Maritime Cybersecurity Leveraging Artificial Intelligence Mechanisms Unveiling Recent Innovations and Projecting Future Trends

Parasuraman Kumar[1*], and Arumugam Maharajan[2]
[1] Associate Professor, Department of Information Technology and Engineering, Manonmaniam Sundaranar University (School of Computer Science and Engineering), Tirunelveli, Tamil Nadu, India
[e-mail: kumarcite@gmail.com]
[2] Research Scholar, Department of Information Technology and Engineering, Manonmaniam Sundaranar University, (School of Computer Science and Engineering), Tirunelveli, Tamil Nadu, India
[e-mail: mahapadmavathy@gmail.com]
[*]Corresponding author: Parasuraman Kumar

Received June 14, 2024; revised August 6, 2024; revised September 12, 2024; accepted September 25, 2024; published October 31, 2024

Abstract

This research delves into the realm of Maritime Cybersecurity, focusing on the application of Artificial Intelligence (AI) mechanisms, namely K-Nearest Neighbors (KNN), Random Forest (RF), and Artificial Neural Networks (ANN). The maritime industry faces evolving cyber threats, necessitating innovative approaches for robust defense. The maritime sector is increasingly reliant on digital technologies, making it susceptible to cyber threats. Traditional security measures are insufficient against sophisticated attacks, necessitating the integration of AI mechanisms. This research aims to evaluate the effectiveness of KNN, RF, and ANN in fortifying maritime cybersecurity, providing a proactive defense against emerging threats. Investigate the application of KNN, RF, and ANN in the maritime cybersecurity landscape. Assess the performance of these AI mechanisms in detecting and mitigating cyber threats. Explore the adaptability of KNN, RF, and ANN to the dynamic maritime environment. Provide insights into the strengths and limitations of each algorithm for maritime cybersecurity. The study employs these AI algorithms to analyze historical maritime cybersecurity data, evaluating their accuracy, precision, and recall in threat detection. Results demonstrate the effectiveness of KNN in identifying localized anomalies, RF in handling complex threat landscapes, and ANN in learning intricate patterns within maritime cybersecurity data. Comparative analyses reveal the strengths and weaknesses of each algorithm, offering valuable insights for implementation. In conclusion, the integration of KNN, RF, and ANN mechanisms presents a promising avenue for enhancing maritime cybersecurity. The study underscores the importance of adopting AI solutions to the maritime domain's unique challenges. While each algorithm demonstrates efficacy in specific scenarios, a hybrid approach may offer a comprehensive defense strategy. As the maritime industry continues to evolve, leveraging AI mechanisms becomes imperative for staying ahead of cyber threats and

http://doi.org/10.3837/tiis.2024.10.010 **ISSN : 1976-7277**

safeguarding critical assets. This research contributes to the ongoing discourse on maritime cybersecurity, providing a foundation for future developments in the field.

Keywords: Accuracy, Artificial Neural Networks (ANN), K-Nearest Neighbors (KNN), Maritime Cybersecurity, Precision, Random Forest (RF), Recall, Threat Detection.

1. Introduction

The maritime industry, a cornerstone of global trade and commerce, has undergone a transformative shift towards digitalization in recent years. The integration of advanced technologies, while enhancing operational efficiency, has concurrently exposed the maritime sector to an escalating and sophisticated threat landscape of cyber risks. Cybersecurity in the maritime domain has become a critical concern as malicious actors seek to exploit vulnerabilities in critical systems, posing significant risks to the safety, integrity, and economic stability of maritime operations [1].

In response to the pressing challenges posed by cyber threats, the incorporation of Artificial Intelligence (AI) mechanisms has emerged as a promising frontier for fortifying cybersecurity defenses in the maritime sector. This research focuses on evaluating the application of three distinct AI algorithms: K-Nearest Neighbors (KNN), Random Forest (RF), and Artificial Neural Networks (ANN) intending to uncover their potential in safeguarding maritime assets and operations. Through the utilization of these sophisticated mechanisms, the maritime industry aims to proactively address cyber threats, anticipating and mitigating risks to ensure the resilience of global maritime trade [2].

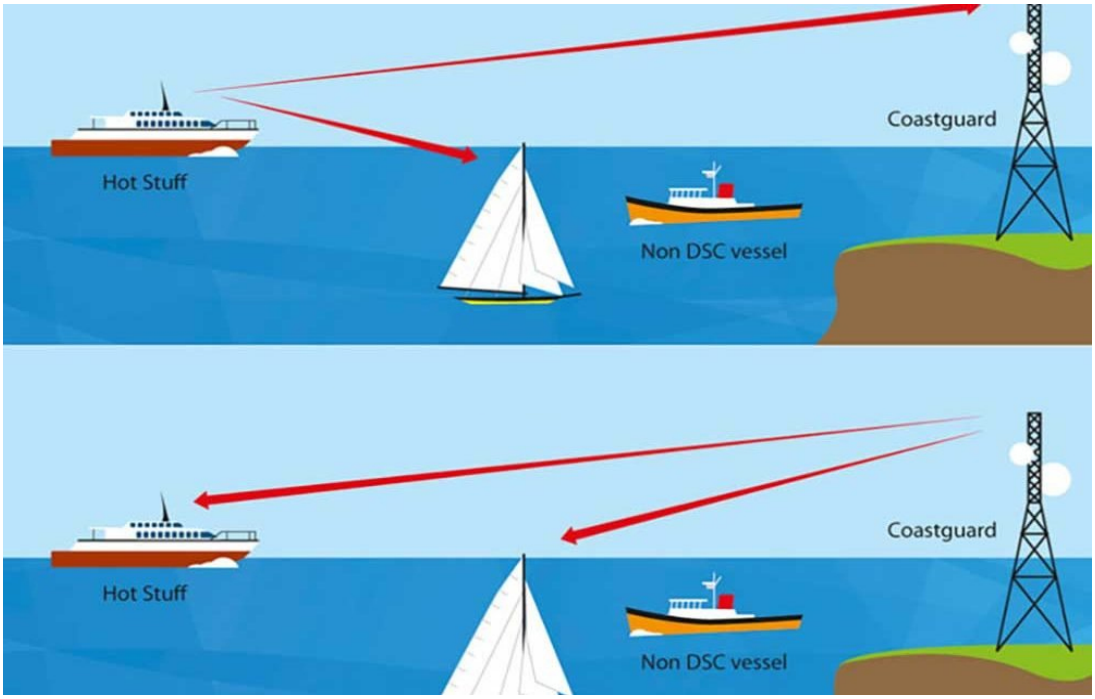

Fig. 1. Architecture for Maritime Data Transaction

Fig. 1, illustrates a maritime data communication scenario involving a vessel named Hot Stuff, a sailboat referred to as a Non-DSC vessel, and a coastguard station. The Hot Stuff emits a red signal line, representing a digital selective calling (DSC) signal, which is a standardized communication protocol used to initiate ship-to-shore, ship-to-ship, or other types of maritime distress calls. This signal is directed towards the coastguard station, indicating that the Hot Stuff is likely sending a distress signal or other important communication directly to the coastguard. The Non-DSC vessel, which does not have DSC capabilities, is not involved in this direct digital communication with the coastguard. The Hot Stuff is again emitting the DSC signal, but this time the signal is not reaching the coastguard station directly. Instead, the signal is reflected off the sailboat (Non-DSC vessel), which then reaches the coastguard. This may represent an indirect method of communication, perhaps in a scenario where the direct line to the coastguard is obstructed or out of range, and the signal is being bounced off the sailboat to reach the coastguard station. This kind of reflection could be a metaphor for relay communication in maritime operations, where a signal from one vessel is relayed by another vessel to reach the intended recipient, which can be crucial when direct communication is not possible.

This research is motivated by the acknowledgment of the maritime industry's susceptibility to cyber threats and the imperative to adopt advanced cybersecurity measures. Traditional security approaches often prove inadequate in the face of increasingly sophisticated attacks, necessitating a paradigm shift towards innovative solutions, particularly those leveraging AI. The motivation stems from the urgency to explore these cutting-edge solutions to fortify maritime cybersecurity and ensure the uninterrupted flow of global maritime trade.

1.1 Background

The maritime industry, a linchpin of global commerce, has undergone a digital transformation marked by increased automation, connectivity, and data-driven operations. This evolution, while enhancing efficiency and competitiveness, has concurrently exposed the maritime sector to a burgeoning threat landscape in the form of cyber-attacks. Maritime cyber threats encompass a spectrum of malicious activities, including unauthorized access to ship systems, data breaches, and potential disruptions to navigation and communication systems [3, 8].

Traditional maritime cybersecurity measures, primarily reliant on firewalls and antivirus software, are proving insufficient against the escalating sophistication of cyber adversaries. As vessels and port facilities become more interconnected and reliant on digital infrastructure, there is a critical need to enhance cybersecurity strategies with advanced technologies. Artificial Intelligence (AI) mechanisms, such as Machine Learning (ML) algorithms, offer a paradigm shift in fortifying maritime cybersecurity by providing adaptive, real-time threat detection and response capabilities [6].

As the maritime industry continues to navigate the digital waters, the integration of AI mechanisms becomes imperative to anticipate and mitigate cyber threats. This research aims to explore recent innovations in AI, including K-Nearest Neighbors (KNN), Random Forest (RF), and Artificial Neural Networks (ANN), to provide a comprehensive understanding of their applicability in bolstering maritime cybersecurity and projecting future trends in this critical domain.

1.2 Problem Statement

The maritime industry, a vital component of global trade and transportation, is increasingly reliant on digital technologies for operational efficiency and communication. However, this growing interconnectedness has exposed the maritime sector to a rising tide of cyber threats,

encompassing attacks on navigation systems, communication networks, and critical infrastructure [3]. These cyber risks pose a significant challenge to the safety, security, and economic stability of maritime operations, demanding innovative cybersecurity measures to safeguard against evolving threats [1].

As maritime cyber threats become more sophisticated and targeted, the need for advanced cybersecurity mechanisms is paramount. Traditional security approaches have proven inadequate in mitigating the dynamic and complex nature of cyber risks faced by the maritime industry [3]. Therefore, there is a pressing demand for a proactive and adaptive cybersecurity framework that leverages Artificial Intelligence (AI) mechanisms to detect, prevent, and respond to cyber threats in real-time [6].

1.3 Objective

Investigate the Application of AI in Maritime Cybersecurity: This study aims to delve into the practical applications of KNN, RF, and ANN mechanisms, exploring how these AI algorithms can be effectively integrated into the maritime cybersecurity framework.

Assess the Performance of KNN, RF, and ANN: The primary objective is to evaluate the efficacy of these AI algorithms in detecting and mitigating cyber threats in the maritime context. The study seeks to quantify their accuracy, precision, and recall to gauge their real-world applicability.

Explore Adaptability to the Dynamic Maritime Environment: Operating in a dynamic and complex environment, the maritime industry requires cybersecurity solutions that can adapt to the ever-changing nature of threats. This research aims to assess how well KNN, RF, and ANN mechanisms meet this need in the maritime cybersecurity landscape.

Provide Insights into Strengths and Limitations: By conducting a thorough analysis, the research endeavors to offer valuable insights into the unique strengths and limitations of each AI algorithm. This understanding is crucial for developing targeted and effective cybersecurity strategies in the maritime sector.

As the maritime industry navigates the uncharted waters of an increasingly digitalized landscape, this research contributes to the ongoing discourse surrounding cybersecurity. By exploring the potential of AI mechanisms, specifically KNN, RF, and ANN, the study aims to equip stakeholders with the knowledge needed to make informed decisions in securing maritime assets and operations against the ever-evolving cyber threat landscape.

