# Aastha Mehta

*Assistant Professor (tenure-track)*
*Computer Science Department, University of British Columbia, Vancouver*

*aasthakm@gmail.com*
*aasthakm.github.io*

## Education

2012 – 2020 **Ph.D. in Computer Science (Summa Cum Laude)**
Max Planck Institute for Software Systems (MPI-SWS), Saarbrücken, Germany
and Saarland University (UdS), Saarbrücken, Germany
Advisors: Peter Druschel, Deepak Garg
Thesis: Ensuring Compliance with Data Privacy and Usage Policies in Online Services

2007 – 2011 **B.E. (Hons.) in Computer Science**
Birla Institute of Technology and Science (BITS) Pilani, Pilani Campus, India

## Work Experience

2021 – **Assistant Professor (tenure-track)**
Computer Science Department, University of British Columbia, Vancouver, Canada

2020 – 2021 **Postdoctoral Researcher (Nov 2020 – Feb 2021)**
Max Planck Institute for Software Systems (MPI-SWS), Saarbrücken, Germany
Advisor: Peter Druschel
Focus Area: Privacy-preserving digital contact tracing for epidemic risk mitigation

2015 **Research Intern (three months)**
Systems and Networking Group, Microsoft Research, Cambridge, UK
Mentor: Manuel Costa
Focus areas: Secure multiparty computation in the Cloud, and designing oblivious ML algorithms.

2011 – 2012 **Member of Technical Staff**
NetApp Inc., Bengaluru, India
Manager: Paramita Das
Focus areas: Optimizing performance of the WAFL (Write Anywhere File Layout) file system checker.

2011 **Intern (six months)**
Advanced Technology Group, NetApp Inc., Bengaluru, India
Mentor: Ajay Bakre and Priya Sehgal
Focus areas: Improving the capacity utilization in Hadoop storage clusters.

2010 **Summer Research Intern (three months)**
MPI-SWS, Saarbrücken, Germany
Mentor: Peter Druschel
Focus areas: Deterministic record and replay for multicore systems.

## Grants

2025 – 2028 **National Cybersecurity Consortium**, lead PI
ICS Security in the Age of Industry 4.0

2023 – 2026 **NSERC Alliance**, co-PI
Transformative server architectures for next-generation AI systems

2022 – 2025 **Intel (Transformative Server Architectures)**, co-PI
Blended systems: Building Efficient and Secure Next-Generation Datacenter Hardware and Software

2022 – 2025 **DND IDEaS Innovation Network**, co-PI
A Platform for Secure and Dependable Hierarchical Edge Processing on 5G

2022 – 2023 **UBC STAIR Grant**, lead PI
Serverless Should Not Be Privacy-Less

2021 – 2024 **DND/NSERC Discovery Grant Supplement**, PI
Mitigating Side-Channel Leaks in Next-Generation Cloud Systems

2021 – 2026 **NSERC Discovery Grant**, PI
Mitigating Side-Channel Leaks in Next-Generation Cloud Systems

## Honors and Awards

2018 **Invited to Rising Stars Workshop in EECS**
One of 76 women researchers in Computer Science, and one out of only 3 from Europe selected to attend this academic career workshop.

2016 **Invited to the 4$^{th}$ Heidelberg Laureate Forum**
One of 200 young researchers selected to attend the forum. Also awarded Romberg travel grant fellowship, which covered the travel expenses.

## Publications

### Peer Reviewed

PLOS'25 **Comparing Isolation Mechanisms with OSmosis**
Sidhartha Agrawal, Shaurya Patel, Linh Pham, Arya Stevinson, Ilias Karimalis, Hugo Lefeuvre, **Aastha Mehta**, Reto Achermann, Margo Seltzer
Workshop on Programming Languages and Operating Systems (PLOS), Seoul, Korea

USENIX Security'25 **Relocate-Vote: Using Sparsity Information to Exploit Ciphertext Side-Channels**
Yuqin Yan, Wei Huang, Ilya Grishchenko, Gururaj Saileshwar, **Aastha Mehta**, David Lie
USENIX Security Symposium, Philadelphia, USA

S&P'25 **Growlithe: A Developer-Centric Compliance Tool for Serverless Applications**
Praveen Gupta, Arshia Moghimi, Devam Sisodraker, Mohammad Shahrad, **Aastha Mehta**
IEEE Oakland S&P, San Francisco, USA

