Cybersecurity Considerations for the Design of an AI-Driven Distributed Optimization of Container Carbon Emissions Reduction for Freight Operations

Carlos Paternina-Arboleda(✉), Alexander Nestler, Nicholas Kascak, and Morteza Safaei Pour

Department of Management Information Systems, San Diego State University, San Diego, CA 92182, USA
cpaternina@sdsu.edu

Abstract. The transportation industry is a vital component of the global economy, responsible for the movement of goods between different locations. The intermodal freight transportation system involves the use of different modes of transportation, such as trucks, trains, and ships, to move freight containers. However, this system is loaded with inefficiencies due to the poor availability of real-time coordination and disruptions, causing delays, increased costs, and thus, higher carbon emissions. AI has the potential to improve the intermodal freight transportation system's efficiency by optimizing operations in real-time and self-evolving the models to make better/faster decisions. While both policymaking and business operations would benefit from using real-time optimization models, the implications and applications of these models are different in each context. In policymaking, real-time optimization models are used to improve public services, reduce overall network costs, and setting regulations for sustainable management of the network. The system can consider real-time traffic conditions, weather, and other factors to optimize the routing of the trucks, reducing transportation costs, improving delivery times, maintaining resiliency, and managing emissions. This work aims to contribute with a better understanding on how these information systems can be protected from cyberthreats, while performing the optimization of freight synchromodal transportation operations in real-time in terms of efficiency, cost-effectiveness, and carbon emissions reduction, considering the dynamic nature and heterogeneity of the intermodal freight system.

Keywords: Cybersecurity · Digital Twins · Transportation · AI-Driven Optimization · Environmental Impact

1 Introduction

If anything, the last three years have taught the maritime industry that the supply chain is vulnerable and very much dependent on global events. Ports around the world have witnessed some of the biggest cargo congestion challenges in modern history. This

J. R. Daduna et al. (Eds.): ICCL 2023, LNCS 14239, pp. 56–84, 2023.
https://doi.org/10.1007/978-3-031-43612-3_4

congestion, driven by a continuous increase in the gap between consumer demand and logistics supply, exacerbated by supply-chain disruptions (among which, cybersecurity breaches are a main concern), is negatively impacting the maritime footprint, despite large investments by the industry to streamline, modernize, and reduce supply chain carbon emissions. Consumer demand for goods shipped across the world is set to be steady or increase. Major ports around the world are witnessing similar trends, leading to a rise in regional congestion and emissions at bottlenecks, whether in the port, at port gates, or in dray corridors. Saxon and Stone (2017) build on the container disruption of the shipping business and how the industry unfolds in the next 50 years. They suggest that by 2067, the annual growth of global trade of containers will range from 1.9% to 3.2% in the high case scenario. This equates to an increase from 182M TEUs (2016) to 464M TEUs and 858M TEUs by 2067 respectively for low and high. Every year, container ships plying the world's waterways spew about 1 billion metric tons of CO2 into the air (about 3% of global greenhouse gas emissions). Transportation stakeholders must continue to invest and develop groundbreaking solutions that monitor, track, and reduce cargo's carbon footprint.

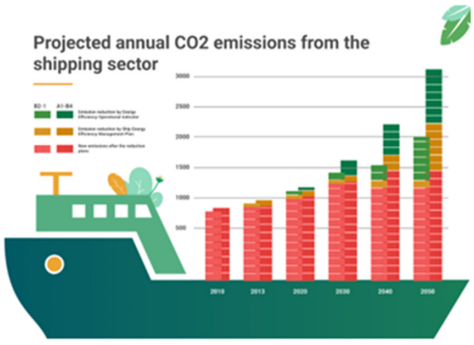

Fig. 1. Projected CO2 emissions, shipping

The increase of a global cargo movement, coupled with the added complexity of equipment and systems that are deployed to optimize the movement of goods, pose a new challenge of measuring the impact of intermodal container travel. This comes at a critical time as private sectors and government agencies are seeking reliable measurement sources to accurately assess carbon neutrality and drive decarbonization. Despite many efforts to measure carbon impact, there continue to be a lack of standardization and discrepancies among the metrics deployed to measure GHG emissions and their impact. The goal is to accurately measure GHG emissions and levelized costs of Mt-km (LCOTKM) analyzing the multi-variation by modes of energy and goods transportation and compare to projected values**.** Figure 1 shows a shipping emissions projection.

To control carbon emissions, we first need to accurately measure their impact. We propose a Digital-Twin enabled, AI-driven RT Distributed Optimization Platform, based upon a system level view of the intermodal network, mapping energy consumption, and calculating emissions, and offering suggestions for route and mode switching of containers, which could greatly improve those metrics. Due to the diversity and complexity of

data this Platform would depend upon, success requires a massive data ingestion from hundreds of data sources while combining extensive data modeling, AI processing, and algorithms along with simulation. Investing in a high-fidelity simulation Platform such as Argonne's POLARIS simulation (Auld et al., 2016), and proven optimization meta-modeling information systems (Velasquez-Bermudez, 2020), is more beneficial and rewarding in the long run, as real-time Intermodal efficient mode switch is essential for these systems to convey good results. Jubiz-Diaz et al. (2021) modeled the Colombia Intermodal Transportation Network, and examine the relationship between infrastructure investment, freight accessibility, and GDP, with a data-driven geospatial approach, targeting investments with greatest GDP impact.

A digital twin is a virtual model designed to accurately reflect a physical object by using real-time data (IBM, n.d.). According to IBM, there are four types of digital twins depending on the level of magnification. To successfully implement a digital twin infrastructure capable of real-time coordination and reduce carbon emissions for intermodal freight transportation systems in the United States, several sources of data and information will need to be integrated to form various component twins.

An AI-driven real-time distributed optimization (RT-DO) system is deployed, considering the dynamic nature of the intermodal freight transportation system. The model uses real-time data and analytics to optimize operations, reducing costs and carbon emissions. The system considers real-time data on transportation routes, cargo volumes, and costs. The modeling methodology is based on the concepts of advanced parallel, and distributed analytics, as support to "artificial brains," the decision support systems in the era of Industry 4.0. The system is deployed at different levels. The first level presents real-time distributed optimization mathematical models for cargo routing which are used to determine the most efficient/sustainable path for traffic flow in a transportation network, considering a wide range of factors such as intermodal switching, traffic, and demand resource limitations. Intermodal switching refers to the transfer of cargo between different modes of transportation, such as from a ship to a truck or from a train to a waterway. We base our RT Optimization modeling framework in Large-Scale Optimization theories, such as Benders/Lagrangean decomposition, and a novel Event-Driven Real-Time modeling structure described in Abril et al. (2023). Paternina-Arboleda et al. (2008) show an integrated simulation-optimization framework for logistical systems.

The main contribution of the research paper entitled "Cybersecurity Considerations for the Design of a Digital Twin Enabled AI-Driven Real-Time Distributed Optimization of Container Carbon Emissions Reduction for Synchromodal Freight Operations" lies in highlighting and addressing the crucial cybersecurity considerations associated with the design and implementation of a digital twin-enabled AI-driven real-time distributed optimization system for synchromodal freight operations.

The paper identifies the specific cybersecurity challenges that need to be taken into account when designing such a system, including securing the data flow, ensuring the security of digital twin models, and safeguarding the system against cyber-attacks. It proposes practical solutions to address these challenges, such as implementing encryption mechanisms, access control policies, anomaly detection systems, and other cybersecurity measures.

From the cybersecurity perspective, Wang and Liu (2022) discusses the increasing application of cyber-physical systems (CPSs) in the rail industry and the corresponding rise in cyber threats that can cause significant failures and consequences. The authors propose a risk management methodology for addressing cyber security risks in rail CPSs, focusing on proactive identification, clear definition, and proper handling of these risks. Beaumont (2018) presents a case study of automated maritime container terminals (CTs). It has the aim of demonstrating that the risks derived from the use of technology associated with the Fourth Industrial Revolution (4IR) are both real and dangerous. In the shipping industry, the four largest shipping lines in the world have been hit by cyber-attacks since 2017 (Song, 2021). Cybersecurity is significant in maritime transportation because the costs of cyberattacks can be vast and the consequences fatal. For instance, digital navigation systems could be manipulated so that they sheer off or run aground, which would endanger the lives of the crew, people at sea and on land. The financial effects on shipowners and ship operators would also be immense (Tsvetkova et al., 2021). Woschank et al. (2020) mentions that AI may be used also in higher-level processes to detect fraud, prevent cybersecurity threats, and generally optimize higher-level processes for Smart Logistics in the future. De la Peña-Zarzuelo et al. (2020), present Internet of Things and sensing solutions, cybersecurity, horizontal and vertical system integration, cloud computing, 3D printing and additive manufacturing, big data and business analytics, augmented reality and simulation and modeling are the pillars of Industry 4.0. From all viewpoints, cybersecurity is a top concern for all AI-driven digital systems of today's logistics industry.

The paper emphasizes the critical importance of protecting the integrity, confidentiality, and availability of data in a digital twin-enabled AI-driven system. It underscores the potential risks and vulnerabilities that can arise in the transportation industry, especially when leveraging advanced technologies for real-time optimization and carbon emissions reduction. This paper is significant as it sheds light on the importance of cybersecurity in the context of digital twin-enabled AI-driven systems for synchromodal freight operations. It provides valuable insights for researchers, practitioners, and decision-makers in the transportation industry, offering a foundation for the development and implementation of secure and resilient systems that can effectively reduce carbon emissions, optimize operations, and improve sustainability.

