DOCS 2023 Special Session Proposal

**Topic:** Secure, Privacy-Preserving, and Fairness-Aware Optimization

# Aim and Scope

Optimization problems are widespread in many real-world fields, including science, engineering, and technology. Despite the many studies on optimization, most current optimization techniques rely on a traditional centralized model. However, with the increasing storage capacity and computational power of edge devices in modern distributed networks, there has been an emergence of decentralized computing such as federated optimization. This novel approach enables optimization to be executed locally at edge devices with minimal communication between them. While this method has great potential, it also presents new challenges and privacy concerns given the large amount of data collected by edge devices.

In addition to standard optimization considerations like maximizing performance, users in some scenarios also care about fairness in decision-making, multi-objective preference or model construction. Thus, developing new algorithmic ideas is paramount for optimizing both overall performance and considerations related to fairness.

Given these considerations, there is currently increased attention to developing secure and privacy-preserving optimization techniques that are also fair-aware. Some of the research topics include security and robustness, privacy-preservation, fairness, verifiability, and transparency when designing optimization algorithms. Notably, significant issues remain unresolved in this field.

It is important to discuss the definitions of security, privacy and fairness concerning optimization since many researchers understand these concepts differently. Finding an appropriate balance between performance optimization alongside privacy/fairness/security guarantees represents another challenge. Additionally, long-standing factors that affect distributed and federated machine learning methods need reevaluation within the context of optimization including non-IID data and enhancing communication efficiency.

Therefore, designing new benchmark problems and performance indicators for evaluating secure, privacy-preserving and fair-aware optimization methods remains key towards addressing open questions on this subject matter.

The aim of this special session is to bring together researchers from different application fields working on optimization and present new solutions to the above-discussed challenges. The special session will focus on new advances, review and discuss the state-of-the-art in the theory, algorithm design, and applications of using secure, privacy-preserving, and fairness-aware solutions in optimization.

Authors are invited to submit papers on one or more of the following topics:

* Privacy-preserving Bayesian optimization
* Privacy-preserving evolutionary algorithm
* Privacy-preserving distributed optimization
* Secure federated data-driven optimization
* Federated surrogate models
* Fairness-aware acquisition function
* Attacks and defenses in optimization
* Fairness-aware multi-objective optimization
* Fairness-aware data-driven optimization
* Fairness-aware federated optimization
* Fairness-aware multi-objective machine learning
* Benchmark problems for secure, privacy-preserving and fairness-aware optimization
* Performance indicators for secure, privacy-preserving and fairness-aware optimization

# Organizers:

**Dr Yang CHEN,** School of Electrical Engineering, China University of Mining and Technology, Jiangsu, 221116, China. Email: [fedora.cy@gmail.com](mailto:fedora.cy@gmail.com)

**Dr Liming YAO,** School of Mechanical and Aerospace Engineering，Nanyang Technological University, 639798, Singapore. Email: [liming.yao@ntu.edu.sg](mailto:liming.yao@ntu.edu.sg)

**Ms Yuping YAN (Ph.D. Candidate)**, Department of Informticas, Eötvös Loránd University, Hungary. [Email: yupingyan@inf.elte.hu](mailto:yupingyan@inf.elte.hu)

**Dr Ying HU**, School of Computer and information， Anhui Normal University，Anhui, 241002， China. Email: [hy200712008@126.com](mailto:hy200712008@126.com)

**Dr Qiqi LIU**, Department of Artificial Intelligence, Hebei University of Technology, Bielefeld University,Tianjin, 300401, China. Email: [qiqi6770304@gmail.com](mailto:qiqi6770304@gmail.com)

