

A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry

Imran Ashraf, Yongwan Park, Soojung Hur, Sung Won Kim[✉], Roobaea Alroobaea[✉],

Yousaf Bin Zikria[✉], Senior Member, IEEE, and Summera Nosheen[✉]

Abstract—Impressive technological advancements over the past decades commenced significant advantages in the maritime industry sector and elevated commercial, operational, and financial benefits. However, technological development introduces several novel risks that pose serious and potential threats to the maritime industry and considerably impact the maritime industry. Keeping in view the importance of maritime cyber security, this study presents the cyber security threats to understand their impact and loss scale. It serves as a guideline for the stakeholders to implement effective preventive and corrective strategies. Cyber security risks are discussed concerning maritime security, confidentiality, integrity, and availability, and their impact is analyzed. The proneness of the digital transformation is analyzed regarding the use of internet of things (IoT) devices, modern security frameworks for ships, and sensors and devices used in modern ships. In addition, risk assessment methods are discussed to determine the potential threat and severity along with the cyber risk mitigation schemes and frameworks. Possible recommendations and countermeasures are elaborated to alleviate the impact of cyber security breaches. Finally, recommendations about the future prospects to safeguard the maritime industry from cyber-attacks are discussed, and the necessity of efficient security policies is highlighted.

Index Terms—Maritime security, IoT, cyber security threats, vulnerability, malware.

I. INTRODUCTION

TECHNOLOGICAL developments have shown unprecedented speed over the past decade and revolutionized

Manuscript received 14 December 2021; revised 1 March 2022; accepted 30 March 2022. Date of publication 15 April 2022; date of current version 8 February 2023. This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) by the Ministry of Education under Grant NRF-2021R1A6A1A03039493; in part by NRF Grant by the Korean Government through the Ministry of Science and ICT (MSIT) under Grant NRF-2022R1A2C1004401; and in part by the Taif University Researchers Supporting Project, Taif University, Taif, Saudi Arabia, under Grant TURSP-2020/36. The Associate Editor for this article was A. K. Bashir. (*Imran Ashraf and Yongwan Park are co-first authors.*) (*Corresponding authors: Yousaf Bin Zikria; Summera Nosheen.*)

Imran Ashraf, Yongwan Park, Soojung Hur, Sung Won Kim, and Yousaf Bin Zikria are with the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: imranashraf@ynu.ac.kr; ywpark@yu.ac.kr; sjheo@yu.ac.kr; swon@yu.ac.kr; yousafbzinckria@ynu.ac.kr).

Roobaea Alroobaea is with the Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia (e-mail: r.robai@tu.edu.sa).

Summera Nosheen is with the Faculty of Engineering, School of Computer Science, The University of Sydney, Sydney, NSW 2006, Australia (e-mail: summera.nosheen@sydney.edu.au).

Digital Object Identifier 10.1109/TITS.2022.3164678

many fields by incorporating novel technologies, policies, and operational procedures. Analogous to several other domains, advanced digitization, information, and operation technology have also made their way in the maritime industry.

The maritime freight-forwarding industry serves as the foundation for international trade carrying around 80% of goods globally and contributing 70% of trade value [1], [2]. Consequently, large investments from multinational companies like Maersk, IBM, and Google, etc., accelerated the revolutionization of the maritime industry. Not only that, Maersk and IBM are working on projects to commercialize the blockchain technology for digital global trade platforms [3]. Shipping automation and incorporation of intelligent systems in maritime is to be deployed by Google, and Rolls Royce [4]. Similarly, projects on digitizing the platforms are carried out under Det Norske Veritas, and Germanischer Lloyd [5]. With the digitalization of the maritime operational platforms, safe navigation, low manning requirements, and security are visioned. With a large increase in the operations of the maritime freight industry over the past decade, further, expansion is expected in the near future. Figure 1 shows the statistics of container throughput for worldwide ports for this decade, indicating a substantial increase in the throughput from 622 million twenty-foot equivalent units (TEUs) in 2012 to an expected 945 million TEUs in 2024 [6].

The maritime industry has evolved from traditional mechanical systems to electromechanical and digital systems involving changes in industrial control systems over the past decade. Consequently, the modern maritime industry operates on semi-automatic/automatic controlled systems, automated harbors, satellite communication, and navigation systems. Such systems combine sophisticated hardware and software systems operated through mobile networks involving the maritime industry stakeholders. Marine communication is carried out using board systems involving shore stations and satellites. Digital selective calling (DSC) is used for distress alerts, safety calls, and routine priority messages, digital selective calling (DSC) is used, which can be integrated with very high frequency (VHF) radios used for ship-to-ship communication. Similarly, satellite communication is used for areas where the shore stations have no coverage [7]. Maritime communication systems contain equipment and devices, a large number of which are connected to the internet or telecommunication systems [8] and can be attacked remotely using both simple as well as sophisticated cyber attacks. Predominantly, the maritime organizations are

TABLE I
A SUMMARY OF CYBER SECURITY THREATS, THREAT ACTORS AND OBJECTIVES

Threat	Level	Threat actors	Objectives
Cyber vandalism	1	Hackers, vandalist, angered employees, activist	Data stealing, destroying, or public posting for media coverage.
Cyber Theft	2	Individual, small groups (political, ideological), spammers	Information, disruption or destruction of business operations, profit or ideological gains
Cyber Incursion	3	Organized enterprise, government entity, terrorist groups	Information of weaknesses, backdoor planting, access, alter or destroy information.
Cyber Sabotage	4	Organized professional organizations, military secret operatives	High-level information regarding secret R&D critical for organization/government, cracking security procedures, infiltration
Cyber Conflict	5	Government operatives, highly skilled terrorist groups, sophisticated hacker group	Infrastructure destruction, high importance mission-critical information
Cyber Internal	6	Employees, workers, third party service providers	Non-intentional mistakes, carelessness, lack of skill to open opportunities for 1 to 5 discussed threats.

not well prepared to handle cyber attacks, as pointed out in [9]. For different kinds of breaches, the preparedness varies with respect to the size and scope of the organization. For example, large companies are well prepared for data breaches which are primarily attributed to the higher ratio of data breaches that occurred in large companies. The capability of handling cyber attacks is increased for those organizations who report such attacks and devise countermeasures to prevent similar future attacks. In this regard, this study makes the following contributions

- This study conducts an extensive review of the security threats for the IoT-enabled maritime industry.
- Comprehensive background on maritime security threats space is provided where different threats, threat actors, and objectives for threats are discussed.
- Cybersecurity threats related to the maritime industry are analyzed regarding different elements of maritime infrastructure like vessels, offshore units, etc., and the onboard devices like navigation systems, data recorders, logistics, etc.
- For assessing the potential threat and risk of cyberattacks, various risk analysis methods are elaborated with their advantages and disadvantages. In addition, different threat mitigation methods are discussed.
- A brief and compact prospective discussion is provided for the shortcomings of existing defense strategies for handling the maritime risks, and future directions are outlined.

A taxonomy of the research papers covered in this study is provided in Figure 2. The rest of the study is organized in the following fashion. Section II provides the background of the cyber security threats and their various types. Maritime cyber security threats are discussed in Section III. Risk impact analysis of cyber security threats is performed in Section IV while risk mitigation schemes are given in Section V. Overview of probable threats with respect to Industry 4.0 is described in Section VI. Future research directions are provided in Section VII while the conclusion is given in Section VIII.

II. BACKGROUND ON CYBER SECURITY THREATS

Keeping in view the proneness of the electromechanical and digital systems, involving connected hardware and software components, the associated risks and threats are large and complex, necessitating the extensive evaluation of

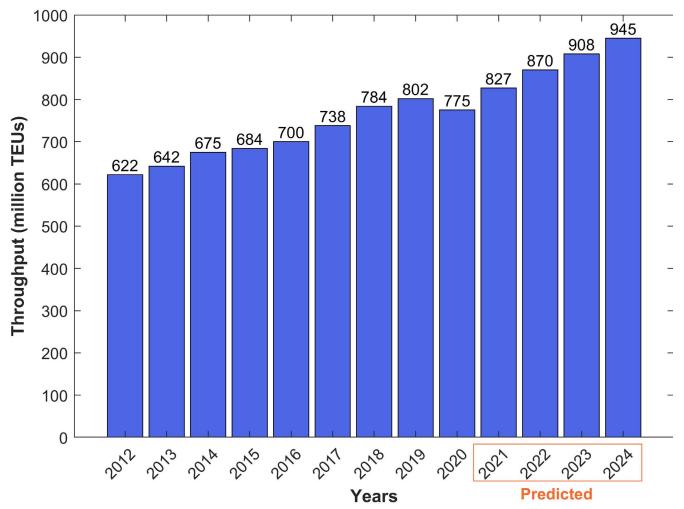


Fig. 1. Container throughput in million TEUs for maritime worldwide [6].

systems' vulnerabilities. The security threats become worse when geopolitical disputes and piracy attacks are considered. Maritime security threats can be broadly categorized under two groups: intentional threats and unintentional threats.

A. Intentional Threats

Intentional direct threats are cyber security threats caused by a large number of adversaries and involve different methods and techniques.

1) *Cyber Vandalism*: Representing an ideological motivation, such individuals/groups steal sensitive information to exploit their target. Often inspired by different individuals, cyber vandalists, also called hacktivists, misuse the stolen data for malicious purposes, such as blackmail, extortion, and ransom, etc. [10].

2) *Cyber Sabotage*: Cyber sabotage, also called espionage, threats come from industry rivals and market competitors, often targeting the intellectual properties of a target company [11]. It is the planned and organized intrusion to steal confidential information, alter if it provides an institutional benefit, or destroy data/products to outwit the competitor. Espionage aims at obtaining a competitive edge by empowering own skills by stealing intellectual property or disrupting the competitors' business operations [12].

