AI And Blockchain-Driven Cybersecurity Approaches For Real-Time Maritime Systems

MS Shilpa Tanwar
Research Scholar
Department Of Computer Science & Applications
Baba Mastnath University
Rohtak, India

Dr Reena
Assistant Professor
Department Of Computer Science & Applications
Baba Mastnath University
Rohtak, India

Abstract:
Modern technologies like the cloud, AI, and the Internet of Things (IoT) are swiftly changing the maritime sector digitally. This makes navigation, freight management, and operations more efficient. Marine operations are becoming more and more reliant on digital technology, which makes them more vulnerable to a range of cybersecurity problems.

Some of these hazards include data breaches that affect important marine infrastructure, attacks on navigation systems, and people getting into networks on board without permission.

Strong cybersecurity rules help protect ships, ports, and the global supply chain.

For marine operations to be aware of their surroundings, recognize threats, and make decisions on their own, they need to be able to exchange data in real time.

This article talks about how crucial cybersecurity is for real-time operational maritime systems. It talks about major threats, weaknesses, and ways to secure marine operations.

Maritime cybersecurity is mostly concerned with navigation and communication technologies such as AIS, GPS, and ECDIS.

Malware assaults, GPS spoofing, or jamming can let intruders penetrate these systems and modify the path of ships, steal goods, or cause crashes.

Ransomware and denial-of-service (DoS) attacks are especially bad for port and logistics cybersecurity because they can stop cargo tracking, customs clearance, and vessel scheduling. These are all aspects of systems that are connected to each other and regulate world trade.

There are cybersecurity worries since more and more boats are self-driving or remotely piloted. These boats rely on cloud-based control systems that are easy to hack and provide data in real time. One major issue is that different shipping companies and cargo ships have varying policies and requirements for cybersecurity. The ISPS Code and the International Maritime Organization's (IMO) suggestions are two examples of rules that help people understand how to protect their computers.

But we need a stronger legal system to make sure that these laws are obeyed and to make systems stronger. Most of the time, cyberattacks arise because of mistakes made by people. That's why it's so crucial to constantly training personnel, holding cybersecurity drills, and running awareness campaigns.

Intrusion prevention systems, real-time threat monitoring, and anomaly detection that use AI and machine learning are all critical parts of a multi-layered cybersecurity system that tries to decrease these risks.

Edge computing lets essential data be handled on the spot, which means that centralized cloud services are less necessary and cyber dangers are less likely to happen.

Blockchain technology might be able to help the marine industry move data safely and permanently.

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

Date of Submission: 18-09-2025 Date of Acceptance: 28-09-2025

I. Introduction

Blockchain, the Internet of Things (IoT), and artificial intelligence (AI) are all new technologies that are making the maritime industry safer and more efficient. Some of the cybersecurity issues that come up due of how quickly things are going digital are data breaches, ransomware attacks, and attacks on navigation systems. We need robust cybersecurity standards to secure maritime activities and minimize risks because we are using digital infrastructure more and more. Many research on cybersecurity in the maritime industry have found possible threats and suggested different ways to fix them. The emergence of autonomous maritime systems and the constant evolution of cyber threats necessitate continued research into robust cybersecurity solutions. This article examines the existing literature on marine cybersecurity, identifies shortcomings, and outlines potential solutions to improve the industry's security. The structured table below in the introduction talks about the range, issues, possible uses, and future directions of maritime cybersecurity and other related topics.

Table 1: Application 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.

Existing research work

Recent research indicates that blockchain and artificial intelligence have the potential to significantly improve various domains. Akhtar (2025) [1] discusses the potential transformation of manufacturing with AI and blockchain in the digital era. Gupta and Gupta (2025) examine tokenomics to promote enduring growth in ecosystems by contrasting solutions like liquidity pools and token burning [2]. Saidu et al. (2025) [3] say that blockchain, the Internet of Things, and AI can all help with improved data management and tracking in complicated systems. Rahman et al. (2025) [4] demonstrate the potential of distributed ledger applications to enhance supply chain transparency, whereas Reem et al. (2025) [5] investigate the application of blockchain and AI in the management of biofilms within food processing. Sachdeva et al. (2025) discuss the potential of blockchain to facilitate cross-border collaboration among tourism enterprises. They underline how crucial it is for operations to be clear and safe [6]. Bommali (2024) has noted that innovative concepts in shipping and port management can enhance operational efficiency and promote environmental sustainability [7]. Achebe et al.

