Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions

DOI: 10.38124/ijsrmt.v3i10.73

Akan Ime Ibokette[1], Tunde Olamide Ogundare[2], Abraham Peter Anyebe[3]
Idoko Innocent Odeh[4], Francisca Chinonye Okafor[5]

[1] Institute of Engineering, Technology and Innovation Management, University of Port Harcourt, Port Harcourt, Nigeria.
[2] Department of Nautical Science, Liver John Moores University, United Kingdom.
[3] Department of Navigation and Direction, Nigerian Navy Naval Unit, Abuja, Nigeria.
[4] Professional Services Department, Layer3 Ltd, Wuse Zone 4, Abuja, Nigeria
[5] Department of Geosciences, University of Lagos, Lagos State, Nigeria

Abstract

The maritime industry is increasingly confronted with a myriad of cybersecurity challenges exacerbated by extreme environmental conditions, technological advancements, and heightened reliance on automation. This review paper discusses the intersection of these factors, focusing on the adoption of artificial intelligence (AI)-based intrusion detection systems (IDS) and network automation as vital strategies for mitigating cybersecurity risks. The paper begins by outlining the unique cybersecurity threats faced by the maritime sector, which include data breaches, phishing attacks, and malware threats, all amplified by adverse weather and geographical isolation. In light of these challenges, the rationale for integrating AI-driven solutions into maritime operations is discussed. AI-based IDS can enhance threat detection capabilities through advanced machine learning algorithms that adapt to evolving cyber threats while minimizing false positives. Additionally, network automation can improve connectivity and data security, facilitating real-time monitoring and response to incidents. The review also addresses the critical need for collaboration between maritime and technology industries, emphasizing how partnerships can foster innovation and provide tailored solutions to the sector's specific needs. Furthermore, the paper examines current implementations and case studies that illustrate successful applications of AI and automation in adverse maritime conditions. While recognizing the potential benefits, the review highlights the technical and operational challenges inherent in these implementations, including data integration, regulatory compliance, and cultural differences between sectors. Ultimately, this paper aims to provide a comprehensive overview of the state of maritime cybersecurity and the pivotal role of AI and automation in shaping a resilient, secure maritime future. The findings underscore the importance of ongoing research and development, collaborative efforts, and the necessity of adaptable strategies to safeguard maritime operations against the evolving landscape of cyber threats.

Keywords: *Maritime Cybersecurity, AI-Based Intrusion Detection Systems (IDS), Network Automation, Extreme Environmental Conditions and Mitigation.*

I. INTRODUCTION

A. Overview of Cybersecurity Challenges in the Maritime Industry.

The maritime industry, characterized by its reliance on increasingly sophisticated digital systems, faces a growing number of cybersecurity challenges. As vessels and ports integrate more operational technologies (OTs) and information technologies (ITs) to improve efficiency, they become more vulnerable to cyber-attacks. One significant challenge is the complexity of maritime networks, which often involve a combination of aging legacy systems and newer digital platforms. This combination creates potential entry points for cybercriminals, especially as many of these older systems were not designed with modern cybersecurity in mind (Nawaz et al., 2024).

How to Cite: Ibokette, A. I., Ogundare, T. O., Anyebe, A. P., Alao, F. O.-O., Odeh, I. I., & Okafor, F. C. (2024). Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions. *International Journal of Scientific Research and Modern Technology*, *3*(10). https://doi.org/10.38124/ijsrmt.v3i10.73

A notable risk comes from the maritime industry's dependence on satellite communications for both operational and commercial purposes. Cybercriminals can exploit vulnerabilities in these systems to intercept or manipulate communications, potentially leading to significant disruptions in navigation, cargo handling, or vessel tracking (Ijiga et al., 2024). This issue is exacerbated by the fact that maritime vessels often operate in isolated areas where real-time monitoring and support are limited, making it more difficult to detect and respond to cyber threats promptly.

Also, human factors contribute significantly to cybersecurity risks. Crew members may lack adequate training in cybersecurity protocols, inadvertently exposing systems to malware or phishing attacks. This is further complicated by the transient nature of maritime personnel, with crews frequently changing, making consistent cybersecurity practices challenging to enforce (Jones et al., 2016).

In addition, the increasing connectivity between ships, ports, and logistics companies through the Internet of Things (IoT) adds another layer of complexity. While IoT technologies improve operational efficiency, they also widen the attack surface. Hackers could potentially target these connected systems, disrupting the supply chain, and causing significant economic and operational impacts (Cho et al., 2022). The interconnectedness of maritime operations means that a single cybersecurity breach in one part of the system can have cascading effects throughout the industry.

The illustrations in figure 1 depict an overview of the cybersecurity within the maritime space designed to allow offshore vessels to access real time data and critical updates under secured conditions.

Fig 1 Overview of Cybersecurity within the Maritime Environment.

Extreme environmental conditions significantly impact maritime networks and systems, posing challenges to both cybersecurity and overall operational reliability. Maritime operations occur in harsh environments, where weather conditions such as storms, high humidity, saltwater exposure, and extreme temperatures can degrade network infrastructure, disrupt communication systems, and expose vulnerabilities in both hardware and software (Wei et al., 2021). For instance, strong winds and rough seas can physically damage equipment, while electromagnetic interference from storms can disrupt satellite communications, impairing the functioning of critical systems, such as GPS, AIS (Automatic Identification System), and radar (Yuan et al., 2017).

These environmental challenges are exacerbated by the isolated nature of maritime operations, where ships and offshore platforms often operate far from maintenance hubs and reliable network support. Prolonged exposure to such conditions can weaken system components, leading to increased risk of hardware failures or compromised communication links (Alqurashi et al., 2022). Moreover, saltwater corrosion and humidity can affect the integrity of electronic systems and network devices, leading to increased downtime and the need for frequent repairs or replacements.

Extreme conditions not only strain physical systems but also create opportunities for cyber-attacks. Environmental factors can cause intermittent connectivity, leading to delays in updates or patches that are crucial for securing maritime networks. Cyber attackers may exploit such downtimes to infiltrate systems, especially when vessels are operating autonomously with limited human oversight (Tabish & Chaur-Luh, 2024). Additionally, during environmental crises such as storms, maritime personnel are often preoccupied with safety operations, potentially neglecting cybersecurity protocols, thus heightening the risk of successful attacks.

In extreme environments, maintaining secure and reliable communication systems is a significant challenge. Satellite communication, the backbone of maritime networks, is particularly vulnerable to environmental disruptions, leading to loss of real-time data transmission and leaving vessels exposed to navigational risks (Alqurashi et al., 2022). As maritime operations increase their reliance on automation and the Internet of Things (IoT), ensuring the resilience of these systems in harsh environmental conditions becomes paramount for maintaining both cybersecurity and operational integrity.

Figure 2 illustrates the maritime communications workflow execution framework, where communication workflows are scheduled and managed using cloud-based resources. Users submit communication workflows to a task-oriented smart controller, which analyzes them and categorizes the resulting tasks into three groups: high-performance latency-aware prioritized tasks, computational tasks, and data-oriented tasks. These tasks are then forwarded to the maritime communication workflow scheduler. Simultaneously, the cloud computing resources are assessed by a resource-aware smart controller, which classifies them into three types: high-performance latency-aware resources, computation-aware resources, and data-aware resources. These resources are also submitted to the scheduler. The maritime communication workflow scheduler matches tasks to appropriate cloud resources and dispatches them to the execution engine. Once execution is complete, the results are returned to the user (Ahmad et al., 2023).

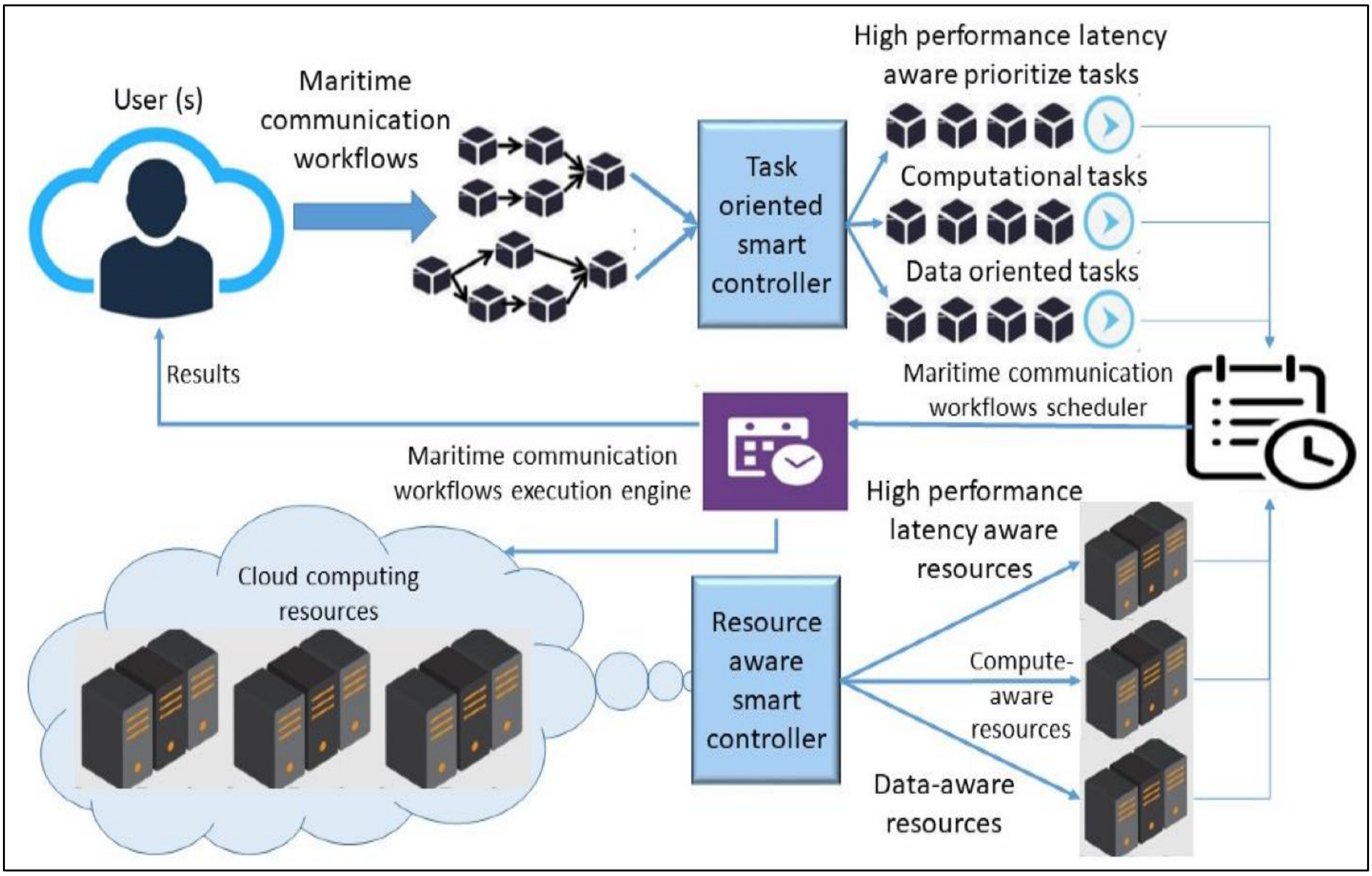
User (s)
Maritime communication workflows
Task oriented smart controller
High performance latency aware prioritize tasks
Computational tasks
Data oriented tasks
Maritime communication workflows scheduler
Results
Maritime communication workflows execution engine
Cloud computing resources
Resource aware smart controller
High performance latency aware resources
Compute-aware resources
Data-aware resources

Fig 2 A Framework for Maritime Communication Workflows Execution.
Source: Ahmad, Z., Acarer, T., & Kim, W. (2023). Optimization of maritime communication workflow execution with a task-oriented scheduling framework in cloud computing

B. Motivation for AI-Based Solutions

The maritime industry is increasingly relying on automation and digital technologies to improve operational efficiency, safety, and profitability. This digital transformation is driven by advancements in artificial intelligence (AI), machine learning, the Internet of Things (IoT), and robotics, which are helping to optimize navigation, cargo handling, and overall vessel management (Fruth & Teuteberg, 2017). One of the most significant applications of automation in maritime operations is the rise of autonomous ships, which utilize advanced navigation systems and sensors to operate with minimal human intervention. These vessels can significantly reduce operational costs and human error, while also enhancing safety and fuel efficiency (Evensen 2020).

Digital technologies are also transforming port operations through automation in cargo handling and logistics management. Automated cranes, guided vehicles, and digital tracking systems enable ports to manage cargo more efficiently, reducing turnaround times and improving supply chain coordination (Awotiwon et al., 2024). These innovations in port automation also facilitate real-time tracking of cargo, allowing for better transparency and coordination between shipping companies, port authorities, and logistics providers.

In addition, the IoT is playing a crucial role in the digitization of maritime operations. By connecting ships, ports, and offshore platforms through smart sensors and devices, IoT enables real-time monitoring of equipment performance, fuel consumption, and environmental conditions (Idoko et al., 2024). This data-driven approach helps in predictive maintenance, reducing the likelihood of equipment failures, and ensuring the operational readiness of vessels even in challenging conditions. For instance, sensors can detect mechanical issues before they become critical, allowing for timely maintenance and avoiding costly downtime.

However, the increasing reliance on automation and digital technologies also raises cybersecurity concerns. As more systems become interconnected, the attack surface for cyber threats expands, making maritime operations vulnerable to potential disruptions (Tam & Jones, 2018). Protecting these digital infrastructures from cyber-attacks becomes a critical priority, especially as the industry moves toward more autonomous and IoT-enabled operations.

The adoption of AI-based Intrusion Detection Systems (IDS) and network automation in maritime cybersecurity is increasingly necessary to address the growing sophistication of cyber threats and the complexity of modern maritime networks. Traditional IDS, which rely on predefined signatures of known threats, are often insufficient for identifying emerging, unknown, or evolving threats. AI-based IDS offer a significant advantage by using machine learning algorithms to detect anomalies and patterns indicative of new or evolving cyberattacks, making them particularly suited for complex and dynamic maritime environments (kumar et al., 2021).

One of the key rationales for using AI in IDS is its ability to process vast amounts of data in real-time and identify subtle irregularities that might escape traditional systems. Maritime operations generate large volumes of data from various sources, such as navigation systems, onboard sensors, and communication networks. AI-based IDS can continuously monitor this data, detect abnormal patterns, and trigger alerts for potential security breaches before they escalate into more severe incidents (Katterbauer 2022). This proactive approach reduces the time required to detect and respond to attacks, ultimately enhancing the overall security posture of maritime networks.

Additionally, AI-driven automation can improve resilience during cyberattacks by autonomously applying security patches, updating firewall configurations, or deploying additional defensive measures based on the nature of the threat (Katterbauer 2022). Given that maritime operations often occur in remote locations with limited access to real-time IT support, the ability to automate threat detection and response significantly enhances the system's security. This is especially important for vessels and offshore platforms where manual intervention may not be immediately available.

C. *Objectives of the Review*

The primary objective of this review is to analyse how AI-based Intrusion Detection Systems (IDS) and network automation can be effectively deployed to mitigate cybersecurity risks in maritime operations, particularly under extreme environmental conditions. As cyber threats continue to evolve, maritime systems, which are becoming increasingly digital and interconnected, are exposed to new vulnerabilities (Tam & Jones, 2018). Therefore, the review seeks to provide a comprehensive understanding of the current cybersecurity landscape in the maritime industry, identify the challenges posed by extreme environments, and assess the capabilities of AI-driven solutions in addressing these challenges.

Another key objective is to evaluate the effectiveness of AI-based IDS in detecting and mitigating emerging cyber threats in maritime networks. Traditional IDS models often struggle to keep up with new, unknown attacks, whereas AI-based systems can adopt machine learning to identify anomalies and suspicious patterns that signal potential breaches (kumar et al., 2021). This review aims to highlight the potential of AI to improve threat detection, particularly in environments where traditional methods may fail.

Finally, this review will examine the role of network automation in maintaining operational continuity during cyberattacks or environmental disruptions. Network automation, powered by technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV), allows for real-time reconfiguration of networks to isolate compromised systems, ensuring the overall resilience of maritime operations (Katterbauer, 2022). By assessing case studies and research on automated network defense, the review will underscore how these technologies can enhance the security and reliability of maritime communication systems.

