Applications of AI/ML in Maritime Cyber Supply Chains

Rafael Diaz  
*Old Dominion University*, rdiaz@odu.edu

Ricardo Ungo  
*Old Dominion University*, rungo@odu.edu

Katie Smith  
*Old Dominion University*

Lida Haghnegahdar  
*Old Dominion University*, lhaghneg@odu.edu

Bikash Singh  
*Old Dominion University*, bsingh@odu.edu

See next page for additional authors

Follow this and additional works at: [https://digitalcommons.odu.edu/cybersecurity-pubs](https://digitalcommons.odu.edu/cybersecurity-pubs)

🔗 Part of the Aeronautical Vehicles Commons, Artificial Intelligence and Robotics Commons, Information Security Commons, and the Operations and Supply Chain Management Commons

**Original Publication Citation**


This Conference Paper is brought to you for free and open access by the School of Cybersecurity at ODU Digital Commons. It has been accepted for inclusion in School of Cybersecurity Faculty Publications by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.
Authors
Rafael Diaz, Ricardo Ungo, Katie Smith, Lida Haghnegahdar, Bikash Singh, and Tran Phuong

This conference paper is available at ODU Digital Commons: https://digitalcommons.odu.edu/cybersecurity-pubs/6
5th International Conference on Industry 4.0 and Smart Manufacturing

Applications of AI /ML in Maritime Cyber Supply Chains

Rafael Diaz,*, Ricardo Ungo, Katie Smith, Lida Haghnegahdar, Bikash Singh, Tran Phuong

*Old Dominion University, Interdisciplinary Studies, School of Cybersecurity, Norfolk, VA, USA
bOld Dominion University, Virginia Modeling, Analysis, and Simulation Center, Norfolk, VA, USA

Abstract

Digital transformation is a new trend that describes enterprise efforts in transitioning manual and likely outdated processes and activities to digital formats dominated by the extensive use of Industry 4.0 elements, including the pervasive use of cyber-physical systems to increase efficiency, reduce waste, and increase responsiveness. A new domain that intersects supply chain management and cybersecurity emerges as many processes as possible of the enterprise require the convergence and synchronizing of resources and information flows in data-driven environments to support planning and execution activities. Protecting the information becomes imperative as big data flows must be parsed and translated into actions requiring speed and accuracy. Machine learning and artificial intelligence have become critical in supporting extensive data collection and real-time processing to assist decision-makers in configuring scarce resources. In this paper, we present four different applications that investigate issues related to the broader maritime supply chain security domain affecting the planning, execution, and performance of complex systems while exploring novel frontiers in cyber research and education. This paper will focus on Machine Learning and AI applications on Unmanned Aerial Systems and Cryptography related to Cybersecurity in Maritimes and Shipbuilding Spheres.

© 2024 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 5th International Conference on Industry 4.0 and Smart Manufacturing

Keywords: Supply Chain Cybersecurity; Maritime and Shipbuilding; Artificial Intelligence; Machine Learning

1. Introduction

The role of the global maritime supply chains is vital. Seaborne trade accounts for almost 70% of US international

* Corresponding author. Tel.: +1-757-683-3030.
E-mail address: rdiaz@odu.edu

© 2024 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 5th International Conference on Industry 4.0 and Smart Manufacturing
10.1016/j.procs.2024.02.140
trade weight\textsuperscript{†}. Global supply chains crucially depend on information exchange among the different actors to ensure efficient trade flows. Likewise, in naval shipbuilding, the manufacturing environment is characterized by the extensive large of suppliers, tier and sub-tier levels distributed worldwide. Any disruption will propagate across all links in the chain, affecting the whole chain's performance and the efficient cargo or parts flow for final customers. The disruption created by the pandemic revealed significant gaps in how supply chain actors communicate and share information. Many of those gaps were related to a lack of end-to-end visibility due to the complexities of long global supply chains. The need for advancing the current trends of digitalization of the supply chain was evident. Digitalization has strengthened the shift towards logistics ecosystems, where multiple actors collaborate and coordinate cargo and supply flows [1, 2]. Because of this, the information is becoming one of the most valuable assets for the participants in the chain. Efficient communication on freight activities leads to greater reliability and profitability.

