Ensuring resilience in ocean energy power plants: a review on cybersecurity

Thalita Nazaré, Lucas Nardo, Janier Arias-Garcia, and Erivelton Nepomuceno

Abstract—**The present review delves into the escalating significance of cybersecurity within the domain of Ocean Renewable Energy (ORE), with emphasis on wave energy power plants. The susceptibility of crucial infrastructure to cyber threats has been amplified by the escalation in interconnectivity and digitalization of energy systems. The absence of a thorough academic investigation into cybersecurity remedies for ocean energy systems has been recognized, despite the pressing demand. This research conforms to the systematic literature review standards established by Kitchenham and Charters. The study investigates three principal areas of interest:** ***smart ocean*****,** ***cybersecurity for renewable energy systems*****, and** ***marine data security*****. The results highlight the necessity of improving the ability of power plants to withstand cyber attacks and emphasize the potential of various technologies, including the Internet of Things, blockchain, artificial intelligence, and cloud computing in achieving this objective. The aforementioned analysis emphasizes the importance of ongoing exploration and advancement in cybersecurity protocols. It recommends that forthcoming efforts concentrate on quantum computing and policy frameworks that facilitate the establishment of robust, all-encompassing, and just cybersecurity resolutions in the domain of ocean energy.**

Index Terms—**Ocean Energy, Cybersecurity, Marine Data, Smart Ocean.**

I. Introduction

THERE is a massive surge in renewable energy sources, predominantly solar and offshore wind, contributing to increased diversity in energy generation [1]. Other forms of energy such as wave and tidal power are not to be overlooked as they are also important and consistently evolving [2–4]. Evidence of the sustained interest in these topics was observed at the recent IEEE OCEANS 2023 conference held in June 2023 in Limerick, Ireland, where offshore renewable energy themes were notably highlighted. This contemporary shift in the energy landscape is largely driven by increasing concerns over climate change, the urgent need to transition towards energy sources with lower carbon emissions, and the depletion of conventional fossil fuel reserves.

Among Offshore Renewable Energy (ORE) sources, wave power stands as a prominent solution to the issues of energy security and environmental sustainability. They are deemed practical and environmentally friendly, with vast potential to alleviate these concerns. Wave energy serves as a notable example of ORE sources [5, 6]. Once ORE facilities, like wave power plants, are established, they inherently become significant assets, playing a crucial role as critical infrastructures within a country. These infrastructures are not only pivotal in producing sustainable energy, thereby addressing issues of environmental sustainability and energy security, but also in maintaining the functionality of the society and the economy.

However, the reality of the modern era is that these critical infrastructures are largely controlled and managed by computerized systems. In this way, governments are currently facing the challenge of addressing cybersecurity as a critical issue that is gaining significance [7, 8]. The plausibility of cyberattacks on energy infrastructure is progressively materializing as the interconnectivity of energy systems expands and digital technologies proliferate. The concern is particularly pronounced about critical infrastructure, which encompasses indispensable services for both society and the economy, such as the energy sector [9]. Given this circumstance, international entities such as the European Commission have underscored the significance of enhancing the resilience of critical infrastructure and mitigating its vulnerability to cyber assaults.

Despite the growing recognition of the importance of cybersecurity in energy systems, academic investigations and research that focus exclusively on this domain are comparatively incipient. It is evident that a thorough evaluation of cybersecurity measures, particularly concerning ocean energy, has not been conducted thus far. However, recent technical reports developed between 2020 and 2021 have addressed methodologies for cybersecurity in ocean energy, as shown in Section III. Hence, given the importance of the topic and its status as a nascent field of inquiry, it is imperative to verify the bibliographic references. To date, there is a dearth of literature reviews that are specifically focused on the subject of ocean energy.

Consequently, this study aims to address the knowledge gap by conducting a comprehensive assessment of the cybersecurity measures currently implemented in the field of ocean energy. The present review is being conducted to fulfill the research objectives. Following the guidelines established in Kitchenham and Charters' criteria for conducting systematic literature reviews [10], a comprehensive examination of several scientific

© 2023 European Wave and Tidal Energy Conference. This paper has been subjected to single-blind peer review.

This work was promoted by Maynooth University and the Federal University of Minas Gerais.

T. Nazaré and E. Nepomuceno are with the Center for Ocean Energy Research, Department of Electronic Engineering, Maynooth University, Ireland, (e-mail: thalita.nazare.2023@mumail.ie, erivelton.nepomuceno@mu.ie).

L. Nardo and J. Arias-Garcia are with the Graduate Program in Electrical Engineering and the Department of Electronic Engineering, Federal University of Minas Gerais, Brazil (e-mail: nardo@ufmg.br, janier-arias@ufmg.br).

Digital Object Identifier:
https://doi.org/10.36688/ewtec-2023-452

papers was conducted. Our study has focused on three key domains, namely the “smart ocean”, “cybersecurity for renewable energy systems”, and “marine data security”. The interconnectivity of these concepts implies that acquiring knowledge of any one of them enhances one’s understanding of the rest.

The *smart ocean* concept, for instance, encapsulates an integrated marine environment augmented by sensors, communication capabilities, and computing power, connecting various objects both on the surface and underwater [11]. As this ecosystem evolves, Wave Energy Converters (WECs) become crucial nodes that require robust safety systems. This need was succinctly articulated in the first report on cybersecurity guidance for Marine Renewable Energy (MRE) systems by the Pacific Northwest National Laboratory (PNNL) [12], where various threats and vulnerabilities to information technology (IT) and operational technology (OT) equipment used in WECs were thoroughly assessed.