1.4 Specific Innovations

Our research revealed that each of the aforementioned internet service providers has security flaws. For instance, these service providers do not do source screening. They don't verify if the supposed message-sending vessel is located in the same geographical area as the message-originating vessel.

The same holds for the lack of identification that would verify the identity of the vessel delivering the AIVDM punishment. As we will see below, the vulnerabilities that have been discovered make it possible for an attacker to launch spoofing and Man-in-the-Middle attacks on the impacted service providers. For spoofing, it is possible to create seemingly legitimate AIS data such as a ship or navigational aid from a location far from any sea or actual AIS station. First, we generated a harmless AIVDM phrase signaling low tide in a neighboring closed lake using our AIVDM Encoder [1] to confirm this danger.

As yet, no method has been developed to meet this difficulty. Finding and interpreting data about resources that are dynamically assigned is a significant challenge for digital forensics in cloud computing since resource allocation occurs in real-time. Data overwriting in shared

environments is another major issue with digital investigations on the cloud. It is particularly difficult to obtain dates previous to erased data since one user's file gets overwritten by data from another user [2].

Domain generation algorithms (DGAs) are used by several kinds of malware to set up C&C links. However, models with small datasets don't always pick up on novel DGA variations [14].

These above problems are solved to this my work, to achieve the problems are listed below.

1. Using some ML algorithms for using KNN, ANN, and RF.
2. Threat identification is an easy way.
3. A large no of datasets should be provided in this work.
4. Authentication is highly secure for all sending and receiving data.
5. Files are not overwritten; each data file is individually stored in a cloud area.

2. Related Works

The cyber landscape is evolving rapidly, with an increasing number of sophisticated threats targeting various sectors, including maritime systems, cloud computing, industrial Internet of Things (IIoT), and machine learning applications in cybersecurity. The challenges posed by these threats necessitate a comprehensive understanding of the existing vulnerabilities and the development of robust cybersecurity measures. The following problem statement encapsulates the key issues addressed in the related works:

The security evaluation of AIS (Automatic Identification System) highlighted in [1] work identifies vulnerabilities in maritime communication systems. However, the maritime industry continues to face challenges in implementing effective security measures to protect against evolving cyber threats. There is a need to address the identified vulnerabilities and enhance the cybersecurity framework for maritime systems.

The survey delves into the intersection of cloud computing and forensics, shedding light on potential security implications. As organizations increasingly rely on cloud services, understanding and mitigating the associated cybersecurity risks become critical. The problem lies in developing adaptive security protocols that align with the dynamic nature of cloud environments [2].

Interim guidelines provide a foundational framework for maritime cyber risk management. However, the evolving nature of cyber threats necessitates continuous refinement of these guidelines. The problem is to ensure that the guidelines are adaptive and capable of addressing emerging cyber risks in the maritime sector [3].

The survey on data mining and machine learning methods for cybersecurity intrusion detection underscores the potential of advanced technologies. However, the challenge lies in effectively integrating these methods into cybersecurity systems to enhance real-time threat detection and response capabilities [4].

An adaptive ensemble intrusion detection system showcases the efficacy of machine learning techniques. However, the problem persists in developing adaptive systems that can dynamically adjust to evolving cyber threats and maintain high detection accuracy [5].

Review [6] emphasizes the role of artificial intelligence in enhancing cybersecurity. Despite the promising applications, challenges such as explainability and adaptability of AI algorithms in real-world scenarios need to be addressed.

The review focuses on the cybersecurity challenges in the Industrial Internet of Things (IIoT). The problem lies in developing security measures that can safeguard interconnected industrial systems against both traditional and novel cyber threats [7].

The comprehensive review of maritime cybersecurity highlights the specific challenges faced by the maritime industry. The problem involves developing tailored cybersecurity solutions that consider the unique characteristics and vulnerabilities of maritime systems [8].

The exploration of machine learning techniques applied to cybersecurity identifies the potential of these techniques. However, the problem is in optimizing and customizing these techniques for specific cybersecurity use cases to ensure effective threat detection and mitigation [9].

The work on dynamic evolving neural networks for phishing email detection addresses a specific threat. However, the challenge is in scaling these solutions to handle the vast and evolving landscape of phishing attacks [10].

The application of a novel neural network in phishing detection showcases innovation. However, the problem is in integrating such innovative approaches into existing cybersecurity frameworks to enhance overall threat detection capabilities [11].

The work on detecting algorithmically generated domains using semantic analysis focuses on a specific type of cyber threat. However, the problem is in developing scalable solutions that can identify diverse types of algorithmically generated domains [12].

The exploration of DeepLocker highlights the potential threat of AI-powered malware. The problem involves developing countermeasures that can effectively detect and mitigate the risks associated with stealthy AI-powered malware [13].

DeepDGA presents challenges in the context of adversarially tuned domain generation and detection. The problem is in developing adaptive detection mechanisms that can stay ahead of adversaries tuning domain generation techniques [14].

The work on artificial intelligence and machine learning in cybersecurity provides an overview of the landscape. However, the problem involves effectively integrating AI and ML into existing cybersecurity frameworks to strengthen overall security postures [15].

The simulation of watchdog placement addresses anomaly detection in Bluetooth mesh intrusion detection systems. The challenge is in applying such simulations to real-world scenarios and ensuring the scalability of anomaly detection mechanisms [16].

The work on helicopter maritime search area planning identifies challenges in optimizing search and rescue operations. The problem involves developing efficient planning algorithms that consider real-time data and adapt to dynamic search scenarios [17].

They conducted a systematic survey of recent advances and future trends in cybersecurity within the maritime industry. They highlighted the importance of understanding emerging cyber threats and implementing robust security measures to protect critical maritime infrastructure and ensure uninterrupted operations [18].

To explore the utilization of AI and ML in cybersecurity for sustainable development, emphasizing the role of advanced technologies in improving threat detection and mitigation capabilities to safeguard critical infrastructure and promote economic growth [19].

They conducted a survey on AI-based cybersecurity in the context of Industry 4.0, highlighting the potential of AI-driven solutions to bolster defense mechanisms against cyber threats in industrial settings [20].

The proposed formulating cybersecurity requirements for autonomous ships using the SQUARE methodology focuses on developing comprehensive security protocols to safeguard against potential cyber-attacks [21].

3. Methods and Techniques

3.1 Maritime Automation Systems

The sea is now much safer than it used to be because of the many sophisticated automated technologies that modern, autonomous ships are outfitted with. However, since they are seen as less essential to security and performance, several of these systems are often unsafe and open to attack. The systems depicted in **Fig. 1** comprise radio detection and ranging (radar), communications, Devices for Automatic Identification (DAI), navigation, and control systems for various electromechanical systems on board ships, including the main engine, generators, converter drives, and so forth. **Fig. 3** illustrates the Global Positioning System (GPS), the International Satellite Navigation System (ISNS), and the Projection and Reporting of Digital Charts (PRDC) are examples of navigation systems. Globally, GPS and ISNS are essential enablers for contemporary, autonomous seafaring.

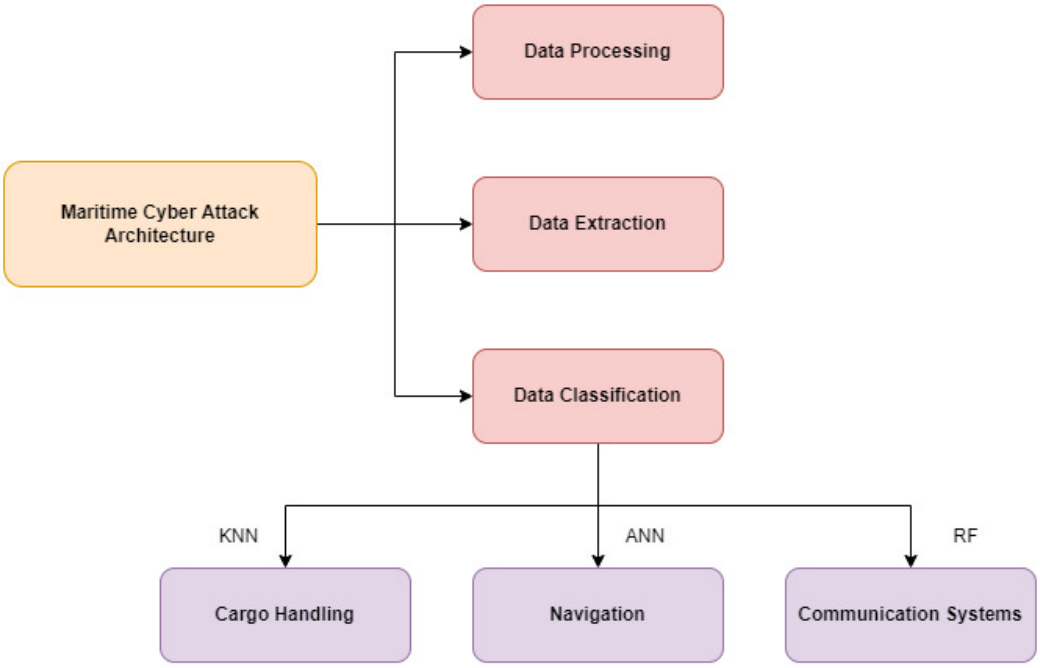

Fig. 2. Proposed Architecture

When making decisions, satellite positioning may be used in combination with other situational awareness systems that provide relative location data. Operating on both ships and coasts, the Devices for Automatic Identification is a radio broadcasting system shown in **Fig. 2**. It is used to alert port and maritime authorities to the position of the ship as well as to monitor and help with vessel traffic. Weather forecasting, search and rescue missions, and accident investigations may all benefit greatly from it as well]. In actuality, maintaining situational awareness and preventing maritime accidents depends heavily on the capacity to rely on sent data. An integrated electronic navigation system, or PRDC, shows data as a visual picture by combining information from many electronic navigation sensors, including GPS, radar, and AI. All commercial boats are required by the Organization of the European Maritime Union (EMU) to carry a PRDC, which is normally mounted on the bridge. For contemporary ships, radio detection and ranging, or radar, is especially essential since it not

only uses radio waves such as microwaves in the electromagnetic spectrum to detect physical things, but it also gives useful information about the ship's surroundings.

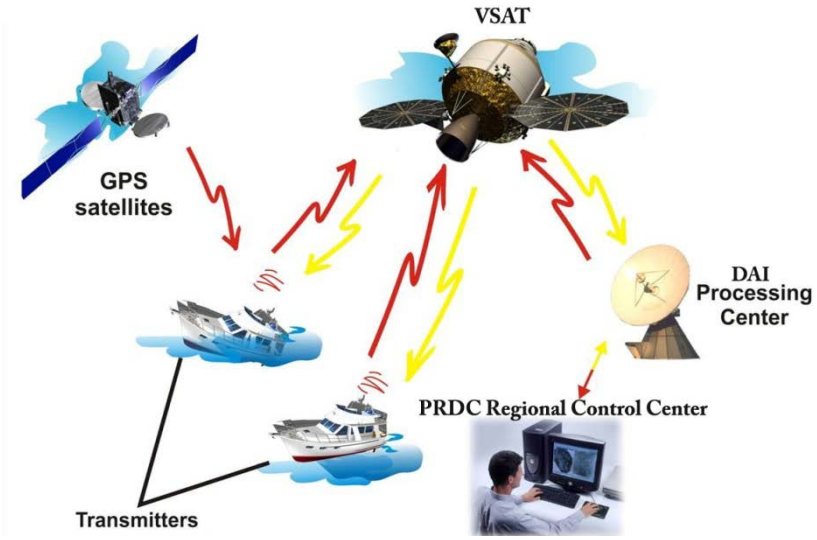

Fig. 3. Maritime Cyber-attack Architecture

The majority of contemporary ships and vessels are outfitted with the Maritime Very Small Aperture Terminal (VSAT), which serves as a ground station for the satellite to broadcast and receive data from the antenna to guarantee high-speed data transfer rates during naval operations. The control unit, which acts as the computer's interface, is situated below the deck and is positioned above the transceiver to line with the satellite view. In addition to PRDC, AI, phone, Internet, cargo management, wireless integration, crew welfare, and weather forecasting, VSAT provides a wide range of communication and security capabilities. The need for automated intelligent video surveillance systems to monitor transport operations is also growing in the contemporary maritime sector. These systems are particularly needed to keep an eye on big storage spaces, generators, and huge boats transporting precious goods.

