IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 March 2024, accepted 9 April 2024, date of publication 11 April 2024, date of current version 19 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3387529

RESEARCH ARTICLE

An Edge Computing-Based Preventive Framework With Machine Learning-Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications

ABDULMOHSEN ALGARNI[1], **TAYFUN ACARER**[2], **AND ZULFIQAR AHMAD**[3]
[1]Department of Computer Science, King Khalid University, Abha 61421, Saudi Arabia
[2]Maritime Transportation and Management Vocational School of Higher Education, Piri Reis University, Tuzla, 34940 Istanbul, Turkey
[3]Department of Computer Science and Information Technology, Hazara University, Mansehra 21300, Pakistan

Corresponding author: Zulfiqar Ahmad (zulfiqarahmad@hu.edu.pk)

This research was financially supported by the Deanship of Scientific Research at King Khalid University under research grant number (R.G.P.2/93/45).

ABSTRACT The safety of maritime environments in context with effective and secure wireless communication networks is required for ships, coastal stations, and maritime authorities. The dynamic nature of marine environments, where ships traverse vast and unpredictable expanses of oceans and seas, presents big challenges to safety and risk management. Wireless communication technology is widely employed in maritime activities for communication via ocean networks and underwater wireless sensor networks (UWSNs). Maintaining the safety of the maritime environment, effective anomaly detection, prompt risk mitigation, and real-time communication becomes more difficult due to its dynamic nature. International trade and transportation are facilitated by the maritime industry. In addition to protecting lives and averting environmental disasters, maritime safety is important for maintaining the effectiveness and dependability of shipping routes. To handle the intricacies of maritime safety, this work proposes a novel preventive framework for anomaly detection and risk management in Maritime Wireless Communications (MWC). The proposed framework is based on edge computing and machine learning models. The framework makes use of edge computing technology to process data locally, lowering latency and enabling real-time communication in maritime environments. A proactive safety approach has been adopted to ensure the well-being of seafarers, safeguard vessels, and protect the marine environment. As maritime cybersecurity threats continue to evolve, the proposed research aims to enhance the cybersecurity posture of MWC. The framework will incorporate measures to detect and respond to potential cyber threats, ensuring the integrity and security of communication channels under international maritime cybersecurity standards. The proposed anomaly detection framework incorporates machine learning models such as Long Short-Term Memory (LSTM) and Isolation Forests (IF). The proposed framework also places a strong emphasis on preventative safety measures, including cybersecurity safeguards to protect communication channels in the constantly changing digital marine operations environment. To demonstrate the effectiveness of the proposed framework, the experiments were performed based on a publicly available dataset and implemented in the context of marine communications. The results show significant accuracy as well as high precision, recall, and F1-score metrics generated by the LSTM and IF models. The results highlight that the proposed framework can detect anomalies and potential threats in real-time marine communications.

The associate editor coordinating the review of this manuscript and approving it for publication was Tao Wang.

INDEX TERMS Machine learning, intelligent systems, sustainable navigation, autonomous vessels, ship safety management systems, maritime shipping, satellite technology, sensing and communication in maritime, automatic identification system, edge computing, prevention of ship accidents.

I. INTRODUCTION

Over time, both the volume and value of the cargo carried have increased. For this reason, the damages caused by accidents in maritime transportation are also increasing. It is not possible to define the cost of loss of life in monetary terms during these accidents [1], [2], [3]. The dynamic and ever-evolving field of maritime safety deals with the particular difficulties presented by the enormous and frequently inaccessible regions of the world's oceans and seas [4]. Wireless communication networks are important components for ships, coastal stations, and maritime authorities to communicate effectively and securely [5]. In this case, ensuring maritime safety entails harnessing technology improvements, putting in place efficient processes, and addressing particular wireless communication issues. Reliable and instantaneous information exchange between ships and land-based stations is made possible by maritime wireless communication (MWC) [1]. It is worth consideration in emergency response, coordination, and navigation. To avoid mishaps and guarantee the general safety of maritime operations, communication systems, such as satellite communication and Very High Frequency/Ultra High Frequency (VHF/UHF) radio are required to be reliable [6]. The Automatic Identification System (AIS) greatly enhances maritime safety by giving vessels real-time information on the positions, courses, and speeds of other adjacent ships [7], [8], [9], [10]. This helps with navigation and collision avoidance, enabling ships to modify their paths to avoid mishaps and guarantee safe travel. MWC has been used in emergencies for search and rescue operations. Distress signals guarantee a prompt reaction from maritime authorities and other vessels. They are typically sent by Digital Selective Calling (DSC) on VHF radios [11], [12]. Navigators can plan routes that avoid bad weather conditions since wireless connectivity makes it easier to receive weather reports on time. With the ability to provide precise and current meteorological information, this capability is required for minimizing weather-related mishaps and maximizing maritime safety [13], [14]. Maintaining communication system cybersecurity has significant importance because maritime communication is growing more digital and depends on wireless technologies. The integrity and safety of marine activities are preserved by preventing illegal access, manipulation, and disruptions to communication channels through the use of cybersecurity preventions [10], [15], [16], [17]. Integrating Internet of Things (IoT) devices and sensor networks with MWC improves safety by facilitating the real-time data gathering and transfer of environmental factors, equipment status, and vessel conditions. Preventive and proactive risk management are also important factors to enhance maritime safety [3], [6], [18]. The International Maritime Organization (IMO) have declared the "*urgent need to raise awareness on cyber-risk threats and vulnerabilities, to support safe and secure shipping, which is operationally resilient to cyber-risks encouraging administrations to ensure that cyber-risks are appropriately addressed in safety management systems*" [19], [20]. New developments in wireless communication technology offer better connectivity, lower latency, and more capacity. One such development is the implementation of 5G networks in maritime environments. Because they enable increasingly complex applications like remote monitoring, augmented reality navigation, intelligent systems and autonomous vessel operations [21], [22].

By moving computation and data storage closer to the point of data generation, edge computing has the ability to significantly improve MWC [15], [23]. This lowers latency, enhances real-time processing, and facilitates effective communication in maritime situations. By processing data at or close to the network's edge, edge computing reduces the time it takes to send information to a centralized cloud server and get a response. In marine environments, lower latency is required to maintain communication system efficiency through quick decision-making. The common features of MWC include real-time data sharing such as the interchange of navigational data, weather reports, and vessel positions [12]. With the help of edge computing, such type of data can be processed locally, facilitating speedy analysis and decision-making without being exclusively dependent on distant cloud servers. Edge computing allows information to be filtered and aggregated locally at the edge before being sent to the central cloud as given in Figure 1. Marine wireless communication systems are required to be benefited from the redundancy and robustness provided by the edge computing. Edge nodes can function independently even in the event of a disruption in the connection to the central cloud, guaranteeing the dependability of essential communication tasks. IoT devices and sensors are frequently deployed in maritime environments to gather data. By offering a distributed computing architecture, edge computing has the ability to enhance the environment of marine communication and makes it more extensive and decentralized [24], [25], [26], [27].

In MWC, machine learning models can be implemented for risk management and anomaly detection [28], [29], [30]. Isolation Forests (IF) [1], One-Class Support Vector Machine (SVM) [31], Autoencoders [32], and LSTM [33] are some of the examples of machine learning methods that can be used for anomaly detection and risk management in MWC. Isolation forests perform better for finding abnormalities and outliers in data and it can be used to detect unusual network behaviors or anomalous communication patterns. One-Class Support Vector Machine is specifically designed for datasets with few abnormalities, and it can be used to create a model of typical communication patterns. Autoencoders can learn a

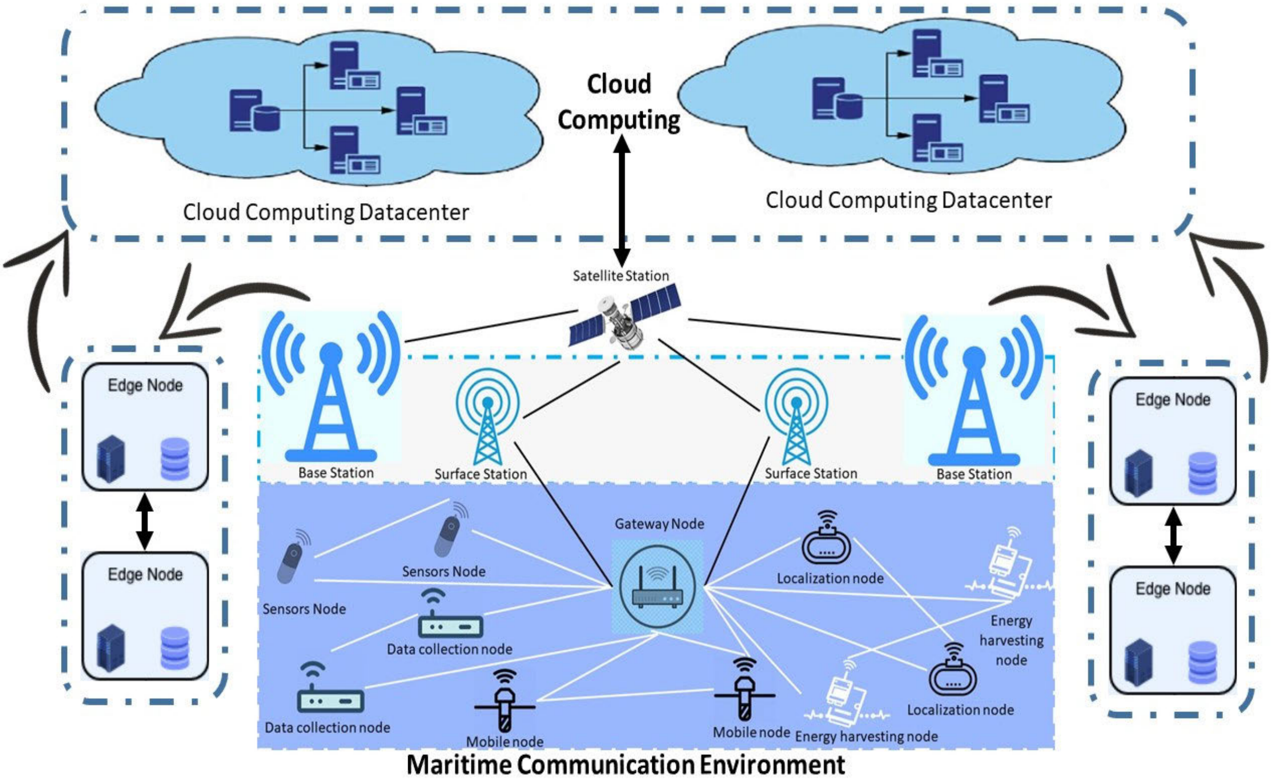

FIGURE 1. Edge computing-based data processing in maritime communication environment.

condensed representation of communication patterns. They perform better for encapsulating intricate connections in communication data. LSTMs can be used in marine wireless communications to evaluate transmission sequences over time and spot patterns or variations that point to abnormalities or possible threats [34], [35].