By analyzing these interrelated themes, we offer an expansive overview of the application of cybersecurity measures in the context of ocean energy. Our findings underscore the urgency of enhancing the resilience of power plants against cyber threats and serve as a valuable resource for future research aiming to fortify the security of renewable energy systems. This endeavor contributes substantially to the ongoing efforts to secure our energy future in the face of ever-evolving cyber threats and a rapidly changing energy landscape.

II. Methodology

In this study, a comprehensive literature review was conducted between 2012 and the present day to examine the resilience of ocean energy power plants. The primary objective of the literature review was to identify existing research on the topic and synthesize the findings to provide a comprehensive overview of the current state of research in this field. The process for conducting the literature review was established after careful consideration of the research questions and objectives. As shown in Figure 1, the steps involved in the review process included identifying relevant databases, selecting appropriate search terms, screening relevant articles, and synthesizing the findings. These steps were carefully followed to ensure that the review process was rigorous and comprehensive, and that the resulting findings were valid and reliable. The authors searched four main sources, namely SCOPUS, WEB OF SCIENCE, IEEE XPLORE, and PUBLISH OR PERISH using specific search queries that were tailored to each source. The first advanced search key used was: *(("Document Title":Cybersecurity) AND ("Abstract":Energy) OR ("Abstract":Marine Energy) OR ("Abstract":Renewable Energy))*, and among the documents found, using a combination of the terms “cybersecurity” and “marine energy”, articles that are part of this work were filtered.

Following this initial screening, the authors conducted a thorough evaluation of the abstracts of the selected papers to assess their relevance and suitability for inclusion in the review. Duplicate articles were excluded, and some papers were included based on the authors’ expertise in the field. To gain a comprehensive understanding of the applications and to comprehend state-of-the-art, a full-text examination was conducted on the selected articles.

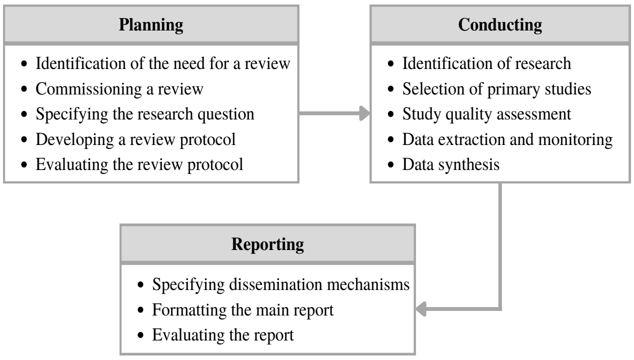
Planning
• Identification of the need for a review
• Commissioning a review
• Specifying the research question
• Developing a review protocol
• Evaluating the review protocol
Conducting
• Identification of research
• Selection of primary studies
• Study quality assessment
• Data extraction and monitoring
• Data synthesis
Reporting
• Specifying dissemination mechanisms
• Formatting the main report
• Evaluating the report

Fig. 1. Three stages of the proposed methodology for the bibliographic review. The first stage is the selection of the databases used for the search, followed by the second stage of the application of the inclusion and exclusion criteria to the articles found. The third and final stage is the analysis of the selected articles and the extraction of relevant information, such as the areas and keywords addressed in the articles.

III. Technical Reports

Once the WECs are installed, it is also essential to develop safety systems for these devices, as demonstrated in the first report on cybersecurity guidance for MRE systems [12] prepared by the Pacific Northwest National Laboratory. In preparation for this report, researchers reviewed the cyber threats and vulnerabilities of information technology (IT) and operational technology (OT) equipment used in various WEC models. Figure 2 presents an example of the possible threats and attacks on WEC devices.

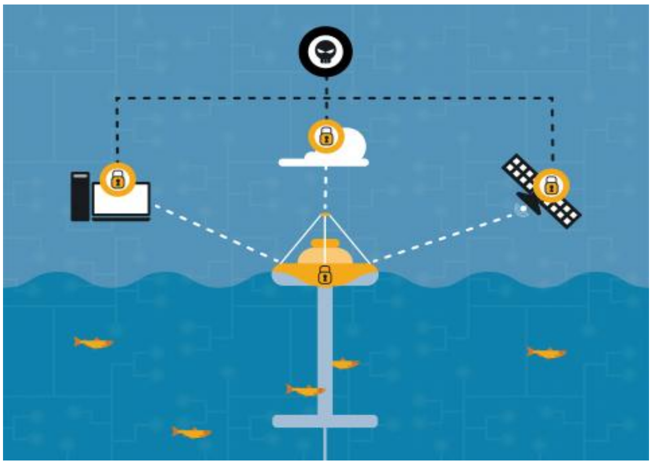

Fig. 2. PNNL’s report incorporates cybersecurity guidance on how to protect an MRE device from potential threats to a system through a satellite, Wi-Fi, or cloud computing and threats to the actual physical device itself. (Illustration by Stephanie King | Pacific Northwest National Laboratory.) Source: *Pacific Northwest National Laboratory.*

A. Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems [13]

In this technical report, the authors present a method for assessing cybersecurity threats to the MRE sector. The study, conducted by the Pacific Northwest National Laboratory, emphasizes the importance of identifying vulnerabilities and quantifying risk levels to address and prevent potential cybersecurity breaches.

