Hybrid Blockchain-Assisted Federated Learning Intrusion Detection System for DoS Attacks in UAV Sensor Network

Odinachi U. Nwankwo, Simeon Okechukwu Ajakwe*, Dong-Seong Kim, Jae Min Lee
Department of IT Convergence, Kumoh National Institute of Technology, Gumi, South Korea
*ICT Convergence Research Centre Kumoh National Institute of Technology, Gumi, South Korea
{odinachi, simeon.ajakwe, dskim, ljmpaul}@kumoh.ac.kr

***Abstract*—Unmanned Aerial Vehicles (UAVs) are increasingly deployed in mission-critical domains, raising significant security concerns. This paper presents a Federated Learning-based Intrusion Detection System (PureChain-FL) for UAV clients, focusing on Denial-of-Service (DoS) attack detection. To enhance trust and auditability, the proposed architecture integrates PureChain, a lightweight blockchain framework based on the Proof of Authority Association (PoA^2) consensus algorithm for secure logging of detected threats. The system features client-based localized model training using the WSN-DS dataset and a global FL server for model aggregation. A smart contract governs audit logging, enabling verifiable and tamper-resistant record-keeping. Evaluation of multilayer perceptron (MLP), one-dimensional convolutional neural network (1D CNN), and CNN combined with long-short-term memory (CNN-LSTM) models over 20 FL rounds with five clients using the Flower framework and TensorFlow in a Google collaborative environment revealed CNN-LSTM as the best-performing model with 99.3% accuracy. Figures and diagrams illustrating system architecture, communication flow, and model training are integrated into the discussion for clarity. The results show promise in the system's effectiveness in privacy-preserving and trustworthy intrusion detection for unmanned aerial wireless sensor networks.**

***Index Terms*—Federated Learning, UAV Network, Denial-of-Service, Blockchain, PureChain, Intrusion Detection.**

I. Introduction

The rapid proliferation of Unmanned Aerial Vehicles (UAVs) in smart cities, military surveillance, and environmental monitoring has made UAV swarms a critical component of modern wireless networks. These UAV networks [1], especially when deployed in a clustered formation, offer flexibility, scalability, and extended coverage [2]. However, their wireless and decentralized nature makes them highly vulnerable to security breaches such as denial-of-service (DoS) attacks, grayhole, blackhole, and other network layer threats [3], [4]. Centralized intrusion detection systems (IDS) are ill-suited for UAV swarms owned and operated by different clients or companies due to data privacy risks and lack of trust [5]. Federated Learning (FL) offers a privacy-preserving alternative by enabling local model training without sharing raw data [5] [6] [7]. This work used FL-based architecture to train UAV swarms owned and operated by five clients in a decentralized manner without sharing raw data between the clients involved in the training, thereby preserving their data privacy. The artificial intelligence (AI) model used for the FL is deployed on each Backbone UAV of each client at the cluster level to detect DoS attacks. PureChain, a lightweight blockchain, is employed to keep an immutable record of the detected threats.

FL has recently emerged as a privacy-preserving solution that enables multiple distributed client nodes to collaboratively train a deep learning model without sharing raw data [7] [8] [9]. However, there is limited literature that substantially covers the application of FL to UAV client domains. Before being deployed on each Backbone UAV, AI enables all UAV clients that participate in FL to locally train using local data while contributing knowledge to a global model hosted on a central server. Existing intrusion detection systems for UAV networks rely on centralized architectures, which compromise data privacy, scalability, and trust, and lack support for decentralized, auditable threat logging.

To address these challenges, this research proposes a blockchain-powered FL-based Intrusion Detection System (PureChain-FL) for five clients that own and operate UAV swarms for different applications to equip their UAVs with immunity against wireless sensor network-level DoS attacks. The proposed architecture leverages PureChain, a lightweight blockchain, to ensure malicious activities are logged on the blockchain to prevent tampering and facilitate forensic analysis. Despite advances in UAV swarm communication, securing such networks against evolving cyberattacks remains a pressing challenge. Existing intrusion detection methods require central data aggregation, violating privacy, security, and trust.