2 Decision Support System Description

2.1 LCA and GHG Emissions

The first step is to define the system boundaries, which determine processes and activities that will be included in the analysis. The next step is to collect data on the energy source and the processes included in the system boundary. This involves data from suppliers, manufacturers, and energy producers, as well as conducting on-site measurements and calculations. Using the collected data, the GHG emissions associated with each process and activity are calculated. This involves using emissions factors or equations that estimate GHG emissions based on energy consumption, fuel use, and production processes. The GHG emissions calculated for each process and activity are then aggregated to determine the total GHG emissions associated with the low carbon energy source. This

will become either an objective function or a constraint in our optimization models. We use a modified version to the framework proposed by Guo et al. (2022). In their article, the authors present a methodology for estimating carbon emissions in hinterland-based container inter-modal networks. Their study focuses on a specific intermodal network in China to show the application of the methodology which involves an estimation model that considers factors such as distance traveled, mode used, cargo type, and considers energy consumption of different modes and emissions associated. The study found that carbon emissions can be reduced by optimizing the network, including increased use of rail, reduced distance traveled, and use of clean energy sources.

The network estimation model evaluates carbon emissions in a specific period. Paternina-Arboleda et al. (2023), show an estimation of SO2 emissions derived from ships when hoteling and maneuvering, and cruising in the port, showing predictive modeling of port emissions inventories. The data relates to vessel's AIS, and Port's IoT environmental sensor network. Cammin et al. (2023) also present a similar approach to the one above mentioned (Fig. 2).

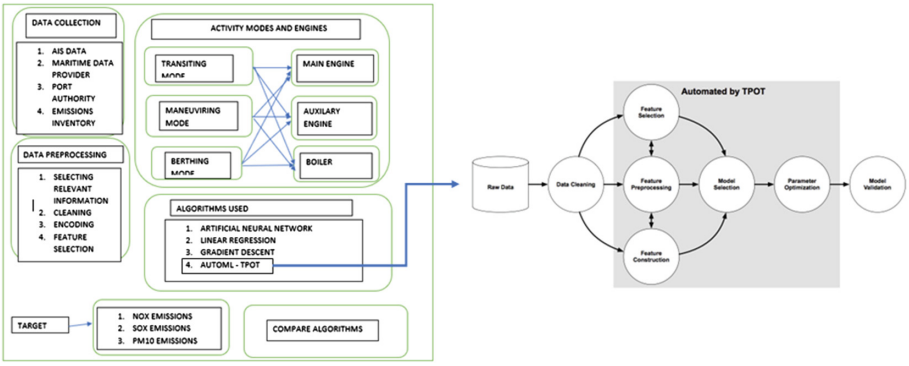

Fig. 2. Methodology for predicting Emissions Inventories (an example for Port Emissions), Paternina-Arboleda et al. (2023)

We are expanding the methodology to account for geospatial emissions for the intermodal network to be optimized based on the predicted metrics, with valuable insights to improve environmental practices and foster sustainable development.

2.2 Disruption Management

The system is designed to implement level metrics to assess the resiliency of a given "sustainable transportation network." These metrics provide a way to measure the ability of a transportation system to withstand and recover from disruptions/stresses, while still providing reliable and efficient transportation services to users.

A resilient transportation network should (a) have enough capacity to handle expected traffic volumes, while also being able to adapt to changes in demand and unexpected disruptions, (b) have high travel time reliability, to expect consistent travel times even in the face of disruptions, (c) be adaptable, to quickly adjust to changing circumstances

and provide reliable and efficient services, (d) have an appropriate level of redundancy, to have multiple options for reaching their destination in the event of disruptions, and (e) be environmentally sustainable (Yang et al., 2023). The global resiliency metric of a system depends on the resiliency of each individual transportation mode within because a transportation system is made up of multiple modes, each of which has its own characteristics and vulnerabilities. The mode switching optimization models must be tightly coupled with the disruption models. Some metrics proposed for our system are:

- System capacity as a measure of the ability to handle traffic volumes during normal/peak periods, considering number/capacity of lanes, number/frequency of vehicles, availability of modes.
- Travel time reliability as a measure of the predictability of travel times of a network. This metric considers i.e., congestion, incidents, and weather conditions that can cause delays or disruptions.
- System adaptability as a measure of the ability of a transportation network to adapt to changes in demand, technology, or other factors that can impact services. This metric considers factors such as new technologies, flexibility to adjust based on demand, and respond to disruptions.
- System redundancy as a measure of availability of alternative routes or modes in the event of disruptions to the primary network. This metric considers factors such as number and location of alternative routes, availability of transit or other modes, and ability to switch between modes.
- Environmental impact as a measure of the sustainability, which takes into consideration factors such as energy consumption, emissions, and the impact on local ecosystems.

The resiliency of each transportation mode is influenced by a range of factors, including quality and age of infrastructure, availability of alternative transportation modes, the level of investment in research and development, and the degree of coordination and communication between transportation providers and policymakers (Trucco and Petrenj, 2023). Understanding resiliency of individual transportation modes is critical to developing strategies for enhancing resiliency of whole transportation systems. Our proposed solution is designed to determine the sensitivity to inputs such as routes, low carbon infrastructure rollout, GHG reductions, and other variables that can help foster resiliency in several ways. The solution can help identify vulnerabilities in the transportation system by simulating the effects of various input scenarios on system performance via a digital twin. We can simulate the impact of a disruption to a key route or a delay in the rollout of low carbon infrastructure and help identify areas where the system is most vulnerable.

We could prioritize investments in infrastructure and other resources based on the potential impact on system performance (identify most critical investments to enhance resiliency of the system and reduce vulnerability to disruptions), while testing strategies to enhance the resiliency of the system. It provides a visual representation of the system's performance under different input scenarios to help understand the potential impact of actions and decisions on the resiliency of the system to promote more effective collaboration. Intermodal logistics can be impacted by a range of disruptions (local and

global). Some examples are: (a) natural disasters, (b) labor strikes, (c) disruptions in the supply chain, (d) global trade disruptions, (e) Pandemics, (f) Network Congestion, and the focus of this article, (g) **Cybersecurity threats**. Effective management of disruptions requires a comprehensive understanding of the system's vulnerabilities, as well as proactive planning and response strategies to mitigate the impact of disruptions and maintain the resiliency of the transportation system.

2.3 Full Synchromodal System Optimization

Intermodal transportation systems are an essential component of modern logistics and supply chain management. The complexity of these systems presents significant challenges in terms of optimizing routes, minimizing costs, and ensuring deliveries. Real-time (RT) optimization is a promising approach to address these challenges by leveraging advanced data analytics and optimization algorithms to make informed decisions in real-time. It allows transportation planners to respond quickly to unexpected events, such as traffic congestion or delays in shipments, and make necessary adjustments to routes and schedules to ensure efficient and timely delivery. Zhang et al. (2018), present an approach to RT optimization for transportation networks which discusses a method for optimizing the dynamic stowage of cargo at highway freight stations. They propose an algorithm that considers the cargo, the available space on the trucks, and the order in which the cargo is loaded and unloaded using a combination of dynamic programming and branch-and-bound techniques. They also use simulation to test the effectiveness of the algorithm under different scenarios.

The proposed system is designed to implement a framework for Autonomous Real-Time Distributed Optimization (ARTDO), as described in Velasquez-Bermudez et al. (2020). It enables autonomous optimization of transportation logistics in real-time, using distributed decision-making algorithms. The methodology improves transportation efficiency while minimizing the environmental impact of transportation systems in real-time. It involves: (1) Autonomous Distributed decision-making, with nodes equipped with decision-making algorithms that make autonomous decisions based on local data and feedback allowing the system to adapt to changing conditions in real-time. (2) Real-time data collection, to inform decision-making, including information on routes, schedules, capacities, and other factors that may impact transportation logistics. (3) Optimization algorithms. (4) Feedback mechanisms for nodes to provide/receive feedback and learn/improve based on their performance. To automatically run this math framework as required, we must embed all the models as a library of smart algorithms for the Optimization of the Intermodal Network, independently engaged in parallel but mathematically coordinated to achieve ARTDO across the full network. We will use the optimization platform to integrate the framework as a set of massive distributed although interconnected parallel routines. We must connect all the data models, and math models with data sources, to automatically generate (and maintain) master tables for the whole intermodal network. The system can incorporate real-time data on GHG emissions from transportation modes to identify the most efficient transportation modes and routes for minimizing GHG emissions, while meeting transportation needs, optimizing transportation modes and routes in RT, based on RT data on traffic congestion, weather conditions, and other factors. The system can be programmed to switch transportation modes/routes

in response to changing conditions for GHG emissions or the economic cost of avoided carbon, while meeting efficiency needs (economic cost/freight ton-Km).

2.4 Designing the Decision Support Information System

The DSS is built in OPTEX (Velasquez-Bermudez, 2020), and it will group all math models, and predictive/prescriptive analytics for the system. The MMIS (Math Modeling information system) manages elements (objects, entities) i.e., tables, fields, indexes, sets, variables, parameters, constraints, equations, objectives, problems, models, DSS, and applications. MMIS standardizes the management of entities and relationships centered on its database algebraic language for linear/non-linear equations. These objects are critical to address large-scale problems by coordinating multi-problem models and the information flow. The output of one model is used as the input to others. Due to the complexity of the real system, the DSS consists of multiple math models integrated through the data stream, thereby generating the information required by the decision maker to address all levels (strategy/tactic/real-time). The different models share information stored on a common/coherent standardized database to allow for data integration along with the decision-making chain, so that this coordinated effort guarantees "optimization" of the entire system. The latter is practically impossible to obtain with a single model. From the platform we can generate math programs in high-level algebraic languages, like GUROBI or CPLEX. Optex (Fig. 3) is a generic meta-platform that works as interface for multiple technologies. The modular concept is fundamental to implement large-scale methodologies, based on partitioning and system decomposition.