(2024) offer blockchain frameworks to improve corporate fraud risk management [9], whereas Islam et al. (2024) assess blockchain-enabled cybersecurity for scalable heterogeneous networks [8]. Arinze et al. (2024) emphasize the utilization of AI in oil and gas engineering to improve efficiency and safety [11], whilst Oyeyemi et al. (2024) highlight the amalgamation of blockchain and AI in fostering supply chain transparency [10]. Gupta, Gupta, and Duggal (2023) [12] discuss the impact of NFT culture on digital assets, whereas Van Nguyen et al. (2023) [13] examine the potential applications of blockchain in supply chain management. Both papers attempt to identify research issues and prospective opportunities. Sadri et al. (2023) investigate the integration of blockchain and digital twins inside intelligent built environments [15], whereas Zaman et al. (2023) concentrate on blockchain and Industry 4.0 technologies to improve supply chain efficiency [14]. Gupta (2023) investigates the correlation between blockchain technology and NFTs inside significant markets, while Lun et al. (2023) address advancements in shipping technology designed to improve efficiency and stimulate innovation [16]. Wang et al. (2023) investigate the utilization of blockchain technology in the Internet of Vehicles (IoV), highlighting the associated obstacles and potential solutions [18]. Matenga and Mpofu (2022) suggest a cloud-based supply chain management system employing blockchain technology, whereas Begum et al. (2022) examine blockchain technology in trade finance and banking, emphasizing transparency and security [19]. Shahzad, Aseeri, and Shah (2022) provide a blockchain-based authentication solution for 6G networks [22], and Hasan, Chaudhary, and Alam (2022) create a blockchain federated safety-as-a-service framework for industrial IoT [21]. Brohi (2021) analyzes the integration of IoT and blockchain to improve data integrity, whereas Kapadiya et al. (2022) explore blockchain and AI for detecting healthcare insurance fraud [23]. while Brohi (2021) reviews IoT-blockchain integration for improved data integrity [24]. Velmovitsky et al. (2021) [25] assert that the implementation of blockchain technology in healthcare could enhance transparency and accountability.

Table 2: Existing research work

Ref. No	Author / Year	Objective	Methodology	Conclusion
1	Akhtar, Z. B. (2025)	Explore AI integration with blockchain across industries	Literature review and conceptual analysis	AI and blockchain together can drive digital transformation, improving efficiency and decision-making across sectors
2	Gupta, M., & Gupta, D. (2025)	Compare token burning and liquidity pool strategies for sustainable growth	Comparative analysis of tokenomics strategies	Token burning and liquidity pools enhance ecosystem sustainability, with different trade-offs for growth
3	Saidu, Y. et al. (2025)	Review convergence of blockchain, IoT, and AI for traceability	Systematic literature review	Integration improves traceability systems, offering better transparency and real-time monitoring
4	Rahman, M. S. et al. (2025)	Investigate blockchain for supply chain transparency	Data-driven analysis using case studies	Blockchain enhances supply chain transparency and accountability in logistics
5	Reem, C. S. A. et al. (2025)	Apply blockchain and AI to biofilm control in food processing	Literature review and experimental insights	Blockchain-AI integration improves monitoring and control of biofilms in food safety
6	Sachdeva, C. et al. (2025)	Study cross-border collaboration using blockchain in tourism	Review and case analysis	Blockchain enables secure, transparent, and efficient international collaboration in travel
7	Bommali, T. (2024)	Examine digital innovations in port and shipping management	Case studies and industry review	Digital transformation improves operational efficiency and sustainability in shipping
8	Islam, M. et al. (2024)	Explore blockchain-enabled cybersecurity for heterogeneous networks	Comprehensive survey	Blockchain enhances network security and scalability in heterogeneous systems
9	Achebe, V. C. et al. (2024)	Address corporate fraud risk via blockchain	Conceptual framework and case analysis	Blockchain improves data integrity and legal accountability in corporate environments
10	Oyeyemi, B. B. et al. (2024)	Explore synergies between blockchain and AI in supply chains	Review and application analysis	Integration of AI and blockchain enhances supply chain visibility and efficiency
11	Arinze, C. A. et al. (2024)	Integrate AI in engineering for oil & gas operations	Case studies and simulation	AI improves efficiency, safety, and decision-making in engineering processes
12	Gupta, M., D. Gupta, & A. Duggal (2023)	Examine NFT culture and implications	Literature review	NFTs create new digital asset ecosystems and cultural engagement
13	Van Nguyen, T. et al. (2023)	Review blockchain applications in supply chain management	Data-driven literature review	Blockchain adoption in supply chains improves traceability and efficiency, highlighting key research themes

