A SYNERGISTIC DIFFERENTIAL PRIVACY-ENHANCED FEDERATED LEARNING FRAMEWORK FOR HETEROGENEOUS IOT ENVIRONMENTS

Yinqiang Zhu, student
Supervisor - Candidate of Technical Sciences, Associate Professor **Yuriy Skorin**
Semen Kuznets Kharkiv National University of Economics

Today's IoT devices make up a huge network, generating a continuous and massive flow of data that provides an unprecedented opportunity to use machine learning to create intelligent applications that can provide accurate predictions and highly personalized services. However, traditional centralized machine learning approaches, which require transmitting and storing this often sensitive raw data on central cloud servers, face fundamental challenges.

Problem statement. Collaboratively training machine learning models on resource-constrained edge devices, while ensuring user data privacy, has become a key and challenging research challenge. Federated learning (FL) provides a basic framework for this purpose, however, its practical application still faces complex, interconnected challenges due to the introduction of differential privacy (DP) noise, imperfectly distributed data (Non-IID), and communication bottlenecks. Most existing research focuses on solving one of these problems in isolation, often ignoring the complex trade-offs between them.

The research undertaken should fill this research gap by designing, implementing, and evaluating a synergistic and optimized federated learning infrastructure with differential privacy called PriFed-IoT, specifically designed for IoT edge computing scenarios. The infrastructure integrates a new synergistic mechanism, which combines dynamic client clustering based on data distribution similarity with server-side adaptive differential privacy noise scheduling. The central idea is to use adaptive differential privacy to create an environment with a higher signal-to-noise ratio for the late-stage clustering algorithm, allowing for more accurate client separation. In turn, more accurate clustering provides more valuable information for allocating adaptive privacy budgets, generating a positive "1+1 > 2" feedback. In addition, the infrastructure includes lightweight model compression techniques to overcome communication gaps. limitations of edge devices.

Purpose of the study. This work aims to fill this research gap by designing, implementing, and evaluating a synergistic and optimized federated learning infrastructure with differential privacy called PriFed-IoT, specifically designed for edge computing IoT scenarios. The main innovation of this work is to create a system of several modules working together, rather than a simple combination of techniques. The infrastructure integrates a new synergistic mechanism that combines dynamic client clustering based on data distribution similarity with server-side adaptive differential privacy noise scheduling. The central idea is to use adaptive differential privacy to create an environment with a higher signal-to-noise ratio for the clustering algorithm in the later stages of training, allowing for more accurate separation of clients. In turn, more accurate clustering provides more valuable information for

allocating adaptive privacy budgets, forming a positive feedback"1+1 > 2". In addition, the infrastructure includes lightweight model compression techniques to overcome the communication limitations of edge devices.

Conclusions and prospects. Thus, the work carried out successfully completed the full cycle of research from identifying a critical gap in research to proposing an innovative solution and testing it with reliable empirical evidence. The proposed PriFed-IoT framework provides a valuable and comprehensive solution to achieve secure, efficient, and reliable distributed intelligent applications in IoT edge computing.

References

1. Aledhari, M. Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications / M. Aledhari, R. Razzak, R. M. Parizi, F. Saeed // IEEE Access. 2020. Vol. 8. P. 140699-140725.
2. Chen, M. FedSA: A staleness-aware asynchronous Federated Learning algorithm with non-IID data / M. Chen, B. Mao, T. Ma // Future Generation Computer Systems. 2021. Vol. 120. P. 1-12.
3. Demelius, L. Recent Advances of Differential Privacy in Centralized Deep Learning: A Systematic Survey / L. Demelius, R. Kern, A. Trügler // arXiv preprint arXiv:2309.16398. 2023. – URL: https://arxiv.org/abs/2309.16398.

ПРОБЛЕМИ ІНТЕГРАЦІЇ УКРАЇНСЬКОГО БІЗНЕСУ ДО ЄДИНОГО РИНКУ ЄС

Буштин Ю.С., здоб. ОС «бакалавр»
Науковий керівник - канд. екон. наук, доц. **Г.І. Костьов'ят**
ДВНЗ «Ужгородський національний університет»

На українському ринку переважають мікро-, малі та середні підприємства, які становлять близько 99,97 % усіх суб'єктів господарювання та забезпечують понад 63 % зайнятості населення [2]. Їх роль у процесах євроінтеграції є визначальною, адже саме цей сектор формує основу національної економіки. Водночас поточні соціально-економічні виклики, спричинені війною та структурною перебудовою, ускладнюють їхній розвиток. Саме тому одним із ключових напрямів політики Європейського Союзу щодо України є підтримка інтеграції МСП до внутрішнього ринку ЄС у межах Поглибленої та всеосяжної зони вільної торгівлі.

Єдиний ринок ЄС - це спільний економічний простір, у межах якого реалізується принцип «чотирьох свобод»: вільного руху товарів, послуг, капіталу та робочої сили [1]. Для українських підприємств інтеграція до цього ринку означає не лише нові можливості, а й необхідність глибокої адаптації до вимог європейського бізнес-середовища. Серед ключових переваг інтеграції слід виокремити розширення партнерських можливостей, залучення нових клієнтів і