

Md Nazmul Kabir Sikder

Norfolk, VA | msikder@odu.edu | +1 (571) 277-0159

Publications appear under *M. N. K. Sikder*; pre-2016 work under *N. K. Sikder*.

Professional Summary

Research Assistant Professor focused on Generative AI security, cybersecurity, critical infrastructure protection, and trustworthy embedded AI. Previously a Presidential Postdoctoral Fellow specializing in secure, privacy-aware, and explainable AI for critical infrastructure. My research spans hybrid AI, including LLMs, agentic AI, computer vision, and time-series forecasting, to secure AI-enabled systems, support anomaly detection, and enable robust decision-making in cyber-physical environments, with interdisciplinary publications and contributions to NSF proposal development.

Areas of Expertise

- **Critical Infrastructure and Control Systems.** SCADA and industrial control system (ICS) security; water and wastewater treatment systems; operational technology (OT) monitoring; cyber-physical system resilience.
- **Cybersecurity.** Intrusion detection and automated response; IoT and cross-layer (network/host) threat detection; adversarial machine learning; threat-intelligence grounding (MITRE ATT&CK, CVE/NVD).
- **Artificial Intelligence.** Security and trustworthiness of large language models and agentic AI systems; AI assurance, validation, and explainability; anomaly detection; time-series forecasting; generative modeling (GANs, diffusion models).
- **Digital Media Forensics.** Detection and source attribution of synthetic and adversarially manipulated imagery.
- **Telecommunications.** LTE radio access network rollout, operations, and monitoring automation.

Expert Witness and Litigation Consulting Experience

No prior expert witness engagements, reports, depositions, or trial testimony as of July 2026.

Academic Appointments

- **Old Dominion University, Norfolk, VA**
Research Assistant Professor, December 2025 – Present.
- **Virginia Tech, Arlington, VA**
Presidential Postdoctoral Fellow, January 2025 – December 2025.

- **Virginia Tech**, Arlington, VA
Graduate Research Assistant, August 2019 – December 2024.

Honors and Fellowships

- **Presidential Postdoctoral Fellow** (competitive university-wide fellowship), Virginia Tech (2025).

Education

- **Virginia Polytechnic Institute and State University** Arlington, VA
Ph.D., Computer Engineering, August 2019 – December 2024.
Doctoral Dissertation: Sikder, M. N. K. (2024). *AI Methods for Anomaly Detection in Cyber-Physical Systems: With Application to Water and Agriculture*. Ph.D. dissertation, Virginia Polytechnic Institute and State University. Advisor: Feras A. Batarseh. [PDF]
- **Virginia Polytechnic Institute and State University** Falls Church, VA
M.S., Computer Engineering, August 2019 – May 2022. GPA: 3.67/4.0
- **Bangladesh University of Engineering and Technology (BUET)** Dhaka, Bangladesh
B.S., Electrical and Electronic Engineering, May 2010 – September 2015. GPA: 3.65/4.0

Awards and Recognition

- Winner, *2022 Intelligent Water Systems Challenge* (The Water Research Foundation).
<https://www.waterrf.org/news/2022-intelligent-water-systems-challenge>
- Awarded 2nd best team, line following robot contest (BUET), 2014.

Research Interests

Security and Trustworthiness of LLMs and Agentic AI; Cybersecurity; Trustworthy and Secure Embedded AI for Cyber-Physical Systems; Anomaly Detection and AI Assurance.

Publications

Doctoral Dissertation

Sikder, M. N. K. (2024). *AI Methods for Anomaly Detection in Cyber-Physical Systems: With Application to Water and Agriculture*. Ph.D. dissertation, Virginia Polytechnic Institute and State University. Chair: Feras A. Batarseh. <https://hdl.handle.net/10919/124470>

Refereed Journal Articles

1. Sikder, M. N. K., & Batarseh, F. A. (2025). *Context-driven Deep Learning Forecasting for Wastewater Treatment Plants*. ACM Transactions on Cyber-Physical Systems. DOI: <https://doi.org/10.1145/3744350>

2. Sikder, M. N. K., Wang, Y., & Batarseh, F. A. (2025). *Assessing the Fidelity and Utility of Water Systems Data Using Generative Adversarial Networks: A Technical Review*. IEEE Access. DOI: <https://doi.org/10.1109/ACCESS.2025.3577969>
3. Sikder, M. N. K., Nguyen, M. B., Elliott, E. D., & Batarseh, F. A. (2023). *Deep H2O: Cyber attacks detection in water distribution systems using deep learning*. Journal of Water Process Engineering, 52, 103568. DOI: <https://doi.org/10.1016/j.jwpe.2023.103568>
4. Kulkarni, A., Yardimci, M., Kabir Sikder, M. N., & Batarseh, F. A. (2023). *P2O: AI-Driven Framework for Managing and Securing Wastewater Treatment Plants*. Journal of Environmental Engineering, 149(9), 04023045. DOI: <https://doi.org/10.1061/JOEEDU.EEENG-7266>

