AMLB-FL: A Privacy-Preserving Blockchain and Federated Learning Architecture for UAV Networks

Karanam Sunil Kumar[1], S.K. Manju Bargavi [2]

[1] Postdoctoral Researcher, Lincoln University College, Malaysia

[2] Professor, School of Computer Science and IT, Jain Deemed to be University, Bengaluru, India

Email ID: pdf.sunilkaranam@lincoln.edu.my, cloudbargavi@gmail.com

Abstract: There are critical security concern along with issues pertaining to privacy and scalability towards the open-air mode exchange of data in Unmanned Aerial Vehicle (UAV) networks. The current solutions are noted to adopt centralized security measure, isolated blockchain, and even federated learning and yet they cannot mitigate issues pertaining to unreliable fusion of model, communication overhead, and single-point failures. These problems are addressed in proposed study model named as Adaptive Multi-Layer Blockchain and Federated Learning (AMLB-FL) meant for securing data exchange in UAV networks. The framework is structured with three layers meant for trust management, blockchain operation, and anomaly detection with privacy preservation. Experimental outcome shows proposed model to offer notably higher detection accuracy, lower latency, increased scalability, and increased energy efficiency in contrast to most relevant baseline models.

Keywords: Unmanned Aerial Vehicle, Security, Blockchain, Federated Learning, data exchange, Privacy preservation, anomaly detection

Introduction

There are extensive ranges of applications of Unmanned Aerial Vehicle (UAV) that calls for securing the networks as they operate in open airspace and dynamic environment [1]. There are various possibility of security violations like physical damage, mission failure, data leakage that may cost the value of sensitive data being exchanged in UAV networks. There are different form of attacks like model poisoning, sybil attack, denial-of-service attack, man-in-the-middle attack, spoofing attack etc where it is very much possible for attacker to control the updates of local model in order to degrade the performance of global learning [2][3]. Existing solution for such issues are via privacy-preserving model using federated learning trust management using blockchain, encryptions, centralized authentication, etc. Irrespective of advanced technology, conventional security methods are noted to have different levels of shortcomings. Existing centralized system are vulnerable to single-point failures especially when subjected to dense deployment of UAV while most emerging blockchain technology induces intensive communication overhead as well as maximized computational burden. All these are absolutely not appropriate for UAV nodes which are low-resource devices [4]. Existing federated learning models are also noted with reduced degree of robustness towards model verification making the UAV nodes susceptible to malicious updates and poisoning. Hybrid approaches are known for combining multiple approaches to enhance security; however, they adaptability towards dynamic environment is highly questionable [5].

Proposed Method

The research work introduces an innovative security-centric communication model towards safeguarding any form of data exchange with network of UAV called as Adaptive Multi-Layer Blockchain and Federated Learning (AMLB-FL). Figure 1 showcase 3-layered architecture consisting of control layer, consensus layer, and learning layer.

