Md Hasan Shahriar

PhD Candidate, Department of Computer Science, Virginia Tech

Email: hshahriar@vt.edu Website: shahriar0651.github.io GitHub: shahriar0651

Research Overview

My research lies at the intersection of **security and privacy** in **cyber-physical systems** (CPS), with a particular focus on domains such as **connected and autonomous vehicles**, **healthcare**, and the **smart grid**. I explore both the **security of machine learning**—ensuring the robustness and trustworthiness of ML models—and **machine learning for security**—leveraging ML techniques to detect, prevent, and respond to cyber threats in CPS environments.

Education

PhD in Computer Science **January 2021 – May 2026 (Expected)**
Dissertation: *Fortifying the Security of Autonomous Vehicles: From Networking to Perception*
Advisor: Wenjing Lou
Virginia Tech

MS in Computer Engineering **March 2016**
Thesis: *Deception Defense against Stealthy Attacks in Power Grids*
Advisor: Mohammad Ashiqur Rahman
CGPA 4.00/4.00
Florida International University

BSc in Electrical and Electronic Engineering **December 2020**
Thesis: *Transient Stability Analysis of Smart Grids with Impacts of Distributed Generation*
Advisor: Dr. Md Forkan Uddin
CGPA 3.40/4.00
Bangladesh University of Engineering and Technology

Research Experience

Graduate Research Assistant, Complex Network and Security Research Lab, Virginia Tech *2021 – Present*
- Developed defenses against adversarial and backdoor attacks in deep learning.
- Proposed robust misbehavior detection systems for vehicular networks.

Amazon Fellow, Amazon-VT Initiative for Efficient and Robust Machine Learning, *Aug 2024 – May 2025*
- Conduct research on adversarial attacks and defenses in multimodal fusion for autonomous driving.
- Developed novel defenses detecting misaligned sensor inputs with near-perfect accuracy on real-world datasets.

Graduate Research Assistant, Analytics for Cyber Defense Lab, Florida International University *2019 – 2020*
- Modeled cyberattacks and defenses in cyber-physical power systems.
- Mentored undergraduate students in deep learning applications.

Teaching Experience

Lecturer, Department of Computer Science, Uttara University *2016 – 2017*
- *EE 101: Electrical Circuits*
- *EE 205: Basic Electronics*
- *EE 210: Digital Logic Design*
- *EE 315: Microprocessor Interfacing*

Taught and led lab sessions for undergraduate courses, integrating hands-on experiments with core theoretical concepts.

Industry Research Internships

Interim Engineering Intern, Qualcomm Incorporated, San Diego, CA *Summers 2022 & 2023*

- **Summer 2023**: *Transferability Analysis of Real-world Adversarial Attacks on Object Detection Models*: Executed real-world adversarial attacks on traffic sign detection systems. Developed DVC-based pipelines for artifact tracking and dataset management. Evaluated transferability of adversarial examples and assessed robustness across diverse object detection models.
  Manager: *Jonathan Petit*, **Mentor**: *Jean-Philippe Monteuuis*
- **Summer 2022**: *Security of Connected Automated Vehicles using GANs*: Investigated generative models to create realistic-but-malicious V2X messages. Designed a GAN-based misbehavior detection framework to identify adversarial basic safety messages (BSMs) in vehicular networks.
  Manager: *Jonathan Petit*, **Mentor**: *Rashed Ansari*

Publications

Journal Articles

[J3] **M. H. Shahriar**, M. R. Ansari, M. S. Haque, J.-P. Monteuuis, C. Chen, J. Petit, Y. T. Hou, W. Lou. "**VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems.**" *ACM Transactions on Cyber-Physical Systems (ACM TCPS)*, 2025. (Impact Factor: 4.9). [PDF] [Code]

[J2] **M. H. Shahriar**, M. A. Rahman, M. Jafari, S. Paudyal. "**Formal Analytics for Stealthy Attacks against Contingency Analysis in Power Grids.**" *Sustainable Energy, Grids and Networks (SEGAN)*, 2024. (Impact Factor: 4.9). [PDF] [Code]

[J1] **M. H. Shahriar**, Y. Xiao, P. Moriano, W. Lou, Y. T. Hou. "**CANShield: Deep Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal-Level.**" *IEEE Internet of Things Journal (IEEE IoT-J)*, 2023. (Impact Factor: 9.0). [PDF] [Code]

Conference Papers

[C10] **M. H. Shahriar**, N. Wang, N. Ramakrishnan, Y. T. Hou, W. Lou. "**Let the Noise Speak: Harnessing Noise for a Unified Defense Against Adversarial and Backdoor Attacks.**" *European Symposium on Research in Computer Security (ESORICS)*, **2025**. Acceptance rate: 20–25%. [PDF] [Code]

