Scientiarum: A Multidisciplinary Journal
Volume 2, Issue 3, June 2026, pp. 1–6
DOI: 10.54646/SAPARS.2026.32

SAPAR SERVICES LLP
Scholarly Articles Publication And Repository Services

ORIGINAL RESEARCH

Cyber-attack detection on maritime autonomous surface ships: python based predictive analysis

Joseph Mino[1]* and Mukesh Krishnan[2]

[1]Department of Computational Technology, SRM Institute of Science and Technology, Chennai, India
[2]Department of Networking and Communication, SRM Institute of Science and Technology, Chennai, India

***Correspondence:**
Joseph Mino,
joseph.mino@gmail.com

Received: 29 April 2026; **Accepted:** 08 May 2026; **Published:** 31 May 2026

Maritime Autonomous Surface Ships (MASS) that are used for navigation, cargo handling and communication on a digital system. It improves operational efficiency and maximizes cyber risk threats. This project is based on the framework that incorporates cybersecurity methodology and examines dynamic data such as geo-location coordinates, timestamp, navigation map status, performance, efficiency, cargo type, data source and destination port that are grounded in the operating unit. By understanding these analytics based on Python, machine learning (ML) and deep learning techniques that use the system to easily analyze both real-time and Automatic Identification System (AIS) datasets that helps to detect any anomalies present in the patterns that are linked to potential cyber threats. Anomalies are detected in an early phase and the model supports the risk mitigation and strengthens the autonomous maritime operations. Informed decision making can support proactive monitoring of maritime which is supported by AIS data feature which also improve accuracy and reliability. This paper aim is to propose the model which is more reliable, expandable, and accurate prediction through the use of hybrid model which also incorporates the concept of long short-term memory (LSTM) and random forest which is also helpful in further classification and extraction. The model aims to enhance the detection accuracy with techniques such as deep learning and ML.

Keywords: maritime cybersecurity, autonomous surface ships, MASS, AIS data analysis, anomaly detection, predictive security, python-based modelling, MASS cyber threat detection

Introduction

Maritime Autonomous Surface Ships (MASS) transforms the traditional operations into the automated ship operations. In this ships are interconnected with digital systems that used to exchange all the function in an effective way. This reliance on the technologies increases the sensitive information to the cyber risks. The ships are dependent on digital system at which the data are exchanged to the proper function effectively. This growth reliance on the technologies not only increases the cyber risk threat but also interfere with navigation systems and tries to manipulate operational data and threaten safety exists. These vulnerabilities try to emphasizes the adopting of the proactive cybersecurity methodologies for the maritime systems.

This project developed is to use dynamic vessel information to predict cybersecurity framework. It tells the information about the navigation map status, speed, heading, geographic measures and destination port etc. With the mechanism of Python that are used for data processing and machine learning (ML), where the system need to analyze the real-time Automatic Identification System (AIS) data and any historic information so that it can able to identify any abnormal behavior that are associated with cyber threats. Integrating the various operational features into the model

improves better decision making, predictive measure and accuracy. The key objective of this project is to improve reliability, resilience and security concerns of autonomous maritime operations through the early phase threat identification and proper immediate response mechanism.

Literature survey

Cheng et al. (1), this study deeply examines the interfaces that are human-oriented occurring in control systems for identifying autonomous vessels. The research mainly highlights what are the frequent operational errors and the related stressed and shows the importance of improved training programs and better-designed.

Human–machine interfaces for reducing the cybersecurity and operation based risks.

Kim et al. (2), the authors bring the application of text mining and network analysis to easily evaluate the deployment that are in the shipboard electronic systems. These findings not only reveal the cybersecurity concerns but also reveals the operational weakness that are associated in the maritime vessels.

Tabish and Chaur-Luh (3), this paper explores what are the current cyber threats that exists in the defense mechanism and what are the further research methodology that are related to autonomous ship. This study strongly emphasizes the predictive and intelligence cybersecurity solutions that tends to address the evolving risks in the maritime vessels.

Amro et al. (4), this propose of communication framework in this research is to strengthen the data transmission and the network reliability which is present in the passenger ships. This study mainly focuses on minimizing the cyber threats within the communication systems.

