

Shaikh Akib Shahriyar

Ph.D. Candidate in Computing and Information Sciences

 akibshahriyar8751@gmail.com  Rochester, NY
 [linkedin.com/in/akibshahriyar](https://www.linkedin.com/in/akibshahriyar)  Google Scholar

AI Security • Adversarial Machine Learning • Multimodal Robustness • Secure Agentic AI • Synthetic-Media Forensics

Academic Appointments

Adjunct Faculty

Rochester Institute of Technology

Dec. 2024 – May 2025
Rochester, NY

Assistant Professor

Khulna University of Engineering & Technology (KUET)
Held concurrently with Ph.D. studies through approved institutional study leave until formal resignation in September 2023.

Jan. 2021 – Sep. 2023
Khulna, Bangladesh

Lecturer

Khulna University of Engineering & Technology (KUET)

Jan. 2018 – Dec. 2020
Khulna, Bangladesh

Lecturer

North Western University (NWU)

May 2017 – Dec. 2017
Khulna, Bangladesh

Education

Ph.D. in Computing and Information Sciences

Rochester Institute of Technology, Rochester, NY

Fall 2026 (expected)

Advisor: Dr. Matthew Wright

Dissertation: RobustDF: Developing a Practical and Robust Defense Framework for Deepfake Detection

M.Sc. Eng. in Computer Science and Engineering

Khulna University of Engineering & Technology, Khulna, Bangladesh

2019

Thesis: Speech Enhancement Using Convolutional Denoising Autoencoder

B.Sc. Eng. in Computer Science and Engineering

Khulna University of Engineering & Technology, Khulna, Bangladesh

2017

Thesis: An Efficient Error Correction Approach by Using Successive Parity Generation

Ranked **1st of 59** in Computer Science and Engineering and **1st of 390** in the Faculty of Electrical and Electronic Engineering.

Research Interests

AI security and Adversarial machine learning; Multimodal practical robustness; Deepfake and synthetic-media forensics; Multi-Agent system security; Task-preserving attacks and authorization-aware agent evaluation; Persistent-memory security.

Under Review Manuscripts

- U1. **Shaikh Akib Shahriyar**, Ben Brown, Armon Barton, Ning Zhang, Matthew Wright, “SoK: The Practical Robustness Frontier: Cost-Aware Vulnerability Analysis for Deepfake Detectors,” *Manuscript in preparation for the 48th IEEE Symposium on Security and Privacy (S&P)*, 2027.
- U2. **Shaikh Akib Shahriyar**, Akil Iftae, Armon Barton, Matthew Wright, “What Counts as the Same Task? Executable Contracts for Robustness Evaluation of Tool-Using Agents,” *under review at the 26th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2027.

Peer-Reviewed Publications

Journal Articles

- J1. Armon Barton, Matthew Wright, **Shaikh Akib Shahriyar**, Edgar Jatho, Mohammad Saidur Rahman, Kantha Girish Gangadhara, Jiang Ming, “PadNet: Defending Neural Networks Against Adversarial Examples,” *ACM Transactions on Privacy and Security*, 2026.

- J2.** Anas Basalamah, Mahedi Hasan, Shovan Bhowmik, **Shaikh Akib Shahriyar**, “A Highly Accurate Dysphonia Detection System Using Linear Discriminant Analysis,” *Computer Systems Science and Engineering*, 2023.
- J3.** M. A. H. Akhand, Safial Islam Ayon, **Shaikh Akib Shahriyar**, N. Siddique, H. Adeli, “Discrete Spider Monkey Optimization for Traveling Salesman Problem,” *Applied Soft Computing*, 2020.

