

Phat Tuan Tran-Truong (Leo)

· LECTURER & RESEARCHER @ HCMUT, VNU-HCM | BENG. (HONS) & MENG. IN COMPUTER SCIENCE ·

Address: 268 Ly Thuong Kiet Street, Dien Hong Ward, Ho Chi Minh City, Vietnam
☎ (+84) 368865745 | ✉ phatddd@hcmut.edu.vn | 🌐 tuanphat | 🎓 Phat T. Tran-Truong

Education

Ho Chi Minh City University of Technology, Vietnam National University

Ho Chi Minh city, Vietnam

MENG. (BY RESEARCH), COMPUTER SCIENCE

2021 - 2023

- **CGPA - 9.05/10** (4.0/4.0 - Excellence)
- **Thesis** - Privacy-Preserving Deep Learning Methods - **Grade 9.34/10**
- **Supervisor** - Assoc. Prof. Hong Trang Le and Assoc. Prof. Tran Khanh Dang

Ho Chi Minh City University of Technology, Vietnam National University

Ho Chi Minh city, Vietnam

BENG. (HONORS), COMPUTER SCIENCE

2016 - 2020

- **CGPA - 8.0/10** (Very good)
- **Thesis** - Privacy-Preserving Open Data Publishing Based-on Data Anonymization - **Grade 9.85/10**
- **Project** - Chief member with the B.Eng. thesis associated with the project [Anonymization Infrastructure for Open Data](#) (funded by HCMC Department of Science and Technology - Lead by [Dr. Tuan Anh Truong](#)).

Professional Experience

Ho Chi Minh City University of Technology, Vietnam National University

Ho Chi Minh city, Vietnam

TEACHING/ RESEARCH ASSISTANT (PART-TIME); THEN FULL-TIME LECTURER/ RESEARCHER (FULL-TIME SINCE JUN. 2024)

2019 - onward

- **Full-time Lecturer/ Researcher** | [Department of Software Engineering, Faculty of Computer Science & Engineering](#)

- Projects

- * **[Ongoing]** Low-resource multilingual LLMs - collaborative research agreement between School of Computing @National University of Singapore (NUS), Singapore and CSE@HCMUT, Vietnam.
(**Type: Research, Role:** Researcher, work with [A/Prof. Tho Quan \(CSE@HCMUT\)](#) and [NLP Group@ NUS](#)).
- * **[Ongoing]** Leverage Large Language Models for program generation and verification.
(**Type: Research, Role:** Lead researcher, work with [Dr. Xuan-Bach Le \(CSE@HCMUT\)](#), funded by VNU-HCM Project Type C).
- * **[Ongoing]** Research on Application of Large Language Models in Detecting Malicious Packages in the NPM Ecosystem.
(**Type: Research, Role:** Lead researcher, work with [Dr. Duc-Ly Vu](#), initial results are submitted to [ESORICS](#)).
- * **[Finished]** Improve open-source LLMs' performance on Educational Multiple-Choice Questions Answering.
(**Type: Research, Role:** Lead researcher, work with [A/Prof. Tho Quan](#), funded by USAID PHER, published in the [Elsevier's CAEAI](#)).
- * **[Finished]** Hung Vuong Hospital's Intelligent maternity ward: AI applications in obstetric diagnosis and treatment.
(**Type: Application, Role:** Tech lead/PM - Faculty-Industry project, work with [Hung Vuong Hospital, Sao Bac Dau Group](#)).
- * **[Finished]** Machine learning for Individual Privacy Preference Prediction in Medical, Health & Fitness Android Apps.
(**Type: Research, Role:** Lead researcher, results are published in the [Springer's IJIS article](#)).
- * **[Finished]** Analysis of NIST standards alignment and industry implementation of digital payment systems.
(**Type: Research, Role:** Lead researcher, work with [Dr. Son Ha \(RMIT university\)](#), results are published in the [Elsevier's JSA article](#)).
- * **[Finished]** Develop a curriculum to foster LLM proficiency for high school students and deploy at the faculty's summer school.
(**Type: Application, Role:** Chief member/Mentor/Organizer, results are published in the [AIED paper](#)).

