**MD TAMJID HOSSAIN, CISSP, Ph.D.**
Assistant Professor (Tenure-track)
Department of CEMS, College of Arts and Sciences
Texas A&M University-San Antonio (TAMU-SA)

**Official Email:** mhossain@tamusa.edu
**Official Phone:** 210-784-2369
Official Website | LinkedIn
GitHub | Google Scholar

## CAREER SUMMARY

Md Tamjid Hossain is a privacy and security expert currently serving as an Assistant Professor (Tenure-track) of Computer Science and Cybersecurity at Texas A&M University-San Antonio (TAMU-SA). His research interests include *secure and trustworthy AI/ML applications*, *adversarial machine learning*, *federated learning*, *reinforcement learning*, *blockchain*, and *critical infrastructure security*. He has authored/co-authored **10+** papers published in top conferences and journals, including IROS 2023, ICMLC 2023, ISGT NA 2023, CNS 2021, MSN 2021, CPSCom 2021, and IEMTRONICS 2021. Dr. Hossain has also served as a reviewer for **15+** major conferences and journals, such as ICRA 2024, ICRA 2023, IEEE IoT, TII, TDSC, and Sensors. During his time as a PhD candidate in the *Advanced Robotics and Automation (ARA) Laboratory* at the University of Nevada, Reno, he contributed to two (02) **grant proposal** preparation efforts: the DoD (AFOSR) DEPSCoR program ($600K/3 years; PI: *Dr. Hung La*, Co-PI: *Dr. Alireza Tavakkoli*) and the NSF SaTC program ($1.2M/4 years; *PI: Dr. Hung La).*

In addition to his research accomplishments, Dr. Hossain has mentored **700+** undergraduate and graduate students at UNR and TAMU-SA from 2020 to 2024. He is also an active member of the TAMU-SA **Faculty Search Committee**. His leadership skills, organizational abilities, and collaborative approach to technical problem-solving have been recognized with prestigious awards, including the 2023 GSA Travel Grant and the 2016 Grameenphone Best Employee Award.

## EDUCATION

- University of Nevada, Reno (UNR), NV, USA
  - Ph.D. in Computer Science and Engineering (Specialized in Cybersecurity and Data Privacy) | *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 | *May 2022*
    *Thesis:* Analysis of Privacy-Aware Data Sharing in Cyber-Physical Energy Systems | *Advisor*: Dr. Hung La
- Chittagong University of Engineering and Technology (CUET)
  - BS in Electrical and Electronic Engineering | *October 2014*
    *Project:* Design and Development of automatic and load control system of a cable-propelled transit | *Advisor: Dr. Nipu Kumar Das*

## PROFESSIONAL WORK AND RESEARCH EXPERIENCE

- **Assistant Professor (Tenure-track) |** *September 2024 - Present*
  Department of Computational, Engineering, and Mathematical Sciences (CEMS)
  College of Arts and Sciences
  Texas A&M University-San Antonio, Texas
  - Mentoring undergraduate and graduate students in their research, coursework, and career development.
  - Performing research and scholarly work in areas including cybersecurity, trustworthy AI, and critical infrastructure systems.
  - Preparing external research grant proposals to contribute to the growth of the department's research capacity.
  - Teaching core and advanced courses in Computer Science and Cybersecurity— advancing student engagement through innovative and hands-on learning approaches.
  - Collaborating with interdisciplinary teams to produce high-impact publications and conference presentations.
  - Developing new course curricula to align with emerging trends in technology and industry needs.
  - Serving on departmental and university committees to support academic programs and institutional initiatives.

- **Ph.D. Candidate & Graduate Research and Teaching Assistant** | *January 2020 – May 2024*
  Advanced Robotics and Automation (ARA) Lab
  University of Nevada, Reno (UNR), Nevada
  - 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 10+ peer-reviewed articles in reputable IEEE conferences, including IEEE/RSJ IROS 2023, IEEE ICMLC 2023, IEEE CNS 2021, MSN 2021, CPSCom 2021, and ISGT NA 2023.
  - Served as a reviewer for 12+ scholarly articles in top-notch conferences/journals (e.g., ICRA, IEEE IoT, TII, TDSC, Sensors, SMC, etc.).
  - Mentored and guided 500+ students as 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, Technology Division
  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** | Role: Asst. Prof. (Fa.2024-Present), TA (Fa.2020 – Sp.2024)

| No | Semester | Course taught | Number of enrollments |
|---|---|---|---|
| **10** | Spring 2025 | CSEC/CISA-4323: Computer Forensics | 36 |
| | | CSEC-5311/CETE-4392: Big Data Analysis & Security | 11 |
| **9** | Fall 2024 | CSCI-3366: Programming Languages | 48 |
| | | CISA-4323: Computer Forensics | 17 |
| | | CSEC-4323/5310: Advanced Computer Forensics | 35 |
| **8** | Spring 2024 | CPE201: Digital Design (Lab: 1102+1101) | 36+33 |
| **7** | Fall 2023 | CPE201: Digital Design (Lab: 1102+1101) | 37+37 |
| **6** | Spring 2023 | CPE201: Digital Design (Lab: 1102+1101) | 39+35 |
| **5** | Fall 2022 | CPE201: Digital Design (Lab: 1101+1102) | 41+41 |
| **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 |

