ISSN: 2182-2069 / E-ISSN: 2182-2077

Modeling and Assessing Cyber Threats in Cloud-Based Vessel Traffic Management Systems

Yeshwanth Raj[1*], and Rajendran Palanivelu[2]

[1*]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.
yeswanthraj@ametuniv.ac.in, https://orcid.org/0009-0003-4467-3389

[2]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.
rajendran.p@ametuniv.ac.in, https://orcid.org/0000-0001-5016-9742

Received: May 21, 2025; Revised: July 08, 2025; Accepted: August 11, 2025; Published: August 30, 2025

Abstract

The adoption of cloud technology is rapidly changing the maritime sector, including the development of Vessel Traffic Management Systems (VTMS). VTMS systems are critical to the improvement and growth of navigational safety, vessel movement control, and general maritime traffic efficiency. However, the application of cloud computing gives rise to various cybersecurity issues regarding the confidentiality, integrity, and availability of essential maritime operations. In this paper, we propose a systematic approach for modeling and evaluating cyber threats in VTMS residing in the cloud. We start with the examination of the architecture of modern VTMS solutions and attempt to determine the possible threat opportunities that cloud technology and data processing at remote sites may pose. We use systematic threat modeling frameworks for STRIDE, attack tree analysis and other techniques to classify and assess possible breaches of control, data, denial of service attacks, and unauthorized manipulation of control. To showcase the practical outcomes, a maritime case study was conducted simulating an attack scenario on a cloud-connected VTMS controlling a port with high vessel traffic. Results have shown how cyber threats can inhibit vessel to traffic control communication, slow down critical decision making, and increase the likelihood of maritime accidents. Based on this examination, we propose a risk mitigation framework including, but not limited to, anomaly identification, encryption procedures, and industry specific adaptive response planning automation mechanisms aligned with the IMO's cybersecurity for ships guidelines. This investigation offers important contributions pertinent to stakeholders in the maritime domain, developers of VTMS, and cybersecurity experts focused on protecting cloud-based VTMS infrastructure and maritime activities from emerging vulnerabilities.

Keywords: Cybersecurity, Vessel Traffic Management Systems (VTMS), Cloud Computing, Threat Modeling, Maritime Security, Cyber Threat Assessment, Critical Infrastructure Protection.

1 Introduction

1.1 Vessel Traffic Management Systems: an Overview

As far as monitoring and controlling maritime traffic within ports and coastal areas is concerned, Vessel Traffic Management Systems (VTMS) are crucial since they enhance safety, environmental protection, and the overall efficiency of port operations. VTMS employs a multitude of technologies including

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 523-538.
DOI: *10.58346/JISIS.2025.I3.036*

*Corresponding author: Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.

radars, Automatic Identification Systems (AIS), meteorological units, and radios to track and control vessel movements (Claresta & Baldauf, 2020). A VTMS is a collection of centers that allow for the acquisition, processing, and communication of navigational data information so as to allow for an appropriate response to emergencies. The rapid growth in traffic volume and its complexity has prompted the adoption of advanced digital solutions in modern maritime operations. Cloud computing is one of the latest technologies that provide these benefits with its scalable resources, real-time processing, and data sharing among disparate users (Eriksen, 2017). VTMS servces makes use of cloud infrastructure to increase the real-time data processing capability from various ports, thereby improving traffic control agility and coordination. This also adds to the concept of e-navigation which aims at integrated and automated systems for improved maritime safety (Hahn et al., 2016).

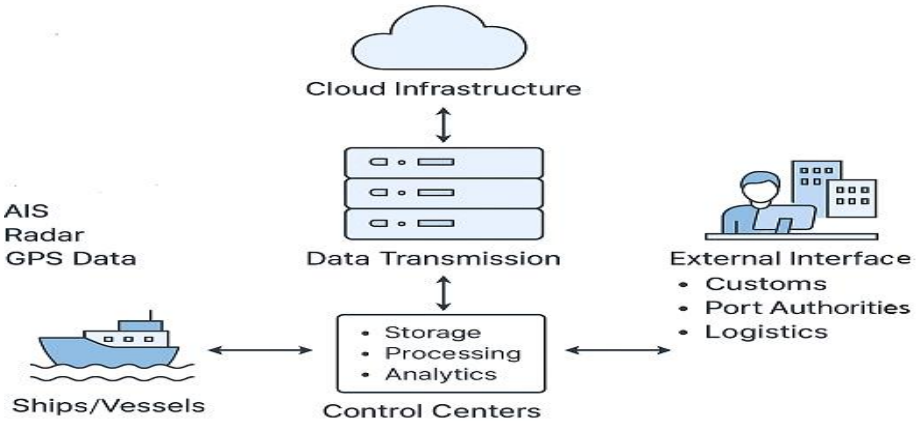

Figure 1: Architecture of a Cloud-based Vessel Traffic Management System (VTMS)

The diagram (Figure 1) shows a cloud-based Vessel Traffic Management System (VTMS) with its main components including data flow architecture. On the operational level, ships and vessels equipped with sensors such as AIS (Automatic Identification System), radar, and GPS provide real-time navigation and positioning data. This data is sent through communication satellites, WHF radios, or internet-based protocols) to cloud infrastructure where data is stored, monitored, and analyzed. These satellites serve as intermediaries and securely route sensitive information to cloud spaces for storage, processing, and statical analysis. This cloud saves space and improves accessibility, ensuring that data is managed and shared. Humancontrolled control centers enable VTMS supervisors to monitor and manage data as well as the vessels using dashboards for ship traffic monitoring, port operation, and anomalous event management. Furthermore, VTMS associates with other systems such as customs offices, port authorities, and third party logistics to security coordinate and manage the flow of cargo(Nandy & Dubey, 2024). The illustration explains the rapidly rising reliance of maritime operations towards digitally controlled infrastructures thus incorporating an extensive range of gaining cybersecurity complications.

1.2 Importance of Cybersecurity in Maritime Operations

Cybersecurity concerns have come to the forefront for maritime authorities with the digitization and cloud adoption of VTMS. In the past, maritime systems functioned in relative calm isolation, however, the adoption of inter-linked technologies opens them to cyber threats that were previously non-existent within the industry (Tam & Jones, 2018; Hlushenkova et al., 2024). Nowadays, threats are present not only in onboard systems, but also in port facilities, communication systems, and cloud services (Hossain et al., 2024). This, in addition to obsolete legacy systems, absence of uniform minimum standards of

cybersecurity, and lack of adequate training for personnel, compounds the problem (Akpan et al., 2022). Cyberattacks targeting maritime assets have already proved how tangible and damaging the consequences of such security lapses can be. The NotPetya ransomware attack in 2017, which brought Maersk global operations to a standstill, perhaps serves as the most definitive example.

