Benjamin Liu

U.S. Citizen
Toronto, Ontario
☎ 339-240-2265 ✉ benliu0001@gmail.com github.com/benliu0001 linkedin.com/in/benliu0001

Education

University of Toronto **September 2021 - December 2025**
Honors Bachelor of Science, Computer Science *Toronto, Canada*

Technical Skills

Languages: Python, Java, C/C++, SQL, Assembly Languages
Developer Tools: Shell Scripting in Linux, Git, Agile Methodologies, Google Cloud CLI, Docker, AWS
Technologies/Frameworks: Numpy, OpenCV, PyTorch, Pandas, Pyplot, Scipy, Transformers, RAG

Experience

ML Project Developer | *PyTorch, Hugging Face, Pandas* **January 2024 – April 2024**
mhapy *Toronto, ON*

- Trained a BERT model to analyze the sentiment of users' responses to mental health assessment questions.
- Used Pandas to clean and preprocess Hugging Face datasets to fine tune the BERT model to achieve 60% accuracy.
- Worked with startup to develop a mental health assessment platform, taking into account use cases and user experience.
- Deployed Postman API to AWS and then Railway to allow for other teams to access the model.

Projects

Deep Learning Side Channel Attack | *Python, PyTorch, Numpy, Scipy* **January 2024 – Present**

- Developed LSTM, Resnet, and Transformer models to perform a deep-learning side channel attack on an STM32 microcontroller running TinyAES.
- Assumed profiling attack paradigm to collect training data using a microcontroller and oscilloscope to capture power traces of plaintext-ciphertext pairs.
- Researched various methods to extract features from power traces and optimize the models to improve the attack's success rate.
- Recruited, organized, and led a team of 6 other students to work on the project, and managed the project's timeline.
- Presented weekly to introduce essential concepts in hardware security to team members.

Image Generation Knowledge Distillation | *Python, PyTorch, Numpy* **January 2024 – April 2024**

- Developed a model distillation technique, reducing the size of a large pre-trained VAE by 30x while maintaining comparable performance for text-to-image generation.
- Designed and implemented a 7-layer convolutional neural network to mimic both the encoder and decoder of a VAE, achieving efficient latent space encoding and image reconstruction.
- Trained models on datasets including CIFAR-10, Harvard Flower, CC12M, and Deep Fashion-MultiModal to ensure generalization across diverse image sets.
- Demonstrated strong model generalization on unseen and cross-dataset data, optimizing performance through MSE loss, dropout, and weight decay.

MIT Embedded Security CTF | *C, Python* **February 2020 – August 2020**

- In a team of 4, designed and implemented a secure firmware update system for an IoT device using C and Python.
- Based on MITRE eCTF competition, assumed man in the middle paradigm to attack other teams by exploiting vulnerabilities in their firmware update systems using python scripts, earning 3rd place in the competition.
- Utilized an HMAC to authenticate users, AES, RSA, and SHA to encrypt firmware, and a Stream Cipher for key generation.
- Received intensive instruction from leading researchers on embedded software, computer architecture, memory management, assembly, cryptography, security, interface analysis, and bit manipulation.

Relevant Coursework

- **Computer Vision**
- **Deep Learning**
- **Algorithms**
- **Software Engineering**
- **Databases**
- **Operating Systems**
- **Data Structures**
- **Multivariable Calculus**
- **Probability and Statistics**