Gargi Mitra

Systems and Network Security Researcher

Vancouver, BC, Canada (open to relocation) | gargimiitm@gmail.com | gargi-mitra.github.io/website | Google Scholar | LinkedIn

Profile

New technologies rarely replace legacy infrastructure. Instead, they are layered on top, invalidating the security and privacy assumptions of the original threat model. I take an interdisciplinary systems approach to identify the assumptions that no longer hold during such integrations, demonstrate them with proof-of-concept attacks, and recommend effective mitigations accordingly.

Focus areas: encrypted network traffic analysis · industrial control system (ICS/OT) security · security of AI/ML-enabled safety-critical systems · AI for security · IoT privacy

Selected highlights

- Conceived and led **ICS-Sniper**, the first targeted blackhole attack on encrypted ICS traffic (NDSS 2027), and built the project's hardware and software water-treatment testbeds.
- Designed the first traffic-analysis attack that defeats **HTTP/2 multiplexing** (IEEE/IFIP DSN 2020).
- Inferred viewers' choices in Netflix's interactive **"Black Mirror: Bandersnatch"** from encrypted traffic with a worst-case accuracy of 96%; covered by WIRED, and Netflix adopted one of the proposed mitigations after responsible disclosure.
- Co-authored a **CAD 500K** National Cybersecurity Consortium grant (2024); contributed to projects funded by the National Research Council and the Department of National Defence of Canada.
- Presented security findings on AI/ML-enabled medical devices to the **FDA** and to industry executives at **Medtronic, GE and Medcrypt**.
- **ACM CCS 2024 Distinguished Reviewer** (top 10% of 527 PC members); PC member for ACM CCS 2024–2026 and ACM AsiaCCS 2026.

Employment

Postdoctoral Research Fellow Jan 2023 – Aug 2026

Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, Canada

Advisors: Karthik Pattabiraman (ECE) and Aastha Mehta (CS).

ICS-Sniper: security of cloud-connected industrial control systems (lead researcher and mentor)

- Conceived and designed the first targeted blackhole attack that exploits the metadata of encrypted ICS/OT network traffic [C6, W2].
- Developed the full analysis chain: feature extraction from TLS- and VPN-encapsulated SCADA traffic, recovery of control-loop periodicity, clustering to identify target flows, and selective packet dropping in live traffic.
- Built the first realistic testbed for studying network attacks on cloud-connected ICS: hardware and software water-treatment testbeds (H-SWaT, S-SWaT) with Allen-Bradley PLCs; evaluated network-layer mitigations such as traffic shaping.
- Made the attack code, the testbed code and the detector baselines publicly available at github.com/ICS-Sniper.
- Led the five-member, multi-year project; co-authored the NCC proposal funded at CAD 500K (2024); planned milestones, trained students and interns on the testbed, and reported progress to the consortium every quarter.

Security of AI/ML-enabled medical devices (researcher and mentor)

- Systematized the identification of inference-time security risks that emerge when AI/ML is integrated with legacy medical infrastructure [C4, B1, W1].
- Defined threat models and built LLM- and RAG-based tools that identify these risks from a system's design, informed by MITRE ATT&CK and ATLAS [W1, W3, U2].
- Extended the work to detector robustness: evasion attacks on DNN-based anomaly detectors, and risk-profiling defenses against them [S2, U1].
- Collaborated with students at IIT Madras [W3] and with Homa Alemzadeh's group at the University of Virginia [B1, W1, U2]; presented the findings to the FDA and to industry executives at Medtronic, GE and Medcrypt.

IoT privacy and information flow control (collaborating researcher)

- Contributed privacy research ideas to, and co-authored, Turnstile, a hybrid information flow control framework for GDPR-compliant IoT applications [C5].
- Co-authored ImmunoPlane, a middleware that brings adaptivity to distributed IoT applications [C3].

Also co-supervised 1 PhD and 2 MASc students (see Mentoring) and contributed to NRC- and DND-funded projects (see Research Funding).

Mitacs Globalink Research Intern Sep – Dec 2021
The University of British Columbia (with IIT Madras), Vancouver, Canada
Encrypted traffic analysis-based attacks on Internet-connected industrial control systems. Host advisor: Karthik Pattabiraman.

Programmer Analyst 2013 – 2015
Cognizant Technology Solutions India Pvt. Ltd., India
Data warehousing for enterprise data systems, within production software development workflows.

Education

PhD (MS + PhD Dual Degree), Computer Science and Engineering 2015 – 2022
Indian Institute of Technology Madras (IIT Madras), Chennai, India

- Advisors: Kamakoti Veezhinathan (CSE) and Nitin Chandrachoodan (EE).
- Dissertation: Encrypted Traffic Analysis-Based Cyber Surveillance and Possible Mitigation Techniques.
- Research: webpage fingerprinting for mass surveillance (Snoopy) [J2]; the first traffic-analysis attack on HTTP/2 [C2]; the first side-channel attack on Netflix's interactive streaming traffic (White Mirror) [S1]; QoS measurement in untrusted multi-vendor service function chains [C1].
- Collaboration: kernel implementation of SCION, a secure Internet architecture, with Prof. Adrian Perrig's group at ETH Zurich.

