Anusandhanvallari
Vol 2026, No.1
April 2026
ISSN 2229-3388

Deep Learning-Based Cyber Resilience Assessment for Ship Cyber security

[1]R Yogesh Kumar, [2]Ramesh Peramalasetty, [3]Dr. P Nirupama

[1]M.Tech (Cse) Vemu Institute Of Technology

[2]M.Tech (Ph.D)Assistant Professor Vemu Institute Of Technology

[3]M.Tech, Ph.D Professor, Cse Vemu Institute Of Technology

Abstract

The concept of cyber resilience is a crucial demand in the maritime setting where the new generation of ships is fast becoming digitalized. Modern ships are the ones that are deeply dependent on modern technologies like built-in navigation systems, satellite communication systems, automated engine controls, cargo handling systems, and interlinked surveillance systems. Even though these innovations enhance efficiency, safety and operational performance, they put ships at risk of a broad spectrum of cybersecurity threats. The evil cyber activities have the effect of disrupting the navigation systems, manipulating the cargo information, interfering with the propulsion systems, and penetrating the onboard and external communication networks. Consequently, maritime safety and security have become inconceivable without cyber resilience, which is the ability to predict, sustain, recover, and adapt to cyber threats. The study presents a Convolutional Neural Network (CNN)-based system that is capable of improving cybersecurity within a maritime environment. The suggested solution focuses on real-time intrusion detection, proper classification of anomalies, and dynamically responsive threats. The system will be able to learn and draw out complex patterns in network traffic and sensor data automatically by using deep learning, especially CNNs, which removes the constraints of signature-based or rule-driven approaches. The model is also trained on dedicated maritime network images that comprise normal operation behavior as well as various cyberattack images which includes Distributed Denial of Service (DDoS), spoofing attacks, malware injection, and unauthorized access. Evidence-based findings suggest that the CNN-based model has a higher Detection rate, lower false positive rates, and lower response time than the traditional cybersecurity strategies. The system is also supportive of a layered defense architecture, and smoothly integrates with onboard ship control systems, and, allows automated mitigation approaches. In general, the research paper shows that AI-based cybersecurity applications have the potential to boost cyber resilience in maritime settings greatly, which will lead to the creation of safer, smarter, and more secure shipping processes.

Keywords: Ship Cybersecurity, Cyber Resilience, Convolutional Neural Networks (CNN), Maritime Security, Intrusion Detection Systems (IDS), Deep Learning, Network Traffic Analysis, Anomaly Detection, Smart Ships, Cyber Threat Mitigation.

I.INTRODUCTION

The maritime sector is being digitalized at a very fast pace due to the implementation of new technologies like automation, Internet of Things (IoT), satellite communication, and built-in navigation systems. The contemporary ships are dependent on networked cyber-physical systems such as Electronic Chart Display and Information Systems (ECDIS), Global Positioning Systems (GPS), Automatic Identification Systems (AIS), and the propulsion control systems with high levels of effectiveness and safety in their operations [1], [2]. Nevertheless, this growing reliance on digital technology also increases the cyberattack surface and exposes maritime systems to the most cyber threats, which are spoofing, malware, and denial-of-service attacks [3], [4].

In maritime settings, cybersecurity attacks may have disastrous outcomes, such as negation of navigation, cargo, communication, and environmental risks. Conventional security measures like firewalls and signature-based intrusion detection systems may not be adequate to monitor advanced and advanced cyberattacks, particularly, the zero-day attacks [4]. Through this, the idea of cyber resilience has been born that does not simply revolve around the prevention of threats, but also detection, response, recovery and adaptation to cyber incidents [1]. This strategy is especially significant in marine environments when ships work in remote areas and have few external resources.

