

Josué Martínez-Martínez, PhD

✉ josuemartinezphd@gmail.com | 🏠 <https://martinez-hub.github.io/> | 💼 <https://www.linkedin.com/in/josuemartinezmartinez/>

Education

University of Connecticut

Storrs, Connecticut

PH.D. IN COMPUTER SCIENCE AND ENGINEERING

August 2021 – August 2025

- Dissertation focused on adversarial robustness and distribution shift in deep learning, conducted in collaboration with MIT Lincoln Laboratory.
- Resulted in multiple first-author publications at leading machine learning venues, including **NeurIPS** and **AAAI workshops**, and was supported by competitive federal and industry fellowships and research grants, including **NSF**, **General Electric**, **NASA**, and the **GEM Fellowship**.

University of Connecticut

Storrs, Connecticut

M.S. IN COMPUTER SCIENCE AND ENGINEERING

August 2021 – May 2025

Earned en route to Ph.D.

Universidad Ana G. Méndez, Gurabo Campus

Gurabo, Puerto Rico

B.S. IN COMPUTER ENGINEERING

August 2017 – July 2021

- Undergraduate research supported by **U.S. Department of Energy (DOE)** and **U.S. Department of Transportation (DOT)** fellowships, complemented by multiple research internships, including at the **National Energy Technology Laboratory (NETL)**, leading to early publications and conference presentations.

Universidad Complutense de Madrid

Madrid, Spain

UNDERGRADUATE STUDENT EXCHANGE

January 2017 – June 2017

Research Experience

Orbis Operations

Remote

AI RESEARCH ENGINEER

March 2026 – Present

- **Multimedia Agents Leadership:** Lead the development of multimedia AI agents for media analysis, spanning deepfake detection across **audio, image, and video** modalities, content **provenance** verification, and **social media post classification**, as well as speech/audio agents for **speaker identification**, transcription, emotion recognition, translation, and **audio event detection**.
- **Client Demos & Rapid Prototyping:** Partnered with multiple teams to deliver client-facing demonstrations, developing and training AI models under tight timelines, including work with **Cursor on Target (CoT)** and radar data to showcase detection and sensing capabilities.
- **Model Deployment & Infrastructure:** Deployed production AI models across **GCP (Vertex AI)** and **Cloudflare**, integrating third-party AI APIs (**Gemini**, **AssemblyAI**, **Anthropic**) and managing training and serving infrastructure with modern AI-assisted tooling.
- **Research Roadmap & Mentorship:** Contributed to the AI/ML research roadmap and mentored a **master's student** over the summer, providing technical guidance on model design, training, and evaluation.

MIT Lincoln Laboratory

Lexington, Massachusetts

RESEARCH INTERN

May 2022 – December 2025

- **Research Leadership, Grant Writing, and Community Contributions:** Contributed to research proposals for national security and intelligence community sponsors. Led the development of a workshop proposal on *Synthetic & Adversarial Forensics*, accepted at **WACV and CVPR 2026** and is under review for **NeurIPS 2026**.
- **Synthetic Media Detection (June 2025 – December 2025):** Designed and implemented deepfake detection pipelines using Joint Embedding Predictive Architecture (JEPA) representations, training lightweight classifiers (MLPs and GP-augmented MLPs) for uncertainty-aware detection. Achieved **95–99% AUC** on synthetic media benchmarks using raw embedding features, demonstrating strong separability without task-specific fine-tuning.
- **Artificial Intelligence Technology and Systems Group (June 2024 – May 2025):** Led research on underconfidence-inducing adversarial attacks for imaging classification, proposing a novel attack that reduced model confidence without inducing misclassification and outperformed state-of-the-art methods by **20% on ImageNet**. Developed a complementary defense method improving robustness to both misclassification and underconfidence attacks while using **50% fewer computational resources** than existing defenses. This work resulted in a **main-author conference paper**.
- **MIT Air Force AI Accelerator (December 2024 – April 2025):** Mentored an Air Force intern on the development of machine learning algorithms for a weapon recommendation system, providing technical guidance on model design, evaluation, and deployment considerations. Project culminated in a **white paper delivered to the MIT Air Force AI Accelerator**.
- **Integrated Missile Defense Technology Group (May 2023 – May 2024):** Conducted research within the Integrated Missile Defense Technology Group to improve robustness of machine learning models operating on **Synthetic Aperture Radar (SAR)** imagery under natural distribution shifts and adversarial perturbations. Evaluated model-based robust training strategies for conditions such as snow and rain, analyzing trade-offs between computational cost and robustness gains. Demonstrated that resource-intensive generative approaches do not necessarily outperform lightweight stochastic sampling methods. This work resulted in **two main-author conference papers**.
- **Responsible AI Toolbox Team (May 2022 – September 2022):** Developed a joint optimization framework combining data augmentation and adversarial training to improve robustness against adversarial attacks and common natural image corruptions. This work led to a **main-author conference paper**.