II. CYBERSECURITY THREATS IN MARITIME ENVIRONMENTS

A. *Types of Cybersecurity Threats*

The maritime industry faces a diverse range of cybersecurity threats, driven by the increasing digitization of operations and reliance on interconnected systems. These threats pose significant risks to the safety, security, and efficiency of maritime operations, especially in the context of cyber-physical systems that control critical functions such as navigation, cargo management, and communication.

- *Malware Attacks*

Malware, including ransomware, is one of the most common cybersecurity threats in the maritime sector. Ransomware attacks encrypt critical systems, such as those used for cargo tracking or navigation, demanding a ransom to restore functionality. A notable example was the 2017 attack on the global shipping company Maersk, where the NotPetya malware caused operational disruption across ports and shipping lines, resulting in a multi million-dollar loss (Adu-Twum et al., 2024). Malware can also be introduced via infected USB devices, emails, or compromised software updates, making it crucial for maritime organizations to maintain robust malware defenses (Tam & Jones, 2018).

- *Phishing and Social Engineering*

Phishing and social engineering attacks target individuals within maritime organizations to gain unauthorized access to networks or sensitive information as shown in figure 3. Cybercriminals use fraudulent emails, messages, or websites to deceive employees into revealing login credentials or downloading malicious software. These attacks exploit human vulnerabilities rather than technical ones, making them harder to detect and prevent (Ayoola et al., 2024). In a maritime context, social engineering attacks can lead to unauthorized access to ship control systems, cargo manifests, or financial transactions.

Fig 3 Phishing as a Cyberthreat in the Maritime Space.

- *Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks*

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks aim to disrupt the availability of network services by overwhelming systems with a flood of traffic. In the maritime industry, such attacks can cripple communication networks, GPS, or navigation systems, rendering vessels unable to operate effectively (Jones et al., 2016). DDoS attacks, in particular, are challenging to mitigate, as they often involve multiple compromised systems sending massive volumes of data to the target. This type of attack can paralyze port operations or disable critical onboard systems, leading to severe operational delays and financial losses.

- *Supply Chain Attacks*

In the highly interconnected maritime industry, supply chain attacks represent a growing threat. These attacks occur when cybercriminals compromise third-party vendors, suppliers, or service providers to infiltrate maritime networks. For example, a compromised software update from a vendor could introduce malware into a ship's control systems, or a third-party service provider could inadvertently expose sensitive data (Nawaz et al., 2024). With the growing reliance on outsourced technologies and services, the maritime industry is vulnerable to supply chain attacks that can have widespread effects across multiple operations.

- *GPS Spoofing and Jamming*

GPS spoofing and jamming are unique threats to the maritime industry, as vessels heavily rely on satellite-based navigation systems. Spoofing involves transmitting fake GPS signals to mislead a ship's navigation system, causing it to follow an incorrect route. Jamming, on the other hand, disrupts GPS signals, preventing vessels from receiving accurate location data (Androjna & Perkovič, 2021). These attacks can be used to hijack vessels, reroute them into dangerous waters, or cause collisions. Given the critical role of GPS in navigation, GPS spoofing and jamming pose serious risks to maritime safety.

The conceptual framework of GPS spoofing is depicted in Figure 4. The input consists of a stream of NMEA sentences, generated by at least two GPS receivers within a network. Alternatively, pre-recorded network trace files can serve as input. For each detection method, specific fields within the NMEA sentences that are relevant to the respective detection approach are identified. These fields are continuously monitored, and any state change activates the corresponding detection method(s) (Spravil et al., 2023).

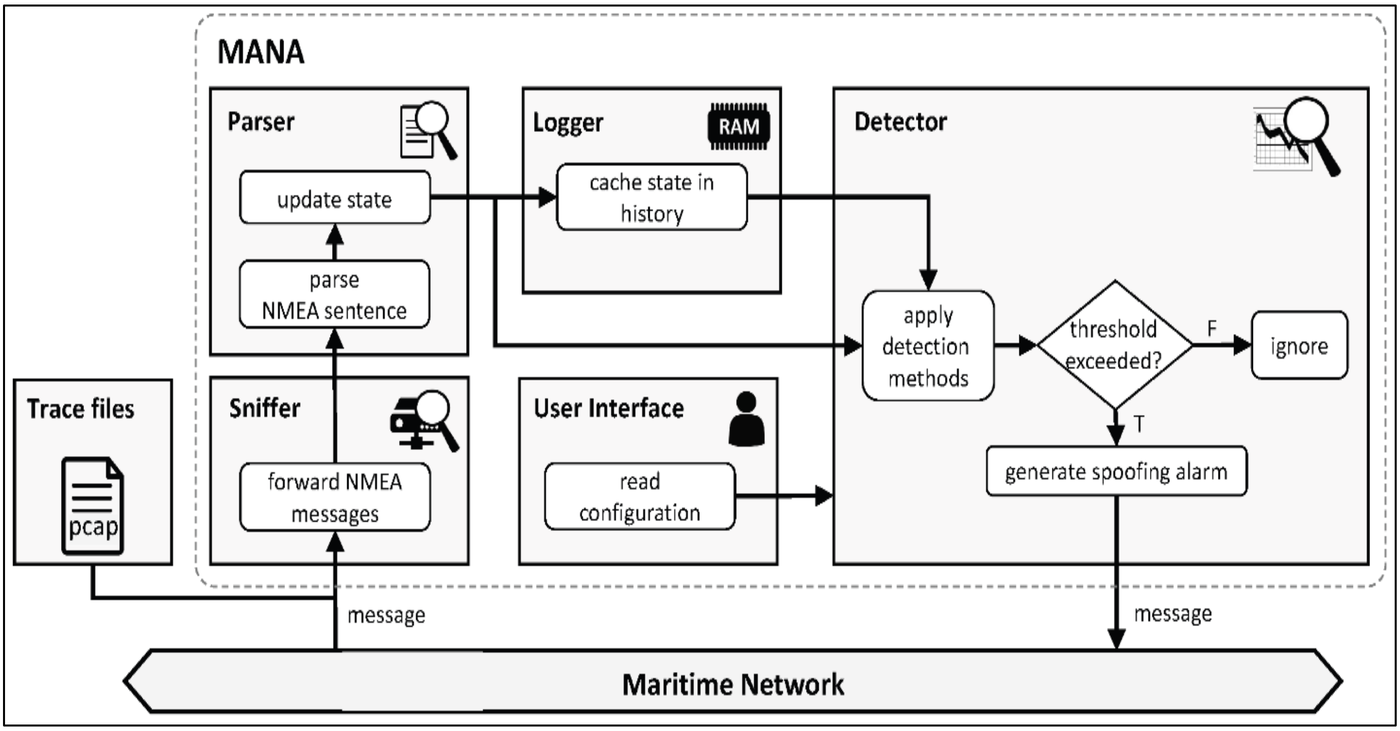

Fig 4 Conceptual Overview of the GPS Spoofing MANA Framework and its Components.
Source: Spravil, J., et al., (2023). Detecting maritime gps spoofing attacks based on nmea sentence integrity monitoring. *Journal of Marine Science and Engineering*, *11*(5), 928.

B. Impact of Extreme Environmental Conditions

Extreme weather, geographical isolation, and harsh marine environments significantly exacerbate cybersecurity risks in the maritime industry. These factors introduce unique challenges to both the physical and digital security of maritime operations, making vessels and offshore platforms more vulnerable to cyber threats and complicating the detection and response process.

➢ *Impact of Extreme Weather on Cybersecurity*

Extreme weather conditions such as storms, high winds, and rough seas can physically damage onboard network infrastructure and communication equipment, leading to operational failures and increasing susceptibility to cyber-attacks. For instance, during severe weather events, critical communication systems like satellite links, which are essential for the ship's navigation and coordination, can be disrupted (Wei et al., 2021). These disruptions create vulnerabilities, as attackers can exploit periods of limited connectivity or system degradation to launch cyberattacks. Furthermore, extreme weather often diverts the attention of the crew to safety operations, reducing their ability to focus on cybersecurity protocols, thereby increasing the risk of successful breaches (Jones et al., 2016).

In particular, weather-related delays in software updates or security patches can leave systems exposed to known vulnerabilities. When a ship's communication systems are compromised or degraded due to weather conditions, critical updates are delayed, giving cybercriminals a window of opportunity to exploit weaknesses in the system (Alqurashi et al., 2022). Additionally, natural events like solar storms can cause electromagnetic interference, affecting GPS signals, navigation systems, and even onboard cybersecurity defenses, leaving ships more vulnerable to spoofing and jamming attacks (Androjna & Perkovič, 2021).

➢ *Geographical Isolation and Remote Operations*

Maritime vessels often operate in remote areas, far from shore-based support or reliable internet access, which poses significant challenges for cybersecurity. The geographical isolation of ships and offshore platforms makes it difficult to detect, monitor, and respond to cyber threats in real-time. Unlike land-based industries, where cybersecurity personnel can quickly intervene, maritime operations rely heavily on automated systems and intermittent communication, which may not be sufficient to address sophisticated cyberattacks (Mraković & Vojinović 2019).

Moreover, this isolation often leads to longer response times for cybersecurity incidents. When a vessel's systems are compromised, the limited connectivity makes it harder to collaborate with shore-based IT teams or cybersecurity experts, prolonging the vulnerability period (Katterbauer, 2022). For example, if a vessel in a geographically isolated location is targeted by a ransomware attack or suffers a network breach, the crew may not have the expertise or resources to mitigate the threat until they are within range of external support.

➢ *Harsh Marine Environments and Equipment Vulnerability*

The maritime environment is inherently harsh, with high humidity, saltwater exposure, and temperature extremes that can degrade hardware and networks over time. Saltwater corrosion is a particular concern, as it can weaken the physical components of network infrastructure, leading to equipment failures that expose systems to cyber threats (Yuan et al., 2017). Additionally, the harsh environmental conditions require robust and resilient systems that can withstand wear and tear, but the frequent need for repairs or replacements can open the door to cyber vulnerabilities, especially if compromised equipment is replaced with insecure or outdated devices.

The frequent maintenance required in these environments can lead to increased use of third-party services, which introduces further risk through potential supply chain attacks. For example, compromised hardware or software provided by external vendors may introduce malware into the ship's network, further exacerbating the risks posed by the already harsh operating conditions (Nawaz et al., 2024). Harsh environments can also cause intermittent power outages, leading to unexpected system reboots or unsynchronized security measures, further complicating the ship's defense against cyber threats (Okeke et al., 2024).

C. *Challenges in Maintaining Connectivity and Secure Communications.*

Maintaining connectivity and secure communications in maritime operations presents significant challenges due to the unique operational environment, which includes geographical isolation, extreme weather conditions, and the technical limitations of existing communication infrastructures. These factors complicate the ability of vessels and offshore platforms to maintain continuous, secure, and reliable communications, leaving them vulnerable to cyberattacks and operational disruptions.

➢ *Limited Communication Infrastructure*

One of the major challenges in maritime operations is the limited availability of reliable communication infrastructure. Ships often operate in remote areas of the ocean, far from terrestrial communication networks, relying heavily on satellite-based systems for connectivity (Wei et al., 2021). However, satellite communication has inherent limitations, such as high latency, limited bandwidth, and susceptibility to signal interference. These constraints not only slow down data transmission but also create gaps in coverage, making it difficult to maintain continuous, secure connections for critical systems like navigation, cargo management, and monitoring (Yuan et al., 2017).

This lack of reliable, high-speed communication infrastructure can hinder the timely application of security patches and updates, leaving maritime networks vulnerable to known cyber threats. Moreover, the limited bandwidth available through satellite connections makes it challenging to implement advanced encryption and security protocols, as these often require significant processing power and data throughput (Mraković & Vojinović 2019). The resulting security gaps make ships and offshore installations prime targets for cyberattacks, as attackers can exploit these weak points to intercept or manipulate data.

The illustrations in figure 5 show an overview of communication arrangement (vessel-to shore communication) intended to allow offshore vessels to access real time data and at the same time send and receive critical updates when in coastal environment.

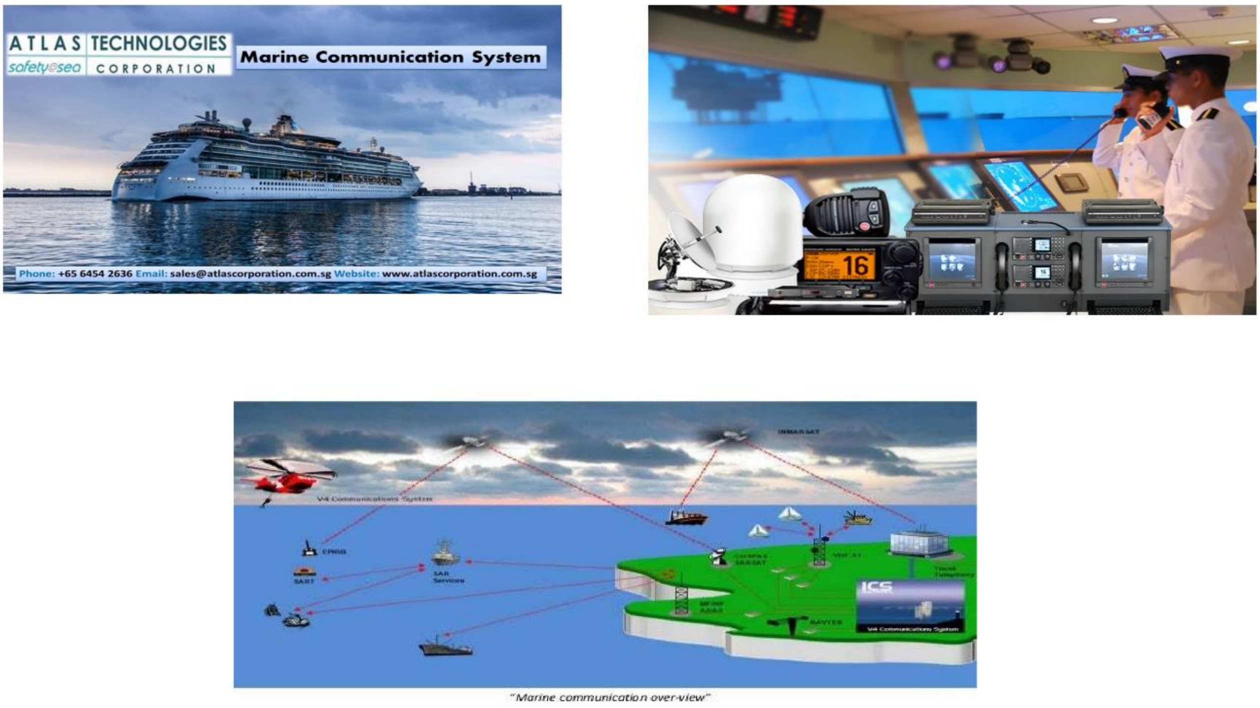

Fig 5 An Overview of Communication System in the Maritime Environment
Source: Ibokette et al., (2024). Optimizing maritime communication networks with virtualization, containerization and IoT to address scalability and real – time data processing challenges in vessel – to –shore communication.

- *Latency and Data Transmission Delays*

High latency in satellite communications poses a serious challenge to secure maritime communications. Due to the long distance between vessels and satellites, real-time data transmission is often delayed, impacting the ability to monitor and respond to cyber threats in a timely manner (Alqurashi et al., 2022). This delay also affects critical functions, such as navigation updates, system diagnostics, and communications with shore-based support teams. For instance, in the event of a cyberattack, the latency in detecting, reporting, and responding to security breaches can lead to prolonged exposure to threats, increasing the potential damage to operational systems.

Latency also complicates the implementation of real-time encryption and decryption processes, which are necessary to secure sensitive data in transit. Advanced encryption protocols, while crucial for preventing unauthorized access, require high processing speeds and low-latency communication to function effectively. In high-latency environments, such as those dependent on satellite communication, the encryption process can experience delays, leaving data transmissions exposed to interception or tampering during transit (Wei et al., 2021).

When a packet is completed, the network device activates an interrupt to inform the system of the event. The real-time process (RT task) that handles this event must be scheduled, processed, and then respond, leading to processing delays after the packet reaches the real-time system control device as shown in figure 6. Two main sources of delay can be identified in this process. Interrupt latency occurs when the system is unable to immediately handle the interrupt due to other operations, including saving the processor's state and processing the interrupt itself. Dispatch latency happens after the interrupt is handled, when the RT task is ready to run but experiences delay due to context switching, scheduling, and other conflicts during the dispatch process (Queiroz et al., 2023).

