MD TAMJID HOSSAIN

CISSP and Ph.D. Computer Science and Engineering

Email : tamjid.m.hossain@gmail.com GitHub: Personal | Google Scholar

Mobile: +1 (775) 200 3959 Website: Personal | LinkedIn

BRIEF INTRODUCTION

Md Tamjid Hossain is an expert privacy and security researcher. His research interest involves *secure and trustworthy AI/ML applications, adversarial machine learning, federated learning, reinforcement learning, Blockchain, critical infrastructure security,* etc. He has **authored/co-authored 8+ papers** in top conferences and journals (IROS2023, ICMLC2023, ISGT NA2023, CNS2021, MSN2021, CPSCom2021, IEMTRONICS2021, etc.). He has also served as a **reviewer for 12+** major conferences and journals (ICRA2024, ICRA2023, IEEE IoT, TII, TDSC, Sensors, etc.). He is a key member of the *Advanced Robotics and Automation (ARA) laboratory* at the University of Nevada, Reno, and currently leading **2 grant proposal** preparation work for DoD (AFOSR) DEPSCoR ($600K/3yrs) and NSF SaTC ($1.2 Million/4yrs) program. Besides he has **mentored 500+ UNR undergraduate students** over the academic year 2020 to 2023. As a recognition of his leadership abilities, exemplary organizational skills, and collaborative approach to technical problem-solving, Mr. Hossain received prestigious awards including the 2023 GSA Travel Grant, and 2016 Grameenphone's Best Employee Awards.

EDUCATION

- **Ph.D.** in Computer Science and Engineering (Concentrated in AI/ML Cybersecurity), University of Nevada, Reno, USA | *January 2020 - May 2024* | Dissertation Topic: *Privacy and Security for Trustworthy AI/ML in Multi-Agent Critical Infrastructures: An Analysis of Adversarial Dynamics and Protective Strategies* | Advisor*:* Dr. Hung La
- **MS** in Computer Science and Engineering, University of Nevada, Reno | *January 2020 - May 2022* | Thesis*: Analysis of Privacy-Aware Data Sharing in Cyber-Physical Energy Systems* [Online] | Advisor: Dr. Hung La
- **BS** in Electrical and Electronic Engineering, Chittagong University of Engineering and Technology, Bangladesh | March 2010 - *October 2014* | Thesis: *Design and Development of automatic and load control system of a cable-propelled transit* | Advisor*:* Dr. Nipu Kumar Das

GRANT PROPOSAL

- Assisted in grant proposal preparation titled "*ARMOR: Adversarial Robust Multi-agent Optimization and Resilience for Coordinated Adaptive Learning*" for DoD's (AFOSR) DEPSCoR program for FY2023, award amount: $600K/3yrs, PI: Dr. Hung La, Co-PI: Dr. Ali Reza Tavakkoli.
- Assisted in grant proposal preparation titled "*AGILE-MC: Adaptive Generative Integrated Learning Environment for Multi-agent Coordination*," for NSF's Secure and Trustworthy Cyberspace (SaTC) program, award amount: $1.2 Million/4yrs, PI: Dr. Hung La.

PROFESSIONAL EXPERIENCE

Graduate Research and Teaching Assistant | *January 2020 – August 2024*

Advanced Robotics and Automation (ARA) Lab | University of Nevada, Reno (UNR), Nevada, USA

- Led ARA lab's data privacy and information systems research as a Ph.D. candidate, supported by NSF, from Dec. 2022. Focusing on data science, artificial intelligence, cyber security measures, secure and private data communication, risk assessment, risk control, and security compliance of critical infrastructure.

- Developed novel adversarial machine learning techniques, poisoning attacks and defense strategies, Blockchain, and Differential Privacy (DP) algorithms to enhance multi-agent systems' data privacy & security.
- Conducted Threat Modeling, Ethical Hacking, Risk Analysis, and IT Risk Management, adhering to standards such as NIST CSF, ISO/IEC 27032, and information privacy and regulation.
- Dedicated 1000+ hours to Python programming for research and class projects, resulting in the publication and presentation of 8+ peer-reviewed articles in reputable conferences/journals, including IEEE/RSJ IROS 2023, ACM JATS, IEEE ICMLC 2023, IEEE CNS 2021, MSN 2021, CPSCom 2021, and ISGT NA 2023.
- Served as a reviewer for 12+ scholarly articles in conferences/journals (e.g., ICRA, IEEE IoT, TII, TDSC, etc.).
- Mentored and guided 500+ students as a teaching assistant (TA). Responsible for teaching courses: **Computer Communication Network (CPE 400/600)** and **Digital Design (CPE 201)** at the CSE Department of UNR.
- Mentored undergraduate students, illuminating research and learning avenues at UNR. Steered potential graduate students to forge meaningful relationships with advisors during their Gradventures and On-campus visits, and outreach. Collaborated with professors to design course curriculum development and grant proposals.

