GEORGIOS KAISSIS

Technical University of Munich
Institute for AI in Medicine
Einsteinstr. 25
81675 München

RESEARCH FOCUS

Privacy-preserving machine learning with a focus on differential privacy and its applications to deep learning; federated learning; probabilistic machine learning; machine learning foundations; computer vision and medical imaging analysis.

CURRENT POSITIONS

2022-	**Principal Investigator and Research Group Leader, Privacy-preserving and Trustworthy Machine Learning**, Institute for AI in Medicine, Technical University of Munich
2022-	**Principal Investigator and Research Group Leader, Reliable AI**, Institute for Machine Learning in Biomedical Imaging, Helmholtz-Zentrum Munich
2022-	**Fellow, Konrad-Zuse School of Excellence in Reliable AI**, Technical University of Munich, Focus Areas: Privacy, ML Foundations, Medicine & Healthcare
2022-	**Visiting Researcher,** Imperial College London, Department of Computing, London, UK
2021-	**Member and Principal Investigator, Privacy-preserving and Trustworthy ML Focus Group**, Munich Data Science Institute
2020-	**Adjunct Professor (Privatdozent),** Technical University of Munich
2020-	**Consultant Radiologist (Oberarzt)**, Institute for Radiology, Klinikum Rechts der Isar, Technical University of Munich

PROFESSIONAL BACKGROUND

2020-2022	**Senior Research Scientist**, Institute for AI in Medicine, Technical University of Munich
2022	**Fellow,** Foresight Institute
2020-2022	**Postdoctoral Researcher in Artificial Intelligence and Machine Learning**, Imperial College London, Department of Computing, London, UK
2020-2022	**Healthcare Unit and Research Unit Leader**, OpenMined

PROFESSIONAL QUALIFICATIONS

2020	**Postdoctoral lecturing qualification (Habilitation)**, Technical University of Munich. Title: „Artificial-Intelligence-based Radiological Imaging Analysis“
2019	**Specialist Radiologist Certification** (Facharzt für Radiologie)
2019	**Master's Degree in Health Business Administration**, Friedrich-Alexander Universität Erlangen-Nürnberg
2015	**Doctoral Thesis** (Dr. med.). Title: (124)-I-PET Assessment of Human Sodium Iodide Symporter Gene Activity for Highly Sensitive In Vivo Monitoring of Teratoma Formation in Mice. Grade: *magna cum laude.* Advisor: Prof. P. Bartenstein, Klinik und Poliklinik für Nuklearmedizin, Ludwig-Maximilians-Universität München
2011-2015	**Doctoral Programme in Molecular Medicine and Systems Biology**, Ludwig-Maximilians-Universität München
2007-2014	**Medical Degree**, Ludwig-Maximilians-Universität München. Grade: 1,5 (top 10% of graduates)
2007	**Abitur**, Deutsche Schule Thessaloniki. Grade: 1,0

FURTHER QUALIFICATIONS

2023	**Professional Training Certificate: Diversity, Inclusion and Belonging**, Society for Human Resource Management
2023	**Professional Training Certificate: Inclusive Mindset**, National Association of State Boards of Accountancy
2021	**Certificate of Higher Education Teaching (Zertifikat Hochschullehre),** Technical University of Munich

FUNDING

2023	**Privacy-Preserving AI and Survival Prediction for Pancreatic Cancer Patients,** German Research Foundation (under review)	**455.850€**
2023	**PrivateAIM,** Federal Ministry for Education and Science (BMBF, co-PI)	**940.000 €**
2022	**Helmholtz Junior Research Group,** Helmholtz-Society	**760.000€**
2022	**Privacy-preserving machine learning for nosocomial infection chain tracing,** Special Research Programme of the State of Bavaria	**75.000€**
2020	**Clinician Scientist Programme,** Technical Universtiy of Munich	**75.000€**

2019	**UPGRADE,** German Centre for Translational Cancer Research (co-PI)	**150.000€**
2017	**GPU Grant,** NVIDIA	**5.000€**

AWARDS & SCHOLARSHIPS

Awards

2023	**Publication Award,** Bavarian Centre for Cancer Research (BZKF)
2023	**Publication Award,** German Society for Digital Medicine (DGDM)
2022	**Honourable Mention, Best Paper of the Year Award,** Munich Data Science Institute
2021	**Eugen-Münch-Award, Category Science,** Münch Foundation
2021	**Supervisory Award,** TUM CEDOSIA
2019	**Top-20 Presenter Award,** European Society of Gastrointestinal and Abdominal Radiology
2019	**Young Investigator Award,** German Roentgen Society
2017 & 2018	**Invest in the Youth Award**, European Society of Radiology
2017	**Best Scientific Paper Award,** European Society of Radiology
2017	**Travel Award,** Radiological Society of North America

Scholarships

2007-2014	**German National Merit Foundation (Studienstiftung des Deutschen Volkes),** Full Scholarship
2011-2012	**Research and Teaching Programme (Förderungsprogramm für Forschung und Lehre),** LMU Munich, Scholarship
2006	**Niedersachsen Foundation (Stiftung Niedersachsen),** Scholarship

SELECTED PUBLICATIONS

For a full publication list, please see my Google Scholar profile.

