Cyber-Attack Detection on Maritime Autonomous Surface Ships: Python-based Predictive Analysis

Joseph Mino, Mukesh Krishnan

Department of Networking and Communications, SRM Institute of Science and Technology, India

joseph.mino@gmail.com, mailmino@yahoo.com

ABSTRACT

Maritime Autonomous Surface Ships that are used for navigation, cargo handling and communication on a digital system. It improves operational efficiency and maximises cyber risk threats. This project is based on a framework that incorporates cybersecurity methodologies and examines dynamic data, such as geo-location coordinates, timestamps, navigation map status, performance, efficiency, cargo type, data source, and destination port, grounded in the operating unit. By leveraging Python, machine learning, and deep learning techniques, the system can easily analyse both real-time and Automatic Identification System datasets to detect anomalies linked to potential cyber threats. Anomalies are detected early, and the model supports risk mitigation and enhances autonomous maritime operations. Informed decision-making can support proactive maritime monitoring, with Automatic Identification System data features that improve accuracy and reliability. This paper proposes a hybrid model that combines LSTM and random forests to improve reliability, expandability, and predictive accuracy. The model aims to enhance the detection accuracy with techniques such as deep learning and machine learning.

Keywords: Maritime Cybersecurity, Autonomous Surface Ships, MASS, AIS Data Analysis, Anomaly Detection, Python-Based Modelling, Vessel Monitoring, Cyber Threat Detection

1.INTRODUCTION

Maritime Autonomous Surface Ships (MASS): transforms traditional ship operations into automated ones. In this, ships are interconnected with digital systems that enable the effective exchange of all functions. This reliance on technology increases the risk of sensitive information being compromised by cyber threats. The ships depend on a digital system for exchanging data to ensure proper functioning. This reliance on technology increases cyber risks, interferes with navigation systems, attempts to manipulate operational data, and threatens safety. These vulnerabilities try to emphasise the adoption of proactive cybersecurity methodologies for maritime systems.

This project uses dynamic vessel information to predict cybersecurity risks. It provides information on the navigation map status, speed, heading, geographic coordinates, and destination port, etc. Using Python mechanisms for data processing and machine learning, the system needs to analyse real-time AIS data and historical information to identify abnormal behaviour associated with cyber threats. Integrating the various operational features into the model improves decision-making, predictive measures, and accuracy. The key objective of this project is to improve the reliability, resilience, and security of autonomous maritime operations through early-phase threat identification and an effective immediate response mechanism.

2. LITERATURE SURVEY

T. Cheng et al. [1] This study deeply examines the human-oriented interfaces occurring in control systems for identifying autonomous vessels. The research primarily highlights frequent operational errors and the related stress, and underscores the importance of improved training programs and better-designed systems.

J. Kim et al. [2] apply text mining and network analysis to evaluate deployments in shipboard electronic systems easily. These findings not only reveal cybersecurity concerns but also operational weaknesses associated with maritime vessels.

Proceedings of ICICCS-2026 (Poster Papers), DMPedia Lecture Notes in Computer Science & Engineering.
ISBN: 978-81-993813-1-5

N. Tabish and T. Chaur-Luh [3]. This paper explores current cyber threats to defence mechanisms and further research methodologies related to autonomous ships. This study strongly emphasises predictive, intelligent cybersecurity solutions that address evolving risks in maritime vessels.

A. Amro et al. [4] The purpose of this communication framework in this research is to strengthen the data transmission and the network reliability that is present in the passenger ships. This study primarily focuses on minimising cyber threats in communication systems.

Y. Ashraf et al. [5] This research investigates the ways cyberattacks occur in IoT-enabled environments. These authors identify vulnerabilities in sensor networks, underscoring the need for stronger security controls in connected ship infrastructure.

