Thibault Simonetto

ML Engineer

Albanastrasse, 16
54290 Trier
Germany
+352 661 696 690
thibault.simonetto@outlook.com
thibault-simonetto-514511193
thibaultsmnt

Experience

Oct. 2024 – Current **Postdoctoral Researcher**, *SnT, University of Luxembourg*, Luxembourg
Development of an AI testing platform. Industrialization of research outcomes in partnership with BGL BNP Paribas.
My research interests are:
- Security testing of ML models;
- Quality assessment of ML-based systems;
- Automation of ML models development processes.

Nov. 2020 – Oct. 2024 **Doctoral Researcher**, *SnT, University of Luxembourg*, Luxembourg
PhD in collaboration with BGL BNP Paribas titled: Enhancing Machine Learning Robustness for Critical Industrial Systems.
Activities beyond research:
- Participation in international conferences (NeurIPS, ICML, IJCAI, KDD) and summer/winter schools (OxML and Cyberwal);
- System administration providing computing resources for 40+ users.
- Teaching "AI and cybersecurity" in Master in Cybersecurity.

Oct. 2016 – Jan. 2020 **Research Support**, *DCS, University of Luxembourg*, Luxembourg
Development of internal DevOps solutions; DevOps research; Project management; Web development; Promotion of the new Bachelor in Computer Science (BiCS).

Education

2020 – 2024 **PhD in Computer Science**, *University of Luxembourg*, Luxembourg
Enhancing Machine Learning Robustness for Critical Industrial Systems: Constrained Adversarial Attacks and Distribution Drift Solutions.

2018 – 2020 **Master in Information and Computer Science**, *University of Luxembourg*, Luxembourg, *High Honours*
Specialization in Artificial Intelligence and Reliable Software Systems.

2015 – 2018 **Bachelor of Applied Sciences in Computer Science**, *University of Luxembourg*, Luxembourg, *High Honours*
With six months spent at the Free University of Bozen-Bolzano, Italy.

Publications

2024 Thibault Simonetto, Salah Ghamizi, and Maxime Cordy. "TabularBench: Benchmarking Adversarial Robustness for Tabular Deep Learning in Real-world Use-cases". Advances in Neural Information Processing Systems (NeurIPS). 2024.

2024 Thibault Simonetto, Salah Ghamizi, and Maxime Cordy. "Constrained Adaptive Attack: Effective Adversarial Attack Against Deep Neural Networks for Tabular Data". Advances in Neural Information Processing Systems (NeurIPS). 2024.

2024 Thibault Simonetto, Salah Ghamizi, Maxime Cordy, Yves Le Traon, Clément Lefebvre, Andrey Boystov and Anne Goujon. "On the Impact of Industrial Delays when Mitigating Distribution Drifts: an Empirical Study on Real-world Financial Systems". KDD 2024 International Workshop on Discovering Drift Phenomena in Evolving Landscapes. 2024.

2024 Thibault Simonetto, Salah Ghamizi, and Maxime Cordy. "Towards Adaptive Attacks on Constrained Tabular Machine Learning". ICML 2024 Next Generation of AI Safety Workshop. 2024.

2023 Salijona Dyrmishi, Salah Ghamizi, Thibault Simonetto, Yves Le Traon, and Maxime Cordy. "On the empirical effectiveness of unrealistic adversarial hardening against realistic adversarial attacks." In 2023 IEEE symposium on security and privacy (SP). IEEE, 2023.

2022 Thibault Simonetto, Salijona Dyrmishi, Salah Ghamizi, Maxime Cordy, and Yves Le Traon. "A Unified Framework for Adversarial Attack and Defense in Constrained Feature Space." In Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence (IJCAI). 2022.

Projects

A4S Creator, architect and developer of A4S: AI Testing Platform. *Soon to be released*.

TabularBench Creator and maintainer of TabularBench: Adversarial robustness benchmark for tabular data `https://github.com/serval-uni-lu/tabularbench`.

Drift robustness Creator of Drift robustness: Evaluation of distribution drift robustness under realistic settings `https://github.com/serval-uni-lu/drift-robustness`.

IDOML Requirement analyst and architecture for IDOML: A simple MLOps platform for small scale ML projects. *Soon to be released*.

Technical skills

Programming Languages Python, Java, TypeScript, Latex

Data Science scikit-learn, TensorFlow, PyTorch, pandas, numpy, seaborn, FastAPI, SQLModel, Celery

DevOps GitHub/GitLab, CI/CD pipelines, Containerization/Docker, Docker Swarm Clustering, Ansible, MinIO

MLOps MLflow, Evidently.ai

Misc HPC environments, Unit testing, Front-end visualization

Linguistic skills

English Fluent

French Native

German Basic