HALIMA BOUZIDI

Looking for Research and Development opportunities beginning Winter 2025.
Address: 3430 Engineering Hall, University of California, Irine, CA, USA
+1(949) 678-xxxx ◇ hbouzidi@uci.edu ◇ linkedin.com/halimabouzidi ◇ halimabouzidi.github.io/

SUMMARY

Machine Learning and Security researcher with 5+ years of experience in developing efficient AI systems and adversarial security tools. Proven expertise in Secure and Trustworthy AI, Adversarial Machine Learning, and Edge/Embedded AI deployment. Experienced in leading research projects (DARPA, academic, and industry collaborations) and translating cutting-edge innovations into practical solutions for AI systems security and safety.

EDUCATION

Postdoctoral Scholar, *Aug 2024, Current*
University of California, Irvine, CA, USA
Topic: Secure Machine Learning, Autonomous Systems Security, AI for Security, Red-Teaming
Advisors: Prof. Mohammad Al Faruque (Primary: UCI), Prof. Qi Alfred Chen (Co-PI, UCI)

Ph.D in Computer Engineering, *Jan 2021, Jan 2024*
National Institute of Applied Sciences of Hauts-de-France
Thesis: Efficient Deployment of Deep Neural Networks on Hardware Devices for Edge AI
Committee: Prof. Olivier Sentieys (Chair), Prof. Tulika Mitra, Prof. Clarisse Dhaenens, Dr. Nicolas Ventroux.
Advisors: Prof. Smail Niar, Prof. El-Ghazali Talbi, Dr. Hamza Ouarnoughi

B.Sc/M.Sc in Computer Engineering, *Sep 2015, Sep 2020*
The Higher National School of Computer Science of Algiers, Algeria
Thesis: Performance Modeling of Computer Vision-based CNN on Edge GPUs

RESEARCH INTERESTS

Secure Machine Learning: Adversarial Machine Learning, Robustness Evaluation, Red-Teaming of AI Systems, AI for Security, Security of Autonomous Systems, Privacy Attacks (Membership Inference, Model Hijacking)

Efficient Machine Learning: Hardware-Aware Neural Architecture Search (NAS), Graph Neural Networks, Edge AI, Energy-Efficiency, Model Compression (pruning, quantization), Co-Optimization of Algorithms and Hardware.

EMPLOYMENT HISTORY

Postdoctoral Scholar Aug 2024, Current
University of California, Irvine, USA

Lecturer (Advanced C Programming) Jan 2025, Mar 2025
University of California, Irvine, USA

Research Fellow in Trustworthy AI Jan 2024, Jul 2024
Queen's University of Belfast, UK

Graduate Teaching Assistant Nov 2021, Mar 2023
National Institute of Applied Sciences of Hauts-de-France

Graduate Research Assistant Jan 2021, Jan 2024
National Institute of Applied Sciences of Hauts-de-France

Research Intern Jan 2020, Jun 2020
Polytechnic University of Hauts-de-France, France

Software Developer Intern Jun 2018, Sep 2018
SONELGAZ Company for Electricity and Natural Gas Distribution in Algeria

PROFESSIONAL EXPERIENCES

Postdoctoral Scholar: Secure AI Systems *Aug 2024, Current*

Research Lead of the AICPS@UCI Security Group: [C10-C12], [D1-W1], [U2-U5] *Irvine, CA, USA*

- Leading the AICPS Security Group to investigate emerging threats to AI-driven autonomous systems, including evasion attacks on Machine Learning models such as Transformers, Diffusion models, and LLM/VLM.
- Developing new physical adversarial attacks and defenses for End-to-End ML-driven autonomous Systems.

Applied Research Program (DARPA FIRE: UCI + ASU + HII) [C12], [D1-W1], [U2-U5] *Irvine, CA, USA*

- Collaborating with teams from Arizona State University (ASU) and Huntington Ingalls Industries (HII) to develop physics-aware red-teaming framework to identify vulnerabilities in autonomous systems.
- Developing a knowledge base (SACI-DB) with over 90 cyber-physical exploits and vulnerabilities, adopted by our contractor HII to accelerate red-teaming to under 30 days for various DARPA challenges.

