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 lies at the intersection of cyber-physical systems (CPS), artificial intelligence (AI), and cybersecurity. I focus on uncovering and mitigating security vulnerabilities in safety-critical CPS—particularly in embodied AI systems such as connected and autonomous vehicles—by developing scalable, attack-resilient, and trustworthy AI frameworks that can operate safely under real-world uncertainty and adversarial conditions.

Education

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

- Dissertation: *Toward Trustworthy Cyber-physical Systems: Robust Machine Learning for Secure Sensing, Perception, and Control*
- Advisor: Dr. Wenjing Lou

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

- Thesis: *Deception Defense against Stealthy Attacks in Power Grids*
- Advisor: Dr. Mohammad Ashiqur Rahman

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**, *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] **Md Hasan Shahriar**, Mohammad Raashid Ansari, M. S. Haque, Jean-Philippe Monteuuis, Cong Chen, Jonathan Petit, Y. Thomas Hou, Wenjing Lou. "VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems." In *ACM Transactions on Cyber-Physical Systems **(ACM TCPS)***, 2025. (Impact Factor: 2.0).

[J2] **Md Hasan Shahriar**, Y. Xiao, P. Moriano, Wenjing Lou, Y. Thomas Hou. "CANShield: Deep Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal-Level." In *IEEE Internet of Things Journal **(IEEE IoT-J)***, 2023. (Impact Factor: 10.6).

[J1] **Md Hasan Shahriar**, M. A. Rahman, M. Jafari, S. Paudyal. "Formal Analytics for Stealthy Attacks against Contingency Analysis in Power Grids." In *Sustainable Energy, Grids and Networks **(SEGAN)***, 2024. (Impact Factor: 5.6).

Conference Papers (Selected)

[C12] **Md Hasan Shahriar**, Ning Wang, Naren Ramakrishnan, Y. Thomas Hou, Wenjing Lou. "Let the Noise Speak: Harnessing Noise for a Unified Defense Against Adversarial and Backdoor Attacks." In Proceedings of *European Symposium on Research in Computer Security (**ESORICS**)*, 2025. (Acceptance rate: 17%).

[C11] **Md Hasan Shahriar**, Mohammad Raashid Ansari, Jean-Philippe Monteuuis, Cong Chen, Jonathan Petit, Y. Thomas Hou, Wenjing Lou. "VehiGAN: Generative Adversarial Networks for Adversarially Robust V2X Misbehavior Detection Systems." In Proceedings of *IEEE International Conference on Distributed Computing Systems (**ICDCS**)*, 2024. (Acceptance rate: 21%).

[C10] **Md Hasan Shahriar**, Wenjing Lou, Y. Thomas Hou. "CANtropy: Time Series Feature Extraction-Based Intrusion Detection Systems for Controller Area Networks." In Proceedings of *Symposium on Vehicle Security and Privacy (**VehicleSec**)*, 2023. **Best Paper Runner-Up Award**. (Acceptance rate: 36.0%)

[C9] S. Shi, Y. Xiao, C. Du, **Md Hasan Shahriar**, A. Li, Ning Zhang, Y. Thomas Hou, Wenjing Lou. "MS-PTP: Protecting Network Timing from Byzantine Attacks." In Proceedings of *ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**)*, 2023. (Acceptance rate: 25.4%)

[C8] **Md Hasan Shahriar**, Y. Xiao, P. Moriano, Wenjing Lou, Y. Thomas Hou. "CANShield: Signal-based Intrusion Detection for Controller Area Networks." In *Embedded Security in Cars (**ESCAR**)*, 2022.

[C7] **Md Hasan Shahriar**, Mohammad Ashiqur Rahman, Nur Imtiazul Haque, Badrul Chowdhury, S. G. Whisenant. "iDDAF: An Intelligent Deceptive Data Acquisition Framework for Secure Cyber-Physical Systems." In Proceedings of *EAI International Conference on Security and Privacy in Communication Networks (**SecureComm**)*, 2021. (Acceptance rate: 34%)

[C6] **Md Hasan Shahriar**, Mohammad Ashiqur Rahman, Nur Imtiazul Haque, Badrul Chowdhury. "DDAF: Deceptive Data Acquisition Framework against Stealthy Attacks in Cyber-Physical Systems." In Proceedings of *IEEE 45th International Conference on Software Engineering (**COMPSAC**)*, 2021. (Acceptance rate: 27%)

[C5] **Md Hasan Shahriar**, Alvi Ataur Khalil, Mohammad Ashiqur Rahman, Mohammad Hossein Manshaei, Dong Chen. "iAttackGen: Generative Synthesis of False Data Injection Attacks in Cyber-Physical Systems." In Proceedings of *IEEE Conference on Communications and Network Security (**CNS**)*, 2021. (Acceptance rate: 26%)

[C4] M. Jafari, **Md Hasan Shahriar**, Mohammad Ashiqur Rahman, S. Paudyal. "False Relay Operation Attacks in Power Systems with High Renewables." In Proceedings of *IEEE Power & Energy Society General Meeting (**PESGM**)*, 2021.

