Advances in Human Factors of Transportation, Vol. 186, 2025, 644–655
https://doi.org/10.54941/ahfe1006554

Enhancing Data Privacy in Maritime Operations With Federated Learning: A YOLOv8 Object Detection Approach

Vo Ngoc Thy Thao Vo, Amin Majd, Mehdi Asadi, Juha Kalliovaara, Tero Jokela, and Jarkko Paavola

Turku University of Applied Sciences, Turku, Finland

ABSTRACT

The maritime industry is currently experiencing a period of rapid transformation, driven by the integration of artificial intelligence (AI) technologies. This integration is enabling advancements in autonomous navigation systems, remote monitoring capabilities, and operational efficiency. However, these innovations are accompanied by substantial privacy challenges, particularly in the management of sensitive data collected from vessels. In this work, we propose a Federated Learning (FL) framework tailored for the maritime environment. This framework aims to address privacy concerns while leveraging the capabilities of AI. Utilizing the TUAS dataset, which contains images, and employing the YOLOv8 object detection model, we demonstrate how FL enables vessels to collaboratively train robust machine learning models without sharing raw data. Our approach ensures that data collected on vessels, such as images for navigation and object detection, remains onboard, thereby safeguarding sensitive information. Each vessel trains a local YOLOv8 model on its image dataset and shares encrypted model updates with a central server for aggregation. This global model is then disseminated back to the vessels, ensuring enhanced performance across the fleet without compromising data privacy. A comparison of our FL-based approach to traditional centralized training methods is presented, highlighting the trade-offs in model accuracy, privacy preservation, and communication overhead. The findings demonstrate that FL with YOLOv8 attains object detection performance that is competitive with other methods, while addressing privacy concerns by keeping raw image data localized. Integrating FL into the maritime industry provides a scalable and secure solution for AI-powered applications, ensuring data privacy while promoting innovation. Experimental result is a substantial contribution to the development of privacy-preserving AI solutions for autonomous maritime operations and remote monitoring, demonstrating FL's potential to transform the maritime industry.

Keywords: Federated learning, Maritime AI, YOLOv8, Privacy-preserving AI, Autonomous navigation, Object detection, Remote monitoring, Decentralized machine learning, Secure AI training, Maritime surveillance

INTRODUCTION

FL is a decentralized machine learning approach that enables collaborative model training across multiple entities without requiring the sharing of raw data. This privacy-preserving framework is particularly well-suited for the maritime industry, where data sensitivity and operational confidentiality are critical considerations (Khan et al., 2022). Artificial intelligence (AI) has revolutionized the maritime sector by enhancing safety, efficiency, and operational effectiveness. However, its implementation is often impeded by privacy concerns and the inherently distributed nature of maritime data sources. FL is a machine learning method that minimizes privacy risks by enabling local model training in the maritime industry. It mines information from identically distributed datasets, eliminating the need for centralized data collection. Clients train models using their own data, and updated parameters are transmitted back to a central server for global parameter updates.

The Federated Averaging (FedAvg) algorithm, introduced by McMahan et al. (2017), is a foundational method in FL and forms the basis for most subsequent research in this field. FedAvg is a simple yet effective aggregation rule used in collaborative model training to achieve a globally accurate model through iterative communication, ensuring data privacy while facilitating updates from all participating clients.

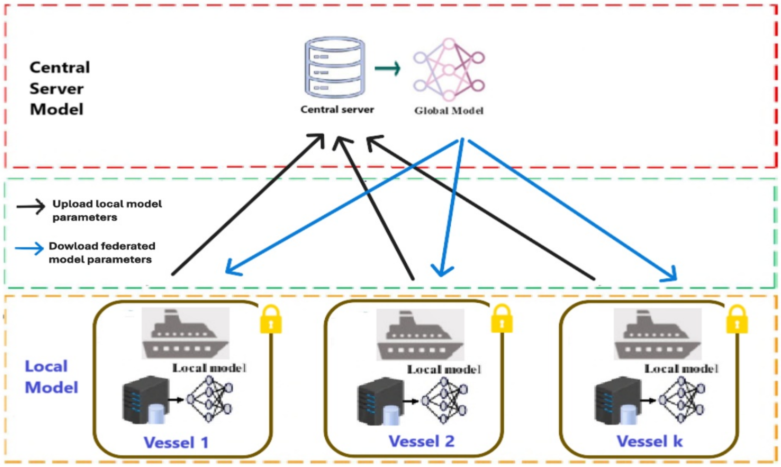


Figure 1: Workflow of a FL architecture in maritime industry.