A. RESEARCH MOTIVATION

Safety and risk management in maritime environments are always challenging due to its changing situations as ships are traveling over huge, unpredictably sized stretches of oceans and seas. For communication over ocean networks and underwater wireless sensor networks (UWSN), wireless communication technology is extensively used in maritime activities [23], [29]. However, it is challenging to maintain the safety, efficient anomaly detection, timely risk mitigation, and real-time communication in maritime environments. The maritime industry supports international trade and transportation. Maritime safety plays a significant role in preserving the efficiency and dependability of shipping routes, saving lives, and preventing environmental disasters [3], [6]. Due to the potential for wireless communication anomalies and hazards to endanger public safety, it is imperative to develop a preventive framework. With the increasing digitization of maritime communication, new cybersecurity challenges arise. Cyberattacks have the potential to compromise the integrity of communications and endanger maritime safety [30], [36], [37], [38], [39]. A preventive framework combining edge computing and machine learning methods would be the better is solution for real-time cybersecurity risk detection and mitigation. The application of edge computing completely transforms marine safety. Relocating computation closer to the data source allows edge computing to speed up reaction times, reduce latency, and enable real-time analytics [27]. Machine learning algorithms have demonstrated efficacy in interpreting complex datasets and identifying patterns that indicate anomalies. Applying machine learning to the maritime sector provide a proactive approach to safety through risk prediction and prevention. Bandwidth limitations are common in wireless communications for marine applications [21], [26], [40]. The proposed preventive system maximizes bandwidth consumption with local data processing and filtering at the edge. This is driven by the need to minimize data transfer to central servers to maintain bandwidth and ensure efficient communication, particularly in distant marine areas. The proposed preventive framework is in line with the increasing focus on utilizing cutting-edge technologies to both fulfill and surpass safety requirements of international marine organizations.

B. MAIN CONTRIBUTIONS

Main contributions of this paper are briefed as follows:

- Development of a novel edge computing-based preventive framework for MWC.

- Integration of machine learning methods to the proposed preventive framework for providing a robust and efficient solution for anomaly detection and risk management in maritime environments.
- Implementation of a proactive safety approach, ensuring the well-being of seafarers, safeguarding vessels, and protecting the marine environment.
- Implementation of customized machine learning methods to detect real-time anomalies in MWC.
- To acknowledge and adopt the unique challenges of the maritime environment including its dynamic conditions, limited connectivity, and the need for resilience.
- As maritime cybersecurity threats continue to evolve, the research aims to enhance the cybersecurity posture of MWC. The framework will incorporate measures to detect and respond to potential cyber threats, ensuring the integrity and security of communication channels in accordance with international maritime cybersecurity standards.

C. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows. Section II presents the related work in context with maritime safety, edge computing technology and implementation of machine learning models in situations similar with maritime environments. Section III presents the system design and model. Section IV provides 'an edge computing-based preventive framework for anomaly detection and risk management in MWC'. Section V presents the performance evaluation method. Section VI provides experiments, results and discussions. Section 7 concludes the article with future directions.

II. RELATED WORK

This section reviews the related work by categorizing it into the techniques used for maritime safety, edge computing technology and the machine learning approaches used for anomaly detection and risk management in maritime intelligent systems.

The ability of future Maritime Autonomous Surface Ships to recognize possible threats and respond appropriately are important for their safety. The study in [4] set out to determine the research paths for the most important safety indicators in the three operational safety-sensitive areas of Maritime Autonomous Surface Ships: communication, intact stability, and collision avoidance. The findings show that many academics agree that operational leading safety indicators are necessary, and occasionally they even offer recommendations for the indicators' specific composition [4]. Several prominent safety markers for self-navigating boats are easily recognized in scholarly works and applied in contemporary operations.

Spaceborne Synthetic Aperture Radar (SSAR) and Automatic Identification System (AIS) are being used in a variety of research projects for applications that support marine security and safety. However, it is necessary to open a separate parenthesis for AIS among these systems. Because AIS devices automatically detect other AIS devices within the coverage area and receive their navigation information such as position, speed, route, etc. It also sends information about itself to surrounding ships and Coast Radio Stations (CRS) [41]. In densely populated shipping areas, the data association becomes further challenging as ships seen using SSAR imaging may be mistakenly linked to AIS observations. This frequently leads to an inaccurate or erroneous impression of the marine environment. In order to categorize ship kinds in SSAR imagery, a classification-aided data association strategy is developed [42] that makes use of a transfer learning mechanism. In particular, AIS data is used to train a ship categorization model, which is subsequently applied to forecast SSAR ship detections. These predictions are then applied to the data association process, which creates a strong match between the data by using a rank-ordered assignment technique. Based on the types of SSAR products utilized for maritime surveillance, two case studies in the UK are used to assess the effectiveness of the classification-aided data association technique: targeted data association in the Solent and wide-area and large-scale data association in the English Channel [42]. The results demonstrate a high degree of correlation between the data that is resistant to heavy shipping or traffic, and the use of class (i.e., ship type) information increases the trust in the data linkage.

The creation of a virtual training tool for marine safety education is discussed in [43]. A diverse team made up of business developers, VR experts, computer scientists, and maritime specialists built this solution. The technology is a portable, reasonably priced maritime training system that may be utilized at home, in training facilities, or even on board. When an officer has time for training, using VR-training programs to improve situation awareness in navigation is a simple and effective approach to practice. This can be accomplished in an enjoyable and efficient manner, providing quantifiable training progress indices. The necessity of VR training for the shipping sector, its obstacles, and the proof-of-concept using MarSEVR (Maritime Safety Education with VR) technology are all highlighted in [43]. This primary goal of the study is to demonstrate a technology prototype that can be used to provide immersive training scenarios for experts and learners.

In [44], the authors examine possible solutions to the problems related to the implementation of edge computing for autonomous vehicles. The ultimate challenge of designing an edge computing ecosystem for autonomous vehicles is to provide sufficient computing capacity, redundancy, and security to ensure the safety of autonomous vehicles including maritime intelligent systems. In particular, autonomous driving systems are highly sophisticated, tightly integrating a wide range of technologies, such as sensing, localization, perception, and decision-making, in addition to seamless cloud platform interactions for the creation of high-definition (HD) maps and data storage [44]. Autonomous driving edge computing systems must process massive amounts of data in real time, with extremely diverse incoming input from many sensors. Edge computing systems with autonomous driving capabilities frequently have very stringent energy consumption limitations since they are mobile. Therefore, it is essential to provide adequate processing power while maintaining a reasonable energy consumption to ensure the safety of autonomous vehicles—even when they are traveling at high speeds. Second, vehicle-to-everything (V2X) relieves severe performance and energy constraints on the edge side and offers redundancy for autonomous driving workloads besides the edge system design [44].

By offering a unified platform for networking, processing, and storage resources, edge computing makes it possible to analyze data quickly and effectively close to its source [45]. As a result, the industrial Internet of things now uses it as its foundational platform (IIoT). But the special qualities of computing have also brought up new security issues. In [45], an edge computing-based blockchain-based identity management and access control method is devised to address the issue. To achieve network entity registration and authentication, self-certified cryptography is used. The authors created a blockchain-based identity and certificate management system and connect the implicit certificate that is generated to its identity. Second, a Bloom filter-based access control system is created and linked with identity management.

The majority of container transportation from the Republic of Korea, Republic of China, Japan and Singapore to other nations or continents, both by land and sea, takes more than a week. Cargoes in reefer containers need to be maintained at the proper temperatures in such an environment. These containers must be inspected daily to prevent cargo spoiling throughout the lengthy navigation period. However, because they are dispersed throughout the distinct cargo holding area of a ship, it can be challenging to frequently check and maintain them with the limited crew on board. A reefer container monitoring system that can gather data from the device sensors and makes use of the current onboard power line(s) is suggested as a solution to such a scenario in [46]. One benefit of this system is that it doesn't require more wiring, which means shipping companies may put it on their ships at a minimal expense.

Ship groundings frequently result in damages, such as oil spills, flooding, and eventual capsizing of the ship. Risks can be assessed objectively by analyzing statistics on maritime traffic or qualitatively by consulting experts. In [34], the authors propose a big data analytics approach to assess grounding risk in actual environmental settings. The technique uses nowcast data, bottom depth data from the General Bathymetric Chart of the Oceans (GEBCO), and massive data streams from the Automatic Identification System (AIS). In shallow water, the evasive maneuvers of passenger ships functioning in the role of Ro-Pax are modeled in a variety of traffic patterns that correspond to side- or forward-grounding scenarios. As a result, to detect possible grounding scenarios, an Avoidance Behavior-based Grounding Detection Model (ABGD-M) is presented, and the grounding probability risk is measured at observation stations along ship routes in different voyages. The technique is used aboard a Ro-Pax ship that sails the Gulf of Finland during a 2.5-year ice-free season. The findings show that depending on the operational conditions, observation stations, and trip routes, grounding probabilistic risk estimation can take many different forms.

In [16], a deep reinforcement learning (DRL) system for autonomous ship collision avoidance in continuous action spaces is presented. With the help of dynamic ship data, the obstacle zone by target (OZT) algorithm calculates the potential collision region. Agents of DRL use a virtual sensor known as the grid sensor to identify the approach of many ships. Agents used the Imazu problem, a series of hypothetical ship contact scenarios, to learn collision avoidance movements. In [16], the authors provided a novel DRL-based collision avoidance strategy with a greater safe passing distance. The authors created a brand-new technique called inside OZT, which extends OZT and boosts learning consistency. Using the long short-term memory (LSTM) cell, the authors redesigned the network and trained in continuous action spaces to create a model that has a longer safe distance than the one investigated previously.

The growing globalization of navigation and the dehumanization of ships have led to a mismatch between the growing need for oversight of ship behavior and the scarce resources of traffic services. This has resulted in a high frequency of maritime accidents [1]. An essential component of marine transportation is the observation of unusual ship behavior. The automatic identification system (AIS) is widely utilized in the management of ship static information and the real-time transmission of dynamic information due to the growing popularity of the system and increased marine research. The authors identified abnormal ship behavior from the perspective of spatial information and thematic information based on moving ship trajectory data, taking into account the state of abnormal ship behavior research at the time. For this reason, the cognition of aberrant ship behavior was first modeled in [1]. The authors identified and explained the anomalous behavior indicated by ship thematic data using the isolation forest algorithm. The experimental findings demonstrate the effectiveness of the methodology this research proposes for identifying anomalous ship behavior.

Reliable vessel trajectory forecasting is necessary for managing and controlling maritime traffic. Precise vessel trajectory prediction not only helps prevent collisions but also shortens sailing distances, improves navigation efficiency, and helps design navigation routes. In the maritime industry, vessel trajectory prediction using automated identification system (AIS) data has so garnered significant attention [7]. Because original AIS data may contain noise, its use in actual maritime traffic management is limited. This paper [7] suggests a vascular trajectory prediction technique that combines a deep learning prediction model with data denoising in order to solve this issue. Three phases are involved in this process to achieve data denoising: trajectory separation, data denoising, and standardization. The moving average approach is used to further clean up the data once outliers from the initial

AIS data samples are eliminated. Eventually, the denoised data are standardized into uniformly distributed time-series data. Next, the use of bidirectional long short-term memory (Bi-LSTM) is used to forecast vessel trajectory.