Research Fellow: Trustworthy AI Systems *Jan 2024, Jul 2024*

Researcher at CSIT, Queen's University of Belfast [C8-C9], [P2-P4] *Belfast, UK*

- Analyzed the threat posed by stealthy digital and physical adversarial attacks on machine learning-based methods for Hardware Trojan detection (HT), focusing mainly on CNN/LSTM models processing Hardware net-lists.
- Developed novel training-free model-hijacking attacks and evaluated defenses like differential privacy, model compression, and unlearning to mitigate hijacking and reprogramming.

Graduate Research Assistant: Efficient AI Systems *Jan 2021, Jan 2024*

National Institute of Applied Sciences of Hauts-de-France [B1], [C1-C8], [J1-J2], [M1-M2], [P1] *Valenciennes, France*

- Designed a hardware-aware Neural Architecture Search (NAS) framework integrated with dynamic voltage and frequency scaling (DVFS) for energy-efficient and accurate Deep Neural Networks in computer vision.
- Developed dynamic NAS techniques, using supernets and evolutionary search methods, enabling ML models to reconfigure on-the-fly based on input data complexity and hardware states, ensuring energy-efficient inference.
- Designed optima Graph Neural Networks for distributed execution on heterogeneous NVIDIA MPSoCs through SW/HW co-design, maximizing parallelism and resource utilization and minimizing energy costs.

SELECTED OPEN-SOURCE PROJECTS

[P4] **MLPrivacyAudit.** Privacy auditing framework for different Machine Learning architectures (MLP, CNN, and Transformer) under a range of membership inference attacks: (Link)

[P3] **SnatchML.** Training-free ML model hijacking attack demonstrating how an adversary can repurpose a pre-trained victim model to perform tasks different from its original task: (Link)

[P2] **Adv-TruDetect.** Security auditing tool for assessing the vulnerability of Hardware Trojan detection models to adversarial attacks, focusing on the resilience of CNN and LSTM classifiers under adversarial perturbations: (Link)

[P1] **Harmonic-NAS:** Multimodal and Hardware-aware Neural Architecture Search (MM-HW-NAS) framework leveraging both evolutionary and differentiable search algorithms: (Link)

SELECTED AWARDS AND HONOR

Travel Grant: Women in Machine Learning Travel Funding for attending the WiML@NeurIPS workshop. Oct 2025
Research Grant: Safety of Intelligent Traffic Management against Adversarial Attacks (UCITS $100K). Aug 2025
Notable Reviewer in the International Conference on Learning Representations (ICLR 2025) (Website) May 2025
Award from the High Performance Embedded Architectures and Compilers (HiPEAC 2024) (Certificate) Jan 2024
Ph.D. Forum Lightning talk in, CASES at the Embedded Systems Week, 2023 (Poster) Sep 2023
ACM Student Travel Grant for CASES at the Embedded Systems Week, 2023 ($500) Sep 2023
Best Paper Award Candidate Nomination in DATE, 2023 (DATE 2023 Awards) Apr 2023
Higher National School of Computer Science Entrance Exam: Ranked 11th/450 top candidates Jul 2017
National Entrance Exam to University in Math and Science: Ranked 1st/∼10.000 in Algeria/South Jul 2015

SELECTED ACADEMIC PUBLICATIONS AND PREPRINTS

Citations: 188 | **h-index: 07** | **i10-index: 05** | As of November 2025

Conferences († for co-first authorship, # for alphabetic order)

[C12] Shaoyuan Xie, Mohamad Fakih, Fayzah Alshammari, Ningfei Wang, Junchi Lu, Takami Sato, **Halima Bouzidi**, Mohammad Al Faruque, Qi Alfred Chen. "FlyTrap: Physical Distance-Pulling Attack Towards Camera-based Autonomous Target Tracking Systems". *the 33rd Network and Distributed System Security (NDSS) Symposium*, 2026