University of Connecticut

Storrs, Connecticut

RESEARCH ASSISTANT

August 2021 – July 2025

- **Robust Training for Biomedical Imaging (PhD Thesis, August 2022 – May 2025):** Conceived and led a multi-year research agenda on robust training methods for biomedical image classification under distribution shift and adversarial perturbations in collaboration with a MIT Lincoln Laboratory Research Scientist. Developed and evaluated novel robustness techniques across multiple imaging modalities, emphasizing generalization to out-of-distribution data. This work resulted in **four main-author conference papers**. Served as **primary author of two NASA research grant proposals** supporting this research. Awarded the **NSF Team-Terra Fellowship**, the **GEM Fellowship**, and an **NSF NAIR Co-Pilot award** providing large-scale computational resources. Recognized with **three University of Connecticut Outstanding Research Awards**.
- **Mentorship & Research Leadership (2023 – 2025):** Mentored junior graduate and undergraduate researchers within the laboratory, providing guidance on experimental design, model development, and scientific writing. Supported onboarding and project planning for new lab members during the final two years of the PhD.
- **Cyberattacks and Communication Networks for Smart Power Grids (January 2022 – May 2022):** Designed and implemented an IoT communication network in GNS3 to monitor and control a smart power grid simulated in RTDS. Developed and evaluated multiple denial-of-service (DoS) attack scenarios to identify vulnerabilities in cyber-physical grid infrastructure. This work established the technical foundation for subsequent lab research and a peer-reviewed publication, in which contributions were **acknowledged (non-author)**.

Universidad Ana G. Mendez, Gurabo Campus

Gurabo, Puerto Rico

UNDERGRADUATE RESEARCH ASSISTANT

August 2018 – July 2021

- **ML-Enabled Cyber-Physical Infrastructure for Energy Systems (NETL Collaboration, Jan 2021 – Jul 2021):** Designed and implemented the end-to-end communication and control infrastructure enabling real-time data flow from simulated energy systems to machine learning models and back to turbine-level control using the OPC UA protocol. Built the system backbone supporting model inference, decision routing, and actuation in closed-loop operation. Work was conducted in collaboration with the **National Energy Technology Laboratory (NETL)** and enabled subsequent peer-reviewed research, in which contributions were **acknowledged (non-author)**.
- **Secured IoT Scheme for Microgrids (Aug 2019 – May 2020):** Designed a secure IoT network and mobile app for microgrid monitoring and control, reducing energy waste and improving resilience to **DoS** and brute-force attacks; resulted in a **main-author conference paper** and a **main-author journal publication**.
- **Honeywell UAV Navigation Challenge (Sept 2018 – May 2019):** Led the design and development of an autonomous/manual UAV using Honeywell's Navigator N580, ensuring compliance with the NASA Systems Engineering Handbook; awarded **1st place** in a Puerto Rico-wide engineering school competition.

National Energy Technology Laboratory

SUMMER RESEARCH INTERN

Morgantown, West Virginia

June 2020 – August 2020

- **Data Analysis and Machine Learning for Pressure Gain Combustion:** Applied classical supervised learning methods (including logistic regression and related models) and neural networks to classify wave modes generated within a rotating detonation engine under pressure gain combustion. Achieved **90–98% classification accuracy** across multiple operating conditions. In parallel, independently learned core machine learning workflows and developed a data compression program to reduce storage and processing overhead for high-frequency experimental data.

University of Texas at El Paso

SUMMER RESEARCH INTERN

El Paso, Texas

May 2019 – August 2019

- **UAV-Assisted Power Plant Inspection in GPS-Denied Environments:** Developed a navigation algorithm for UAV inspection tasks in GPS-denied environments using a Kalman filter applied to sonar- or LiDAR-based sensing. Converted raw range measurements into spatial coordinates for state estimation, validated the approach through flight simulations, and conducted field flights to evaluate performance in operational settings. This work resulted in a **coauthor conference paper**.

Delaware State University

SUMMER RESEARCH INTERN

Dover, Delaware

June 2018 – August 2018

- **Magnetic Field Mapping with a Flux-Gate Sensor:** Conducted high-rate magnetic field mapping using a flux-gate sensor in an experimental physics laboratory, optimizing data acquisition and real-time 3D analysis at **3,000 signals per second**. Performed experimental setup and calibration using laboratory instrumentation including a **Helmholtz coil, oscilloscope, and LabVIEW-based acquisition systems**. Awarded **3rd place** at the OSCAR poster session.

Teaching Experience

Algorithms

University of Connecticut

TEACHING ASSISTANT

Spring 2025

- Led office hours and recitation sessions, assisted with grading, and provided student support for an undergraduate algorithms course, emphasizing algorithmic problem solving and rigorous reasoning.

Software Engineering

University of Connecticut

LABORATORY INSTRUCTOR

Spring 2022

- Served as the primary instructor for the software engineering laboratory section, delivering hands-on lab instruction, supervising programming activities, and evaluating student assignments and projects.

Publications

Martínez-Martínez J.; Holodnak J.; Brown O.; Nabavi S.; Aguiar D.; Wollaber A. Improving Vision Model Robustness against Misclassification and Uncertainty Attacks via Underconfidence Adversarial Training, **NLDL 2026**.

