IEEE Aerospace and Electronic Systems Society Request for Proposals

for

Solutions to IEEE AESS Challenge Problem II:
Cybersecure and Resilient Avionics Operations

Abstract

The IEEE Aerospace and Electronic Systems Society (AESS) invites innovative proposals addressing critical challenges in Cybersecure and Resilient Avionics Operations. This Request for Proposals (RFP) seeks practical, high-impact solutions to advance the cybersecurity, reliability, and autonomy of avionics and unmanned aerial systems operating in contested and resource-constrained environments.

Building on prior work, this initiative emphasizes the development of lightweight, real-time, and data-efficient approaches for detecting, mitigating, and recovering from cybersecurity and operational threats. Key areas include cyber anomaly detection, resilient communication, robust federated learning, adaptive swarm coordination, and deployable artificial intelligence for constrained platforms.

Proposers are encouraged to develop proof-of-concept solutions that demonstrate measurable performance, scalability, and integration with real-world avionics or UAV systems. Participants will utilize the existing open-source federated learning framework (https://github.com/I-Fusion/drift-fairroad/tree/v2), whose development was funded by the AESS. This framework provides datasets, tools, and evaluation infrastructure to accelerate development and assessment of solutions on common scenarios and challenges.

Selected proposals will receive funding support and the opportunity to present their work at leading IEEE conferences, contributing to the advancement of cybersecure and resilient aerospace systems. This effort aims to foster innovation, collaboration, and transition of research into practical capabilities that enhance the cybersecurity and safety of next-generation aviation platforms.

1. Introduction

The IEEE AESS has advanced its mission to enhance the cybersecurity and resilience of avionics operations with the second phase of a multi-stage initiative. AESS now calls for innovative solutions to address pressing threats. As part of a prior effort, Intelligent Fusion Technology developed an extensive federated learning framework, see details in Appendix A. A related publication is attached in Appendix B.

2. Objectives

This Request for Proposals (RFP) solicits solutions for challenges in Cybersecure and Resilient Avionics Operations. The challenge problems address critical areas for avionics including cybersecurity, artificial intelligence, resilience, and operations.

Participants are encouraged to propose innovative solutions, focusing on proof-of-concept prototypes with measurable outcomes. Submissions should demonstrate practical implementations for UAV or avionics systems, ensuring resilience and safety under real-world operating conditions.

Participants are required to utilize the federated learning framework and resources provided at https://github.com/I-Fusion/drift-fairroad/tree/v2.

Challenge Problems for IEEE AESS: Cybersecure and Resilient Avionics Operations

This section outlines the challenges for which proposers can provide solutions.

Challenge 1: Real-Time Detection and Resilient Mitigation of Cyber Attacks in Avionics Systems

Design efficient, lightweight, and real-time systems for detecting and mitigating cyber-attacks in avionics platforms under resource-constrained conditions. Solutions must achieve a balance between detection accuracy and low false alarm rates while enabling rapid recovery and continued safe operation.

The system should support distributed, data-efficient learning and operate across both onboard endpoints and communication channels. While the framework should generalize to a broad class of cyber threats, GNSS (GPS) or communications spoofing and jamming attacks serve as example scenarios for validation.
Key Focus Areas:

- Real-time anomaly detection with lightweight models and low false alarms.
- Attack detection (spoofing/jamming) via signal and/or sensor validation.
- Secure, efficient communication with compressed updates.
- Robust, scalable design for multiple threats with graceful degradation.

Challenge 2: Lightweight AI for Avionics and Resource-Limited UAVs

Develop deployable AI solutions optimized for avionics and drones operating under resource constraints.
Proposals should emphasize efficient algorithms that fit the operational limits of avionics and UAV systems, including memory, computational overhead, and energy-consumption.
Practical solutions should also consider mission-critical responsibilities like real-time local

inference and communication during diverse tasks.
Key Focus Areas:

- Model compression and energy-aware architectures.
- On-device feature engineering for reduced flight-time computational load.
- Benchmark testing environments using time-series, telemetry, and adversarial datasets.