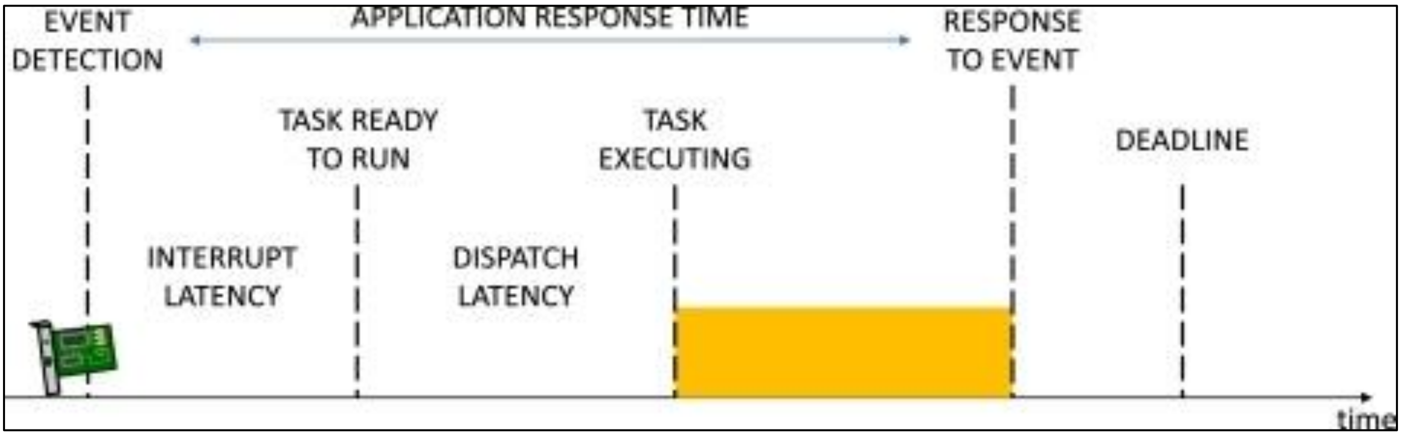

Fig 6 Processing Latency
Source: Queiroz, R., et al., (2023): Container-Based Virtualization for Real-Time Industrial System – A Systematic Review.

- *Vulnerability to Signal Jamming and Interference*

Another significant challenge in maritime communications is the vulnerability to signal jamming and interference. Given the reliance on satellite and radio frequency (RF) communications, ships are susceptible to deliberate jamming attacks or environmental interference that can disrupt or block communication signals. Signal jamming can prevent the transmission of vital information, such as navigation coordinates or distress signals, compromising both safety and security (Androjna & Perkovič, 2021). Additionally, natural phenomena, such as solar flares or electromagnetic interference, can further degrade the quality of satellite communications, making secure, continuous connectivity difficult to maintain.

These disruptions can be especially dangerous in critical moments, such as during navigation in congested waters or in response to emergency situations. For example, an attacker could jam the GPS signals used by a vessel, causing it to veer off course without the crew realizing it. In such cases, the inability to communicate with shore-based authorities or other vessels due to jamming or interference can result in severe operational risks (Bari et al., 2016).

- *Cybersecurity Threats to Communication Systems*

The maritime industry is increasingly targeted by cyberattacks aimed at compromising communication systems. Hackers may attempt to intercept, alter, or block data transmissions to gain control of a ship’s systems or steal sensitive information. Without strong encryption and authentication measures in place, cybercriminals can exploit communication vulnerabilities to conduct man-in-the-middle attacks, where they insert themselves into the communication stream between ships and shore-based control centres (Mraković & Vojinović 2019). This can lead to unauthorized access to critical systems, such as navigation, engine control, or cargo management.

The challenge is further compounded by the use of legacy communication systems in many maritime operations. These systems may not have been designed with modern cybersecurity needs in mind and often lack the necessary protections against cyber threats. As maritime organizations transition to more digital and automated systems, the need to upgrade legacy communication infrastructures become paramount to ensure that communications remain secure and resilient in the face of evolving cyber threats (Nawaz et al., 2024).

III. AI-BASED INTRUSION DETECTION SYSTEMS (IDS)

A. Overview of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are a critical component of cybersecurity infrastructure, designed to monitor network traffic and detect suspicious activities or policy violations that may indicate a security breach. An IDS acts as an early warning system by analyzing data for signs of malicious activities, such as unauthorized access, abnormal patterns, or system vulnerabilities, and alerting security administrators to take preventive actions (Patel et al., 2013).

IDS are generally classified into two broad categories: **Network-based IDS (NIDS)**, which monitor network traffic, and **Host-based IDS (HIDS)**, which monitor activity on individual devices or systems. Both play crucial roles in detecting cyber threats across different layers of an organization's IT environment, providing defense against a wide range of potential attacks, including malware, denial-of-service (DoS), and insider threats (Asharf et al., 2020).

- *Network-Based Intrusion Detection Systems (NIDS)*

NIDS monitor the entire network for malicious activities by analyzing packets that travel through the network. These systems are usually placed at strategic points, such as network gateways or critical junctions within an organization's infrastructure, to inspect incoming and outgoing traffic in real-time. By using predefined rules or behavioral analysis, NIDS can detect unusual patterns that may indicate an attack, such as unauthorized data exfiltration, DDoS attacks, or port scanning (Deshpande et al., 2018).

One of the key advantages of NIDS is that it allows for the monitoring of multiple devices simultaneously, making it scalable for large organizations, including those in the maritime industry where communication networks extend across fleets and offshore installations. However, a limitation of NIDS is that encrypted traffic is challenging to analyze, which can hinder its ability to detect threats within secure communications (Patel et al., 2013).

As shown in Figure 7 this model is divided into two components: a sensor, which gathers data from an information source, and a detector, which handles the analysis. The system is comprised of multiple sensors and detectors. In practical applications, it collects data from various sources, which are then processed by a central detector. The detector is designed to identify known intrusions, learn new intrusion patterns, and respond to events as they occur, triggering an alarm when necessary (Sodiya et al., 2014).

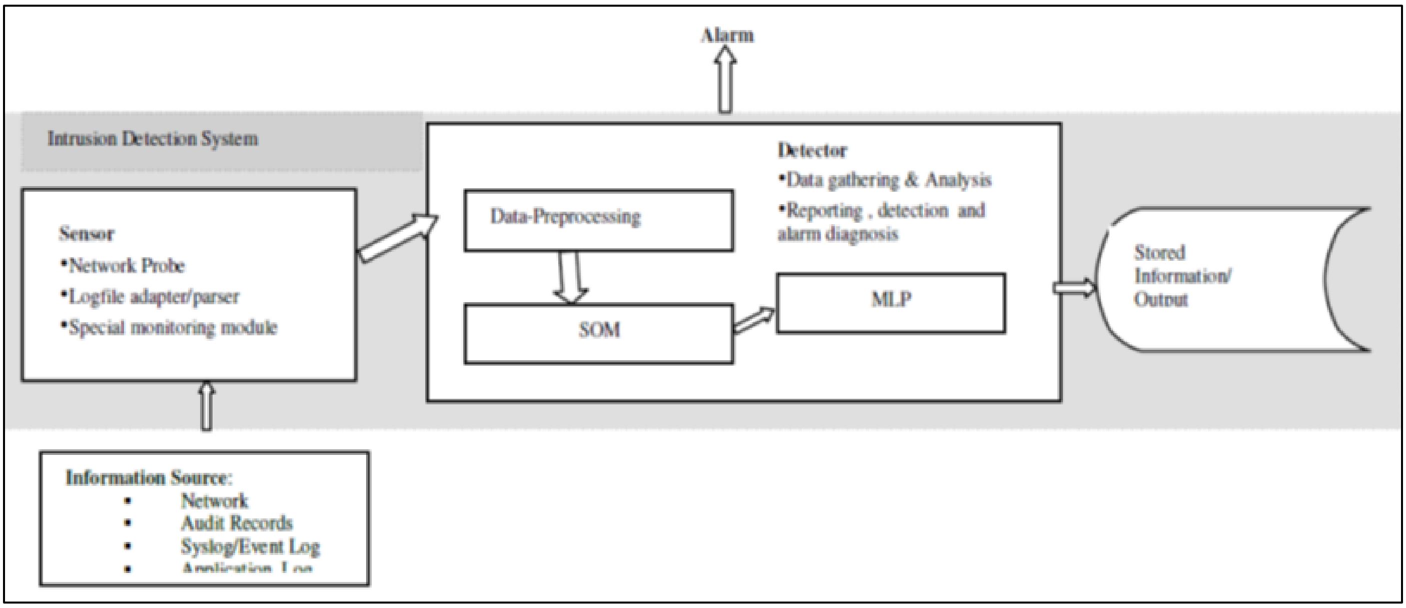

Fig 7 Artificial Neural Network Based IDS Model.
Source: Sodiya et al., (2014). Neural network-based intrusion detection systems.

- *Host-Based Intrusion Detection Systems (HIDS)*

HIDS focus on monitoring individual systems or hosts for suspicious activities by analyzing system logs, file integrity, and application behavior. These systems are especially useful in identifying threats that have bypassed network defenses, such as malware infections or unauthorized file modifications (Scarfone & Mell, 2010). In the maritime sector, HIDS can be deployed on shipboard systems, ensuring that critical systems like navigation and engine control are continuously monitored for unauthorized access.

HIDS are highly effective in detecting insider threats and sophisticated malware attacks that target specific hosts. However, they require substantial resources for deployment and maintenance, as each host must be equipped with its own IDS system, which can lead to challenges in scaling for large or distributed operations (Deshpande et al., 2018).

A Host-based Intrusion Detection and Prevention System (HIDPS) monitors various types of host events and activities to identify malicious code and intrusion attempts on host systems, including desktops, mail servers, DNS servers, web servers, and database servers. When HIDPS detects malicious code or abnormal behaviors, such as buffer overflow or unauthorized file system access, it prevents their execution. HIDPS gathers information from host systems, including file system usage, network events, and system calls, to detect intrusions (Letou et al., 2013). The proposed HIDPS model is illustrated in Figure 8, and its components include Data Pre-processing, Feature Extraction, Feature Selection, Misuse Detection Engine, Anomaly Detection Engine, Knowledge-based Database, Behavior-based Database, Countermeasure, Launch Action, and System Administrator.

- **Data Pre-processing**: Data is filtered and segmented for analysis.
- **Feature Extraction**: Network packets are decomposed to extract relevant features.
- **Feature Selection**: Feature vectors are selected to be used as inputs for machine learning algorithms.

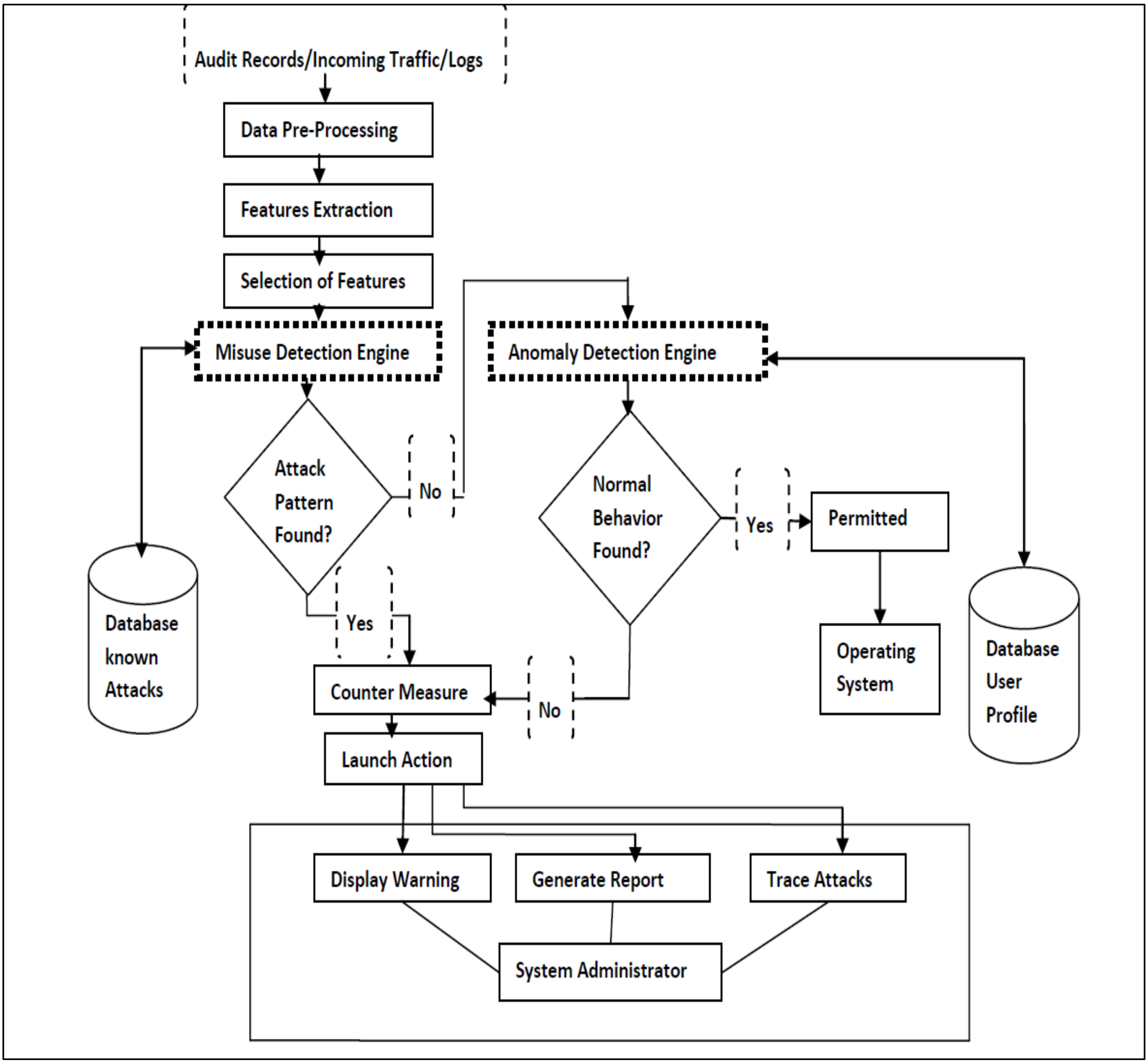

Fig 8 Proposed Host-based Intrusion Detection and Prevention System Model
Source: Letou et al. (2013). Host-based intrusion detection and prevention system (HIDPS). *International Journal of Computer Applications*, *69*(26), 28-33.

- **Misuse Detection Engine**: This engine processes input data, searching for known attack signatures, events, and alerts based on past attacks.
- **Anomaly Detection Engine**: This engine processes input data by comparing it against a user-defined profile of normal behavior, identifying any deviations or abnormal system activities.
- **Knowledge-based Database**: Stores records of previously known attacks, events, and alerts, which the Misuse Detection Engine utilizes.
- **Behavior-based Database**: Stores profiles of normal behavior, events, and alerts, required by the Anomaly Detection Engine.

- **Countermeasure**: Reacts to detected attacks by blocking and preventing them from causing further damage.
- **Launch Action**: Displays warnings, generates reports on system events, and tracks the activities of potential attackers or intruders.
- **System Administrator**: The administrator takes appropriate action based on the warnings displayed, reports generated, and intruder activity tracking.

B. Signature-Based vs. Anomaly-Based Detection

Intrusion detection systems employ different methodologies for identifying potential threats, the most common being **signature-based detection** and **anomaly-based detection**.

➢ *Signature-Based Detection:*

This approach relies on a predefined database of known attack patterns or signatures. When an incoming traffic pattern matches one of these signatures, the IDS generates an alert. While signature-based detection is highly effective in identifying known threats, it struggles to detect new or unknown attacks (Patel et al., 2013). In dynamic environments like maritime networks, where new threats can emerge rapidly, this approach has limitations in providing comprehensive security.