[C3] Nur Imtiazul Haque, **Md Hasan Shahriar**, Md Golam Dastgir, Anjan Debnath, Imtiaz Parvez, Arif Sarwat, and Mohammad Ashiqur Rahman. "Machine Learning in Generation, Detection, and Mitigation of Cyberattacks in Smart Grid: A Survey." In Proceedings of *North American Power Symposium* (**NAPS**), 2021.

[C2] **Md Hasan Shahriar**, Nur Imtiazul Haque, Mohammad Ashiqur Rahman, Miguel Alonso Jr. "G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System." In Proceedings of *IEEE 45th International Conference on Software Engineering (**COMPSAC**)*, 2020. (Acceptance rate: 24%)

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

Theses

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

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

[T1] **Md Hasan 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)

[**O4**] Kuan Yu Chen, **Md Hasan Shahriar**, Wen Wei Li, Shi Cho Cha, Wenjing Lou. "HotWire: Real-World Impersonation and Discharge Attacks on Electric Vehicle Charging Systems" Under review at *IEEE Symposium on Security and Privacy (**S&P**)*, 2026.

[**O3**] **Md Hasan Shahriar**, Ning Wang, Amit Kumar Sikder, Naren Ramakrishnan, Y. Thomas Hou, Wenjing Lou. "Noise, Why Can't You Bend? Detecting Adversarial Perturbations in Wireless Sensing via Structural Fragility" Under review at *ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, 2026.

[**O2**] **Md Hasan Shahriar**, Mohaimin Al Barat, Harshavardhan Sundar, Ning Zhang, Naren Ramakrishnan, Y. Thomas Hou, Wenjing Lou. "Temporal Misalignment Attacks against Multimodal Perception in Autonomous Driving" Under review at *IEEE Conference on Secure and Trustworthy Machine Learning (**SaTML**)*, 2026.

[**O1**] **Md Hasan Shahriar**, Mohaimin Al Barat, Harshavardhan Sundar, Ning Zhang, Naren Ramakrishnan, Y. Thomas Hou, Wenjing Lou. "Detecting Temporal Misalignment Attacks in Multimodal Fusion for Autonomous Driving" Under review at *The International Conference on Learning Representations (**ICLR**)*, 2026.

Presentations & Talks

Invited Research Talks:

- *"Temporal Misalignment Attack against Multimodal Fusion in Autonomous Driving"*
  4th Workshop on Future Automotive Research Datasets, November 2025.
- *"Security of Connected and Autonomous Vehicles: From In-vehicular Networks to Multimodal Fusion"*
  Amazon VT Initiative Kickoff, Invited Talk, Blacksburg, VA, Fall 2024.
- *"Generating State-of-the-art V2X Misbehavior Detection Dataset and a Robust Detection Approach"*
  3rd Workshop on Future Automotive Research Datasets, April 2024.
- *"CANShield: Signal-based Intrusion Detection for Controller Area Networks"*,
  1st Workshop on Future Automotive Research Datasets, April 2021 and
  ACIC–DoD ROLLCAGE TEM, November 2021.
- *"A Survey on CAN Intrusion Detection Dataset"*
  1st Workshop on Automotive Research Datasets, November 2021.
- *"Deception-based Defense against False Data Injection Attacks in Power Grids"*
  CAPER Meeting (Virtual), 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.

Sponsored Research Projects (Contributor)

List of funded research projects to which I contributed as a *Graduate Research Assistant* during my M.S. and Ph.D. studies.

- **ONR Grant**. U.S. Office of Naval Research (Award #N00014-24-1-2730)
  Byzantine Resilient Federated Learning in Sporadically Connected Wireless Networks
- **NSF CPS: Medium**. U.S. National Science Foundation (Award #2235232)
  Robust Sensing and Learning for Autonomous Driving Against Perceptual Illusion
- **NSF NeTS: Medium**, U.S. National Science Foundation, (Award #2312447)
  An Integrated Multi-Time Scale Approach to High-Performance, Intelligent, and Secure O-RAN based NextG
- **ONR MURI Grant**. U.S. Office of Naval Research (Award #N00014-19-1-2621)
  Science of Tracking, Control, and Optimization of Information Latency for Dynamic Military IoT Systems
- **NSF SaTC: CORE: Medium**. U.S. National Science Foundation (Award #1916902)
  Toward Enforceable Data Usage Control in Cloud-based IoT Systems
- **NSF CPS: Medium**. U.S. National Science Foundation (Award #CNS-1837519)
  S2Guard: Building Security and Safety in Autonomous Vehicles via Multi-Layer Protection
- **NSF CRII**. U.S. National Science Foundation (Award #CNS-1929183)
  Noninvasive Security Analysis for Smart Grid Energy Management System

