Malte Josten

malte.josten@proton.me linkedin.com/malte-josten maltejosten.com

Work Experience

University of Duisburg-Essen (Duisburg, Germany) **2020/04 - today**

Research Assistant, full-time *2023/06 - today*

- [QuantumNRW] Conceptualizing new teaching concepts to introduce school and college students to quantum computing
- [QuantumNRW] Developed an augmented reality app for iOS devices using Unity and C#, and created 3D-models and animations of quantum computing processes and principles.
- [FooSH] Developed a Java Spring Boot Framework to connect arbitrary outcome-oriented (AI-driven) prediction models to an existing smart home system by providing necessary abstractions and a sophisticated REST API. This enables users to define goals (outcomes) instead of multiple instructions, to ultimately reach a desired smart home state.
- Continued work on the projects hKI-Chemie and Boarding

Research Assistant, part-time *2022/10 - 2023/05*

- [hKI-Chemie] Developed a visualisation tool in form of a web application using JavaScript, HTML, and CSS to evaluate user behaviour during AI nudging studies
- [hKI-Chemie] Developed a cross-platform, AI-assisted web tool for route-planning of cargo wagons in an industrial rail park using a JavaScript/HTML frontend and Python backend
- [Boarding] Project management, development, and administration

Student & Scientific Assistant, part-time *2020/04 - 2022/09*

- [AR-InGo] Developed an augmented reality app for iOS devices using Unity and C#, incorporating 3D-models of scientific instruments and experiments (at the nanometer level) created with Blender.
- Teaching and tutoring students in the courses Computer Architecture, Computer Networks and Communication Systems, Internet Technologies and Web Engineering, and Operating Systems.

Japan Advanced Institute of Science and Technology (Nomi, Ishikawa, Japan) **2025/12 - 2025/12**

Guest Researcher

- Collaborative efforts to develop an attack module to evaluate LLM safeguards against prompt injections.

Freelance Web Developer (North Rhine-Westphalia, Germany) **2021/12 - 2025/12**

Freelancer

- Designing, deploying, and maintaining websites using the WordPress ecosystem

Netto Marken-Discount (Mülheim an der Ruhr, Germany) **2017/10 - 2019/10**

Temporary Retail Worker, part-time

Krankikom GmbH (Duisburg, Germany) **2015/02**

Internship, full-time

- Web design, project management and administration, and agile software development

Education

University of Duisburg-Essen (Duisburg, Germany) **2017/10 - today**

PhD Student (Dr.-Ing.) at the chair for Distributed Systems *2024/01 - today*

- Research area: (Explainable) Security in Distributed Systems

Master of Science in Applied Computer Science *2021/04 - 2023/12*

- Final Grade: 1.3 (German) / 3.7 (GPA) - with distinction
- Focus: Distributed, reliable systems
- Thesis: "FooSH: A Framework for outcome-oriented Smart Homes" - Grade: 1.0 (German, equivalent to 4.0 GPA)

Bachelor of Science in Applied Computer Science *2017/10 - 2021/03*

- Final Grade: 1.6 (German) / 3.4 (GPA)
- Thesis: "Development of an augmented reality app for iOS devices to control IoT devices" - Grade: 1.0 (German, equivalent to 4.0 GPA)

Publications

Conference Papers

[C5] T. Nguyen, **M. Josten**, K. Yotsunayagi, T. Weis, and R. Beuran; *"When Text Isn't Text: Benchmarking LLM Safeguards and Defenses Against Non-Natural Language Obfuscated Attacks"*; 22nd ACM ASIA Conference on Computer and Communications Security; TBD

[C4] **M. Josten**, G. Kämmerer, A. Kummerow, and T. Weis; *"Size Does Matter: The Impact of Embedding Models and Sizes on Spam Email Classification"*; Proceedings of the 23rd International Conference on Security and Cryptography (SECRYPT 2026); 10.5220/0015082300004103