Propelled by the pandemic, the supply chain industry is increasing its reliance on digital technologies, adopting port, shipbuilder, and warehouse automation advancements, emphasizing smart concepts, and focusing on integrating various networks faster. Although these developments generate gains in operational efficiencies, the new advances in digitalization and IoT also bring greater exposure to cyber threats [3]. Hence, the cybersecurity of the digital supply chain is also an essential component in the evolution of the industry, where malicious actors can target important logistical assets to disrupt the flow of global commerce [3]. This means that digitalization and cybersecurity become the two sides of the same coin. Smart global supply chains require the adoption of secure information exchange to drive efficiencies and increase resilience. The complex nature of long lead times amplifies this exposure to cybercrime, international supply chains, and the diverse universe of supply chain partners involved in the logistics and manufacturing ecosystems [4].

One of the main features of the cybersecurity of a chain of actors is that a particular agent in the chain is responsible for its own security and the cyber-resilience of the whole chain. By the same token, the agents must prepare to face cyber threats to their own facilities and simultaneously prepare the cyber response to attacks aimed at other actors in the chain. As supply chains play a fundamental role in trade and commerce, their resilience and protection against cyber threats are vital, as highlighted in the US Executives Orders (No. 14017, February 2021) “Securing America’s Supply Chains” and (No. 14028, May 2021) “Improving the Nation’s Cybersecurity”. By adopting better data-sharing practices, stakeholders can improve the resilience of the whole logistics and shipbuilding ecosystem.

This paper presents a sample of issues related to the broader maritime supply chain security domain affecting the planning, execution, and performance of complex systems. Our investigations focus on applications of Machine Learning and AI on several dimensions of supply chain cybersecurity as follows. Section 2 presents the foundations of the application of the methodology Adaptive Risk Network Dependency Analysis (ARNDA) to detect hypervulnerabilities that arise over time, float among different nodes (representing suppliers) in a supplier network, and determine their ripple effects. Section 3 presents several ideas related to a Machine Learning (ML)-based security solution for distributed autonomous Unmanned Aerial Vehicles (UAV) swarms and decentralized detection to provide mission assurance in contested environments. Section 4 explores the components of designing and reinforcing resilience against cyberattacks in transfer autonomous learning. Section 5 presents the ideas related to the core ideas of developing a trustworthy smart Data connection to enhance safety at sea for IoT-enabled maritime transportation systems. Finally, Section 6 suggests exploring research lines in the cyber supply chain environment.

2. ARANDEMCMC

The application of Adaptive Risk Network Dependency Analysis (ARNDA) in the naval shipbuilding supply chain [5] is complex. It requires careful considerations whose central idea is to use machine learning to capture dynamic vulnerabilities over time that may be produced by demand, supply, or both simultaneously [6]. This cybersecurity systems framework is under construction that combines a probabilistic graphical model, particularly a dynamics Bayesian Network, with a functional dependency model. Functional dependency models, such as System Operational Dependency Analysis (SODA), allow for lower computational costs and use parameters that have intuitive meaning

\textsuperscript{†} BTS, May 2021
regarding the dependencies between subsystems and components [7]. Our research extends and applies a new risk management framework (ARNDA) and builds a testable prototype to perform a cybersecurity assessment of the supply network connected to the defense shipbuilding supply chain, and particularly, prepares shipbuilders to transition to the Cybersecurity Maturity Model Certification (ARNDA-CMMC). The ARNDA-CMMC framework considers the systematic examination of strategic sectors of the defense shipbuilding industry to monitor disruptions in real-time, determine ripple effects, and enhance the ability of the supply portfolio to recover from node failures in the presence of a cyberattack.