Refereed Conference Proceedings

1. Sikder, M. N. K., Batarseh, F. A., Wang, P., & Gorentala, N. (2022). *Model-Agnostic Scoring Methods for Artificial Intelligence Assurance*. In 2022 IEEE 29th Annual Software Technology Conference (STC) (pp. 9–18). IEEE. DOI: <https://doi.org/10.1109/STC55697.2022.00011>
2. Gurrapu, S., Batarseh, F. A., Wang, P., Sikder, M. N. K., Gorentala, N., & Gopinath, M. (2021). *DeepAg: Deep Learning Approach for Measuring the Effects of Outlier Events on Agricultural Production and Policy*. In *Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1–8), Orlando, FL, USA. DOI: <https://doi.org/10.1109/SSCI50451.2021.9659921>
3. Usman, M. U., Haque, A., Sikder, M. N. K., Cai, M., Bradley, S. R., Pandey, S., Kliros, C., & Zhang, L. (2021). *Quantification of Peak Demand Reduction Potential in Commercial Buildings due to HVAC Set Point and Brightness Adjustment*. 2021 IEEE Power & Energy Society General Meeting (PESGM), 1–6. DOI: <https://doi.org/10.1109/PESGM46819.2021.9638053>
4. Chakma, S., Sikder, N. K., Khan, S. I., & Akhter, S. (2015). *Implementation of microcontroller based Maximum Power Point Tracker (MPPT) using SEPIC converter*. 2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), 374–377. DOI: <https://doi.org/10.1109/WIECON-ECE.2015.7443942>

Book Chapters

1. Sikder, M. N. K., & Batarseh, F. A. (2023). *Outlier detection using AI: a survey*. In *AI Assurance: Towards Valid, Explainable, Fair, and Ethical AI* (pp. 231–291). Academic Press. DOI: <https://doi.org/10.1016/B978-0-32-391919-7.00020-2>
2. Williams, M. J., Sikder, M. N. K., Wang, P., Gorentala, N., Gurrapu, S., & Batarseh, F. A. (2023). *The application of artificial intelligence assurance in precision farming and agricultural economics*. In *AI Assurance: Towards Valid, Explainable, Fair, and Ethical AI* (pp. 501–529). Academic Press. DOI: <https://doi.org/10.1016/B978-0-32-391919-7>

Preprints / Technical Reports

1. Nguyen, M. B. T., Sikder, M. N. K., & Wang, C. (2022). *Time-Series Generative Adversarial Networks for Cyber-Physical Systems*. Technical report and open-source release. [PDF]

Posters and Presentations

1. Gurrapu, S., Sikder, N., Wang, P., Gorentala, N., Williams, M., & Batarseh, F. A. (2021). *Applications of Machine Learning for Precision Agriculture and Smart Farming*. The International FLAIRS Conference Proceedings, 34. DOI: <https://doi.org/10.32473/flairs.v34i1.128497>
2. Batarseh, F. A., Yardimci, M. O., Suzuki, R., Sikder, M. N. K., Wang, Z., & Mao, W. (2022). *Realtime Management of Wastewater Treatment Plants Using AI*. Virginia Tech & DC Water. https://www.waterrf.org/sites/default/files/file/2022-11/2022_IWS-Challenge-Solution_Virginia-Tech.pdf

Research Funding and Grant Activity

Awarded

- **Commonwealth Cyber Initiative (CCI)**. *Agentic AI for Scalable and Cost-Effective Protection of Critical Infrastructure*. Total award: \$100000; period: 1 Year. Role: [Co-PI / Senior Personnel]. PI: Daniel Takabi; Co-PIs: Murat Kantarcioglu Institution: Old Dominion University, Virginia Tech

Submitted / Under Review

- **National Science Foundation (Cyber-Physical Systems Program)**. *Securing Water and Agricultural Cyber-Physical Systems Using Foundational AI*. Total budget: \$1,000,000; duration: 4 years. Role: Senior Personnel and Methodology Lead. PI: Feras A. Batarseh; Co-PIs: Manish Bansal, Jonathan Czuba, Dong Ha, Abhilash Chandel, Azahar Ali. Institution: Virginia Tech. Submitted.