The main contributions of this work are:

- Adaptive AI model training and comparison based on FL using the WSN-DS dataset: Three deep learning models were trained to detect DoS wireless sensor network-level attacks. FL training was implemented and benchmarked using three AI models (MLP, 1D CNN, and CNN-LSTM) under a non-IID dataset setting. The FL-IDS supports DoS detection with privacy-preserving properties.
- Strategic deployment of IDS on the Backbone UAV for

TABLE I: Comparative Analysis of Related Works

Study	Technology Used	Key Strengths	Limitations
MetaFedNet [10]	FL	Integrated blockchain and IPFS; incentivized participation	Domain limited to metaverse; not UAV-specific
DroneGuard [11]	CL	Explainable ML for UAV GPS spoofing and DoS threats	No federated learning; lacked decentralized audit mechanism
As-Fed [12]	FL	Explored FL in the UAV domain using GPS and Edge-IIoTset dataset	No support for blockchain audit trail
Our work (2025)	FL + BC	Explored FL and BC in the UAV domain using DoS	None.

monitoring and detecting DoS threats emanating from wireless sensor network traffic.

- Each backbone UAV is connected to a PoA²-based PureChain ledger that hosts the (*Attack_Log*) smart contract, while running only a light client on board to avoid validator and runtime overhead. When a threat is detected (timestamp, client, UAV ID, attack class), the UAV signs and submits a logAttack transaction to edge/Ground Control Station validators; the contract records the entry and emits AttackLogged.

The remainder of this paper is organized as follows: Section II reviews related works. Section III presents the system architecture and methodology, including the UAV IDS design, dataset preprocessing, and the federated learning pipeline. Section IV evaluates the performance of three AI models and discusses the results. Finally, Section V concludes the paper and outlines directions for future research.

II. RELATED WORKS

Most existing intrusion detection systems (IDS) rely heavily on centralized learning architectures, which introduce significant concerns related to data privacy, security, and trust. This centralized paradigm requires the aggregation of raw data from distributed sources, thereby increasing the risk of data exposure. Although FL has gained traction in addressing privacy challenges in Industrial Internet of Things (IIoT) environments [13], its application within the UAV domain remains notably limited. The unique characteristics of UAV networks, such as high mobility, dynamic topologies, and sensitivity to communication latency, necessitate IDS solutions that surpass conventional centralized designs.

Authors [10] presented an FL-based IDS for SDN-enabled Industrial Cyber-Physical Systems using the InSDN and Edge-IIoTset datasets. Their approach demonstrated the potential of FL in preserving data privacy while detecting attacks such as Distributed Denial of Service (DDoS), malware, and Man in the Middle (MITM). However, this solution was confined to IIoT environments and was not extended to UAV scenarios, nor did it incorporate auditability of security events. In a subsequent work, the authors introduced MetaFedNet, an FL-powered IDS for metaverse environments leveraging blockchain (Proof-of-Authority) and Interplanetary File System (IPFS) to improve model update transparency and decentralization. Although this system used ERC-20 tokens to incentivize client participation and improve distributed storage, the study was not meant for UAV-specific applications.

Meanwhile, authors [11] developed an explainable IDS for UAV environments using the AV-GPS and WSN-DS datasets. Though the model addressed GPS spoofing and DoS threats with explainability tools, it did not incorporate federated learning, limiting scalability and collaborative learning among UAVs. In earlier work, the same author explored FL using UAV GPS data and the Edge-IIoTset dataset, demonstrating promise in distributed threat detection. However, the architecture lacked robust support for a secure and decentralized audit trail of detected threats in UAV swarm operations [12]. In summary, while FL has shown potential in improving privacy and decentralization in IoT-based IDS, its adoption in UAV networks remains underdeveloped. Notably, the current literature lacks a detailed incorporation of FL for UAV swarm security for different clients, with support for auditable logs of detected threats. These gaps underscore the need for a fully decentralized, FL-based IDS tailored for UAVs, incorporating integrated threat audit trail mechanisms. Table I summarizes the strengths and limitations of the works reviewed in the literature.

