Gargi Mitra

Postdoctoral Research Fellow | Security of Modern Networked Systems

Vancouver, BC, Canada
gargimiitm@gmail.com
linkedin.com/in/gargimitraiitm
Google Scholar: M216DzwAAAAJ
Website: `https://gargi-mitra.github.io/website/`

Research Interest and Experience

I investigate the security and privacy of *modern networked systems*, focusing on those that integrate their legacy system components with emerging technologies such as Artificial Intelligence or cloud-based services. My research reveals that such integrations create new vulnerabilities that traditional security and privacy measures were not designed to address. In safety-critical environments, such vulnerabilities can directly endanger human lives or disrupt essential services; in domains like IoT and web applications, they can lead to serious privacy breaches and regulatory violations. Yet, these modern technologies are meant to benefit society in substantial ways. *My long-term vision is to ensure that this technological progress remains secure, safe, and trustworthy, enabling the society to reap its benefits without any hidden risks.*

In the aforementioned context, my research has uncovered emerging security and privacy risks in *modern web applications, AI/ML-enabled medical devices, cloud-integrated industrial automation systems, and modern cloud-connected IoT applications*. My research has been published in reputed security and systems venues, including IEEE TDSC, DSN, CHASE, Springer Nature, EuroSys, IoTDI, and workshops co-located with CCS and NeurIPS, and has received media coverage (WIRED) and won awards. I am an active Program Committee member of top security conferences, and won the Distinguished Reviewer Award at ACM CCS 2024.

Professional Experience

Postdoctoral Research 2023–Present
The University of British Columbia (UBC), Vancouver, Canada
- Advisors: Karthik Pattabiraman, Aastha Mehta
- Research Area: Identifying emerging security and privacy vulnerabilities in modern safety-critical and networked systems, such as AI/ML-enabled medical devices, cloud-integrated industrial automation systems, and modern cloud-connected IoT applications

Programmer Analyst 2013–2015
Cognizant Technology Solutions India Pvt.Ltd.
- Domain: Data warehousing

Academic Background

PhD and MS under Dual Degree Program (Computer Science and Engineering) 2015–2022
Indian Institute of Technology Madras (IIT Madras), Chennai, India
- Advisors: Kamakoti Veezhinathan, Nitin Chandrachoodan
- Dissertation Title: Encrypted Traffic Analysis-Based Cyber Surveillance and Possible Mitigation Techniques
- Additional collaborations: Kernel implementation of SCION, a secure Internet communication protocol; Measuring quality of service in untrusted multi-vendor service function chains: Balancing security and resource consumption; Blockchain design alternatives for approximation-tolerant resource-constrained applications

Mitacs-SICI Indo-Canadian Research Internship Sep 2021–Dec 2021
UBC + IIT Madras
- Research Internship Topic: Encrypted Traffic Analysis-based attacks on Internet-connected ICS

Bachelor in Technology (Computer Science and Engineering) 2009–2013
St. Thomas' College of Engineering & Technology , Kolkata, India
- Research Internship Topic: Space-efficient synthesis of reversible logic circuits

Peer-Reviewed Publications

Area: Security of cloud-connected ICS OT networks

1. **Under Review** *ICS-Sniper: A Targeted Blackhole Attack on Encrypted ICS Traffic (Full version)*, **Gargi Mitra**, Chayuan Liu[1], Pritam Dash, Yingao Elaine Yao, Alain Zhiyanov[1], Aastha Mehta, Karthik Pattabiraman.
2. **RICSS'24 workshop (co-located with ACM CCS'24)** *ICS-Sniper: A Targeted Blackhole Attack on Encrypted ICS Traffic (Work-in-progress version)*, **Gargi Mitra**, Pritam Dash, Yingao Elaine Yao, Aastha Mehta, Karthik Pattabiraman. Link to ArXiv paper
3. **Co-authored a grant proposal** as project member, with Prof. Karthik Pattabiraman and Prof. Aastha Mehta, which was awarded 500K CAD by the National Cybersecurity Consortium in 2024.