[C11] Mohamad Fakih, Rahul Dharmaji, **Halima Bouzidi**, Gustavo Quiros Araya, Oluwatosin Ogundare, Mohammad Al Faruque. "LLM4CVE: Enabling Iterative Automated Vulnerability Repair with Large Language Models", *the IEEE Euromicro Conference on Digital System Design (DSD)*, 2025

[C10] Mohamad Fakih, Rahul Dharmaji, Youssef Mahmoud, **Halima Bouzidi**, Mohammad Al Faruque. "Invisible Ears at Your Fingertips: Acoustic Eavesdropping via Mouse Sensors", *the Annual Computer Security Applications Conference (ACSAC)*, 2025. **Featured in many media outlets; GitHub repository starred over 185 times.**

[C9] Mahmoud Ghorbel†, **Halima Bouzidi**†, Ioan Marius Bilasco, Ihsen Alouani. "SnatchML: Hijacking ML models without Training Access", *the 3rd IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, 2025

[C8] Marwa Diaf, **Halima Bouzidi**, Ihsen Alouani. "Adversarially Evasive Hardware Trojans via Approximate Designs", the *Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2025

[C7] Eric Jenn, Floris Thiant, Theo Allouche, **Halima Bouzidi**, Ramon Conejo-Laguna, Omar Hlimi, Cyril Louis-Stanislas, Christophe Marabotto, Smail Niar, Serge Tembo-Mouafo and Philippe Thierion. "An Evaluation Bench for the Exploration of Machine Learning Deployment Solutions on Embedded Platforms", *the European Congress on Embedded Real Time Systems (ERTS)*, 2024

[C6] Mohamed Imededdine Ghebriout†, **Halima Bouzidi**†, Smail Niar, Hamza Ouarnoughi. "Harmonic-NAS: Hardware-Aware Multimodal Neural Architecture Search on Resource-constrained Devices", *the Asian Conference on Machine Learning (ACML), Proceedings of Machine Learning Research*, 2024

[C5] **Halima Bouzidi**†, Mohanad Odema†, Hamza Ouarnoughi, Smail Niar, Mohammad Al Faruque. "MaGNAS: A Mapping-Aware Graph Neural Architecture Search Framework for Heterogeneous MPSoC Deployment", *the ACM International Conference on Compilers, Architectures, and Synthesis for Embedded Systems (ESWEEK)*, 2023

[C4] **Halima Bouzidi**, Mohanad Odema, Hamza Ouarnoughi, Smail Niar, Mohammad Al Faruque. "Map-and-Conquer: Energy-Efficient Mapping of Dynamic Neural Nets onto Heterogeneous MPSoCs", *the ACM/IEEE International Conference on Design Automation Conference (DAC)*, 2023, **Received the HiPEAC Paper Award.**

[C3] **Halima Bouzidi**, Mohanad Odema, Hamza Ouarnoughi, Mohammad Al Faruque, Smail Niar. "HADAS: Hardware-Aware Dynamic Neural Architecture Search for Edge Performance Scaling", *the IEEE Conference on Design, Automation & Test in Europe Exhibition (DATE)*, 2023, **Nominated for the Best Paper Award.**

[C2] **Halima Bouzidi**, Hamza Ouarnoughi, Smail Niar, El-Ghazali Talbi, and Abdessamad Ait El Cadi. "Co-Optimization of DNN and Hardware Configurations on Edge GPUs", *the IEEE Euromicro Conference on Digital System Design (DSD)*, 2022

[C1] **Halima Bouzidi**, Hamza Ouarnoughi, Smail Niar, and Abdessamad Ait El Cadi. Performance Prediction for Convolutional Neural Networks on Edge GPUs, *the ACM Conference on Computing Frontiers (CF)*. 2021

Workshops, Demos, and Posters

[W1] **Halima Bouzidi**, Haoyu Liu, Mohammad Al Faruque. "See No Evil: Adversarial Attacks Against Linguistic-Visual Association in Referring Multi-Object Tracking Systems", *Reliable ML from Unreliable Data Workshop @ the Annual Conference on Neural Information Processing Systems (NeurIPS)*. 2025.