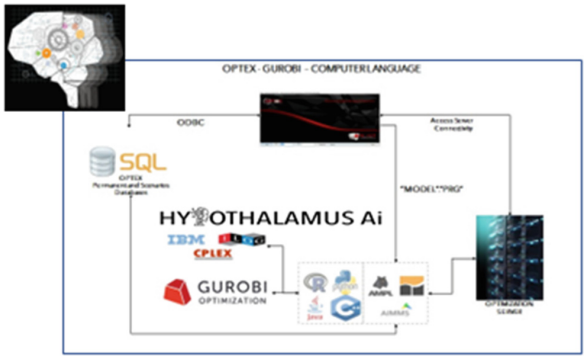

Fig. 3. The Optex meta-modeling system

The main large-scale concept in our system is Real-Time Distributed Optimization (RT-DO), where multiple agents coordinately keep the system on the optimality path (Velasquez-Bermudez et al., 2020). It follows a standard 7-step process:

- Step 1 – Algebraic Model Load: Fill the database to the MMIS and follow next steps.
- Step 2 – Model Data Load: Generated simultaneously with the loading of math models (table structures determined by the math model), by sets, parameters, variables, constraints.

- Step 3 – Generation of the visual user Interface: The system automatically generates a user interface. The shell windows are associated with main/secondary tables.
- Step 4 – Analysis and Review of the Algebraic Model Formulation: It involves coordinating two simultaneous activities: Review loaded algebraic formulation into MMIS, and results.
- Step 5 – Run the system and store the Algebraic Model results: Performed automatically.
- Step 6 – Set the Algebraic Model: Necessary changes to the MMIS and IDIS. This cyclic process ends when the implemented model produces the correct results, ready to be delivered.
- Step 7 – Data Access by the end-user: Finally, the end-user can access the model for use, based on the data stored in the IDIS and results generated by the models.

2.5 System's Artificial Intelligence

A decision support module will need to run in parallel to the AI process. As the AI optimizes, updates, or forecasts routes, the schedule will need to be updated to reflect these changes. Further, common routes and common alternate routes for each region optimized by the system or updated due to new routes (i.e., construction) need to be stored as the system generates them for efficient retrieval in the future. This will allow the system to retrieve optimal routes previously generated providing operators with options that are already optimized for CO2 emission reduction.

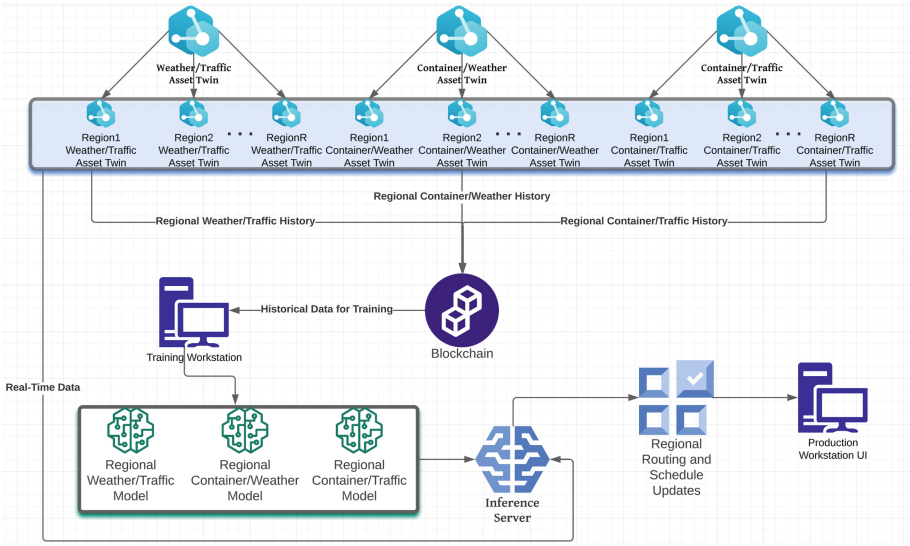

Fig. 4. High level view of the proposed AI process

The predictions from all three base models will be combined for the final regional inference of the best route the container should take based on the location, traffic conditions, and weather. The algorithms for the AI need to focus specifically on minimizing

the CO2 emissions overall based on the ton-mileage and minimizing the time-to-arrival when taking the route by avoiding any traffic. Since CO2 emissions are based on ton-mileage, without exact emissions per hour data, the best the system can do is avoid idling in traffic to reduce those idling emissions by minimizing the time-to-arrival and ton-mileage for the route (Cammin et al., 2023; Paternina-Arboleda et al., 2023).

The AI system will continuously update this information as historical data continues to be generated and new optimized or updated routes are discovered. Figure 4 shows a high-level view of the AI Process from collecting regional historical data to generating decisions from inferences made by the system. In previous research articles, Paternina-Arboleda and Das (2001, 2005) demonstrate how artificial intelligence techniques, specifically Multi-Agent RL, can be used to address complex logistics problems. By leveraging the power of AI, logistics companies can optimize their operations, reduce costs, and improve efficiency and customer satisfaction.

3 Data Types and Structures

To successfully implement a digital twin infrastructure capable of real-time coordination and reduce carbon emissions for intermodal freight transportation systems, several sources of data and information will need to be integrated to form various component twins. There will need to be lots of data and information inputs needed to build out an AI-based model that will provide positive value to a transportation service business. The AI-based model portion of the system will be built out using the information and data inputs that are laid out below.

For this system to work and function as intended, there is a large amount of raw data that the system collects from various sources. These sources include the Global Positioning Systems (GPS), local cyber sensors at each fielded unit, historical transportation metrics, personnel information, real-time traffic, and weather data, vessel AIS data, among others. There will be more added as the project continues to grow in scope. The more data that can be cleaned, indexed, and inserted into the system, the more AI can learn and adapt to optimize the transportation routes. Dzemydienė et al. (2023) present a system architecture for monitoring and managing freight intermodal transportation using the IoT and WSNs.

Before any data or information is collected, there needs to be a shared data repository to collect the data. This data repository, also known as a data lake, will be primarily in the cloud with incremental, local hard drive backups. The repository will be internal to the company's private network and protected through various cybersecurity controls. After the shared data repository is established, data can start getting collected. The system will have a centralized data collection point at the Hub as well as local storage of data on the system data sensor. The sensor will also monitor data as it transits through the network and into the model to make sure the data is not compromised.

Historical transportation production data will be used to have a baseline of the historically best routes to take. The historical data should be gathered and broken up in a logical manner for ease of analysis. This includes recent data on the actual paths the truck, train or boat took to get from point A to point B. The inputted data can be broken up by month, year, season, quarters, and year over year changes. Different months and

seasons have different weather patterns that must be kept in mind. Comparing yearly data could prove to show an abundance of statistical insights. By gathering this historical data, the AI model will have some data points and ability to make rudimentary decisions.

There is a variety of different information metrics that will assist in the training of the model. To start off, priority levels need to be set for each method of transportation, cost, schedule, weather, payload type and traffic patterns. These set priority levels will lead the model to make more accurate predictions. These priority levels will also be a large part of the COA selection list that the model outputs.

The mode of transportation and associated personnel are required to physically move the goods from point A to point B. Trucks are, and will continue to be, the primary method of travel. However, the transportation method could also be a boat or train and the associated personnel for each method. Driver information for each situation will have to be inputted into the system and protected. Driver will be used as a colloquial term in this paper to represent a truck driver, ship driver and train driver into one central category. This information varies from driver to driver and method to method. For example, a truck driver will need to have all their medical information, personal information such as social and next of kin, time on the road, consecutive days traveled, average speed, follow on trip and GPS positioning data.

The system will need to keep payload information with set priorities for different manifests. Each item or good will include the name, Radio Frequency ID (RFID), weight and priority level. Each item in the manifest will combine to bring the overall payload to a quantifiable level of priority. This will be inserted into the model for further course of action training of data.

For the data to reach the Hub and central data repository securely, a data transportation method needs to be established. The endpoint devices and users will be connected to the Hub via a private Virtual Private Network (VPN). A VPN is used to "mitigate the security risks inherent to providing remote network access by offering strong encryption to provide data security and strong authentication to limit access to applications based on defined security policies" (Loshin, 2019). Aggarwal, (2022), and Aggarwal (2023) define data encryption as a security tool that transforms plaintext data into encoded data called ciphertext that can only be read with a unique key that is given at the time of the encryption, which can be used for both in transit and at rest data. The two different types of VPN that the system can implement are TLS VPN or IPsec VPN in tunnel mode. Both modes reach the same conclusion of secure data traffic and communication through slightly different means. A TLS VPN lives in the application layer, layer 4. IPSec VPNs live in the network layer, layer 3. In other words, "The major difference between an IPsec VPN and an SSL VPN comes down to the network layers at which encryption and authentication are performed" (Loshin, 2019). Again, both VPNs provide a private, secure network for communication, data storage, data transmission and network operations. The project manager can implement whichever one his engineering team recommends.

The above criteria, data, and information can be combined for model use to output the Courses of Action (COAs). The model will use the data as inputs and produce COAs that show cost-reduction, environmental benefit, scheduling patterns, transportation method,

destinations, and departure suggestions. These COAs will be the optimal transportation strategy and give management options to pursue.

3.1 Identifying and Structuring the Data

The goal of our system is to provide transportation efficiency through automation, costs-reducing methods, and increase sustainability of the transportation ecosystem. Artificial intelligence (AI) has the potential to improve the intermodal freight transportation system's efficiency by optimizing operations in real-time and self-evolving the models to make better/faster decisions. The system accomplishes this goal. For the system to give accurate predictive and reactive solutions, there needs to be data structure, software system, and hardware system requirements of the system. When implemented correctly, the system will output a corrective course of action that is an optimal solution.