Area: Security of AI/ML-based Medical Devices

1. **Under review** *SAMD: A Tool for Identifying False Data Injection Scenarios in AI/ML-enabled Medical Devices*, Mohammadreza Hallajiyan[1], Xueren Ge, **Gargi Mitra**, Shahrear Iqbal, Homa Alemzadeh, Karthik Pattabiraman.
2. **Under review** *ROAST: Risk-aware Outlier-exposure for Adversarial Selective Training of Anomaly Detectors Against Evasion Attacks*, Mohammed Elnawawy[1], **Gargi Mitra**, Shahrear Iqbal, Karthik Pattabiraman.
3. **Springer Nature HealthSec 2024 Journal** *Systems-Theoretic and Data-Driven Security Analysis in ML-enabled Medical Devices*, **Gargi Mitra**, Mohammadreza Hallajiyan[1], Inji Kim, Athish Pranav Dharmalingam[1], Mohammed Elnawawy[1], Shahrear Iqbal, Karthik Pattabiraman, Homa Alemzadeh. [Invited paper undergoing editorial process]
4. **DSML'25 workshop (co-located with DSN'25)** *Learning from the Good Ones: Risk Profiling-Based Defenses Against Evasion Attacks on DNNs*, Mohammed Elnawawy[1], **Gargi Mitra**, Shahrear Iqbal, and Karthik Pattabiraman, Oral presentation only. Link to paper on ArXiv [Acceptance rate: 64%]
5. **'Red Teaming GenAI' workshop (co-located with NEURIPS'24)** *MedAIScout: Automated Retrieval of Known Machine Learning Vulnerabilities in Medical Applications*, Athish Pranav Dharmalingam[1], **Gargi Mitra**, In Red Teaming GenAI: What Can We Learn from Adversaries?. 2024
6. **HealthSec'24 workshop (co-located with ACM CCS'24)** *SAM: Foreseeing Inference-Time False Data Injection Attacks on ML-enabled Medical Devices*, Mohammadreza Hallajiyan[1], Athish Pranav Dharmalingam[1], **Gargi Mitra**, Homa Alemzadeh, Shahrear Iqbal, and Karthik Pattabiraman, In Proceedings of the 2024 Workshop on Cybersecurity in Healthcare 2023 Nov 20 (pp. 77-84). [Acceptance rate: 57%]
7. **CHASE'24** *Systematically Assessing the Security Risks of AI/ML-enabled Connected Healthcare Systems*, Mohammad ElNawawy[1], Mohammadreza Hallajiyan[1], **Gargi Mitra**, Shahrear Iqbal, and Karthik Pattabiraman, In Proceedings of the IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2024. [Acceptance rate: 28.4%]

Area: Security of IoT Applications

1. **EuroSys'26** *Turnstile: Hybrid Information Flow Control Framework for Managing Privacy in Internet-of-Things Applications*, Kumseok Jung, Mohanna Shahrad, **Gargi Mitra**, and Karthik Pattabiraman, To appear in the Proceedings of EuroSys Conference, 2026. [Acceptance rate: 17%]
2. **IoTDI'24** *ImmunoPlane: Middleware for Providing Adaptivity to Distributed Internet-of-Things Applications*, Kumseok Jung, Mohanna Shahrad, **Gargi Mitra**, and Karthik Pattabiraman, In Proceedings of the IEEE/ACM Conference on Internet of Things Design and Implementation (IoTDI), 2024. [Acceptance rate: 36.7%]

Area: Encrypted Traffic Analysis-Based Cyber Surveillance on Users of Web Applications

1. **TDSC'22** *Snoopy: A Webpage Fingerprinting Framework with Finite Query Model for Mass-Surveillance*, **Gargi Mitra**, Prasanna Karthik Vairam, Sandip Saha, Nitin Chandrachoodan, Kamakoti Veezhinathan, In

[1] Indicates students I co-mentored

IEEE Transactions on Dependable and Secure Computing (TDSC) 2022. DOI: 10.1109/TDSC.2022.3222462 [Acceptance rate: 10-12%, Impact factor: 7.5]