The attack forced a temporary shutdown of Maersk's shipping, port and logistics systems, resulting in losses which exceeded $300 million (Brother, 2024); Sharma & Rajput, 2024). While the assault was not aimed at Maersk, it did highlight how interconnected and vulnerable maritime infrastructure has become. (Anderson et al., 2013) that by 2025, cybercrime will inflict damages exceeding $10 trillion annually to the economy. Maritime transport is crucial for global trade, and therefore a prime target as well (Das & Kapoor, 2024). Ports are now referred to as “smart” ecosystems, meaning that systems such as the VTMS, Customs, Terminal Operations and Logistics Platforms are integrated as one and individually susceptible (Progoulakis et al., 2023). In response, international organizations have developed policies to mitigate maritime cyber risks. The International Maritime Organization (IMO) issued guidelines (MSC-FAL.1/Circ.3) recommending shipowners and operators to integrate cyber risk and safety management systems (2017). These guidelines propose the adoption of a comprehensive strategy towards cybersecurity, focusing on the detection, assessment, reduction, and management of risks and threats.

1.3 Research Aim and Objectives

The goal of this research is to model and evaluate cyber threats within cloud-based vessel traffic management systems in order to gain insights into their vulnerabilities and enhance cybersecurity frameworks in the maritime domain. As VTMS are increasingly relying on cloud technology, the added danger posed by remote access, shared resources, and complex digital ecosystems needs to be addressed. To describe the possible cyber threats by analyzing the architecture of cloud-integrated VTMS, mapping out the system components and critical access points. The threat models are designed using frameworks such as STRIDE and simulate real world scenarios using attack trees. To assess operational and safety risks associated with cyber events on VTMS and control or monitor impacts to Maritime traffic control. Analyze the extent of existing security controls in VTMS deployed in the cloud and measure their effectiveness against international standards outlining minimum requirements and existing gaps (Deshmukh & Nair, 2024). Develop a comprehensive cybersecurity approach with mitigation measures, policy recommendations, best practices, and defined maritime system governance for systems hosted on the cloud.

This project focuses on modeling cybersecurity threats through applied research on vessel traffic management systems hosted on cloud solutions which enables addressing the existing gap in maritime cybersecurity literature. Its results are intended to assist policymakers, technology developers, and operators in strengthening the security posture of vessel traffic management systems and enhancing maritime infrastructure resilience for imminent security threats.

2 Literature Review

2.1 Vessel Traffic Management Systems Cyber Threat Overview

VTMS, an abbreviation for Vessel Traffic Management Systems, is susceptible to multiple cyber threats due to the increasing dependence on digital systems within the maritime sector. These threats can critically impact the operational integrity of the maritime industry, which can be detrimental. Cyber threats associated with VTMS have been noted to include unauthorized access, data manipulation, DoS

attacks, and systems compromised through malware or ransomware. These concerns are more disturbing because VTMS is vital in maintaining navigational safety and operational efficiency along busy sea lanes (Bolbot et al., 2020). The use of VTMS cloud-based integrations also increases cybersecurity vulnerabilities. While offering data scaling along with remote access and processing, cloud environments present additional vulnerabilities such as insecure APIs, and data breach, and leakage (Krishnamurthy & Parvatham, 2023). Hackers can take advantage of cloud misconfiguration, allowing access to classified vessel information, prompting the possibility of manipulating vessel activities, or disrupting activities at the port (Iqbal et al., 2025). The cyber threats in VTMS can also be categorized into internal and external threats. External threats are usually from cybercriminals and nation-state actors who seek financial or political motives from VTMS (Arvinth, 2023). Such attacks include phishing and DDoS attacks, where systems are flooded to gain access to confidential information. Internal threats, on the other hand, stem from the malicious actions of disgruntled employees and insiders, which is more difficult to manage and control (Kechagias et al., 2022). With the intricacies and interrelation of modern maritime activities, the potential for cascading system failures renders these threats particularly detrimental.

Table 1: Categorization of Cybersecurity Threats in a Vehicle Traffic Management System (VTMS) Environment

Categorization of Cyber Threats in VTMS Environment			
Network-Based Attacks	**Application-Level Threats**	**Insider Threats**	**Cloud-Specific Risks**
Threats: DoS, Spoofing	**Threats:** Ransomware, SQL Injection	**Threats:** Access Misuse	**Threats:** Misconfiguration, Data Breaches
Vulnerabilities: System Downtime	**Impacts:** Data Loss, Unauthorized Access	**Impacts:** Operational Disruption, Data Leaks	**Impacts:** Information Exposure, Service Outage
Examples: Patching	**Examples:** Code Reviews	**Examples:** Employee Training, Access Controls	**Examples:** Security Audits, Encryption

The table (Table 1) captures the pertinent cyber threats that are associated with the operation of VTMS in a systematic manner. It classifies the threats into four categories: Network-Based Attacks, Application level Threats, Insider Threats, and Cloud-Specific Threats. Each category contains description of common threats such as DoS, ransomware, authorization abuse, and misconfiguration as well as their impacts like downtime, data loss, disruption of business, and exposure of sensitive information. Moreover, the table describes relevant vulnerabilities and mitigation strategies that need to be undertaken such as patching, code review, training, removing access, security audits, and encryption. These classifications assist in comprehending and mitigating cybersecurity vulnerabilities to improve cybersecurity vigilance of VTMS infrastructure.

2.2 Current Cyber Security Policies within the Maritime Sector

With the understanding that maritime cybersecurity (Tusher et al., 2022) is increasingly important, a number of procedures have been put in place to protect systems such as VTMS. International Maritime Organization (IMO) has been one of the leaders, advocating the stipulation of strict cyber policies in the maritime industry. As noted in IMO guidelines of 2017 (MSC-FAL.1/Circ.3), there has to be a provision for managing cyber risks within safety management systems which compels operators to evaluate and mitigate potential cyber threats to the operation of vessels and port infrastructure (IMO, 2017; Ziwei &

Han, 2023). Resulting from these regulations, port authorities alongside shipping companies have started to adopt various protective digital infrastructure technologies and organizational approaches. These include the installation of firewalls, IDPS, encryption, and secure communication interfaces (Aderlard & Penrod, 2023). Further, organizations are improving their comprehensive risk mitigation strategies through investments focused on advanced cyber risk assessments and penetration testing Heighted, 2020) to identify weaknesses proactively. Although these actions address already identified risks, the changeable nature of cyber threats in VTMS implies the need to continuously adapt maritime cybersecurity frameworks. There is a shift toward developing VTMS maritime cybersecurity policies guided by ISO/IEC 27001 and the NIST Cybersecurity Framework, which focus on the craft's information security management system (Neumann, 2024). They contribute towards defining holistic policies geared towards achieving cybersecurity that extends beyond technical measures to staff training and awareness initiatives. In addition, response to cybersecurity incidents has increasingly become part of the standard maritime organizational procedures. These plans specify steps to be taken so that the organization can respond and recover services in the least disruptive manner possible. Equipping crews and other personnel to identify, mitigate cyber threats, and secure their workstations is becoming common practice (Alcaidd & Llave, 2020).