Identifying and establishing a data structure is the beginnings of building out the system. The data structure needs to be set up in a way that optimizes the dashboard's utilities. The structure of the data will be in a data frame form. What this will do is allow for data to be structured cleanly and in a format that can be queried. A data frame is defined as "a data structure that organizes data into a 2-dimensional table of rows and columns, much like a spreadsheet" ("Data Frames," 2022). This allows for easy sorting and indexing of the raw data. The data structure will be set up very similarly to an excel spreadsheet with numbered rows and columns. Data frames are "one of the most common data structures used in modern data analytics because they are a flexible and intuitive way of storing and working with data" ("Data Frames," 2022). This ease of implementation and flexibility will pay dividends once queries, analysis and data start to flow through. As an AI-based model that will be learning from the data provided, the flexibility of data frames allows for results to be optimized.

The proposed decision support system follows as an extension of Port Community Systems (PCS), Freight optimization systems, and Freight brokering systems. A PCS is a platform that connects the various stakeholders in a port community, such as shipping companies, freight forwarders, port authorities, and customs officials, to facilitate communication, coordination, and collaboration. Data is a crucial component of a PCS, and various data types are involved in the system (Moros-Daza et al., 20167, 2018, 2020). Vehicle routing optimization (VRO) is the process of finding the most efficient routes for vehicles to transport goods or people. Data is a crucial component of VRO, and various data types are involved in the optimization process (De la Cruz et a., 2013, Amador et al., 2014, Palma et al., 2019). A freight brokering system is a platform that connects shippers with carriers to facilitate the movement of goods. Data is a crucial component of a freight brokering system, and various data types are involved in the system (Moros-Daza et al., 2019). Sarabia et al. (2006), present simulation-based decision support models as computer-based tools used to optimize river cargo transportation. These models simulate the river system and cargo flows to help decision-makers identify the most efficient transportation routes and schedules. Various data types are involved in SDSM for river cargo transportation. The typical data types that need to be consider in such systems follow (Table 1).

3.2 System Data Flow Model

This section focuses on the design of the data flow system that enables real-time synchromodal transportation optimization using digital twin technology and AI. The proposed system aims to provide a comprehensive view of the transportation network, including infrastructure, assets, and operations, to optimize the transportation flow and minimize carbon emissions. The system's design includes the integration of various data sources, such as real-time sensor data, historical transportation data, and external data sources, to enable the AI algorithms to make informed decisions in real-time. Figure 4 shows the context diagram for the system data flow.

The primary data input into the system at regular intervals will be the GPS technology tracking the containers. The GPS tracking will be used by the system to create the content twin of the containers as they are moved between modes of transport from starting point to destination. Supplemental information such as the current engine being used to move the container, current starting point, and destination will also need to be gathered each time the container changes mode of transport until the container reaches its destination. This information will allow the system to track CO2 emissions based on the engine being used for transport and calculate anticipated & actual CO2 emissions based on the starting point, destination, and actual miles traveled.

To create the content twins of weather and traffic conditions, real-time weather, and traffic data APIs such as Weather.gov, WeatherAPI.com and Google Traffic will be utilized to access the available data from the cloud. With this information collected, the system will be able to monitor the weather conditions and local traffic conditions where transport is taking place. Adjustments to routes will be made possible by analyzing the weather and traffic data allowing the system to make routing decisions in a timely and emission friendly manner. Figure 5 shows the context diagram of the system data flow.

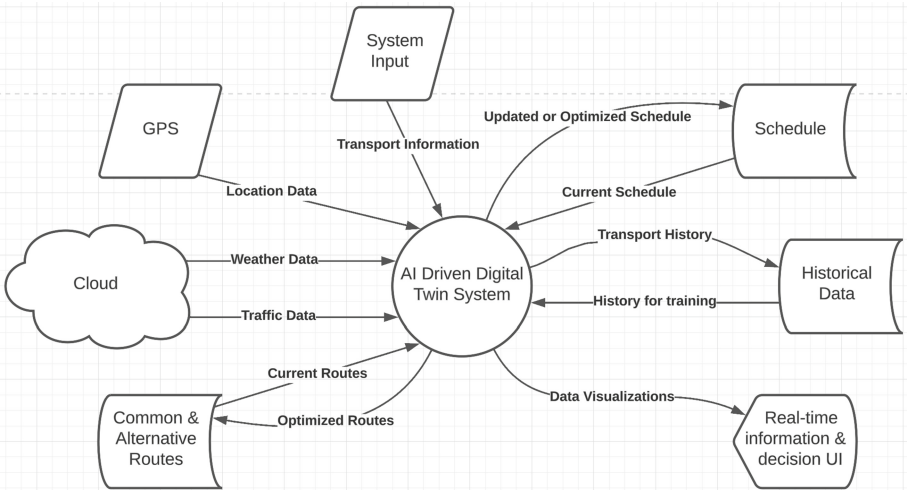

Fig. 5. Context Diagram of System Data Flow

The core component twins of the container, weather, and traffic will work together to form three distinct asset twins within the digital twin system. Container and weather component twins will form a single asset twin to study the interactions of the container routes and weather. Similarly, the container and traffic component twins will form a single asset twin to study the interactions between container routes and traffic.

Finally, the weather and traffic component twins will form a single asset twin to study the interactions between weather and traffic where intermodal transport occurs. The data collected from these three asset twins will be processed and analyzed by the system for optimization of routes, schedules, and CO2 emission reduction during intermodal container transport, forming the complete digital twin data structure (Fig. 6).

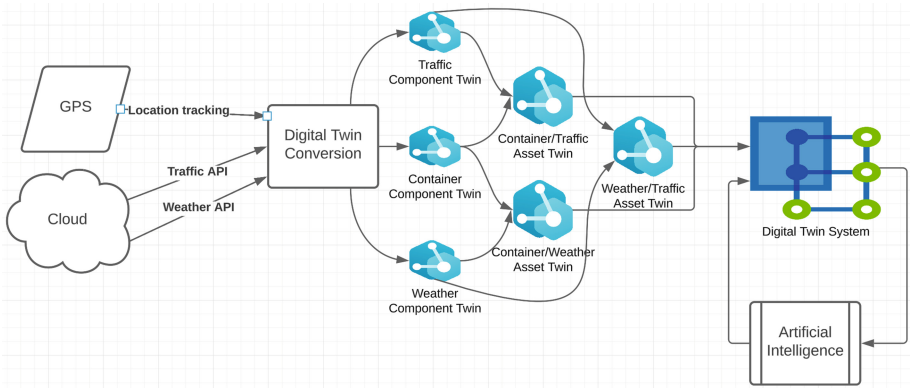

Fig. 6. High-Level Data Structure of the Digital twin system.

3.3 Dynamic Data Acquisition

Real-time data can be obtained from a variety of sources. Advanced analytics and ML algorithms can be used to process and analyze real-time data, providing insights and suggestions to stakeholders in real-time. Table 1 specifies the update frequency, latency, and spatial granularity of dynamic data. The goal is for system level optimizations to be computed within a day and dynamic adjustments in under 1 h. Real-time data can be critical for optimizing intermodal transportation networks by providing up-to-date information on infrastructure, traffic patterns, weather conditions, and other factors that can impact transportation operations. Some common types of RT data used in intermodal transportation optimization include Vessel AIS, GPS data, Rail freight traffic, road Traffic, Port traffic, Weather, Inventory and shipment data, and data from Customer Experience (CX) and Customer Relationship Management (CRM) platforms along with feedback channels (for which Natural Language Processing models are needed). All the above sources can provide RT or near-RT information. Effective use of RT data improves network optimization, leading to increased efficiency, reduced costs, and improved customer satisfaction.

Table 1. Sample Data Sources

Requirement	Historic data source	Dynamic data source: freq., latency, spatial dimension
Maritime freight traffic	Same as dynamic, 60 days active, 4+ years in cold store, Port of Los Angeles 5+ years Wharfinger, Spire	Customs and Border Protection, Manifest for the Port of Los Angeles This applies to the main ocean carriers except for COSCO, Wan Hai shipping lines
Rail freight traffic	Rail data provider such as Railinc	Rail data provider such as Railinc
Road freight traffic	5+ years in-gate/out-gate for POLA	POLA In/out-gate (Excludes Road traffic), GeoStamp
Maritime routes	Reports from ocean carriers' web	Dynamic routes accessible from carriers' websites
Rail routes	Class 1 and short lines, Wabtec	Class 1 and short lines, Wabtec
Inland Waterways routes	Inland waterways Carriers	Information on the river system, such as its topology, current, and water levels. This data is used to simulate the river system and the flow of cargo on it
Truck routes	Dray providers	Providers (area of focus). Data can be provided daily
Port traffic	2+ Y historical of Marine Exchange, Spire Global API, Live data for ALL vessels within USA EEZ	Marine Exchange, GeoStamp Vessel to Port ETA functionality. Ability to call on all historical data Spire has (back to 2011)
Security Data	Own source	Security threats, risk assessments, and incident reporting. This data is used to ensure the safety and security of the port community
Shipment Data	On demand Freight data	O/D, type of goods being transported, and desired delivery date. Used to match shippers with carriers to meet needs
Weather Data	Several sources	The latency and frequency of weather data can vary depending on the source and the type of data. Data collected from ground-based sensors may have lower latency and higher frequency than weather data collected from satellites. Similarly, certain types of weather data, such as temperature and precipitation, may be collected and updated more frequently than other types of weather data, such as cloud cover or wind speed

4 Cybersecurity Considerations

The CIA triad, which stands for Confidentiality, Integrity, and Availability, is a fundamental concept in cybersecurity that applies to various systems and technologies, including digital twins. Let's discuss the CIA triad in the context of ports, container, and shipping digital twin systems:

Confidentiality: Confidentiality in the context of digital twin systems for ports, containers, and shipping refers to protecting sensitive information from unauthorized access. It involves ensuring that only authorized individuals or entities can access and view the data related to the digital twin system. Confidentiality measures can include strong access controls, encryption of sensitive data, and secure communication channels to prevent eavesdropping or data interception. For example, in a shipping digital twin, confidential information may include cargo details, shipping schedules, or trade secrets of the involved parties. Safeguarding this information is critical to prevent unauthorized disclosure or exploitation by malicious actors.

