









Scott Freitas







I'm a Senior Applied Scientist at Microsoft working at the intersection of applied and theoretical machine learning, with a focus on **graph mining** and **deep learning**. My goal is to develop explainable, robust, and efficient next-generation cybersecurity systems.



I completed my Machine Learning PhD at [Georgia Tech](#) where I worked with [Polo Chau](#). I co-authored several winning research proposals, including a multi-million dollar [DARPA grant](#); was awarded PhD fellowships from [IBM Research](#), [NSF GRFP](#) and [Raytheon](#); and was fortunate to work with amazing engineers and scientists at [IBM Research](#), [Amazon](#), [Microsoft Advanced Threat Protection](#), [Microsoft Research](#), [Intel](#) and the [Naval Air Warfare Center](#).

 scottfreitas.com
 safreita1@gmail.com
 Google Scholar
 Blog Posts
 Curriculum Vitae (PDF)

 Github
 LinkedIn
 @scottafreitas

Education

- Dec. 2021 — **Ph.D. in Machine Learning**
Aug. 2018 — Georgia Institute of Technology, Atlanta, GA
Advisor: Duen Horng (Polo) Chau
Thesis: *Developing Robust Models, Algorithms, Databases and Tools with Applications to Cybersecurity and Healthcare*
Committee: Duen Horng (Polo) Chau, Srijan Kumar, Diyi Yang, B. Aditya Prakash, Hanghang Tong
 Thesis  Thesis Recording (Proposal)  Thesis Slides
- May 2018 — **M.S. in Computer Science**
May 2017 — Arizona State University, Tempe, AZ
Advisor: Hanghang Tong
Thesis: *Mining Marked Nodes in Large Graphs*
Committee: Hanghang Tong, Ross Maciejewski, Yezhou Yang
GPA: 4.00/4.00
 Thesis
- May 2017 — **B.S. in Computer Science**
Aug. 2015 — Arizona State University, Tempe, AZ
Advisor: Ross Maciejewski
Thesis: *Guided Augmented Reality Tours using Landmarks and Social Media*
GPA: 3.98/4.00
 Thesis  Thesis Recording

May 2014 — **B.S.E. in Electrical Engineering**
Aug. 2010 Arizona State University, Tempe, AZ
Advisor: James Aberle
Thesis: *Multi-Stage Linear Electromagnetic Accelerator Using Optical Triggering*
GPA: 3.64/4.00
 Thesis  Thesis Recording

Honors and Awards

2021 IBM PhD Fellowship
One of sixteen fellows; awarded for my work in developing next-generation explainable defenses

2021 Nvidia Data Science Teaching Kit
Helped develop one of five Nvidia teaching kits used by educators around the world

2019 Raytheon Research Fellowship
Awarded for my PhD work in adversarial machine learning

2018 — 2021 NSF Graduate Research Fellowship
National Science Foundation recognizes and supports outstanding graduate students in STEM fields

2018 Outstanding Computer Science Masters Student (ASU)
Awarded to single master student demonstrating exemplary performance

2017 Best Demo Award, Runner Up at CIKM '17
For "Rapid Analysis of Network Connectivity"

2017 CIKM Travel Grant
Funding from NSF and SIGWEB to present at CIKM

2016 — 2017 FURI Grant
Undergraduate research grant awarded for work in network connectivity

2016 — 2017 Arizona Graduate Scholar Award
Merit scholarship awarded to select number of master students

2010 — 2014 Provost's Scholarship
Merit scholarship awarded to select number of incoming undergraduate students

Industry Research Experience

Present — **Microsoft**, Redmond, WA
Jan. 2022 *Senior Applied Scientist, Microsoft Security Research*
Design ML systems to automatically correlate cross-product security alerts into rich incident events

Dec. 2021 — **IBM Research**, Yorktown Heights, NY
Sep. 2021 *Research Intern, Cyber Security Intelligence (CSI) Team*
Mentor: Teryl Taylor, Frederico Araujo, Jiyong Jang
Developed unsupervised graph representation learning techniques to detect suspicious activity in cloud platforms

Aug. 2021 — **Amazon**, Seattle, WA
May 2021 *Applied Scientist Intern, Fraud Detection and Risk Transaction (CTPS)*
Mentor: Hao Zheng, Yanni Lai
Created unsupervised and semi-supervised approaches to prevent fraudulent transactions across the Amazon marketplace