Martínez-Martínez J.; Brown O.; Zeno G.; Khorrami P.; Rajmonda C. From Snow to Rain: Evaluating Robustness, Calibration, and Complexity of Model-Based Robust Training, **NeurIPS LatinXAI workshop 2025**.

Martínez-Martínez J., Brown, O.; Karami M.; Nabavi S. Robust Training with Data Augmentation for Medical Imaging Classification. In Health Intelligence Workshop of the **AAAI 2025**.

Martínez-Martínez, J., Brown, O.; Bai, J.; Nabavi S. Robust training of deep learning models for mammogram classification **ISBI 2025**.

Martínez-Martínez, J.; Brown, O.; Caceres, R.; Towards Robustness to Natural Variations and Distribution Shift. Student Abstract Competition. **AAAI 2024**

Martínez-Martínez, J.; Nabavi, S.; Addressing Vulnerability in Medical Deep Learning through Robust Training. Main Conference. **IEEE CAI 2023**

Martínez-Martínez, J.; Brown, O.; RobustAugMix: Joint Optimization of Natural and Adversarial Robustness. Machine Learning Safety Workshop. **NeurIPS Workshop 2022**

Martínez-Martínez, J.; Aponte-Roa, D.; Vergara-Laurens, I.; Weaver, W.W. A Low-Cost Secure IoT Mechanism for Monitoring and Controlling Polygeneration Microgrids. **MDPI Journal article**

Martínez-Martínez J., Carvajal-Jiménez C. & Aponte-Roa D.A, "A Secured IoT Scheme for Microgrids Monitoring," 2020 10th Annual Computing and Communication Workshop and Conference **IEEE CCWC**.

Habib N., Flores-Abad A., **Martínez-Martínez J.**, Aponte-Roa D.A. & Espinoza A. July 27-31, 2020. Unmanned Autonomous Aerial Navigation in GPS-Denied Environments. **LACCEI 2020**

Awards, Fellowships, & Grants

- 2025 **Anthony W. DeSio Endowed Fellowship**, University of Connecticut
- 2024 **NSF NAIR Co-Pilot Award**, National Science Foundation
- 2024 **Hispanic Scholarship Award**, Hispanic Scholarship Fund
- 2024 **NASA Graduate Fellowship Grant**, NASA Connecticut Space Grant Consortium (CTSGC)
- 2024 **Predoctoral Fellowship (Outstanding Research Award)**, University of Connecticut
- 2023 **John Lof Leadership Academy Award**, University of Connecticut
- 2023 **NASA Graduate Fellowship Grant**, NASA Connecticut Space Grant Consortium (CTSGC)
- 2023 **General Electric Fellowship**, General Electric
- 2023 **Predoctoral Fellowship (Outstanding Research Award)**, University of Connecticut
- 2022 **GEM Fellowship**, The National GEM Consortium
- 2022 **NSF Team-TERRA Fellowship**, National Science Foundation
- 2021 **Bridge+ Program**, University of Connecticut
- 2021 **Consortium of Hybrid Resilient Energy Systems Fellowship**, U.S. Department of Energy
- 2020 **Dwight David Eisenhower Transportation Fellowship**, U.S. Department of Transportation
- 2020 **Google Latinx Student Leadership Community Summit**, Google
- 2020 **Mickey Leland Energy Summer Fellowship**, U.S. Department of Energy
- 2019 **CIESESE Fall-Spring Undergraduate Research Fellowship**, U.S. Department of Energy
- 2019 **Ing. Jose Romero Villanueva Grant**, Colegio de Ingenieros y Agrimensores de PR (CIAPR)
- 2019 **CIESESE Summer Undergraduate Research Fellowship**, U.S. Department of Energy
- 2018 **OSCAR Summer Undergraduate Research Fellowship**, NASA
- 2017 **AEELA Student Grant**, Asociacion de Empleados del ELA

Outreach & Professional Development

TECHNICAL SKILLS (SELECTED)

Programming: Python, C++, SQL

ML & AI: PyTorch, HuggingFace, scikit-learn, NumPy, Pandas, TensorFlow, Hydra-Zen, MIT LL Responsible AI Toolbox

Research Areas: Adversarial machine learning, robustness under distribution shift, synthetic media detection, generative AI

Robotics & CPS: ROS, ArduPilot, MAVLink, MAVROS, QGroundControl, JMavSim

Languages: Spanish (Native), English (Fluent)

PROFESSIONAL SERVICE, LEADERSHIP, AND OUTREACH

- 2025–2026 **CVPR Synthetic & Adversarial ForEnsics (SAFE) Workshop 2026**, Main Organizer
- 2025–2026 **CVPR SPAR in 3D Generative Vision Models Workshop**, Co-Organizer
- 2025–2026 **WACV Synthetic & Adversarial ForEnsics (SAFE) Workshop 2026**, Main Organizer
- 2024–2025 **MIT Air Force AI Accelerator**, Mentor
- 2024–2025 **MIT Lincoln Laboratory / PandaHat UPRM**, Mentor
- 2023–2024 **Society of Hispanic Professional Engineers (SHPE)**, Vice President
- 2019–2020 **Association for Computing Machinery (ACM)**, Chair