- Teaching courses:

Course	Teaching load & Frequency	Roles
Software Engineering	<ul style="list-style-type: none">* 15 lectures for >240 students per semester* Deliver almost every semesters	Co-lecturer
1. Advanced Programming Paradigms 2. Principles of Programming Languages	<ul style="list-style-type: none">* 15 lectures for >240 students per semester* Deliver almost every bi-semesters* Take charge of APP more often than PPL.	Co-lecturer
Software Architecture & Design	<ul style="list-style-type: none">* 15 lectures for ~ 120 students per semester* Elective course - deliver almost every semesters for SE specializations.	Coordinator
1. Software Security 2. Software Maintenance and Evolution 3. Advanced Software Engineering	<ul style="list-style-type: none">* 15 lectures for ~60 students* Elective course - deliver when assigned (If enough students register).	Co-lecturer
1. Introduction to AI 2. Machine Learning 3. Introduction to Computing	<ul style="list-style-type: none">* 15 lectures for >240 students per semester* Deliver almost every semesters.	Co-lecturer
SE/AI projects	<ul style="list-style-type: none">* Include Programming integration projects; Multidisciplinary projects; Specialized projects & Capstone projects.* Mentor/Instruct ~20 groups/semester; Supervise >10 Bachelor's theses	Instructor/ Mentor/ Supervisor

- * **Other courses** (have experiences but not often): Discrete Mathematics, Probability and Statistics, Mathematical Modeling, Operating System, Next-gen Software Engineering (New elective course), Application of IT Skills (for students from other backgrounds).

• **Teaching/ Research Assistant (Part-time)**

– **Projects**

- HCMUT Survey: a survey system that stores users’ responses on blockchain.
(**Type: Application, Role:** Member, student research project (Jul. 2019 - Jan. 2020), deployed faculty-wide to collect feedback on thesis evaluations for the 2021 and 2022 academic years.)
- CVSS: a blockchainized certificate verifying support system
(**Type: Application, Role:** Member, student research project (Sep. 2018 - Jul. 2019)).
- Open Data Anonymization: implemented a hands-on module for anonymizing open dataset before publishing in an open data portal. The module included many state-of-the-art techniques such as: *k*-anonymity, *l*-diversity, *t*-closeness, *δ*-presence, etc.
(**Type: Research/ Application, Role:** Chief member, [Ho Chi Minh City research project](#) - funded by HCMC Department of Science and Technology (2018 - 2021) - lead by [Dr. Tuan Anh Truong](#), resulted in the BEng. thesis).

- **Assistant courses:** Introduction to Computing, Operating System, Computer Network, and Advanced Programming Project.

Ho Chi Minh City University of Industry & Trade

Ho Chi Minh city, Vietnam

ASSOCIATE LECTURER, SOFTWARE ENGINEER LEAD & DEPUTY HEAD OF [INSTITUTE OF DIGITAL TRANSFORMATION](#)

May 2022 - Jun. 2024

• **Associate Lecturer**

- **Teaching courses:** Database System, NoSQL Database, Information Systems Security, Discrete Mathematics, Application of IT Skills, Applied Cryptography, Biometrics, and Java Technology.
- Homeroom lecturer of a class with 60 students.
- Supervise more than 20 bachelor’s theses & capstone projects in software development and AI topics.

• **Secondment: Software Engineer Lead & Deputy Head**

- Organize a software development team; design, develop and allocate tasks.
- Train more than 10 new engineers and interns.
- Administrate cloud servers of the institute: VPS, AWS server and Naver AI server.

• **Projects**

- Design a privacy-preserving deep learning method based on differential privacy and distributed learning (Oct. 2022 - Mar. 2024).
- HUIT-Elab: E-Laboratory Management System of Ho Chi Minh city of Industry & Trade (Jul. 2022 - Jan. 2024).
- HUFU-STPMS: Students’ Training Points Management System of Ho Chi Minh city of Industry & Trade (Jul. 2022 - Jan. 2024).

