Antoni Kowalczuk

(+48) 733 654 493
(+49) 171 920 18 24
antonikowalczuk@gmail.com
www.antonikowalczuk.com

Experience

CISPA Helmholtz Center for Information Security, Saarbrücken—*PhD candidate*

January 2024 – Now

Co-author of **Privacy Attacks on Image AutoRegressive Models**, published at **ICML 2025**

Co-author of **CDI: Copyrighted Data Identification in Diffusion Models**, published at **CVPR 2025**

Co-author of **Benchmarking Robust Self-Supervised Learning Across Diverse Downstream Tasks** – published at the **ICML 2024** Workshop on Foundation Models in the Wild

CVLab@WUT, Warsaw—*Student Research Assistant*

January 2023 – December 2023

Co-author of **Towards More Realistic Membership Inference Attacks on Large Diffusion Models** – published at **WACV 2024**

Work on adversarial examples against SSL vision encoders; cooperation with CISPA.

OLX Group, Warsaw—*Junior Data Scientist*

July 2021 – January 2023

Consumer Intelligence, Warsaw—*Data Scientist*

September 2020 – February 2021

Education

Universität des Saarlandes, Saarbrücken—*PhD*

April 2024 – Now

Warsaw University of Technology, Warsaw—*Bachelor's of Science and Engineering*

October 2020 – February 2024

Computer Science, specialization in Artificial Intelligence. Graduated with honors. President of the biggest AI Student society in Poland: Golem.

Achievements

Winner Quantum AI Foundation Contest for the Best Bachelor's Thesis in Poland

Best poster award ML in PL Conference 2023

Winner/podium AI Games Hackathon (2020 & 2022), BiteHack (2022), CERN Winter Campus Hackathon (2022)

Activity

President AI Student Society Golem @ WUT (2021-2022)

Organizer ML in PL Conference (2021-2024)

Project Leader KNUMxGolem AI&DS Hackathon (2022)

Organizer EnsembleAI Hackathon (2024 & 2025)

Languages

Polish—Native Speaker
English—C1
German—A2