➢ *Anomaly-Based Detection:*

Anomaly detection focuses on identifying deviations from normal network behavior. This is particularly useful in environments with unpredictable traffic patterns, such as maritime networks, where ships and ports may have varying communication loads depending on operational conditions (Ijiga et al 2024). Anomaly-based systems can detect novel attacks by flagging unusual behavior, though they can also generate a higher rate of false positives, which requires careful tuning to avoid alert fatigue.

C. Role of IDS in the Maritime Industry

In the maritime sector, where operations depend on interconnected networks, intrusion detection systems are essential for defending against cyber threats. Given the increasing reliance on automated and digital technologies for navigation, cargo handling, and communications, maritime vessels and ports face growing exposure to cyber-attacks (Mraković & Vojinović 2019). IDS can provide a first line of defense by continuously monitoring networks for threats, thereby reducing the risk of cyber incidents that could jeopardize the safety and security of maritime operations.

Furthermore, the maritime industry's geographically dispersed nature, with vessels and offshore platforms operating in isolated areas, increases the importance of IDS as a mechanism to ensure secure communication and timely detection of threats. IDS solutions tailored to the maritime environment, such as those equipped with anomaly-based detection, can enhance the sector’s resilience to cyber threats, especially in scenarios where connectivity is intermittent and satellite communications are used (Alqurashi et al., 2022).

Despite their benefits, deploying IDS in maritime operations comes with challenges. These include the need to manage high volumes of network traffic, ensure compatibility with legacy systems, and cope with high-latency satellite communications (Wei et al., 2021). Additionally, IDS must be capable of operating in harsh environmental conditions where system reliability can be affected by factors such as extreme weather, geographical isolation, and limited bandwidth (Yuan et al., 2017).

D. Key Metrics for Evaluating IDS Performance

The effectiveness of Intrusion Detection Systems (IDS) can be assessed through various performance metrics, which provide insights into their operational efficiency, detection capabilities, and overall security contributions. Understanding these metrics is essential for evaluating and comparing different IDS implementations, particularly as cyber threats evolve.

Key metrics for evaluating IDS performance include detection rate, false positive rate, false negative rate, precision and recall.

➢ *Detection Rate (True Positive Rate)*

The detection rate, also known as the true positive rate, measures the proportion of actual attacks that the IDS successfully identifies. It is calculated as follows:

$$Detection\ Rate = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Negatives\ (FN)}$$

A high detection rate indicates that the IDS is effective in identifying genuine threats. This metric is crucial for organizations, especially in critical sectors like maritime operations, where undetected threats can lead to severe consequences (Almaiah et al, 2022).

➢ *False Positive Rate*

The false positive rate measures the proportion of benign activities incorrectly classified as attacks. It is calculated as:

$$False\ Positive\ Rate = \frac{False\ Positives\ (FP)}{False\ Positives\ (FP) + True\ Negatives\ (TN)}$$

A high false positive rate can lead to alert fatigue among security personnel, making it challenging to focus on genuine threats (Wei et al., 2021). Therefore, an effective IDS should aim to minimize false positives while maintaining a high detection rate.

➢ *False Negative Rate*

The false negative rate measures the proportion of actual attacks that the IDS fails to detect. It is calculated as:

$$False\ Negative\ Rate = \frac{False\ Negatives\ (FN)}{False\ Negatives\ (FN) + True\ Positives\ (TP)}$$

A high false negative rate indicates that the IDS is missing a significant number of threats, which can have dire implications for an organization's security posture (Saranya et al., 2020). It is essential for organizations to balance the trade-off between false negatives and false positives to ensure comprehensive threat detection.

- *Precision*

Precision, also known as positive predictive value, measures the accuracy of the IDS in identifying true threats among all the alerts generated. It is calculated as follows:

$$Precision = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP)+False\ Positives\ (FP)}$$

High precision indicates that the IDS generates fewer false alerts, enhancing the credibility of the alerts that are issued (Georgescu, 2020, Hodge & Austin, 2004). This is particularly important in operational environments, such as maritime systems, where timely and accurate responses to alerts are critical.

- *Recall (Sensitivity)*

Recall, or sensitivity, measures the proportion of actual attacks that the IDS successfully identifies. It is synonymous with the detection rate, but it emphasizes the importance of recognizing true attacks within the overall context of the IDS's performance. Recall is calculated as:

$$Recall = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP)+False\ Negatives\ (FN)}$$

A high recall value indicates that the IDS is effective at capturing most attacks, thus preventing potential breaches and damages (Almaiah et al, 2022, Georgescu, T. M. 2020).

E. AI Techniques in Intrusion Detection

The increasing sophistication and frequency of cyberattacks necessitate the development of advanced Intrusion Detection Systems (IDS) capable of identifying and mitigating threats in real-time. Artificial Intelligence (AI) techniques have emerged as vital tools in enhancing the effectiveness of IDS by enabling the automation of threat detection processes, improving accuracy, and reducing false positive rates.

An Intrusion Detection System (IDS) is a security mechanism that continuously monitors the activities of a computer system or network to detect potential security breaches and notify the user. Figure 9 presents the components of a typical IDS. The IDS functions in three phases: data collection, detection, and response. During the data collection phase, events are generated from log data, which are derived from the target system. These data sources can include network traffic, operating system logs, and device logs.

In the detection phase, the analysis engine employs detection algorithms, using scripts to match text patterns associated with specific intrusions. This phase aims to distinguish between normal and abnormal behaviors within the target system. The final phase, the response stage, processes the information about events classified as normal or abnormal and determines the appropriate action, such as alerting the system administrator, automatically reconfiguring the system to block the intruder, or offering response mechanisms for manual intervention.

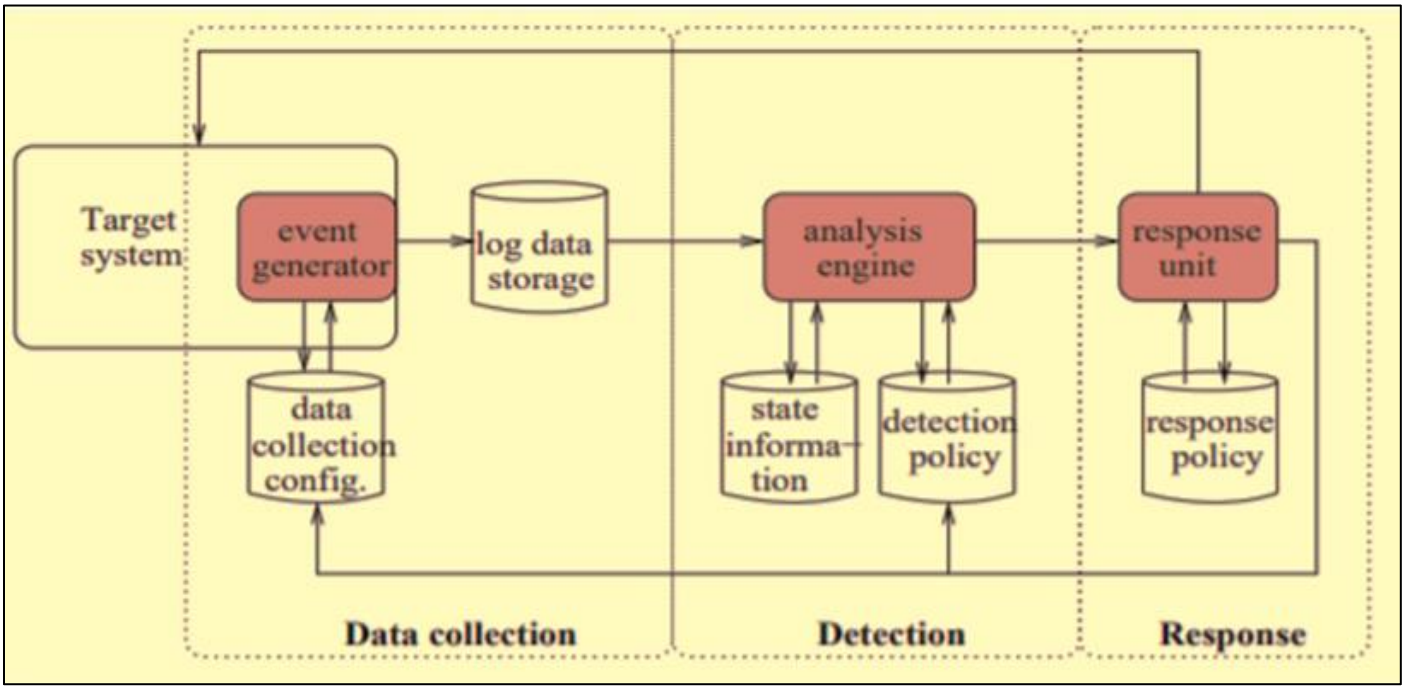

Fig 9 The Components of a General IDS.
Source: Almaiah et al., (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels.

This section discusses three AI techniques employed in intrusion detection, specifically machine learning, deep learning, and natural language processing.

➢ *Machine Learning Approaches*

Machine learning (ML) is a subset of AI that involves training algorithms to recognize patterns in data. In the context of intrusion detection, ML algorithms can learn from historical data to identify normal behavior and detect anomalies that may indicate malicious activities. Common ML techniques used in IDS include supervised learning, unsupervised learning, and semi-supervised learning.

- *Supervised Learning:*

In supervised learning, models are trained on labeled datasets, where each data point is associated with a known outcome (i.e., normal or malicious). Techniques such as Support Vector Machines (SVM), Decision Trees, and Random Forests are frequently used. These models excel in detecting known threats but may struggle with novel attacks not represented in the training data (Saranya et al., 2020).

- *Unsupervised Learning:*

Unsupervised learning approaches do not rely on labeled datasets, making them particularly useful for identifying previously unknown attacks. Clustering algorithms, such as K-Means and DBSCAN, can group similar data points together, helping to reveal unusual patterns or outliers that may indicate an intrusion (Adu-Twum et al., 2024). This approach is especially beneficial in dynamic environments, such as maritime networks, where new types of attacks frequently emerge.

- *Semi-Supervised Learning:*

Combining aspects of supervised and unsupervised learning, semi-supervised learning uses a small amount of labeled data along with a larger set of unlabeled data. This technique can significantly enhance detection performance when labeled examples are scarce, which is often the case in cybersecurity applications (Asharf et al., 2020).

Most Intrusion Detection Systems (IDS) follow a standard structure that consists of: (1) a data collection module that gathers data potentially containing evidence of an attack, (2) an analysis module that identifies attacks by processing the data, and (3) a reporting mechanism for alerting about the attack. In the data collection module, input data from various parts of IoT systems are collected and analyzed to establish patterns of normal behavior, enabling the detection of malicious activities at an early stage. The analysis module can utilize different techniques, but machine learning (ML) and deep learning (DL) approaches are particularly effective and widely used. These methods are capable of learning both normal and abnormal behaviors based on interactions between IoT devices and systems. Moreover, ML/DL techniques can anticipate new types of attacks, even those that differ from previously encountered ones, by learning from existing legitimate samples to predict future, unknown threats. Figure 10 illustrates the components of a typical IDS utilizing ML/DL methods.

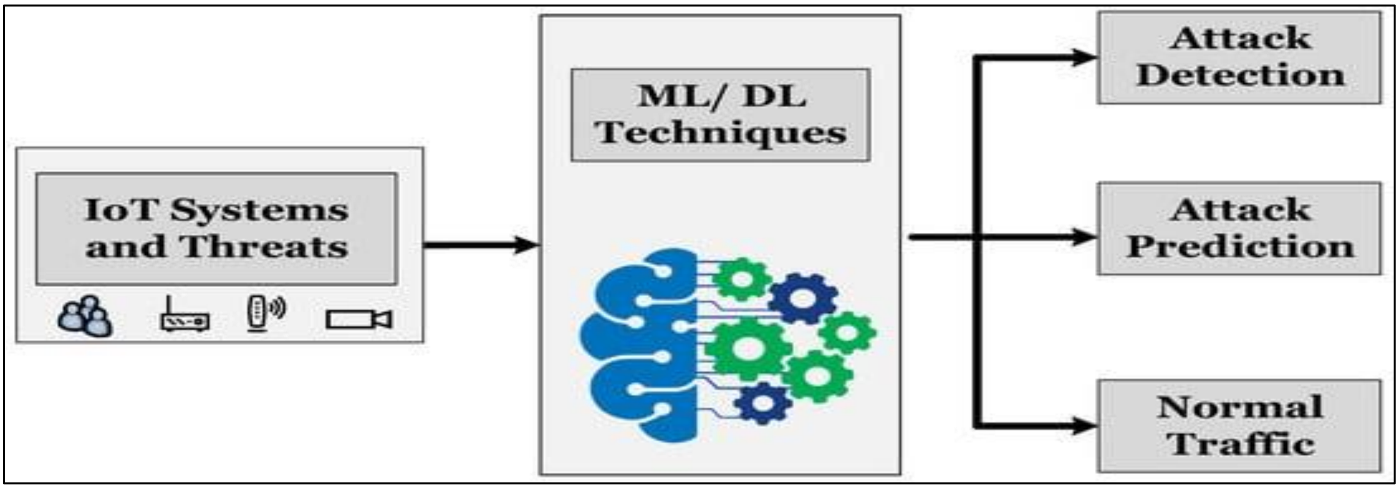

Fig10 Role of Machine Learning/Deep Learning (ML/DL) Based IDS for IoT system.
Source: Asharf, J., et al (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions.

➢ *Deep Learning Techniques*

Deep learning, a more advanced subset of machine learning, utilizes neural networks with multiple layers to model complex patterns in data. Deep learning techniques have shown promise in improving intrusion detection capabilities due to their ability to handle vast amounts of data and automatically extract relevant features (Almaiah et al, 2022).

- *Convolutional Neural Networks (CNNs):*

CNNs are particularly effective in analyzing structured data, such as network traffic and logs. They can learn spatial hierarchies of features, making them suitable for detecting sophisticated attack patterns that might be missed by traditional methods (Oyebanji et al., 2024).

- *Recurrent Neural Networks (RNNs):*

RNNs, including Long Short-Term Memory (LSTM) networks, excel at processing sequential data. In the context of IDS, they can analyze time-series data from network traffic to identify trends and patterns indicative of attacks, making them particularly effective for detecting ongoing attacks (Pitropakis et al., 2020).

➢ *Natural Language Processing (NLP)*

Natural Language Processing (NLP) techniques are increasingly being applied to intrusion detection systems, particularly for analyzing logs and textual data generated by network devices. NLP can help convert unstructured log data into structured information, enabling more effective analysis (Georgescu, 2020).

- *Text Classification:*

Using techniques like bag-of-words and word embeddings, NLP models can classify logs based on their content, identifying abnormal entries that may signify security incidents (Chen et al., 2021). By automating the analysis of large volumes of log data, organizations can enhance their ability to detect and respond to incidents in real time.

- *Sentiment Analysis*:

Although primarily used in social media and customer feedback analysis, sentiment analysis techniques can also be adapted for cybersecurity applications. By analyzing the tone and context of communication within a network, systems can identify potential insider threats or compromised accounts (Chen et al., 2021).

F. Applications of AI-Based IDS in Maritime

As maritime operations increasingly adopt digital technologies, the integration of Intrusion Detection Systems (IDS) has become crucial for safeguarding maritime networks against cyber threats. This section examines current implementations of IDS in the maritime industry and presents relevant case studies that illustrate their effectiveness in real-world scenarios.

➢ *Implementations of IDS in Maritime Operations*

The maritime industry is adopting a variety of IDS solutions tailored to meet the unique challenges posed by maritime environments. Key implementations include:

- *Network-Based Intrusion Detection Systems (NIDS):*

NIDS monitor network traffic for suspicious activities and are widely used in maritime operations. For example, the Royal Navy has adopted NIDS to secure communications between ships and shore-based facilities. By analyzing network packets in real time, the system can detect unauthorized access attempts and potential malware (Ali et al., 2020).

- *Host-Based Intrusion Detection Systems (HIDS):*

HIDS operate on individual hosts or devices, monitoring system calls, file modifications, and application logs. The shipping company Maersk implemented HIDS across its fleet to enhance endpoint security, ensuring that each vessel's onboard systems are protected from internal and external threats (Mishra et al., 2024).

- *Anomaly Detection Systems:*

Many maritime organizations are utilizing anomaly detection techniques that uses machine learning to identify deviations from normal operational patterns. For instance, a case study involving the Port of Rotterdam demonstrated the application of an anomaly detection model to monitor shipping data and flag unusual behavior that could indicate cyber intrusions (Jović et al., 2019).

