Meenatchi Sundaram Muthu Selva Annamalai

✉ *meenatchi.annamalai.22@ucl.ac.uk*
https://msundarmsa.github.io
https://github.com/msundarmsa

Professional Experience

2021 Jun — 2022 Aug **Research Engineer**, Institute for Infocomm Research.
Conducted research on privacy attacks against synthetic data and secure federated bio-analytics.

Education

2022 Sep — **PhD Computer Science & Engineering**, *University College London*, United Kingdom.

2018 Sep — 2021 Jun **BEng Computing**, *Imperial College London*, United Kingdom.
First Class Honours

Honors and Awards

2021 **Winton Capital Applied Undergraduate Project Computing Prize**, *Best final year project*.

2021 **Governors' Prize**, *Best overall student performance*.

2019 — 2021 **Dean's List Years 1 to 3**, *Top 10% of year*.

2016 **National Science Scholarship (BS-PhD)**, *Full overseas scholarship from Bachelor's to PhD*.

Internships

2020 Jun — 2020 Aug **Undergraduate Research Opportunities Programme**, Imperial College London.
Designed and created interactive re-identification risk assessment tool for real-world data collections.

2019 Jun — 2019 Aug **8 Week Research Attachment**, Institute for Infocomm Research.
Conducted research on secure training of LSTMs using HE.

Publications

To Shuffle or not to Shuffle: Auditing DP-SGD with Shuffling, *Under Review*.
Annamalai MSMS, Balle B, De Cristofaro E, Hayes J.

The Importance of Being Discrete: Measuring the Impact of Discretization in End-to-End Differentially Private Synthetic Data, *Under Review*.
Ganev G, **Annamalai MSMS**, Mahiou S., De Cristofaro E.

Understanding the Impact of Data Domain Extraction on Synthetic Data Privacy, *SynthData @ ICLR 2025*.
Ganev G, **Annamalai MSMS**, Mahiou S., De Cristofaro E.

The Elusive Pursuit of Replicating PATE-GAN: Benchmarking, Auditing, Debugging, *Transactions on Machine Learning Research (TMLR 2025)*.
Ganev G, **Annamalai MSMS**, De Cristofaro E.

Beyond the Crawl: Unmasking Browser Fingerprinting in Real User Interactions, *The Web Conference (WWW 2025)*.
Annamalai MSMS, De Cristofaro E., Bilogrevic I.

Nearly Tight Black-Box Auditing of Differentially Private Machine Learning, *In 38th Annual Conference on Neural Information Processing Systems (NeurIPS 2024)*.
Annamalai MSMS, De Cristofaro E.

It's Our Loss: No Privacy Amplification for Hidden State DP-SGD With Non-Convex Loss, *In 17th ACM Workshop on Artificial Intelligence and Security (AISec 2024)*.
Annamalai MSMS.

"What do you want from theory alone?" Experimenting with Tight Auditing of Differentially Private Synthetic Data Generation, *In 33rd USENIX Security Symposium (USENIX Security 2024)*.
Annamalai MSMS, Ganev G, De Cristofaro E.

A Linear Reconstruction Approach for Attribute Inference Attacks against Synthetic Data, *In 33rd USENIX Security Symposium (USENIX Security 2024)*.
Annamalai MSMS, Gadotti A, Rocher L.

FP-Fed: Privacy-Preserving Federated Detection of Browser Fingerprinting, *In 31st Network and Distributed System Security Symposium (NDSS 2024)*.
Annamalai MSMS, Bilogrevic I, De Cristofaro E.

CoVnita, an end-to-end privacy-preserving framework for SARS-CoV-2 classification., *In Scientific Reports 13*.
Sim JJ, Zhou W, Chan FM, **Annamalai MSMS**, Deng X, Tan BHM, Aung KMM.

Communication-Efficient Secure Federated Statistical Tests from Multiparty Homomorphic Encryption., *In Applied Sciences 12*.
Annamalai MSMS, Jin C, Aung KMM.

Pool Inference Attacks on Local Differential Privacy, *In 31st USENIX Security Symposium (USENIX Security 2022)*.
Gadotti A, Houssiau F, **Annamalai MSMS**, de Montjoye YA.

The Observatory of Anonymity: An Interactive Tool to Understand Re-Identification Risks in 89 countries, *In Companion Proceedings of the Web Conference 2021 (pp. 687-689)*.
Rocher L, **Muthu MS**, de Montjoye YA.

Privacy Preserving Collective Learning with Homomorphic Encryption, *In IEEE Access*.
Paul J, **Annamalai MSMS**, Ming W, Al Badawi A, Veeravalli B, Aung KMM.

Service

2025 **Reviewer for The Web Conference (WWW)**.

Teaching

Undergraduate Teaching Assistant

2021 **Discrete Structures, Logic, Reasoning about Programs and Graphs and Algorithms**, *Imperial College London*.
Conducted weekly tutorial sessions and graded homework

Presentations

2024 **Thinking Inside the Box: How Private is Black-Box DP-SGD?**.
Microsoft Research, Cambridge

2024 **(Open) Challenges in Evaluating Synthetic Data**.
National University of Singapore

2024 **(Open) Challenges in Deploying and Evaluating PETS**.
University of California, Riverside

Personal Projects

2022 **STASYS**.
Created a cross-platform open source aim tracing application for air pistol/air rifle targets using OpenCV, React, Typescript and Rust. https://github.com/msundarmsa/stasys-tauri

2022 **Solli**.
Created a Wordle clone in Tamil using Vue and Javascript. https://github.com/msundarmsa/wordle-tamil-src

2013 **Encrichment Science and Training Programme**.
Developed mobile app to enhance classroom learning.

2011 **Special Programme in Enquiry and Research**.
Programmed a hygenic, non-touch interface for feedback systems deployed in unsanitary locations using Microsoft Kinect.

Computer skills

Languages: Python, Typescript/Javascript, Go, Rust, C/C++, Java, Haskell, Elixir

Experiences in: Software engineering and design, Secure multiparty computation (MP-SPDZ), Homomorphic encryption (Lattigo, Microsoft SEAL), Web, mobile and desktop applications, Multiprocess parallel programming, Machine Learning/Deep Learning, Numerical integration

Extra-curriculars

2019 **Major Event Officer of Imperial College Singapore Society**.
Produced a student-written and performed full-length musical

2014 **Vice President of IT & Innovation Club**.
Organized and taught programming courses and workshops for members, lead teams in competitions and managed club's administrative affairs