Integrity: Integrity refers to the assurance that the data and information within the digital twin system remain accurate, unaltered, and trustworthy. It involves protecting the data from unauthorized modifications, ensuring that it reflects the true state of the physical system being represented. In the context of ports, containers, and shipping digital twins, maintaining data integrity is crucial to avoid manipulation or tampering that could result in incorrect decisions, compromised safety, or financial losses. Implementing integrity controls such as data validation, digital signatures, and audit trails can help ensure the reliability and authenticity of the digital twin's data.

Availability: Availability refers to ensuring that the digital twin system is accessible and operational whenever it is needed. It involves safeguarding the system against disruptions, outages, or denial-of-service attacks that could render it inaccessible or unusable. For ports, containers, and shipping digital twins, availability is vital for maintaining smooth operations and efficient logistics. Downtime or unavailability of the digital twin system can lead to delays, inefficiencies, and potential financial losses. Implementing robust backup and disaster recovery mechanisms, redundancy, and proactive monitoring can help ensure high availability of the digital twin system.

In brief, the CIA triad provides a comprehensive framework for addressing cybersecurity concerns in ports, container, and shipping digital twin systems. By prioritizing confidentiality, integrity, and availability, organizations can establish a strong security foundation to protect sensitive data, maintain the accuracy of information, and ensure the continuous and reliable operation of their digital twin systems.

4.1 System's Cybersecurity Factors

The proposed optimization system will have cyber-attack resiliency through addressing key security factors. These key security factors aim to address the confidentiality, integrity, and availability (CIA) cybersecurity triad. Although the following factors are not fully encompassing of all security measures, they are the foundational factors for basic cyber hygiene.

Access controls is the first step to ensure data confidentiality. Limiting access to the system data lakes in the cloud, locally on premises, or off premises is essential to denying cyber-attacks. Access controls also play the role of giving the system's end user the proper level of access needed to do their jobs. For example, a system administrator, security analyst and truck driver will all need different levels of access. The later needing access to their specific data that is relevant to their logistic routes. Along with access control, authentication measures that match users with their digital identity is critical. The foundational authentication measures include using FIDO-compliant technology, a PKI

methodology, and asymmetric encryption methods. A more in-depth description on these authentication measures will be covered in the next section regarding protecting privacy of sensitive data. The system will need to establish an asset management program to track, monitor and update assets as needed to complete orders. By having a comprehensive list and inventory of assets allows the security team to manage the security requirements of each asset and their associated components. The system assets fall into four general categories that need to be managed. These categories are central hub assets, digital assets, transportation assets, and local driver assets. Each category will have their own asset inventory list with full detail of the assets themselves. Knowing what assets and data goes along with those assets is critical to being able to protect them from cyber-attacks and implement a change management program. The change management program is another key cybersecurity measure to consider when designing the system. The goal is to track and document all proposed engineering changes to individual subsystems and components. These changes will be analyzed with a wholistic view. This validates that the changes to each subsystem or component will not degrade or eliminate the functionality of the system.

Another key security factor is being able to protect the data and system in case of catastrophic loss through an attack. The cybersecurity measure of Backup and Restore (BAR) is vital to success. The copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or catastrophe, and backups provide a way of restoring deleted files or recovering a file when it is accidentally overwritten or becomes corrupted or may support recovery from a cyber-incident. To ensure successful backup and restore functionality, a full periodic full backup of the digital twin will be required at the current baseline. A full backup is the most complete type of backup where you duplicate all the selected data of the digital twin's configuration. This includes files, folders, SaaS applications, hard drives and more; while a full backup requires minimal to restore data, it takes longer to backup compared to other types of backups and places a burden on required storage space. When you back up data, all the information on your disk is saved as a single file called an image. If your digital twin crashes or gets corrupted, you may lose some or all your data. You can use this file to restore your digital twin exactly back to how it was before data loss.

Security monitoring is an important measure to implement to mitigate potential security violations and cyber-attacks. The Security Orchestration, Automated Response (SOAR) method security alert subsystem will have to be implemented to respond to the security alerts and potential attacks. This automated response method, SOAR, builds off the previously mentioned SIEM (security information and event management) alerting structure. Although the Security Incident/Event Management Subsystem is sufficient to accomplish security monitoring, SOAR takes things one step further by automating an actual response to help mitigate the risk as quickly as possible. Although SOAR is a more recent method to accomplishing security alert system along with the follow-on response playbooks. This is a cost-saving and efficiency optimization measure. Security alerts responses will largely be automated except for egregious violations.

SOAR improves the security operations when the subsystem is allowed to "automate investigation path workflows can significantly cut down on the amount of time required to handle alerts. They also provide lessons about the security admin skill set required

to complete an investigation path" (Froehlich, 2023). This analysis by former Cisco Enterprise-level IT security professional, Andrew, points out two key factors of SOAR that provide an added security layer of responses to security alerts.

To effectively protect an AI-driven real-time optimization information system for synchromodal freight operations, it is essential to utilize industry-standard cybersecurity frameworks and guidelines such as the Security Technical Implementation Guideline (STIG), ISO 27002, and NIST standards.

As with the Security Technical Implementation Guideline (STIG), these guidelines are specifically designed for the technology stack and components used in the AI-driven system. Regularly update and patch software and hardware components as per STIG guidelines to address vulnerabilities and protect against emerging threats. Conduct periodic STIG compliance assessments and audits to ensure ongoing adherence to the guidelines.

ISO 27002 could also be adopted as a comprehensive framework for establishing and maintaining an information security management system (ISMS). The IT managers could conduct a risk assessment to identify potential security risks and vulnerabilities in the AI-driven system. Develop and implement security policies, procedures, and controls based on ISO 27002 to mitigate identified risks. Regularly monitor, review, and update the security controls to align with evolving threats and organizational requirements. Ensure compliance with ISO 27002 through internal audits and periodic assessments.

Last, follow the NIST Cybersecurity Framework, which provides a flexible and customizable approach to managing and improving cybersecurity. Identify and categorize the AI-driven system's assets, assess risks, and develop risk mitigation strategies following NIST guidelines. Implement appropriate security controls, such as access controls, encryption, intrusion detection systems, and incident response plans, as recommended by NIST. Continuously monitor, detect, respond to, and recover from security incidents by aligning with NIST's incident response and recovery best practices.

By leveraging the Security Technical Implementation Guideline (STIG), ISO 27002, and NIST standards, organizations can establish a robust security posture for their AI-driven real-time optimization information systems in synchromodal freight operations. These frameworks provide comprehensive guidance and best practices to mitigate risks, protect sensitive data, and ensure the system's resilience against cyber threats.

4.2 System's Cybersecurity Risks

A digital twin-enabled, AI-driven optimization system for intermodal freight operations is a semi-autonomous system that leverages digital twins and Artificial Intelligence (AI) to optimize logistical operations. This is accomplished by collecting raw data from active operations, analyzing real-time goods movement data, and generating insights on how to improve the system.

The first cybersecurity risk that arises is faulty code that is at fault due to malicious actors. A large part of cybersecurity checks and evaluations has historically been solely at the end of the development process. This is dangerous for a variety of reasons and allows these malicious actors to start their cyber-attack early in the process and hide a trojan-type virus into the system's code. To field a testable digital twin that mimics systems in production, the code cannot have this potential vulnerability.

The first code type that logically should be secured is the source code. The source code that is used as a baseline configuration for all development could potentially be compromised and go undetected until deployment. This type of source code data poisoning and embedded viruses can hide if the malicious actor enters them smartly in the beginning of the development process. These data vulnerabilities can be part of the implementation process and deployed to production units without the developer's knowledge. Drivers and cyber operations dashboards would not be able to track security alerts and be utilized as they were intended. To mitigate this risk, a best practice known as "Shift-Left" can be implemented into the systems' security posture.

The Development, Security, Operations (DevSecOps) process incorporates security into the early stages of the software development life cycle. According to IBM, DevSecOps "integrates application and infrastructure security seamlessly into Agile and DevOps processes and tools. It addresses security issues as they emerge when they are easier, faster, and less expensive to fix. Additionally, DevSecOps makes application and infrastructure security a shared responsibility of development, security, and IT operations teams, rather than the sole responsibility of a security silo" ("DevSecOps," 2023). DevSecOps gives developers access to security tools throughout the process so that there are no integration problems at the end. The security vulnerabilities and flaws would be shifted left and found sooner rather than later.

"Shift left", promotes the integration of security measures into the early stages of the DevOps process ("DevSecOps", 2023). By moving security from the right (end) to the left (beginning) of the development cycle, software engineers are encouraged to prioritize security from the very beginning of the project. In a DevSecOps environment, cybersecurity architecture and development engineering is incorporated as part of the development team to guarantee that every phase has security measures. Furthermore, the configuration items in the stack are securely patched, configured, and documented. This will benefit change management and version control measures. By adopting a shift left approach, DevSecOps teams can detect security risks and vulnerabilities early and take immediate action to address them. This ensures that not only is the product being built efficiently, but that security is also being implemented simultaneously.

