Mohammad Saidur Rahman

Assistant Professor

msrahman3@utep.edu +1-(915) 747-5882 rahmanmsaidur.com

Appointments

Assistant Professor — September 2024 –
University of Texas at El Paso (UTEP) — *El Paso, TX*

Security Research Intern — June 2023 – June 2024
Cisco Quantum Lab, Cisco — *Los Angeles, CA*
Manager: Stephen DiAdamo, Former Manager: Alireza Shabani

Graduate Research Assistant — January 2017 – May 2024
Rochester Institute of Technology — *Rochester, NY*

Adjunct Faculty — January 2023 – May 2023
Rochester Institute of Technology — *Rochester, NY*

Networking Bell Labs Summer Intern — June 2021 – August 2021
Nokia Bell Labs — *Murray Hill, NJ*
Manager: Randeep Bhatia

Data Science Intern — June 2020 – August 2020
Mandiant (now part of Google) — *Reston, VA*
Manager: Scott Coull, Mentor(s): Philip Tully and Ethan Rudd

Education

Ph.D. in Computing & Information Sciences — 2018 – 2024
Rochester Institute of Technology, Rochester, NY.
Adviser: Matthew Wright
Thesis: Continual Learning for an Ever Evolving and Intelligent Malware Classification System

MS in Computing Security — 2016 – 2018
Rochester Institute of Technology, Rochester, NY.
Adviser: Matthew Wright
Thesis: Using Packet Timing Information in Website Fingerprinting

Bachelor's in Management Information Systems — 2012 – 2016
University of Dhaka, Dhaka, Bangladesh.

Selected Publications (Google Scholar)

Journal Articles

J1. **MS Rahman**, M Imani, N Mathews, M Wright,"Mockingbird: Defending Against Deep-Learning-Based Website Fingerprinting Attacks with Adversarial Traces," *IEEE Transactions on Information Forensics and Security (TIFS) 2021.*

J2. SE Oh, N Mathews, **MS Rahman**, M Wright, N. Hopper, "GANDaLF: GAN for Data-Limited Fingerprinting," *Privacy Enhancing Technologies Symposium (PETS) 2021.*

J3. **MS Rahman**, P Sirinam, N Mathews, KG Gangadhara, M Wright, "Tik-Tok: The Utility of Packet Timing in Website Fingerprinting Attacks," *Privacy Enhancing Technologies Symposium (PETS) 2020.*

Conference Proceedings

C1. Jimin Park, AHyun Ji, Minji Park, **MS Rahman**, SE Oh, "MalCL: Leveraging GAN-Based Generative Replay to Combat Catastrophic Forgetting in Malware Classification," *AAAI Conference on Artificial Intelligence (AAAI) 2025.*

C2. **MS Rahman**, Scott Coull, Qi Yu, M Wright, "MADAR: Continual Learning for Malware Analysis with Diversity-Aware Replay," *2025 (work in progress).*

C3. **MS Rahman**, S DiAdamo, M Mehic, C Fleming, "Quantum Secure Anonymous Communication Networks," *IEEE International Conference on Quantum Communications, Networking, and Computing (QCNC) 2024.*

C4. N Mathews, JK Holland, SE Oh, **MS Rahman**, N Hopper, M Wright, "SoK: A Critical Evaluation of Efficient Website Fingerprinting Defenses," *IEEE Symposium on Security and Privacy (IEEE S&P) 2023.*

C5. **MS Rahman**, Scott Coull, M Wright, "On the Limitations of Continual Learning for Malware Classification," *Conference on Lifelong Learning Agents (CoLLAs) 2022.*

C6. SE Oh, T Yang, N Mathews, JK Holland, **MS Rahman**, N Hopper, M Wright, "DeepCoFFEA: Improved Flow Correlation Attacks on Tor via Metric Learning and Amplification," *IEEE Symposium on Security and Privacy (IEEE S&P) 2022.*

C7. P Sirinam, N Mathews, **MS Rahman**, M Wright, "Triplet Fingerprinting: More Practical and Portable Website Fingerprinting with N-shot Learning," *ACM Conference on Computer and Communications Security (CCS) 2019.*