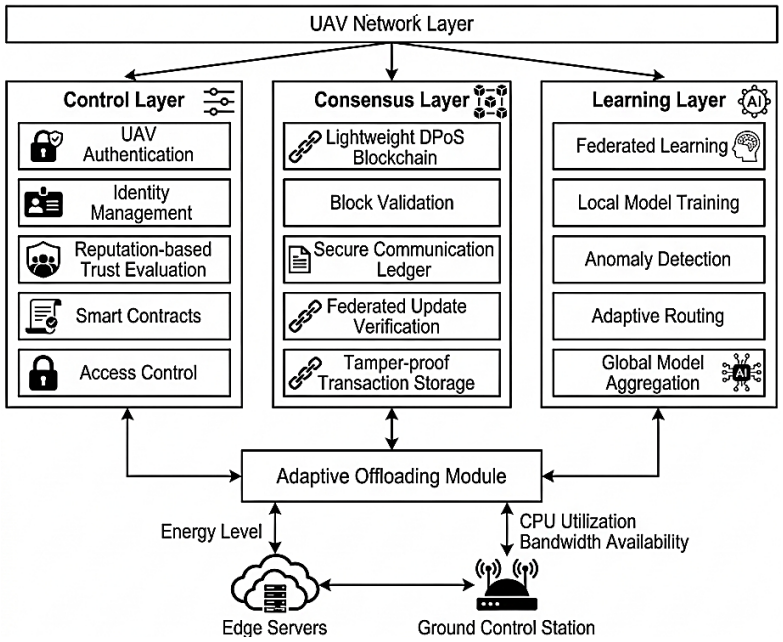
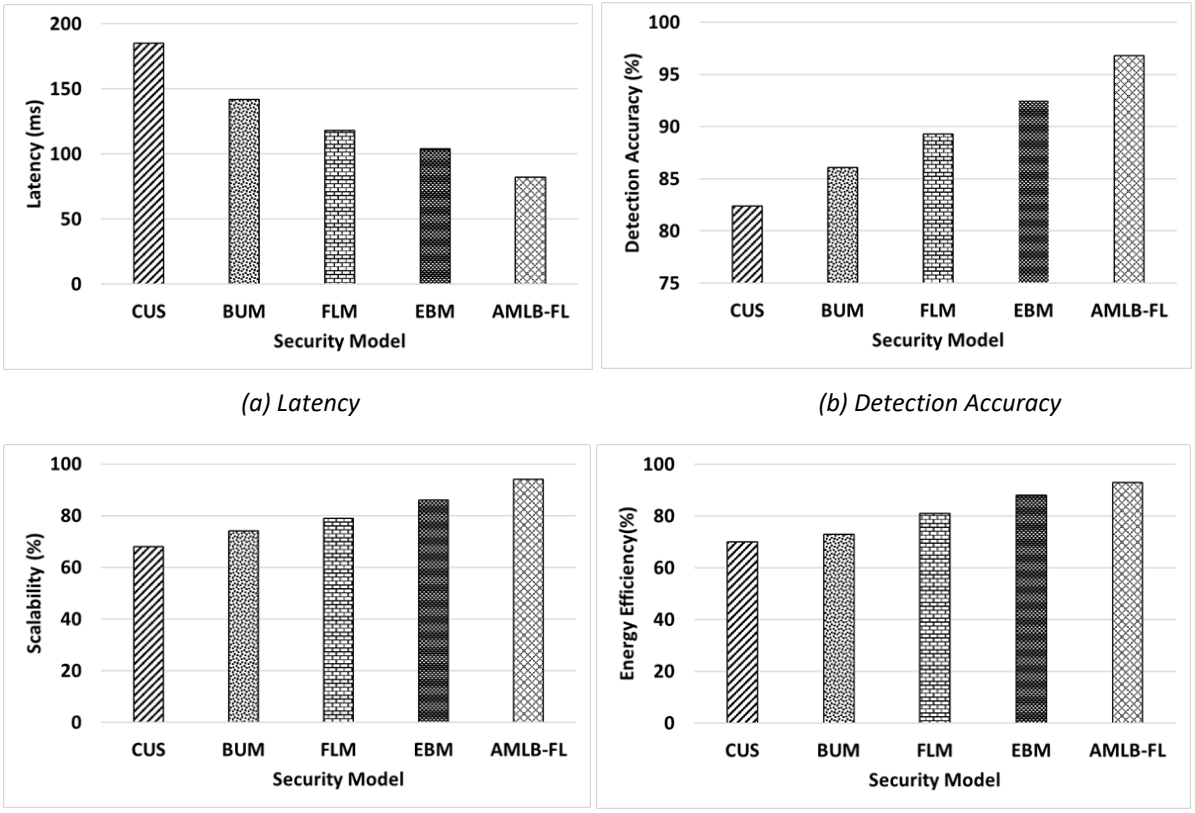


Figure 1. Architecture

The control layer is responsible for facilitating smart-contract based access control followed by evaluation of trust as well as authenticating UAV nodes. The consensus layer validates records of data exchange by UAV network system by using lightweight Delegated Proof-of-Stake (DPoS) blockchain. The latency is further controlled using updates from federated model. The learning layer collaborates federated learning towards adaptive routing and joint anomaly detection without any dependency for forwarding original UAV data. Apart from this, both federated learning operations and computationally intensive blockchain are dynamically transferred to edge server (i.e., ground station) using adaptive offloading module based on processing constraint, bandwidth, and energy.

Result Analysis

The assessment has been performed using standard and benchmark CICoD2023 dataset that consists of both normal traffic details of UAV as well as different cases of cyberattacks. The simulation study has been performed using both MATLAB and Python where TensorFlow library has been used for implementing federated learning. Using normal 64-bit windows machine, the experiment has been performed considering following configuration of hyperparameters viz. batch size=32, learning rate=0.001, aggregation rounds of federated learning=100, adaptive offloading threshold=0.65, and validator count of DPoS=15. Further comparative analysis has been carried out with four baseline models viz. i) Centralized UAV security (CUS), ii) Blockchain-only UAV Model (BUM), iii) Federated Learning-only Model (FLM), and iv) Edge-assisted Blockchain-FL Model (EBM). The assessment is done via energy efficiency, scalability, detection accuracy, and latency.



