Blockchain-Based Federated Learning System in UAV-MEC Networks

Subjects: Computer Science, Information Systems
Contributor: Chaoyang Zhu, Xiao Zhu, Tuanfa Qin

The widespread use of UAVs in smart cities for tasks like traffic monitoring and environmental data collection creates significant privacy and security concerns due to the transmission of sensitive data. Traditional UAV-MEC systems with centralized data processing expose this data to risks like breaches and manipulation, potentially hindering the adoption of these valuable technologies. UBFL, is a novel privacy-preserving federated learning mechanism that integrates blockchain technology for secure and efficient data sharing. Unlike traditional methods relying on differential privacy (DP), UBFL employs an adaptive nonlinear encryption function to safeguard the privacy of UAV model updates while maintaining data integrity and accuracy.

Keywords: unmanned aerial vehicles ; data privacy ; federated learning ; blockchain

1. Introduction

Unmanned aerial vehicles (UAVs) have emerged as a crucial innovation in wireless communication networks, offering significant benefits such as easy deployment, improved mobility, and direct connectivity with a clear line of sight. This technological advancement has sparked a notable increase in both academia and industry's focus on UAV wireless communication networks. In this field, UAV-assisted Mobile Edge Computing network (UAV-MEC) has gained recognition as a transformative concept. MEC utilizes artificial intelligence (AI) to process the vast amount of data collected by widespread drone networks, enabling the provision of intelligent services [1]. However, deploying these edge computing networks in potentially hostile environments presents various security and privacy challenges. Innovative methods are crucial to safeguard data privacy, maintain model accuracy, and enable robust data processing auditability within the UAV-MEC network [2].

Federated learning (FL) emerges as a novel AI approach that utilizes decentralized data and training [3][4]. It empowers UAVs to leverage their locally collected data to build localized deep learning models. These models are then transmitted to a central node for aggregation, resulting in a global model. Ntizikira et al. [5] proposed the SP-IoUAV model, combining FL with CNN-LSTM networks to achieve both operational security and data privacy in the Internet of Unmanned Aerial Vehicles (IoUAV). This model outperforms previous approaches with its real-time anomaly detection and multi-factor authentication capabilities. Ref. [6] explores a group signature-based algorithm for federated learning in FANETs, highlighting its ability to safeguard node identities, minimize communication overhead, and improve security and privacy.

However, existing FL approaches in UAV-MEC networks face security and privacy risks due to the large number of UAVs and need for real-time response [7][8]. The central curator, which aggregates insights from distributed UAV nodes, is often a primary target for cyber-attacks, jeopardizing the integrity and confidentiality of the collective learning process [9]. Moreover, the system's reliance on accurately recording contributions from diverse UAVs introduces vulnerabilities, as malicious entities can manipulate or falsify their contributions, resulting in skewed or compromised learning outcomes [6].

Blockchain technology offers a promising solution by enabling secure and decentralized data sharing, mitigating central server vulnerabilities, and facilitating tamper-proof record keeping of transactions through its immutability and auditability features [10]. This paves the way for enhanced security and privacy in collaborative learning within UAV-MEC networks. Ref. [11] proposes FedEx, a novel FL framework that utilizes mobile transporters to establish indirect communication channels between server and clients, achieving convergence in both synchronous and asynchronous versions.

Nevertheless, deploying blockchain-based FL (BFL) in UAV-MEC networks confronts various hurdles, including limited computational resources on UAVs, potential scalability issues with large numbers of participants, and inherent trade-offs between security and performance [12]. In certain fields, like healthcare, the integration of BFL is further complicated by the limited availability of data from various sources, such as hospitals and clinics [13]. Furthermore, the Internet of Things

(IoT) environment presents its own unique set of challenges, including concerns regarding security and privacy [14][15]. Another challenge in federated learning is ensuring the quality of local training data, as there is no control over the data used for training.