2.3 Previous Studies on Cybersecurity in Cloud-Based Systems

The shift in VTMS to cloud-based systems comes with its own set of cybersecurity concerns. There has been some research on cybersecurity issues related to cloud acceptance in the maritime field. (Iqbal et al., 2025) pointed out that, among other things, cloud computing is beneficial because it consolidates data, has higher processing power, and is scalable. On the other hand, he also pointed out some disadvantages such as inadequate data encryption, possible breaches in cloud access security, and potential data loss through other means or system failures. One of the most important issues for cloud-based VTMS is the secure configuration of the cloud. Inadequately configured clouds can result in the leakage of maritime sensitive data or grant unauthorized access to it (Papastergiou et al., 2020). This is especially true for third party clouds where SLAs do not guarantee security and transparency of provisions put in place. The work (Aisyah et al., 2021) did, emphasized how the infrastructure of cloud platform technology is susceptible to DDoS attacks, which leads to the unavailability of VTMS, hampering operations. Although most service providers have effective ways to lessen risk in place, the ever increasing difficulty technology attacks inflicts is a problem for maritime industry (Jassim, 2023). As with the previous studies, it is clear that data integrity and secure communications are features in VTMS operating in cloud environments (Atashsooz et al., 2019). The increasing use of cloud technologies for sharing data leads to sensitive maritime data being shared, hence maintaining confidentiality and integrity is very important (Kechagias et al., 2022). Protection of vessel tracking data and communication between ships and port authorities is achieved through the use of encryption technologies and SSL (Perumal, 2024). Maritime cybersecurity research is increasingly focusing on cloud-based vulnerability management concepts. Research highlights the importance of continuously assessing the security of a cloud-hosted VTMS and actively finding its vulnerabilities to mitigate cyber threats (Krishnamurthy & Parvatham, 2023; Jasim, 2024). This includes vulnerability scanning and managing patches, as well as ensuring compliance to standards like ISO/IEC 27018 which lends a focus on privacy in cloud computing (Krishnamurthy & Parvatham, 2023).

Cybersecurity remains a challenge as the maritime industry advances towards more VTMS cloud services. The modern intricacies of maritime operations, in conjunction with the constantly extending avenues for an attack, demand dynamic cybersecurity strategies. With prior works focusing on the cyber

threat mitigation groundwork for VTMS, there still remains an important gap that needs filling concerning cloud infrastructures and protecting cyber threats in international maritime trade.

3 Methodology

3.1 Approaches to Data Collection

The efficiency of constructing models and evaluating cyber threats on cloud-based VTMS highly depends on precise and thorough data collection. Specifically, data collection aims to gather both qualitative and quantitative information about system vulnerabilities, potential threats, and current cybersecurity measures. Academic literature, industry reports, and guidelines on cybersecurity in the maritime domain will be assessed thoroughly. This will enable the identification of primary vulnerabilities and the overall threat landscape for VTMS. The literature review will be focused on the history of VTMS, the adoption of cloud technologies, and cyber-attacks in the maritime industry. This approach assists in gaining a historical perspective on the system and enables the tracking of common threats and protective countermeasures employed. The maritime sector has many professionals, such as port operators, VTMS developers, and cybersecurity professionals. Their insights are important and will be explored through interviews. Their thoughts on modern practices to protect cloud systems in the maritime sphere, vulnerabilities to contemporary cyber defense systems, and the limitation of these systems will be interrogated. This will enhance the broad understanding of cyber risks and mitigating factors prevalent in the modern world. Examining cyberattacks maritime region will illustrate the ways in which modern cyber threats have impacted VTMS systems, or similar ones. We will chart the cyber assaults undertaken in port facilities, shipping companies, and critical maritime infrastructure, analyzing how these attacks were executed, what flaws were exploited, and how effective the response was. This will broaden understanding concerning the possible persistence of VTMS cyber threats in attempt to devise more sophisticated countermeasures. A cyberattack simulation with the cloud-based VTMS will be conducted to test the system's vulnerabilities in a closed environment. Scenarios including DDoS, malware attacks, and sensitive information disclosure will be crafted to monitor which parts of the system respond and how. Cybersecurity simulation data collected during these exercises will enrich understanding concerning VTMS constancy against real-time attacks and what improvements are needed.

3.2 Cyber Threat Modeling Methods

Upon the completion of data collection, the subsequent step is to model the myriad of cyber threats capable of impacting cloud-based VTMS. Cyber threats pose a serious risk to cloud-based VTMS functioning and their cyber threat modeling requires identifying risks, analyzing attack vectors, and evaluating system vulnerabilities. The STRIDE framework categorizes cyber threats into six distinct categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. This framework will be applied on VTMS and its subclasses to systematically identify cyber threats. For instance, in the case of Spoofing, a perpetrator impersonating an actual vessel could gain access through the VTMS and subsequently manipulate steering commands. In the case of Denial of Service, the attacker could target the cloud infrastructure with DoS attacks, aiming to render the VTMS inoperative. This technique is useful as it enables one to pinpoint all types of spoofing vulnerabilities from user access to data transmission. As with any potentially maleficent undertaking, the achievement of any goal is domain competent. Compromising a system can be quite elaborate or as basic as a single step breach. For the wants of this article we will keep it simple and begin at the apex

which is VRM VTMS functionality crippling and subdivide it into a tree like structure outlining the sub techniques. Every single step taken by an adversary provides an additional possibility. For instance, through cloud infrastructure, data can be maliciously altered for advanced purposes. This visual method employs analysis of systematic components revealing critical vulnerability pointers fuelling cyber threats while emphasizing multi-vectored assaults. Under the umbrella of DFD lies both the processing and transferment of data. All places of storage serve as potential breach points of attack as the data montain shows. Utilizing the DFD methodology provides an accurate representation of all interrelations, abstracts, compilations, or pipework pertaining to siphoning and guarantee that in the course of threat modeling there are zero pathway omissions. Throughout the previously mentioned processing, division, and transport breaching in the form of capturing, switching, or widening are all possible outcomes. The Kill Chain framework facilitates a comprehension of the stages of a cyberattack as well as points of possible detection or intervention within the attack sequence. The Kill Chain categorizes the attack into Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objetives. When applied to VTMS, scholars utilizing the Kill Chain are able to follow an attack's lifecycle and identify optimal locations for security interventions that would neutralize or mitigate damage caused by an attack at several phases.