Lead Engineer | *December 2014 – June 2020*
Operation Support System (OSS), Service Operations | Grameenphone Limited, Dhaka, Bangladesh

- Spearheaded the industry research: the development of security measures, ensuring the telecommunication network's reliability and information assurance through engineering support, collaboration, verbal and written communication, and coordination with stakeholders in an ethical manner.
- Initiated the idea and collaborated with cross-functional teams to lead the 'Smart Configuration Management, Scripting, and Auditing' project that saved 1152+ man-hours and $20k Operational Expenses per annum.
- Developed Python scripts for auto-capturing the graphical user interface (GUI) of Grameenphone's web services to enable real-time traffic and network speed monitoring, resulting in a 54% man-hour reduction.

TEACHING SUMMARY WITH EVALUATION (Role: Teaching Assistant)					
No	Semester	Course taught	Number of enrollments	Overall eval of teaching	Department mean
7	Fall 2023	CPE201: Digital Design (Lab: 1102+1101)	37+37	3.70/4	-
6	Spring 2023	CPE201: Digital Design (Lab: 1102+1101)	39+35	2.71/4	2.78/4
5	Fall 2022	CPE201: Digital Design (Lab: 1101+1102)	41+41	2.86/4	2.80/4
4	Spring 2022	CPE400/600: Computer Comm. Network	73	-	-
3	Fall 2021	CPE400/600: Computer Comm. Network	82	-	-
2	Spring 2021	CPE400/600: Computer Comm. Network	64	-	-
1	Fall 2020	CPE400/600: Computer Comm. Network	90	-	-

TECHNICAL SKILLS

- Programming/Coding: C, C++, Python, PHP, MySQL
- Data Tools: NumPy, Pandas, PyTorch, Matplotlib, Tableau
- Cybersecurity: Threat and Risk Analysis, NMAP, Wireshark, Zeek, IP Tables, Vulnerability Assessment
- ML Techniques: Machine Learning, Deep Learning, Reinforcement Learning, Federated Learning model
- Tools & Software: GitHub, Microsoft Office Suite, Slack
- OS & Server: Windows, Linux, Unix (Mac), Oracle VM VirtualBox
- Enterprise Security: Identity Access Management, Authentication, Endpoint Security, User Administration
- Others: Data Analysis, Visualization, Version Control, Dashboard Preparation

MAJOR PUBLICATIONS

Google Citation (since 2020): 88, h-index: 04, i10-index: 03

Peer-reviewed Conference Paper (published)**:**

1. M. T. Hossain, H. La, and S. Badsha, "RAMPART: Reinforcing Autonomous Multi-agent Protection through Adversarial Resistance in Transportation," ACM Journal on Autonomous Transportation Systems (ACM JATS), 2023 (Undergoing minor revision). GitHub Link
2. M. T. Hossain, H. M. La, and S. Badsha, "BRNES: Enabling Security and Privacy-aware Experience Sharing in Multiagent Robotic and Autonomous Systems," ***The 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2023)*** (Accepted for publication). Paper Link
3. M. T. Hossain, and H. M. La, "Hiding in Plain Sight: Differential Privacy Noise Exploitation for Evasion-resilient Localized Poisoning Attacks in multiagent Reinforcement Learning," ***The International Conference on Machine Learning and Cybernetics (ICMLC), 2023***. Paper Link
4. S. Islam, I. Zografopoulos, M. T. Hossain, S. Badsha, C. Konstantinou, "A Resource Allocation Scheme for Energy Demand Management in 6G-enabled Smart Grid," ***IEEE ISGT NA***, **2023**. Paper Link
5. M. T. Hossain, S. Badsha and H. Shen, "Privacy, Security and Utility Analysis of Differentially Private CPES Data," ***9th IEEE Conference on Communications and Network Security (IEEE CNS 2021)***, 2021. Paper Link
6. M. T. Hossain, S. Islam, S. Badsha, and H. Shen, "DeSMP: Differential Privacy-exploited Stealthy Model Poisoning Attacks in Federated Learning," ***17th International Conference on Mobility, Sensing and Networking (IEEE MSN 2021)***, 2021. Paper Link
7. A. Bhattacharjee, S. Badsha, M. T. Hossain, C. Konstantinou, and X. Liang, "Vulnerability Characterization and Privacy Quantification for Cyber-Physical Systems," ***2021 IEEE International Conference on Cyber, Physical and Social Computing (IEEE CPSCom-2021)***, 2021. Paper Link
8. M. T. Hossain, S. Badsha, and H. Shen, "PoRCH: A Novel Consensus Mechanism for Blockchain-Enabled Future SCADA Systems in Smart Grids and Industry 4.0," ***2020 IEEE International IOT, Electronics and Mechatronics Conference (IEEE IEMTRONICS)***, 2020, pp. 1-7, Doi: 10.1109/IEMTRONICS51293.2020.9216438. Paper Link