2. UAV-Enabled Mobile Edge Computing

Mobile Edge Computing (MEC) signifies a transformative shift in cloud computing, strategically situating computing and storage resources within the radio access network. This paradigm is instrumental in propelling applications, data, and services proximally to mobile users, thereby offering substantial reductions in latency, enhanced location awareness, and alleviated network congestion. This approach marks a significant departure from the traditional centralized cloud services, introducing a new dimension of efficiency and responsiveness in mobile computing. The integration of MEC nodes at the edge of UAV networks, as comprehensively analyzed in [16], proposes a UAV-assisted MEC offloading scheme, specifically designed to minimize task completion time for computation-intensive IoT tasks. Furthermore, Refs. [17][18] have developed a mobility-aware caching scheme within UAV networks enabled by MEC. This scheme is meticulously tailored to optimize content placement, trajectory planning, and bandwidth allocation, thereby minimizing latency and enhancing overall network performance.

3. Privacy Preserving of Federated Learning for Wireless Nework

Federated Learning emerges as a cutting-edge distributed machine learning approach, wherein participants engage in training local data and subsequently upload updated parameters to a centralized server for aggregation [19][20]. This innovative approach not only enhances learning efficiency but also effectively resolves the challenges of data silos and fortifies local data privacy, thereby representing a significant advancement over traditional machine learning paradigms. In contemporary neural network models, gradient descent is employed for parameter updates. However, this process poses a risk, as the exposure of participant gradients can inadvertently lead to the leakage of sensitive network parameters [21] [22]. In [23], the paper proposes a channel-aware distribution and aggregation scheme to enforce equal contribution from all devices in the FL training as a means to resolve the global bias problem of aerial FL in large-scale UAV networks.

Differential privacy emerges as a pivotal concept designed to quantify and mitigate the risks associated with personal information exposure. It provides a robust privacy framework, employing sophisticated randomization techniques. The integration of differential privacy mechanisms within federated learning perturbs model parameters, thus safeguarding users' private training data while still enabling the collaborative training of an accurate shared model [24][25]. This strategic approach effectively addresses the privacy concerns that have been a significant impediment to the real-world deployment of federated learning systems. Ref. [26] proposes DPFed, a differential private federated learning algorithm using the moments accountant technique. This achieves tighter privacy guarantees while preserving high model utility. Ref. [27] develops a Laplace mechanism-based differential private algorithm for federated learning. This leverages the exponential mechanism to preserve user privacy in model training.

In summary, while existing studies demonstrate that differential privacy can facilitate privacy-preserving federated learning, there is a pressing need for more comprehensive evaluations that consider factors such as single points of failure. Moreover, the differential privacy algorithm faces significant challenges due to its over-reliance on empirical methods for the selection of differential parameters.

4. Blockchain-Enabled UAV Federated Learning

Blockchain technology, characterized by its decentralization, immutability, and distributed ledger features, functions as a digital transaction ledger that is replicated and shared across network nodes, thereby eliminating the necessity for a central authority.

Its applicability in UAV scenarios is particularly highlighted by these inherent features. Ref. [28] proposes a blockchain-based incentive mechanism for UAV networks using a privacy-aware auction and consensus algorithm. This approach introduces a privacy-respecting reward mechanism to stimulate participation. Ref. [29] develops a distributed path planning and target tracking algorithm for UAVs using smart contracts on blockchain. This preserves participants' privacy while enabling real-time path optimization in a collaborative manner.

Overall, these studies underscore the advantages of blockchain in enhancing UAV privacy, security, and reliability. However, to validate their applicability in real-world scenarios, larger-scale experiments that consider practical constraints, such as energy consumption and flight dynamics, are essential. Additionally, there is a need for an in-depth analysis of the

optimized trade-offs between privacy/security and energy efficiency to further solidify these findings, as will be discussed in the subsequent section.

