# PHUNG LAI

## EDUCATION

**New Jersey Institute of Technology** (NJIT), Newark, NJ — *Graduation: 05/2023*
PhD candidate in Information Technology — GPA: 4.00/4.00
Research topics: Trustworthy Machine Learning/AI through the Lens of Privacy and Security

**Oregon State University** (OSU), Corvallis, OR — *Graduation: 06/2018*
Master of Science in Computer Science — GPA: 3.43/4.00
Thesis: "Multiple instance learning for histopathological image classification"

**Da Nang University of Science and Technology** (DUT), Vietnam — *Graduation: 08/2013*
Bachelor of Science in Electronics and Telecommunications — GPA: 8.52/10.0 (Rank 2/230)
Thesis: "Falling detection based on adaptive background mixture model and hidden markov model"

## PUBLICATIONS

**(*: Co-first author)**

- Truc Nguyen*, **Phung Lai***, Hai Phan, My Thai. XRAND: Differentially Private Defense against Explanation-Guided Attacks. In *Proceedings of AAAI Conference on Artificial Intelligence,* 2023 **(AAAI 2023 Distinguished Paper Award (12 selected/8,777) - Oral presentation)**
- Truc Nguyen, **Phung Lai**, Khang Tran, Hai Phan, and My Thai. Active Membership Inference Attack under Local Differential Privacy in Federated Learning. In *Proceedings of Artificial Intelligence and Statistics Conference (**AISTATS**)*, 2023
- **Phung Lai**, Hai Phan, Tong Sun, Rajiv Jain, Franck Dernoncourt, Jiuxiang Gu, Nikolaos Barmpalios. User and Entity Differential Privacy Preservation in Natural Language Models. In *Proceedings of IEEE International Conf. on Big Data (**IEEE BigData**)*, pp. 1465 – 1474, 2022 **(Oral presentation)**
- Xiaopeng Jiang, Han Hu, Thinh On, **Phung Lai**, Vijaya Mayyuri, An Chen, Devu Shila, Adriaan Larmuseau, Ruoming Jin, Cristian Borcea, Hai Phan. FLSys: Toward an Open Ecosystem for Federated Learning Mobile Apps. In *IEEE Trans. on Mobile Computing (**IEEE TMC**)*, 2022
- Khang Tran, **Phung Lai**, Hai Phan, Issa Khalil, Yao Ma, Abdallah Khreishah, My Thai, Xintao Wu. DPGNN: Differential Privacy Preservation in Graph Neural Networks. In *Proceedings of **IEEE BigData***, pp. 1582 – 1587, 2022 **(Oral presentation)**
- **Phung Lai**, Hai Phan, Han Hu, Ruoming Jin, My Thai, An Chen. Lifelong DP: Consistently Bounded Differential Privacy in Lifelong Learning. In *The Conference on Lifelong Learning Agents (**CoLLAs**), In Proceedings of Machine Learning Research (**JMLR**)*, pp. 778 – 797, 2022
- Pelin Ayranci*, **Phung Lai***, Hai Phan, David Newman, Alexander Kolinowski, Deijing Dou. OnML: an ontology-based approach for interpretable machine learning. In *Journal of Combinatorial Optimization (**JOCO - Springer**)*, vol. 44(1), pp. 770 – 793, 2022
- Pradnya Desai*, **Phung Lai***, Hai Phan, My Thai. Continual Learning with Differential Privacy. In *I.C. on Neural Information Processing (**ICONIP**)*, pp. 334 – 343, 2021 **(Oral presentation)**
- Trung Vu*, **Phung Lai***, Raviv Raich, Anh Pham, Xiaoli Z Fern, UK Arvind Rao. A Novel Attribute-based Symmetric Multiple Instance Learning for Histopathological Image Analysis. In *IEEE Transactions on Medical Imaging (**IEEE T-MI**)*, vol. 39, no. 10, pp. 3125 – 3136, 2020
- **Phung Lai**, Hai Phan, David Newman, Han Hu, Anuja, Dejing Dou. Ontology-based interpretable machine learning with learnable anchors. In *International Joint Conference on Neural Networks (**IJCNN**)*, pp. 1 – 10, 2020 **(Oral presentation)**

- **Phung Lai**, Hai Phan, David Newman, Han Hu, Anuja Badeti, Dejing Dou. Ontology-based interpretable machine learning with learnable anchors. In *Knowledge Representation and Reasoning Meets Machine Learning (**KR2ML, NeurIPS workshop**)*, pp. 1 – 16, 2019 **(Oral presentation)**
- **Phung Lai**, Raviv Raich, Molly Megraw. ConvMD: Convolutive matrix decomposition for classification of matrix data. In *Proceedings of IEEE Statistical Signal Processing workshop (**IEEE SSP**),* pp. 368 – 372, 2018 **(Oral presentation)**
- Tam Nguyen, Raviv Raich, **Phung Lai**. Jeffreys prior regularization for logistic regression. In ***IEEE SSP** workshop,* pp. 1 – 5, 2016 **(Oral presentation)**