III. SYSTEM DESIGN AND MODEL

In this research work, we propose an edge computing-based preventive framework for anomaly detection and risk management in MWC through machine learning methods to enhance maritime safety as shown by Figure 2. The framework unifies cutting-edge technologies i.e., edge computing and machine learning to tackle the ever-changing problems brought up by the maritime environments. By integrating edge computing, data processing has been localized, which lowers latency and makes real-time analysis at the information source possible. This is especially used for making quick decisions during emergencies or avoiding collisions. By filtering and aggregating data locally, the framework maximizes bandwidth use and provides an affordable solution for maritime areas where bandwidth is scarce.

The system gains anomaly detection capabilities from the integration of customized machine learning models i.e., LSTM and Isolation Forests. By guaranteeing the prompt detection of anomalous patterns and possible hazards, this proactive safety framework enhances maritime safety. The framework makes cybersecurity a top priority by processing sensitive data locally via edge computing, which reduces the possibility of tampering or unwanted access during data transfer. The main components of the proposed framework are given as follows:

A. MARITIME ENVIRONMENT

The maritime environment presents intricate challenges in the field of maritime safety including poor connectivity, unpredictable weather, and the requirement for robust communication systems [47]. Let S represents the maritime environment characterized by vastness and unpredictability oceans and seas then challenges in maritime safety (MS) attributed by expansive nature of S is given in equation 1.

$$MS = Complexity\,(S) \times Unpredictability\,(S) \tag{1}$$

Communication infrastructure (CI) required to cover maximum distance efficiently within S to ensure reliable and immediate information sharing and it is represented by equation 2.

$$CI = Efficient_{Trave}\,(S) \times PC + UW + RCS \tag{2}$$

where, PC represents poor connectivity, UW represents unpredictable weather and RCS represents robust communication system.

The foundation of maritime communication is provided by conventional techniques like satellite communication and Very High Frequency/Ultra High Frequency (VHF/UHF) radio [47]. Maritime communication (MC) is based on the shipping and satellite communication (SC) and VHF/UHF and is given by equation 3.

$$MC = SC + VHF/UHF \tag{3}$$

The framework acknowledges that innovation is necessary to address enduring problems like cybersecurity, bandwidth optimization, and dependability. The proposed framework uses edge computing to recognize the need to process data closer to its source. It will achieve low-latency necessary for navigation, emergency response, and collision avoidance. The proposed framework with incorporation of edge computing to address the cybersecurity, bandwidth optimization and dependability is represented by Eq. 4.

$$PFW = EC \times Innovation\,(S) + CS + BO + D \tag{4}$$

where, PFW represents the proposed framework, Innovation (S) is innovation in maritime environment, CS is cybersecurity, BO is bandwidth optimization and D is dependability. The framework presents a proactive safety paradigm through machine learning methods that enables the real-time detection and remediation of anomalies and possible hazards in marine wireless communications.

B. MARITIME WIRELESS COMMUNICATIONS (MWC)

Oceans and seas are large and challenging environments in which MWC are utilized to enable safe, effective, and coordinated activities. These communication systems are essential to ships, coastal stations, and marine authorities because they enable sensitive operations like emergency response, navigation, coordination, and information exchange. A variety of technologies and protocols are available in the MWC space, with the goal of addressing the unique challenges posed by the constantly shifting maritime environment. Mathematically the challenging environment of maritime is employed by the equation 5.

$$S : MWC \rightarrow \{Safe, Effective, Coorindated\ Activities\} \tag{5}$$

where, S represents the unpredictable and vast oceans and seas and MWC represents maritime wireless communication. One of the fundamental components of wireless communication in the maritime environment is satellite communication. Satellites in orbit around the Earth give global coverage, allowing ships to communicate anywhere they are, even over very long distances. This technology is necessary for weather reporting, maritime safety, coordination, and reliable long-range communication. Because UHF and VHF radio communication technologies are so effective at communicating over short to medium distances, they are widely used in maritime settings [6]. In particular, VHF radio is a widely used tool for ship-to-ship and ship-to-shore communication. Applications such as navigation, distress signals, and maritime coordination make extensive use of it. The AIS aims to enhance situational awareness and prevent collisions. Real-time data transmission, including position, and speed, is facilitated by AIS transponder-equipped ships. Ships are used to be interact with one another and reduce the likelihood of collisions through such type of data exchange.

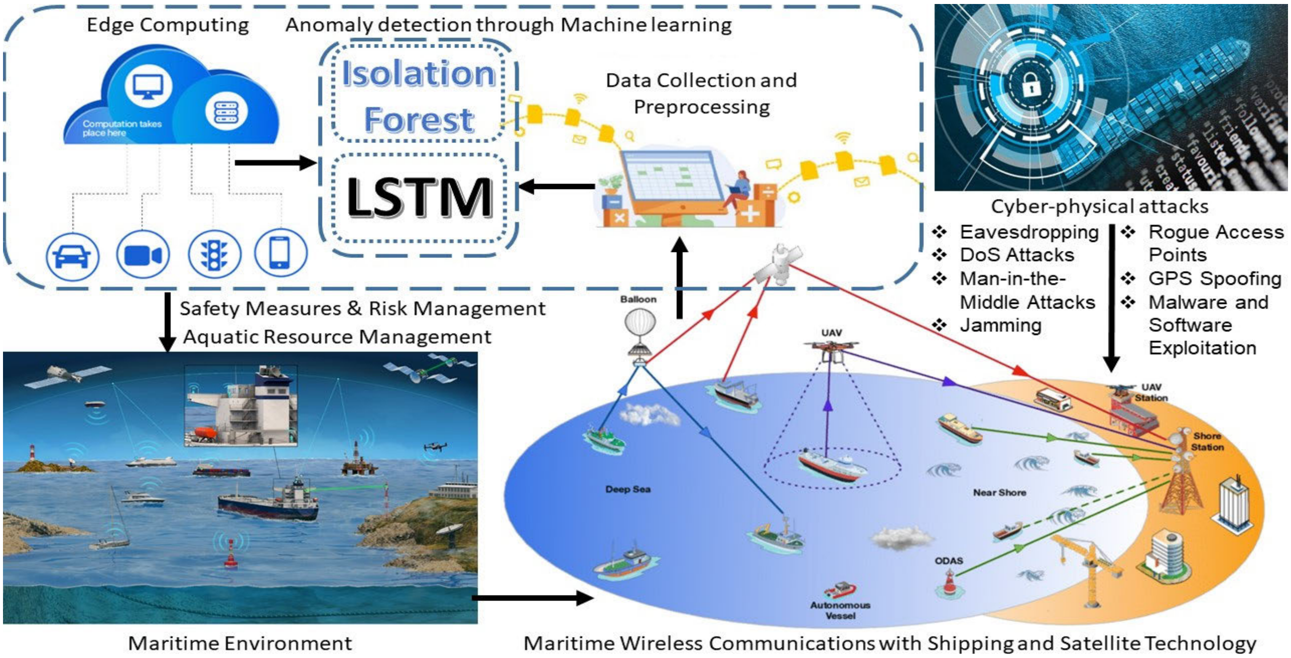
Edge Computing
Anomaly detection through Machine learning
Computation takes place here
Isolation Forest
LSTM
Data Collection and Preprocessing
Cyber-physical attacks
Eavesdropping
DoS Attacks
Man-in-the-Middle Attacks
Jamming
Rogue Access Points
GPS Spoofing
Malware and Software Exploitation
Safety Measures & Risk Management
Aquatic Resource Management
Balloon
UAV
UAV Station
Shore Station
Deep Sea
Near Shore
ODAS
Autonomous Vessel
Maritime Environment
Maritime Wireless Communications with Shipping and Satellite Technology

FIGURE 2. An optimized edge computing-based preventive framework with machine learning-integration for anomaly detection and risk management in maritime wireless communications.

In maritime environments, the usage of Wireless Sensor Networks (WSNs) for data collection and real-time monitoring is increasing exponentially. These networks consist of sensors placed on boats, buoys, or even the ocean floor to collect data. Wireless transmission of such data facilitates timely decision-making. MWC required to remain connected even in inclement weather due to bandwidth limitations, possible cyberattacks, and other issues. The integration of edge computing and machine learning to address such issues is represented by equation 6.

$$MWC : EC + ML \rightarrow CS + BO + RAD \tag{6}$$

where, EC represents edge computing, ML represents machine learning, CS represent cybersecurity, BO represent bandwidth optimization and RAD represents real-time anomaly detection. Innovations like the integration of edge computing and machine learning are meant to help solve these problems by improving cybersecurity, optimizing bandwidth, and facilitating real-time anomaly detection. In MWC, edge computing improves real-time processing by processing data closer to its source, lowering latency. Edge computing can play a key role in supporting time-sensitive applications in MWC, such as navigation and emergency response.

C. CYBER-PHYSICAL ATTACKS

MWC are used for the functioning of various systems within the maritime industry, including navigation, control, monitoring, and communication. As per Maritime Cyber Attack Database (MCAD), Figure 3 shows the numbers and regions of known cyber-attacks in Maritime [48]. Cyber-physical attacks on MWC have serious consequences, potentially leading to navigation errors, communication breakdowns, and compromised safety. Following are the major types of cyber-physical attacks that are used to target MWC:

- GPS Spoofing: GPS spoofing involves sending false signals to a Global Positioning System (GPS) receiver, making it believe it is located at a different location. Ships relying on GPS for navigation are misdirected, leading to collisions, grounding, or navigation into restricted areas. Implementation of signal authentication and deploying secure GNSS receivers with anti-spoofing capabilities mitigate the risk of GPS spoofing.
- Jamming: Jamming attacks involve the intentional interference with radio frequency signals, disrupting normal communication. Maritime communication systems, including distress signals and navigation communication, are rendered ineffective, affecting safety and operational efficiency. Employing frequency-hopping techniques, utilizing spread spectrum modulation, and deploying anti-jamming antennas ensure reliability in martime communication systems.
- Eavesdropping: The unlawful interception of wireless communications in order to get private data. There can be security hazards if confidential information, like cargo data or navigation plans, is compromised. Implementation of end-to-end encryption protocols, use of secure communication channels, and protection of cargo data and navigation plans from unauthorized access are the major preventive measures against eavesdropping.
- Man-in-the-Middle (MitM) Attacks: In order to intercept and maybe modify a message, attackers place