Conference & Workshop Papers

- C1.** Anton Selitskiy, **Shaikh Akib Shahriyar**, Jishnuraj Prakasan, “Discrete Optimal Transport is a Strong Audio Adversarial Attack,” *IEEE/IAPR International Joint Conference on Biometrics (IJCB)*, to appear, 2026.
- C2.** **Shaikh Akib Shahriyar**, Matthew Wright, Armon Barton, “IVORY: Adversarial Purification of Obfuscated Faces to Extract Soft-Biometrics using Diffusion Transformers,” *IEEE International Conference on Automatic Face and Gesture Recognition (FG)*, 2025.
- C3.** **Shaikh Akib Shahriyar**, Matthew Wright, “Evaluating Robustness of Sequence-based Deepfake Detector Models by Adversarial Perturbation,” *Workshop on Security Implications of Deepfakes and Cheapfakes (WDC @ ACM AsiaCCS)*, 2022.
- C4.** **Shaikh Akib Shahriyar**, Shovan Bhowmik, Mahedi Hasan, “DNA Cryptography-Based Speech Security System,” *International e-Conference on Intelligent Systems and Signal Processing (eISSP)*, Springer, 2022.
- C5.** Iftekhher Toufique Imam, Yamin Arafat, Kazi Saeed Alam, **Shaikh Akib Shahriyar**, “DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents,” *International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, 2021.
- C6.** Raisa Tahsin, Mahmudul Hasan Mozumder, **Shaikh Akib Shahriyar**, Md Abdus Salim Mollah, “A Novel Approach for E-mail Classification Using FastText,” *IEEE Region 10 Symposium (TENSYP)*, 2020.
- C7.** M. I. R. Shuvo, **Shaikh Akib Shahriyar**, M. A. H. Akhand, “Bangla Numeral Recognition from Speech Signal Using Convolutional Neural Network,” *International Conference on Bangla Speech and Language Processing (ICBSLP)*, IEEE, 2019.
- C8.** Safial Islam Ayon, M. A. H. Akhand, **Shaikh Akib Shahriyar**, N. Siddique, “Spider Monkey Optimization to Solve Traveling Salesman Problem,” *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, IEEE, 2019.
- C9.** **Shaikh Akib Shahriyar**, M. A. H. Akhand, N. Siddique, T. Shimamura, “Speech Enhancement Using Convolutional Denoising Autoencoder,” *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, IEEE, 2019.
- C10.** **Shaikh Akib Shahriyar**, K. M. Rokibul Alam, S. S. Roy, Y. Morimoto, “An Approach for Multi Label Image Classification Using Single Label Convolutional Neural Network,” *International Conference of Computer and Information Technology (ICCIT)*, IEEE, 2018.
- C11.** **Shaikh Akib Shahriyar**, M. A. Golap, M. S. Sadi, “An Efficient Error Correction Approach by Using Successive Parity Generation,” *International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT)*, IEEE, 2018.
- C12.** S. S. Roy, **Shaikh Akib Shahriyar**, M. Asaf-Uddowla, K. M. R. Alam, Y. Morimoto, “A Novel Encryption Model for Text Messages Using Delayed Chaotic Neural Network and DNA Cryptography,” *International Conference of Computer and Information Technology (ICCIT)*, IEEE, 2017.

Archival Posters

-
- P1.** **Shaikh Akib Shahriyar**, Ben Brown, Armon Barton, Ning Zhang, Matthew Wright, “How Many Queries Does It Take to Break a Deepfake Detector? Preliminary Findings from a Cost-Aware Robustness Audit,” *35th USENIX Security Symposium*, 2026.
 - P2.** **Shaikh Akib Shahriyar**, Matthew Wright, Armon Barton, “DiffTranPure: Diffusion Transformer-based Adversarial Purification to Extract Face and Facial Soft-Biometric Features from Obfuscated Images,” *33rd USENIX Security Symposium*, 2024.

Research Contributions

Practical robustness under realistic attacker access. Developed cost-aware security evaluations that connect adversarial success to transferability, query budgets, attacker access, and preserved utility across deepfake-detector families. **U1, P1, C3.**

Task-preserving security evaluation for tool-using agents. Developed executable task contracts that distinguish task identity from evaluation admissibility and fixed-trajectory rescoring methods that isolate how membership assumptions affect reported agent-security conclusions. **U2**.

Adversarial attacks and defenses for multimodal perception. Developed and evaluated attacks on image, video, and audio authentication systems, with diffusion-transformer purification defense for adversarial faces. **C1, C2, P2**.

Boundary shaping for robust neural networks. Contributed to PadNet’s defense design and adaptive evaluation using a learned barrier class and gradient regularization. **J1**.