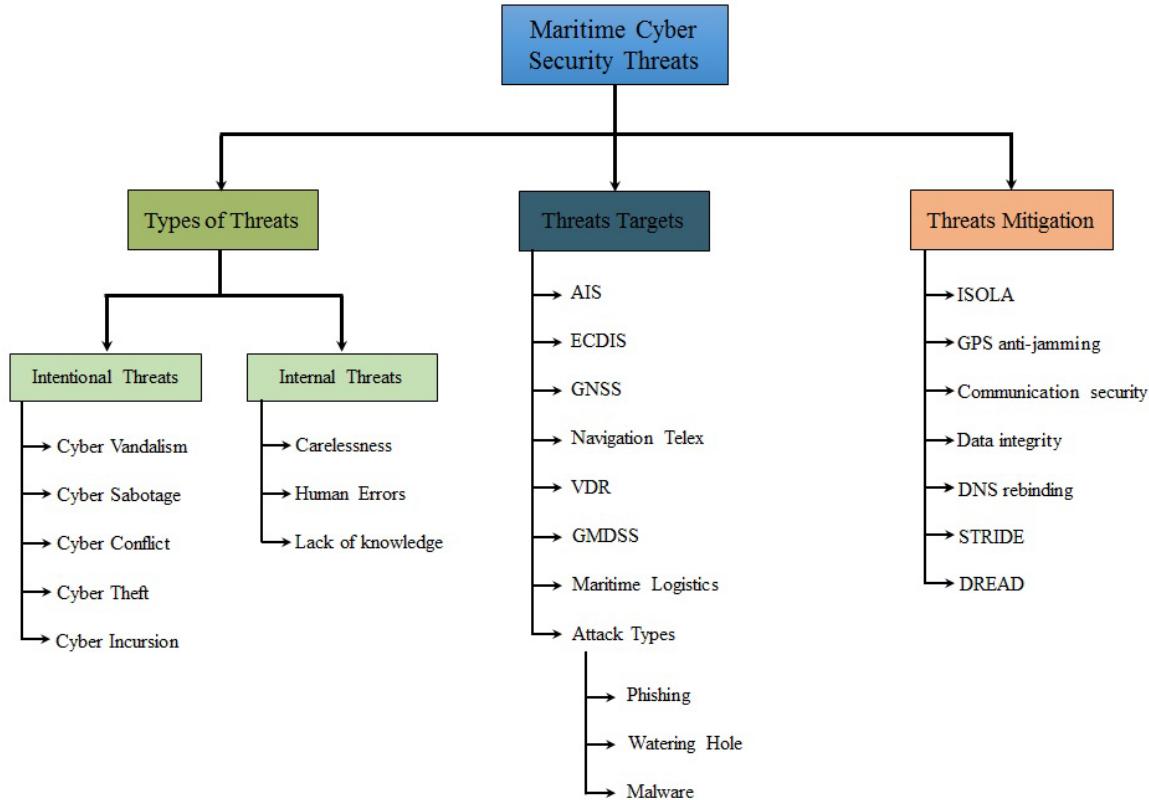


Fig. 2. Taxonomy of the papers discussed in this study.

3) *Cyber Conflict*: The scale and scope of the intentional attacks become wide when it is state-sponsored or government-driven. Countries may launch cyber attacks on the maritime industry of an opponent or competing country [12]. Primarily such attacks are made for obtaining state secrets and similarly other important information that may provide leverage. Similarly, secret business agreements and similar other commercial information of high importance can be targeted [13]. State-sponsored attacks are launched for economic dominance, information control, or national destabilization [14].

4) *Cyber Theft*: Cyber thieves, also called Terrorist groups, are often formed by certain religious, political, and social doctrines and take actions to target the opposing groups, nations, and countries. The maritime sector can also target such groups where the attacks are carried out using electronic and computerized media for obtaining unauthorized access to confidential information. Attacks are aimed at both destroying these resources, as well as using them for ransom and gaining the upper hand [12].

5) *Cyber Incursion*: Individuals or criminal organizations may also launch Cyber-attacks for criminal activities. Such attacks are launched for extortion, fraudulent activities, and illegal access to the intellectual property of an organization [12]. By gaining access to different controlling systems, weapons, drugs, and contraband operations are performed for economic benefits and stealing secret information for blackmail, ransom, and information selling to other groups [15].

B. Internal Cyber Threats

Besides the intentional cyber security threats for the maritime industry, the harm can be done unintentionally due to the negligence of employees or third-party service providers. Threats from internal employees can occur due to carelessness, human errors, or lack of knowledge about particular tools or procedures [16]. The intensity of internal threats varies with respect to the importance of the system being exposed to the security threat. Adversaries can misuse exposed systems to control and exploit them for secret information. Internal threats are often the outcome of improper training, lack of skills to handle a system, human judgmental error, and ignorance [12]. Third-party software and hardware systems can also jeopardize maritime security if software containing back doors, poorly tested software and error-containing systems are installed.

A schematic diagram of cyber security risks in the maritime industry and the associated risk level is portrayed in Figure 3. The number represents the risk level, with a higher number indicating the higher risk. Numbers from 1 to 6 are attributed to 'low', 'moderate', 'high', 'very high', 'severe', and 'extreme' risk for these threats. Cyber internal threats indicate the highest threat level and expose the companies to the maximum risk.

Table I provides the overview of the types of cyber security threats for the maritime industry, along with the possible threat actors and their objectives. The cyber internal threat category is ranked with the highest risk level as employees' carelessness, lack of proper training, and knowledge may expose an organization's infrastructure to all the threats described here.



Fig. 3. Cyber security threats and associated risk level.

III. ANALYZING CYBER SECURITY THREATS RELATED TO MARITIME

Basic components of the maritime infrastructure are depicted in Figure 4 indicating three important components: vessels, ground infrastructure, and communication network. Vessels contain on-board systems such as global maritime distress and safety systems (GMDSS), maritime administrative systems, communication systems, etc., prone to different kinds of cyberattacks. Similarly, off-shore systems comprise public infrastructure, including automatic identification systems for vessels and crew managers, private service providers, off-shore security systems, etc. Different adversaries can attack to obtain unauthorized access. A schematic diagram of on-board and off-board systems is given in Figure 5.

A. Automatic Identification System Related Attacks

An automatic identification system (AIS) provides safe navigation in the sea and collision avoidance by providing navigation-related information of other ships such as ship type, course, speed, ship status (anchor, or underway), etc. AIS aims at reducing the risks of possible collisions with other ships by communicating with them. However, communication makes AIS the most vulnerable system of the ship [17], [18].

With technological advancement, the AIS data can be reproduced, and a virtual ship can be placed with false speed, heading, course, and other information to deceive other ships. Weather information can be generated and sent to other ships to change their route. AIS attacks occur due to a lack of appropriate procedures to ensure integrity and encryption protocols which makes it easy for the attackers to intercept AIS transmission [19]. For example, an Iranian oil ship used falsified AIS data and pretended to be Tanzanian to navigate to Syria [20]. Using a very high frequency (VHF), an attacker can intercept AIS transmission, tamper the AIS data to steal identity information, communicate with a ship by

impersonating port authorities, block the communication with other ships, and direct the vessel to the desired location by impersonating as competent maritime authority [21], [22]. AIS can also be the target of a denial-of-service attack, fake close point to alert collision alert, and data flood by transmitting at higher frequency [22], [23].

B. Electronic Chart Display and Information System

ECIDS has been a mandatory part of the ships since January 1, 2011, and contains several important functions in hardware and software for safe navigation. ECDIS is used for displaying ships course for the crew using the bridge-placed operating system. ECDIS contains position, compass, speed, etc., and is connected to ship systems and sensors and is updated via USB or the internet. Despite being an essential part of ships, it is found to be the easy target of adversaries [24]. The primary source of malicious code execution on ECDIS is the obsolete baseline operating systems or operating systems that do not allow upgrades [25].

C. Global Navigation Satellite System

Similar to navigation at land, GNSS provides important information for safe sailing at sea through guided navigation by GPS. After the AIS, GNSS has been regarded as the most vulnerable asset in the maritime sector [25].

Spoofing and jamming are the two most prominent threats to GPS technology. Spoofing involves using the port, access control address, and internet protocol (IP) to conceal the original identity for performing malicious activities. During the jamming, the GPS signals are disrupted or disturbed by intercepting the boat's frequency. Unlike spoofing, which is an impersonating act, jamming involves electronic or mechanical intervention to disrupt radar or radio communications [26]. Jamming attacks are usually carried out by commercial devices that are low cost and easy to buy online [27]. Spoofing attacks are complex as compared to jamming, as they require simulating the satellite signals that require high power and complicated apparatus [28].

Research shows that the navigational systems are the primary target of maritime cyber attacks due to their vulnerability, followed by ECDIS and engine control [29].

D. Navigation Telex

Navigation Telex (NAVTEX) provides urgent navigation and meteorological information for safe navigation by the port authorities. The information is disseminated by telex in the ship that operates at specific frequencies, and information is available via the website as well [30]. NAVTEX is connected to the internet, storage devices, and other systems prone to attacks. Attacks may result in incorrect messages to misguide the ship and blocking the service to send the messages from the attacker to guide the ship to the location of the attacker's choice [31].