- May 2020 — **Microsoft**, Redmond, WA
Aug. 2020 *Research Intern, Microsoft ATP + Microsoft Research*
Mentor: Karishma Sanghvi, Yuxiao Dong
Designed semi-supervised graph neural network approach to detect malicious software
- Aug. 2019 — **Microsoft**, Redmond, WA
May 2019 *Research Intern, Microsoft Advanced Threat Protection (ATP)*
Mentor: Andrew Wicker, Joshua Neil
Created first framework to model lateral attacks on enterprise networks, enabling IT admins to quantify and mitigate network vulnerability to lateral attacks
- March 2015 — **General Dynamics**, Scottsdale, AZ
Dec. 2014 *Systems Engineer, Mission Systems*
Worked on the Integrated Threat Force team to develop and refine the communication technology systems.
- Aug. 2013 — **Naval Air Warfare Center**, Point Mugu, CA
May 2013 *Research Intern, Naval Research Enterprise Internship Program (NREIP)*
Mentor: Balaji Iyer
Explored methods of preventing electromagnetic interference from coupling into superconducting receivers

Academic Research Experience

- Present — **Georgia Institute of Technology**, Atlanta, GA
Aug. 2018 *Graduate Research Assistant, School of Computational Science and Engineering*
Mentor: Duen Horng (Polo) Chau
Member of the Polo Club of Data Science where we innovate scalable, interactive, and interpretable tools that amplify human's ability to understand and interact with billion-scale data and machine learning models
- May 2018 — **Arizona State University**, Tempe, AZ
Summer 2017 *Graduate Research Assistant, School of Computing, Informatics, and Decision Systems Engineering*
Mentor: Hanghang Tong
Conducted research in graph based connectivity analysis to improve local graph partitioning. Developed web-based prototype for explainable ranking in complex multi-layered networks.
- Aug. 2017 — **Arizona State University**, Tempe, AZ
May 2017 *Summer Research Assistant, School of Computing, Informatics, and Decision Systems Engineering*
Mentor: Ross Maciejewski
Developed interactive augmented reality (AR) graph models in the Microsoft HoloLens.
- May 2017 — **Arizona State University**, Tempe, AZ
Jan. 2016 *Undergraduate Research Assistant, School of Computing, Informatics, and Decision Systems Engineering*
Mentor: Hanghang Tong
Developed fast graph mining algorithms for network connectivity analysis, and award winning web platform for visualization and analysis.

Publications

Graph Vulnerability and Robustness: A Survey

Scott Freitas, Diyi Yang, Srijan Kumar, Hanghang Tong, Duen Horng (Polo) Chau
IEEE Transactions on Knowledge and Data Engineering (TKDE). 2022.

[PDF](#) [BibTeX](#)

MalNet: A Large-Scale Image Database of Malicious Software

Scott Freitas, Rahul Duggal, Duen Horng (Polo) Chau

ACM International Conference on Information and Knowledge Management (CIKM). Atlanta, GA, 2022.

[Demo](#) [PDF](#) [Code](#) [BibTeX](#)

A Large-Scale Database for Graph Representation Learning

Scott Freitas, Yuxiao Dong, Joshua Neil, Duen Horng (Polo) Chau

Neural Information Processing Systems Datasets and Benchmarks (NeurIPS). Virtual, 2021.

[Project](#) [Demo](#) [PDF](#) [Blog](#) [Code](#) [BibTeX](#)

Evaluating Graph Vulnerability and Robustness using TIGER

Scott Freitas, Diyi Yang, Srijan Kumar, Hanghang Tong, Duen Horng (Polo) Chau

ACM International Conference on Information and Knowledge Management (CIKM). Virtual, 2021.

[PDF](#) [Blog](#) [Video](#) [Code](#) [BibTeX](#) [Featured in Nvidia Data Science Toolkit](#)

EnergyVis: Interactively Tracking and Exploring Energy Consumption for ML Models

Omar Shaikh, Jon Saad-Falcon, Austin P Wright, Nilaksh Das, Scott Freitas, Omar Asensio, Duen Horng Chau

ACM Conference on Human Factors in Computing Systems (CHI). Virtual, 2021.