## GRANT PROPOSAL

- Assisted in writing grant proposal titled "**ARMOR: Adversarial Robust Multi-Agent Optimization and Resilience for Coordinated Adaptive Learning**" intended for *The Defense Established Program to Stimulate Competitive Research (DEPSCoR)* program of DoD for FY2023, PI: Dr. Hung La, Co-PI: Dr. Alireza Tavakkoli
- Assisted in writing grant proposal titled "**SENTRY: Secure Neuroadaptation in Trustworthy Reinforcement System**" intended for *Secure and Trustworthy Cybersecurity (SaTC)* program of National Science Foundation (NSF) for FY2023, PI: Dr. Hung La

## MAJOR RESEARCH AND DEVELOPMENT PROJECTS

***Analysis of adversarial AI/ML Systems in 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).
- Developed novel poisoning attacks and defenses using intelligent privacy level selection in Federated Learning.

***Privacy, Security, and Vulnerability Characterization and Quantification in Cyber-physical Energy Systems***

- 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 PUBLICATIONS

- **M. T. Hossain**, et al., "Exploiting Gaussian Noise Variance for Dynamic Differential Poisoning in Federated Learning," IEEE Transactions on Artificial Intelligence (IEEE TAI), 2024. (Under Major Review)
- **M. T. Hossain**, et al. 2024. RAMPART: Reinforcing Autonomous Multi-Agent Protection through Adversarial Resistance in Transportation. ACM J. Auton. Transport. Syst. https://doi.org/10.1145/3643137
- **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).
- **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.
- 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).
- **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 (CNS), 2021.
- **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.
- A. Bhattacharjee, S. Badsha, **M. T. Hossain**, C. Konstantinou and X. Liang, "Vulnerability Characterization and Privacy Quantification for Cyber-Physical Systems," submitted in the 2021 IEEE International Conference on Cyber, Physical and Social Computing (IEEE CPSCom-2021), 2021.
- **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 (IEMTRONICS), 2020, pp. 1-7, doi: 10.1109/IEMTRONICS51293.2020.9216438.

## PRESENTATION/TALKS

- *Security and Privacy-aware experience sharing in multi-agent systems*, The 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2023), 01st-05th October 2023, Detroit, USA (upcoming).
- *Localized poisoning in multi-agent reinforcement learning*, The 22nd International Conference on Machine Learning and Cybernetics (ICMLC), 9th-11th July 2023, The University of Adelaide, Adelaide, Australia.
- *Model poisoning attacks in Federated Learning*, 2021 17th International Conference on Mobility, Sensing, and Networking (MSN), 13th-15th December 2021, Virtual conference.
- *Privacy, security, and utility analysis of Differential Privacy (DP)*, IEEE Conference on Communications and Network Security (CNS), 4th-6th October 2021, Virtual conference.
- *Lightweight Blockchain Technology for Industrial Control Systems (ICSs)*, International IOT, Electronics and Mechatronics Conference (IEMTRONICS 2020), 9th-12th September 2020, Vancouver, Canada.

## TECHNICAL SKILLS

- **Programming/Coding**: 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 TRAININGS

- 30 hours - CCNA Routing & Switching Exploration Training-IICT, CUET, BD - 3/1/13 to 4/30/14.
- 15 hours - Mathematical Analysis: Linear algebra, Optimization, learning theory - UNR - 2/4/20 to 4/30/22.
- 13 hours - Encryption, Message Authentication, Digital Signature, Hashing - UNR - 8/24/20 to 11/19/20.
- 5.9 hours - Hardware Security Training on Side Channel and Poisoning Attacks - UNR - 2/8/21 to 2/22/21.
- 10.35 hours - Machine Intelligence: Designing Neural Network, PCA, SVM - UNR - 8/23/21 to 10/25/21.
- 30 hours - Cybersecurity Disciplines and Frameworks - UNR - 8/30/22 to 12/9/22
- 28 hours - FTK Imager 4.2.1 by Access Data for Digital Forensics - UNR - 9/6/22 to 12/9/22

## CERTIFICATIONS

**Certified Information Systems Security Professional (CISSP)**

**Certification Number:** 2004136
**Issuing Authority:** International Information System Security Certification Consortium (ISC2)
**Issued Date:** June 01, 2024
**Certification Link:** https://www.credly.com/badges/0548a7f4-c717-4ff7-8aa0-e067484d857f

## HONORS/AWARDS

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

## ACTIVITIES

- IEEE Graduate Student Member | *December 2021 – Present*
- Founding President, Car Lovers of UNR | *September 2021 – August 2022*
- Co-founder and General Secretary, ASRRO, CUET | *February 2013 – June 2014*