# Potential Contributors

* Prof. Santu Rana, Applied Artificial Intel Institute, Deakin University (Australia), [santu.rana@deakin.edu.au](mailto:santu.rana@deakin.edu.au)
* Hong-You Chen, Department of Computer Science and Engineering, Ohio State University, USA, [chen.9301@osu.edu](mailto:chen.9301@osu.edu)
* Dr. Peter Fenner, IBM Research UK, UK, [peter.fenner1@ibm.com](mailto:peter.fenner1@ibm.com)
* Dr. Edward O. Pyzer-Knapp, IBM Research UK, UK, [epyzerk3@uk.ibm.com](mailto:epyzerk3@uk.ibm.com)
* Dr. Antti Honkela, Department of Computer Science, University of Helsinki, Finland, [antti.honkela@helsinki.fi](mailto:antti.honkela@helsinki.fi)
* Dr. Laila Melkas, Department of Computer Science, University of Helsinki, Finland, [laila.melkas@helsinki.fi](mailto:laila.melkas@helsinki.fi)
* Haolin Yu, University of Waterloo, Waterloo, Canada, [h89yu@uwaterloo.ca](mailto:h89yu@uwaterloo.ca)
* Idan Achituve, Bar-Ilan University, Israel, [idan.achituve@biu.ac.il](mailto:idan.achituve@biu.ac.il)
* Dr. Zhongxiang Dai, Dept. of Computer Science, National University of Singapore, Singapore, [daizhongxiang@comp.nus.edu.sg](mailto:daizhongxiang@comp.nus.edu.sg)
* Dr. Tobias Rodemann, Honda Research Institute Europe, Germany, [tobias.rodemann@honda-ri.de](mailto:tobias.rodemann@honda-ri.de)
* Dr. Chao Qian, School of Artificial Intelligence, Nanjing University, China, [chaoqian@ustc.edu.cn](mailto:chaoqian@ustc.edu.cn)
* Prof. Ke Tang, Department of Computer Science and Engineering, Southern University of Science and Technology, China, [tangk3@sustech.edu.cn](mailto:tangk3@sustech.edu.cn)
* Dr. Caroline J. Jagtenberg School of Business and Economics, Vrije Universiteit Amsterdam, the Netherlands, [c.j.jagtenberg@vu.nl](mailto:c.j.jagtenberg@vu.nl)
* Prof. Michael Kostreva, Department of Mathematical Sciences, Clemson University, USA, [flstgla@clemson.edu](mailto:flstgla@clemson.edu)
* Aniekan A. Ebiefung, Department of Mathematics, University of Tennessee, USA, [Aniekan-Ebiefung@utc.edu](mailto:Aniekan-Ebiefung@utc.edu)
* Prof. Włodzimierz Ogryczak, Institute of Control and Computation Engineering, Warsaw University of Technology, Poland, [ogryczak@ia.pw.edu.pl](mailto:ogryczak@ia.pw.edu.pl)
* Dr. Michael P. Kim, UC Berkeley, Google Research, [mpkim@berkeley.edu](mailto:mpkim@berkeley.edu)
* Serena Wang, UC Berkeley, Google Research, [serenalwang@berkeley.edu](mailto:serenalwang@berkeley.edu)
* Yiliang Zhang, University of Pennsylvania, USA, [zylthu14@sas.upenn.edu](mailto:zylthu14@sas.upenn.edu)
* Dr. Chongjie Zhang, Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, China, [chongjie@tsinghua.edu.cn](mailto:chongjie@tsinghua.edu.cn)
* Dr. Julie Shah, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, USA, [julie\_a\_shah@csail.mit.edu](mailto:julie_a_shah@csail.mit.edu)
* Sarah Bird, Microsoft, [slbird@microsoft.com](mailto:slbird@microsoft.com)
* Prof. Jun Zhang, Zhejiang Normal University and Hanyang University, [junzhang@ieee.org](mailto:junzhang@ieee.org)

## Prof. Zhi-Hui Zhan, School of Computer Science and Engineering, South China University of Technology, [zhanapollo@163.com](mailto:zhanapollo@163.com)

* Prof. Kay Chen Tan, Department of Computing, The Hong Kong Polytechnic University, [kctan@polyu.edu.hk](mailto:kctan@polyu.edu.hk)

## Prof. Yang Tang, Department of Automation, East China University of Science and Technology, [yangtang@ecust.edu.cn](mailto:yangtang@ecust.edu.cn)