G. Case Studies of IDS in Maritime Cybersecurity

➢ *Case Study: Maersk's Cybersecurity Strategy*

Following the NotPetya ransomware attack in 2017, Maersk recognized the critical need to enhance its cybersecurity posture. The company implemented a comprehensive IDS solution that combined NIDS and HIDS across its global operations. This multi-layered approach enabled real-time threat detection and improved response times to security incidents. Maersk's investment in advanced IDS technologies not only helped in mitigating the impact of future attacks but also ensured compliance with international cybersecurity regulations, such as the International Maritime Organization (IMO) guidelines (Mishra et al., 2024).

➢ *Case Study: The Port of Rotterdam*

The Port of Rotterdam, one of the busiest ports in the world, has adopted advanced cybersecurity measures, including IDS, to protect its critical infrastructure. The port implemented a hybrid IDS that utilizes both signature-based and anomaly-based detection methods. By continuously analyzing traffic patterns and user behavior, the system can identify potential cyber threats before they cause significant disruptions. This proactive approach has proven effective in safeguarding the port's operations against emerging cyber threats (Jović et al., 2019).

➢ *Case Study: Royal Caribbean International*

Royal Caribbean International has integrated IDS within its operational technology (OT) environment to secure its fleet against cyber threats. By employing both HIDS and NIDS, the company monitors communications and interactions between shipboard systems and external networks. This implementation has been crucial in identifying unauthorized access attempts and ensuring the integrity of critical onboard systems. The case highlights the importance of IDS in the cruise industry, where maintaining secure and reliable operations is essential for passenger safety and business continuity (Ali et al., 2020).

H. How AI-Driven Intrusion Detection Systems Can Adapt to Extreme Environmental Conditions

Artificial Intelligence (AI) has emerged as a powerful tool for enhancing Intrusion Detection Systems (IDS), particularly in environments subject to extreme conditions, such as maritime operations. The application of AI in IDS enables systems to adapt dynamically to various challenges, improving their effectiveness in detecting and mitigating cyber threats. This section provides analyses on how AI-driven IDS can adapt to extreme environmental conditions, focusing on their capabilities to analyze data, learn from patterns, and respond to specific threats.

➢ *Real-Time Data Processing and Anomaly Detection*

AI-driven IDS can process vast amounts of data in real-time, allowing them to identify unusual patterns and behaviors that may signify potential threats. In maritime environments, where operational conditions can be unpredictable due to factors such as weather and geographical isolation, the ability to quickly analyze incoming data streams is critical. Machine learning algorithms can continuously learn from new data, improving their accuracy over time (Almaiah et al, 2022). For instance, a study by Kim et al. (2021) demonstrated that an AI-based IDS could successfully identify anomalies in network traffic during extreme weather conditions, allowing for timely interventions and reduced risk of cyber incidents.

- *Adaptive Learning and Continuous Improvement*

One of the significant advantages of AI-driven IDS is their ability to learn and adapt to new threats. Through techniques such as reinforcement learning, these systems can modify their detection strategies based on the evolving nature of cyber threats. In maritime settings, where environmental conditions can drastically impact network performance and system behavior, AI-driven IDS can adjust their algorithms to accommodate these variations. For example, an AI-based system may recognize that certain communication patterns are more prevalent during storms and adjust its detection criteria accordingly, thus minimizing false positives and ensuring relevant alerts (Elsayed et al., 2022).

- *Contextual Awareness and Environmental Adaptation*

AI-driven IDS can be designed to incorporate contextual awareness, allowing them to consider environmental factors when assessing network security. This capability is particularly important in maritime environments, where factors like geographical location, vessel type, and operational status can influence vulnerability to cyber threats. By utilizing contextual data, AI systems can enhance their detection capabilities and provide tailored security responses (Ghaleb et al., 2022). For instance, a case study by Ali et al. (2020) illustrated that an AI-driven IDS employed in a maritime operation could adjust its alert thresholds based on the vessel's operational state and environmental conditions, improving the accuracy and relevance of security alerts.

- *Resilience to Environmental Disruptions*

Extreme environmental conditions, such as severe weather events or physical obstructions, can disrupt communication and data transmission in maritime settings. AI-driven IDS can enhance resilience by employing decentralized architectures and edge computing strategies. These approaches enable data processing and analysis to occur closer to the source of data, minimizing the impact of connectivity issues (Ashraf et al., 2020). For example, a maritime operation utilizing edge computing with AI-driven IDS demonstrated improved performance in detecting anomalies during adverse weather conditions, ensuring continuous monitoring and rapid threat response.

IV. NETWORK AUTOMATION IN MARITIME CYBERSECURITY

A. *Role of Network Automation*

The maritime industry is increasingly embracing automation to enhance the efficiency and security of its networks. As digital technologies and interconnected systems become more prevalent, automation plays a critical role in managing maritime operations and safeguarding sensitive data. This section reveals the importance of automation in managing maritime networks and securing data, highlighting the benefits, challenges, and recent advancements in this field.

- *Enhancing Operational Efficiency*

Automation in maritime networks enables organizations to streamline operations and optimize resource allocation. Automated systems can monitor network performance, detect anomalies, and facilitate rapid decision-making. For instance, vessel traffic services (VTS) have integrated automated systems to track and manage ship movements, ensuring safe navigation and efficient port operations (Wei et al., 2021). Such automation not only reduces human error but also enhances the overall safety and efficiency of maritime activities.

- *Automated Intrusion Detection and Response*

Automated Intrusion Detection Systems (IDS) are essential for identifying and mitigating cyber threats in maritime networks. By employing machine learning algorithms, these systems can analyze vast amounts of network traffic in real time to detect malicious activities. For example, recent research by Sowmya & Anita, (2023) demonstrated an automated IDS specifically designed for maritime operations, capable of identifying unauthorized access attempts and quickly responding to potential threats. The automation of threat detection and response mechanisms reduces the reliance on human intervention, allowing security teams to focus on more strategic tasks.

- *Data Security and Compliance*

With the growing reliance on digital technologies, securing sensitive data in maritime operations has become paramount. Automation can help enforce security policies and ensure compliance with regulatory standards. Automated data encryption, access controls, and monitoring systems can protect critical information from unauthorized access and data breaches. A study by Jones et al (2016) emphasized the effectiveness of automated data security measures in maritime environments, highlighting how these systems can enforce compliance with international regulations, such as the International Maritime Organization’s (IMO) guidelines.

- *Integration of Internet of Things (IoT) Technologies*

The integration of IoT devices in maritime operations presents both opportunities and challenges for data management and security. Automated systems can facilitate the secure management of data generated by IoT devices, ensuring that information is collected, transmitted, and stored securely. For instance, IoT sensors deployed on vessels can monitor environmental conditions, equipment status, and operational metrics. An automated data management system can analyze this data in real time, providing insights for optimizing operations and enhancing safety (Chi et al., 2020).

Cyber-physical systems in the maritime sector involve the integration of information technology (IT) and operational technology (OT) systems, along with human factor considerations. This integration, illustrated in Figure 11a, defines cyber-physical systems and encompasses most onboard systems of maritime vessels. Figure 11b presents a simplified diagram of the communication pathways between shore-based and vessel-based stakeholders and IT/OT platforms, highlighting the interaction between IT and OT systems. Maritime vessels, managed by human operators, contain an interface between IT and OT systems that links processes, systems, components, and both technical and operational performance. A naval vessel can be seen as a system of systems, equipped with IT and OT devices. The crew operates these systems and is responsible for ensuring the vessel's overall operational and performance integrity.

Similarly, shipping companies maintain an IT interface that supports vessels technically and operationally, with human operators using IT systems to achieve performance and financial objectives that support maritime operations. Ports interact with vessels on both a shore-to-ship and ship-to-shore level, handling the loading and unloading of maritime goods. This process relies on a combination of IT and OT platforms, such as cargo management systems, cranes, and utilities. These platforms support maritime assets technically and operationally, with human operators managing and configuring the cyber-physical systems. Maintenance of OT devices and systems is performed either physically or remotely (Progoulakis, et al., 2021).

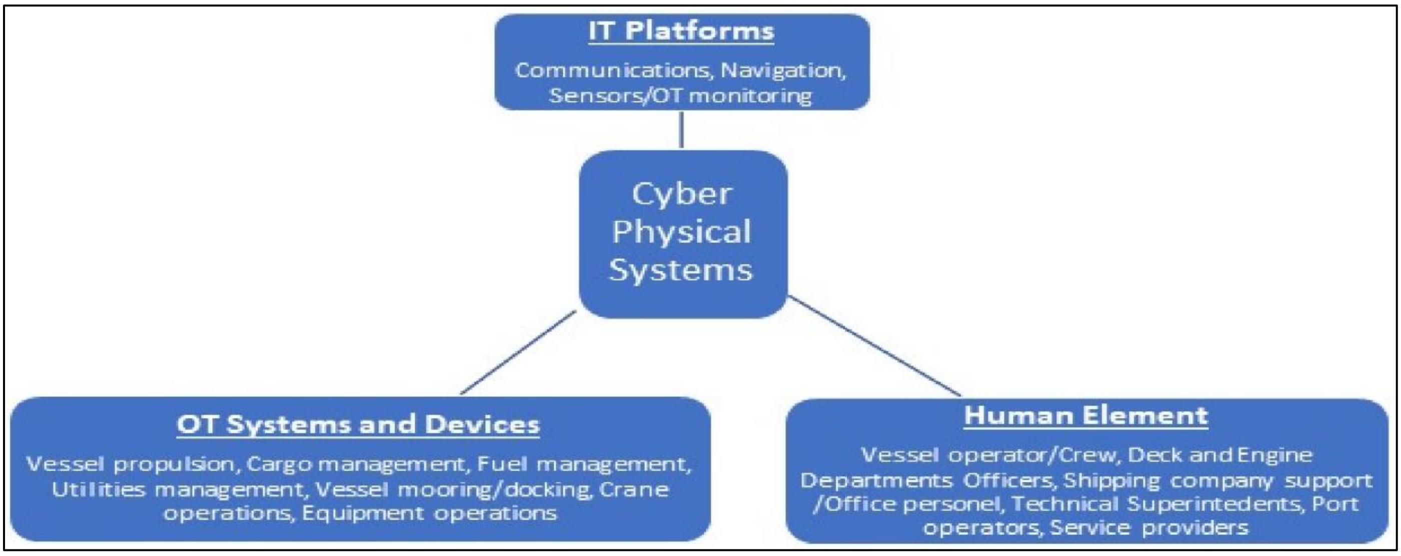
IT Platforms
Communications, Navigation, Sensors/OT monitoring
Cyber Physical Systems
OT Systems and Devices
Vessel propulsion, Cargo management, Fuel management, Utilities management, Vessel mooring/docking, Crane operations, Equipment operations
Human Element
Vessel operator/Crew, Deck and Engine Departments Officers, Shipping company support /Office personel, Technical Superintedents, Port operators, Service providers

Fig 11a IT, OT, and human element interface in cyber physical systems.
Source: Progoulakis, et al., (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), 1384.

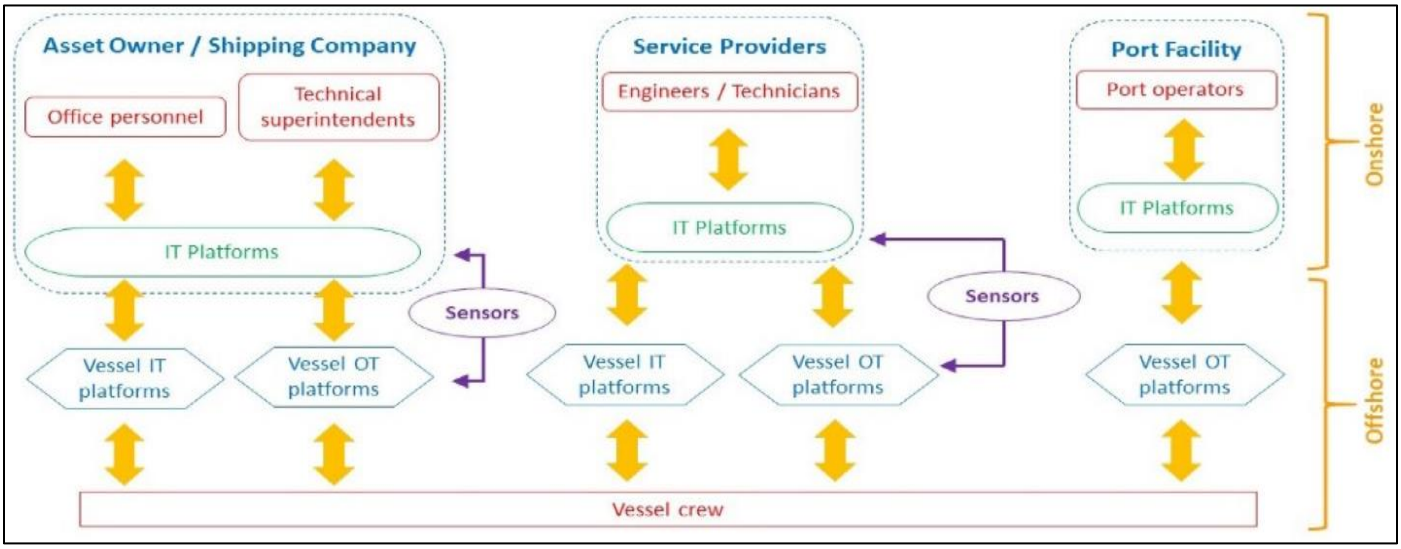

Fig 11b Communication paths of shore-based and vessel-based stakeholders and IT/OT platforms.
Source: Progoulakis, et al., (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), 1384.

B. Autonomous Decision-Making for Responding to Cyber Threats

As the maritime industry becomes increasingly reliant on digital technologies, the potential for cyber threats has escalated significantly. Autonomous decision-making systems are emerging as critical tools for responding to these threats, enabling organizations to react swiftly and effectively to cybersecurity incidents. This section exposes the concept of autonomous decision-making in the context of cyber threat response, highlighting its importance, methodologies, and challenges.

➢ *The Need for Autonomous Decision-Making*

Cyber threats in maritime environments can arise from various sources, including malware, phishing, and Distributed Denial of Service (DDoS) attacks. These threats can disrupt operations, compromise sensitive data, and endanger safety (Maddireddy & Maddireddy, 2022). Traditional response mechanisms often rely on human intervention, which can introduce delays and increase the likelihood of errors in high-pressure situations. Autonomous decision-making systems can mitigate these issues by providing rapid, data-driven responses to detected threats, thus enhancing the resilience of maritime operations (Tinga et al., 2017).

➢ *Methodologies for Autonomous Decision-Making*

- *Machine Learning and Artificial Intelligence*

Machine learning (ML) and artificial intelligence (AI) techniques are at the forefront of autonomous decision-making systems. These technologies enable the analysis of vast amounts of data to identify patterns and anomalies indicative of cyber threats. For example, an AI-driven system can continuously monitor network traffic, learning from previous attacks to improve its detection capabilities and automate responses (Almaiah et al, 2022). Research by Tinga et al. (2017) demonstrated that an ML-based autonomous system could effectively classify cyber threats in real-time, facilitating immediate countermeasures without human intervention.

- *Rule-Based Systems*

In addition to ML and AI, rule-based systems are commonly employed in autonomous decision-making. These systems use predefined rules to assess potential threats and determine appropriate responses. For instance, a rule-based IDS might automatically isolate a compromised device from the network to prevent further spread of an attack (Wei et al., 2021). While less adaptable than AI-driven systems, rule-based approaches can be effective in environments where threat scenarios are well-understood.

➢ *Autonomous Incident Response Strategies*

Autonomous decision-making can facilitate several incident response strategies:

- *Automated Threat Containment:*

Upon detection of a threat, an autonomous system can automatically implement containment measures, such as blocking malicious IP addresses or quarantining affected systems. This immediate response helps prevent the escalation of incidents and minimizes damage (Uzoma et al., 2023).

- *Dynamic Risk Assessment:*

Autonomous systems can perform real-time risk assessments based on the current threat landscape and organizational context. This capability enables them to prioritize responses and allocate resources more effectively (Ray et al., 2013).