[D1] Shaoyuan Xie, Mohamad Fakih, Fayzah Alshammari, Ningfei Wang, Junchi Lu, Takami Sato, **Halima Bouzidi**, Mohammad Al Faruque, Qi Alfred Chen. "Demo: FlyTrap: Physical Distance-Pulling Attack Towards Camera-based Autonomous Target Tracking Systems", *The 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec '25 Demos, Posters, and Tutorials)*. 2025

Journals

[J2] **Halima Bouzidi**†, Mohanad Odema†, Hamza Ouarnoughi, Smail Niar, and Mohammad Al Faruque. "MaGNAS: A Mapping-Aware Graph Neural Architecture Search Framework for Heterogeneous MPSoC Deployment", *ACM Transactions on Embedded Computing Systems (TECS)*. 2023

[J1] **Halima Bouzidi**, Hamza Ouarnoughi, Smail Niar, and Abdessamad Ait El Cadi. "Performances Modeling of Computer Vision-based CNN on Edge GPUs", *ACM Transactions on Embedded Computing Systems (TECS)*. 2022

Book Chapters

[B1] **Halima Bouzidi**, Hamza Ouarnoughi, El-Ghazali Talbi, Abdessamad Ait El Cadi, and Smail Niar. Evolutionary-Based Co-optimization of DNN and Hardware Configurations on Edge GPU. In: Optimization and Learning. (OLA) 2022. Communications in Computer and Information Science, vol 1684. Springer Nature.

Preprints

[M2] **Halima Bouzidi**, Hamza Ouarnoughi, Smail Niar, El-Ghazali Talbi. "SONATA: Self-Adaptive Evolution for Multi-objective Hardware-aware Neural Architecture Search. [ArXiv]

[M1] Hadjer Benmezianе†, **Halima Bouzidi**†, Hamza Ouarnoughi, Ozcan Ozturk, Smail Niar. Treasure What You Have: Exploiting Similarity in Deep Neural Networks for Efficient Video Processing. [ArXiv]

Under-Review

[U5] **Halima Bouzidi**, Haoyu Liu, Yonatan Achamyeleh, Praneet Iddamsetty, Mohammad Al Faruque. Out of Sight, Out of Track: Adversarial Attacks on Propagation-based Multi-Object Trackers.

[U4] Yonatan Achamyeleh, Praneet Iddamsetty,, **Halima Bouzidi**, Mboutidem Mkpong, Haoyu Liu, Mohammad Al Faruque. Misaligned by Deception: How Physical Sensor Attacks Decouple Action from Intent in Embodied AI.

[U3] Yonatan Achamyeleh, Mboutidem Ekemini Mkpong, **Halima Bouzidi**, Qi Alfred Chen, Mohammad Al Faruque. FlowForge: Breaking UAV Energy Estimation via Airspeed Sensor Spoofing.

[U2] Fayzah Alshammari, Dhruv Kandula, **Halima Bouzidi**, Mboutidem Mkpong, Shaoyuan Xie, Junchi Lu, Mohammad Al Faruque, Qi Alfred Chen. CPExploiter: Understanding the End-to-End Physical Attack Capability of Cyber-Attacks on Robotic Vehicles

[U1] Ildi Alla†, **Halima Bouzidi**†, Marco Levorato, Hamza Ouarnoughi, Valeria Loscri. Real-Time Small UAV Detection: Fusing Audio and Visual Sensors for Enhanced Security.

RESEARCH GRANTS & PROPOSALS

Research Proposal: Collaborative Research: UC Noyce Initiative – Challenge 3: Securing the AI/ML Pipeline for Societal-Scale Systems. I contributed core techniques [U4-U5], [W1], research idea formulation, and proposal writing with five (05) Co-PIs from UC Irvine + UC Berkeley + UC Davis. Nov. 2025 **(Under Review)**

Research Grant: UC Intelligent Transportation Systems (UCITS) – Research Area 7: Intelligent Transportation Systems, Emerging Technologies, & Big Data. I contributed core techniques [U4-U5] and [W1], research idea formulation, and proposal writing with one (01) PI from UC Irvine. May. 2025 **(Accepted: Grant $100K)**