[C9] **M. H. Shahriar**, M. R. Ansari, J.-P. Monteuuis, C. Chen, J. Petit, Y. T. Hou, W. Lou. "**VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems.**" *IEEE International Conference on Distributed Computing Systems (ICDCS)*, **2024**. Acceptance rate: 18–22%. [PDF] [Code]

[C8] **M. H. Shahriar**, W. Lou, Y. T. Hou. "**CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks.**" *Network and Distributed Systems Security Symposium – Vehicle Security Workshop (NDSS VehicleSec)*, **2023**. Best Paper Runner-Up Award. Acceptance rate: 30–40%. [PDF] [Code]

[C7] S. Shi, Y. Xiao, C. Du, **M. H. Shahriar**, A. Li, N. Zhang, Y. T. Hou, W. Lou. "**MS-PTP: Protecting Network Timing from Byzantine Attacks.**" *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, **2023**. Acceptance rate: 20–25%. [PDF] [Code]

[C6] **M. H. Shahriar**, Y. Xiao, P. Moriano, W. Lou, Y. T. Hou. "**CANShield: Signal-based Intrusion Detection for Controller Area Networks.**" *Embedded Security in Cars (ESCAR)*, **2022**. Acceptance rate: 25–30%. [PDF] [Code]

[C5] **M. H. Shahriar**, A. A. Khalil, M. Rahman, M. Manshaei, D. Chen. "**iAttackGen: Generative Synthesis of False Data Injection Attacks in Cyber-Physical Systems.**" *IEEE Symposium on Security and Privacy (CNS)*, **2021**. Acceptance rate: 25%. [PDF] [Code]

[C4] **M. H. Shahriar**, M. Rahman, N. Haque, B. Chowdhury, S. G. Whisenant. "**iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-Physical Systems.**" *IEEE Secure and Trustworthy Computing Conference (SecureComm)*, **2021**. Acceptance rate: 20–25%. [PDF] [Code]

[C3] **M. H. Shahriar**, M. Rahman, N. I. Haque, B. Chowdhury. "**DDAF: Deceptive Data Acquisition Framework against Stealthy Attacks in Cyber-Physical Systems.**" *IEEE 45th International Conference on Software Engineering (COMPSAC)*, **2021**. Acceptance rate: 30–35%. [PDF] [Code]

[C2] M. Jafari, **M. H. Shahriar**, M. Rahman, S. Paudyal. "**False Relay Operation Attacks in Power Systems with High Renewables.**" *IEEE Power & Energy Society General Meeting (PESGM)*, **2021**. Acceptance rate: 30–35%. [PDF] [Code]

[C1] **M. H. Shahriar**, N. Haque, M. Rahman, M. Alonso Jr. "**G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System.**" *IEEE 45th International Conference on Software Engineering (COMPSAC)*, **2020**. Acceptance rate: 30–35%. [PDF] [Code]

Under Review

[R2] M. H. Shahriar, N. Wang, A. Sikder, N. Ramakrishnan, Y. T. Hou, W. Lou. "**NOIFI: Decoding the Signal in the Noise for On-the-Fly Detection of Adversarial Attacks in WiFi Sensing.**" *Annual Computer Security Applications Conference (ACSAC)*, **2025**.

[R1] M. H. Shahriar, M. M. Barat, H. Shundar, N. Ramakrishnan, Y. T. Hou, W. Lou. "**On the Fragility of Multimodal Perception to Temporal Misalignment in Autonomous Driving.**" *Network and Distributed System Security (NDSS) Symposium*, **2026**.

Google Scholar

h-index: 8, i10-index: 7, citations: 387 (as of 1 July, 2025)
Link to Google Scholar : https://scholar.google.com/citations?user=TcCzjTQAAAAJ&h

Awards & Travel Grants

[A7] **Amazon Fellowship** from *Amazon-VT Initiative for Efficient and Robust Machine Learning*, 2024-2025.

[A6] **Travel grants** from **IEEE ICDCS (2024), CyberTruck Challenge (2024), VehicleSec (2023), ACM WiSec (2029).**

[A5] **Best Paper Runner Up Award** at *VehicleSec*, 2023.

[A4] **Fellowship for Graduate Student First-Author Papers**, **Virginia Tech**, 2023.

[A3] **Bangladesh-Sweden Trust Fund Scholarship**, July 2021.

[A2] **Admission Test Excellency Scholarship**, *Bangladesh University of Engineering and Technology*, 2011.

[A1] **Education Board Scholarship**, *Government of Bangladesh*, 2008 & 2010.