Research Appointments

[R3] **Graduate Student Researcher** **2021 – Present**
Complex Network and Security Research (CNSR) Lab, Virginia Tech *Arlington, Virginia, USA*
Advisor: *Dr. Wenjing Lou*
My Ph.D. research integrates cybersecurity, machine learning, and CPS to develop robust, resilient, and trustworthy AI for connected and autonomous vehicles. I designed intrusion detection systems for CAN and V2X networks to counter stealthy and adversarial attacks [J1, J2; C6–C9], investigated network-induced and multimodal fusion attacks on autonomous perception [O1–O2], and developed a unified defense framework that mitigates both adversarial and backdoor ML threats across diverse modalities [C10; O3]. In addition, I mentored several graduate students whose work contributed to peer-reviewed and ongoing publications.

[R2] **Graduate Student Researcher** **2019–2020**
Analytics for Cyber Defense (ACyD) Lab, Florida International University *Miami, Florida, USA*
Advisor: *Dr. Mohammad Ashiqur Rahman*
My M.S. research focused on securing cyber-physical systems, particularly detecting and mitigating stealthy threats in the smart grid. I developed a threat synthesizer combining formal methods and GANs to model complex attack behaviors [J1, C4, C5]. Building on this, I proposed a deception-based moving target defense to counter stealthy intrusions [C6, C7] and explored GAN-based defense models for network security [C2, C3], while mentoring several undergraduate researchers.

[R1] **Undergradudate Student Researcher** **2014–2016**
Bangladesh University of Engineering and Technology *Dhaka, Bangladesh*

Advisor: *Dr. Forkan Uddin*
My undergraduate research focused on analyzing the robustness of different Maximum Power Point Tracking algorithms for the smart grid under cyberattacks and developing strategies to improve system resilience [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 adversarial robustness.
- 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*

- 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

- **Kuan Yu Chen (MS, National Taiwan University of Science and Technology)**: EV Charging Security.
- **Md Mohaimin Al Barat (PhD, Virginia Tech)**: Security of Multimodal Fusion in Autonomous Driving.
- **Sydney Johns (PhD, Virginia Tech)**: Practical Intrusion Detection Systems for Cyber-physical Systems.
- **Md Shahedul Haque (MS, Virginia Tech)**: Defacing Technique in MRI data for Privacy Preserving ML.
- **Samara Ruiz Sandoval (Undergrad, Florida International University)**: ML for Security of Smart Grid.

Featured

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

Professional Services

Artifact Evaluation Committee:

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

Journal Reviewer:

- IEEE Internet of Things Journal (IoT-J) — 2025
- 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:

• ACM ASIA Conference on Computer and Communications Security (AsiaCCS)	2025
• 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

Community and Outreach Involvement:

- Student Volunteer, IEEE International Conference on Distributed Computing Systems (ICDCS), 2024
- Session Chair, IEOM North American Industrial Engineering and Operations Management Conference, 2022
- Student Volunteer, ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec), 2020
- Judge, Engineering Section, Northern Virginia Regional Science Fair, 2022
- Campus Representative, Graduate Student Assembly (GSA) – DC Region, Virginia Tech, 2023

References

Dr. Wenjing Lou
IEEE Fellow, ACM Fellow
W. C. English Endowed Professor
Department of Computer Science
Virginia Tech
900 N Glebe Road, Arlington, VA 22203
Email: wjlou@vt.edu
Phone: (703)-538-3774

Dr. Y. Thomas Hou
IEEE Fellow
Bradley Distinguished Professor
Department of Electrical and Computer Engineering
Virginia Tech
2040-K Torgersen Hall, Blacksburg, VA 24061
Email: thou@vt.edu
Phone: (540) 231-2950

Dr. Naren Ramakrishnan
IEEE Fellow, ACM Fellow, AAAS Fellow
Thomas L. Phillips Professor of Engineering
Department of Computer Science
Virginia Tech
3625 Potomac Avenue, Alexandria, VA 22305
Email: naren@vt.edu
Phone: (571) 858-3331

Dr. Ning Zhang
Associate Professor
Department of Computer Science and Engineering
Washington University in St. Louis
1 Brookings Drive, St. Louis, MO 63130
Email: zhang.ning@wustl.edu
Phone: (314)-935-6576