The framework will identify hyper-vulnerable nodes, determine propagation effects, generate data to predict potential supply failures, suggest portfolio reconfigurations, and confirm the adequacy of such measures after implementation, emphasizing cybersecurity disruptions, vulnerability, and disruption effects (e.g., delays). Particularly, our endeavors are focused on providing a machine learning-enabled model that allows stakeholders to explore and determine potential interventions, including balancing cybersecurity compliance with other types of risks.

The research questions we are exploring include examining how cybersecurity compliance issues affect levels of risk and disruption in supply chain networks, more specifically, how non-compliance with DoD-mandated CMMC requirements by various suppliers related to major shipbuilding firms in terms of impact on cost and schedule.

These research questions open doors to examining the extent to which planners can explore and determine potential interventions (policies and practices) to allow them to balance risk trade-offs from cybersecurity compliance issues with other types of risk (e.g., known reliable versus unknown suppliers). The overall focus of the model for the network dependency layer will be a directed graphical model, which is briefly explained as follows.

A theoretical supply chain for a shipboard watertight door will be presented (Fig. 1) as an example to apply ARNDA. This section will present a highly simplified supply network to elucidate concepts and show initial and stochastic results from this novel methodology by modeling typical raw material and manufacturing issues stressing the overall supply chain [8].

![Simplified network representing the supply chain for a watertight door on a ship](image)

**Fig. 1. Simplified network representing the supply chain for a watertight door on a ship [8].**

### 2.1. Multi-layered Networks – The Basics

In general, the network structure for the dependency analysis model can change based on which outputs or performance characteristics are considered. This, coupled with the sparsity of the matrices in the generalized equations under development, means that implementing updated outputs is more natural to view on a layered set of networks with each layer independently. It calculates the updates to one or more output parameters whose dependencies correspond to the given network structure. To simplify the explanations, it will be assumed that each output has a separate corresponding network layer. However, if the graphical forms of the connected network layers for two outcomes are the same, these outputs can be combined into vectors, and their updates can be computed simultaneously. Consider again the supply chain example of a watertight door. Considering the supply chain network from only one perspective, for example, available supply, inhibited the ability of the network dependency analysis model to capture the behavior of the lower-tier suppliers. Now, that same supply chain network will be represented by two separate layers, i.e., supply and demand, each with its network structure (Fig. 2). From an application perspective, this
improvement allows for the consideration of two completely different perspectives in this case, a capacity-based and an information-based view.

The final consideration is handling the aggregation of results into a final output that can be used to calculate resilience behavior over time. This methodology will assume that the specific choice of this aggregation function is application dependent. For example, in a supply chain operating under a produce-to-order inventory control policy, the number of items produced at a given node would be, in the best case, equal to the demand signal of the node and, in the worst case, similar to the supply capacity.

2.2. System’s Behavior

A single run for the watertight door supply chain will be exhibited to show overall behavior and give an example of three-layer aggregation methodologies [8]. In a basic example, assume the supply internal node health result, the door manufacturer experiences a disruption around time 15, while the frame manufacturer experiences a disruption around time 20. Several interesting observations can be made for the simulation runs shown in Fig. 3 and 4. Looking at the supply operability results corresponding interruptions in the operability of the assembly manufacturer and the installer, the ripple effect of this event through the supply chain is shown to have a decreasing impact further downstream, with the result on the assembly manufacturer being less than on the installer. Another example of the ripple effect occurs shortly after time 60 when the steel supply's internal health is assumed to be disrupted.

Looking at the operability plot, the chock manufacturer and installer are affected by this disruption as they are downstream from the steel supply. Assuming additional disruption to installer demand around time 75 for the demand results. Still, the installer's level of resilience allows the development of the recovery to be a new status quo where the overall demand is increased. The assembly manufacturer's operability demand increases nearly as much as the installer's in the demand operability plot. Finally, looking at the aggregate schemes using minimum, average, and maximum aggregation functions, the overall functionality of the network under different inventory assumptions is captured. Recall that the minimum aggregation function models the expected behavior for a produce-to-order inventory policy. In this example, it can be envisioned that disruptions can be assumed from a cybersecurity incident.