Given the increasing reliance on renewable energy sources in the maritime industry, the safety and security of these MRE systems are crucial. Cybersecurity vulnerabilities could significantly impact the operation of these energy systems, potentially disrupting the energy supply and posing broader economic and environmental threats. The framework proposed in the report aims to support a comprehensive and systematic approach to assess the cybersecurity landscape in the MRE sector, providing a roadmap for managing and mitigating potential risks.

Figures 3 and 4 are provided by the authors and present network architectures as exemplars for two distinct designs of MRE systems. The aforementioned instances are grounded on data obtained from Requests for Information and are in direct alignment with extant systems created by practitioners in the field. The aforementioned network architectures offer a more granular understanding of potential hazards and avenues of attack that may be encountered by MRE.

The paper does not furnish specifics regarding the report's substance; however, such a structure would probably would encompass the identification of potential threats, assessment of vulnerabilities, quantification of risks, and strategies for mitigating said risks. The implementation of regulatory standards and industry best practices could potentially serve as a solution to address the cybersecurity needs in the MRE sector, thereby enhancing its preparedness. The technical report possesses significant value for professionals in the industry, policymakers, and researchers. It serves as a crucial resource for augmenting cybersecurity measures in the marine renewable energy domain.

B. Cybersecurity Resiliency of Marine Renewable Energy Systems-Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk [14]

In the present report, Peralta *et al.* delve into the crucial subject of cybersecurity as it pertains to marine renewable energy systems. The 2020 publication in the Marine Technology Society Journal explores the detection of cybersecurity susceptibilities and the evaluation of correlated hazards within these structures. This research aims to tackle the growing apprehensions about the cybersecurity of marine-based renewable energy systems. Renewable energy sources, including wind, tidal, and wave power, are increasingly being incorporated into the global energy landscape. Nevertheless, similar to any digitally linked infrastructure, these systems are vulnerable to cybersecurity risks. Consequently, comprehending the vulnerabilities and hazards is imperative in guaranteeing the durability and sustained feasibility of marine renewable energy systems. The research conducted by the authors underscores the significance of detecting probable susceptibilities in marine-based renewable energy systems. The study endeavors to identify vulnerabilities in the cybersecurity framework of the systems through a thorough analysis. The present analysis takes into account diverse factors, including communication networks, control systems, data storage, and information exchange protocols.

Additionally, the article underscores the importance of identifying the potential risks that arise from these vulnerabilities. Peralta *et al.* conduct an assessment of the possible ramifications of cyber-attacks on marine renewable energy systems, encompassing interference with power generation, violation of data integrity, and endangerment of personnel and infrastructure. The research endeavors to enhance the resilience of marine renewable energy systems against cyber threats by quantifying and evaluating the associated risks. This contributes to the advancement of cybersecurity strategies that are capable of providing robust protection. The article's findings provide significant insights into the distinct vulnerabilities and risks encountered by marine renewable energy systems. The identification of these vulnerabilities and the quantification of their potential impacts establish a fundamental basis for forthcoming investigations and the creation of specific cybersecurity strategies. The identified risks can be proactively addressed, and suitable security measures can be implemented by stakeholders, such as engineers, policymakers, and cybersecurity professionals.

The research holds a broader significance that transcends the marine renewable energy sector in the short term. The vulnerabilities and risks highlighted in this study have broader implications for the protection of critical infrastructure, given the growing dependence on renewable energy sources worldwide. The analysis of cybersecurity in marine renewable energy systems can provide valuable insights for the creation of secure and resilient infrastructure in various other sectors.

C. Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management [12]

In the subsequent segment of the document titled *Cybersecurity Resiliency of Marine Renewable Energy Systems*, Peralta *et al.* expand upon their prior investigations and conduct a more comprehensive exploration of the subject of cybersecurity in marine renewable energy systems. The 2021 publication in the Marine Technology Society Journal centers on the implementation of cybersecurity best practices and risk management strategies as means of bolstering the resilience of such systems. The primary aim of this study is to furnish pragmatic directives and suggestions for the implementation of efficacious cybersecurity measures in marine renewable energy systems. The authors endeavor to devise a comprehensive framework that can effectively mitigate potential cyber threats and ensure the long-term security and reliability of these systems

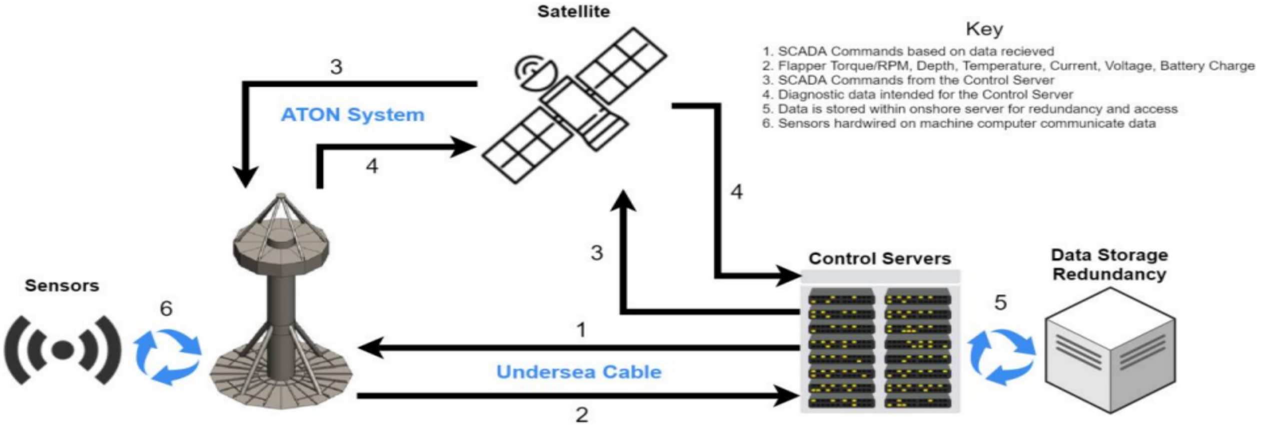
Satellite
Key
1. SCADA Commands based on data recieved
2. Flapper Torque/RPM, Depth, Temperature, Current, Voltage, Battery Charge
3. SCADA Commands from the Control Server
4. Diagnostic data intended for the Control Server
5. Data is stored within onshore server for redundancy and access
6. Sensors hardwired on machine computer communicate data
3
ATON System
4
4
3
Sensors
6
Control Servers
Data Storage Redundancy
5
1
Undersea Cable
2

