Adapting Federated Learning to Dynamic and Non-Stationary Data: An Online Learning Approach

Jaemin Kim
Dept. of Computer Science and Engineering
Chung-Ang University
Seoul, Korea
jmkim@uclab.re.kr

Donghyeon Hur
Dept. of Computer Science and Engineering
Chung-Ang University
Seoul, Korea
dhhur@uclab.re.kr

Dongwook Won
Dept. of Computer Science and Engineering
Chung-Ang University
Seoul, Korea
dwwon@uclab.re.kr

Sungrae Cho
Dept. of Computer Science and Engineering
Chung-Ang University
Seoul, Korea
srcho@cau.ac.kr

***Abstract*—Online learning-based optimization represents a novel approach that integrates the principles of federated learning and online learning to effectively handle dynamic data distributions and continuous learning scenarios. This paper offers a comprehensive survey of the latest developments in online federated learning, focusing on optimizing communication efficiency in federated learning environments through online learning techniques. We delve into foundational concepts, key methodologies, challenges, and diverse applications of this emerging field.**

***Index Terms*—Federated Learning, Online Learning, Online Federated learning.**

I. Introduction

Federated Learning (FL) and Online Learning are two critical paradigms in modern distributed machine learning. Each addresses distinct challenges in data privacy, adaptability, and real-world applicability. Their integration forms the foundation of Online Federated Learning (OFL), which combines the strengths of both approaches [1]–[4].

Federated Learning is a decentralized machine learning framework that enables multiple devices or clients to collaboratively train a shared model without exposing their local data. By keeping data on-device, FL preserves user privacy and adheres to data governance regulations [4]–[6]. This approach is particularly beneficial in privacy-sensitive domains like healthcare, finance, and personal device applications. The central server aggregates locally trained models from clients to construct a global model, typically using algorithms like FedAvg [7]. However, traditional FL operates under the assumption of static, stationary data distributions, limiting its applicability in dynamic environments [2].

In many real-world applications, data distributions are not only non-stationary but also vary significantly over time due to external factors such as user behavior, environmental changes, and evolving application requirements [8]. For instance, in autonomous vehicles, data related to traffic patterns, weather conditions, and road hazards change continuously. Similarly, wearable health devices must adapt to variations in user activity and physiological states. These scenarios highlight the limitations of static FL and underscore the need for a more flexible approach that can accommodate changing data patterns and maintain robust performance over time [9].

Online Learning is a paradigm that allows models to learn incrementally from a continuous stream of data. Instead of training on a fixed dataset, models update as new data arrives, making this approach well-suited for non-stationary and time-sensitive environments [10]. Online learning excels in applications where rapid adaptation is critical, such as stock market prediction, anomaly detection, and personalized recommendation systems. However, its focus on single-device learning often overlooks privacy and scalability, which are essential in distributed systems [11].

The objectives of this study are threefold:

- To provide a comprehensive understanding of online federated learning, including its fundamental principles and integration strategies.
- To analyze key challenges and methodologies, such as communication optimization, privacy protection, and robustness to dynamic data.
- To examine practical applications across various domains and propose future directions for research and development.

The combination of these two paradigms addresses their individual limitations while leveraging their strengths. By incorporating online learning principles into FL, it becomes possible to adapt to dynamic, non-stationary data environments while maintaining the privacy-preserving and distributed nature of FL. This integration, termed Online Federated Learning, enables:

- **Adaptability**: Models that continuously evolve with new

data.

- **Privacy-Preservation**: Training without exposing raw data.
- **Efficiency**: Optimized communication and computational resources.

This paper aims to explore the methodologies, challenges, and applications of Online Federated Learning, with a particular focus on optimizing communication efficiency, handling non-IID data, and ensuring robust privacy protection.

II. Literature Review

A. Integration of Online Learning and Federated Learning

The integration of online learning and federated learning represents a significant advancement in distributed machine learning [12], [10]. Traditional FL operates in iterative rounds, where clients locally train models using static data and send updates to a central server for aggregation. This approach works well in controlled environments but struggles with dynamic data streams, where frequent updates and non-stationary distributions are common [2].

Online federated learning (OFL) modifies this paradigm by incorporating online learning principles, enabling incremental updates to the global model. This continuous learning approach allows models to adapt to changes in real-time without requiring retraining from scratch [9]. However, achieving this adaptability while maintaining the core benefits of FL—such as data privacy and communication efficiency—requires careful consideration of several factors:

- **Dynamic Aggregation**: Unlike traditional FL, where aggregation occurs at fixed intervals, OFL necessitates adaptive aggregation methods. These methods must account for client availability, data heterogeneity, and the temporal relevance of updates. Techniques such as weighted averaging and time-sensitive aggregation are commonly employed to enhance the relevance of updates [13].
- **Client Selection**: Effective client selection is critical to reducing communication overhead while maximizing model performance. Clients with significant updates or those representing diverse data distributions should be prioritized. Adaptive algorithms, such as reinforcement learning-based selection, have shown promise in optimizing this process [11].
- **Scalability**: As the number of participating clients increases, managing communication and computation demands becomes challenging. Hierarchical FL architectures, where local aggregations occur before global updates, provide a scalable solution for large-scale deployments [14].

This integration also demands robust solutions for handling non-IID data distributions, a common characteristic in FL environments. Clients often generate data reflecting unique local patterns, which can lead to biased global models if not addressed. Meta-learning approaches, personalized models, and adaptive learning rates are among the strategies employed to mitigate this issue.

