Md Hasan Shahriar

PhD Candidate, Department of Computer Science
Virginia Tech, 900 N Glebe Road, Arlington, VA 22203, USA.
hshahriar@vt.edu shahriar0651.github.io
(U.S. Permanent Resident, authorized to work in the U.S.)

Research Interests

My research interests lie at the intersection of cyber-physical systems (CPS), machine learning (ML), and cybersecurity. I focus on identifying security vulnerabilities in safety-critical CPS, such as smart grids, vehicular networks, and autonomous systems, and on developing scalable, attack-resilient, and trustworthy CPS/ML systems capable of withstanding emerging cyber threats in real-world applications.

Education

PhD in Computer Science **Jan 2021–May 2026**
Virginia Tech *Arlington, Virginia, USA*

- Dissertation: *Toward Trustworthy CPS: Robust ML for Secure Sensing, Perception, and Control*
- Advisor: Wenjing Lou
- GPA 3.93/4.00

MS in Computer Engineering **Jan 2019–Dec 2020**
Florida International University *Miami, Florida, USA*

- Thesis: *Deception Defense against Stealthy Attacks in Power Grids*
- Advisor: Mohammad Ashiqur Rahman
- GPA 4.00/4.00

BSc in Electrical and Electronic Engineering **Feb 2011–Mar 2016**
Bangladesh University of Engineering and Technology *Dhaka, Bangladesh*

- Thesis: *Transient Stability Analysis of Smart Grids with Impacts of Distributed Generation*
- Advisor: Dr. Md Forkan Uddin

Awards, Fellowships, & Grants

[**A10**] **Amazon Fellowship**, *Amazon-VT Initiative for Efficient and Robust Machine Learning*, 2024-2025.
[**A9**] **Student Travel Grant for Attending IEEE ICDCS**, *U.S. National Science Foundation*, 2024.
[**A8**] **Student Travel Grant**, *CyberTruck Challenge*, 2024.
[**A7**] **Best Paper Runner Up Award**, *Symposium on Vehicle Security and Privacy (VehicleSec)*, 2023.
[**A6**] **Student Travel Grant**, *Inaugural Symposium on Vehicle Security and Privacy (VehicleSec)*, 2023.
[**A5**] **Fellowship for Graduate Student First-Author Papers**, *the University Graduate School, Virginia Tech*, 2023.
[**A4**] **Bangladesh-Sweden Trust Fund Scholarship**, July 2021.
[**A3**] **Student Travel Grant for Attending ACM WiSec**, *U.S. Army Research Office*, 2019.
[**A2**] **Admission Test Excellency Scholarship**, *Bangladesh University of Engineering and Technology*, 2011.
[**A1**] **Education Board Scholarship**, *Government of Bangladesh*, 2008 & 2010.

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: 2.0).

[J2] **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: 10.6).

[J1] **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: 5.6).

Conference Papers (Selected)

[C12] **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: TBA%).

[C11] **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: 21%).

[C10] **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* ***(VehicleSec)***, 2023. **Best Paper Runner-Up Award**. (Acceptance rate: 36.0%)

[C9] 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: 25.4%)

[C8] **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: TBA)

[C7] **M. H. Shahriar**, M. Rahman, N. Haque, B. Chowdhury, S. G. Whisenant. "iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-Physical Systems." *EAI International Conference on Security and Privacy in Communication Networks* ***(SecureComm)***, 2021. (Acceptance rate: 34%)

[C6] **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: 27%)

[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 Conference on Communications and Network Security* ***(CNS)***, 2021. (Acceptance rate: 26%)

[C4] 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: 50%)

[C3] N. I. Haque, **M. H. Shahriar**, M. Dastgir, A. Debnath, I. Parvez, A. Sarwat, and M. Rahman. "Machine Learning in Generation, Detection, and Mitigation of Cyberattacks in Smart Grid: A Survey." North American Power Symposium (**NAPS**), 2021.