The maritime industry is currently undergoing a profound transformation with the integration of advanced automation systems, marking a significant departure from traditional approaches to vessel operations. This paradigm shift is propelled by the industry's collective commitment to enhancing efficiency, safety, and sustainability. Maritime automation systems, spanning from fundamental control mechanisms to cutting-edge autonomous capabilities, herald a new era of innovation and efficiency. Automated navigation systems, a cornerstone of this evolution, play a pivotal role in enhancing the precision and reliability of vessel movements. The integration of GPS, radar, and sensor data optimizes navigation routes, mitigates collision risks, and ensures strict compliance with international maritime regulations. Concurrently, smart monitoring and diagnostic systems have revolutionized maintenance practices. Leveraging sensor networks and advanced analytics, these systems enable real-time condition-based maintenance, predicting potential failures and optimizing maintenance schedules to minimize downtime and operational costs. The exploration of unmanned and autonomous vessels represents a frontier in maritime automation. By leveraging artificial intelligence, machine learning, and advanced sensor arrays, these vessels navigate and make decisions autonomously, addressing challenges posed by a shortage of skilled seafarers and enhancing safety by minimizing human error. Extending beyond vessel operations, the integration of automation in cargo handling systems streamlines logistical processes.

Automated container handling, crane operations, and inventory management contribute to heightened port efficiency and expedited vessel turnaround times. However, as the maritime industry embraces these transformative technologies, the critical need for robust cybersecurity measures is emphasized. Safeguarding against potential threats exploiting vulnerabilities in automated maritime systems becomes paramount in ensuring the integrity and security of these advanced systems. In conclusion, the integration of maritime automation systems signifies a groundbreaking shift, propelling the industry into a future characterized by innovation and operational efficiency. As these technologies continue to evolve, a comprehensive approach addressing technical, regulatory, ethical, and cybersecurity considerations will be crucial for unlocking their full potential.

3.2 Incidents of cyber-attacks targeting ship control systems

Ship automation systems' cybersecurity vulnerabilities have an opportunity to result in catastrophic effects, such as unauthorized vessel control, disturbances in navigation, or even bodily harm. Below are many important factors in cyberattacks on ship automation systems.

3.2.1 Maersk's Experience of the NotPetya Attack in 2017

The previously stated NotPetya ransomware assault had an around-the-world impact on Maersk's operations, namely targeting its automation and communication systems. Although its main focus was on IT systems, the event brought attention to the possible consequences for operational technology (OT) systems, which include ship automation and associated functions.

3.2.2 Risk Guidelines

The International Maritime Organization (IMO) acknowledges the growing cybersecurity menace to the maritime sector and has created recommendations to tackle cyber vulnerabilities. The International Maritime Organization's "Guidelines on Maritime Cyber Risk Management" provide suggestions for protecting the maritime industry against cyber-attacks, including those that aim at automation systems.

3.2.3 Raising Awareness and Implementing Regulations

The marine sector has developed a heightened awareness of the need for strong cybersecurity protocols. Authorities and regulatory agencies are striving to enforce and revise legislation to bolster the cybersecurity stance of ships. Adhering to these standards aids in mitigating the vulnerability to cyberattacks.

3.2.4 Cooperation and Exchange of Information

Maritime industry participants, such as shipowners, operators, and cybersecurity specialists, are progressively working together to exchange information and adopt optimal strategies for cybersecurity. Disseminating information on the most recent threats and vulnerabilities helps the whole sector maintain readiness and resilience. Due to the dynamic nature of cybersecurity threats, it is crucial to be informed of the most recent advancements. Monitor industry publications, warnings from pertinent maritime organizations, and cybersecurity news to get insight into cyber risks to ship automation systems.

3.3 Device for Automatic Identification

Fig. 3, shows devices for Automatic Identification (DAI) play a crucial role in maritime communication and navigation. These devices are designed to automatically and autonomously exchange information between ships and shore stations, enhancing situational awareness and promoting maritime safety. DAI devices typically operate in the VHF maritime band and transmit essential information, such as vessel identification, position, course, and speed. By continuously broadcasting this data, DAI helps prevent collisions, improve navigation efficiency, and facilitate search and rescue operations.

Ships are equipped with DAI transponders that regularly broadcast information, allowing nearby vessels and shore-based stations to receive and process the data. The information transmitted by DAI devices can be displayed on electronic chart displays, radar screens, and other navigation systems, enabling mariners to identify nearby vessels and make informed decisions to avoid potential hazards.

Additionally, DAI technology aids in maritime traffic management, port operations, and maritime domain awareness. It has become a standard tool for monitoring vessel movements, ensuring compliance with navigational regulations, and responding effectively to emergencies. While DAI enhances safety and efficiency, it's crucial to address potential cybersecurity concerns to prevent unauthorized access or tampering with the information exchanged by these devices. As technology continues to evolve, the maritime industry will likely see advancements in DAI capabilities and increased integration with other navigation and communication systems.

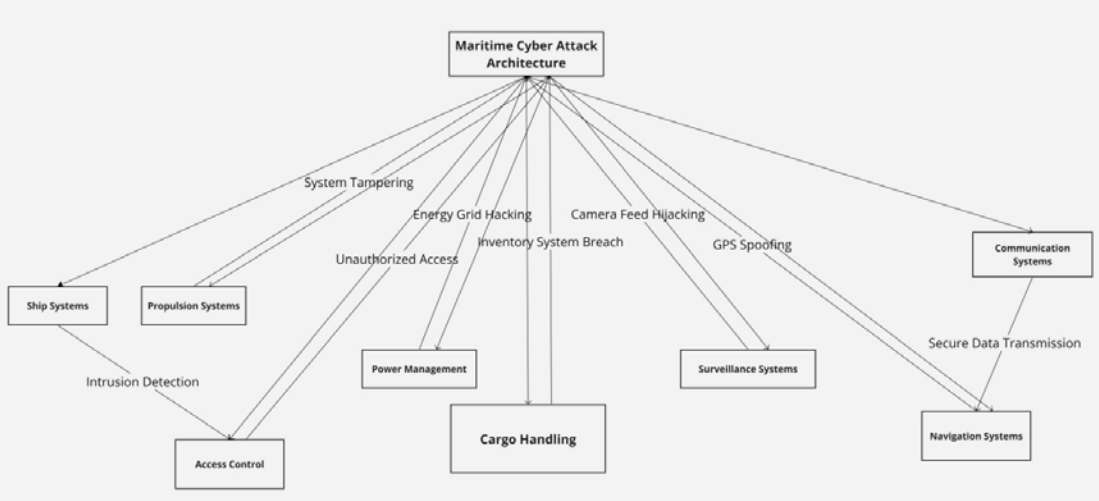

Fig. 4. Maritime Cyber Attack Automatic Identification Architecture

3.4 International Satellite Navigation System

The International Satellite Navigation System provides worldwide positioning, navigation, and timing information to users. One of the most well-known examples of such a system is the Global Positioning System (GPS). GPS, owned and operated by the United States government, is a constellation of satellites that enables users with compatible receivers to determine their precise location, velocity, and time.

In addition, **Fig. 4** shows that, in GPS, there are other global or regional satellite navigation systems developed by various countries or international organizations. The Russian GLONASS, the European Union's Galileo, and China's BeiDou Navigation Satellite System are notable examples. These systems work by using a network of satellites in orbit around the Earth to transmit signals that can be received by ground-based receivers. By triangulating signals from multiple satellites, these receivers can calculate the user's exact position and provide accurate navigation information.

The collaboration and interoperability of different satellite navigation systems have become increasingly important, with efforts to ensure global coverage and enhance the overall accuracy and reliability of positioning data. International partnerships and agreements encourage the compatibility of different ISNS systems, allowing users to benefit from signals transmitted by multiple constellations simultaneously. This not only improves the availability of satellite signals in challenging environments but also enhances the resilience and robustness of satellite navigation services on a global scale. As technology continues to advance, the collaboration among nations in the realm of satellite navigation systems will likely play a pivotal role in shaping the future of global navigation and positioning capabilities.

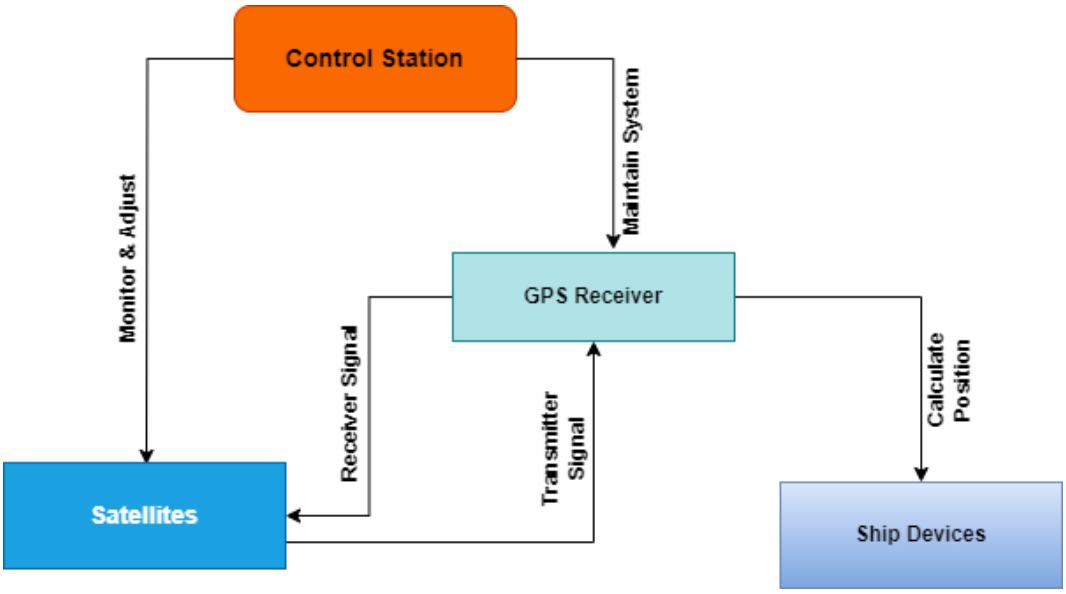

Fig. 5. Maritime GPS System

3.5 Projection and Reporting of Digital Charts

The projection and reporting of digital charts represent integral components of modern navigation systems, providing mariners with essential tools for safe and efficient seafaring. Digital charts, electronic representations of traditional paper charts, utilize various map projections to depict the Earth's surface accurately. These projections convert the three-dimensional surface of the Earth into a two-dimensional representation, allowing for efficient navigation. Common projections include the Mercator projection, which preserves angles and is often used for navigation, and the Winkel Tripel projection, which balances size and shape distortion in **Fig. 5** to **Fig. 7**.

The reporting of digital charts involves the communication and visualization of vital navigational information. Advanced navigation systems use digital chart plotters to display

real-time data, including vessel position, course, speed, and environmental conditions. Mariners can customize these digital displays to overlay additional information, such as AIS data, radar images, and weather forecasts. This integrated approach enhances situational awareness, aiding in collision avoidance and efficient route planning.

