Ashutosh Ghimire

Fairborn, OH, USA | ashutosh.ghimire@wright.edu | https://aashutoshghimire.github.io
Google Scholar: https://scholar.google.com/citations?user=mhTDRysAAAAJ&hl=en
ORCID: https://orcid.org/0000-0001-6210-1219
LinkedIn: https://www.linkedin.com/in/ashutoshghimire
GitHub: https://github.com/aashutoshghimire

SUMMARY

Computer Science and Engineering PhD candidate at Wright State University working across trustworthy AI, adversarial machine learning, hardware security, side-channel analysis, LLM-assisted systems, and applied scientific machine learning. Portfolio reports 231+ Google Scholar citations across 33+ scholar-listed papers as of 2026-05-04. Three years of prior software engineering experience building REST APIs, backend systems, production web applications, and customer-facing software.

TECHNICAL SKILLS

AI / Machine Learning: Python, scikit-learn, pandas, NumPy, TensorFlow, Keras, PyTorch, Transformers, CNNs, self-attention, clustering, anomaly detection

Trustworthy AI and ML Security: Adversarial ML, ART, robustness testing, explainable AI, SHAP, LIME, pseudo-labeling, synthetic augmentation

Hardware Security: Hardware Trojan detection, FPGA, Basys 3, Ring Oscillator Networks, power/EM side-channels, feature extraction, golden-reference-free detection

LLMs and NLP: LLM-assisted explainability, rubric-aware scoring, synthetic transcripts, Longformer, DistilBERT, SBERT, NLP classification

Systems / HPC: Linux, SLURM, Docker, Singularity, Jupyter, SSH/SCP, Bash, distributed workflows, experiment management

Web, APIs, and Security: REST APIs, microservices, Swagger, Postman, Git, Go, C/C++, Wireshark, tcpdump, Zeek, Ghidra, Binary Ninja

EDUCATION

PhD in Computer Science and Engineering, Wright State University

Present

Technical focus: trustworthy AI, hardware security, side-channel analysis, adversarial ML, LLM systems, and AI for security.

Master of Science in Computer Science, Wright State University

April 2024

Thesis: An ML-Assisted Golden-Free Hardware Trojan Localization and Detection Approach for Trusted Microelectronics.

Bachelor of Engineering in Computer Engineering, Tribhuvan University

February 2019

Engineering foundation in software, systems, and computer engineering.

EXPERIENCE

Graduate Research Assistant, Wright State University

May 2025 - Present | Fairborn, OH, USA

- Designed and evaluated adversarially robust ML pipelines for side-channel hardware security datasets, including work publicly reported with zero false negatives under adversarial perturbation.
- Built feature extraction, clustering, and adversarial evaluation workflows for hardware Trojan detection using Ring Oscillator Network and related side-channel measurements.
- Refactored preprocessing and inference stages for deterministic, reproducible batch experimentation.

Teaching Assistant and Research Mentor, Wright State University / NSF REU led by WSU and co-led by AFIT

Spring 2026 / June 9 - August 7, 2025 | Fairborn, OH, USA

- Supported 2 graduate courses, CEG 7350 Computer Architecture and CEG 7900 Trustworthy AI Hardware, through grading, exams, presentations, and student help hours.
- Designed lecture, assignment, and lab material across 6 AI-hardware/security topic areas: buffer overflows, ML/deep learning, PUF attacks, Trojan detection, side-channel analysis, and adversarial robustness.
- Mentored 2 NSF REU 2025 students, Cole Castronova and Ryan Dang, from June 9 to August 7, 2025 on adversarially robust hardware Trojan detection with synthetic data augmentation.
- Supported WSU-led interview and onboarding work for 18 NSF REU interns across the 2025 and 2026 cohorts, with 9 interns selected each year.

Research Associate, Wright State University

August 2024 - April 2025 | Fairborn, OH, USA

- Developed adaptive ensemble learning models for real-time financial fraud detection under concept drift.
- Integrated explainability methods to improve trust and usability in security-critical ML systems.
- Contributed technical framing and white-paper drafting for a publicly listed $100K funded Trustworthy AI / Explainable AI initiative.