3. PROPOSED SYSTEM

The proposed system uses the suggested machine-learning framework to collect dynamic data from AIS records. This framework uses multiple parameters, including geo-location coordinates, timestamp, navigation map status, performance and efficiency, cargo type, data source, destination port, vessel capacity, departure, and arrival time. These parameters are primarily used to detect unusual patterns in the system by analysing historical and real-time data, enabling the system to signal a suitable mechanism to take immediate action. By doing this, the system performs well in terms of performance and reliability, and ensures proper safety measures and safe communication against the prevailing cyber risks.

4. ARCHITECTURE DIAGRAM

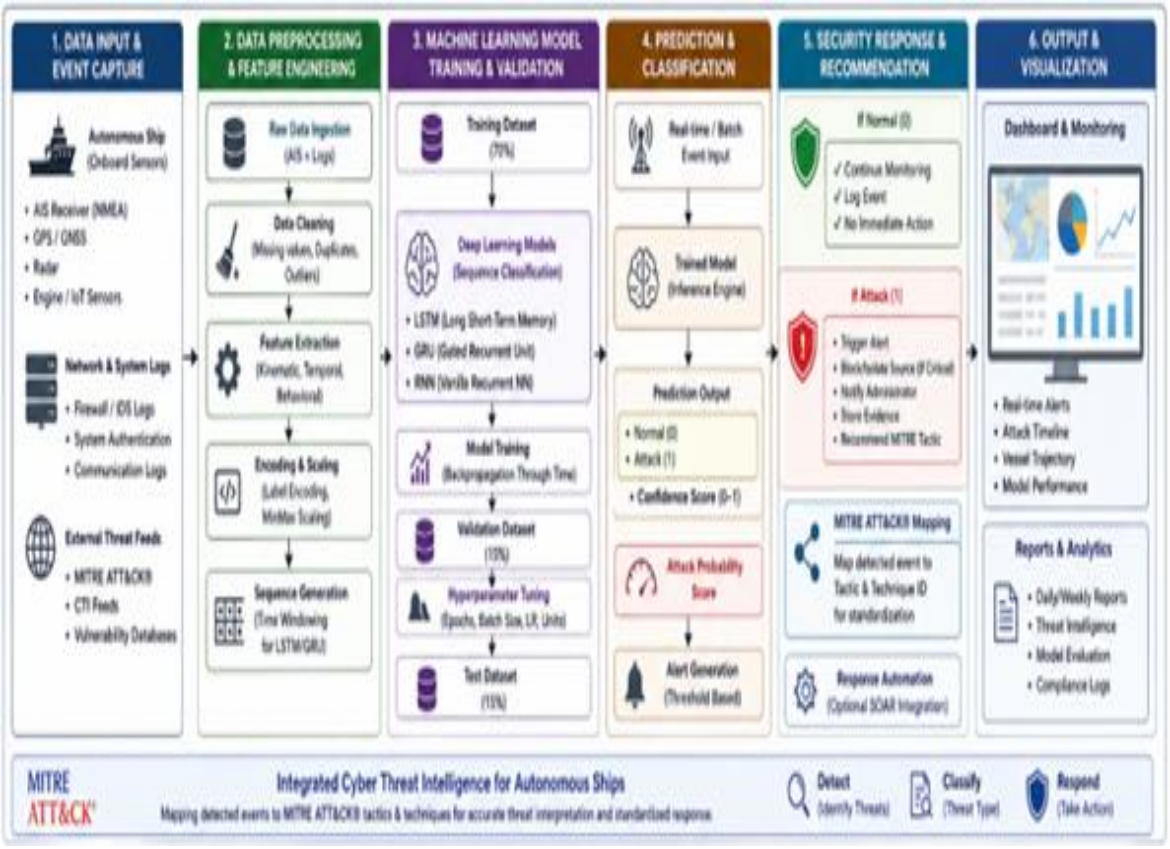

Fig 1: Architecture Diagram

5. MODULES

Maritime Data Collection

As per Fig. 1,This phase serves as the basis for the proposed cybersecurity framework for Maritime Autonomous Surface Ships. Operational and navigational information is gathered primarily from the Automatic Identification System (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 behaviour 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

The raw AIS system experiences communication failures, hardware issues, and other environmental factors. Preprocessing is performed to improve data quality and maximise identification of sensitive data, including abnormal values and inconsistent duplicate entries. For this, effective data normalisation techniques help maintain consistent values across all parameters. It also helps to order and sequence the movements in the system. It minimises noise and organises unstructured data. Proper preprocessing reduces false detections and improves the processing of the vessel's actual behaviour.