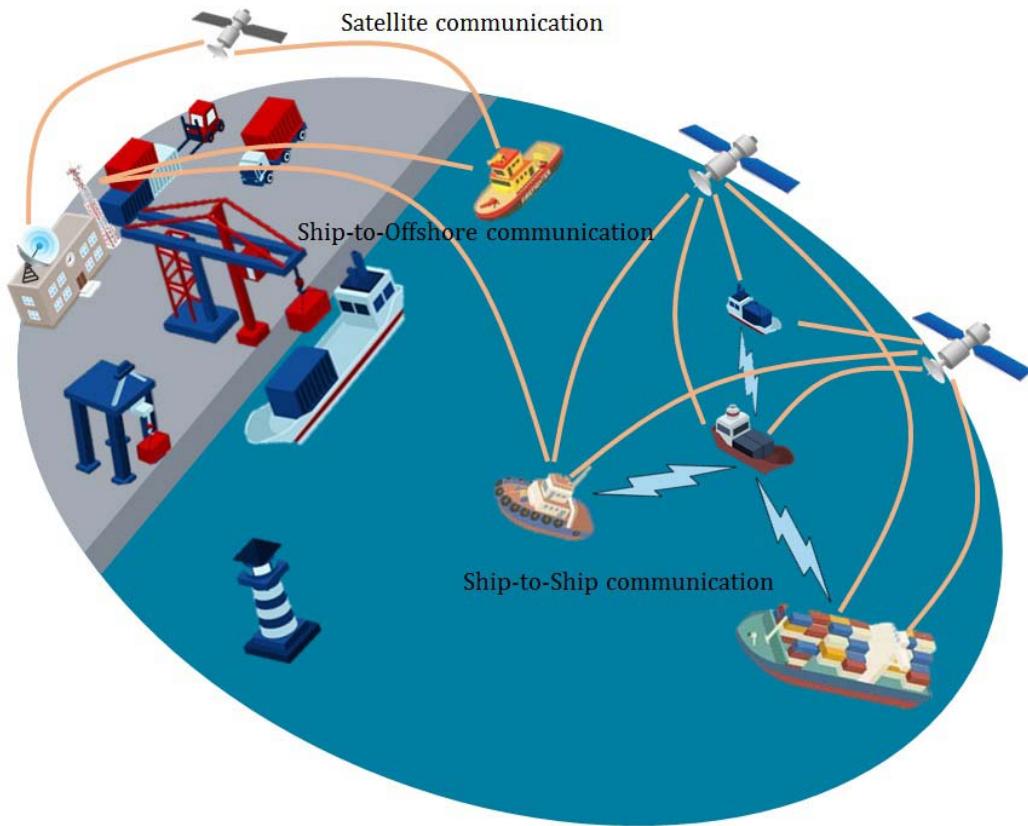


Fig. 4. Basic components of maritime infrastructure.

E. Voyage Data Recorders

A voyage data recorder (VDR) is used to store the voyage details of the ship and can be a potential tool for investigating ship accidents. It serves a similar purpose, as BlackBox does for the airplane, with superior functions. It records the speed, direction, position, conversations, etc. of the last 12 hours that can be used to analyze ship performance, accident analysis, and damage analysis. VDR is prone to intruder attacks, and the attacker needs to be inside the ship as it is connected to a local area network (LAN). Attacks happen due to inappropriate authentication mechanisms, weak encryption protocols, and obsolete firmware [32], [33]. VDR can be attacked for denial of service for obfuscation through the USB, CD, and DVD, etc. [34].

F. Global Maritime Distress and Safety System

GMDSS is the fundamental system for distress management and involves sending distress messages to shores and requesting search and rescue support. It also broadcasts the maritime safety information (MSI) for other ships in the vicinity that could help the distressed ship to a safe route [4]. Malware infections are targeted on GMDSS, resulting in partial damage or complete destruction. The control can also be taken to guide the ship to a designated location by the attacker. The identity of another ship can be spoofed using the GMDSS to initiate communication with other ships for influencing cargo safety. GMDSS interactions with SCC (shore control

center) can be compromised to steal sensitive information of ship operations. Owing to the importance of GMDSS during emergency and rescue operations, any disruption can risk the rescue operations [35]. Similarly, jamming attacks can cause damage and denial-of-service for GMDSS [36]. To mitigate the impact of cyber attacks on GMDSS, counterpart systems are a potential solution [37].

G. Threats to Maritime Logistics Environment

With the advancements in technology, traditional supply chain and logistics systems have been transformed into supervisory control and data acquisition (SCADA) systems where the flow of goods can be remotely controlled. This infrastructure involves internet of things (IoT) platforms, satellites, and ICT procedures to control and monitor the maritime logistics and supply chain (MLSC). Consequently, SCADA infrastructure and cyber-physical systems (CPS) are prone to cyber-attacks from adversaries. MLSC systems comprise several CPS that has been the target of adversaries during the recent events [38]–[40].

SCADA systems in the current maritime sector involve interoperable components integrated with ICT systems and involve communication. Sensors and devices used for position tracking and monitoring, such as IoT sensors and cameras, satellite communication, etc., are susceptible to different cyberattacks [41]. SCADA systems can be the victim of five different kinds of cyberattacks.

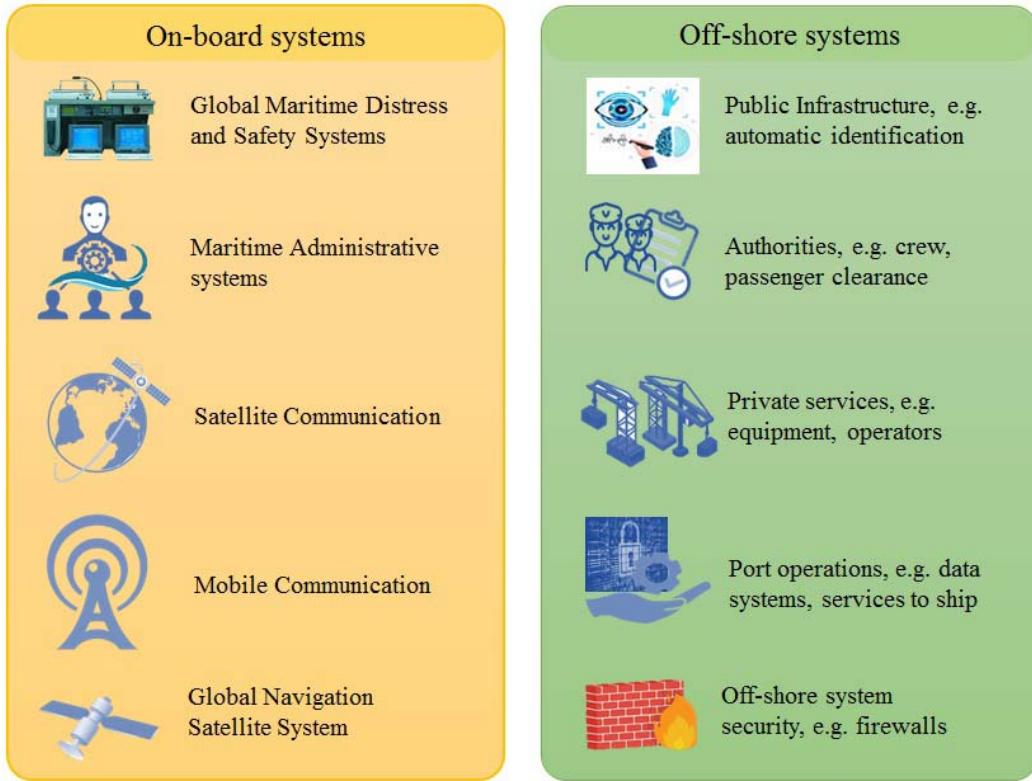


Fig. 5. Maritime systems for on-board and off-shore platforms.

- 1) Attacks can be directed to a communication stack such as a network layer.
- 2) Transport layer can be attacked using SYN flood attack types which involves sending transmission control protocol (TCP) connection requests faster, making it impossible for the machine to handle it. It leads to a denial-of-service (DoS) outcome.
- 3) Attacks like packet replay on the application layer. Such attacks normally happen due to weak security controls.
- 4) Adversaries attack hardware to obtain unauthorized access and remotely control the devices. Hardware attacks traditionally occur where the authentication controls or appropriate or missing.
- 5) Software cyber attacks include attacking the software working as an application layer between the sensors and application packages. For example, structure query language (SQL) can be the victim of SQL injection attacks.

In addition to the above-discussed SCADA attacks, the use of social media platforms for accessing the alerts, news regarding hazards, and similar other events can affect the operational capability of such system in emergency response scenarios [42].

H. Cyberattacks in Maritime

1) *Phishing Attacks:* The phishing attack is the most commonly used cyberattack, including social engineering and malware attacks. The former utilizes email services and fake

websites to inflict damage or steal information, while the latter uses different malware installed on a personal computer. Phishing attacks aim at getting the users' personal information such as username, and password, etc., by tricking the user into visiting a fake website [43]. Phishing also includes a sub-category, spear phishing targets the company's employees through emails very similar to the company's legitimate emails. The email contains an attachment that can steal sensitive information stored on the computer once it is clicked to view.

2) *Watering Hole Attack:* Watering hole attacks target a specific group for a security exploit by using the group's specific websites known to be visited. Such attacks are specifically targeted on the employees of an organization/crew members to gain access to their personal computer by infecting the legitimate websites [44]. Malicious codes are placed on famous websites by exploiting their vulnerabilities and weaknesses and redirecting the users to attackers' websites [45]. Although uncommon, watering hole attacks are harder to detect as they come from legitimate and famous websites. Systems that analyze the compromised websites have been proposed to alleviate the cyber risks of watering hole attacks [46]–[48].

3) *Malware:* Malware is a group of computer code programs intended to steal or destroy the data on a computer using viruses, spyware, and ransomware. Malware is used for recording a user's activity and stealing confidential information for blackmail and publishing online [49]. With the increase in the number of IoT devices for the modern maritime industry, experts have regarded malware as an attractive choice to

penetrate and breach cyber security [50]. Malware is also used for identity fraud and to commit crimes and terrorist activities in the maritime sector. Similarly, ransomware is also malware containing the zip or other files where opening these files can block access to resources. The attacker requires a ransom amount to allow access. The malware aims at creating man-in-the-middle attacks by exploiting (SSL) or (TSL) weaknesses to download important data from the user's computer [51], [52].

IV. CYBER RISK ANALYSIS METHODS

International maritime organization (IMO) is the central agency from the United Nations (UN) to devise policies and procedures for the maritime industry's safety and security, including the risks to the maritime sector and maritime induced risks for the environment. For safeguarding the ships from cyber attacks, it has defined protocols and procedures for a preventive and corrective course of actions, including the elements of cyber risk management [53], as shown in Figure 6. IMO defines five elements for cyber risk management, including identification, protection, detection, responding to risks, and recovering. In addition, the national institute of standards and technology of the United States (US) further elaborates this framework and provides detailed discussions on how to use it [54]. Similarly, the institute of engineering and technology (IET) [55] provides the code of practicing cyber security for ships, and the Baltic and international maritime council (BIMCO) drafts the guidelines for onboard ships [21]. Several models have been contrived to analyze risk impact analysis for maritime cyber risks based on these elements. On the other hand, several individual works outline the guidelines for cyber security for commercial maritime and policies for managing cyber risk [56].