Fig. 3. An in-production MRE system powers the grid using a wave point absorber design. This concept sends sensor data to control servers onshore via undersea cable for redundancy and processing. The buoy system talks to a satellite and back to the onshore control servers for redundancy. Source: [13].

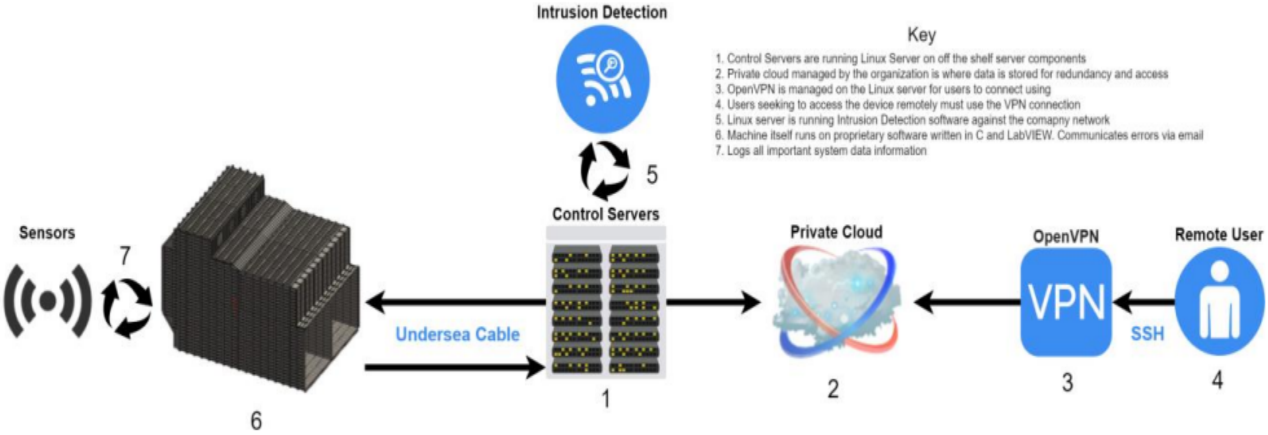
Intrusion Detection
Key
1. Control Servers are running Linux Server on off the shelf server components
2. Private cloud managed by the organization is where data is stored for redundancy and access
3. OpenVPN is managed on the Linux server for users to connect using
4. Users seeking to access the device remotely must use the VPN connection
5. Linux server is running Intrusion Detection software against the comapny network
6. Machine itself runs on proprietary software written in C and LabVIEW. Communicates errors via email
7. Logs all important system data information
5
Control Servers
Sensors
7
Private Cloud
OpenVPN
Remote User
VPN
SSH
Undersea Cable
1
2
3
4
6

Fig. 4. Oscillating water column architecture for large-scale grid power. This technology feeds MRE device sensor data to onshore control servers via an underwater cable. Linux servers have network intrusion detection software. Remote users may utilize a virtual private network to access the information in a private cloud. Source: [13].

by scrutinizing the vulnerabilities and risks identified in the first part of the study.

The article underscores the significance of implementing cybersecurity measures that are optimized to suit the distinct attributes and complexities of marine renewable energy systems. The authors investigate multiple facets, encompassing system architecture, network security, access controls, encryption protocols, intrusion detection systems, incident response plans, and employee training. The research endeavors to establish a fundamental framework for organizations to enhance their cybersecurity stance by delineating these optimal methodologies.

The authors' approach to cybersecurity resiliency places significant emphasis on the pivotal role of risk management. The proponents of risk management recommend a proactive and iterative approach to risk assessment. This entails the identification and prioritization of risks, the implementation of risk mitigation strategies, and the continuous monitoring and evaluation of the efficacy of these measures. The article underscores the importance of conducting routine security audits, vulnerability assessments, and penetration testing to detect and remediate potential vulnerabilities in the system's protective measures. Additionally, the study recognizes the cooperative aspect of cybersecurity within the marine renewable energy industry. The significance of information sharing and collaboration among stakeholders, such as industry professionals, government agencies, and cybersecurity experts, is underscored by the authors. The research endeavors to promote the sharing of knowledge and experiences by creating a collaborative environment, with the ultimate goal of enhancing cybersecurity practices and standards.