Meiser, P., Knolle, M., [...], **Kaissis, G**.* and Böttcher, J.* (*equal contribution), 2023. A distinct stimulatory cDC1 subpopulation amplifies CD8+ T cell responses in tumors for protective anti-cancer immunity, *Cancer Cell*

Mueller, T.T., Usynin, D., Paetzold, J.C., Rueckert, D. and **Kaissis, G.**, 2023. Differentially Private Guarantees for Analytics and Machine Learning on Graphs: A Survey of Results. *Journal of Privacy and Confidentiality* (accepted)

Usynin, D., Rueckert, D. and **Kaissis, G.**, 2023. Beyond gradients: Exploiting adversarial priors in model inversion attacks. *ACM Transactions on Privacy and Security* (TOPS)

Mueller, T.T., Paetzold, J.C., Prabhakar, C., Usynin, D., Rueckert, D. and **Kaissis, G.,** 2022. Differentially Private Graph Neural Networks for Whole-Graph Classification. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (TPAMI)

Ziller, A., Mueller, T.T., Braren, R., Rueckert, D. and **Kaissis, G.**, 2022. Privacy: An axiomatic approach. *Entropy*

Kaissis, G., Knolle, M., Jungmann, F., Ziller, A., Usynin, D. and Rueckert, D., 2022. A Unified Interpretation of the Gaussian Mechanism for Differential Privacy Through the Sensitivity Index. *Journal of Privacy and Confidentiality*

Usynin, D., Ziller, A., Makowski, M., Braren, R., Rueckert, D., Glocker, B., **Kaissis, G.** and Passerat-Palmbach, J., 2021. Adversarial interference and its mitigations in privacy-preserving collaborative machine learning. *Nature Machine Intelligence*

Ziller, A., Usynin, D., Braren, R., Makowski, M., Rueckert, D. and **Kaissis, G.**, 2021. Medical imaging deep learning with differential privacy. *Scientific Reports*

Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., Lima Jr, I., Mancuso, J., Jungmann, F., Steinborn, M.M. and Saleh, A., 2021. End-to-end privacy preserving deep learning on multi-institutional medical imaging. *Nature Machine Intelligence*

Dou, Q., So, T.Y., Jiang, M., Liu, Q., Vardhanabhuti, V., **Kaissis, G.**, Li, Z., Si, W., Lee, H.H., Yu, K. and Feng, Z., 2021. Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study. *NPJ Digital Medicine*

Kaissis, G.A., Makowski, M.R., Rückert, D. and Braren, R.F., 2020. Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence*

Nasirigerdeh, R., Torkzadehmahani, J., Rueckert, D. and **Kaissis, G.**, Kernel Normalized Convolutional Networks for Privacy-Preserving Machine Learning. *First IEEE Conference on Secure and Trustworthy Machine Learning.* (SaTML)

Usynin, D., Rueckert, D., Passerat-Palmbach, J. and **Kaissis, G.**, 2022. Zen and the art of model adaptation: Low-utility-cost attack mitigations in collaborative machine learning. *Proc. Priv. Enhancing Technol.* (PETS)

Hou, B., **Kaissis, G.,** Summers, R.M., Kainz, B., 2021, RATCHET: Medical Transformer for Chest X-ray Diagnosis and Reporting. International Conference on Medical Image Computing and Computer Assisted Interventions (MICCAI)

Müller, P., **Kaissis, G.**, Zou, C., Rueckert, D., 2022. Radiological Reports Improve Pre-training for Localized Imaging Tasks on Chest X-Rays. International Conference on Medical Image Computing and Computer Assisted Interventions (MICCAI)

Shit, S., […], **Kaissis G.**, […] and Menze, B., 2022. Relationformer: A Unified Framework for *Image-to-Graph* Generation. European Conference on Computer vision (ECCV)

Müller, P., **Kaissis, G.,** Zou, C., Rueckert, D., 2022, Joint Learning of Localized Representations from Medical Images and Reports. European Conference on Computer vision (ECCV)

Tanida, T., Müller, P., **Kaissis, G.,** Rueckert, D., 2023 Interactive and Explainable Region-Guided Radiology Report Generation, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)

Müller, P., **Kaissis, G.,** Rueckert, D., 2022, The Role of Local Alignment and Uniformity in Image-Text Contrastive Learning on Medical Images, NeurIPS 2022 Workshop: Self-Supervised Learning - Theory and Practice

Meissen, F., Wiestler, B., **Kaissis, G.,** Rueckert, D., 2022, On the Pitfalls of Using the Residual Error as Anomaly Score, International Conference on Medical Imaging with Deep Learning (MIDL)