The maritime industry is a critical sector that requires the protection of sensitive data from various stakeholders, including ship operators, ports, logistics providers, and regulatory authorities. Key aspects of privacy include operational privacy, commercial privacy, personal data protection, regulatory compliance, and security concerns (Graser, 2021). Operational privacy involves maintaining confidentiality of ship routes, cargo manifests, fuel consumption, and maintenance schedules, while commercial privacy protects trade secrets and financial transactions. Security concerns involve mitigating cyberattack risks.

FL, a privacy-preserving mechanism, is crucial for maritime applications like fuel consumption prediction, anomaly detection, and predictive maintenance. It allows ship operators to share fuel efficiency insights without revealing proprietary operational details, promoting collective optimization (Li, 2020). FL enhances situational awareness and safety in maritime operations by facilitating secure and efficient collaboration among stakeholders, as illustrated in Figure 1.

Despite its potential, FL faces challenges such as data variability between vessels and communication overhead during model aggregation, which may limit its scalability. Nonetheless, FL provides a robust solution to protect sensitive maritime data while promoting innovation and collaboration within the industry.

The study explores the use of FL to address privacy concerns in the maritime industry, focusing on safeguarding sensitive operational data in the era of AI integration. It uses the TUAS dataset and YOLOv8 object detection model to demonstrate how FL allows vessels to train machine learning models locally while sharing encrypted updates for centralized aggregation. FL's robust object detection makes it suitable for applications like autonomous navigation, remote monitoring, and operational optimization. The findings contribute to the advancement of privacy-preserving AI solutions in the maritime sector.

The rest of the paper is structured as follows: **Section 2** discusses the theoretical background and related work, focusing on FL concepts and their challenges in maritime applications. **Section 3** details the methodology for the FedAvg algorithm, including its design, collaborator selection, and weight aggregation. **Section 4** provides an in-depth analysis of the dataset, its experimental setup, and the specifics of its implementation. **Section 5** provides an evaluation of the results and advantages of FL in maritime applications. **Section 6** of the paper provides a summary of the findings, their implications for the maritime industry, and future research directions.

BACKGROUND

This section explores the application of FL in autonomous systems and the maritime industry, examining previous methodologies, their limitations, and highlighting the motivation behind our proposed approach. FL is a popular method for training machine learning models collaboratively while maintaining data privacy. The basis for FL, a decentralized learning paradigm that combines local model updates to create a global model while preserving local data privacy (Li, 2018). Improved FedAvg by introducing a proximal term in the local objective function to mitigate non-IID data effects.

Autonomous systems, including autonomous vehicles, utilize robust machine learning models for navigation, anomaly detection, and decision-making, with FL leveraging distributed data while maintaining data privacy. Lu et al. (2019) and Brik et al. (2020) used FL in autonomous vehicles and drones for traffic prediction and object detection, demonstrating its effectiveness in reducing communication costs and improving model accuracy, while also mitigating privacy concerns and enabling data sharing across devices.