Moreover, the advent of technologies like the Electronic Chart Display and Information System (ECDIS) has transformed chart reporting. ECDIS not only allows for the real-time projection of digital charts but also automates the process of route planning and monitoring. Mariners can receive timely warnings about potential navigational hazards and deviations from planned routes. Furthermore, these systems enable the logging and reporting of navigational data, facilitating compliance with maritime regulations and enhancing post-voyage analysis.

In summary, the projection and reporting of digital charts in modern navigation systems exemplify the seamless integration of technology to improve maritime safety and efficiency. By employing accurate projections and real-time reporting tools, mariners can navigate with precision, respond to dynamic conditions, and comply with regulatory requirements in an increasingly interconnected and technologically advanced maritime environment.

DDoS attacks typically involve overwhelming a target system or network with a flood of traffic, rendering it inaccessible to legitimate users. While DDoS attacks have been prevalent in various industries, including finance, e-commerce, and online services, the maritime industry has also been working to strengthen its cybersecurity posture to mitigate such threats.

In the context of maritime systems, including radar and other navigation technologies, potential cyber threats are a growing concern. The International Maritime Organization (IMO) has recognized the importance of cybersecurity in the maritime sector and has developed guidelines to address cyber risks. These guidelines include recommendations for implementing cybersecurity measures to safeguard critical systems on ships, including navigation and communication systems.

It's crucial for the maritime industry to stay vigilant against evolving cyber threats, including DDoS attacks, and to implement robust cybersecurity measures to protect critical systems. Regular cybersecurity assessments, employee training, and the adoption of best practices outlined by relevant maritime authorities are essential to mitigate the risks associated with cyber threats. Additionally, ongoing collaboration among industry stakeholders, government agencies, and cybersecurity experts is vital to staying ahead of emerging threats and ensuring the resilience of maritime systems.

3.6 Cybersecurity Considerations Video Surveillance Systems for Maritime

Cybersecurity considerations are paramount in the implementation of video surveillance systems for maritime monitoring. As these systems become integral to enhancing maritime security and situational awareness, safeguarding them against cyber threats is crucial. The interconnected nature of modern surveillance systems, often involving cameras, networks, and data storage, poses potential vulnerabilities that malicious actors could exploit. Maritime entities must employ robust cybersecurity measures to prevent unauthorized access, data tampering, or disruption of video feeds. This includes implementing encryption protocols for data transmission, securing network infrastructure, and regularly updating firmware and software to patch known vulnerabilities. Additionally, the use of strong authentication mechanisms and access controls ensures that only authorized personnel can manipulate or view sensitive video footage. Ongoing cybersecurity training for maritime personnel is essential to raise awareness about potential threats and promote a culture of vigilance. As technology evolves, incorporating cybersecurity best practices into the design, deployment,

and maintenance of video surveillance systems will be vital to maintaining the integrity and reliability of these crucial components in maritime security frameworks.

4. Results and Discussions

Before analyzing the physical and digital outcomes, it is worthwhile to go more into the human aspect of this situation. According to a ship engineer, the engineering staff can circumvent any compromised systems and directly attach a physical wheel to the steering gear as a manual override. Nevertheless, it was also stated that the detection of drift would probably need a minimum of ten minutes or more. Unfortunately, in this particular scenario, that duration has been sufficient to result in harmful consequences. However, only a limited number of experts have primarily hypothesized this. Now that this case study can be replicated as a training scenario on a portable CR, it can be implemented in other training sites. Subsequent research will focus on subjecting multiple crews to this scenario and collecting data on their responses to establish statistical patterns. This proposed expansion aims to identify and rectify deficiencies in training, hence enhancing the overall effectiveness of the job, as outlined. Despite the limited validation testing conducted in this study to ensure realism, there were instances of simulated scenarios where, even if a skilled crew was aware of the attack, it was challenging to prevent damage due to the specific position and inertia of shipC and the layout of portV.

4.1 Physical Results

There is a particular scenario variation when the ship obstructed all of portV's container terminal, resulting in the greatest substantial disruption to port operations. During simulations, ShipC and her cargo often suffered physical harm. In the unlikely event that this situation came to pass, cleaning the surrounding area would be required to get back to the best possible operating efficiency. It is important to note that it was very unlikely to do enough damage in the simulated scenarios to sink shipC or ignite a significant fire on board. However, some containers could come loose and fall off, and our discussion with the port has given our throughput model details on how long it will take for normal operations to resume due to the shipC and/or the recovery of floating cargo.

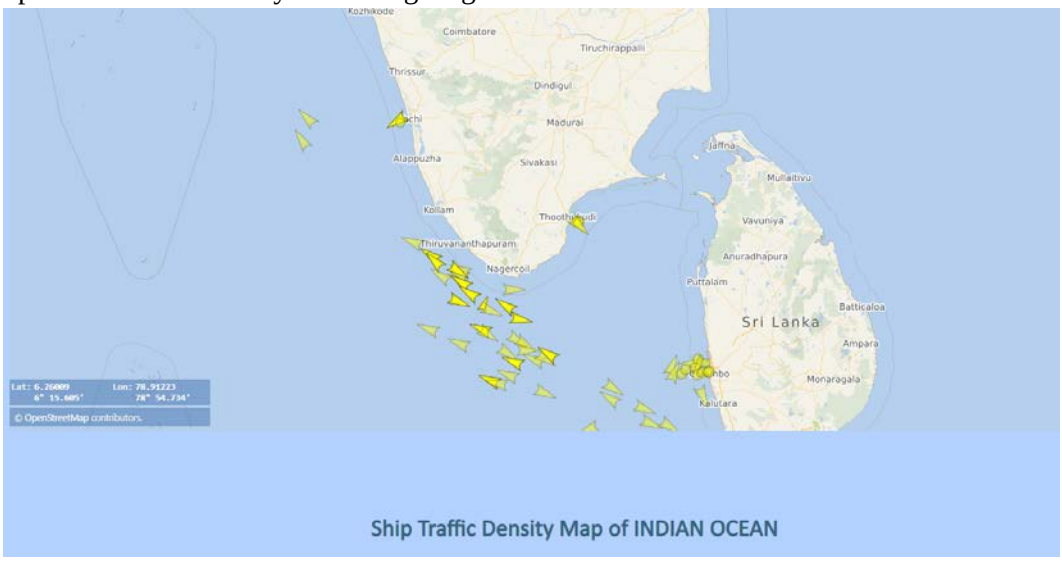

Fig. 6. Simulink for Maritime Traveling

To further understand the overall physical effects on the transportation supply chain, the authors include case study downtime and portV data into a model. The model employs discrete event simulation techniques to assess port container operations; the details of which are beyond the scope of this study. Instead of discussing the mathematical aspects, this study primarily focuses on using this method to calculate downtimes. As a preliminary note, these models use the sim events and Simulink applications on the MATLAB platform shown in **Fig. 8** to **Fig. 15**. As a result, port delays have a greater level of accuracy in determining outcomes, and the ship simulator's ability to adjust to the conditions in the port throughput simulation is more advantageous. To comprehend the duration required for the retrieval of floating or submerged containers, one must possess an understanding of port repair and recovery protocols, as well as the necessary equipment for their execution. However, this scenario does not include that level of detail; instead, it uses an average timeframe for repair or recovery.

Fig. 7. Simulink for Maritime Traveling Details

POSITION & VOYAGE DATA

Port Walcott, Australia
ATA: Feb 7, 01:57 UTC ARRIVED

Predicted ETA	-
Distance / Time	-
Course / Speed	233.8° / 0.0 kn
Current draught	5.7 m
Navigation Status	Under way
Position received	0 min ago
IMO / MMSI	9635901 / 503726000
Callsign	VJN3837
Flag	Australia
Length / Beam	32 / 13 m

Port Walcott, Australia
ATD: Feb 7, 01:04 UTC (5 hours ago)

Fig. 8. Data for Position and Voyage

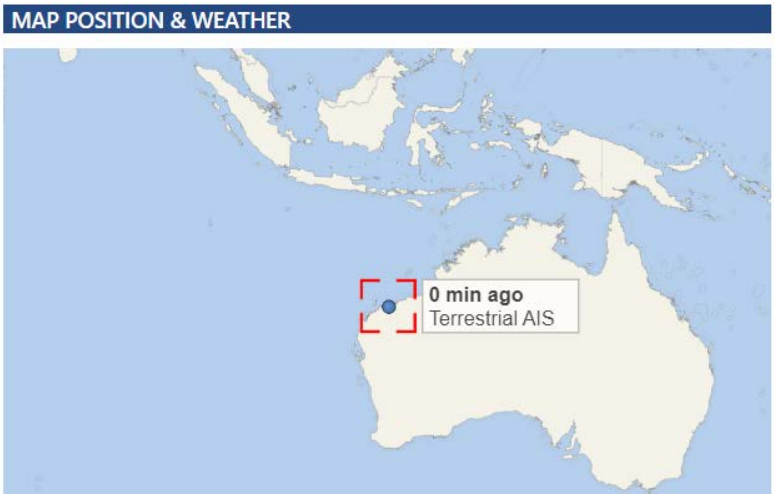

Fig. 9. Ship Position and Weather

The modeling of port throughput using a queue-based system models many port activities, including the movement of goods, transportation within the port, and operations at the container yard. The key factors that influence the modeling process are as follows: 1) The total quantity of vessels handled by the port of Valencia in 2020; 2) The average duration of servicing a vessel; 3) The proportion of land-based transportation that relies on trucks or railways; and 4) The average amount of time containers spend at the yard.

The model predicts that the arrival times of vessels will conform to a Poisson distribution, but the distributions of service times will conform to an Erlang distribution. These model projections align with the normal traffic and service distributions seen at ports, as well as the distributions recommended by PRDC for port development. While the details of the simulation are not discussed in this study, its outcomes are crucial for understanding the implications of the situation.