The next cybersecurity risk that will be relevant to the system is the risk of lateral movement, network device compromises and privilege escalation after bypassing the initial access controls and authentication stages. This risk is because of the increased attack surface of traditional cybersecurity measures that focus on this initial access barrier (North/South traffic) and allow freedom to move around within the network (East/West traffic). To mitigate this risk, using zero trust cybersecurity practices would be a sufficient mitigation path. Zero Trust Architecture (ZTA) takes an orthogonal view of cybersecurity by accounting for internal movement and east/west traffic within a network. This lets ZTA be viewed as "data-centered" rather than "user-centered". ZTA secures the data that flows all through the network while traditional measures attempted to secure the users in entering the network. The United States Government Accountability Office (GAO), states "Zero trust architecture (ZTA) is a cybersecurity approach that authenticates and authorizes every interaction between a network and a user or device" (Zero Trust Architecture, 2022). In a normal cybersecurity paradigm, a network user is allowed to roam freely east and west through the network once access is granted. An

attack surface is much smaller using a zero-trust mindset because there are consistent authorization measures that are implemented into the system design. This will be implemented as Policy-as-Code and will be automated through firewall parameters, router rules and ACLs. ZTA will be very important for the system because of the data structure and hybrid-cloud environment. The GAO describes the importance of ZTA with some background. "Given the increasingly complex nature of IT networks, including cloud and hybrid environments, ZTA's goals are to reduce opportunities for attackers by restricting access and to detect attacks by monitoring user behavior and other network activity" (Zero Trust Architecture, 2022). Given the hybrid data storage and data movement paths through secure VPNS, this major reduction of attack surface will directly lower system's security risk.

The last major cybersecurity risks the system will be faced with is being in the dark about security threats and attacks. The system will need the ability to receive notifications of cyber security attacks. Whenever there is data out there that can be compromised, the system vulnerabilities will be attacked by cyber criminals. The criminals hope to gain some sort of gain. Whether that gain be a financial, competitive advantage, competitor insights or some sort of notoriety. When these cyber-attacks occur, the system will have a prompt, security alert and security management subsystem to alert security analysts of the breach. As mentioned, the Security Incident/Event Management (SIEM) subsystem is sufficient to mitigate this cybersecurity risk and accomplish security monitoring. This subsystem will be expanded on in the next section to automate the responses. However, to automate a response to a security breach, a type of SIEM subsystem is the foundation for mitigating security alerts that will arise. The SIEM tools are "a way to centrally collect pertinent log and event data from various security, network, server, application, and database sources. SIEMs then detect and alert on security events" (Froehlich, 2023). This allows security analysts to review the log data, identify the threat, isolate, and mitigate as appropriate. As mentioned, this will be automated by another subsystem in later phases. Another benefit of the SIEM subsystem is that "Aggregated data is analyzed by the SIEM in real time to spot potential security issues. Because multiple data sources are analyzed, the SIEM identifies threats by correlating information from more than one source" (Froehlich, 2023). The system will leverage this feature to collect and store data at each local host and aggregated host data at the hub. Additionally, "The SIEM then intelligently ranks the events in order of criticality" (Froehlich, 2023). The SIEM AI feature that stacks and ranks the security alerts will be very beneficial to cost savings and efficiency. Buckbee (2022) states some of the top SIEM tools used including Splunk, IBM QRadar, and Logrhythm.

Table 2 shows a summary of the cybersecurity considerations and the measures to counteract.

Table 2. Cybersecurity threats and measures for system design

Cybersecurity threat	Measures suggested for system design
Malware and Ransomware Attacks	Implement Strong Endpoint Protection, Patch and Update Software, Conduct Employee Awareness Training, Enable Email Filtering and Spam Detection, Implement Network Segmentation, Regularly Backup and Encrypt Data, Enforce Strong Password Policies, Maintain Incident Response and Recovery Plans, Monitor Network Traffic and Behavior, Regularly Test and Update Security Measures
Phishing and Social Engineering	Employee Education and Awareness, Implement Email Filtering and Spam Detection, Multi-Factor Authentication (MFA), Encourage Reporting of Suspicious Activities, Strong Password Policies, Incident Response and Mock Exercises, Implement Web Filtering
Insider Threats	User Access Control, User Behavior Monitoring, Employee Awareness and Training, Confidentiality Agreements and Policies, Regular Security Awareness Programs, Segregation of Duties, Employee Offboarding Processes, Cultivate a Positive Work Environment
Distributed Denial of Service (DDoS) Attacks	Network Monitoring and Traffic Analysis, DDoS Mitigation Services, ensure a Scalable Network Infrastructure, Traffic Filtering and Rate Limiting, Content Delivery Network (CDN) Services, Deploy Intrusion Detection and Prevention Systems (IDPS), Incident Response Planning, Deploy Redundancy and Failover Systems, Traffic Scrubbing and Blackholing, Regular Testing and Preparedness
Data Breaches and Unauthorized Access	Data Encryption, Access Controls and Authentication, Secure Network Infrastructure, Vulnerability Assessments and Penetration Testing, Employee Education and Awareness, Data Backup and Disaster Recovery (Business Continuity), Intrusion Detection and Monitoring, Incident Response Planning, Data Privacy and Compliance, Regular Security Audits and Compliance Assessments
Supply Chain Attacks	Vendor Risk Management, Secure Development Lifecycle, Continuous Monitoring, Multi-Factor Authentication (MFA), Secure Software and Firmware Updates, Secure Configuration Management, Incident Response and Recovery Planning, Threat Intelligence Sharing, Employee Awareness and Training, Supply Chain Resilience, Use secure protocols, such as HTTPS or SFTP, for transmitting origin/destination data over networks, Minimize the collection, storage, and retention of origin/destination data to reduce the potential impact of a data breach, Third-Party Risk Management
IoT and Operational Technology (OT) Vulnerabilities	Implement strong security controls for IoT and OT devices, Network Segmentation, Access Control and Privileged Access Management, Regular Patching and Updates, Secure Configuration Management, Network Monitoring and Intrusion Detection, Security Testing and Penetration Testing, Vendor Management and Supply Chain Security, Employee Training and Awareness, Incident Response and Business Continuity Planning

4.3 Preserving Security and Privacy of Sensitive Data

There is a large need for the system to have overarching security protections on sensitive data to protect customer, supplier, and employee information. Data Privacy rulesets are baked into the source code that the system uses. Both data at rest and data in transit should have cybersecurity measures built into the system design.

The primary method to store and secure the data will be in a cloud instance. This allows the cloud storage infrastructure to be managed at the Hub and treats the production units as Thin Clients. Thin clients are defined as "a virtual desktop computing model that runs on the resources stored on a central server instead of a computer's resources" (Gillis, 2021). Both cloud and hard drive based local backup methods have advantages and disadvantages. To take advantage of both and fully address any possible data loss, a hybrid backup strategy is recommended, where backups are created locally and in the cloud. The 3-2-1 backup rule industry standard describes that the data is kept in three places, across two media, with one backup stored offsite, such as in the cloud.

Local hard drive data storage will be utilized on an incremental, scheduled basis. This local, hard drive backup refers to the process of backing up the system, applications, and data to a device located internally or as a connected component, such as tape, disk, hard disk, flash drive, CD, external hard drive, or other media. This type of backup will be located and kept solely by data custodians located on site at the Hub. Due to the growing storage capacity restraints for the massive amounts of data that gets produced, this will not be a full data storage strategy. However, a very important data storage strategy if the cloud was ever compromised.

On-Prem means the data is stored on the Hub's premises but in a cloud storage location. Cloud based data storage on-premises backup refers to the process of backing up the system, applications, and data to a public or private cloud that is located on the Hub premises. The cloud will be configured as a secure database that collects the data and stores it into the centralized servers. These servers are located on site at the Hub. Off-premises backup refers to the process of backing up the system, applications, and data to a public or private cloud that is located off the premises. (i.e., on a production unit). This will be the primary method of collecting and storing data for the different transportation methods and personnel involved. Off Prem is when the data is not part of the centralized cloud storage infrastructure. Rather, a means to store local data of driver information and movement in a separate, secure cloud storage that acts as a thin client. Thin clients are very useful because it reduces the cyber-attack surface and protects the data that is generated by each unit. However, there is a drawback. This drawback being "Normally thin clients take the form of low-cost computing devices that heavily rely on a server for computation" (Gillis, 2021). This puts the computational power back onto the server side located at the Hub instead of the clients themselves on the truck, train, or boat.

Protecting data at rest within the Hub database and storage locations can be accomplished by enforcing three key security procedures of database encryption, access and authentication ("Protecting data at rest," 2023). Enforcing access controls and proper authentication using MFA points protects the core cybersecurity triad. Confidentiality, data integrity and availability are protected because there is no unauthorized access to the data being stored. All data that is meant to be seen by authorized personnel is available.

If there is unauthorized access, the database encryption is the fallback security measure that ensures the sensitive data is protected. The method to protect sensitive data in transit is to set up an enterprise level Virtual Private Network (VPN) and direct, secure connection between the Hub and fielded units. This method of protecting sensitive data in transit allows the system to mitigate security risks inherent to providing remote network access by offering strong encryption to provide data security and strong authentication, to limit access to applications based on security policies (Loshin, 2019).

Having the ability to hide the identity of information is another way to protect private data, as it would make it difficult to pinpoint whose data it is. QueryPie (2022) goes into detail about the difference between anonymization and pseudonymization, but how both can be beneficial to protecting personal data. Anonymization is the process of eliminating all identifiers from the data, whereas pseudonymization uses a pseudonym identifier takes place of the actual identifier of the data.

Cybersecurity and data privacy are prioritized steps to ensuring safe use of the proposed optimization system. To reach the appropriate level of security and privacy for the system, there are several legal and regulatory issues that must be addressed. Intellectual Property (IP) rights are one of the leading legal obstacles that must be considered when using AI-driven models and algorithms. Medeiros and Sanft (2018) state that IP is associated with inventions, brands, new technologies, source code, and artistic work that have patents, trademarks, and copyright ownership.

5 Key Challenges in Integrating Cybersecurity and Data Privacy Considerations into the Proposed Optimization System

There are many cybersecurity and data privacy concerns that will need to be addressed before design and implementation occurs. This section will address and dive into three key challenges that the system will face integrating cybersecurity and data privacy. After the key challenge is identified and defined, the follow-on framework to address the privacy concern will be laid out.

