

Dr Erik Buchholz

📍 Sydney, Australia
✉ erik@erikbuchholz.de

🖥 erikbuchholz.de
🖥 [linkedin.com/in/erik-buchholz/](https://www.linkedin.com/in/erik-buchholz/)

Profile

- Conducting research in **cybersecurity, privacy** and **artificial intelligence (AI)** at CSIRO's Data61
- Developed an encryption suite under the **Defence Trailblazer** with UNSW and GuardWare
- Completed a PhD at **UNSW Sydney (THE top 100)** on AI-driven trajectory privacy with **CSIRO's Data61**
- Authored seven publications at top venues (**four CORE A**), receiving the **Best Paper Award** at PST'24
- Awarded Arc PGC **Research Candidate Award** and selected as **Top100 Future Leader 2025**

Education

PHD IN COMPUTER SCIENCE | CSIRO'S DATA61 & UNSW SYDNEY 2021 – 2025

- Conferred: August 2025
- **Thesis Title:** "The Long Road to Trajectory Privacy: Differential Privacy and Generative Models"
- Scholarship: Cyber Security Cooperative Research Centre (CSCRC)
- Supervisors: [Prof. Salil S. Kanhere](#) and [Dr. Surya Nepal](#)

MASTER OF COMPUTER SCIENCE WITH DISTINCTION | RWTH AACHEN 2017 – 2020

- Final Grade: 1.0 (excellent – [German Grading System](#))
- **Study Focus:** IT Security, Cryptography, Internet Technology, Seminar on App Fingerprinting
- Master's Thesis: Privacy-Preserving Exchange of Process Parameters

BACHELOR OF COMPUTER SCIENCE WITH DISTINCTION | RWTH AACHEN 2013 – 2017

- Final Grade: 1.1 (excellent – [German Grading System](#))
- **Study Focus:** Advanced & Mobile Internet Technology, Seminar on Privacy
- Bachelor's Thesis: A User-controlled Data Market for Privacy-preserving Data Analyses

Publications (selected): Refer to [Google Scholar](#)

Synthetic Trajectory Generation Through Convolutional Neural Networks

- Awarded *Best Paper Award* at the International Conference on Privacy, Security, and Trust ([PST'24](#))
- Investigates the use of convolutional neural networks for trajectory generation ([source code published](#))

SoK: Can Trajectory Generation Combine Privacy and Utility?

- Accepted at [PETS'24](#) (CORE A, 19.5% Acceptance Rate); [source code published](#) and independently reviewed
- Systemises and evaluates generative models for privacy-preserving trajectory synthesis

Reconstruction Attack on Differential Private Trajectory Protection Mechanisms

- Accepted at [ACSAC'22](#) (CORE A, 24.1% Acceptance Rate); [source code published](#) and independently reviewed
- Targets a deep learning-based reconstruction attack on trajectories protected with differential privacy

Privacy-Preserving Production Process Parameter Exchange

- Accepted at [ACSAC'20](#) (CORE A, 23.2% Acceptance Rate); [source code published](#) and independently reviewed
- Motivated by a real-world use case from the injection moulding industry

Research and Professional Experience

RESEARCH SCIENTIST | CSIRO'S DATA61 APR 2026 – PRESENT

- Conducting innovative cybersecurity research focused on the security and privacy of AI systems
- Producing scientific publications, client reports, and patent applications; presenting at conferences
- Supervising students and research interns; undertaking feasibility studies
- Collaborating across multi-disciplinary teams to deliver on CSIRO's strategic objectives

RESEARCH ASSOCIATE | UNSW SYDNEY & GUARDWARE MAR 2025 – APR 2026

- Key researcher for the Defence Trailblazer project "Resilience of Supply Chain Unstructured Data"
- Conducted industrial research in data encryption, key management, and protection of unstructured data
- Developed the encryption software "PROTECT" offering protection across the entire Defence supply chain
- Devised a novel cryptographic protocol for the first-of-its-kind capability to persistently encrypt design files

VOLUNTEER SERVER ADMINISTRATOR | UNSW SYDNEY DEC 2023 – APR 2026

- Managed five GPU servers for the ISPri Research Group at UNSW Sydney
- Performed all administration tasks, including patching, user management, technical support, troubleshooting, and system security

TUTOR | UNSW SYDNEY SEP 2022 – MAY 2024

- Presented tutorials, led labs, and corrected assignments for "*Computer Networks and Applications*"