14	Zaman, S. A. A. et al. (2023)	Study blockchain-driven supply chain and Industry 4.0 integration	Review analysis	Blockchain integration with Industry 4.0 enhances efficiency and transparency in supply chains
15	Sadri, H. et al. (2023)	Integrate blockchain with digital twins in smart environments	Systematic review	Blockchain and digital twins improve monitoring, automation, and data security in built environments
16	Lun, Y. V. et al. (2023)	Explore new technology adoption in shipping	Literature review	Adoption of digital technologies improves shipping industry efficiency and competitiveness
17	Gupta, M. (2023)	Review relationship between blockchain and NFTs in marketplaces	Literature review	NFTs and blockchain together transform digital marketplaces and asset ownership
18	Wang, X. et al. (2023)	Study blockchain for Internet of Vehicles (IoV)	Review and survey	Blockchain enhances IoV intelligence, addressing security and operational challenges
19	Begum, A. et al. (2022)	Review blockchain in trade finance and banking	Systematic review	Blockchain improves security, transparency, and efficiency in trade finance and banking
20	Matenga, A. E., & Mpofu, K. (2022)	Develop blockchain-based cloud manufacturing SCM	Case study	Blockchain-enabled SCM enhances collaboration and traceability in manufacturing
21	Hasan, N. et al. (2022)	Propose blockchain federated safety-as-a-service for IIoT	ML-based framework development	Federated blockchain improves industrial IoT safety and predictive analytics
22	Shahzad, K. et al. (2022)	Blockchain-based authentication for 6G networks	Technical framework and simulation	Blockchain strengthens 6G network security and authentication
23	Kapadiya, K. et al. (2022)	Blockchain-AI for healthcare insurance fraud detection	Architecture design and analysis	Integrated approach enhances fraud detection accuracy and efficiency
24	Brohi, M. N. (2021)	Integrate IoT with blockchain	Conceptual and technical review	IoT-blockchain integration supports secure, real-time data management
25	Velmovitsky, P. E. et al. (2021)	Apply blockchain in healthcare and public health	Literature review and case analysis	Blockchain increases transparency, data security, and trust in healthcare systems

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.

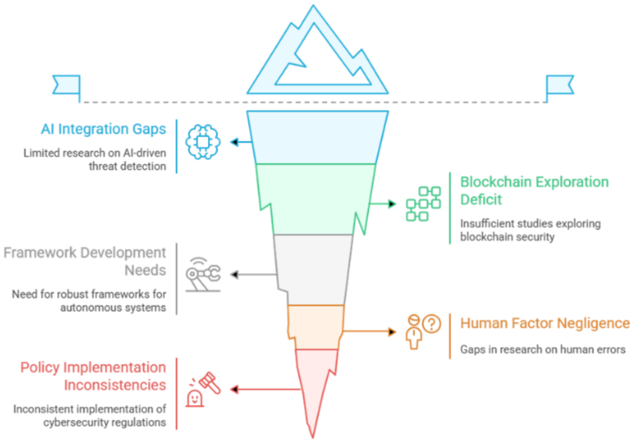
AI Integration Gaps
Limited research on AI-driven threat detection
Blockchain Exploration Deficit
Insufficient studies exploring blockchain security
Framework Development Needs
Need for robust frameworks for autonomous systems
Human Factor Negligence
Gaps in research on human errors
Policy Implementation Inconsistencies
Inconsistent implementation of cybersecurity regulations

Figure 1: Research Gap

Problem Statement

There has been some progress in maritime cybersecurity, but there are still a lot of issues to work out. The marine industry has a lot of security challenges because it relies on digital infrastructure and cyber attacks are getting better. When it comes to linked Internet of Things devices and autonomous maritime systems, current cybersecurity rules don't always do a good job of dealing with new threats. Another disadvantage of not having good cybersecurity training and awareness programs all the time is that human error makes vulnerabilities worse. The marine industry requires full cybersecurity solutions right away to keep maritime activities safe from threats. These systems need to have the latest encryption, be watched all the time, and be able to discover threats right away.