The API STD 780 SRA methodology assesses and allows for the management of security risks through a risk-based, performance-oriented management process aimed at the protection and security of assets, people, and the environment (Progoulakis, et al., 2021). The SRA is a five-step process involving characterization, threat assessment, vulnerability assessment, risk evaluation and risk treatment as shown in Figure 12.

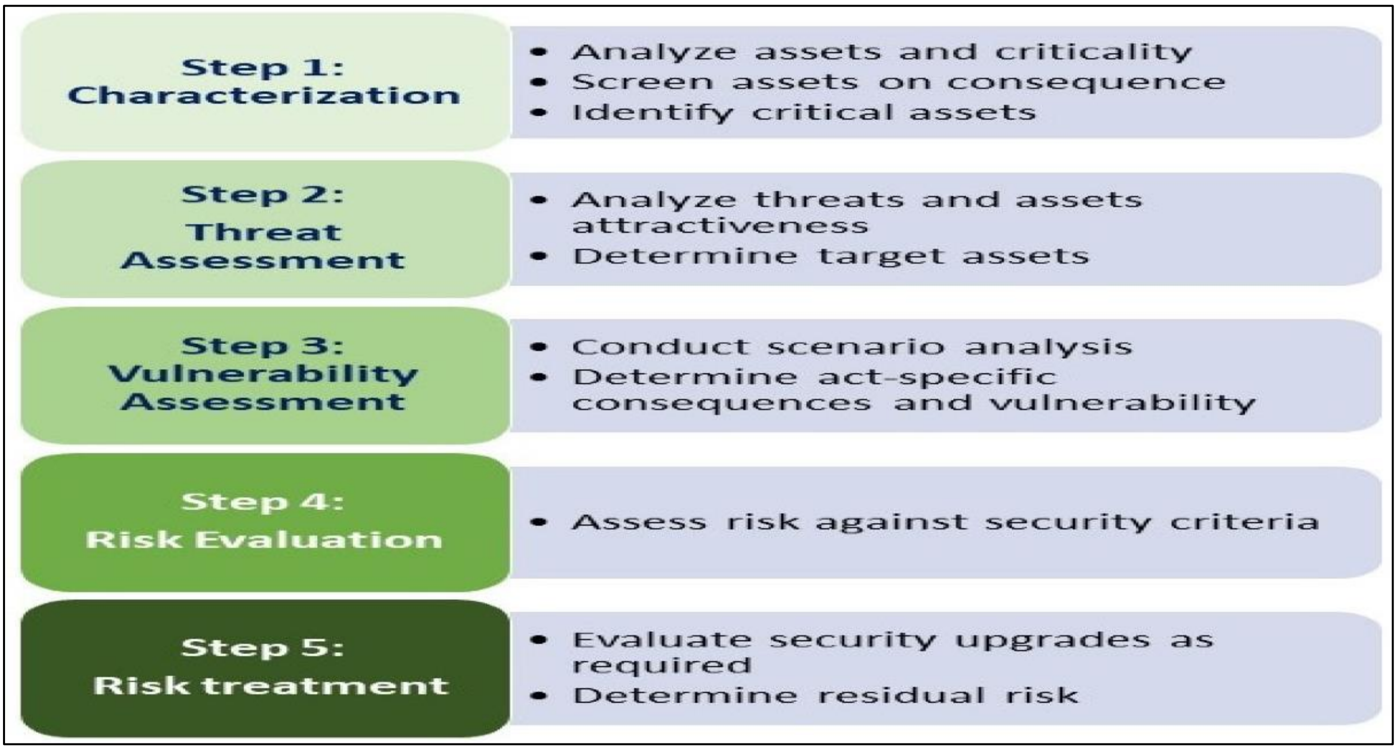
Step 1: Characterization
• Analyze assets and criticality
• Screen assets on consequence
• Identify critical assets
Step 2: Threat Assessment
• Analyze threats and assets attractiveness
• Determine target assets
Step 3: Vulnerability Assessment
• Conduct scenario analysis
• Determine act-specific consequences and vulnerability
Step 4: Risk Evaluation
• Assess risk against security criteria
Step 5: Risk treatment
• Evaluate security upgrades as required
• Determine residual risk

Fig 12 API SRA Method of Security Risk Management.
Source: Progoulakis, et al., (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), 1384.

- *Incident Recovery and Forensics:*

After a cyber incident, autonomous systems can assist in recovery efforts by restoring affected systems and analyzing logs for forensic purposes. This process is essential for understanding the attack and preventing future incidents (Maddireddy & Maddireddy, 2022).

➢ *Challenges in Autonomous Decision-Making*

While the benefits of autonomous decision-making for responding to cyber threats are evident, several challenges must be addressed:

- *Trust and Transparency:*

Organizations must develop trust in autonomous systems, which can be difficult when the decision-making process is opaque. Ensuring that stakeholders understand how decisions are made is critical for fostering confidence in these systems (Ibokette et al., 2024).

- *False Positives and Negatives:*

Autonomous systems are not infallible and can generate false positives or negatives, leading to unnecessary disruptions or missed threats. Continuous training and refinement of algorithms are essential to minimize these occurrences (Almaiah et al, 2022).

- *Ethical Considerations:*

The use of autonomous systems in cybersecurity raises ethical questions regarding accountability and responsibility for decisions made by machines. Establishing clear guidelines for accountability is crucial as these technologies become more prevalent (Tinga et al., 2017).

C. *Technologies Enabling Network Automation*

Network automation has become a cornerstone of modern maritime operations, driven by the need for increased efficiency, enhanced security, and streamlined management of complex systems. Various technologies play a pivotal role in enabling network automation, allowing organizations to automate routine tasks, optimize network performance, and respond to cybersecurity threats in real time. This section discusses the key technologies that facilitate network automation in the maritime industry.

➢ *Software-Defined Networking (SDN)*

Software-Defined Networking (SDN) is a revolutionary approach that decouples the network control plane from the data plane, allowing for centralized management and dynamic configuration of network resources. SDN enables maritime organizations to automate network provisioning, monitoring, and management, significantly improving flexibility and scalability (Cardona et al., 2020). For example, in maritime contexts, SDN can facilitate the dynamic allocation of bandwidth to different vessels based on real-time demands, ensuring optimal utilization of network resources (Simion et al., 2024).

➢ *Network Functions Virtualization (NFV)*

Network Functions Virtualization (NFV) complements SDN by virtualizing network functions that traditionally run on dedicated hardware. By deploying network functions as software applications on standard hardware, NFV allows maritime organizations to reduce costs and enhance operational agility (Cardona et al., 2020). NFV enables the automated deployment of services such as firewalls, intrusion detection systems, and load balancers, making it easier to adapt to changing operational requirements and improve overall network performance.

➢ *Artificial Intelligence and Machine Learning*

Artificial Intelligence (AI) and Machine Learning (ML) technologies are integral to automating network management and security. AI algorithms can analyze network traffic patterns to detect anomalies, identify potential threats, and optimize performance (Ibokette et al., 2024). For instance, an AI-driven system can automate incident response by dynamically adjusting security policies based on real-time threat assessments (Katterbauer, 2022). Additionally, AI can enhance predictive analytics, allowing organizations to foresee network issues and proactively address them before they escalate into critical incidents.

➢ *Internet of Things (IoT)*

The Internet of Things (IoT) plays a crucial role in enabling network automation by connecting a myriad of devices and sensors to maritime networks. IoT devices generate vast amounts of data, which can be used to automate various processes, from monitoring equipment status to tracking environmental conditions. For example, IoT sensors on vessels can provide real-time data on fuel consumption, enabling automated adjustments to optimize fuel efficiency (Chi et al., 2020). Furthermore, the integration of IoT with network automation allows for more responsive and adaptive networks, enhancing situational awareness and operational efficiency.

➢ *Cloud Computing*

Cloud computing provides a flexible and scalable infrastructure for deploying automated network services. By using cloud resources, maritime organizations can automate the deployment and management of applications, data storage, and analytics tools without the need for extensive on-premises hardware (Ahmad et al., 2023). Cloud-based automation solutions can streamline processes such as software updates, data backups, and security monitoring, allowing organizations to focus on their core operations while maintaining a secure and efficient network environment.

D. *Resilience During Extreme Environmental Conditions*

Ensuring reliable connectivity and optimal system performance in harsh maritime environments is critical for the safety and efficiency of maritime operations. The unique challenges posed by extreme weather conditions, geographical isolation, and the inherent complexities of maritime systems necessitate the integration of automation technologies. This section reveals how automation can enhance connectivity and system performance in these demanding environments.

- *Challenges of Harsh Maritime Environments*

Maritime operations face numerous challenges, including severe weather, high waves, and extreme temperatures, which can adversely affect connectivity and system performance. For instance, strong winds and heavy rainfall can disrupt satellite communications and degrade signal quality, leading to potential data loss or latency (Wei et al., 2021). Additionally, the corrosive nature of marine environments can impact the physical integrity of communication systems, further complicating the maintenance of reliable connectivity (Chi et al., 2020).

- *Automation for Network Resilience*

Automation plays a vital role in enhancing network resilience in harsh maritime conditions. Automated network management systems can continuously monitor network performance and adaptively allocate resources to ensure stable connectivity. For example, intelligent traffic management systems can dynamically adjust bandwidth allocation based on real-time demands, ensuring that critical communications remain intact even during adverse conditions (Sowmya & Anita 2023). Furthermore, automated failover mechanisms can reroute data traffic through alternative pathways if primary connections are compromised, thereby minimizing disruptions (Ghaleb et al., 2022).

- *Predictive Maintenance and Monitoring*

Predictive maintenance, enabled by automation and IoT technologies, is crucial for maintaining connectivity and system performance in harsh environments. Automated monitoring systems can collect and analyze data from various sensors deployed throughout maritime equipment and communication infrastructure. By using machine learning algorithms, these systems can predict potential failures and recommend maintenance actions before issues escalate (Ibokette et al., 2024). For instance, predictive analytics can identify wear and tear in communication equipment, allowing timely interventions that ensure continued operational efficiency (Sowmya & Anita 2023**)**.

- *Adaptive Communication Protocols*

Automated systems can also facilitate the use of adaptive communication protocols that adjust to changing environmental conditions. For example, software-defined networking (SDN) can enable the reconfiguration of communication pathways in response to signal degradation due to weather impacts. This adaptability ensures that maritime operations maintain connectivity even when faced with challenging conditions (Cardona et al., 2020). By automating these adjustments, organizations can minimize manual intervention and enhance the reliability of their communication systems.

- *Data Integrity and Security*

In harsh maritime environments, ensuring data integrity and security is paramount. Automated systems can implement robust cybersecurity measures that protect data transmitted over potentially vulnerable connections. For instance, end-to-end encryption and automated intrusion detection systems can safeguard communications from interception or tampering, ensuring that critical information remains secure (Tinga et al., 2017). The automation of security protocols also enables real-time threat detection and response, further enhancing the resilience of maritime networks against cyber threats.

E. Case Studies of Automation in Adverse Maritime Conditions

Automation in maritime operations has been increasingly recognized as a critical solution for overcoming challenges posed by adverse environmental conditions. This section discusses several case studies that demonstrate the effective implementation of automation technologies in enhancing operational resilience, safety, and efficiency in harsh maritime settings.

- *Autonomous Vessels in Extreme Weather Conditions*

One prominent case study involves the use of autonomous vessels for operations in severe weather conditions. The Yara Birkeland, an autonomous container ship, is designed to transport goods without a crew, aiming to reduce emissions and enhance safety (Rødseth et al., 2023). During trials, the vessel operated in rough sea conditions, utilizing advanced automation technologies for navigation and obstacle avoidance. The ship's automation systems continuously monitored environmental data, allowing it to adjust its course and speed dynamically to maintain safety and efficiency during storms (Evensen 2020). This case illustrates how automation can enhance operational safety in extreme maritime environments by enabling real-time decision-making.

In Figure 13, the Instrument Layer, positioned at the base, includes navigational sensors such as AIS and GNSS, which are essential for navigational awareness, along with internal automation sensors that monitor parameters like pressure, temperature, torque, and vibration, as well as actuators that manage the ship's machinery operations. These sensors and actuators are grouped by their functions at the Process Layer and connected to system components within the Integrated Ship Control Layer, where key ship operations are conducted. Above the Integrated Ship Control Layer is the General Ship Layer, where additional administrative functions like reporting and record-keeping are carried out. At the top of the architecture is the Off Ship Layer, which facilitates communication with external entities (Cho et al., 2022).

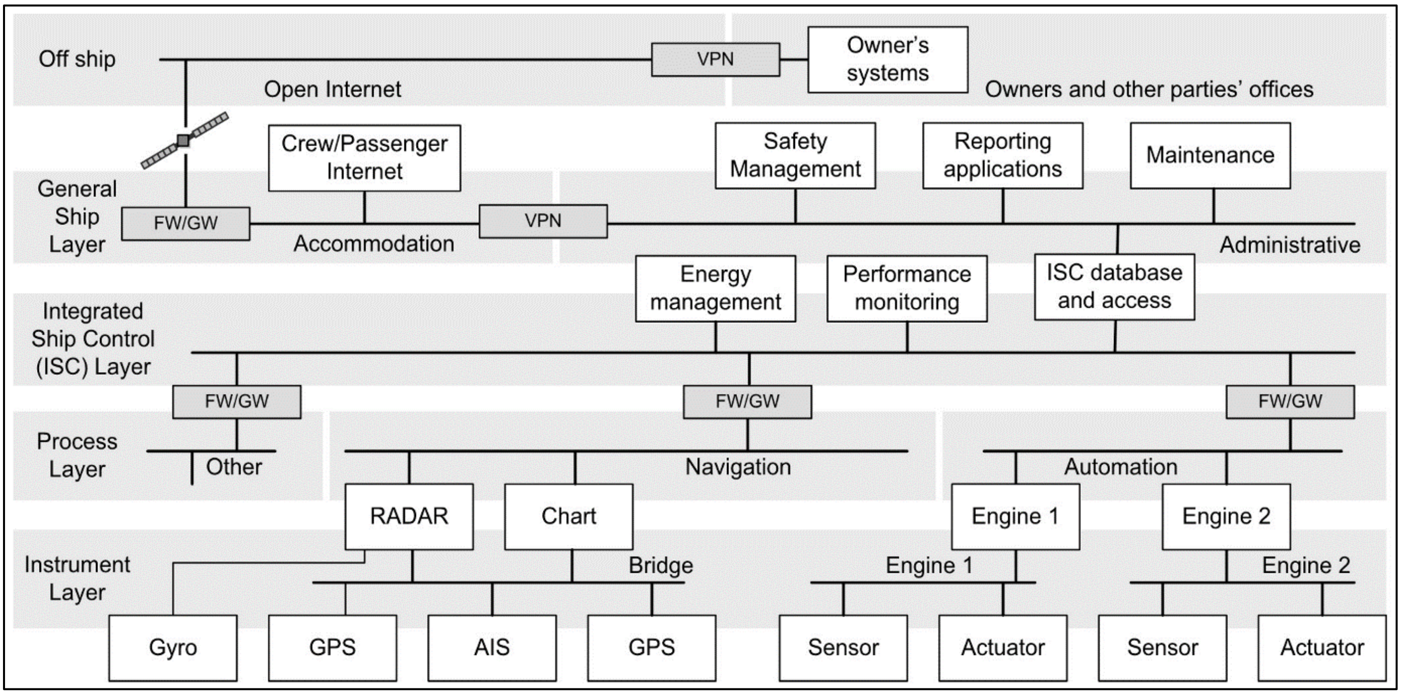

Fig 13 Architectural Overview f Unmanned Ships
Source: Cho, S., et al., (2022). Cybersecurity Considerations in Autonomous Ships.

➢ *Automated Monitoring Systems for Offshore Platforms*

Another case study is the implementation of automated monitoring systems on offshore oil platforms, where harsh weather conditions and corrosive environments pose significant operational challenges. The Equinor-operated Johan Sverdrup field in the North Sea employs automated monitoring technologies that utilize IoT sensors to collect real-time data on equipment performance and environmental conditions (Ibokette et al., 2024). These systems automate data analysis and anomaly detection, enabling proactive maintenance actions and reducing the risk of operational failures during severe weather events. The automated systems have improved safety and efficiency by facilitating remote monitoring and reducing the need for personnel to operate in hazardous conditions.