Key challenge 1 (KC1) touches on both cybersecurity and data privacy considerations of the system through policy implementation. This key challenge is a cybersecurity policy implementation measure while also striving to protect data privacy. The second key challenge, KC2, will be to keep the system up to date with security and vulnerability guidance on the system components and subsystems. This mainly addresses the cybersecurity consideration portion. The third key challenge, KC3, is a pure data privacy consideration that involves securing personal data. The framework for this key challenge builds off the FIDO-based security technology that includes a public key infrastructure (PKI) and asymmetric encryption.

The first key challenge that the system will be faced with is policy implementation and policy enforcement. Cybersecurity policies implementation and enforcement is important because these policies "defines which conditions must be met in order for a code to pass a security control and be deployed" (Carroll, 2023). The system will be leveraging the DevSecOps process with built in policy implementation that act as guardrails. If these policies are violated, the code is considered to be not secure and should be flagged as a security alert. To address this policy implementation challenge,

Policy-as-Code (PaC) will be embedded to automate the process. Policy-as-Code (PaC) is defined as "an approach to policy management in which policies are defined, updated, shared, and enforced using code. By leveraging code-based automation instead of relying on manual processes to manage policies, policy-as-code allows teams to move more quickly and reduce the potential for mistakes due to human error" (Carroll, 2023). PaC allows policy enforcement and implementation to be automated, cheaper to audit, and allows for more efficiencies throughout the system. Implementing the PaC framework to put up guardrails during initial design and fielding puts security in a better posture as well. PaC is set up to be a collaboration tool as well. The system can use "a policy-as-code approach to domains like security makes it possible to define and manage policies in ways that different types of stakeholders – such as developers and security engineers – can understand" (Carroll, 2023). This improves the developer and manager collaboration and project communication. Regardless of technical skill or policy expertise, the PaC explicitly outlines the policies and sets up enforcement guidelines at the same time.

The next key challenge to cybersecurity and data privacy is to address security technical implantation guidance (STIGs) updates and procedures. STIGs are used "for verifying that the product has been configured properly, and/or for identifying unauthorized configuration changes to the product" (Quinn et al., 2018). Historically, this was very much a manual process of reviewing the STIGs and finding out how they differ than what is currently fielded. STIGS can be automatically delta checked and implemented through an automated checklist program. The checklist will be designed like how the U.S. government uses the National Checklist Program (NCP). The NCP is "the U.S. government repository of publicly available security checklists (or benchmarks)" (National Checklist Program, 2023). These components and subsystems that will need constant security implementation include operating systems, AI-model, the SIEM subsystem, database, and cloud services (i.e., AWS), firewalls, routers, switches, network logging subsystem, vulnerability subsystem, audit collection subsystem and the virtual hosting environment. The NCP is beneficial because "Applying checklists to operating systems and applications can reduce the number of vulnerabilities that attackers can attempt to exploit and lessen the impact of successful attack" (Quinn et al., 2018). Essentially, the checklist is a proactive security process that shores up the system for known vulnerabilities. The NCP is a checklist "that provides detailed low-level guidance on setting the security configuration of operating systems and applications" (Quinn et al. 2018). NIST identifies the main security benefit of using the NCP is to "minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected" (Quinn et al., 2018). Lower impact, reduced vulnerabilities and less attack surface leads to lower project cost, heightened security posture and faster project implementation.

The last key challenge that will be addressed that poses a risk to the system operations is data privacy and governance of a data privacy program. The governance portion really looks at the business operations and aligns the data privacy measures accordingly. Using the appropriate level of data privacy measures and establishing a framework for the system is how this key challenge can be addressed.

6 Managerial Insights

This article highlights the critical managerial insights for designing an AI-driven distributed optimization system with a strong focus on cybersecurity considerations. By adopting a cybersecurity-first approach, investing in robust cybersecurity measures, fostering awareness, collaborating with industry partners, conducting regular risk assessments, and planning for incident response and recovery, managers can enhance the security and resilience of the system, protecting valuable data and ensuring the successful implementation of container carbon emissions reduction in freight operations.

It highlights the importance of adopting a cybersecurity-first approach when designing an AI-driven distributed optimization system for container carbon emissions reduction in freight operations. Managers should prioritize cybersecurity considerations right from the system's design phase to mitigate potential risks and safeguard sensitive data.

It highlights the importance of investing in robust cybersecurity measures. Given the increasing connectivity and interdependence of systems in the freight industry, it is imperative to invest in robust cybersecurity measures. Managers should allocate resources for implementing encryption mechanisms, access controls, anomaly detection systems, and other cybersecurity solutions to protect the system against cyber-attacks and unauthorized access.

The article also highlights the importance of fostering a culture of cybersecurity awareness. It is essential to conduct regular risk assessments and audits to identify vulnerabilities, evaluate the effectiveness of implemented cybersecurity measures, and ensure compliance with relevant industry standards and guidelines. Managers should allocate resources for periodic assessments, penetration testing, and audits to detect and address any weaknesses or gaps in the system's security.

Last, the article shows the importance of planning for incident response and recovery. Despite preventive measures, it is important to have a well-defined incident response plan in place. Managers should establish protocols for detecting, responding to, and recovering from cybersecurity incidents. This includes defining roles and responsibilities, establishing communication channels, and regularly testing incident response plans through tabletop exercises and simulations.

7 Conclusions

The design of a digital twin-enabled AI-driven real-time distributed optimization system for synchromodal freight operations has the potential to significantly reduce carbon emissions and increase efficiency in the transportation industry. However, with the use of advanced technologies also comes the potential for cybersecurity risks.

This article highlights the key cybersecurity considerations that need to be addressed in the design of such a system. These include securing the data flow, ensuring the security of the digital twin models, preserving the privacy for all stakeholders, and protecting the system against cyber-attacks. The proposed solutions to these challenges include the use of encryption, access control, and anomaly detection systems, and mitigation strategies when an attack happens, among others.

The success of the proposed system depends on the implementation of these cybersecurity measures. The transportation industry must prioritize cybersecurity to ensure

the safety and integrity of the transportation network and its stakeholders. By adopting a cybersecurity-first approach, the users of this system can mitigate risks and ensure that the benefits of the system are fully realized.

Future research should focus on further refining the proposed cybersecurity solutions and addressing new cybersecurity challenges that may arise as the system is deployed. One area that requires attention is the potential impact of emerging technologies, such as quantum computing, on the security of the system. Quantum computing has the potential to break the encryption algorithms currently used to secure data, and thus, there is a need to explore new encryption methods that are resistant to quantum attacks.

Another area of interest is the development of improved, more automated machine learning algorithms that can detect and prevent cyber-attacks in real-time. Traditional cybersecurity measures, such as firewalls and intrusion detection systems, may not be sufficient in detecting sophisticated cyber-attacks that can exploit system vulnerabilities. Machine learning algorithms can learn from past cyber-attacks and detect new and unknown cyber-attacks, leading to better and more effective cybersecurity measures.

Furthermore, future research should also explore the potential of blockchain technology in securing the system. Blockchain technology provides a decentralized and tamper-proof data storage and transaction control mechanism that can enhance data security and integrity, making it a promising technology for securing digital twin-enabled AI-driven real-time distributed optimization systems.

Overall, this paper describes certain topics as to how a cybersecurity-aware design approach can enable the successful implementation of a digital twin-enabled AI-driven real-time distributed optimization system for synchromodal freight operations, leading to significant benefits for the transportation industry and the environment.

References

Cost of a Data Breach Report 2022. IBM (2022). https://www.ibm.com/reports/data-breach?utm_medium=OSocial&utm_source=Blog&utm_content=SSSWW&utm_id=Security-Intelligence-Blog-Banners%20&_ga=2.169531361.1119445732.1681783239-1093745095.1681783239. Accessed 14 Apr 2023

What is DevSecOps? IBM (2023). https://www.ibm.com/topics/devsecops#Benefits%20of%20DevSecOps. Accessed 17 Apr 2023

Zero Trust Architecture. GAO (2022). https://www.gao.gov/products/gao-23-106065. Accessed 15 Apr 2023

Protecting data at rest. AWS Inc. (2023). https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-data-at-rest.html. Accessed 17 Apr 2023

US Department of Commerce, National Oceanic and Atmospheric Administration: API web service (2023). https://www.weather.gov/documentation/services-web-api. Accessed 10 Apr 2023

NIST. Post-quantum cryptography: CSRC (2017). https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed 18 Apr 2023

NIST. Round 3 submissions - post-quantum cryptography: Computer Security Resource Center (CSRC) (2023). https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions. Accessed 17 Apr 2023

NVIDIA. NVIDIA H100 Tensor Core GPU Datasheet. NVIDIA (2022). https://resources.nvidia.com/en-us-tensor-core/nvidia-tensor-core-gpu-datasheet. Accessed 13 Apr 2023

NVIDIA. Triton Inference Server. NVIDIA Developer (2023). https://developer.nvidia.com/nvidia-triton-inference-server#ecosystem. Accessed 14 Apr 2023

NVIDIA. Nvidia TENSORRT. NVIDIA Developer (2023). https://developer.nvidia.com/tensorrt. Accessed 14 Apr 2023

JSON and XML weather API and Geolocation Developer API. Free Weather API - WeatherAPI.com (n.d.). https://www.weatherapi.com/. Accessed 10 Apr 2023

Abril, D., Velasquez-Bermudez, J., Paternina-Arboleda, C.D., Cantillo, V.: Integrated tactical-operational event-driven real-time optimization framework for smart ports operations planning. Marit. Econ. Logist. (2023, Submitted)

Aggarwal, B.K., Gupta, A., Goyal, D., Gupta, P., Bansal, B., Barak, D.D.: A review on investigating the role of block-chain in cyber security. Mater. Today Proc. **56**(Part 6), 3312–3316 (2022). ISSN: 2214-7853. https://doi.org/10.1016/j.matpr.2021.10.124

