Dr. Nicolas Müller

nicolas.mueller@aisec.fraunhofer.de
+49 152 5342 7451
Website (Link)
LinkedIn (Link)
Google Scholar (Link)

PROFIL

KI-Forscher und -Ingenieur mit über 8 Jahren Berufserfahrung in der Entwicklung, Bewertung und dem produktiven Einsatz von Deep-Learning-Systemen. Fachlicher Schwerpunkt auf Audio-Deepfake-Erkennung, Sprachverarbeitung sowie robuster und vertrauenswürdiger Künstlicher Intelligenz.

Promotion in Informatik an der Technischen Universität München. Mehrjährige Tätigkeit am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC). Seit 2024 nebenberuflich beratend für Resemble AI im Bereich Audio-Deepfake-Erkennung, mit Fokus auf fachliche Beratung, Modellbewertung und Einsatzszenarien für Industrie- und Behördenanwendungen.

Regelmäßiger Ansprechpartner für Medien, Politik und Öffentlichkeit zu den Themen Deepfakes, KI-Risiken, Desinformation und Wahlmanipulation. Umfangreiche Erfahrung in Vorträgen, Workshops und Schulungen.

BERUFSERFAHRUNG

Senior Research Engineer Jul 2017 – heute
Fraunhofer AISEC, München

- Forschung zu sicherer und vertrauenswürdiger KI, insbesondere Deepfakes, adversariale Angriffe, Robustheit und Erklärbarkeit.
- Leitung nationaler und europäischer Forschungs- und Industrieprojekte im Bereich KI-Sicherheit und Sprachsynthese.
- Aufbau und Veröffentlichung international genutzter Datensätze (u. a. MLAAD, In-the-Wild) und der Plattform Deepfake-Total.com

Research Consultant (nebenberuflich) Nov 2024 – heute
Resemble AI, San Francisco, USA

- Fachliche Beratung im Bereich Audio-Deepfake-Erkennung und Bewertung synthetischer Sprachmanipulation.
- Unterstützung bei Konzeption, Analyse und Validierung von KI-Modellen für industrielle Anwendungsfälle.

AUSBILDUNG

Technische Universität München *März 2018 – Dez 2022*
Promotion (Dr. rer. nat.) in Informatik
Thema: Integrity and Correctness of Machine Learning Data
Betreuerin: Prof. Dr. Claudia Eckert

Universität Freiburg *Okt 2010 – Jun 2017*
Staatsexamen Informatik, Mathematik und Theologie
Abschlussnote: 1,3

AUSGEWÄHLTE PROJEKTE

- **Deepfake-Total.com**
  Öffentlich zugängliche Plattform zur Erkennung von Audio-Deepfakes. Vollständige Umsetzung von Datensatzaufbau über Modelltraining bis Deployment (PyTorch, FastAPI, Docker).
- **MLAAD Datensatz**
  Mehrsprachiger Open-Source-Datensatz zur Audio-Anti-Spoofing-Forschung, international in Wissenschaft und Industrie im Einsatz.

MEDIENPRÄSENZ (AUSWAHL)

Expertenbeiträge und Interviews u. a. bei: ZDF (Heute Journal, Nano), 3sat, Galileo, Deutsche Welle, ARD, BR, HR, MDR, NTV, Pro7, France 24, Financial Times, Die ZEIT, Tagesspiegel, Handelsblatt, Frankfurter Rundschau, DPA Faktencheck, Focus Online.

Themenschwerpunkte: Audio-Deepfakes, Wahlmanipulation, KI und Desinformation, Regulierung von KI.

VORTRÄGE & LEHRE (AUSWAHL)

- *Deepfakes: Technische Hintergründe und Erkennungsmaßnahmen*, Law School Hamburg (Lehrauftrag)
- *Künstliche Intelligenz in der Unternehmenssicherheit*, Frankfurt am Main, 2025
- *Replay Attacks on Audio Deepfake Detection*, Rotterdam, 2025
- *Deepfakes und das Recht*, Institut für Urheber- und Medienrecht, München, 2025
- *Risiken automatisierter Methoden zur Manipulation medialer Identitäten*, Wien, 2024
- *MLAAD: The Multi-Language Audio Anti-Spoofing Dataset*, Tokyo, 2024
- Vorlesung *IT-Sicherheit und Machine Learning*, Technische Universität München, 2022–2024

PUBLIKATIONEN

Über 20 peer-reviewte wissenschaftliche Veröffentlichungen zu Deepfake-Erkennung und Sprachverarbeitung (u. a. Interspeech, IJCNN, BMVC). Siehe Google Scholar