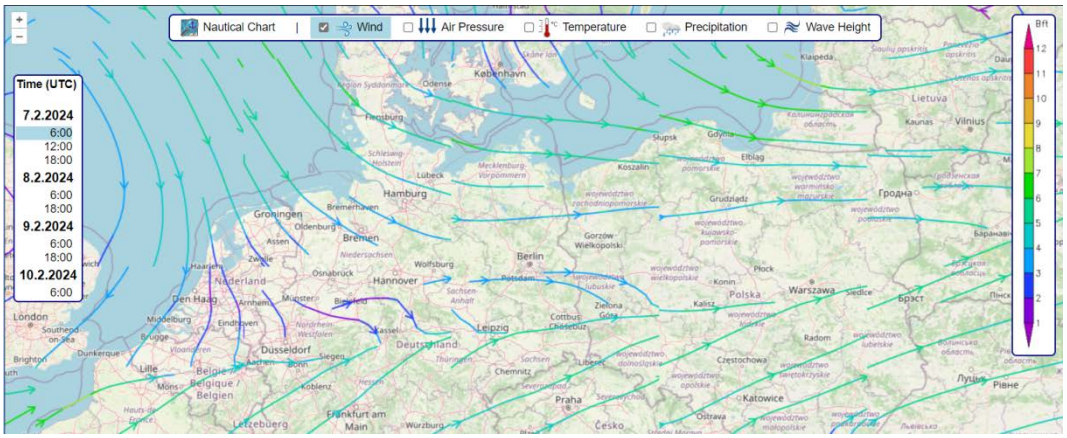

Fig. 10. Whether Reports for all climates

Fig. 11. Whether Reports for Pressure

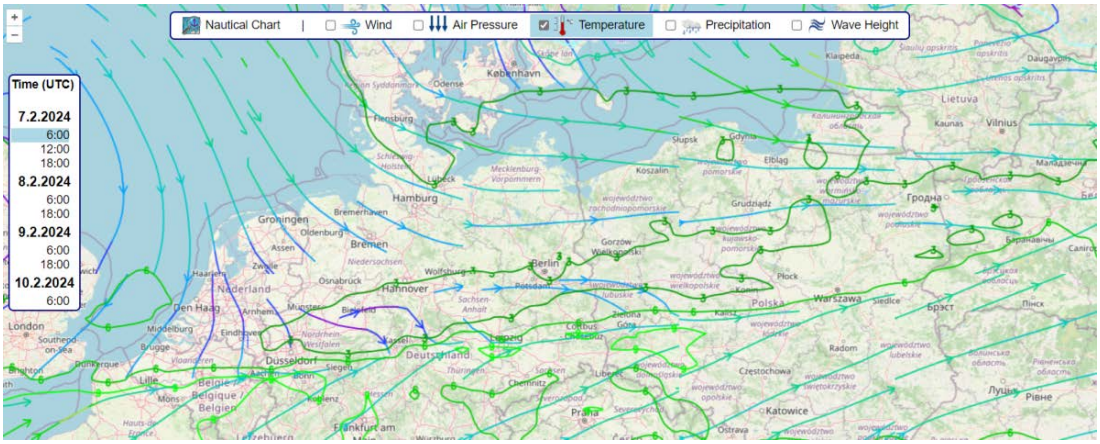

Fig. 12. Whether Reports for Temperature

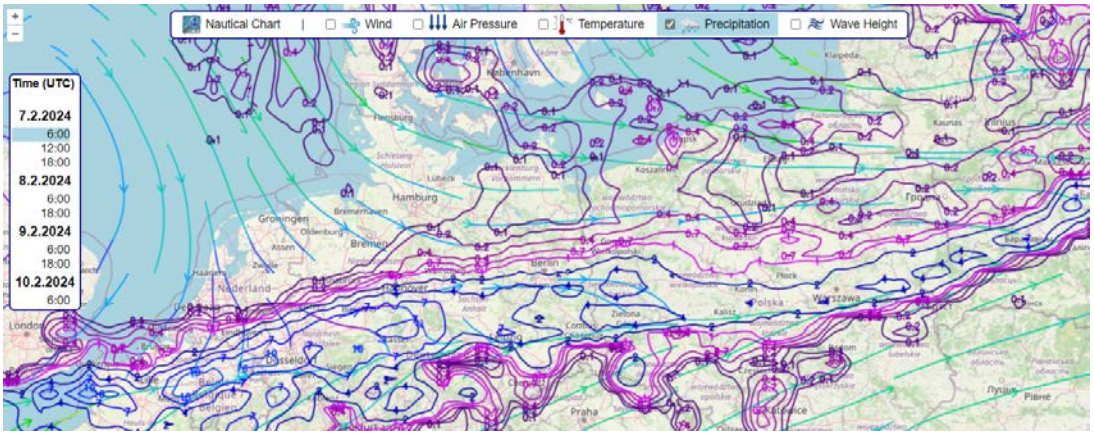

Fig. 13. Whether Reports for Perception

Fig. 14. Whether Reports for Wave Speed

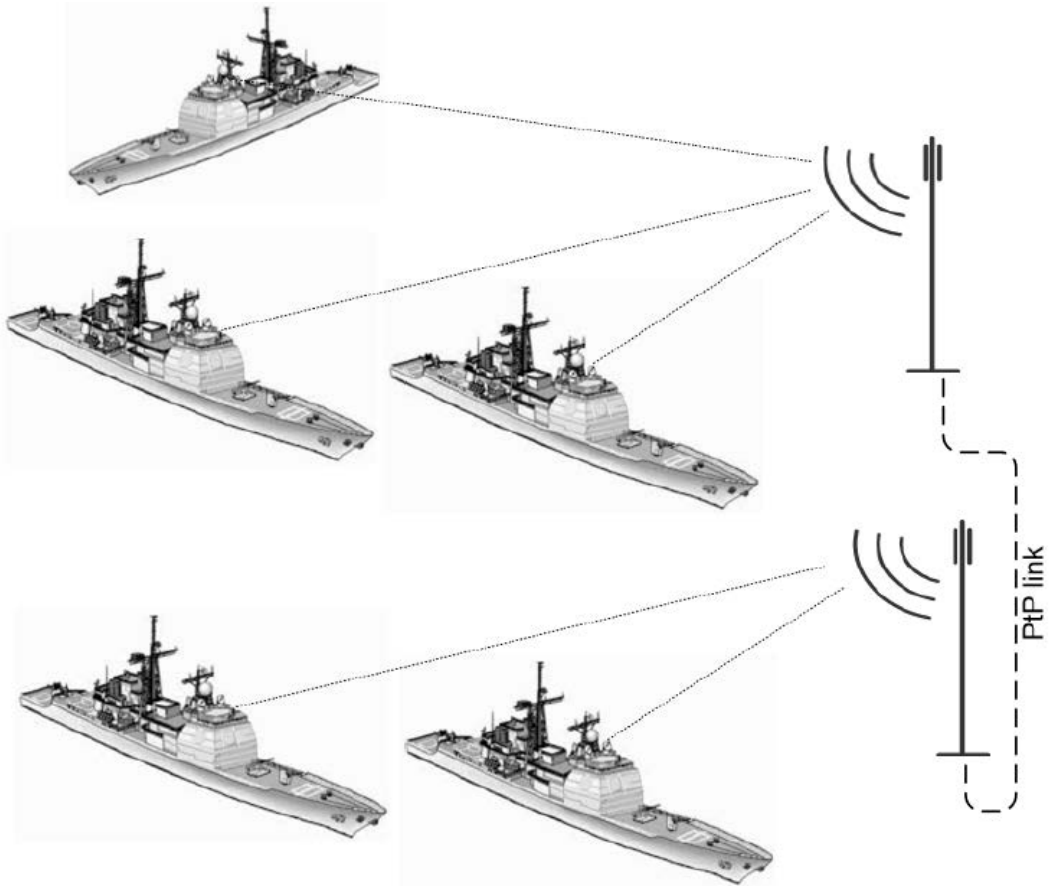

Fig. 15. Data Transmission to satellite link

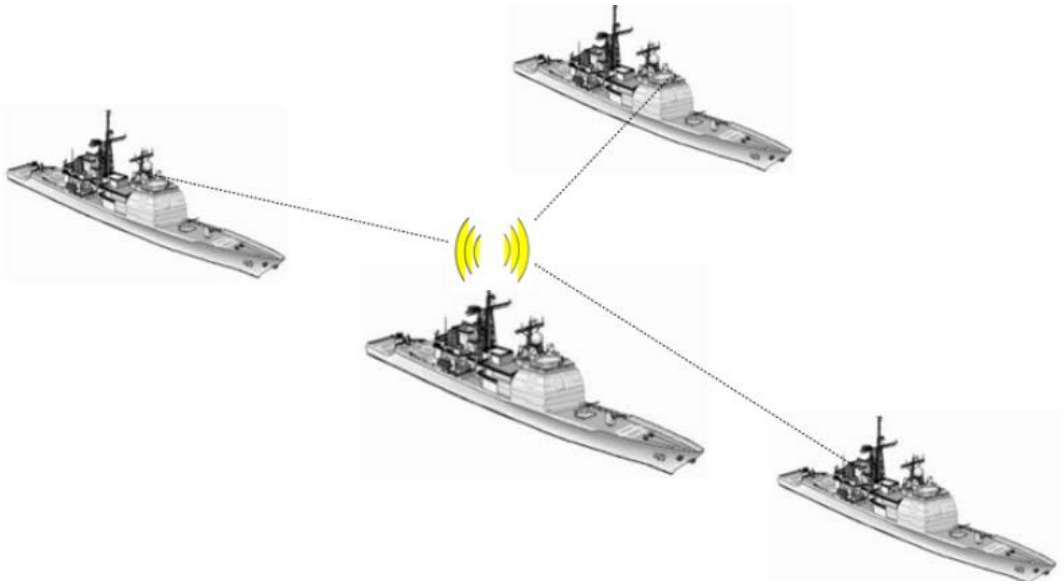

Fig. 16. Data Transmission from one to other ships

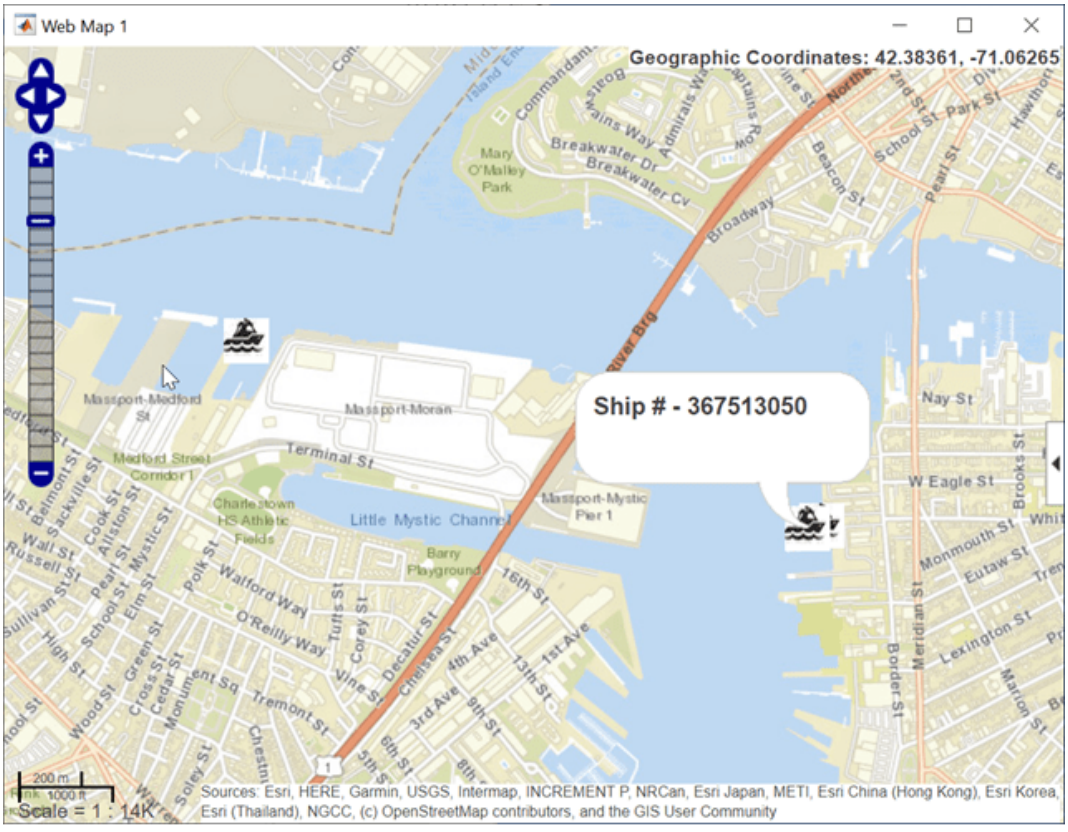

Fig. 17. Ship Tracker

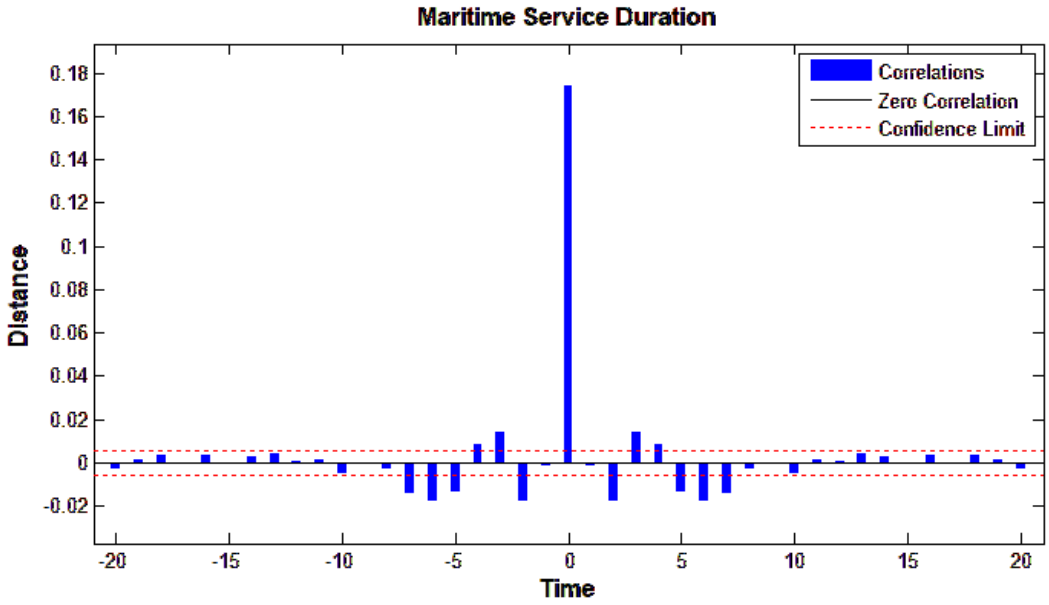

Fig. 18. Duration of Threat Services

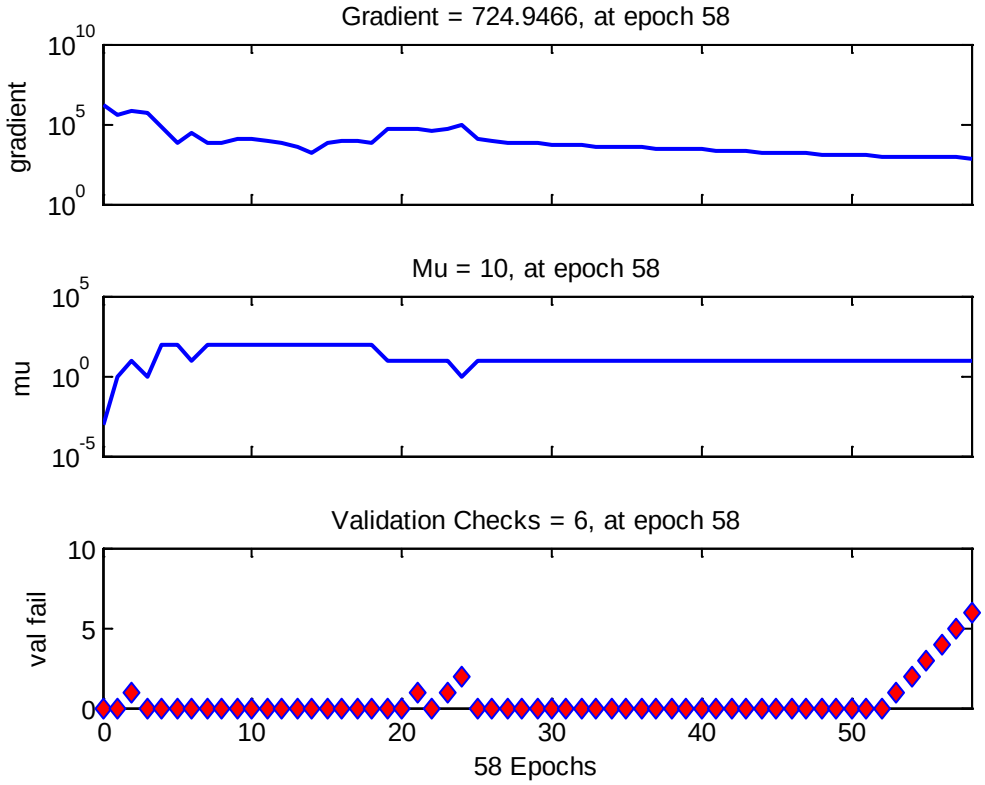

Fig. 19. Waiting Vessels in Time

The service and waiting hours for boats in the case of a six-day complete blockage interruption at the port are shown in **Fig. 3** and **Fig. 4**. This is within the upper limit of possible interruption as described in the study scenario. Each unit on the graphs represents fifteen minutes. The service length graph shows how much shipping would be disrupted if port operations were to completely stop. The time needed to service the vessels that were the most severely affected would increase from one day on average to eight days at most. Six of those days would be spent waiting for port operations to start, which would cause traffic jams and delays.

More than 35 vessels would be on the waiting list when it was at its peak. The simulated data suggests that the disruption occurs when the port is typically seeing an average amount of traffic. When this occurs during peak port hours, the level of disruption might be more than what is shown in **Fig. 6** and **Fig. 7**. From a physical safety perspective, shipC's hull was damaged in many case study variants, and in certain cases, cargo may have slipped or fallen off in the most severe versions. Everyone on board, including the crew, is in peril, but if there are tugs, the onshore residents may be put in harm's way. There are currently few concerns about the safety of shipC colliding with other ships, cargo, cruise ships, or any other object as of the date of the simulation. Can we predict if portV will be more or less busy on a given day, and how that will affect throughput and other aspects of ship safety?

4.2 Digital Results

Maritime cybersecurity is a critical aspect of ensuring the safety, integrity, and resilience of maritime systems against cyber threats. The application of Artificial Intelligence (AI) mechanisms, including K-Nearest Neighbors (KNN), Random Forest (RF), and Artificial Neural Networks (ANN), plays a significant role in enhancing the capabilities of cybersecurity solutions in the maritime domain.

4.2.1 K-Nearest Neighbors (KNN)

Fig. 20 shows that KNN is a supervised machine-learning algorithm commonly used for classification and regression tasks. In the context of maritime cybersecurity, KNN can be applied for anomaly detection and classification of network activities. KNN works by classifying data points based on the majority class of their k-nearest neighbors. In cybersecurity, it can analyze network traffic patterns, identifying deviations from normal behavior that may indicate a cyber threat. KNN's adaptability makes it suitable for dynamic maritime environments where normal patterns may evolve.

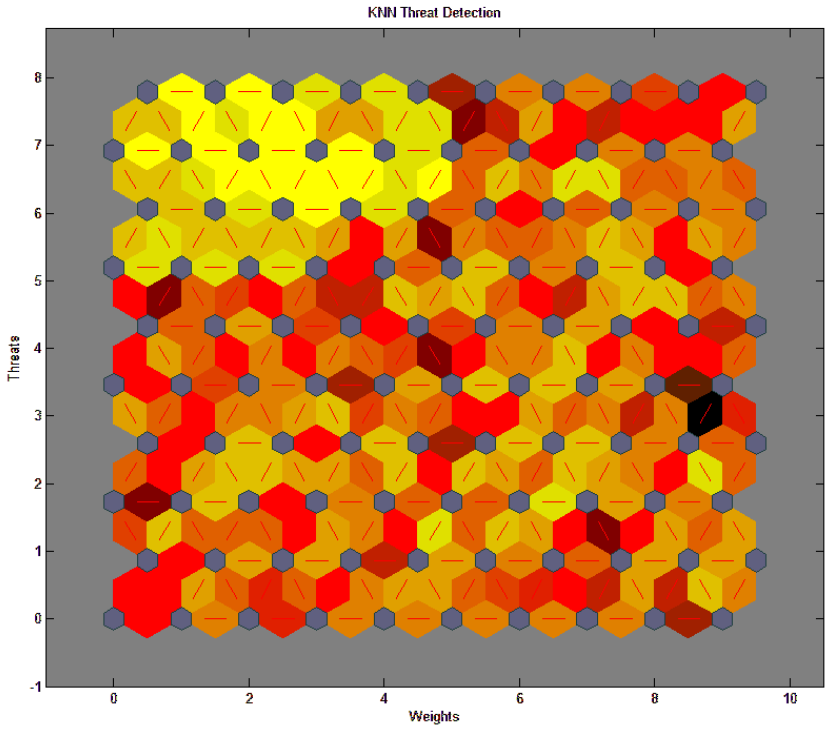

Fig. 20. KNN Threat Detection