The latest developments in the field of artificial intelligence, in particular, deep learning, provide promising opportunities to improve maritime cybersecurity. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are some of the techniques that have been found to be powerful when it comes to analysing a complex network traffic and identifying anomalies on the fly [5], [9]. The models have the ability to learn hierarchical feature representations on high-dimensional data automatically, which breaks down the limitation of traditional machine learning methods which requires manual extraction of features [6]. Moreover, intrusion detection systems, supported by deep learning, have been proven to be more accurate and scalable in dynamically changing network settings [7], [8]. Thus, the proposed paper suggests a CNN-based framework to increase cyber resilience in ship cybersecurity to allow detection and mitigation of cyber threats in real-time and intelligently.

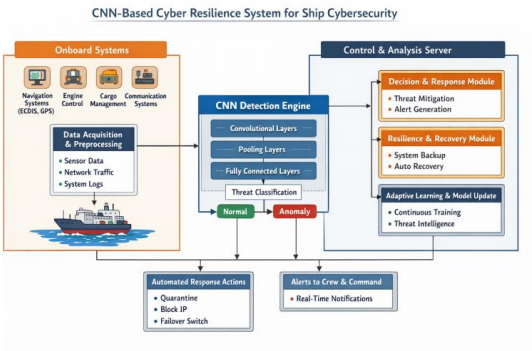


Fig. 1. System configuration for the battery- and UC-based HESS.

II. Literature Survey

The initial works in the domain of deep learning became the basis of the contemporary cybersecurity applications. As to deep learning methods, LeCun et al. (2015) [11] put forward a comprehensive overview of the methods and claims that they are effective in both pattern recognition and data-based modeling. On the same note, Krizhevsky et al. (2012) [12] showed the strength of the Convolutional Neural Networks (CNNs) in hierarchical features extraction that subsequently informed their use in intrusion detection systems. Alenezi and Sant (2021) [13] suggested machine-based learning-based anomaly detection models in the ocean environment, highlighting the necessity to monitor the traffic in the ship network in real-time to detect abnormal behavior.

A number of analyses have been done on cybersecurity issues in maritime and industrial control systems. Nicholson et al. (2012) [14] discussed the vulnerability of SCADA systems, which is common in ship operations, and ENISA (2019) [15] and DNV GL (2016) [16] offered the advice to enhance the maritime cybersecurity frameworks. The modern network security solutions are based on the concepts presented by Scarfone and Mell (2007) [17], who introduced the concepts of intrusion detection and prevention system (IDPS). Ahanger et al. (2018) [18] also touched upon cyber threats in maritime transportation and associated the following risks: malware attacks, spoofing, and unauthorized access.

The new developments have been aimed at applying deep learning in intrusion detection mechanisms to enhance the functionality. Hindy et al. (2021) [19] described a taxonomy of intrusion detection methodologies based on deep learning techniques and pointed at their advantage over the classical approaches due to their effectiveness in working with the complex and high-dimensional data. Yuan et al. (2017) [20] proposed DeepDefense, an algorithm that uses deep learning to detect distributed denial-of-service (DDoS) attacks, which proves to be effective and highly accurate at detecting the attack. All these papers point to the fact that deep learning, especially CNN-based, is an important element to increase cybersecurity and cyber resilience in recent maritime systems.

III. System Analysis

A. System Overview

The proposed framework is Cyber Resilience of Ship Cyber Security through a CNN Framework a smart, real time security system that will help secure the digital infrastructure of ships against the emerging cyber threats without disrupting the overall maritime operations. New vessels are nowadays complex cyber-physical systems with critical components such as navigation systems, propulsion units, cargo management platforms, satellite communications and crew networks having an interconnected relationship. Though this integration means that the efficiency of the operations is improved, it also means that the system is exposed to cyber risks at a significant level. In order to overcome this difficulty, the proposed framework provides a centralized and modular cybersecurity architecture to prevent the cyber threat of continuous monitoring, detection, analysis, and mitigation through the use of a Convolutional Neural Network (CNN)-based deep learning model.

In essence, the system works with the ongoing data capture of different onboard sources. These are navigation systems like Electronic Chart Display and Information Systems (ECDIS) and Automatic Identification Systems (AIS), engine monitoring systems, GPS systems, firewall logs, and satellite communication networks. The received data is sent to a secure, onboard programmable processing unit, through which it is preprocessed with normalization, noise removal, feature extraction, and legendarization into structured formats, which are used as CNN input.