Several models have been designed to analyze the cyber risks with the maritime industry. Maritime risk assessment utilizes qualitative and quantitative methods where the former prioritizes the risks based on their probability. At the same time, the latter performs numerical analysis by awarding risk values to each risk. Predominantly, maritime physical risks analysis relies on probability analysis based on empirical statistics [57], [58]. A qualitative risk analysis is performed for inertial navigation system-related cyber risks in [59]. In addition to the crew interviews, testing is also performed to analyze different vulnerabilities. Results show that remote desktop, terminal service, and remote protocols are vulnerable to arbitrary remote code and man-in-the-middle attacks, respectively. A more critical risk is the server message block service which can be exploited to arbitrary code execution and disclosure of sensitive information. An interview and survey-based method is adopted by [60] for ECDIS cyber vulnerabilities. Unsupported windows, server message block (SMB) vulnerability, improper handling of remote procedure call (RPC), SMB remote execution, and SMB security update are critical risks for ECDIS in maritime ships.

The authors perform cyber risk analysis with a framework based on IMO and IET guidelines in [61] following an on-board survey and cyber security testing for analyzing ECDIS-related cyber risks. Cyber security testing involves

vulnerability scanning and penetration testing techniques. The study finds out that the Apache webserver poses a high level of risk as it is obsoleted. As a result, the functionality of the ECDIS can be fully destroyed. Similarly, an experimental ship assessment is carried out in [62] involving the cyber security survey and cyber vulnerability computational scanning to analyze the ECDIS vulnerabilities. Results suggest that obsolete operating systems, server service vulnerability, SMB vulnerability, and SBM security updates are the cyber threats that can be exploited to run arbitrary code from a remote location. Along the same direction, study [63] performs cyber security testing for ECDIS vulnerabilities. Web servers are outdated, printer sharing and operating systems are vulnerable to unauthorized access, leading to a denial of service, crashing ECDIS, stealing sensitive information, man-in-the-middle attacks, etc. In addition, the study analyzes the cyber security risks associated with the third-party service provided and finds out that third-party abandoned and out-of-date components and components involving insecure setup are the major threats.

A survey is conducted in [64] for cyber security vulnerabilities in maritime involving mariners, port officers, IT system experts, and third-party service providers. Survey results highlight the crew-training standards inappropriate (74%), followed by the cyber-attacks with 55%. A total of 60% are found to be explaining the lack of cyber security training. Additionally, 50% of the participants blamed IT as the vulnerable technology for cyber-attacks, while 41% regarded IT and OT as equally responsible. Regarding the cyber crimes, malware, phishing scams, and web-based attacks have been placed at the top three with 31%, 13%, and 13%, respectively of all the cyber crimes in the maritime. The authors of [65] investigate the factors responsible for cyber threats in maritime through a survey. An 80% of the participants considered the crew training insufficient, while 56% ranked cyberattacks as the leading problem for the maritime sector. The majority of the participants (57%) did not receive training regarding cyber security, and 80% suggested the importance of maritime cyber training over general cyber security training. Malware, phishing, and web attacks have been regarded as the leading cyber attacks with 26%, 16%, and 16%, respectively, of all the cyber attacks in the maritime sector.

In the same fashion, the role of human behavior on the cyber security of maritime systems is studied in [66], where the crew members are divided into different groups such as introvert, extrovert, and intuitive, etc. Interviews with the crew members indicate that majority of the people attached with the IT have a medium or low level of knowledge. Despite the installed security systems on the ships, the crew members are not well trained to operate the sophisticated programs. Often, cyber incidents happen due to operators' mistakes due to lack of proper training, carelessness, or poor skill set. A future prospect of the maritime cyber risk is presented in [67] by conducting a survey where 93% of the respondents suggest that the frequency and intensity of the cyber attacks will increase. In addition, the perceptions and potential of social media as a tool for cyber attacks are evaluated, indicating that 74% of the participants believe social media is a potential source of cyber attacks. An 87% believe that the cyberattacks

can be handled more prudently if properly reported and investigated to mitigate future attacks. Study [68] discusses the cyber threats to critical maritime infrastructure, including on-board systems and port operations. Analyzed incidents include high-value cargo theft by infecting authentication data, software malware to shut down port operations, and software infection to interrupt port operations. The study discusses several challenges associated with maritime cyber attacks handling.

The maritime cyber risk analysis (MaCRA) model is one of the risk assessment models in the maritime sector [69] that combines cyber and maritime factors for risk analysis. By considering ship functions, configurations, users, and environmental factors, the framework provides the maritime cyber risks associated with a particular ship type and assists in devising appropriate security procedures. The MaCRA model is extended for risk analysis in the autonomous ships by [34] to provide anticipated risks for the futuristic ships. In this regard, the risks are discussed with respect to navigation systems and cargo systems, considering the reward, ease of exploit, and system vulnerability.

GPS jamming has significant repercussions for navigation. [70] shows that the positioning error during GPS jamming is too high to produce catastrophic outcomes if the sailing is continued. Similarly, GPS jamming makes AIS useless as AIS uses GPS signals for slot timing sources which are required for VHS communication based on self-organized time division multiple access (SOTDMA). Jamming GPS also has a strong impact on radar communications, and radar-based detection has erroneous estimations [70]. In addition, if the GPS data is used for slot timing in digital communication such as cellular telephone and satellite communication, GPS jamming would affect these systems.

Risk assessment methods for SCADA can be qualitative, quantitative, and hybrid, combining the first both. Fault tree events analysis [71], object-based event scenario tree [72] and probabilistic risk analysis tools [73] follow a semi-qualitative approach while [74], [75] present quantitative models for risk assessment. For SCADA-related risks assessment, several important research works can be found that extensively studied different approaches for the past two decades [60], [76]–[78]. These research works cover risk assessment methods for static and real-time systems, including monitoring, detection, impact analysis, and countermeasures.

The study [79] presents an automated threat modeling approach regarding cyber security threats to the maritime industry. It comprises three modules each for feature extraction, cyber threat intelligence (CTI)-based detection, and CTI-based attack categorization. The proposed approach performs automated CTI contrary to traditional systems where threat-related features are manually extracted [80]. The model provides increased accuracy as compared to the state-of-the-art approaches.

V. THREAT MITIGATION METHODS

In general, the maritime sector lacks a timely response to introduce the appropriate countermeasures for resolving

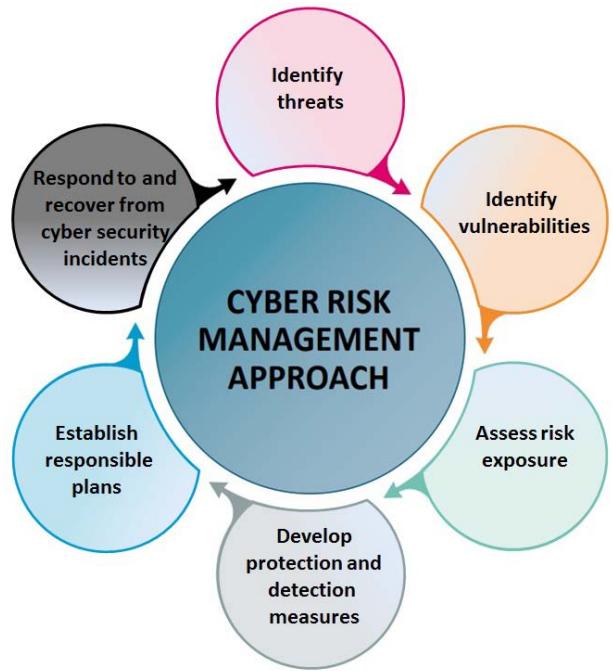


Fig. 6. Elements of cyber risk management, adopted from [21].

technical vulnerabilities, which increase the susceptibility of the onboard systems [81]. Due to the better maintenance off-shore systems in the maritime sector, they experience a low number of cyberattacks compared to their counterparts. Secondly, onboard systems rely on obsolete underlying operating systems or those operating systems that do not allow upgrades. The upgrade failures may occur due to conflicting IT and OT technologies standards where the upgrade of one may not support the other. Out of date systems put the entire ship at the hand of the adversaries. Maritime needs to prioritize the critical systems and ensure their safety first, such as navigation, ECDIS, and VDR [82].

Several frameworks and techniques have been presented to mitigate the probability of cyber risks by building detection and correction procedures for cyber attacks. For example, A novel framework, innovative and integrated security system onboard covering the life cycle of a passenger ships voyage (ISOLA), is presented in [83] that performs risk analysis for cruising ships at sea. The analysis covers both vulnerabilities and threats for onboard and off-shore cyber attacks and recommends several data fusion solutions to mitigate the risk impact. The authors present an integrated framework in [84] to monitor the air-sea-ground space for oil ships. Comprising of sensing, network, and application layers, the sensing layer is used to collect the data from air, sea, and ground transmitted via the network layer. The spaceborne synthetic aperture radar (SAR) is used for data collection. The collected observations combined with the forecasting model can provide reliable and accurate trajectory predictions in case of distress situations.

With increasing threats to GPS spoofing and jamming, an authentication scheme is presented by [85] for 6G-IoT-enable maritime transportation. The proposed approach is

TABLE II
A BRIEF SUMMARY OF MODELS USED FOR CYBER RISK ANALYSIS

Ref.	Model	Application	Objectives
[34]	maCRA for autonomous ships	Autonomous ships	Anticipation of probable risks for futuristic autonomous ships in maritime sector.
[59]	Qualitative	INS risk analysis	Analyzing risks associated with navigation tools, charts and interfaces.
[60]	Qualitative	ECDIS risk analysis	Risk analysis for ECDIS components such as SMB, RPC, etc.
[61]	maCRA	Ship with different functionalities, users and configurations	Risk analysis for different kinds of ships, by considering ease of vulnerabilities and exploit reward.
[62]	Mixed	ECDIS risk analysis	Risk analysis using vulnerability scanning and penetration testing techniques.
[63]	Mixed	ECDIS vulnerability	Onboard ship security survey and computational scanning for cyber vulnerability.
[64]	Computational penetration testing	ECDIS third-party service vulnerability	Computational penetration for cyber security threats associated with ECDIS third party services.
[65]	Survey	Maritime cyber risk analysis	Highlighting the most vulnerable component of the maritime including the crew, IT, and operation technology.
[66]	Interviewing	Human factors in cyber risk	Evaluating and highlighting the human factors leading to cyber attacks.
[67]	Survey	Factors for cyber risk	Analyze factors responsible for cyber risks in maritime such as training, IT procedures vulnerability, etc.
[68]	Survey	Cyber risk analysis	Finding factors related to maritime cyber attack to mitigate risk impact, such as social media, human factors, etc.

based on a lightweight message exchange protocol with increased security following initialization, vessel registration, and mutual authentication. The protocol is validated by using the Real-Or-Random model. Results indicate the superior performance of the proposed approach with respect to security and security-to-efficiency trade-off. Along the same lines, an attribute-based data aggregation scheme is proposed in [86] that focuses on the security of isolated IoT-enabled maritime ships. In the proposed scheme, onboard sensors are incorporated for the aggregation of the maritime terminal. The zero-knowledge proof ensures that only legitimate participants can participate in the communication. Results prove the security reliability of the scheme and the reduced computation cost.