Graduate Research Assistant, Wright State University

September 2022 - April 2024 | Fairborn, OH, USA

- Implemented distributed federated learning systems for secure and privacy-aware AI hardware.
- Developed ML-assisted hardware Trojan localization and detection algorithms, contributing to golden-free side-channel work publicly reported at 93% published detection accuracy.
- Designed parallel ML approaches for multicore environments and contributed to hardware security publications.

Research Student, Jeonbuk National University

September 2021 - August 2022 | Jeonju, South Korea

- Developed CSatDTA for drug-target affinity prediction using convolutional self-attention, published in *International Journal of Molecular Sciences* 23(15), 8453.
- Worked with large-scale drug-target interaction data and preprocessing workflows.
- Combined AI, chemistry, pharmacology, and biology concepts for computational drug discovery.

Software Engineer, YBC Services

May 2021 - August 2021 | Remote / Aldershot, UK

- Developed RESTful APIs serving React and Flutter frontends for HR management software.
- Supported production software handling 1,000+ concurrent users.
- Led team planning, blocker tracking, and API development workflows.

Software Engineer, Bent Ray Technologies

December 2018 - June 2021 | Lalitpur, Nepal

- Built and deployed production web applications across e-commerce and enterprise platforms.
- Designed REST APIs for staffing and business systems with secure data exchange.

TEACHING, SERVICE, AND LEADERSHIP

IEEE SaTC Conference Coordination and Program Operations

IEEE Conference on Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics | 2025 - 2026

- Supported program structure, session planning, speaker coordination, chair communication, logistics, and recognition materials for 2025 and 2026 conferences.
- Built full program agendas, coordinated keynote/invited/panel participants, and distributed signed certificates.
- Supported in-person registration, name tags, swag, on-site logistics, and volunteer mentoring.

Research Mentorship and Lab Coordination, SMART Cybersecurity Research Lab

Coordinated research tasks, trained new students, supported documentation, and helped organize lab activities.

Nepalese Student Association Treasurer, Wright State University

Managed operations and logistics for a 200+ participant student organization.

AWARDS

Graduate Student Excellence Award, Wright State University

April 2025

Awarded by the College of Graduate Programs and Honors Studies with a $400 graduate student excellence award.

Funded Trustworthy AI / XAI White-Paper Contribution

Contributed technical framing and white-paper drafting for a $100K funded Trustworthy AI / Explainable AI initiative under Dr. Fathi Amsaad's guidance.

PUBLICATIONS

1. **AI-enabled image processing approach for efficient clustering and identification of hardware Trojans.** Ashutosh Ghimire, Mohammed Alkurdi, Saraju P. Mohanty, Fathi Amsaad. *Integration*, Volume 107, Article 102628, 2026. DOI: 10.1016/j.vlsi.2025.102628.
2. **Adversarial Attack Resilient ML-Assisted Golden Free Approach for Hardware Trojan Detection.** Ashutosh Ghimire, Mohammed Alkurdi, Ghazal Ghajari, Mohammad Arif Hossain, Fathi Amsaad. *Microelectronics* 2(1), 2, 2026. DOI: 10.3390/microelectronics2010002.
3. **A Golden-Free Unsupervised ML-Assisted Security Approach for Detection of IC Hardware Trojans.** Ashutosh Ghimire, Mohammed Alkurdi, Md. Tauhidur Rahman, Saraju Mohanty, Fathi Amsaad. *ACM Journal on Emerging Technologies in Computing Systems* 21(3), 2025. DOI: 10.1145/3748652.
4. **A Survey on Application of AI on Reverse Engineering for Software Analysis and Security.** Ashutosh Ghimire, Sahasra Rao Lingala, Junjie Zhang, Faris Alsulami, Fathi Amsaad. *IEEE Access* 13, 152903-152913, 2025. DOI: 10.1109/ACCESS.2025.3593456.
5. **CSatDTA: Prediction of Drug-Target Binding Affinity Using Convolution Model with Self-Attention.** Ashutosh Ghimire, Hilal Tayara, Zhenyu Xuan, Kil To Chong. *International Journal of Molecular Sciences* 23(15), 8453, 2022. DOI: 10.3390/ijms23158453.