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

[Google Scholar]

Recycling Scraps: Improving Private Learning Using Intermediate Checkpoints [pdf]
Virat Shejwalkar, Arun Ganesh, Rajiv Matthews, Om Thakkar, Abhradeep Guha Thakurta

Backdoor Attacks on Semi-supervised Learning [pdf]
Virat Shejwalkar, Lingjuan Lyu, Amir Houmansadr.

Back to the Drawing Board: A Critical Evaluation of Poisoning Attacks on Production Federated Learning [pdf]
Virat Shejwalkar, Amir Houmansadr, Peter Kairouz, and Daniel Ramage
*IEEE Symposioum on Security and Privacy **(Oakland)**, 2022*

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*

Machine Learning with Differentially Private Labels: Mechanisms and Frameworks [pdf]
Shinyu Tang, Milad Nasr, Saeed Mahloujifar, **Virat Shejwalkar** Liwei Song,, Amir Houmansadr and Prateek Mittal
*Proceedings on Privacy Enhancing Technologies **(PETS)** Symposium, 2022*

Improving Differentially Private Deep Learning using Adaptive Origin Selection
Milad Nasr, Saeed Mahloujifar, Shinyu Tang, **Virat Shejwalkar**, Amir Houmansadr and Prateek Mittal
*ICML Workshop on Theory and Practice of Differential Privacy **(TPDP)**, 2022*

FSL: Federated Supermask Learning [pdf]
Hamid Mozaffari, **Virat Shejwalkar**, and Amir Houmansadr
FL-AAAI 2022 (Oral)

Systematic Privacy Risk Analysis of Natural Language Processing Classification Models
Virat Shejwalkar, Huseyin Inan, Amir Houmansadr, and Robert Sim
*Workshop on Privacy Preserving Machine Learning (**NeurIPS PPML**), 2021*

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

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*

Membership Privacy for Machine Learning Models through Knowledge Transfer [pdf]
Virat Shejwalkar and Amir Houmansadr

*AAAI Conference on Artificial Intelligence (**AAAI**), 2021*

Quantifying Privacy Leakage in Graph Embedding [pdf]
Vasisht Duddu, **Virat Shejwalkar**, and Antoine Boutet
***EAI MobiQuitous**, 2021*

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*

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
*Annual Computer Security Applications Conference (**ACSAC**) 2019*

Work Experience

Improving the Utility of Differentially Private Learning Pipeline Jun'22 - Present
Research Intern at Google (Collaborators: Om Thakkar, Abhradeep Guha Thakurta)

- Designed production friendly algorithms to improve the utility of differentially private training
- Designed novel algorithms to quantify uncertainty in ML models due to differential privacy noise

Fairness Assessment of Object Detection Learning Pipelines Sep'21 - Dec'21
Research Intern at Google (Collaborators: Candice Schumann, Hao Wu)

- Understanding the impact of knowledge distillation on the fairness of object detection models

Privacy of Natural Language Processing Machine Learning Jun'21 - Aug'21
Research Intern at Microsoft Research (Collaborators: Robert 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: 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 (Collaborators: 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: Alex Biryukov)

- Designed FELIECS framework to benchmark lightweight authenticated encryption algorithms

WCDMA Radio Resource Control Layer Software Dev Jul'15 - Dec'16
Software Engineer at Qualcomm, Hyderabad (Advisor: Suresh Sanka)

- Developed and maintained 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: 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

- 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, Jax, Tensorflow Federated

References

- Available upon request