RICSS'25 **Targeting the Blind Spot: Evaluating Modern ICS Security Against A Novel Denial of Service (DoS) Attack**
Gargi Mitra, Pritam Dash, Elaine Yao, **Aastha Mehta**, Karthik Pattabiraman
Workshop on Re-design Industrial Control Systems with Security (RICSS), Salt Lake City, USA

USENIX Security'24 **NetShaper: A Differentially Private Network Side-Channel Mitigation System**
Amir Sabzi, Rut Vora, Swati Goswami, Margo Seltzer, Mathias Lécuyer, **Aastha Mehta**
USENIX Security Symposium, Philadelphia, USA

EdgeSys'24 **Stream Processing with Adaptive Edge-Enhanced Confidential Computing**
Yuqin Yan, Pritish Mishra, Wei Huang, **Aastha Mehta**, Oana Balmau, David Lie
Workshop on Edge Systems, Analytics and Networking (EdgeSys), Athens, Greece

PriSC'24 **Michroarchitectural Side-Channel Mitigations for Serverless Applications**
Yayu Wang, **Aastha Mehta**
Workshop on Principles of Secure Compilation (PriSC) 2024, London, UK

PLAS'23 **Michroarchitectural Side-Channel Mitigations for Serverless Applications**
Yayu Wang, **Aastha Mehta**
Workshop on Programming Languages and Analysis for Security (PLAS), Copenhagen, Denmark

USENIX Security'22 **Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud**
**Aastha Mehta**, Mohamed Alzayat, Roberta De Viti, Björn B. Brandenburg, Peter Druschel, Deepak Garg
USENIX Security Symposium, Boston, USA

Scientific Reports, 2022 **Listening to Bluetooth Beacons for Epidemic Risk Mitigation***
Gilles Barthe, Roberta De Viti, Peter Druschel, Deepak Garg, Manuel Gomez-Rodriguez, Pierfrancesco Ingo, Heiner Kremer, Matthew Lentz, Lars Lorch, **Aastha Mehta**, Bernhard Schölkopf
(*Authors listed in alphabetical order)

USENIX Security'17 **Qapla: Policy compliance in database-backed systems**
**Aastha Mehta**, Eslam Elnikety, Katura Harvey, Deepak Garg, Peter Druschel
USENIX Security Symposium, Vancouver, Canada

USENIX Security'16 **Thoth: Comprehensive Policy Compliance in Data Retrieval Systems**
Eslam Elnikety, **Aastha Mehta**, Anjo Vahldiek-Oberwagner, Deepak Garg, Peter Druschel
USENIX Security Symposium, Austin, USA

USENIX Security'16 **Oblivious Multi-Party Machine Learning on Trusted Processors**
Olga Ohrimenko, Felix Schuster, Cédric Fournet, **Aastha Mehta**, Sebastian Nowozin, Kapil Vaswani, Manuel Costa
USENIX Security Symposium, Austin, USA

EuroSys'15 **Guardat: Enforcing data policies at storage layer**
Anjo Vahldiek-Oberwagner, Eslam Elnikety, **Aastha Mehta**, Deepak Garg, Peter Druschel, Ansley Post, Rodrigo Rodrigues, Johannes Gehrke
European Conference on Computer Systems (EuroSys), Bordeaux, France

HiPC'11 **HDFS Space Consolidation**
**Aastha Mehta**, Deepti Banka, Kartheek Muthyala, Priya Sehgal, Ajay Bakre
Student Research Symposium, International Conference on High Performance Computing (HiPC)

### Non-Peer Reviewed

2025 **LDPKiT: Recovering Utility in LDP Schemes by Training with Noise^2**
Kexin Li, Yang Xi, **Aastha Mehta**, David Lie

2024 **ICS-Sniper: A Targeted Blackhole Attack on Encrypted ICS Traffic**
Gargi Mitra, Pritam Dash, Elaine Yao, **Aastha Mehta**, Karthik Pattabiraman

2022 **Reconciling Security & Utility in Next-Generation Epidemic Risk Mitigation Systems**
Pierfrancesco Ingo, Nichole Boufford, Ming Cheng Jiang, Rowan Lindsay, Roberta De Viti, Matthew Lentz, Gilles Barthe, Manuel Gomez-Rodriguez, Bernhard Schölkopf, Deepak Garg, Peter Druschel, **Aastha Mehta**
arXiv: CoRR/abs/2011.08069