Sungkyunkwan University & Hippo T&C Company

Suwon City, South Korea

RESEARCH INTERN

Jul. 2023 - Jan. 2024

- Conduct research & assist in Healthcare and Digital Therapeutics projects using the IoT devices & AI.
- Projects between Internet Management Technology Laboratory, College of Computing and Informatics, SKKU and Hippo T&C company.

• **Projects**

- Build a mobile application for collecting data from IoT devices.
- Build deep learning models for speech emotion recognition.

- **Tech stack:** Python, TensorFlow, AWS, Linux server.

Viettel High Technology Industries Corporation, Viettel Group

Hanoi, Vietnam

SOFTWARE ENGINEER (SPECIALIZED IN BIG DATA PROCESSING & ANALYSIS)

Sep. 2020 - Mar. 2022

• **Projects**

- Weather information management system: Develop & deploy some backend microservices; Design & build a full-text search function using Elasticsearch.
- Open-source intelligence system (OSINT): Build & deploy a Kafka cluster service for streaming data and synchronize data between data sources; Deploy & orchestrate backend microservices using Prometheus, Docker and K8s.
- Vessel management & weather-hydrography management: Design & build CI/CD pipelines for the frontend of two projects; Build a library for managing the company’s common UIs using Storybook.

- **Tech stack:** Java, Java Spring, Python, Javascript/Typescript, React/Redux, MongoDB, Elasticsearch, Docker, K8s.

Achievements, Grants & Honors

2025	National “Creative Youth” Award for Vietnamese people under 35 , Central Committee of the Vietnamese Youth Union	<i>Vietnam</i>
2023	Excellent Master Student Award , Awarded merit certificate granted by the President of HCMUT for outstanding postgraduates in the master course	<i>Ho Chi Minh city</i>
2020	Consolation prize , Top 15 finalist in Bach Khoa Innovation contest	<i>Ho Chi Minh city</i>
2018-2019	Excellent Comprehensive Student , Awarded merit certificate granted by the President of HCMUT for excellent academic achievements	<i>Ho Chi Minh city</i>
2018 – 2019	HCMUT Student of 5 merits , Awarded merit certificate granted by the HCMUT Student Association for outstanding students in term of 5 criteria: ethics - learning - physical strength - volunteer - integration	<i>Ho Chi Minh city</i>
2017 - 2020	HCMUT Honors Program Scholarship , Awarded to top Honors students in my university	<i>Ho Chi Minh city</i>
2016	Direct University Admission , Get direct admission to two prestigious engineering and science universities of Vietnam National University (HCMUT and HCMUS, VNU-HCM)	<i>Ho Chi Minh city</i>
2015-2016	Silver Medal , High-school Math Olympic competition & summer camp	<i>Southern Vietnam</i>
2015-2016	First prize , High-school Math competition for Vinh Long city & Vinh Long province 2015, 2016	<i>Vinh Long, Vietnam</i>










Research interests

- **AI:** privacy-preserving AI, trustworthy AI, federated/ distributed learning, multi-agent system, self-supervised learning, multimodal learning, AI safety.
- **Security & Privacy:** decentralized systems (Blockchain-based), privacy-preserving techniques, privacy policy, anomaly detection, adversarial attacks, software supply chain attacks, cryptography.




Publications









[Google Scholar Link](#) 

