Meisam Mohammady

CONTACT INFORMATION

Department of Computer Science
Iowa State University
https://www.cs.iastate.edu/people/meisam-mohammady/

Address: 232 Atanasoff--Hall, 2434 Osborn Dr
Ames, IA 50011
E-Mail:meisam@iastate.edu

RESEARCH INTERESTS

Differential Privacy, Secure Federated Learning, Anonymity, Computational Learning Theory, Secure Multiparty Computation, Fairness

EDUCATION

Concordia University, Montréal, Canada
Ph.D. in *Information Systems Engineering* November 2020
Dissertation: Novel Approaches to Preserving Utility in Privacy Enhanced Technologies
Distinguished Doctoral Dissertation Prize Winner in the Category of the Natural Science and Engineering
Advisors: Prof. Lingyu Wang & Prof. Yuan Hong

École Polytechnique de Montréal, Montréal, Canada
M.Sc. in *Electrical & Computer Engineering* May 2015
Thesis: Differentially Private Event Stream Filtering with an Application to Traffic Estimation
Advisor: Prof. Jerome Le Ny

Sharif University of Technology
B.Sc. in *Electrical & Computer Engineering* September 2012
Thesis: Backstepping Controlling of Four-wheel Mobile Robots
Advisor: Prof. Mehrzad Namvar

PROFESSIONAL EXPERIENCE

Assistant Professor October 2022 to Present
Department of Computer Science
Iowa State University, Ames, IA, USA

Research Scientist October 2020 to October 2022
Data61
CSIRO, Sydney, Australia

Applied Researcher May 2015 to September 2020
Ericsson Research Canada
Concordia University, Montréal, QC, Canada

Applied Researcher January 2013 to 2015
The Group for Research in Decision Analysis (GERAD)
Department of Electrical Engineering
École Polytechnique Montréal, Montréal, QC, Canada

RESEARCH GRANTS

Awarded Grants

- **Data 61 PhD Scholarship Grant**
  "Sub-optimal but Comprehensive Approach for AI with Differential Privacy and

Fairness"
Role: **PI**. Project Duration: 08/01/2021-08/31/2025. Awarded Amount: $55,000 per annum

- **Vacation Students Scholarship Grant**
  "Utility-driven Statistical Inference Engine with Local Differential Privacy"
  Role: **PI**. Project Duration: 12/01/2021-03/31/2022. Awarded Amount: $22,000 (CSIRO Data 61, Pawsey Supercomputing)

REFEREED PUBLICATIONS

[1] Qin Yang*, **Meisam Mohammady***, Han Wang, Ali Payani, Ashish Kundu, Kai Shu, Yan Yan, Yuan Hong. LMO-DP: Optimizing the Randomization Mechanism for Differentially Private Fine-Tuning Language Models. To be presented at the 2024 International Conference on Machine Learning (ICML'24). *Equal Contribution (Co-First Authors).

[2] Shuya Feng*, **Meisam Mohammady***, Han Wang, Xiaochen Li, Zhan Qin, Yuan Hong. *DPI: Ensuring Strict Differential Privacy for Infinite Data Streaming.* The 45th IEEE Symposium on Security and Privacy (S&P' 24). *Acceptance rate:* 202/1389 ∼ 14.5%. *Equal Contribution (Co-First Authors).

[3] Pathum Chamikara Mahawaga Arachchige, Seung Ick Jang, Ian Oppermann, Dongxi Liu, Musotto Roberto, Sushmita Ruj, Arindam Pal, **Meisam Mohammady**, Seyit Camtepe, Sylvia Young, Chris Dorrian, Nasir David. *Towards Usability of Data with Privacy: A Unified Framework for Privacy-Preserving Data Sharing with High Utility.* The 24th Privacy Enhancing Technologies Symposium (PETS'24), *Acceptance rate:* 55/284 ∼ 19.1%.

[4] Thirasara Ariyarathna, **Meisam Mohammady**, Hye-Young (Helen) Paik and Salil S Kanhere. *VLIA: Navigating Shadows with Proximity for Highly Accurate Visited Location Inference Attack against Federated Recommendation Models.* The 19th ACM ASIA Conference on Computer and Communications Security (ASIACCS'24). *Acceptance rate:* 55/284 ∼ 19%.