Challenge 3: Federated Learning Resilient to Poisoning and Malicious Updates

Submissions using the provided GitHub federated learning framework (see Appendix A) are encouraged. Develop advanced federated learning techniques designed to withstand poisoning attacks and malicious updates across avionics and drone systems.
Participants should focus on ensuring model integrity despite adversarial endpoints, heterogeneous data, and limited bandwidth. Solutions must validate model updates, counter failures, and maintain system robustness under real-world operational constraints.
Key Focus Areas:

- Robust federated learning aggregation techniques with byzantine-tolerant methods and malicious node detection.
- Validation and trust-building mechanisms for client-side and global updates.
- Federated learning -based countermeasures against “brute force” jamming attacks.
- Use of federated learning to contrast the adversarial spoofing of drone control signals.
- Metrics for system resilience under poisoned inputs.

Challenge 4: Resilient Communication for Command-and-Control Networks

Develop robust communication protocols and encryption schemes for ensuring the integrity, confidentiality, and availability of command-and-control communication links in avionics and drone systems.

The solution should mitigate threats such as eavesdropping, man-in-the-middle (MITM) attacks, jamming, and spoofing while maintaining low latency and supporting resource-constrained environments.
Key Focus Areas:

- Lightweight encryption algorithms optimized for real-time communication.
- Jamming detection and mitigation techniques in contested environments.
- Redundancy and channel-switching protocols for fail-safe communication in drones and avionics.
- Threat scenarios testing protocol robustness and performance.

Challenge 5: Dynamic Task Allocation for Aerospace Swarms

Propose solutions for adaptive task and resource allocation in distributed aerospace swarms (e.g., UAV fleets).
The framework must enable dynamic and resilient swarm operations under adversarial conditions, model drift, and intermittent connectivity. Key objectives involve maximizing mission continuity and resource efficiency while addressing cybersecurity vulnerabilities in inter-swarm communications and decision-making.
Key Focus Areas:

- Swarm intelligence and decentralized optimization techniques.
- Secure communication protocols for task synchronization.
- Robustness to failures, such as node dropout or malicious agents.
- Lightweight algorithms for real-time task scheduling.

3. Program and Schedule

Proposals are due 22 May 2026, and should be submitted via e-mail to Victor Murray at victor.murray@swri.org, Jeffery Chavis Jeffrey.Chavis@jhuapl.edu, and Candace Jay candace.jay@swri.org. Proposals should include a cost estimate that shall not exceed $25,000. Solution developers should scope their proposal so that one working in your area can provide a meaningful contribution for less than $25,000. The IEEE AESS BoG will select up to four (4) solutions for funding, and funding will be made available prior to 22 July 2026. The solution developer will deliver the solution and technical report by 22 October 2026.

It should be assumed that any solution developer will have knowledge and experience in the challenge problem areas defined in Objectives and have access to standard software and hardware tools.

Table 1. Planned Schedule for Cybersecurity Challenge Problem Solutions.

Event	Due Date
Proposals for AESS Challenge Problem Solutions: Cybersecure and Resilient Avionics Operations	22 May 2026
Selection of four (4) Solutions for Funding	8 June 2026
Funding to Develop Solutions	22 July 2026
Technical Report and Delivery of Solutions	22 October 2026
Papers Describing Solutions for the Challenge Problem for IEEE Conference	Deadline is conference dependent.

4. Format and Content of Proposals

Proposals should not exceed five (5) pages in 12 pt font. Biographical information may be included in an appendix and that is not subjected to the limits. Proposals should include the following sections.

Cover Letter: List title, challenge problem, and authors.

Abstract: Abstract for the proposal with less than 250 words.

Introduction: Introduce the reader to the area of research of your proposed solution, summarize the research surrounding your problem (briefly stating the innovation of your proposed approach), and explain your connection to the area.

Motivation: Motivate the investment of IEEE AESS in your proposal solution.

Technical Description of Problem: Provide a technical description of the proposed solution with references.

Performance Metrics: Describe the metrics by which contributors will be scored and ranked and include any performance constraints. Describe the collection method for the metrics. Metrics for the complexity, cost, or computational cost of the different solutions will likely be needed.

Implementation Plan: Explain the implementation plan for your solution. For example, a software program will be provided to detect cyber-attacks based on training data, collect the results of the proposed solution, and compile results. Requirements should be specified in general terms and include scenarios for development and evaluation.

Milestone Schedule and Developers: Include a milestone schedule that includes one (1) in-progress report and one (1) briefing. Also, provide a list of proposed deliverables. Deliverables should include a technical report with presentation, problem description for solution proposers, paper for an IEEE conference that describes the problem, and software and hardware needed to implement the solution.