BTech, Computer Science and Engineering 2009 – 2013
St. Thomas' College of Engineering & Technology (affiliated to MAKAUT), Kolkata, India

- Research topic: space-efficient synthesis of reversible logic circuits. Advisor: Dipak Kumar Kole.

Research Funding

National Cybersecurity Consortium (NCC), CAD 500K 2024
Security of cloud-integrated industrial control systems, with Karthik Pattabiraman and Aastha Mehta (UBC)
Role: conceived the attack, co-authored the proposal, set up the project testbed, planned milestones, performed the research, and trained students.

Also contributed to projects funded by the National Research Council (NRC) and the Department of National Defence (DND), including technical and progress reports.

Awards and Honors

2024	ACM CCS Distinguished Reviewer Award (top 10% of 527 program committee members)
2024	Ideas with Impact Competition, 2nd prize, ICICS, UBC (for MedAIScout; judged across all UBC departments for commercial potential)
2021	Mitacs Globalink Research Award (Mitacs and Shastri Indo-Canadian Institute)
2021	Star TA Award, Department of CSE, IIT Madras (also awarded in 2017 and 2020)
2020	CSAW'20 India, Applied Research Competition, 1st prize (NYU and IIT Kanpur); open to all PhD students in India working in cybersecurity
2019	AWSAR Award, top 100 of 4,993 entrants in a national science-writing competition (Department of Science & Technology, Government of India)
2018	Gandhi Hazare Award, 1st prize (Centre for Social Innovation and Entrepreneurship, IIT Madras)
2018	TCS Research Poster Competition, 2nd prize
2017	CSAW'17 India, Embedded Security Challenge, 1st prize (NYU and IIT Kanpur), leading IIT Madras's first all-women team, for "Eradicator: An Integrated Approach for Defense against Cyber Attacks in PLC-based Industrial Control Systems"

Publications

† Student I co-supervised or co-mentored. Titles link to the papers; [DOI] links go to the publisher's version.

Postdoc (UBC) PhD (IIT Madras)

Conference Papers

C6. **NDSS'27 ICS-Sniper: A Targeted Blackhole Attack on Encrypted ICS Traffic**. **Gargi Mitra**, Chanyuan Liu†, Pritam Dash, Yingao Elaine Yao, Alain Zhiyanov†, Aastha Mehta, Karthik Pattabiraman. Network and Distributed System Security Symposium (NDSS), 2027, to appear. Earlier version [W2]. [Code]

C5. **EuroSys'26 Turnstile: Hybrid Information Flow Control Framework for Managing Privacy in Internet-of-Things Applications**. Kumseok Jung, Mohanna Shahrad, **Gargi Mitra**, Karthik Pattabiraman. European Conference on Computer Systems (EuroSys), 2026. [Acceptance rate: 17%] [DOI]

C4. **CHASE'24 Systematically Assessing the Security Risks of AI/ML-enabled Connected Healthcare Systems**. Mohammed Elnawawy†, Mohammadreza Hallajiyan†, **Gargi Mitra**, Shahrear Iqbal, Karthik Pattabiraman. IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2024. [DOI]

C3. **IoTDI'24 ImmunoPlane: Middleware for Providing Adaptivity to Distributed Internet-of-Things Applications**. Kumseok Jung, **Gargi Mitra**, Sathish Gopalakrishnan, Karthik Pattabiraman. IEEE/ACM Conference on Internet of Things Design and Implementation (IoTDI), 2024. [DOI]

C2. **DSN'20 Depending on HTTP/2 for Privacy? Good Luck!** **Gargi Mitra**, Prasanna Karthik Vairam, Patanjali SLPSK, Nitin Chandrachoodan, Kamakoti Veezhinathan. IEEE/IFIP Conference on Dependable Systems and Networks (DSN), 2020. [Acceptance rate: 16.5%] [DOI]

C1. **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, Byrav Ramamurthy, Kamakoti Veezhinathan. IEEE Conference on Computer Communications (INFOCOM), 2019. [Acceptance rate: 19.7%] [DOI]

Journal and Magazine Articles

J2. **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. IEEE Transactions on Dependable and Secure Computing (TDSC), 2022. [Impact factor: 7.5] [DOI]

J1. **MCOMSTD'18 ApproxBC: Blockchain Design Alternatives for Approximation-Tolerant Resource-Constrained Applications**. Prasanna Karthik Vairam, **Gargi Mitra**, Chester Rebeiro, Byrav Ramamurthy, Kamakoti Veezhinathan. IEEE Communications Standards Magazine, 2018. [DOI]