3.3 Risk Evaluation Strategies

Once the cyber risks within the VTMS are identified, a thorough assessment regarding their magnitude and probability is conducted. The essence of risk assessment is to ensure that cybersecurity investments are appropriately prioritized and managed within the available budgets. Qualitative Risk Assessment method involves evaluating the risks based on expert opinions. This research will obtain primary information from key informants, analyze case studies, and assess various threat impacts in order to categorize risks as high, medium, or low. These evaluations might be helpful in scenarios where data is limited or challenging to quantify. High-priority risks identified through the first assessment will include sensitive data breach or system downtime risks. A quantitative approach alongside qualitative analysis will be used to measure risks. This is done by determining how likely it is that an attack will happen, and what its impact will be on the VTMS. A Probability-Impact Matrix will be used for all the threats to be categorized according to the probability and impact of each threat so as to rank them in the order they should be addressed. This approach is most useful when there is numerical information regarding cyber incidents because such information can lead to more accurate risk scores. Monte Carlo Simulation will be the method of choice in capturing the estimation of the uncertainty and variability in the risk assessment. By employing Monte Carlo simulations, a wide variety of outcomes can be produced based on changing inputs like estimation of the threat, how effective the mitigations are, and the financial implications. These simulations offer a comprehensive view of the diverse outcomes and assist in evaluating the risks associated with cloud-based VTMS. The ISO 31000 framework will support the overarching risk management process by systematically guiding risk identification, evaluation, treatment, and monitoring. This is an international standard which calls for an ongoing iterative process of risk management so that VTMS cybersecurity measures are responsive to new and evolving threats and vulnerabilities.

The approach presented in this research offers a systematic framework for identifying, modeling, and evaluating the cyber threats directed towards cloud-based Vessel Traffic Management Systems. The focus of this study is to create a clear picture of cybersecurity in maritime systems through a combination of data collection, threat modeling, and risk assessment methodologies. This approach is designed so that the study produces practical recommendations on VTMS security, thereby minimizing the effects of cyberattacks on international maritime activities.

4 Cyber Threat Modeling in Cloud-Based Vessel Traffic Management Systems

4.1 Identifying Possible Cyber Threats

Potential cyber threats for cloud-based Vessel Traffic Management Systems (VTMS) cybersecurity are vital for understanding-it in the context of the maritime industry. VTMS is a subsystem of Maritime Traffic Services responsible for the Traffic Separation Scheme, as well as the port controlling and monitoring subsystems. With better integrated cloud-based solutions, these systems are becoming increasingly vulnerable to attack. Cyber spoofing or impersonation remains a prominent risk to VTMS. Cyber attackers can distort certain information regarding vessels, like their location and name, for certain purposes. Through the manipulation of GPS coordinates and signals from the Automatic Identification System (AIS), attackers can inject errors into operational systems, thereby creating hazardous conditions at sea. Data manipulation is another major concern now. Cybercriminals do face the risk of altering vital data that is exchanged between the VTMS and the vessels. An excellent example would be altering communication between vessels and the port authorities. Attackers could impact scheduling decisions, docking, along with the navigation routes. In cloud-based VTMS, where data is transmitted in large volumes over networks, these changes may be catastrophic and go unnoticeable. Doing so may have disastrous outcomes. There are other arguably bigger threats that come from denial of service (DoS) attacks. Tis the season for other attackers DoS vandals to flood the system with traffic streams, blocking access to real time vessel data. Accessibility being everything that port operations are founded on will be paralyzed ushering in repercussions for scheduling, routing, navigation, and coordination along the vessels. Cybercriminals targeting critical system data and holding it hostage will invariably encrypt data in the nautical domain making the sphere vulnerable to ransomware where the logistics in operations restoring breaching periods will incur.

4.2 Examination of Vulnerabilities for Cloud Based Systems

While Cloud-based Vessel Traffic Management Systems offer great scalability and flexibility, they also have a custom set of vulnerabilities. One of the greatest gaps stems from the insecure APIs that permit interactions between various system modules. These unsecured APIs can be exploited by malicious actors to gain unauthorized access to the system. With cloud infrastructure increasingly leaning towards APIs as means of communication for the VTMS and other external components like weather stations, navigation systems, or vessel databases, any inadequacy within the API security framework might allow unauthorized access to the system protections, leading to data theft or manipulation. This threat is heightened within cloud environments where systems are routinely linked with other third party utilities. The other misconfiguration is one of the most severe vulnerabilities that a cloud-based VTMS faces. While providing a considerable degree of elasticity, the scope of misconfiguration, like inadequate security controls, granting access to a database to any internet user, poses massive security risks. Shared cloud infrastructure, although cost-efficient, poses a peculiar problem: the entire system may be at risk from attack due to one misconfigured setting in some other part of the infrastructure. Another severely compromising misconfiguration is data leakage. Severe cloud misconfigurations include the storing of sensitive information such as vessel schedules, cargo particulars, and operational data in the cloud without sufficient encryption and inadequate control settings. This would enable malignant actors to access and manipulate crucial operational information or sensitive data disguising themselves as authoritative figures in a maritime scenario. The term multi-tenancy refers to sharing a particular infrastructure, which poses new risks. In the case of cloud-based VMS, several organizations can utilize

the same infrastructure. This means that one system's breach can give attackers unrestricted access to the rest of the systems. Also, the use of weak VTMS components authentication can be granted to users who should otherwise be denied access. The system is at risk of credential theft or abuse when strong multifactor authentication (MFA) along with adequate user role management is absent. Improper restraining of user privileges can result in the attainment of undue access to vital parts of the system where attackers are able to modify or delete data and services.