➢ *Predictive Maintenance in Fishing Vessels*

The fishing industry is another area where automation has proven beneficial in adverse conditions. The case of the commercial fishing vessel *Ocean Harvest* illustrates the implementation of predictive maintenance solutions to ensure equipment reliability during harsh weather. The vessel utilizes an automated monitoring system that collects data on engine performance, temperature, and vibration levels (Ibokette et al., 2024). By applying machine learning algorithms, the system predicts potential failures and schedules maintenance before critical breakdowns occur. This approach has allowed the vessel to maintain operational readiness and reduce downtime, even in adverse weather conditions, thereby enhancing overall fishing efficiency.

➢ *Automated Traffic Management Systems*

The Port of Rotterdam has implemented an automated traffic management system to optimize maritime traffic flow in adverse weather conditions. The system uses real-time data from various sources, including weather forecasts, vessel traffic information, and port infrastructure conditions, to automate decision-making processes (Marks et al., 2013). During storms or foggy conditions, the automated system can reroute vessels and adjust schedules to minimize risks and delays. This automation not only improves safety by preventing collisions but also enhances operational efficiency by optimizing berth utilization and reducing turnaround times for vessels.

➢ *Remote-Controlled Drones for Search and Rescue Operations*

In maritime search and rescue operations, automation technologies have demonstrated their effectiveness in adverse conditions. The use of remote-controlled drones has been explored in various case studies, including operations conducted by the Norwegian Coast Guard. Drones equipped with advanced sensors and imaging technologies are deployed to survey large areas of ocean during search missions, even in challenging weather (Panić et al., 2021). The drones can relay real-time data to command centres, facilitating faster decision-making and more efficient search patterns. This automation enhances the Coast Guard's ability to respond to emergencies in harsh maritime environments while minimizing the risk to personnel.

V. CHALLENGES AND LIMITATIONS

A. *Technical Challenges in Maritime Cybersecurity and Automation*

The integration of automation and cybersecurity solutions in maritime operations presents a myriad of technical challenges. These challenges arise from the unique characteristics of maritime environments, the complexity of maritime systems, and the ever-evolving landscape of cyber threats. This section reveals some of the key technical challenges that maritime organizations face when implementing automated systems and cybersecurity measures.

- *Legacy Systems Integration*

One of the significant technical challenges in maritime operations is the integration of new automation and cybersecurity technologies with legacy systems. Many vessels and maritime infrastructure still rely on outdated technologies that were not designed with modern cybersecurity threats in mind (Ibokette et al., 2024). Integrating automated solutions with these legacy systems often requires significant customization, which can lead to increased costs and extended implementation timelines (Progoulakis et al., 2021). Moreover, the lack of interoperability between legacy and modern systems can create vulnerabilities, making it difficult to ensure a seamless and secure operational environment.

- *Data Management and Analytics*

The maritime industry generates vast amounts of data from various sources, including sensors, navigation systems, and environmental monitoring tools. Effectively managing and analyzing this data presents a significant technical challenge (Idoko et al., 2024). Automated systems require robust data management frameworks to ensure data integrity, accuracy, and accessibility. Moreover, the analysis of large datasets often necessitates advanced machine learning and artificial intelligence algorithms, which can be complex to implement and optimize for specific maritime applications (Ijiga et al., 2024). The challenge lies not only in processing this data in real-time but also in deriving actionable insights that enhance decision-making.

- *Cybersecurity Threat Landscape*

The maritime sector faces a diverse range of cybersecurity threats, including malware attacks, phishing attempts, and denial-of-service (DoS) attacks (Mishra et al., 2024). These threats are continually evolving, necessitating the implementation of advanced intrusion detection systems (IDS) and automated response mechanisms. However, developing effective IDS that can operate in the complex and dynamic maritime environment is a significant technical challenge (Al Ali et al., 2021). For instance, the high volume of legitimate data traffic can lead to false positives, where benign activities are incorrectly flagged as threats. Balancing sensitivity and specificity in IDS is crucial for ensuring operational continuity while maintaining security.

- *Limited Connectivity and Redundancy*

Maritime operations often take place in remote and isolated areas where connectivity can be limited or unreliable. This poses challenges for the deployment of automated systems that rely on constant data exchange and communication (Chi et al., 2020). In cases of limited connectivity, automated systems may struggle to receive updates or operate effectively, increasing the risk of operational failures. Furthermore, ensuring redundancy in communication pathways to maintain connectivity during adverse conditions is a technical challenge that requires careful planning and investment in infrastructure (Wei et al., 2021).

- *Environmental Factors*

Harsh environmental conditions, such as extreme weather, high salinity, and temperature fluctuations, can adversely affect the performance of automated systems and communication equipment. Corrosion, signal degradation, and equipment failure are common issues faced in maritime environments (Sowmya & Anita 2023). Designing automation solutions that are resilient to these factors requires extensive testing and validation under various environmental conditions. Additionally, maintaining the reliability of sensor systems and communication links in such settings adds to the complexity of system design and implementation (Ibokette et al., 2024).

- *Regulatory Compliance*

Compliance with maritime regulations and standards presents another technical challenge. Various international and national regulations govern cybersecurity practices in maritime operations, including the International Maritime Organization (IMO) guidelines and the General Data Protection Regulation (GDPR) (Mishra et al., 2024). Ensuring that automated systems meet these regulatory requirements often involves intricate technical considerations, such as data protection measures and reporting protocols. Organizations must also stay updated with evolving regulations, which can necessitate frequent adjustments to their cybersecurity frameworks and automation systems.

B. *Operational Challenges in Maritime Cybersecurity and Automation*

The maritime industry is undergoing a significant transformation with the integration of automation and cybersecurity technologies. However, several operational challenges impede the successful implementation and utilization of these innovations. This section outlines key operational challenges faced by maritime organizations in their efforts to enhance cybersecurity and automation.

- *Skilled Workforce Shortage*

One of the foremost operational challenges in the maritime sector is the shortage of skilled personnel capable of managing and maintaining advanced automated systems and cybersecurity measures. Many maritime organizations struggle to find employees with the requisite knowledge in cybersecurity, data analysis, and automation technologies (Dasgupta et al., 2022). This skills gap can hinder the effective deployment and operation of automated systems, as well-trained personnel are essential for monitoring, troubleshooting, and ensuring compliance with cybersecurity protocols (Fruth & Teuteberg, 2017). The ongoing technological advancements further exacerbate this challenge, as existing workforce training programs may not keep pace with emerging technologies.

- *Integration of Systems and Processes*

Integrating new automated systems with existing maritime operations and processes poses a considerable operational challenge. Many maritime organizations rely on a diverse array of legacy systems and technologies that were not designed to work together seamlessly (Progoulakis et al., 2021). Ensuring compatibility between these systems and new automation solutions can lead to complications and increased operational risks. Additionally, the integration process often necessitates extensive testing and validation to ensure that all components function correctly together, which can be time-consuming and resource-intensive (Wei et al., 2023).

- *Cybersecurity Threats and Incident Response*

The dynamic nature of cybersecurity threats presents a significant operational challenge for maritime organizations. Cyberattacks are becoming increasingly sophisticated, and the maritime sector is a prime target due to its reliance on interconnected systems (Chi et al., 2020). Organizations must implement comprehensive cybersecurity frameworks and incident response plans to mitigate risks effectively.

However, the rapid evolution of cyber threats makes it challenging to keep security measures up to date (Al Ali et al., 2021). Additionally, incident response requires coordination among various stakeholders, which can complicate the process and lead to delays in addressing security breaches.

- *Operational Downtime and Recovery*

Operational downtime caused by cybersecurity incidents or failures in automated systems can significantly impact maritime operations. Unplanned outages can lead to financial losses, disruptions in supply chains, and reputational damage (Idoko et al., 2024). Organizations must establish robust contingency plans and recovery strategies to minimize the impact of such incidents. However, the effectiveness of these plans is often tested during real crises, revealing gaps in preparedness and response capabilities (Sowmya & Anita 2023). Continuous training and simulation exercises are necessary to ensure that personnel are equipped to handle emergencies effectively.

VI. FUTURE DIRECTIONS AND OPPORTUNITIES

A. Advances in AI for Cybersecurity

Artificial Intelligence (AI) has emerged as a transformative technology in the field of cybersecurity, significantly enhancing the ability of organizations to detect, respond to, and mitigate cyber threats. As cyber threats become increasingly sophisticated and pervasive, AI-driven solutions are proving essential for safeguarding sensitive data and ensuring operational continuity. This section outlines recent advances in AI technologies applied to cybersecurity, highlighting their impact, effectiveness, and future potential.

- *Enhanced Threat Detection*

One of the primary applications of AI in cybersecurity is threat detection. Machine learning algorithms are capable of analyzing vast amounts of data to identify patterns indicative of potential security breaches. For instance, anomaly detection systems utilize unsupervised learning techniques to establish baseline behavior for network activity and flag deviations that may signify an intrusion (Dasgupta et al., 2022). Research has shown that AI-based threat detection systems can significantly reduce false positives while improving the speed and accuracy of identifying potential threats (Akpan et al., 2022).

- *Predictive Analytics*

AI technologies are increasingly being used for predictive analytics in cybersecurity. By using historical data and machine learning models, organizations can forecast potential threats and vulnerabilities before they materialize. Predictive models analyze trends and patterns in cyber incidents, allowing organizations to take proactive measures to mitigate risks (Ijiga et al., 2024). For example, AI-driven threat intelligence platforms can aggregate data from multiple sources to predict emerging threats, helping organizations prioritize their security investments effectively (Pitropakis et al., 2020).

- *Automated Incident Response*

AI is revolutionizing incident response by enabling automation and orchestration of security protocols. Automated systems can respond to detected threats in real time, significantly reducing the response time to incidents (Uzoma et al., 2023). AI-driven Security Orchestration, Automation, and Response (SOAR) solutions integrate various security tools and streamline incident response processes, allowing security teams to focus on more complex threats. Studies indicate that organizations employing AI-driven automation experience a considerable reduction in incident response times, enhancing overall cybersecurity resilience (Uzoma et al., 2023).

- *User Behavior Analytics (UBA)*

User Behavior Analytics (UBA) employs AI algorithms to monitor user activity and detect anomalies that may indicate compromised accounts or insider threats. By establishing a baseline of normal user behavior, UBA systems can identify unusual patterns, such as unauthorized access or unusual data transfers (G. Martín et al., 2021). This capability is critical for organizations in preventing data breaches and ensuring compliance with regulatory standards, as it enables timely detection and mitigation of insider threats (Singh et al., 2020).

- *AI in Network Security*

AI is increasingly integrated into network security solutions to enhance the protection of critical infrastructure. AI-driven firewalls and intrusion detection systems can analyze network traffic in real time, adapting to new threats and evolving attack vectors (Sowmya & Anita 2023). These systems utilize machine learning algorithms to recognize legitimate traffic patterns, enabling them to block suspicious activity proactively. Research indicates that AI-powered network security solutions significantly enhance the overall security posture of organizations by reducing vulnerabilities and improving threat response (Ijiga et al., 2024).

B. Development of Maritime-Specific AI Models

The maritime industry is increasingly turning to artificial intelligence (AI) to enhance operational efficiency, safety, and security. However, the unique challenges and requirements of maritime operations necessitate the development of maritime-specific AI models tailored to address the sector's complexities. This section discloses the development of these specialized AI models, highlighting their applications, benefits, and the factors influencing their design.

- *Understanding Maritime-Specific Challenges*

Maritime operations encompass a range of activities, including navigation, logistics, and maintenance, all of which present unique challenges. These challenges include harsh environmental conditions, geographical isolation, complex regulatory frameworks, and the need for real-time decision-making (Fruth & Teuteberg, 2017). Consequently, AI models designed for the maritime industry must consider these factors to be effective. For example, models need to account for varying weather patterns, tidal changes, and navigational hazards that are critical for safe operations (Rawson & Brito, 2023).

- *Data Collection and Integration*

The development of maritime-specific AI models relies heavily on data collection from various sources, including satellite imagery, weather data, ship sensors, and AIS (Automatic Identification System) data. Integrating this diverse data into a cohesive framework is crucial for training AI models effectively. Researchers have emphasized the importance of high-quality, real-time data to enhance the predictive capabilities of maritime AI models (Dalaklis et al., 2023). Additionally, the integration of IoT (Internet of Things) devices on vessels allows for continuous data collection, enabling AI models to adapt to changing conditions in real time (Ibokette et al., 2024).

- *Machine Learning Techniques for Maritime Applications*

Several machine learning techniques have been successfully applied to develop maritime-specific AI models. For instance, supervised learning algorithms are commonly used for predictive maintenance by analyzing historical data to forecast equipment failures (Simion et al., 2024). Unsupervised learning techniques, such as clustering, are utilized to identify anomalies in vessel behavior, which can indicate potential security threats or operational inefficiencies (Adu-Twum et al., 2024). Furthermore, reinforcement learning is being explored for optimizing route planning and fuel efficiency, enabling vessels to navigate more efficiently under varying conditions (Dasgupta et al., 2022).

- *AI for Predictive Analytics in Maritime Operations*

Predictive analytics powered by AI is transforming maritime operations by enabling organizations to anticipate potential issues before they arise. For example, AI models can analyze historical voyage data to predict delays caused by weather conditions or port congestion (Mao & Larsson, 2023). This capability not only enhances operational efficiency but also improves customer satisfaction by providing more accurate arrival times. Moreover, predictive maintenance models can optimize maintenance schedules based on usage patterns, reducing downtime and operational costs (Tinga et al., 2017).

- *Enhanced Safety and Navigation*

AI models specifically designed for navigation and safety have the potential to significantly reduce accidents at sea. For instance, collision avoidance systems utilize AI algorithms to analyze real-time data from surrounding vessels, weather conditions, and navigational charts to suggest optimal routes (Pedrielli et al., 2019). These systems can alert operators to potential collisions, enabling timely interventions to prevent accidents. Additionally, AI-driven decision support systems can assist crew members in making informed choices during critical situations, thereby enhancing overall safety (Ray et al., 2013).

C. Collaboration Between Maritime and Tech Industries

The maritime industry is experiencing a significant transformation driven by the adoption of advanced technologies, particularly those originating from the tech industry. Collaboration between these two sectors has become essential to address the complexities of modern maritime operations, enhance safety, improve efficiency, and mitigate environmental impacts.

- *The Need for Collaboration*

The maritime industry faces numerous challenges, including rising operational costs, regulatory compliance, environmental sustainability, and cybersecurity threats. To effectively address these challenges, maritime companies are increasingly looking to technology firms for innovative solutions (Fruth & Teuteberg, 2017). By using technologies such as artificial intelligence (AI), the Internet of Things (IoT), and big data analytics, maritime operators can enhance operational efficiency and adapt to the rapidly changing maritime landscape (Idoko et al., 2024).

- *Areas of Collaboration*

- *Data Analytics and Decision Support*

One of the most prominent areas of collaboration between the maritime and tech industries is in data analytics. Technology firms are providing maritime companies with tools to collect, analyze, and interpret vast amounts of data from various sources, including sensors on vessels, weather data, and AIS (Automatic Identification System) information (Šekularac-Ivošević & Milošević 2019). This collaboration facilitates better decision-making, predictive maintenance, and operational optimization. For example, big data analytics can identify patterns in fuel consumption and port operations, allowing shipping companies to reduce costs and improve efficiency (Bari et al., 2016).

- *Cybersecurity Solutions*

As the maritime industry becomes increasingly digitized, the importance of cybersecurity has grown. Collaboration with tech firms specializing in cybersecurity is vital for safeguarding critical infrastructure and sensitive data from cyber threats (Akpan et al., 2022). Technology companies are developing AI-driven cybersecurity solutions that can monitor maritime networks in real time, detect anomalies, and respond to potential threats proactively. By partnering with tech firms, maritime organizations can enhance their cybersecurity posture and ensure compliance with regulatory standards (Tam & Jones, 2018).

- *Autonomous and Remote Operations*

The development of autonomous vessels and remote operations represents another significant area of collaboration. Tech companies are at the forefront of creating the AI and sensor technologies necessary for autonomous navigation (Idoko et al., 2024). Collaborations between maritime firms and tech startups have led to the testing and implementation of autonomous vessels that can operate with minimal human intervention, enhancing safety and reducing labor costs. These partnerships are essential for navigating the regulatory landscape and ensuring that autonomous technologies meet safety and operational standards (Idoko et al., 2024).