## Invited Talks

Mar 2025 **Growlithe: A Developer-Centric Compliance Tool for Serverless Applications**
Uber (virtual)

Oct 2024 **Growlithe: A Developer-Centric Compliance Tool for Serverless Applications**
UBC-MSRA Workshop, Canada

Mar 2024 **Microarchitectural Side Channel Mitigations for Serverless Applications**
Shonan seminar, "Web Application Security", Japan

Nov 2023 **Microarchitectural Side Channel Mitigations for Serverless Applications**
Dagstuhl seminar, "Microarchitectural Attacks and Defenses", Germany

Oct 2023 **NetShaper: A Differentially Private Network Side-Channel Mitigation System**
Max Planck Institute for Software Systems (MPI-SWS), Germany
TU Darmstadt, Germany

Aug 2023 **Mitigating Network Side Channels: From Internet to Interconnect**
Intel Transformative Server Architectures (TSA) Monthly Talk (virtual)

Dec 2022 – Mar 2023 **Security by Design in Practical Systems**
Chalmers University, Sweden (virtual)
Dept. of Computer Science, University of Sydney, Australia (virtual)
Dept. of Computer Science, Boston University, USA
Dept. of Computer Science, TU Delft, Netherlands (virtual)
Dept. of Computer Science, University of Toronto, Canada
Dept. of ECE, University of Waterloo, Canada
Institute of Science and Technology, Austria

Aug 2022 **PanCast: Listening to Bluetooth Beacons for Epidemic Risk Mitigation**
IIT Delhi, India

Apr 2022 **Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud**
McGill University, Canada

Feb 2022 **Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud**
University of Toronto, Canada

Sep 2021 **Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud**
ENS Lyon, France

May 2021 **PanCast: Listening to Bluetooth Beacons for Epidemic Risk Mitigation**
UC San Diego, USA

Mar 2021 **Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud**
IIT Kharagpur, India

Feb – Mar 2020 **Policy Compliance in Online Services**
IMDEA Software Institute, Spain
CISPA Helmholtz Center for Information Security, Germany
Microsoft Research Redmond, USA
Dept. of Computer Science, Washington University in St. Louis, USA
Dept. of Computer Science, University of British Columbia, Canada
David R. Cheriton School of Computer Science, University of Waterloo, Canada
Dept. of Computer Science, George Mason University, USA
Dept. of Computer Science, Duke University, USA
Dept. of Computer Science, Northwestern University, USA
Dept. of EECS, Oregon State University, USA
School of Computing Science, Simon Fraser University, Canada

May 2019 **Pacer: Network Side-Channel Mitigation in the Cloud**
University of Maryland, USA, Host: Bobby Bhattacharjee

Nov 2018 **Pacer: Network Side-Channel Mitigation in the Cloud**
Systems lunch at Cornell University, USA, Host: Lorenzo Alvisi

Jul 2018 **Pacer: Efficient I/O Side-Channel Mitigation in the Cloud**
First Workshop on Speculative Side Channel Analysis (WoSSCA), Amsterdam, Netherlands

Aug 2017 **Qapla: Policy Compliance in Database-Backed Systems**
USENIX Security Symposium, Vancouver, Canada

## Professional Activities

### Organizer

USENIX Security Vice Chair at USENIX Security Symposium, 2026
SysDW Panelist at SOSP Doctoral Workshop, 2023
SOSP Poster Session Chair at Symposium on Operating Systems Principles, 2023
SRC Chair of ACM Student Research Competition at SOSP 2023
OSDI Mentorship OSDI Mentorship Scheme (co-organizer), 2020

### Other events

Shonan Invited to NII Shonan seminar "Web Application Security", 2024
Dagstuhl Invited to Dagstuhl seminar "MAD: Microarchitectural Attacks and Defenses", 2023

### Program Committee

CCS ACM Conference on Computer and Communication Security (2025)
ASPLOS Architectural Support for Programming Languages and Operating Systems (2025)
SysTex Workshop on System Software for Trusted Execution (2023)

S&P IEEE Oakland S&P (2023)

USENIX Security USENIX Security Symposium (2022, 2023, 2025)
**Noteworthy Reviewer Award, USENIX Security 2023**

EuroSys European Conference on Computer Systems (2021, 2022)

SYSTOR Systems and Storage Conference (2021)

PriSC Workshop on Principles of Secure Compilation (2021)

EuroDW EuroSys Doctoral Workshop (2021)

MiddlewareDW Middleware Doctoral Symposium (2020)

