Quan Nguyen

PhD. Student, Computer Science
University of Florida

Email: quan.nguyen1@ufl.edu
Links: Personal Website / Github

Research Interests

Trustworthy & Secure AI (TSAI), Foundation Models (FMs), Distributed ML, Medical AI.

Differential Privacy, Adversarial ML, Vision-Language Models (VLMs), Large-Language Models (LLMs), Vision Transformers, Multimodal Representation Learning, Federated Learning, Parameter-efficient Fine-tuning, Medical Deep Learning, Medical Physics.

Education

2025 - now **Ph.D.** University of Florida, PhD. Student, Computer Science.
2024 **M.Sc.** Technical University of Munich, M.Sc. Biomedical Computing.
2021 **B.Sc.** Hanoi University of Science and Technology, B.Sc. Biomedical Engineering

Experience

May 2026 - Aug 2026 **Ph.D.Research Intern** - ML and Security **Seagate Technology, U.S**.

- **Adversarial Federated Learning:** Perform fundamental research in data security and write peer-reviewed scientific papers. Designing new Adversarial Federated Learning Technologies and mitigation techniques.

2025 - now **Research Assistant** - Adaptive Learning and Optimization Lab **University of Florida, U.S**.

- **AI Security:** Develop novel privacy attacks against Foundation Models (LLMs, VLMs, Vision Transformers). Work on differentially private mechanisms to mitigate adversarial privacy risks. **[ICML '25, AISTATS '26].**

- **Decentralized Foundation Models:** Work on decentralized training/ Parameter-efficient fine-tuning of Multimodal Foundation Models in Heterogeneous Environments.

2024 - 2024 **Master's Thesis Student** - AI in Medicine Lab **TU Munich/ Siemens Healthineers, Germany**

- **Differentially Private and Fair Deep Learning:** Investigate the disparate impact of differential privacy on the fairness of AI models. Analyze subgroup disparities and identify algorithmic encoding of protected patients' characteristics through the lens of shortcut learning. Develop fairness-aware clipping and noise-addition mechanisms for DP-SGD.

2023 - 2024 **Internship** - Computer Vision and Algorithmic Team **Luma Vision GmbH, Germany**

- **Deep Learning for Ultrasound Imaging:** Build an end-to-end deep learning framework for 4D intracardiac ultrasound image segmentation. Implement a deep learning-based speckle filtering model and SVD clutter filtering to enhance image quality. Deploy on a real-world prototype. **[IEEE IUS'24]**

2022 - 2022 **Research Assistant** - Security and Artificial Intelligence Lab **VinUni, Vietnam**

- **Federated Learning on Edge Devices:** Develop a federated learning algorithm that decomposes a large model into an ensemble of lightweight sub-models, enabling clients to train them in parallel across multiple devices without sharing data via split learning. This approach achieves 4-8× reduction in client memory usage while preserving privacy and incurring no additional server overhead. **[IEEE TNSM '23]**

2021 - 2021 **Computer Vision Engineer** - AI Camera Team **Viettel High Tech, Vietnam**

- **AI on Edge Devices:** Develop face recognition algorithms on edge devices for evaluation in the **National Institute of Standards and Technology (NIST) Face Recognition Technology Evaluation Test.** Achieve #1 rank in BORDER category among Vietnamese vendors at the time of submission. Report.

Develop real-time people detection algorithms for fisheye cameras and AI-powered traffic cameras for automatic traffic violations identification. [**IEEE AVSS '21 & ICISN '21**]

Selected Publications

1. Preprint **Quan Minh Nguyen**, Min-Seon Kim, Hoang M. Ngo, Trong Nghia Hoang, Hyuk-Yoon Kwon, My T. Thai. "Leveraging Soft Prompts for Privacy Attacks in Federated Prompt Tuning".

2. Conference **[AISTATS '26]** Hoang M.N, Nhat H.X, **Quan Minh Nguyen**, Nguyen H. K. D., Incheol Shin, My T. Thai, "Q-ShiftDP: A Differentially Private Parameter-Shift Rule for Quantum Machine Learning," Twenty-Ninth Annual Conference on Artificial Intelligence and Statistics (AISTATS). A* Conference.