Student Mentorship

- Md Shahedul Haque, PhD Student, Virginia Tech: Project on Privacy Preserving Machine Learning.
- Md Mohaimin Al Barat, PhD Student, Virginia Tech: Testbed Implementation for Automotive Ethernet.
- Samara Ruiz Sandoval, Undergrad, Florida International University: Deep Learning for Security of Smart Grid.

Presentations & Talks

Research Talks

[R4] **Amazon VT Initiative Kickoff**, *"Security of Connected and Autonomous Vehicles: From In-vehicular Networks to Multimodal Fusion"*, Invited Talk, Blacksburg, VA, Fall 2024.

[R3] **3rd Workshop on Future Automotive Research Datasets**, *"Generating State-of-the-art V2X Misbehavior Detection Dataset and a Robust Detection Approach"*, April 2024.

[R2] **ACIC–DoD ROLLCAGE TEM / 1st Workshop on Automotive Research Datasets**, *"A Survey on CAN Intrusion Detection Dataset"*, April & November 2021.

[R1] **CAPER Meeting (Virtual)**, *"Deception-based Defense against False Data Injection Attacks in Power Grids"*, Fall 2020.

Paper Presentations

[T5] **IEEE ICDCS 2024**, *"VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems"*, Oral Presentation, July 2024.

[T4] **VehicleSec 2023**, *"CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks"*, Oral Presentation, February 2023.

[T3] **ESCAR USA 2022**, *"CANShield: Signal-based Intrusion Detection for Controller Area Networks"*, Oral Presentation, June 2022.

[T2] **IEEE COMPSAC 2021**, *"DDAF: Deceptive Data Acquisition Framework against Stealthy Attacks in Cyber-Physical Systems"*, Oral Presentation, July 2021.

[T1] **EAI SecureComm 2021**, *"iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-physical Systems"*, Oral Presentation, September 2021.

Poster Presentations

[P4] **Amazon-VT'24**, "VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems," Fall Kickoff Meeting of Amazon-VT Initiative, Blacksburg, VA, 2024.

[P3] **VehicleSec'23**, "CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks," Symposium on Vehicle Security and Privacy (VehicleSec), 2023.

[P2] **FICS'19**, "False Data Injection Attacks against Contingency Analysis in Power Grids," FICS Research Annual Conference on Cybersecurity, University of Florida, 2019.

[P1] **WiSec'19**, "False Data Injection Attacks against Contingency Analysis in Power Grids," ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2019.

Featured

Amazon-Virginia Tech Initiative awards two student fellowships, five faculty research awards [VT News Link]

Professional Engagement

[P2] Graduate Student Member, Institute of Electrical and Electronics Engineers (IEEE)

[P1] Campus Representative, Graduate Student Assembly (GSA) – DC Region, Virginia Tech, 2023

Honors and Awards

[H7] **Travel grants** from NSF for **IEEE ICDCS (2024)**, **CyberTruck Challenge (2024)**, **VehicleSec (2023)**, and ARO for **ACM WiSec (2019)**.

[H6] A**mazon Fellowship** from the Amazon-VT Initiative for Efficient and Robust Machine Learning, awarded for academic year 2024–2025.

[H5] **Best Paper Runner-Up Award at VehicleSec** 2023, San Diego, CA.

[H4] Virginia Tech Fellowship for Graduate Student First-Author Publications, 2023.

[H3] **Bangladesh–Sweden Trust Fund**, July 2021.

[H2] **Admission Test Excellency Scholarship**, BUET, Dhaka, Bangladesh, 2011.

[H1] **Government Merit Scholarships**: Education Board Scholarships (2008 & 2010), Primary & Junior School Scholarships (2002 & 2006), Bangladesh.

Professional Services

Program Committee Member
ACM CCS (Artifact Evaluation) (2025)

Reviewer: ACM Transactions on Cyber-Physical Systems (TCPS) (2025), IEEE Transactions on Vehicular Technology (2024), IEEE Transactions on Computers (2024), Computers & Security (2024), IEEE Sensors Journal (2023), IEEE Transactions on Information Forensics and Security (2023), Vehicular Communications (2023), IEEE PES Transactions on Power Systems (2021), International Journal of Electronic Security and Digital Forensics (IJESDF) (2021)

Sub-reviewer: IEEE S&P (2022–2025), ACM WiSec (2022–2025), ESORICS (2022–2024), IEEE CNS (2022–2024), ICCCN (2023), IEEE ICDCS (2022), IEEE ICC (2020), NSysS (2019)

Session Chair: IEOM 7th North American Industrial Engineering and Operations Management Conference, Orlando, USA (2022), Session: Data Analytics

Conference Organization: Student Volunteer, ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec) (2020), Miami, FL

References

Available upon request.