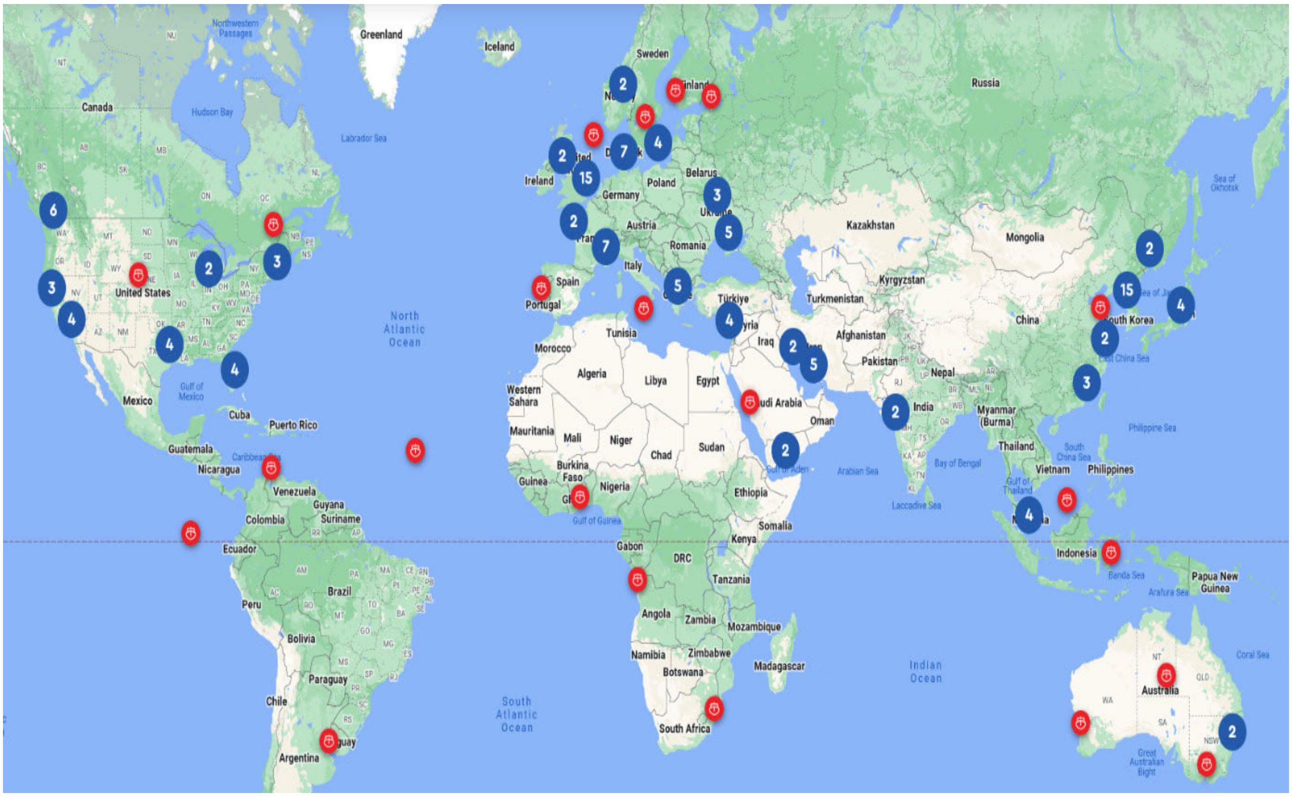

FIGURE 3. The numbers and regions of known cyber-attacks in Maritime [48].

themselves in the middle of the communication channel. Attackers tamper with communications sent between a ship and a shore station, spreading false information or gaining unapproved authority. Strong cryptographic protocols, like Transport Layer Security (TLS) and mutual authentication between the ship and the shore station, protect the integrity of communication and stop people from getting to send data without permission.

- Rogue Access Points: Unauthorized wireless access points installed with the intention of gaining access to communication networks. Attackers breach the communication network to take over important systems or pilfer private data. Implementation of a wireless intrusion detection system to monitor for unauthorized access points, as well as regular network scans to detect and remove rogue devices, can prevent unauthorized access or data theft.
- Malware and Software Exploitation: Introduction of harmful software or taking advantage of holes in communication software are examples of malware and software exploitation. The integrity of communication systems can be compromised by malware, which might result in illegal access or interfere with regular operations. Regularly updating software and firmware to patch vulnerabilities and implementing robust antimalware safeguards the integrity of communication systems and prevents unauthorized access or disruption of operations.
- Denial of Service (DoS) Attacks: Overloading networks or systems to prevent them from functioning normally. Limiting the availability of vital communication services, which has an impact on safety, control, and navigation systems. Implementation of network traffic monitoring and filtering mechanisms to detect and mitigate abnormal traffic patterns ensures the reliability of vital communication services for safety, control, and navigation systems.
- Firmware Manipulation: Tampering with the firmware of communication devices or systems. Manipulating firmware leads to unauthorized control over communication systems, allowing attackers to interfere with maritime operations. Using secure boot mechanisms to verify the firmware integrity during startup and only allowing authorized sources to update the firmware prevents unauthorized users from taking control of communication systems and ensures the safety of maritime operations.

D. PROBLEM FORMULATION

The dynamic and expansive features of maritime environments, characterized by large and frequently unreachable oceans and seas, present distinct problems for the maritime safety area. Wireless communication networks are the core components of coastal stations, and maritime authorities to communicate securely and effectively. MWC system is used for emergency response, coordination, and navigation; however, several issues including bandwidth optimization, cybersecurity, and dependability still exist. Marine organizations rely on communication methods, such as satellite communication and VHF/UHF radio, there is an increased requirement for reliable and fast information sharing. By giving real-time information on vessel positions, courses, and speeds, technologies like the AIS improve safety by making navigation and collision avoidance easier. In order to prevent accidents and guarantee the general safety of maritime activities, the dynamic maritime environment necessitates constant innovation in communication systems. Mathematically, maritime communication system at time t is represented by Equation 7.

$$C\left(t\right)=\begin{bmatrix} B\left(t\right) \\ CS\left(t\right) \\ R\left(t\right) \end{bmatrix} \tag{7}$$

where, C represents maritime communication system, B represents bandwidth optimization, CS represents cybersecurity and R represents risk management. Maritime communication system in context with risk management at time t is represented by Equation 8

$$R\left(t\right)=\begin{bmatrix} ER\left(t\right) \\ CO\left(t\right) \\ N\left(t\right) \end{bmatrix} \tag{8}$$

where, ER represents emergency response, CO represents coordination and N represents Navigation of marine communication network at time t. Let MWC (t) be the matrix representing maritime wireless communication methods at time t then mathematically it is represented by Equation 9. Each row represents the communication method at time t and each column represents the risk management aspects including reliability, anomaly detection and bandwidth optimization, in maritime communication networks.

$$MWC(t)=\begin{bmatrix} MWC_{1,1}(t) & MWC_{1,2}(t) & \cdots & MWC_{1,n}(t) \\ MWC_{2,1}(t) & MWC_{2,2}(t) & \cdots & MWC_{2,n}(t) \\ : & : & \cdots & \vdots \\ : & \vdots & \cdots & \vdots \\ MWC_{n,1}(t) & MWC_{n,2}(t) & \cdots & MWC_{n,n}(t) \end{bmatrix} \tag{9}$$

The objective function of safety in maritime activities is represented by $S\left(t\right)$ and it is a function "f" of sum of C(t), R(t) and MWC (t) as given in Equation 10.

$$S\left(t\right)=f\left(\sum_{i=1}^{n}\left\{C\left(t_i\right)\times R\left(t_i\right)\times MWC\left(t_i\right)\right\}\right) \tag{10}$$

The components C(t), R(t), and MWC(t) are the independent factors collectively contributing to the overall safety function for maritime environments. The function 'f' represents the overall performance in terms of weight obtained by adding the products of all the three components for 'n' number of maritime environments. The multiplicative effect represents that all the factors are equally important, and deficiencies in any one factor significantly impact the overall safety performance.

Cybersecurity challenges are raised by the growing digitization of maritime communication, which calls for precautions against unauthorized access, channel manipulation, and disruption. Real-time data collection on environmental variables, equipment status, and vessel conditions is made easier by the integration of IoT devices and sensor networks with marine wireless communication. Enhancing maritime safety requires both proactive and preventive risk management, especially considering recent advancements in wireless communication technologies, such as the possible deployment of 5G networks in maritime contexts. These developments enable the adoption of sophisticated applications like remote monitoring and autonomous vessel operations by providing better connectivity, reduced latency, and expanded capacity.

The proposed research aims to create a novel preventive framework based on edge computing to address the above-mentioned issues. The goal of this framework is to apply machine learning techniques to risk management and anomaly detection in MWC. Edge computing improves real-time processing, reduces latency, and maximizes bandwidth use by relocating computation closer to the data source. Machine learning models i.e., LSTM and IF are used for real-time anomaly identification and risk management.

IV. AN EDGE COMPUTING-BASED PREVENTIVE FRAMEWORK WITH MACHINE LEARNING-INTEGRATION FOR ANOMALY DETECTION AND RISK MANAGEMENT IN MARITIME WIRELESS COMMUNICATIONS

This study proposes a novel approach to improve the safety MWC by using the edge computing in combination with machine learning models for anomaly detection and risk management. Edge computing processes and analyses MWC data in close proximity to its source, which includes communication nodes or sensors accountable for data transmission and collection. The integration of edge computing into MWC for the purpose of anomaly detection and risk management presents a multitude of benefits. These include the ability to conduct analyses in real time, reduced latency, and effective allocation of resources. This is accomplished by means of the implementation of interconnected smart devices. Edge computing enables the prompt assessment of risk management and, consequently, expedites the detection of anomalies. It also prevents the transmission of sensitive data across networks and guarantees its localization, thus mitigating the potential for data breaches and safeguarding user privacy. The data analysis process is further optimized by the edge devices performing preprocessing operations directly. Machine learning models are hosted on high-performance edge devices, providing immediate feedback regarding anomaly detection and risk management. IF and LSTM machine learning models have been customized in context with maritime environments and are used to find abnormalities and possible hazards in the data. This makes it possible to proactively mitigate or stop adverse situations.

Algorithm 1 shows the process of the proposed framework in which an edge computing technology has been integrated with machine learning methods for anomaly detection and risk management to enhance maritime safety. The algorithm presents a novel preventive approach for risk management and anomaly. It implements machine learning techniques integrated with edge computing technology. The initial parameters are the number of edge computing nodes, the duration of the data processing window, and the total number of features in the dataset. The system collected data from sources of marine wireless communication. The edge computing nodes process the data locally and make it ready for anomolies detection. The machine learning models are integrated for risk management and anomaly detection. The processed data is used to train LSTM and IF models, which give the system the capacity to identify abnormalities and evaluate the risks associated with them. Each edge computing node uses the learned IF and LSTM models to analyze its processed data in real-time anomaly detection, alerting users or initiating preventive measures when abnormalities are detected. Risk evaluations are carried out according to the degree of irregularities found. The processed data, anomaly alarms, and risk evaluations are the outcomes that are shared with central monitoring stations or other appropriate authorities.

V. EXPERIMENTS, RESULTS & DISCUSSIONS

We perform the simulations and evaluate the performance of proposed framework in context with the safety of MWC.

A. EVALUATION METRICS

We use the evaluation metrics of Accuracy, Precision, Recall and F1 score for evaluating the performance of the proposed framework [49]. These values are calculated based on the following terms [38].

