

Session B

Time Friday, 1 Dec 2023 at 09:15-16:00 (Finnish timezone)

Zoom <https://aalto.zoom.us/j/63886836862>

Chair Antti Ylä-Jääski

Timeslot	Presenter	Title	Opponent
9:10-9:15	Antti Ylä-Jääski	Opening words and instructions	
9:15-9:35	Wang Ziqi	Decoding the Black-Box: A Review of Machine Learning Explainability Methods	Jussi Vaitomaa
9:35-9:55	Sonika Baniya	Pulsing Convex DDoS Attack in CDN Networks	Arthur Becker
9:55-10:15	Reda Bellafqih	Privacy and Dark Patterns	Jonas Bäck
10:15-10:35	Gabriel Gomes Ziegler	Learning Models - A Literature Review	Markus Granström
Break			
10:40-11:00	Jussi Vaitomaa	Microservices - when and how to use them	Wang Ziqi
11:00-11:20	Xu Yu	Neural Radiance Fields (NeRF): Current State of Art and Ongoing Challenges	Xinyu Zhang
11:20-11:40	Jonas Bäck	Software supply chain security: the SLSA specification	Reda Bellafqih
11:40-12:00	Markus Granström	Unidirectional gateways for security of OT networks	Gabriel Gomes Ziegler
Lunch Break			
13:00-13:20	Xinyu Zhang	Amortized Meta Bayesian Optimization	Xu Yu
13:20-13:40	Arthur Becker	Calibration in quantized LLMs	Sonika Baniya
13:40-14:00	Daniel Kaluski	Do cookie consent forms protect your data?	Roni Kirla
14:00-14:20	Danila Mokeev	Investigating temporal Gaussian processes for solar PV forecasting.	Niko Nästi
Break			
14:30-14:50	Roni Kirla	Prospects of WebAssembly to address performance and security challenges beyond the browser	Daniel Kaluski
14:50-15:10	Niko Nästi	Advancements in Neural Radiance Fields: A Comparative Study of Instant NeRF and BakedSDF	Danila Mokeev
15:10-15:30	Leevi Parkkinen	Software supply chain security: the SLSA specification	Juho Pellinen
15:30-15:50	Juho Pellinen	CDN attacks	Leevi Parkkinen