Book Chapters

B1. **CCIS'26 (invited) Systems-Theoretic and Data-Driven Security Analysis in ML-enabled Medical Devices**. **Gargi Mitra**, Mohammadreza Hallajiyan†, Inji Kim, Athish Pranav Dharmalingam†, Mohammed Elnawawy†, Shahrear Iqbal, Karthik Pattabiraman, Homa Alemzadeh. Springer Nature Communications in Computer and Information Science (CCIS), vol. 2716, 2026. [DOI]

Workshop Papers

W3. **Red Teaming GenAI (NeurIPS'24 workshop) MedAIScout: Automated Retrieval of Known Machine Learning Vulnerabilities in Medical Applications**. Athish Pranav Dharmalingam†, **Gargi Mitra**. Red Teaming GenAI: What Can We Learn from Adversaries? (co-located with NeurIPS 2024). [Workshop page]

W2. **RICSS'24 (CCS'24 workshop) 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. RICSS Workshop (co-located with ACM CCS 2024). Full version at NDSS'27 [C6].

W1. **HealthSec'24 (CCS'24 workshop) SAM: Foreseeing Inference-Time False Data Injection Attacks on ML-enabled Medical Devices**. Mohammadreza Hallajiyan†, Athish Pranav Dharmalingam†, **Gargi Mitra**, Homa Alemzadeh, Shahrear Iqbal, Karthik Pattabiraman. Workshop on Cybersecurity in Healthcare (HealthSec, co-located with ACM CCS 2024), pp. 77–84. [DOI]

Short Papers, Posters and Extended Abstracts

S2. **DSML'25 (DSN'25 workshop) Learning from the Good Ones: Risk Profiling-Based Defenses Against Evasion Attacks on DNNs**. Mohammed Elnawawy†, **Gargi Mitra**, Shahrear Iqbal, Karthik Pattabiraman. DSML Workshop (co-located with IEEE/IFIP DSN 2025), short paper and oral presentation. [DOI]

S1. **SIGCOMM'19 Poster White Mirror: Leaking Sensitive Information from Interactive Netflix Movies using Encrypted Traffic Analysis**. **Gargi Mitra**, Prasanna Karthik Vairam, Patanjali SLPSK, Nitin Chandrachoodan, Kamakoti Veezhinathan. ACM SIGCOMM 2019 Posters and Demos (extended abstract). [DOI] Covered by WIRED, Financial Express and Gadgets 360; Netflix adopted one of the proposed mitigations after responsible disclosure.

Under Review and In Preparation

U2. **SAMD: A Tool for Identifying False Data Injection Scenarios in AI/ML-enabled Medical Devices**. Mohammadreza Hallajiyan†, Xueren Ge, Athish Pranav Dharmalingam†, **Gargi Mitra**, Shahrear Iqbal, Homa Alemzadeh, Karthik Pattabiraman.

U1. **ROAST: Risk-aware Outlier-exposure for Adversarial Selective Training of Anomaly Detectors Against Evasion Attacks**. Mohammed Elnawawy†, **Gargi Mitra**, Shahrear Iqbal, Karthik Pattabiraman.

Ongoing Independent Projects

- **Agentic security tooling.** Agentic, self-improving tools that identify vulnerabilities and attacks in networked multi-vendor systems.
- **Detection characteristics framework.** Uses AI to translate attack tactics and techniques from MITRE ATT&CK and ATLAS into queryable network characteristics, specifying what each detection observes.
- **Zeek and Kitsune network IDS.** A live pipeline with Zeek for capture and features and Kitsune's autoencoder ensemble as the detector.

