Title : Cybersecurity in Maritime IoT and Critical Systems: A Comprehensive Review

Affiliations

Omkar Santosh Ghodekar
Student
Department Of Computer Engineering,
D.Y. Patil College Of Engineering Akurdi,
Pune, Maharashtra, India.
omkarghodekar140803@gmail.com

Mrs. Dipalee D. Rane
Assistant Professor
Department Of Computer Engineering,
D.Y. Patil College Of Engineering Akurdi,
Pune, Maharashtra, India.
ddrane@dypcoeakurdi.ac.in

Tejas Sanjay Vadar
Student
Department Of Computer Engineering,
D.Y. Patil College Of Engineering Akurdi,
Pune, Maharashtra, India.
tejasvadar2810@gmail.com

Abstract

The research report provides a comprehensive analysis of cybersecurity challenges and strategies in key areas, focusing on maritime IoT cybersecurity, big data security, cyber (CPS) and electronic equipment. It examines vulnerabilities and threats related to maritime management, where increasing reliance on Internet of Things technology has created new risks. The maritime sector is particularly vulnerable to cyberattacks that can disrupt operations, threaten security and cause serious damage to businesses and the environment. The report examines cybersecurity frameworks and risk assessments specifically designed for the maritime sector, as well as various studies on how to mitigate threats. It is also growing exponentially. The report explores many aspects of big data security and processes, including the integration of advanced technologies and hardware solutions. Key issues such as data ownership, privacy, and environmental justice are addressed, providing important insights into understanding current security practices and developing strategies against big data in the future. . Develops research on intrusion detection, stealth detection, and intrusion prevention, with a special emphasis on the use of deep learning, machine learning, and neural networks. This technology is increasingly used to protect smart projects, business management, and IoT environments. The report also discusses the integration of cyber threat intelligence and machine learning to improve threat detection and response, and highlights the need for CPS to measure security and robustness. Like CyberTOMP, which provides a way to manage cybersecurity responsibilities. This includes defining the role of the Cybersecurity Committee (ACC) and establishing cybersecurity guidelines. Conducts a comparison of industry cybersecurity models to identify differences and overlaps that may impact

compliance and security effectiveness. Importance of cybersecurity education and advanced threat management techniques. The information provided is designed to inform researchers, policymakers, and business professionals about current challenges, solutions, and future directions in cybersecurity.

Introduction

The rapid transformation of the maritime sector due to the integration of Internet of Things (IoT) technology has also brought about changes in maritime operations. This technological revolution has improved efficiency, communication, and emergency services. However, the increasing reliance on IoT systems has also created new cybersecurity challenges, which are particularly important for maritime industry security and infrastructure development. In particular, a comprehensive cybersecurity status assessment of maritime IoT transport systems. Numerous research articles and studies have emerged that demonstrate the vulnerability, risk, and threat of cyberattacks on maritime transport management. The complexity of these interconnected systems makes them vulnerable to cyber risks that can lead to serious operational disruptions, data breaches, and even environmental and safety issues. The current study provides important methods for detecting and mitigating cyber threats in this area. Particular attention will be paid to intrusion detection systems (IDS), cybersecurity frameworks for maritime applications, and the role of machine learning and artificial intelligence in advanced security measures. The review also examines regulations and international standards that address cybersecurity issues in the maritime environment. Addressing vulnerabilities in maritime IoT systems is critical not only to ensuring global business continuity, but also to ensuring the safety of people, cargo, and the environment. Finally, the survey aims to contribute to current discussions and developments in the field of maritime cybersecurity by providing a deeper understanding of the issues for researchers, professional leaders and policy makers working to secure the future of shipping.

Keywords

- Cybersecurity
- Safety Assessment
- Critical Infrastructure
- Cyber-Physical Systems (CPS)
- Network Defense Techniques
- Instrumentation and Control Systems (I&C)
- Cybersecurity Maturity Frameworks
- Industry 4.0
- Homomorphic Encryption
- Maritime Cybersecurity
- Risk Mitigation
- Industrial Control Systems (ICS)

Literature Survey

1. Cybersecurity in Critical Industries

Cybersecurity has become a critical issue in the industry with the increasing need to protect critical systems from increasing cyber threats. This research paper examines the recent developments in cybersecurity, focusing on key research topics such as security and cybersecurity analysis, cyber defense mechanisms, encryption systems, and technology launch and development models for critical businesses. Growing cybersecurity industries such as nuclear energy, oil and gas, and transportation rely on modern instrumentation and control (I&C) systems to pose cybersecurity risks. The search scheme presented by [Sau et al., 2022] identifies cybersecurity assessment methods used in key industries, identifies gaps, and current good practices. This study reveals the problems caused by Industry 4.0 technology, which increases the openness and interoperability of systems, making them more vulnerable to cyberattacks.