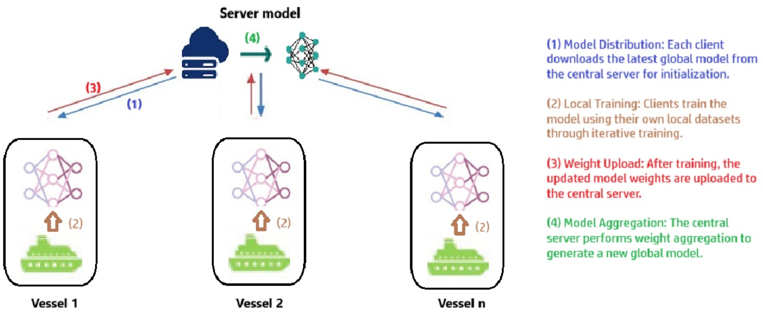
The maritime industry presents unique challenges for FL due to decentralized vessels, non-IID data distributions, and data privacy. FL has been used in marine navigation systems and anomaly detection, but convergence challenges arise due to heterogeneity in maritime data. Improved aggregation techniques are needed to handle diverse and non-IID data distributions. FLCSDet, a cross-spatial vessel detection framework, enhances accuracy while preserving privacy and addressing data aggregation and heterogeneity issues. FL enables decentralized model training for maritime vessels operating independently and in remote locations, enhancing data privacy and preventing centralized access and breaches. Techniques like Federated Entropy Pooling (FedEP) can address these issues by utilizing local data distribution statistical characteristics for improved model aggregation.

The adaptability of FL and YOLOv8 in promoting real-time decision-making and privacy preservation is further demonstrated by applications in driverless cars. YOLOv8 is optimized for object detection in vehicular networks, as shown by Quéméneur and Cherkaoui (2024), improving the capabilities of autonomous cars in real-time situations. Additionally, FL makes it possible to train models without sending sensitive data, which is essential for protecting user privacy in ecosystems of connected vehicles (Quéméneur and Cherkaoui, 2024).

Section 2 explores the use of FL concepts in the maritime industry, highlighting their potential to address privacy concerns and improve operational efficiency. Key applications include navigation systems, anomaly detection, and environmental monitoring. However, challenges with handling non-IID data distributions and model resilience persist. Advanced aggregation methods and encryption technologies are crucial. Section 3 examines a proposed methodology using YOLOv8 and FL to address these issues.

METHODOLOGY

This chapter explores the use of the FedAvg algorithm and YOLOv8 object detection model to improve detection capabilities while maintaining data privacy. It covers preprocessing, model architecture, FL setup, FeDAvg aggregation method, and performance evaluation metrics for the Turku UAS DeepSeaSalama GAN dataset (Asadi et al., 2024). The FedAvg algorithm is a decentralized model training system that enhances FL effectiveness and efficiency, especially in distributed and private data settings. The algorithm operates in the following steps and illustrated in Figure 2.



(1) Model Distribution: Each client downloads the latest global model from the central server for initialization.

(2) Local Training: Clients train the model using their own local datasets through iterative training.

(3) Weight Upload: After training, the updated model weights are uploaded to the central server.

(4) Model Aggregation: The central server performs weight aggregation to generate a new global model.

Figure 2: Overview of the general FL framework.

Clients download the latest global model for initialization and perform local training using their private datasets. After training, updated model weights are uploaded to the server for weighted aggregation, generating a new global model. This updated model is redistributed to all clients for the next round, repeating until convergence.

FedAvg is a machine learning algorithm that prioritizes efficient training and privacy preservation. It reduces communication overhead by computing weights locally during training rounds and uploading them to the cloud after a defined interval. Only learned parameters are shared with the central server, ensuring decentralized and private raw data. However, it lacks theoretical convergence guarantees and can diverge in practical settings (Prashant et al., 2023; Oudarja et al., 2023; Xin et al., 2023). The FeDAvg algorithm aggregates model updates across multiple clients using the formula (1) as following:

$$\mathbf{w}^{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} \cdot \mathbf{w}_i^t \tag{1}$$

Where: w^{t+1}: the updated global model weights after aggregation in round t + 1; w_i^t: The local model weights of the i-th client after local training in round t; n_i: The number of training samples held by the i-th client; $n = \sum_{i=1}^{n} n_i$: The total number of training samples across all clients; N: The total number of participating clients; t: The time slot for the aggregation step, which is an integer multiplier of E (the number of local epochs before aggregation).

The Turku UAS DeepSeaSalama GAN dataset (TDSS-G1) is a collection of synthetic and real maritime images captured under various environmental conditions using GANs. Collaborators are assigned a distinct subset of the dataset, simulating real-world FL conditions with data distribution and privacy (Asadi et al., 2024; Kalliovaara, 2024).

