

Stephan Rabanser

Last update: September 25, 2023

✉ stephan@cs.toronto.edu

🏠 <https://www.cs.toronto.edu/~stephan>

EDUCATION

- **PhD in Computer Science** Toronto, Canada
University of Toronto, advised by Prof. Nicolas Papernot *September 2020 – August 2025 (exp.)*
 - **Supervisory Committee:** Prof. Nicolas Papernot, Prof. Rahul Krishnan, Prof. David Duvenaud, Prof. Roger Grosse, Prof. Zachary Lipton
 - **Research Interests:** Machine Learning, Robustness, Safety, Reliability, Uncertainty, Causality, Generative Modeling, Representation Learning, Probabilistic Deep Learning, Anomaly Detection, Distribution Shifts, Out-of-Distribution Sample Detection, Healthcare Applications.
 - **TAing:** CSC2541: Neural Network Training Dynamics (Winter 2022), CSC2515: Introduction to Machine Learning (Fall 2022), ECE1784: Trustworthy Machine Learning (Fall 2022), CSC311: Introduction to Machine Learning (Fall 2023)
- **Visiting Graduate Student** Cambridge, UK
University of Cambridge, advised by Prof. David Krueger *June 2023 – September 2023*
- **M.Sc. in Computer Science** Munich, Germany
Technical University of Munich (TUM), advised by Prof. Stephan Günnemann *October 2015 – July 2019*
- **Visiting Research Scholar** Pittsburgh, PA
Carnegie Mellon University (CMU), advised by Prof. Zachary Lipton *August 2018 – January 2019*
- **Honours Degree in Technology Management** Munich, Germany
Center for Digital Technology and Management (CDTM) *August 2015 – June 2017*
- **Visiting Research Student** Cambridge, MA
Massachusetts Institute of Technology (MIT), advised by Prof. Thomas Malone *February 2016 – June 2016*
- **B.Sc. in Computer Science, Minor in Economic Sciences** Munich, Germany
Technical University of Munich (TUM) *October 2012 – October 2015*

EXPERIENCE

- **Machine Learning Researcher** Toronto, CA
Vector Institute for Artificial Intelligence *September 2020 – Present*
- **Intern Applied Scientist** Munich, Germany
Amazon, AWS AI Labs *June 2021 – October 2021*
 - Designed context-invariant time series representations using contrastive and domain-adversarial learning.
- **Intern Applied Scientist** Munich, Germany
Amazon, AWS AI Labs *September 2019 – July 2020*
 - Systematically assessed the impact of I/O representations for deep-learning-based time-series forecasting.
- **Intern Applied Scientist** Munich, Germany
Amazon, AWS AI Labs *May 2018 – August 2018*
 - Evaluated existing and developed new ML-based algorithms for large-scale lossless data compression.
 - Implemented autoencoder-based probability distribution estimation for arithmetic coding on tabular data.
- **Intern Software Development Engineer** Berlin, Germany
Amazon, Core Machine Learning *August 2017 – October 2017*
 - Received an overview of standard time series analysis / forecasting techniques.
 - Implemented [Bayes by Backprop](#) (weight uncertainty quantification) for plain MLPs & RNNs in MXNet.

PUBLICATIONS

- Stephan Rabanser, Anvith Thudi, Abhradeep Thakurta, Krishnamurthy Dvijotham, and Nicolas Papernot. **Training Private Models That Know What They Don't Know**. In *Advances in Neural Information Processing Systems*, 2023 (to appear) [paper, slides]
- Nicholas Franzese, Adam Dziedzic, Christopher A. Choquette-Choo, Mark R. Thomas, Muhammad Ahmad Kaleem, Stephan Rabanser, Congyu Fang, Somesh Jha, Nicolas Papernot, and Xiao Wang. **Robust and Actively Secure Collaborative Machine Learning**. In *Advances in Neural Information Processing Systems*, 2023 (to appear)
- Adam Dziedzic, Stephan Rabanser, Mohammad Yaghini, and Nicolas Papernot. **p -DkNN: Out-of-Distribution Detection through Statistical Testing of Deep Representations**. *arXiv preprint arXiv:2207.12545*, 2022 [paper]
- Stephan Rabanser, Tim Januschowski, Kashif Rasul, Oliver Borchert, Richard Kurlle, Jan Gasthaus, Michael Bohlke-Schneider, Nicolas Papernot, and Valentin Flunkert. **Intrinsic Anomaly Detection in Multi-Variate Time Series**. *arXiv preprint arXiv:2206.14342*, 2022 [paper]
- Stephan Rabanser, Anvith Thudi, Kimia Hamidieh, Adam Dziedzic, and Nicolas Papernot. **Selective Classification Via Neural Network Training Dynamics**. *arXiv preprint arXiv:2205.13532*, 2022 [paper]
- Stephan Rabanser, Tim Januschowski, Valentin Flunkert, David Salinas, and Jan Gasthaus. **The Effectiveness of Discretization in Forecasting: An Empirical Study on Neural Time Series Models**. In *7th KDD Workshop on Mining and Learning from Time Series (MiLeTS)*, 2020. **Oral presentation**. [paper, slides]
- Stephan Rabanser, Stephan Günnemann, and Zachary Lipton. **Failing Loudly: An Empirical Study of Methods for Detecting Dataset Shift**. In *Advances in Neural Information Processing Systems*, 2019 [paper, poster, slides]
- Stephan Rabanser, Oleksandr Shchur, and Stephan Günnemann. **Introduction to Tensor Decompositions and their Applications in Machine Learning**. *arXiv preprint arXiv:1711.10781*, 2017 [paper]

AWARDS & HONORS

- **Member of the Elite Network of Bavaria** *Since 2016*
- **Apple WWDC Student Scholarship** *June 2013*

COMMUNITY SERVICE

- **Reviewing:** NeurIPS (2023, 2022, 2021), ICML (2022, 2021), ICLR (2024), Distribution Shift Workshop @ ICML (2022), Distribution Shift Workshop @ NeurIPS (2023, 2022, 2021 – *outstanding reviewer*), Human Evaluation of Generative Models Workshop @ NeurIPS (2022), Time Series Workshop @ ICML (2021), Time Series Workshop @ KDD (2022), AAAI (2020)
- **Talks:** Google DeepMind London (Sep 2023), MIT MIMO Student Research Forum (Oct 2022), Intel Private AI Institute Fall Workshop (Oct 2022), Microsoft Security Data Science Colloquium (Jul 2021)

SELECTED COURSEWORK

- **Data Science in Astrophysics and Industry** Munich, Germany
Interdisciplinary Project @ Max Planck Institute for Astrophysics (MPA) *March 2017 – July 2017*
 - Optimized the algorithmic implementation of a GMM model (e.g. number of mixture components, hyper-parameters) and explored different training methods (stochastic vs. deterministic and expectation maximization (EM) vs. gradient descent vs. Newton).
 - Researched, implemented, and improved online learning techniques for GMMs and compared them to standard EM and tensor decomposition approaches.

PROGRAMMING SKILLS

- **Languages:** Python, Java, Swift, HTML/CSS/JS **ML Frameworks:** PyTorch, JAX