2.3. Stochastic Analysis

To bring stochastic components to these examples, a Monte Carlo method can be used to simulate many randomized simulation results and report on statistically generalized results [8]. Supply and demand can be modeled as performance values between 0 and 100. Since the limiting values and the expected value, of operations, are known, the triangular distribution can be used to model the data. This is selected as opposed to the normal distribution since operability and internal health are deemed limited to values on [0; 100], and the normal distribution can take matters on (0;1). Now, the probability of disruption needs to be estimated. Based on a survey of work in supply chain disruption research, local disruptions were usually assumed to be between 0.5% and 20%, while global disruptions were estimated between 0.5% and 1% [8]. In this work, the global disruptions will be considered as prior probabilities, and the local will be posterior probabilities based on additional evidence provided in each node. Conditional
probability tables can be built and deemed to reject this assumption. In this sense, a 1% chance of disruption will be assumed for the system network nodes, increasing to 80% when one relevant Risk occurs and 90% for two relevant risks arising. As a result, an experimental matrix with the probability of each state of risk occurrence can be produced.

Fig. 3. Supply layer results for one simulation run showing the (a) internal health and (b) performance values plotted against time.

Fig. 4. Demand layer results for one simulation run showing the (a) internal health and (b) performance values plotted against time.

A set of runs for each possible set of risk occurrences has been produced (not shown in this paper, given space constraints, but the avid reader referenced to [8]). Then, descriptive statistics showing characteristic values for each network node have been calculated and plotted. In an applied case study, subject matter experts could select sets of risks they were most interested in for analysts to study in greater detail.

This methodology has the potential to be effectively applied to more complex, real-world applications focused on being resilient to recurrent, low-impact events while simultaneously becoming more competent at addressing less frequent, high-impact events. By combining the analyses for the Risk and the system models, this methodology allows for the investigation and quantification of both scenarios [5, 6, 8-10].

In another example, a triangular distribution with minimum and maximum values is assumed to be 5% of the mode. The mode for the self-efficacy of each node was initialized at 80% operability. Disruptions had probabilities of 1% in general, increasing to 80% and 90% when one or two of the risks the node was dependent on occurred. When a disruption occurs, the mode of the node behaves in a manner consistent. An example of the initial probability distribution showing a histogram with 10,000 samples, the PDF, and CDF is presented in Fig. 5. Results have been generated using minimum, average, and maximum approaches to aggregate the operability values from the supply and demand layer. The period for each run was 100 days, and each run was repeated 300 times. Different aggregation methods could be used for supply chain models to implement inventory policies and, thus, find out to what extent an inventory buffer can absorb shocks from cybersecurity incidents. In our outputs, values plotted are the percentage of
operability maintained over the simulated time, even with disruptions. These were calculated as the ratio of the area under the operability curve for a given node compared to the area if the operability had remained at 100% for the entire simulation. A given risk, Risk $b$, affects the most significant number of nodes and will act similarly to global disruption. A more elaborate example follows these lines in [8].

![Example histogram, PDF, and CDF for a triangular distribution](image)

**Figure 5 - Example histogram, PDF, and CDF for a triangular distribution**

### 3. Explainable Artificial Intelligence (XAI) Security for Distributed UAV Swarms and Other Autonomous Cyber-Physical Systems

