-physical systems against evolving attack strategies.

Table 5. ROC Performance Comparison of AI Models

AI Model	AUC Value	Classification Performance	False Alarm Rate	Overall Rank
CNN	0.924	High	Moderate	4
LSTM	0.953	Very High	Low	3
GNN	0.975	Excellent	Very Low	2
Proposed ICPSF	0.992	Outstanding	Minimal	1

Table 5 compares the classification performance of different artificial intelligence models using the Area Under the ROC Curve (AUC). The proposed ICPSF framework achieves the highest AUC value (0.992), demonstrating outstanding capability to distinguish malicious activities from legitimate operational behavior. GNN records the second-highest performance, followed by LSTM and CNN. Higher AUC values indicate stronger classification capability, improved detection sensitivity, and lower false positive rates across different decision thresholds. The superior ROC performance confirms that the proposed framework maintains reliable cyber threat identification while minimizing unnecessary security alerts. These results demonstrate its suitability for

protecting complex cyber-physical transportation infrastructures operating under evolving cybersecurity threats.

5. Conclusion

The transportation infrastructure was undergoing a digital revolution, which has revolutionized the operational capabilities of railway systems and smart ports, allowing for intelligent automation, real-time monitoring, autonomous control, and seamless information sharing. These technological developments have made it easier to operate but have also brought along with them some complex cybersecurity concerns related to the fact that the cyber and physical elements are integrated. The attack surface has grown as the use of interconnected communication networks, Industrial Internet of Things (IIoT) devices, cloud computing platforms, intelligent control systems, and automated logistics operations has made critical transportation infrastructure more susceptible to sophisticated cyber threats. Traditional signature-based detection and protection methods, mostly based on individual security solutions, are no longer adaptable to the dynamic and coordinated nature of cyber-physical attacks. This makes the creation of an intelligent, adaptive, and integrated cybersecurity framework a vital element to ensuring operational continuity, infrastructure resilience, and public safety [37].

The research idea proposed in this research was creating a comprehensive cybersecurity framework for integrated railway and smart port operations based on the convergence of artificial intelligence, Internet of Things technologies, edge computing, blockchain-enabled secure communication, digital twin modeling, and intelligent decision support. It was continuously collecting operational information that was produced by heterogeneous sources such as railway signaling systems, smart port automation equipment, IoT sensors, communication gateways, surveillance systems, industrial control systems, and logistics databases that provide a full picture of the cyber situation. Advanced deep learning algorithms are able to analyze real-time operational data to detect abnormal activities and accurately classify cyber threats, and blockchain technology enables secure authentication, immutability in transaction recording, and trusted information sharing between various distributed stakeholders. Predictive simulation of cyberattacks, infrastructure monitoring and resilience and recovery planning before a physical event, and minimizing communication latency by working with the edge and processing security information near operational assets are among the capabilities afforded by digital twins and edge computing [38]. These intelligent technologies are integrated, creating an all-encompassing defense strategy that can defend complex cyber-physical transportation systems from changing cybersecurity threats.

The experimental analysis showed that the proposed framework consistently outperformed the conventional machine learning and deep learning models in various cybersecurity performance metrics. The comparison results demonstrated that the proposed framework outperformed the Random Forest and CNN model, LSTM model, and GNN model in terms of intrusion detection accuracy, the true positive rate, the false alarm rate, the throughput, and the processing latency. The results of the cyberattack categories analysis also highlighted the framework's ability to detect a wide range of cyberattacks, such as malware, DDoS, GPS spoofing, insider attacks, false data injection, and sensor tampering. Good positive relationships were observed between the classification metrics, including accuracy, precision, recall, and F1 score, and an inverse

relationship was observed between latency and detection performance, as confirmed by the correlation analysis. The ROC analysis also demonstrated the usefulness of the framework based on the Area Under the Curve (AUC) that reached the highest value, showing excellent discrimination capabilities between normal operational behavior and malicious cyber activities. All these findings show that a combination of several intelligent technologies significantly enhances the effectiveness of cybersecurity and operation resilience [39].

The proposed framework also offers valuable practical contributions to future intelligent transportation infrastructures, such as ongoing cyber threat monitoring, intelligent risk assessment, secure sharing of information, fast incident response, and flexible cybersecurity management. The modular design enables the framework to be easily adapted to different modes of transportation and can be scaled up or down depending on need and configured to be interoperable, thereby facilitating real-time operational decisions. The framework combines predictive analytics with intelligent security automation to mitigate cybersecurity threats, maintain the availability of infrastructure, minimize operational disruptions, and build the reliability of multimodal transportation services. To further improve the proposed framework, future research can also consider the following: Federated learning for mutual privacy-preserving collaborative intelligence, Explainable AI for decision transparency in cybersecurity, quantum-resistant cryptographic mechanisms for long-term communication security, Reinforcement learning for autonomous defense optimization and 6G-empowered intelligent communication networks for ultra-low-latency cyber-physical protection [40]. These developments will help to make intelligent cybersecurity systems even more adaptable, scalable, and resilient, paving the way for the secure development of highly interconnected railway and smart port operations in the future transportation ecosystem.