2. Network Defense and Countermeasure Techniques

Although many assessment methods have been used for decades, this study reveals a new trend towards integrated security and cybersecurity analysis and recommends further research in this area. Defense systems should be based on the effectiveness of cyber threats. A study by [Sau et al., 2021] established six quantitative technology protection measures to ensure that organizations pay attention to the importance of reducing technology-based threats due to poor system and network environments. This study demonstrates an electronic tool that selects appropriate protection, which shows a significant improvement in communication by closing many flaws. This study also demonstrates the future potential of automated systems to collect and monitor in-flight vulnerabilities, indicating a transition to a more powerful and responsive cybersecurity defense system.

3. Security-by-Design in Cyber-Physical Production Systems (CPPS)

As cyber-physical manufacturing systems (CPPS) are increasingly integrated into business operations, ensuring security and quality control is of vital importance. The QualSec method proposed by [Sau et al., 2022] provides quality control with security risks by using Petri nets and semantic engineering models to identify cascading effects in CPPS. This approach can identify attack vectors that may affect product quality, which is an important step in protecting the security and integrity of important products and the enterprise.

4. Cybersecurity Maturity Frameworks for Technology Startups

Due to the limited resources for cybersecurity measures, startups are vulnerable to cyberattacks. A qualitative literature review by [Sau et al., 2022] revealed significant differences in cybersecurity maturity frameworks suitable for start-ups. The review identified the need for an end-to-end framework that can measure cyber growth levels and quantify the return on investment in cybersecurity. While the current framework is applicable to large organizations, it does not address the unique challenges faced by startups, making them vulnerable to becoming an entry point for attackers targeting large, connected organizations. This study highlights the importance of developing a framework that will help startups justify their security investments and increase their cyber resilience.

5. Encrypted Control Systems and Real-Time Attack Detection

A new area of security. [Written et al., 2023] A recent study proposed an antivirus control system that can detect cyberattacks using the concept of key homomorphic encryption. The system is used to detect real-time attacks such as false signals in commercial engine control systems. This study shows that encryption-based control systems can provide security and efficiency, reduce computational costs, and improve detection. This study highlights the importance of encryption techniques in maintaining control in a business environment.

6. Cybersecurity in the Maritime Industry

A study by [Author et al., 2023] investigates cybersecurity risks in maritime systems, especially in the context of IoT devices and modern ship frameworks. The study examines vulnerabilities associated with digital transformation and discusses cyber risk mitigation strategies for maritime security. The study also provides recommendations to protect offshore operations by emphasizing the need for effective cybersecurity management against evolving business threats.

Methodologies Used/ Discussed

1. **Cyber Risk Assessment Framework**
    - **Data Flow Diagrams (DFDs)** are an essential tool for visualizing and analyzing data flows in maritime applications. In this context, DFDs help identify potential attack vectors by mapping interactions between ships, ports, and shore-based control systems. DFDs break down complex systems into simpler components, highlighting areas where sensitive information can be intercepted or altered. For example, you can visualize connections between navigation systems, cargo management, and data transfer from ship to port.
    - **Risk Management:** Organizations use DFDs to identify potential threats and then assess the likelihood and impact of each threat. Marine systems can prioritize vulnerabilities using quantitative risk assessment techniques (e.g., probability and impact analysis).
    - **Continuous improvement:** Particularly in the dynamic threat environment of the transportation sector, regular updates to the risk assessment process are necessary. By continuously monitoring for new vulnerabilities, the risk assessment framework evolves to ensure system resilience to new threats.

2. **Intrusion Detection System (IDS) and Anomaly Detection**
    - **Signature-based intrusion detection systems:**
      Signature-based intrusion detection works by detecting known cyber threats based on predefined patterns, or “signatures.” In maritime environments, it monitors communications between ships, ports, and shore systems to ensure that no known malicious activity or communications are occurring. For example, it may detect suspicious data packets sent from unauthorized systems, or monitor the integrity of communications between a ship’s engine management system and a shore-based command center.