Anticipated Participants: Provide a list of researchers who are anticipated to participate in the development of solutions to your challenge problem.

Key Investigators: Provide very brief biography of key investigators that will be developing the solution.

Cost: Provide a cost estimate for the development of your solution. Costs may include materials and supplies and employee labor.

References: Provide references to key research in your proposed solution.

5. Evaluation Criteria

Proposals for the challenge problem will be judged on the following criteria:

1.	IEEE AESS area of interest	15%
2.	Alignment with challenge problems listed in Objectives	15%
3.	Anticipated success of proposed solution	15%
4.	Subject matter expertise of developers	15%
5.	Anticipated impact on real-world aviation and space systems	15%
6.	Solution and Outcome Definitions	25%

6. Concluding Remarks

It is anticipated that this RFP will lead to funding for the development of solutions for the challenge problems to stimulate excitement in the cybersecurity community. The solutions will be made available to the public.

Appendix A. Background Information from Initial Phase

As part of a prior effort, Intelligent Fusion Technology developed an extensive federated learning framework, publicly accessible here:

https://github.com/I-Fusion/drift-fairroad/tree/v2

The repo includes tools for attack detection, evaluation, and datasets from UAV operations. It provides participants with a starting point to adapt innovative approaches. The AESS initiative drives cutting-edge research and promotes real world applications, contributing to a more secure and resilient drone and aviation ecosystem.

Drone Simulations

Several open-source tools were used during phase 1 including ArduPilot screen shot is shown in Figure 1. This software was used to generate data sets stored on github.

