MD. SAZEDUR RAHMAN

Ph.D. Researcher | Secure Federated Learning | Cybersecurity for Autonomous & Mining Systems

Rolla, Missouri, USA | rahman.mdsazedur49@gmail.com | +15736472108 | Google Scholar | LinkedIn | Portfolio

RESEARCH PROFILE

Computer Science Ph.D. researcher at Missouri University of Science and Technology working with Prof. Dr. Sanjay Madria in the Wireless and Cloud Computing Laboratory. Research focuses on trustworthy distributed intelligence for safety-critical environments, including federated learning security, adversarial machine learning, autonomous underground mining,backdoor attacks and defenses.

RESEARCH INTERESTS

Secure and Trustworthy AI; Federated Learning; Adversarial Machine Learning; Cybersecurity for Cyber-Physical Systems; Autonomous Mining; Edge/IoT Intelligence; Computer Vision; Privacy-Preserving Learning; Backdoor and Data-Poisoning Defense.

EDUCATION

Ph.D. in Computer Science | *Missouri University of Science and Technology* [August 2023- Present]

- Advisor: Prof. Dr. Sanjay Madria; Wireless and Cloud Computing (W2C) Laboratory.
- Passed the Ph.D. Qualifying Examination, April 16, 2025.
- Coursework: Network Security, Data Mining, Algorithms, Clustering, Applied SNA,Advanced AI, and Bioinformatics.

B.Sc. in Computer Science and Engineering | *Khulna University of Science and Technology* [January 2018- February 2023]

- CGPA 3.80/4.00 (class position 8th)
- Advisor: Prof. Dr. K.M Azharul Hasan.
- Thesis Title:Computing Skyline Query on Incomplete Data.

SELECTED PUBLICATIONS

1. **Md. Sazedur Rahman**, Sanjay Madria, Samuel Frimpong, *Label-Flip Attack Detection via Trust-Weighted Aggregation in Federated Learning for Underground Mine Security*, ACM DEBS, 2026.
2. **Md. Sazedur Rahman**, Mohamed Elmahallawy, Sanjay Madria, Samuel Frimpong, *Detecting Untargeted Attacks and Mitigating Unreliable Updates in Federated Learning for Underground Mining Operations*, IEEE MASS, 2025.
3. **Md. Sazedur Rahman**, Mohamed Elmahallawy, Sanjay Madria, Samuel Frimpong, *CAV-AD: A Robust Framework for Detection of Anomalous Data and Malicious Sensors in CAV Networks* , IEEE MASS, 2024.
4. **Md. Sazedur Rahman**, M. R. Jewel, Sanjay Madria, *Future Mining: Learning for Safety and Security*,COMSNETS, 2026.

RESEARCH EXPERIENCE

Graduate Research Assistant | *Missouri S&T—W2C Laboratory* August 2023-Present

- Developed TrustFed, an unsupervised trust-weighted aggregation framework for detecting label-flip attacks in non-IID federated learning without trusted server data.
- Developed MINEDETECT,a history-aware method to identify untargeted attacks and unreliable mine clients.

MineSigns Dataset and FL Testbed | *Missouri S&T Experimental Mine* 2025

- Created a 13-class underground safety-sign dataset from five mine videos; annotated objects in CVAT and prepared YOLO-format splits.

TECHNICAL SKILLS

Languages: Python, C, C++, Java, Assembly
Machine Learning: Federated learning, deep learning, clustering, adversarial ML, vision-language models,knowledge

distillation
Security: Poisoning defense, backdoor analysis, robust aggregation, Paillier encryption, functional encryption
Tools and Frameworks: PyTorch,Tensorflow,scikit-learn, Git/GitHub, Linux, LaTeX,CVAT

PRESENTATIONS AND SERVICE

- Author Presenter, IEEE MASS 2025, Chicago.
- Poster Presenter, STL CyberCon 2025.
- Author Presenter, IEEE MASS 2024, Seoul, South Korea.
- Poster Presenter, STL CyberCon 2025.

AWARDS

- Best Poster Award -NextGen Precision Health [March 2026]
- Best Poster Award -STL CyberCon 2024[Nov 2024]
- Best Paper Award- BIM 2023