This study uses YOLOv8, a more advanced version of the YOLO series, for instance segmentation, object identification, and image classification. Unlike other object detection algorithms, YOLOv8 uses a deep convolutional neural network to process an entire image in a single forward pass. The YOLO algorithm segments an input image into an S × S grid, predicting predefined bounding boxes for each grid cell. It calculates class probabilities and confidence scores, indicating the likelihood of an object within a bounding box. Non-Maximum Suppression (NMS) is a crucial enhancement to refine detection accuracy.

The integration of FL with YOLOv8 involves a distributed target detection system where multiple devices collaborate to train a shared YOLOv8 model. This method ensures localized data, reduces central storage, and enhances privacy. The process begins with configuring the YOLOv8 model and selecting an appropriate FL framework. Data is distributed across local devices, with privacy-preserving mechanisms. The FL framework controls model updates and communication protocols, improving the global model's accuracy and robustness. The trained models are deployed for real-time inference in target detection tasks, followed by performance evaluation and optimization.

The study incorporates YOLOv8 into the FedAvg algorithm implementation methodology, enhancing detection accuracy and efficiency. The FedAvg framework, including design, collaborator selection, and weight aggregation strategies, is used to ensure robust performance in maritime object detection and classification under diverse conditions.

IMPLEMENTATION AND EXPERIMENTS

The Turku UAS DeepSeaSalama - GAN (TDSS-G1) dataset is a maritime dataset designed for object detection and classification in marine environments. It combines real-world maritime images with synthetic images generated through GANs, enhancing diversity and robustness. The dataset is annotated with multi-label information, including item categories, bounding box coordinates, and environmental metadata, ensuring reliable training data. It was created by extracting images from MPEG format videos at a 100 millisecond extraction rate and 720p resolution. The distribution of labels within the dataset is as follows: motorboats (62.1%), sailing boats (16.8%), and seamarks (21.1%) (Asadi et al., 2024). Despite the advantages of synthetic data augmentation, the TDSS-G1 dataset faces challenges such as data heterogeneity, class imbalance, and adverse real-world conditions. Variability in object size, shape, and environmental factors, including low visibility conditions, complicates detection. Additionally, the overrepresentation of larger cargo ships introduces class imbalance, negatively impacting model accuracy. To address these issues, robust preprocessing techniques such as adaptive contrast enhancement are used to improve model generalization, particularly in low-visibility scenarios.

The study uses a privacy-preserving distributed training setup called FL to train local models independently on edge devices like autonomous maritime vessels. The devices train local models independently and share encrypted updates with a central server, preserving sensitive data privacy. The aggregation of local model updates is achieved using FedAvg, while efficient data exchange is facilitated through the Message Passing Interface. Federated training is implemented using frameworks like PyTorch, TensorFlow Federated, and OpenMPI, with optimization techniques like adaptive learning rate decay and weighted aggregation.

Hybrid encryption techniques, combining symmetric AES encryption for model gradients and public-key cryptography for secure communication, are used in the TDSS-G1 dataset. YOLOv8, a state-of-the-art object detection model, is used for its speed and accuracy, extracting maritime features and predicting bounding box coordinates and object classifications. Training involves YOLO loss for bounding box regression and cross-entropy loss for classification. The YOLOv8 model is evaluated using metrics like Mean Average Precision (mAP), communication overhead, inference speed, and model convergence to assess its accuracy and efficiency. However, challenges like domain shifts between real and synthetic images persist. Domain adaptation techniques like adversarial training improve robustness across different data sources. Oversampling and focal loss address class imbalance, detecting underrepresented object classes more effectively. Weight pruning and model compression optimize communication efficiency, reducing model updates size without sacrificing accuracy. The experimental setup uses a FL framework to train a global object detection model using the YOLO architecture across multiple clients, aiming to simulate a decentralized learning environment where clients train locally on private datasets and share model updates with a central server.

The YOLO model is trained locally using PyTorch for a specific number of epochs, with parameters like image size, batch size, and optimizer configuration defined through command-line arguments. The global model is distributed to all clients at the beginning of each federated round, with the latest checkpoint loaded if a client has a previously trained model. Each client fine-tunes the model using local data, and updated parameters are sent back to the central server. The system monitors results and compiles global performance statistics, providing insights into the model's learning behavior across clients.