International Journals








- 2026 [JNCA'26]  **P. T. Tran-Truong***, Trung Mai* et al., "POP2TIC: Performance Optimization for Privacy-Preserving Fog Computing using TEE and Intelligent Caching", *Journal of Network and Computer Applications*, [Accepted], 2026. (SCIE, SCImago Q1, IF: 8.0)
- 2026 [CAEAI'26]  P. Q. Dang*, **P. T. Tran-Truong*** et al., "Enhancing Large Language Model Performance for Automatic Zero-Shot Multiple-Choice Question Answering via Single-Token Logit Prompting," *Computers & Education: Artificial Intelligence*, vol. 10, no. 100578, pp. 1-18, 2026. (ESCI, SCImago Q1, Top 1 Journal in Education)
- 2026 [COMNET'26]  **P. T. Tran-Truong***, Trung Mai* et al., "PrivacyGuard: A Hierarchical Privacy-Preserving Framework for IoT-Fog-Cloud Architectures", *Computer Networks*, vol. 278, no. 112076, pp. 1-17, 2026. (SCIE, SCImago Q1, IF: 4.6)
- 2026 [EAAI'26]  Anh Q. Nguyen*, **P. T. Tran-Truong*** et al., "LiteFormer: A Lightweight Encoder-Only Transformer for Efficient Financial Time Series Forecasting Across Global Stock Indices," *Engineering Applications of Artificial Intelligence*, vol. 167, Part 2, 113681, pp. 1-33, 2026. (SCIE, SCImago Q1, IF: 8.0)
- 2025 [PMC'25]  **Phat T. Tran-Truong***, Trung D. Mai*, Ha X. Son et al., "SecureWearTrade: A Comprehensive Blockchain-Enabled IoT Framework for Secure Personal Data Trading from Wearable Devices," *Pervasive and Mobile Computing*, vol. 115, no. 102130, pp. 1-24, Jan. 2026. (SCIE, SCImago Q1, IF: 3.5)
- 2025 [HCCOM'25]  **Phat T. Tran-Truong** et al., "TACKLE: Time-based Access Control and Key delegation for Letter of credit Ecosystems", *High-Confidence Computing*, [Accepted], vol. , no. , pp. 1-24, October 2025. (SCIE, SCImago Q1, IF: 3.0)
- 2025 [IJIS'25]  Phien N. Nguyen, **P. T. Tran-Truong**, H. X. Son et al., "CI2P-MedHFDroid: A Context-Aware Individual Privacy Preferences Model for Medical, Health & Fitness Android Apps", *International Journal of Information Security*, vol. 26, no. 176, pp. 1-31, July 2025. (SCIE, SCImago Q2, IF: 3.2)
- 2025 [JSA'25]  **Phat T. Tran-Truong** et al., "A Systematic Review of Multi-Factor Authentication in Digital Payment Systems: NIST Standards Alignment and Industry Implementation Analysis," *Journal of Systems Architecture*, vol. 162, no. 103402, pp. 1-38, May 2025. (SCIE, SCImago Q1, IF: 4.1)
- 2024 [SNCS'24]  T. K. Dang* and **Phat T. Tran-Truong***, "A Pragmatic Privacy-Preserving Deep Learning Framework Satisfying Differential Privacy," *SN Computer Science*, vol. 5, no. 130, pp. 1-25, Jan. 2024. (Scopus, SCImago Q2, IF: 3.1)

International Conferences

- 2026 [ICSA'26]  Khang Vo, Ha Vo, Nhut Tran, **Phat T. Tran-Truong** and Son Ha, "Exploring the Reasoning Depth of Small Language Models in Software Architecture: A Multidimensional Evaluation Framework Towards Software Engineering 2.0", *2026 IEEE 23rd International Conference on Software Architecture (ICSA)*, (Amsterdam, Netherlands), [Accepted], 2026. (CORE Rank A)
- 2026 [LM4UC@AAAI]  Ty Nguyen, **P. T. Tran-Truong**, Long Nguyen, Sang Nguyen, Tho Quan, "Sentence-Aware Baharic-Vietnamese Lexical Mapping with Contrastive Contextual Representations", *Second Workshop on Language Models for Underserved Communities (LM4UC)*, AAAI, [Accepted], Singapore, 2026, pp. 1-10. (Workshop at CORE Rank A*)
- 2025 [ICSOC'25]  H. X. Son, Anh Q. Nguyen, **P. T. Tran-Truong** et al., "SLIE: A Secure and Lightweight Cryptosystem for Data Sharing in IoT Healthcare Services", *International Conference on Service Oriented Computing (ICSOC)*, (Shenzhen, China), [Accepted], 2025. (CORE Rank A)