- True Positives (TP): The number of tuples that are really found to be intrusive at the end of the process. In the proposed framework, TP has been used for correctly identification of risky situation in anomaly detection and risk management.
- True Negatives (TN): The number of valid tuples that are found at the end of the detecting process. In the proposed framework, TN has been used for correctly identification of the situation as not being risk in anomaly detection and risk management.
- False Positives (FP): The number of safe tuples that, at the conclusion of the detection process, are identified as intrusions. In the proposed framework, FP has been used for identification of unnecessary alerts or action, potentially causing disruptions in anomaly detection and risk management.
- False Negatives (FN): The quantity of dangerous tuples that, at the conclusion of the detection process, are found normally. In the proposed framework, FN has been used for identification of situation where a system fails to detect an actual risk in anomaly detection and risk management.

Accuracy is a frequently employed metric for evaluating the performance of classification models, especially in binary classification tasks. By calculating the percentage of accurately predicted instances among all the instances in the dataset, it evaluates the overall accuracy of the model's predictions [38]. Mathematically, it is calculated with the help of Equation 11.

$$A = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

Precision is a metric used to assess the efficacy of a classification model. It measures the percentage of true positive predictions among all positive predictions, or true positives plus false positives, in order to assess the model's accuracy in making positive predictions [38]. Mathematically, it is represented by Equation 12.

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

Recall is a metric used to assess a classification model's performance. It is sometimes referred to as Sensitivity or True Positive Rate. The model's recall quantifies its capacity to accurately identify each and every positive case in the dataset [38]. Mathematically, it is given by Equation 13.

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

The *F1 score* is a way to measure how well classification models work, especially when they are asked to choose between two options. When there is an imbalance between precision and recall, the F1 score becomes helpful [38]. Mathematically, it is calculated with the help of Equation 14.

$$F1Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{14}$$

B. DATASET

In order to evaluate the proposed framework, a publically available dataset on a Kaggle website with title, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks" [50] has been used. The dataset replicates many Denial-of-Service (DoS) attacks on WSN using the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. It includes Blackhole, Grayhole, Flooding, and Scheduling attacks, which are four different categories of attacks. In the Blackhole attack, at the beginning of a round, an attacker assumes the identity of a Cluster Head (CH). When nodes connect to this fake CH, they unintentionally submit their data packets to it, which are then transmitted to the Base Station (BS). As with the Blackhole attack, attackers assume the identity of CHs in the Grayhole assault. These attackers do this on the basis of the sensitivity of the data included in the

Algorithm 1 An Edge Computing-Based Preventive Framework with Machine Learning-Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications

```
Input:      MWC:      Maritime Wireless Communications
Output:     AR-MWC:   Anomaly detection and Risk management in MWC
Procedure:  Anomaly Detection & Risk Management (MWC)
1.      Parameter Initialization
    i.   N: Number of edge computing nodes
    ii.  T: Time stamp for data processing
    iii. K: Number of features in the dataset
2.      Data Collection
    i.   MWSN: Data collection from maritime WSN
    ii.  $Di$ : Store the collected data in a local buffer
3.      Edge Computing Processing
    i.   for each computing node $i$
         $Pi$ = Local_Processing ($Di$)
4.      Machine Learning Model Integration
    i.   Train and deploy machine learning methods
    ii.  $M_{IF} = TrainIsolationForest(P_1, P_2, \ldots, P_N)$
    iii. $M_{LSTM} = TrainLSTM(P_1, P_2, \ldots, P_N)$
5.      Real-time anomaly detection
    i.   For each edge computing node $i$
             $A_{IF(i)} = ApplyIsolationForest(P_i, M_{IF})$
             $A_{LSTM(i)} = ApplyLSTM(P_i, M_{LSTTM})$
    ii.  If anomalies detected on node $i$
             $Maritime\_Safety_i = Trigger(PreventiveActions, Alert, SafetyMeasures)$
6.      Risk Management
    i.   Assess the severity of detected anomalies and determine risk management
             $R_{IF(i)} = AssessRisk(R_{IF(i)})$
             $R_{LSTM(i)} = AssessRisk(R_{LSTM(i)})$
7.      Result Generation
    i.   Assess the severity of detected anomalies and determine risk management
             $AR - MWC = Detected\ anomalies\ and\ subsequent\ risk\ management$
8.      Return $AR - MWC$
```

packets they drop or delete. The goal of the flooding attack is to flood the network with too many high-transmission-power advertising CH messages. The scheduling attack takes place in the setup stage of the LEACH protocol. Assuming the role of CHs, attackers provide every node the same time slot for data transmission, which causes packet collisions and eventual data loss.

The proposed study focuses on wireless communications in maritime environments, and while there are similarities between maritime and conventional wireless communications, we understand the necessity of addressing potential differences in attack vectors and environmental factors. We have carefully aligned the attacks considered in the proposed study dataset with those commonly encountered in maritime scenarios. Despite the existence of frequency range variations between maritime and conventional wireless communications, we clarify that the proposed framework remains independent of these considerations.

C. EXPERIMENTAL DESIGN

The evaluation of the models integrated within the proposed framework was conducted using "WSN-DS," a dataset specifically designed for intrusion detection systems in wireless sensor networks. There are two parts to the dataset: the training set and the test set. Eighty percent of all the records in the dataset were in the training set. While the test set was 20% of all the records. The "cross_val_score" function from scikit-learn was used to perform cross-validation on LSTM. For IF, on the other hand, we used a train-test split with an 80:20 ratio to make sure the model was correct, since

TABLE 1. Classification report of results generated by LSTM.

	Precession	Recall	F1-Score	Accuracy
Normal	0.99	1.00	0.99	0.99
Anomaly	0.95	0.91	0.93	
Macro Average	0.97	0.95	0.96	
Weighted Average	0.99	0.99	0.99	

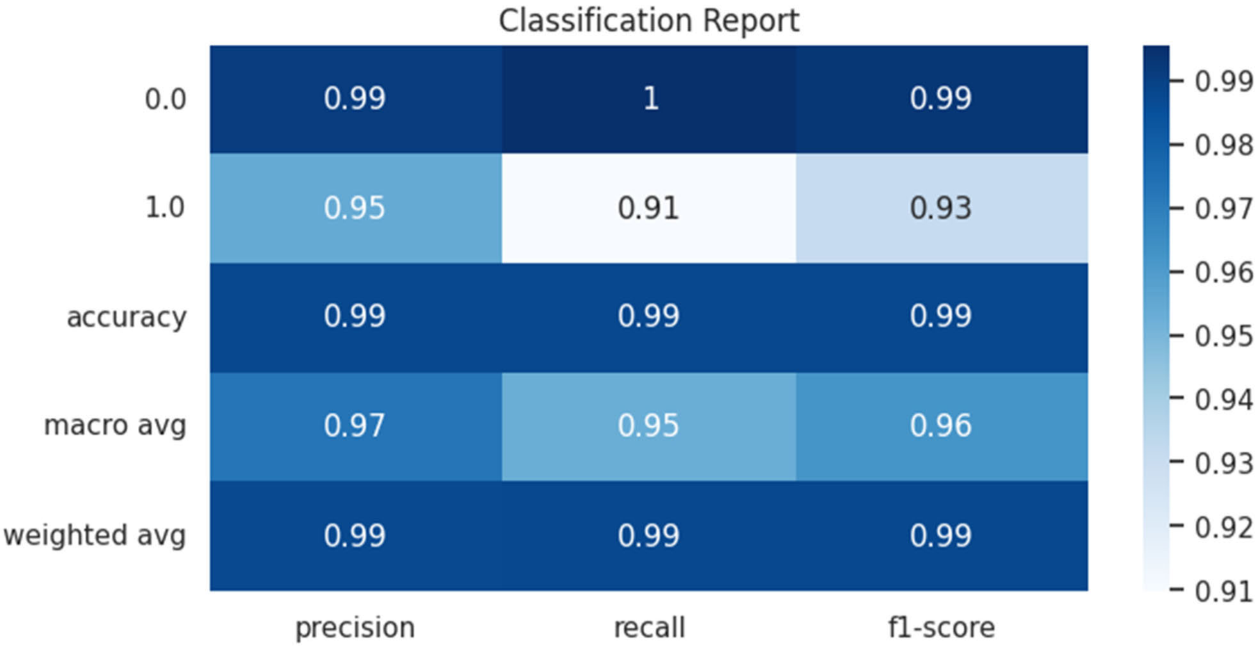

FIGURE 4. Classification report of LSTM.

cross-validation does not work for unsupervised learning. All of the tests are performed in Python on a GPU-based system with a CPU speed of 1.8 GHz and 16 GB of RAM. The pre-configured machine learning packages and libraries have been used: Numpy, Seaborn, LabelEncoder, OneHoTencoding, Pandas, and Matplotlib.

D. RESULTS AND EVALUATION

The experiments were performed by implementing two machine learning methods i.e., LSTM and IF. The evaluation results for each model is given below:

1) LSTM

The LSTM model is used to detect the anomalies with Python libraries and modules including Pandas and Sklearn. Table 1 shows the results in the form of classification report generated by LSTM on a given dataset which is further visualized in Figure 4. The results show that the framework performs well in differentiating between "Normal" and "Anomaly" cases. A variety of attacks that affect WSNs are simulated by the dataset. These attacks include flooding, scheduling, blackhole, grayhole, and flooding, all of which have distinct challenges for detection. The LSTM model achieves more than 0.90 as values of recall, precision, and F1-score for both classes. The model performed well in recognizing cases classified as "Normal," obtaining nearly flawless precision, recall, and F1-score. With an accuracy of 0.95, recall of 0.91, and an F1-score of 0.93, the model demonstrated a great performance even though it was marginally less accurate in classifying "Anomaly" occurrences.

The 99% overall accuracy with support of 74931 number of actual instances highlights how well the framework works to find intrusions in the simulated WSN environment. With excellent results in terms of precision, recall, and F1-score metrics, the weighted averages and macros further confirm the models' resilience. These findings imply that the proposed framework is a good fit for the job of anomaly detection in WSNs of marine environment. It demonstrates its dependability in recognizing typical network activity and its ability to distinguish anomalies even when complex attack techniques like flooding, scheduling, blackhole, and grayhole attacks are present. The efficacy of the framework in guaranteeing the security and integrity of maritime wireless sensor networks is attributed to the amalgamation of LSTM model.

