Mohammad Saidur Rahman

3rd Year Ph.D. Student

saidur.rahman@mai.rit.edu +1-585-284-4652 rahmanmsaidur.com msrocean Rochester, NY.

Education

Ph.D. in Computing & Information Sciences **CGPA: 3.95/4.00**
Rochester Institute of Technology *August 2018 – Present*
Courses: Deep Learning for Vision, Sensor and SCADA Security, Cyberinfrastructure Foundations, Quantitative Foundations

MS in Computing Security **CGPA: 3.88/4.00**
Rochester Institute of Technology *August 2016 – August 2018*
Courses: Penetration Testing, Network Security, Internet Security & Privacy, Computer Systems Security, Cryptography & Authentication, Machine Learning

Bachelors in Management Information Systems **CGPA: 3.76/4.00**
University of Dhaka *January 2012 – July 2016*
Courses: Programming Fundamentals, Programming for Information Systems, Data Communication, Database Systems Management, Project Management, Telecommunications, Decision Support Systems, Statistics, Matematics I & II

Research Interests

Privacy Enhancing Technologies, Traffic Analysis, Malware Analysis, Deep Learning, Lifelong Learning (Continual Learning), and Adversarial Machine Learning.

Experience

Graduate Research Assistant January 2017 – Present
Global Cybsersecurity Institute (Center for Cybsesecurity), Rochester Institute of Technology *Rochester, NY*

- Investigating vulnerabilities in network traffic using deep-learning techniques.
- Investigating defenses against website fingerprinting attacks.
- Investing intelligent malware detection systems.

Data Science - Cybersecurity Intern June 2020 – August 2020
FireEye Inc. *Reston, VA*

- Static malware analysis and detection using natural language processing based models.
- Analysing the entropy of malware raw bytes sequences and investigating data compression techniques to compress malware raw bytes sequence.

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.

Selected Publications

[2021] **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.*

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

[2020] **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.*

[2019] 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.*

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

[More] Google Scholar.

Technical Skills

Languages: Python, C, MATLAB, C++ (basic), Java (basic), Bash
Machine Learning & Deep Learning: TensorFlow, Keras, PyTorch, CNN, RNN, LSTM, Capsule Network, AE, NLP, Transformer, k-NN, SVM, RDF, Numpy, Sklearn, Scipy, Matplotlib, Jupyter Notebook, Jupyter Hub
Security Tools: CobaltStrike, Armitage, Metasploit-Framework, Nmap, Netcat, Cryptcat Socat, OpenVAS, Nessus, Snort
Networking: TCP, UDP, BGP, VLAN, Access Control, Firewalls, IDS, IPS
Operating Systems: Ubuntu, Kali Linux, CentOS, Red Hat Linux, Linux Mint, XUbuntu, Windows

Academic Projects

[**Fall 2018**] Generating Adversarial Packets for Website Fingerprinting Defense.
[**Spring 2018**] Cybersecurity Report of Intel Corporation.
[**Fall 2017**] Optimizing Smart Grid Aggregators and Measuring Degree of Privacy in a Distributed Trust Based Anonymous Aggregation System.
[**Spring 2017**] Evaluation of Input Data Representations of Website Fingerprinting Attack on Deep Learning Performance.
[**Spring 2017**] Evaluation of SVM and k-NN in Website Fingerprinting Attack.
[**Spring 2017**] Password Hash Cracking Using Amazon Web Service (AWS) Elastic Compute Cloud (EC2).
[**Fall 2016**] Implementation of DHCP Failover methodology within the Dominican Republic's small businesses & organizations information technology platform.

Certifications

Mathematics for Machine Learning Specialization Coursera
- Linear Algebra, Multivariate Calculus, Principle Component Analysis (PCA)

Deep Learning Specialization Coursera
- Neural Networks and Deep Learning, Improving Deep Neural Networks: Hyperparameter tuning, Regularization and Optimization, Structuring Machine Learning Projects, Convolutional Neural Networks, Sequence Models

Awards & Grants

CCS 2019 Travel Grant. Received travel grant from ACM CCS 2019 to attend the event
Bronze Medal Winner 2019. 8th Annual Conference of the UPSTATE Chapters of the American Statistical Association
Winner 2018. Three-Minute Thesis Presentation Competition 2018 at Rochester Institute of Technology
Winner 2017. Graduate Research Showcase 2017 at Rochester Institute of Technology

Activities

Reviewer. USENIX Security 2021 Artifact Evaluation Committee
Reviewer. IEEE Access