4.3 Effects of Cyber Security Risks on Vessel Operations

Vessel Traffic Management System (VTMS) operations, as well as the operation of ports and the entire maritime industry, could be are severely affected by cyber threats aimed at cloud-based VTMS systems. Such attacks could severely compromise VTMS's ability to provide updates and information critical for navigation such as real-time traffic and congestion data, availability of ports, vessel positions, and other vessels on the route. For example, not having access to real-time service information can severely impair scheduled vessel arrivals and departures. These disruptions can lead to congestion at ports which is accompanied by ineffective use of resources, chronic delays, and weak shipping deadlines which in turn adversely affect port authorities and shipping companies in terms of costs. Also, cyber-attacks pose a risk to the safety of ships and their crews. If attackers change important navigation data or provide misleading information, vessels could be navigated to high risk areas which increases the possibility of collision, grounding, or other accidents. A Denial of Service (DoS) attack on a VTMS can render tracking and communication capabilities inoperable. As a result, vessels could be left traversing in circles without receiving up-to-date information on weather, traffic, and other hazards around them. This remains a maritime safety danger, particularly in busy or dangerous waters where accurate vessel tracking is vital for avoiding collisions. Cyberattacks can bear significantly dire consequences on the finances of VTMS. Cyber incidents, including ransomware or DoS attacks, inflict debilitating damages to a firm's operational efficiency, creating prolonged downtimes along with exorbitant recovery expenses. Apart from direct monetary damages, such attacks incur indirect expenses due to protracted litigations, business relationship controversies governing financial regulations, and reputational imbalances. Civil lawsuits and punitive regulations are applicable with regard to breach of cybersecurity in the maritime organization, especially when dealing with sensitive information like passengers, or cargo, which constitutes an invasion of privacy. Additionally, the aftermath of a cyberattack inflicts deep damages on the reputation of a firm, creating a sense of distrust in clients collaborating with maritime corporations. Partners and industry regulators tend to lose trust in a firm's data integrity safeguards and operational functional systems, resulting in long-term brand trust erosion, tarnished market perception, and loss of prospective clients. Finally, cyber risks in cloud-based VTMS could also lead to legal and regulatory issues for some maritime organizations. Governments as a whole are paying more attention to cybersecurity, having specific laws dealing with vital parts like maritime (Liu et al., 2023) systems. These laws, especially after suffering a cyberattack, have significant consequences if they are not observed. Apart from that, the lack of sufficient measures to defend against cyber risks invites harsher restrictions, increased attention from regulators, and higher compliance costs for maritime operators in the future.

5 Assessing Cyber Threats in Cloud-Based Vessel Traffic Management Systems

Identifying the cyber risks associated with a cloud-based system, such as the Vessel Traffic Management Systems (VTMS), requires a systematic risk assessment process. It is worth evaluating critical threats

such as Denial of Service (DoS) attacks, ransomwares, and spoofing. It is easy to attribute overwhelming control, which brings a system to halt, as a DoS attack. Equally, ransomware capable of locking crucial operational data brings a business to operational standstill. The danger posed by spoofing where attackers manipulate the location data of vessels can result in unsafe navigation and potential vessel collisions unlike any other. Likewise compromising vessel related information by data tampering could alter important operational decisions compromising safety and port operations. Equally important for risk assessment are the vulnerabilities posed by the cloud infrastructure. These include unsecured APIs, weak authentication safeguards, and misconfigured settings within the cloud itself. Each of them increases the likelihood of an attack. Assessing the chances of these vulnerabilities being covered and what results entail gives a better scope at implementing cybersecurity measures. For example, exposing confidential information due to weak access controls changes the risk barometer along with unauthorized entry through misconfigured controls into the hosted cloud services.

Analytical comprehensive assessments or current cloud-based VTMS cybersecurity measures assess the functionality of existing security mechanisms like firewalls, encryption, and intrusion detection systems (IDS). These systems are vital in the protection of controlled data flow, preventing unauthorized access, and the capture of confidential information. Critical components of VTMS multi-factor authentication (MFA) and role-based access control (RBAC) permeate restrictiveness. However, these measures may not address the evolving sophisticated cyber threats. For example, more sophisticated APTs (advanced persistent threats) targeting cloud infrastructures tend to elude detection by traditional firewalls and antivirus solutions. Additionally, due to the cloud resource sharing paradigm, there is a lack of isolation between system components which leads to shared vulnerabilities; if one breach area occurs, it could compromise other sections. Having frequent updates and strong configurations is mandatory in meeting the demands of tertiary risk exposure.

AI-based anomaly detection tools are capable of identifying abnormal actions and even potential cyber threats. In addition, they can help achieve the real-time alerting and self-initiated mitigation of adverse impacts scenarios during an attack.

