UABDIVULGA
BARCELONA RECERCA I INNOVACIÓ

06/06/2023

# How can we guarantee privacy in federated learning algorithms?

A study in which the Department of Information and Communications Engineering of the UAB participates presents a new framework for machine learning algorithms in a distributed fashion that increases the privacy guarantees of the clients. To this end, they propose the unification of the Particle Swarm Optimization algorithm with federated learning and differential privacy techniques.

iStock/Marcela Vieira

Federated learning (FL) makes it possible to implement machine learning algorithms in a distributed fashion. The objective of machine learning systems is to train a model from a set of data. In this sense, FL provides a framework where these data are distributed among different locations (e.g., devices) or clients that generate local models trained from their own data. A central server trains a global model by aggregating these local models through a process that is usually iterative: the server sends the global model to the clients, which in turn send model updates based on their data and local models, and so on until the global model converges.

One of the most attractive points of FL systems is that the data used to train the final model never leaves the client device. This guarantees a certain level of privacy if these data contain private information. This is one of the main reasons why companies such as Google are starting to use FL (for example to train a predictive text system from the Gboard application).

However, the privacy provided by FL may be illusory. Recent research has shown that FL can indeed present privacy issues. For example, it is possible to infer private information from the updates that each client sends to the server. Moreover, private information can be leaked from the global model depending on how the models or updates that each client contributes are aggregated.

In this paper, we focus on a type of algorithm known as Particle Swarm Optimization (PSO). In PSO we have a set of agents with a position in the solution space, and the goal is to search for an optimal solution among all of them. The name is inspired by the fact that we can consider each agent (possible solution) as a particle. Each particle improves its position until they all converge at the same point, the optimal solution.

The article proposes solutions to guarantee privacy both in the data sent by each client and in the aggregation performed by the final node. For this purpose, techniques based on the differential privacy principle are used to obtain strong privacy guarantees. Our experiments show that the same solution can be obtained under differential privacy as in the non-private case, although this leads to a slightly longer convergence time. That is, it takes a little longer to obtain the solution, but we can give guarantees on the private information that can be leaked in the whole process.

**Guillermo Navarro Arribas**
(1) Department of Information and Communications Engineering, Universitat Autònoma de Barcelona (UAB).
(2) CYBERCAT.
guillermo.navarro@uab.cat

## References

V. Torra, E. Galván, G. Navarro-Arribas, **PSO + FL = PAASO: Particle Swarm Optimization + Federated Learning = Privacy-Aware Agent Swarm Optimization,** *International Journal of Information Security*, vol. 21, no. 6, pp. 1349–1359, Dec. 2022, ISSN: 1615-5270. DOI: https://doi.org/10.1007/s10207-022-00614-6

View low-bandwidth version