# Mabon Manoj Ninan

513-850-6582 | ninanmm@mail.uc.edu | www.linked in.com/in/ninanmm | mabonmn.github.io

## EDUCATION

**University of Cincinnati, Cincinnati OH**

**BS in Computer Engineering with Minor Computer Science** (Summa Cum Laude) **Class of 2024**

- **Honors and Awards:** Undergrad. Research Fellow, UC International Scholarship **GPA: 3.953**
- **Thesis Advisor:** Dr. Boyang Wang

## PUBLICATIONS

### Published Papers

- ***"A Second Look at the Portability of Deep Learning Side-Channel Attacks over EM Traces"**, In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (**RAID 2024**)
  - **Presented** this paper at the 27th RAID Conference at Padua, **Italy** *(DOI: 10.1145/3678890.3678900)*
- ***"TinyPower: Deep-Learning Side-Channel Attacks with Tiny Neural Networks"**, In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**), 2024 (23.02% acceptance)
  - **Presented** this paper at the 2024 IEEE HOST Conference, Washington DC, **USA**
  - **BEST STUDENT PAPER AWARD** *(DOI: 10.1109/HOST55342.2024.1054538)*
- *"**Portability of Deep-Learning Side-Channel Attacks against Software Discrepancies**," In Proceedings of the 16th ACM (**WiSec'23**), May 29-June 1, 2023, Guildford, **United Kingdom** (18.5% acceptance)
  - **Presented** paper at the 16th ACM WiSec Conference at Guilford, United Kingdom *(DOI 10.1145/3558482.3590177)* www.youtube.com/watch?v=h-T1jcrd0IU&t=791s
- **"EvilELF: Evasion Attacks on Deep-Learning Malware Detection over ELF Files,"** In Proceedings of the 22nd IEEE International Conference on Machine Learning and Applications (**ICMLA**), 2023 (32% acceptance)
  - Best Paper Nominee *(DOI 10.1109/ICMLA58977.2023*

### InProgress

- ***"TinyRadio: Tiny Neural Networks for Fingerprinting Radio Frequency Signals"**
- ***"CLIPTEXT: Multimodal Agents for ML Augmented Clinical Workflows using Chest X-Rays"**
- ***"Pediatric CXR-Vision: Machine Learning Medical Image Classification on Pediatric Data"**

***** ***Projects I lead***

## POSTER PRESENTAIONS

- "**Tiny Networks For SCA",** CHEST. Annual Conference, University of Connecticut, 2024.
- "**Second Look at EM Side Channel Leakage",** Senior Thesis, University of Cincinnati, 2024.
- "**Side Channel Attacks across Different EM probe locations",** REU Conference, University of Cincinnati, 2023.
- "**Robust Cross Side-Channel Attacks",** CHEST. Annual Conference, University of Cincinnati 2023.

## RESEARCH EXPERIENCE

**Research Scientist |** Translational AI Lab @Cincinnati Children Hospital, *OH* April 2024 - Present

- Developing foundations models for CXR imaging enhancing the interpretability in pediatric clinical settings
- Researching methods to establish a proposed evaluation metric that integrates both textual and visual features, aiming to enhance the assessment of radiology reports
- Quantify uncertainty introduced by pediatric data on SOTA clinical models and working on methods better reinforce models to suit pediatric data
- Leveraging BERT models to classify and label pediatric reports into twelve common diseases, establishing ground truths for subsequent downstream tasks

**Researcher Assistant |** Data Security Lab @University of Cincinnati, *OH* July 2022 – July 2024

- Led research on deep learning side-channel attacks and radio fingerprinting
- Developed custom pruning algorithm to reduce model complexity while retaining model performance
- Designed custom kernels to deploy ML models on microcontrollers (Jetson Nano, RbPi-4 and FPGA)
- Proposed a new metric for statistical analysis of model performance to compare ML architectures
- Conceptualized new method for unsupervised training "On-the-Fly labeling" for data without labels
- Demonstrated the feasibility of domain adaptation for side-channel models by developing methods to reduce discrepancies across software, hardware, and location in the context of Electromagnetic (EM) attacks
- Explored reinforcement learning-based architecture search to develop optimized models for high-noise data
- Developed pipeline using Python to capture and process high sampling rate data from both EM and Power traces
- Supervised a team of three undergraduate students for acquisition of large-scale datasets for side channel attacks

**NSF-REU Research Assistant |** University of Cincinnati, *OH* May 2023 – July 2023

- Investigated evasion attacks on end-to-end deep-learning malware detection over ELF binaries using pytorch
- Tested modified binary files using deep-learning detectors MalConv and FireEye along with 62 real world detectors using VirusTotal

**Software Engineer |** College of Engineering and Applied Sciences (UC), *OH* May 2022 – July 2022

- Lead the development of the University's auto grading solution using GradeScope and its integration
- Created a docker based auto-grader utilizing Otter to grade Python Notebooks integrated with GradeScope

**Research Assistant |** Video Summarization Lab @University of Cincinnati, *OH* Jan 2022 – July 2022

- Processed videos using pretrained machine learning models like CLIP and GoogLe-Net to extract features for video summarization and video classification using PyTorch
- Developed a pipeline to extract frames, preprocess images and run specified computer vision models on frames, followed by generating frame probabilities utilizing python

**Research Assistant |** Spatio-Temporal Data Lab @University of Cincinnati, *OH* Nov 2021 - Jan 2022

- Utilized JULIA to preprocess data from simulations, creating of matrices and data frames for research purposes
- Identified areas for improvement in the data collection process and recommended changes to optimize quality

## TEACHING

**Supplementary Instructor Department Coordinator |** University of Cincinnati, *OH* July 2021 – Dec. 2022

- Facilitated and lead interactive group learning sessions for Chemistry and Calculus-based Physics 2
- Served as the Department Coordinator, overseeing 35 other Supplementary Instructor

## SKILLS SUMMARY

- **Programming Technologies:** Python, C++, C, Julia, JAVA, MATLAB
- **ML Frameworks:** TensorFlow, PyTorch, Scikit, Pandas, Numpy, Numba, Open-CV, cuDNN, Weights and Bias
- **Data Analysis and Visualization:** Matplotlib, Plotly, Seaborn, Tensor Board
- **Other Technologies:** Docker , AWS, Azure, GCP, GIT, Run AI
- **Medical Imaging Frameworks**: Monai, Hydra