PureChain-Integrated Optimized ML-Agent for Adaptive Threat Detection in Marine Networks

Mohtasin Golam, Jae-Min Lee, and Dong-Seong Kim
ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea
(golam248, ljmpaul, and dskim)@kumoh.ac.kr

***Abstract*—Marine networks present distinct security challenges due to their complex, distributed infrastructure, limited connectivity, and susceptibility to sophisticated zero-day attacks that often bypass traditional detection mechanisms. This paper introduces a blockchain (PureChain)-integrated optimized machine learning agent model, an adaptive threat detection framework to enable dynamic threat detection and secure collaborative intelligence sharing across distributed marine networks. The ML agent adapts to evolving attack patterns by continuously refining detection policies, while PureChain ensures an immutable and decentralized ledger to manage access control policies and model updates securely, ensuring data integrity and transparency despite connectivity constraints. Experimental results demonstrate the proposed model's superior performance in detecting and classifying maritime-specific threats with 96.3% accuracy while maintaining a low false positive 3.2%, outperforming conventional systems in accuracy by over 2.7%. The proposed framework effectively addresses operational constraints while providing resilient protection against emerging cyber threats, including advanced persistent threats (APTs) that target navigation systems and vessel operational technology.**

***Index Terms*—Adaptive threat detection, PureChain, machine learning agent, and marine networks.**

I. Introduction

Marine networks are essential for facilitating maritime operations, interconnecting components such as vessels, navigation systems, ports, shore-based facilities, and autonomous underwater vehicles. These networks enable critical functions such as real-time tracking, traffic management, and safety systems, supporting global maritime trade. However, the distributed and dynamic nature of these networks, combined with their limited bandwidth and intermittent connectivity, makes them highly susceptible to cyber threats [1]. Traditional security solutions often fail to effectively detect emerging threats, such as advanced persistent threats (APTs) and zero-day attacks, which can evade conventional detection methods. Existing artificial intelligence (AI)-based intrusion detection system (IDS) in maritime environments exhibit substantial shortcomings when confronting sophisticated cyber threats such as APTs and zero-day attacks [2]. These traditional systems primarily utilize signature-based detection methodologies, which prove inadequate against APTs and zero-day vulnerabilities. The main limitation of signature-based detection is that it can only recognize known attack patterns, leaving new threats unidentifiable. The intermittent connectivity characteristic of vessels at sea compromises the effectiveness of centralized security architectures, creating a vulnerable single point of failure (SPoF).

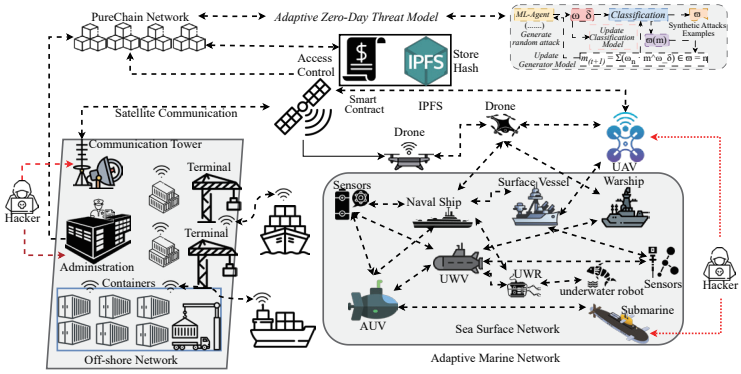

Fig. 1: Architecture of the Proposed PureChain-integrated ML-driven Marine Network

The distributed marine network topology, comprising vessels, ports, and diverse communication channels, requires security solutions that operate autonomously during connectivity lapses while preserving full threat visibility across the entire infrastructure. Navigation systems, operational technology, and safety mechanisms require continuous protection that adapts to evolving threat vectors [1]. Furthermore, maritime IDS implementations generate excessive false positives while demonstrating insufficient responsiveness to emerging threats. While deep learning (DL) and federated learning (FL) have shown promise in improving IDS accuracy, they still face challenges related to high computational costs and privacy concerns. Although FL addresses privacy by decentralizing the training process, it is often vulnerable to SPoF and adversarial model updates, which can degrade its effectiveness [3]. In response to these challenges, this paper introduces a blockchain-integrated optimized ML agent for adaptive threat detection in marine networks. By integrating PureChain technology, the proposed framework ensures a secure, decentralized threat detection model, enhancing data integrity and trust [4]. This approach enables adaptive model refinement while mitigating privacy risks, providing a robust, scalable solution that significantly outperforms traditional IDS in detecting cyber threats within marine networks.

