

# Yujie Ji

<https://laraji.github.io/>

Email : yujie.ji.lu@gmail.com

Mobile : +1-484-541-3708

New grad focused on software development. Offering hands-on experience in machine learning and data mining.

## INTERN EXPERIENCES

---

- **Kika Tech, Inc.** May. 2018 - Aug. 2018  
*Software Engineer(intern), Recommendation Algorithm Team* Beijing, China
  - Improved word recommendations by implementing long sentence prediction.
  - Built the long sentence prediction model based on Seq2Seq model, utilizing TensorFlow.
  - Cleaned the corpus based on Stanford CoreNLP in Java to improve the prediction accuracy.

## PROJECT EXPERIENCES

---

- **Poisoning Attack and Adversarial Attack against Deep Neural Networks** Nov. 2018 - May. 2019  
*Software Engineer, Algorithmic Learning, Privacy and Security (ALPS) Lab* Lehigh University, PA, USA
  - Demonstrated the vulnerability of the model if an attacker performs poisoning attack and adversarial attack simultaneously, and proposed an attack mechanism that cannot be detected by any existing defenses.
  - Designed and implemented a platform which allows to perform both poisoning attacks and adversarial attacks against Deep Neural Networks in Python.
  - Implemented poisoning attacks, e.g StingRay, and adversarial detection methods, e.g, Feature Squeezing.
- **Model Attack and Defense for Deep Learning Systems** Feb. 2017 - Oct. 2018  
*Software Engineer, Algorithmic Learning, Privacy and Security (ALPS) Lab* Lehigh University, PA, USA
  - Revealed security risks of reusing pre-trained models in building Machine Learning systems, and proposed an attack algorithm to fool the model, published papers in *CCS 2018*, and was awarded **best paper** at *CNS 2017*.
  - Designed and implemented attack mechanisms to trigger the misclassification of the domain-transferred models.
  - Built Neural Networks for image and audio analysis based on PyTorch.
  - Implemented model transfer tools between different platforms, e.g, Keras and PyTorch.
- **Detection of Adversarial Samples on Deep Neural Networks** Oct. 2016 - May. 2018  
*Software Engineer, Algorithmic Learning, Privacy and Security (ALPS) Lab* Lehigh University, PA, USA
  - Demonstrated the difference between benign inputs and malicious inputs from a dynamic aspect, and published a poster paper in *CCS 2018*.
  - Built Neural Networks for image classification based on Keras.
  - Proposed and implemented an adversarial sample detection mechanism based on TensorFlow.
  - Implemented several baseline adversarial attack and defense methods against DNN models.
  - Implemented a DNN model compression method based on Network Trimming.
  - Implemented the adversarial images analysis algorithm from the Mutual Information perspective.
- **Chinese Social Media Analysis for Disease Surveillance** Oct. 2014 - Dec. 2014  
*Software Engineer, Big Data and Cloud Computation Laboratory* Wuhan University, Hubei, China
  - Reported the outbreak of flu 5 days earlier than the national official report, and published one journal paper in *Pers Ubiquit Comput (2015)*.
  - Implemented K-means and KNN in Java.

## EDUCATION

---

- **Lehigh University** Bethlehem, PA  
*Master of Science in Computer Science, GPA: 3.85/4.0* Aug. 2016 – Dec. 2019
- **Wuhan University** Hubei, China  
*Bachelor of Engineering in Software Engineering, GPA: 3.5/4.0* Sept. 2012 – Jun. 2016

## SKILLS & TECHNIQUES

---

Languages: Python, Java; MySQL; MATLAB.

Technologies: Linux; PyTorch, Keras, TensorFlow, sklearn.