Bangalore, India
mukherjeeprateeti01@gmail.com | t-pmukherjee@microsoft.com
LinkedIn : https://www.linkedin.com/prateeti
Github : https://github.com/Prateeti98
Website: https://prateeti98.github.io

Prateeti Mukherjee

Research Fellow, Microsoft Research India

Education

Institute of Engineering and Management, India
Major in Computer Science and Engineering *Aug' 17 - Jun' 21*
GPA: 9.5/10

Research Interests

Machine Learning, Differential Privacy, Online Learning, Causality, Information Theory

Experience

Microsoft Research India *Aug '21 - Present*
Research Fellow Advisor: Satya Lokam

Amazon India *Feb '21 - Jul '21*
Software Development Engineer Intern

Aalto University, Finland *Jun '20 - Jan '21*
Research Assistant Advisors: Yki Kortesniemi, Dmitrij Lagutin, Raimo Kantola

University of Turku, Finland *March '20 - May '20*
Research Assistant Advisor: Tomi Westerlund

Hankuk University of Foreign Studies (HUFS), South Korea *June '19 - Aug '19*
Summer Research Intern Advisor: Dhananjay Singh

Selected Publications

Prateeti Mukherjee, Satya Lokam, "Non-Asymptotic Lower Bounds for Data Reconstruction Attacks" [*Under Review*][Link]

Prateeti Mukherjee, Sayak Ray Chowdhury, Satya Lokam, "On the Query Complexity of Class-Adaptive Auditing" [*In preparation*]

Andrea Lisi*, **Prateeti Mukherjee***, Laura De Santis, Lei Wu, Dmitrij Lagutin, Yki Kortesniemi, "Automated Responsible Disclosure of Security Vulnerabilities" *IEEE Access 2021* [Link]

Victor Sarker*, **Prateeti Mukherjee***, Tomi Westerlund "Enhanced Reliability of Mobile Robots with Sensor Data Estimation at Edge" *IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT) 2020* [Link]

Prateeti Mukherjee, Amartya Mukherjee, Nilanjan Dey, Debashis De, "QoS-aware edge-assisted IoDT for real-time stride analysis" *Computers and Electrical Engineering 2021* [Link]

** indicates equal contribution*

Selected Projects

Non-Asymptotic Lower Bounds for Data Reconstruction Attacks
Satya Lokam (MSR India) *Sep '22 - Jan '23*

- Derived non-asymptotic minimax lower bounds on the reconstruction error of computationally unrestricted whitebox *Data Reconstruction Adversaries* (DRAs) on ϵ-DP learning algorithms.
- Extended the analysis of DRAs to *Lipschitz Privacy*, a generalization of DP that accounts for the underlying metric structure of the data beyond the Hamming metric, and demonstrated that our analysis covers the high-dimensional regime.
- Extended the privacy analysis of common mechanisms for differential privacy, such as the Gaussian mechanism, and learning algortihms, such as DP-SGD and Projected Noisy SGD, to cover the broader notion of Lipschitz privacy.

Pure Exploration for Class-Adaptive ML Audits

Satya Lokam (MSR India) *Nov '22 - Present*

- Developing a *class-adaptive* framework for auditing the privacy guarantees of ϵ-DP algorithms.
- Proposed framework converts the claimed DP guarantee into an equivalent failure probability guarantee for a relevant class of adversarial attacks chosen by the auditor to assess the algorithm.
- Derives query complexity lower bounds and optimal auditing strategies by reformulating the problem as *pure exploration* in a Multi-Armed Bandit setting.

Identifying Best Interventions in Causal Bandits

Gaurav Sinha (MSR India) *Feb '23-Present*

- Working on causal bandit problems with a particular focus on the best arm setting, where each arm is a soft intervention in the causal graph, with known topology but unknown interventional distributions.

Confidential Computing for Trustworthy Data Governance

Satya Lokam, Pantazis Deligiannis, Akash Lal,
Kapil Vaswani (MSR India) [Code] *Aug '21-Sep '22*

- Worked in collaboration with Microsoft product teams, iSpirit, and Sahamati (a nonprofit foundation) to enable trustworthy and secure data governance in adherence to India's Data Empowerment and Protection Architecture (DEPA).
- Automated financial information processing in adherence to data protection policies, operating in a novel hardware-assisted privacy construct called Confidential Clean Rooms. Extended the implementation to cover scenarios in the Ads space.
- Further strengthened security guarantees of the platform by incorporating differentially private transformations to input data via multiplicative weight updates with exponential mechanism.

Self-Service Tool for On-boarding in Amazon Payment Products

Siddhi Gauns (Amazon India) *Feb '21-July '21*

- Developed an interactive and secure self-service tool for Banking clients to seamlessly on-board Amazon's Rewards and Benefits Platform.
- Was one of the few interns to deliver a complete product, from ideation to launch, within a 6-month period. Awarded full-time position from Amazon Payment Products.

Interledger Support for Automated Responsible Disclosure and Bug Bounty Payments

Prof. Raimo Kantola (Aalto University, Finland) [Paper][Code] *Jun '20-Jan '21*

- Built a novel platform for the automated disclosure of vulnerabilities, detected as part of bug-bounty programs, within a transparent, traceable, and secure ecosystem.
- Created Interledger to enable cross-platform data transfer between multiple public and private DLTs, allowing Fabric and Ethereum networks to co-exist in a single solution.
- Paper published at *IEEE Access 2021.*

Efficient Recursive Bayesian Estimation for Sensor Data Reconstruction at Edge

Prof. Tomi Westerlund (University of Turku, Finland) [Paper] *Mar '20-May '20*

- Designed and implemented Sequential Approximate Bayesian Inference Algorithms for sensor data retrieval in multi-agent environments comprising of low-power embedded devices.
- Paper published at *IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT) 2020*

Skills

Languages: *Proficient*: C++, Python, Rust, Rego, TypeScript *Familiar*: Go, Solidity
Deep Learning Frameworks: Pytorch, Tensorflow, Keras
Data Science Libraries: NumPy, Pandas, Scipy, Scikit-Learn, Matplotlib, Seaborn
Tools and Technologies: Azure, AWS Lambda, Coral, Hyperledger Fabric, CouchDB, IBM Cloudant, Ethereum, MapReduce, Onnx
Utilities: Linux Shell, Git, VSCode, Docker, Kubernetes, Amazon Web Services (AWS), Amazon Mechanical Turk, LaTeX

Relevant Coursework

Computer Science	Principles of Computer Programming, Algorithms I & II , Formal Languages and Automata Theory, Cryptography, Software Tools
Information Theory and Statistics	Information Theory, Communication and Coding Theory, Artificial Intelligence
Mathematics	Real Analysis, Linear Algebra & ODE, Discrete Mathematics, Numerical Methods, Operations Research

Reference List

- **Satya Lokam**
  Principal Researcher, Microsoft Research India
  "Vigyan", No. 9, Lavelle Road, Bengaluru, Karnataka, 560 001, India

  satya@microsoft.com
  (+91) 80 6658 6000

- **Yki Kortesniemi**
  Research Fellow, Aalto University Dept. Communications and Networking
  A207, Konemiehentie 2, 00076 Finland

  yki.kortesniemi@aalto.fi
  (+358)45 203 1255

- **Dmitrij Lagutin**
  Research Fellow, Aalto University Dept. Communications and Networking
  A125, Konemiehentie 2, 00076 Finland

  dmitrij.lagutin@aalto.fi
  (+358)50 367 6759