Bui Duc Manh

Mail: manhbui1208@gmail.com | Website: https://manhbui1208.github.io | Mobile: (+65) 86798675 | Google Scholar

Education

University of Technology Sydney (UTS)
Master of Science (Research) in Computing Science ***2023 - 2025***

- Researched the topic "*Advanced Machine Learning for Privacy-Preserving Intrusion Detection in IoT Networks*" under the supervision of Assoc. Prof. Hoang Dinh and Assoc. Prof. Diep Nguyen (Conferred in March/2025)
- Specialized knowledge: Privacy-Preserving Deep Learning, Fully Homomorphic Encryption, Federated Learning

Vietnam National University - University of Engineering and Technology (VNU - UET)
Bachelor of Electronic and Communication Engineering ***2019 - 2023***

- Thesis: "*Real-time multiple attack detection in the Ethereum 2.0 system*" (score 9.1/10, evolved in the **list of high-distinction theses** at VNU-UET)
- Specialized knowledge: IoT, Blockchain Networks and Machine Learning

Research Experience

School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
Research Associate ***May/2025 - Present***

- Working with Asst. Prof. Lin Wang in AI spatial intelligence through insights from neuroscience, focusing on reinforcement learning alignment and 3D memory for embodied AI.

5G/6G Wireless Communications and IoT Networking Lab, University of Technology Sydney, Australia
Research Assistant ***May/2024 - May/2025***

- Participated in Australian government-funded project "Australia-Vietnam 5G/6G Centre" as a research engineer within the demo Privacy-Preserving AI in 5G Edge Computing [link]
- Developed a CNN for blockchain bytecode classification, achieving **award [A1]** in UTS Tech Fest 2024.
- Co-supervised internship student to build a lightweight NLP-inspired MLP for blockchain attack detection using **Tensorflow/Keras** (overseas intern program from Nanyang Technological University)

M.Sc. Researcher ***Sep/2023 - Mar/2025***

- Proposed a novel DNN-based FHE for private training/inference on encrypted data, integrating **Pytorch** and **OpenFHE** to achieve 0.01% accuracy gap to non-encryption baselines ([J1], [C1])
- Designed and deployed a federated learning testbed on encrypted data, optimizing training efficiency through gRPC server configuration and the **Flower** framework (part of [J1])
- Presented conference paper [C1] at IEEE Vehicular Technology Conference (VTC) in Washington DC, USA, October 2024, engaging an international audience.

Radio Communication Lab, VNU - UET, Vietnam
Undergraduate Research Intern ***Feb/2022 - Jun/2023***

- Experienced with Wireshark, Hping3, and BTAT tools for blockchain security experiments
- Developed a multi-modal deep learning method, combining RNN and MLP to jointly process byte-level and network features using **Tensorflow**, achieving **awards [A2], [A3],** and **a High-Distinction thesis** at VNU-UET.

Teaching Experience

Faculty of Engineering and Information Technology, UTS
Casual Academic ***Jan/2024 - May/2025***

- Teaching and designing the Cisco Lab for the IoT Security subject (42037)
- Teaching in the Laboratory of Cybersecurity for Mobile Platform subject (42036)

Engineering Experience

Viettel High Tech – R&D Department for 5G Network Protocol Software, Vietnam
Internship Engineer ***May/2022 - Sep/2022***

- Experienced with C/C++ to operate on RRC attach procedure between User Equipment and gNodeB.

Awards

- [A1] UTS Tech Festival 2024 - Cybersecurity Showcase: Macquarie Cloud Services' Best Choice Award
- [A2] 1st prize in the faculty-hosted undergraduate research competition, VNU-UET (March 2023)
- [A3] 2nd prize in university-hosted undergraduate student research competition at the VNU-UET (May 2023)

Certificates

- Stanford - Supervised Machine Learning: Regression and Classification
- Cisco IoT Fundamental: IoT Security
- IELTS - International English Language Testing System: 6.5 (Jan/2023 - Jan/2025)

Publications

Journals

- [J1] **B. D. Manh**, Z. Zhang, D. Shriram, D. Soumya, and L. Wang, "Mind Meets Space: Critics of Agentic Spatial Intelligence from Neuroscience-inspired Perspective", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2025. (Q1, **highest ranked journal in AI**, currently under review)
- [J2] **B. D. Manh**, C. H. Nguyen, D. T. Hoang, and D. N. Nguyen, "Privacy-Preserving Cyberattack Detection in Blockchain-Based IoT Systems Using AI and Homomorphic Encryption", *IEEE Internet of Things Journal*, Jan 2025, doi: 10.1109/JIOT.2025.3535792. [link] (IF=8.2, Q1, **highest ranked IEEE journal** in IoT).
- [J3] M. A. Hassan, M. B. Jamshidi, **B. D. Manh**, N. H. Chu, C. -H. Nguyen, N. Q. Hieu, C. T. Nguyen, D. T. Hoang, D. N. Nguyen, N. V. Huynh, M. A. Alsheikh and E. Dutkiewicz, "Enabling Technologies for Web 3.0: A Comprehensive Survey", *Elsevier Computer Networks.* [preprint] (IF=4.4, Q1, accepted Mar. 2025).
- [J4] M. A. Hassan, **B. D. Manh**, C. T. Nguyen, C. H. Nguyen, D. T. Hoang, D. N. Nguyen, N. V. Huynh and D. Niyato, "SBW 3.0: A Blockchain-Enabled Framework for Secure and Efficient Information Management in Web 3.0", *IEEE Transactions on Network and Service Management,* 2025. (Q1, **highest ranked journal in networking service**, currently in major revision).
- [J5] N. V. Duc, **B. D. Manh**, Q. T. Luu, D. T. Hoang, N. V. Linh, and D. N. Nguyen, "Secure and Efficient UAV-Based Face Detection via Homomorphic Encryption and Edge Computing", *IEEE Transactions on Vehicular Technology,* 2025. [preprint] (Q1, **highest ranked journal in Vehicular-IoT**, currently under review).

Conferences

- [C1] **B. D. Manh**, C. H. Nguyen, D. T. Hoang, and D. N. Nguyen, "Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained IoV Networks" *IEEE Vehicular Technology Conference* (VTC), October 2024, Washington DC, USA. [link] (**top-tier conference** in vehicular-related technologies).
- [C2] C. H. Nguyen, **B. D. Manh**, D. T. Hoang, and D. N. Nguyen, "Towards Secure AI-empowered Vehicular Networks: A Federated Learning Approach using Homomorphic Encryption" *IEEE Vehicular Technology Conference* (VTC), October 2024, Washington DC, USA. [link]
- [C3] D. H. Son, **B. D. Manh**, T. V. Khoa, N. L. Trung, D. T. Hoang, H. T. Minh, Y. Alem and L. Q. Minh, "Semi-Supervised Learning for Anomaly Detection in Blockchain-based Supply Chains" *IEEE International Symposium on Communications and Information Technologies* (ISCIT), September 2024, Bangkok, Thailand.

Book Chapters

- [B1] **B. D. Manh**, N. Q. Hieu, D. T. Hoang, D. N. Nguyen, and E. Hossain "Machine Learning for Cyberattack Detection in Internet of Things Networks: An Overview" *Elsevier* Advanced Machine Learning for Cyber-Attack Detection in IoT Networks. [link]
- [B2] N. Q. Hieu, **B. D. Manh**, D. T. Hoang, D. N. Nguyen, and E. Hossain "Challenges and Potential Research Directions for Machine Learning-based Cyberattack Detection in IoT Networks" *Elsevier* Advanced Machine Learning for Cyber-Attack Detection in IoT Networks. [link]