Unlike existing blockchain-federated learning frameworks [9] [10] tailored to IIoT or metaverse domains, PureChain-FL introduces a Proof-of-Authority-and-Association (PoA^2) consensus that prioritizes trusted GCS validators. This design enables deterministic block generation with low overhead, achieving 41.3% lower latency and 36.5% energy savings while ensuring auditable, privacy-preserving UAV intrusion detection.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

The proposed system architecture in Fig. 1 illustrates a federated learning-based intrusion detection framework for a UAV wireless sensor network, where multiple UAV clients collaborate with a central federated learning server/aggregator to train intrusion detection models without sharing raw data. Each client, composed of backbone UAVs and other UAVs, uses IDS based on WSN-DS datasets to monitor intra-UAV communications. In the event of a malicious actor launching DoS or packet injection attacks through a rogue drone, the attacks are detected and flagged. As each client's Backbone UAV is connected to the PureChain network, detected attacks are then recorded on the PureChain blockchain network deployed only on each client's GCS nodes, thereby ensuring secure,

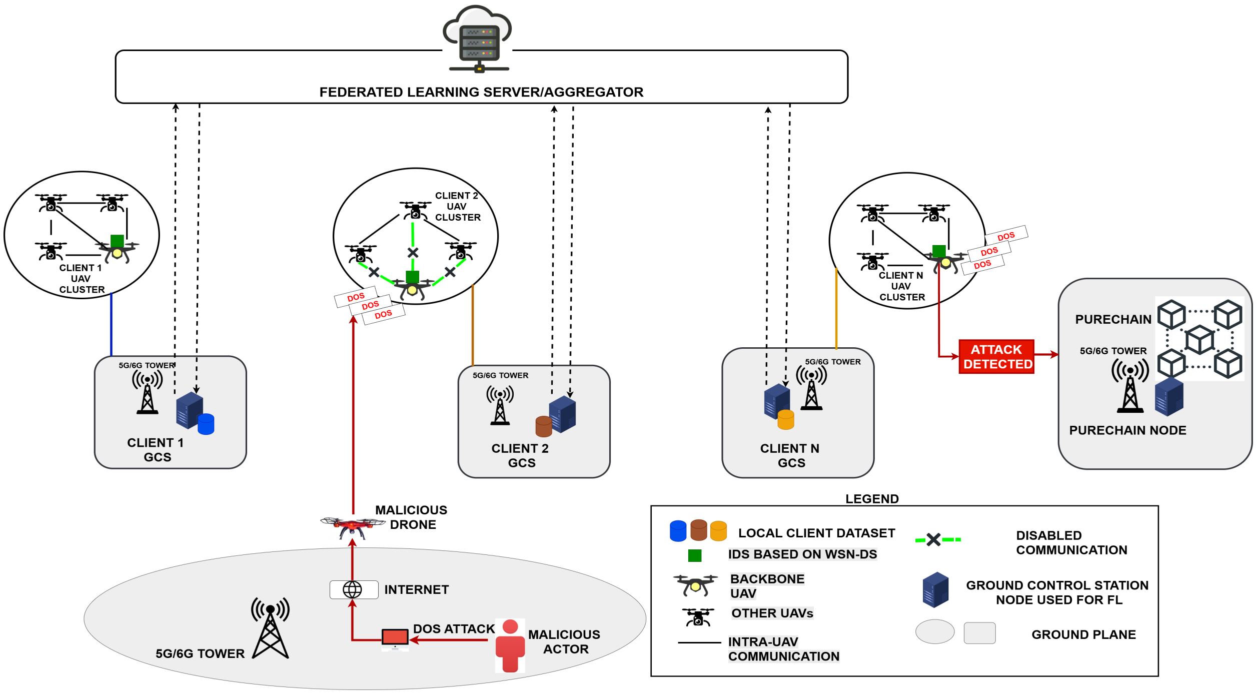

Fig. 1: The ground station nodes used for FL, shown in the architecture, are located at ground control stations (GCS) belonging to each client. FL training takes place at each client's GCS node before the aggregated AI models are deployed on UAVs for real-time intrusion detection. Only each Backbone UAV in the cluster of each client is equipped with an intrusion detection system (IDS), represented by a green square. Detected attacks are immutably logged on the Purechain blockchain, ensuring auditability and resilience against tampering. Note that the Backbone UAV runs only a PureChain light client, which does not download blockchain blocks.

immutable logging of intrusion events. Edge nodes at each client GCS act as local processing units for federated learning and host the PureChain network. Overall, this methodology integrates federated learning, blockchain, and edge intelligence to enhance the resilience, security, and trustworthiness of UAV swarm communications against sensor network-level DoS threats for each client. The diagram also shows a malicious ground-based device launching a DoS attack through a rogue drone.