(a) Latency *(b) Detection Accuracy*

(c) Scalability *(d) Energy Efficiency*

Figure 2. Benchmarked Study Outcome

The accomplished outcome of the study infers that proposed system achieves 40.25% of minimized latency, 10.53% of increased accuracy, 22.48% of enhanced scalability, and 19.23% of increased energy efficiency in contrast to mean of all baseline models. It has been noted that CUS approach showcased minimized scalability and increased latency as all mechanism of decision-making operations, monitoring, and authentication is highly dependent upon centralized servers that give rise to single-point failures or communication bottlenecks when exposed to environments with dense UAVs. The BUM framework is noted to enhanced communication integrity and better trust management via distributed ledgers and yet increased energy consumption and maximized computational overhead surfaces in low-resource UAV nodes due to continuous consensus validation and blockchain synchronization. The FLM model facilitates local model training and hence it experiences minimized communication overhead; however, lack of efficient verification for federated updates lead this model to be highly susceptible to unreliable model aggregation. This degrades the detection accuracy score for FLM model. Further, it was observed that issues related to computational limitation is partially mitigated by EBM models via distribution of static task and with assistance from edge nodes. However, inadequate adaptive coordination minimizes its effectiveness when subjected to conditions of dynamic mobility of UAV nodes.

On the contrary, proposed AMLB-FL model is observed with better performance which is mainly due to collaboration with adaptive offloading methods, federated anomaly learning, and DPoS blockchain validation. All these operation takes place in 3-layer architecture. The verification process that is aided with blockchain is noted with an enhanced reliability of federated updates yielding to increase detection

accuracy while the edge server are assigned with learning task and intensive blockchain allocated by adaptive offloading strategy depending upon processing condition, bandwidth, and UAV energy. This results in minimization of excessive resource utilization onboard UAV nodes that also leads to increased energy efficiency and maximized scalability with reduced delay even in presence of UAV networks with higher range of dynamicity. Table 1 showcases that proposed AMLB-FL offers

Table 1. Comparison with State-of-the-art-methods

Feature/Capability	**CUS**	**BUM**	**FLM**	**EBM**	**AMLB-FL**
Trust Management	Centralized Control	Blockchain Trust	No Validation	Partial Verification	Secure FL-Blockchain
Scalability	Low Scalability	Consensus Overhead	Resource Limited	Partial Offloading	Adaptive Offloading
Privacy Detection	Low Privacy	Moderate Privacy	Unverified FL	Secure Edge-FL	Verified Federated Detection

Conclusion

The proposed model of AMLB-FL presents a novel secure UAV network communication system by integrating adaptive resource optimization, distributed intelligence, and trust management. Different from baselines (CUS, BUM, FLM, EBM), proposed model uses blockchain for validating updates of federated learning apart from its immutability property. The model contributes to adaptive offloading policy where computation is intelligently distributed over ground station, edge server and UAV nodes considering states of real-time resources. Effective privacy preservation within anomaly detection is presented without sharing any original network data leading to increased reliability.

References

1. J. Medhi, R. Liu, Q. Wang, and X. Chen, “A lightweight and efficient intrusion detection system (IDS) for unmanned aerial vehicles,” Neural Comput. Appl., vol. 37, no. 20, pp. 15819–15836, 2025, doi: 10.1007/s00521-025-11276-5.
2. L. Chen, W. Zhai, X. Bu, M. Sun, and C. Zhu, “A lightweight robust training method for defending model poisoning attacks in federated learning assisted UAV networks,” Drones, vol. 9, no. 8, p. 528, 2025, doi: 10.3390/drones9080528
3. A. Pithani and R. R. Rout, “FedSyPo: Detection of Sybil-Poisoning attack in federated leaning on non-IID data for 6G-based IoT-Edge Network,” Comput. Netw., vol. 272, no. 111656, p. 111656, 2025, doi: 10.1016/j.comnet.2025.111656.
4. K. W. Goh, B. U. I. Khan, A. R. Khan, D. S. Putra, S. Sankaranarayanan, and M. A. Bhuyian, “3L-BC: a three-layer blockchain architecture for collaborative machine learning in secure drone communications,” J. King Saud Univ. - Comput. Inf. Sci., vol. 37, no. 8, 2025, doi: 10.1007/s44443-025-00197-x
5. Y. Liu, H. Zhang, M. Wang, Q. Xie, and Z. Sun, “AntidoteFL: Enhancing defense against poisoning attacks in federated learning,” Comput. Netw., vol. 269, no. 111427, p. 111427, 2025, doi: 10.1016/j.comnet.2025.111427