B. Communication Efficiency, Privacy, and Robustness

Communication overhead is a major challenge in OFL, particularly in resource-constrained environments [12], [14] .Frequent model updates can strain network resources and impact latency-sensitive applications. Strategies to enhance communication efficiency include:

- **Gradient Compression**: Techniques like sparsification and quantization reduce the size of model updates, minimizing transmission costs. These methods balance communication savings with potential impacts on model accuracy [14].
- **Periodic Updates**: Aggregating updates at defined intervals, rather than continuously, reduces communication frequency. Adaptive thresholds can further optimize this process by aggregating only when significant updates are available. [10]
- **Federated Averaging Variants**: Modifications to the FedAvg algorithm, such as FedProx and FedNova, address inefficiencies in handling heterogeneous data and communication intervals. [7]

While FL inherently enhances privacy by keeping data local, the continuous interactions in OFL introduce new vulnerabilities [6]. For instance, frequent updates increase the risk of model inversion attacks, where adversaries reconstruct private data from shared gradients. Advanced techniques are needed to address these risks:

- **Secure Aggregation**: Encrypting updates ensures that individual contributions remain confidential [4]. Protocols like secure multi-party computation (SMPC) provide robust protection against data leakage.
- **Differential Privacy**: By adding noise to model updates, differential privacy guarantees that individual data points cannot be inferred from the aggregated model. This approach balances privacy and utility, ensuring meaningful contributions to the model while safeguarding client data [4].

OFL must also contend with robustness issues arising from non-IID data, adversarial attacks, and unreliable clients. Techniques such as robust optimization, anomaly detection, and adversarial training improve model stability and reliability. Additionally, reinforcement learning can be integrated to adaptively adjust learning parameters, further enhancing robustness.

III. Conclusion

Online learning-based federated learning represents a paradigm shift in distributed machine learning, addressing the limitations of traditional FL in dynamic environments. By integrating online learning principles, OFL achieves adaptability, efficiency, and privacy preservation in scenarios involving non-stationary and heterogeneous data.

Despite its potential, several challenges remain. Enhancing communication efficiency, developing robust privacy protections, and ensuring scalability are critical areas for future research. Specific directions include:

- **Dynamic Aggregation Mechanisms**: Tailored aggregation strategies that adapt to client-specific data and update patterns.
- **Scalable Architectures**: Hierarchical or decentralized models to manage large-scale deployments effectively.
- **Enhanced Privacy Measures**: Combining cryptographic techniques with advanced differential privacy mechanisms to address emerging vulnerabilities.
- **Application-Specific Customization**: Developing domain-specific adaptations of OFL for applications such as healthcare, autonomous systems, and industrial IoT.

These advancements will not only enhance the performance and reliability of OFL but also broaden its applicability across diverse and critical domains. By addressing these challenges, OFL can unlock new opportunities in distributed learning and pave the way for more intelligent and responsive systems.

ACKNOWLEDGMENT

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2025-RS-2024-00436887) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation)

REFERENCES

[1] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6g internet of things: Recent advances, use cases, and open challenges," *ICT express*, vol. 9, no. 3, pp. 296–312, 2023.

[2] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated learning on non-iid data: A survey," *Neurocomputing*, vol. 465, pp. 371–390, 2021.

[3] D. Kwon, J. Jeon, S. Park, J. Kim, and S. Cho, "Multiagent ddpg-based deep learning for smart ocean federated learning iot networks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9895–9903, 2020.

[4] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE transactions on information forensics and security*, vol. 15, pp. 3454–3469, 2020.

[5] X. Cheng, M. Gao, Q. Gao, and X.-H. Peng, "Impact of network settings on reinforcement learning based caching policy in cooperative edge networks," *ICT Express*, vol. 9, no. 6, pp. 1122–1127, 2023.

[6] L. Lyu, H. Yu, X. Ma, C. Chen, L. Sun, J. Zhao, Q. Yang, and S. Y. Philip, "Privacy and robustness in federated learning: Attacks and defenses," *IEEE transactions on neural networks and learning systems*, 2022.

[7] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "Scaffold: Stochastic controlled averaging for federated learning," in *International conference on machine learning*. PMLR, 2020, pp. 5132–5143.

[8] X. Dong, Z. Yu, W. Cao, Y. Shi, and Q. Ma, "A survey on ensemble learning," *Frontiers of Computer Science*, vol. 14, pp. 241–258, 2020.

[9] V. C. Gogineni, S. Werner, F. Gauthier, Y.-F. Huang, and A. Kuh, "Personalized online federated learning for iot/cps: Challenges and future directions," *IEEE Internet of Things Magazine*, vol. 5, no. 4, pp. 78–84, 2022.

[10] S. Liu, S. Xue, J. Wu, C. Zhou, J. Yang, Z. Li, and J. Cao, "Online active learning for drifting data streams," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 1, pp. 186–200, 2021.

[11] F. Haddadpour, M. M. Kamani, A. Mokhtari, and M. Mahdavi, "Federated learning with compression: Unified analysis and sharp guarantees," in *International Conference on Artificial Intelligence and Statistics*. PMLR, 2021, pp. 2350–2358.

[12] C. Wu, F. Wu, L. Lyu, Y. Huang, and X. Xie, "Communication-efficient federated learning via knowledge distillation," *Nature communications*, vol. 13, no. 1, p. 2032, 2022.

[13] M. Ye, X. Fang, B. Du, P. C. Yuen, and D. Tao, "Heterogeneous federated learning: State-of-the-art and research challenges," *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–44, 2023.

[14] Y. Xue, L. Su, and V. K. Lau, "Fedocomp: Two-timescale online gradient compression for over-the-air federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 19 330–19 345, 2022.