XIN YANG

(+1) 587-589-8816 | xin.yang@ualberta.ca | www.neilyxin.com
Edmonton, AB, Canada

EDUCATION

University of Alberta — Edmonton, AB, Canada
Ph.D. Candidate in Computing Science — GPA: 4.0/4.0 — 09/2021 - Present
Supervisor: Dr. Omid Ardakanian

Rutgers University-New Brunswick — New Brunswick, NJ, USA
M.S. in Computer Engineering — GPA: 4.0/4.0 — 09/2017 - 05/2019
Supervisor: Dr. Yingying Chen

University of Electronic Science and Technology of China — Sichuan, China
B.E. in Computer Science and Technology — GPA: 3.61/4.0 — 09/2014 - 06/2017

RESEARCH EXPERIENCE

Sustainable Computing Lab, University of Alberta, Edmonton, AB, CA 09/2021 - Present
Research Assistant

- **Guiding Diffusion Models for Privacy Protection in Sensor Networks**
  - Proposed using denoising diffusion models to generate privacy-preserving time-series sensor data, achieving state-of-the-art privacy-utility trade-offs against attribute inference attacks.
  - Designed novel positive and negative conditioning techniques for guiding diffusion models, enabling precise control over the inclusion and exclusion of specific information in generated data.
  - Disentangled positive and negative conditions in diffusion models by minimizing mutual information, enhancing guidance performance for multiple entangled conditions.
- **Efficient Homomorphic Encryption in Federated Learning (Mitacs Accelerate Intern)**
  - Developed a privacy-preserving federated learning platform with the Flower library, incorporating Multi-key Homomorphic Encryption to protect machine learning model privacy.
  - Implemented the first Python library for Multi-key Homomorphic Encryption (MKHE), facilitating seamless integration with popular deep learning frameworks such as PyTorch and TensorFlow.
  - Explored the combination of model sparsification with homomorphic encryption, reducing communication and computation overhead by up to 8× for MKHE-based FL.
- **End-to-end Privacy Protection in Sensing Systems via Personalized Federated Learning**
  - Designed distributed generative models for sensor data obfuscation using generative adversarial networks (GAN) and variational autoencoders (VAE), delivering end-to-end privacy protection.
  - Devised personalized federated learning algorithm that trains generative models using meta-learning, improving distributed learning performance on non-IID datasets.
  - Deployed model onto Android smartphones and NVIDIA Jetson for real-world run-time analysis, demonstrating feasibility for real-time data obfuscation on mobile and edge IoT devices.

WINLAB, Rutgers University, North Brunswick, NJ, USA 09/2019 - 08/2020
Research Assistant

- **Multiple People Identification Using Millimeter Wave**
  - Proposed a multi-user identification system that analyzes lower-limb gait patterns for up to 4 users simultaneously using a single off-the-shelf mmWave sensor.
  - Devised novel environment-independent gait features by analyzing sensor data in the spatiotemporal domain and designed clustering-based feature segmentation algorithms.
- **Finger-input Authentication on Ubiquitous Surfaces via Physical Vibration**
  - Implemented a finger-input authentication system that performs frequency analysis on vibrations on solid surfaces, delivering touchscreen-like experiences and user authentication capabilities.

- Improved authentication accuracy to 97% and increased the authentication area by 77% using deep learning models, validated authentication performance on various surface materials.

WORK EXPERIENCE

Cisco Systems, Inc., San Jose, CA, USA 06/2020 - 08/2020
Software Engineer Intern (R&D) Supervisor: Dr. David A. Maluf

- Prototyped a real-time multi-factor authentication system using optimization algorithms and collaborated with the Cisco engineering team to enhance system functionality.
- Designed device-free user positioning algorithms utilizing 802.11 wireless networking devices, evaluated through simulation, and delivered code into Cisco products.
- Explored the feasibility of WiFi-based device-free motion detection and localization algorithms by analyzing the phase and angle of arrival (AoA) of WiFi signals.

Amerilink International Corporation, North Brunswick, NJ, USA 06/2018 - 08/2018
Software Engineer Intern

- Developed two native Android apps independently for B2B and B2C travel booking, implemented core functionality, UI, API integrations, multilingual support, and SDKs for map and payment.
- Managed alpha and beta testing for both Android apps, published the 1.0 version of the Aichotels app and AicTours Hotel app on the Google Play Store.
- Refactored backend RESTful APIs in JavaScript and PHP for ordering, payment, and user profiling, improving both security and responsiveness.

