Fnu Suya

✉ suya@virginia.edu • 🌐 fsuya.org • in suya • suyafnu
suyeecav • Updated on February 27, 2023

Education

○ Ph.D. in Computer Science, University of Virginia	Aug 2017 – Dec 2023
○ Ph.D. in Computer Science, Arizona State University	Aug 2015 – May 2017
○ B.Eng. in Electrical Engineering, China Agricultural University	Aug 2010 – May 2014

Research Interests

I am interested in the trustworthy aspect of machine learning, including both the security and privacy and their possible interactions.

Research Experience

○ University of Virginia, David Evans, Yuan Tian ○ Machine Learning Security in Training and Inference Time	Aug 2017 – Present
○ Qualcomm Technologies, Inc., Aleksei Triastcyn ○ Poisoning Attacks on Federated Learning	May 2021 – Aug 2021
○ Amazon Web Services, Inc., MohamadAli Torkamani ○ Robust Learning on Extremely Large Graphs	Jan 2021 – Apr 2021
○ Bosch Center for Artificial Intelligence, Anit Kumar Sahu ○ Query Efficient Black-box Attacks	June 2020 – Aug 2020
○ Arizona State University, Guoliang Xue, Paolo Papotti ○ Incentive Mechanism Design, Machine learning Privacy	Aug 2015 – Jul 2017
○ Tsinghua University, Bo Bai ○ Energy Efficient Wireless Communication	Aug 2014 – Feb 2015

Teaching Experience

○ Learning Theory (UVA CS 6501-005), TA	S2019
○ Cryptography (UVA CS 6501-009), TA	S2019
○ Game Theory (ASU CSE 556), TA	F2016
○ Introduction to C++ Programming (ASU CSE 100), TA	F2015 – S2016
○ Introduction to Programming Languages (ASU CSE 240), TA	F2015 – S2016

Honors & Awards

○ CS Graduate Research Award, University of Virginia	2018
○ CS Department Fellowship, University of Virginia	2017
○ NSF Travel Grant, GlobalSIP	2016
○ CIDSE Doctoral Fellowship, Arizona State University	2015
○ Outstanding Student Scholarship, China Agricultural University	2011 – 2013

Service

Conference Reviewer	AISTATS 2023, CVPR 2023, IJCAI 2021-2024, ICML 2020-2023, NeurIPS 2021-2022, ICLR 2021-2023, IEEE S&P 2018-2023, Usenix Security 2018-2023, NDSS 2018-2023, CCS 2018-2022, Sensys 2021-2022, ASIACCS 2019, Euro S&P 2019-2022, AAAI 2017-2019, SIGMOD 2017, DASFAA 2017, MobiHoc 2016
Journal Reviewer	Artificial Intelligence, TMLR
Program Committee	IJCAI 2021-2024

Skills

Programing	Python, Matlab, C, C++, LaTeX
Frameworks	TensorFlow, PyTorch, MXNet, NumPy, SciPy, Scikit-learn
Systems	Linux, OSX
Languages	Mongolian (native), Chinese, English

Publications

Google Scholar ID: OmLIG8EAAAAJ

2023a **F. Suya**, X. Zhang, Y. Tian, D. Evans. "Understanding Inherent Vulnerabilities of Datasets to Poisoning Attacks". In: *Under Submission*.

2023b Y. Tian, **F. Suya**, A. Suri, F. Xu, D. Evans. "Manipulating Transfer Learning for Property Inference". In: *The IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2023)*.

2022a E. Rose, **F. Suya**, D. Evans. "Poisoning Attacks and Subpopulation Susceptibility". In: *Best Paper Award, 5th Workshop on Visualization for AI Explainability (VISxAI workshop)*. URL: https://uvasrg.github.io/poisoning/.

2022b **F. Suya**, A. Suri, T. Zhang, S. Hong, Y. Tian, D. Evans. "SoK: What Have We Learned About Black-box Attacks Against Classifiers?" In: *Under Submission*.

2022c Y. Tian, **F. Suya**, F. Xu, D. Evans. "Stealthy Backdoors as Compression Artifacts". In: *IEEE Transactions on Information Forensics and Security* 17, pp. 1372–1387. URL: https://arxiv.org/abs/2104.15129.

2021 **F. Suya**, S. Mahloujifar, A. Suri, D. Evans, Y. Tian. "Model-Targeted Poisoning Attacks with Provable Convergence". In: *The Thirty-eighth International Conference on Machine Learning (ICML 2021)*. URL: https://arxiv.org/abs/2006.16469.

2020a **F. Suya**, J. Chi, D. Evans, Y. Tian. "Hybrid Batch attacks: Finding Black-box Adversarial Examples with Limited Queries". In: *29th USENIX Security Symposium (USENIX Security 2020)*. URL: https://arxiv.org/abs/1908.07000.

2020b J. Wang, M. Luo, **F. Suya**, J. Li, Z. Yang, Q. Zheng. "Scalable Attack on Graph Data by Injecting Vicious Nodes". In: *The European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2020)*. URL: https://arxiv.org/abs/2004.13825.

2019 Y. Chen, M. Zha, N. Zhang, D. Xu, Q. Zhao, X. Feng, K. Yuan, **F. Suya**, Y. Tian, K. Chen, X. Wang, W. Zou. "Demystifying Hidden Privacy Settings in Mobile Apps". In: *2019 IEEE Symposium on Security and Privacy (S&P 2019)*. URL: https://ieeexplore.ieee.org/abstract/document/8835388.

2018 **F. Suya**, D. Evans, Y. Tian. "Poster: Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers". In: *2018 IEEE Symposium on Security and Privacy (S&P 2018)*. URL: https://www.ieee-security.org/TC/SP2018/poster-abstracts/oakland2018-paper37-poster-abstract.pdf.

2017 **F. Suya**, Y. Tian, D. Evans, P. Papotti. "Query-limited Black-box Attacks to Classifiers". In: *NIPS Workshop on Machine Learning and Computer Security (MLSec)*. URL: https://arxiv.org/abs/1712.08713.

2016 **F. Suya**, Y. Shi, B. Bai, W. Chen, J. Zhang, K. B. Letaief, S. Zhou. "Optimal Stochastic Power Control with Compressive CSI Acquisition for Cloud-RAN". In: *IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2016*. URL: https://ieeexplore.ieee.org/abstract/document/7906068.