Planned/Targeted Proposals (PI or Co-PI)

- **NSF Secure and Trustworthy Cyberspace (SaTC 2.0)**. Proposed topic: Secure and trustworthy generative-AI systems for cyber-physical and critical-infrastructure security (e.g., water and energy). Status: Concept development and team formation; target submission in 2026.
- **NSF Cyber-Physical Systems (CPS)**. Proposed topic: AI-enabled security, privacy, and resilience for networked and embedded cyber-physical systems in critical infrastructure. Status: Planned proposal leveraging CPS testbeds and prior foundations; target submission

in 2026.

- **DARPA (I2O) – Office-Wide BAA.** Proposed topic: Robust and secure agentic-AI and generative-AI systems for cyber operations and critical-infrastructure defense. Status: White-paper/abstract planning; rolling opportunities through 2026.
- **Office of Naval Research (ONR) – Long-Range BAA.** Proposed topic: Trustworthy AI and secure machine learning for resilient cyber-physical and autonomous systems. Status: Concept development; rolling opportunities through 2026.
- **Anthropic-National Lab Partnerships (e.g., PNNL / DOE).** Proposed topic: AI-accelerated adversary emulation and cyber-defense for water, energy, and industrial control systems, inspired by Claude-based red-teaming on CPS testbeds. Status: Concept development for public-private collaborative proposals.

Research Experience

Research Assistant Professor – Old Dominion University

- Serving as Co-Investigator on a CCI-funded program developing agentic AI for scalable, cost-constrained protection of critical infrastructure, spanning threat detection, automated response, and operational deployment cost.
- Designed and implemented H-CLAIR, a two-tier cross-layer intrusion detection and response framework pairing an always-on lightweight ensemble (isolation forest, random forest, autoencoder, TabNet, graph attention networks) fused by weight-of-evidence log-odds with an LLM verifier grounded in MITRE ATT&CK and CVE/NVD, and a constrained-MDP response agent operating over a bounded action space. Evaluated across network and host layers on ToN_IoT, SWaT, and WADI.
- Built a production-grade agentic anomaly detection pipeline for multilayer network data on the Wahab HPC cluster (SLURM scheduling, H100 GPUs, containerized inference, retrieval-augmented multi-model ensemble).
- Improved graph deviation network (GDN) anomaly detection on industrial control system benchmarks via orthogonal initialization, a frozen reconstruction decoder, and model ensembling, raising significant performance over the published baseline.
- Authored or co-authored 2 federal and foundation proposals, including NSF SaTC and Schmidt Sciences submissions.
- Supervising 2 graduate students.

Presidential Postdoctoral Fellow – Virginia Tech, Commonwealth Cyber Initiative (CCI)

- Leading the design and prototyping of LLM- and computer-vision-based anomaly detection systems for critical infrastructure, including benchmarked evaluation harnesses comparing classical and deep learning approaches to reduce false alerts.

- Developing production-ready trustworthy-AI components, including data-quality validation, retraining triggers, model cards, and containerized inference pipelines in collaboration with interdisciplinary engineering and operations teams.
- Serving as Senior Personnel and methodology lead on a large-scale NSF CPS proposal, contributing to system architecture, experimental design, and evaluation frameworks for trustworthy AI in cyber-physical systems.

Graduate Research Assistant – Virginia Tech, Commonwealth Cyber Initiative (CCI)

- Developed advanced AI models (High Confidence AutoEncoders, GANs) for real-time cyber-physical threat detection in water supply systems.
- Built a context-aware forecasting framework (Temporal Fusion Transformer) integrating external data for improved water systems prediction.
- Developed AI-based decision support and anomaly detection for SCADA using deep recurrent models (LSTM/GRU).
- Applied isolation-forest-based modeling for agricultural production forecasting and policy analysis.
- Contributed to AI assurance methods for fairness, security, and explainability across applied AI systems.

Graduate Research Assistant – Virginia Tech (Advanced Research Institute)

- Developed data-driven energy-efficient building models using real-time data to support HVAC optimization.
- Performed demand-response analysis for appliance scheduling and AI-based policy recommendations.

Undergraduate Student – BUET Projects (Selected)

- Power electronics and renewable energy systems: LED driver design; DC–AC conversion; SEPIC-based solar charge controller (thesis).
- Embedded systems and robotics: microcontroller-based maze solver; line-following robot; color-detecting camera using Arduino.
- Signal processing and pattern recognition: MATLAB-based voice pitch analysis; recognition of alphanumeric characters.