The article's findings offer pragmatic perspectives and suggestions for augmenting the cybersecurity resilience of marine renewable energy systems. Organizations within this sector can enhance their resilience against cyber threats by adhering to established best practices and executing risk management tactics. The study provides direction to engineers, policymakers, and cybersecurity experts in creating all-encompassing security frameworks that safeguard vital infrastructure and guarantee the uninterrupted functioning of marine renewable energy activities. Additionally, the study recognizes the dynamic character of cybersecurity hazards and emphasizes the necessity for continuous surveillance and adjustment. The authors advocate for organizations to remain knowledgeable about emerging threats, remain current with technological advancements, and consistently reevaluate their cybersecurity measures to effectively tackle new challenges.

IV. Smart Ocean

The present research papers provide an in-depth exploration of the Internet of Things (IoT) and its utilization in maritime ecosystems, commonly known as the "Smart Ocean". The authors underscore the crucial significance of cybersecurity, underscoring the pertinence of safeguarding data and privacy in interconnected expansive ecosystems. Figure 5 presents an illustration of possible connections and systems present in the Smart Ocean.

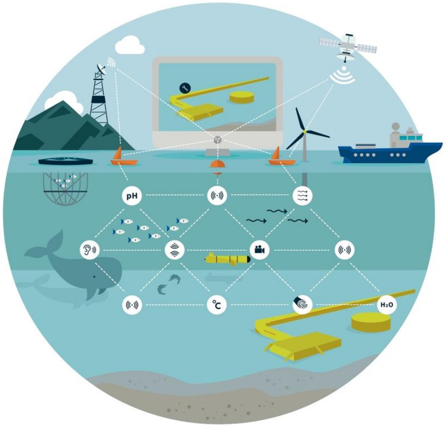

Fig. 5. A visual representation depicting a specific instance of the numerous interconnections and systems that exist within the Smart Ocean. Source: [15].

The authors in [16] initiate the discourse by examining the essential technical elements of the IoT, including machine-to-machine communication, random access, and relay protocols in the Smart Ocean framework. The study highlights the fundamental cybersecurity factors that are involved in enabling dependable and secure data transmission in oceanic settings. In addition, Lin *et al.* [17] elucidate the vast potential that the IoT offers for the advancement of Smart Ocean. They also call attention to the critical function that secures data transfer and integrity play in the effective deployment of such technologies.

Shen *et al.* [18] provide a more comprehensive analysis of the topic of safeguarding data. They propose a two-factor-based public data protection scheme for Smart Ocean management, highlighting the crucial nature of data security in preventing unauthorized access and maintaining data integrity in these vast interconnected systems. The present article offers preliminary insights into the necessity of implementing strong cybersecurity protocols to ensure the seamless functioning of Internet of Things applications in the context of Smart Ocean. Building on this theme of data security, Tian *et al.* [19] introduce an Ocean Oriented Blockchain System (OOBS) for cross-organizational data sharing. The authors' methodology places significant emphasis on the potential of blockchain technology to serve as a secure, transparent, and tamper-resistant medium for data sharing. This approach offers a novel perspective on cybersecurity in Smart Ocean applications.

The role of artificial intelligence (AI) in marine governance is discussed by Bakker [20]. Dai *et al.* [11] underscore the importance of integrating sensing, communication, and computing networks in the context of Smart Oceans. The significance of safeguarding advanced technologies from potential cyber threats is implicitly emphasized in both articles. Han *et al.* [21] suggest a data importance-based scheme that utilizes an Autonomous Underwater Vehicle (AUV) to safeguard location privacy in Smart Ocean. The authors emphasize the significance of privacy in the realm of cybersecurity. Yu *et al.* [22] propose a privacy preservation mechanism utilizing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) within the context of crowdsourcing-IoT. The aforementioned papers underscore the imperative to safeguard personal and location data in IoT networks, thereby underscoring an additional crucial aspect of cybersecurity in the context of Smart Ocean. Hu *et al.* [23] address the concerns pertaining to the secure and efficient collection and storage of data in the Smart Ocean Internet of Things domain. The authors' research highlights the correlation between proficient data management and successful cybersecurity by prioritizing the principles of data integrity, confidentiality, and accessibility.

The aforementioned articles collectively establish an interrelated network of scholarly investigations that highlight the intersection of IoT, Smart Ocean, and cybersecurity. The authors shed light on the intricate nature of safeguarding data and privacy in vast, interlinked marine environments, underscoring the significance of strong cybersecurity protocols in the advancement of Smart Ocean endeavors.

V. Marine Data

Marine big data, an exponentially growing dataset produced from a multitude of marine data acquisition techniques, has garnered significant attention in the realm of marine sciences and technology. As pointed out by [24], marine big data harbors immense potential value for a wide array of marine-related fields, including tsunami and red tide warnings, disaster prevention and forecasting, as well as visualization modeling post-disasters. Despite its prospective advantages, the management and utilization of this data present a myriad of challenges, including difficulties in data capture, storage, analysis, applications, data quality control, and notably, data security.

As the volume of marine data grows, the challenges for data storage and transmission become increasingly pronounced. Traditional information security methods, characterized by centralization, fail to provide comprehensive protection, sparking a need for new solutions. The paper [25] proposes a shift from these centralized methods towards a decentralized approach, specifically highlighting the potential of blockchain technology. Initially gaining popularity in the financial sector, blockchain technology ensures data security and reliability through its decentralized design, which could prove instrumental in resolving issues with data storage and transmission in the marine big data landscape.