Ashraf et al. (5), this research investigates the cyberattack way that are present in the IoT enabled environments. These authors identify the vulnerabilities present in the sensor networks that underlines the stronger security controls in the connected ship infrastructures.

Proposed system

The proposed system utilizes the suggested framework with ML technologies to collect the dynamic data from AIS records. This framework uses multiple parameters including geo-location coordinates, timestamp, navigation map status, performance, efficiency, cargo type, data source, destination port, vessel capacity and departure, along with arrival time. These parameters are mostly used to detect any unusual patterns present in the system. By properly analyzing the old data and real-time dynamic data which helps the system to signals suitable mechanism to take immediate action. By doing this, the system performs well in terms of performance, reliability and ensures proper safety measures with safe communication against the prevailing cyber risks.

Architecture diagram

Refer to **Figure 1** for additional information.

Modules

Maritime data collection

This phase serves as the basis for the proposed cybersecurity framework for MASS. Operational and navigational information is gathered primarily from the AIS, which transmits details such as timestamps, geographic coordinates, vessel speed, heading direction, navigational condition, cargo category, destination port, estimated arrival time, and source identifier. These characteristics together reflect the real-time behavior of autonomous ships. As MASS operations rely on digital navigation and communication systems, AIS data acts as a key source for detecting abnormal activities. Continuous collection of vessel data allows the system to establish standard movement patterns, making it easier to differentiate between normal operational variations and suspicious cyber-induced anomalies. Precise and comprehensive data collection is crucial for dependable predictive analysis in later stages.

AIS data preprocessing

With the raw AIS system that has issues such as failures related to communication, hardware and other environmental factors. Preprocessing is done in the process so that it improves data quality and also maximizes identification in the sensitive data including abnormal values and inconsistent duplicate entries. For this, effective data normalization techniques help to maintain consistent values across all the parameters. It also helps to order and sequence the movements in the system. It minimizes noise and sorts the unstructured data. The proper preprocessing reduces the false detection and increases the processing of the actual behavior of the vessel.

Feature extraction

AIS characteristics needs the effective cyber detection in the session. Every parameter affects the behavior of the parameter in the same way as the system used to evaluate the performance, electronic fluctuations, route inconsistencies, complexity, timings and speed. The relationship that exists is used to uncover the hidden patterns in the movements,