Teaching

Teaching Experience

- **Research Mentoring (Virginia Tech).** Mentored graduate students on experimental design, reproducible ML practice, and scientific writing in secure AI for cyber–physical systems.

- **Technical Training (DC Water / AlexRenew research teams).** Delivered internal tutorials on deep learning model development and evaluation for time-series anomaly detection and computer-vision robustness.

Teaching Interests

Trustworthy and Secure AI; Cybersecurity and Critical Infrastructure; Machine Learning for Cyber-Physical Systems; Generative AI and LLM Security; Applied Deep Learning (Vision and Time Series); AI Assurance and Anomaly Detection.

Industry and Professional Experience

AI Systems Lead – DC Water Operational Analytics, Washington, DC (2023–2025)

- Led development, deployment, and validation of AI-driven embedded systems for real-time wastewater tunnel monitoring and anomaly detection at one of the largest municipal water utilities in the United States.
- Delivered production components in live operational use: data-quality validation, retraining triggers, model cards, and containerized inference pipelines, in direct collaboration with utility engineering and operations staff.
- Benchmarked deep learning approaches against classical baselines to reduce false alert rates supporting operator decision-making.

BEM Controls LLC, McLean, VA (Graduate Research Intern, May 2020 – Aug. 2020)

- Developed and tested enterprise-level smart grid software (BEMOSS) for device-level load control across heterogeneous communication protocols and demand response estimation.

Grameenphone Ltd., Dhaka, Bangladesh (System Engineer, Oct. 2015 – Jul. 2019)

- Led LTE network rollout execution in Dhaka city; recognized for rapid rollout performance.
- Designed and maintained a Telegram BOT Android application for network monitoring and maintenance.
- Developed protection systems and operational tools (billing automation; fuel generator controller) reducing operational expenditures.

Advising and Mentoring

- **Trey Ward** (M.S. Student, Virginia Tech). Co-mentored for a journal manuscript in preparation for *Nature Scientific Reports* on secure and trustworthy computer vision for agricultural cyber-physical systems. Supervised problem formulation, experimental design, model development, and manuscript preparation.

- **Shubham Deshmukh** (M.S. Student, Virginia Tech). Co-mentored on the same research project, contributing to dataset generation, adversarial and generative modeling pipelines, and evaluation of detection and attribution models.
- Research project: *Unified Detection and Attribution of Synthetic and Adversarial Images in Agricultural Cyber-Physical Systems*. Led the design of a multi-generator evaluation framework using GANs (StyleGAN2, StyleGAN3, R3GAN) and diffusion models (Instruct-Pix2Pix, BLIP-Diffusion, Dreamshaper-8) across multiple crops (apple, maize, tomato), and guided the use of CNN and Vision-Transformer backbones (EfficientNet-B0, ResNet-50, CLIP) for health-state classification, source detection, and generator attribution.
- Trained students in reproducible ML pipelines, dataset curation, cross-model evaluation, and scientific writing for high-impact interdisciplinary venues bridging AI, cybersecurity, and agriculture.

Professional Service

Proposal Review and Panel Service

- **Commonwealth Cyber Initiative (CCI), Virginia – External Reviewer (2025)**
Reviewed and formally scored proposals for the CCI Request for Proposals: *Cybersecurity for Critical Infrastructure*.
 - *HPC-LEAKSCAN: A Holistic Data Leakage Detection Framework for GPU-Accelerated High Performance Computing Infrastructure* Principal Investigators: Xiaokuan Zhang (George Mason University), Jie Ren (William & Mary). Total award requested: \$100,000.
 - *Graceful Degradation in the Air: Operational Resilience in Drone-Based Emergency Deliveries* Principal Investigators: Vikas Ashok (Old Dominion University), Samy El-Tawab (James Madison University). Total award requested: \$100,000.

Peer Review and Editorial Service

- **Environmental Monitoring and Assessment** (Springer Nature). Reviewer for manuscript on AI-based intelligent environmental monitoring using hybrid optimization and reinforcement learning (SFFO-RL) (2026).
- **Journal of the ASABE** (American Society of Agricultural and Biological Engineers). Reviewer for manuscript on AI-driven cybersecurity and resilience in agricultural cyber-physical systems (2025).
- **Journal of Computer Virology and Hacking Techniques** (Springer Nature). Reviewer for “A Hybrid Heuristic Framework for Severity Prediction in Network-Based Intrusions: Integrating Virology-Inspired Algorithms with Ensemble Learning” (2025).
- **Scientific Reports** (Nature Portfolio). “Data Driven Water Quality Assessment using Machine Learning and Synthetic Data Generation” (2025).
- **International Journal of Data Science and Analytics** (Springer Nature). “A

Multi-Stage Hybrid Deep Learning Framework for Interpretable Anomaly Detection in Environmental Sensor Networks” (2025).