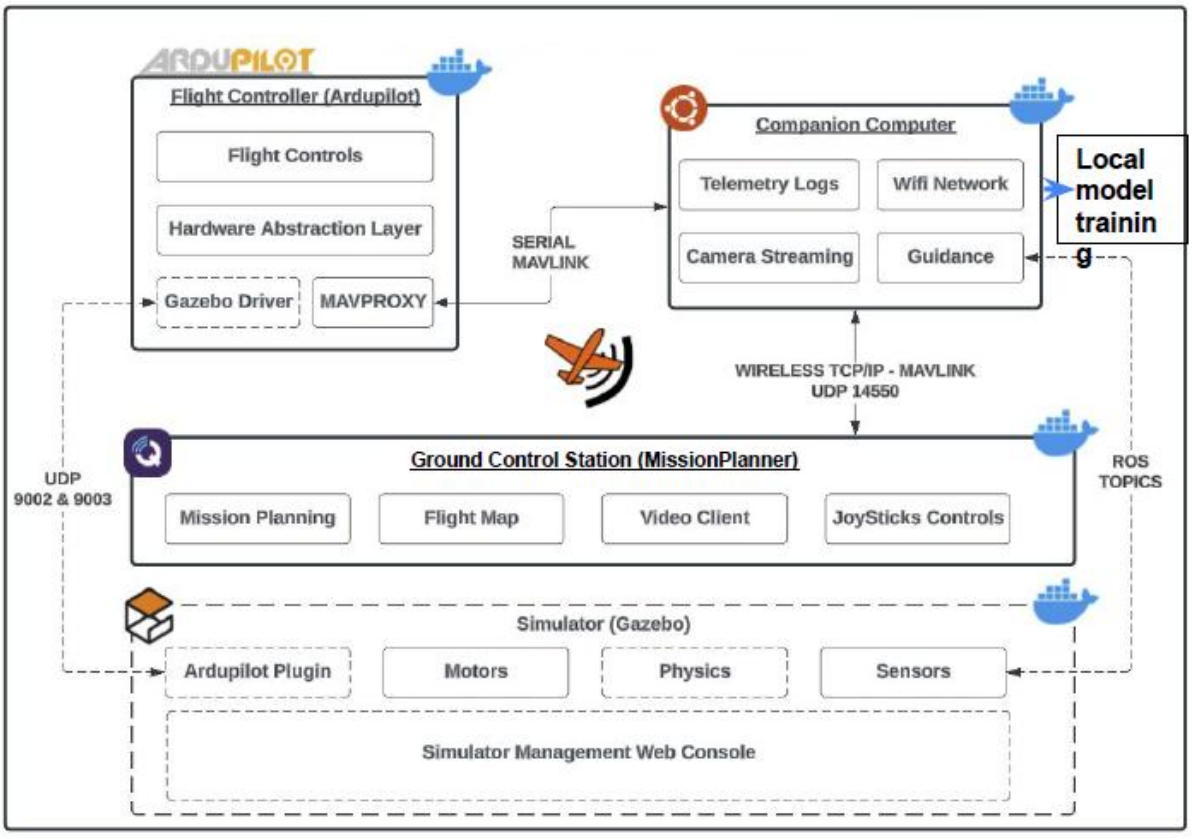

Figure 1. Ardupilot Drone Simulation Open-Source Software

Federated Learning

Federated learning offers an approach to collaboratively training AI/ML models for collective defense against threats while preserving privacy and adhering to operational constraints. In a federated learning system, each end point trains a local AI/ML model using its sensor and network data. Instead of sharing raw data, they transmit model updates to a central server, such as ground control, which aggregates these updates into an aggregated defense model and distributes it back to the end points. This iterative process enables airborne systems to continuously learn from and benefit from one another's experiences, enhancing overall capabilities without compromising privacy. An overview of the github hosted Federated AI model is shown in Figure 1.

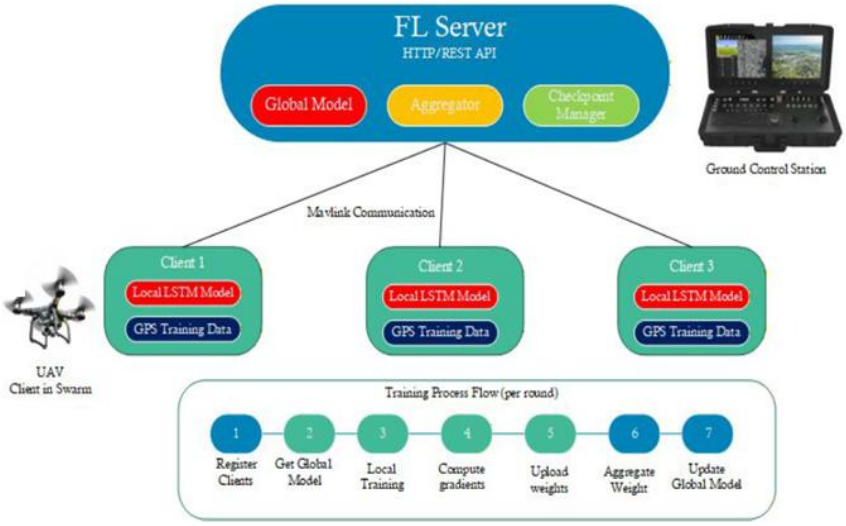

Figure 2. Federated AI block diagram for github hosted repo.

Cross-Layer Protection of Multi-UAS Systems Using Federated Learning

Deeraj Nagothu[1], Yajie Bao[1], Genshe Chen*[1], Erik Blasch[2], Victor C. Murray [3]

[1]*Intelligent Fusion Technology Inc.*, Germantown, MD, USA

[2]*Air Force Research Laboratory*, Arlington, VA, USA

[3] *Southwest Research Institute*, San Antonio, TX, USA

***Abstract*—The rise of autonomous unmanned aerial systems (UAS) has introduced critical cybersecurity vulnerabilities across GPS/GNSS navigation, Automatic Dependent Surveillance-Broadcast (ADS-B) communications, and command-and-control links. Traditional isolated anomaly-detection models struggle to adapt quickly to new or distributed threats. This paper presents federated learning (FL) as a unifying framework that addresses cybersecurity challenges across three critical layers simultaneously: (1) network-level attacks targeting communication protocols (2) adversarial threats against AI/ML models, and**

(3) distributed system resilience challenges. The proposed FL for Enhanced Drone Resilience framework demonstrates that FL enables privacy-preserving collaborative defense by allowing drone fleets to jointly train anomaly-detection models without ex-changing raw data. This approach transforms typical multi-UAS constraints, such as heterogeneous data, intermittent connectivity, and limited bandwidth, into advantages of a distributed defense system, positioning FL as a scalable and resilient solution for cybersecurity on next-generation autonomous aerospace platforms.

