Reviewing the need and scope of cybersecurity in real time maritime applications

Shilpa Tanwar[1], Dr. Reena[2]
[1,2]*Department of Computer Science and Application, Baba Mastnath University, Rohtak, Haryana, India-124001*

Abstract: Modern technologies such the cloud, artificial intelligence (AI), and the Internet of Things (IoT) are rapidly transforming the maritime industry digitally, thereby enhancing navigation, cargo handling, and operating effectiveness. Rising reliance on digital technology means that marine operations are more vulnerable from a variety of cybersecurity concerns. Among these hazards include data breaches affecting important maritime infrastructure, attacks on navigation systems, and invasions into onboard networks. Strong cybersecurity rules help to protect ships, ports, and global supply chains. Real-time data exchange is fundamental for maritime operations in situational awareness, threat identification, and autonomous decision making. Covering significant dangers, vulnerabilities, and methods of safeguarding marine operations, this paper explores the vital role of cybersecurity in real-time operating marine systems. Navigational and communication technologies like AIS, GPS, and ECDIS especially interest maritime cybersecurity. By means of malware attacks, GPS spoofing, or jamming, intruders may compromise these systems and redirect ships, pilfers goods, or causes collisions. Because they may disrupt integrated systems that regulate world trade by stopping cargo tracking, customs clearance, and vessel scheduling, ransomware and denial-of- service (DoS) assaults seriously jeopardise port and logistics cybersecurity. The rise of autonomous and remotely piloted watercraft raises cybersecurity issues as these boats rely on control systems in the cloud sensitive to hacks and real-time data flow. One major challenge is that various cargo vessels and transportation firms follow different cybersecurity policies and regulations. Though regulations encouraging cybersecurity awareness—the ISPS Code and the International Maritime Organization's (IMO) guidelines—a more robust legal framework is required to guarantee compliance and increase resilience. Since human mistake is still a main contributor to cyberattacks, constant staff training, cybersecurity exercises, and awareness campaigns are very vital. Essential parts of a multi-layered cybersecurity system meant to reduce these risks include intrusion prevention systems powered by artificial intelligence and machine learning as well as real-time threat monitoring and anomaly detection. While edge computing enables local processing of essential data, hence reducing dependency on centralised cloud services and limiting cyber threats, blockchain technology may provide solutions for secure and irreversible data transmission in the maritime sector.

Keywords: Cybersecurity, DoS, Real time Maritime application, IMO

I. INTRODUCTION

Modern technologies such blockchain, the Internet of Things (IoT), and artificial intelligence (AI) are helping the maritime industry increase operational efficiency and security. Among the cybersecurity issues raised by the quick digitisation are data breaches, ransomware attacks, and assaults on navigation systems. Given the increasing reliance on digital infrastructure, strong cybersecurity rules are very necessary to lower risks and guarantee the security of maritime activities. Several research on cybersecurity in the maritime sector have highlighted possible vulnerabilities and provided various remedies. Conversely, given the growth of autonomous maritime systems and the always changing character of cyberthreats, creating strong cybersecurity methods is an ongoing research focus. This paper examines the present literature on maritime cybersecurity, identifies the gaps, and outlines the future approaches to help to better safeguard the marine sector. The introductory section's structured table below addresses the scope, issues, possible uses, and future directions of marine cybersecurity as well as related aspects.

Table 1Application Areas, Challenges, Scope, and Future Research Directions in maritime cybersecurity