[C3] **M. Josten**; *"Large Language Models as a Cyber Threat: Towards Countering LLM-based Spam Attacks"*; 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops); PerComWorkshops65533.2025.00138

[C2] **M. Josten**, M. Schaffeld, R. Lehmann, and T. Weis; *"Navigating the Security Challenges of LLMs: Positioning Target Defenses and Identifying Research Gaps"*; Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 2 (ICISSP 2025); 10.5220/0013274700003899

[C1] **M. Josten** and T. Weis; *"Investigating the Effectiveness of Bayesian Spam Filters in Detecting LLM-modified Spam Mails"*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 613. Springer (ICDF2C 2024); 10.1007/978-3-031-89363-6_16

Workshop Papers

[W1] V. Matkovic, **M. Josten**, and T. Weis; *"Optical Token Transmission for Secure IoT Device Discovery and Control in Ubiquitous Environments"*; Companion of the 2025 ACM International Joint Conference on Pervasive and Ubiquitous Computing; 10.1145/3714394.3756299

Demo Papers

[D1] E. Becks, **M. Josten**, V. Matkovic, and T. Weis; *"Revising Poor Man's Eyetracking For Crowd-Sourced Studies"*; 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops); 10.1109/PerComWorkshops56833.2023.10150386

Artifact Paper

[A1] E. Becks, **M. Josten**, V. Matkovic, and T. Weis; *"Artifact: Revising Poor Man's Eye Tracker for Crowd-Sourced Studies"*; 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops); 10.1109/PerComWorkshops56833.2023.10150307

Projects

EIN Quantum NRW **2024/01 - 2026/12**
Developing a modern and digital education concept for school and university students to introduce them to the world of quantum computing.

hKI-Chemie: Human-centered AI in the chemical industry **2022/06 - 2024/06**
Researched and developed self-explainable AI solutions to:

- Optimize processes with the help of AI-based process parameter evaluation
- Support employees in identifying process problems at an early stage and selecting suitable solutions
- Optimize availability of machine-learned connections across shifts and personnel changes

Boarding: Automated Attendance Checks **2022/09 - 2023/12**
Developed a GDPR and Common Criteria (EAL 4+) compliant cross-platform mobile application for automated attendance checks for university-related events, e.g., exams.

AR-InGo: Augmented Reality for Engineering **2020/01 - 2022/04**
Developed a modern and digital education concept for school and university students visiting the NanoSchoolLab. The concept provides easily comprehensible 3D models of complex scientific instruments and experiments (including SEM, STM, and solar cells), and uses gamification mechanics to encourage a playful learning experience.

Activities

Reviewer	Knowledge-Based Systems (Vol. 349)	
	AAAI/ACM Conference on AI, Ethics and Society	2026
	International Conference on Intelligent Environments	2025
	International Conference on Pervasive Computing and Communications	2025
Web Chair	International Conference on Internet of Things	2024
Organiser	International Workshop on Negative Results in Pervasive Computing	2027
	International Workshop on Longevity and Sustainability of IoT Systems	2026
	International Workshop on Negative Results in Pervasive Computing	2026
	International Workshop on Longevity and Sustainability of IoT Systems	2025
	International Workshop on Security and Privacy-Preserving AI/ML	2025
	International Workshop on Negative Results in Pervasive Computing	2025
	International Workshop on Longevity and Sustainability of IoT Systems	2024
	International Workshop on Negative Results in Pervasive Computing	2024
Editor	Proceedings of the 1st International Workshop on Security and Privacy-Preserving AI/ML	2026
Member	Global Youth Tech Assembly	2026/07 - today
	WEF GlobalShapers @Düsseldorf Hub	2025/08 - today
	IEEE CS SYP Micro Mentoring	2024/09 - today
	Appointment Committee, W3 Professorship "Verification of Complex Systems"	2024/10 - 2025/10

Skills

Languages

- German (Native)
- English (Full professional proficiency)
- French (Elementary proficiency // B1, 2017)
- Mandarin (Elementary proficiency // HSK 2, 2026)