A. *Dataset Description and Preprocessing*

Selecting an appropriate dataset is essential for building effective AI models, particularly in scenarios that require practical deployment, such as UAV networks. UAV swarms operate as airborne wireless sensor networks (WSNs), carrying out real-time tasks like monitoring and surveillance. To address security challenges in such environments, we utilized the WSN-DS dataset, which was specifically created for cybersecurity applications within WSNs. The WSN-DS dataset is tailored for detecting Denial-of-Service (DoS) attacks in sensor network environments. It includes four common types of DoS threats relevant to UAV networks: Blackhole, Grayhole, Flooding, and TDMA-based Scheduling attacks. In total, the dataset comprises 374,661 labeled samples, encompassing 18 input features and five classification labels. This diversity allows for robust training and validation of machine learning models aimed at detecting malicious behaviors in UAV swarm operations. Preprocessing steps performed on the dataset include cleaning of missing or inconsistent entries, normalization of feature scales, one-hot encoding of categorical variables, and class balancing techniques to address potential bias. These steps ensured that the models trained under the federated learning framework could effectively generalize to unseen threats to the UAV network. Fig. 2 shows the confusion matrix of the CNN-LSTM model, showing a high overall accuracy of 98.3% and an average F1 score of 98.2% in the normal, TDMA, black hole, gray hole, and flooding attack categories. The dataset was finally partitioned into five non-IID datasets for five participating clients using the Dirichlet partitioner with alpha set to 0.3.

B. *Federated Pipeline, Model Collection and Global Aggregation Process*

As illustrated in Fig. 3, the FL pipeline involves local data collection, preprocessing (e.g., feature selection, encoding), and model training on the WSN-DS dataset. The FL simulation was conducted using five clients over 20 rounds in a Google Colab environment. The implementation leveraged the Flower federated learning framework integrated with TensorFlow. Each client emulates an edge node located at the ground control station; each client is responsible for local training. The FL server aggregates these models using the FedAvg algorithm and redistributes the updated global model to the clients for the next round. In the proposed PureChain-FL framework,

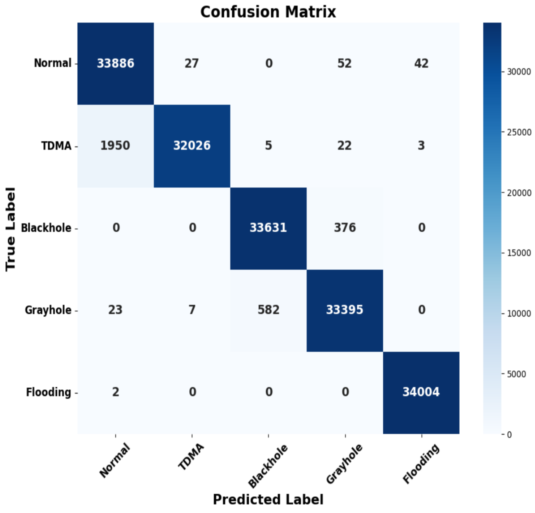

Fig. 2: The confusion matrix illustrates the performance of the CNN-LSTM model, centrally trained on the WS-DS dataset before starting FL, showing classification across Normal, TDMA, Blackhole, Grayhole, and Flooding attacks.

all participating clients initialize their local models with the same global parameters $\theta^{(0)}$ broadcast by the FL server. At each communication round t, client k locally trains its model on non-IID data D_k for E epochs using stochastic gradient descent and obtains updated parameters $\theta_k^{(t)}$. The FL server synchronously collects all local model updates and computes the global model using the FedAvg aggregation rule:

$$\theta^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{\sum_{j=1}^{K} n_j} \theta_k^{(t)}, \tag{1}$$

where n_k denotes the number of training samples at client k. The updated global model is then redistributed to all clients for the next training round. Blockchain operations are decoupled from model aggregation and are used solely for secure attack logging.