[Demo](#) [PDF](#) [Video](#) [Code](#) [BibTeX](#)

UnMask: Adversarial Detection and Defense Through Robust Feature Alignment

Scott Freitas, Shang-Tse Chen, Zijie J. Wang, Duen Horng (Polo) Chau

IEEE International Conference on Big Data (Big Data). Atlanta, GA, 2020.

[Project](#) [PDF](#) [Blog](#) [Video](#) [Code](#) [BibTeX](#)

HAR: Hardness Aware Reweighting for Imbalanced Datasets

Rahul Duggal, Scott Freitas, Sunny Dhamnani, Duen Horng (Polo) Chau, Jimeng Sun

IEEE Conference on Big Data (Big Data). Orlando, USA, 2021.

[PDF](#) [Video](#) [BibTeX](#)

Argo Lite: Open-Source Interactive Graph Exploration and Visualization in Browsers

Siwei Li, Zhiyan Zhou, Anish Upadhayay, Omar Shaikh, Scott Freitas, Haekyu Park, Zijie J. Wang, Susanta Routray, Matthew Hull, Duen Horng (Polo) Chau

ACM International Conference on Information and Knowledge Management (CIKM). Virtual, 2020.

[Demo](#) [PDF](#) [Code](#) [BibTeX](#)

REST: Robust and Efficient Neural Networks for Sleep Monitoring in the Wild

Rahul Duggal*, Scott Freitas*, Cao Xiao, Duen Horng (Polo) Chau, Jimeng Sun

The Web Conference (WWW). Taipei, Taiwan, 2020.

[Project](#) [PDF](#) [Blog](#) [Video](#) [Code](#) [BibTeX](#) * Authors contributed equally

D²M: Dynamic Defense and Modeling of Adversarial Movement in Networks

Scott Freitas, Andrew Wicker, Duen Horng (Polo) Chau, Joshua Neil

SIAM International Conference on Data Mining (SDM). Cincinnati, Ohio, 2020.

[Project](#) [PDF](#) [Blog](#) [BibTeX](#)

Extracting Knowledge For Adversarial Detection and Defense in Deep Learning

Scott Freitas, Shang-Tse Chen, Duen Horng (Polo) Chau

KDD Workshop: Learning and Mining for Cybersecurity (LEMNCS). Anchorage, Alaska, 2019.

[PDF](#) [BibTeX](#)

Local Partition in Rich Graphs

Scott Freitas, Nan Cao, Yinglong Xia, Duen Horng (Polo) Chau, Hanghang Tong

IEEE International Conference on Big Data (Big Data). Seattle, Washington, 2018.

[Project](#) [PDF](#) [BibTeX](#)

X-Rank: Explainable Ranking in Complex Multi-Layered Networks

Jian Kang*, Scott Freitas*, Haichao Yu, Yinglong Xia, Hanghang Tong

ACM International Conference on Information and Knowledge Management (CIKM). Turin, Italy, 2018.

[Project](#) [PDF](#) [BibTeX](#) * Authors contributed equally

Rapid Analysis of Network Connectivity

Scott Freitas, Hanghang Tong, Nan Cao, Yinglong Xia

ACM International Conference on Information and Knowledge Management (CIKM). Singapore, 2017.

[Project](#) [PDF](#) [Video](#) [Code](#) [BibTeX](#) [Best Demo Paper, Runner up](#)

Talks

Clustering Process Activity in Cloud Environments using Graph Representation Learning

Dec. 2021

IBM Research

Dec. 2021

DARPA CHASE: Cyber-Hunting at Scale

Detecting Financial Fraud in Online Marketplaces

August 2021

Amazon

Developing Robust Models, Algorithms, Databases and Tools with Applications to Cybersecurity and Healthcare

Dec. 2021

Georgia Institute of Technology

May 2021

Georgia Institute of Technology

Exploring Graph Neural Networks for Malware Detection

July 2020

Microsoft Advanced Threat Protection

On the Robustness and Vulnerability of Graphs

April 2020

Georgia Institute of Technology

D²M: Dynamic Defense and Modeling of Adversarial Movement in Networks

Aug. 2019

Microsoft Advanced Threat Protection Research Expo

Mining Marked Nodes in Large Graphs

Dec. 2018

Microsoft Advanced Threat Protection Group

May 2018

Arizona State University

Local Partition in Rich Graphs

Dec. 2018 IEEE International Conference on Big Data

Rapid Analysis of Network Connectivity

Nov. 2017 ACM International Conference on Information and Knowledge Management (CIKM)