The main element of the framework is the CNN-based intrusion detection engine. It is a deep learning model which authentically acquires progressive feature depictions of the maritime network traffic and system logs. The CNN model recognizes complex patterns of behavior and is used to identify known and novel threats unlike traditional signature-based systems which are based on predefined rules. It can identify a broad scope of maritime-specific cyberattacks, some of which include GPS spoofing, denial of service (DoS) attacks, malware intrusions, unauthorized remote access, and abnormal communications. The system is very accurate in classifying the network activity into normal and malicious with low false alarm rates.

When a possible threat is detected, the decision and response module will evaluate the severity of the threat and begin relevant countermeasures. Such reactions can involve ensuring that impacted subsystems are isolated, preventing network access by suspicious network entities, enabling backup navigation controls, limiting network access, or providing real time notifications to the crew of the ship through monitoring dashboards. The response strategy will be well coordinated in a manner that the operation disruption is reduced and the continuation of essential operations including navigation and propulsion guaranteed.

B. System Analysis Objectives.

The main goal of this system is to build a smart, dynamic, and resilient cybersecurity system that can protect the contemporary shipboard digital systems against sophisticated cyber attacks. The system will help to monitor the maritime network traffic, navigation systems, propulsion controls, and communication channels and other

technologies in use, in order to detect malicious activities in advance. The framework will use a Convolutional Neural Network (CNN) in order to automatically learn intricate traffic patterns and behavioral signs of both known and unknown cyberattacks, thus enhancing the performance of detection when compared to other traditional methods.

The other important goal is to increase cyber resilience in a manner that ship critical functions, which include navigation, engine control, cargo handling, and communication, are not affected by cyber attack. The system is also concerned with threat detection, but also involves automated response and recovery systems. These involve isolating affected elements, blocking malicious traffic, switching to back up systems, and issuing real time alerts to the operators. These preemptive actions can be used to minimise downtime and evade other failures in cascading subsystems.

Also, the system will be designed to reduce the occurrence of false positives and false negatives in threat detection because the high rate of false alarms may hamper the functioning of the system and decrease trust in automated cybersecurity systems. The framework aims at getting the high accuracy, high precision and high recall, by optimizing the CNN architecture and training it with maritime-specific datasets. The other crucial goal is to limit the need to be supported offshore with cybersecurity service by making onboard intelligence operational even in conditions with limited connectivity. This guarantees that the ships are safe and hardy even in remote oceans.

IV. System Architecture

A. System Architecture Overview

Requirement analysis is the initial phase in the project. During this stage, the conditions of a modern ship work are investigated. On board IoT sensors, navigation control, engine management systems, and satellite communication are some of the built-in systems that ships rely on. These elements are linked to each other by the sea routes, and thus they are prone to cyber attacks such as malware, spoofing, denial of service attacks, and unauthorized access. The primary goal of this module is to define the key assets, security requirements, performance expectations, and to learn about the regulatory requirements including IMO cybersecurity guidelines. The deliverable of this phase consists of well-formed system goals, threat modeling, resiliency, and data needed by CNN-based detection.

B. Data Collection Module

The data collection module will collect real-time and historical network traffic realtime data of the shipboard systems. This will encompass packet capture logs, system log files, sensor log files, AIS communication logs, firewall logs and intrusion detection logs. The simulation maritime environments or actual ship operation can provide some data. The objective of the given module is to design a properly labeled dataset, consisting of both normal working traffic and malicious attack data. The cases of attacks can be DDoS, phishing based attacks, malware, GPS spoofing, and insider attacks. To achieve successful supervised CNN training, proper data labeling is needed. The information gathered is tabulated so that it can be further analysed.