[5] Thirasara Ariyarathna, **Meisam Mohammady**, Hye-Young (Helen) Paik and Salil S Kanhere. *User GPS Trajectory Reconstruction from Federated Route Recommendation Models.* ACM Transactions on Intelligent Systems and Technology (ACM TIST'24). *IF: 10.489.*

[6] Kane Walter, **Meisam Mohammady**, Surya Nepal, Salil S. Kanhere. *Mitigating Distributed Backdoor Attack in Federated Learning Through Mode Connectivity.* The 19th ACM ASIA Conference on Computer and Communications Security (ASIACCS'24). *Acceptance rate:* 55/284 ∼ 19%.

[7] G Thedchanamoorthy, M Bewong, **M Mohammady**, TA Zia, MZ Islam. *Optimization of UD-LDP with statistical prior knowledge.* The 22nd International Conference on Pervasive Computing and Communications (PerCom 2024).

[8] Kane Walter, **Meisam Mohammady**, Surya Nepal, Salil S. Kanhere. *Optimally Mitigating Backdoor Attacks in Federated Learning.* The IEEE Transactions on Dependable and Secure Computing (TDSC' 23) (IF: 7.3).

[9] **Meisam Mohammady**, Reza Arablouei. *Efficient Privacy-Preserved Processing of Multimodal Data for Vehicular Traffic Analysis.* The 2023 Symposium on Vehicles Security and Privacy (VehicleSec'23).

[10] **Meisam Mohammady**, Momen Oqaily, Lingyu Wang, Yuan Hong, Habib Louafi, Makan Pourzandi and Mourad Debbabi. "A Multi-view Approach to Preserve Both Privacy and Utility in Network Trace Anonymization." *ACM Transactions on Privacy and Security (**TOPS**) (formerly known as TISSEC)*, Published, 2020.

[11] Shangyu Xie, **Meisam Mohammady**, Han Wang, Yuan Hong, Lingyu Wang, and Jaideep Vaidya. "Generalizing Prefix-Preserving Data Outsourcing: Ensuring both Privacy and Utility." *IEEE Transactions on Knowledge and Data Engineering (**TKDE**)*, Published , 2020.

[12] **Meisam Mohammady**, Shangyu Xie, Yuan Hong, Mengyuan Zhang, Lingyu Wang, Makan Pourzandi, Mourad Debbabi."R^{2}DP: A Universal and Automated Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions."*ACM Conference on Computer and Communications Security (**CCS' 20**)*, Published, 2020 [Acceptance rate: 11%].

[13] Momen Oqaily, Yosr Jarrya, **Meisam Mohammady**, Suryadipta Majumdar, Lingyu Wang, Makan Pourzandi and Mourad Debbabi, " SegGuard: Protecting Audit Data Using Segmentation-based Anonymization for Multi-tenant Cloud Auditing." *IEEE Transactions on Dependable and Secure Computing (**TDSC**)*, Published, 2019 [impact factor: 6.864].

[14] Bingyu Liu, Shangyu Xie, Han Wang, Yuan Hong, Xuegang Ban, **Meisam Mohammady**. "VTDP: Privately Sanitizing Fine-grained Vehicle Trajectory Data with Boosted Utility." *IEEE Transactions on Dependable and Secure Computing (**TDSC**)*, Published, 2019 [impact factor: 6.864].

[15] Suryadipta Majumdar, Azadeh Tabiban, **Meisam Mohammady**, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang and Mourad Debbabi."Proactivizer: Transforming Existing Verification Tools into Efficient Solutions for Runtime Security Enforcement." In *Proceedings of the 24th European Symposium on Research in Computer Security (**ESORICS' 19**)*, Published, 2019, [Acceptance rate: 19.5%].

[16] Suryadipta Majumdar, Azadeh Tabiban, **Meisam Mohammady**, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang and Mourad Debbabi."Multi-Level Proactive Security Auditing for Clouds." In *Proceedings of the 2019 IEEE Conference on Dependable and Secure Computing (**DSC' 19**)*, Published 2019.