Network Connectivity Analysis and Visualization in Large Graphs

April 2017 Keynote Speaker: ASU Fulton Undergraduate Research Initiative (FURI)

Nov. 2016 ASU FURI Research Symposium

Press

Dec. 2021 "Congratulations to the Newest PhDs from Georgia Tech",

June 2021 "New NVIDIA Partnership Bridges Education Gap for Data Science and Machine Learning",

April 2021 "ML Student Earns Prestigious IBM Ph.D. Fellowship Award",

April 2021 "IBM PhD Fellowship Awardees Announced",

April 2021 "Accelerated Data Science in the Classroom: Teaching Analytics and Machine Learning with RAPIDS",

April 2020 "Georgia Tech and Intel Awarded Multimillion-Dollar Program to Defend Against Attacks on AI",

April 2020 "DARPA Snags Intel to Lead its Machine Learning Security Tech",

April 2020 "Machine Learning Technique Helps Wearable Devices Get Better at Diagnosing Sleep Disorders and Quality",

Feb. 2019 "Raytheon Awards Two ML@GT Students Graduate Research Assistantships",

July 2018 "NSF Graduate Research Fellow wants to use computer science to solve society's toughest problems",

Grants and Funding

2021 **IBM PhD Fellowship**
IBM Research PhD Fellowship Awardee
Funded: \$95,000

2020 **Google Cloud Research Grant**
Large Scale Malware Analysis
Funded: \$5,000 Google cloud credits

2018 — 2022 **Guaranteeing AI Robustness against Deception (GARD)**
DARPA Research Grant
Co-PIs: Jason Martin, Duen Horng (Polo) Chau
Funded: multi-million
Helped formulate adversarial defense techniques

2018 **Amazon AWS Research Grant**
Adversarial Re-Training and Model Vaccination for Robust Deep Learning
Funded: \$5,000 AWS cloud credits

- 2018 **Nvidia GPU Grant**
Defending Adversarial Attacks by Robust, Inference-time Local Linear Approximation
Funded: Nvidia Titan V GPU worth \$3,000
- 2019 **Raytheon Research Fellowship**
Extracting Knowledge For Adversarial Detection and Defense
Funded: \$25,000
- 2018 — 2023 **NSF Graduate Research Fellowship Program (GRFP)**
Multi-level Interdiction and Assistance Modeling for Natural Disasters
Funded: Full tuition + \$102,000
- 2016 — 2017 **FURI Grant**
Network Connectivity Analysis and Visualization in Large Graphs
Funded: \$3,000

Teaching

- Spring 2021 **Graduate Teaching Assistant**
Georgia Institute of Technology, Atlanta, GA
Data and Visual Analytics, Instructor: Duen Horng (Polo) Chau
- Fall 2020 **Graduate Teaching Assistant**
Georgia Institute of Technology, Atlanta, GA
Data and Visual Analytics, Instructor: Duen Horng (Polo) Chau
- Fall 2013 **Undergraduate Teaching Assistant**
Arizona State University, Tempe, AZ
Fulton Undergraduate Research Experience (FSE 294), Instructor: Joshua Lyon
Designed and taught introductory lesson plans to new engineering students

Mentoring

- Present — **Omar Shaikh**
Spring 2020 *B.S. in Computer Science, Georgia Institute of Technology*
- Present — **Jon Saad-Falcon**
Spring 2020 *B.S. in Computer Science, Georgia Institute of Technology*
- Present — **Frank Zhou**
Spring 2020 *B.S. in Computer Science, Georgia Institute of Technology*
- Present — **Kevin Li**
Summer 2020 *B.S. in Computer Science, Georgia Institute of Technology*

Service

Program Committee

Association for the Advancement of Artificial Intelligence (**AAAI**) at AAAI 2021

ACM International Conference on Information and Knowledge Management (**CIKM**) at ACM CIKM 2020

Reviewer

Practice of Knowledge Discovery in Databases (**ECML-PKDD**) 2021

International Conference on Computer Vision (**ICCV**) 2021

Conference on Computer Vision and Pattern Recognition (**CVPR**) 2021

ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**) 2019

International Conference on Machine Learning (**ICML**) 2019