Fatemeh Dana

Worcester, MA | fdana@wpi.edu | 774 420 0854 | linkedin

Ph.D. researcher in Electrical and Computer Engineering with hands-on experience and a growing focus on artificial intelligence and machine learning. My coursework and research have given me a strong foundation in data analysis, feature engineering, dimensionality reduction, neural networks, autoencoders, and classical machine learning algorithms. I am excited to apply AI/ML methods to real-world problems and develop systems that are practical, effective, and impactful.

ML Coursework

Introduction to Data Science

- Applied data preprocessing, exploratory data analysis, and visualization techniques to understand structured datasets and prepare them for machine learning tasks.
- Worked with dimensionality reduction and data representation methods including PCA and t-SNE for feature analysis, visualization, and pattern discovery in high-dimensional data.
- Implemented machine learning algorithms such as KNN, regression, and classification models, and evaluated their performance on real datasets.
- Used Python-based data science tools including pandas, NumPy, matplotlib, and scikit-learn for analysis, modeling, and result interpretation.

Machine Learning for Engineering and Science Applications

- Trained and evaluated machine learning models using PyTorch, including experiments executed on high-performance computing (HPC) systems for large-scale model development and analysis.
- Familiar with AWS EC2 and S3, GPU/cloud computing, and scalable compute environments for machine learning and scientific workloads. Trained in AWS-based cloud computing concepts, including compute provisioning, storage services, and GPU-enabled infrastructure for large-scale data (big data) and ML applications.
- Implemented and compared machine learning models including linear regression, decision trees, random forests, and neural networks for engineering and scientific prediction tasks.
- Developed deep learning models including autoencoders and feedforward neural networks for representation learning, reconstruction, and nonlinear prediction.
- Performed model training, hyperparameter tuning, overfitting analysis, and evaluation using metrics such as MAE, RMSE, accuracy, and R^2.
- Applied feature engineering, data normalization, train/test splitting, and validation workflows to improve model robustness and generalization.

Research Publications

Chypnosis: Undervolting-based Static Side-channel Attacks. *(IEEE S&P, 2026)*

- Characterized PLL-based and delay-chain-based clock-freeze countermeasures under undervolting, exposing timing and response failures in security-critical clocking circuits.
- Co-designed an undervolting-resilient clock-freeze countermeasure using complementary registers with asynchronous preset/reset.
- Built custom RTL on FPGA platforms to implement undervolting experiments, on-chip sensors, UART validation logic, and resilient countermeasures.
- Skills and Tools: Hardware Security, Verilog/SystemVerilog, Xilinx Vivado, Python, Jupyter Notebook, ChipWhisperer, function generators.
- paper: https://arxiv.org/pdf/2504.11633

GlitchSnipe: Toward Localized Voltage Fault1 Attacks *(CHES, 2026)*

- Modeled and profiled the chip power-delivery network (PDN) using S11 and frequency-domain analysis to identify resonant conditions for localized fault injection.
- Performed end-to-end Differential Fault Analysis (DFA) on AES by targeting spatially sensitive regions, generating exploitable faulty ciphertexts for key recovery.
- Skills and Tools: Xilinx Vivado, Verilog/SystemVerilog, Jupyter Notebook, ChipWhisperer, Python, function generator, vector network analyzer (VNA), cryptographic hardware, AES, DFA.

Logical Maneuvers: Detecting and Mitigating Adversarial Hardware Faults in Space. ***(SpaceSec, 2025)***

- Designed and implemented a custom RISC-V processor in Verilog and verified it by running C/C++ code and benchmark programs on the architecture.
- Developed supporting software infrastructure, including an assembler to convert standard RISC-V assembly into a custom assembly format.
- Skills and Tools: Hardware Security, Python, C, C++, FPGA prototyping, RISC-V processor design, hardware/software co-design, AlphaNov.
- https://arxiv.org/pdf/2501.13894

Rubber Mallet: A Study of High Frequency Localized Bit Flips and Their Impact on Security. ***(DRAMSec, 2025)***

- Explored hardware-level fault effects on ML inference stacks, demonstrating how targeted memory corruption can manipulate LLM tokenization and safety behavior.
- Performed large-scale token-swap search on GPT-2, LLaMA, and T5 tokenizers.
- Demonstrated how localized bit flips can bypass LLM guardrails by changing safety instructions.
- Skills and Tools: computer architecture, memory fault analysis, Git, C/C++, Python, DDR4.
- https://arxiv.org/pdf/2505.01518

A Reliability Framework for NB-IoT Devices: Addressing Transient Faults and Silent Data Corruptions. ***(Computers and Electrical Engineering Journal, 2025)***

- Implemented embedded C/C++ code to manage packet transmission, fault injection control, and reliability experiments
- Built a host-side reliability framework in Python with supporting Bash scripts to log results and analyze packet drops and silent data corruptions across devices.
- Skills and Tools: C/C++, Python, LPWAN, Bash script.
- https://www.sciencedirect.com/science/article/pii/S0045790625003489

Work Experience

Teacher Assistant (WPI) Jan 2025 – Dec 2025

- Digital Signal Processing (DSP): Covered sampling/aliasing, DFT/FFT, convolution, FIR/IIR, z-transform, and frequency response.
- Cryptography & Security: Covered symmetric/asymmetric crypto, hashes/MACs, digital signatures, and key exchange.
- Microelectronic Circuits II: Covered analog and mixed-signal circuit analysis/design, including op-amps, feedback, Bode plots, active filters, oscillators, sample-and-hold circuits, and A/D and D/A interfacing.
- Advanced Digital System Design With FPGAs: Covered FPGA architecture, HDL-based FPGA design, Verilog modules and arithmetic, sequential logic, clocks/counters, testbenches, state machines, shift registers, simulation/debugging, I/O timing constraints, external device interfacing, embedded processors, memory, FIFOs, and XADC.

Lab Instructor (AUT) Jan 2020 – Jan 2023

- Computer Architecture: Instructed students in VHDL/Verilog and digital design to implement core computer-architecture features (pipelining, memory hierarchy, basic CPU modules). Used tools such as Vivado, Xilinx ISE, and Modelsim, and Cadence.
- Operating Systems: Guided students through processes/threads, scheduling, synchronization, memory management, and file systems.
- Microprocessors: Guided hands-on sessions with Arduino interfacing for practical hardware education

Education

Ph.D. in Electrical and Electronic Engineering, Worcester Polytechnic Institute (WPI), Sept 2024 – Present

- Research Focus: Embedded Security Engineer, Reliable System Design

M.Sc. in Computer Engineering, Amirkabir University of Technology (AUT) Sept 2019 – June 2022

- Thesis: Vulnerability Evaluation and Reliability Improvement in LPWAN Devices

B.Sc. in Computer Engineering, University of Isfahan, Sept 2015 – Sept 2019

- Thesis: Implementation of a smart parking system