[17] **Meisam Mohammady**, Lingyu Wang, Yuan Hong, Habib Louafi, Makan Pourzandi and Mourad Debbabi. "Preserving Both Privacy and Utility in Network Trace Anonymization." In *Proceedings of the 25th ACM Conference on Computer and Communications Security (**CCS' 18**)*, Published, 2018 [Acceptance rate: 16.5%].

[18] Jerome Le Ny and **Meisam Mohammady**. "Differentially private MIMO filtering for event streams." *IEEE Transactions on Automatic Control*, Published, 2018 [impact factor: 5.625].

[19] Jerome Le Ny and **Meisam Mohammady**. "Differentially private MIMO filtering for event streams and spatio-temporal monitoring." In *Proceedings of the 53rd IEEE Conference on Decision and Control (**CDC' 14**)*, Published, 2014 [H Index: 118].

UNDER REVIEW & SUBMISSION

[1] Kane Walter, **Meisam Mohammady**, Surya Nepal and Salil Kanhere."No Free Lunch in Federated Learning: Larger Model Size Increases Backdoor Attack Surface."*IEEE Transactions on Dependable and Secure Computing (**TDSC**' 22)*, Under Review.

[2] **Meisam Mohammady**, Han Wang, Yuan Hong, Mengyuan Zhang, Suryaipta Majumdar, Lingyu Wang, Makan Pourzandi and Mourad Debbabi. "DPOAD: Differentially Private Outsourcing of Anomaly Detection with Optimal Sensitivity Learning." *ACM Conference on Computer and Communications Security (**CCS' 22**)*, Under Review.

[3] **Meisam Mohammady**, Dongxi Liu, Surya Nepal and Salil Kanhere. "Accurate Statistical Inference in Piece-wise Applications Under Differential Privacy." *44rd IEEE Symposium on Security and Privacy **S&P' 23***, To be Submitted.

[4] **Meisam Mohammady**, Surya Nepal and Salil Kanhere. "Sub-optimal Tool for AI with Differential Privacy and Fairness." *Thirty-sixth Conference on Neural Information Processing Systems **NeurIPS' 22***, To be Submitted.

Patents

[1] **Meisam Mohammady**, Han Wang, Yuan Hong, Mengyuan Zhang, Suryaipta Majumdar, Lingyu Wang, Makan Pourzandi and Mourad Debbabi. *Dpod: differentially private outsourcing of anomaly detection.* US Patent App. 18/005,761, 2023.

[2] Mengyuan Zhang, Yosr Jarraya, Makan Pourzandi, **Meisam Mohammady**, XIE Shangyu, Yuan Hong, Lingyu Wang, Mourad Debbabi. *Utility optimized differential privacy system.* US Patent App. 17/610,795, 2022.

[3] **Meisam Mohammady**, Yosr Jarraya, Lingyu Wang, Mourad Debbabi and Makan Pourzandi. *Partition-based prefix preserving anonymization approach for network traces containing ip addresses.* US Patent 11,316,831, 2022.

Supervision

Mr. Kane Walter Ph.D., the University of New South Wales jointly with Dr. Surya Nepal and Dr. Salil Kanhere
Mr. Gnanakumar Thedchanamoorthy Ph.D., the Charles Sturt University jointly with Dr. Zahid Islam
Mr. Thirasara Ariyaratna Ph.D., the University of New South Wales jointly Co-supervisors: Dr. Salil Kanhere Dr. Qinghua Lu, CSIRO's Data61 and Dr. Helen Paik, Commenced in October 2020.
Hrishi Masurkar Honorary, the University of New South Wales jointly with Dr. Clement Cannone

Invited Talks

[1] "Preserving Both Privacy and Utility in Network Trace Anonymization", Université du Québec à Montréal (UQAM), Montréal, Canada, November 22, 2019

[2] "R^{2}DP: A Universal Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions", Université du Québec à Montréal (UQAM), Montréal, Canada, November 22, 2019

[3] "DP-IDS: Differentially Private Intrusion Detection System ", Security, Privacy and Forensics (SPF) seminars, Montréal, Canada, May 10, 2019

[4] "R^{2}DP: A Universal Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions", The CSIRO, Data61 Reading seminar, Sydney, Australia, November 22, 2020

[5] Novel Approaches to Preserving Utility in Privacy Enhancing Technologies, Discovery Partners Institute (DPI) RD Seminar, Chicago, IL, USA, September 9, 2021

