

Yue Tan

✉ tany2851@gmail.com | 🌐 www.tan-yue.com

- 6+ years' experience in optimizing and building cloud systems for security and performance.
- Looking forward to building more secure and more performant systems (ML, serverless...)!

PROJECTS AND EXPERIENCE

Ph.D. Thesis Work | An Architecture and Implementation for Securing Cloud Applications 2021 - Current

- A new cloud system architecture makes the platforms responsible for enforcing user-centric data policies and holds applications untrusted by default.
- Combines the Function-as-a-Service (FaaS) programming model's event-driven nature and the decentralized information flow control (DIFC) security model's binding policies to users, code, and data.
- Free fault tolerance and scalability from non security-critical system components.
- Built a prototype cloud system in **~7K lines of Rust**: a gateway, a cluster scheduler, the security critical, virtual machine manager-embedded CloudCall, a driver for the disaggregated key-value store.
- Built the CloudCall wrapper library each in ~400 lines of code for Python and Node.js applications.
- Operated for several university classes an auto-grader on the Nix-based deployment of the prototype.

Microsoft Research Intern | eZT: Easy Zero Trust in the Cloud May 2023 - Current

- Combines the ideas of confidential computing and information flow control to protect cloud users from the cloud provider and from their own buggy code.
- Uses and trusts SmartNICs as the interposer that regularize the outgoing data streams to prevent the untrusted host machine from leaking secrets.
- Designed and built a NCCL network plugin and a SmartNIC program that enforce the regularization.
- Evaluated target applications' (e.g., PyTorch-based minGPT training) performance degradation.

Ph.D. Thesis Work | Practical Cold-Start Performance Limits in Function-as-a-Service 2019 - 2021

- A research project that explores what the practical cold-start performance limits are while preserving the full Linux programming interface.
- Built our snapshot mechanisms on top of Amazon Firecracker.
- Built the packaging toolchain that formats function code and runtimes as filesystem images.
- Evaluated how different snapshot strategies impact the cold-start performance.

Undergraduate Research | Performance Isolation in Hardware Kernel-Bypass Networks 2017 - 2018

- Enables software multi-tenancy for hardware-based Remote Direct Memory Access (RDMA).
- Designed and implemented the traffic management algorithm as modified RDMA driver code.

Pure Storage Software Engineer Intern May - July 2018

- Built a prototype failover solution in C++ for Pure Storage's core product, storage controller.

TECHNICAL SKILLS

Experienced in Rust, Python, virtualization, C++, C, Linux kernel. **Knowledgeable** about Node.js, NCCL, PyTorch, NVIDIA SmartNICs, RDMA. **Tools**: git, cargo, make, Docker, Nix.

EDUCATION

Princeton University, Princeton, NJ

September 2018 – August 2024 (expected)

Doctor of Philosophy in Computer Science

University of Michigan, Ann Arbor, MI

Graduated in April 2018

Bachelor of Science in Computer Science