New cyber-physical systems (CPSs) that integrate the physical and digital (cyber) spaces must be protected on critical infrastructures. Among new CPSs to support operations, Unmanned Aerial Vehicles (UAV) are increasingly used in monitoring and communications for remote reconnaissance missions, surveillance operations, and supporting command and control. Many of these applications are distributed, requiring coordination, planning, and often runtime reconfiguration to conduct operations. Traditionally, human decision-making controls UAV operations' movement and task completion [11]. Artificial Intelligence (AI) has emerged as a critical tool to overcome these limitations. Here, a Machine Learning (ML)-based security solution for distributed autonomous UAV Swarms and Decentralized Detection can provide strong mission assurance in contested environments. A popular approach to overcome the complexity of cybersecurity and the sophistication of cyber-attacks is implementing AI-based security controls that integrate ML algorithms into security control domains (e.g., intrusion and malware detection). These AI-based security controls are more effective than traditional signature-based and heuristics-based controls. However, the growing adoption of advanced ML algorithms is turning these AI-based security controls into black-box systems. The authors propose that methods would make risk mitigation and informed decision-making challenging. Compared to traditional intrusion detection systems, ML-based systems require less human intervention and are more effective in detecting new attacks.

Security for UAV swarms presents significant technical challenges, such as providing a group of networked, distributed, and UAVs protection against intrusions. Techniques so far have attempted to add intelligence to the (individual) UAV controllers to work around these attacks. The proposed approach significantly improves state-of-the-art design methods, where security guarantees for UAV swarm missions typically need to be clarified. Most current UAV research focuses on a centralized form of the problem from an optimal control standpoint [12]. These studies consider the lower-level controller loss function using the distance between the UAV's current and desired states, such as position and velocity [12]. Conversely, UAV swarms with varying levels of autonomy and human interaction need to operate even in challenging circumstances. Unfortunately, as with other CPSs, UAV’s sensors or computational systems may be altered differently [13]. Communication channels between the different UAVs may be compromised, interrupted, captured, or jammed via intrusion actions or malicious interferences in radio frequency noises. Several techniques have incorporated validation using cryptographic approaches [14]and signal processing,
i.e., GPS-based methods [15]; however, they are limited due to the requirement for specific hardware and lead to many false alarms due to their restricted physical dynamics and flexibility.

New techniques, e.g., [16, 17], are trying to bring intelligence to the UAV controllers to work on the attacks or failures in the system. However, detection mechanisms for distributed UAV swarms are required for sensing and propulsion information. Additional challenges UAVs face include battery life and expensive computational processes. Artificial Intelligence (AI) emerges as a critical tool to overcome these limitations.

3.1. Significance

Here, the authors target an innovative data-driven approach to create robust models employing a decentralized Generative Adversarial Network (GAN) to overcome vulnerability to failure and intrusion. Our research aims to develop a GAN model, a class of deep machine learning frameworks. GAN is a prominent framework for approaching generative AI that typically has two parts, including a generator and a discriminator. A short description of our idea and method follows.

The generator learns to generate reasonable data and training examples for the discriminator. Then the discriminator learns how to distinguish the generated fake data from real data [18, 19]. The results show [18] that the GAN-based data augmentation technique can enhance data discretization and improve drone performance as well.

Such techniques enhanced the security of drones through sensor data and control signals [19, 20]. Figure 6 represents the Generative adversarial network structure and illustrates how the generator and discriminator procedures run inside the GAN in each loop and how it differentiates and signifies real data from fake data. The proposed model will capture the dynamics of the dataset and UAVs.

4. Reinforcing Resilience Against Cyberattacks in Transfer Learning

Machine Learning (ML) and Deep Learning (DL) techniques are utilized to uncover patterns and structures within data, empowering autonomous learning. The development of ML/DL models is deeply rooted in data. Yet, the effectiveness of machine learning models in real-world applications hinges significantly on the availability of extensive, well-labeled high-quality datasets. However, obtaining ample well-labeled data is typically unpredictable, costly, and challenging [21, 22]. Moreover, traditional ML/DL assumes similar distributions for training and test data, which may not match real-world situations, causing model drift. In addition, privacy concerns also arise with sensitive data, posing legal and ethical challenges for data access [23]. In addressing these challenges, this paper aims to leverage transfer learning.