Research Experience

Graduate Research Assistant

ESL Global Cybersecurity Institute, Rochester Institute of Technology

Advisor: Matthew Wright

Aug. 2020 – Present

Rochester, NY

- Developed **RobustDF**, a research framework for measuring and strengthening deepfake-detector robustness under white-box, black-box, transfer, query-bounded, and defense-adaptive attacks.
- Developed the **Practical Robustness Frontier (PRF)**, a cost-aware evaluation framework that relates attack success to adversary access, interaction/query budgets, transferability, and preserved utility across twelve deepfake detectors from four architectural families.
- Developed an executable **task-contract framework for tool-using agents**, separating specified task identity from evaluation admissibility; evaluated representation proxies and fixed-trajectory rescoring in controlled agent environments.
- Developed and evaluated adversarial defenses including diffusion-transformer purification and boundary shaping, and extended adversarial analysis to audio anti-spoofing and multimodal security.
- Collaborated across RIT, the Naval Postgraduate School, and partner institutions on adversarial machine learning, synthetic-media forensics, trustworthy AI, and secure agent evaluation.

Sponsored Research Contributions

VARUNA: A User-Centered All-in-One Media Forensics Platform

2025 – Present

Research Contributor; National Science Foundation Award 2429835; **\$1.5M total award** (\$1.125M to RIT).

Contribute adversarial-robustness and deepfake-detection research to a multi-institutional platform for journalists and forensic analysts.

Deepfake Detection for Journalists / DeFake Project

2020 – Present

Research Contributor; supported by the National Science Foundation and the John S. and James L. Knight Foundation, including a **\$200,000 Knight Foundation award**.

Developed adversarial evaluations and robustness methods for usable, interpretable media-forensics tools within a program with more than **\$2M** in combined support.

Research Methods and Technical Expertise

Adversarial ML & AI Security

Threat modeling; white-box, black-box, transfer, query-bounded, and adaptive attacks; robustness benchmarking; adversarial training; BPDA/EOT; boundary shaping; diffusion purification.

Agentic AI Security

Tool-using agents; indirect prompt-injection evaluation; task contracts; perturbation validity; authorization-aware evaluation; fixed-trajectory rescoring; AgentDojo; tool- and state-based attack surfaces.

Multimodal & Generative AI

Deepfake and audio anti-spoofing; vision, audio, and multimodal evaluation; diffusion and transformer models; LLM-diffusion workflows; evaluator models; provenance, consistency, and safety evaluation.

Research Engineering

Python, PyTorch, TensorFlow, Keras, Scikit-learn, OpenCV, Diffusers, NumPy, Pandas, Docker, Git, Jupyter, AWS/GCP; reproducible experiments and collaborative research codebases.

Professional Research Experience

Lead Machine Learning Research Engineer

SmartRoad.AI, Remote via Upwork

Jun. 2019 – Dec. 2020

Vitry-sur-Seine, France

Led a four-engineer team developing automatic number-plate recognition and manipulated-plate detection; achieved 98% detection accuracy and reduced inference time by 47% for edge deployment.

Teaching Experience

CSEC 720: Deep Learning Security

Spring 2023, Spring 2025

Rochester Institute of Technology

Rochester, NY

Instructor; graduate course with 25 M.S. and junior Ph.D. students. Designed lectures, reproducible laboratories, assessments, and research projects in adversarial ML, privacy, and robust learning.

CSEC 140: Introduction to Cybersecurity

Fall 2022, Fall 2026

Rochester Institute of Technology

Rochester, NY

Instructor; approximately 30 students. Taught threats, risk, cryptography, systems, networks, privacy, and secure computing.

Machine Learning; Computer Security; Mobile Computing; Software Engineering; Computer Networks; Algorithm Analysis & Design

Khulna University of Engineering & Technology

Khulna, Bangladesh

Instructor; approximately 120 students across multiple sections per course; combined lectures, laboratories, projects, and advising.

Artificial Intelligence; Neural Networks and Fuzzy Systems; Software Engineering; Computer Networks; Algorithm Analysis & Design

North Western University

Khulna, Bangladesh

Instructor; approximately 40 students per course.

Machine Learning; Computer Networks

Govt. Teachers' Training Institute

Khulna, Bangladesh

Instructor; approximately 20 K-12 teachers per course.

Student Mentoring

Ph.D. Student(s)

- Ben Brown, Ph.D. Student in Electrical and Computer Engineering, RIT.
- Y. Kelly Wu, Ph.D. Student in Computing and Information Sciences, RIT.
- Bryce Gernon, Ph.D. Student in Computing and Information Sciences, RIT.
- Ishmam Bin Rofi, Ph.D. Student in Computing and Information Sciences, RIT.
- Akil Iftee, Ph.D. Student in Computing and Information Sciences, RIT.