- 2025 [AIED'25]  **Phat Tran**, Dang Le, Sang Truong, Sanmi Koyejo, Cuong Le & Tho Quan, "Riding on The Back of A Whale: A Hackathon Framework for Introducing High School Students to Large Language Models", *International Conference on Artificial Intelligence in Education (AIED)*, (Palermo, Italy), 2025, pp. 201-209. **(CORE Rank A)**
- 2025 [IJCCI'25]  Tam Nguyen, **P. T. Tran-Truong**, Anh Tuan Truong, "GADA: An Adaptive Genetic Algorithm-Based Framework for Dynamic University Course Timetabling", in *17th International Joint Conference on Computational Intelligence (IJCCI)*, (Marbella, Spain), Springer, 2025, 1-20. **(CORE Rank C)**
- 2024 [ICSOCW'24]  **P. T. Tran-Truong** et al., "Decoding the privacy policy implications of personal data processing: A framework for GDPR Compliance in Business and Social apps", in *22nd International Conference on Service Oriented Computing Workshops (ICSOC)*, (Tunis, Tunisia), LNCS, Springer, 2024, pp. 1-12. **(Workshop at CORE Rank A)**
- 2024 [PDCAT'24]  **P. T. Tran-Truong**, Trung P. H. T., and Bang L. K., "Decentralizing Energy Trading for Electric Vehicles using Blockchain Technology", in *25th Intl' Conference on Parallel and Distributed Computing, Applications and Technologies*, (Hong Kong, China), LNCS, Springer, 2024, pp. 1-12. **(CORE Rank C)**
- 2024 [IMCOM'24]  H. H. X. Nguyen, T. K. Dang and **P. T. Tran-Truong**, "Money Laundering Detection using A Transaction-based Graph Learning Approach", in *2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, (Kuala Lumpur, Malaysia), IEEE, 2024, pp. 1-8.
- 2023 [FDSE'23]  T. K. Dang, **P. T. Tran-Truong** and N. T. H. Trang, "An Enhanced Incentive Mechanism for Crowdsourced Federated Learning Based on Contract Theory and Shapley Value", in *Future Data and Security Engineering (FDSE): 10th Intl' Conference*, (Da Nang, Vietnam), 2023, pp. 1–16.
- 2022 [FDSE'22]  **P. T. Tran-Truong** and T. K. Dang, "pPATE: A Pragmatic Private Aggregation of Teacher Ensembles Framework by SVT-Based Differential Privacy, Paillier Cryptosystem and Human-in-the-loop", in *Future Data and Security Engineering: 9th Intl' Conference*, (HCMC, Vietnam), Springer, 2022, pp. 332–346.
- 2020 [ACOMP'20]  T. K. Dang, **P. T. T. Truong**, and P. T. Tran, "Data poisoning attack on deep neural network and some defense methods," in *2020 International Conference on Advanced Computing and Applications (ACOMP)*, (Quy Nhon City, Vietnam), IEEE, 2020, pp. 15–22.