Demonstrations

"Preserving Both Privacy and Utility in Network Trace Anonymization", Ericsson Security Research, Montréal, Canada, May, 2018

"R^{2}DP: A Universal and Automated Approach to Optimizing the Randomization Mechanisms of Differential Privacy for Utility Metrics with No Known Optimal Distributions", Ericsson Security Research, Montréal, Canada, October, 2019

"DPOAD: Differentially Private Outsourcing of Anomaly Detection with Optimal Sensitivity Learning", Ericsson Security Research, Montréal, Canada, October, 2020

Awards

Recognized as Global Talent by Australian Government and Being Granted with Citezinship 2021
PhD Dissertation selected as Concordia University nominee for both of CAGS and ADESAQ Competitions 2021
Distinguished PhD Dissertation Awards, Concordia University 2020
Student Travel Grant/Award 2018, 2019
Tuition Award of Excellence ($ 41,313), Concordia University 2017
Tuition Exemption Award ($ 15,000), École Polytechnique Montréal 2014

Professional Activities

TPC Member

- CM Conference on Computer and Communications Security (CCS'23)
- The Journal Proceedings on Privacy Enhancing Technologies (PoPETs'21,22,24)
- IEEE Transactions on Dependable and Secure Computing (TDSC' 19,20,21)
- the Thirty-Sixth AAAI Conference on Artificial Intelligence (AAAI' 22)
- IEEE Transactions on Services Computing (TSC' 21)

Publicity Chair

- The 2021-2 Privacy Enhancing Technologies Symposium (PETS 2021)
- The CRC Security Automation and Orchestration (SAO) Seminar Series 2021
- The 2021 workshop on Cloud S&P

Journal External Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Automatic Control
- Journal of Information Sciences
- Transaction on Management Information Systems
- IEEE Transactions on Parallel and Distributed Systems (TPDS)
- Information Systems Research (ISR), INFORMS
- Journal of Computer Security (JCS), IOS Press

Conference External Reviewer

- IEEE International Conference on Computer Communications (INFOCOM)
- The European Symposium on Research in Computer Security (ESORICS)
- IEEE International Conference on Data Engineering (ICDE)
- International Conference on Distributed Computing Systems (ICDCS)
- International Information Security and Privacy Conference (SEC)
- International Conference on Applied Cryptography and Network Security (ACNS)

- IEEE International Conference on Communications (ICC)
- IEEE Conference on Network Softwarization (IEEE NetSoft)
- IEEE International Conference on Cloud Networking (CloudNet)

Membership

- Association for Computing Machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)

Teaching

University of Waterloo

CS 458/658 (Computer Security and Privacy): Instructor, Spring'21

Concordia University

INSE 6130 (Operating System Security): TA/POD, Winter'20
INSE 6620 (Cloud Computing Security and Privacy): TA/POD, Winter'18
INSE 6160 (Database Security and Privacy): Guest lecture, Summer'18

Sharif University Of Technology

Linear Control Systems: Fall'10, and Fall'12
Communication Systems I: Fall'11

Media Coverage

[1] Talk on "Preserving Both Privacy and Utility in Network Traces" appeared in ACM.

[2] Talk on "R^2DP: A Universal Approach to Optimizing the Randomization Mechanisms of
Differential Privacy for Utility Metrics with No Known Optimal Distributions" appeared in ACM.

References

Dr. Lingyu Wang

Professor and NSERC/Ericsson Senior Industrial Research Chair (IRC) in SDN/NFV Security, Concordia Institute for Information Systems Engineering (CIISE), Montréal, QC, Canada, E-Mail: wang@ciise.concordia.ca

Dr. Yuan Hong

Assistant Professor, Department of Computer Science and Engineering, University of Connecticut, CT 06269, IL, E-Mail: yuan.hong@uconn.edu

Dr. Makan Pourzandi

Research Leader, Ericsson Security Research Canada, and Affiliate Associate Professor at Concordia Institute for Information Systems Engineering (CIISE), Montréal, QC, Canada, E-Mail:makan.pourzandi@ericsson.com

Dr. Salil Kenhere

Professor, School of Computer Science and Engineering, UNSW, Sydney, E-Mail: salil.kanhere@unsw.edu.au