Transfer learning is a method that utilizes knowledge from one model (the source model) to construct a new model (the target model), as illustrated in Figure 8. By leveraging existing knowledge, transfer learning accelerates the creation of new models, even for distinct domains. However, despite the benefits of transfer learning, it comes with specific challenges [24]. One concern stems from possible inaccuracies in the knowledge of the source model, which could transfer to the target model during domain adaptation. Additionally, there's a risk associated with exposing the layers of the source model used in the target model, potentially being exploited by malicious actors and resulting in different types of attacks in the realm of transfer learning. Addressing these concerns, this paper creates a defense model tailored to these specific challenges. Specifically, we advocate for designing defense models within
the realm of transfer learning to prevent adversarial attacks and reduce the transfer of imprecise knowledge from source models to target models.

4.1. Defense Model

Challenges associated with transfer learning include i) the possible existence of error-prone knowledge in the source model that the target model may inherit and ii) the susceptibility of the open-source model to exploitation by malicious actors, enabling the introduction of defects or extraction of information. In Figure 7, the left side illustrates the source model containing error-prone knowledge that could potentially transfer to the target model. Our goal in this scenario is to mitigate the transfer of this knowledge, as shown on the right side of Figure 7. To mitigate the transfer of flaws from the source model to the target model, we can improve the design by generating multiple target models through layer segmentation of the source model. These segmented layers are assessed using a subset of the target domain dataset, aiming to maximize the accuracy of the target model. We repeat this process for several target models and select the one with the least error with the target dataset, effectively reducing the transfer of problematic knowledge to the target models. Furthermore, assuming the attacker has white-box access to the source model, they possess knowledge that the initial TL layers of the target model are derived from the source model and remain unchanged during training. In such a scenario, the attacker manipulates the source input to induce a misclassification, making it appear to belong to the same category as a specific target input. Leveraging the source model, the attacker computes perturbations that replicate the internal representation of the target input at layer TL. This internal representation is obtained by inputting the target input into the source model and extracting the values of the corresponding neuron outputs at layer TL [25]. To defend against such attacks in transfer learning, this paper presents two potential methods: i) Layer Fusion, and ii) Ensemble Learning.

- **Layer Fusion.** The approach involves merging layers from the source model to create fresh, adjustable layers for the target model. Assuming the attacker's familiarity is limited to the source model, adding these new layers can effectively deter adversarial attacks on the target model. This study focuses on the weight vectors of each layer within the source model to accomplish this goal. It endeavors to devise a method for aggregating weight vectors of successive layers in the source model, generating novel layers that align with the target model, enhancing its accuracy, and reducing the similarity in internal representations of input samples from the source model to the target model. We accomplish this by introducing random modifications to the target model. As a result, this defensive approach provides several benefits: i) a decrease in computational demand due to smaller layer sizes, easing the load on computational resources, ii) increased complexity for potential attackers attempting to replicate the input data representation from the source model to the target model.

- **Ensemble Learning.** We produce several target models by randomly choosing layers from the source model. These models collaborate and employ majority voting to predict labels. This research embraces ensemble learning, forming multiple target models by merging layers from the source model. Consequently, if an attacker succeeds in misleading one target model within the ensemble, the other models might retain their resilience since the adversarial sample is tailored for a specific target model. However, it's essential to acknowledge that this concept has been previously investigated in various contexts [26]. Additionally, it's evident that the source model may contain potentially erroneous knowledge that could transfer to the target model. To mitigate the potential
transfer of these inaccuracies from the source model to the target model, we elaborate on the creation of multiple target models. This involves segmenting the layers of the source model, excluding the segments prone to flaws, and evaluating the remaining layers using a subset of the target domain dataset. Our objective is to optimize ensemble learning, minimizing the transfer of problematic knowledge to the target models. While this approach may increase computational costs, it presents several benefits: i) it strengthens the defense against mimic attacks, ii) it reduces the transfer of flawed knowledge from the source model to the target model.