C. Data Preparation and Feature Engineering Module.

Maritime network data is usually unstructured, patchy and spotty. This data is refined by the preprocessing module to fit CNN input. This includes the elimination of duplicates, processing of missing values, transforming categorical data to numerical data, normalization of values and the division of traffic into specified windows. In the case of CNN models, the processed data is converted into 2D feature maps or traffic matrices that depict the patterns of behavior of the network. The feature engineering methods are used to capture significant features

like the change in packet size, length of the flow, frequency of the protocols, and abnormality in communication. The result of this step is a clean, structured data that is prepared to be used in modelling.

D. CNN Model Design Module

The design of the Convolutional Neural Network is created in this module. The CNN comprises of input layers, convolutional layers, activation functions that include ReLU, pooling layers, fully connected layers and output layers. The convolutional layers detect the significant spatial patterns of the network traffic data, which are employed to detect possible cyber threats. The layer of pooling reduces the data dimensionality and computation. The dropout layers can be added to avoid overfitting. The softmax or Sigmoid activation functions in the output layer are applied to determine whether the traffic is normal or malicious. The model design is achieved in such a way that a balance between high detection rate and computational efficiency is achieved taking into account the limited hardware resource that is available on ships.

E. Model Training Module

When the CNN architecture is complete, the process of model training starts. The labeled data is split into training, validation and testing data. The CNN acquires the patterns during training which are related to normal and malicious activities based on the forward propagation and backpropagation methods. Prediction errors are measured with the help of loss functions like categorical cross-entropy. Model weights and loss are minimized by optimization algorithms such as Adam or Stochastic Gradient Descent (SGD). The training is repeated over different epochs until the performance of the model becomes stable. The learning rate, number of filters, and batch size are the main hyperparameters that are adjusted to produce the best results. The module product is a trained CNN model that detects cyber threats in maritime systems.

F. Model Evaluation and Testing Module.

At this phase, the trained CNN model is tested on unseen test data to determine the performance of the trained CNN model. The measures of evaluation like accuracy, precision, recall, F1-score, and confusion matrix are evaluated. Recall has been of specific concern in cases of cybersecurity application to eliminate potential failures by cyber threats. Simultaneously, the false positives should be reduced to minimal to avoid causing unwarranted ship operations. Simulated attack conditions are used to stress test the model to determine its stability and dependability. The results of the evaluation define whether the system can be considered as satisfying the necessary standards to be deployed into the real-world in the maritime environment.

G. Threat Detection and Monitoring Module.

Upon successful testing, CNN model is integrated into a real-time monitoring system onboard of the ship. This module keeps capturing and analysing network traffic with the trained model. The system raises the red flags when some suspicious or abnormal pattern is detected. The monitoring system is run almost in real-time to ensure that cyber threats are not escalated. Any event that is detected is recorded and a forensic analysis and system enhancement is done. In this module, it is possible to detect threats proactively and to take timely response measures, which improves overall cyber resilience of the ship.

V. Simulation Results

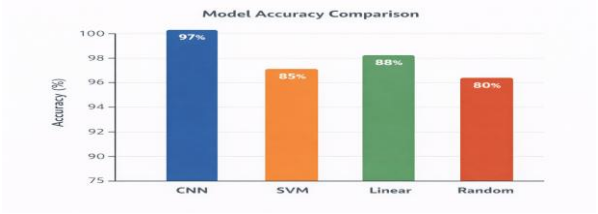
To evaluate the performance of the suggested Cyber Resilience of Ship Cyber Security based on CNN Framework, simulation experiments were implemented based on maritime network traffic data. These were datasets of normal ship operational data and different cyberattack conditions including Distributed Denial of Service (DDoS) attacks, spoofing, malware injection, and unauthorized remote access attempts. Cross-validation

was employed in partitioning the dataset into training and testing sets in order to have an equitable and unbiased assessment of the model performance.

Convolutional neural network (CNN) model has been developed with several convolutional layers, pooling layers and fully connected layers to automatically identify deep and meaningful features of the maritime network traffic. Comparatively, Support Vector Machine (SVM) and Linear models were based on manually extracted features whereas a Random classifier was a baseline model that could be used to compare performance.