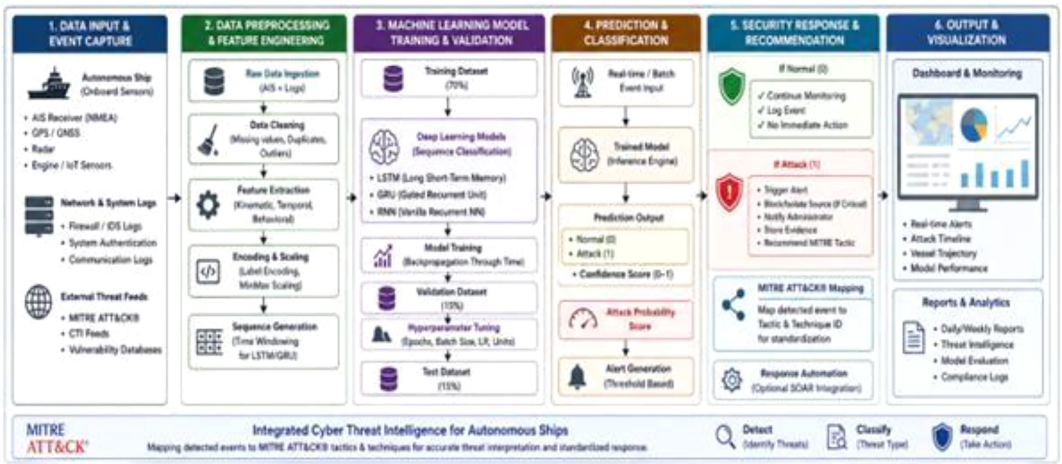

FIGURE 1 | Architecture diagram.

```
Epoch 3/5
40/40 ━━━━━━━━━━━━━━━━━━━━ 0s 4ms/step - accuracy: 0.8263 - loss: 0.4467 - val_accuracy: 0.8813 - val_loss: 0.4139
Epoch 4/5
40/40 ━━━━━━━━━━━━━━━━━━━━ 0s 4ms/step - accuracy: 0.8699 - loss: 0.3803 - val_accuracy: 0.8813 - val_loss: 0.4019
Epoch 5/5
40/40 ━━━━━━━━━━━━━━━━━━━━ 0s 5ms/step - accuracy: 0.8724 - loss: 0.4012 - val_accuracy: 0.8969 - val_loss: 0.3972
13/13 ━━━━━━━━━━━━━━━━━━━━ 0s 13ms/step

✅ RNN Test Accuracy: 90.75%

📊 Confusion Matrix:
[[189  17]
 [ 20 174]]

📋 Classification Report:
              precision    recall  f1-score   support

      Attack       0.90      0.92      0.91       206
     Defense       0.91      0.90      0.90       194

    accuracy                           0.91       400
   macro avg       0.91      0.91      0.91       400
weighted avg       0.91      0.91      0.91       400
```

FIGURE 2 | Recurrent neural network (RNN) test accuracy.

```
🔄 Training GRU...

Epoch 1/3
40/40 ━━━━━━━━━━━━━━━━━━━━ 2s 13ms/step - accuracy: 0.5548 - loss: 0.6641 - val_accuracy: 0.7656 - val_loss: 0.5685
Epoch 2/3
40/40 ━━━━━━━━━━━━━━━━━━━━ 0s 5ms/step - accuracy: 0.8065 - loss: 0.5499 - val_accuracy: 0.8531 - val_loss: 0.4909
Epoch 3/3
40/40 ━━━━━━━━━━━━━━━━━━━━ 0s 5ms/step - accuracy: 0.8754 - loss: 0.4547 - val_accuracy: 0.8813 - val_loss: 0.4411
13/13 ━━━━━━━━━━━━━━━━━━━━ 0s 18ms/step

✅ GRU Test Accuracy: 91.25%

📊 Confusion Matrix:
[[191  15]
 [ 20 174]]

📋 Classification Report:
              precision    recall  f1-score   support

      Attack       0.91      0.93      0.92       206
     Defense       0.92      0.90      0.91       194

    accuracy                           0.91       400
   macro avg       0.91      0.91      0.91       400
weighted avg       0.91      0.91      0.91       400
```

FIGURE 3 | Gated recurrent unit (GRU) test accuracy.

```
13/13 ━━━━━━━━━━━━━━━━━━━━ 0s 22ms/step

✅ LSTM Test Accuracy: 92.00%

📊 Confusion Matrix:
[[189  17]
 [ 15 179]]

📋 Classification Report:
              precision    recall  f1-score   support

      Attack       0.93      0.92      0.92       206
     Defense       0.91      0.92      0.92       194

    accuracy                           0.92       400
   macro avg       0.92      0.92      0.92       400
weighted avg       0.92      0.92      0.92       400
```

FIGURE 4 | Long short-term memory (LSTM) test accuracy.

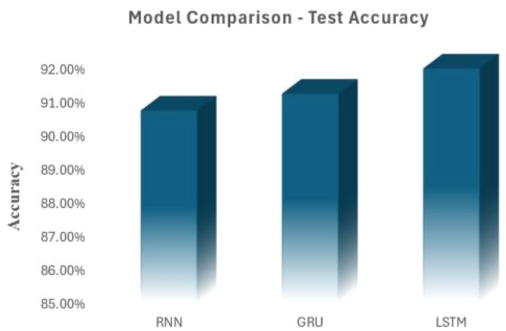

FIGURE 5 | Model comparison – test accuracy.

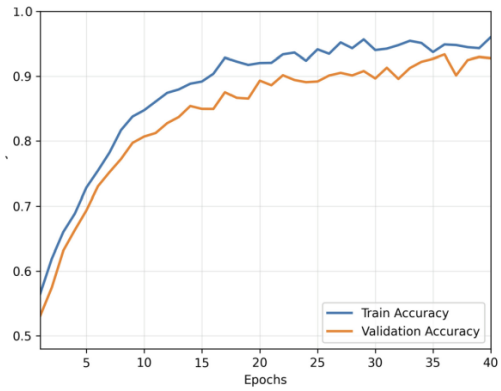

FIGURE 6 | Hybrid LSTM-GRU training vs. validation accuracy.