II. Proposed Methodology

The architecture depicted in Fig. 1 consists of multiple marine network entities, including vessels, navigation systems, underwater vehicles, and shore-based facilities, interconnected through heterogeneous communication channels with

TABLE I: Performance comparison on TON-IoT and CICIoT-23 datasets

Model	TON-IoT					CICIoT-23 Dataset				
	Accuracy (%)	Recall (%)	F1-Score (%)	FPR (%)	Loss	Accuracy (%)	Recall (%)	F1-Score (%)	FPR (%)	Loss
Proposed	96.02	96.89	97.16	3.02	0.041	96.31	97.87	96.64	3.27	0.034
[1]	9.73	95.39	96.85	3.28	0.048	96.82	96.71	96.92	3.09	0.033
[2]	94.18	94.85	95.11	3.56	0.047	95.12	95.48	94.87	4.11	0.043
[5]	94.92	94.22	94.76	3.87	0.050	94.53	94.98	94.39	4.33	0.049

intermittent and bandwidth-constrained connectivity. The ML agent employs an optimized classification model trained on diverse marine cybersecurity datasets to recognize and classify evolving attack patterns dynamically. The agent's optimization objective can be formulated as minimizing the composite loss function. The ML agent minimizes a composite loss function combining classification error, regularization, and adaptation terms to continuously refine detection policies $_d$ via gradient-based updates, thereby dynamically adjusting to emerging attack patterns. The ML-agent-based model updates $\triangle m_\delta^\omega$ from distributed nodes are securely validated and aggregated through the PureChain blockchain using a trust-weighted sum: $m_{t+1} = \overset{\varpi}{_{n=1}} {}_n m_\delta^\omega \in = n$, where, m_δ trust weights assigned based on node reliability and m_δ^ω are the model parameters (e.g., weights and biases). To overcome connectivity constraints and prevent SPoF, PureChain integrates a Proof-of-Authority-And-Association (PoA^2) [4] consensus mechanism that ensures fast, secure consensus among authorized marine network nodes. Smart contracts enforce access control mechanisms, preserving data integrity and authorized sharing within an immutable ledger. This blockchain-enabled aggregation removes SPoF and adversarial risks, enabling resilient collaborative intelligence sharing. The system iteratively performs local detection, incremental training, secure update submission, consensus validation, and global policy dissemination, providing a scalable, secure, and adaptive threat detection solution optimized for connectivity-constrained marine environments.

III. Performance Evaluation

The performance evaluation of the proposed model was conducted using two benchmark datasets, TON-IoT [6] and CICIoT-23 [5], both of which are widely recognized for cybersecurity research. The TON-IoT dataset comprises telemetry, network traffic, and system log data collected from various IoT devices, offering a comprehensive range of attack scenarios, including DoS, DDoS, and ransomware. In contrast, the CICIoT-23 dataset focuses on IoT network traffic in smart environments and features up-to-date attack types, such as botnets, reconnaissance, and infiltration attempts, with detailed flow-based features.

A. Threat Detection Performance Validation

The experimental evaluation of the proposed model demonstrates its efficacy in enhancing threat detection capabilities within marine networks. As shown in Table I, the proposed model achieves an accuracy of 96.02% on the TON-IoT and 96.31% on the CICIoT-23 dataset, outperforming baseline methods by up to 2.6%. Notably, the model obtains high recall values of 96.89% and 97.87%, alongside F1-scores of 97.16% and 96.64% on the respective datasets, indicating robust detection and classification performance across varying attack scenarios. Furthermore, the model maintains a low false positive rate (FPR) of 3.02% and 3.27%, thereby minimizing erroneous detection, which is critical for operational reliability in distributed marine environments. The loss metrics remain consistently low (0.041 and 0.034), underscoring the stability and generalization of the detection framework. The proposed approach offers a resilient and scalable solution for mitigating advanced persistent threats (APTs) and zero-day attacks, thereby enhancing the security of maritime systems.

IV. Conclusion and Future Work

The proposed PureChain-integrated ML agent framework effectively addresses marine network security vulnerabilities by implementing a decentralized architecture that eliminates SPoF while maintaining 96.02-96.31% detection accuracy across benchmark datasets. Experimental results demonstrate a 2.6% performance improvement over baseline methods with consistently low false positive rates (3.02-3.27%) and loss metrics (0.034-0.041). The PureChain integration enables secure adaptive detection mechanisms that counter APTs and zero-day attacks. This approach balances computational efficiency with detection performance, creating a resilient security solution optimized for the distributed and connectivity-constrained nature of maritime operational technology environments.

V. Acknowledgment

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korean government (MSIT) (IITP-2025-RS-2020-II201612, 50%) and by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003 50%).

References

[1] A. Zainudin, R. N. Alief, M. A. P. Putra, R. Akter, D.-S. Kim, and J.-M. Lee, "Blockchain-based decentralized trust aggregation for federated cyber-attacks classification in sdn-enabled maritime transportation systems," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2023, pp. 182–187.

[2] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Zero-trust marine cyberdefense for iot-based communications: An explainable approach," *Electronics*, vol. 13, no. 2, p. 276, 2024.

[3] M. Golam, M. M. Alam, D.-S. Kim, and J.-M. Lee, "Blm-chain: Ai-driven blockchain for uav threat resistance in iobt," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2024, pp. 1609–1613.

[4] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-authority-and-association consensus algorithm for iot blockchain networks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2025, pp. 1–6.

[5] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023.

[6] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion detection system using machine learning for vehicular ad hoc networks based on ton-iot dataset," *IEEE access*, vol. 9, pp. 142 206–142 217, 2021.