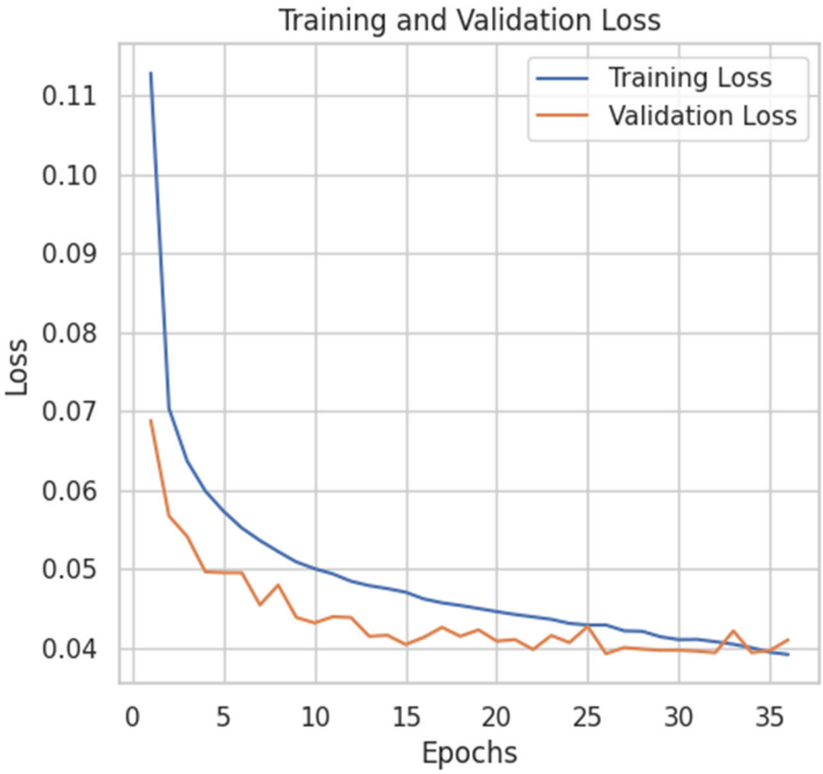

FIGURE 5. Training and validation loss.

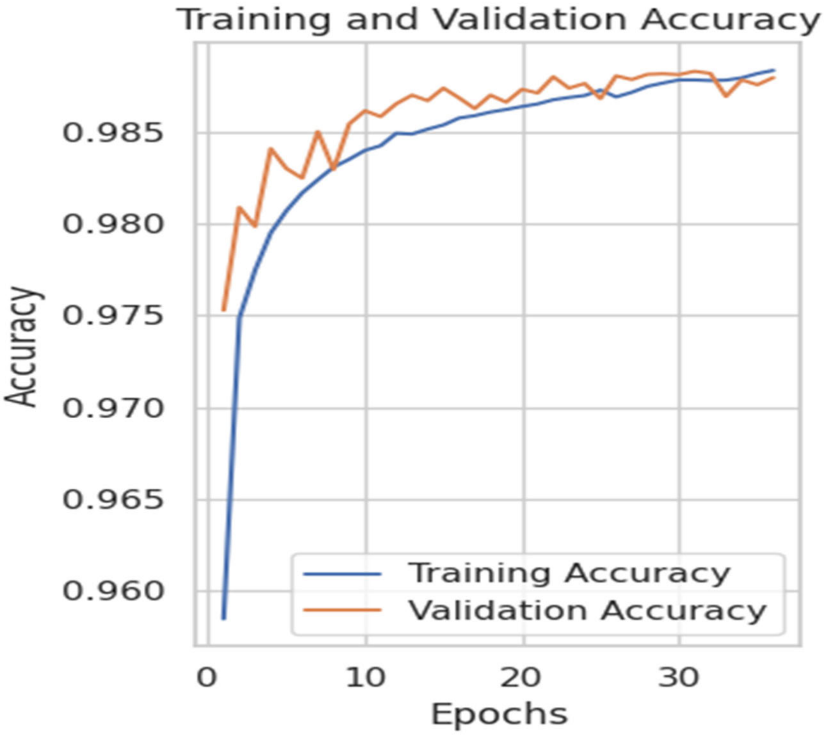

FIGURE 6. Training and validation accuracy.

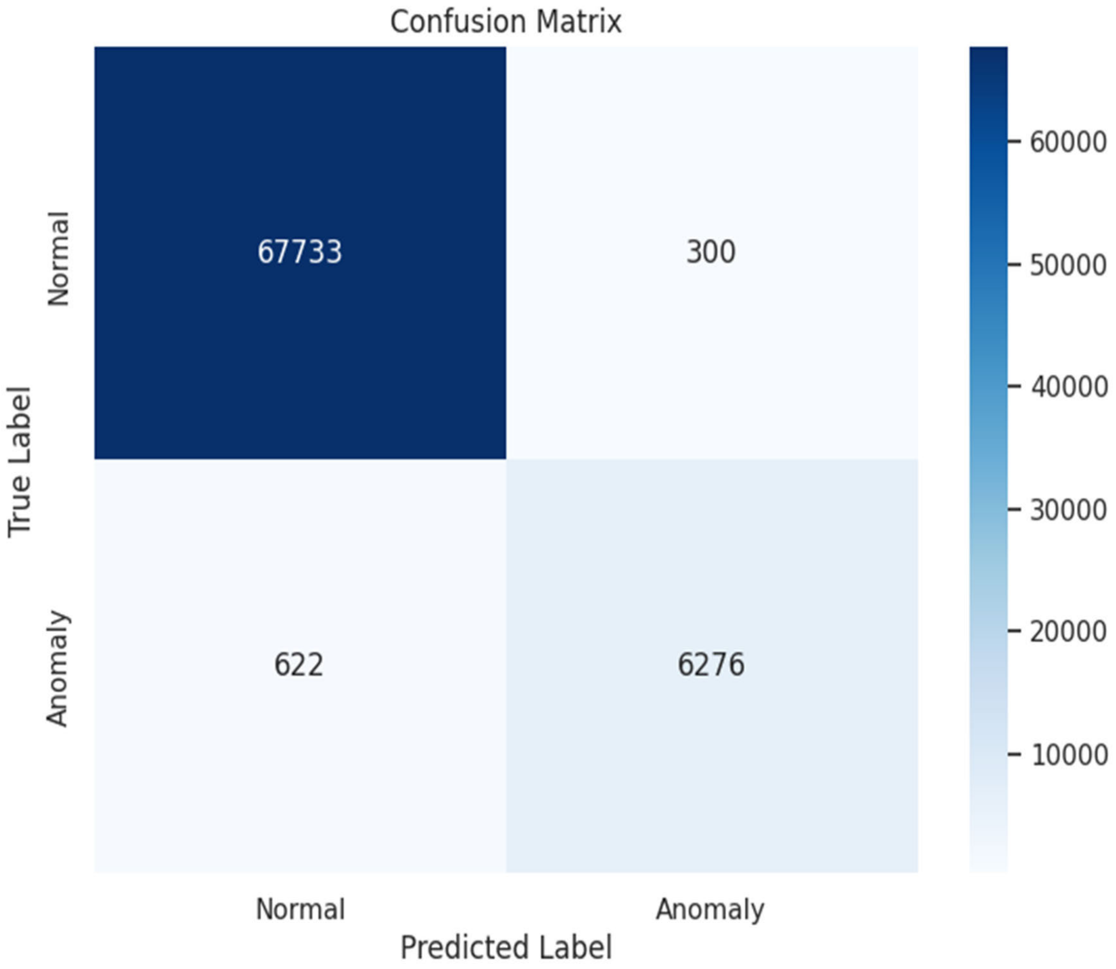

FIGURE 7. Confusion matrix generated by LSTM.

Figure 5 shows the comparison of training and validation loss. A satisfactory fit is indicated by a steady reduction and plateau in loss during both training and validation. Since, the validation loss closely tracks the training loss and does not rise, there is no indication of overfitting. An additional indication that the model is not overfitting is the convergence of the training and validation loss curves.

Figure 6 shows the comparison of training and validation accuracy. An encouraging sign is that the accuracy for both training and validation is high and exhibits a similar trend. The model performs well on the validation data in addition to matching the training data well, indicating strong generalization. At times, the validation accuracy even marginally outperforms the training accuracy. There is a regularization impact of dropout during training and the same is not present during the validation set evaluation.

Figure 7 shows the confusion matrix generated by LSTM. To identify the risky and normal situations correctly and incorrectly, we divide the predictions in four categories i.e., TP, TN, FP and FN. The model detected 67733 instances as TP, 6276 instances as TN, 300 instances as FP and 622 instances as FN. The high proportion of true positives shows that the model detects normal cases with 99% precision. The low percentage of normal instances being wrongly classified as anomalies indicates the small number of false positives (300). The model displays a greater quantity of false negatives (622), signifying situations where real anomalies are wrongly categorized as normal. Despite this, the overall performance is strong, as evidenced by the 99% accuracy.

2) ISOLATION FOREST (IF)

The IF model is used to detect the anomalies with Python libraries and modules including Pandas and Sklearn. Table 2 shows the results in the form of classification report generated by IF on a given dataset which is further visualized in Figure 8. The classification report shows that a dataset included by two classes, represented by the numbers "−1" and "1." The IF model shows an accuracy of 0.39 for the anomalous class ("−1"), meaning that only 39% of the cases identified as anomalies were actual anomalies. This class has a somewhat greater recall (0.72), meaning that 72% of

TABLE 2. Classification report of results generated by IF.

	Precession	Recall	F1-Score	Accuracy
Normal (1)	0.97	0.88	0.92	0.87
Anomaly (-1)	0.39	0.72	0.50	
Macro Average	0.68	0.80	0.71	
Weighted Average	0.91	0.87	0.89	

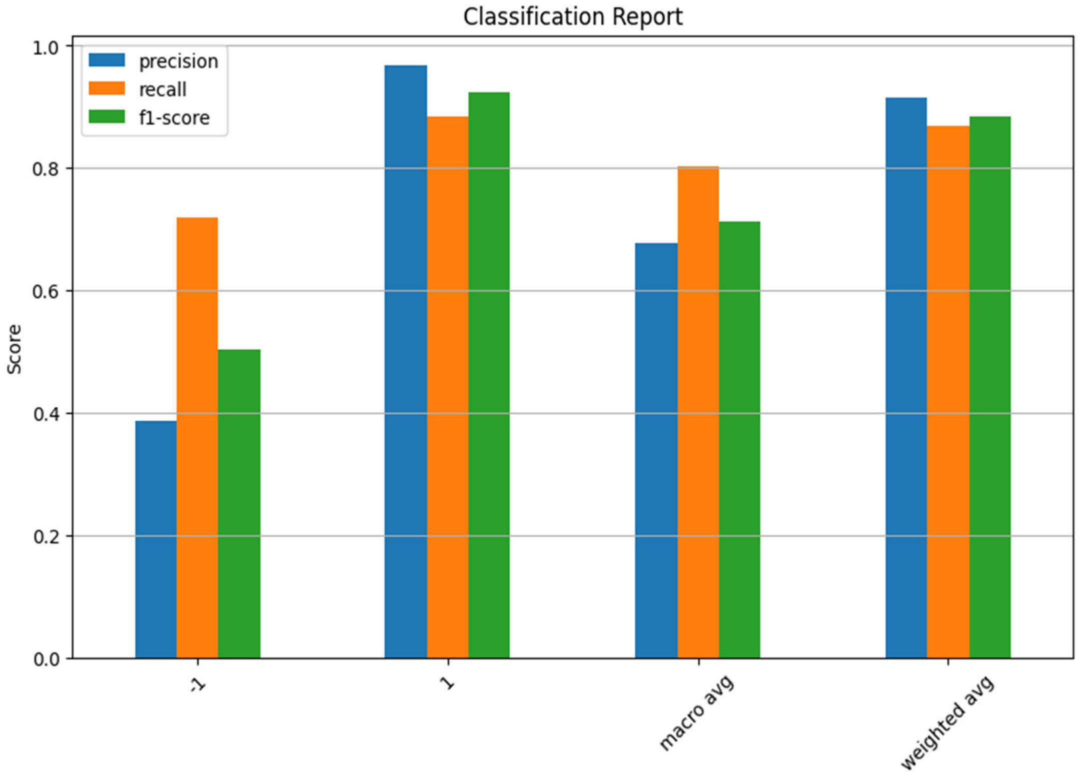

FIGURE 8. Classification report of IF.

real anomalies were correctly detected by the model. For the anomalous class, the F1-score is reported as 0.50, indicating a trade-off between memory and precision. The model exhibits a high precision of 0.97 for the normal class ("1"), meaning that 97% of the occurrences predicted as normal were in fact normal. With a recall of 0.88 for the normal class, 88% of real normal occurrences were correctly identified. The normal class F1-score is 0.92, indicating a performance that strikes a balance between recall and precision. The overall accuracy is stated to be 87%, and metrics that are weighted and macro-averaged offer more information about how well it performs. The related weighted averages are 0.91, 0.87, and 0.89, but the macro-averaged precision, recall, and F1-score are 0.68, 0.80, and 0.71, respectively. These findings imply that although the model does a great job of classifying typical cases, it has the ability do a better job of accurately identifying anomalies.