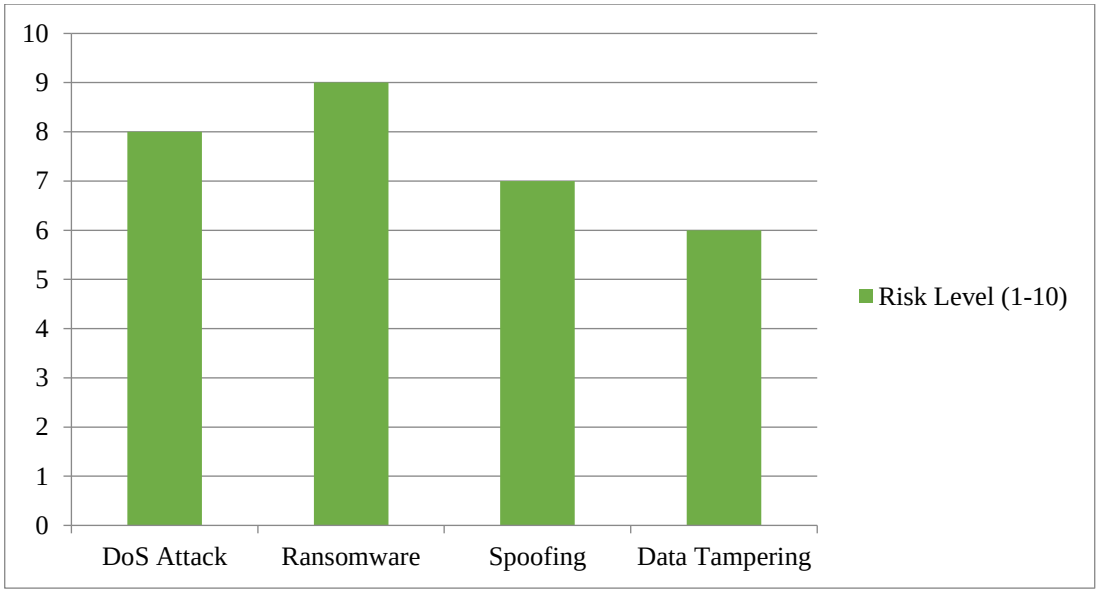

Figure 2: Risk Assessment of Identified Cyber Threats

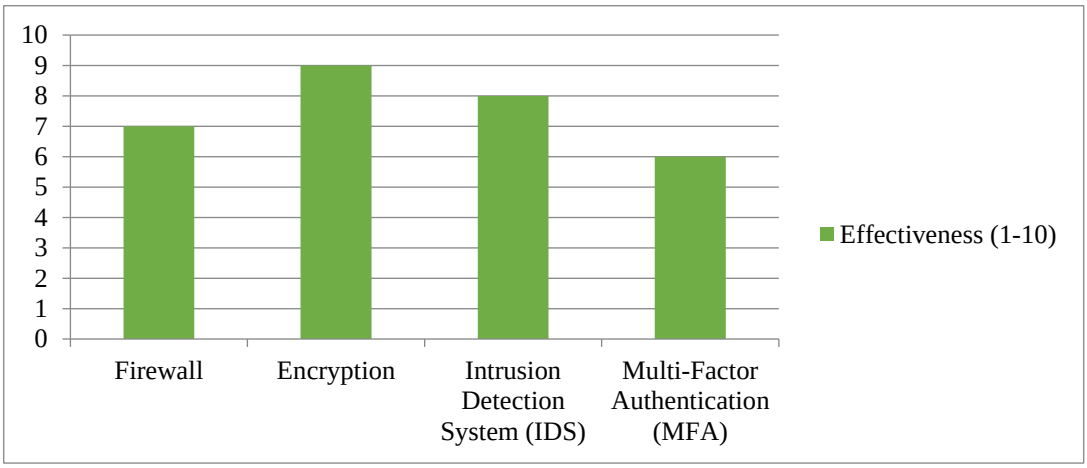

Figure 3: Effectiveness of Current Cybersecurity Measures

In Figure 2, a bar chart is given depicting the risk appraisal of detected cyber threats toward a cloud-based Vessel Traffic Management System (VTMS). The chart analyzes four predominant threats - DoS attacks, ransomware, spoofing and data tampering - concerning their risks rated on a scale of 1 to 10. Based on the assessment of threats, ransomware has the highest risk at (9) and DoS attacks follow closely at (8), whereas spoofing and data tampering pose slightly lesser threats with the scores of 7 and 6 respectively. This chart is helpful in organizing the sequence of tasks in cybersecurity by demonstrating the primary focuses of attention. Figure 3 depicts the current cybersecurity measures established in cloud-based Vessel Traffic Management Systems. Based on our assessment, encryption is the most effective rated at 9, followed by IDS at 8. Firewalls peripherally perform as well achieving a score of 7. Multi-Factor Authentication, despite being important, is rated lower at 6. The evaluation suggests the focus of mitigation strategies should account for the encryption and IDS while also potential to improve execution of MFA framework.

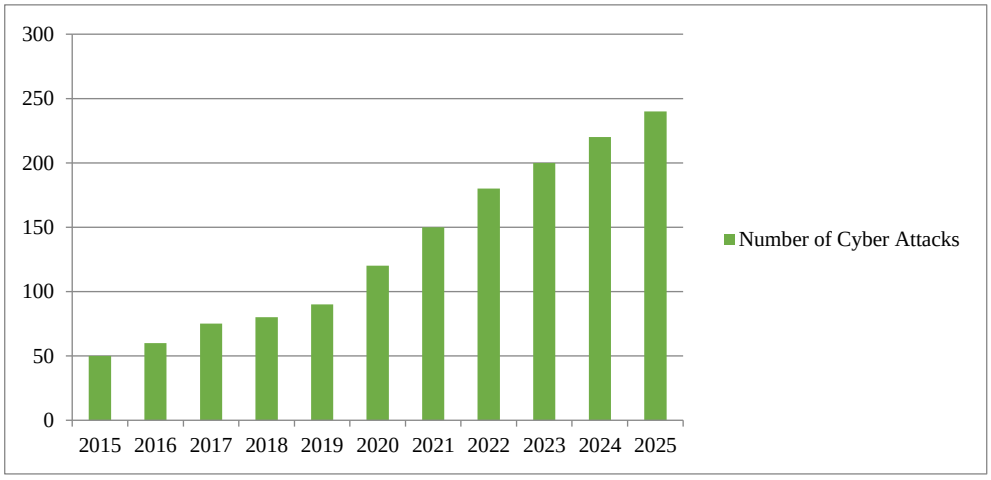

Figure 4: Frequency of Cyber Attacks in Maritime Industry (2015-2025)

As depicted in Figure 4, there is a notable rise in the frequency of cyber attacks in the maritime industry from the year 2015 and estimating this to the year 2025. The widespread cyber attacks are anticipated to spike from around 50 in 2015 to nearly 250 by 2025 which demonstrates a pronounced growth trend. Furthermore, this chronic cyber proliferation illustrates the expanding front of concern in cybersecurity with cloud systems VTMS and its subsystems clearly exhibiting a need for substantial

bolstering of protective actions. As shown in Figure 5, different types of cyber threats have varying impacts on vessel operational downtime. Of all the threats considered, ransomware results in the greatest amount of disruption with about 24 hours of downtime. DoS attacks come next at 12 hours, followed by spoofing at 8 hours and data tampering at 6 hours. This information further attributes the title of the most disruptive to ransomware, underscoring the necessity of strong preventative policies aimed at minimizing operational hold-ups in Vessel Traffic Management Systems. Multi-Factor Authentication (MFA) for all system users along with the practice of least privilege can lower the risk of unauthorized access. Maintenance of these sensitive information access restrictions through regular audits also help prevent breaches. For ever the setting of On-Premise or Cloud Infrastructure, they should apply continuous patching and updates to avoid living vulnerabilities. Continuous observation of resource providers for gaps and having intelligent responses active enhances security posture. VTMS systems store sensitive data that can be intercepted, therefore requiring cloud based VTMS systems to employ AES-256 encryption protocols to guarantee encryption of data in rest and transit.

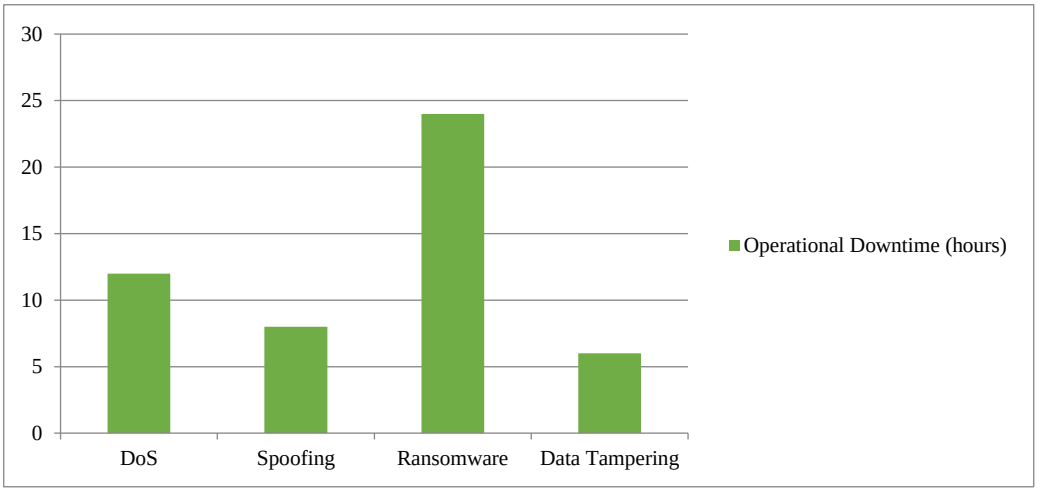

Figure 5: Impact of Cyber Threats on Vessel Operations (Operational Downtime)

A comprehensive incident response plan (CIRP) should be formulated alongside set protocols for responsiveness to cyber-attacks, building proper containment protocols for communication, and reducing bottlenecks that stall progression grit commercially recoverable. Applying Cybersecurity International Standards frameworks ISO/IEC 27001 and NIST Cybersecurity Framework strengthen the over-arching security framework of VTMS, collaborative association with industry counter forward coming threats. By adopting these strategies, VTMS operators will be able to better counter progressing cyber concerns while maintaining the security and effectiveness of maritime activities.

