## 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 Security** and **AI for Cybersecurity**. 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–Present (Expected Graduation: 12/2028)
**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
• Designed PHILTER, an LLM-assisted evaluation framework to uncover security and functional gaps in phishing detection; SoK accepted at USENIX Security 2026.
• Designed a large-scale analysis framework to uncover infrastructure and registration patterns in toll scam domains; accepted at APWG eCrime 2025.
• Designed TransFuzz, a coverage-guided DNN security testing framework to uncover targeted and untargeted adversarial vulnerabilities in vision and speech models; under review.
• Designed AI-FLARE, an LLM-assisted evaluation framework to uncover diagnostic, functional, and generality gaps in AI model fuzzing; under review.
**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.
• Explored LLM-assisted Linux kernel fuzzing using LLM-generated C programs validated with LLVM.
• Mentored an undergraduate student (co-author on published paper).

### PUBLICATIONS

• **M. Alam**, M. L. Rahman, S. K. Paul, A. W. Hays, A. Hussain, M. I. Huq, and N. Saxena. "PHILTER: Uncovering Security and Functional Gaps in AI-based Phishing Website Detection Literature via an LLM-based Reasoning Framework." *35th USENIX Security Symposium*, Baltimore, MD, USA, 2026 ***(to appear)***.
• 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.
• **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.

### SELECTED PROJECTS

**Malware Detection (Course Project) – Champion (Defense), 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

### 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%.
• 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–Aug 2025

### TRAINING, CERTIFICATIONS, & AWARDS

AWS Solutions Architect – Pro, AWS DevOps Engineer – Pro,Certified Kubernetes Administrator, Linux Foundation SysAdmin
2nd Runner-Up, Software Project Show, 2nd International Conference on Networking Systems and Security, 2016

### SKILLS

Python, C/C++, Java, Data Structures & Algorithms, Deep Learning, AI Security, PyTorch, TensorFlow, AWS, Docker, Terraform.