**FORTHCOMING**

- **Phung Lai**, Khang Tran, Hai Phan, Li Xiong, My Thai, Tong Sun, Franck Dernoncourt, Jiuxiang Gu, Nikolaos Barmpalios, and Rajiv Jain. Scalable Dimensionality in Local Differential Privacy for Federated Learning. In *ACM Conference on Computer and Communications Security*, 2023 **(Tentative Submission)**

## PATENTS

- **Phung Lai**, Tong Sun, Rajiv Jain, Franck Dernoncourt, Jiuxiang Gu, and Nikolaos Barmpalios. Privacy-Aware Language Models Training. Filing Non-provisional US Patent in 21/02/2023
- **Phung Lai**, Tong Sun, Rajiv Jain, Franck Dernoncourt, Jiuxiang Gu, and Nikolaos Barmpalios. Privacy-Aware Language Models Training. Provisional Adobe Patent, 2022
- **Phung Lai**, Tong Sun, Rajiv Jain, Franck Dernoncourt, Jiuxiang Gu & Nikolaos Barmpalios. Preserving User-Entity Differential Privacy in Natural Language Modeling. Filed Non-provisional US Patent, 2021 (To be published in 2023)
- **Phung Lai**, Tong Sun, Rajiv Jain, Franck Dernoncourt, Jiuxiang Gu & Nikolaos Barmpalios. User-Entity Differential Privacy in Natural Language Modeling. Provisional Adobe Patent, 2021

## RESEARCH EXPERIENCE

**NJIT – Department of Informatics**, Newark, NJ *09/2018 – 05/2023*

***Research Assistant***

- Cooperate with Qualcomm to create personalized, quantized, and privacy-preserving federated learning mechanisms for mobile devices
- Cooperate with NSF, UOregon, and Adobe to prove theories, implement, and conduct experiments for Trustworthiness in Machine Learning and Deep Learning using Python

**Qualcomm Inc.**, San Diego, CA *02/2020 – 05/2023*

- Collaborate in Project: Detecting Human Behaviors from Smartphones using Federated Machine Learning in the Wild
- Build real-world federated machine learning on mobile devices with novel privacy-preserving mechanisms and diverse deep learning models
- Develop adaptive quantization on different model architectures for federated learning

**Adobe Systems – Document Intelligence Labs**, San Jose, CA *01/2020 – 01/2021*

***Machine Learning Research Intern***

- Explored the research frontiers in applying state of art deep learning and AI methods in Document Understanding and Intelligent Document Agent
- Investigated the feasibility of applying scientific principles and concepts to inventions/products
- Built rapid research experiments and proof-of-concepts and participate in patent applications
- Led to a strong and long-term collaboration *2022 – 05/2023*

**Wells Fargo**, San Francisco, CA *09/2018 – 08/2021*

- Collaborated to create OnML: an ontology-based approache for interpretable machine learning
- Financed by Wells Fargo to create a drug abuse ontology and a financial ontology using Protégé

**OSU – Electrical Engineering and Computer Science**, Corvallis, OR *09/2015 – 06/2018*

***Research Assistant***

- Collaborated with NSF and University of Texas to generate a Symmetric Multiple instance learning framework for histopathological image analysis using Matlab for reducing manual annotation
- Cooperated with NSF and Dept. of Botany & Plant Pathology to develop a Convolutive-based matrix decomposition framework and conduct experiments in plant transcripts using Matlab

**NTU – Electrical and Electronic Engineering**, Singapore *06/2013 – 01/2014*

***Research Assistant***

- Simulated and conducted experiments about the effects of thermal, mechanical, and material changes on wafer bonding in 3D IC using Comsol simulation

**DUT – Department of Electronics and Telecommunications**, Vietnam *09/2010 – 08/2015*

***Research Assistant***

- Developed machine learning techniques, i.e., Hidden Markov and Gaussian mixture model, for a surveillance system using Matlab to detect falling actions and then make alarms for the elderly
- Designed digital filters using Matlab and analog filters in a Wireless ECK monitor system

## TEACHING EXPERIENCE

**NJIT – Department of Informatics**, Newark, NJ *09/2018 – 05/2023*

***Instructor***

- IS 665 – Data Analytics for Information Systems: Taught, conducted labs, graded exams