Workshops & Posters

WP1. Jimin Park, AHyun Ji, Minji Park, **MS Rahman**, SE Oh, "MalCL: Leveraging GAN-Based Generative Replay to Combat Catastrophic Forgetting in Malware Classification," *Annual Computer Security Applications Conference (ACSAC) 2024.*

WP2. EM Rudd, **MS Rahman**, P Tully, "Transformers for End-to-End InfoSec Tasks: A Feasibility Study," *ACM Workshop on Robust Malware Analysis (WoRMA) 2022.*

WP3. **MS Rahman**, Scott E. Coull, and M Wright, "Poster: Towards Continual Learning for Malware Classification," *IEEE Symposium on Security and Privacy (IEEE S&P) 2023.*

WP4. **MS Rahman**, N Matthews, and M Wright, "Poster: Video Fingerprinting in Tor," *ACM Conference on Computer and Communications Security (CCS) 2019.*

WP5. N Mathews, **MS Rahman**, and M Wright, "Poster: Evaluating Security Metrics for Website Fingerprinting," *ACM Conference on Computer and Communications Security (CCS) 2019.*

WP6. **MS Rahman**, M Imani, M Wright, "Adversarial Traces for Website Fingerprinting Defense," *ACM Conference on Computer and Communications Security (CCS) 2018.*

Patents

USPT1. E Kaur, S DiAdamo, C Fleming, MJ Kilzer, **MS Rahman**, P Zhao,"Hybrid Classical-Quantum Transmission for Eavesdropper Detection Over Classical Channels," *App: US18629095 (Pending)* .

USPT2. **MS Rahman**, S DiAdamo, M Mehic, C Fleming,"Quantum Secure Anonymous Communication Networks," *App: US18430099 (Pending)* .

Teaching Experience

CS-4390/5390: Quantum Information Science Spring 2025
Dept. of Computer Science, University of Texas at El Paso (UTEP) *El Paso, TX*

CS-5375: Software Reverse Engineering) Fall 2024
Dept. of Computer Science, University of Texas at El Paso (UTEP) *El Paso, TX*

Adjunct Faculty (CSEC-759 : Advanced Malware Forensics) Spring 2023
Dept. of Computing Security, Rochester Institute of Technology *Rochester, NY*

- Research seminar course designed to train students on i) ML and adversarial ML based malware research, and ii) malware analysis tools to perform dynamic, memory, and enterprise-level malware analysis.

Graduate Teaching Assistant Spring 2018, 2019, and 2020
Rochester Institute of Technology *Rochester, NY*
Courses: Deep Learning Security, Anonymity & Tor, Internet Security & Privacy.

- Developed Simulations: i) Timing Analysis of Network Traffic, ii) Website Fingerprinting with Deep Learning, iii) LSTM for Attack Prediction, and iv) Fooling a CNN with Adversarial Examples.

Student Advising and Mentoring

PhD Student(s)

- Md Ahsanul Haque, PhD Student in Computer Science, UTEP.

BS/MS Student(s)

- Jesus Lopez, BS/MS Student in Computer Science, UTEP.
- Eduardo Menendez, BS Student in Computer Science, UTEP.
- Viviana Cadena, BS Student in Computer Science, UTEP.

Graduated PhD, MS, and BS Students

- Mina Mahbub Hossain, PhD in Data Science, Utah State University, Logan, Utah.
- Sirapat Thianphan, MS in Cybersecurity, RIT.
- Kartavya Manojbhai Bhatt, MS in Computer Science, RIT.
- Kantha Girish Gangadhara, MS in Computer Science, RIT.
- Anmol Tiwari, MS in Computer Science, RIT.
- Md. Rakibul Hasan, MS in Computer Science, Morgan State University, Baltimore, Maryland.
- Perry Deng, BS in Computer Science, RIT.