With the evolution of maritime operations and the advent of autonomous ships, the urgency of addressing maritime cybersecurity has heightened. Recent incidents involving security breaches have not only led to substantial financial losses for shipping companies but have also posed serious risks to marine ecosystems by disabling ship controls, thereby increasing the likelihood of collisions and hazmat spills. As McGillivary [26] elucidates, maritime cybersecurity is not only a valid area of scientific policy research but also pivotal for safe ocean science operations and improved environmental security. In response to these growing concerns, innovative methods, including optical communications and quantum encryption, are being proposed to bolster maritime cybersecurity.

A critical application for secure data transmission within the maritime sector is the Automatic Identification System (AIS). This system serves as a crucial element for traffic control and collision avoidance services. However, inherent security vulnerabilities in AIS could lead to privacy invasions and potentially facilitate intentional collision attacks. The article [27] suggests the application of encryption methods like Identity-Based Public Cryptography and Symmetric Cryptography to enhance AIS's security properties.

Data authenticated aggregation is a significant concern in the context of Wireless Sensor Networks (WSNs), including those found in marine environments. Marine sensors are typically deployed in remote locations, making secure data aggregation a key issue attracting the attention of researchers and engineers. Wei *et al.* [28] provide a valuable contribution to this field with their proposition of Provably Secure Data Authenticated Aggregation Protocols (PSDAAP) utilizing identity-based multi-signature in marine WSNs. Their protocols leverage multi-signatures, a method enabling data authentication of various signers through a single signature, fitting for data authenticated aggregation in marine WSNs. Notably, they provide two efficient identity-based multi-signature schemes that prove secure data authenticated aggregation protocols under the cubic residue assumption, an aspect critical for the secure transmission of data.

Simultaneously, in marine wireless sensor networks, marine sensors collect multidimensional data - ranging from temperature, salinity, and dissolved oxygen to chlorophyll concentration - for further statistical analysis. To process this massive influx of data, computations are often outsourced to more capable systems like satellites, vessels, or even cloud services. Given that the outsourcing entities might not be fully trustworthy, the Verifiable Computation (VC) technique, which allows computationally weak parties to verify returned results from outsourced data computations, becomes crucial in the marine WSNs. Addressing this concern, the article [29] proposes a secure publicly verifiable computation protocol supporting both public delegation and public verifiability properties. This protocol securely handles outsourced functions and outsourced datasets together, significantly enhancing the reliability of the computational results from marine WSNs.

Additionally, there is a need for secure data forwarding protocols in multi-hop marine sensor networks. Marine sensors collect a variety of data, and these data often need to be relayed to final destinations such as satellites or vessels through multiple hops. Traditional use of homomorphic encryption, which allows arithmetic operations performed over encrypted data to yield equivalent results as if conducted over original plaintext, does not serve this multi-hop requirement well. Addressing this issue, Wei *et al.* [30] propose a secure data forwarding protocol leveraging the Paillier homomorphic encryption and multiuse proxy re-encryption. This protocol allows data to remain encrypted throughout multi-hop transmission until it reaches its final destination, thus ensuring data confidentiality during transmission.

The maritime industry, while known for its importance in global trade and transportation, also has unique security concerns, particularly when it comes to data integrity and access control. Addressing these concerns, the paper [31] delves into systems of identification, authentication, and encoding within the maritime industry. Their research focuses on the usage of authentication systems for electronic data, primarily employed to confirm the authenticity of the author's signature and the integrity of transmitted documents. They examine the use of digital signatures, which provide additional authenticating information transferred alongside the signed text. Besides, they explore disk data encryption systems, applied when limiting user access to information media is not feasible. These encryption systems render data inaccessible to users without the appropriate key, thereby securing the data at the file or disk level. By evaluating these systems' strengths and weaknesses, the authors shed light on their reliability against external and internal attacks, an important factor in the maritime industry's cybersecurity efforts.

On a different yet equally significant note, the spatial layout of the marine industry has been facing challenges due to the continuous expansion of the marine economy. These challenges include space intensification, low space utilization, unreasonable industrial structure, poor management system, inadequate scientific research and innovation capabilities, subpar ecological environment, imbalanced load, and high resource consumption. Responding to these issues, Wang *et al.* [32] propose an optimization method for the spatial layout of the marine industry, leveraging cloud computing. This approach involves collecting Hilbert values of all data and arranging nodes in construction time order to improve the Hilbert R-tree structure. Furthermore, they introduce clustering to prevent data overlap and establish an access control model for the marine industry spatial layout platform using the spatial correlation coefficient. The proposed method not only drastically reduces the time consumed in handling ocean remote sensing images under the ocean information cloud platform but also showcases impressive performance in the encryption and decryption test process of the pairing method. This confirms its feasibility and effectiveness in optimizing the marine industry's spatial layout, providing a sound theoretical foundation for future improvements.

VI. Discussion

The issue of ensuring resilience in ocean energy power plants is a multifaceted and complex one, with cybersecurity assuming an increasingly pivotal role. The previous sections have presented comprehensive research that underscores the convergence of secure data handling, information transmission, and advanced technological solutions in safeguarding and augmenting the integrity of ocean energy systems.

The concept of Smart Ocean is an approach based on the IoT that aims to manage marine ecosystems. This concept provides a framework for discussing the integration of advanced technologies in oceanic environments. This scenario presents various challenges, particularly in guaranteeing the secure and dependable transmission of data within these expansive ecosystems. The technical components that are fundamental to the IoT, including machine-to-machine communication and relay protocols, are of significant importance in the domain of ocean energy power plants. These elements may serve as the fundamental infrastructure for data transmission, which is crucial for monitoring and managing these facilities. The inclusion of data integrity, confidentiality, and accessibility principles from the initial stages of system development has the potential to significantly bolster system resilience.