[C2] **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: 24%)

[C1] **M. H. Shahriar**, M. Sadiq, M. Uddin, "Stability Analysis of Grid-connected PV Array Under Maximum Power Point Tracking". International Conference on Electrical and Computer Engineering (**ICECE**), 2016.

Theses

[T3] **M. H. Shahriar**. "Toward Trustworthy Cyber-physical Systems: Robust Machine Learning for Secure Sensing, Perception, and Control" In Virginia Tech Theses and Dissertations, 2026 (Anticipated).

[T2] **M. H. Shahriar**. "Deception Defense against Stealthy Attacks in Power Grids." In Florida International University Theses and Dissertations, 2020.

[T1] **M. H. Shahriar**. "Transient Stability Analysis of Smart Grids with Impacts of Distributed Generation." In Bangladesh University of Engineering and Technology Theses and Dissertations, 2016.

Under Review (Ongoing)

[**O3**] **M. H. Shahriar**, N. Wang, A. Sikder, N. Ramakrishnan, Y. T. Hou, W. Lou. "Noise, Why Can't You Bend? Detecting Adversarial Perturbations in Wireless Sensing via Structural Fragility" *ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, 2026.

[**O2**] **M. H. Shahriar**, M. M. Barat, H. Shundar, N. Zhang, N. Ramakrishnan, Y. T. Hou, W. Lou. "Temporal Misalignment Attacks against Multimodal Perception in Autonomous Driving" *IEEE Conference on Secure and Trustworthy Machine Learning (**SatML**)*, 2026.

[**O1**] **M. H. Shahriar**, M. M. Barat, H. Shundar, N. Zhang, N. Ramakrishnan, Y. T. Hou, W. Lou. "Detecting Temporal Misalignment Attacks in Multimodal Fusion for Autonomous Driving" *The International Conference on Learning Representations (**ICLR**)*, 2026.

Presentations & Talks

Invited Research Talks:

- **Amazon VT Initiative Kickoff**, *"Security of Connected and Autonomous Vehicles: From In-vehicular Networks to Multimodal Fusion"*, Invited Talk, Blacksburg, VA, Fall 2024.
- **3rd Workshop on Future Automotive Research Datasets**, *"Generating State-of-the-art V2X Misbehavior Detection Dataset and a Robust Detection Approach"*, April 2024.
- **1st Workshop on Future Automotive Research Datasets & ACIC–DoD ROLLCAGE TEM**, *"CANShield: Signal-based Intrusion Detection for Controller Area Networks"*, April & November 2021.
- **1st Workshop on Automotive Research Datasets**, *"A Survey on CAN Intrusion Detection Dataset"*, November 2021.
- **CAPER Meeting (Virtual)**, *"Deception-based Defense against False Data Injection Attacks in Power Grids"*, Fall 2020.

Paper Presentations:

- **ESORICS 2025**, *"Let the Noise Speak: Harnessing Noise for a Unified Defense Against Adversarial and Backdoor Attacks."*, September 2025.
- **IEEE ICDCS 2024**, *"VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems"*, July 2024.
- **VehicleSec 2023**, *"CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks"*, February 2023.
- **ESCAR USA 2022**, *"CANShield: Signal-based Intrusion Detection for Controller Area Networks"*, June 2022.
- **IEEE COMPSAC 2021**, *"DDAF: Deceptive Data Acquisition Framework against Stealthy Attacks in Cyber-Physical Systems"*, July 2021.
- **EAI SecureComm 2021**, *"iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-physical Systems"*, September 2021.

Poster Presentations:

- **Amazon-VT'24**, "VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems," M. H. Shahriar, M. R. Ansari, J.-P. Monteuuis, C. Chen, J. Petit, Y. T. Hou, W. Lou, Fall Kickoff Meeting of Amazon-VT Initiative, Blacksburg, VA, 2024.
- **VehicleSec'23**, "CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks," M. H. Shahriar, W. Lou, Y. T. Hou. Symposium on Vehicle Security and Privacy (VehicleSec), 2023.
- **WiSec'19 & FICS'19**, "Poster: False Data Injection Attacks against Contingency Analysis in Power Grids," M. Rahman, M.H. Shahriar, R. Masum, ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2019 & also in FICS Research Annual Conference on Cybersecurity, University of Florida, 2019.