The study uses the TDSS-G1 dataset, YOLOv8, and FL to improve real-time maritime object detection and classification. It overcomes challenges like data imbalance, heterogeneity, and adverse environmental conditions. The proposed framework demonstrates decentralized, real-time surveillance for intelligent maritime navigation systems, with FL facilitating privacy-preserving training and communication-efficient updates. This work lays the groundwork for future maritime monitoring systems that are privacy-conscious and effective in complex, dynamic environments. The experimental results are evaluated across various scenarios.

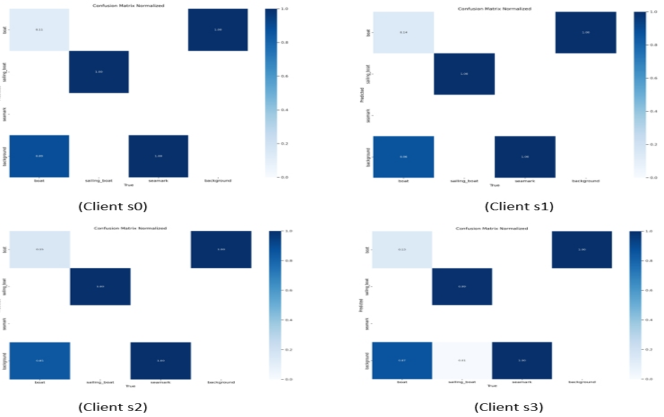
RESULTS

The study evaluates a proposed object detection model for maritime applications using traditional training and a FL framework. The model aims to predict bounding boxes and classify object labels in maritime environments while maintaining data privacy. The TDSS-G1 dataset was used for training, validation, and test sets. The model was trained for 10 epochs across four FL clients, with parameter optimization for performance. The FL framework allowed each client to train locally, maintaining data control and contributing to a globally optimized model crucial in maritime operations.

Table 1: Federated learning model performance metrics on TDSS-G1 by client.

Client	Train Box Loss	Train Classification Loss	Train DFL Loss	Precision (B)	Recall (B)	mAP 50 (B)
SO	1.2065	0.94665	0.79625	0.84018	0.39328	0.41109
S1	1.2218	0.98624	0.79429	0.84378	0.39773	0.4177
S2	1.2419	0.96985	0.79737	0.83629	0.39546	0.40676
S3	1.2736	0.94589	0.79228	0.83296	0.39365	0.40833

Table 1 assesses a FL model's performance on the TDSS-G1 dataset, focusing on key metrics like train box loss, train classification loss, train DFL loss, precision, recall, and mean average precision. Client S1 demonstrated superior accuracy and sensitivity in object detection, but the mAP 50–95 metric revealed greater variability, indicating uniform performance across all clients. Further insights were gained from the analysis of normalized confusion matrices (Figure 3), which reveal significant local shortcomings in detecting the "boat" class. Recall values were notably low across clients—11% for Client S0, 14% for Client S1, 15% for Client S2, and 13% for Client S3—indicating that the majority of actual boat instances were missed. These low recall values and high false negative rates indicate that each client's local model misses the majority of actual boat instances.



(Client s0)

(Client s1)

(Client s2)

(Client s3)

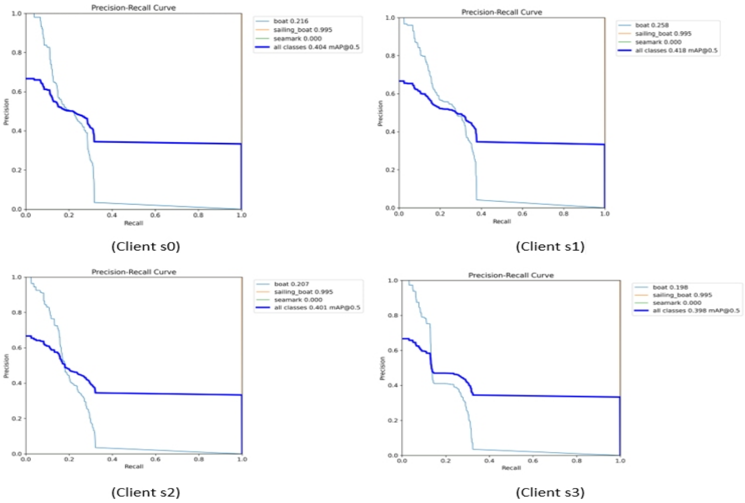
Figure 3: Normalized confusion matrices of local models for clients s0–s3.