The potential advantages of utilizing blockchain technology in the management of marine data have been extensively discussed, particularly for ocean energy power plants. The implementation of a secure and transparent system has the potential to facilitate data logging, transmission, and sharing among multiple entities involved in the operation and maintenance of a plant. Furthermore, it is imperative to conduct further exploration of sophisticated techniques, such as quantum encryption, to ensure the security of data transmission within these systems. In addition, the utilization of machine learning and artificial intelligence methodologies scrutinizing and projecting system behaviors, as referenced in the "Smart Ocean" segment, is expected to play a crucial role in achieving genuinely robust oceanic energy facilities. Given appropriate precautions, these technologies have the potential to facilitate instantaneous monitoring, anticipatory maintenance, and adaptable reactions to fluctuating ecological circumstances, thereby enhancing system efficiency while reducing potential hazards.

Security in data transmission is of utmost importance, especially considering the automatic identification systems used for traffic control and collision avoidance. Any breach could potentially lead to catastrophic incidents, underlining the need for robust encryption methods to protect sensitive data. Techniques such as Identity-Based Public Cryptography and Symmetric Cryptography, as suggested by [27], could be particularly relevant in this regard. Furthermore, the importance of secure data aggregation protocols cannot be overstated, considering the vast amounts of data collected by marine sensors and processed in ocean energy systems. Proposals such as Provably Secure Data Authenticated Aggregation Protocols (PSDAAP) utilizing identity-based multi-signature, as put forward by [28], provide promising avenues for ensuring data integrity in such scenarios.

The discourse of optimization techniques for spatial arrangement within the marine sector may have implications for the effective configuration and management of oceanic energy production facilities. The use of cloud computing for managing large-scale spatial data, as proposed by [32], could contribute to optimizing plant layout, improving maintenance routines, and potentially enhancing overall system performance.

VII. Conclusion

The present review underscores the pivotal significance of cybersecurity in the realm of ocean energy power plants. The utilization of cutting-edge technologies, such as the Internet of Things, blockchain, artificial intelligence, and cloud computing, is crucial in improving the security and efficiency of marine data management and transfer. The text highlights the noteworthy potential of blockchain technology as a reliable medium for sharing data and emphasizes the role of artificial intelligence in integrating networks that involve sensing, communication, and computing. Furthermore, the emergence of resilient data encryption techniques and the utilization of cloud computing for spatial arrangement optimization highlight the ongoing progressions in the field.

The aforementioned technological advancements exhibit potential, however, the review highlights the necessity for continuous research and development in cybersecurity measures to mitigate the possible cyber threats that may arise from these innovations. The marine industry's resilience strategies are contingent upon proactive measures to anticipate and mitigate cyber threats as the industry progresses.

To address the increasingly intricate nature of marine environments, it is recommended that future perspectives focus on the development of more comprehensive and integrated cybersecurity systems. Moreover, a deeper investigation into the possibilities of promising technologies such as quantum computing and their implementation in the field of cybersecurity may yield revolutionary resolutions within the field of ocean energy. A comprehensive analysis of policy frameworks and standards is imperative to direct the implementation of these technologies in a way that guarantees resilient, comprehensive, and fair cybersecurity in the ocean energy domain.

Acknowledgment

This work was promoted by Maynooth University and the Federal University of Minas Gerais. Thalita Nazaré, MEng, was supported by John and Pat Hume Doctoral Award – WISH. Lucas Nardo, MEng, was supported in part by FAPEMIG and by the Coordination for the Improvement of Higher Education Personnel – Brazil (CAPES) – Finance Code 001. Erivelton Nepomuceno, PhD, was supported under the Grant number SFI/21/FFp-P/10065.

References

[1] L. Lizuma, Z. Avotniece, S. Rupainis, and A. Teilans. Assessment of the present and future offshore wind power potential: A case study in a target territory of the Baltic sea near the Latvian coast. *The Scientific World Journal*, 2013:1–10, 2013.

[2] K. Khan, S. Miah, I. Ali, S. Sharma, and A. Quader. Studies on wave and tidal power converters for power production. *International Journal Of Advance Research And Innovative Ideas In Education*, 4:94–105, 11 2018.

[3] S. Amjad. Harnessing ocean energy from coastal and offshore Pakistan. *The 1st International Conference on Energy, Power and Environment*, 12(1):78, 1 2022.

[4] G. Todeschini, D. Coles, M. Lewis, I. Popov, A. Angeloudis, I. Fairley, F. Johnson, A. Williams, P. Robins, and I. Masters. Medium-term variability of the UK's combined tidal energy resource for a net-zero carbon grid. *Energy*, 238:121990, 1 2022.

[5] Y. Zhou, D. Ning, W. Shi, L. Johanning, and D. Liang. Hydrodynamic investigation on an OWC wave energy converter integrated into an offshore wind turbine monopile. *Coastal Engineering*, 162:103731, 12 2020.

[6] A. Bahaj. Generating electricity from the oceans. *Renewable and Sustainable Energy Reviews*, 15(7): 3399–3416, 9 2011.

[7] S. Murphy. Modernizing the U.S. electric grid: A proposal to update transmission infrastructure for the future of electricity. *Environmental Progress & Sustainable Energy*, 41(2), 3 2022.