C. Blockchain-Enabled Detection Logging

Once a threat is detected, the Backbone UAV logs the incident to PureChain. Each log entry includes the client ID, attack type, timestamp, and UAV ID. This secure, immutable log enables decentralized trust and forensic analysis. Algorithm 1 summarizes the FL-based IDS procedure.

SMART CONTRACT FUNCTIONALITY

The *Attack_Log* smart contract maintains an on-chain audit trail of detected attacks. It provides three core functions: **logAttack**, which records new attack entries and emits an on-chain **AttackLogged** event; **getLog**, which retrieves a specific attack record; and **totalLogs**, which reports the total number of stored entries. These mechanisms ensure that all attack information is securely stored, audited, and tracked directly on-chain. Algorithm 2 presents the pseudocode of the smart contract logic.

Algorithm 1: Federated Blockchain-Integrated Intrusion Detection for UAV Swarms

```
Input: Local UAV wireless sensor network traffic
  datasets $D_1, D_2, ..., D_N$ at ground station nodes
Output: Global IDS model $f$; Blockchain log $B$
Procedure FL_IDS_Pipeline
while True do
    // Initialization
        Initialize Federated Learning Server (FLS)
        Initialize clients' Ground Station Node $N_i$
        Initialize lightweight blockchain ledger
      (PureChain)
    // Federated Training Loop
    for each training round do
        for each cluster $C_i$ do
            Collect and preprocess local traffic data $D_i$
            Train local model $f_i$ on $N_i$ using $D_i$
            Send local model weights $\theta_i$ to FLS
        end
        Aggregate local model weights:
          $f \leftarrow \text{FedAvg}(\theta_1, ..., \theta_N)$
        Distribute global model $f$ back to $N_i$
    end
    // Real-time Intrusion Detection & Response
    for each incoming traffic sample $x$ at a Backbone
      UAV do
        Preprocess sample $x$
        Predict $y \leftarrow f(x)$
        if $y = Attack$ then
            Log: attack type, timestamp, UAV ID,
              cluster ID
            Disable communication with malicious
              UAV
            Append alert to blockchain ledger $B$
        end
        else
            Permit normal communication
        end
    end
end
```

IV. PERFORMANCE EVALUATION

Experiments were conducted using the WSN-DS dataset over 20 FL rounds. We evaluated MLP, 1D CNN, and CNN-LSTM. Fig. 4 shows accuracy trends; CNN-LSTM outperformed others with 99.3% final accuracy. Fig. 5 displays loss trends, hence confirming CNN-LSTM's effectiveness, with a low value of 0.0271. Both MLP and 1D CNN plateaued at

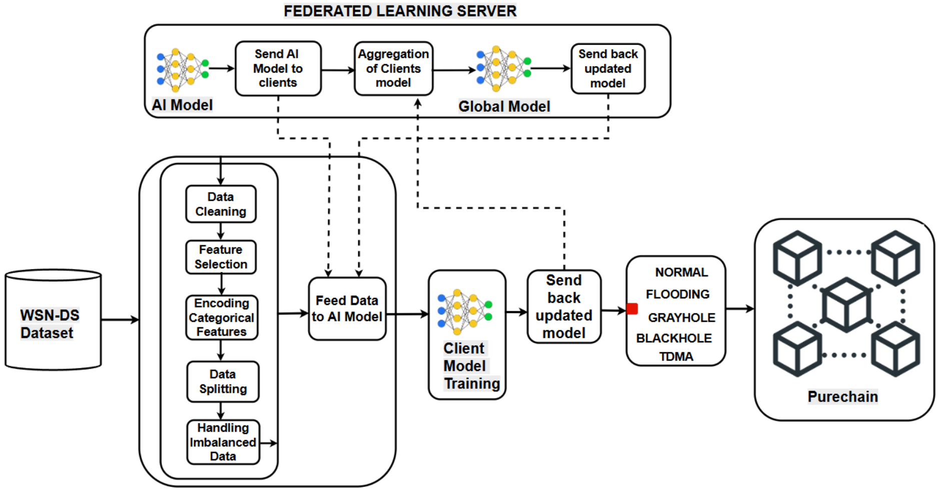

Fig. 3: illustrates a federated AI model training workflow using the WSN-DS dataset. Client devices train models locally and send updates to a FL server, which aggregates them into a global model. The model detects wireless sensor network-level DoS attacks, and results are stored securely on the Purechain blockchain.