The K-Nearest Neighbors (KNN) algorithm is a simple, non-parametric method used for classification and regression. Below is a high-level pseudocode for implementing the KNN algorithm for a classification problem described in **Table 1**.

Table 1. K-Nearest Neighbors Pseudocode

```
Define KNN_Classify(X_train, Y_train, X_test, k, distance_metric):
   For each point in X_test:
       {
      If (Calculate the distance from this point to all points in X_train using
the specified distance_metric)
         {
       Sort the distances in increasing order.
       Take the first k elements from the sorted list of distances
       Get the labels of these k elements
       Determine the most frequent label among these k labels
       Assign the label to the test point
        }
       }
   Return the list of predicted labels for each point in X_test.
```

Certainly! The K-Nearest Neighbors (KNN) algorithm is a simple, non-parametric method used for classification and regression. Below is a high-level pseudocode for implementing the KNN algorithm for a classification problem:

1. **Input:** Your inputs are the training data X_train with labels Y_train, the test data X_test for which you want to predict the labels, the number k representing the number of nearest neighbors to consider, and the distance_metric which could be Euclidean,

Manhattan, etc.

2. **Distance Calculation:** For each example in your test data (X_test), compute the distance to every example in your training data (X_train). This is typically done in a loop that goes through each instance of the test data.
3. **Sorting Distances:** Sort these distances in ascending order, so the nearest neighbors are first.
4. **Selecting Neighbors:** Select the top k examples from the sorted list. These are the k nearest neighbors.
5. **Voting:** Look at the labels Y_train of these k neighbors and count the occurrences of each class.
6. **Assign Label:** The class that appears the most among the k neighbors is the prediction for the test example.
7. **Output:** After running through all the test examples, return the predictions.

KNN is lazy-learning and non-parametric, meaning it does not make any assumptions about the underlying data distribution and it doesn't learn a discriminative function from the training data but instead memorizes the training dataset.

4.2.2 Random Forest (RF)

Fig. 21 shows that RF is an ensemble learning algorithm that operates by constructing multiple decision trees during training and outputting the class that is the mode of the classes (classification) or mean prediction (regression) of the individual trees. In maritime cybersecurity, RF can be employed for intrusion detection and the analysis of complex datasets. It excels at handling large amounts of data and can identify patterns indicative of cyber threats. RF's ability to handle diverse data types and its resistance to overfitting make it a valuable tool for detecting anomalies and potential security breaches in maritime networks.

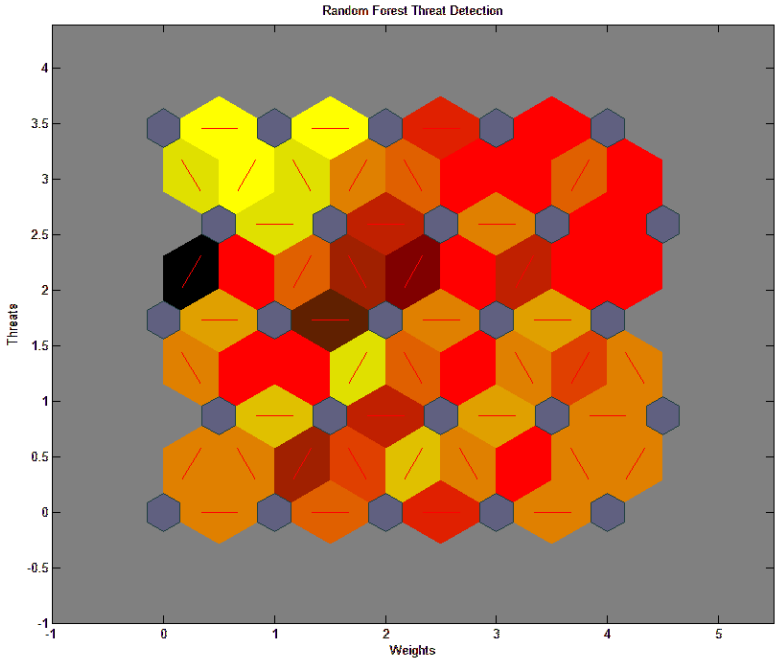

Fig. 21. RF Threat Detection

Random Forest is an ensemble learning method for classification, regression, and other tasks that operates by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes (classification) or mean prediction (regression) of the individual trees. Here is a simplified pseudocode for Random Forest, focusing on classification in described **Table 2**.