Feature Extraction

AIS characteristics require effective cyber detection during the session. Every parameter affects the behaviour of the parameter in the same way as the system used to evaluate performance, electronic fluctuations, route inconsistencies, complexity, timing, and speed. The relationship is used to uncover hidden patterns in movements and may signal threats such as GPS spoofing or issues with map status data. It is important to select the informative variables that minimise the threat. By properly selecting the features that may help easily identify some of the variations that upset the operations

Predictive Cyber-Attack Detection

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

Prediction Output and System Analysis

The system provides better predictions, indicating whether the vessel's 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 assess the model accurately but also helps understand how navigational factors contribute to anomaly detection. This prediction stage completes the workflow by validating the system's effectiveness in addressing cybersecurity risks in autonomous maritime environments through predictive data analysis.

6. RESULT

```
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
```

Fig 2: RNN Test Accuracy

The model achieves high performance, with an overall accuracy of 90.75%, maintaining balanced precision and recall across both attack and defence categories. The confusion matrix and classification report confirm reliable predictions, indicating robust classification capabilities as per Fig. 2.

```
🔄 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
```

Fig 3: GRU Test Accuracy

The GRU model achieves high test accuracy, demonstrating its ability to capture sequential dependencies. Its balanced precision and recall reflect strong generalisation across classes in the classification task as per Fig. 3.

```
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
```

Fig 4: LSTM Test Accuracy

The LSTM model exhibits strong test accuracy, reflecting its ability to learn long-term dependencies in the data. The recall and precision values explain the reliability across all classification categories as per Fig. 4.

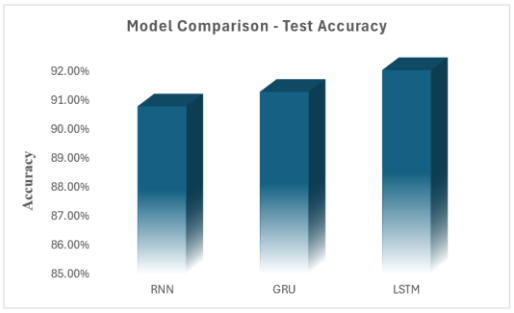

Fig 5: Model Comparison – Test Accuracy

The analysis clearly shows the variety of test accuracy, highlighting that each model has a distinct aptitude for pattern recognition. It not only guides the optimal model but is also tailored to specific classification challenges as per Fig. 5.

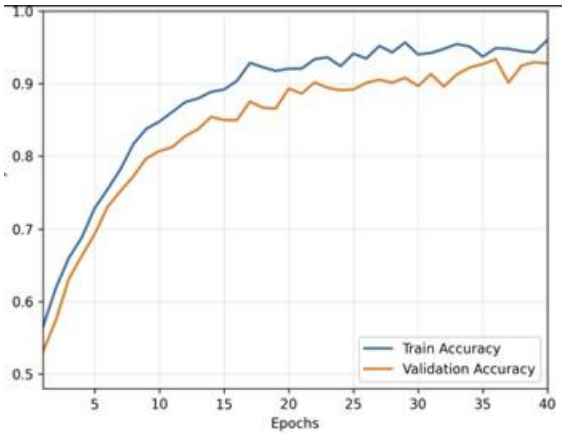

Fig 6: Hybrid LSTM-GRU Training vs Validation Accuracy

This effective learning has been demonstrated by a hybrid LSTM-GRU model that does not overfit, and it aligns with both validation and training accuracy. This balance underscores the robustness of generalisation, helping unseen data during training as per Fig. 6.