5. Anomaly Detection Using Random Cut Forest

Random Cut Forest (RCF) is an advanced unsupervised algorithm designed for anomaly detection within datasets, identifying data points that significantly deviate from established patterns or structures [30][31]. Anomalies, such as unexpected spikes in time series data or atypical data points, can drastically increase the complexity of machine learning tasks [32].

RCF assigns an anomaly score to each data point, where low scores denote normality and high scores indicate the presence of anomalies. The determination of these scores is application-specific, but typically, scores exceeding three standard deviations from the mean are considered anomalous. RCF's adaptability extends to handling multi-dimensional input, setting it apart from many algorithms that are confined to one-dimensional time series data. Amazon SageMaker's implementation of RCF demonstrates effective scalability with respect to the number of features, dataset size, and the number of instances.

The fundamental principle of RCF involves constructing a forest of trees, each originating from a partition of a sample of the training data. For instance, a random sample is divided according to the number of trees in the forest, with each tree organizing its subset of points into a k-d tree. The anomaly score for a data point is determined by the expected change in the tree's complexity upon incorporating that point, inversely proportional to the point's depth in the tree. RCF calculates an anomaly score by averaging the scores from each constituent tree and scaling the result in relation to the sample size.

References

1. Shakhatreh, H.; Sawalmeh, A.H.; Al-Fuqaha, A.; Dou, Z.; Almaita, E.K.; Khalil, I.M.; Othman, N.S.; Khreishah, A.; Guizani, M. Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges. IEEE Access 2019, 7, 48572–48634.
2. Zhou, Y.; Pan, C.; Yeoh, P.L.; Wang, K.; Elkashlan, M.; Vucetic, B.; Li, Y. Secure communications for uav-enabled mobile edge computing systems. IEEE Trans. Commun. 2020, 68, 376–388.
3. McMahan, H.B.; Yu, F.; Richtarik, P.; Suresh, A.; Bacon, D. Federated learning: Strategies for improving communication efficiency. In Proceedings of the 29th Conference on Neural Information Processing Systems (NIPS), Barcelona, Spain, 5–10 December 2016; pp. 5–10.
4. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.y. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
5. Ntizikira, E.; Lei, W.; Alblehai, F.; Saleem, K.; Lodhi, M.A. Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. Sensors 2023, 23, 8077.
6. Kanchan, S.; Choi, B.J. An efficient and privacy-preserving federated learning scheme for flying ad hoc networks. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 1–6.
7. Benmalek, M.; Benrekia, M.A.; Challal, Y. Security of federated learning: Attacks, defensive mechanisms, and challenges. Rev. d'Intell. Artif. 2022, 36, 49–59.
8. Brik, B.; Ksentini, A.; Bouaziz, M. Federated learning for uavs-enabled wireless networks: Use cases, challenges, and open problems. IEEE Access 2020, 8, 53841–53849.
9. Liao, J.; Jiang, B.; Zhao, P.; Ning, L.; Chen, L. Unmanned aerial vehicle-assisted federated learning method based on a trusted execution environment. Electronics 2023, 12, 3938.
10. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
11. Bian, J.; Shen, C.; Xu, J. Federated learning via indirect server-client communications. In Proceedings of the 2023 57th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 22–24 March 2023; pp. 1–5.
12. Oktian, Y.E.; Lee, S.-G. Blockchain-based federated learning system: A survey on design choices. Sensors 2023, 23, 5658.