### Editorial Board

JSys Journal of Systems Research, Systems Security track (2022, 2023)

### External Reviewer

ASPLOS Architectural Support for Programming Languages and Operating Systems (2022)

HotOS Hot Topics in Operating Systems (2017)

OSDI Operating Systems Design and Principles (2016)

FC Financial Cryptography (2016)

ASPLOS Architectural Support for Programming Languages and Operating Systems (2015)

MobiSys Mobile Symposium (2015)

EuroSys European Conference on Computer Systems (2014)

## Teaching Experience

Fall 2025 **Instructor**, CPSC 538M, Systems Security (grad course)

Fall 2024 **Instructor**, CPSC 538M, Systems Security (grad course)

Spring 2024 **Instructor**, CPSC 317, Internet Computing (undergraduate course)

Spring 2023 **Instructor**, CPSC 317, Internet Computing (undergraduate course)

Fall 2022 **Instructor**, CPSC 538M, Systems Security (grad course)

Fall 2021 **Instructor**, CPSC 538M, Security & Privacy in the Era of Side Channels (grad course)

Winter 2019 **Co-instructor**, Operating Systems (core course), MPI-SWS/UdS
Lectures on storage subsystem.

Summer 2016 **Teaching Assistant**, Secure Information Flow Control in Systems (seminar), MPI-SWS/UdS
Assisted in seminar design, teaching, and evaluation

Summer 2013 **Teaching Assistant**, Operating Systems (core course), MPI-SWS/UdS
Assisted in designing and evaluating assignments and exams.

## Advising

### Postdoc

2026 – Peterson Yuhala, PhD, University of Neuchâtel (UniNE), Switzerland

2026 – Kha Dinh Duy, PhD, Sungkyunkwan University, Suwon, South Korea

2025 – Gargi Mitra, PhD, IIT Madras, India

### PhD

2025 – Kevin Wang, PhD, UBC

2025 – Yayu Wang, PhD, UBC

### Masters

2025 – Cathy Liu, PhD-track, UBC

2025 – Hanson Liang, PhD-track, UBC
2025 – Chanyuan Liu, MASc, UBC (co-supervised with Karthik Pattabiraman, ECE)
2024 – Angela Demarco, MSc, UBC (co-supervised with Joanna McGrenere)
2024 – Kjell Dankert, MSc, UBC
2022 – 2025 Yayu Wang, MSc, UBC
2022 – 2025 Rut Vora, MSc, UBC
2022 – 2024 Praveen Gupta, MSc, UBC (co-supervised with Mohammad Shahrad, ECE)
2022 – 2024 Arshia Moghimi, MASc, UBC (co-supervised with Mohammad Shahrad, ECE)
2021 – 2023 Amir Sabzi, MSc, UBC (co-supervised with Mathias Lécuyer)

### Undergraduate

2025 – Anmol Ghadia, UG Hons. thesis, UBC
2024 – 2025 Arun Balamural, UG Hons. thesis, UBC, (Received Rick Sample Memorial Award)
2024 – 2025 Aidan Shields, UG Hons. thesis, UBC, (Selected for CMMRS Workshop 2025)
2024 – 2024 Lucas Qin, USRA, UBC, NSERC USRA Award
2024 – 2024 Marcus Lai, USRA, UBC, SURE Award
2024 – 2024 Ngoc Bui, USRA, UBC, WLIUR Award
2023 – 2024 Devam Sisodraker, UG Hons. thesis, UBC
2022 – 2023 Tanya Prasad, UG thesis, BITS Pilani
2021 – 2022 Kasra Kamal, UG Hons. thesis, UBC, (Received Rick Sample Memorial Award)
2021 – 2022 Nichole Boufford, MSc, UBC
2021 – 2021 Ming Cheng Jiang, USRA, UBC, Work Learn International Undergraduate Research (WLIUR)
2021 – 2021 Rowan Lindsay, USRA, UBC, SURE Award
2021 – 2021 Nichole Boufford, USRA, UBC, Science Undergraduate Research Experience (SURE) Award

## Mentoring

2021 – 2024 Pierfrancesco Ingo (Ph.D. student, MPI-SWS)
2017 – 2022 Roberta De Viti (Ph.D. student, MPI-SWS)
2016 – 2019 Mohamed Alzayat (Ph.D. student, MPI-SWS)
2016 Katura Harvey (Graduate Intern, MPI-SWS)