BS/MS Student(s)

- Anurag Mishra, MS in Data Science, RIT.
- Rajat Sahay, MS in Data Science, RIT.
- Matt Emerick, BS/MS in Cybersecurity, RIT.
- Robert McCall, BS/MS in Cybersecurity, RIT.
- Trevor Jarrett, BS in Cybersecurity, RIT.
- Christopher Sorrentino, BS in Cybersecurity, RIT.
- Oleksandr Maniukhin, BS in Cybersecurity, RIT.
- Shane Russell, BS in Cybersecurity, RIT.
- Meghan Briskey, BS in Cybersecurity, RIT.
- Jonathan Ho, BS in Cybersecurity, RIT.
- Shree Kumar, BS in Cybersecurity, RIT.
- Aidan Morgan, BS in Cybersecurity, RIT.
- Alexander Kilroy, BS in Cybersecurity, RIT.
- Griffin Vella, BS in Cybersecurity, RIT.
- Alexander Noble, BS in Cybersecurity, RIT.
- Jeffrey Burke, BS in Cybersecurity, RIT.
- Evelyn Gerber, BS in Cybersecurity, RIT.
- Jared Korwatch, BS in Cybersecurity, RIT.
- Anushka Tilara, BS in Cybersecurity, RIT.

Undergraduate Research and Capstone Advising

Khulna University of Engineering & Technology

Mentored more than 65 students and co-authored 7 student-led peer-reviewed publications in machine learning, computer vision, security, speech processing and blockchain systems.

2017 – 2023

Khulna, Bangladesh

Selected Talks and Presentations

-
- | | |
|-----------|--|
| Sep. 2026 | When Accuracy Is Not Security: Measuring and Improving Practical Robustness in Deepfake Detection. GCCIS PhD Colloquium Series, Rochester Institute of Technology, Rochester, NY. |
| Aug. 2026 | How Many Queries Does It Take to Break a Deepfake Detector? Preliminary Findings from a Cost-Aware Robustness Audit. Poster, 35th USENIX Security Symposium, Baltimore, MD. |
| May 2025 | Towards Trustworthy Deepfake Detection: Systematizing Adversarial Robustness and Charting Future Defenses. Doctoral Consortium, IEEE FG, Clearwater, FL. |
| Aug. 2024 | DiffTranPure: Diffusion Transformer-based Adversarial Purification to Extract Face and Facial Soft-Biometric Features from Obfuscated Images. Poster, 33rd USENIX Security Symposium, Philadelphia, PA. |
| Jan. 2023 | Adversarial ML to Adversarial Deepfakes: Attacks and Countermeasures. Guest talk, CSEC 720 Deep Learning Security, Rochester Institute of Technology. |

Awards and Honors

-
- | | |
|---|------|
| Prime Minister Gold Medal of Bangladesh; ranked first in the Faculty of Electrical and Electronic Engineering, KUET. | 2017 |
| President Gold Medal of Bangladesh; ranked first in the Department of Computer Science and Engineering, KUET. | 2017 |
| Best Student Poster Award, UPSTAT, Rochester, NY. | 2023 |
| Best Student Poster Award, IEEE Western New York Image and Signal Processing Workshop. | 2021 |

Professional Service

-
- | | |
|-------------------------------|--|
| Program Committee (PC) | International Conference on Autonomous Agents and Multiagent Systems (AAMAS) 2027 |
| Program Committee (PC) | IEEE International Conference on Automatic Face and Gesture Recognition (FG) 2026, 2027 |
| Program Committee (PC) | EAI International Conference on Digital Forensics and Cyber Crime (ICDF2C) 2020-2023 |
| Reviewer | International Conference on Autonomous Agents and Multiagent Systems (AAMAS) 2027 |
| Reviewer | IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2026 |
| Reviewer | IEEE International Conference on Automatic Face and Gesture Recognition (FG) 2025-2027 |
| Reviewer | IEEE Transactions on Dependable and Secure Computing (TDSC) |
| Reviewer | ACM Transactions on Privacy and Security (TOPS) |
| Reviewer | IEEE Access |
| Reviewer | International Journal of Electronics and Communications (IJECE) |
| Reviewer | EAI International Conference on Digital Forensics and Cyber Crime (ICDF2C) 2020-2022 |
| Reviewer | IEEE International Conference on Technology for Education (TCCE), 2020. |
| Academic Leadership | Vice President, Doctoral Student Association, Rochester Institute of Technology, 2022-2025; coordinated professional-development programming and conference-participation awards for Ph.D. students. |