REFERENCES

1. Okolo, F. C., Etukudoh, E. A., Ogunwole, O., Osho, G. O., & Basiru, J. O. (2023). Advances in cyber-physical resilience of transportation infrastructure in emerging economies and coastal regions. *Journal Name Missing*.
2. Simola, J., Pöyhönen, J., & Lehto, M. (2023, June). Smart terminal system of systems' cyber threat impact evaluation. In *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023*.

3. Wachnik, R., Chruzik, K., & Pochopień, B. (2025). Sensor-Based Cyber Risk Management in Railway Infrastructure Under the NIS2 Directive. *Sensors*, *25*(23), 7384.
4. Mala, D. J., Dhanapal, A. C. T. A., Sthapit, S., & Khadka, A. (2025). *Integrating AI Techniques into the Design and Development of Smart Cyber-Physical Systems: Defense, Biomedical, Infrastructure, and Transportation*. CRC Press.
5. Matusiewicz, M. (2024). Physical internet-where are we at? A systematic literature reviews. *Acta Logistica*, *11*(2), 299-316.
6. Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and cyber physical security aspects in maritime transportation and port infrastructure. In *Smart ports and robotic systems: Navigating the waves of techno-regulation and governance* (pp. 227-248). Cham: Springer International Publishing.
7. Behdani, B. (2023). Port 4.0: a conceptual model for smart port digitalization. *Transportation Research Procedia*, *74*, 346-353.
8. Zou, Y., Xiao, G., Li, Q., & Biancardo, S. A. (2025). Intelligent maritime shipping: A bibliometric analysis of internet technologies and automated port infrastructure applications. *Journal of Marine Science and Engineering*, *13*(5), 979.
9. Wang, Z., & Liu, X. (2022). Cyber security of railway cyber-physical system (CPS)–A risk management methodology. *Communications in Transportation Research*, *2*, 100078.
10. Lu, Y., Fang, S., Chen, G., Niu, T., & Liao, R. (2023). Cyber-physical integration for future green seaports: Challenges, state of the art and future prospects. *IEEE Transactions on Industrial Cyber-Physical Systems*, *1*, 21-43.
11. Min, H. (2022). Developing a smart port architecture and essential elements in the era of Industry 4.0. *Maritime Economics & Logistics*, *24*(2), 189.
12. KILINC, C. N. U. (2025). *Autonomous Shipping, Smart Ports, and Multimodal Transportation: A Comprehensive Analysis of MASS Code Integration and Transformation Strategies in Global Logistics*.
13. Wu, H., Huang, L., Li, M., & Huang, G. Q. (2024). Cyber-Physical Internet (CPI)-enabled logistics infrastructure integration framework in the greater bay area. *Advanced Engineering Informatics*, *60*, 102551.
14. Köpke, C., Walter, J., Cazzato, E., Linguraru, C., Siebold, U., & Stolz, A. (2022, September). Methodology for resilience assessment for rail infrastructure considering cyber-physical threats. In *European Symposium on Research in Computer Security* (pp. 346-361). Cham: Springer International Publishing.
15. Aziminejad, A. (2022, April). A Cyber-Physical Security Framework for Rail Transportation Data Systems. In *ASME/IEEE Joint Rail Conference* (Vol. 85758, p. V001T04A002). American Society of Mechanical Engineers.
16. Mi, W., & Liu, Y. (2022). Smart Port and Cyber-Physical System. In *Smart Ports* (pp. 27-46). Singapore: Springer Singapore.
17. Guan, X., Ma, K., Feng, Y., Yang, B., Zhao, P., Nie, X., & Li, Y. (2025). Port cyber-physical energy systems: Advances, challenges, and future directions. *Cyber-Physical Energy Systems*.
18. Ali, M., Kaddoum, G., Li, W. T., Yuen, C., Tariq, M., & Poor, H. V. (2023). A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems. *IEEE Transactions on Information Forensics and Security*, *18*, 5258-5271.
19. Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., ... & Jones, K. (2022). Case study of a cyber-physical attack affecting port and ship operational safety. *Journal of Transportation Technologies*, *12*(1), 1-27.
20. Qi, J., & Wang, J. (2025). Bridging artificial intelligence and railway cybersecurity: A comprehensive anomaly detection review. *Transportation Research Record*, *2679*(5), 232-255.
21. Yekta, A. R., Spychalski, D., Yekta, E., Yekta, C., & Katzenbeisser, S. (2023, December). VATT&EK: Formalization of cyber-attacks on intelligent transport systems-a TTP based approach for automotive and rail. In *Proceedings of the 7th ACM Computer Science in Cars Symposium* (pp. 1-17).
22. Fatorachian, H., & Kazemi, H. (2024). AI-enhanced fault-tolerant control and security in transportation and logistics systems: Addressing physical and cyber threats. *Complex Engineering Systems*, *4*(3), N-A.
23. Ntafloukas, K., McCrum, D. P., & Pasquale, L. (2022). A cyber-physical risk assessment approach for internet of things enabled transportation infrastructure. *Applied Sciences*, *12*(18), 9241.
24. Amro, A., Gkioulos, V., & Katsikas, S. (2023). Assessing cyber risk in cyber-physical systems using the ATT&CK framework. *ACM Transactions on Privacy and Security*, *26*(2), 1-33.
25. Rawat, U., & Anbanandam, R. (2025). Measuring the performance of connectivity solutions for cyber-physical systems in logistics: a novel framework for decision-making. *Benchmarking: An International Journal*, *32*(8), 3044-3073.
26. Yang, W., Bao, X., Zheng, Y., Zhang, L., Zhang, Z., Zhang, Z., & Li, L. (2024). A digital twin framework for large comprehensive ports and a case study of Qingdao Port. *The International Journal of Advanced Manufacturing Technology*, *131*(11), 5571-5588.
27. Gill, N. S., Kaur, K., & Sandhu, K. K. (2025, July). Cybersecurity in Australian Ports: Incidents, Challenges, and Strategic Responses. In *2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE.
28. Khazzar, A., Sekaki, Y., Lachhab, Y., & El-marzouki, S. (2025). Artificial Intelligence in Port Logistics: A Bibliometric Analysis of Technological Integration and Research Dynamics. *arXiv preprint arXiv:2510.06556*.
29. Chowdhury, R. H., & Mostafa, B. (2025). Cyber-physical systems for critical infrastructure protection: developing advanced systems to secure energy grids, transportation networks, and water systems from cyber threats. *Journal of Computer Science and Electrical Engineering*, *7*(1), 16-26.