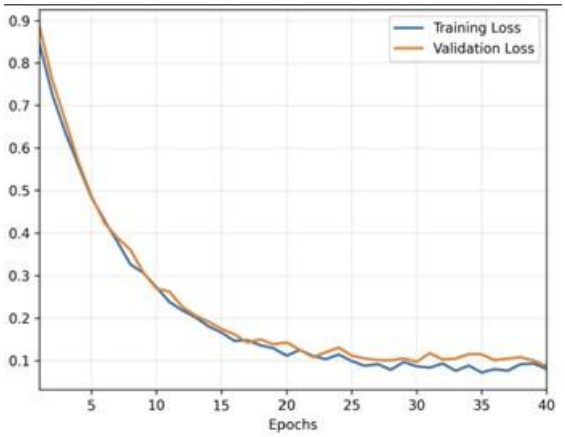

Fig 7: Hybrid LSTM-GRU Training vs Validation Loss

The tuned hybrid model has more stable validation performance with minimised divergence across validation and training loss. It indicates that the model was unable to save the training sequences, but it was simply learning the temporal patterns relevant to maritime cyber threat detection as per Fig. 7.

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

Fig 8: Final Output

From the output, we confirm that the model is not only used for learning but also produces attack-labelled sequences with high-priority recall and acceptable precision. It is particularly relevant for autonomous maritime systems. It is particularly important to understand maritime systems where cyber threats affect route navigation, communication reliability, and decision-making. The results indicate that the proposed system can easily support real-time monitoring by detecting suspicious AIS behaviour 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 as per Fig. 8.

7. FUTURE SCOPE

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

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

REFERENCE

[1] T. Tam and A. Bucknall, “Maritime cyber security: Risks, threats and vulnerabilities,” Journal of Transportation Security, vol. 13, no. 1, pp. 1–15, 2020.

[2] Proceedings of the International Association of Maritime Universities Conference. Massachusetts Maritime Academy. 2024.

[3] J. Liu, Z. Shi, and W. Liu, “AIS data-driven vessel behavior analysis and anomaly detection,” Ocean Engineering, vol. 186, pp. 106–123, 2019.

[4] Y. Tu, G. Zhou, and L. Zhang, “Anomaly detection in AIS trajectories using machine learning techniques,” IEEE Access, vol. 8, pp. 113–125, 2020.

[5] A. D. Tsou, “Maritime situational awareness using AIS and data analytics,” Journal of Navigation, vol. 72, no. 1, pp. 1–19, 2019.

[6] M. Riveiro, G. Falkman, and T. Ziemke, “Visual analytics for maritime anomaly detection,” IEEE Computer Graphics and Applications, vol. 38, no. 4, pp. 42–53, 2018.

[7] S. Ferrari and R. Fierro, “Cyber-physical security in autonomous maritime systems,” IEEE Systems Journal, vol. 14, no. 2, pp. 2345–2356, 2020.

[8] H. Lee, S. Kim, and J. Park, “Machine learning-based intrusion detection for maritime cyber systems,” Sensors, vol. 21, no. 5, pp. 1–17, 2021.

[9] P. Cheng, X. Wang, and L. Zhang, “AIS spoofing detection using statistical and learning-based methods,” Ocean Engineering, vol. 234, pp. 1–12, 2021.

[10] G. Shrivastava, K. Sharma, M. Khari, S.E. Zohora, “Role of cyber security and cyber forensics in India,” In Handbook of research on network forensics and analysis techniques, pp. 143-161. IGI Global Scientific Publishing, 2018.

[11] C. M. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.

[12] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed., Morgan Kaufmann, 2012.

[13] K. P. Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2013.

[14] A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, O’Reilly Media, 2019.

[15] Nanjappan, M., Pradeep, K., Natesan, G. et al. DeepLG SecNet: Utilising deep LSTM and GRU with a secure network for enhanced intrusion detection in IoT environments. Cluster Computing, 27, 5459–5471, 2024.