Mahbub Alam

L.F. Peterson Building, Room 230, Texas A&M University, College Station, TX
mahbub.alam@tamu.edu | +1 (315) 949-9277 | itsmahbub.github.io | linkedin.com/in/alam-mahbub

EDUCATION

Doctor of Philosophy in Computer Science Fall 2024 – Present
Texas A&M University, College Station, TX
Advisor: Dr. Nitesh Saxena

Bachelor of Science in Computer Science and Engineering 2013 – 2017
Bangladesh University of Engineering and Technology, Dhaka, Bangladesh

RESEARCH INTERESTS

AI Safety and Security, LLM Robustness and Red-Teaming, Adversarial Machine Learning, Phishing Detection, Software Supply-Chain Defense, and Predatory Research Detection.

RESEARCH EXPERIENCE

LLM-Assisted Literature Analysis for Security Research 2024 – Present
Texas A&M University

- Developed an LLM-assisted reasoning framework for systematic literature analysis across multiple security research problems.
- Applied this framework to analyze more than 50 studies on AI-based phishing website detection, identifying security and functional gaps and resulting in a top-tier publication.
- Applied the framework to analyze more than 30 studies on DNN fuzzing, revealing key limitations in existing approaches to AI security failure discovery.
- Extending this line of work to predatory research detection and research compliance analysis.

Coverage-Guided Fuzzing for AI Security 2024 – Present
Texas A&M University

- Developed TransFuzz, a coverage-guided DNN fuzzing framework based on perturbation-centric cross-input mutation that addresses key limitations of prior DNN fuzzers in input plausibility, failure reproducibility, and exploration efficiency.
- Extending this approach to LLMs and AI agents to discover vulnerabilities such as jailbreaks, backdoor behaviors, and prompt injection attacks.

PUBLICATIONS

Conference Papers

C_3 [**USENIX Security 2026**] **Mahbub Alam**, Muhammad Lutfor Rahman, Sonjoy Kumar Paul, Amy W. Hays, Aftab Hussain, Md Imanul Huq, and Nitesh Saxena. *"PHILTER: Uncovering Security and Functional Gaps in AI-based Phishing Website Detection Literature via an LLM-based Reasoning Framework."* In the 35th USENIX Security Symposium, 2026 (to appear).

C_2 [**eCrime 2025**] Morium Akter Munny, **Mahbub Alam**, Sonjoy Kumar Paul, Daniel Timko, Muhammad Lutfor Rahman, and Nitesh Saxena. *"Infrastructure Patterns in Toll Scam Domains: A Comprehensive Analysis of Cybercriminal Registration and Hosting Strategies."* In the APWG Symposium on Electronic Crime Research (eCrime), 2025.

C_1 [**SecDev 2024**] **Mahbub Alam**, Siwei Zhang, Eric Rodriguez, Akib Nafis, and Endadul Hoque. *"iConPAL: LLM-guided Policy Authoring Assistant for Configuring IoT Defenses."* In the IEEE Secure Development Conference (SecDev), 2024.

Under Review

U_2 **Mahbub Alam**, Aftab Hussain, and Nitesh Saxena. *"TransFuzz: Coverage-Guided DNN Fuzzing via Cross-Input Perturbation Mutation."*

U_1 **Mahbub Alam**, Aftab Hussain, Sonjoy Kumar Paul, Amy W. Hays, Md Imanul Huq, and Nitesh Saxena. *"SoK: FUZZCHECK.AI: On the Limitations of DNN Fuzzing to Discover Security Failures."*

PROFESSIONAL EXPERIENCE

Graduate Assistant – Research Aug 2024 – Present
Texas A&M University, College Station, TX

- Led research on AI-based phishing detection, analyzing 50+ studies to uncover security and functional gaps, resulting in a USENIX Security publication.
- Developed a coverage-guided DNN fuzzing framework for discovering vulnerabilities in machine learning systems, grounded in large-scale analysis of prior work.

Graduate Research Assistant Aug 2023 – Jun 2024
Syracuse University, Syracuse, NY

- Led a research project on using LLMs to translate natural-language IoT policies into formal security specifications, resulting in a peer-reviewed publication.

Senior Site Reliability Engineer Aug 2019 – Jul 2023
Intuitive Web Solutions (BriteCore), Remote
Progression: Cloud Engineer → Senior Cloud Engineer → Senior Site Reliability Engineer

- Collaborated with security, development, and support teams to strengthen AWS security controls and maintain cloud infrastructure reliability.
- Integrated Datadog with AWS to improve monitoring and automate failure recovery, contributing to a 10% infrastructure cost reduction.
- Implemented infrastructure as code using AWS CDK and CloudFormation.

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

- Developed API endpoints for a sales distribution application, refactored legacy modules for reuse, and resolved client-reported issues.

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

- Built an automated code-generation script for project scaffolding, reducing setup time and improving developer productivity.
- Resolved critical bugs in production systems to improve reliability and stability.

SERVICE

Sub-reviewer

[1] **The Web Conference (WWW)** 2025

AWARDS

[1] **2nd Runner-Up, Software Project Show** 2016
2nd International Conference on Networking Systems and Security, Bangladesh

PROFESSIONAL DEVELOPMENT & CERTIFICATION

[6] **Texas A&M Systems – AI Security Learning Experience + Cisco AI Defense CTF** 2026
Placed 5th, World Wide Technology Cyber Range

[5] **GCRI & Akamai Network Security Workshop** 2026
Texas A&M University

[4] **AWS Certified Solutions Architect – Professional** 2022
Issued by Amazon Web Services

[3] **CKA: Certified Kubernetes Administrator** 2022
Issued by The Linux Foundation

[2] **LFCS: Linux Foundation Certified Systems Administrator** 2022
Issued by The Linux Foundation

[1] **AWS Certified DevOps Engineer – Professional** 2021
Issued by Amazon Web Services

LEADERSHIP EXPERIENCE

[1] **Secretary, Computer Science & Engineering Graduate Student Association** 2024 – 2025
Texas A&M University, College Station, TX