Peer-reviewed Journal (undergoing major revision)**:**

9. M. T. Hossain, H. La, and S. Badsha, " Exploiting Gaussian Noise Variance for Dynamic Differential Poisoning in Federated Learning," IEEE Transactions on Artificial Intelligence (IEEE TAI), 2024," (Undergoing major revision). GitHub Link

Conference/Journal paper (submitted/under review):

10. G. Srikar, M. T. Hossain, and H. La, "CRADLE: Cooperative Adaptive Decentralized Learning and Execution for UAV network to monitor Wildfire Front," ***2024 IEEE International Conference on Robotics and Automation (ICRA 2024)***. *[Rejected]* GitHub Link

Conference/Journal paper (to be submitted):

11. G. Srikar, M. T. Hossain, and H. La, "Multi-UAV Collaborative Deep Learning and Consensus to Maximize Coverage Over Continuous and Dynamic Wildfire Environment".
12. M. T. Hossain, S. Sengupta, S. Badsha, and H. La, "Game of Trade-off in Differential Privacy".

PRESENTATION/TALKS

13. 01st-05th October 2023, Detroit, USA. **Topic:** *Security and Privacy-aware experience sharing in multi-agent systems,* **Organizer:** The 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2023).

14. 9th-11th July 2023, The University of Adelaide, Australia. **Topic:** *Localized poisoning in multi-agent reinforcement learning,* **Organizer:** The 22nd International Conference on Machine Learning and Cybernetics (ICMLC)

15. 13th-15th December 2021, Virtual (Zoom). **Topic:** *Model poisoning attacks in Federated Learning,* **Organizer:** 2021 17th International Conference on Mobility, Sensing, and Networking (MSN)

16. 4th-6th October 2021, Virtual (Zoom). **Topic:** *Privacy, security, and utility analysis of Differential Privacy (DP),* **Organizer:** IEEE Conference on Communications and Network Security (CNS).

1. 9th-12th September 2020, Vancouver, Canada. **Topic:** *Lightweight Blockchain Technology for Industrial Control Systems (ICSs),* **Organizer:** International IOT, Electronics and Mechatronics Conference (IEMTRONICS 2020).

MAJOR RESEARCH AND DEVELOPMENT PROJECTS

Analysis of adversarial AI/ML systems in multi-agent cyber-physical critical infrastructures

- Developed novel experience sharing for multiagent reinforcement learning (MARL): defined adaptive neighbor zone, performed weighted experience aggregation, and implemented Local Differential Privacy (LDP).

Privacy, security, and vulnerability characterization and quantification in cyber-physical energy systems (CPES)

- Identified backdoor attack vulnerability through novel adversarial noise distribution technique, and designed reinforcement learning (RL)-based privacy level selection strategies for DP algorithms.

Lightweight Blockchain framework for supervisory control and data acquisition (SCADA) systems

- Developed a lightweight, computationally efficient, and scalable consensus protocol for Blockchain-driven SCADA systems, which is also extendible to cryptocurrencies, vehicular networks, and/or healthcare systems.

Smart configuration management, scripting, and auditing tool

- End-to-end solution for generating & executing scripts in multiple servers, validating and tuning network parameters for inconsistencies after re-homing the Ericsson & Huawei-based BTSs using Python, and MySQL.

MAJOR TRAININGS

- 30 hours - CCNA Routing & Switching Exploration Training-IICT, CUET, BD - 3/1/2013 to 4/30/2014.
- 15 hours - Mathematical Analysis: Linear Algebra, Optimization, and Learning - UNR - 2/4/2020 to 4/30/2022.
- 3.45 hours - Network data analysis using Wireshark, Zeek, Socket - UNR - 3/17/2020 to 3/24/2020.
- 13 hours - Encryption, Message Authentication, Digital Signature, Hashing - UNR - 8/24/2020 to 11/19/2020.
- 5.9 hours - Hardware Security Training on Side Channel and Poisoning Attacks - UNR - 2/8/2021 to 2/22/2021.
- 10.35 hours - Machine Learning: Designing Neural Network, PCA, SVM - UNR - 8/23/2021 to 10/25/2021.
- 30 hours - Cybersecurity Disciplines and Frameworks - UNR - 8/30/2022 to 12/9/2022
- 28 hours - FTK Imager 4.2.1 by Access Data for Digital Forensics - UNR - 9/6/2022 to 12/9/2022

HONORS/AWARDS:

- 'GSA Travel Award' by University of Nevada, Reno, NV, USA | *August 2023*
- 'Best Employee' Award by Grameenphone Limited, Dhaka, Bangladesh | *November 2016*

ACTIVITIES

- IEEE Graduate Student Member | *December 2021 – 2024*
- Founding President, Car Lovers of UNR | *September 2021 – August 2022*