1st Workshop on Federated Learning Technologies

1st Workshop on Federated Learning Technologies

Mirko Polato
mirko.polato@unito.it
University of Turin
Turin, Italy

Roberto Esposito
roberto.esposito@unito.it
University of Turin
Turin, Italy

Walter Riviera
walter.riviera@intel.com
Intel Corporation
Swindon, United Kingdom

Zenglin Xu
zenglin@gmail.com
Harbin Institute of Technology
Shenzhen, China

Irwin King
irwinking@gmail.com
The Chinese University of Hong Kong
Hong Kong, China

ABSTRACT

AI-based systems, especially those based on machine learning technologies, have become central in modern societies. In the meanwhile, users and legislators are becoming aware of privacy issues. Users are increasingly reluctant in sharing their sensitive information, and new laws have been enacted to regulate how private data is handled (e.g., the GDPR).

Federated Learning (FL) has been proposed to develop better AI systems without compromising users' privacy and the legitimate interests of private companies. Although still in its infancy, FL has already shown significant theoretical and practical results making FL one of the hottest topics in the machine learning community.

Given the considerable potential in overcoming the challenges of protecting users' privacy while making the most of available data, we propose a workshop on Federated Learning Technologies (FLT) at TheWebConf 2023.

The goal of this workshop is to focus the attention of the TheWebConf research community on addressing the open questions and challenges in this thriving research area. Given the broad range of competencies in the TheWebConf community, the workshop will welcome foundational contributions as well as contributions expanding the scope of these techniques, such as improvements in the interpretability and fairness of the learned models.

CCS CONCEPTS

• **Computing methodologies** → **Learning settings**.

KEYWORDS

federated learning, distributed learning, deep learning

ACM Reference Format:
Mirko Polato, Roberto Esposito, Walter Riviera, Zenglin Xu, and Irwin King. 2023. 1st Workshop on Federated Learning Technologies. In *Companion Proceedings of the ACM Web Conference 2023 (WWW '23 Companion), April 30-May 4, 2023, Austin, TX, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3543873.3589741

WWW '23 Companion, April 30-May 4, 2023, Austin, TX, USA

ACM ISBN 978-1-4503-9419-2/23/04.
https://doi.org/10.1145/3543873.3589741

THEMES AND ORGANIZATION

The workshop is centered on the theme of improving and studying the Federated Learning setting. It includes applicative and theoretical contributions as well as contributions about specific settings and benchmarking tools. The topics include:

- Algorithmic and theoretical advances in FL
- Federated Learning with non-iid data distributions
- Security and privacy of FL systems (e.g., differential privacy, adversarial attacks, poisoning attacks, inference attacks, data anonymization, model distillation, secure multi-party computation …)
- Other non-functional properties of FL (e.g., fairness, interpretability/explainability, personalization …)
- Applications of FL (e.g., FL for healthcare, advertising, social network, blockchain, web search, metaverse …)

The workshop puts a high emphasis on spreading operative knowledge on FL technologies and it includes one keynote and two hands-on sessions, organized according to the following schedule:

Opening remarks	Workshop organizers
Keynote	Marco Aldinucci, University of Turin *High Performance Computing and FL*
Hands-on session	Intel (OpenFL)
Coffee break	
Paper presentations	(12m+3m presentations) × 4
Hands-on session	Dr. Chaoyang He (FedML)
Closing remarks	Workshop organizers

ACKNOWLEDGMENTS

The European PILOT project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No.101034126. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Spain, Italy, Switzerland, Germany, France, Greece, Sweden, Croatia, and Turkey.

The EPI SGA2 project has received funding from the European High-Performance Computing Joint Undertaking (JU) under Framework Partnership Agreement No 800928 and Specific Grant Agreement No 101036168. The JU receives support from the European Union's Horizon 2020 research and innovation programme and from Croatia, France, Germany, Greece, Italy, Netherlands, Portugal, Spain, Sweden, and Switzerland.