The study [87] proposes a framework to detect and defend against the domain name system (DNS) rebinding attacks. A Markov chain model is used to model the DNS rebinding attack. The important attributes are extracted and used with a novel detection model. Experimental results show that the model is suitable for onboard local IoT devices and provides a defense mechanism against DNS rebinding attacks. Similarly, a security and privacy-preserving protocol is proposed in [88] to secure the communication between the maritime electric vehicles and charged grids. The proposed solution is based on blockchain technology and utilizes encryption and consensus algorithms to ensure secure communication [89]. Another endeavor to secure the data sharing between maritime ships and offshore servers is [90] that designed an identity-based information-sharing scheme. The scheme utilizes the blockchain in the fog environment, and smart contracts are used to control secure access to the data. With the proposed scheme, increased security is obtained with reduced computational complexity. Similarly, the authors propose a data integrity framework for maritime transportation systems in [91]. The data blocks are encoded using the erasure coding that provides security against malicious attacks. The data is stored on the cloud and can be recovered in case of data loss. The proposed approach proves to have a low computational head.

Several threat modeling approaches have been devised and adopted for maritime cyber risk analysis and mitigation. STRIDE covers six security threats: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges and performs qualitative analysis of cyber risks [92]. Threat analysis is carried out by developing attack scenarios regarding security objectives such as integrity, authorization, etc. STRIDE is especially useful for discovering vulnerabilities in the systems under design, thus enabling the authorities to eliminate such vulnerabilities in the design process [93], [94]. DREAD is another model for risk mitigation that weights the risks by considering five aspects, including damage potential, reproducibility, exploitability, affected users, and discoverability [35]. Damage refers to the content inflicted to the system regarding the affected things (both users and systems). Reproducibility is the attackers' ability to reproduce it, and exploitability is the extent to which the systems are vulnerable. In contrast, the ability of the attacker to find the system's vulnerability is discoverability. Unlike STRIDE, which focuses on a qualitative analysis, DREAD quantifies the risks by performing a quantitative risk analysis. The values of DREAD elements are determined into high, medium, and low that are used to assign a cyber attack weight for each of the CPS [95].

A hybrid framework based on STRIDE and DREAD is presented in [96] for minimizing the threat of cyber attacks in the maritime sector. By analyzing various CPS's qualitative and quantitative risk factors, the study suggests appropriate controls to alleviate the risk of maritime cyber-attacks. The authors present MITIGATE, a threat mitigation scheme for maritime supply chain [97]. It can be used for MLSC infrastructure and the SCADA system to analyze the risk of cyber risk in a dynamic environment.

VI. INDUSTRY 4.0

Industry 3.0, which focused on automation, computers, and electronics, has been shifting towards Industry 4.0. It includes cyber-physical systems, the internet of things, networks, and

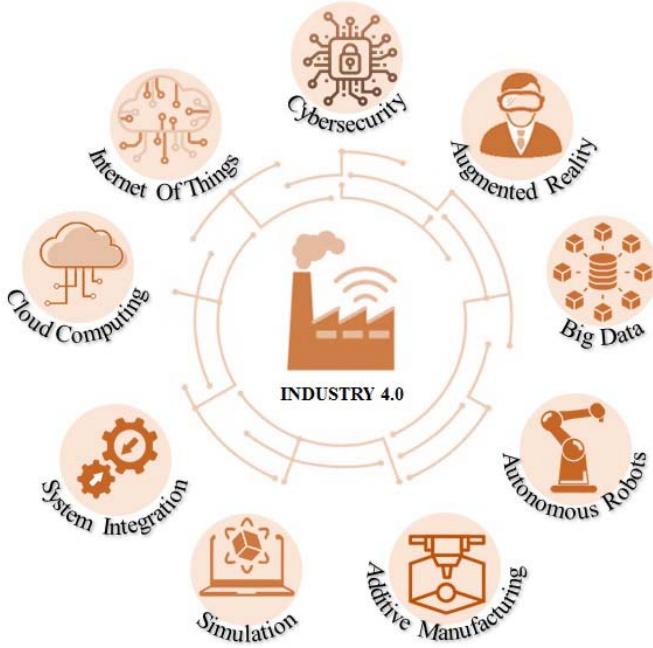


Fig. 7. Industry 4.0 envisions digital transformation, adopted from [98].

many more, as shown in Figure 7 is now performing digital transformation of maritime and its related industries. Using information and communication technology, Industry 4.0 aims at integrating machines and processes to make intelligent networks.

Technology and systems are becoming complicated and connected with every passing day. The concept of digital twins [99] and virtual reality based on the simulation present significant opportunities for the maritime sector to offer training and knowledge for crew members, third-party staff, and other people related to maritime [100]. Although digital twins are not very useful for analyzing cyber risks, virtual reality can play a significant role. It can be used to study maritime vulnerabilities arising in the foreseen Industry 4.0, where everything is connected.

Industry 4.0 is heavily reliant on the concept of IoT, where different small devices communicate via the internet, and the IoT networks can be very complex, and massive [101]. With the availability of cheaper computing power and the proliferation of mobile devices, a massive number of devices will be connected and communicating regarding ships/ports. This ubiquity will also increase the vulnerability of the communication network as more and more devices are connected [102]. So, real-time connected systems are to be modeled to study the probable cyber risks and analyze their impact. This need is further enhanced with the inception of autonomous ships, which are built on the IoT network [103]. With autonomous ships, cyber-physical systems become more prevalent and imminent because a higher number of devices will be used in physical operations.

The major cyber threats are directed remotely via the internet. However, with short-range communication in IoT devices for Industry 4.0, the intrusion threats are expected

to be higher than remote threats necessitating tightly secured and well-encrypted protocols. Three important steps for the safekeeping of maritime IT and OT systems are the IT security procedures, cyberattack response and recovery, and preparedness for cyberattacks [104]. The manager should be trained to accept and embrace the IT security mechanisms and protocols to implement IT hygiene. Cyber security training should be considered an integral part of maritime security, and appropriate response and recovery procedures should be in place [105]. Additionally, the procedures should be updated periodically to ensure that they are up-to-date. Last but most importantly, a risk-free cyber environment does not exist. No matter how advanced the technologies become, related vulnerabilities and cyber risks emerge in new forms, which necessitates the importance of being prepared to expect the threats and respond to them accordingly.

VII. DISCUSSIONS AND FUTURE DIRECTIONS

A. Ship Diversity and Disparate Environment

Many challenges in maritime cyber security bar appropriate cyber security measures and mechanisms. A major challenge is the diversity of the ships and the disparate environments they operate. With ships from different classes, the installed systems, operated environments, requirements for onboard systems, and security procedures vary significantly, making it very difficult to define standard security mechanisms that would fit all. Another problem is the lack of reliable cyber security protocols for ship equipment like GPS and ECDIS [106] due to heterogeneous vendors and manufacturers where the implementation of a security protocol may be very different. The third complexity arises from the third-party service providers that deal with the maritime operational systems. The short visitations during the ashore stay of the ship limit their capability to fix problems appropriately.

B. Improper Cyber Security Risk Assessment

One major shortcoming for the secured maritime industry is the improper risk assessment of cyber security threats. For example, different nations in the European Union (EU) implement disparate security policies and practices, complicating risk assessment comparison. In addition, targeted risk assessment procedures should be developed with respect to the nature of the MLSC infrastructure, where processes are both distributed and interconnected. Research shows that the training and knowledge of the crew member are not up to the mark to deal with the cyber risks. The majority of maritime professionals suggest a lack of knowledge specifically in the field of maritime cyber security [50]. Lack of training and expertise for cyber security led to 88% to 90% of the shipping accidents, as stated in [107], [108]. Similarly, the reliance on obsolete and outdated systems in the maritime is a major problem [109], [110].

C. Lack of Real-World Testing

Poor crew skills, complexity and sophistication of on-board systems, outdated and vulnerable information systems, inappropriate integration of IT and OT procedures, network/system

heterogeneity, and lack of updating the cyber security procedures are the leading challenges for elevated maritime cyber security risks. Lack of real-world testing systems can make it very difficult to analyze the risk impact of cyber attacks fully. Especially, systems for penetration testing in the dynamic environment are needed for futuristic cyber attacks analysis and prevention. Ethical hacking should also be promoted to make beforehand preparations to counter cyber risks [111]. GPS jamming and spoofing is the leading cyberattack that caused potential damage to the maritime industry. Relying on one navigation guide technology seems a bottleneck and inappropriate. With more sensors on-board such as radar and LIDAR (light detection and ranging) in future ships, these sensors can be used for navigation and utilize other resources for navigation guides.