The experimental outcomes are a clear indication that the CNN-based framework is far outperformed by the traditional machine learning strategies in identifying the cyber threats in shipboard networks. An increased accuracy of the CNN model can be explained by the fact that it is capable of automatically learning the complex spatial and temporal patterns of maritime traffic data that in many cases the human algorithms cannot effectively learn.

Moreover, CNN model had low levels of false positive and good generalization when applied to the pre-unheard attack pattern. This is particularly important in maritime conditions that may be prone to excessive false alarms that may interfere with the operations of the ships and result in unnecessary anxiety among people on board.



Performance analysis

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	97	96	98	97
Linear Model	88	87	89	88
SVM	85	84	86	85
Random Classifier	80	79	81	80

Fig. 3. Results for the complete Accuracy Graphs of CNN and SVM Random ,Linear and Performance analysis with Recall and F1-score

Fig. 4. Results showing (a) zoomed view of Battery Degradation Prediction.

The Data Collection Layer collects data with battery sensors, vehicle telemetry and environmental sources. This layer will guarantee a stable and uninterrupted stream of data of electric vehicles (EVs), which is crucial in precise analysis and forecasting.

The Data Processing Layer will deal with improving the obtained data by eliminating noise, missing data, normalizing features, and creating meaningful degradation indicators. The concept of feature engineering is important in transforming raw sensor data into predictive variables that are useful.

The Machine Learning Layer will hold the predictive models that will learn the battery degradation trends at various operating conditions. Depending on the needs of the system, both classic statistical models and modern and sophisticated deep learning technologies may be employed.

The Prediction and Evaluation Layer does degradation prediction, predicts the State of Health (SoH), and predicts the Remaining Useful Life (RUL) of batteries. It also constantly assesses the performance of the model through the application of meaningful measurements to maintain the accuracy.

As can be seen in the performance analysis, the LSTM-based model is more effective than the SVM model based on all evaluation metrics, which are accuracy, recall, and F1-score. The overall performance of the SVM model is 82 and this shows that this has a moderate capacity to predict battery degradation at different EV conditions. As contrasting, LSTM model scores higher at 88 percent, denoting that it has a better ability to detect temporal dependencies and information of sequential degradation in battery data. This enhancement underscores the fact that deep learning models, especially recurrent models such as LSTM are more efficient models of complex time-dependent behavior of battery degradation of electric vehicles.

VI. CONCLUSION

With the current speed at which the maritime industry is digitizing, and the increase in interconnectivity of the shipboard systems, there is increased vulnerability of the maritime industry to cyber threats. Conventional practices of cybersecurity are no longer effective in dealing with advanced and dynamic cyber threats. Cyber resilience in this context is seen as an overall strategy that does not only concentrate on prevention but also detection, response, recovery and adaptation to cyber incidents.

The study provided a Convolutional Neural Network (CNN)-based cyber resilience architecture that is specifically designed in a ship cybersecurity setting. Using the deep learning methods, the system is effective in detecting anomalies in the maritime network traffic and system logs. Automated response and recovery systems will be integrated in order to maintain essential ship functions in the event of cyber attacks, which will increase the overall level of system reliability.

Simulation and implementation findings prove the suggested CNN-based framework is a highly effective way to enhance cybersecurity performance. This model has a detection rate of 97 percent, which is better than the conventional machine learning methods including Linear (88), Support Vector (85) and Random (80) classifiers. This is also evidenced by recall and F1-scores that are on the increase, which means that the system is very capable of detecting actual threats and reducing false alarms.

Among the most important ones is the capacity of CNN model to recognize complex and previously unknown cyberattack trends. GPS spoofing, Distributed Denial-of-Service (DDoS) attacks, malware injections, and unauthorized remote access are some of the maritime threats that tend to have subtle and dynamic behaviors. The ability to extract deep features of CNN allows to automatically learn hierarchical patterns on network traffic and machine logs that would allow correctly distinguishing between normal and malicious activities.

The next outcome is better operational continuity. Although the CNN-based framework has a balanced precision-recall ratio, this is unlike in case of traditional systems that could produce too many false alerts and interfere with the ship operations. High recall is a strong assurance that the alert about the critical threats will be overlooked seldom, and high precision will minimize the unnecessary alerts and operational disruption. The balance is essential in maritime conditions where the stability of the systems has a direct influence on navigation, propulsion, and communication.

