JIAMENG PU

jmpu@vt.edu · https://jmpu.github.io/

EDUCATION

Ph.D. in Computer Science (Expected May 2022) Aug. 2017 – Present

Advisor: Dr. Bimal Viswanath

Virginia Polytechnic Institute and State University, Blacksburg, VA
Research Interests: Data-driven security, machine learning

B. Eng in Computer Science Aug. 2013 – May. 2017

Wuhan University, Wuhan, China

EXPERIENCE

Graduate Research Assistant at Virginia Tech Nov. 2018 – present

Advisor: Dr. Bimal Viswanath

Topic: Security and machine learning; Defending against threats posed by advances in ML; Using ML for better security.

Graduate Research Assistant at Biocompleixty Institute, Virginia Tech Aug. 2017 – Aug. 2017

Advisor: Dr. Anil Vullikanti, Dr. Samarth Swarup

Topic: Understanding information propagation in complex networks using deep learning.

Data Scientist Intern at IBM China Development Labs Aug. 2016 – Nov. 2016

Advisor: Xinyu Wu (Senior Researcher)

Topic: Building machine learning tools for quality assessment in business scenarios.

Undergraduate Research Assistant at Wuhan University Aug. 2015 – Aug. 2016

Advisor: Dr. Bo Du, Dr. Lefei Zhang

Topic: Data clustering algorithms using matrix approximations

PUBLICATIONS

- "Throwing Darts in the Dark? Detecting Bots with Limited Data using Neural Data Augmentation"
  Steve T.K. Jan, Qingying Hao, Tianrui Hu, **Jiameng Pu**, Sonal Oswal, Gang Wang, and Bimal Viswanath
  IEEE S&P (Oakland) 2020, San Francisco, CA, USA, May 2020
- "Jekyll: Attacking Medical Image Diagnostics Using Neural Translation"
  Neal Mangaokar, **Jiameng Pu**, Parantapa Bhattacharyam, Chandan Reddy, and Bimal Viswanath
  IEEE EuroS&P 2020, Genova, Italy, June 2020
- "Multiview Clustering Based on Robust and Regularized Matrix Approximation"
  Jiameng Pu, Qian Zhang, Lefei Zhang, and Bo Du
  International Conference on Pattern Recognition, Cancun, Mexico, Nov 2016.

HONORS AND AWARDS

Visa Research Scholarship, awarded by IEEE S&P'20 in San Francisco, CA. May. 2020
Student Travel Grant, awarded by NDSS'19 in San Diego, CA. Feb. 2019
National Endeavor Scholarships (given to top 5% students), awarded by Chinese Ministry of Education. 2014, 2015

PROJECTS

Detecting GAN-generated Images at Virginia Tech

- Designed and built a system that can detect fake images generated using AI models—*Generative Adversarial Networks(GANs)* with upto 99.5% accuracy.
- Evaluated the detection system with 11 datasets of diverse content from 4 state-of-the-art GANs.

Investigating Attacks on Medical Image Diagnostics at Virginia Tech

- Designed and implemented a GAN-based tool that can inject a specific disease condition to a patient's image, while preserving their identity.
- Demonstrated the attack feasibility on two popular biomedical image modalities, X-rays and retinal fundus images, and conducted user studies with medical professionals.

Bot Detection with Limited Data at Virginia Tech

- Developed a GAN-based data synthesis method to enable effective model training with limited labeled data.
- Validated our system using real-world datasets from 3 different online services.

Defending Against Backdoor Attacks on Deep Text Models at Virginia Tech

- Designed a tool to investigate NLP classifiers affected by backdoor attacks.

TECHNICAL SKILLS

- **Languages:** *Python, Java, MATLAB, Javascript, C++, C, MySQL, Bash.*
- **Frameworks:** *Tensorflow, PyTorch, Keras, Scikit-Learn, DL models (CNNs, LSTMs, RNNs, etc.).*
- **Tools:** *Git, LaTeX, Unix systems.*