D. Increased Dependence on Cyber Technology

Recent automation and digitization have evolved the maritime sector by combining IT and OT more than ever. With the advanced digital technology, the maritime infrastructure relies on cyber technology increasing its proneness to different kinds of cyberattacks. Maritime-related cyberattacks are challenging due to a lack of information on the cyberattacks, economic and disruptive impact, and insightful investigations. Cyber attacks on the maritime can target navigation, cargo movement, ECDIS elements, off-shore AIS, third-party service providers, and other processes and threaten human lives, ecosystem, and maritime trade. Cyber attackers aim to obtain media attention, ransom, destroy an organization's resources, sell confidential data, and sabotage. In addition, ship transportation to the desired location, intervening in cyber security defense, and gaining critical information regarding national infrastructure are the primary goals of different types of adversaries. However, most of these attacks happen due to obsolete operational systems, especially software, and the carelessness of the maritime staff. The proper training and knowledge of Crews can significantly enhance the defense against such attacks, and so can the up-to-date operational procedures. A recent increase in maritime cyber security threats requires next-generation cyber security dealing procedures in real-time which means that the equipment and protocols to perform real-world experiments using vulnerability testing and penetration testing are need of the hour.

E. Need to Adopt Emerging Solutions

To ensure increased defense against evolving cyber attacks, novel and emerging solutions must be adopted. In this regard, two technologies can play a pivotal role in alleviating the risk of cyber attacks on maritime ships: satellite IoT and high altitude platform (HAP) solutions. With increased GPS jamming and spoofing attacks on maritime ships, satellite IoT can work as a complementary solution with wide coverage and therefore can be advantageous in many ways [112]. Such low orbit satellites can provide communication at lower latency with lower transmission loss and supplement the GNSS [113], [114]. The third generation partnership project (3GPP) incorporates the solutions for new radio (NR) to support non-

terrestrial networks (NTN) communications [115]. In the same way, HAP systems can provide broadband connectivity and telecommunication services to remote areas where connectivity to the core network is not possible. In case of distress situations, HAP systems can provide the connectivity for mobile and core network for backhauling [116]. Since HAP systems require minimal ground infrastructure, they can be pivotal for disaster, distress, and emergency response cases.

VIII. CONCLUSION

With rapid technological advancements, the maritime sector has prospered regarding technology like sensors, communication, and security. Despite the potential benefits of embracing such digital transformation, the proneness of the maritime industry has been substantially increased as well, opening new ways and paradigms for cyber attacks. This study analyzes the cyber security threats for the maritime industry regarding the devices used for sensing, communication, navigation, and emergency response in case of distress. It is observed that the ships lack the technical staff to handle the under attack situation. The ship crew does not possess competence or is not well trained to handle cyberattacks, and the cyber security aspect of ships is overlooked. Despite several systems being in place, the relied-on systems/software are often obsolete, not fully operational, or unsuitable for real-world situations. In addition, security devices and frameworks are heterogeneous and lack standard operating procedures.

REFERENCES

- [1] European Community Shipowners' Associations, *Shipping and Global Trade Towards an EU External Shipping Policy*. Accessed: Nov. 22, 2021. [Online]. Available: <https://www.ecsa.eu/sites/default/files/publications/2017-02-27-ECSA-External-Shipping-Agenda-FINAL.pdf>
- [2] M. Kalouptsidi, *The Role of Shipping in World Trade*. Accessed: Nov. 22, 2021. [Online]. Available: <https://econofact.org/the-role-of-shipping-in-world-trade>
- [3] A. Roger. (2018). *Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitise Supply Chains*. [Online]. Available: <https://www.forbes.com/sites/rogeraitken/2018/01/16/ibm-forges-global-joint-venture-with-maersk-applying-blockchain-to-digitize-global-trade/?sh=3d6b0a36547e>
- [4] B. S. Rivkin, "Unmanned ships: Navigation and more," *Gyroscope Navigat.*, vol. 12, no. 1, pp. 96–108, Jan. 2021.
- [5] L. Register, "Cyber-enabled ships shipright procedure assignment for cyber descriptive notes for autonomous & remote access ships," *Lloyd's Register*, London, U.K., Tech. Rep., 2017.
- [6] M. Placek. (2021). *Container Throughput at Ports Worldwide From 2012 to 2020 With a Forecast for 2021 Until 2024*. [Online]. Available: <https://www.statista.com/statistics/913398/container-throughput-worldwide/>
- [7] A. Chakrabarty. *What Marine Communication Systems Are Used in the Maritime Industry*. Accessed: Nov. 27, 2021. [Online]. Available: <https://www.marineinsight.com/marine-navigation/marine-communication-systems-used-in-the-maritime-industry/>
- [8] Y.-C. Lee, S.-K. Park, W.-K. Lee, and J. Kang, "Improving cyber security awareness in maritime transport: A way forward," *J. Korean Soc. Mar. Eng.*, vol. 41, no. 8, pp. 738–745, Oct. 2017.
- [9] A. R. Lee and H. P. Wogan, "All at sea: The modern seascape of cybersecurity threats of the maritime industry," in *Proc. OCEANS MTS/IEEE Charleston*, 2018, pp. 1–8.
- [10] J. J. George and D. E. Leidner, "From clicktivism to hacktivism: Understanding digital activism," *Inf. Org.*, vol. 29, no. 3, Sep. 2019, Art. no. 100249.
- [11] A. Bagchi and J. A. Paul, "Espionage and the optimal standard of the customs-trade partnership against terrorism (C-TPAT) program in maritime security," *Eur. J. Oper. Res.*, vol. 262, no. 1, pp. 89–107, Oct. 2017.

- [12] H. Boyes, R. Isbell, and A. Luck, "Code of practice: Cyber security for ports and port systems," *Inst. Eng. Technol.*, vol. 28, p. 2016, Oct. 2016.
- [13] A. Oruc and M. S. M. MIMarEST, "Claims of state-sponsored cyberattack in the maritime industry," in *Proc. Int. Naval Eng. Conf. & Exhib.*, 2020, doi: [10.24868/issn.2515-818X.2020.021](https://doi.org/10.24868/issn.2515-818X.2020.021).
- [14] D. Volz, "Chinese hackers target universities in pursuit of maritime military secrets," *Wall Street J.*, Jan. 2019. Accessed: Nov. 29, 2021. [Online]. Available: <https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800>
- [15] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, "Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels," in *Proc. IEEE 2nd Int. Conf. social Comput.*, Oct. 2010, pp. 1147–1152.
- [16] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, "Cyber physical systems security for maritime assets," *J. Mar. Sci. Eng.*, vol. 9, no. 12, p. 1384, Dec. 2021.
- [17] J. DiRenzo, D. A. Goward, and F. S. Roberts, "The little-known challenge of maritime cyber security," in *Proc. 6th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, 2015, pp. 1–5.
- [18] B. Mednikarov, Y. Tsonev, and A. Lazarov, "Analysis of cybersecurity issues in the maritime industry," *Int. J. Inf. Secur.*, vol. 47, no. 1, pp. 27–43, 2020.
- [19] G. C. Kessler, J. P. Craiger, and J. C. Haass, "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system," *Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 12, no. 3, p. 429, 2018.
- [20] BIMCO. (2016). *The Guidelines on Cyber Security onboard Ships*. [Online]. Available: [https://www.liscr.com/sites/default/files/online_library/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016\(3\).pdf](https://www.liscr.com/sites/default/files/online_library/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016(3).pdf)
- [21] *The Guidelines Cyber Secur. Onboard Ships*, BIMCO, Copenhagen, Denmark, 2016.
- [22] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, 2014, pp. 436–445.
- [23] B. Hyra, "Analyzing the attack surface of ships," M.S. thesis, DTU Comput. Dept. Appl. Math. Comput. Sci., Technical Univ. Denmark, Lyngby, Denmark, 2019. [Online]. Available: https://backend.orbit.dtu.dk/ws/portalfiles/portal/174011206/190401_Analyzing_the_Attack_Surface_of_Ships.pdf
- [24] B. Svilicic, D. Bráic, S. Žućkin, and D. Kalebic, "Raising awareness on cyber security of ECDIS," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 13, no. 1, pp. 231–236, 2019.
- [25] T. Pseftelis and G. Chondrokoukis, "A study about the role of the human factor in maritime cybersecurity," *SPOUDAI-J. Econ. Bus.*, vol. 71, nos. 1–2, pp. 55–72, 2021.
- [26] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION, J. Inst. Navigat.*, vol. 64, no. 1, pp. 51–66, 2017.
- [27] M. Filić, "Foundations of GNSS spoofing detection and mitigation with distributed GNSS SDR receiver," *Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 12, no. 4, pp. 1–8, 2018.
- [28] M. S. K. Awan and M. A. Al Ghadri, "Understanding the vulnerabilities in digital components of an integrated bridge system (IBS)," *J. Mar. Sci. Eng.*, vol. 7, no. 10, p. 350, 2019.
- [29] A. Androjna and M. Perković, "Impact of spoofing of navigation systems on maritime situational awareness," *Trans. Maritime Sci.*, vol. 10, no. 2, pp. 361–373, Oct. 2021.
- [30] K. Korcz, "Maritime radio information systems," *J. KONES*, vol. 24, pp. 1–8, Dec. 2017.
- [31] K. Tam, K. Moara-Nkwe, and K. Jones, "The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training," *Maritime Technol. Res.*, vol. 3, no. 1, pp. 16–30, Jul. 2020.
- [32] R. Santamarta, "Maritime security: Hacking into a voyage data recorder (VDR)," IOActive, Seattle, WA, USA, 2016. Accessed: Nov. 29, 2021. [Online]. Available: <https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/>
- [33] A. Cantelli-Forti, "Forensic analysis of industrial critical systems: The costa concordia's voyage data recorder case," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 458–463.
- [34] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services*, Jun. 2018, pp. 1–8.
- [35] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *Computing Security*. Cham, Switzerland: Springer, 2018, pp. 20–36.
- [36] K. Tam and K. D. Jones, "Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping," *J. Cyber Policy*, vol. 3, no. 2, pp. 147–164, May 2018.
- [37] F. X. M. de Osés and A. U. Juncadella, "Global maritime surveillance and oceanic vessel traffic services: Towards the E-navigation," *WMU J. Maritime Affairs*, vol. 20, no. 3, pp. 1–14, 2021.
- [38] L. O'Donnell-Welch. (2021). *Cybercriminals Target Transport and Logistics Industry*. [Online]. Available: <https://duo.com/decipher/cybercriminals-target-global-logistics-industry>
- [39] A. Kinsey. (2021). *Cyber Security Threats Challenge International Shipping Industry*. [Online]. Available: <https://www.maritimeprofessional.com/news/cyber-security-threats-challenge-international-369770>
- [40] C. Clmpau. (2020). *All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyber-Attacks*. [Online]. Available: <https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/>
- [41] E.-M. Kalogeraki, N. Polemi, S. Papastergiou, and T. Panayiotopoulos, "Modeling SCADA attacks," in *Smart Trends System, Security Sustainability*. Cham, Switzerland: Springer, 2018, pp. 47–55.
- [42] D. Kravets. (2009). *Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System*. [Online]. Available: <http://www.wired.com/2009/03/feds-hacker-dis>
- [43] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017.
- [44] J. Allen *et al.*, "Mnemosyne: An effective and efficient postmortem watering hole attack investigation system," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 787–802.
- [45] K. A. Ismail, M. M. Singh, N. Mustaffa, P. Keikhsorokiani, and Z. Zulkefli, "Security strategies for hindering watering hole cyber crime attack," *Proc. Comput. Sci.*, vol. 124, pp. 656–663, Oct. 2017.
- [46] K. Borgolte, C. Kruegel, and G. Vigna, "Delta: Automatic identification of unknown web-based infection campaigns," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 109–120.
- [47] K. Borgolte, C. Kruegel, and G. Vigna, "Meerkat: Detecting website defacements through image-based object recognition," in *Proc. 24th Secur. Symp.*, 2015, pp. 595–610.
- [48] Z. Li, S. Alrwaisi, X. Wang, and E. Alowaisheq, "Hunting the red fox online: Understanding and detection of mass redirect-script injections," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 3–18.
- [49] P. R. Toth *et al.*, "Small business information security: The fundamentals," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Interagency Rep. (NISTIR) 7621 Rev. 1, 2016.
- [50] J. I. Alcaide and R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," *Transp. Res. Proc.*, vol. 45, pp. 547–554, Jan. 2020.
- [51] Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, "Internet of Things and the man-in-the-middle attacks—security and economic risks," *MEST J.*, vol. 5, no. 2, pp. 15–25, 2017.
- [52] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *J. Pendidikan Teknol. Inf.*, vol. 2, no. 2, pp. 109–134, 2019.
- [53] *Guidelines on Maritime Cyber Risk Management*, Int. Maritime Org. London, U.K., 2017.
- [54] M. P. Barrett *et al.*, "Framework for improving critical infrastructure cybersecurity version 1.1," Nat. Inst. Standards and Technol., Gaithersburg, Maryland, USA, Tech. Rep., 2018. [Online]. Available: <https://www.nist.gov/cyberframework>, doi: [10.6028/NIST.CSWP.04162018](https://doi.org/10.6028/NIST.CSWP.04162018)
- [55] H. Boyes and R. Isbell, *Code Practice: Cyber Security for Ships*. London, U.K.: Institution of Engineering and Technology, 2017.
- [56] A. Rana, "Commercial maritime and cyber risk management," *Saf. Defense*, vol. 5, no. 1, pp. 46–48, 2019.
- [57] J. Montewka, S. Ehlers, F. Goerlandt, T. Hinz, K. Tabri, and P. Kujala, "A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving RoPax vessels," *Rel. Eng. Syst. Saf.*, vol. 124, pp. 142–157, Apr. 2014.
- [58] J. Nordström *et al.*, "Vessel TRIAGE: A method for assessing and communicating the safety status of vessels in maritime distress situations," *Saf. Sci.*, vol. 85, pp. 117–129, Jun. 2016.
- [59] R. Svilicic J. Zec, "A study on cyber security threats in a shipboard integrated navigational system," *J. Mar. Sci. Eng.*, vol. 7, no. 10, p. 364, Oct. 2019.
- [60] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2015.