➢ *Challenges in Collaboration*

Despite the numerous benefits of collaboration, several challenges hinder effective partnerships between the maritime and tech industries. One significant challenge is the cultural gap between the two sectors. The maritime industry has traditionally been conservative and slow to adopt new technologies, while tech firms are often more agile and innovative (Šekularac-Ivošević & Milošević, 2019). This cultural difference can lead to misunderstandings and misaligned expectations.

Additionally, the complexity of maritime operations requires tailored solutions that may not always align with the standardized products offered by tech companies. Successful collaboration requires a deep understanding of maritime processes and operational nuances, which can be challenging for tech firms that lack industry experience (Fruth & Teuteberg, 2017).

VII. SUMMARY AND CONCLUSION

A. *Summary of Key Findings*

The maritime industry is at a pivotal juncture, navigating the challenges posed by an increasingly complex operational landscape characterized by rising cybersecurity threats, environmental concerns, and the demands for greater efficiency and safety. The integration of advanced technologies, particularly artificial intelligence (AI) and network automation, has the potential to revolutionize maritime operations, making them more resilient, secure, and sustainable.

The influence of extreme environmental conditions on maritime operations cannot be overstated. Harsh weather and geographical isolation exacerbate existing vulnerabilities, necessitating robust cybersecurity frameworks to safeguard critical systems and ensure uninterrupted operations (Akpan et al., 2022). The integration of AI-driven intrusion detection systems (IDS) can significantly enhance the maritime industry's ability to mitigate these risks through real-time monitoring and adaptive response mechanisms (Bari et al., 2016).

While the benefits of technology adoption in the maritime industry are clear, challenges remain, including the need for cultural alignment between maritime and tech sectors, data integration issues, and regulatory compliance. Addressing these challenges requires a concerted effort from all stakeholders involved, including policymakers, industry leaders, and technology providers. Continued investment in research and development, along with strong partnerships, will be vital in shaping the future of maritime operations (Idoko et al, 2024).

B. *Conclusion*

Finally, the path forward for the maritime industry lies in embracing digital transformation through strategic collaboration with tech partners. By adopting cutting-edge technologies and innovative practices, the maritime sector will not only enhance its operational capabilities but also build a more sustainable and secure future, ultimately contributing to the resilience of global supply chains.

REFERENCES

[1]. Adu-Twum, H. T., Sarfo, E. A., Nartey, E., Adesola Adetunji, A., Ayannusi. A. O.& Walugembe, T. A. (2024). Role of Advanced Data Analytics in Higher Education: Using Machine Learning Models to Predict Student Success. *International Journal of Computer Applications Technology and Research.* Volume 13–Issue 08, 54 – 61, 2024, ISSN: 2319–8656. DOI:10.7753/IJCATR1308.1006

[2]. Ahmad, Z., Acarer, T., & Kim, W. (2023). Optimization of maritime communication workflow execution with a task-oriented scheduling framework in cloud computing. *Journal of Marine Science and Engineering*, *11*(11), 2133.

[3]. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123-138.

[4]. Al Ali, N. A. R., Chebotareva, A. A., & Chebotarev, V. E. (2021). Cyber security in marine transport: opportunities and legal challenges. *Pomorstvo*, *35*(2), 248-255.

[5]. Ali, M., Hu, Y. F., Luong, D. K., Oguntala, G., Li, J. P., & Abdo, K. (2020, October). Adversarial attacks on ai based intrusion detection system for heterogeneous wireless communications networks. In *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)* (pp. 1-6). IEEE.

[6]. Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, Al-Zahrani, A., Lufti, A., Awad, A. B. & Aldhyani, T. H. (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. *Electronics*, *11*(21), 3571.

[7]. Alqurashi, F. S., Trichili, A., Saeed, N., Ooi, B. S., & Alouini, M. S. (2022). Maritime communications: A survey on enabling technologies, opportunities, and challenges. *IEEE Internet of Things Journal*, *10*(4), 3525-3547.

[8]. Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, *10*(02), 361-373.

[9]. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics*, *9*(7), 1177.

[10]. Awotiwon, B. O., Enyejo, J. O., Owolabi, F. R. A., Babalola, I. N. O., & Olola, T. M. (2024). Addressing Supply Chain Inefficiencies to Enhance Competitive Advantage in Low-Cost Carriers (LCCs) through Risk Identification and Benchmarking Applied to Air Australasia's Operational Model. *World Journal of Advanced Research and Reviews, 2024, 23(03), 355–370.*

[11]. Ayoola, V. B., Ugoaghalam, U. J., Idoko P. I, Ijiga, O. M & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances*, 2024, 20(03), 094–117.

[12]. Bari, F., Chowdhury, S. R., Ahmed, R., Boutaba, R., & Duarte, O. C. M. B. (2016). Orchestrating virtualized network functions. *IEEE Transactions on Network and Service Management*, *13*(4), 725-739.

[13]. Cardona, N., Coronado, E., Latré, S., Riggio, R., & Marquez-Barja, J. M. (2020). Software-defined vehicular networking: Opportunities and challenges. *IEEE Access*, *8*, 219971-219995.

[14]. Chen, Z., Liu, J., Gu, W., Su, Y., & Lyu, M. R. (2021). Experience report: Deep learning-based system log analysis for anomaly detection. *arXiv preprint arXiv:2107.05908*.

[15]. Chi, H., Du, Y., & Brett, P. M. (2020). Design of a marine environment monitoring system based on the Internet of Things. *Journal of Coastal Research*, *110*(SI), 256-260.

[16]. Cho, S., Orye, E., Visky, G., & Prates, V. (2022). Cybersecurity Considerations in Autonomous Ships. *NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, Estonia*.

[17]. Dalaklis, D., Nikitakos, N., Papachristos, D., & Dalaklis, A. (2023). Opportunities and challenges in relation to big data analytics for the shipping and port industries. *Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance*, 267-290.

[18]. Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57-106.

[19]. Deshpande, P., Sharma, S. C., Peddoju, S. K., & Junaid, S. (2018). HIDS: A host based intrusion detection system for cloud computing environment. *International Journal of System Assurance Engineering and Management*, *9*, 567-576.

[20]. Elsayed, M. A., Wrana, M., Mansour, Z., Lounis, K., Ding, S. H., & Zulkernine, M. (2022). AdaptIDS: Adaptive intrusion detection for mission-critical aerospace vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *23*(12), 23459-23473.

[21]. Evensen, M. H. (2020). *Safety and security of autonomous vessels. Based on the Yara Birkeland project* (Master's thesis, The University of Bergen).

[22]. Fruth, M., & Teuteberg, F. (2017). Digitization in maritime logistics—What is there and what is missing?. *Cogent Business & Management*, *4*(1), 1411066.

[23]. Georgescu, T. M. (2020). Natural language processing model for automatic analysis of cybersecurity-related documents. *Symmetry*, *12*(3), 354.

[24]. Ghaleb, F. A., Saeed, F., Alkhammash, E. H., Alghamdi, N. S., & Al-Rimy, B. A. S. (2022). A fuzzy-based context-aware misbehavior detecting scheme for detecting rogue nodes in vehicular ad hoc network. *Sensors*, *22*(7), 2810.

[25]. G. Martín, A., Fernández-Isabel, A., Martín de Diego, I., & Beltrán, M. (2021). A survey for user behavior analysis based on machine learning techniques: current models and applications. *Applied Intelligence*, *51*(8), 6029-6055.

[26]. Hodge, V. J., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review*, 22(2), 85-126.

[27]. Ibokette, A. I. Ogundare, T. O., Danquah, E. O., Anyebe, A. P., Agaba, J. A., & Agaba, J. A. (2024). Optimizing maritime communication networks with virtualization, containerization and IoT to address scalability and real – time data processing challenges in vessel – to –shore communication. *Global Journal of Engineering and Technology Advances, 2024, 20(02), 135–174.*

[28]. Ibokette., A. I. Ogundare, T. O., Danquah, E. O., Anyebe, A. P., Agaba, J. A., & Olola, T. M. (2024). The impacts of emotional intelligence and IOT on operational efficiency in manufacturing: A cross-cultural analysis of Nigeria and the US. *Computer Science & IT Research Journal P-ISSN: 2709-0043, E-ISSN: 2709-0051.*

[29]. Idoko, D. O., Agaba, J. A., Ijeoma, N., Badu, S. G., Ijiga, A. C., & Okereke, E. K. (2024). The role of HSE risk assessments in mitigating occupational hazards and infectious disease spread: A public health review. *Open Access Research Journal of Biology and Pharmacy*, *11*(2), 011-030.

[30]. Idoko, I. P., Igbede, M. A., Manuel, H. N. N., Adeoye, T. O., Akpa, F. A., & Ukaegbu, C. (2024). Big data and AI in employment: The dual challenge of workforce replacement and protecting customer privacy in biometric data usage. *Global Journal of Engineering and Technology Advances*, *19*(02), 089-106.

[31]. Idoko, I. P., Ijiga, O. M., Agbo, D. O., Abutu, E. P., Ezebuka, C. I., & Umama, E. E. (2024). Comparative analysis of Internet of Things (IOT) implementation: A case study of Ghana and the USA-vision, architectural elements, and future directions. *World Journal of Advanced Engineering Technology and Sciences*, *11*(1), 180-199.

[32]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention.

[33]. Jones, K., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security.

[34]. Jović, M., Tijan, E., Aksentijević, S., & Čišić, D. (2019, May). An overview of security challenges of seaport IoT systems. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1349-1354). IEEE.

[35]. Katterbauer, K. (2022). Shipping of the future-cybersecurity aspects for autonomous AI-driven ships. *Australian and New Zealand Maritime Law Journal*, *36*(1), 1-12.

[36]. Letou, K., Devi, D., & Singh, Y. J. (2013). Host-based intrusion detection and prevention system (HIDPS). *International Journal of Computer Applications*, *69*(26), 28-33.

[37]. Kim, D., Antariksa, G., Handayani, M. P., Lee, S., & Lee, J. (2021). Explainable anomaly detection framework for maritime main engine sensor data. *Sensors*, *21*(15), 5200.

[38]. Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2472-2481.

[39]. Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 270-285.

[40]. Marks, P., van Sluis, A. R. I. E., Vervooren, A. N. D. R. E., & Zeer, M. A. R. I. E. L. L. E. (2013). Improving policing in the port of Rotterdam, the Netherlands. *Policing Global Movement: Tourism, Migration, Human Trafficking, and Terrorism*, 21-39.

[41]. Mishra, A. K., Mandalia, S. H., & Upadhyay, M. H. C. (2024). Safeguarding Maritime Operations: A Proactive Approach to Maritime Cybersecurity. *Journal of Maritime Research*, *21*(2), 278-283.

[42]. Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats?. *Transactions on maritime science*, *8*(01), 132-139.

[43]. Nawaz, H., Sethi, M. S., Nazir, S. S., & Jamil, U. (2024). Enhancing National Cybersecurity and Operational Efficiency through Legacy IT Modernization and Cloud Migration: A US Perspective. *Journal of Computing & Biomedical Informatics*, *7*(02).

[44]. Okeke, R. O., Ibokette, A. I., Ijiga, O. M., Enyejo, L. A., Ebiega, G. I., & Olumubo, O. M. (2024). The reliability assessment of power transformers. *Engineering Science & Technology Journal*, *5*(4), 1149-1172.

[45]. Oyebanji, O. S., APAMPA, A. R., Afolabi, O., Eromonsei, S. O., & Babalola, A. (2024). Performance benchmarking of convolutional neural networks and ensemble machine learning techniques for automated mammographic breast cancer detection: A comparative study. *World Journal of Advanced Engineering Technology and Sciences*, 2024, 12(02), 808–83.

[46]. Patel, A., Taghavi, M., Bakhtiyari, K., & Júnior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications*, *36*(1), 25-41.

[47]. Pedrielli, G., Xing, Y., Peh, J. H., Koh, K. W., & Ng, S. H. (2019). A real time simulation optimization framework for vessel collision avoidance and the case of singapore strait. *IEEE Transactions on Intelligent Transportation Systems*, *21*(3), 1204-1215.

[48]. Pitropakis, N., Logothetis, M., Andrienko, G., Stefanatos, J., Karapistoli, E., & Lambrinoudakis, C. (2020). Towards the creation of a threat intelligence framework for maritime infrastructures. In *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5* (pp. 53-68). Springer International Publishing.

[49]. Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), 1384.

[50]. Queiroz, R., Cruz, T., Mendes, J., Sousa, P., & Simões, P. (2023). Container-based virtualization for real-time industrial systems—a systematic review. *ACM Computing Surveys*, *56*(3), 1-38.

[51]. Panić, I., Ćelić, J., Bistrović, M., & Škrobonja, A. (2021). Drone as a part of maritime search and rescue operations. *Technologies, Techniques and Applications Across PNT*, 63.

[52]. Rawson, A., & Brito, M. (2023). A survey of the opportunities and challenges of supervised machine learning in maritime risk analysis. *Transport Reviews*, *43*(1), 108-130.

[53]. Ray, A. (2013, April). Autonomous perception and decision-making in cyber-physical systems. In *2013 8th International Conference on Computer Science & Education* (pp. 1-10). IEEE.

[54]. Rødseth, Ø. J., Nesheim, D. A., Rialland, A., & Holte, E. A. (2023). The societal impacts of autonomous ships: the Norwegian perspective. In *Autonomous Vessels in Maritime Affairs: Law and Governance Implications* (pp. 357-376). Cham: Springer International Publishing.

[55]. Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, 1251-1260.

[56]. Scarfone, K., & Mell, P. (2010). Intrusion detection and prevention systems. In *Handbook of information and communication security* (pp. 177-192). Berlin, Heidelberg: Springer Berlin Heidelberg.

[57]. Šekularac-Ivošević, S., & Milošević, D. (2019). Innovation through collaboration: the application in maritime industry. In *1st International Conference of Maritime Science & Technology Naše More* (pp. 17-18).

[58]. Simion, D., Postolache, F., Fleacă, B., & Fleacă, E. (2024). AI-Driven Predictive Maintenance in Modern Maritime Transport. Enhancing Operational Efficiency and Reliability.

[59]. Sodiya, A. S., Ojesanmi, O. A., Akinola, A., & Aborisade, O. (2014). Neural network-based intrusion detection systems. *International Journal of computer applications*, *106*(18).

[60]. Mao, W., & Larsson, S. (2023). Increase shipping efficiency using ship data analytics and AI to assist ship operations.

[61]. Singh, M., Mehtre, B. M., & Sangeetha, S. (2020). Insider threat detection based on user behaviour analysis. In *Machine Learning, Image Processing, Network Security and Data Sciences: Second International Conference, MIND 2020, Silchar, India, July 30-31, 2020, Proceedings, Part II 2* (pp. 559-574). Springer Singapore.

[62]. Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors*, *28*, 100827.

[63]. Spravil, J., Hemminghaus, C., von Rechenberg, M., Padilla, E., & Bauer, J. (2023). Detecting maritime gps spoofing attacks based on nmea sentence integrity monitoring. *Journal of Marine Science and Engineering*, *11*(5), 928.

[64]. Tabish, N., & Chaur-Luh, T. (2024). Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. *IEEE Access*.

[65]. Tam, K. & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147-164.

[66]. Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships. In *2018 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-8). IEEE.

[67]. Tinga, T., Tiddens, W. W., Amoiralis, F., & Politis, M. (2017, June). Predictive maintenance of maritime systems: models and challenges. In *European Safety and Reliability Conference, ESREL 2017* (pp. 421-429). Taylor & Francis.

[68]. Uzoma, J., Falana, O., Obunadike, C., Oloyede, K., & Obunadike, E. (2023). Using artificial intelligence for automated incidence response in cybersecurity. *International Journal of Information Technology (IJIT)*, *1*(4).

[69]. Wei, T., Feng, W., Chen, Y., Wang, C. X., Ge, N., & Lu, J. (2021). Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: Key technologies, opportunities, and challenges. *IEEE Internet of things journal*, *8*(11), 8910-8934.

[70]. Yuan, Y., Li, Z., Malekian, R., & Yan, X. (2017). Analysis of the operational ship energy efficiency considering navigation environmental impacts. *Journal of Marine Engineering & Technology*, *16*(3), 150-159.