[8] I. Semertzis, V. Rajkumar, A. Stefanov, F. Fransen, and P. Palensky. Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs. *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pages 1–6, 5 2022.

[9] X. Zhang, H. Ma, and C. Tse. Assessing the robustness of cyber-physical power systems by considering wide-area protection functions. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 12(1):107–114, 3 2022.

[10] B. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University, 07 2007.

[11] M. Dai, Y. Li, P. Li, Y. Wu, L. Qian, B. Lin, and Z. Su. A survey on integrated sensing, communication, and computing networks for smart oceans. *Journal of Sensor and Actuator Networks*, 11(4):70, 10 2022.

[12] F. Peralta, M. Watson, R. Bays, J. Boles, and F. Powers. Cybersecurity resiliency of marine renewable energy systems - Part 2: Cybersecurity best practices and risk management. *Marine Technology Society Journal*, 55(2):104–116, 3 2021.

[13] F. Peralta, A. Gorton, M. Watson, R. Bays, J. Castleberry, J. Boles, and F. Powers. Framework for identifying cybersecurity vulnerability and determining risk for marine renewable energy systems. Technical Report PNNL-29802, Pacific Northwest National Laboratory, 2020.

[14] F. Peralta, A. Gorton, M. Watson, R. Bays, J. Boles, B. Gordon, J. Castleberry, and F. Powers. Cybersecurity resiliency of marine renewable energy systems - Part 1: Identifying cybersecurity vulnerabilities and determining risk. *Marine Technology Society Journal*, 54(6):97–107, 11 2020.

[15] University of Bergen. Creating a smarter ocean. https://www.uib.no/en/smartocean/136758/creating-smarter-ocean, 3 2020. Accessed: June 2023.

[16] L. Bai, R. Han, J. Liu, J. Choi, and W. Zhang. Random access and detection performance of Internet of Things for smart ocean. *IEEE Internet of Things Journal*, 7(10):9858–9869, 10 2020.

[17] B. Lin, L. Zhao, H. Suraweera, T. Luan, D. Niyato, and D. Hoang. Guest editorial special issue on internet of things for smart ocean. *IEEE Internet of Things Journal*, 7(10):9675–9677, 10 2020.

[18] J. Shen, X. Jiang, Y. Cho, D. Liu, and T. Zhou. Two-factor-based public data protection scheme in smart ocean management. *Sensors*, 19(1):129, 1 2019.

[19] Y. Tian, Y. Wang, W. Tian, H. Du, X. Li, and D. Zhu. *SOBC: A smart ocean oriented blockchain system for cross-organizational data sharing*, volume 1454 Communications in Computer and Information Science. Springer Singapore, 2021.

[20] K. Bakker. Smart oceans: Artificial intelligence and marine protected area governance. *Earth System Governance*, 13:100141, 8 2022.

[21] G. Han, Y. Chen, H. Wang, Y. He, and J. Peng. AUV-Aided data importance based scheme for protecting location privacy in smart ocean. *IEEE Transactions on Vehicular Technology*, 71(9):9925–9936, 9 2022.

[22] Y. Yu, L. Guo, S. Liu, J. Zheng, and H. Wang. Privacy protection scheme based on CP-ABE in crowdsourcing-IoT for smart ocean. *IEEE Internet of Things Journal*, 7(10):10061–10071, 10 2020.

[23] C. Hu, Y. Pu, F. Yang, R. Zhao, A. Alrawais, and T. Xiang. Secure and efficient data collection and storage of IoT in smart ocean. *IEEE Internet of Things Journal*, 7(10):9980–9994, 10 2020.

[24] D. Huang, D. Zhao, L. Wei, Z. Wang, and Y. Du. Modeling and analysis in marine big data: Advances and challenges. *Mathematical Problems in Engineering*, 2015:1–13, 2015.

[25] Z. Yang, W. Xie, L. Huang, and Z. Wei. Marine data security based on blockchain technology. *IOP Conference Series: Materials Science and Engineering*, 322(5):052028, 3 2018.

[26] P. McGillivary. Why maritime cybersecurity is an ocean policy priority and how it can be addressed.

Marine Technology Society Journal, 52(5):44–57, 9 2018.

[27] A. Goudossis and S. Katsikas. Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, 24(2):410–423, 6 2019.

[28] L. Wei, L. Zhang, D. Huang, K. Zhang, L. Dai, and G. Wu. PSDAAP: Provably secure data authenticated aggregation protocols using identity-based multi-signature in marine WSNs. *Sensors*, 17(9): 2117, 9 2017.

[29] K. Zhang, L. Wei, X. Li, and H. Qian. Provably secure dual-mode publicly verifiable computation protocol in marine wireless sensor networks. *International Conference on Wireless Algorithms, Systems, and Applications*, Lecture Notes in Computer Science, 10251:210–219, 2017.

[30] L. Wei, K. Zhang, L. Zhang, and D. Huang. A secure data forwarding protocol for data statistic services in multi-hop marine sensor networks. *Fundamenta Informaticae*, 157(1-2):63–78, 1 2018.

[31] S. Chernyi, V. Marley, S. Lopyrev, A. Bulov, and A. Bordug. Systems of identification authentication and encoding in maritime industry. *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 125:37–39, 1 2018.

[32] F. Wang, X. Qi, J. Dong, and Y. Jiang. Optimization method of spatial layout of marine industry based on cloud computing. *Mathematical Problems in Engineering*, 2022:1–10, 10 2022.