INTEGRATED DIFFERENTIAL PRIVACY LEARNING SYSTEM FOR EDGE COMPUTING IN IOT NETWORKS

Zhu YINQIANG, master student
ORCID ID: 0009-0007-5445-8761
Semen Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine

As a result of the significant growth of the Internet of Things (IoT), a large number of smart devices are being deployed around the world in various industries, from smart homes and smart cities to industrial automation and connected healthcare.

These devices, such as portable health monitors, smart vehicles, and industrial sensors, form a vast network, generating a continuous and massive stream of data. This data 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 this often-sensitive raw data to be transmitted and stored on central cloud servers, face fundamental challenges. This paradigm not only poses significant privacy risks, making it difficult to comply with increasingly stringent data protection regulations, but also imposes a significant burden on network bandwidth, potentially leading to unacceptable latency in time-critical applications [2]. To address these challenges, federated learning (FL) is seen as a new privacy-preserving distributed learning paradigm [1]. But the practical deployment of FL at the edge of the Internet of Things faces a number of interrelated and complex challenges: Conflict of confidentiality and usefulness; The problem of data heterogeneity; Limitation of system resources.

A comprehensive analysis of the existing literature shows that most current research focuses on addressing one of these problems separately, often without taking into account internal trade-offs and negative interactions between them.

The purpose of the study is to design, implement, and evaluate a lightweight and reliable federated learning system called PriFed-IoT.

The proposed PriFed-IoT framework provides insights with direct practical value. It can provide a low-cost, easy-to-deploy technical solution that combines privacy protection with model performance for various IoT applications that handle sensitive user data, such as monitoring personal health in smart healthcare, analyzing the online behavior of vehicle drivers, and predicting user habits in smart homes.

To fill this gap, the paper sets the following specific research tasks that directly lead to the development of the PriFed-IoT framework in the following section:

1. To conduct a systematic analysis of the key challenges faced by federated learning in IoT edge applications, confirming the theoretical and practical significance of the identified research gap;
2. Develop a unified framework architecture capable of synergistically solving the above problems, and propose a new synergistic mechanism that combines an adaptive differential noise privacy planning strategy with a dynamic client clustering method to explicitly resolve the "noise-cluster conflict";
3. Implement the proposed frameworks and algorithms using software simulations and create an experimental environment that simulates real-world IoT scenarios with varying degrees of non-IID data and privacy restrictions.
4. Evaluate and verify the complex effectiveness of the proposed structure through large-scale comparative experiments, with special emphasis on analyzing and proving the existence of the proposed synergistic effect "1+1 > 2" between its main modules.

The proposed PriFed-IoT framework provides a valuable and comprehensive solution to achieve secure, efficient, and reliable distributed intelligent applications in IoT edge computing.

Although the study carried out brought the expected results, it also opens up several promising avenues for future research. Based on the results and limitations of the current work, future research can be expanded in the following areas:

1. more reliable clustering algorithms;
2. integration of more comprehensive security;
3. Deploy and test real equipment.

References

1. Abrahamsson P. Agile Software Development Methods: Review and Analysis / P. Abrahamsson, O. Salo, J. Ronkainen, et al. – URL: https://doi.org/10.48550/arXiv.1709.08439.
2. Bardsiri V. K. A Flexible Method to Estimate the Software Development Effort Based on the Classification of Projects and Localization of Comparisons / V. K. Bardsiri, D. N. A. Jawawi, S. Z. M. Hashim, et al. – URL: https://doi.org/10.1007/s10664-013-9241-4.
3. Beecham S. Software Process Improvement Problems in Twelve Software Companies: An Empirical Analysis / S. Beecham, T. Hall, A. Rainer, et al. – URL: https://doi.org/10.1023/A:1021764731148.