PUBLICATIONS

Refereed Journal Articles:

- S. Xaviar, **X. Yang** and O. Ardakanian, "Centaur: Robust Multimodal Fusion for Human Activity Recognition," IEEE Sensors Journal, 2024. (IF: 4.3)
- **X. Yang** and O. Ardakanian, "Blinder: End-to-end Privacy Protection in Sensing Systems via Personalized Federated Learning," ACM Transactions on Sensor Networks **(TOSN)**, 2023. (IF: 4.1.)
- **X. Yang**, S. Yang, J. Liu, C. Wang, Y. Chen, and N. Saxena, "Enabling Finger-touch-based Mobile User Authentication via Physical Vibrations on IoT Devices," IEEE Transactions on Mobile Computing **(TMC)**, 2021. (IF: 7.7. Flagship Journal)

Refereed Conference and Workshop Papers:

- **X. Yang** and O. Ardakanian, "Privacy through Diffusion: Utility-Aware Anonymization of Sensor Data using Conditional Diffusion Model," The 5th Workshop on CPS&IoT Security and Privacy **(CPSIoTSec)**, Copenhagen, Denmark, November 2023.
- **X. Yang**, "PhD Forum Abstract: Towards Utility-Aware Privacy-Preserving Sensor Data Anonymization in Distributed IoT," ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation **(BuildSys)**, Coimbra, Portugal, November 2021.
- Y. Yang, R. D'Oliveira, S. Rouayheb, **X. Yang**, H. Seferoglu, and Y. Chen, "Secure Coded Computation for Efficient Distributed Learning in Mobile IoT," IEEE International Conference on Sensing, Communication and Networking **(SECON)**, Virtual Conference, July 2021. (Acceptance Rate: 37/140 = 26.4%)
- **X. Yang**, J. Liu, Y. Chen, X. Guo, and Y. Xie, "MU-ID: Multi-user Identification Through Gaits Using Millimeter Wave Radios," IEEE International Conference on Computer Communications **(INFOCOM)**, Virtual Conference, July 2020. (Top Conference. Orally Presented. Acceptance Rate: 268/1354 = 19.8%)

Posters and Demos:

- Y. Bai*, **X. Yang***, C. Liu, J. Wain, R. Wang, J. Cheng, C. Wang, J. Liu, and Y. Chen, "Demo: Monitoring Movement Dynamics of Robot Cars and Drones Using Smartphone's Built-in Sensors,"

IEEE International Symposium on Dynamic Spectrum Access Networks **(DySPAN)**, Newark, NJ, November 2019. (*Co-first Authors)

- S. M. Kwon, S. Yang, J. Liu, **X. Yang**, W. Saleh, S. Patel, C. Mathews, and Y. Chen, "Demo: Hands-Free Human Activity Recognition Using Millimeter-Wave Sensors," IEEE International Symposium on Dynamic Spectrum Access Networks **(DySPAN)**, Newark, NJ, November 2019.

PROFESSIONAL PRESENTATIONS

- "Privacy through Diffusion: Utility-Aware Anonymization of Sensor Data using Conditional Diffusion Model," The 5th Workshop on CPS&IoT Security and Privacy, Copenhagen, Denmark, November 2023.
- "MU-ID: Multi-user Identification Through Gaits Using Millimeter Wave Radios," IEEE International Conference on Computer Communications, Virtual Conference, July 2020.

TEACHING EXPERIENCE

- TA, CMPUT 274 - Intro to Tangible Computing I, University of Alberta — Fall 2022
- TA, CMPUT 275 - Intro to Tangible Computing II, University of Alberta — Winter 2022, 2023
- TA, CMPUT 404 - Web Apps and Architecture, University of Alberta — Fall 2021, Winter 2024
- TA, 16:332:563 - Computer Architecture I, Rutgers University — Fall 2019
- Mentored 19 undergraduate students on 5 computer engineering projects. — 2019 - 2020

AWARDS AND SCHOLARSHIPS

- **Alberta Graduate Excellence Scholarship** - $12000 — 11/2024
- **Alberta Graduate Excellence Scholarship** - $12000 — 11/2023
- **Mary Louise Imrie Graduate Student Award** - $1500 — 10/2023
- **Alberta Graduate Excellence Scholarship** - $12000 — 11/2021
- **University of Alberta Graduate Recruitment Scholarship** - $5000 — 05/2021
- **IEEE INFOCOM Student Conference Award** — 06/2020

PROFESSIONAL ACTIVITIES

- **ACM e-Energy 2025 Organization Committee** - Web Chair — 2024
- **ACM ACSAC Artifacts Evaluation Program Committee** - Student Reviewer — 2020