The study indicates that local data limitations, including insufficient boat examples, data bias, and labeling noise, are affecting model performance, highlighting the need for local and global data augmentation strategies, balanced data collection, and careful monitoring.

This performance variability across clients underscores the importance of privacy-preserving collaborative learning in maritime applications. The decentralized nature of FL ensures that local models can be continuously refined using aggregated global knowledge without ever exposing raw data. This approach mitigates the risk of data leakage in highly sensitive maritime operations, such as vessel tracking, port security, and naval surveillance.

The YOLOv8 model shows exceptional detection of the "sailing_boat" class, achieving near-perfect Average Precision scores across all clients. This is crucial for maritime situational awareness and operational safety. The "boat" class shows a decline in precision as recall increases, while the "seamark" class achieves an AP of 0.000. These trends demonstrate the effectiveness of the FL framework in preserving data privacy and providing insights for targeted improvements through collaborative learning, data augmentation, and model updates.

Building on these findings, Figure 5 presents the Precision-Confidence curves for each client, further validating the effectiveness of our YOLOv8 approach in a privacy-preserving FL setup. Despite variations in local data, all clients achieve near-perfect precision for the “sailing_boat” class across various confidence thresholds, underscoring the model’s capability to accurately detect key maritime objects without centralized data storage. While the curves for the “boat” and “seamark” classes indicate lower performance, they also reveal opportunities for future enhancements via collaborative model aggregation—ensuring that local data peculiarities are balanced out to enhance global detection capabilities.



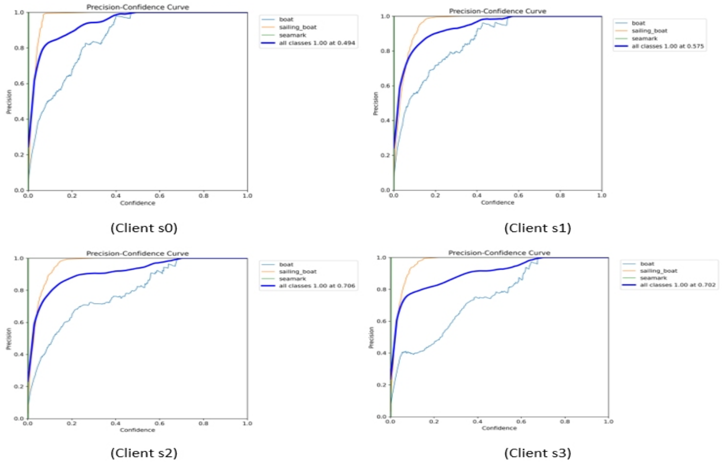
(Client s0)

(Client s1)

(Client s2)

(Client s3)

Figure 4: Precision-recall curves for local models (clients s0–s3).



(Client s0)

(Client s1)

(Client s2)

(Client s3)

Figure 5: Precision-confidence curves for maritime object detection (Clients s0–s3).

The YOLOv8 model, a FL framework, has been tested for maritime object detection, showing robust performance and data privacy. It is effective in detecting the “sailing_boat” class, crucial for maritime safety. However, challenges persist for the “boat” and “seamark” classes due to local data heterogeneity. Future improvements include adaptive model aggregation and targeted data augmentation. Further research should focus on reducing local performance variability, refining model aggregation strategies, and improving detection capabilities for underrepresented classes.

DISCUSSION

The study tested a YOLOv8-based object detection model for maritime applications using the TDSS-G1 dataset. It showed exceptional performance in detecting the “sailing_boat” class, achieving near-perfect Average Precision scores. This robust detection is crucial for maritime situational awareness and operational safety, ensuring key objects are reliably identified while preserving sensitive maritime data. The FL framework, despite its promising results, faced challenges in detecting other maritime classes, particularly the “boat” class due to data heterogeneity, imbalances in training examples, and potential issues with data quality. However, the federated approach safeguards sensitive information and leverages diverse local datasets to enhance detection capabilities.

