Virat Shejwalkar

Contact Information

vshejwalkar@cs.umass.edu
https://people.cs.umass.edu/vshejwalkar
Github: https://github.com/vrt1shjwlkr

Interests

- Privacy, Security, and Fairness of Machine Learning and Federated Learning

Education

University of Massachusetts, Amherst Sep'17 - (Expectced Dec'22)
MS/PhD in Computer Science, GPA: 3.92/4.0
Advisor: Prof Amir Houmansadr

Indian Institute of Technology, Bombay Jul'10- Aug'15
BTech + MTech in Electrical Engineering, GPA 8.01/10 (Specialization: 9.23/10)
Thesis: Secure Scan Architectures to Prevent Side Channel Attacks
Advisor: Prof. Virendra Singh

Publications

Mitigating Membership Inference Attacks by Self-Distillation Through a Novel Ensemble Architecture [pdf]
Shinyu Tang, Saeed Mahloujifar, Liwei Song, **Virat Shejwalkar**, Milad Nasr, Amir Houmansadr and Prateek Mittal
***USENIX Security**, 2022*

Back to the Drawing Board: A Critical Evaluation of Poisoning Attacks on Federated Learning [pdf]
Virat Shejwalkar, Amir Houmansadr, Peter Kairouz, and Daniel Ramage
Conditionally accepted at IEEE Security and Privacy, 2022

Cronus: Robust Collaborative Learning Using Low-Dimensional Black Box Knowledge Transfer [pdf]
Hongyan Chang*[1], **Virat Shejwalkar***, Reza Shokri and Amir Houmansadr
*NeurIPS Workshop on New Frontiers in Federated Learning (**NFFL**), 2021*

FSL: Federated Supermask Learning [pdf]
Hamid Mozaffari, **Virat Shejwalkar**, and Amir Houmansadr
Under submission at ICLR 2022

Systematic Privacy Risk Analysis of Natural Language Processing Classification Models
Virat Shejwalkar, Huseyin Inan, Amir Houmansadr, and Robert Sim
Under submission at AAAI 2022

Manipulating the Byzantine: Optimizing Model Poisoning Attacks and Defenses for Federated Learning [pdf]
Virat Shejwalkar and Amir Houmansadr
*Networks and Distributed Systems Security (**NDSS**), 2021*
*NeurIPS Workshop on Scalability, Privacy, and Security in Federated Learning (**SpicyFL**), 2020*

Membership Privacy for Machine Learning Models through Knowledge Transfer [pdf]
Virat Shejwalkar and Amir Houmansadr
*AAAI Conference on Artificial Intelligence (**AAAI**), 2021*
*NeurIPS Workshop on Privacy Preserving Machine Learning (**PPML**), 2020*

GECKO: Reconciling Privacy, Accuracy and Efficiency in Embedded Deep Learning [pdf]
Vasisht Duddu, Antoine Boutet, and **Virat Shejwalkar**
*NeurIPS Workshop on Privacy Preserving Machine Learning (**PPML**), 2020*

Quantifying Privacy Leakage in Graph Embedding [pdf]
Vasisht Duddu, **Virat Shejwalkar**, and Antoine Boutet
***EAI MobiQuitous**, 2020*

[1] *Equal contribution

Leveraging Prior Knowledge Asymmetries in the Design of Location Privacy-Preserving Mechanisms [pdf]
Nazanin Takbiri, **Virat Shejwalkar**, Amir Houmansadr, Dennis Goeckel, and Hossein Pishro-Nik
IEEE Wireless Communications Letters, 2020

Revisiting Utility Metrics for Location Privacy Preserving Mechanisms [pdf] [code]
Virat Shejwalkar, Amir Houmansadr, Hossein Pishro-Nik and Dennis Goeckel
*In 35th ACM Annual Computer Security Applications Conference (**ACSAC**) 2019*

Work Experience

Fairness Assessment and Mitigation of Machine Learning Algorithms Sep'21 - Dec'21
Research Intern at Google Research (Advisors: Candice Schumann, Hao Wu)
- Understanding and mitigating bias due to knowledge distillation in object detection models

Privacy of Natural Language Processing Machine Learning Jun'21 - Aug'21
Research Intern at Microsoft Research (Advisors: Rober Sim, Huseyin Inan)
- Privacy leakage assessment of natural language processing models used for text classification

Privacy and Security of Machine Learning and Federated Learning Sep'17 - present
Research Assistant at University of Massachusetts, Amherst (Advisor: Prof. Amir Houmansadr)
- Working on privacy, security, and fairness of machine learning, with special focus on federated learning

Robust Aggregation Algorithms in Federated Learning May'18 - Aug'18
Visiting Researcher at National University of Singapore (Advisor: Prof. Reza Shokri)
- Introduced knowledge transfer based robust and communication efficient federated learning algorithms

FELICS - Fair Evaluation of Lightweight Cryptographic Systems Mar'17 - Aug'17
Research Associate at CryptoLux Group of University of Luxembourg (Advisor: Prof. Alex Biryukov)
- Extended FELIECS framework to benchmark lightweight authenticated encryption with associated data and hashes

Hardware countermeasures against side channel attacks Jan'17 - Mar'17
Research Assistant at Cybersecurity Group, HKUST (Advisors: Prof. Tao Wang Prof. Tim Cheng)
- Worked on security analysis of test data compression algorithms in hardware testing

WCDMA Radio Resource Control Layer Software Dev Jul'15 - Dec'16
Software Engineer at Qualcomm, Hyderabad (Advisor: Suresh Sanka)
- Worked on developing and maintaining key 3GPP features of 3G Resource Controller Layer of WCDMA protocol

Secure Scan Architectures to Prevent Side Channel Attacks Jan'15-Jun'15
Research Assistant at CADSL Lab, IIT Bombay (Advisor: Prof. Virendra Singh)
- Introduced dynamic multiple input signature register against differential input signature analysis

Scholastic Achievements

- All India rank 212 in the Joint Entrance Exam (IIT JEE), 2010 (half a million candidates)
- State Rank 92, all India rank 910 in All India Engineering Entrance Exam, 2010 (a million candidates)
- Received Merit-cum-Means scholarship awarded by IIT for two consecutive years
- Received Association of Mathematics Teachers of India scholarship (*0.1% selection*)

Relevant Courses

- Completed: Research Methods in Empirical Computer Science, Theoretical Machine Learning, Neural Networks, Advanced Algorithms, Probabilistic Graphical Models, Advanced Information Assurance, Compute Networks.

Programming Skills

- Preferred language: Python
- Deep learning frameworks: Pytorch, Tensorflow

References

- Available upon request