SCIENCE ASSISTANT | RWTH AACHEN APR 2019 – SEP 2019

- Evaluated software projects for publication and assisted in writing scientific papers: AsiaCCS'20 publication

PYTHON TUTOR | UNIVERSITY OF TECHNOLOGY SYDNEY (UTS) AUG 2017 – NOV 2017

- Established a new course for students of all faculties, including the creation of materials and presentation

TUTOR | RWTH AACHEN 2015 – 2018

- Tutored three different subjects over five semesters

Awards

- 2025 | **Research Candidate Award**: Arc PGC Faculty of Engineering
- 2025 | **Top100 Future Leader Award Finalist**: GradConnection Top 100
- 2024 | **Best Paper Award**: 21st Annual International Conference on Privacy, Security, and Trust (PST2024)
- 2024 | **Engineering Industry Engagement Grant**
- 2023 | **Best Poster Award**: SecEdu Conference 2023
- 2023 | **AGSE 3 Minute Thesis Competition**: People's Choice & 2nd Place Overall
- 2023 | **AGSE Industry PhD Program**: For a PhD with Industry Engagement
- 2022 | **ACSAC Student Conferenceship**: Valued at \$1,900 USD
- 2021 | **CSCRC PhD Scholarship**: May 2021 – May 2024
- 2021 | **University International Postgraduate Award (UIPA) Scholarship**: May 2021 – November 2024
- 2020 | **Vöcking Master Award**: Outstanding master's thesis
- 2020 | **FOLKS Award for Best Master's Thesis**
- 2019 | **Dean's List of RWTH Aachen** (4x) – Top 5% of CS students: 2013/14, 2014/15, 2017/18, 2019/20
- 2018 | **German Education Fund** (3x): Study years 2015/2016, 2017/2018, and 2018/2019
- 2016 | **Seminar Award of FOLKS**
- 2013 | **Best High School Graduate in the City of Wolfsburg**

Supervision & Academic Leadership

- 2026 | **ACM CCS 2026 PC Member** | Review of publications submitted to the “Privacy and Anonymity” track.
- 2026 | **ATSE Emerging Leaders Member** | Contributing to national STEM policy and advocacy through evidence-based decision-making.
- 2025 | **Web Chair of Australian Summer School on Privacy** | Managed website and handled participant communication for the Australian Summer School on Privacy hosted at UNSW Sydney.
- 2024 – Present | **Research Intern Supervision** | Supervised three research interns at UNSW Sydney.
- 2023 – Present | **Thesis Supervision** | Co-Supervised two Honours Theses at UNSW Sydney.
- 2022 – Present | **Paper Reviews** | Reviewed 25 papers, including for ACM CCS, AsiaCCS, and IEEE TDSC.
- 2024 – 2025 | **Student Advisory Board of AGSE Industry PhD** | Advising on program direction.
- 2024 – 2025 | **Capstone Project Supervision** | Supervised five capstone projects with 28 students total, resulting in an international publication and two PhD applications.
- 2023 | **Panellist** | Participated as a panellist for the AGSE Industry PhD Program discussion at UNSW Sydney.
- 2023 | **Presentation** | Presented at the PETS workshop “*Current Challenges and Emerging Technologies*”.
- 2022 – 2023 | **HDR Peer Mentor** | Mentored 17 first-year PhD candidates at UNSW Sydney.
- 2022 | **Conference Student Workshop Committee** | Organised IFCYBER Thesis Competition.

Qualifications & Courses (Selected)

- 2023 | **HDR Employability Program** | UNSW Sydney
- 2023 | **IMNIS Engage** | Mentoring Program
- 2022 | **Leadership Foundations Program** | UNSW Sydney
- 2021 | **Deep Learning Specialisation** | DeepLearning.AI
- 2021 | **Personalised English Learning Enhancement** | UNSW Sydney – 94% Grade

Skills

- **Research Areas:** Cybersecurity & Privacy (Differential Privacy, Applied Cryptography, Encryption, Key Management), Artificial Intelligence (Deep Learning, Generative Models)
- **Programming:** Python, PyTorch, TensorFlow/Keras, C++, Microsoft CNG, C, Hugo
- **Systems:** Ubuntu Server Management, Git CI/CD, Docker, System Automation
- **Languages:**
 - English: Expert User (IELTS Overall Score: 9.0)
 - German: Native Speaker
 - Spanish: Level B2

Personal Interests

- CrossFit
- Nutrition
- Marathon Running
- Wildlife Photography
- Spanish
- Travel