Aspect	Details
Application Areas	- Autonomous Ships: Ensuring secure communication, navigation, and control in autonomous vessels. - Port Security: Protection of port infrastructure, cargo tracking, and logistics networks. - Maritime IoT& Smart Shipping: Securing IoT devices used in fleet management, fuel monitoring, and predictive maintenance. - Maritime Cloud Computing: Data protection in cloud-based vessel management systems. - Naval & Defense Systems: Securing naval operations from cyber warfare and espionage threats. - Blockchain-based Shipping & Transactions: Enhancing security in digital transactions and trade documentation.
Challenges	- Cyber Threats: Increasing ransomware, phishing, and malware attacks targeting maritime systems. - Lack of Awareness & Training: Crew members often lack cybersecurity expertise. - Legacy Systems & Integration Issues: Many maritime systems operate on outdated technology with weak security protocols. - Data Privacy & Compliance: Ensuring compliance with global cybersecurity regulations (e.g., IMO 2021, GDPR). - Scalability & Real-time Response: Securing communication between multiple vessels in real-time without latency. - Supply Chain Vulnerabilities: Risk of cyberattacks in interconnected supply chain networks.
Scope	- Developing AI-driven cybersecurity solutions for anomaly detection in maritime networks. - Enhancing blockchain integration for secure maritime transactions and document verification. - Implementing real-time intrusion detection systems in vessel communication. - Strengthening collaborations between maritime industries and cybersecurity experts. - Adoption of zero-trust architecture for access control in maritime operations.
Future Research Directions	- Quantum Cryptography: Exploring quantum-resistant encryption for secure maritime communication. - Federated Learning for Cybersecurity: Decentralized AI models for threat detection in smart ships. - Integration of 5G & Edge Computing: Ensuring secure, low-latency communication between vessels and ports. - Game Theory-Based Attack Prevention: Using game-theoretic models to predict and prevent cyberattacks. - Enhanced Simulation & Digital Twins: Creating cybersecurity testbeds for maritime security validation.

II. LITERATURE REVIEW

Maritime cybersecurity has gained significant attention as the industry undergoes digital transformation, integrating technologies such as IoT, AI, and blockchain.

2.1 Existing research work

Katsikas et al. (2025) discuss upcoming trends in maritime cybersecurity, highlighting the need for advanced cybersecurity frameworks and proactive threat management. Tabish and Chaur-Luh (2024) identify cyber-physical vulnerabilities and countermeasures via the lens of cybersecurity challenges in Maritime Autonomous Surface Ships (MASS). Valky et al. (2024) propose a hybrid cybersecurity research and education ecosystem to enhance cyber resilience via policy formation and training.

The most recent research on marine cybersecurity by Yu et al. (2023) reveals security flaws in navigation and communication systems. Complete cybersecurity integration into maritime navigation equipment is supported by Boudehenn et al. (2023), who emphasise system-wide security protocols. In their systematic review of recent developments and forthcoming trends in maritime cybersecurity, Ben Farah et al. (2022) pinpoints knowledge gaps in artificial intelligence (AI)-driven threat detection and blockchain security.

Marine monitoring system suggested by Freire et al. (2022) that uses blockchain technology and the Internet of Things (IoT) to improve security and scalability In his discussion on cybersecurity in the maritime industry, Neumann (2024) proposes complex methods for evaluating potential threats. Kechagias et al. (2022) explore the digital revolution in marine cybersecurity, with a focus on systemic security measures. Akpan et al. (2022) investigate cybersecurity concerns, highlighting the need of legislative frameworks in enhancing maritime security.

To back up more effective awareness efforts, Canepa et al. (2021) assess the effectiveness of cybersecurity training in the maritime industry. Androjna et al. (2020) evaluate cyberspace issues in sea navigation, stressing the significance of real-time threat detection. In their investigation of emerging technologies in maritime cybersecurity, Tam and Jones (2019) look at new attack vectors and ways to protect against them. A unified mechanism for reporting cybersecurity incidents is recommended for the maritime sector by Silverajan and Vistiaho (2019).

Examining maritime cybersecurity models, Lagouvardou (2018) highlights conceptual challenges and policy limitations. The importance of understanding cybersecurity in sea transportation is highlighted by Lee et al. (2017). Hassani et al. (2017) investigate cyber risks in navigation systems from a control point of view. Boyes (2014) and Fitton et al. (2015) discuss safeguarding maritime digital infrastructure, with an emphasis on initial cybersecurity concerns and guidelines.

2.2 Research Gap

Despite extensive research on maritime cybersecurity, several gaps remain:

- Integration of AI in Threat Detection: Limited research on AI-driven predictive analytics for real-time cyber threat mitigation.
- Blockchain for Secure Communication: Insufficient studies exploring blockchain-based maritime communication security.
- Cybersecurity Frameworks for Autonomous Systems: Need for robust frameworks addressing cybersecurity in MASS.
- Human Factor Considerations: Gaps in research on human errors and cybersecurity awareness in maritime operations.
- Standardized Regulatory Policies: Inconsistent implementation of cybersecurity regulations across global maritime operations.