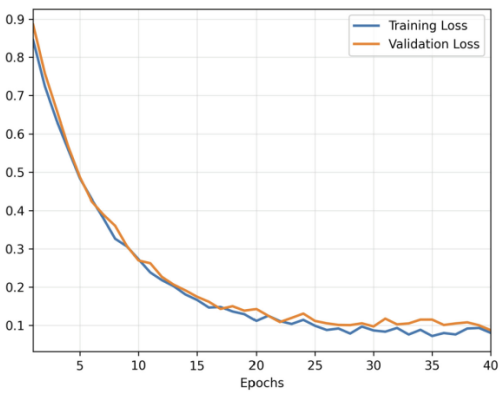

FIGURE 7 | Hybrid LSTM-GRU training vs. validation loss.

and it may signal threat signals like global positioning system (GPS) spoofing or any of the map status data. It is important to select the informative variables that minimizes the threat.

By properly selecting the features which may help easily to identify some of the variation that upset the operations.

Predictive cyber-attack detection

This framework ideology is to represent the analytical element by the module. When the normal vessel navigation including regular routes, constant direction, and time behaviors is learned from the old AIS information using ML algorithm that is clearly implemented using Python. The baseline patterns are implemented the sensitive data are clearly captured against the learned behavior. The deviations such as inconsistent updates, speed changes and performance are considered as signs of the cyber manipulation. Predictive method identifies the threat early in the process and enables strengthening of cybersecurity technologies and threat detection in the maritime.

Prediction output and system analysis

The system provides better prediction which shows whether the system vessel activity is typical or compromised. The framework is simple so it presents the results in a consolidated way.

It is more appropriate for the system assessment and proper monitoring. The system analytical prediction not only helps to assess the model in an accurate way but also helps to understood how the navigational factors contribute to the anomaly detection. This prediction stage completes the workflow by properly validating the effectiveness of the system in the cybersecurity risks within the autonomous maritime environments through predictive data analysis.

Result

The recurrent neural network (RNN) model achieves high performance with an overall accuracy of 90.75% (refer **Figure 2**), maintaining balanced precision and recall for both attack and defense categories. The confusion matrix and classification report confirm reliable predictions, indicating robust classification capabilities.

The gated recurrent unit (GRU) model attains notable test accuracy (refer **Figure 3**), demonstrating its capability to capture sequential dependencies. Its balanced precision and recall reflect strong generalization across classes in the classification task.

The LSTM model exhibits strong test accuracy (refer **Figure 4**), reflecting its ability to learn long-term dependencies in the data. The value of the recall

Classification Report – Hybrid LSTM-GRU Model

	precision	recall	f1-score	support
Normal (0)	0.98	0.97	0.97	10866
Attack (1)	0.91	0.95	0.93	4134
accuracy			0.96	15000
macro avg	0.95	0.96	0.95	15000
weighted avg	0.96	0.96	0.96	15000

FIGURE 8 | Final output.

and precision explains the dependable across all the classification categories.

The variety of test accuracy are clearly shown by the analysis (refer **Figure 5**) that highlights that each model has special aptitude for pattern recognition. It not only guides the optimal model but also tailored to specific classification challenges.

This effective learning has shown by hybrid LSTM-GRU's model without overfitting (refer **Figure 6**) and it aligns with validation accuracy and training. This balance underscores the robustness in generalization that helps to unseen the data during training process.

The tuned hybrid model has more stable validation performance with minimized divergence across validation and training loss (refer **Figure 7**). It indicates that the model was not able to save the training sequences but it was simply learning the temporal patterns which are relevant to maritime cyber threats detection.

From the output (refer **Figure 8**) we confirm that the model is not only used for learning purposes but also has the attack-labeled sequences with the high priority recall with an acceptable precision. It is particularly relevant for autonomous maritime systems. It is particularly important for knowing maritime systems where the cyber threats affect the route navigation, communication reliability and better decision-making process. The results indicate that the proposed system can easily support real-time monitoring by detecting suspicious AIS behavior and obtaining reliable alerts. Overall, this classification not only strengthens the claim but also the hybrid LSTM-GRU for predicting the cybersecurity framework for MASS.