Algorithm 2: Attack_Log Smart Contract

```
Input: AttackType, UAV_ID, Cluster_ID
Output: Stored attack log entry; AttackLogged
  event; queryable logs
Procedure SimpleAttackLog()
    // Initialize storage
    Logs ← empty list;
Function logAttack (AttackType, UAV_ID,
  Cluster_ID):
    id ← length(Logs);
    timestamp ← current time;
    newLog ← { id, AttackType, UAV_ID, Cluster_ID,
      timestamp };
    Append newLog to Logs;
    Emit event AttackLogged(id, AttackType,
      UAV_ID, Cluster_ID, timestamp);
Function totalLogs ():
    return length(Logs);
Function getLog (id):
    if id < length(Logs) then
        return Logs[id];
    end
    else
        return "Invalid log id";
    end
```

0.4261. Fig. 6 highlights F1-score trends; an F1-score of 0.99 confirms CNN-LSTM's effectiveness.

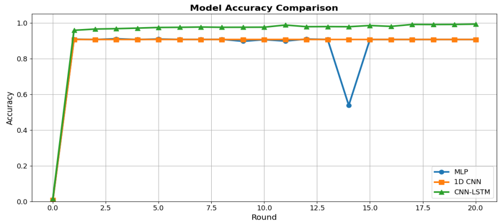

Fig. 4: Graph comparing the accuracy performance of three AI models: MLP, 1D CNN, and CNN-LSTM, across 20 federated learning rounds.

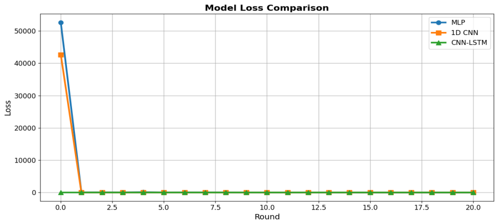

Fig. 5: The loss comparison illustrates model convergence behavior over training rounds.

Training time analysis showed that CNN-LSTM required 26 minutes, 1D CNN took 16 minutes, and MLP completed in 12 minutes, but exhibited inconsistency during client UAV training. The size of the trained CNN-LSTM model in .h5 format, which is 25MB, makes it suitable for deployment on edge devices like the Raspberry Pi.

Table II presents a comparative analysis of three deep learning models, CNN 1D, MLP, and CNN-LSTM, based on three key performance metrics. Final Accuracy, Final F1-Score, and Final Loss. The evaluation provides insight into the

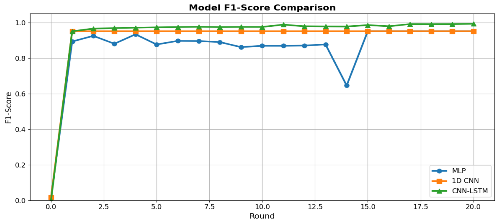

Fig. 6: The F1-score trends reflect the models' classification robustness. CNN-LSTM shows superior and stable performance (F1 0.99), indicating good precision-recall balance.

detection effectiveness of each model within the context of the intrusion detection or classification task. Table III compares previous studies with our work and shows that the proposed approach ticked all the boxes.

TABLE II: Comparison: 1D CNN vs MLP vs CNN-LSTM

Model	Final Accuracy	Final F1-Score	Final Loss
1D CNN	90.7%	0.9512	0.4261
MLP	90.7%	0.9512	0.4261
CNN-LSTM	**99.3%**	**0.9929**	**0.0271**

TABLE III: Evaluation with Related Works

Authors	Privacy Preservation	UAV Domain	Blockchain Audit
[10]	✓	✗	✓
[11]	✗	✓	✗
[12]	✓	✓	✗
This work	✓	✓	✓

A. Blockchain Transaction Latency and Throughput Performance for Attack Log

Key metrics considered in PureChain performance included blockchain transaction latency during log recording and transaction throughput for attack logs. The results indicated that attack logs, representing detected threats, were securely logged on the PureChain blockchain with minimal impact on transaction latency. Specifically, the blockchain transaction latency per log averaged around 112 ms, while the throughput remained steady at 24 transactions per second (TPS) under the PoA^2 consensus. These results show promise that PureChain can handle attack log recording efficiently, supporting the system's feasibility for real-time UAV operations.