Research Appointments

[**R4**] **Graduate Research Assistant** **2021 – Present**
Complex Network and Security Research (CNSR) Lab, Virginia Tech *Arlington, Virginia, USA*
Advisor: *Dr. Wenjing Lou*
Building on the foundation of my M.S. research, my Ph.D. work focused on developing trustworthy cyber-physical

systems, with an emphasis on connected and autonomous vehicles (CAVs) through robust machine learning techniques. In this pursuit, I designed novel intrusion detection systems capable of identifying cyberattacks across multiple automotive network layers—such as the Controller Area Network (CAN) and vehicle-to-everything (V2X) communications—addressing both stealthy data manipulation and ML-based adversarial threats. These efforts resulted in multiple peer-reviewed publications, including journal articles [J1, J2] and conference papers [C6–C9], along with ongoing studies on network-induced attacks targeting multimodal fusion–based perception in autonomous driving [O1–O2]. In addition to my research contributions, I have mentored several M.S. and Ph.D. students at Virginia Tech.

[R3] **Amazon Fellow** **Aug 2024 – May 2025**
AMAZON-VT INITIATIVE FOR EFFICIENT AND ROBUST ML, VIRGINIA TECH *Arlington, Virginia, USA*
PI: *Dr. Wenjing Lou* and *Dr. Naren Ramakrishnan*
During my fellowship on Efficient and Robust Machine Learning, I developed a unified defense framework that mitigates both adversarial and backdoor attacks across diverse modalities and threat models. This research resulted in one conference publication [C10] and an ongoing study on robust ML for wireless sensing applications [O3].

[R2] **Graduate Research Assistant** **2019–2020**
ANALYTICS FOR CYBER DEFENSE (ACYD) LAB, FLORIDA INTERNATIONAL UNIVERSITY *Miami, Florida, USA*
Advisor: *Dr. Mohammad Ashiqur Rahman*
My M.S. research centered on the security of cyber-physical systems, with a primary focus on uncovering and mitigating stealthy threats in the smart grid. I developed a novel threat synthesizer that integrates formal methods with Generative Adversarial Networks (GANs) to model and analyze sophisticated attack behaviors, resulting in one journal [J1] and two conference publications [C4, C5]. Building on these insights, I designed a deception-based moving target defense framework to counter stealthy attacks, which led to two additional conference papers [C6, C7]. In parallel, I led research efforts exploring the application of GAN-based defense models in network security [C2, C3] and mentored several undergraduate students during my time at FIU.

[R1] **Undergradudate Researcher** **2014–2016**
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY *Dhaka, Bangladesh*
Advisor: *Dr. Forkan Uddin*
Conducted undergraduate thesis research on the transient stability of grid-connected photovoltaic (PV) arrays, analyzing the impact of various maximum power point tracking (MPPT) algorithms under grid disturbances and exploring methods for performance improvement; results published in [C1].

INDUSTRIAL EXPERIENCE

[I3] **Interim Engineering Intern** **May 2023–Aug 2023**
QUALCOMM INCORPORATED *San Diego, California, USA*
Manager: *Jonathan Petit*, **Mentor:** *Jean-Philippe Monteuuis*
- Executed real-world adversarial attacks on traffic sign detection systems to quantify vulnerabilities.
- Investigated the transferability of adversarial examples across diverse object detection models.
- Developed DVC-based pipelines for systematic dataset management and reproducible experiments.