- [61] B. Svilicic, J. Kamahara, J. Celic, and J. Bolmsten, "Assessing ship cyber risks: A framework and case study of ECDIS security," *WMU J. Maritime Affairs*, vol. 18, no. 3, pp. 509–520, Sep. 2019.
- [62] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime cyber risk management: An experimental ship assessment," *J. Navigat.*, vol. 72, no. 5, pp. 1108–1120, Sep. 2019.
- [63] B. Svilicic and I. Rudan, "Shipboard ECDIS cyber security: Third-party component threats," *Pomorstvo*, vol. 33, no. 2, pp. 176–180, Dec. 2019.
- [64] K. Tam and K. Jones, "Situational awareness: Examining factors that affect cyber-risks in the maritime sector," *Int. J. Cyber Situational Aware.*, vol. 4, pp. 40–68, 2019.
- [65] K. Tam and K. Jones, "Factors affecting cyber risk in maritime," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment*, 2019, pp. 1–8.
- [66] R. Hanzu-Pazara, G. Raicu, and R. Zagan, "The impact of human behaviour on cyber security of the maritime systems," *Adv. Eng. Forum*, vol. 34, pp. 267–274, Oct. 2019.
- [67] S. Karamperidis, G. Koligiannis, and F. Moustakis, "Building a digital armour for the maritime sector against cyber-attacks," *Tech. Rep.*, 2020.
- [68] A. Androjna and E. Twrdy, "Cyber threats to maritime critical infrastructure," *Cyber Terrorism Extremism as Threat to Crit. Infrastructure Protection*. Ljubljana, Slovenia: Ministry Defence Republic, 2020.
- [69] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU J. Maritime Affairs*, vol. 18, no. 1, pp. 129–163, Mar. 2019.
- [70] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *J. Navigat.*, vol. 62, no. 2, pp. 173–187, Apr. 2009.
- [71] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594, 2007.
- [72] G. D. Wyss and F. A. Durán, "OBEST: The object-based event scenario tree methodology," Sandia National Labs., Albuquerque, NM, USA, Tech. Rep. SAND2001-0828, 2001.
- [73] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Quantitative cyber risk reduction estimation methodology for a small SCADA control system," in *Proc. 39th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2006, p. 226.
- [74] D. I. Gertman, R. Folkers, and J. Roberts, "Scenario-based approach to risk analysis in support of cyber security," in *Proc. Int. Topical Meeting Nucl. Plant Instrum. Controls, Hum. Mach. Interface Technol.*, 2006, pp. 1–5.
- [75] C. Beggs and M. Warren, "Safeguarding Australia from cyber-terrorism: A proposed cyber-terrorism SCADA risk framework for industry adoption," *J. Inf. Warfare*, vol. 7, no. 1, pp. 24–35, 2008.
- [76] J. D. Markovic-Petrovic and M. D. Stojanovic, "An improved risk assessment method for SCADA information security," *Elektron. Elektrotehn.*, vol. 20, no. 7, pp. 69–72, Sep. 2014.
- [77] M. Keshk, N. Moustafa, E. Sitnikova, and G. Creech, "Privacy preservation intrusion detection technique for SCADA systems," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2017, pp. 1–6.
- [78] T. Marsden, N. Moustafa, E. Sitnikova, and G. Creech, "Probability risk identification based intrusion detection system for scada systems," in *Int. Conf. Mobile Netw. Manage.* Cham, Switzerland, Springer, 2017, pp. 353–363.
- [79] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 16, 2021, doi: [10.1109/TITS.2021.3122368](https://doi.org/10.1109/TITS.2021.3122368).
- [80] R. Arul, S. Basheer, A. Abbas, and A. K. Bashir, "Role of deep learning algorithms in securing Internet of Things applications," in *Deep Learning for Internet Things Infrastructure*. Boca Raton, FL, USA: CRC Press, 2021, pp. 145–164.
- [81] A. Androjna, T. Brcko, I. Pavic, and H. Greidanus, "Assessing cyber challenges of maritime navigation," *J. Mar. Sci. Eng.*, vol. 8, no. 10, p. 776, Oct. 2020.
- [82] D. Trimble, J. Monken, and A. F. Sand, "A framework for cybersecurity assessments of critical port infrastructure," in *Proc. Int. Conf. Cyber Conflict*, 2017, pp. 1–7.
- [83] P. M. Laso *et al.*, "ISOLA: An innovative approach to cyber threat detection in cruise shipping," in *Developments and Advances in Defense and Security*. Singapore, Springer, 2022, pp. 71–81.
- [84] Q. Pan *et al.*, "Space-air-sea-ground integrated monitoring network-based maritime transportation emergency forecasting," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2843–2852, Mar. 2021.
- [85] S. A. Chaudhry *et al.*, "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 22, 2021, doi: [10.1109/TITS.2021.3134643](https://doi.org/10.1109/TITS.2021.3134643).
- [86] C. Wang, J. Shen, P. Vijayakumar, and B. B. Gupta, "Attribute-based secure data aggregation for isolated IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 1, 2021, doi: [10.1109/TITS.2021.3127436](https://doi.org/10.1109/TITS.2021.3127436).
- [87] X. He *et al.*, "DNS rebinding threat modeling and security analysis for local area network of maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 22, 2021, doi: [10.1109/TITS.2021.3135197](https://doi.org/10.1109/TITS.2021.3135197).
- [88] A. Barnawi, S. Aggarwal, N. Kumar, D. M. Alghazzawi, B. Alzahrani, and M. Boularas, "Path planning for energy management of smart maritime electric vehicles: A blockchain-based solution," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 15, 2021, doi: [10.1109/TITS.2021.3131815](https://doi.org/10.1109/TITS.2021.3131815).
- [89] Z. Zheng, T. Wang, A. K. Bashir, M. Alazab, S. Mumtaz, and X. Wang, "A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid," *IEEE Trans. Comput.*, early access, Nov. 24, 2021, doi: [10.1109/TC.2021.3130402](https://doi.org/10.1109/TC.2021.3130402).
- [90] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 15, 2021, doi: [10.1109/TITS.2021.3125402](https://doi.org/10.1109/TITS.2021.3125402).
- [91] D. Liu, Y. Zhang, W. Wang, K. Dev, and S. A. Khowaja, "Flexible data integrity checking with original data recovery in iot-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, Nov. 15, 2021, doi: [10.1109/TITS.2021.3125070](https://doi.org/10.1109/TITS.2021.3125070).
- [92] A. Shostack, *Threat Modeling: Designing for Security*. Hoboken, NJ, USA: Wiley, 2014.
- [93] D. Seifert and H. Reza, "A security analysis of cyber-physical systems architecture for healthcare," *Computers*, vol. 5, no. 4, p. 27, Oct. 2016.
- [94] G. Kavallieratos and S. Katsikas, "Attack path analysis for cyber physical systems," in *Computing Security*. Cham, Switzerland: Springer, 2020, pp. 19–33.
- [95] P. Nespoli, D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1361–1396, 2nd Quart., 2018.
- [96] G. Kavallieratos and S. Katsikas, "Managing cyber security risks of the cyber-enabled ship," *J. Mar. Sci. Eng.*, vol. 8, no. 10, p. 768, Sep. 2020.
- [97] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, "A novel risk assessment methodology for SCADA maritime logistics environments," *Appl. Sci.*, vol. 8, no. 9, p. 1477, Aug. 2018.
- [98] I. Sceep. (2021). *Industry 4.0 and the Fourth Industrial Revolution Explained*. [Online]. Available: <https://www.i-scoop.eu/industry-4-0/>
- [99] F. Tao, F. Sui, A. Liu, Q. Qi, M. Zhang, B. Song, Z. Guo, S. C.-Y. Lu, and A. Y. C. Nee, "Digital twin-driven product design framework," *Int. J. Prod. Res.*, vol. 57, no. 12, pp. 3935–3953, 2018.
- [100] S. Frydenberg, K. Nordby, and J. O. Eikenes, "Exploring designs of augmented reality systems for ship bridges in Arctic waters," *Hum. Factors*, vol. 26, p. 27, Dec. 2018.
- [101] S. D. Pizzo, A. De Martino, G. De Viti, R. L. Testa, and G. De Angelis, "IoT for buoy monitoring system," in *Proc. IEEE Int. Workshop MetroL. Sea, Learn. Measure Sea Health Parameters (MetroSea)*, Oct. 2018, pp. 232–236.
- [102] A. Zolich *et al.*, "Survey on communication and networks for autonomous marine systems," *J. Intell. Robot. Syst.*, vol. 95, no. 3, pp. 789–813, 2019.
- [103] K. Tam, K. Forshaw, and K. Jones, "Cyber-SHIP: Developing next generation maritime cyber research capabilities," in *Proc. Conf. ICMET Oman*, 2019.
- [104] H. Oe and H. Nguyen, "Opportunities, challenges, and the future of cruise ship tourism: Beyond covid-19 with ubiquitous information sharing and decision-making," *Int. J. Manage. Decis. Making*, vol. 20, no. 3, pp. 221–240, 2021.
- [105] G. Kavallieratos, V. Diamantopoulou, and S. K. Katsikas, "Shipping 4.0: Security requirements for the cyber-enabled ship," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6617–6625, Oct. 2020.
- [106] L. Kelion. (2018). *Ship Hack 'Risks Chaos In English Channel*. Accessed: Dec. 2, 2021. [Online]. Available: <https://mfame.guru/ship-hack-risks-chaos-in-english-channel/>
- [107] C. Heij and S. Knapp, "Predictive power of inspection outcomes for future shipping accidents—An empirical appraisal with special attention for human factor aspects," *Maritime Policy Manage.*, vol. 45, no. 5, pp. 604–621, Jul. 2018.