Figure 9 shows the confusion matrix generated by IF. The model accurately classified 24,906 cases as anomalies ("-1") and 30,505 instances as part of the normal class ("1"). False positive errors 9689 were made by it, identifying occurrences as normal while in fact they belonged to the anomaly class. False negative errors of 39,561 were found, showing cases where normal occurrences were wrongly classified as anomalies. The confusion matrix shows how well the model differentiates between normal and anomaly cases.

The utilization of edge computing instead of centralized servers for machine learning-based analysis itself presents various benefits, such as instantaneous analysis, reduced latency, maintenance of privacy, and effective resource management. Since edge computing allows processing and analysis of data directly at or near the source of data generation, it provides immediate assessment of anomalies, facilitating prompt decisions. The potential challenges in implementing the proposed framework in live maritime environments include cost overhead, hardware limitations, data management, and real-time analysis through high-performance computational resources. Edge devices typically have limited computational resources compared to centralized servers. Careful consideration of resource utilization is required to handle large-scale data or var-

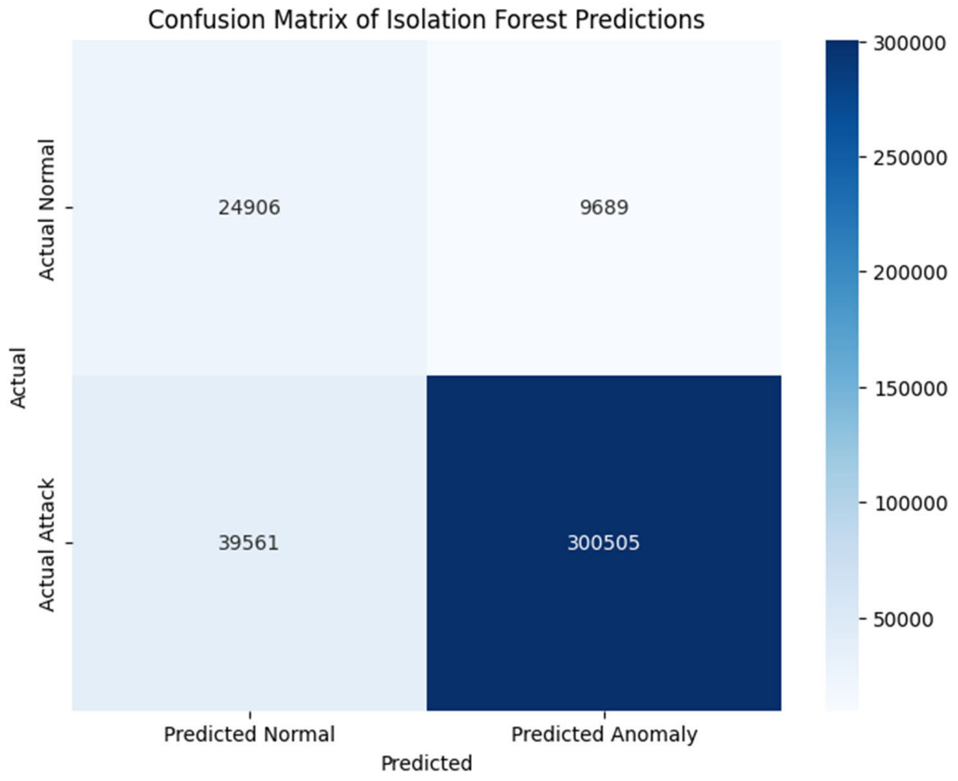

FIGURE 9. Confusion matrix generated by IF.

ied types of sensor inputs while maintaining adequate performance.

VI. CONCLUSION AND FUTURE WORK

This study proposes a preventive framework for risk management and anomaly detection in MWC. The framework uses edge computing and machine learning to handle the difficulties in safety presented by large and usually inaccessible maritime environments. Data processing is localized through the integration of edge computing, which lowers latency and permits real-time analysis at the information source. This is important when it comes to making quick judgments in an emergency or preventing mishaps. By filtering and aggregating data locally, the framework maximizes bandwidth use and offers a cost-effective solution for maritime locations with restricted bandwidth. The incorporation of machine learning models including LSTM and IF, gives the system the ability to detect anomalies. The framework places a high priority on cybersecurity by using edge computing to process sensitive data locally, which lowers the possibility of data transfer manipulation or unauthorized access. It recognizes established lines of communication such as satellite communication and VHF/UHF radio, guaranteeing consistent and timely information sharing in maritime operations. The usefulness of the proposed framework is demonstrated by the experimental findings, which are based on a publicly accessible dataset that simulates attacks on WSN in marine communications. The capacity of proposed framework is to identify anomalies and possible threats in real-time and is demonstrated by the high precision, recall, and F1-score metrics displayed by both the LSTM and IF models. Overall, the results reveal that the LSTM model, with an accuracy of 99%, outperformed the IF model.

In the future, we aim to explore algorithms with a hybrid nature to improve performance in risk assessment and anomaly identification with more advanced attack types. We also intend to implement fog computing-based fuzzy logic systems to optimize the performance of 5G communication technology in the context of maritime communications.

ACKNOWLEDGMENT

This research was financially supported by the Deanship of Scientific Research at King Khalid University under research grant number (R.G.P.2/93/45).

REFERENCES

[1] Y. Shi, C. Long, X. Yang, and M. Deng, "Abnormal ship behavior detection based on AIS data," *Appl. Sci.*, vol. 12, no. 9, p. 4635, May 2022, doi: 10.3390/app12094635.

[2] G. Kodak and T. Acarer, "Evaluation of the effect of maritime traffic regulations on the accident rate in the strait of Istanbul," *Aquatic Res.*, vol. 4, no. 2, pp. 181–207, 2021, doi: 10.3153/ar21015.

[3] O. Eulaerts and G. Joanny, "Weak signals in border management and surveillance technologies," EUR 31126 EN, Publications Office Eur. Union, Luxembourg, U.K., Tech. Rep. JRC128871, 2022, doi: 10.2760/784388.

[4] K. Wróbel, M. Gil, P. Krata, K. Olszewski, and J. Montewka, "On the use of leading safety indicators in maritime and their feasibility for maritime autonomous surface ships," *Proc. Inst. Mech. Eng., O, J. Risk Rel.*, vol. 237, no. 2, pp. 314–331, Apr. 2023, doi: 10.1177/1748006x211027689.

[5] N. Nomikos, P. K. Gkonis, P. S. Bithas, and P. Trakadas, "A survey on UAV-aided maritime communications: Deployment considerations, applications, and future challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 56–78, 2023, doi: 10.1109/OJCOMS.2022.3225590.

[6] T. Acarer, "VHF Kısa Mesafe Deniz Haberleşmesinin Data İletişimine Dönüşmesinin Deniz İşletmelerinin Gemi Yönetimleri İçin Temin Edeceği Olanaklar," *Denizcilik Araştırmalarý Dergisi, Amfora*, vol. 2, no. 3, pp. 15–31, 2023.

[7] C.-H. Yang, C.-H. Wu, J.-C. Shao, Y.-C. Wang, and C.-M. Hsieh, "AIS-based intelligent vessel trajectory prediction using bi-LSTM," *IEEE Access*, vol. 10, pp. 24302–24315, 2022, doi: 10.1109/ACCESS.2022.3154812.

[8] A. Siddiqa, I. A. T. Hashem, I. Yaqoob, M. Marjani, S. Shamshirband, A. Gani, and F. Nasaruddin, "A survey of big data management: Taxonomy and state-of-the-art," *J. Netw. Comput. Appl.*, vol. 71, pp. 151–166, Aug. 2016, doi: 10.1016/j.jnca.2016.04.008.

[9] Z. Ahmad, T. Acarer, and W. Kim, "Optimization of maritime communication workflow execution with a task-oriented scheduling framework in cloud computing," *J. Mar. Sci. Eng.*, vol. 11, no. 11, p. 2133, Nov. 2023, doi: 10.3390/jmse11112133.

[10] K. Tran, S. Keene, E. Fretheim, and M. Tsikerdekis, "Marine network protocols and security risks," *J. Cybersecurity Privacy*, vol. 1, no. 2, pp. 239–251, Apr. 2021, doi: 10.3390/jcp1020013.

[11] A. A. Periola, A. A. Alonge, and K. A. Ogudo, "Architecture and system design for marine cloud computing assets," *Comput. J.*, vol. 63, no. 1, pp. 927–941, Jan. 2020, doi: 10.1093/comjnl/bxz169.

[12] S. A. H. Mohsan, Y. Li, M. Sadiq, J. Liang, and M. A. Khan, "Recent advances, future trends, applications and challenges of Internet of Underwater Things (IoUT): A comprehensive review," *J. Mar. Sci. Eng.*, vol. 11, no. 1, p. 124, Jan. 2023, doi: 10.3390/jmse11010124.

[13] K. Sathish, R. C. Venkata, R. Anbazhagan, and G. Pau, "Review of localization and clustering in USV and AUV for underwater wireless sensor networks," *Telecom*, vol. 4, no. 1, pp. 43–64, Jan. 2023, doi: 10.3390/telecom4010004.

[14] K. Saeed, W. Khalil, A. S. Al-Shamayleh, S. Ahmed, A. Akhunzada, S. Z. Alharthi, and A. Gani, "A comprehensive analysis of security-based schemes in underwater wireless sensor networks," *Sustainability*, vol. 15, no. 9, p. 7198, Apr. 2023, doi: 10.3390/su15097198.

