Malte Josten

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

Berufserfahrung

Universität Duisburg-Essen (Duisburg, Deutschland) **2020/04 - heute**

Wissenschaftlicher Mitarbeiter, Vollzeit *2023/06 - heute*

- [QuantumNRW] Konzeptionierung neuer Lehrkonzepte zur Einführung von Schülern und Studenten in das Thema Quantencomputing
- [QuantumNRW] Entwicklung einer Augmented Reality App für iOS-Geräte mit Unity und C#, sowie Erstellung von 3D-Modellen und Animationen von Quantencomputingprozessen und -eigenschaften
- [FooSH] Entwickelung eines Java Spring Boot Framework, um beliebige ergebnisorientierte (KI-basierte) Vorhersagemodelle mit einem bestehenden Smart-Home-System zu verbinden, indem es notwendige Abstraktionen implementiert und eine REST-API bereitstellt. Dies ermöglicht es Benutzern, anstelle mehrerer Anweisungen Ziele zu definieren, um letztendlich den gewünschten Smart Home-Zustand zu erreichen.
- Fortsetzung der Arbeit an den Projekten hKI-Chemie und Boarding

Wissenschaftlicher Mitarbeiter, Teilzeit *2022/10 - 2023/05*

- [hKI-Chemie] Entwicklung eines web-basierten Visualisierungstools mit JavaScript, HTML und CSS, um Nutzerverhalten während KI-Nudging Studien zu evaluieren
- [hKI-Chemie] Entwicklung eines cross-plattform, KI-unterstützten Webtools zur Routenplanung für Rangierer in einem Industriepark bestehend aus einem JavaScript/HTML Frontend und Python Backend
- [Boarding] Projektmanagement, Softwareentwicklung und -administration

Studentische & wissenschaftliche Hilfskraft, Teilzeit *2020/04 - 2022/09*

- [AR-InGo] Entwicklung einer Augmented Reality App für iOS-Geräte mit Unity und C#, sowie Erstellung von 3D-Modellen von wissenschaftlichen Instrumenten und Experimenten im Nanometerbereich.
- Tutor für die Kurse Betriebssysteme, Internettechnologien und Web Engineering, Rechnerarchitektur, Rechnernetze und Kommunikationssysteme.

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

Gastforscher

- Entwicklung eines Angriffsmoduls zur Bewertung der LLM-Sicherheitsvorkehrungen gegen Prompt Injections.

Freelance Webentwickler (Nordrhein-Westfalen, Deutschland) **2021/12 - 2025/12**

Freelancer

- Erstellung, Gestaltung und Wartung von Websites in WordPress

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

Aushilfe, Teilzeit

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

Praktikant, Vollzeit

- Webdesign, Projektmanagement und -administration sowie agile Softwareentwicklung

Ausbildung

Universität Duisburg-Essen (Duisburg, Deutschland) **2017/10 - heute**

Doktorand (Dr.-Ing.) am Lehrstuhl für Verteilte Systeme *2024/01 - heute*

- Forschungsbereich: (Erklärbare) Sicherheit in verteilten Systemen

Master of Science im Studiengang Angewandte Informatik (Note: 1.3, mit Auszeichnung) *2021/04 - 2023/12*

- Fokus: Verteilte, verlässliche Systeme
- Thesis: "FooSH: A Framework for outcome-oriented Smart Homes" (Note: 1.0)

Bachelor of Science im Studiengang Angewandte Informatik (Note: 1.6) *2017/10 - 2021/03*

- Thesis: Ëntwicklung einer Augmented Reality App für iOS-Geräte zur Bedienung von IoT-Geräten"(Note: 1.0)

Publikationen

Konferenz Paper

[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; *SSize 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; *Ïnvestigating 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 Paper

[W1] V. Matkovic, **M. Josten**, and T. Weis; *Öptical 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 Paper

[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

Artefakt Paper

[A1] E. Becks, **M. Josten**, V. Matkovic, and T. Weis; *Ärtifact: 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

Projekte

EIN Quantum NRW **2024/01 - 2026/12**
Entwicklung eines modernen und digitalen Bildungskonzepts für Schüler und Studenten, um sie in die Welt des Quantencomputings einzuführen.

hKI-Chemie: Human-centered AI in the chemical industry **2022/06 - 2024/06**
Erforschung und Entwicklung von selbsterklärenden KI-Lösungen die die folgenden Ziele erreichen:

- Optimierung von Prozessen durch KI-basierte Auswertung der Prozessparameter
- Unterstützung der Mitarbeiter*innen bei der frühzeitigen Erkennung von Prozessproblemen und bei der Auswahl geeigneter Lösungen
- Verfügbarkeit maschinell gelernter Zusammenhänge über Schichten und Personalwechsel hinweg

Boarding: Automatische Anwesenheitskontrollen **2022/09 - 2023/12**
Entwicklung einer DSGVO und Common Criteria (EAL 4+)-konformen plattformübergreifenden mobilen Anwendung für automatisierte Anwesenheitskontrollen für universitätsbezogene Veranstaltungen, z.B. Klausuren.

AR-InGo: Augmented Reality für die Ingenieurwissenschaften **2020/01 - 2022/04**
Entwicklung eines modernen und digitalen Bildungskonzepts für Schüler und Studierende, die das NanoSchoolLab besuchen. Das Konzept stellt leicht verständliche 3D-Modelle komplexer wissenschaftlicher Instrumente und Experimente (einschließlich REM, RTM und Solarzellen) bereit und nutzt Gamification-Mechaniken, um ein spielerisches Lernerlebnis zu fördern.

Aktivitäten

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
Organisator	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
Mitglied	Global Youth Tech Assembly	2026/07 - heute
	WEF GlobalShapers @Düsseldorf Hub	2025/08 - heute
	IEEE CS SYP Micro Mentoring	2024/09 - heute
	Berufungskomission, W3 Professur "Verifikation komplexer Systeme"	2024/10 - 2025/10

Skills

Sprachen

- Deutsch (Muttersprache)
- Englisch (Verhandlungssicher)
- Französisch (Grundkenntnisse // B1, 2017)
- Mandarin (Grundkenntnisse // HSK 2, 2026)