Research Proposal: DARPA SABER – Response to Request for Information (RFI) on Current Techniques and Tools for Vulnerability Assessment of AI-enabled Systems. I contributed core techniques [C12], [U4-U5]; and writing with two (02) Co-PIs from UC Irvine. March. 2025 **(Under Review)**

MEDIA COVERAGE

The Register — "Mouse microphones can be hacked to record you" (Oct 2025). Coverage of Mic-E-Mouse research on acoustic side-channel attacks. (Article)

UCI News — "UCI Team Collaborates on $15M Grant to Secure Cyber-Physical Systems" (Article)

PROFESSIONAL SERVICES

Nonprofit Organizations

Member in the Advisory Board of GHOST Day: AMLC (Website) *Dec 2024, Current*
Member in Women in CyberSecurity (WiCyS) Organization (Website) *Sep 2023, Current*
Co-founder and Programming Workshops Organizer in Code&Share Student Club (Website) *Jan 2018, Sep 2020*

Program Committee

(*25'*): NeurIPS, ICML, ICLR, AAAI, AISTATS, ACM CCS, EuroSys, DATE, NLDL *2025*
(*24'*): NeurIPS, ACML, DSD, ScaDL, NLDL *2024*

Artifact Evaluation Committee

(*25'*): AE@NDSS, AE@USENIX *2025*

Reviewer of Conferences/Workshops

(*25'*): NeurIPS, AAAI, ICML, ICLR, AISTATS, EuroSys, NLDL, DATE, AI4Science@ICML, GenBio@ICML, MusIML@ICML, WiML@NeurIPS, AI4Science@NeurIPS, SPIGM@NeurIPS *2025*
(*24'*): NeurIPS, ACML, ISCAS, NLDL, DATE, ICML-AI4Science *2024*
(*23'*): ISPASS, DATE, IEEE EDGE, GenBio@NeurIPS, AI4Science@NeurIPS *2023*

Reviewer of Journals

IEEE Transactions on Network and Service Management (TNSM) *2025*
IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) *2025*
ACM Transactions on Computer Systems (TOCS) *2024*
ACM Transactions on Embedded Computing Systems (TECS) *2024*

Events Organization Committee

Volunteer at The Thirty-Ninth Annual Conference on Neural Information Processing Systems (NeurIPS) *2025*

Volunteer Chair at the Cyber-Physical Systems and Internet-of-Things Week (CPS-IoT) *2025*

SEMINARS AND INVITED TALKS

Poznań University of Technology, Poland
Invited Speaker, GHOST Day: Applied Machine Learning Conference "Chasing the Efficiency in the Era of LLMs" Poznań University of Technology, Poland. 05-06 April 2024. (Speakers) (Slides)

National Institute of Applied Sciences of Hauts-de-France
Ph.D Defense "Towards Efficient Deployment of Deep Neural Networks on Hardware Devices for Edge AI", National Institute of Applied Sciences of Hauts-de-France, France. January 29, 2024. (Slides)

INRIA Nord-Europe Research Center, France
Seminar on "Bridging the Gap Between Neural Networks and Edge Devices" at the Self-Organizing Future Ubiquitous Networks (FUN) Group, INRIA Nord-Europe Research Center, Lille, France. July 18, 2023

CRISTAL-CNRS, INRIA Lille, France
Invited Talk on "Evolutionary-Based Co-Optimization of DNN and Hardware Configurations on Edge GPU" in the AutoDeepML Workshop: Design and Optimization of Deep Neural Networks, May 10-11, 2022

University of Hauts-de-France, France
Group Seminar on "Optimization of DNN and Hardware Configurations on Edge GPUs" LAMIH, Polytechnic University of Hauts-de-France (UPHF), Valenciennes, France. April 21, 2021

POSTERS AND PRESENTATIONS

(Talk) CPExploiter: The E2E Physical Attack Capability of Cyber-Attacks QPR@DARPA, *Feb. 2025*
(Pitch) Software-Aware Cyber-Physical Vulnerability Database IV&V@ASU, *Feb. 2025*
(Conference) Harmonic-NAS: Hardware-Aware Multimodal Neural Architecture Search ACML, *Sep. 2024*