Table 2 Summary Table

S.No	Author(s)	Year	Objective	Methodology	Limitation
1	Katsikas et al.	2025	Future trends in maritime cybersecurity	Literature review	Lacks empirical validation of proposed trends
2	Tabish&Chaur-Luh	2024	Cybersecurity challenges in MASS	Review and analysis	Limited focus on real-world implementation

S.No	Author(s)	Year	Objective	Methodology	Limitation
3	Visky et al.	2024	Hybrid cybersecurity research and education	Case study	Lacks scalability assessment
4	Yu et al.	2023	State-of-the-art maritime cybersecurity	Systematic review	Limited real-time threat evaluation
5	Boudehenn et al.	2023	Holistic cybersecurity in navigation equipment	Case study	Does not address regulatory compliance
7	Ben Farah et al.	2022	Advances and future trends in maritime cybersecurity	Survey analysis	Limited focus on blockchain integration
8	Freire et al.	2022	Blockchain-based maritime monitoring	System design	Requires further scalability testing
8	Neumann	2024	Maritime industry cybersecurity challenges	Risk assessment models	Limited empirical validation
10	Kechagias et al.	2022	Cybersecurity systemic approach in maritime	Theoretical framework	Needs practical implementation
11	Akpan et al.	2022	Cybersecurity challenges in maritime	Literature review	Does not address AI-based threat detection
13	Canepa et al.	2021	Cybersecurity training effectiveness	Empirical study	Needs long-term assessment
14	Androjna et al.	2020	Cyber challenges in maritime navigation	Review study	Limited focus on autonomous navigation
15	Tam & Jones	2019	Review of emerging maritime cybersecurity tech	Literature review	Lacks implementation strategies
16	Silverajan&Vistiaho	2019	Incident reporting and cybersecurity handling	Case study	Needs a larger data sample
17	Lagouvardou	2018	Maritime cybersecurity models	Theoretical analysis	Lacks real-world validation
18	Lee et al.	2017	Improving cyber awareness in maritime transport	Survey analysis	Limited regional scope
19	Hassani et al.	2017	Cyber threats in maritime navigation systems	Control analysis	Lacks AI-driven mitigation techniques
20	Fitton et al.	2015	Future of maritime cybersecurity	Theoretical review	Needs updated analysis
21	Boyes	2014	Securing maritime digital seaways	Literature review	Lacks focus on evolving threats

III. PROBLEM STATEMENT

The field of maritime cybersecurity has made some progress, but it still faces several challenges. From a security perspective, there are significant issues due to the maritime industry's reliance on digital infrastructure and the increasing sophistication of cyber assaults. Particularly in the setting of connected Internet of Things devices and autonomous maritime systems, existing cybersecurity standards often fall short in dealing with increasing threats. The fact that human error exacerbates vulnerabilities is another

consequence of the ongoing lack of adequate cybersecurity training and awareness programs. The marine sector is in dire need of all-encompassing cybersecurity solutions to safeguard maritime operations against cyberattacks. These solutions must include advanced encryption technologies, constant monitoring, and real-time threat identification.

IV. SIGNIFICANCE OF RESEARCH

This sort of research is essential for finding solutions to the growing cybersecurity problems in the maritime industry. This paper analyses existing research and identifies vulnerabilities to assist design cybersecurity solutions that are more efficient. Marine operations that prioritise cybersecurity protect vital infrastructure in addition to crew members, products, and global supply chains. Additionally, in line with international maritime security regulations, strengthening cybersecurity measures promotes resilience against cyber risks and reduces financial losses associated with cyber occurrences.

V. REVIEW OF INFLUENCING FACTORS

Marine cybersecurity is impacted by emerging cyberthreats, human factors, legal systems, technical innovations, and regulatory frameworks. New security paradigms brought about by the extensive use of artificial intelligence and blockchain provide opportunities as well as hazards. Although regulatory bodies like the International Maritime Organisation (IMO) help to establish cybersecurity rules, enforcement and compliance across different sectors remain lacking uniformity. Human factors include cybersecurity awareness and education significantly influence the effectiveness of security systems. Since cyberattacks are becoming more complex, cybersecurity solutions also must be continuously upgraded to address flaws in new digital systems.