- [108] C. Park, W. Shi, W. Zhang, C. Kontovas, and C. Chang, "Cybersecurity in the maritime industry: A literature review," in *Proc. 20th Commemorative Annu. Gen. Assem.*, 2019, pp. 79–86.
- [109] R. Sen, "Cyber and infomation threats to seaports and ships," *Maritime Secur.*, vol. 4, pp. 281–302, Dec. 2016.
- [110] K. D. Jones, K. Tam, and M. Papadaki, "Threats and impacts in maritime cyber security," *Eng. Technol. Ref.*, vol. 1, 2012.
- [111] R. Chia, "The need for ethical hacking in the maritime industry," *Soc. Nav. Architects Mar. Eng.*, vol. 38, pp. 108–121, Sep. 2019.
- [112] D. Yang, Y. Zhou, W. Huang, and X. Zhou, "5G mobile communication convergence protocol architecture and key technologies in satellite Internet of Things system," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 465–476, Feb. 2021.
- [113] M. Jia and Q. Guo, "Editorial: Intelligent cognitive internet of integrated space and terrestrial things," *Mobile Netw. Appl.*, vol. 24, no. 6, pp. 1924–1925, Dec. 2019.
- [114] Y. Qian, L. Ma, and X. Liang, "The performance of chirp signal used in LEO satellite Internet of Things," *IEEE Commun. Lett.*, vol. 23, no. 8, pp. 1319–1322, Aug. 2019.
- [115] *Solutions for NR to Support Non-Terrestrial Networks (NTN)*, document 38.821, 3GPP, 2019.
- [116] M. Q. Vu, N. T. Dang, and A. T. Pham, "HAP-aided relaying satellite FSO/QKD systems for secure vehicular networks," in *Proc. IEEE 89th Veh. Technol. Conf.*, Apr. 2019, pp. 1–6.



Imran Ashraf received the M.S. degree (Hons.) in computer science from the Blekinge Institute of Technology, Karlskrona, Sweden, in 2010, and the Ph.D. degree in information and communication engineering from Yeungnam University, Gyeongsan, South Korea, in 2018. He has worked as a Post-Doctoral Fellow at Yeungnam University. He is currently working as an Assistant Professor with the Information and Communication Engineering Department, Yeungnam University. His research areas include positioning using next-generation networks, communication in 5G and beyond, location-based services in wireless communication, smart sensors (LIDAR) for smart cars, and data analytics.



Yongwan Park received the B.E. and M.E. degrees in electrical engineering from Kyungpook University, Daegu, South Korea, in 1982 and 1984, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the State University of New York at Buffalo, USA, in 1989 and 1992, respectively. He worked at the California Institute of Technology as a Research Fellow from 1992 to 1993. From 1994 to 1996, he served as a Chief Researcher for developing IMT-2000 system at SK Telecom, South Korea. Since 1996, he has been a Professor of information and communication engineering at Yeungnam University, South Korea. From January 2000 to February 2000, he was an Invited Professor at the NTT DoCoMo Wireless Laboratory, Japan. He was also a Visiting Professor at UC Irvine, USA, in 2003. From 2008 to 2009, he served as the Director of the Technology Innovation Center for Wireless Multimedia, Korean Government. From 2009 to March 2017, he also served as the President of the Gyeongbuk Institute of IT Convergence Industry Technology (GITC), South Korea. He is also serving as the Chairman of 5G Forum Convergence Service Committee, South Korea. His current research interests include 5G systems in communication, OFDM, PAPR reduction, indoor location-based services in wireless communication, and smart sensors (LIDAR) for smart car.



Soojung Hur received the B.S. degree from Daegu University, Gyeongbuk, South Korea, in 2001, the M.S. degree in electrical engineering from San Diego State University, San Diego, in 2004, and the M.S. and Ph.D. degrees in information and communication engineering from Yeungnam University, South Korea, in 2007 and 2012, respectively. She is working as a Research Professor with the Mobile Communication Laboratory, Yeungnam University. Her current research interests include the performance of mobile communication, indoor/outdoor location, and unnamed vehicle.



Sung Won Kim received the B.S. and M.S. degrees from the Department of Control and Instrumentation Engineering, Seoul National University, South Korea, in 1990 and 1992, respectively, and the Ph.D. degree from the School of Electrical Engineering and Computer Sciences, Seoul National University, in August 2002. From January 1992 to August 2001, he was a Researcher at the Research and Development Center of LG Electronics, South Korea. From August 2001 to August 2003, he was a Researcher at the Research and Development Center of AL Tech, South Korea. From August 2003 to February 2005, he was a Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, USA. In March 2005, he joined the Department of Information and Communication Engineering, Yeungnam University, Gyeongsangbuk-do, South Korea, where he is currently a Professor. His research interests include resource management, wireless networks, mobile computing, performance evaluation, and machine learning.



Roobaea Alroobaea received the bachelor's degree (Hons.) in computer science from King Abdulaziz University (KAU), Saudi Arabia, in 2008, and the master's degree in information system and the Ph.D. degree in computer science from the University of East Anglia, U.K., in 2012 and 2016, respectively. He is currently an Associate Professor with the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include human-computer interaction, software engendering, cloud computing, the Internet of Thing, artificial intelligent, and machine learning.



Yousaf Bin Zikria (Senior Member, IEEE) is currently working as an Assistant Professor with the Department of Information and Communication Engineering, Yeungnam University, South Korea. He authored more than 100 refereed articles, conference papers, book chapters, and patents. His journal article's cumulative impact factor (IF) is more than 320. He published papers at the top venue, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE Wireless Communications Magazine, IEEE NETWORK, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Future Generation Computer Systems (Elsevier), Sustainable Cities and Society (Elsevier), and Journal of Network and Computer Applications (Elsevier). He has managed numerous FT/SI in SCIE indexed journals. His research interests include the IoT, 5G, machine learning, wireless communications and networks, WSNs, routing protocols, CRAHN, CRASN, transport protocols, VANETS, embedded systems, and network and information security. He also held the prestigious CISA, JNCIS-SEC, JNCIS-ER, JNCIA-ER, JNCIA-EX, and Advance Routing Switching and WAN Technologies certifications. He is listed in the world's top 2% of researchers published by Elsevier and Stanford University. GoogleScholar: <https://scholar.google.com/citations?user=K90qMyMAAAJhl=en> Website: <https://sites.google.com/view/ybzikria> Researchgate: <https://www.researchgate.net/profile/Yousaf-Zikria>



Summera Nosheen received the Ph.D. degree from the School of Electrical Engineering and Computing, The University of Newcastle, NSW, Australia, in 2021. She is currently with the Faculty of Engineering, The University of Sydney, NSW, Australia. She received the Commonwealth Department of Education, Science and Training and The University of Newcastle Research Training Program (RTP) tuition fee and stipend scholarships. Her research interests include wireless networks, quality of service, quality of experience, and MAC layer resource allocation.