***Index Terms*—Federated Learning, Multi-UAS, Distributed framework**

I. Introduction

Digital avionics and the rapid adoption of autonomous unmanned aerial systems (UAS) have reshaped the aerospace threat landscape. Proper UAS functioning depends on tightly coupled digital subsystems like ADS-B for surveillance, GPS/GNSS for navigation, ACARS for data-link communications, and dedicated RF command-and-control (C&C) links for mission execution. While this connectivity enables reliable operations, it also widens the cyber-attack surface [1]. Inci-dents such as GPS spoofing of objects of interest in conflict zones, ADS-B injection, and RF jamming confirm that the cyber threats are operational hazards. As the attack surface scales, it significantly increases the risk of cascading failures, making cyber threat defense and analysis a priority [2].

The multi-UAS operational challenge stems from the fact that distributed drone fleets cannot rely on the centralized data collection and processing pipelines that traditional cybersecurity solutions use. Drones in different operational scenarios collect highly heterogeneous and non-IID datasets that limit the generalizability of models trained on a single vehicle's experience [3]. Given the network bandwidth limitations for remote operations, relying on a cloud server for continuous raw sensor logs is impractical when it scales. With data sharing limitations, safety-critical anomaly detection must run in near-real time and adhere to the cloud-based approach with data privacy constraints.

Federated learning (FL) directly addresses the above para-dox. FL enables collaborative model training without trans-mitting raw data, where the standard FL cycle follows global model distribution, local training on its own data, update com-pression, secure aggregation at the server, and model broad-cast in multiple iterations [4]. When applied to multi-UAS cybersecurity, FL yields several decisive advantages such as Privacy Preservation, Bandwidth efficiency, Collective defense and Robustness to heterogeneity.

Regardless, FL itself becomes a target in adversarial environments. Compromised drones can submit poisoned updates, embed backdoors, or act as Byzantine participants, while communication channels may be jammed or tampered with. Therefore, a secure FL deployment for UAS must target three interconnected layers,

- **Network layer**: detection and mitigation of attacks on UAV communication link (MAVLink)
- **AI/ML layer**: safeguarding the federated training process against poisoning, backdoors, and model-level sabotage.
- **Distributed-system layer**: ensuring convergence and stability despite non-IID data, partial participation, and limited resources.

This work presents the FL for Enhanced Drone Resilience, a multi-layered framework that simultaneously resolves the primary cybersecurity challenges of distributed aerospace systems. Performance metrics that span all three security layers represent how FL transforms the multi-UAS operational constraints into a secure distributed framework.

II. Multi-Layered Federated Learning Framework for UAS Cybersecurity

The FL for Enhanced Drone Resilience framework presented in 1 showcases how federated learning can serve as a unified defense architecture by which the three individual challenge domains, network-level attacks, adversarial AI/ML threats, and distributed-system constraints. Built on open-source components for federated orchestration, the system adopts a client-server topology in which every drone acts as a federated client. Each client ingests time-ordered streams from onboard sensors (ADS-B kinematics, GPS/GNSS data, telemetry logs) and runs a lightweight local anomaly detector. Periodically, whenever a salient anomaly is observed, the

client performs a bounded number of training epochs on the buffer of labeled or pseudo-labeled samples and then transmits a compressed model update to a central aggregator/server (Ground control station). The aggregator fuses updates using optimal Federated Averaging algorithm, and redistributes the refined global model back to the fleet. Crucially, the architecture tolerates partial participation and client dropouts, mirroring real-world conditions where intermittent connectivity and bandwidth limitations.

When the network-layer subproblem is solved by equipping each client with a model capable of recognizing GPS/GNSS spoofing, or ADS-B injection, the resulting local signatures become part of the federated update, allowing the global model to learn a richer representation of attack patterns without ever exposing raw flight trajectories. Likewise, once the AI/ML adversarial subproblem is mitigated through robust aggregation, update validation, differential-privacy noise injection, and secure aggregation protocols. The federated process itself remains trustworthy, preventing poisoned updates or backdoor triggers from degrading detection performance [4]. Finally, the distributed-system subproblem is addressed by employing gradient quantization, sparse update transmission, or knowledge-distillation to smaller on-board models, ensuring the compute constraints and elimits of battery-powered drones.