Aggarwal, A., Dhurkari, R.K.: Association between stress and information security policy non-compliance behavior: a meta-analysis. Comput. Secur. **124**, 102991 (2023). ISSN: 0167-4048. https://doi.org/10.1016/j.cose.2022.102991

Amador-Fontalvo, J.A., Paternina-Arboleda, C.D., Montoya-Torres, J.R.: Solving the heterogeneous vehicle routing problem with time windows and multiple products via a bacterial meta-heuristic. Int. J. Adv. Oper. Manag. **6**(1), 81–100 (2014)

Auld, J., Hope, M., Ley, H., Sokolov, V., Xu, B., Zhang, K.: POLARIS: agent-based modeling framework development and implementation for integrated travel demand and network and operations simulations. Transp. Res. Part C Emerg. Technol. **64**, 101–116 (2016)

Beaumont, P.: Cybersecurity risks and automated maritime container terminals in the age of 4IR. In: Information and Cybersecurity in the Fourth Industrial Revolution. IGI Global (2018). https://doi.org/10.4018/978-1-5225-4763-1.ch017

Cammin, P., Yu, J., Voß, S.: Tiered prediction models for port vessel emissions inventories. Flex Serv. Manuf. J. **35**, 142–169 (2023). https://doi.org/10.1007/s10696-022-09468-5

Cobb, M.: What is the RSA algorithm? Definition from search security. Security (2021). https://www.techtarget.com/searchsecurity/definition/RSA. Accessed 17 Apr 2023

De la Cruz, J.J., Paternina-Arboleda, C.D., Cantillo, V., Montoya-Torres, J.R.: A two-pheromone trail ant colony system—tabu search approach for the heterogeneous vehicle routing problem with time windows and multiple products. J. Heuristics **19**, 233–252 (2013). https://doi.org/10.1007/s10732-011-9184-0

De la Peña-Zarzuelo, I., Soeane, M.J.F., Bermúdez, B.L.: Industry 4.0 in the port and maritime industry: a literature review. J. Ind. Inf. Integr. **20**, 100173 (2020). ISSN: 2452-414X. https://doi.org/10.1016/j.jii.2020.100173

Dzemydienė, D., Burinskienė, A., Čižiūnienė, K., Miliauskas, A.: Development of E-service provision system architecture based on IoT and WSNs for monitoring and management of freight intermodal transportation. Sensors **23**(5), 2831 (2023). https://doi.org/10.3390/s23052831

Froehlich, A.: SOAR vs. SIEM: What's the difference? Tech Target (2023). https://www.techtarget.com/searchsecurity/answer/SOAR-vs-SIEM-Whats-the-difference. Accessed 15 Apr 2023

Gillis, A.: Thin client (lean client). Tech Target (2021). https://www.techtarget.com/searchnetworking/definition/thin-client. Accessed 16 Apr 2023

Guo, X., He, J., Lan, M., Yu, H., Yan, W.: Modeling carbon emission estimation for hinterland-based container intermodal network. J. Clean. Prod. **378**, 134593 (2022). ISSN: 0959-6526. https://doi.org/10.1016/j.jclepro.2022.134593

Jubiz-Diaz, M.A., Saltarin-Molino, M.A., Arellana, J., Paternina-Arboleda, C.D., Yie-Pinedo, R.: Effect of infrastructure investment and freight accessibility on gross domestic product: a data-driven geographical approach. J. Adv. Transp. **2021** (2021). Article ID: 5530114. https://doi.org/10.1155/2021/5530114

Lipner, S.B., et al.: Security kernels. In: Proceedings of the May 6–10, 1974, National Computer Conference and Exposition on - AFIPS 1974, vol. 43, pp. 977–978 (1974). https://doi.org/10.1145/1500175.1500361

Loshin, P.: IPsec vs. SSL VPN: comparing speed, security risks and technology. Tech Target (2019). https://www.techtarget.com/searchsecurity/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks

Moros-Daza, A., Solano, N.C., Amaya, R., Paternina, C.: A multivariate analysis for the creation of Port Community System approaches. Transp. Res. Procedia **30**, 127–136 (2018). ISSN: 2352-1465. https://doi.org/10.1016/j.trpro.2018.09.015

Moros-Daza, A., Hoz, D.-D., Jaller-Martelo, M., Paternina-Arboleda, C.D.: Using advanced information systems to improve freight efficiency: results from a pilot program in Colombia. In: Paternina-Arboleda, C., Voß, S. (eds.) ICCL 2019. LNCS, vol. 11756, pp. 22–38. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31140-7_2

Moros-Daza, A., Amaya-Mier, R., Paternina-Arboleda, C.: Port Community Systems: a structured literature review. Transp. Res. Part A Policy Pract. **133**, 27–46 (2020). ISSN: 0965-8564. https://doi.org/10.1016/j.tra.2019.12.021

Möller, M., Vuik, C.: On the impact of quantum computing technology on future developments in high-performance scientific computing. Ethics Inf. Technol. **19**(4), 253–269 (2017). https://doi.org/10.1007/s10676-017-9438-0

Nichols, B.: The Current State of DevSecOps Metrics. CMU (2021). https://insights.sei.cmu.edu/blog/the-current-state-of-devsecops-metrics/

Palma-Blanco, A., González, E.R., Paternina-Arboleda, C.D.: A two-pheromone trail ant colony system approach for the heterogeneous vehicle routing problem with time windows, multiple products and product incompatibility. In: Paternina-Arboleda, C., Voß, S. (eds.) ICCL 2019. LNCS, vol. 11756, pp. 248–264. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31140-7_16

Paternina-Arboleda, C.D., Das, T.K.: A multi-agent reinforcement learning approach to obtaining dynamic control policies for stochastic lot scheduling problem. Simul. Model. Pract. Theory **13**(5), 389–406 (2005)

Paternina-Arboleda, C.D., Das, T.K.: Intelligent dynamic control policies for serial production lines. IIE Trans. **33**(1), 65–77 (2001). https://doi.org/10.1023/A:1007641824604

Paternina-Arboleda, C.D., Montoya-Torres, J.R., Fabregas-Ariza, A.: Simulation-optimization using a reinforcement learning approach. In: 2008 Winter Simulation Conference, Miami, FL, USA, pp. 1376–1383 (2008). https://doi.org/10.1109/WSC2008.4736213

Paternina-Arboleda, C.D., Agudelo-Castañeda, D., Voß, S., Das, S.: Prediction of SO2 ports emissions inventories. Sustainability (2023, Submitted)

Rakos, D.: Understanding GPU caches. [web log] (2021). https://www.rastergrid.com/blog/gpu-tech/2021/01/understanding-gpu-caches/. Accessed 12 Apr 2023

Sarabia, Carolina, M., John, H., Rios-Griego, Carlos, D., Paternina-Arboleda: Simulation-based decision support models for river cargo transportation. In: 2006 IEEE Systems and Information Engineering Design Symposium, pp. 142–145 (2006)

Saxon, S., Stone, M.: Container shipping: the next 50 years. A McKinsey & Company report (2017)

Saxena, A.: What are AI accelerators and how does it work? BISinfotech (2022). https://www.bisinfotech.com/what-are-ai-accelerators-and-how-does-it-work/. Accessed 14 Apr 2023

Shankland, S.: Quantum computers could crack today's encrypted messages. That's a problem. CNET (2021). https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/. Accessed 17 Apr 2023

Song, D.: A literature review, container shipping supply chain: planning problems and research opportunities. Logistics **5**, 41 (2021). https://doi.org/10.3390/logistics5020041

Trucco, P., Petrenj, B.: Characterisation of resilience metrics in full-scale applications to interdependent infrastructure systems. Reliab. Eng. Syst. Saf. **235**, 109200 (2023). ISSN: 0951-8320. https://doi.org/10.1016/j.ress.2023.109200

Tsvetkova, A., Gustafsson, M., Wikström, K.: Digitalizing maritime transport: digital innovation as a catalyzer of sustainable transformation. In: Montero, J., Finger, M. (eds.) A Modern Guide to the Digitalization of Infrastructure. Elgar Modern Guides, pp. 123–148. Edward Elgar (2021)

Velasquez-Bermudez, J.M., Abril, D., Paternina-Arboleda, C.D.: Optimizing port operations to cope with shipping congestion in South American countries. OR/MS Today **49**(2) (2022)

Velásquez-Bermúdez, J.M., Khakifirooz, M., Fathi, M. (eds.): Large Scale Optimization in Supply Chains and Smart Manufacturing: Theory and Applications. Springer, Cham (2020). ISBN: 978-3-030-22790-6. https://doi.org/10.1007/978-3-030-22788-3

Wang, Z., Liu, X.: Cyber security of railway cyber-physical system (CPS) – a risk management methodology. Commun. Transp. Res. **2**, 100078 (2022). ISSN: 2772-4247. https://doi.org/10.1016/j.commtr.2022.100078

Woschank, M., Rauch, E., Zsifkovits, H.: A review of further directions for artificial intelligence, machine learning, and deep learning in smart logistics. Sustainability **12**, 3760 (2020). https://doi.org/10.3390/su12093760

Yang, Z., et al.: Indicator-based resilience assessment for critical infrastructures – a review. Saf. Sci. **160**, 106049 (2023). ISSN: 0925-7535. https://doi.org/10.1016/j.ssci.2022.106049

Zemp, B.: The Intersection Between AI and Blockchain Technology – Industries of Tomorrow. Forbes (2023). https://www.forbes.com/sites/forbesbooksauthors/2023/02/28/the-intersection-between-ai-and-blockchain-technology--industries-of-tomorrow/?sh=1731ee7d4de7. Accessed 14 Apr 2023

Zhang, W., Guhathakurta, S., Khalil, E.B.: The impact of private autonomous vehicles on vehicle ownership and unoccupied VMT generation. Transp. Res. Part C Emerg. Technol. **90**, 156–165 (2018)