6 Case Study

To better reflect the use of cyber threat modeling in maritime settings, let us discuss Port of NovaMar, an international landmark port that recently upgraded its Vessel Traffic Management System (VTMS) to a cloud-based system. The upgrade was intended to enhance system accessibility, performance optimization, and real-time communication between vessels and port control centers. The port started to encounter unusual issues such as erratic data updates for tracking vessels and unauthorized access indications soon after mounting the system. These deviations prompted track anomalies which delayed the vessel tracking processes and data access control issues. Subsequently, the cybersecurity unit decided to implement the STRIDE approach where the team delineates potential Spoofing, Tampering,

Repudiation, Information Disclosure, DoS, and Exploit Elevation threats. The investigation zeroed in on critical areas of vessel tracking subsystems, cloud APIs, communicating units, and the database management system. APIs related to virtually all components exposed glaring security holes.

Among the results that came from an analysis, a variety of high-threat risks were observed. The most urgent one was AIS (Automatic Identification System) spoofing which included tampering with the positioning of vessels for navigational purposes with one almost docking collision, and near-miss. Equally important in the analysis was the finding of access control misconfigurations within the cloud infrastructure that had inadvertently disclosed sensitive files like crew manifests and internal port communications. In addition, the logs revealed that the VTMS cloud servers had undergone some form of sustained DoS attack with a total outage of twenty minutes during peak service of cargo operations. Moreover, the audits of the system's security logs revealed a number of attempts at unauthorized access via known passwords which can be linked to a phishing attack directed at the employees of the port, some of whom logged in using weak or frequently repeated passwords. Such observations pointed out the need for improved maritime security mechanisms towards Cloud Systems integrated within navigational structures.

This case brings forward several notable discoveries in the field of maritime cyber security. First, it underlined the importance of proactive modeling both before a system is put into operation and after its deployment. STRIDE was utilized hierarchically by NovaMar’s team which would have identified and prioritized threats that posed challenges within exploitation. Second, it showed that cloud environments have distinctive risks of their own to be addressed with cloud-centric security solutions- conventional firewall and antivirus based perimeter defenses do not adequately protect disbursed infrastructure and virtualized environments. Third, it emphasized again the role of human factor in cyber security. Attempts to phish for credentials certainly remind provided the most ironclad systems are susceptible if end users are not appropriately trained. Lastly, the port backup and recovery processes, along with recovery time objectives, uncovered during the assessment phase incident response exercise drove a change in perception toward port procedures. This gave an overhaul to NovaMar's cyber incident response strategy by incorporating off-site encrypted backups, real-time surveillance of backup, and enhanced communication protocols with project stakeholders. In the end, the case is a reminder that tools alone, however advanced they may be, do not by themselves implement security policies, user training, and collaboration between different departments to build an effective cyber-security posture.

7 Conclusion

This research has emphasized the need for cybersecurity measures for cloud-based Vessel Traffic Management Systems (VTMS). This is important due to the increasing digitization of maritime operations. Using modeling and assessment techniques, we detected numerous cyber threats including spoofing, denial of service, and cloud misconfiguration which can fundamentally undermine the safety and security of port operations. The case study from Port of NovaMar demonstrated how sophisticated threat modeling techniques such as STRIDE are capable of revealing malign omissions and facilitating effective risk mitigation. Moreover, risk assessment techniques enabled the ordering of threats in terms of their impact and probability streamlined leading to focused and economically efficient counter-defensive measures. At this point and based on the results of this research, it is evident that the maritime industry needs to have a holistic approach to cybersecurity relative to the particular operational environment. While ports and shipping companies continue to embrace modern cloud-based systems, the threat environment becomes more dynamic and traditional defenses are no longer adequate. To remain competitive and proactively defend against threat advances, the maritime industry must invest in

cloud security, robust real-time monitoring, staff education programs, and more. Equally important, working together is also needed from ports, government institutions, and cybersecurity professionals to come up with common policies and intelligence sharing agreements. It is clear from this research as well as other existing literature that cybersecurity as part of very deep maritime digital transformation is no longer optional, but critical to operational resilience. The capability of artificial intelligence (AI) and machine learning (ML) technologies 'spectives with cybersecurity for VTMS to provide automated response, as well as predictive threat detection, should be pursued in future works. Advanced cyber risk quantitative benchmarks with specific industry focus can also be developed which may aid regional port authorities make informed decisions on security spending; such works would be equally valuable. Comparative research on cloud-based and hybrid architectures of VTMS could also shed light on the balance between flexibility, performance, and risk. Finally, multi-stage longitudinal studies assessing the impact of enduring security changes would provide insight on how changes withstand the test of time against diverse and evolving threats. These works will foster a more resilient, secure maritime cyber environment.

References

[1] Adelard, C., & Penrod, O. (2023). Implementation of Network Security System Using Firewall Technology and Intrusion Detection System (IDS). *Idea: Future Research*, *1*(3), 113-121.

[2] Aisyah, N. (2021). Quantitative Analysis of Distributed Denial-of-Service Mitigation Approaches in Global E-Commerce Cloud Operations. *Perspectives on Next-Generation Cloud Computing Infrastructure and Design Frameworks*, *5*(10), 1-8.

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

[4] Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547-554.

[5] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Berlin, Heidelberg: Springer Berlin Heidelberg.

[6] Arvinth, N. (2023). Digital Transformation and Innovation Management: A Study of How Firms Balance Exploration and Exploitation. *Global Perspectives in Management*, *1*(1), 66-77.

[7] Atashsooz, A., Nejad, R. E., & Sahraiy, M. (2019). Relationship between Personality Traits and Occupational Burnout in the Employees of Mahabad City Government Offices. *International Academic Journal of Organizational Behavior and Human Resource Management*, *6*(1), 52-57. https://doi.org/10.9756/IAJOBHRM/V6I1/1910006

[8] Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A security evaluation of AIS automated identification system. In *Proceedings of the 30th annual computer security applications conference* (pp. 436-445).

[9] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety science*, *131*, 104908. https://doi.org/10.1016/j.ssci.2020.104908

[10] Brother, D. S. L. (2024). The Evolution of the Known. Terrorism in Youth Popular Culture: Teaching the Next Generation from the Cold War to the Present, 169.