Significance of Research

We need this kind of research to find methods to tackle the maritime industry's growing cybersecurity problems. This article looks at existing studies and points out problems to help make better cybersecurity solutions. Cybersecurity is very crucial for marine operations that protect important infrastructure, crew members, goods, and global supply networks. Also, following international marine security laws, improving cybersecurity helps keep cyber threats at bay and minimizes the costs of cyber catastrophes.

Review of Influencing Factors

Cybersecurity for ships is affected by new cyberthreats, human factors, legal systems, technology advances, and regulatory frameworks. The increased use of blockchain and artificial intelligence has led to new security models that have both pros and cons. Even though groups like the International Maritime Organization (IMO) help create standards for cybersecurity, not all industries follow them all the time. Two major human factors that determine how well security solutions perform are knowledge and education about cybersecurity. As cyberattacks get more intricate, cybersecurity solutions need to be updated all the time to fix problems in new digital systems.

Future Scope

Future research ought to focus on developing adaptive cybersecurity frameworks that integrate AI-driven threat detection with blockchain-based data protection. It is vital to teach maritime workers more about cybersecurity to make them less dangerous. Collaboration between different domains, such as the marine industry and cybersecurity research, could result in the development of security standards that are applicable to all sectors. We need to learn more about how quantum computing will change maritime cybersecurity and what the next generation of encryption technologies will look like. Future research that examines these concerns and ensures the sustainability of the digital revolution in the maritime sector will enhance the marine environment's resilience and safety.

Reference

[1]. Akhtar, Z. B. (2025). Artificial Intelligence (AI) Meets Blockchain: Transforming Industries For The Next Digital Era. Interdisciplinary Systems For Global Management, 1(1), 59-75.

[2]. M. Gupta And D. Gupta, "Enhancing Tokenomics: A Comparative Study Of Token Burning And Liquidity Pool Strategies For Sustainable Ecosystem Growth," Sci. J. Metaverse Blockchain Technol., Vol. 3, No. 1, Pp. 8–26, 2025, Doi: 10.36676/Sjmbt.V3.I1.54.

[3]. Saidu, Y., Shuhidan, S. M., Aliyu, D. A., Aziz, I. A., & Adamu, S. (2025). Convergence Of Blockchain, Iot, And AI For Enhanced Traceability Systems: A Comprehensive Review. IEEE Access.

[4]. Rahman, M. S., Hossain, M. S., Rahman, M. K., Islam, M. R., Sumon, M. F. I., Siam, M. A., & Debnath, P. (2025). Enhancing Supply Chain Transparency With Blockchain: A Data-Driven Analysis Of Distributed Ledger Applications. Journal Of Business And Management Studies, 7(3), 59-77.

[5]. Reem, C. S. A., Chowdhury, M. A. H., Ashrafudoulla, M., & Ha, S. D. (2025). Leveraging Blockchain And AI For Biofilm Control In Food Processing Environments. Comprehensive Reviews In Food Science And Food Safety, 24(5), E70261.

[6]. Sachdeva, C., Kaur, P., Gangwar, V. P., &Jasrai, L. (2025). Cross-Border Collaboration In New Digital Era With Blockchain Integration. In Blockchain In The Tourism Industry: A New Era Of Secure And Transparent Travel Solutions (Pp. 235-266). Cham: Springer Nature Switzerland.

[7]. Bommali, T. (2024). Innovations In Port And Shipping Management: Enhancing Operational Efficiency, Sustainability, And Digital Transformation. International Journal Of Applied Science And Engineering, 12(2), 161-191.

[8]. Islam, M., Rahman, M., Ariff, M., Ajra, H., Ismail, Z., & Zain, J. (2024). Blockchain-Enabled Cybersecurity Provision For Scalable Heterogeneous Network: A Comprehensive Survey. Computer Modeling In Engineering & Sciences, 138(1), 43.

