IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 1, May 2023

# Securing Federated Learning Based on Blockchain Technology

Aswin K[1], Kamali R[2], Kurin Firathos S[3], Jeevitha G[4], Nandhini E[5]

Faculty, Department of Computer Science & Engineering[1]
Students, Department of Computer Science & Engineering[2,3,4,5]
Dhanalakshmi Srinivasan Engineering College, Perambalur, India

**Abstract***:* *A blockchain-based federated learning approach with secure aggregation in a trusted execution environment for the Internet of Things (IoT). The proposed approach aims to address the privacy and security concerns associated with federated learning in IoT environments. The approach involves using a blockchain to store the learning model and to maintain a distributed ledger of transactions. The learning model is trained on local IoT devices using federated learning techniques, with each device contributing its local data. The aggregation of the model updates is performed securely within a trusted execution environment, using homomorphism encryption and secret sharing techniques. The proposed approach offers several advantages over traditional federated learning approaches, including improved privacy and security, increased scalability, and enhanced trustworthiness. It also enables the creation of a decentralized and democratic learning environment, where each device has an equal say in the learning process.*

*The approach is evaluated using a real-world dataset, and the results demonstrate its effectiveness in terms of accuracy and privacy preservation. The paper concludes that the proposed approach has the potential to enable secure and scalable federated learning in IoT environments, with applications in healthcare, smart cities, and other domains.*

*This paper offers a blockchain-based federated learning (FL) framework with an Intel Software Guard Extension (SGX)-based trusted execution environment (TEE) for safely aggregating local models in the Industrial Internet of Things (IoT) Local models in FL can be modified with by attackers. As a result, a global model derived from manipulated local models may be incorrect. As a result, the proposed system makes use of a blockchain network to secure model aggregation. Each blockchain node contains an SGX-enabled CPU that secures the FL-based aggregating processes required to construct a global model. Blockchain nodes may validate the aggregated model's validity, perform a blockchain consensus method to secure the model's integrity, and add it to the distributed ledger for tamper-proof storage. . Before utilising the aggregated model, each cluster can acquire it from the blockchain and validate its fidelity. To assess the performance of the proposed system, we ran many experiments using various CNN models and datasets.*

**Keywords:** Blockchain

## REFERENCES

[1]. M. Alazab, S. P. RM, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, “Federated learning for cybersecurity: Concepts, challenges and future directions,” IEEE Trans. Ind. Inform., vol. 18, no. 5, pp. 3501–3509, May 2022.

[2]. L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, “Exploiting unintended feature feakage in collaborative Slearning,” in Proc. IEEE Symp. Secur. Privacy, 2019, pp. 691–706.

[3]. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, May 2020.

[4]. L. Yin, J. Feng, H. Xun, Z. Sun, and X. Cheng, “A privacy-preserving federated learning for multiparty data sharing in social IoTs,” IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2706–2718, Jul.–Sep. 2021.

DOI: 10.48175/IJARSCT-9705

**[5].** Y. Liu, J. Nie, X. Li, S. H. Ahmed, W. Y. B. Lim, and C. Miao, "Federated learning in the sky: Aerial-ground air quality sensing framework with UAV swarms," IEEE Internet Things J., vol. 8, no. 12, pp. 9827–9837, Jun. 2021.

**[6].** Lin Tao, Kong Lingjing, Sebastian U Stich and Martin Jaggi, "Ensemble Distillation for Robust Model Fusion in Federated Learning", Advances in Neural Information Processing Systems, 2020.

**[7].** Swaroop Ramaswamy, Rajiv Mathews, Kanishka Rao and Françoise Beaufays, "Federated learning for emoji prediction in a mobile keyboard", arXiv preprint, 2019.

**[8].** Hongyi Wang, Mikhail Yurochkin, Yuekai Sun, Dimitris Papailiopoulos and Yasaman Khazaeni, "Federated Learning with Matched Averaging", Inter- national Conference on Learning Representations, 2020.

**[9].** M. Alazab, S. P. RM, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, "Federated learning for cybersecurity: Concepts, challenges and future directions," IEEE Trans. Ind. Inform., vol. 18, no. 5, pp. 3501–3509, May 2022

**[10].** T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, May 2020.

DOI: 10.48175/IJARSCT-9705