Fnu Suya

suya@umd.edu • fsuya.org • suya • suyafnu
suyeecav • Updated on March 15, 2026

Professional Appointments

Tenure-track Assistant Professor 08/2024 – Present
Min H. Kao Department of EECS, University of Tennessee, Knoxville
MC2 Postdoctoral Fellow 08/2023 – 07/2024
Maryland Cybersecurity Center, University of Maryland, College Park

Education

Ph.D. in Computer Science, *University of Virginia* 08/2017 – 07/2023
Thesis: *On the Limits of Data Poisoning Attacks*
Advisor: Yuan Tian (UCLA), David Evans

M.Sc. in Computer Science, *University of Virginia* 08/2017 – 12/2022
Advisor: Yuan Tian (UCLA), David Evans

Ph.D. in Computer Science, *Arizona State University* 08/2015 – 07/2017
Advisor: Paolo Papotti (EURECOM), discontinued due to advisor relocation

B.Eng. in Electrical Engineering (Honors), *China Agricultural University* 09/2010 – 07/2014

Research Interests

Trustworthy Machine Learning, Machine Learning for Security

Internship Experience

Research Intern, *Qualcomm*, San Diego (with Aleksei Triastcyn on robust FL) 05/2021– 08/2021
Research Intern, *Amazon AWS*, New York City (with MohamadAli Torkamani on GNNs) 01/2021 – 04/2021
Research Intern, *Bosch AI Center*, Pittsburgh (with Anit Kumar Sahu on black-box attacks) 06/2020 – 08/2020
Research Intern, *Tsinghua University*, China (with Bo Bai on wireless communication) 08/2014 – 02/2015

Conference and Journal Papers

Google Scholar ID: OmLIG8EAAAAJ

2026a A. Al Nomaan Nafi, H. Rahaman, Z. Haider, T. Mahfuz, **F. Suya**, S. Bhunia, P. Chakraborty. "DAASH: A Meta-Attack Framework for Synthesizing Effective and Stealthy Adversarial Examples". In: *CVPR 2026*.
2026b S. Amgain, D. Lobo, A. Chatterjee, S. Bhunia, **F. Suya**. "HAMLOCK: HArdware-Model LOgically Combined attacK". In: *USENIX Security 2026*.
2026c T. Zhang, **F. Suya**, R. Jha, C. Zhang, V. Shmatikov. "Adversarial Hubness in Multi-Modal Retrieval". In: *IEEE S&P (Oakland) 2026*.
2024 F. Suya, A. Suri, T. Zhang, S. Hong, Y. Tian, D. Evans. "SoK: Pitfalls in Evaluating Black-Box Attacks". In: *IEEE SaTML 2024*.
2023a F. Suya, X. Zhang, Y. Tian, D. Evans. "What Distributions are Robust to Indiscriminate Poisoning Attacks for Linear Learners?" In: *NeurIPS 2023*.

2023b Y. Tian, **F. Suya**, A. Suri, F. Xu, D. Evans. "Manipulating Transfer Learning for Property Inference". In: *CVPR 2023*.
2022 Y. Tian, **F. Suya**, F. Xu, D. Evans. "Stealthy Backdoors as Compression Artifacts". In: *IEEE TIFS*.
2021 F. Suya, S. Mahloujifar, A. Suri, D. Evans, Y. Tian. "Model-Targeted Poisoning Attacks with Provable Convergence". In: *ICML 2021*.
2020a F. Suya, J. Chi, D. Evans, Y. Tian. "Hybrid Batch attacks: Finding Black-box Adversarial Examples with Limited Queries". In: *USENIX Security 2020*.
2020b J. Wang, M. Luo, **F. Suya**, J. Li, Z. Yang, Q. Zheng. "Scalable Attack on Graph Data by Injecting Vicious Nodes". In: *ECML-PKDD 2020*.
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: *IEEE S&P (Oakland) 2019*.
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: *GlobalSIP 2016*.