V. CONCLUSION AND FUTURE WORK

This work used an FL-based IDS with blockchain logging for DoS detection at the network level of a wireless sensor network of five UAV clients. Local models are trained within each client to preserve data privacy, while the PureChain blockchain secures threat logs. CNN-LSTM delivered the best results (99.3% accuracy), though it was computationally intensive in terms of training time. The privacy-preserving attribute of this research will enable participating clients to collaborate and equip their surveillance UAVs with IDS, hence making them immune to wireless sensor network DoS attacks without exposing each member's data. Future work will focus on investigating the performance of the PureChain-FL system with varying numbers of clients to assess scalability, as well as exploring the scalability of PureChain under heavy traffic conditions in real-world deployments. Additionally, DoS threats will be examined across different scenarios to ensure a robust design. Finally, the single point of failure (SPOF) associated with FL will also be addressed.

ACKNOWLEDGEMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government(MSIT) (IITP-2025-RS-2020-II201612, 25%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program(IITP-2025-RS-2024-00438430, 25%). This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2025-25431637, 25%).

REFERENCES

[1] L. Kou, S. Ding, T. Wu, W. Dong, and Y. Yin, "An Intrusion Detection Model for Drone Communication Network in SDN Environment," *Drones*, vol. 6, no. 11, 2022. [Online]. Available: https://www.mdpi.com/2504-446X/6/11/342

[2] S. O. Ajakwe, K. L. Olabisi, and D.-S. Kim, "Multihop intruder node detection scheme (minds) for secured drones' fanet communication," *IET Intelligent Transport Systems*, vol. 19, no. 1, p. e70080, 2025.

[3] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for uav communications and flying ad-hoc networks," *Ad Hoc Networks*, vol. 133, no. C, p. 102894, 2022.

[4] S. O. Ajakwe and D.-S. Kim, "Time sensitive anti-infoswarm agnostic intelligence for safe uav communication," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 10 2024, pp. 1614–1619.

[5] O. Ceviz, P. Sadioglu, S. Sen, and V. G. Vassilakis, "A novel federated learning-based ids for enhancing uavs privacy and security," *Internet of Things*, vol. 31, p. 101592, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660525001052

[6] H. Alaya, A. Ben Letaifa, and A. Rachedi, "State of the art and taxonomy survey on federated learning and blockchain integration in uav applications," *The Journal of Supercomputing*, vol. 81, no. 5, p. 655, 2025.

[7] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks," *Network*, vol. 3, no. 1, pp. 158–179, 2023. [Online]. Available: https://www.mdpi.com/2673-8732/3/1/8

[8] F. Mosaiyebzadeh, S. Pouriyeh, R. M. Parizi, M. Han, and D. M. Batista, "Intrusion detection system for ioht devices using federated learning," in *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2023, pp. 1–6.

[9] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," *International journal of machine learning and cybernetics*, vol. 14, no. 2, pp. 513–535, 2023.

[10] A. Zainudin, M. A. P. Putra, R. N. Alief, R. Akter, D.-S. Kim, and J.-M. Lee, "Blockchain-inspired collaborative cyber-attacks detection for securing metaverse," *IEEE Internet of Things Journal*, vol. 11, no. 10, pp. 18 221–18 236, 2024.

[11] V. U. Ihekoronye, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "Droneguard: An explainable and efficient machine learning framework for intrusion detection in drone networks," *IEEE Internet of Things Journal*, vol. 12, no. 7, pp. 7708–7722, 2025.

[12] V. U. Ihekoronye, C. I. Nwakanma, D.-S. Kim, and J. M. Lee, "Asr-fed: agnostic straggler-resilient semi-asynchronous federated learning technique for secured drone network," *International Journal of Machine Learning and Cybernetics*, vol. 15, no. 11, pp. 5303–5319, 2024.

[13] X. Liu, X. Dong, N. Jia, and W. Zhao, "Federated learning-oriented edge computing framework for the iiot," *Sensors*, vol. 24, no. 13, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/13/4182