Table 2. Random Forest Pseudocode

```
Define Random_Forest_Train(Dataset, num_trees, max_features):
{
   Forest <- Empty list to hold decision trees
   For (i = 1 to num_trees);
        {
      Bootstrap_Sample <- Randomly select samples from Dataset with replacement
      Decision_Tree <- Train_Decision_Tree(Bootstrap_Sample, max_features)
      Add Decision_Tree to Forest
        }
   Return Forest
Define Random_Forest_Classify(Forest, Test_Instance):
{
   Predictions <- Empty list to hold predictions from all trees
   ForEach (Decision_Tree in Forest);
      {
      Prediction <- Classify(Test_Instance using Decision_Tree)
      Add Prediction to Predictions
       }
}
}
   Return Mode of Predictions (most frequent class)
```

1. Training (Random_Forest_Train)
   - Forest Initialization: Start with an empty list to hold all the decision trees.
   - Bootstrap Sampling: For each tree, create a bootstrap sample. This is a sample of the dataset selected randomly with replacement, meaning some instances may be repeated in the sample.
   - Train Decision Trees: Each decision tree is trained with the bootstrap sample and a random subset of features (max_features). This is to ensure that each tree learns from different patterns and the trees are decorrelated.
   - Forest Construction: Add the trained decision tree to the forest. Repeat this process until you have `num_trees` decision trees in your forest.
2. Classification (Random_Forest_Classify)
   - Collect Predictions: For a given test instance, make predictions using each decision tree in the forest.
   - Voting: Aggregate the predictions from all decision trees to find the mode, i.e., the most frequently predicted class. This is the final output of the random forest for the given test instance.
   - The power of the Random Forest algorithm comes from the diversity of the decision trees which is a result of both the bootstrap sampling and the feature subset selection for training individual trees. This diversity makes Random Forests very robust against overfitting and provides a more generalized model.

4.2.3 Artificial Neural Networks (ANN)

Fig. 22 shows that ANN is a computational model inspired by the structure and functioning of the human brain. It consists of interconnected nodes or neurons organized in layers and can learn complex patterns from data. In maritime cybersecurity, ANN can be used for tasks such as threat detection and risk assessment. It excels at processing large datasets and identifying non-linear relationships within the data. The deep learning variant of ANN, known as Deep Neural Networks (DNN), can further enhance detection capabilities by automatically learning hierarchical features from raw data.

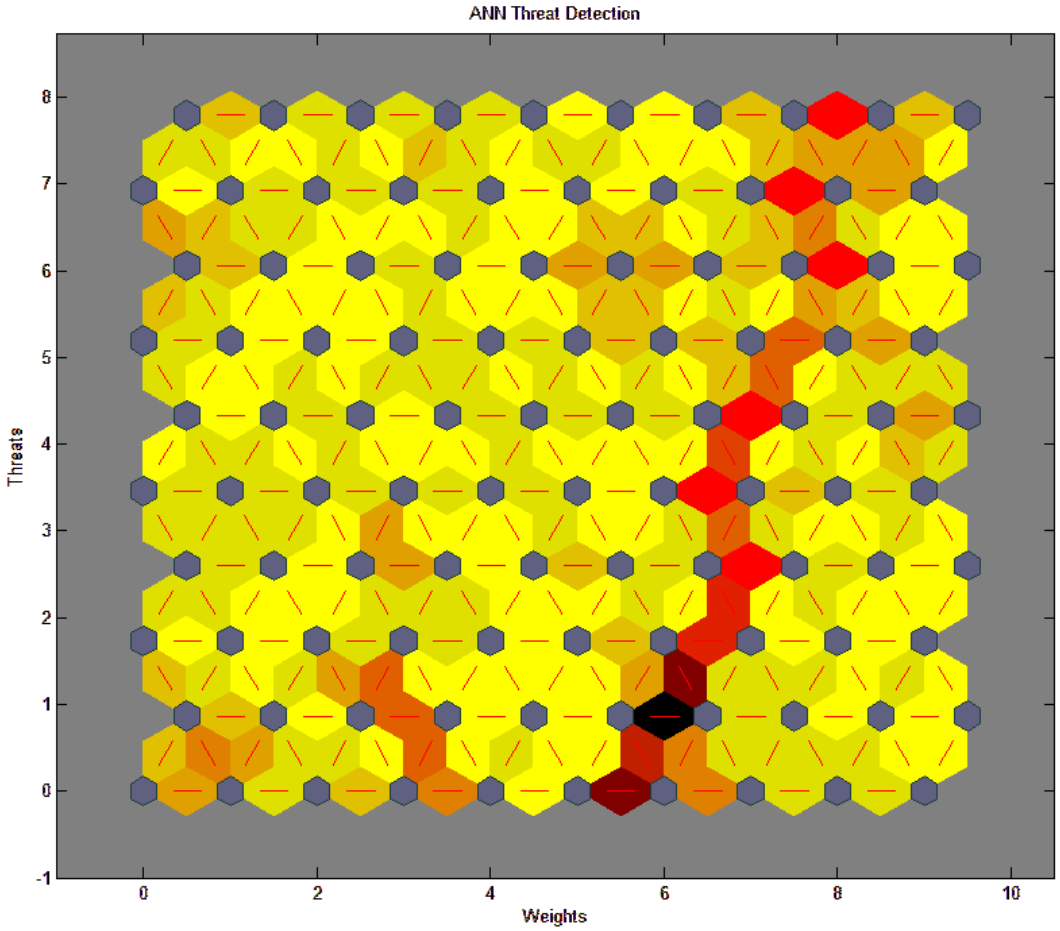

Fig. 22. ANN Threat Detection

Artificial Neural Networks (ANNs) are a fundamental component of machine learning that attempts to mimic the network of neurons in a human brain to interpret data patterns. Here's a basic outline of how an ANN might be structured in pseudocode, specifically focusing on a feedforward neural network for supervised learning in described **Table 3**.

Table 3. Artificial Neural Network Pseudocode

```
Define ANN_Train(Dataset, Architecture, Learning_Rate, Epochs):
{
   Initialize Network Weights randomly based on the Architecture
   ForEach (epoch in Epochs);
        {
      ForEach (Dataset);
           {
        Input <- example.features
        True_Output <- example.label
        Predicted_Output <- Forward_Propagate(Network, Input)
        Loss <- Calculate_Loss(Predicted_Output, True_Output)
        Gradients <- Backward_Propagate(Loss, Network)
        Update_Network_Weights(Network, Gradients, Learning_Rate)
           }
       }
}
return 0;
Define Forward_Propagate(Network, Input):
{
   ForEach (networklayers);
    {
     Input <- Activate(dot_product(Input, layer.weights) + layer.bias)
    }
   return;
Define Backward_Propagate(Loss, Network):
{
   Calculate gradients for each layer in the Network in reverse order
   Return Gradients
Define Update_Network_Weights(Network, Gradients, Learning_Rate):
{
   ForEach (networklayrs):
   {
      layer.weights <- layer.weights - Learning_Rate * Gradients. weights
      layer.bias <- layer.bias - Learning_Rate * Gradients.bias
   }
}
}
}
```

1. Training (ANN_Train)
   - Initialize the neural network with random weights.
   - Loop through the training dataset for several epochs.
   - In each epoch, perform forward propagation, loss calculation, backpropagation, and weight updates for each training example.
2. Forward Propagation (Forward_Propagate)
   - Process the input data through each layer of the network. At each layer, compute the dot product of the input and weights, add the bias, and apply an activation function.
3. Loss Calculation
   - After forward propagation, compare the network's prediction with the true output to calculate the loss (often using mean squared error for regression or cross-entropy for classification).

4. Backward Propagation (Backward_Propagate)
   - Calculate the gradients of the loss function concerning the network's weights. This process involves applying the chain rule to find the derivative of the loss concerning the weights at each layer, moving from the output layer back to the input layer.
5. Update Weights (Update_Network_Weights)
   - Adjust the weights and biases in the direction that most reduces the loss, scaled by the learning rate. This pseudocode is a very high-level representation. In practice, ANNs include more complexities such as different types of layers (convolutional, recurrent, etc.), regularization techniques, various activation functions (ReLU, sigmoid, etc.), and optimization algorithms (like Adam or SGD with momentum).

4.2.4 Integration of AI Mechanisms in Maritime Cybersecurity

The effectiveness of these AI mechanisms in maritime cybersecurity lies in their ability to analyze vast amounts of data, identify patterns, and detect anomalies indicative of cyber threats. Training these algorithms requires relevant maritime cybersecurity datasets, including normal and malicious network behaviors, to enable them to learn and generalize from examples. Continuous monitoring and updating of AI models are essential to adapt to evolving cyber threats and changing network dynamics in the maritime environment. While AI enhances automated threat detection, human expertise remains crucial for interpreting results, refining algorithms, and making informed decisions in response to cyber incidents.

KNN, with its ability to classify data based on the majority class of its k-nearest neighbors, may exhibit varying levels of accuracy in predicting cyber-attacks in maritime environments. The ME, RMSE, and MAE metrics provide quantitative insights into the disparities between predicted and actual outcomes, helping to refine the model's parameters and enhance its efficacy.

KNN, ANN, and RF are known for their ensemble learning approach, for example, KNN is both easy to use and very good at detecting anomalies, which is a major plus for the suggested methods. ANN is quite good at dealing with complicated, non-linear data and pattern recognition. RF is perfect for detecting cyber threats and guaranteeing marine security because of its ensemble learning, which gives strong performance and resistance to overfitting.

Evaluating **Fig. 23** shows that ME, RMSE, and MAE for RF in maritime cybersecurity provide a comprehensive understanding of the model's predictive performance. This analysis aids in optimizing hyperparameters and addressing potential overfitting or underfitting issues. Logistic Regression, a linear model widely used in binary classification tasks, including cyber-attack prediction, benefits from ME, RMSE, and MAE assessments to gauge its accuracy. The metrics help discern the model's strengths and limitations in capturing the complexity of maritime cyber threats. Artificial Neural Networks, with their ability to learn intricate patterns in data, are instrumental in maritime cybersecurity predictions. Evaluating ME, RMSE, and MAE for ANN provides insights into the model's predictive accuracy shown in **Fig. 23**, and aids in fine-tuning its architecture and parameters for optimal performance. In the maritime cybersecurity context, selecting the most appropriate model involves a trade-off between accuracy, interpretability, and computational efficiency. ME, RMSE, and MAE analyses offer valuable insights into the predictive capabilities of KNN, RF, LR, and ANN, facilitating informed decision-making in the deployment and refinement of these models to fortify maritime systems against cyber threats. Regular updates and continuous monitoring of these models are imperative to adapt to evolving cyber threats in the dynamic maritime environment.

In summary, the application of AI mechanisms like KNN, RF, and ANN in maritime cybersecurity empowers the industry to proactively identify and respond to cyber threats, ultimately strengthening the overall resilience of maritime systems against evolving cybersecurity challenges.