The proposed object detection model, trained using a FL framework, has the potential to revolutionize maritime applications by improving accuracy, efficiency, and security in real-time object detection systems. It enhances decision-making and situational awareness in dynamic maritime environments and enables rapid deployment across distributed networks. Future research should focus on underrepresented classes like boats and seamarks, adopting advanced data augmentation techniques, comprehensive data audits, and adaptive model aggregation methods.

The study suggests that YOLOv8, when integrated with a federated learning framework, provides a promising and privacy-preserving solution for maritime object detection. However, challenges with boat and seamark detection highlight the need for further research and refinement. Addressing data imbalances and using adaptive aggregation techniques are crucial for improving detection capabilities and operational efficiency in real-time maritime surveillance systems.

ACKNOWLEDGMENT

The authors would like to express their gratitude to TUAS for providing the necessary resources and infrastructure to conduct this research. We extend our appreciation to our colleagues and mentors for their valuable insights and constructive feedback, which greatly contributed to improving this work. Finally, we would like to thank the research community for their continuous efforts in advancing FL and object detection methodologies, which served as the foundation for our work.

REFERENCES

Asadi, M., Majd, A., Auranen, J., & Turku University of Applied Sciences. (2024). The Turku UAS DeepSeaSalama - GAN dataset 1 (TDSS-G1) (1.0) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.10714823

Brik, Bouziane & Bouaziz, Maha & Ksentini, Adlen. (2020). Federated Learning for UAVs-Enabled Wireless Networks: Use Cases, Challenges, and Open Problems. IEEE Access. 8. 53841–53849. 10.1109/ACCESS.2020.2981430.

Daryn, Monteiro., Ishaan, Mavinkurve., Parth, Kambli., Prof., Sakshi, Surve. (2024). Federated Learning for Privacy-Preserving Machine Learning: Decentralized Model Training with Enhanced Data Security. International Journal for Research in Applied Science and Engineering Technology, doi: 10.22214/ijraset.2024.65062.

Duong, A.-K., La, T.-V., Lê, H. An, & Pham, M.-T. (2024). FedShip: Federated learning for ship detection from multi-source satellite images. IEEE Geoscience and Remote Sensing Letters.

Giannopoulos, A., Gkonis, P., Bithas, P., Nomikos, N., Ntroulias, G., & Trakadas, P. (2023). Federated Learning for Maritime Environments: Use Cases, Experimental Results, and Open Issues. https://doi.org/10.36227/techrxiv.22133549.v1

Graser, F., Teixeira, A., & Bruhn, W. (2021). Cybersecurity and data privacy in the maritime sector: Challenges and solutions. Maritime Policy & Management, 48(7), 935–948. https://doi.org/10.3390/network2010009

Huang, Y., Liu, W., Lin, Y., Kang, J., Zhu, F., & Wang, F.-Y. (2025). Flcsdet: Federated Learning-driven cross-spatial vessel detection for maritime surveillance with privacy preservation. IEEE Transactions on Intelligent Transportation Systems, 26(1), 1177–1192. https://doi.org/10.1109/tits.2024.3488497

Kalliovaara, J., Jokela, T., Asadi, M., Majd, A., Hallio, J., Auranen, J., Seppänen, M., Putkonen, A., Koskinen, J., Tuomola, T., Mohammadi Moghaddam, R., & Paavola, J. (2024). Deep Learning Test Platform for Maritime Applications: Development of the eM/S Salama Unmanned Surface Vessel and Its Remote Operations Center for Sensor Data Collection and Algorithm Development. Remote Sensing, 16(9), 1545. https://doi.org/10.3390/rs16091545

Khan, M. I., Jafaritadi, M., Alhoniemi, E., Kontio, E., & Khan, S. A. (2022). Adaptive Weight Aggregation in Federated Learning for Brain Tumor Segmentation. In Lecture Notes in Computer Science (Vol. 12963, pp. 455–469). (Lecture Notes in Computer Science). Springer International Publishing AG. https://doi.org/10.1007/978-3-031-09002-8_40.