3. Conference **[ICML '25] Quan Minh Nguyen***, Minh N. Vu*, Truc Nguyen, My T. Thai. Theoretically Unmasking Inference Attacks Against LDP-Protected Clients in Federated Vision Models. Fourty-Second International Conference on Machine Learning (ICML). A* Conference.

4. Journal **[IEEE TNSM '23] Nguyen, Q**., Pham, H. H., Wong, K. S., Le Nguyen, P., Nguyen, T. T., & Do, M. N. (2023). FedDCT: Federated Learning of Large Convolutional Neural Networks on Resource Constrained Devices Using Divide and Collaborative Training. IEEE Transactions on Network and Service Management Q1 Journal.

5. Conference **[IEEE IUS'24]** Martina Casagrande, **Quan Nguyen**, Ivan Dudurych, Christoph Hennersperger, Stefan Wörz. Advancing 3D ICE: Challenges and Deep Learning Strategies in Atrium Segmentation. IEEE Ultrasonics, Ferroelectrics, and Frequency Control Joint Symposium. Flagship conference of IEEE UFFC Society.

6. Conference [**IEEE AVSS '21**] **Minh, Q. N**., Le Van, B., Nguyen, C., Le, A., & Nguyen, V. D. (2021, November). ARPD: Anchor-free Rotation-aware People Detection using Topview Fisheye Camera. In 2021 17th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)

7. Conference **[ICISN '21]** Nguyen, V. D., Pham, P. N., Nguyen, X. B., Tran, T. M., & **Nguyen, M. Q.** (2021, March). Incorporation of panoramic view in fall detection using omnidirectional camera. In The International Conference on Intelligent Systems & Networks.

Technical Skills

- **Programming Languages:** C, C++, Python, Gleam.
- **Libraries:** Pytorch, Tensorflow, Numpy, Pandas, Sklearn, SciPy, Opacus, JAX Privacy, OpenCV, Wandb, Flower, CuPy, Hugging Face, Matplotlib, Seaborn, ONNX, TensorRT.
- **Systems/ Tools:** Git, LaTeX, HPC, Linux, Docker, Slurm, Google Cloud.

Activities

Awards

CISE Graduate Scholarship at University of Florida (2026)
Scholarship - The 9th Vietnam Summer School of Science (2023)
Scholarship - "Modern machine learning: Foundations and applications" Program. (2023)
First prize in Vietnam AI Day 2022 - with solution: "VAIPE: Protective healthcare monitoring and supporting system for Vietnamese" (2022)
Third prize in Hanoi University of Science & Tech **Academic Research Contest** (2021)
Scholarship - Hanoi University of Science & Tech students with **top academic results** (2020)
Scholarship - FPT Center for Young Talents (25 awarded nationwide per year) (2019)
International Exchange Scholarship at Temasek Polytechnic, Singapore (2018)

Teaching

COMP 1020 - OOP & Data Structures - VinUni (S'22), CDA 3101 - Comp. Org. - UF (S'26).

Services

IEEE AVSS 2022, IEEE ACCESS (**Reviewer**), VinUni-Illinois Smart Health Center Workshop 2022 (**Workshop Organizer**) ,SOICT 2023 (**Reviewer / Program Committee**)

Language

8.5 IELTS (C2 Level), A2 German, Vietnamese (Native).

References

1. **Prof. My T. Thai**, UF Research Foundation Professor of Computer & Information Sciences & Engineering and Associate Director of Warren B. Nelms Institute, IEEE Fellow, University of Florida. mythai@cise.ufl.edu
2. Dr. Stefan Wörz, Head of Computer Vision and Algorithmics, LUMA Vision. stefan.woerz@lumavision.com
3. Asst. Prof. Huy Hieu Pham, Associate Director, VinUni – Illinois Smart Health Center. hieu.ph@vinuni.edu.vn