2. **DSN'20** *Depending on HTTP/2 for Privacy? Good Luck!*, **Gargi Mitra**, Prasanna Karthik Vairam, Patanjali SLPSK, Nitin Chandrachoodan, Kamakoti Veezhinathan, In IEEE/IFIP Conference on Dependable Systems and Networks (DSN) 2020. DOI: 10.1109/DSN48063.2020.00044 [Acceptance rate: 16.5%]

3. **SIGCOMM'19 Extended Abstract** *White Mirror: Leaking Sensitive Information from Interactive Netflix Movies using Encrypted Traffic Analysis*, **Gargi Mitra**, Prasanna Karthik Vairam, Patanjali SLPSK, Nitin Chandrachoodan, Kamakoti Veezhinathan, In ACM SIGCOMM 2019 (Poster Session). DOI: 10.1145/3342280.3342330 [Acceptance rate: 55%]

Other collaborative works on network security in multi-vendor environments

1. **INFOCOM'19** *Towards Measuring Quality of Service in Untrusted Multi-Vendor Service Function Chains: Balancing Security and Resource Consumption*, Prasanna Karthik Vairam, **Gargi Mitra**, Vignesh Manoharan, Chester Rebeiro, Bhaskar Ramamurthy, Kamakoti Veezhinathan, In IEEE Conference on Computer Communications (INFOCOM) 2019. DOI: 10.1109/INFOCOM.2019.8737487 [Acceptance rate: 19.7%]

2. **MCOMSTD'18** *ApproxBC: Blockchain Design Alternatives for Approximation-Tolerant Resource-Constrained Applications*, Prasanna Karthik Vairam, **Gargi Mitra**, Chester Rebeiro, Bhaskar Ramamurthy, Kamakoti Veezhinathan, In IEEE Communications Standards Magazine. DOI : 10.1109/MCOMSTD.2018.1800021

Teaching Experience

2023, 2024 • Taught the course 'Algorithms and the Internet' to international students in the Vancouver Summer Program, UBC.

2022 • Teaching Assistant for an industry-sponsored course on 'Elements of Computing', IITM.

2021 • Teaching Assistant for 'Foundations of Computer Systems Design' at National Programme on Technology Enhanced Learning (NPTEL), India.

2018 – 2021 • Teaching Assistant for 'CAD for VLSI' and 'Digital System Testing' courses at IITM.

2017 • Teaching Assistant for the course 'Digital Design Verification' at IITM.

2016 • Teaching Assistant for the course 'Computer Organization' at IITM.

Mentoring Experience

- **PhD Student**

  1. Mohammed Elnawawy (UBC, 2023–Present)

- **MASc Students**

  1. Mohammadreza Hallajiyan (UBC, 2024–2024)
  2. Chanyuan Liu (UBC, 2025–Present)

- **Undergraduate students and interns** (for final-year project)

  1. Athish Pranav Dharmalingam (presently Software Engineer at Agrani Labs, India)
  2. Sandip Saha (presently Embedded Software Developer at MIPS, India)
  3. Animesh Singh (presently a PhD candidate at IIT Kharagpur, India)
  4. Krithika Swaminathan (presently a Master's student at North Carolina State University)

5. Aritri Paul (currently Software Engineer at Microsoft, India)
6. Nilufa Islam (currently Software Engineer at Mitsogo)
7. Vandana Dave (presently Senior Engineer at Sandisk, India)
8. Deep Bhattacharjee (presently Senior Site Reliability Engineer at Visa)
9. Barun Birendra Kumar Gupta (presently Senior Lead Engineer at Qualcomm, India)
10. Soumya Bhattacharya (presently Software Engineer at Media.net, India)

Awards and Recognitions

2024
- *ACM CCS 2024 Distinguished Reviewer Award*, awarded to **top 10% of 527** PC members
- *Ideas with Impact Competition, **second prize***, issued by Institute for Computing, Information and Cognitive Systems (ICICS), UBC, for presenting MedAIScout, a tool for automating cybersecurity assessment of machine-learning-enabled medical devices. It is an annual showcase and competition that invites **graduate students and postdocs across all departments of UBC** to showcase their research from the perspective of commercial potential.