Manuscripts/ Preprints

- 2026 [ESORICS]  Dang-Khoa Nguyen, Gia-Thang Ho, Quang-Minh Pham, Tuyet A. Dang- Thi, Minh-Khanh Vu, Thanh-Cong Nguyen, **Phat T. Tran-Truong**, and Duc-Ly Vu, "Taint-Based Code Slicing for LLMs-based Malicious NPM Package Detection", *[Under submission - 31st European Symposium on Research in Computer Security (ESORICS)]*, 2026.
- 2026 Nguyen Quoc Anh, **Phat T. Tran-Truong** et al., "Candlestick Is All You Need for Temporal Recognition in Finance", , 2026.
- 2026 [PAKDD]  Duy D. Nguyen, **P. T. Tran-Truong**, "SegMaFormer: A Hybrid State-Space and Transformer Model for Efficient Segmentation", *arXiv preprint arXiv:2603.22002*, 2026.
- 2026 [InfoSci]  **Phat T. Tran-Truong** et al., "PA-EWD: Privacy-Preserving Federated Analytics on Encrypted Wearable Data", *[Under submission - Elsevier's Information Sciences]*, 2026.
- 2025 [MONET] **P. T. Tran-Truong** et al., "SPM-HealSer: Hierarchical Identity-Based Encryption for Scalable and Privacy-Preserving Mobile Health Services", *[Under submission - Mobile Networks and Applications]*, 2026.
- 2025 [IPM]  **P. T. Tran-Truong***, Kiet Le* et al., "Generative AI for User Experience: A Holistic Taxonomy of Tools across the Design Thinking Framework", *[Under submission - Information Processing & Management]*, 2026.
- 2025 [JPDC]  **P. T. Tran-Truong***, Vinh Nguyen* et al., "SHIELD-Traffic: A Comprehensive Fog-Assisted Architecture for Secure and Privacy-Preserving Traffic Data Sharing in Smart Cities", *[Under review - Journal of Parallel and Distributed Computing]*, 2025.
- 2025 [Cluster]  Ha X. Son*, **P. T. Tran-Truong*** et al., "CertiMed: Identity-Aware Access Framework for Electronic Health Records", *[Under review - Springer's Cluster Computing]*, 2025.
- 2024 [TOPS] **P. T. Tran-Truong***, Trung Mai* et al., "Bpids: A Blockchain-Based Personal Iot Data Storage Framework with Time-Bounded Hierarchical Access Control", *[Under review - ACM Trans. on Pri. & Sec.]*, 2025.
- 2024 [COSE]  Phien N. Nguyen, **P. T. Tran-Truong** et al., "Acb: Authority Control Bluetooth Devices in Smarthome Environment System", *[1st revision under review - Computers & Security]*, 2024.

Professional services

- **Reviewer/ PC member:**

Journals: Information sciences, Information Processing & Management; Computer Networks; Blockchain: Research and Applications (Elsevier); SN Computer Science, AI & Ethics, Artificial Intelligence Review, Cluster Computing, Discover Computing; journal of supercomputing; Journal of big data; Scientific reports; Journal of King Saud University (Springer Nature);

Conferences: FDSE'22, FDSE'23, ACOMP A'21, ACOMP A'22, ACOMP A'23, MIWAI'25, MIWAI'26.

Professional Skills

- **Soft skills:** Communication, active listening, self-motivation, critical thinking, teamwork, time management, problem-solving, adaptability.

- **Languages:** Vietnamese (Native), English (**IELTS 7.0**)

- **Hard skills:**

Programming lang.	familiar with Java, Python, JavaScript/TypeScript, C/C++, SQL, LaTeX.
Data Sci. & DL tools	familiar with Pytorch, Tensorflow, LangChain, Numpy, Pandas, PySpark
ML/ DL	Supervised/ Unsupervised/ Self-supervised Learning, CNN-based models, Transformer Architecture, Large language models, Federated learning, etc.
Data privacy	Differential privacy, Data anonymization techniques, Homomorphic encryption, etc.
Security	Blockchain architectural design, Cryptography, Access control techniques, Program analysis, etc.
Math	Probability, Statistics, Linear Algebra, Game theory, Optimization

Social activities (Selected)

Green Summer Campaign 2017

LEADER OF CSE-HCMUT SQUAD

Ho Chi Minh city, Vietnam

Jun. 2017 - Aug. 2017

National University Entrance Exam Support Campaign 2018

LEADER OF CSE-HCMUT SQUAD

Ho Chi Minh city, Vietnam

Jun. 2018

CSE-HCMUT Student Association Board

PERMANENT BOARD MEMBER

Ho Chi Minh city, Vietnam

2016 - 2020

Certificate of merit for helping Ho Chi Minh City People's Committee and HCMC University of Medicine and Pharmacy to screen and allocate Covid-19 patients

COVID-19 VOLUNTEER

Ho Chi Minh city, Vietnam

Aug. 2021 - Oct. 2021

CSE-HCMUT Large Language Model Summer School

ORGANIZER & MENTOR

Ho Chi Minh city, Vietnam

Jul. 2024