[11] Claresta, G., & Baldauf, M. (2020). Vessel Traffic Services (VTS) and e-Navigation to safely and efficiently connect Regions. *Journal für Mobilität und Verkehr*, (6), 29-38.

[12] Das, A., & Kapoor, S. (2024). Comprehensive Review of Evidence-Based Methods in Preventive Cardiology Education: Perspective from Analytical Studies. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 16-22. https://terminologyresearch.com/index.php/gjmtri/article/view/GJMTRI24403

[13] Deshmukh, A., & Nair, K. (2024). An Analysis of the Impact of Migration on Population Growth and Aging in Urban Areas. *Progression Journal of Human Demography and Anthropology*, 1-7. https://hdajournal.com/index.php/pjhda/article/view/PJHDA24401
[14] Eriksen, A. A. (2017). The Risks of Marine Cloud Computing (Master's thesis, NTNU).
[15] Hahn, A., Bolles, A., Fränzle, M., Fröschle, S., & Park, J. H. (2016). Requirements for e-navigation architectures. *International Journal of e-Navigation and Maritime Economy*, *5*, 1-20.
[16] Hlushenkova, A., Kalinin, O., Navrozova, Y., Navolokina, A., Shcherbyna, V., & Doroshenko, T. (2024). Management of Strategies for Shaping the Innovative and Investment Potential of Enterprises as a Factor Ensuring Their Economic Security. *Indian Journal of Information Sources and Services, 14*(3), 16–22. https://doi.org/10.51983/ijiss-2024.14.3.03
[17] Hossain, A. B. M. A., Siddiqua, A., Islam, M. E., Kabir, S. M. H., & Mahdi, G. M. A. (2024). Economic supply chain analysis of Hilsa Fish Landing Centers (Maach Ghats) in Bangladesh: Operational insights and strategies. *International Journal of Aquatic Research and Environmental Studies*, *4*(2), 69-88. http://doi.org/10.70102/IJARES/V4I2/5
[18] IMO. (2017). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3). *International Maritime Organization.*
[19] Iqbal, A. B., Tariq, F., Sumra, I. A., & Rasheed, K. (2025). The Digital Evolution of the Maritime Industry: Unleashing the Power of IoT and Cloud Computing. *Journal of Computing & Biomedical Informatics*, *9*(01). https://doi.org/10.56979/901/2025
[20] Jasim, A. T. (2024). Investigating the Potential of Remote Sensing for Sustainable Urban Renewal and Regeneration: A Review. *International Academic Journal of Science and Engineering*, *11*(1), 54-64. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1108
[21] Jassim, A. (2023). Modern tourism strategies and their impact on revitalizing international tourism. *Sustainable Tourism Review*, *12*(2), 98-115. https://doi.org/10.9756/IAJSS/V10I2/IAJSS1008
[22] Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection, 37*, 100526. https://doi.org/10.1016/j.ijcip.2022.100526
[23] Krishnamurthy, N., & Parvatham, S. (2023). Exploring the Cloud: Vulnerabilities and Cybersecurity Challenges. *International Journal on Recent and Innovation Trends in Computing and Communication*.
[24] Liu, S., Zhu, L., Huang, F., Hassan, A., Wang, D., & He, Y. (2023). A survey on air-to-sea integrated maritime internet of things: Enabling technologies, applications, and future challenges. *Journal of Marine Science and Engineering, 12*(1), 11. https://doi.org/10.3390/jmse12010011
[25] Nandy, M., & Dubey, A. (2024). Effective Surveillance of Water Quality in Recirculating Aquaculture Systems through the Application of Intelligent Biosensors. *Natural and Engineering Sciences*, *9*(2), 234-243. https://doi.org/10.28978/nesciences.1575456
[26] Neumann, T. (2024). Cybersecurity in maritime industry. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 18*.
[27] Papastergiou, S., Kalogeraki, E. M., Polemi, N., & Douligeris, C. (2020). Challenges and issues in risk assessment in modern maritime systems. *Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris*, 129-156.
[28] Perumal, N. (2024). A study to examine vessel traffic services in the context of maritime autonomous surface ships: Strait of Malacca as a case study.
[29] Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and cyber physical security aspects in maritime transportation and port infrastructure. In *Smart ports and robotic systems: Navigating the waves of techno-regulation and governance* (pp. 227-248). Cham: Springer International Publishing.

[30] Sharma, N., & Rajput, A. (2024). Development of A Genomic-based Predictive Model for Warfarin Dosing. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(2), 11-19. https://cjmhp.com/index.php/journal/article/view/2.2.02
[31] 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.
[32] Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime economics & logistics*, *24*(2), 208-227.
[33] Ziwei, M., & Han, L. L. (2023). Scientometric Review of Sustainable Land Use and Management Research. *Aquatic Ecosystems and Environmental Frontiers*, *1*(1), 21-24. https://aquaticfrontiers.com/index.php/aqu/article/view/AF23005

Authors Biography

Capt. Yeshwanth Raj Studied ta Don Bosco High School, Chennai till Matric Exam and Pre university at MCC, Chennai. Joines Training ship Dufferin for Merchant navy training 1970 to 72. Served at sea from 1975 to 2000 in various ascending capacities and had command experience for 20 years. Took to training of cadets joining Amet University from 2000 to date. Currently serving as professor of practise. Also serving as External examiner for conducting Masters, Mates, Ratings examinations. Member of Company of Master Mariners.

Captain P. Rajendran – A Master Mariner and Nautical Visionary, with an unshakable command forged over 28 years at sea, Captain P. Rajendran stands as a stalwart of maritime excellence. Having sailed across the globe on a wide spectrum of merchant vessels — including bulk carriers, general cargo ships, container vessels, Ro-Ro ships, and offshore support vessels. He was spent onboard Dynamic Positioning (DP) vessels and various supply ships, where he executed high-risk deep-sea towing and other operations with precision and expertise. Captain Rajendran has also contributed to maritime education and governance as an External Examiner for GP Rating Examinations (conducted by BEST Mumbai for the Southern Region) and for Second Mate Oral Examinations under the Directorate General of Shipping, MMD. In July 2013, he dropped anchor at AMET University, bringing his vast sea knowledge ashore. Since then, he has been passionately mentoring cadets in various subjects of Nautical Science. His core competencies include: Meteorology, Oceanography, Marine Environmental Science, Chart Work, Cargo Handling and Stowage, Rules of the Road, Ship Operation Technology in last 12 years shaping the next generation of mariners. For the past three years, he has been steering the department as Head of the Department and Course In-Charge, upholding academic standards while infusing real-world maritime acumen into the curriculum. Captain P. Rajendran's journey is not just one of sailing across oceans — it is one of navigating futures, building competence, and embodying the true spirit of a mariner.