5. Trustworthy Smart Data Connection to Enhance Safety at Sea for IoT-Enabled Maritime Transportation System

What does the future hold for safety at sea, and how should the industry adapt to prevent serious accidents from occurring and, ultimately, save lives? The accuracy of decision-making of data can diminish the risks at sea operations. According to Industrial IoT at Land and Sea [27], a maritime report found that 47 percent of shipping respondents collect data for environmental monitoring every year. Regarding this report, the embedded sensors in IoT components can collect more detailed and relevant data than surface-mounted sensors. Consequently, how vessel performance the onboard crew and ship managers can monitor? Is there a safe space for data sharing at sea, where terrestrial networking is not persistent? Indeed, privacy-preserving data sharing on IoT devices has not been investigated meticulously in the above contexts of the maritime transportation system. IoT devices are resource-constrained [28]; likewise, they are designed by low-power devices to adapt to modest physical space. Hence, in the lack of terrestrial infrastructure such as the sea, how can low-power remote vessels transmit data securely to a central satellite? Most of the current IoT devices embedded in the smart vessels connect to the satellite, the central system for data storage and communication to the sensors embedded in the red buoy [29, 30].

Recently, the “smartness” of IoT has been empowered by data-driven applications to enhance the smart connection/cognition from various smart connected vessels, tankers, and buoys [31] to be collected, transmitted, and processed by reaping the benefits of IoTs. The maritime transportation system can conduct predictive or condition-based on the sea environment by collecting much data from IoT-enabled devices. How can we preserve the low-power remote devices such as the IoT-enabled vessels and IoT at the red buoy to transmit secure data to a satellite from locations that lack terrestrial infrastructure in the sea environment? It’s critical that we consider the efficient privacy-preserving data-sharing mechanism when designing and implementing IoT solutions in the maritime industry. The proposed framework aims to develop trustworthy data-sharing space to enhance smart data connection for IoT-Enabled maritime transportation systems.

To respond to the above-mentioned gaps, enabling technologies for implementing and fully exploiting the future revolutionized IoT in the maritime system is critical. The overarching objective of the framework idea to pursue this research is to design, analyze, and implement a new privacy-preserving data-sharing platform with a special focus on enhancing the safety of smart maritime transportation systems. Specifically, the central idea is on sensor data from smart vessels such as engine and machinery components, cargo containers, fleet management, connected ports, the radar, video camera, GPS, and temperature, accompanied by local sensors at the edge such as camera and red buoy. Based on the sustainable incorporation between the edge and vessels, we are building a robust platform for data storage/data retrieval and privacy-preserving data aggregation to support data analysis for the maritime information system.

6. Summary and Future Work

This paper presents a sample of issues related to particular applications of ML/AI to the broader maritime supply chain security domain affecting the planning, execution, and performance of complex systems. Our investigations focus on applications of these techniques in several dimensions of supply chain cybersecurity. In this paper, we explored the foundations of applying the Adaptive Risk Network Dependency Analysis (ARNDA-CMMC) methodology to detect hypervulnerabilities that arise over time, float among different nodes (representing suppliers) in a supplier network, and determine their ripple effects, taking the perspective of balancing our cybersecurity compliance and other risks. In our quest to illustrate the applications of ML/AI, we presented a potential application in developing a (ML)-based security solution for distributed autonomous Unmanned Aerial Vehicles (UAV) swarms and decentralized detection to provide mission assurance in contested environments. We also presented our ideas in exploring the components of
designing and reinforcing resilience against cyberattacks in transfer autonomous learning. Similarly, we presented the ideas related to the core ideas of developing a trustworthy smart data connection to enhance safety at sea for IoT-enabled maritime transportation systems. Finally, Section 6 suggests exploring research lines in the cyber supply chain environment. The future is advancing toward creating trusted data-sharing spaces protected by sound cybersecurity practices and models.

References