FEDERATED LEARNING FOR SECURE AND PRIVACY-AWARE AI IN NEXT-GENERATION TELECOM NETWORKS

Khaydaraliyeva Khilola Farhod qizi
Tashkent University of Information Technologies named after Muhammad al Khwarazmiy Assistent
hilolahaydaraliyeva@gmail.ru
Ergashova Durdona Khusniddin kizi
Tashkent University of Information Technologies named after Muhammad al Khwarazmiy 3rd year student of the Faculty of Mobile Communication Technology
durdonaergasheva676@gmail.com

Abstract. *As artificial intelligence becomes central to telecom service optimization and personalization, ensuring the privacy of user data is a growing challenge. Traditional centralized machine learning methods require raw data aggregation, exposing sensitive information and risking regulatory violations. This paper presents a federated learning (FL) approach tailored for telecom environments, enabling AI model training directly on distributed user devices without transferring personal data to central servers. The proposed system integrates differential privacy and secure aggregation mechanisms to enhance protection while preserving model performance. Experimental evaluations using synthetic mobile usage data demonstrate that our FL models achieve up to 96% of the accuracy of centralized baselines, while significantly reducing privacy leakage risks. The results confirm that federated learning is a scalable, privacy-preserving solution for AI-driven telecom services that aligns with global data protection standards.*

Keywords: *Federated Learning, User Privacy, AI in Telecom, Secure Aggregation, GDPR Compliance, Edge Intelligence, Differential Privacy*

Introduction

The rise of artificial intelligence (AI) in the telecommunications sector has enabled advanced features such as predictive network maintenance, intelligent traffic routing, and personalized service delivery. These innovations rely heavily on the analysis of vast amounts of user-generated data collected through mobile applications, devices, and network logs. However, this data often contains sensitive information such as location, usage behavior, and personal preferences, raising significant concerns about user privacy and data protection.

Traditional AI development in telecom environments typically involves centralized machine learning models, where raw user data is transmitted to a central server for training. While effective in performance, this approach poses major privacy risks and may violate data protection regulations such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), and similar laws worldwide.

Moreover, the growing public demand for digital privacy and transparency has pressured telecom operators to seek alternative, privacy-preserving solutions.

Federated Learning (FL) emerges as a promising paradigm to address these challenges. Instead of centralizing raw data, FL enables distributed model training across edge devices (e.g., smartphones, IoT nodes, or base stations), where only encrypted model updates are shared with a central aggregator. This decentralized approach not only enhances data privacy but also reduces the risk of large-scale data breaches and lowers bandwidth consumption.

This study investigates the design and implementation of a federated learning framework specifically tailored to AI-driven telecom services. We aim to demonstrate that FL can maintain high model accuracy while significantly improving user data privacy. To further strengthen the privacy guarantees, we integrate differential privacy and secure aggregation techniques into the system architecture. Through simulations on telecom usage data, we evaluate the trade-offs between privacy, accuracy, and communication efficiency, highlighting the practical viability of federated learning in future telecom infrastructures.

Results

The proposed federated learning (FL) framework was evaluated through extensive simulations involving 1,000 distributed clients simulating mobile user devices. The results demonstrate that FL can deliver high model performance while preserving user privacy and ensuring communication efficiency.

3.1 Model Accuracy and Convergence

The FL model trained on distributed telecom usage data achieved a test accuracy of **91.7%**, which is approximately **96%** of the performance of a centralized model trained on the same data. The model converged in **28 global training rounds**, demonstrating stable learning behavior under non-iid (non-identically distributed) data conditions—common in telecom environments where user behavior varies widely.

Model Type	Test Accuracy	Rounds to Converge
Centralized	95.5%	—
Federated (no DP)	93.8%	25
Federated + DP (ε=3)	91.7%	28

The framework scaled effectively to **10,000 simulated clients**, maintaining stability in training accuracy and convergence. Variance across clients was handled via **adaptive client sampling**, ensuring consistent contributions from a representative subset of devices.

Conclusion

This study presents a federated learning (FL) framework tailored to the unique privacy, performance, and scalability requirements of AI-driven telecom services. By decentralizing model training and keeping user data on local devices, the proposed approach effectively addresses key privacy concerns while preserving high model accuracy. The integration of differential privacy and secure aggregation further strengthens the system's protection against inference attacks and data leakage.

Simulation results confirm that FL can achieve over 90% model accuracy compared to centralized baselines, with significantly reduced privacy risks and manageable communication costs. These findings highlight FL's practical potential for enabling intelligent telecom services—such as service recommendations and network optimization—without violating data protection regulations or user trust.

Going forward, federated learning offers a sustainable and user-respecting pathway for telecom operators as they transition toward 5G/6G networks, edge intelligence, and regulatory compliance. Continued research into efficient model architectures, adaptive communication strategies, and real-world deployment scenarios will be essential to realizing the full benefits of FL in next-generation telecommunications.

REFERENCES

1. H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.
2. J. Konecny, H. B. McMahan, F. X. Yu, P. Richtarik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," arXiv preprint arXiv:1610.05492, 2016.
3. N. D. Lane, A. Bhattacharya, S. Georgiev, and P. K. Ravi, "An early resource characterization of deep learning on wearables, smartphones and Internet-of-Things devices," in Proc. 2015 Int. Conf. Internet of Things Design and Implementation (IoTDI), 2015, pp. 1–10.
4. R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. 22nd ACM SIGSAC Conf. Computer and Communications Security (CCS), 2015, pp. 1310–1321.
5. C. Dwork, A. Roth, "The algorithmic foundations of differential privacy," Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.
6. K. Bonawitz et al., "Practical secure aggregation for privacy-preserving machine learning," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), 2017, pp. 1175–1191.
7. S. Wang, T. Tuor, T. Salonidis, K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205–1221, Jun. 2019.
8. Google AI Blog, "Federated Learning: Collaborative Machine Learning without Centralized Training Data," Apr. 2017. [Online]. Available: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

9. G. Zhu, D. Liu, Y. Du, C. You, J. Zhang, and K. Huang, "Towards federated learning in 6G: A survey," IEEE Internet of Things Journal, vol. 8, no. 22, pp. 15784–15816, 2021.

10. European Commission, "General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://gdpr.eu/