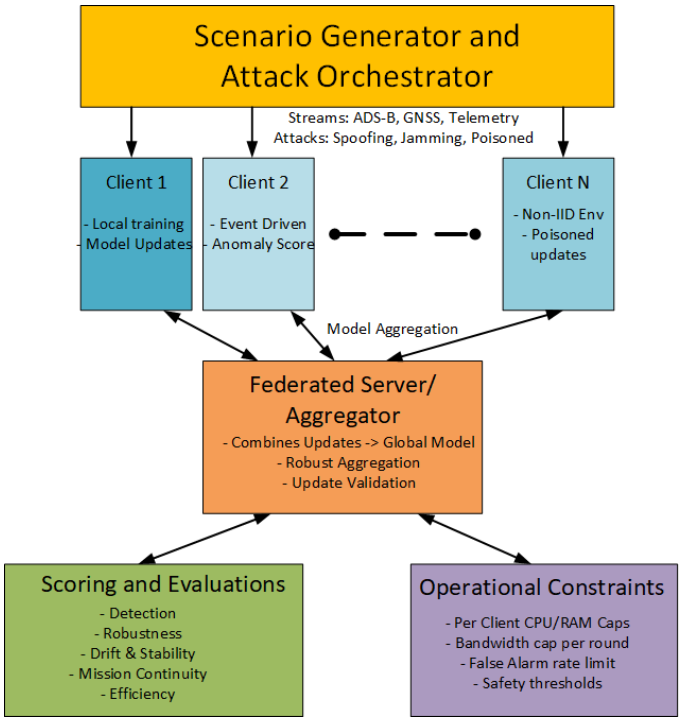

Fig. 1: FL for Enhanced Drone Resilience Framework

To evaluate the efficacy of this integrated framework, we adopt a suite of metrics that span all three security threat models. Detection quality for the network layer is quantified with standard classification scores (AUROC, precision, recall, F1) together with time-to-detect latency and a capped false-alarm rate to preserve operator trust. Robustness of the AI/ML layer is measured by the degradation in detection accuracy as the proportion of malicious clients varies. Additionally, the variance of accuracy across heterogeneous client datasets which reflects resilience to non-IID data [3]. Distributed-system resilience is captured through drift-resistance and model-stability indicators like validation accuracy over successive rounds.

Throughout the testing, overall mission continuity is assessed to ensure that the framework can be deployed on real-world UAV platforms without jeopardizing flight operations. Collectively, these metrics provide a comprehensive, quantitative picture of how federated learning, when each constituent challenge is properly handled, delivers a scalable and robust cybersecurity solution for modern multi-UAS ecosystems.

III. Conclusion and Discussion

This work demonstrates that FL for Enhanced Drone Resilience presents a coherent, multi-layered cybersecurity architecture for distributed UAS operations. By leveraging FL, the framework simultaneously mitigates network-level threats, hardens the AI/ML training pipeline against poisoning and backdoor attacks, and accommodates heterogeneous data and intermittent connectivity. The testbed validates this vision through realistic avionics streams, bandwidth-constrained links, and mission-continuity constraints. Along with a comprehensive metrics established for system performance and degradation, which provides a quantitative basis for evaluating trade-offs across the three layers.

The framework enables a privacy-preserving distributed intelligence that reinforces robust defense against multiple cyber threats and enabling multi-UAS as an enhanced system. The framework can be further extended to multiple applications, enabling cross-domain threat intelligence while preserving privacy and security. Open research avenues include adaptive and secure aggregation schemes and formal verification methods that enables convergence, robustness, and privacy for safety-critical applications. By establishing standardized benchmarks and a reproducible evaluation pipeline, the proposed framework offers a scalable, resilient, and privacy-preserving foundation for the next generation of autonomous aerospace systems.

References

[1] E. Blasch, V. Murray, M. Werthwein, J. S. Chavis, J. Leuchter, A. Roy, J. Lyke, C. C. Insaurralde, and G. Fasano, "Contemporary directions in cybersecurity avionics risk analysis," in *2025 AIAA DATC/IEEE 44th Digital Avionics Systems Conference (DASC)*, 2025, pp. 1–8.

[2] E. Habler, R. Bitton, and A. Shabtai, "Assessing aircraft security: A comprehensive survey and methodology for evaluation," *ACM Computing Surveys*, vol. 56, no. 4, pp. 1–40, 2023.

[3] Z. Lu, H. Pan, Y. Dai, X. Si, and Y. Zhang, "Federated learning with non-iid data: A survey," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 188–19 209, 2024.

[4] S. Han, B. Buyukates, Z. Hu, H. Jin, W. Jin, L. Sun, X. Wang, W. Wu, C. Xie, Y. Yao *et al.*, "Fedsecurity: A benchmark for attacks and defenses in federated learning and federated llms," in *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2024, pp. 5070–5081.