VI. FUTURE SCOPE

The primary focus of future research should be on developing adaptive cybersecurity frameworks that integrate AI-driven threat detection with blockchain-based data protection. Efforts to better educate maritime professionals on cybersecurity are crucial to lowering risks caused by humans. Collaboration across sectors, such as the maritime industry and cybersecurity research, might lead to the development of industry-wide security standards. The impact of quantum computing on maritime cybersecurity and the prospect of next-generation encryption technologies are further areas that need more investigation. A stronger and safer marine environment may be achieved via future research that addresses these factors and ensures the sustainability of digital transformation in the maritime industry.

REFERENCE

[1] Katsikas, S. K., Kavallieratos, G., &Amro, A. (2025). Future Trends in Maritime Cybersecurity. In *Computer and Information Security Handbook* (pp. 1663-1678). Morgan Kaufmann.

[2] Tabish, N., &Chaur-Luh, T. (2024). Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access*, *12*, 17114-17136.

[3] Visky, G., Šiganov, A., urRehman, M., Vaarandi, R., Bahşi, H., Bahsi, H., &Tsiopoulos, L. (2024, September). Hybrid Cybersecurity Research and Education Environment for Maritime Sector. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 644-651). IEEE.

[4] Yu, H., Meng, Q., Fang, Z., & Liu, J. (2023). Literature review on maritime cybersecurity: state-of-the-art. *The Journal of Navigation*, *76*(4-5), 453-466.

[5] Boudehenn, C., Cexus, J. C., Abdelkader, R., Lannuzel, M., Jacq, O., Brosset, D., &Boudraa, A. (2023, March). Holistic approach of integrated navigation equipment for cybersecurity at sea. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales* (pp. 75-86). Singapore: Springer Nature Singapore.

[6] Yu, H., Meng, Q., Fang, Z., & Liu, J. (2023). Literature review on maritime cybersecurity: state-of-the-art. *The Journal of Navigation*, *76*(4-5), 453-466.

[7] Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I.,

&Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), 22.

[8] Freire, W. P., Melo Jr, W. S., do Nascimento, V. D., Nascimento, P. R., & de Sá, A. O. (2022). Towards a secure and scalable maritime monitoring system using blockchain and low-cost IoT technology. *Sensors*, *22*(13), 4895.

[9] Neumann, T. (2024). Cybersecurity in Maritime Industry. *TransNav: International Journal on Marine Navigation & Safety of Sea Transportation*, *18*(4).

[10] 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.

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

[12] Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., &Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), 22.

[13] Canepa, M., Ballini, F., Dalaklis, D., &Vakili, S. (2021). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. In *INTED2021 Proceedings* (pp. 3489-3499). IATED.

[14] Androjna, A., Brcko, T., Pavic, I., &Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), 776.

[15] Tam, K., & Jones, K. (2019). A cyber-security review of emerging technology in the maritime industry.

[16] Silverajan, B., &Vistiaho, P. (2019, August). Enabling cybersecurity incident reporting and coordinated handling for maritime sector. In *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)* (pp. 88-95). IEEE.

[17] Lagouvardou, S. (2018). Maritime Cyber Security: concepts, problems and models. *KongensLyngby, Copenhagen*.

[18] Lee, Y. C., Park, S. K., Lee, W. K., & Kang, J. (2017). Improving cyber security awareness in maritime transport: A way forward. *Journal of Advanced Marine Engineering and Technology (JAMET)*, *41*(8), 738-745.

[19] Hassani, V., Crasta, N., &Pascoal, A. M. (2017, June). Cyber security issues in navigation systems of marine vessels from a control perspective. In *International Conference on Offshore Mechanics and Arctic Engineering* (Vol. 57748, p. V07BT06A029). American Society of Mechanical Engineers.

[20] Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. *Lancaster University*, 8.

[21] Boyes, H. A. (2014). Maritime cyber security–securing the digital seaways. *Engineering & Technology Reference*, (2014).