13. Shaikh, J.A.; Wang, C.; Khan, M.A.; Mohsan, S.A.H.; Ullah, S.; Chelloug, S.A.; Muthanna, M.S.A.; Muthanna, A. A uav-assisted stackelberg game model for securing lomt healthcare networks. Drones 2023, 7, 415.
14. Xiong, H.; Qu, Z.; Huang, X.; Yeh, K.-H. Revocable and unbounded attribute-based encryption scheme with adaptive security for integrating digital twins in internet of things. IEEE J. Sel. Areas Commun. 2023, 41, 3306–3317.
15. Xiong, H.; Wang, H.; Meng, W.; Member, K.-H.Y. Attribute-based data sharing scheme with flexible search functionality for cloud assisted autonomous transportation system. IEEE Trans. Ind. Inform. 2023, 19, 10977–10986.
16. Zhou, F.; Hu, R.Q.; Li, Z.; Wang, Y. Mobile edge computing in unmanned aerial vehicle networks. IEEE Wirel. Commun. 2020, 27, 140–146.
17. Yang, L.; Yao, H.; Wang, J.; Jiang, C.; Benslimane, A.; Liu, Y. Multi-uav-enabled load-balance mobile-edge computing for iot networks. IEEE Internet Things J. 2020, 7, 6898–6908.
18. Wang, S.; Zhang, X.; Zhang, Y.; Wang, L.; Yang, J.; Wang, W. A survey on mobile edge networks: Convergence of computing, caching and communications. IEEE Access 2017, 5, 6757–6779.
19. Niknam, S.; Dhillon, H.S.; Reed, J.H. Federated learning for wireless communications: Motivation, opportunities, and challenges. IEEE Commun. Mag. 2020, 58, 46–51.
20. Tran, N.H.; Bao, W.; Zomaya, A.Y.; Nguyen, M.N.H.; Hong, C.S. Federated learning over wireless networks: Optimization model design and analysis. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 1387–1395.
21. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-preserving blockchain-based federated learning for traffic flow prediction. Future Gener. Comput. Syst. 2021, 117, 328–337.
22. Liu, H.; Zhang, S.; Zhang, P.; Zhou, X.; Shao, X.; Pu, G.; Zhang, Y. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. IEEE Trans. Veh. Technol. 2021, 70, 6073–6084.
23. Zhagypar, R.; Kouzayha, N.; ElSawy, H.; Dahrouj, H.; Al-Naffouri, T.Y. Characterization of the global bias problem in aerial federated learning. IEEE Wirel. Commun. Lett. 2023, 12, 1339–1343.
24. Hao, M.; Li, H.; Xu, G.; Liu, S.; Yang, H. Towards efficient and privacy-preserving federated deep learning. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
25. Xiang, L.; Yang, J.; Li, B. Differentially-private deep learning from an optimization perspective. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 559–567.
26. Jia, B.; Zhang, X.; Liu, J.; Zhang, Y.; Huang, K.; Liang, Y. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot. IEEE Trans. Ind. Inform. 2022, 18, 4049–4058.
27. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farhad, F.; Jin, S.; Quek, T.Q.S.; Poor, H.V. Federated learning with differential privacy: Algorithms and performance analysis. IEEE Trans. Inf. Forensics Secur. 2019, 15, 3454–3469.
28. Toyoda, K.; Zhang, A.N. Mechanism design for an incentive-aware blockchain-enabled federated learning platform. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 395–403.
29. Aloqaily, M.; Bouachir, O.; Boukerche, A.F.M.; Ridhawi, I.A. Design guidelines for blockchain-assisted 5g-uav networks. IEEE Netw. 2021, 35, 64–71.
30. Guha, S.; Mishra, N.; Roy, G.; Schrijvers, O. Robust random cut forest based anomaly detection on streams. In Proceedings of the International Conference on Machine Learning, New York, NY, USA, 19–24 June 2016; pp. 2712–2721.
31. Yeom, S.; Jung, J.-H. Weighted random cut forest algorithm for anomaly detection. arXiv 2022, arXiv:2202.01891.
32. Kumar, S.; Dua, S.; Rastogi, S. Anomaly detection: A machine learning and deep learning perspective. In Proceedings of the 2023 International Conference on Computer, Electronics & Electrical Engineering & Their Applications (IC2E3), Srinagar Garhwal, India, 8–9 June 2023; pp. 1–6.

Retrieved from https://encyclopedia.pub/entry/history/show/126077