2021
- *Mitacs Globalink Research Award*, sponsored by Mitacs and Shastri Indo-Canadian Institute, for collaborative research between India and Canada, and **open to all Doctoral students of India**.
- *Star TA Award*, from the Department of CSE, IIT Madras for contributions as a Teaching Assistant.

2020
- *Applied Research Competition, **first prize***, at Cyber Security Awareness Week (CSAW), organized by NYU and IIT Kanpur, **open to all PhD students across India working in the domain of cybersecurity**.
- *Star TA Award*, from the Department of CSE, IIT Madras for contributions as a Teaching Assistant.

2019
- *AWSAR top 100 Award*, awarded to the **top 100 out of 4993** contestants in a national scientific story-writing competition organized by the Department of Science & Technology, Govt. of India, as part of the AWSAR (Augmenting Writing Skills for Articulating Research) initiative.

2018
- *Gandhi Hazare Award*, **first prize**, awarded by the Centre for Social Innovation and Entrepreneurship, IIT Madras, for proposing technical solutions to fight corruption in the public distribution system in the country, **open to all students of IIT Madras**.
- *TCS Poster Competition Winner, **second prize***, awarded by TCS Research India, for presenting ‘Ankapala: The Account Book for Fighting Corruption in Public Distribution System’. The competition was **open to all Indian undergraduate and graduate students of all disciplines**.

2017
- *Embedded Security Challenge Winner, **first prize*** at Embedded Security Challenge, Cyber Security Awareness Week, organized by NYU and IIT Kanpur, for presenting ‘Eradicator: An Integrated Approach for Defense against Cyber Attacks in PLC based Industrial Control Systems’. The competition was **open to students of all Indian universities**.
- *Star TA Award*, from the Department of CSE, IIT Madras for contributions as a Teaching Assistant.

Academic Services

- **PC Member**

  1. ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2026
  2. ACM Conference on Computer and Communications Security (CCS) 2024, 2025, 2026 (Upcoming)
  3. IEEE International Conference on Cyber Security and Resilience (CSR) 2025
  4. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) artifact evaluation committee 2024

- **Journal Paper Reviewer**

  1. IEEE Internet of Things Journal
  2. IEEE Communications Magazine

- **Admission Reviewer**

  1. African Computer Vision Summer School (ACVSS) 2025

Press Coverage of Research

- Leaking Sensitive Information from Interactive Netflix Movies using Encrypted Traffic Analysis (2019)
  (a) Wired, **(b)** Financial Express, **(c)** Gadgets 360

Talks and Posters

USENIX'25, NCC Conference'25, Invited Talk at Idaho National Laboratory ('24)	• *ICS-Sniper: Targeting the Blind Spot of Modern Industrial Control Systems* **Gargi Mitra**, Pritam Dash, Elaine Yingao Yao, Alain Zhiyanov, Aastha Mehta, Karthik Pattabiraman.
USENIX'23	• *AI/ML-enabled Connected Healthcare Systems: New Remedies or New Risks?* **Gargi Mitra**, Mohammad Elnawawy, Mohammadreza Hallajiyan, Shahrear Iqbal, Karthik Pattabiraman, at Usenix Security Symposium 2023.
IMC'17	• *Hastakshara: A passive side-channel-based webpage fingerprinting attack for uncovering client intent*, **Gargi Mitra**, Prasanna Karthik Vairam, Nitin Chandrachoodan, Kamakoti Veezhinathan, at ACM Internet Measurement Conference 2017. (IMC)
ISEA'17	• *Blockchain as an infrastructure to build secure network services*, **Gargi Mitra**, Nitin Chandrachoodan, Kamakoti Veezhinathan, at PhD Conclave, ISEA Asia Security and Privacy Conference 2017.
IMC'17	• *Samata: A framework for identifying net-neutrality violations using evidence structures*, Prasanna Karthik Vairam, Karan Saxena, **Gargi Mitra**, Chester Rebeiro, Kamakoti Veezhinathan, at ACM Internet Measurement Conference (IMC).