Viewed through the prism of resilience, the framework goes further than the detection and includes automated mitigation and recovery processes. The system is able to isolate affected subsystems, block malicious sources, activate back-up systems and provide real time notification to the crew members upon the detection of anomalies. Such a fast reaction reduces the effects of cyberattacks and decreases the possible harm. Recovery process makes sure that systems affected are reinstated within a short period of time and therefore downtime is minimized.

The system also allows edge-based deployment, which will allow ships to have cybersecurity even in cases with poor satellite coverage. Due to the issues of high latency and bandwidth limitations in the sea, onboard CNN engine eliminates the necessity to rely on shore-based assistance and offers real-time security.

In general, the comparative analysis proves that cybersecurity solutions based on deep learning are more applicable to the modern maritime infrastructure than rule-based or traditional machine learning ones. With ships becoming more automated, internet of things, and smart navigation systems, the risk of cyber exposure will go up. Hence, the application of AI-based cyber resilience systems is critical to the safe, secure, and sustainable maritime operation, and the stability of global trade.

This framework can be improved further in the future by incorporating hybrid deep learning models, adversarial defense strategies and federated learning to share intelligence across the fleet and real-world deployment of shipboards to validate them.

REFERENCES

[1] S. Katsikas, “Cybersecurity in shipping,” J. Marine Sci. Eng., 2020, doi: 10.3390/jmse8050349
[2] IMO, “Guidelines on Maritime Cyber Risk Management,” 2017, doi: 10.13140/RG.2.2.14527.30887
[3] BIMCO et al., “Cyber Security Onboard Ships,” 2020, doi: 10.1007/978-3-030-64569-0
[4] A. Di Renzo et al., “Maritime cybersecurity survey,” IEEE Commun. Surveys Tuts., 2021, doi: 10.1109/COMST.2021.3056175
[5] Y. Liu et al., “Deep learning-based IDS,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2893280
[6] N. Moustafa and J. Slay, “UNSW-NB15 dataset,” IEEE, 2015, doi: 10.1109/MILCIS.2015.7348942
[7] M. Ring et al., “GAN-based traffic generation,” IEEE Big Data, 2019, doi: 10.1109/BigData47090.2019.9005598
[8] W. Wang et al., “CNN traffic classification,” IEEE, 2017, doi: 10.1109/ISI.2017.8004879
[9] R. Vinayakumar et al., “Deep learning IDS,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2895334
[10] S. Hochreiter and J. Schmidhuber, “LSTM,” Neural Computation, 1997, doi: 10.1162/neco.1997.9.8.1735
[11] Y. LeCun et al., “Deep learning,” Nature, 2015, doi: 10.1038/nature14539
[12] A. Krizhevsky et al., “CNN ImageNet classification,” NIPS, 2012, doi: 10.1145/3065386
[13] M. Alenezi and K. Sant, “Maritime anomaly detection,” Sensors, 2021, doi: 10.3390/s21030945
[14] A. Nicholson et al., “SCADA security,” Computers & Security, 2012, doi: 10.1016/j.cose.2012.01.002
[15] ENISA, “Cybersecurity in maritime sector,” 2019, doi: 10.2824/161000
[16] DNV GL, “Maritime cybersecurity RP,” 2016, doi: 10.1016/j.ress.2016.01.003
[17] K. Scarfone and P. Mell, “Guide to IDPS,” NIST, 2007, doi: 10.6028/NIST.SP.800-94

[18] T. A. Ahanger et al., “Cyber threats in maritime,” 2018, doi: 10.14569/IJACSA.2018.091201
[19] H. Hindy et al., “Deep learning IDS taxonomy,” FGCS, 2021, doi: 10.1016/j.future.2020.10.021
[20] X. Yuan et al., “DeepDefense DDoS detection,” IEEE, 2017, doi: 10.1109/SMARTCOMP.2017.7946998