- **Anomaly detection:**
  Anomaly-based SIGNs go beyond known threats and detect deviations from normal behavioral patterns. Since maritime systems rely on predictable communication patterns (e.g., regular data transfers between ships and ports), irregular activity can be a sign of a cyber attack. This method is particularly effective at identifying zero-day attacks (unknown vulnerabilities) that traditional signature-based intrusion detection systems may fail to detect. This allows the system to flag suspicious activity, such as unusual network traffic from a ship's navigation system or excessive data transmission at unusual times.

3. **Blockchain for secure communications**
   - **Distributed Ledger:** Blockchain records messages and transactions in an immutable distributed ledger, ensuring data integrity and security. This is particularly useful for communications between ships, ports, and coastal authorities where sensitive information (such as cargo details or navigation data) must be transmitted securely. The distributed nature of blockchain eliminates single points of failure, making it more resistant to unauthorized access. All data transactions are encrypted and recorded in immutable blocks once confirmed, ensuring that communications between IoT devices (such as ship navigation systems and port authorities) cannot be altered or deleted.
   - **Operational Security:** Maritime organizations can use blockchain to enhance the security of critical operational processes such as cargo handling, port planning, and vessel tracking, as well as communications. For example, you can record and track the entire shipping route or cargo manifest, reducing the risk of fraud or tampering.

4. **Multi-Layer Encryption Protocol**
   - **Advanced Encryption Standard (AES)** is a widely used method for protecting sensitive data during transmission. IoT-enabled maritime transport systems use AES to encrypt messages between onboard IoT devices (e.g. sensors) and shore systems, ensuring data security both during transmission and at rest. These systems often transmit real-time information related to navigation, engine control, cargo, and weather conditions. AES ensures that this data remains confidential and protected from interception by cybercriminals.
   - **Multi-layer encryption** means applying encryption at different levels of communication. For example, data transmitted from an IoT device on a ship to a shore-based control center can be encrypted at both the application layer (using data encryption) and the network layer (using VPN or SSL/TLS encryption). This approach provides end-to-end security even if one encryption layer is compromised.

5. AI-Based Hybrid Security Solutions

- **AI-based security systems** combine traditional cybersecurity approaches with machine learning (ML) and artificial intelligence (AI) to provide advanced threat detection capabilities. AI-based systems can predict and mitigate future cyberattacks by analyzing historical data and learning from previous incidents. In maritime IoT systems, AI can detect abnormal behavior in communication networks, port operations, and ship control systems, alerting security teams in real time to potential threats.
- **Hybrid models:** These systems combine proactive measures (e.g., firewalls, antiviruses) with reactive measures (e.g., IDS and incident response). For example, an AI model could monitor all communications on a ship in real time, compare them to an extensive database of known attack patterns, and respond to anomalies. When an anomaly is detected, AI can automatically apply security patches or isolate affected components.
- **Enhanced threat detection:** AI reduces the number of false alarms from intrusion detection systems and enables the maritime industry to respond to threats more quickly and accurately. AI's ability to continuously learn ensures that maritime IoT systems stay ahead of emerging threats.

6. Cyber-Physical Systems (CPS) Security Model

- **Cyber-Physical Systems (CPS)** in the maritime environment involve the integration of computing systems and networks with physical processes (e.g., navigation and propulsion control). The CPS security model focuses on protecting these critical systems from cyberattacks that could result in physical damage or disruption. Navigation and propulsion control systems are critical in the maritime environment. Unauthorized access to or manipulation of these systems can result in safety risks, such as vessel misdirection or engine failure.
- **Security Protocols:** The CPS security model isolates these critical systems from cyber threats through strong encryption, access control, and continuous monitoring. It focuses on preventing unauthorized actions, such as attempts to manipulate navigation data or engine commands. The model also integrates redundancy and fault tolerance mechanisms into critical systems to ensure that the vessel can continue to operate safely even in the event of an attack. For example, in the event of a cyberattack on the primary system, a backup control system can take over navigation control.

