Mahbub Alam

mahbub.alam@tamu.edu | +1 (315) 949-9277 | itsmahbub.github.io | linkedin.com/in/alam-mahbub

PROFESSIONAL PROFILE

PhD student in Computer Science at Texas A&M focusing on **AI Safety & Security** (adversarial attacks, hallucination, jailbreaks, prompt injection) and **AI for Cybersecurity** (phishing, scams, social engineering, deepfakes). Experienced in phishing/scam detection and fuzzing-based frameworks for AI vulnerability detection, with 5+ years of industry experience in cloud infrastructure, DevOps, and large-scale systems reliability.

EDUCATION

Texas A&M University, PhD in Computer Science (CGPA: 4.0/4.0) — Aug 2024–May 2028 (expected)

Bangladesh University of Engineering and Technology, BSc in CSE (CGPA 3.5/4.0) — Feb 2013–Sep 2017

RESEARCH EXPERIENCE

Graduate Assistant – Research, SPIES Lab, Texas A&M University — Aug 2024–Present

- Develop a multi-agent LLM framework for evaluating AI fuzzing and phishing detection literature, yielding two SoK papers under review (NDSS, USENIX Security 2026).
- Analyze large-scale toll scam datasets to uncover attacker infrastructure patterns, resulting in a paper accepted at eCrime 2025.
- Build a fuzzing-based benchmarking framework for evaluating AI security and robustness, exposing vulnerabilities in vision/speech models and extending to LLM threats (hallucination, prompt injection, jailbreaks, misalignment).

Graduate Research Assistant, SYNE Lab, Syracuse University — Aug 2023–Jun 2024

- Developed iConPAL, an LLM tool translating natural language IoT policies into formal specs, published at IEEE SecDev 2024.
- Mentored an undergraduate student (co-author on published paper).

PUBLICATIONS

- **M. Alam**, S. Zhang, E. Rodriguez, A. Nafis, and E. Hoque. “iConPAL: LLM-guided Policy Authoring Assistant for Configuring IoT Defenses.” *IEEE Secure Development Conference (SecDev),* Pittsburgh, PA, 2024.
- M. A. Munny, **M. Alam**, S. K. Paul, D. Timko, M. L. Rahman, and N. Saxena. “Infrastructure Patterns in Toll Scam Domains: A Comprehensive Analysis of Cybercriminal Registration and Hosting Strategies.” *APWG Symposium on Electronic Crime Research (eCrime)*, San Diego, CA, USA, 2025 **(*to appea*r**).

SELECTED PROJECTS

Malware Detection (Course Project) – Champion (Defense), 2nd Runner-Up (Attack) — Texas A&M, Fall 2024

- Designed and implemented machine learning-based malware detection approaches for a competitive class project.
- Source code: github.com/itsmahbub/malware-detector

AI Model Fuzzing Framework – Research Prototype — SPIES Lab, Aug 2024–Present

- Developed a fuzzing-based benchmarking framework exposing vulnerabilities in vision and speech models, with planned extensions to LLM safety and security.

INDUSTRY EXPERIENCE

Cloud Engineer (2019-2021) | Senior Cloud Engineer (2021-2022) | Senior Site Reliability Engineer (2022-2023)

Intuitive Web Solutions (BriteCore), Remote — Aug 2019–Jul 2023

- Integrated Datadog with AWS to enhance monitoring, automate failure recovery, and reduce infrastructure costs by 10%.
- Developed a multi-tenant search app with AWS Elasticsearch, supporting multiple clients and products.
- Implemented infrastructure as code with AWS CDK and CloudFormation.

Software Engineer | Field Information Solutions Ltd, Dhaka — May 2018–Jul 2019

- Developed API endpoints for a sales distribution app, refactored legacy code for reusability, and resolved client-reported issues.

Junior Software Engineer | REVE Systems, Dhaka — Oct 2017–Apr 2018

- Built a code generation script for project skeletons and fixed bugs in production systems.

LEADERSHIP & SERVICE

General Secretary, Computer Science & Engineering Graduate Student Association (CSEGSA), Texas A&M — Sep 2024–Present

TRAINING & CERTIFICATIONS

AWS Solutions Architect – Pro, AWS DevOps Engineer – Pro,Certified Kubernetes Administrator, Linux Foundation SysAdmin

AWARDS

2nd Runner-Up, Software Project Show, 2nd International Conference on Networking Systems and Security, 2016

SKILLS

Deep Learning, Multi-agent LLM orchestration, AI Security, PyTorch, TensorFlow, AWS, Docker, Terraform, Python, C/C++, Java.