- Jack Hyland, BS in Cybersecurity, RIT.
- Christian Halbert, BS in Cybersecurity, RIT.
- Tyler Zimmermann, BS in Cybersecurity, RIT.
- Lucas Christian, BS in Cybersecurity, RIT.
- Max Maurin, BS in Cybersecurity, RIT.
- Andrew Botschagow, BS in Cybersecurity, RIT.

Talks and Presentations

- Towards Continual Learning for Malware Analysis, Oklahoma State University 2024, Virtual.
- Machine Learning for Offensive and Defensive Network Security, NSF RET, UTEP 2024, El Paso, TX.
- Towards Continual Learning for Malware Analysis, RIT PhD Colloquium 2024, Rochester, NY.
- Machine Learning for Cyber Defense: From Network Security and Endpoint Security Perspectives, Cybersecurity Rising Star Symposium, IEEE COMSOC TCCN SIG in AI and Machine Learning in Security, 2024.
- On the Limitations of Continual Learning for Malware Classification, Conference on Lifelong Learning Agents (CoLLAs) 2022, Montreal, Canada.
- Transformers for end-to-end infosec tasks: A feasibility study, Workshop on Robust Malware Analysis (co-located with ACM AsiaCCS, 2022
- Brain-inspired Machine Learning for Malware Classification, Cybersecurity Healthy Arguments about Advancing The State-of-the-art (CHAATS), Rochester, NY.
- Mockingbird: Defending Against Deep-Learning-Based Website Fingerprinting Attacks with Adversarial Traces, RIT PhD Colloquium 2020, Rochester, NY.
- Tik-Tok: The Utility of Packet Timing in Website Fingerprinting Attacks, Privacy Enhancing Technologies Symposium (PETS) 2020, Virtual.
- Adv-DWF: Defending against deep-learning-based website fingerprinting attacks with adversarial traces, 8th Annual Conference of the Upstate New York Chapters of the American Statistical Association, 2019, Rochester, NY.
- Adversarial Traces for Website Fingerprinting Defenses, RIT Graduate Research Showcase 2017, Rochester, NY.
- Using Packet Timing in Website Fingerprinting Attacks, RIT Graduate Research Showcase 2017, Rochester, NY.

Selected Media Coverage

1. Blind Spots in AI Just Might Help Protect Your Privacy, WIRED. [URL]
2. How Can Blind Spots in AI Help Foster Online Privacy?, DATAFLOQ. [URL]
3. RIT cyber fighters go deep on Tor security, RIT News. [URL]
4. RIT cybersecurity research recognized at top computing conference in London, RIT News. [URL]

Awards & Grants

$ ***Travel Grant.*** Received travel grant from ACM CCS 2019

🏆 ***Bronze Medal Winner.*** 8th Annual Conference of the UPSTATE Chapters of the American Statistical Association, 2019.

🏆 ***Champion.*** Three-Minute Thesis Presentation Competition 2018 at Rochester Institute of Technology

🏆 ***Champion.*** Graduate Research Showcase 2017 at Rochester Institute of Technology

Professional Activities

Program Committee (PC). IEEE European Symposium on Security and Privacy (EuroS&P) 2025

Reviewer. International Conference on Learning Representations (ICLR) 2024

Program Committee (PC). Conference on Applied Machine Learning in Information Security (CAMLIS) 2024

Program Committee (PC). 21st Annual Scientific Computing with Python Conference (SciPy 2022)

Program Committee (PC). International Conference on Emerging Security Information, Systems and Technologies (SECURWARE) 2021 & 2022

Reviewer. IEEE Network Magazine

Reviewer. IEEE Transactions on Network and Service Management (TNSM)

Reviewer. IEEE Transactions on Information Forensics and Security (TIFS)

Reviewer. IEEE Transactions on Neural Networks and Learning Systems (TNNLS)

Reviewer. IEEE Transactions on Dependable and Secure Computing (TDSC)

Reviewer. Security and Communication Networks Journal

External Reviewer. Privacy Enhancing Technologies Symposium (PETS) 2021 & 2022

Reviewer. Computers & Security Journal

Reviewer. USENIX Security 2021 Artifact Evaluation Committee

Reviewer. IEEE Access