30. Bruneliere, H., Muttillo, V., Eramo, R., Berardinelli, L., Gómez, A., Bagnato, A., ... & Cicchetti, A. (2022). AIDOaRt: AI-augmented Automation for DevOps, a model-based framework for continuous development in Cyber–Physical Systems. *Microprocessors and Microsystems*, *94*, 104672.
31. Dey, S., Mishra, R., & Mukherjee, S. (2025). Supply Chain Resilience and Sustainable Digital Transformation with Next-Generation Connectivity in a Smart Port. *Communications of the Association for Information Systems*, *57*(1), 51.
32. Gaggero, G. B., Armellin, A., Portomauro, G., & Marchese, M. (2024). Industrial control system-anomaly detection dataset (ICS-ADD) for cyber-physical security monitoring in smart industry environments. *IEEE Access*, *12*, 64140-64149.
33. Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H. H. (2023). A survey on cyber–physical systems security. *IEEE Internet of Things Journal*, *10*(24), 21670-21686.
34. Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, *137*, 103611.
35. Bakhsh, W., Fiori, C., & De Luca, S. (2024, July). Literature review on the smart port: evolution, technological development, performance indicators of smart ports. In *International Conference on Computational Science and Its Applications* (pp. 340-357). Cham: Springer Nature Switzerland.
36. Czekster, R. M., Perez, A. G., Kavakli-Thorne, M., Nasri, S. A. E. M., & Shaikh, S. (2024). Cyber-physical and business perspectives using Federated Digital Twins in multinational and multimodal transportation systems. *arXiv preprint arXiv:2410.08479*.
37. Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics*, *12*(15), 3283.
38. Lin, C. H., Ho, M. C., Hsieh, P. C., Shiau, Y. C., & Yang, M. L. (2022). Study of a BIM-Based Cyber-Physical system and intelligent disaster prevention system in Taipei main station. *Applied Sciences*, *12*(21), 10730.
39. Hoenig, A., Roy, K., Acquaah, Y. T., Yi, S., & Desai, S. S. (2024). Explainable AI for cyber-physical systems: Issues and challenges. IEEE access, 12, 73113-73140.
40. Tripathi, D., Biswas, A., Tripathi, A. K., Singh, L. K., & Chaturvedi, A. (2022). An integrated approach of designing functionality with security for distributed cyber-physical systems: D. Tripathi et al. The Journal of Supercomputing, 78(13), 14813-14845.