[I2] **Interim Engineering Intern** **May 2022–Aug 2022**
QUALCOMM INCORPORATED *Boxborough, Massachusetts,, USA*
Manager: *Jonathan Petit*, **Mentor:** *Rashed Ansari*
- Researched and evaluated generative AI models (GANs) to synthesize realistic yet fake V2X messages.
- Designed a GAN-based misbehavior detection to effectively detect anomalous basic safety messages (BSMs).
- Continued the collaboration beyond internship and extended this project, which resulted in [C11,J3].

[I1] **Assistant Engineer (Electrical)** **Sep 2017 – Dec 2018**
ELECTRICITY GENERATION COMPANY BANGLADESH LTD. *Dhaka, Bangladesh*
Manager: *AKM Manzur Kadir*
- Operated a 2x120 MW gas turbine power plant by coordinating with the national load dispatch center.
- Developed operational and maintenance schedules to minimize downtime through proactive planning.

TEACHING EXPERIENCE

Lecturer, Department of Computer Science **May 2016 – May 2017**
UTTARA UNIVERSITY *Uttara, Dhaka, Bangladesh*
Taught the following undergraduate courses and led corresponding lab sessions:

- **EE 101: Electrical Circuits** Fall 2016
- **EE 205: Basic Electronics** Spring 2017
- **EE 210: Digital Logic Design** Fall 2016, Spring 2017
- **EE 315: Microprocessor Interfacing** Fall 2016, Spring 2017

Student Mentorship

- **Md Mohaimin Al Barat (PhD, Virginia Tech)**: Automotive Ethernet Testbed Implementation for Multimodal Fusion-based Perception in Autonomous Driving.
- **Md Shahedul Haque (MS, Virginia Tech)**: Defacing Technique in MRI data for Privacy Preserving Machine Learning for Healthcare Systems.
- **Samara Ruiz Sandoval (Undergrad, Florida International University)**: Deep Learning for Security of Smart Grid.

Featured

Amazon-Virginia Tech Initiative awards two student fellowships, five faculty research awards, VT News, 10/22/2024

Professional Engagement

- Graduate Student Member, Institute of Electrical and Electronics Engineers (IEEE)
- Member, Association for Computing Machinery (ACM)
- Campus Representative, Graduate Student Assembly (GSA) – DC Region, Virginia Tech, 2023

Professional Services

Artifact Evaluation Committee:

- ACM Conference on Computer and Communications Security (ACM CCS) (2025)

Journal Reviewer:

- IEEE Transactions on Big Data (TBD) 2025
- ACM Transactions on Cyber-Physical Systems (TCPS) 2025
- IEEE Transactions on Vehicular Technology (TVT) 2024
- IEEE Transactions on Computers (TC) 2024
- Computers & Security (C&S) 2024
- IEEE Sensors Journal (SJ) 2023
- IEEE Transactions on Information Forensics and Security (TIFS) 2023
- Vehicular Communications (VehiCom) 2023
- IEEE Power & Energy Society Transactions on Power Systems (IEEE PES) 2021
- International Journal of Electronic Security and Digital Forensics (IJESDF) 2021

External Conference Reviewer:

- IEEE Symposium on Security and Privacy (IEEE S&P) 2022–2025
- European Symposium on Research in Computer Security (ESORICS) 2022–2024
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2022–2025
- IEEE Conference on Communications and Network Security (IEEE CNS) 2022–2024
- International Conference on Computer Communication and Networks (ICCCN) 2023
- IEEE International Conference on Distributed Computing Systems (ICDCS) 2022
- IEEE International Conference on Communications (ICC) 2020
- International Symposium on Network Systems Security (NSysS) 2019

Organization:

- Student Volunteer, IEEE International Conference on Distributed Computing Systems (ICDCS), 2024
- Session Chair, IEOM North American Industrial Engineering and Operations Management Conference, 2022
- Judge, Engineering Section, Northern Virginia Regional Science Fair, 2022
- Student Volunteer, ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec), 2020

Google Scholar

h-index: 8, i10-index: 8, citations: 429 (as of 5 October, 2025)
Link to Google Scholar : https://scholar.google.com/citations?user=TcCzjTQAAAAJ&h

References

Available upon request.