Research Outcomes

1. **Increased Cybersecurity Risks:** Maritime IoT integration has introduced significant cybersecurity vulnerabilities, impacting operational continuity and environmental safety.
2. **Advanced Detection Technologies:** Deep learning and machine learning are enhancing intrusion detection and response systems, offering improved protection against sophisticated threats.
3. **Big Data Security Challenges:** Issues related to data ownership, privacy, and security are prominent, with advanced encryption techniques being crucial for safeguarding data integrity.
4. **Need for Tailored Frameworks:** Existing cybersecurity frameworks require adaptation to address the unique risks of maritime IoT systems, including specialized approaches for startups.
5. **Regulatory Compliance:** Adherence to international standards and continuous updates to cybersecurity practices are essential for maintaining robust protection and ensuring global business continuity.

Conclusion

This overview explores the changing cybersecurity landscape and key developments in maritime IoT, highlighting the opportunities and challenges associated with technological advancements. Outsourcing companies benefit from increased efficiency and communication as they rely on IoT technologies, but they also face increased cybersecurity risks. These interconnected systems are particularly vulnerable to cyberattacks that can disrupt operations, compromise data, and create environmental threats. Important: Adapt existing measures to address new and evolving threats. Learning technologies such as deep learning, machine learning, and neural networks have proven to be critical to improving access and response pipelines. Integrating large data sets raises privacy and data security concerns, requiring the use of advanced encryption techniques such as homomorphic encryption and multi-layer procedures, and the need to update procedures and practices. A cybersecurity concept designed for release and implementation is considered necessary to reduce risks through the integration of various technologies. Overall, this document calls for continued research and development to keep pace with cyber threat dynamics and provide effective defense against maritime operations and infrastructure panics.

References

[1] Marican, Mohamed Noordin Yusuff, et al. "Cyber security maturity assessment framework for technology startups: A systematic literature review." *Ieee Access* 11 (2022): 5442-5452.

[2] Tatipatri, Naveen, and S. L. Arun. "A Comprehensive Review on Cyber-attacks in Power Systems: Impact Analysis, Detection and Cyber security." *IEEE Access* (2024).

[3] Babeshko, Ievgen, and Felicita Di Giandomenico. "Safety and Cybersecurity Assessment Techniques for Critical Industries: A Mapping Study." *IEEE Access* (2023).

[4] Domínguez-Dorado, Manuel, et al. "CyberTOMP: A novel systematic framework to manage asset-focused cybersecurity from tactical and operational levels." *IEEE Access* 10 (2022): 122454-122485.
[5] Djebbar, Fatiha, and Kim Nordström. "A comparative analysis of industrial cybersecurity standards." *IEEE Access* (2023).
[6] Gaba, Shivani, et al. "A systematic analysis of enhancing cyber security using deep learning for cyber physical systems." *IEEE Access* (2024).
[7] Jisoo, Jang, et al. "Research on Quantitative Prioritization Techniques for Selecting Optimal Security Measures." *IEEE Access* (2024).
[8] Yeboah-Ofori, Abel, et al. "Cyber threat predictive analytics for improving cyber supply chain security." *IEEE Access* 9 (2021): 94318-94337.
[9] Rawat, Danda B., Ronald Doku, and Moses Garuba. "Cybersecurity in big data era: From securing big data to data-driven security." *IEEE Transactions on Services Computing* 14.6 (2019): 2055-2072.
[10] Li, Zedong, et al. "Detecting Cyber-Attacks Against Cyber-Physical Manufacturing System: A Machining Process Invariant Approach." *IEEE Internet of Things Journal* (2024).
[11] Tantawy, Ashraf, Sherif Abdelwahed, and Abdelkarim Erradi. "Cyber lopa: An integrated approach for the design of dependable and secure cyber-physical systems." *IEEE Transactions on Reliability* 71.2 (2022): 1075-1091.
[12] Ashraf, Imran, et al. "A survey on cyber security threats in IoT-enabled maritime industry." *IEEE Transactions on Intelligent Transportation Systems* 24.2 (2022): 2677-2690.
[13] Eckhart, Matthias, et al. "Qualsec: An automated quality-driven approach for security risk identification in cyber-physical production systems." *IEEE Transactions on Industrial Informatics* 19.4 (2022): 5870-5881.
[14] Miyamoto, Masaki, et al. "Cybersecurity-enhanced encrypted control system using keyed-homomorphic public key encryption." *IEEE Access* 11 (2023): 45749-45760.
[15] Lee, Donghwan, et al. "ICSTASY: an integrated cybersecurity training system for military personnel." *IEEE Access* 10 (2022): 62232-62246.