(Conference) MaGNAS: A Mapping-Aware Graph Neural Architecture Search — ESWEEK *Sep 2024*
(Poster) HADAS: Hardware-Aware Dynamic Neural Architecture Search — ESWEEK, *Sep 2024*
(Conference) Map-and- Conquer: Energy-Efficient Mapping of Dynamic Neural Nets — DAC, *Jul. 2023*
(Conference) HADAS: Hardware-Aware Dynamic Neural Architecture Search — DATE, *Apr. 2023*
(Conference) Co-Optimization of DNN and Hardware Configurations on Edge GPUs — DSD, *Sep. 2022*
(Conference) Performance Prediction for Convolutional Neural Networks on Edge GPUs — CF, *Dec. 2021*

TEACHING SERVICES

EECS Department at University of California, Irvine
Instructor: EECS-22 Course on Advanced C Programming, UCI — *Winter 2025*

CS Department at INSA Hauts-de-France
TA: Introduction to Computer Architectures and Operating Systems, INSA Hauts-de-France — *Fall 2023*
TA: Introduction to Computer Architectures and Operating Systems, INSA Hauts-de-France — *Fall 2022*
TA: Introduction to Algorithm and Programming, INSA Hauts-de-France — *Fall 2022*
TA: Introduction to Computer Architectures and Operating Systems, INSA Hauts-de-France — *Fall 2021*

Training Programs Attended
Google Course on "Foundations of Cybersecurity", Grade: 87.59%, (Certificate) — *Nov. 2023*
Google Course on "Play It Safe: Manage Security Risks", Grade: 92.57%, (Certificate) — *Nov. 2023*
Participation in the NCC Portugal Nways to GPU Programming Bootcamp (Certificate) — *Nov. 2022*
The AutoML Fall School Participation at Freiburg, Germany 2021 (Virtual Event: Certificate) — *Nov 2021*
The Cisco Certified Network Associate Routing and Switching (CCNA: Certificate) — *Feb 2019*

TECHNICAL SKILLS

- **Data Science**: Data Modeling, Visualization, Statistical Analysis (Python, Pandas, SciPy, Matplotlib, Seaborn)
- **Machine Learning & Deep Learning**: Supervised/Unsupervised Learning, Neural Networks, Transformer Models, Natural Language Processing (NLP), Computer Vision (CV), Time-Series Forecasting
- **ML Frameworks & Tools**: PyTorch, TensorFlow, Keras, Scikit-learn, Hugging Face, ONNX, TensorRT
- **Security & Adversarial ML**: Adversarial Attacks, Adversarial Training, Model Robustness, Membership Inference Attacks, Model Hijacking, Red-Teaming AI Systems
- **Optimization & AutoML**: Evolutionary Algorithms, Reinforcement Learning, Bayesian Optimization, Neural Architecture Search (NAS), Hyperparameter Tuning, Graph NAS
- **MLOps & Cloud**: Model Deployment, CI/CD, Docker, Kubernetes, Git, AWS, GCP, Azure (familiar)
- **Embedded & Edge AI**: NVIDIA Jetson/Edge GPUs, Raspberry Pi, Google Coral TPU, Heterogeneous MPSoCs, Hardware/Software Co-Design
- **Programming & Parallel Computing**: Python, C/C++, CUDA, OpenMP, OpenACC, Java, JavaScript
- **Operating Systems & Virtualization**: Linux (RHEL, Ubuntu, Debian), VMware, VirtualBox, Docker
- **Documentation & Communication**: LaTeX, Markdown, LibreOffice/OpenOffice, Microsoft Office Suite

LANGUAGES

English: Full professional proficiency: Fluent in formal and informal contexts.
French: Native or bilingual proficiency: Fluent in formal and informal contexts.
Arabic: Native or bilingual proficiency: Fluent in formal and informal contexts.
Algerian: Native or bilingual proficiency: Fluent in spoken dialect for cultural communication.

ACTIVITIES & INTERESTS

Sports, Kickboxing, Photography, Chess, and Meditation
Part-time Freelance (Machine Learning Developer)
Volunteering (Organization of Computer Programming Workshops for Children)