- **Environmental Health** (Springer Nature). “Adaptive Binary Search Trees for Real-Time Environmental Intelligence: A Novel Framework for Multi-Scale Climate and Pollution Monitoring Systems” (2025).
- **SN Computer Science** (Springer Nature). “Remote Sensing Images for Water Quality Monitoring Based on Deep Learning Model” (2025).
- **Neural Computing and Applications** (Springer Nature). Formally nominated by Prof. Feras A. Batarseh to serve as reviewer for “Optimizing Hyper-parameter Configurations in Deep LSTM Networks for Enhanced Forecasting of Sea Water Tidal Shifts” (2025).
- **Journal of Cybersecurity and Privacy** (MDPI). “A Comprehensive Review: The Evolving Cat-and-Mouse Game in Network Intrusion Detection Systems Leveraging Machine Learning” (2025).

Leadership and Outreach

- **AI Systems Lead, DC Water Operational Analytics (2023–2025)**. Led the development, deployment, and validation of AI-driven embedded systems for real-time wastewater tunnel monitoring and anomaly detection, supporting operational decision-making and system reliability for one of the largest municipal water utilities in the United States.
- Volunteer, **IEEE Innovation Smart Grid Technologies (ISGT)**, North America, 2020.
- Volunteer, **AEE World Energy Conference and Expo**, Washington, DC, 2019.
- Coordinator, **Inter-university Project Show and Departmental Festival**, 2014.
- Organizing Member, **PES 2014 Inter-university Robotics Competition**, BUET Energy Club.

Selected Talks and Presentations

- **SDSS 2022** – Presentation: *Model-Agnostic Scoring Methods for Artificial Intelligence Assurance* (2022).

Open-Source Software and Datasets

- **Context-Driven Forecasting (Dataset + Code)**. Dataset and reproducible software package supporting the context-driven forecasting study (time-series data processing, modeling, and evaluation). https://github.com/nazmulkabir/Context_water
- **AgriVision Synthetic/Adversarial Image Detection (Dataset + Framework)**. Curated dataset for synthetic/adversarial image detection in agriculture and an accom-

panying benchmark framework for detection/attribution experiments. <https://github.com/AI-VTRC/AgriVision.AI>

Professional Memberships

- **Institute of Electrical and Electronics Engineers (IEEE)** – Member; IEEE Computer Society.
- **Association for Computing Machinery (ACM)** – Member.

Media Coverage

- Intelligent Water Systems Challenge winner coverage (The Water Research Foundation). <https://www.waterrf.org/news/2022-intelligent-water-systems-challenge>
- Virginia Tech media: AI solution implementation in DC Water. https://vtx.vt.edu/videos/k/2022/09/1_029flkz1.html
- Commonwealth Cyber Initiative news: protecting water systems from cyber threats. <https://cyberinitiative.org/cci-news/2022>

Technical Skills

- **Programming:** Python, C++, SQL
- **ML/AI:** PyTorch, TensorFlow, Keras; Hugging Face Transformers; Ray RLlib
- **Data:** Pandas, NumPy, Scikit-learn; Apache Spark
- **DevOps/MLOps:** Docker, Kubernetes, Jenkins, Apache Airflow; MLflow; Weights & Biases; Terraform
- **Cloud/Edge:** AWS (SageMaker), Azure, Google Cloud; TensorFlow Lite; AWS IoT
- **Security:** OpenSSL, JWT, PyCrypto

References

- **Dr. Feras A. Batarseh** (Ph.D. Chair), Associate Professor, Biological Systems Engineering, Virginia Tech.
batarseh@vt.edu | 571-858-3126
- **Dr. Luiz A. DaSilva** (Ph.D. Co-chair), Bradley Professor of Cybersecurity and Executive Director, Commonwealth Cyber Initiative, Virginia Tech.
Virginia Tech Research Center – Arlington, 900 N. Glebe Road, Arlington, VA 22203.
ldasilva@vt.edu | 571-858-3251
- **Dr. Vassilis Kekatos**, Associate Professor, Elmore Family School of Electrical and Computer Engineering, Purdue University.
[REAL-ADDRESS]@purdue.edu | 765-494-5486
- **Dr. Daniel Takabi**, Professor and Batten Endowed Chair in Cybersecurity, School of Cybersecurity, Old Dominion University.

takabi@odu.edu | 757-683-4586