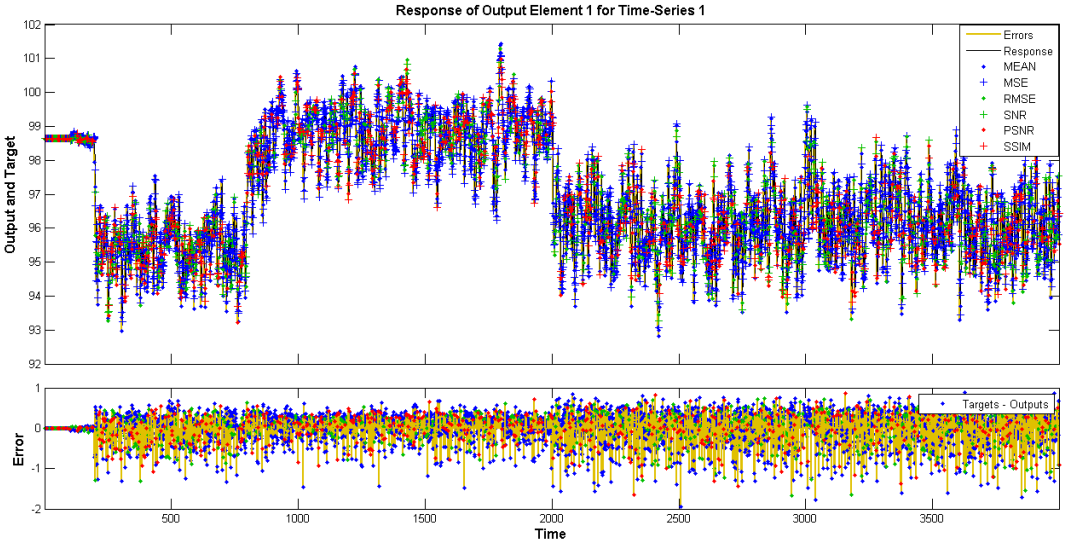

Fig. 23. ANN, KNN, and RF Mean Values Prediction

4.3 Comparisons

Table 4. Comparison Table

References	Merits	Precision Rate
22	To the trust assessment module, the strategy modification module supplies the evaluation approach. It is now possible to identify the trust evaluation module's trust calculation function.	0.5
23	To develop a method to evaluate the trustworthiness of federated learning users to improve the reliability of Digital Twin for Mobile Networks (DTMN) models built using the algorithm. Multiple behavioral factors and their temporal association are assessed in this examination. We implemented and proved the trust assessment technique.	0.9
24	Researchers present an intelligent routing architecture for hierarchical UANETs that can adjust to new circumstances in the network without compromising topology stability or the package delivery ratio.	0.7
Proposed Work	Marine cybersecurity systems must adapt to changing threats in complex environments. This research compares KNN, RF, and ANN for maritime cybersecurity.	0.97

5. Conclusion

In conclusion, the integration of Artificial Intelligence (AI) mechanisms, particularly K-Nearest Neighbors (KNN), Random Forest (RF), and Artificial Neural Networks (ANN) represents a significant stride forward in enhancing maritime cybersecurity. Recent innovations in predictive modeling using these AI techniques have demonstrated promising results in identifying and mitigating cyber threats within the maritime domain. KNN, leveraging its adaptability and ability to discern anomalies from normal patterns, showcases potential in real-time anomaly detection and classification in maritime networks. RF, with its ensemble learning capabilities, excels in handling diverse and complex datasets, providing robust intrusion detection and security analysis. Meanwhile, the deep learning capabilities of ANN, including its ability to learn intricate patterns, position it as a powerful tool for threat detection and risk assessment in maritime cybersecurity. Recent advancements in model architectures, training methodologies, and the availability of large-scale maritime cybersecurity datasets have significantly improved the accuracy and efficiency of these AI mechanisms. The fusion of traditional cybersecurity measures with AI-driven approaches enhances the industry's ability to proactively respond to emerging threats, ensuring the safety and resilience of maritime systems. Looking ahead, future trends in maritime cybersecurity are likely to witness further refinements in AI models, potentially incorporating advanced techniques such as explainable AI to enhance interpretability and trust in model predictions. The deployment of decentralized and distributed AI systems may become prevalent, allowing for real-time threat analysis and response. Additionally, ongoing collaboration between cybersecurity experts, maritime authorities, and AI researchers will be crucial for staying ahead of evolving cyber threats in this dynamic and interconnected environment. In essence, the application of KNN, RF, and ANN in maritime cybersecurity heralds a new era of proactive threat detection and response. As these AI mechanisms continue to evolve, they will play a pivotal role in fortifying maritime systems against cyber threats, ensuring the security and resilience of this critical domain in the face of an ever-evolving cyber landscape.

Future research should integrate AI and quantum computing to improve maritime cybersecurity. Quantum technology can do complicated calculations at fast rates, which might assist AI models like KNN, RF, and ANN in identifying and decreasing cyber threats. Exploring quantum machine learning (QML) techniques for maritime cybersecurity might provide predictive analytics and real-time threat identification. Studying hybrid AI systems, which mix conventional and quantum approaches, might lead to advancements in managing cyber risks in the marine industry. Quantum-based artificial intelligence in cybersecurity presents problems and ethical issues that must be considered. To accomplish this, technological advancements must meet moral and legal constraints. This comprehensive research plan will be essential to advancing marine cybersecurity and offering reliable, forward-thinking solutions during rapid technological change.

References

[1] M. Balduzzi, A. Pasta, and K. Wilhoit, “A security evaluation of AIS automated identification system,” in *Proc. of the 30th Annual Computer Security Applications Conference (ACSAC '14)*, pp.436-445, Association for Computing Machinery, New York, NY, USA, Dec. 2014. Article (CrossRef Link)

[2] R. Neware and A. Khan, “Cloud Computing Digital Forensic challenges,” in *Proc. of 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp.1090-1092, Mar. 2018. Article (CrossRef Link)

[3] R. Dremliuga and M. H. B. M. Rusli, "The Development of the Legal Framework for Autonomous Shipping: Lessons Learned from a Regulation for a Driverless Car," *Journal of Politics and Law*, vol.13, no.3, Aug. 2020. Article (CrossRef Link)
[4] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol.18, no.2, pp.1153-1176, Secondquarter 2016. Article (CrossRef Link)
[5] G. Karatas, O. Demir, and O. K. Sahingoz, "Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset," *IEEE Access*, vol.8, pp.32150-32162, Feb. 2020. Article (CrossRef Link)
[6] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol.97, Sep. 2023. Article (CrossRef Link)
[7] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Computers in Industry*, vol.137, May 2022. Article (CrossRef Link)
[8] A. Amro and V. Gkioulos, "Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth," *International Journal of Information Security*, vol.22, no.1, pp.249-288, Feb. 2022. Article (CrossRef Link)
[9] J. M. Torres, C. I. Comesaña, and P. J. García-Nieto, "Review: machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics*, vol.10, no.10, pp.2823-2836, Oct. 2019. Article (CrossRef Link)
[10] S. Smadi, N. Aslam, and L. Zhang, "Detection of online phishing email using dynamic evolving neural network based on reinforcement learning," *Decision Support Systems*, vol.107, pp.88-102, Mar. 2018. Article (CrossRef Link)
[11] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, and J. Wang, "The application of a novel neural network in the detection of phishing websites," *Journal of Ambient Intelligence and Humanized Computing*, vol.15, no.3, pp.1865-1879, Mar. 2024. Article (CrossRef Link)
[12] L. Yang et al., "Detecting Word-Based Algorithmically Generated Domains Using Semantic Analysis," *Symmetry*, vol.11, no.2, Feb. 2019. Article (CrossRef Link)
[13] M. Taddeo, D. McNeish, A. Blanchard, and E. Edgar, "Ethical Principles for Artificial Intelligence in National Defence," *Philosophy & Technology*, vol.34, no.4, pp.1707-1729, Dec. 2021. Article (CrossRef Link)
[14] H. S. Anderson, J. Woodbridge, and B. Filar, "DeepDGA: Adversarially-Tuned Domain Generation and Detection," in *Proc. of the 2016 ACM Workshop on Artificial Intelligence and Security (AISec '16)*, pp.13-21, Association for Computing Machinery, New York, NY, USA, Oct. 2016. Article (CrossRef Link)
[15] R. Prasad and V. Rohokale, Artificial Intelligence and Machine Learning in Cyber Security, Springer Series in Wireless Technology, pp.231-247, Springer, Cham, 2019. Article (CrossRef Link)
[16] M. Krzysztoń and M. Marks, "Simulation of watchdog placement for cooperative anomaly detection in Bluetooth Mesh Intrusion Detection System," *Simulation Modelling Practice and Theory*, vol.101, May 2020. Article (CrossRef Link)
[17] P. Xiong, H. Liu, Y. Tian, Z. Chen, B. Wang, and H. Yang, "Helicopter maritime search area planning based on a minimum bounding rectangle and K-means clustering," *Chinese Journal of Aeronautics*, vol.34, no.2, pp.554-562, Feb. 2021. Article (CrossRef Link)
[18] M. A. B. Farah et al., "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information*, vol.13, no.1, Jan. 2022. Article (CrossRef Link)
[19] P. O. Shoetan, O. O. Amoo, E. S. Okafor, and O. L. Olorunfemi, "Synthesizing AI's Impact on Cybersecurity in Telecommunications: A Conceptual Framework," *Computer Science & IT Research Journal*, vol.5, no.3, pp.594-605, Mar. 2024. Article (CrossRef Link)
[20] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," *Electronics*, vol.12, no.8, Apr. 2023. Article (CrossRef Link)

[21] J. Yoo and Y. Jo, "Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology," *Sensors*, vol.23, no.11, May 2023. Article (CrossRef Link)
[22] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang, D. Wu, "TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning," *IEEE Internet of Things Journal*, vol.7, no.7, pp.6647-6662, Jul. 2020. Article (CrossRef Link)
[23] J. Guo, Z. Liu, S. Tian, F. Huang, J. Li, X. Li, K. K. Igorevich, J. Ma, "TFL-DT: A Trust Evaluation Scheme for Federated Learning in Digital Twin for Mobile Networks," *IEEE Journal on Selected Areas in Communications*, vol.41 no.11, pp.3548-3560, Nov. 2023. Article (CrossRef Link)
[24] J. Guo, H. Gao, Z. Liu, F. Huang, J. Zhang, X. Li, J. Ma, "ICRA: An Intelligent Clustering Routing Approach for UAV Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol.24, no.2, pp.2447-2460, Feb. 2023. Article (CrossRef Link)

Parasuraman Kumar completed a Master of Science (M.Sc.) degree in Information Technology from Alagappa University, India in 2006, completed a Master of Technology (M.Tech.) degree in Computer and Information Technology in 2008 and a Doctor of Philosophy (Ph.D.) in Information Technology-Computer Science and Engineering in 2012 from Manonmaniam Sundaranar University, India and Master of Business Administration (M.B.A.) degree in Systems from Alagappa University, India in 2018. He was appointed as Assistant Professor in the year 2009 and presently serving as Associate Professor in the Department of Information Technology and Engineering (School of Computer Science and Engineering), Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India He has published more than 125 research articles in reputed SCI/Scopus indexed journals and presented his research findings in IEEE/Springer International Conference proceedings/books and has supervised 10 Ph.D. Scholars, 03 Ph.D. scholars are in progress, 55 M.Phil. and more than 100 Master students. Has been a member of the review board for many international journals, conferences, and committees. His current research interests include Signal and Image Processing, Artificial Intelligence, Visual Perception, Cyber Security, Computer Networks, Pattern Recognition, and Data Analytics, Machine Learning and Deep Learning.

Arumugam Maharajan received a B.E. degree in Mechanical Engineering from the Government College of Engineering, Tirunelveli, Tamil Nadu, India in 1991, and M.Tech. Degree in Information Technology from the Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India in 2009, and he is currently pursuing a Ph.D degree with the Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India. His research interests include artificial intelligence and cyber security.