***Teaching Assistant***

- IS 663 – System Analysis and Design: Conducted review sections, graded homework and exams

**OSU – Electrical Engineering and Computer Science**, Corvallis, OR *09/2015 – 06/2018*

***Teaching Assistant***

- ECE 353 – Intro to Probability and Random Signals, CS 225 – Discrete structures in CS, CS 325 – Analysis of Algorithm, and CS 372 – Intro to Computer Networks: Conducted labs and graded

**DUT – Department of Electronics and Telecommunications**, Vietnam *09/2010 – 08/2015*

***Instructor***

- ECE 446 – Machine Learning: Taught, conducted labs, graded homework and exams

***Teaching Assistant***

- ECE 4730 – Intro to Artificial Intelligence: Guided, conducted labs, graded homework and exams

## STUDENT MENTORSHIP EXPERIENCE

**NJIT – Department of Informatics**, Newark, NJ *09/2018 – 05/2023*

- Mentored students doing research on Interpretable ML and Privacy-preserving topics: *Ph.D. students:* Khang Tran, Thinh On, and Pelin Ayranci; *Master student*: Huong Ngo; *Undergraduate students:* Pradnya Desai, Simran Kaur, Vaisnavi Nemala, Hang Nguyen, and Anuja Badeti
- Resulted in six publications: IEEE BigData'22, IEEE TMC'22, JOCO-Springer'22, ICONIP'21 (Rank A, CORE2020), IJCNN'20 (Rank A, CORE2020), KR2ML'19 (a NeurIPS workshop)
- An undergraduate student I supervised published a paper "Continual Learning with Differential Privacy" (ICONIP'21) that opens up a new research direction by discovering unknown privacy risks in continual ML and with an initial solution. Based on that, she won the following awards:
  - Pradnya Desai, Finalist for the NCWIT Collegiate Award 2022
  - Pradnya Desai, Presidential Leadership Awards 2022
  - Pradnya Desai, Dana Knox Student Research Showcase Silver Medal 2022

**OSU – Electrical Engineering and Computer Science**, Corvallis, OR *09/2015 – 06/2018*

- Awarded by Organization of Oregon & SW Washington universities in mentoring three high school students to learn and implement machine learning models using Matlab *08/2017*

**Vietnam Education Foundation 2.0 (VEF 2.0)**, Hanoi, Vietnam *09/2020 – 05/2023*

- Support Vietnamese students to improve knowledge and skills for applying leading US universities
- Successful applications: *Toan Tran* (Emory University (Ph.D., Fall 2023) and University of Tennessee (Master, Fall 2021)); *An La* (University of Massachusetts, Amherst (Master, Fall 2021)); *Cong Tran* (Auckland University of Technology, New Zealand (Master, Spring 2023))

## AWARDS and HONORS

- AAAI 2023 Distinguished Paper Award, Washington DC, Japan *02/2023*
- Student Travel Award to attend IEEE BigData 2022, Japan *12/2022*
- NSF travel award to attend NSF CBL Semiannual Meeting in Gainesville, FL *10/2019*
- Recipient of a six-month research scholarship at School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore *06/2013 – 01/2014*
- 3rd prize (Nation-level round) and 2nd prize (Region-level round) at Vietnam Universities & Texas Instruments Microcontroller Design Contest 2012 *12/2012*
- Sunflower Mission scholarship from Texas Instruments company, USA *12/2012*
- Recipient of scholarships from Takemoto Denki and Ikeshita Japan companies for Outstanding DUT students *12/2010*

## PROFESSIONAL SERVICES

- **Conference and Journal Reviewer:** AAAI 2022, ICLR 2022, IEEE JDSA 2022, IEEE JOCO 2022, WWW 2022, TDSC 2022, BigData 2021, ICML 2021, NeurIPS 2021, SIGIR 2021, ICMLA 2020, ICKM 2019, JBHI 2018, MLSP 2017.
- Lead organizer and Host of The 2023 Annual Conference Vietnamese Scientists and Engineers Network in the U.S, Jersey City, NJ *08/2023*
- Student supporter at IEEE BigData, Osaka, Japan *12/2022*
- Organizer of The 2022 Annual Conference Vietnamese Scientists and Engineers Network in the U.S, San Diego, CA *08/2022*
- Publication Chair of Trustworthy Federated Machine Learning Workshop at IEEE International Conference on Data Mining 2023 (ICDM 2023) *12/2022*
- Invited talks on "Trustworthiness in Machine Learning from Privacy Perspectives" at 1) Kent State Univeristy, OH and at 2) Qatar Computing Research Institute, Qatar *11-12/2022*