Technical Skills

Network protocols and traffic analysis	TCP/IP stack; HTTP/1.1 and HTTP/2; HTTPS and TLS 1.3; DNS; WireGuard and OpenVPN; Modbus/TCP and CIP; encrypted traffic analysis; webpage and application fingerprinting; side-channel feature engineering; phase folding; superperiod detection; hierarchical clustering; HAR and pcap correlation; traffic dataset collection
Attack research	Root-cause and exploitability analysis; protocol- and design-level weaknesses; proof-of-concept development; impact measurement; on-path (MITM) interception; in-path traffic manipulation; targeted denial of service; selective blackholing; side-channel information leakage; false data injection; adversarial evasion
Detection engineering and threat prevention	IDS/IPS evasion analysis; anomaly detection (kNN, One-Class SVM, MAD-GAN); detector robustness under evasion; risk profiling; outlier exposure; Zeek scripting and packages; live capture pipelines; near-real-time flow processing; MITRE ATT&CK mapping; countermeasure evaluation; traffic shaping; testbed validation
Security of AI and ML systems	Adversarial machine learning; evasion attacks; adversarial input generation (URET); inference-time false data injection; robust training of detectors; MITRE ATLAS; safety-critical ML; ML-enabled medical devices; AI-service traffic identification; PyTorch and scikit-learn
AI for security	LLM pipelines with retrieval (RAG); prompt engineering; LLM output evaluation; vulnerability retrieval (CVE, NVD); attack-path generation; alert triage and rule generation
ICS/OT security	Cloud-connected ICS and SCADA; Modbus/TCP; CIP and EtherNet/IP; Allen-Bradley Micro800 PLCs; hardware (H-SWaT) and software (S-SWaT) testbeds; MiniCPS and Mininet emulation; industrial network monitoring; NIST SP 800-82 and IEC 62443
Threat modeling and risk assessment	Structured threat modeling; STPA-Sec (systems-theoretic analysis); attack-path enumeration; MITRE ATT&CK and ATLAS; STRIDE, DREAD, CVSS, FMEA; risk profiling; CVE and NVD analysis; FDA medical device cybersecurity; GDPR
Privacy, IoT and cloud systems	Privacy leakage analysis; information flow control; GDPR-oriented privacy policies; IoT middleware; multi-vendor service function chains; tamper-resistant measurement; evidence Bloom filters, HMAC; blockchain for constrained devices
Programming and tools	Python (primary); C; Bash; PyTorch; scikit-learn; Zeek; Wireshark and tshark; Scapy and pyshark; NetfilterQueue; Docker; Git; Linux; kernel networking (SCION); reproducible research artifacts
Leadership and communication	Research team leadership; project scoping and roadmaps; grant writing; mentoring; teaching; peer review; technical writing; public speaking; industry and regulator engagement; science communication

Talks and Presentations

Invited

2026 ETS Montreal: Uncovering Security Vulnerabilities in Modern Networked Systems

2024 Idaho National Laboratory: ICS-Sniper: Targeting the Blind Spot of Modern Industrial Control Systems

Conference posters and presentations

2025 USENIX Security'25 and NCC Conference'25: ICS-Sniper: Targeting the Blind Spot of Modern Industrial Control Systems

2023 USENIX Security'23: AI/ML-enabled Connected Healthcare Systems: New Remedies or New Risks?

2017 ACM IMC'17: Hastakshara: A passive side-channel-based webpage fingerprinting attack for uncovering client intent

2017 ACM IMC'17: Samata: A framework for identifying net-neutrality violations using evidence structures (co-author)

2017 ISEA Asia Security and Privacy Conference'17, PhD Conclave: Blockchain as an infrastructure to build secure network services

Teaching

Co-instructor (with Prof. Sathish Gopalakrishnan), Algorithms and the Internet 2023, 2024
Vancouver Summer Program, UBC; international senior undergraduate and first-year Master's students

Teaching Assistant, IIT Madras (11 terms) 2016 – 2022
Computer Organization; Digital Design Verification; CAD for VLSI; Digital System Testing; Elements of Computing (industry-sponsored); Foundations of Computer Systems Design (NPTEL)
Star TA Award in 2017, 2020 and 2021.

Mentoring

Graduate students (co-supervised at UBC; publication IDs in brackets)

- Mohammed Elnawawy, PhD (2023 – present): [C4, B1, S2, U1]
- Mohammadreza Hallajiyan, MASc (Jan 2023 – Dec 2024): [C4, B1, W1, U2]
- Chanyuan Liu, MASc (2025 – present): [C6]

Undergraduate researchers and interns: co-mentored 10 on final-year projects, with co-authored papers [C6, J2, B1, W1, W3, U2]. Alumni are now at companies including Meta, Microsoft, Qualcomm, Visa and Sandisk, or doing a PhD (IIT Kharagpur).

Service and Outreach

Program committees	ACM CCS 2024, 2025, 2026; ACM AsiaCCS 2026; IEEE CSR 2025
Artifact evaluation	IEEE/IFIP DSN 2024
Journal reviewing	IEEE Internet of Things Journal 2025; IEEE Communications Magazine 2025
Admissions review	African Computer Vision Summer School (ACVSS) 2025, 2026
Sessions and workshops	Organized Birds-of-a-Feather sessions bridging industrial and academic CPS security research at USENIX Security 2023 and 2025; organized a summer workshop on AI security at UBC (2025); participated in a workshop on AI safety and security at Microsoft, Redmond (Jun 2026)
Industry and regulators	Research findings presented to security practitioners at Medcrypt, Medtronic and GE, and to the FDA; quarterly progress reports to the National Cybersecurity Consortium; technical and progress reports for projects funded by the National Research Council and the Department of National Defence
Science communication	AWSAR national science-writing award (2019); blog writing and webinars for non-specialist audiences
Outreach	Women in CS community, IIT Madras; volunteer teacher for underprivileged children, Kolkata