Workshop Papers and Posters

2023a A. Kinfe, C. Jung, K. Lin, M. Clyburn, **F. Suya**. "HackWrt: Network Traffic-Based Eavesdropping of Handwriting". In: *CPS-IoT Week 2023*.
2023b F. Suya, X. Zhang, Y. Tian, D. Evans. "When Can Linear Learners be Robust to Indiscriminate Poisoning Attacks?" In: *ICML AdvML-Frontiers Workshop 2023*.
2022 E. Rose, **F. Suya**, D. Evans. "Poisoning Attacks and Subpopulation Susceptibility". In: *VISxAI workshop 2022 (Best Paper Award)*.
2018 F. Suya, D. Evans, Y. Tian. "Poster: Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers". In: *IEEE S&P (Oakland) 2018*.
2017 F. Suya, Y. Tian, D. Evans, P. Papotti. "Query-limited Black-box Attacks to Classifiers". In: *N(eur)IPS MLSec Workshop 2017 (Spotlight Presentation)*.

Talks and Presentations

1. An Adversarial Perspective on Machine Learning Pipeline
(Invited Talk) Warren B. Nelms Annual IoT Conference 2024, Gainesville, FL 12/2024
2. What Distributions are Robust to Indiscriminate Poisoning Attacks for Linear Learners?
NeurIPS, New Orleans, LA 12/2023
3. When Can Linear Learners be Robust to Indiscriminate Poisoning Attacks?
ICML Workshop on AdvML-Frontiers, Online 07/2023
4. Model-Targeted Poisoning Attacks with Provable Convergence
ICML, Online 07/2021
5. Hybrid Batch Attacks: Finding Black-box Adversarial Examples with Limited Queries
Usenix Security, Online 08/2020
6. Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers
IEEE S&P (Oakland), San Francisco, CA 05/2018
7. Query-limited Black-box Attacks to Classifiers
N(eur)IPS workshop on MLSec, Long Beach, CA 12/2017
8. Optimal Stochastic Power Control with Compressive CSI Acquisition for Cloud-RAN
GlobalSIP, Washington DC 12/2016

Mentoring Experience

- 2025 - Present, Sanskar Amgain, PhD student, University of Tennessee, Knoxville
- 2025 - Present, Qipan Xu, PhD student, University of Tennessee, Knoxville

Teaching Experience

- Machine learning (UTK COSC 522), Instructor — F2025
- Adversarial Machine learning (UTK COSC 594), Instructor — S2025
- Introduction to Cybersecurity (UTK COSC 366), Instructor — F2024
- 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

Grants

- Support for Affiliated Research Teams (StART), UT-Oak Ridge Innovation Institute (Amount: 100K, Funding Rate: 6%) — 2025
- AI TechX: How Machine Learning Fails in Real-World Network Anomaly Detection?, Joint-Project with Cisco Security Research (Amount: 60K) — 2025

Honors & Awards

- MC2 Postdoctoral Fellowship: awarded annually to one individual by the Maryland Cybersecurity Center (MC2) — 2023
- Outstanding/Top Reviewer: ICLR 2022, NeurIPS 2022, 2023
- CS Graduate Research Award, University of Virginia — 2018
- CS Department Fellowship, University of Virginia — 2017
- NSF Travel Grant — 2016
- CIDSE Doctoral Fellowship, Arizona State University — 2015
- Outstanding Student Scholarship, China Agricultural University — 2011 – 2013

Service

PC/Reviewer	IEEE S&P, Usenix Security, CCS, NDSS, IEEE EuroS&P, AsiaCCS, ICML, NeurIPS, ICLR, ICCV, CVPR, ECCV, AISTATS, IJCAI, AAAI
Journal Reviewer	Artificial Intelligence, TMLR

Skills

Programing	Python, PyTorch, TensorFlow, Matlab, C, C++
Languages	Mongolian (native), Mandarin, English

References

- Available upon request