Lee, H., Kim, J., & Song, Y. (2022). Federated anomaly detection in maritime operations: A privacy-preserving approach. Journal of Maritime Research, 50(7), 345–356. https://doi.org/10.3390/electronics13193912

Li, L., Fan, Y., Tse, M., & Lin, K.-Y. (2020). A review of applications in Federated Learning. Computers & Industrial Engineering, 149, 106854. https://doi.org/10.1016/j.cie.2020.106854

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2018). Federated optimization in heterogeneous networks. Proceedings of the 27th International Conference on Machine Learning (ICML), 1232–1241. https://doi.org/10.48550/arXiv.1812.06127

Lu, H., Zhang, H., & Li, W. (2019). Federated learning for autonomous vehicle traffic prediction. IEEE Transactions on Intelligent Transportation Systems, 20(12), 4204–4216. 10.1109/TITS.2019.2935152

Majd, A., Asadi, M., Kalliovaara, J., Jokela, T., & Paavola, J. (2024). Navigating the seas of automation: Human-informed synthetic data augmentation for enhanced Maritime Object Detection. AHFE International. https://doi.org/10.54941/ahfe1005004

McMahan, B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), PMLR, 54, 1273–1282. https://doi.org/10.48550/arXiv.1602.05629

McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 1273–1282. https://doi.org/10.48550/arXiv.1602.05629

Oudarja, Barman, Tanmoy., Md., Al, Mamun., Sakib, Hasan., Adnan, Anwar. (2023). Enhancing Federated Learning with Globally Shared Model: A Modified FedAVG Approach (GSM-FedAVG). 1–6. doi: 10.1109/eict61409.2023.10427600

Peng, R. (2024). Federated learning-based yolov8 for face detection. Applied and Computational Engineering, 54(1), 14–20. https://doi.org/10.54254/2755-2721/54/20241137

Prashant, Khanduri., B., N., Bharath. (2023). FedAvg for Minimizing Polyak-Łojasiewicz Objectives: The Interpolation Regime. 607–613. doi: 10.1109/ieeeconf59524.2023.10476970.

Quéméneur, C., & Cherkaoui, S. (2024, June 5). *Fedpylot: Navigating Federated Learning for real-time object detection in internet of vehicles*. arXiv.org. https://arxiv.org/abs/2406.03611

S. Bharti and A. Mcgibney, "Privacy-aware resource sharing in crossdevice federated model training for collaborative predictive maintenance," IEEE Access, vol. 9, pp. 120367–120379, 2021.

Sathwik, Narkedimilli., A., Sriram., Sanjay, Raghav. (2024). FL-DABE-BC: A Privacy-Enhanced, Decentralized Authentication, and Secure Communication for Federated Learning Framework with Decentralized Attribute-Based Encryption and Blockchain for IoT Scenarios. doi: 10.48550/arxiv.2410.20259.

Ultralytics. (n.d.). *YOLOv8: Comparison of SOTA object detectors*. Ultralytics. Retrieved February 12, 2025, from https://docs.ultralytics.com/models/YOLOv8/comparison-of-sota-object-detectors.

Xin, Liu., Dazhi, Zhan., Wei, Tao., Xin, Ma., Yu, Pan., Yu, Ding., Zhisong, Pan. (2023). A Neural Tangent Kernel View on Federated Averaging for Deep Linear Neural Network. arXiv.org, abs/2310.05495 doi: 10.48550/arxiv.2310.05495.

Z. Zhang, C. Guan, H. Chen, X. Yang, W. Gong and A. Yang, "Adaptive Privacy-Preserving Federated Learning for Fault Diagnosis in Internet of Ships," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6844–6854, 1 May1, 2022. https://doi.org /10.1109/JIOT.2021.3115817

Z. Zhang, C. Guan, H. Chen, X. Yang, W. Gong, and A. Yang, "Adaptive privacy-preserving federated learning for fault diagnosis in Internet of Ships," IEEE Internet Things J., vol. 9, no. 9, pp. 6844–6854, May 2022.