[9]. Achebe, V. C., Ilori, O., & Isibor, N. J. (2024). Enhancing Data Integrity And Legal Accountability: A Blockchain-Driven Approach To Corporate Fraud Risk Management.

[10]. Oyeyemi, B. B., Orenuga, A., & Adelakun, B. O. (2024). Blockchain And AI Synergies In Enhancing Supply Chain Transparency.

[11]. Arinze, C. A., Izionworu, V. O., Isong, D., Daudu, C. D., &Adefemi, A. (2024). Integrating Artificial Intelligence Into Engineering Processes For Improved Efficiency And Safety In Oil And Gas Operations. Open Access Research Journal Of Engineering And Technology, 6(1), 39-51.

[12]. M. Gupta, D. Gupta, And A. Duggal, "NFT Culture: A New Era," Sci. J. Metaverse Blockchain Technol., Vol. 1, No. 1, Pp. 57–62, 2023, Doi: 10.36676/Sjmbt.V1i1.08.

[13]. Van Nguyen, T., Cong Pham, H., Nhat Nguyen, M., Zhou, L., & Akbari, M. (2023). Data-Driven Review Of Blockchain Applications In Supply Chain Management: Key Research Themes And Future Directions. International Journal Of Production Research, 61(23), 8213-8235.

[14]. Zaman, S. A. A., Dawood, H. M., Zehra, S. N., & Saeed, S. Z. (2023). Blockchain Driven Supply Chain And Industry 4.0 Technologies. In Blockchain Driven Supply Chain Management: A Multi-Dimensional Perspective (Pp. 219-238). Singapore: Springer Nature Singapore.

[15]. Sadri, H., Yitmen, I., Tagliabue, L. C., Westphal, F., Tezel, A., Taheri, A., &Sibenik, G. (2023). Integration Of Blockchain And Digital Twins In The Smart Built Environment Adopting Disruptive Technologies—A Systematic Review. Sustainability, 15(4), 3713.

[16]. Lun, Y. V., Lai, K. H., Cheng, T. E., & Yang, D. (2023). New Technology Development In The Shipping Industry. In Shipping And Logistics Management (Pp. 257-279). Cham: Springer International Publishing.

[17]. M. Gupta, "Reviewing The Relationship Between Blockchain And NFT With World Famous NFT Market Places," SJMBT, Vol. 1, No. 1, Pp. 1–8, Dec. 2023.

[18]. Wang, X., Zhu, H., Ning, Z., Guo, L., & Zhang, Y. (2023). Blockchain Intelligence For Internet Of Vehicles: Challenges And Solutions. IEEE Communications Surveys & Tutorials, 25(4), 2325-2355.

[19]. Begum, A., Munira, M. S. K., &Juthi, S. (2022). Systematic Review Of Blockchain Technology In Trade Finance And Banking Security. American Journal Of Scholarly Research And Innovation, 1(01), 25-52.

[20]. Matenga, A. E., & Mpofu, K. (2022). Blockchain-Based Cloud Manufacturing SCM System For Collaborative Enterprise Manufacturing: A Case Study Of Transport Manufacturing. Applied Sciences, 12(17), 8664.

[21]. Hasan, N., Chaudhary, K., & Alam, M. (2022). A Novel Blockchain Federated Safety-As-A-Service Scheme For Industrial Iot Using Machine Learning. Multimedia Tools And Applications, 81(25), 36751-36780.

[22]. Shahzad, K., Aseeri, A. O., & Shah, M. A. (2022). A Blockchain-Based Authentication Solution For 6G Communication Security In Tactile Networks. Electronics, 11(9), 1374.

[23]. Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., &Bokoro, P. N. (2022). Blockchain And AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, And Future Prospects. Ieee Access, 10, 79606-79627.

[24]. M. N. Brohi, "Integration Of Iot And Blockchain," Tech. Rom. J. Appl. Sci. Technol., Vol. 3, No. 8, Pp. 32–41, 2021, Doi: 10.47577/Technium.V3i8.4692.

[25]. P. E. Velmovitsky, F. M. Bublitz, L. X. Fadrique, And P. P. Morita, "Blockchain Applications In Health Care And Public Health: Increased Transparency," JMIR Med. Inform., Vol. 9, No. 6, P. E20713, 2021.