[15] S. Fattah, A. Gani, I. Ahmedy, M. Y. I. Idris, and I. A. T. Hashem, "A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges," *Sensors*, vol. 20, no. 18, p. 5393, Sep. 2020, doi: 10.3390/s20185393.

[16] R. Sawada, K. Sato, and T. Majima, "Automatic ship collision avoidance using deep reinforcement learning with LSTM in continuous action spaces," *J. Mar. Sci. Technol.*, vol. 26, no. 2, pp. 509–524, Jun. 2021, doi: 10.1007/s00773-020-00755-0.

[17] F. Al-Quayed, Z. Ahmad, and M. Humayun, "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of Industry 4.0," *IEEE Access*, vol. 12, pp. 34800–34819, 2024, doi: 10.1109/ACCESS.2024.3372187.

[18] L. Drazovich, L. Brew, and S. Wetzel, "Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2021, pp. 503–509, doi: 10.1109/CSR51186.2021.9527922.

[19] I. de la Peña Zarzuelo, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue," *Transp. Policy*, vol. 100, pp. 1–4, Jan. 2021, doi: 10.1016/j.tranpol.2020.10.001.

[20] M. S. Karim, "Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?" *Mar. Policy*, vol. 143, Sep. 2022, Art. no. 105138, doi: 10.1016/j.marpol.2022.105138.

[21] M. Abbasi, E. Mohammadi-Pasand, and M. R. Khosravi, "Intelligent workload allocation in IoT–fog–cloud architecture towards mobile edge computing," *Comput. Commun.*, vol. 169, pp. 71–80, Mar. 2021, doi: 10.1016/j.comcom.2021.01.022.

[22] I. A. Alablani and M. A. Arafah, "EE-UWSNs: A joint energy-efficient MAC and routing protocol for underwater sensor networks," *J. Mar. Sci. Eng.*, vol. 10, no. 4, p. 488, Apr. 2022, doi: 10.3390/jmse10040488.

[23] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, "Internet of Underwater Things and big marine data analytics—A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 904–956, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3053118.

[24] S. Muthuramalingam, A. Bharathi, S. R. Kumar, N. Gayathri, R. Sathiyaraj, and B. Balamurugan, "IoT based intelligent transportation system (IoT-ITS) for global perspective: A case study," in *Internet of Things and Big Data Analytics for Smart Generation* (Intelligent Systems Reference Library), vol. 154, V. Balas, V. Solanki, R. Kumar, and M. Khari, Eds. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-04203-5_13.

[25] Z. Lv and W. Xiu, "Interaction of edge-cloud computing based on SDN and NFV for next generation IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 5706–5712, Jul. 2020, doi: 10.1109/JIOT.2019.2942719.

[26] F. M. Talaat, "Effective prediction and resource allocation method (EPRAM) in fog computing environment for smart healthcare system," *Multimedia Tools Appl.*, vol. 81, no. 6, pp. 8235–8258, Mar. 2022, doi: 10.1007/s11042-022-12223-5.

[27] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-Computing-Enabled smart cities: A comprehensive survey," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10200–10232, Oct. 2020, doi: 10.1109/JIOT.2020.2987070.

[28] N. Peppes, E. Daskalakis, T. Alexakis, E. Adamopoulou, and K. Demestichas, "Performance of machine learning-based multi-model voting ensemble methods for network threat detection in agriculture 4.0," *Sensors*, vol. 21, no. 22, p. 7475, Nov. 2021, doi: 10.3390/s21227475.

[29] Q. Gang, A. Muhammad, Z. U. Khan, M. S. Khan, F. Ahmed, and J. Ahmad, "Machine learning-based prediction of node localization accuracy in IIoT-based MI-UWSNs and design of a TD coil for omnidirectional communication," *Sustainability*, vol. 14, no. 15, p. 9683, Aug. 2022, doi: 10.3390/su14159683.

[30] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 305–310, doi: 10.1109/CCWC.2019.8666450.

[31] V. Balasubramaniam, "Artificial intelligence algorithm with SVM classification using dermascopic images for melanoma diagnosis," *J. Artif. Intell. Capsul. Netw.*, vol. 3, no. 1, pp. 34–42, Mar. 2021, doi: 10.36548/jaicn.2021.1.003.

[32] Y. Song, S. Hyun, and Y.-G. Cheong, "Analysis of autoencoders for network intrusion detection," *Sensors*, vol. 21, no. 13, p. 4294, Jun. 2021, doi: 10.3390/s21134294.

[33] G. Rjoub, J. Bentahar, O. A. Wahab, and A. S. Bataineh, "Deep and reinforcement learning for automated task scheduling in large-scale cloud computing systems," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 23, Dec. 2021, Art. no. e5919, doi: 10.1002/cpe.5919.

[34] M. Zhang, P. Kujala, and S. Hirdaris, "A machine learning method for the evaluation of ship grounding risk in real operational conditions," *Rel. Eng. Syst. Saf.*, vol. 226, Oct. 2022, Art. no. 108697, doi: 10.1016/j.ress.2022.108697.

[35] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, Dec. 2018, doi: 10.1186/s13677-018-0123-6.

[36] U. AlHaddad, A. Basuhail, M. Khemakhem, F. E. Eassa, and K. Jambi, "Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks," *Sensors*, vol. 23, no. 17, p. 7464, Aug. 2023, doi: 10.3390/s23177464.

[37] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in Industry 4.0 landscape for secure SECS/GEM communications," *Sustainability*, vol. 14, no. 23, p. 15900, Nov. 2022, doi: 10.3390/su142315900.

[38] A. Kumari, R. K. Patel, U. C. Sukharamwala, S. Tanwar, M. S. Raboaca, A. Saad, and A. Tolba, "AI-empowered attack detection and prevention scheme for smart grid system," *Mathematics*, vol. 10, no. 16, p. 2852, Aug. 2022, doi: 10.3390/math10162852.

[39] S. Kumar and R. R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions," *Prod. Oper. Manage.*, vol. 31, no. 12, pp. 4488–4500, Dec. 2022, doi: 10.1111/poms.13859.

[40] J. Singh, P. Singh, and S. S. Gill, "Fog computing: A taxonomy, systematic review, current trends and research challenges," *J. Parallel Distrib. Comput.*, vol. 157, pp. 56–85, Nov. 2021, doi: 10.1016/j.jpdc.2021.06.005.

[41] T. Acarer, "Endüstr'Deki gelişmelerin denizcilikişletmelerine ait gemilerin yönetiminde temin ettiği yeni olanaklar Ve insansiz gemiler," *Mersin Üniversitesi Denizcilik ve Lojistik Araştırmaları Dergisi*, vol. 5, no. 2, pp. 122–153, Dec. 2023, doi: 10.54410/denlojad.1364567.

[42] M. Rodger and R. Guida, ‘‘Classification-aided SAR and AIS data fusion for space-based maritime surveillance,’’ *Remote Sens.*, vol. 13, no. 1, p. 104, Dec. 2020, doi: 10.3390/rs13010104.

[43] E. Markopoulos, J. Lauronen, M. Luimula, P. Lehto, and S. Laukkanen, ‘‘Maritime safety education with VR technology (MarSEVR),’’ in *Proc. 10th IEEE Int. Conf. Cognit. Infocommunications (CogInfoCom)*, Oct. 2019, pp. 283–288, doi: 10.1109/CogInfoCom47531.2019.9089997.

[44] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, ‘‘Edge computing for autonomous driving: Opportunities and challenges,’’ *Proc. IEEE*, vol. 107, no. 8, pp. 1697–1716, Aug. 2019, doi: 10.1109/JPROC.2019.2915983.

[45] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, ‘‘Identity management and access control based on blockchain under edge computing for the industrial Internet of Things,’’ *Appl. Sci.*, vol. 9, no. 10, p. 2058, May 2019, doi: 10.3390/app9102058.

[46] J.-H. Huh, ‘‘Reefer container monitoring system using PLC-based communication technology for maritime edge computing,’’ *J. Supercomput.*, vol. 76, no. 7, pp. 5221–5243, Jul. 2020, doi: 10.1007/s11227-019-02864-z.

[47] T. Acarer and L. Yilmaz, *GMDSS—Restricted Radio Operator License—Global Maritime Distress and Safety System*. Orlando, FL, USA: Academy Publications, 2015. [Online]. Available: https://www.nadirkitap.com/gmdss-kisitli-telsiz-operator-ehliyeti-kuresel-denizcilik-tehlike-ve-guvenlik-sistemi-tayfun-acarer-levent-yilmaz-kitap14280766.html

[48] NHL Stenden University of Applied Sciences. *Maritime Cyber Attack Database (MCAD)*. Accessed: Dec. 29, 2023. [Online]. Available: https://www.nhlstenden.com/en/maritime-cyber-attack-database

[49] W. M. S. Yafooz, Z. B. A. Bakar, S. K. A. Fahad, and A. M. Mithon, ‘‘Business intelligence through big data analytics, data mining and machine learning,’’ in *Data Management, Analytics and Innovation*, vol. 1016. Singapore: Springer, 2020, doi: 10.1007/978-981-13-9364-8_17.

[50] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, ‘‘WSN-DS: A dataset for intrusion detection systems in wireless sensor networks,’’ *J. Sensors*, vol. 2016, pp. 1–16, Aug. 2016. [Online]. Available: https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

ABDULMOHSEN ALGARNI received the Ph.D. degree from Queensland University of Technology, Australia, in 2012. He was a Research Associate with the School of Electrical Engineering and Computer Science, Queensland University of Technology, in 2012. He is currently an Associate Professor with the College of Computer Science, King Khalid University. His research interests include artificial intelligence, data mining, text mining, machine learning, information retrieval, and information filtering.

TAYFUN ACARER received the B.S. degree in electronics engineering from Istanbul Technical University, Istanbul, Turkey, in 1980, the M.S. and Ph.D. degrees from Istanbul University, Istanbul, in 1992 and 1995, respectively, and the Asst. Prof. Dr. degree from Bilgi University, Istanbul, in 2016. He has worked at different companies in the ICT Sector. His last job was Chair of the ICT Regulatory Body (ICTA). Since 2018, he has been with the National Metrology Institute (UME), Gebze, Turkey, where he is currently a Board Member. He currently lectures on Information Technologies and Marine Communication and Electronics Navigation Systems at six different universities including Maritime Transportation and Management Vocational School of Higher Education, Piri Reis University, Tuzla, Istanbul.

ZULFIQAR AHMAD received the M.Sc. degree (Hons.) in computer science (CS) from Hazara University, Mansehra, Pakistan, in 2012, the M.S. degree in CS from COMSATS University, Abbottabad, Pakistan, in 2016, and the Ph.D. degree in CS from the Department of Computer Science and Information Technology, Hazara University, in 2022. He is the author of several publications in the field of fog computing, cloud computing, high performance computing, and scientific workflows execution and management. His research areas include scientific workflow management in cloud computing, the Internet of Things, fog computing, edge computing, cybersecurity, and wireless sensor networks (WSNs).