CONGZHENG SONG

Curriculum Vitae

Last Updated: 5th October, 2017

Contact

2 W Loop Rd
Cornell Tech
New York, NY, 10044

(678)-882-8741
cs2296@cornell.edu
http://csong27.github.io

Education

Cornell University, Ithaca, NY 2016 – Present
Ph.D. student in Computer Science
Research Interests: Security and Privacy in Machine Learning

Emory University, Atlanta, GA 2012 – 2016
B.S. in Computer Science with Summa Cum Laude
Thesis: *Using Deep Recurrent Neural Networks to Estimate Influenza Prevalence from Mobile Phone Records*

Publications

Peer-reviewed Journal & Conference

1. Safoora Yousefi, Fatemeh Amrollahi, Mohamed Amgad, Coco Dong, Joshua E. Lewis, **Congzheng Song**, David A. Gutman, Sameer H. Halani, Jose Enrique Velazquez Vega, Daniel J. Brat, Lee A.D. Cooper
Predicting Clinical Outcomes from Large Scale Cancer Genomic Profiles with Deep Survival Models
In *Scientific Reports 7* (Nature), *2017.*
2. **Congzheng Song**, Thomas Risternpart, Vitaly Shmatikov
Machine Learning Models that Remember Too Much
In *the ACM Conference on Computer and Communications Security* (CCS), *2017.*
3. Reza Shokri, Marco Stronati, **Congzheng Song**, Vitaly Shmatikov
Membership Inference Attacks against Machine Learning Models
In *38th IEEE Symposium on Security and Privacy* (S&P), San Jose, California, 2017.

Workshop & Poster

1. Safoora Yousefi, **Congzheng Song**, Nelson Nauata, Lee Cooper
Learning Genomic Representations to Predict Clinical Outcomes in Cancer
In *International Conference on Learning Representation Workshop* (ICLR), San Juan, Puerto Rico, 2016.
2. Erik Reinertsen, Niclas Palmius, **Congzheng Song**, Leon Danon, Gudrun Saemundsdottir, Olafur Magnusson, Gari D Clifford, Ymir Vigfusson
Mobile Phone Activity and Population Movement During an Influenza A (H1N1) Outbreak in Iceland
In *Sleep Medicine and Chronobiology Summer Schools Poster Session,* Oxford, UK, 2015.

Research Experience

Graduate Research Assistant 2016 – Present
Department of Computer Science, Cornell University Adviser: Prof. Vitaly Shmatikov
∞ Exploring privacy leakage in machine learning models.

Undergraduate Research Assistant 2015 – 2016
Department of Math & CS, Emory University Adviser: Prof. Ymir Vigfusson

- ∞ Extracted a set of metrics to describe human behavior from mobile phone records.
- ∞ Developed a deep learning model for individual sickness prediction given behavioral features.

Undergraduate Research Assistant 2015 – 2016
Department of Bioinformatics, Emory University Adviser: Prof. Lee Cooper

- ∞ Developed a neural network combining with Cox regression for survival analysis.
- ∞ Applied covolutional neural network in cancer cell image classification.

Undergraduate Research Intern Summer 2015
Department of Computer Science, UC Irvine Adviser: Prof. Sharad Mehrotra

- ∞ Developed a web framework for collecting, querying and visualizing sensor data.
- ∞ Involved in implementing backend server modules to handle user's request for processing sensors' data on multiple platforms.

Teaching Experience

Graduate Teaching Assistant Fall 2016
CS 3410: Computer System Organization and Programming Instructor: Prof. Anne Bracy

Undergraduate Lab Teaching Assistant Fall 2013
Chem 141: General Chemistry I Instructor: Prof. Karl Hagen

Awards

- ∞ Trevor Evans Award 2016
- ∞ Deborah Jackson Award 2015
- ∞ Dean's List 2012 – 2016

Skills

Programming and Scripting Languages: Python, Java, C, JavaScript, HTML & CSS, LaTeX

Software and Tools: Tensorflow, Theano, Matlab, R studio, Node.js, MongoDB, PostgreSQL

Languages: Chinese (Native), English (Professional), Japanese (Basic)

Selected Coursework

Computer Science: Analysis of Algorithm, Bayesian Machine Learning, Advanced Programming Languages , Natural Language Processing, Data Mining, Artificial Intelligence, Theory of Computing, Discrete Structures, Competitive Programming, Computer Security

Mathematics: Probabilities and Statistics, Partial Differential Equations, Numerical Analysis, Optimization Theory, Ordinary Differential Equations, Linear Algebra