Future scope

This framework is used to combine the different data sources, advanced sensor information and satellite communication. It helps to easily attain the threat detection capability with the framework. In the case of the real-time scenario, this process of advanced decision-making not only helps to detect the threat but also effectively makes the proper solutions across all the diverse computing platforms. This needs a few improvements so that it can be adopted in further developments.

In addition to this, it makes the process easier for understanding anomaly detection data which also increases transparency in the process. By extending the monitoring purpose it is helpful for large-scale maritime networks and increases global shipping routes. It also maximizes the practical application and operational impact.

Funding

The authors declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Cheng T, Veitch EA, Utne IB, Ramos MA, Mosleh A, Alsos OA, et al. Analysis of human errors in human-autonomy collaboration in autonomous ships operations through shore control experimental data. *Reliab Eng Syst Saf*. (2024) 246:110080. doi: 10.1016/j.ress.2024.110080
2. Kim J, Han S, Lee H, Koo B, Nam M, Jang K, et al. Trend research on Maritime Autonomous Surface Ships (MASSs) based on shipboard electronics: focusing on text mining and network analysis. *Electronics (Basel)*. (2024) 13(10):1902. doi: 10.3390/electronics13101902
3. Tabish N, Chaur-Luh T. Maritime autonomous surface ships: a review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access*. (2024) 12:17114–36. doi: 10.1109/ACCESS.2024.3357082
4. Amro A, Gkioulos V, Katsikas S. Communication architecture for autonomous passenger ship. *Proc Inst Mech Eng O J Risk Reliab*. (2023) 237(2):459–84. doi: 10.1177/1748006X211002546
5. Ashraf I, Park Y, Hur S, Kim SW, Alroobaea R, Zikria YB, et al. A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Trans Intell Transp Syst*. (2023) 24(2):2677–90. doi: 10.1109/TITS.2022.3164678

Bibliography

6. Tam T, Bucknall A. Maritime cyber security: risks, threats and vulnerabilities. *J Transp Secur*. (2020) 13(1):1–15.
7. International Maritime Organization (IMO). *Guidelines on Maritime Cyber Risk Management*. MSC-FAL.1/Circ.3 (2017).
8. Liu J, Shi Z, Liu W. AIS data-driven vessel behavior analysis and anomaly detection. *Ocean Eng*. (2019) 186:106–23.
9. Tu Y, Zhou G, Zhang L. Anomaly detection in AIS trajectories using machine learning techniques. *IEEE Access*. (2020) 8:113–25.
10. Tsou AD. Maritime situational awareness using AIS and data analytics. *J Navig*. (2019) 72(1):1–19.
11. Riveiro M, Falkman G, Ziemke T. Visual analytics for maritime anomaly detection. *IEEE Comput Graph Appl*. (2018) 38(4):42–53.
12. Ferrari S, Fierro R. Cyber-physical security in autonomous maritime systems. *IEEE Syst J*. (2020) 14(2):2345–56.

13. Lee H, Kim S, Park J. Machine learning-based intrusion detection for maritime cyber systems. *Sensors*. (2021) 21(5): 1–17.
14. Cheng P, Wang X, Zhang L. AIS spoofing detection using statistical and learning-based methods. *Ocean Eng*. (2021) 234:1–12.
15. Goodfellow I, Bengio Y, Courville A. *Deep Learning*. MIT Press (2016).
16. Bishop CM. *Pattern Recognition and Machine Learning*. Springer (2006).
17. Han J, Kamber M, Pei J. *Data Mining: Concepts and Techniques*. 3rd ed. Morgan Kaufmann (2012).
18. Murphy KP. *Machine Learning: A Probabilistic Perspective*. MIT Press (2013).
19. Géron A. *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*. O'Reilly Media (2019).
20. Abadi M, Barham P, Chen J, Chen Z, Davis A, Dean J, et al. TensorFlow: a system for large-scale machine learning. *OSDI*. (2016). p. 265–83.